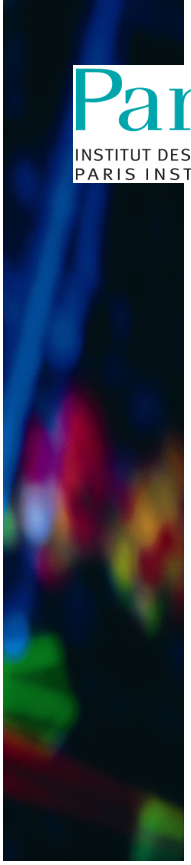
Boolean functions, algebraic curves and complex multiplication

Jean-Pierre Flori



ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2012-ENST-003

EDITE de Paris

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

Télécom ParisTech

Spécialité "Informatique et Réseaux"

présentée et soutenue publiquement par

Jean-Pierre FLORI

le 3 février 2012

Fonctions booléennes, courbes algébriques et multiplication complexe

Directeur de thèse : **Gérard COHEN**
Directeur de thèse : **Hugues RANDRIAM**

Jury

M. Gary MCGUIRE, Professeur Associé, University College Dublin	Rapporteur
M. Igor SHPARLINSKI, Professeur, Macquarie University	Rapporteur
M. Andreas ENGE, Directeur de Recherche, INRIA Bordeaux-Sud-Ouest & IMB	Examinateur
Mme Sihem MESNAGER, Maître de Conférence, Université de Paris VIII	Examinatrice
M. Benjamin SMITH, Chargé de Recherche, INRIA Saclay-Île-de-France & LIX	Examinateur
M. Nicolas M. THIÉRY, Maître de Conférence, Université Paris Sud	Examinateur
M. Gérard COHEN, Professeur, Télécom ParisTech	Directeur de Thèse
M. Hugues RANDRIAM, Maître de Conférence, Télécom ParisTech	Directeur de Thèse

T H È S E

Télécom ParisTech
Grande école de l'Institut Télécom — membre fondateur de ParisTech
46, rue Barrault — 75634 Paris Cedex 13 — Tél. + 33 (0)1 45 81 77 77 — www.telecom-paristech.fr

Boolean functions, algebraic curves and complex multiplication

Jean-Pierre Flori

To Choupi

Abstract

The core of this thesis is the study of some mathematical objects or problems of interest in cryptology. As much as possible, the author tried to emphasize the computational aspects of these problems. The topics covered here are indeed not only favorable to experimental investigations, but also to the quasi direct translation of the mathematical concepts involved into concrete algorithms and implementations.

The first part is devoted to the study of a combinatorial conjecture whose validity entails the existence of infinite classes of Boolean functions with good cryptographic properties. Although the conjecture seems quite innocuous, its validity remains an open question. Nonetheless, the author sincerely hopes that the theoretical and experimental results presented here will give the reader a good insight into the conjecture.

In the second part, some connections between (hyper-)bent functions — a subclass of Boolean functions —, exponential sums and point counting on (hyper)elliptic curves are presented. Bent functions and hyper-bent functions are known to be difficult to classify and to build explicitly. However, exploring the links between these different worlds makes possible to give beautiful answers to theoretical questions and to design efficient algorithms addressing practical problems.

The third and last part investigates the theory of (hyper)elliptic curves in a different direction. Several constructions in cryptography indeed rely on the use of highly specific classes of such curves which can not be constructed by classical means. Nevertheless, the so-called "complex multiplication" method solves some of these problems. Class polynomials are fundamental objects for that method, but their construction is usually considered only for maximal orders. The modest contribution of the author is to clarify how a specific flavor of their construction — the complex analytic method — extends to non-maximal orders.

Résumé

Le cœur de cette thèse est l'étude d'objets ou de problèmes mathématiques intéressants en cryptologie. Autant que possible, l'auteur a essayé de mettre en avant les aspects calculatoires de tels problèmes. Les thèmes traités ici sont en effet non seulement propices aux approches expérimentales, mais aussi à une transposition quasiment immédiate des concepts mathématiques en implémentations concrètes.

La première partie de cette thèse est dévolue à l'étude d'une conjecture combinatoire dont la validité assure l'existence de familles infinies de fonctions booléennes dotées de propriétés cryptographiques intéressantes. Quoique particulièrement innocente au premier abord, la validité de cette conjecture reste un problème ouvert. Néanmoins, l'auteur espère que les résultats théoriques et expérimentaux présentés ici permettront au lecteur d'acquérir un tant soit peu de familiarité avec la conjecture.

Dans la seconde partie de ce manuscrit, des liens entre fonctions (hyper-)courbes — une classe particulière de fonctions booléennes —, sommes exponentielles et courbes (hyper)elliptiques sont présentés. Les fonctions (hyper-)courbes sont en effet particulièrement difficiles à classifier et à construire. L'étude des liens mentionnés ci-dessus permet de résoudre de façon élégante des problèmes d'ordre tout aussi bien théorique que pratique.

La troisième et dernière partie pousse plus avant l'étude des courbes (hyper)elliptiques d'un point de vue sensiblement différent. De nombreuses constructions cryptographiques reposent en effet sur l'utilisation de classes particulières de telles courbes qui ne peuvent être construites en utilisant des méthodes classiques. Cependant, la méthode CM permet de donner une réponse positive à ce problème. Les polynômes de classes sont des objets fondamentaux de cette méthode. Habituellement, leur construction n'est envisagée que pour des ordres maximaux. La modeste contribution de l'auteur est d'expliciter comment une telle construction — la méthode analytique complexe — s'étend aux ordres non-maximaux.

Acknowledgments

> Vladimir. — Quand j'y pense... depuis le temps... je me demande... ce que tu serais devenu... sans moi... (*Avec décision.*) Tu ne serais plus qu'un petit tas d'ossements à l'heure qu'il est, pas d'erreur.
>
> *En attendant Godot*
> Samuel Beckett [11]

> Le Niolo est le bassin supérieur du Golo, en amont du défilé de la Scala di Santa Regina. Large cuvette granitique d'une alt. moyenne de l'ordre de 900 m, dominée au N. par le chaînon du Cinto et au S. par les crêtes qui le séparent de la haute vallée du Tavignano, c'est une région très nettement délimitée qui, avant l'ouverture de la route D84 (ex RF9), n'était accessible que par quelques cols franchis par des sentiers muletiers et bloqués par la neige une partie de l'année. Ce réel isolement par rapport au reste de l'île a fortement marqué la population du Niolo au cours des siècles et lui a conféré une certaine originalité qui se manifeste encore de nos jours dans différents domaines.
>
> *Guide des montagnes corses*
> Michel Fabrikant [88]

I shall first thank both my Ph.D. advisors — Gérard Cohen and Hugues Randriam — without whom this work would have never been possible: you have let me wander in the directions I wanted for three years, and I will always be grateful to you for the wonderful ideas we shared together and that liberty you gave me. Next comes Sihem Mesnager who was kind enough to share her research interests and collaborate with me. Much of the content of this thesis would have been far different if I did not have the chance to meet you. I also had the chance to collaborate with Hervé Chabanne and Alain Patey from Morpho even though no trace of this work appears in the present memoir. As a rather fortunate consequence of this collaboration, I was forced to take my first step on the South-American continent. I am also extremely grateful to Gary McGuire and Igor Shparlinski who accepted to go through the hassle of reading this memoir and to write a report, as well as to Andreas Enge, Nicolas M. Thiéry and Benjamin Smith who accepted to be part of my defense jury. I should not forget the former and current members of the MIC2 team: David Auger and Céline Chevalier with whom I shared my office and my days; David

Madore, Bertrand Meyer and Jacques Sakarovitch who answered my silly questions; and finally Irène Charon, Laurent Decreusefond, Olivier Hudry, Antoine Lobstein and Süleyman Üstünel. From the INFRES department, I also have a thought for Jean Leneutre and Ahmed Serhrouchni — you once saved my computer during one of my lonely Sunday afternoons at Télécom ParisTech. To go on with the scientific aspect of these past three years, I must also thank the fellow members of the "Groupe de Travail de la Butte aux Cailles" — Alain Couvreur, Luca De Feo and Jérôme Plût — for keeping my modest initiative alive for more than two years. I have the feeling that we even managed to build something more than a purely mathematical relation. Finally, I can not omit my new colleagues from the ANSSI: Loïc Duflot, Olivier Levillain, and the members of the "Laboratoire de Cryptographie" — Aurélie Bauer, Thomas Fuhr, Henri Gilbert, Jean-René Reinhard, Yannick Seurin, Joana Treger–Marim. You have warmly welcomed me and offered me exceptional conditions to finish the writing of this manuscript. I hope that the near future will see the beginning of a long lasting collaboration between us.

On the technical side, I guess most of the work I conducted during the past three years would have not been possible without the use of a wide spectrum of free and open source software among which I will only mention a few: the Debian operating system, the LaTeX typesetting system, the GNU Compiler Collection and the Sage project. I will do my best to contribute back to these projects. I am also grateful to the maintainers of the `arxiv.org` and `iacr.org` preprint servers and the numerous authors making their results freely available there. A particular thought goes to the wonderful math webpage of J.S. Milne: this is a goldmine for course notes.

To conclude, I must say that I could not have survived throughout these three years in a purely mathematical world. The bo-buns I ate with Chico and Bertrand; the concerts I attended with Clément; the exotic countries and high routes I traveled with Moche, Rod, Titi and Val; the beers I shared with my fellow comrades from the École Polytechnique and the BôBar — Baptiste, Milpatte and Tipiak — and my old fellow comrades from the Lycée Pasteur and elsewhere — Bousty, Flavien, Franz, Guillaume, Jérémy, Olivier and Victor. On a more personal note, I would like to thank the extended Debarre family — Anne, Becky, Benoît, Clélia, Fanfette, François, Jacques, Magali, Olivier and Paul — for welcoming me into their world. The same must definitely be said for my family — my grandmother, my mother, my uncle Albert and my sister, who bravely brought back stinking cheese from Corsica, despite the interrogative looks of the bus driver. And last but not least comes Marianne who has put up with me and my stupid ideas for all these years.

Contents

List of figures

List of tables

List of algorithms

List of symbols and notation

General

Combinatorics

Boolean functions

$\mathrm{AI}(f)$	Algebraic immunity of f	10
$\deg(f)$	Algebraic degree of f	10
$\mathrm{d_H}(f,g)$	Hamming distance between f and g	11
$\mathrm{nl}(f)$	Nonlinearity of f	11
$\mathrm{supp}(f)$	Support of f	9
$\mathrm{w_H}(f)$	Hamming weight of f	9
f, g	Boolean functions	8

Tu–Deng conjecture

α_i	Size of the i-th subblock of `1`'s of t	35
β_i	Size of the i-th subblock of `0`'s of t	35
$C_{t,k,i}$	Set of modular integers producing $\mathrm{w_H}(t)-i$ carries	29
δ_i	Number of `1`'s in front of the end of the `0`'s subblock of t.	35
ϵ_i	Number of carries not occurring in the i-th block of t while adding a	37
γ_i	Number of `0`'s in front of the end of the `1`'s subblock of t	35
$I_{t,k,i}$	Set of inert modular integers producing $\mathrm{w_H}(t)-i$ carries	80
$\mathcal{D}(\cdot)$	Diagonal of a double power series	73
$O_{t,k,i}$	Set of overflowing modular integers producing $\mathrm{w_H}(t)-i$ carries	81
$P_{t,k}$	Fraction of modular integers in $S_{t,k}$	29
$\mathrm{Res}(f,z)$	Residue of a complex-valued function f at z	73
$S_{t,k}$	Set of the Tu–Deng conjecture	29
$S_{t,v,u,k}$	Set of the generalized Tu–Deng conjecture	21
$\mathrm{w_H}(t)$	Hamming weight of t	21
$a \simeq b$	Cyclotomic equivalence for modular integers	22
$a^{d,n}_{(i_1,\ldots,i_n)}$	Coefficients for the closed-form expression of f_d	48
B	Number of `0`'s of t	35
d	Number of blocks of t	35
$f_d(\beta_1,\ldots,\beta_d)$	Function giving $P_{t,k}$ for a set of β_i's of size d	42
G_i, H_i	Geometrically distributed variables with parameter $1/2$	68
k	Exponent for modulus 2^k-1	21

Bent functions

Elliptic curves

$\langle P, Q \rangle_m$	Tate pairing	136
$\mathcal{L}$	Set of lattices in $\mathbb{C}$	140
$\mathcal{O}$	An order in a quadratic number field	103
$\mathcal{O}_K$	Maximal order of a quadratic number field K	105
$\otimes_{\mathbb{Z}}$	Tensor product of $\mathbb{Z}$-modules	103
$\widetilde{E}$	Reduction of E modulo a prime ideal	139
$\mathrm{SL}_2(\mathbb{Z})$	Special linear group	141
$\widetilde{E}$	Quadratic twist of an ordinary elliptic curve E	105
$\wp(z; \Lambda)$	Weierstraß $\wp$-function	142
$\mathbb{Z}_{p^n}$	Unramified extension of degree n of $\mathbb{Z}_p$	123
E	An elliptic curve	99
$E[n]$	Subgroup of n-torsion of E	103
$e_m(P, Q)$	Weil pairing	137
f	Conductor of an order	105
f_n	n-division polynomial of an elliptic curve	103
g	Genus of a hyperelliptic curve	106
$G_{2k}(\Lambda)$	Eisenstein series	142
H	A hyperelliptic curve	105
$H(\Delta)$	Kronecker class number for discriminant Δ	104
$h(\mathcal{O})$	Class number of an order $\mathcal{O}$	104
$H_{\mathcal{O}}$	Ring class field of $\mathcal{O}$	148
$H_{\mathcal{O}}(X)$	Hilbert class polynomial of $\mathcal{O}$	148
j	j-invariant of an elliptic curve	100
O_E	Point at infinity of E	100
$r(f)$	Reduction factor of a modular function f	153

Algebraic curves

$\deg(\phi)$	Degree of ϕ	133
$\deg(D)$	Degree of D	134
$\mathrm{Div}(C)$	Group of divisors of C	134
$\mathrm{Div}^0(C)$	Group of divisors of degree zero of C	134

$\mathrm{Frac}(\mathcal{O})$	Semigroup of fractional ideals of $\mathcal{O}$	143
$\mathbb{H}_g$	Siegel upper half-space of genus g	163
Λ	A lattice in V	161
N_Φ	Norm type associated with Φ	174
$\mathcal{O}$	An order in a number field K	168
$\mathcal{O}_K$	Maximal order of a number field K	168
$\widehat{A}$	Dual variety of A	164
$\omega(x, y)$	A Riemann form	162
$\widetilde{\mathcal{O}}$	Normalization, or integral closure, of $\mathcal{O}$	168
$\mathrm{PF}(\mathcal{O})$	Group of principal ideals of $\mathcal{O}$	144
$\mathrm{pf}(\omega)$	Pfaffian of ω	163
Φ	A CM type	173
$\mathrm{Pic}(\mathcal{O})$	Picard group of $\mathcal{O}$	144
$\mathrm{Pic}(A)$	Picard group of A	164
$\mathrm{Prop}(\mathcal{O})$	Semigroup of proper ideals of $\mathcal{O}$	144
ψ_L	Polarization associated with a line bundle L	165
$\mathrm{SP}_{2g}(\mathbb{Q})$	Symplectic group	166
$\theta(z)$	A theta function	161
Tr_Φ	Type trace associated with Φ	174
A	An abelian variety	161
E	A CM algebra	173
E^r	Reflex field of a CM algebra E	173
g	Dimension of an abelian variety	161
$H(\mathcal{O})$	Kronecker class number of $\mathcal{O}$	144
$H(x, y)$	A Hermitian form	162
$H^{prop}(\mathcal{O})$	Proper class number of $\mathcal{O}$	144
$L(H, \alpha)$	Line bundle associated with H and α	165
R	An order in a CM algebra E	174
$R(\Lambda)$	The multiplier ring of a lattice	140
$S_\mathcal{O}$	Normalization kernel of $\mathcal{O}$	170

Introduction

Beaucoup d'travail comme pour un album d'Astérix !

L'ère du Stup
Stupeflip [256]

Sed ut perspiciatis, unde omnis iste natus error sit uoluptatem accusantium doloremque laudantium, totam rem aperiam eaque ipsa, quae ab illo inuentore ueritatis et quasi architecto beatae uitae dicta sunt, explicabo. Nemo enim ipsam uoluptatem, quia uoluptas sit, aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos, qui ratione uoluptatem sequi nesciunt, neque porro quisquam est, qui dolorem ipsum, quia dolor sit, amet, consectetur, adipisci uelit, sed quia non numquam eius modi tempora incidunt, ut labore et dolore magnam aliquam quaerat uoluptatem. Vt enim ad minima ueniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur ? quis autem uel eum iure reprehenderit, qui in ea uoluptate uelit esse, quam nihil molestiae consequatur, uel illum, qui dolorem eum fugiat, quo uoluptas nulla pariatur ?

De finibus bonorum et malorum
Marcus Tullius Cicero [50]

Contents

1 Mathematics and cryptology

Cryptology is the art of secret and information security. Its most classical aspect is confidentiality: one wants to share some critical information with a selected number of people without anyone else being able to gain access to it. Nowadays, there are two typical ways to address this problem: symmetric cryptography where both legitimate parties share a common secret and use it to protect their exchanges; and asymmetric cryptography where only one party possesses such a secret. In the latter case, some public data are associated with the secret and make possible the secure transmission of information in a unique direction. Such dichotomies are quite common in cryptology.

For example, it is a more or less customary to divide the world of cryptology into two parts[1]. On the one hand, cryptography is the art of designing as robust and secure as possible algorithms, protocols and systems. On the other hand, cryptanalysis is the art of devising design flaws in such systems and developing attacks jeopardizing their alleged security. The more powerful and general the attacks developed by cryptanalysts are, the more difficult it is for cryptographers to propose suitable constructions. In particular, most cryptographic constructions rely somehow on the difficulty of mathematical problems, from theoretical and computational points of view, and the existence of related mathematical objects. Cryptology is therefore an inexhaustible source of mathematical problems. The motivation of the research presented in this memoir is to study and build mathematical objects verifying suitable properties to be used in a cryptographic context.

2 Computational experiments and implementation

Cryptology is all but a purely theoretical science. The formal study of cryptographic primitive is endowed with a mathematical formalism, but the final goal is to design or to attack concrete systems. Therefore, many problems arising in cryptology have fundamentally computational aspects.

To actually study these aspects, perform experiments and implement algorithms, the author had to choose some piece of software. To add another dichotomy to the previous ones, the author was basically faced with two alternatives: use well-known and robust proprietary software such as Maple [207] and Magma [23] or take the chance to use a quite recent and less polished open source software: Sage [250]. Practical and ethical reasons lead the author to choose the Sage software. The following citation from the Sage documentation describes quite well the philosophy of the project:

"Sage is free open source math software that supports research and teaching in algebra, geometry, number theory, cryptography, and related areas. Both the Sage development model and the technology in Sage itself are distinguished by an extremely strong emphasis on openness, community, cooperation, and collaboration: we are building the car, not reinventing the wheel."

Sage indeed provides an easy interface to already existing and mature open source softwares, as well as to proprietary software. It is conceived as an extension to Python [266], an interpreted language, but compiled code can also be easily generated using Cython [24]. It is therefore a particularly well crafted tool for teaching and experiments, not for record breaking implementations and computations. To this end, a natural choice would be to build a library in a low-level language such as C [148] which could be later interfaced back into Sage.

[1] Of course, one could argue it is not. It however seems to be in France.

3 Outline

The main matter of this thesis consists in three parts. Each part itself is built following the same scheme:

- a first preliminary chapter providing enough background for the unfamiliar reader to understand the next one;
- a second chapter presenting more advanced results and the contribution of the author to the subject.

Part I is devoted to the study of a combinatorial conjecture whose validity entails the existence of infinite classes of Boolean functions with satisfying cryptographic properties. In Chapter 1, some background on such Boolean functions is given, especially on those to be used as filtering functions in stream ciphers. The properties that such functions should meet — balancedness, algebraic degree, algebraic immunity, resistance to fast algebraic attacks and nonlinearity — are defined in Section 1.1. Infinite classes of Boolean functions satisfying these criteria are then described in Section 1.2. Two constructions are of particular interest: those of Tu and Deng [23] and of Tang, Carlet and Tang [259]. They are indeed the most closely linked with the combinatorial problem studied in Chapter 2. To tackle the original conjecture of Tu and Deng [23], later generalized by Tang, Carlet and Tang [259], it is first reformulated in terms of carries occurring in an addition modulo $2^k - 1$ in Section 2.1. Such an approach might at first seem quite down-to-earth, but the difficulty of the problem is precisely that no algebraic structure can be cast upon it. It is however sufficient for us to prove the specific case needed by the family of Tang, Carlet and Tang [259] in Section 2.2. The following sections are devoted to the original conjecture of Tu and Deng [23] whose validity remains an open problem. Nonetheless, by defining a suitable block splitting pattern in Section 2.4, structure enough is cast upon the problem to exhibit quite explicit forms for the quantities of interest in Section 2.5. This also provides a probabilistic interpretation in an asymptotic setting and entails the validity of the conjecture asymptotically as depicted in Section 2.6. This chapter is concluded by providing theoretical evidence that a naive inductive approach is not sufficient in Section 2.7 and experimental evidence that the conjecture is valid in low dimension in Section 2.9.

A more specific class of Boolean functions is studied in Part II: bent and hyper-bent functions. These are functions achieving maximal non-linearity, a criterion already mentioned above. To this end, Chapter 3 presents additional objects used in the study of such functions: the Walsh–Hadamard transform, binary exponential sums and Dickson polynomials in Section 3.1; but also the basic theory of elliptic and hyperelliptic curves over finite fields of even characteristic with a special emphasis on point counting on such curves in Section 3.2. In Chapter 4, these tools will indeed be used to give efficient characterizations of (hyper-)bent functions and design efficient algorithms to explicitly construct them. It is first recalled how the usual characterizations of bentness and hyper-bentness involving the Walsh–Hadamard transform are reformulated in terms of exponential sums in Section 4.1. Furthermore, such results are themselves reformulated in terms of cardinalities of (hyper)elliptic curves in Section 4.2. This fundamental observation leads to the design of efficient algorithms to test (hyper-)bentness of a given function and to actually construct such functions. The concluding sections cover this topic.

Part III, which concludes this memoir, departs from the world of Boolean functions and concentrates on (hyper)elliptic curves which were already introduced in the preceding part. More precisely, the theory of complex multiplication for such curves and the explicit computation of class polynomials using complex analytic methods are studied. The latter polynomials can indeed be used to build the former curves. Chapter 5 exposes the classical situation for curves of genus 1, i.e. elliptic curves, and serves as an introduction to the more involved following chapter. After

giving more general background on algebraic curves in Section 5.1, an alternate point of view is presented in Section 5.2 for the analytic case. Over the complex numbers, elliptic curves can indeed be described as complex tori. Such considerations lead to the main theorems of complex multiplication and the definition of the Hilbert class polynomial in Section 5.3. Some applications of such curves in the context of asymmetric cryptography are given in Section 5.4. The purpose of Chapter 6 is then to extend the results of Chapter 5 to higher dimension with an emphasis on the case of non-maximal orders which is usually dismissed for simplicity or concision. The structure of this chapter is essentially the same as that of the previous one. Section 6.1 provides superficial background on the algebraic and analytic theories of abelian varieties. The theory of fractional ideals in orders of number fields is presented in Section 6.2 where it is shown how class groups and units of non-maximal orders can be explicitly computed. Section 6.3 is devoted to the general theory of complex multiplication whereas Section 6.4 is restricted to dimension 2 and gives algorithms to compute class polynomials in that case — the Igusa class polynomials — for a potentially non-maximal order.

Part I

Boolean functions and a combinatorial conjecture

Chapter 1

Boolean functions in cryptography

> — [...] J'en reviens à notre livre de philosophie, c'est comme les principes rationnels, ou les lois scientifiques, la réalité se conforme à cela, à peu près, mais rappelle-toi le grand mathématicien Poincaré, il n'est pas sûr que les mathématiques soient rigoureusement exactes.
>
> *Le côté de Guermantes*
> Marcel Proust [221]

Contents

Boolean functions are a commonly used building block in the design of symmetric cryptosystems, especially in that of stream ciphers. Obviously, the properties of such functions are critical for the security requirements of the final system built upon them. If not carefully chosen, the use of a *weak* Boolean function can indeed jeopardize the entire system. Therefore, several *cryptographic* properties have been defined and studied to ensure immunity of the system to different kinds of attacks; the ever evolving design of those naturally entails new restrictions on the classes of

eligible Boolean functions, so that they become narrower and narrower and their constructions, or even their characterizations, become harder and harder.

In Section 1.1, we give a slightly more formal description of the context in which Boolean functions are used in cryptography and define the aforementioned properties they should meet. For the sake of the impatient reader, let us already mention these properties: balancedness, high algebraic degree, algebraic immunity, resistance to fast algebraic attacks and high nonlinearity. Some of these notions are naturally incompatible and trade-offs have to be made to meet as many criteria as possible. The corresponding attacks will also be mentioned, but not thoroughly described. For a more classical and deeper exposition we refer the reader to Carlet's one [38] where the notions depicted here and much more can be found.

The above observations might lead the reader to think that building Boolean functions meeting all cryptographic criteria is out of reach. Fortunately, this is not the case. Moreover, existence of classes of such functions is not only theoretical: explicit constructions have been devised. Section 1.2 is devoted to the description of infinite classes of Boolean functions which meet all, or at least most, of the current necessary criteria. The first such family was discovered and analyzed by Carlet and Feng [41] in a family previously introduced by Feng, Liao and Yang [89]. Afterwards, Tu and Deng [264] proposed to apply the ideas of Carlet and Feng to a very classical construction of Dillon [70]. Unfortunately, their family failed to meet one essential cryptographic criterion — immunity to fast algebraic attacks — which makes it more of theoretical than practical interest. Nonetheless, following their ideas, Tang, Carlet and Tang [259] could construct a slightly different class of functions filling that last requirement. Both treatments were subsequently unified by the work of Jin et al. [143]. To conclude, we should state that our interest in those families does not only reside in the fact that they give a positive and concrete answer to an important cryptographic problem, but also in the fact that one of their properties — the high algebraic degree — depends on the validity of a combinatorial conjecture that will be studied deeply in Chapter 2.

1.1 Cryptographic criteria for Boolean functions

1.1.1 The filter and combiner models

Symmetric cryptosystems are commonly used for encryption and decryption owing to their efficiency. Classical models for such cryptosystems are stream ciphers: this design is loosely based on the one-time pad [193, 6.1.1], or Vernam cipher, for which a random bit generator is used to encrypt the plaintext one bit at a time. Hence, to build a stream cipher, a suitable pseudorandom keystream generator must be designed. A common construction is to use one or several linear feedback shift registers [193, 6.2.1] (LFSR) filtered or combined by a Boolean function, that is a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$. The Boolean function should provide confusion, to hide the algebraic nature of the system, and diffusion, so that a minor modification of the input quickly spreads, two fundamental principles stated by Shannon [236]. Both models are depicted in Figures 1.1 and 1.2.

Such cryptosystems have been the objects of a lot of cryptanalyses and several design criteria have been proposed concerning the filtering or combining functions; mainly: balancedness, a high algebraic degree, a high algebraic immunity, resistance to fast algebraic attacks and a high nonlinearity.

1.1.2 Balancedness and resiliency

The two following definitions provide a basic description of the values a Boolean function takes and will be used extensively in the first four chapters of this thesis.

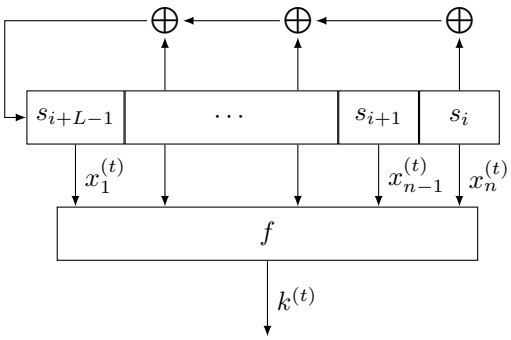


Figure 1.1: The filter model

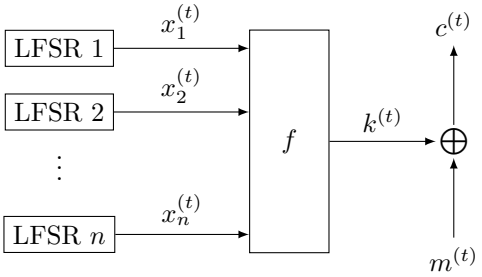


Figure 1.2: The combiner model

Definition 1.1.1 (Support). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function in n variables. The support of f, denoted by* $\mathrm{supp}(f)$*, is the set of $x \in \mathbb{F}_2^n$ such that $f(x) = 1$:*

$$\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\} \quad .$$

The support of a Boolean function provides a complete characterization of it. Most families presented in Section 1.2 will be given in this way.

Definition 1.1.2 (Hamming weight). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function in n variables. The Hamming weight of f, denoted by* $\mathrm{w_H}(f)$*, is the cardinality of its support (or the Hamming weight of its value vector).*

We can now define a first criterion of interest for cryptographic Boolean functions.

Definition 1.1.3 (Balancedness [38, 4.1.3]). *A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ in n variables is said to be balanced if it has Hamming weight 2^{n-1}.*

Hence, a Boolean function is said to be balanced if it takes as often the values 0 and 1. Balancedness is needed to avoid statistical dependence between the input and the output of the stream cipher and to prevent distinguishing attacks [38, 4.1.3].

The notion of balancedness can be generalized as follows.

Definition 1.1.4 (Resiliency [243], [38, 4.1.3]). *A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ in n variables is said to be m-resilient if any of its restrictions with at most m-input fixed is balanced.*

A Boolean function used in the combiner model should be resilient in order to resist correlation attacks [243]. This is not mandatory for functions used in the filter model. In the latter model, 1-resiliency is commonly considered to be sufficient and can be obtained by choosing another function in the same affine equivalence class [121].

1.1.3 Algebraic degree

A common representation for Boolean functions is through algebraic normal forms, i.e. as multivariate polynomials in n variables representing the n inputs. The following proposition states that such a form always exists and can be chosen in a canonical way.

Proposition 1.1.5 (Algebraic normal form [38, 2.1]). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function in n variables. Then f can be uniquely represented as a multivariate polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$ called its algebraic normal form:*

$$f(x_1, \ldots, x_n) = \sum_{I \subset \{1,\ldots,n\}} a_I \prod_{i \in I} x_i, \ a_I \in \mathbb{F}_2 \ .$$

Associated with this representation is the algebraic degree of a Boolean function.

Definition 1.1.6 (Algebraic degree [38, 4.1.1]). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function in n variables. The algebraic degree of f, denoted by $\deg(f)$, is the degree of its algebraic normal form.*

The linear complexity of the pseudorandom generator depends on the algebraic degree of its filtering or combining function, whence the importance for it to have a high algebraic degree in order to avoid the Berlekamp–Massey attacks [187], [193, 6.2.3], [38, 4.1.1] and, for the filter model, the more recent Rønjom–Helleseth attack [226].

It is obviously verified from the definition of the algebraic normal form that the algebraic degree of a Boolean function in n variables is at most n. Furthermore, it should be noted that an m-resilient function satisfies the following inequality [243]:

$$m + \deg(f) \leq n - 1 \ ;$$

this inequality gives a first example of the fact that different cryptographic criteria interact and are in some ways fundamentally incompatible.

1.1.4 Algebraic immunity

Standard algebraic attacks were introduced in 2003 by Courtois and Meier [59]. In view of these attacks, the study of the set of annihilators of a Boolean function has become very important and a Boolean function should have a high algebraic immunity. We define these notions below.

Definition 1.1.7 (Annihilator [190]). *Let f be a Boolean function in n variables. A nonzero Boolean function g is called an annihilator of f if $fg = 0$.*

Definition 1.1.8 (Algebraic immunity [190]). *The algebraic immunity of f, denoted by $\mathrm{AI}(f)$, is the minimum value of d such that f or its complement $1 + f$ admits an annihilator of algebraic degree d.*

The best possible algebraic immunity is $\lceil n/2 \rceil$ [59]. A high algebraic immunity is now an absolutely necessary cryptographic criterion, but it is unfortunately not sufficient anymore.

A more general kind of attacks was indeed introduced by Courtois [58] in 2003 as well: the fast algebraic attacks. For these attacks, the product of f or its complement $1 + f$ with another function g of low degree should not be zero, as for standard algebraic attacks, but of lower degree, hence generalizing the former attacks and making the notion of algebraic immunity already insufficient.

1.1.5 Nonlinearity and bentness

The last cryptographic criterion of interest in this thesis is that of nonlinearity and the related notion of bentness. Nonlinearity characterizes the distance between a Boolean function and the set of affine functions and is naturally defined using the Hamming distance.

Definition 1.1.9 (Hamming distance)**.** *Let f and g be two Boolean functions in n variables. The Hamming distance between f and g, denoted by $\mathrm{d_H}(f,g)$, is defined as*

$$\#\left\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\right\} \ .$$

The distance can also be defined as $\mathrm{d_H}(f,g) = \mathrm{w_H}(f+g)$ (where addition occurs in $\mathbb{F}_2$).

Definition 1.1.10 (Nonlinearity [38, 4.1.2])**.** *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function in n variables. The nonlinearity of f, denoted by $\mathrm{nl}(f)$, is the minimum distance to affine functions (i.e. those of algebraic degree 0 or 1).*

It can be shown that the nonlinearity of a Boolean function in n variables is upper bounded by $2^{n-1} - 2^{n/2-1}$ [38, 4.1.2]. High nonlinearity is important to prevent fast correlation attacks [191] and best affine approximation attacks [72].

Boolean functions achieving maximal nonlinearity are called bent functions.

Definition 1.1.11 (Bentness [70])**.** *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function in n variables. f is said to be bent if it satisfies $\mathrm{nl}(f) = 2^{n-1} - 2^{n/2-1}$.*

Obviously, bent functions only exist when n is even. Such functions can not be directly used in the filter and combiner models; in particular, they are not balanced. They are however a very important building block for many cryptographic systems and Chapter 3 will be devoted to their study.

1.2 Families of Boolean functions with good cryptographic properties

1.2.1 Trade-offs between the different criteria

Building a Boolean function meeting as many criteria as possible is a difficult task. Trade-offs must usually be made between them. Since the introduction of algebraic immunity, several constructions of Boolean functions with high algebraic immunity have been suggested, but very few of them are of optimal algebraic immunity. More importantly, those having other good cryptographic properties, as balancedness or high nonlinearity for instance, are even rarer. Among those having optimal algebraic immunity $\mathrm{AI}(f) = \lceil n/2 \rceil$, most have a poor nonlinearity [40, 64, 177, 178, 42], close to the lower bound of Lobanov [184]:

$$\mathrm{nl}(f) \geq 2^{n-1} - \binom{n}{\lfloor \frac{n}{2} \rfloor} \ .$$

We now present different *good* families, i.e. meeting most of the criteria mentioned in Section 1.1 in a satisfactory way.

1.2.2 The Carlet–Feng family

In 2008, Carlet and Feng [41] studied a family of Boolean functions introduced by Feng, Liao and Yang [89] and devised the first infinite class of functions which seems able to satisfy all of the main criteria for being used as a filtering function in a stream cipher.

Definition 1.2.1 (Construction of Carlet and Feng [41, Section 3]). *Let $n \geq 2$ be a positive integer and α a primitive element of $\mathbb{F}_{2^n}$. Let f be the Boolean function in n variables defined by*

$$\mathrm{supp}(f) = \left\{0, 1, \alpha, \ldots, \alpha^{2^{n-1}-2}\right\} \ .$$

They proved that these functions are

1. balanced,
2. of optimal algebraic degree $n-1$ for a balanced function,
3. of optimal algebraic immunity $\lceil n/2 \rceil$,
4. with good immunity to fast algebraic attacks,
5. and with good nonlinearity

$$\mathrm{nl}(f) \geq 2^{n-1} + \frac{2^{n/2+1}}{\pi} \ln\left(\frac{\pi}{2^n - 1}\right) - 1 \approx 2^{n-1} - \frac{2\ln 2}{\pi} n 2^{n/2} \ .$$

Moreover, it was checked for small values of n that the functions had far better nonlinearity than the proved lower bound.

Afterwards, the same family was reintroduced in a different way by Wang et al. [278, 39] who proved a better lower bound:

$$\mathrm{nl}(f) \geq \max\left(6\lfloor\frac{2^{n-1}}{2n}\rfloor - 2, 2^{n-1} - \left(\frac{\ln 2}{3}(n-1) + \frac{3}{2}\right) 2^{n/2}\right) \ .$$

Finally, Tang, Carlet and Tang [259] proved in 2011 that the following better lower bound is again valid:

$$\mathrm{nl}(f) \geq 2^{n-1} - \left(\frac{n\ln 2}{2\pi} + 0.74\right) 2^{n/2} - 1 \ .$$

1.2.3 The Tu–Deng family

In 2010, Tu and Deng [264] discovered that there may be Boolean functions of optimal algebraic immunity in a classical class of Partial Spread functions due to Dillon [70] provided that the following combinatorial conjecture is correct.

Conjecture 1.2.2 (Tu–Deng conjecture). *For all $k \geq 2$ and all $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 | a + b = t \text{ and } \mathrm{w_H}(a) + \mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

Tu and Deng checked the validity of the conjecture for $k \leq 29$. They also proved that, if the conjecture is true, then one can get in even dimension balanced Boolean functions of optimal algebraic immunity and of high nonlinearity (better than that of the functions proposed in Subsection 1.2.2).

More explicitly, their idea was to apply the idea of Carlet and Feng to the classical construction of Dillon as depicted below.

Definition 1.2.3 (Construction of Dillon [70]). *Let $n = 2k \geq 4$ be an even integer and $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ a balanced Boolean function in k variables. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function defined by*

$$f(x, y) = g\left(\frac{x}{y}\right) \ ,$$

where x/y is understood as xy^{2^n-2}, so equal to 0 when $y = 0$.

These functions form the so-called Partial Spread class $\mathcal{PS}_{ap}$ [70]. In particular, all functions in this class are bent [70] and have algebraic degree $n/2 = k$ [222].

Definition 1.2.4 (First construction of Tu and Deng [264]). *Let $n = 2k \geq 4$ be an even integer, α a primitive element of $\mathbb{F}_{2^n}$, $A = \left\{1, \alpha, \ldots, \alpha^{2^{k-1}-1}\right\}$ and $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ a Boolean function in k variables defined by*

$$\begin{aligned} \mathrm{supp}(g) &= \left\{\alpha^s, \alpha^{s+1}, \ldots, \alpha^{s+2^{k-1}-1}\right\} \\ &= \alpha^s A \ , \end{aligned}$$

for any $0 \leq s \leq 2^k - 2$. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function in n variables defined by

$$f(x, y) = \begin{cases} g\left(\frac{x}{y}\right) & \text{if } x \neq 0 \ , \\ 0 & \text{otherwise} \ . \end{cases}$$

They proved that these functions are

1. bent (because they belong to $\mathcal{PS}_{ap}$),
2. of algebraic degree $n/2 = k$ [222],
3. and of optimal algebraic immunity $n/2 = k$ if Conjecture 1.2.2 is verified.

The approach of Tu and Deng to prove the optimal algebraic immunity was to identify annihilators of the Boolean function with codewords of BCH codes [185, 186, 272]. The role of the conjecture is then to deduce from the BCH bound [185, 186, 272] that those codewords are equal to zero if the algebraic degrees of the corresponding annihilators are less than $n/2 = k$.

These functions can then be modified to give rise to functions with different good cryptographic properties as follows.

Definition 1.2.5 (Second construction of Tu and Deng [264]). *Let $n = 2k \geq 4$ be an even integer, α a primitive element of $\mathbb{F}_{2^n}$, $A = \left\{1, \alpha, \ldots, \alpha^{2^{k-1}-1}\right\}$ and $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ a Boolean function in k variables defined by*

$$\mathrm{supp}(g) = \alpha^s A \ ,$$

for any $0 \leq s \leq 2^k - 2$. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function in n variables defined by

$$f(x, y) = \begin{cases} g\left(\frac{x}{y}\right) & \text{if } xy \neq 0 \ , \\ 1 & \text{if } x = 0 \text{ and } y \in (\alpha A)^{-1} \ , \\ 0 & \text{otherwise} \ . \end{cases}$$

Our definition slightly differs from the original one [264], but, in the end, it is equivalent because

$$\begin{aligned}(\alpha A)^{-1} &= \left\{\alpha^{-1}, \ldots, \alpha^{-(2^{k-1}-1)}, \alpha^{-2^{k-1}}\right\} \\ &= \left\{\alpha^{2^{k-1}-1}, \alpha^{2^{k-1}}, \ldots, \alpha^{2^k-2}\right\} \ .\end{aligned}$$

The cryptographic parameters of the function f are as follows:

1. f is balanced;
2. its algebraic degree is optimal for a balanced function, that is equal to $n-1$;
3. up to Conjecture 1.2.2, f has optimal algebraic immunity that is, $\mathrm{AI}(f) = n$;
4. its nonlinearity satisfies

$$\mathrm{nl}(f) \geq 2^{n-1} - 2^{n/2-1} - \frac{n}{2}2^{n/4}\ln 2 - 1 \ .$$

Afterwards, Tu and Deng [263, 262] modified their original functions to obtain a class of 1-resilient functions with high nonlinearity and high algebraic immunity.

Definition 1.2.6 (Third construction of Tu and Deng [263, 262])**.** *Let $n = 2k \geq 4$ be an even integer, α a primitive element of $\mathbb{F}_{2^n}$, $A = \left\{\alpha, \alpha^2, \ldots, \alpha^{2^{k-1}-1}\right\}$, $0 \leq s \leq 2^k - 2$ an integer and $B = \{0,1\} \cup A^{-1}$. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function in n variables defined by*

$$\mathrm{supp}(f) = \bigcup \begin{cases} \{(x,y) \mid x/y \in \alpha^s A\} & , \\ \{(x,y) \mid y = \alpha^{-s}y, x \in B\} & , \\ \{(x,0) \mid x \in \mathbb{F}_{2^k} \setminus B\} & , \\ \{(0,y) \mid y \in \mathbb{F}_{2^k} \setminus \alpha^{-s}B\} & . \end{cases}$$

They proved that f satisfies the following properties:

1. f is 1-resilient;
2. f is of optimal algebraic degree $\deg(f) = n-2$;
3. up to Conjecture 1.2.2, f has algebraic immunity $\mathrm{AI}(f) \geq n/2 - 1$;
4. f has nonlinearity

$$\mathrm{nl}(f) \geq 2^{n-1} - 2^{n/2-1} - \frac{3}{2}n2^{n/4}\ln 2 - 7 \ .$$

It is in fact proved that f has optimal algebraic immunity depending only on Conjecture 1.2.2 when $n/2$ is odd and on an additional assumption when $n/2$ is even [262].

Finally, Tang et al. [260] applied a degree optimized version of an iterative construction of balanced Boolean functions with very high nonlinearity by Dobbertin [73] to the functions constructed by Tu and Deng [264, 263] and obtained functions with better nonlinearity. For $n = 2k = 2^t m \geq 4$, m odd, their first family is

1. balanced,
2. of optimal algebraic degree $n-1$,

3. of optimal algebraic immunity $n/2$ if Conjecture 1.2.2 is verified,

4. of nonlinearity at least

$$2^{n-1} - \sum_{i=0}^{t-1} 2^{n/(2^{i+1})-1} - 2^{(m-1)/2} \ ;$$

and their second family is

1. 1-resilient,

2. of optimal algebraic degree $n-2$,

3. of algebraic immunity at least $n/2-1$ if Conjecture 1.2.2 is verified,

4. of nonlinearity at least

$$\begin{cases} 2^{n-1} - 2^{n/2-1} - 3\left(\sum_{i=1}^{t-1} 2^{n/(2^{i+1})-1} - 2^{(m-1)/2}\right) & \text{if } m = 1 \ , \\ 2^{n-1} - 2^{n/2-1} - 3\sum_{i=1}^{t-1} 2^{n/(2^{i+1})-1} - 2^{(m+1)/2} - 6 & \text{if } m \geq 2 \ . \end{cases}$$

Unfortunately, Carlet [36] observed that the functions introduced by Tu and Deng are weak against fast algebraic attacks and unsuccessfully tried to repair their weakness. It was subsequently shown by Wang and Johansson [277] that this family can not be easily repaired.

Nonetheless, more recent developments have shown that the construction of Tu and Deng and the associated conjecture are not of purely æsthetic interest, but are interesting tools in a cryptographic context.

1.2.4 The Tang–Carlet–Tang family

In 2011, inspired by the previous work of Tu and Deng [264], Tang, Carlet and Tang [259] constructed an infinite family of Boolean functions with many good cryptographic properties. The main idea of their construction is to change the division in the construction of Tu and Deng by a multiplication. The associated combinatorial conjecture is then modified as follows.

Conjecture 1.2.7 (Tang–Carlet–Tang conjecture)**.** *For all $k \geq 2$ and all $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid a - b = t; \mathrm{w_H}(a) + \mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

They verified it experimentally for $k \leq 29$, as well as the following generalized property for $k \leq 15$ where $u \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ is such that $\gcd(u, 2^k-1) = 1$ and $\epsilon = \pm 1$.

Conjecture 1.2.8 (Tang–Carlet–Tang conjecture)**.** *Let $k \geq 2$ be an integer, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, $u \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ such that $\gcd(u, 2^k-1) = 1$ and $\epsilon \in \{-1, 1\}$. Then*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua + \epsilon b = t; \mathrm{w_H}(a) + \mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

This generalized conjecture includes the original conjecture proposed by Tu and Deng (Conjecture 1.2.2) for $u = 1$ and $\epsilon = +1$.

The construction of their functions is as follows.

Definition 1.2.9 (Construction of Tang, Carlet and Tang [259]). *Let $n = 2k \geq 4$ be an even integer, α a primitive element of $\mathbb{F}_{2^n}$, $A = \left\{1, \alpha, \ldots, \alpha^{2^{k-1}-1}\right\}$ and $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ the Boolean function in k variables defined by*

$$\mathrm{supp}(g) = \alpha^s A \ ,$$

for any $0 \leq s \leq 2^k - 2$. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function in n variables defined by

$$f(x, y) = g(xy) \ .$$

They proved that such a function f is

1. of algebraic degree $n - 2$,
2. of optimal algebraic immunity $n/2$ if Conjecture 1.2.7 is true,
3. of good immunity against fast algebraic attacks,
4. of nonlinearity at least
$$2^{n-1} - \left(\frac{\ln 2}{2\pi} n + 0.42\right) 2^{n/2} - 1 \ .$$

The proof of the optimality of the algebraic immunity is similar to the proof of Tu and Deng [264].

These functions can then be modified using the same procedure as Tang et al. [260] to obtain balanced functions with high algebraic degree and nonlinearity. They proved that, for $n = 2k = 2^t m \geq 4$ and m odd, these modified functions are

1. balanced,
2. of optimal algebraic degree $n - 1$,
3. of optimal algebraic immunity $n/2$ if Conjecture 1.2.7 is true,
4. of good immunity against fast algebraic attacks,
5. of nonlinearity at least
$$\begin{cases} 2^{n-1} - \left(\frac{\ln 2}{2\pi} n + 0.42\right) 2^{n/2} - 2^{\frac{n/2-1}{2}} - 1 & \text{if } t = 1 \ , \\ 2^{n-1} - \left(\frac{\ln 2}{2\pi} n + 0.42\right) 2^{n/2} - \sum_{i=1}^{t-1} 2^{n/(2^{i+1})-1} - 2^{(m-1)/2} - 1 & \text{if } t \geq 2 \ . \end{cases}$$

1.2.5 The Jin et al. family

It should finally be mentioned that Jin et al. [143] generalized the construction of Tang, Carlet and Tang [259] in a way that included back the construction of Tu and Deng [264]. In their paper, the main idea is to replace y by y^{2^k-1-u} in the construction of the function. Hence, the family of Tu and Deng [264] is included for $u = 1$, and the family of Tang, Carlet and Tang [259] for $u = 2^k - 2$. The associated combinatorial conjecture is then modified as follows.

Conjecture 1.2.10 (Jin et al. conjecture). *Let $k \geq 2$ be an integer, $t, u, v \in \left(\mathbb{Z}/(2^k - 1)\mathbb{Z}\right)^*$ such that $\gcd(u, 2^k - 1) = \gcd(v, 2^k - 1) = 1$. Then*

$$\#\left\{(a, b) \in \left(\mathbb{Z}/(2^k - 1)\mathbb{Z}\right)^2 \mid ua + vb = t; \mathrm{w_H}(a) + \mathrm{w_H}(b) \leq k - 1\right\} \leq 2^{k-1} \ .$$

This generalized conjecture obviously includes all the previous ones.

The construction of their functions is as follows.

Definition 1.2.11 (Construction of Jin et al. [143]). *Let $n = 2k \geq 4$ be an even integer, α a primitive element of $\mathbb{F}_{2^n}$, $A = \left\{1, \alpha, \ldots, \alpha^{2^{k-1}-1}\right\}$ and $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ Boolean function in k variables defined by*

$$\mathrm{supp}(g) = \alpha^s A \ ,$$

for any $0 \leq s \leq 2^k - 2$. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function in n variables defined by

$$f(x, y) = g\left(xy^{2^k-1-u}\right) \ .$$

They proved that such a function f is

1. of algebraic degree between $n/2$ and $n-2$ depending on the value of u,
2. of optimal algebraic immunity $n/2$ if Conjecture 1.2.10 is true,
3. of nonlinearity at least

$$2^{n-1} - \frac{2}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/2} - 1 \approx 2^{n-1} - \frac{\ln 2}{\pi} n 2^{n/2} \ .$$

The proof of the optimality of the algebraic immunity is once again similar to the previous ones. It should be noted that resistance to fast algebraic attacks is not studied by Jin et al. [143].

Modifying these functions as before, Jin et al. obtained balanced functions with high algebraic degree and nonlinearity. They proved that for $n = 2k \geq 4$, these modified functions are

1. balanced,
2. of optimal algebraic degree $n-1$,
3. of optimal algebraic immunity $n/2$ if Conjecture 1.2.10 is true,
4. of nonlinearity at least

$$2^{n-1} - \frac{2}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/2} - \frac{2}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/4} - 2 \approx 2^{n-1} - \frac{\ln 2}{\pi} n 2^{n/2} - \frac{\ln 2}{\pi} n 2^{n/4} \ .$$

Jin et al. [142] applied a similar generalization to the 1-resilient Boolean function of Tu and Deng [262] and obtained a family functions which are

1. 1-resilient,
2. of optimal algebraic degree $n-2$,
3. of optimal algebraic immunity $n/2$ up to Conjecture 1.2.10 and an additional assumption,
4. of nonlinearity at least

$$\begin{aligned} &2^{n-1} - \frac{2}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/2} - 2^{n/2-1} - \frac{4}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/4} - 3 \\ &\approx 2^{n-1} - \frac{\ln 2}{\pi}(n+1) 2^{n/2} - \frac{2 \ln 2}{\pi} n 2^{n/4} \ . \end{aligned}$$

Finally, for specific values of the parameter u — in particular for the family of Tang, Carlet and Tang [259] presented in Subsection 1.2.4 —, the conjecture, and so the optimality of the algebraic degree, can be proved using the results of the next chapter.

Chapter 2

On a conjecture about addition modulo $2^k - 1$

Πληθὺν Ἡελίοιο βοῶν, ὦ ξεῖνε, μέτρησον
φροντίδ᾽ ἐπιστήσας, εἰ μετέχεις σοφίης,
πόσση ἄρ᾽ ἐν πεδίοις Σικελῆς ποτ᾽ ἐβόσκετο νήσου
Θρινακίης τετραχῇ στίφεα δασσαμένη
χροιὴν ἀλάσσοντα · τὸ μὲν λευκοῖο γάλακτος,
κυανέῳ δ᾽ ἕτερον χρώματι λαμπόμενον,
ἄλλο γε μὲν ξανθόν, τὸ δὲ ποικίλον. [...]
Ταῦτα συνεξευρὼν καὶ ἐνὶ πραπίδεσσιν ἀθροίσας
καὶ πληθέων ἀποδούς, ξεῖνε, τὰ πάντα μέτρα
ἔρχεο κυδιόων νικηφόρος ἴσθι τε πάντως
κεκριμένος ταύτῃ γ᾽ ὄμπνιος ἐν σοφίῃ.

Πρόβλημα βοεικόν
Ἀρχιμήδης [212]

Contents

As was underlined in the previous chapter, the good cryptographic properties of the Boolean functions of the Jin et al. family [142] described in Subsection 1.2.5, and more precisely the optimality of their algebraic immunity, depend on the validity of a combinatorial conjecture. The purpose of this chapter, if not to prove that conjecture in its full generality, is at least to give a good insight into its expected validity not only through a thorough theoretical study, but also by exposing experimental evidence. Part of the work presented in this chapter is the result of collaborations with Gérard Cohen, Sihem Mesnager and Hugues Randriam and already appeared in different forms [96, 94]. Several preprints [97, 95, 53] including additional results are available as well.

The main approach used in this chapter is that of reformulating the conjecture in terms of *carries* occurring in an addition modulo $2^k - 1$. This formalism and the very basic properties verified by that quantity are developed in Section 2.1. Although such an approach may at first seem quite naive to the reader, what makes the study of the conjecture seemingly so difficult is precisely that a suitable algebraic structure to cast upon the problem has yet to be found, so that only a purely combinatorial point of view is possible as of today.

Nevertheless, the point of view adopted here provides already enough information to prove in Section 2.2 that the special case of the conjecture required by the family of Tang, Carlet and

Tang [259] is true. Thereafter, we concentrate our efforts on the original conjecture of Tu and Deng [264] which is a natural candidate to extend our study[1].

Unfortunately, the situation is already much more involved and its study builds the end of this chapter up. Even though a complete proof has yet to be given, we manage to prove some interesting results giving evidence of the validity of the conjecture. A family of integers reaching the upper bound of the conjecture is first characterized in Section 2.4. A closed-form expression is then deduced in a constrained and better behaved case in Section 2.5. Finally, the conjecture is given a probabilistic interpretation and proved in an asymptotic setting in Section 2.6.

To conclude this general introduction, let us mention that we also provide some evidence that a simple inductive approach is not suitable in Section 2.7 and that the experimental results of Section 2.9 establish the validity of the Tu–Deng conjecture for up to 40 bits, thus extending the original results of Tu and Deng [264]. Finally, other applications of carries in the field of Boolean functions exist and can be found e.g. in the works of Canteaut, Charpin and Dobbertin [35] or Langevin et al. [161].

2.1 General properties

2.1.1 Notation

Unless stated otherwise, we use the following notation throughout this chapter:

- $k \in \mathbb{N}$ is the number of bits (or length of binary strings) we are currently working on;
- $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ is a fixed modular integer.

We use the following function of natural (or modular) integers (or binary strings).

Definition 2.1.1 (Hamming weight)**.** *For $t \in \mathbb{N}$, $\mathrm{w_H}(t)$ is the Hamming (or binary) weight of t, i.e. the number of* 1*'s in its binary expansion. For $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, $\mathrm{w_H}(t)$ is the Hamming (or binary) weight of the unique representative of t in $\{0,\dots,2^k-2\}$.*

From now on, let us denote by $S_{t,v,u,k}$ the set of interest:

$$S_{t,v,u,k} = \left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua+vb=t; \mathrm{w_H}(a)+\mathrm{w_H}(b) \leq k-1\right\} \ ,$$

where $k \geq 2$, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ and $u,v \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^\times$, i.e. u and v are invertible modulo 2^k-1.

We now recall the different flavors of the conjecture already mentioned in Chapter 1.

Conjecture 1.2.2 (Tu–Deng conjecture)**.** *With the above notation,*

$$\#S_{t,+1,1,k} \leq 2^{k-1} \ .$$

Conjecture 1.2.7 (Tang–Carlet–Tang conjecture)**.** *With the above notation,*

$$\#S_{t,-1,1,k} \leq 2^{k-1} \ .$$

Conjecture 1.2.8 (Tang–Carlet–Tang conjecture)**.** *With the above notation,*

$$\#S_{t,\epsilon,u,k} \leq 2^{k-1} \ .$$

Conjecture 1.2.10 (Jin et al. conjecture)**.** *With the above notation,*

$$\#S_{t,v,u,k} \leq 2^{k-1} \ .$$

[1] This was in fact the first proposed flavor of the conjecture, and the first we studied.

2.1.2 Negation and rotation

In this subsection we study the behavior of the Hamming weight under various basic transformations: *binary not* and *rotation*.

Definition 2.1.2. *We define $\overline{a}^k$ as the modular integer whose binary expansion is the binary not on k bits of the binary expansion of the representative of a in $\{0, \ldots, 2^k - 2\}$. We denote it by $\overline{a}$ when there is no ambiguity about the value of k.*

Lemma 2.1.3. *Let $a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ be a non-zero modular integer, then $-a = \overline{a}$ and $\mathrm{w_H}(-a) = k - \mathrm{w_H}(a)$.*

Proof. Indeed $a + \overline{a} = \sum_{i=0}^{k-1} 2^i = 2^k - 1 = 0$. □

Lemma 2.1.4. *For all $i \in \mathbb{Z}$ and $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, we have*

$$\mathrm{w_H}(2^i a) = \mathrm{w_H}(a) \ .$$

Proof. We are working in $\mathbb{Z}/(2^k-1)\mathbb{Z}$ so that $2^k = 1$ and multiplying a modular integer in $\mathbb{Z}/(2^k-1)\mathbb{Z}$ by 2 is just rotating its representation as a binary string on k bits by one bit to the left, whence the equality of the Hamming weights. □

Therefore, we say that, for any $i \in \mathbb{Z}$, $2^i a$ and a are equivalent, or that they are in the same *cyclotomic class* modulo $2^k - 1$, and we write $a \simeq 2^i a$. We now remark that, for a given $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, b must be equal to $v^{-1}(t - ua)$, whence the following lemma.

Lemma 2.1.5. *For $k \geq 2$,*

$$\#S_{t,v,u,k} = \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(v^{-1}(t-ua)) \leq k-1\right\} \ .$$

Using the previous lemmas, we can now show that is enough to study the conjecture for one t, but also one u and one v, in each cyclotomic class.

Lemma 2.1.6. *For $k \geq 2$,*

$$\#S_{t,v,u,k} = \#S_{2t,v,u,k} \ .$$

Proof. Indeed $a \mapsto 2a$ is a permutation of $\mathbb{Z}/(2^k-1)\mathbb{Z}$ so that

$$\begin{aligned}
\#S_{2t,v,u,k} &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(v^{-1}(2t-ua)) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(2a) + \mathrm{w_H}(2v^{-1}(t-ua)) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(v^{-1}(t-ua)) \leq k-1\right\} \\
&= \#S_{t,v,u,k} \ .
\end{aligned}$$

□

Lemma 2.1.7. *For $k \geq 2$,*

$$\#S_{t,v,u,k} = \#S_{t,v,2u,k} \ .$$

Proof. Using the previous lemma,

$$\begin{aligned}
\#S_{t,v,2u,k} &= \#S_{2t,v,2u,k} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(v^{-1}(2t-2ua)) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(v^{-1}(t-ua)) \leq k-1\right\} \\
&= \#S_{t,v,u,k} \ .
\end{aligned}$$

□

Lemma 2.1.8. *For $k \geq 2$,*

$$\#S_{t,v,u,k} = \#S_{t,2v,u,k} \ .$$

Proof. Using the previous lemmas,

$$\begin{aligned}
\#S_{t,2v,u,k} &= \#S_{2t,2v,2u,k} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}((2v)^{-1}(2t-2ua)) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(v^{-1}(t-ua)) \leq k-1\right\} \\
&= \#S_{t,v,u,k} \ .
\end{aligned}$$

□

We now show a more elaborate relation for different values of u, v and t.

Lemma 2.1.9. *For $k \geq 2$,*

$$\#S_{t,v,u,k} = \#S_{(uv)^{-1}t,v^{-1},u^{-1},k} \ .$$

Proof. We use the fact that $a \mapsto u^{-1}(-va+t)$ is a permutation of $\mathbb{Z}/(2^k-1)\mathbb{Z}$ and deduce

$$\begin{aligned}
\#S_{t,v,u,k} &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(v^{-1}(t-ua)) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(u^{-1}(-va+t)) + \mathrm{w_H}(a) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(v((uv)^{-1}t - u^{-1}a)) + \mathrm{w_H}(a) \leq k-1\right\} \\
&= \#S_{(uv)^{-1}t,v^{-1},u^{-1},k} \ .
\end{aligned}$$

□

To conclude this subsection we state the following observation of Jin et al. [143].

Lemma 2.1.10. *For $k \geq 2$ and $c \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^\times$,*

$$\#S_{t,v,u,k} = \#S_{ct,cv,cu,k} \ .$$

Proof. Indeed, we have $ua + vb = t$ if and only if $cua + cvb = ct$ when c is invertible, whence a bijection between the sets $S_{t,v,u,k}$ and $S_{ct,cv,cu,k}$. □

Finally, as noted by Jin et al. [143], their generalized conjecture is then equivalent to the generalized conjecture of Tang, Carlet and Tang [259].

Corollary 2.1.11. *Conjecture 1.2.10 is equivalent to Conjecture 1.2.8.*

Proof. The fact that Conjecture 1.2.10 implies Conjecture 1.2.8 is obvious setting $v = \epsilon$. The converse comes from the above lemma by setting $c = v^{-1}$:

$$\#S_{t,v,u,k} = \#S_{v^{-1}t,1,v^{-1}u,k} \ .$$

□

2.1.3 Carries

We now define the main tool we will use to study the conjectures.

Definition 2.1.12. *For $a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, we set*

$$r(a,t) = \mathrm{w_H}(a) + \mathrm{w_H}(t) - \mathrm{w_H}(a+t) \ ,$$

i.e. $r(a,t)$ is the number of carries occurring while performing the addition. By convention, we set

$$r(0,t) = k \ ,$$

i.e. 0 behaves like the $\underbrace{\texttt{1...1}}_{k}$ binary string. We also remark that $r(-t,t) = k$.

2.2 The case $\epsilon = -1$

2.2.1 Proof of the conjecture of Tang, Carlet and Tang

In this subsection we prove Conjecture 1.2.7 of Tang, Carlet and Tang [259], and so its extension for u equal to any power of 2, that is Conjecture 1.2.8 of the same authors for $u = 2^i$ and $\epsilon = -1$, according to Lemma 2.1.7, thus yielding the following theorem which additionally includes the case $t = 0$.

Theorem 2.2.1. *Let $k \geq 2$ be an integer, $t \in \mathbb{Z}/(2^k - 1)\mathbb{Z}$ and $u = 2^i$ where i is any integer. Then*

$$\#S_{t,-1,u,k} \leq 2^{k-1} \ .$$

Proof. First, we note that for $u = 1$ and $v = -1$, Lemma 2.1.10 becomes

$$\#S_{t,-1,1,k} = \#S_{-t,-1,1,k} \ .$$

Second, for the specific cases $a = 0$ and $a = t$, we have that

- $\mathrm{w_H}(0) + \mathrm{w_H}(-t) = \mathrm{w_H}(-t) \leq k - 1$,
- and $\mathrm{w_H}(t) + \mathrm{w_H}(0) = \mathrm{w_H}(t) \leq k - 1$,

so that we always have

$$\{0, t\} \subset \left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(-(t - a)) \leq k - 1\right\} \ .$$

Finally, for $a \neq 0$ and $a \neq t$, we have that

$$\begin{aligned} \mathrm{w_H}(a) + \mathrm{w_H}(-(t - a)) &= k - \mathrm{w_H}(-a) + k - \mathrm{w_H}(t - a) \\ &= 2k - (\mathrm{w_H}(-a) + \mathrm{w_H}(t - a)) \ . \end{aligned}$$

Now suppose that $t \neq 0$. Then, using the fact that $a \mapsto -a$ is a permutation of $\mathbb{Z}/(2^k - 1)\mathbb{Z}$, we can prove that

$$\begin{aligned} \#S_{t,-1,1,k} &= 2 + \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \setminus \{0, t\} \mid \mathrm{w_H}(a) + \mathrm{w_H}(-(t - a)) \leq k - 1\right\} \\ &= 2 + \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \setminus \{0, t\} \mid \mathrm{w_H}(-a) + \mathrm{w_H}(t - a) \geq k + 1\right\} \\ &= 2 + \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid \mathrm{w_H}(-a) + \mathrm{w_H}(t - a) \geq k + 1\right\} \\ &= 2 + \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(t + a) \geq k + 1\right\} \\ &= 2 + (2^k - 1 - \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(t + a) \leq k\right\}) \\ &\leq 2 + (2^k - 1 - \#\left\{a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(t + a) \leq k - 1\right\}) \\ &\leq 2^k + 1 - \#S_{-t,-1,1,k} \\ &\leq 2^k + 1 - \#S_{t,-1,1,k} \ . \end{aligned}$$

We already mentioned that $\#S_{t,-1,1,k} = \#S_{-t,-1,1,k}$, hence we get the inequality

$$2\#S_{t,-1,1,k} \leq 2^k + 1 \ .$$

But we also know that $\#S_{t,-1,1,k}$ is an integer, which concludes the proof for $t \neq 0$.

In the case where $t = 0$, a similar computation yields a finer result:

$$\begin{aligned}\#S_{0,-1,1,k} &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid 2\,\mathrm{w_H}(a) \leq k-1\right\} \\ &= \sum_{w=0}^{\lfloor \frac{k-1}{2} \rfloor} \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) = w\right\} \\ &= \sum_{w=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k}{w} \ ,\end{aligned}$$

which is equal to $2^{k-1} - \binom{k}{(k+1)/2}$ if k is odd, and $2^{k-1} - \binom{k}{k/2-1} - \binom{k/2}{k}/2$ if k is even. Therefore the conjecture can be naturally extended to include the case $t = 0$. □

2.2.2 Computing the exact gap

If we rewrite the above reasoning more carefully, we find that

$$\#S_{t,-1,1,k} = 2^{k-1} + (1 - \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(t+a) = k\right\})/2 \ .$$

It is an interesting problem to find a closed-form expression for the value of[2]

$$M_k = \min_{t \in (\mathbb{Z}/(2^k-1)\mathbb{Z})^*} M_{t,k} \ ,$$

where

$$M_{t,k} = \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid \mathrm{w_H}(a) + \mathrm{w_H}(t+a) = k\right\} \ .$$

The value for $t = 0$ has been computed in the previous subsection and is

$$M_{0,k} = \sum_{w=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k}{w} \ .$$

We denote by Δ_k the following value

$$\Delta_k = \frac{M_k - 1}{2} \ ,$$

so that $S_{t,-1,1,k} = 2^{k-1} - \Delta_k$.

The experimental results of Tang, Carlet and Tang [259] suggest that the following conjecture is verified.

Conjecture 2.2.2. *For $k \geq 3$, one has*

$$\Delta_{k+1} = \begin{cases} 2\Delta_k + 1 & \text{if } k \text{ is even,} \\ 2\Delta_k + 1 - \Gamma_{(k-1)/2} & \text{if } k \text{ is odd,} \end{cases}$$

where

$$\Gamma_n = 1 + \sum_{w=0}^{n-1} C_w$$

and $C_w = \binom{2w}{w}/(w+1)$ is the w-th Catalan number.

[2] We compute the minimum for t non zero as this is the interesting case for the construction of Tang, Carlet and Tang [259]. Modifying this subsection to include the case $t = 0$ is trivial.

The sequence $\{\Gamma_n\}_{n\in\mathbb{N}}$ is sequence A155587 in the OEIS [140]. Further experimental investigations conducted with Sage [250] showed that the minimal value M_k seems to be attained for $t = 1$ if k is even and $t = 3$ if k is odd. In this subsection we prove Conjecture 2.2.2 under that assumption, i.e.

$$M_k = \begin{cases} M_{1,k} & \text{if } k \text{ is even,} \\ M_{3,k} & \text{if } k \text{ is odd.} \end{cases}$$

Recall that $r(a,t) = \mathrm{w_H}(a+t) - \mathrm{w_H}(a) - \mathrm{w_H}(t)$ can be interpreted as the number of carries occurring while adding a and t. Then, we can describe $M_{t,k}$ as

$$\begin{aligned} M_{t,k} &= \#\left\{a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^* \mid \mathrm{w_H}(a) + \mathrm{w_H}(t+a) = k\right\} \\ &= \#\left\{a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^* \mid 2\,\mathrm{w_H}(a) + \mathrm{w_H}(t) - r(a,t) = k\right\} \\ &= \#\left\{a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^* \mid r(a,t) = -k + \mathrm{w_H}(t) + 2\,\mathrm{w_H}(a)\right\} \ . \end{aligned}$$

The next two propositions give explicit formulae for $M_{1,k}$ and $M_{3,k}$.

Proposition 2.2.3. *For $k \geq 2$,*

$$M_{1,k} = \sum_{w=1}^{\lfloor (k+1)/2 \rfloor} \binom{2w-2}{w-1} \ .$$

Proof. We know that $M_{1,k} = M_{-1,k}$, so we enumerate the set of a's verifying $r(a,-1) = 2\,\mathrm{w_H}(a) - 1$ according to $\mathrm{w_H}(a)$ or equivalently $r(a,-1)$. The binary expansion of -1 is `1---10`.

First, for any number $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, $0 \leq r(a,t) \leq k$, so we deduce that a must verify $1 \leq \mathrm{w_H}(a) \leq \lfloor (k+1)/2 \rfloor$.

Second, for a given number of carries r, a number a verifying $r(a,-1) = r$ must be of the following form

$$\begin{aligned} -1 &= \texttt{1---1---10} \ , \\ a &= \underbrace{\texttt{????}}_{r}\texttt{10---0} \ . \end{aligned}$$

Such a description is valid even if $r(a,-1) = k$. So, for a given weight w, a number a verifying $\mathrm{w_H}(a) = w$ and $r(a,-1) = 2w-1$ must be of the following form

$$\begin{aligned} -1 &= \texttt{1---1---10} \ , \\ a &= \underbrace{\texttt{????}}_{2w-1}\texttt{10---0} \ , \end{aligned}$$

with the other $w-1$ bits equal to `1` anywhere among the $2w-2$ first bits. Hence, there are $\binom{2w-2}{w-1}$ different a's of weight w verifying $r(a,-1) = 2w-1$.

Finally, summing up on $1 \leq w \leq \lfloor (k+1)/2 \rfloor$, we get that $M_{1,k} = \sum_{w=1}^{\lfloor (k+1)/2 \rfloor} \binom{2w-2}{w-1}$. □

Proposition 2.2.4. *For $k \geq 3$,*

$$M_{3,k} = 1 + 2\sum_{w=1}^{\lfloor k/2 \rfloor} \binom{2w-2}{w-1} \ .$$

Proof. We proceed as in the proof of Proposition 2.2.3. The arguments are only slightly more technical.

We know that $M_{3,k} = M_{-3,k}$, so we enumerate the set of a's verifying $r(a,-3) = 2\,\mathrm{w_H}(a) - 2$ according to $\mathrm{w_H}(a)$ or equivalently $r(a,-3)$. The binary expansion of -3 is `1---100`.

First, from $r(a,-3) = 2\,\mathrm{w_H}(a) - 2$, we deduce that $1 \leq \mathrm{w_H}(a) \leq \lfloor k/2 \rfloor + 1$.

Second, for a given number of carries r, there are now different possibilities.

For any $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, there are exactly $\sum_{w=0}^{k-\mathrm{w_H}(t)-1} \binom{k-\mathrm{w_H}(t)}{w}$ different a's producing no carries. Indeed, such a's are characterized by the facts that they have no bits equal to `1` in front of any bit of t equal to `1` and that they can not have only `1`'s in front of the bits of t equal to `0`. For $t = -3$, the such a's are exactly 0, 1 and 2 and both 1 and 2 have weight 1.

Then, for a given number of carries $1 \leq r < 2\lfloor k/2 \rfloor$, a number a verifying $r(a,-3) = r$ can not have its last two bits (in front of the two bits of -3 equal to `0`) equal to `1`. Otherwise it would produce k carries. So, it must be of one of the following forms

$$\begin{aligned} -3 &= \texttt{1---1---100}\ , \\ a &= \underbrace{\texttt{????10--0?0}}_{r}\ , \\ a &= \underbrace{\texttt{???10----01}}_{r-1}\ . \end{aligned}$$

Therefore, for a given weight w, a number a verifying $\mathrm{w_H}(a) = w$ and $r(a,-3) = 2w-2$ must be of one of the following forms

$$\begin{aligned} -3 &= \texttt{1---1---100}\ , \\ a &= \underbrace{\texttt{????10--0?0}}_{2w-2}\ , \\ a &= \underbrace{\texttt{???10----01}}_{2w-3}\ , \end{aligned}$$

with the other $w-1$ bits set to `1` anywhere among the $2w-2$ remaining bits in the first case, and the other $w-2$ bits set to `1` anywhere among the $2w-4$ first bits in the second one. Hence, there are $\binom{2w-2}{w-1} + \binom{2w-4}{w-2}$ different a's of weight w.

Finally, if k is odd and $\mathrm{w_H}(a) = \lfloor k/2 \rfloor + 1$, then $r(a,t) = k-1$ and a must be of the following form

$$\begin{aligned} -3 &= \texttt{1---100}\ , \\ a &= \texttt{????101}\ . \end{aligned}$$

There are $\binom{2w-4}{w-2}$ different such a's. And, if k is even and $\mathrm{w_H}(a) = \lfloor k/2 \rfloor + 1$, then $r(a,t) = k$ and a must be of the following form

$$\begin{aligned} -3 &= \texttt{1---100}\ , \\ a &= \texttt{?????11}\ . \end{aligned}$$

There are also $\binom{2w-4}{w-2}$ different such a's.

Therefore, we find that

$$\begin{aligned} M_{3,k} &= 2 + \sum_{w=2}^{\lfloor k/2 \rfloor} \binom{2w-2}{w-1} + \sum_{w=2}^{\lfloor k/2 \rfloor + 1} \binom{2w-4}{w-2} \\ &= 1 + 2 \sum_{w=1}^{\lfloor k/2 \rfloor} \binom{2w-2}{w-1}\ . \end{aligned}$$

□

We now prove recurrence relations for $M_{1,k}$ and $M_{3,k}$.

Corollary 2.2.5. *If k is even, then*

$$2M_{1,k} + 1 = M_{3,k+1} \ .$$

If k is odd, then

$$M_{3,k} - \Gamma_{(k-1)/2} = (M_{1,k+1} - 1)/2 \ .$$

Proof. The first equality is a simple consequence of the fact $\lfloor k/2 \rfloor = \lfloor (k+1)/2 \rfloor$ when k is even.

For the second one, we write

$$\begin{aligned} M_{3,k} - \Gamma_{(k-1)/2} &= 1 + 2 \sum_{w=1}^{\lfloor k/2 \rfloor} \binom{2w-2}{w-1} - 1 - \sum_{w=0}^{(k-3)/2} \binom{2w}{w}/(w+1) \\ &= 2 \sum_{w=1}^{(k-1)/2} \binom{2w-2}{w-1} - \sum_{w=0}^{(k-3)/2} \binom{2w}{w}/(w+1) \\ &= 1 + \sum_{w=1}^{(k-3)/2} (2 - 1/(w+1)) \binom{2w}{w} \ , \end{aligned}$$

and

$$\begin{aligned} (M_{1,k+1} - 1)/2 &= \sum_{w=2}^{\lfloor k/2 \rfloor + 1} \binom{2w-2}{w-1}/2 \\ &= \sum_{w=1}^{(k-1)/2} \binom{2w}{w}/2 \ , \end{aligned}$$

so that we can equivalently show that

$$\binom{k-1}{(k-1)/2} - 2 = \sum_{w=1}^{(k-3)/2} (3 - 2/(w+1)) \binom{2w}{w} \ ,$$

which follows from a simple induction. For $k = 3$, this reduces to $0 = 0$ which is indeed true; for $k > 3$ odd, we have

$$\begin{aligned} \binom{k+1}{(k+1)/2} - 2 &= 4k/(k+1) \binom{k-1}{(k-1)/2} - 2 \\ &= (4 - 1/(k+1)) \binom{k-1}{(k-1)/2} - 2 \ , \end{aligned}$$

and

$$\sum_{w=1}^{(k-1)/2} (3 - 2/(w+1)) \binom{2w}{w} = \left[\sum_{w=1}^{(k-3)/2} (3 - 2/(w+1)) \binom{2w}{w} \right] + (3 - 1/(k+1)) \binom{k-1}{(k-1)/2} \ . \square$$

To conclude this section, let us note that $M_{1,k} \leq M_{3,k}$ if k is even and $M_{3,k} \leq M_{1,k}$ if k is odd. So, if we assume that these are indeed the minimal values M_k according to the parity of k, then Δ_k is given by

$$\Delta_k = \begin{cases} (M_{1,k} - 1)/2 & \text{if } k \text{ even} \ , \\ (M_{3,k} - 1)/2 & \text{if } k \text{ odd} \ , \end{cases}$$

and the recursive formulae observed experimentally can be proved.

2.3 The case $\epsilon = +1$

We are now interested in the original conjecture proposed by Tu and Deng [264] which can be reformulated as follows.

Conjecture 1.2.2. *For $k \geq 2$ and $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, let $S_{t,k}$ be the following set*[3]*:*

$$S_{t,k} = \left\{ a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid r(a,t) > \mathrm{w_H}(t) \right\} \ ,$$

and $P_{t,k}$ the fraction[4] *of modular integers in $S_{t,k}$:*

$$P_{t,k} = \#S_{t,k}/2^k \ .$$

Then

$$P_{t,k} \leq \frac{1}{2} \ .$$

Tu and Deng verified computationally the validity of this assumption for $k \leq 29$ in about fifteen days on a quite recent computer [264]. We also implemented their algorithm and were able to check the conjecture for $k = 39$ in about twelve hours and fifteen minutes on a pool of about four hundred quite recent cores, and $k = 40$ on a subset of these computers. The algorithm of Tu and Deng [264, Appendix] as well as our implementation are described in Section 2.9.

This conjecture is not only interesting in a cryptographic context, but also for purely arithmetical reasons. For a fixed modular integer $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, it is indeed natural to expect the number of carries occurring when adding a random modular integer $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ to t to be roughly the Hamming weight of t. Following this idea, it is of interest to study the distribution of the number of carries around this value. Quite unexpectedly, the conjecture seems to indicate a kind of regularity.

2.3.1 Notation

We now define the sets we are interested in.

Definition 2.3.1. *Let $k \geq 2$ and $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$. Define:*

- $C_{t,k} = \left\{ (a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid a+b = t \right\}$*, the modular integers whose sum is t;*
- $C_{t,k,i} = \{(a,b) \in C_{t,k} \mid \mathrm{w_H}(a) + \mathrm{w_H}(b) = k+i\}$*, the modular integers whose sum is t and whose sum of weights is $k+i$ for $i \in \mathbb{Z}$;*
- $S_{t,k}$*, the modular integers whose sum is t and whose sum of weights is strictly less than k, i.e. $S_{t,k} = \bigsqcup_{i<0} C_{t,k,i}$;*
- $T_{t,k}$*, the modular integers whose sum is t and whose sum of weights is strictly more than k, i.e. $S_{t,k} = \bigsqcup_{i>0} C_{t,k,i}$;*
- E_t*, the modular integers whose sum is t and whose sum of weights equals k; i.e. $E_t = C_{t,k,0}$.*

The following lemma is obvious.

Lemma 2.3.2. *For $k \geq 2$ and $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$,*

$$C_{t,k} = S_{t,k} \sqcup E_t \sqcup T_{t,k} \ .$$

[3] It is easy to see that this formulation is equivalent to the original one. A formal proof will be given in Corollary 2.3.8.

[4] We are fully aware that there are only $2^k - 1$ elements in $\mathbb{Z}/(2^k-1)\mathbb{Z}$, but we will often use the abuse of terminology we make here and speak of *fraction*, *probability* or *proportion* for $P_{t,k}$.

2.3.2 Mean

For $t \neq t'$, $S_{t,k} \cap S_{t',k} = \emptyset$, so that

$$\begin{aligned} S &= \bigsqcup_{t=0}^{2^k-2} S_{t,k} \\ &= \left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid \mathrm{w_H}(a) + \mathrm{w_H}(b) \leq k-1\right\} \ , \end{aligned}$$

and summing up according to the value of $\mathrm{w_H}(a) + \mathrm{w_H}(b)$, we compute

$$\begin{aligned} \#S &= \sum_{i=0}^{k-1} \binom{2k}{i} \\ &= 2^{2k-1} - \frac{1}{2}\binom{2k}{k} \ . \end{aligned}$$

The following proposition shows that the bound of the conjecture is sharp.

Proposition 2.3.3. *For $k \geq 2$,*

$$\mathrm{E}_t\left(\#S_{t,k}\right) = 2^{k-1}\left(1 - \frac{1}{\sqrt{\pi k}} + o\left(\frac{1}{\sqrt{k}}\right)\right) \ .$$

Proof. Using Stirling's approximation, we have

$$\binom{2k}{k} = \frac{2k!}{k!^2} \sim \frac{2^{2k}}{\sqrt{\pi k}} \ ,$$

and we compute

$$\begin{aligned} \mathrm{E}_t\left(\#S_{t,k}\right) &= \frac{\#S}{2^k-1} \\ &= \frac{2^{2k-1} - \frac{1}{2}\binom{2k}{k}}{2^k-1} \\ &= \frac{2^{2k-1} - \frac{1}{2}\frac{2^{2k}}{\sqrt{\pi k}} + o\left(\frac{2^{2k}}{\sqrt{k}}\right)}{2^k-1} \\ &= \frac{2^{2k-1}}{2^k-1}\left(1 - \frac{1}{\sqrt{\pi k}} + o\left(\frac{1}{\sqrt{k}}\right)\right) \\ &= 2^{k-1}\left(1 + \frac{1}{2^k} + o\left(\frac{1}{2^k}\right)\right)\left(1 - \frac{1}{\sqrt{\pi k}} + o\left(\frac{1}{\sqrt{k}}\right)\right) \\ &= 2^{k-1}\left(1 - \frac{1}{\sqrt{\pi k}} + o\left(\frac{1}{\sqrt{k}}\right)\right) \ . \end{aligned}$$

□

2.3.3 Zero

We now deal with the pathological case $t = 0$.

Proposition 2.3.4. *For $k \geq 2$,*

$$S_{0,k} = \{(0,0)\} \ .$$

Proof. Indeed $(a, b) \in S_{0,k}$ if and only if $b = -a$ and $\mathrm{w_H}(a) + \mathrm{w_H}(-a) = k$ if and only if $a \neq 0$ so that

$$S_{0,k} = \{(0, 0)\} \ .$$ □

Corollary 2.3.5. *For $k \geq 2$,*

$$\#S_{0,k} = 1 \ .$$

From now on, we will always assume that $t \neq 0$, unless explicitly stated otherwise.

2.3.4 Parity

The function swap : $(a, b) \mapsto (b, a)$ is an involution of $C_{t,k,i}$, so that we can prove the following statement.

Proposition 2.3.6. *$S_{t,k}$ is odd if and only if $0 \leq \mathrm{w_H}(t) \leq \frac{k-1}{2}$.*

Proof. Indeed $(b, a) \in S_{t,k}$ if and only if $(a, b) \in S_{t,k}$ and $(b, a) \neq (a, b)$ unless $a = b$, i.e. $a = b = t/2$. Moreover $(t/2, t/2) \in S_{t,k}$ if and only if $2\,\mathrm{w_H}(t/2) \leq k - 1$, i.e. $\mathrm{w_H}(t) = \mathrm{w_H}(t/2) \leq \frac{k-1}{2}$. □

2.3.5 Reformulation in terms of carries

The following proposition is fundamental. It brings to light the importance of the number of carries occurring during the addition.

Proposition 2.3.7. *For $k \geq 2$, $t \in \left(\mathbb{Z}/(2^k - 1)\mathbb{Z}\right)^*$ and $i \in \mathbb{Z}$,*

$$C_{t,k,i} = \{(a, t - a) \mid r(-a, t) = \mathrm{w_H}(t) - i\} \ .$$

Proof. For $(a, b) \in C_{t,k,i}$, we have $a + b = t$, so that $b = t - a$. If $a \neq 0$, using Lemma 2.1.3, our condition for $C_{t,k,i}$ becomes

$$\begin{aligned} \mathrm{w_H}(a) + \mathrm{w_H}(t - a) = k + i &\Leftrightarrow \mathrm{w_H}(-(-a)) + \mathrm{w_H}(-a + t) = k + i \\ &\Leftrightarrow k - \mathrm{w_H}(-a) + \mathrm{w_H}(-a + t) = k + i \\ &\Leftrightarrow r(-a, t) = \mathrm{w_H}(t) - i \ . \end{aligned}$$

We also have $r(-0 = 0, t) = k = \mathrm{w_H}(t) - (\mathrm{w_H}(t) - k)$ so that $(0, t) \in C_{t,k,\mathrm{w_H}(t)-k}$. □

Corollary 2.3.8. *For $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k - 1)\mathbb{Z}\right)^*$,*

$$\#S_{t,k} = \#\left\{a \mid r(a, t) > \mathrm{w_H}(t)\right\} \ .$$

The following lemma allows us to prove some relations between $T_{t,k}$ and $S_{-t,k}$.

Lemma 2.3.9. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k - 1)\mathbb{Z}\right)^*$. If $a \neq 0$ and $a \neq -t$, then*

$$r(a, t) = k - r(-a, -t) \ .$$

If $a = 0$ or $a = -t$, then

$$r(a, t) = r(-a, -t) = k \ .$$

Proof. If $a \neq 0$ and $a \neq -t$, then, going back to the definition of $r(a, t)$, we have

$$\begin{aligned} r(a, t) &= \mathrm{w_H}(a) + \mathrm{w_H}(t) - \mathrm{w_H}(a + t) \\ &= k - \mathrm{w_H}(-a) + k - \mathrm{w_H}(-t) - k + \mathrm{w_H}(-a - t) \\ &= k - r(-a, -t) \ . \end{aligned}$$ □

We introduce the following notation to exclude the special pairs (a, b) involving zero.

Definition 2.3.10. *For $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, we define $S^*_{t,k}$ as*

$$S^*_{t,k} = S_{t,k} \setminus \{(0,t),(t,0)\} \ .$$

We can now relate $T_{t,k}$ and $S_{-t,k}$ either through negation, or through translation.

Proposition 2.3.11. *For $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$T_{t,k} = -S^*_{-t,k} \ .$$

Proof. Indeed, if $(a, t-a) \in T_{t,k}$, then $a \neq 0$, $a \neq t$ and $r(-a,t) < \mathrm{w_H}(t)$, so that $r(a,-t) > \mathrm{w_H}(-t)$ and $(-a, -t+a) \in S^*_{-t,k}$.

Conversely if $(a, -t-a) \in S^*_{-t,k}$, then $(-a, t+a) \in T_{t,k}$. □

Proposition 2.3.12. *For $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$T_{t,k} = t + S^*_{-t,k} \ .$$

Proof. If $(a, -t-a) \in S_{-t,k}$ and $a \neq 0, -t$, then

$$r(-a,-t) = \mathrm{w_H}(-a) + \mathrm{w_H}(-t) - \mathrm{w_H}(-a-t) < \mathrm{w_H}(-t) = k - \mathrm{w_H}(t) \ .$$

Moreover

$$\begin{aligned} r(-t-a,t) &= \mathrm{w_H}(-t-a) + \mathrm{w_H}(t) - \mathrm{w_H}(-t-a+t) \\ &= \mathrm{w_H}(-t-a) + (k - \mathrm{w_H}(-t)) - \mathrm{w_H}(-a) \\ &= k - r(-a,-t) \ , \end{aligned}$$

so that $r(-t-a,-t) > \mathrm{w_H}(t)$ and $t + (a, -t-a) \in T_{t,k}$.

Conversely, if $(a, t-a) \in T_{t,k}$, then $a \neq 0, t$ and $a - t \in S^*_{-t,k}$.

We could also have used the swap function and the previous corollary. □

These relations then relate $S_{t,k}$ and $S_{-t,k}$.

Corollary 2.3.13. *Let $k \geq 2$. If $2t \neq -t$, then*

$$\#S_{t,k} + \#S_{-t,k} \leq 2^k - 1 \ .$$

Otherwise

$$\#S_{t,k} + \#S_{-t,k} \leq 2^k \ .$$

Proof. We already know that $S_{t,k} \sqcup T_{t,k} \subset C_{t,k}$ so that $\#S_{t,k} + \#S_{-t,k} \leq 2^k + 1$. In fact $\mathrm{w_H}(t+t) = \mathrm{w_H}(2t) = \mathrm{w_H}(t)$ so that $(2t, -t)$ and $(-t, 2t)$ are in E_t, i.e. neither in $S_{t,k}$ nor in $T_{t,k}$. Finally

$$\#S_{t,k} + \#S_{-t,k} \leq \begin{cases} 2^k - 1 & \text{if } 2t \neq -t \ , \\ \#S_{t,k} + \#S_{-t,k} \leq 2^k & \text{if } 2t = t \ . \end{cases}$$ □

We can now prove the conjecture in the very specific case where $t \simeq -t$.

Theorem 2.3.14. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$. If $t \simeq -t$, then*

$$\#S_{t,k} \leq 2^{k-1} - 1$$

if $2t \neq -t$, and

$$\#S_{t,k} \leq 2^{k-1}$$

otherwise.

Proof. $t \simeq -t$ so that $\#S_{-t,k} = \#S_{t,k}$. If $2t \neq -t$, then Corollary 2.3.13 becomes

$$\#S_{t,k} \leq 2^{k-1} - \frac{1}{2} \ .$$

But $\#S_{t,k} \in \mathbb{N}$, so that the following inequality holds:

$$\#S_{t,k} \leq 2^{k-1} - 1 \ .$$

If $2t = -t$, then only the following one is true:

$$\#S_{t,k} \leq 2^{k-1} \ . \qquad \square$$

2.3.6 A combinatorial proposition of independent interest

The following quantities may be used to study $\#S_{t,k}$.

Definition 2.3.15. *Let d and n be positive integers and*

- $\Sigma(d,n) = \sum_{l=0}^{n} 2^{-l}\binom{l+d}{d}$,
- $\Delta(d,n) = 2^{-n}\binom{n+d+1}{d}\frac{d-n}{2d+2}$.

They are related through the following combinatorial identity.

Proposition 2.3.16. *For any d, n and e positive integers,*

$$\Sigma(d+e, n+e) = 2^e\Sigma(d,n) + \sum_{l=1}^{e} 2^{e-l}\Delta(d+l-1, n+l-1) \ .$$

Proof. For $e = 1$ and d and n fixed, we compute

$$\begin{aligned}
\Sigma(d+1,n+1) &= \sum_{l=0}^{n+1} 2^{-l} \binom{l+d+1}{d+1} \\
&= \sum_{l=0}^{n+1} 2^{-l} \left(\binom{l+d}{d} + \binom{l+d}{d+1} \right) \\
&= \sum_{l=0}^{n} 2^{-l} \binom{l+d}{d} + 2^{-n-1} \binom{n+d+1}{d} \\
&\quad + \frac{1}{2} \left(\sum_{l=0}^{n+2} 2^{-(l-1)} \binom{(l-1)+d+1}{d+1} \right) \\
&\quad - \frac{1}{2} 2^{-n-1} \binom{n+d+2}{d+1} \\
&= \Sigma(d,n) + 2^{-n-1} \binom{n+d+1}{d} \\
&\quad + \frac{1}{2} \Sigma(d+1,n+1) - \frac{1}{2} 2^{-n-1} \binom{n+d+2}{d+1} \\
&= \Sigma(d,n) + \frac{1}{2} \Sigma(d+1,n+1) \\
&\quad + 2^{-n-1} \binom{n+d+1}{d} \left(1 - \frac{n+d+2}{2d+2} \right) \\
&= \Sigma(d,n) + \frac{1}{2} \Sigma(d+1,n+1) + \frac{1}{2} \Delta(d,n) \ .
\end{aligned}$$

The result follows by induction. □

Corollary 2.3.17. *For any $d \geq 0$ and $e \geq 0$,*

$$\Sigma(d+e,n+e) \geq 2^e \Sigma(d,n)$$

if and only if $n \leq d$.

Proof. Indeed $\Delta(d+i,n+i) \geq 0$ if and only if $n \leq d$. □

As a byproduct, we get the following well-known formula [122, formula 5.20].

Corollary 2.3.18. *For any d positive,*

$$\Sigma(d,d) = 2^d \ .$$

Proof. When $n = d$, the proposition becomes

$$\Sigma(d+e,d+e) = 2^e \Sigma(0,0) = 2^e \ . \qquad \square$$

When $n \to \infty$, the sum converges and we get the following classical result.

Proposition 2.3.19. *Let d be a positive integer. Then*

$$\Sigma(d, "n = \infty") = 2^{d+1} \ .$$

Proof. It follows from the classical identity

$$\frac{1}{(1-z)^{n+1}} = \sum_{k=0}^{\infty} \binom{n+k}{n} z^k \ . \qquad \square$$

2.4 A block splitting pattern

2.4.1 General situation

In this section we often compute $P_{t,k} = \#S_{t,k}/2^k$ rather than $\#S_{t,k}$. Therefore, we use the words *proportion* or *probability* in place of *cardinality*. Moreover, in this subsection, we often compute cardinalities considering all the binary strings on k bits, i.e. including `1...1` and `0...0`. Recall that the modular integer 0 is considered to act as the binary string `1...1`. Hence, the binary string `0...0` should be discarded when doing final computation of $P_{t,k}$. Such a choice ensures that the random variables we construct are truly *independent*.

We split $t \neq 0$ (once correctly rotated, i.e. we multiply it by a power of 2 so that its binary expansion on k bits begins with a `1` and ends with a `0`) in blocks of the form $[\mathtt{1}^*\mathtt{0}^*]$ (i.e. as many `1`'s as possible followed by as many `0`'s as possible) and write it down as follows.

Definition 2.4.1.

$$t = \overbrace{\underbrace{\mathtt{1}\cdots\mathtt{1}\mathtt{0}\cdots\mathtt{0}}_{t_1}}^{\alpha_1\ \beta_1} \cdots \overbrace{\underbrace{\mathtt{1}\cdots\mathtt{1}\mathtt{0}\cdots\mathtt{0}}_{t_i}}^{\alpha_i\ \beta_i} \cdots \overbrace{\underbrace{\mathtt{1}\cdots\mathtt{1}\mathtt{0}\cdots\mathtt{0}}_{t_d}}^{\alpha_d\ \beta_d}$$

with d the number of blocks, α_i and β_i the numbers of `1`'s and `0`'s of the i-th block t_i. We define $B = \sum_{i=1}^{d} \beta_i = k - \mathrm{w_H}(t)$.

We define corresponding values for a (a modular integer to be added to t) as follows.

Definition 2.4.2.

$$t = \overbrace{\mathtt{1}\cdots\mathtt{1}\mathtt{0}\cdots\mathtt{0}}^{\alpha_1\ \beta_1} \cdots \overbrace{\mathtt{1}\cdots\mathtt{1}\mathtt{0}\cdots\mathtt{0}}^{\alpha_i\ \beta_i} \cdots \overbrace{\mathtt{1}\cdots\mathtt{1}\mathtt{0}\cdots\mathtt{0}}^{\alpha_d\ \beta_d},$$

$$a = \underbrace{\mathtt{?}\cdots\mathtt{0}}_{\gamma_1}\underbrace{\mathtt{?}\cdots\mathtt{1}}_{\delta_1} \cdots \underbrace{\mathtt{?}\cdots\mathtt{0}}_{\gamma_i}\underbrace{\mathtt{?}\cdots\mathtt{1}}_{\delta_i} \cdots \underbrace{\mathtt{?}\cdots\mathtt{0}}_{\gamma_d}\underbrace{\mathtt{?}\cdots\mathtt{1}}_{\delta_d},$$

i.e. γ_i is the number of `0`'s in front of the end of the `1`'s subblock of t_i and δ_i is the number of `1`'s in front of the end of the `0`'s subblock of t_i.

One should be aware that γ_i's and δ_i's depend on a and will be considered as variables.
We first "approximate" $r(a,t)$ by $\sum_{i=0}^{d} \alpha_i - \gamma_i + \delta_i$ ignoring the two following facts:

- if a carry goes out of the $i-1$-st block (we say that it *overflows*) and $\delta_i = \beta_i$, the `1`'s subblock produces α_i carries, whatever value γ_i takes;
- and if no carry goes out of the $i-1$-st block (we say that it is *inert*), the `0`'s subblock produces no carries, whatever value β_i takes.

When computing that "approximation" of the number of carries produced by the i-th block, we do as if a carry always goes out of the $i-1$-st block and no carry goes out of the `0`'s subblock. So this is actually the number of carries produced by the $i-1$-st block only in that situation.

Then, $r(a,t) > \mathrm{w_H}(t)$ becomes "approximately" $\sum_{i=1}^{d} \gamma_i < \sum_{i=1}^{d} \delta_i$ and the distributions for γ_i and δ_i, considered as random variables, are given in Table 2.1.

Indeed, for $0 \leq c_i < \alpha_i$,

$$P(\gamma_i = c_i) = 2^{-c_i-1},$$

because we have to set c_i bits to `0` and one bit in front of them to `1` leaving the other bits free, and

$$P(\gamma_i = \alpha_i) = 2^{-\alpha_i}$$

Table 2.1: Distributions of γ_i and δ_i

$c_i =$	0	1	...	c_i	...	$\alpha_i - 1$	α_i	$\alpha_i + 1$	...
$P(\gamma_i = c_i)$	$1/2$	$1/4$	...	$1/2^{c_i+1}$	...	$1/2^{\alpha_i}$	$1/2^{\alpha_i}$	0	...

$d_i =$	0	1	...	d_i	...	$\beta_i - 1$	β_i	$\beta_i + 1$	...
$P(\delta_i = d_i)$	$1/2$	$1/4$	...	$1/2^{d_i+1}$	...	$1/2^{\beta_i}$	$1/2^{\beta_i}$	0	...

and not $2^{-\alpha_i-1}$ because the subblock is already full of `0`'s and there is no `1` in front of them.

The computations are similar for $P(\delta_i = d_i)$ with $0 \leq d_i \leq \beta_i$. Moreover, all the γ_i's and δ_i's are independent, i.e. $P(\gamma_1 = c_1, \ldots, \gamma_d = c_n, \delta_1 = d_1, \ldots, \delta_d = d_d) = \prod_{i=1}^{d} P(\gamma_i = c_i)P(\delta_i = d_i)$.

We modify γ_i and δ_i to take the first fact into account and only do as if a carry always goes out of the $i-1$-st block:

- if $\delta_i \neq \beta_i$, we define $\delta'_i = \delta_i$ and $\gamma'_i = \gamma_i$ as before;
- if $\delta_i = \beta_i$, we define $\delta'_i = \delta_i = \beta_i$ and $\gamma'_i = 0$ (i.e. the carry coming from the previous block goes through the `0`'s subblock so the `1`'s subblock always produces α_i carries).

Then, $\sum_{i=0}^{d} \alpha_i - \gamma'_i + \delta'_i$ should be a better "approximation" of $r(a,t)$, but the γ'_i's and δ'_i's are no longer pairwise independent. Indeed, within the same block, γ'_i and δ'_i are correlated. However, each block remains independent of the other ones and the distributions are given in Table 2.2.

Table 2.2: Distributions for γ'_i and δ'_i

$c_i =$	0	1	...	c_i	...	$\alpha_i - 1$	α_i	$\alpha_i + 1$	...
$P(\gamma'_i = c_i)$	$\frac{1+1/2^{\beta_i}}{2}$	$\frac{1-1/2^{\beta_i}}{4}$	...	$\frac{1-1/2^{\beta_i}}{2^{c_i+1}}$	...	$\frac{1-1/2^{\beta_i}}{2^{\alpha_i}}$	$\frac{1-1/2^{\beta_i}}{2^{\alpha_i}}$	0	...

$d_i =$	0	1	...	d_i	...	$\beta_i - 1$	β_i	$\beta_i + 1$	...
$P(\delta'_i = d_i)$	$1/2$	$1/4$	...	$1/2^{d_i+1}$	...	$1/2^{\beta_i}$	$1/2^{\beta_i}$	0	...

Taking the second fact into account is more difficult, and we do it in an iterative way.

We first take care of the a's such that $r(a,t) = k$, that is exactly those with only `1`'s in front of the `0`'s of t:

- if $\forall i,\ \delta_i = \beta_i$, then $\delta''_i = \delta_i$ and $\gamma''_i = \gamma'_i = 0$.

We now suppose that there exists i_0 such that $\delta_{i_0} \neq \beta_{i_0}$. We first define γ''_{i_0}, then δ''_{i_0-1}, γ''_{i_0-1}, ..., γ''_{i_0+1} and finally δ''_{i_0}:

- set $\gamma''_{i_0} = \gamma_{i_0}$, $i = i_0 - 1$;
- do:
  - $\delta''_i = \delta_i$ if $\gamma_{i+1} \neq \alpha_{i+1}$, 0 otherwise,
  - $\gamma''_i = \gamma_i$ if $\delta''_i \neq \beta_i$, 0 otherwise,
  - $i = i - 1$;

  while $i \neq i_0 - 1$.

The γ_i'''s and δ_i'''s are no longer pairwise independent, even between different blocks, but $r(a,t) = \sum_d \alpha_i - \gamma_i'' + \delta_i''$ and the following proposition is true.

Proposition 2.4.3. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$. Then $a \in S_{t,k}$ if and only if $\sum_d \gamma_i'' < \sum_d \delta_i''$.*

Remember that t is considered to be fixed so that the α_i's and the β_i's are considered to be constants, whereas the other quantities defined in this section depend on a which ranges over all binary strings on k bits and will be considered as random variables, whence the vocabulary we use.

2.4.2 Combining variables

In the previous section we defined two variables for each block. However, we are only really interested in the number of carries, so one should suffice, whence the following definition.

Definition 2.4.4. *We define $\epsilon_i = \gamma_i + \beta_i - \delta_i$, as depicted below:*

$$t = \overbrace{\texttt{1---10}}^{\alpha_1}\overbrace{\texttt{---0}}^{\beta_1}\ldots\overbrace{\texttt{1---10}}^{\alpha_i}\overbrace{\texttt{---0}}^{\beta_i}\ldots\overbrace{\texttt{1---10}}^{\alpha_d}\overbrace{\texttt{---0}}^{\beta_d},$$
$$a = \underbrace{\texttt{?10-0?01-1}}_{\epsilon_1}\ldots\underbrace{\texttt{?10-0?01-1}}_{\epsilon_i}\ldots\underbrace{\texttt{?10-0?01-1}}_{\epsilon_d}.$$

Then ϵ_i is "approximately" the number of carries that do not occur in the i-th block. As in the previous subsection, we define $\epsilon_i' = \gamma_i' + \beta_i - \delta_i'$ and $\epsilon_i'' = \gamma_i'' + \beta_i - \delta_i''$ and Proposition 2.4.3 is reformulated as follows.

Proposition 2.4.5. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$. Then $a \in S_{t,k}$ if and only if $\sum_d \epsilon_i'' < \sum_d \beta_i = B = k - \mathrm{w_H}(t)$.*

2.4.3 One block: $d = 1$

If t is made of only one block, we compute closed-form expressions for $\#C_{t,k,i} = 2^k P(\epsilon'' = k-i)$ for all i where $P(\epsilon'' = k-i)$ is nothing but the probability that i carries occurs while adding t and a, or equivalently the probability that $k-i$ carries are *lost*.

Such a $t \neq 0$ (or an equivalent one) is written $t = 2^k - 2^{k-\alpha}$ (i.e. $t = \underbrace{\texttt{1...1}}_{\alpha}\underbrace{\texttt{0...0}}_{\beta=k-\alpha}$) and its weight is $\mathrm{w_H}(t) = \alpha$ with $\alpha \geq 1$.

In the following proposition, the computations are made without including the binary string `0...0` in contrast with what was done in Subsection 2.4.1 because it does not complicate them too much.

Proposition 2.4.6. *The distribution of ϵ'' is as follows:*

$$P(\epsilon'' = 0) = 2^{-\beta} \ ;$$

for $0 < e < \alpha + \beta$,

$$P(\epsilon'' = e) = 2^{-|e-\beta|}\frac{1-4^{M-m}}{3} \ ,$$

with

$$m = \min(e, \alpha) \text{ and } M = \max(0, e-\beta) \ ;$$

and

$$P(\epsilon'' = \alpha + \beta) = 2^{-\alpha} - 2^{-\alpha-\beta} \ .$$

Proof. If $\delta = \beta$, i.e. if there are only `1`'s in front of the `0`'s of t, then $\gamma'' = 0$ and we lose no carries whatever value γ takes, i.e. whatever is in front of the `1`'s of t. Moreover, such numbers are the only ones such that we lose no carries and the block overflows, therefore

$$P(\epsilon'' = 0) = P(\delta = \beta) = 2^{-\beta} \ .$$

One must be aware that we included the binary string `1...1`, but remember that it accounts for the modular integer 0.

When $\delta \neq \beta$ and $\gamma = \alpha$, we lose all the carries whatever value δ takes, and that is the only possibility to do so. Therefore

$$P(\epsilon'' = \alpha + \beta) = P(\gamma = \alpha, \delta \neq \beta) - 2^{-\alpha-\beta} = 2^{-\alpha} - 2^{-\alpha-\beta} \ .$$

We subtract $2^{-\alpha-\beta}$ because we do not want to count the binary string `0...0`.

Finally, when $\delta \neq \beta$ and $\gamma \neq \alpha$, the situation is described below:

$$t \leftarrow \overbrace{\texttt{1---1}}^{\alpha}\overbrace{\texttt{0---0}}^{\beta}\leftarrow,$$
$$a = \texttt{?}\underbrace{\texttt{10-0?01-1}}_{\epsilon} \ .$$

A carry comes out of the block and goes back into itself. Then, we lose exactly $e = \epsilon'' = \gamma+\beta-\delta = \epsilon$ carries and $0 < e < \alpha + \beta - 1$. We have the following constraints:

$$0 \leq \gamma \leq \alpha - 1 \text{ and } 0 \leq \delta \leq \beta - 1 \ ,$$

but $\delta = \beta + \gamma - e$ so γ must be bounded as follows:

$$M = \max(0, e - \beta) \leq \gamma \leq m - 1 = \min(e, \alpha) - 1 \ .$$

Finally, $P(\epsilon'' = e)$ for $0 < e < \alpha + \beta$ is computed as

$$\begin{aligned} P(\epsilon'' = e) &= \sum_{\gamma=M}^{m-1} 2^{-\gamma-\delta-2} = \sum_{\gamma=M}^{m-1} 2^{e-\beta-2\gamma-2} \\ &= 2^{e-\beta-2M-2} \sum_{\gamma=0}^{m-M-1} 2^{-2\gamma} = 2^{-|e-\beta|-2} \frac{1-(1/4)^{m-M}}{3/4} \\ &= 2^{-|e-\beta|} \frac{1-4^{M-m}}{3} \ . \end{aligned}$$

□

The probabilities that we computed above will be useful in the next sections, so we define them more formally.

Definition 2.4.7. *For $0 \leq e < \alpha + \beta$, we define*

$$P(e) = \begin{cases} 2^{-\beta} & \text{if } e = 0 \\ 2^{-|e-\beta|} \frac{1-4^{M-m}}{3} & \text{if } e \neq 0 \end{cases} \ ,$$

with

$$m = \min(e, \alpha) \text{ and } M = \max(0, e - \beta) \ ;$$

the values of α and β will be clear from the context. Morally, $P(e)$ will be equal to $P(\epsilon'' = e)$ for suitable values of e.

Summing up the above formulae, we get the following theorem.

Theorem 2.4.8. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ made of one block. Then*

$$P_{t,k} = \begin{cases} 2^{-\alpha-\beta}\frac{1-2^{-2\alpha}}{3} & \text{if } 1 \leq \alpha \leq \frac{k-1}{2} \ , \\ \frac{1+2^{-2\beta+1}}{3} & \text{if } \frac{k-1}{2} \leq \alpha \leq k-1 \ . \end{cases}$$

For $\alpha = 1$, it reads $S_{1,k} = 2^{k-2}+1$ and for $\alpha = k-1$, it reads $S_{-1,k} = 2^{k-1}$.

Proof. Propositions 2.4.5 and 2.4.6 say that

$$P_{t,k} = \sum_{e=0}^{\beta-1} P(e) \ .$$

Moreover, for such values of e, $\beta - e$ is always positive so that $|\beta - e| = \beta - e$ and $M = 0$. Finally, $m = e$ as long as $e \leq \alpha$ which is always true if and only if $\beta - 1 \leq \alpha$ or equivalently $\frac{k-1}{2} \leq \alpha$.

If $0 < \alpha < \frac{k-1}{2}$, then $P_{t,k}$ is computed as

$$\begin{aligned} P_{t,k} &= 2^{-\beta} + \sum_{e=1}^{\alpha-1} 2^{e-\beta}\frac{1-4^{-e}}{3} + \sum_{e=\alpha}^{\beta-1} 2^{e-\beta}\frac{1-4^{-\alpha}}{3} \\ &= 2^{-\beta} + \frac{2^{-\beta}}{3}\sum_{e=1}^{\alpha-1}(2^e - 2^{-e}) + \frac{2^{-\beta}(1-4^{-\alpha})}{3}\sum_{e=\alpha}^{\beta-1} 2^e \\ &= 2^{-\beta} + \frac{2^{-\beta}}{3}\left((2^\alpha - 1) + 2\cdot(2^{-\alpha}-1)\right) + \frac{2^{-\beta}(1-4^{-\alpha})}{3}2^\alpha(2^{\beta-\alpha}-1) \\ &= 2^{-\beta} + \frac{2^{\alpha-\beta} - 2^{-\beta} + 2^{-\alpha-\beta+1} - 2^{-\beta+1}}{3} + \frac{1 - 2^{-2\alpha} - 2^{\alpha-\beta} + 2^{-\alpha-\beta}}{3} \\ &= 2^{-\beta} + \frac{1 - 3\cdot 2^{-\beta} - 3\cdot 2^{-\alpha-\beta} - 2^{-2\alpha}}{3} \\ &= 2^{-\alpha-\beta}\frac{1-2^{-2\alpha}}{3} \ . \end{aligned}$$

If $\frac{k-1}{2} \leq \alpha < k$, then the calculation is somewhat easier:

$$\begin{aligned} P_{t,k} &= 2^{-\beta} + \sum_{e=1}^{\beta-1} 2^{e-\beta}\frac{1-4^{-e}}{3} \\ &= 2^{-\beta} + \frac{2^{-\beta}}{3}\sum_{e=1}^{\beta-1}(2^e - 2^{-e}) \\ &= 2^{-\beta} + \frac{2^{-\beta}}{3}\left((2^\beta - 1) + 2\cdot(2^{-\beta}-1)\right) \\ &= 2^{-\beta} + \frac{1 - 2^{-\beta} + 2^{-2\beta+1} - 2^{-\beta+1}}{3} \\ &= \frac{1+2^{-2\beta+1}}{3} \ . \end{aligned}$$

□

2.4.4 A helpful constraint: $\min_i(\alpha_i) \geq B - 1$

Until the end of this section we add the following constraint on t:

$$\min_i(\alpha_i) \geq \sum_{i=1}^{d} \beta_i - 1 = B - 1 = k - \mathrm{w_H}(t) - 1 \ .$$

That condition tells us that, if a is in $S_{t,k}$, then a carry has to go through each subblock of `1`'s, i.e. $\gamma_i'' \neq \alpha_i$, otherwise too many carries would already be lost in the corresponding single block. Indeed, if $\gamma_i'' = \alpha_i$, then $\delta_i'' < \beta_i$ and $\epsilon_i'' = \gamma_i'' + \beta_i - \delta_i'' \geq \alpha_i + 1 \geq B$. This obviously implies that $\sum_{i=1}^{d} \epsilon_i'' \geq B$ and that $a \notin S_{t,k}$. Therefore, if $a \in S_{t,k}$, then each block has to overflow. In such a situation, the blocks are therefore kind of independent.

Recall that the definitions of the quantities γ_i', δ_i', γ_i'' and δ_i'' in Subsection 2.4.1 trivially imply that the inequality $\sum_{i=1}^{d} \gamma_i' < \sum_{i=1}^{d} \delta_i'$ always implies the inequality $\sum_{i=1}^{d} \gamma_i'' < \sum_{i=1}^{d} \delta_i''$. Formulated in a different way, it means that the inequality $\sum_{i=1}^{d} \gamma_i' < \sum_{i=1}^{d} \delta_i'$ always implies that $a \in S_{t,k}$. With our additional constraint the converse, which is obviously false in general, becomes true.

In fact, whether the constraint is verified or not:

- if $\forall i \ \delta_i'' = \beta_i$, then there are only `1`'s in front of the `0`'s of t, and both definitions coincide: $\gamma_i'' = \gamma_i' = 0$ and $\delta_i'' = \delta_i' = \beta_i$ — we always get k carries whatever values the γ_i's take —;

- if $\forall i \ \gamma_i'' \neq \alpha_i$, then a carry goes out of each subblock of `1`'s, and both definitions also coincide: $\gamma_i'' = \gamma_i'$ and $\delta_i'' = \delta_i'$.

Finally, if the constraint is verified and we are not in one of the above two situations, then there are indices i and j such that $\delta_i'' \neq \beta_i$ and $\gamma_j'' = \alpha_j$, which implies that $\sum_{i=1}^{d} \gamma_i'' \geq B > \sum_{i=1}^{d} \delta_i''$. Moreover, $\sum_{i=1}^{d} \gamma_i' \geq \sum_{i=1}^{d} \gamma_i''$ and $B > \sum_{i=1}^{d} \delta_i'$, so that $\sum_{i=1}^{d} \gamma_i' \geq \sum_{i=1}^{d} \delta_i'$.

To summarize, we have just shown that, in our constrained case, there is an equivalence between $a \in S_{t,k}$ and $\sum_{i=1}^{d} \gamma_i' < \sum_{i=1}^{d} \delta_i'$. Hence, we can formulate $P_{t,k}$ as follows.

Proposition 2.4.9. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k - 1)\mathbb{Z}\right)^*$ verifying the constraint*

$$\min_i(\alpha_i) \geq \sum_{i=1}^{d} \beta_i - 1 = B - 1 = k - \mathrm{w_H}(t) - 1 \ .$$

Then

$$P_{t,k} = \sum_{\Delta=1}^{B} \sum_{\Gamma=0}^{\Delta-1} 2^{-\Delta-\Gamma-2d} \sum_{\substack{\sum_d \gamma_i' = \Gamma \\ 0 \leq \gamma_i'}} \sum_{\substack{\sum_d \delta_i' = \Delta \\ 0 \leq \delta_i' \leq \beta_i}} 2^{2\#\{i \mid \delta_i = \beta_i\}} 1_{\delta_i' = \beta_i, \gamma_i' = 0} \ .$$

Proof.

$$\begin{aligned}
P_{t,k} &= P\left[\sum_d \gamma' < \sum_d \delta'\right] \\
&= \sum_{\Delta=1}^{B}\sum_{\Gamma=0}^{\Delta-1} \sum_{\substack{\sum_d \gamma'_i=\Gamma \\ 0\le\gamma'_i}} \sum_{\substack{\sum_d \delta'_i=\Delta \\ 0\le\delta'_i\le\beta_i}} P(\gamma',\delta') \\
&= \sum_{\Delta=1}^{B}\sum_{\Gamma=0}^{\Delta-1} \sum_{\substack{\sum_d \gamma'_i=\Gamma \\ 0\le\gamma'_i}} \sum_{\substack{\sum_d \delta'_i=\Delta \\ 0\le\delta'_i\le\beta_i}} \prod_d P(\gamma'_i,\delta'_i) \\
&= \sum_{\Delta=1}^{B}\sum_{\Gamma=0}^{\Delta-1} \sum_{\substack{\sum_d \gamma'_i=\Gamma \\ 0\le\gamma'_i}} \sum_{\substack{\sum_d \delta'_i=\Delta \\ 0\le\delta'_i\le\beta_i}} \prod_d P(\delta'_i)P(\gamma'_i \mid \delta'_i) \\
&= \sum_{\Delta=1}^{B}\sum_{\Gamma=0}^{\Delta-1} \sum_{\substack{\sum_d \gamma'_i=\Gamma \\ 0\le\gamma'_i}} \sum_{\substack{\sum_d \delta'_i=\Delta \\ 0\le\delta'_i\le\beta_i}} 2^{-\Delta-d+\#\{i\mid\delta_i=\beta_i\}} \prod_d P(\gamma'_i \mid \delta'_i) \\
&= \sum_{\Delta=1}^{B}\sum_{\Gamma=0}^{\Delta-1} \sum_{\substack{\sum_d \gamma'_i=\Gamma \\ 0\le\gamma'_i}} \sum_{\substack{\sum_d \delta'_i=\Delta \\ 0\le\delta'_i\le\beta_i}} 2^{-\Delta-\Gamma-2d+2\#\{i\mid\delta_i=\beta_i\}} 1_{\delta'_i=\beta_i,\gamma'_i=0} \\
&= \sum_{\Delta=1}^{B}\sum_{\Gamma=0}^{\Delta-1} 2^{-\Delta-\Gamma-2d} \sum_{\substack{\sum_d \gamma'_i=\Gamma \\ 0\le\gamma'_i}} \sum_{\substack{\sum_d \delta'_i=\Delta \\ 0\le\delta'_i\le\beta_i}} 2^{2\#\{i\mid\delta_i=\beta_i\}} 1_{\delta'_i=\beta_i,\gamma'_i=0} \ . \qquad \square
\end{aligned}$$

The above discussion also shows that $a \in S_{t,k}$ is equivalent to $\sum_d \epsilon'_i < k - \mathrm{w_H}(t)$. Moreover, as was already mentioned above, if that inequality is verified, then each block overflows into the next one. That is exactly the situation that was studied in the previous subsection when t was made of one block, so that the computations we did there are still valid (only to compute $\#C_{t,k,i}$ with $i < 0$ where only a's in $S_{t,k}$ are enumerated, but not with $i \ge 0$) and we get the following proposition.

Proposition 2.4.10. *Let $k \ge 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ verifying*

$$\min_i(\alpha_i) \ge \sum_{i=1}^{d} \beta_i - 1 = B - 1 = k - \mathrm{w_H}(t) - 1 \ .$$

Then

$$\begin{aligned}
P_{t,k} &= \sum_{E=0}^{B-1} \sum_{\substack{\sum_d e_i=E \\ 0\le e_i}} \prod_d P(e_i) \\
&= 2^{-B}3^{-d} \sum_{E=0}^{B-1} 2^{-E} \sum_{\substack{\sum_d e_i=E \\ 0\le e_i}} \prod_d \left(4^{\max(1,\min(e_i,\beta_i))} - 1\right) \ .
\end{aligned}$$

Proof. We replace α by α_i and β by β_i in the expression of Definition 2.4.7 and get for $1 \leq e_i$ that

$$\begin{aligned} P(e_i) &= 2^{-|e_i-\beta_i|}\frac{1-4^{\max(0,e_i-\beta_i)-e_i}}{3} \\ &= 2^{-\beta_i+e_i-2\max(0,e_i-\beta_i)+2\max(0,e_i-\beta_i)-2e_i}\frac{4^{-\max(0,e_i-\beta_i)+e_i}-1}{3} \\ &= 2^{-\beta_i-e_i}\frac{4^{\min(e_i,\beta_i)}-1}{3} \ . \end{aligned}$$

Considering the case $e_i = 0$ gives the complete formula. □

Using that formula, it is possible to compute the exact value of $P_{t,k}$ for a given d and a corresponding set of β_i's. It is also worth noting that the ordering of the β_i's does not matter because each subblock behaves the same when a is in $S_{t,k}$ — more precisely, it overflows — whence the following definition.

Definition 2.4.11. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ verifying*

$$\min_i(\alpha_i) \geq \sum_{i=1}^{d}\beta_i - 1 = B - 1 = k - \mathrm{w_H}(t) - 1 \ .$$

Then we define $f_d(\beta_1, \ldots, \beta_d)$ as

$$f_d(\beta_1, \ldots, \beta_d) = P_{t,k} \ .$$

The value of $P_{t,k}$ does not depend on the particular choice of t verifying the constraint; in particular it depends neither on the values of k and the α_i's, nor on the exact ordering of the β_i's, so that the function f_d is well defined.

It is in fact enough to have $\min_i(\alpha_i) \geq B - 2$ to ensure that a carry goes through each block when $a \in S_{t,k}$, but when equality holds the blocks are not independent anymore.

2.4.5 Analytic study: $d = 2$

In this subsection we study the function f_d using analytic means when $d = 2$.

Proposition 2.4.12. *The function f_2 is given by*

$$\begin{aligned} f_2(x,y) = \frac{11}{27} &+ 4^{-x}\left(\frac{2}{9}x - \frac{2}{27}\right) \\ &+ 4^{-y}\left(\frac{2}{9}y - \frac{2}{27}\right) + 4^{-x-y}\left(\frac{20}{27} - \frac{2}{9}(x+y)\right) \ . \end{aligned}$$

Proof. Let $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ be any number made of two blocks corresponding to β_1 and β_2 and such that $\min(\alpha_1, \alpha_2) \geq \beta_1 + \beta_2 - 1$. Then

$$P_{t,k} = f_2(\beta_1, \beta_2) \ .$$

According to Proposition 2.4.10, $P_{t,k}$ is given by

$$\begin{aligned} P_{t,k} &= \sum_{E=0}^{B-1} \sum_{\substack{e_1+e_2=E \\ 0\le e_1,e_2}} P(e_1)P(e_2) \\ &= 2^{-\beta_1-\beta_2}(\Sigma_{e_1\neq 0,e_2\neq 0} \\ &\quad + \Sigma_{e_1=0,e_2\neq 0} + \Sigma_{e_1\neq 0,e_2=0} + \Sigma_{e_1=0,e_2=0}) \ , \end{aligned}$$

where

$$\begin{aligned} \Sigma_{e_1\neq 0,e_2\neq 0} &= \sum_{e_1=0}^{\beta_1-1} \frac{2^{e_1}-2^{-e_1}}{3} \left(\sum_{e_2=0}^{\beta_2-1} \frac{2^{e_2}-2^{-e_2}}{3} + \sum_{e_2=\beta_2}^{\beta_1+\beta_2-1-e_1} 2^{-e_2}\frac{4^{\beta_2}-1}{3} \right) \\ &\quad + \sum_{e_1=\beta_1}^{\beta_1+\beta_2-1} 2^{-e_1}\frac{4^{\beta_1}-1}{3} \sum_{e_2=0}^{\beta_1+\beta_2-1-e_1} \frac{2^{e_2}-2^{-e_2}}{3} \\ \Sigma_{e_1=0,e_2\neq 0} &= \sum_{e_2=0}^{\beta_2-1} \frac{2^{e_2}-2^{-e_2}}{3} + \sum_{e_2=\beta_2}^{\beta_1+\beta_2-1} 2^{-e_2}\frac{4^{\beta_2}-1}{3} \\ \Sigma_{e_1\neq 0,e_2=0} &= \sum_{e_1=0}^{\beta_1-1} \frac{2^{e_1}-2^{-e_1}}{3} + \sum_{e_1=\beta_1}^{\beta_1+\beta_2-1} 2^{-e_1}\frac{4^{\beta_1}-1}{3} \\ \Sigma_{e_1=0,e_2=0} &= 1 \ . \end{aligned}$$

An easy but quite lengthy and error-prone calculation, which can be checked with a symbolic calculus software, leads to the desired expression.

This result can also be seen as a consequence of Proposition 2.5.1 in Section 2.5. □

The graph of f_2, computed with Sage [250], is given in Figures 2.1 and 2.2.

Proposition 2.4.13. *For all $x, y \ge 1$ in $\mathbb{N}$,*

$$f_2(x,y) \le \frac{1}{2} \ .$$

Proof.

$$\begin{aligned} \frac{\partial f_2}{\partial x}(x,y) &= \frac{2}{9}4^{-x}\ln 4(4^{-y}-1)x \\ &\quad + \frac{2}{9}4^{-x}\left(4^{-y}\ln 4\left(y-\frac{10}{3}\right) - 4^{-y} + \frac{1}{3}\ln 4 + 1\right) \ , \end{aligned}$$

so that for $y > 0$, $\frac{\partial f_2}{\partial x}(x,y) \ge 0$ is equivalent to

$$x \le \frac{(\frac{1}{3}+\frac{1}{2\ln 2})4^y + y - \frac{1}{2\ln 2} - \frac{10}{3}}{4^y-1} \ .$$

We denote the left hand side of that inequality by $h(y)$. Unfortunately, it happens that $h(y) > 1$ when $y \ge 1$. However, $f_2(\max(1,h(y)),y) \le \frac{1}{2}$ for $y \ge 1$, so that $f_2(x,y) \le \frac{1}{2}$ for $x, y \ge 1$ in $\mathbb{R}$. We do not prove that here for the sake of simplicity, but only that $f_2(x,y) \le \frac{1}{2}$ for $x, y \ge 1$ in $\mathbb{N}$ which is the case we are really interested in.

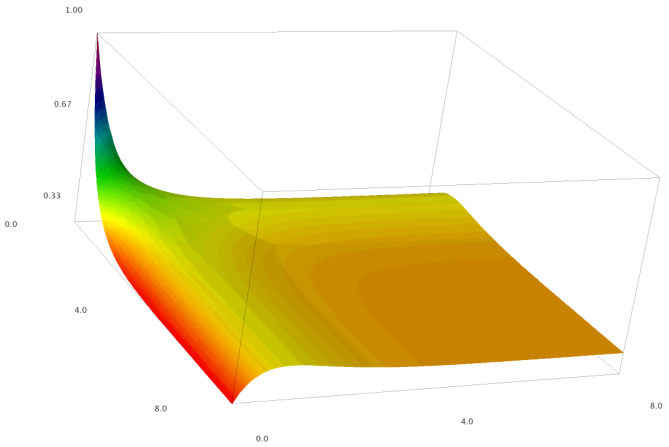


Figure 2.1: Graph of $f_2(x, y)$ for $0 \leq x, y \leq 8$

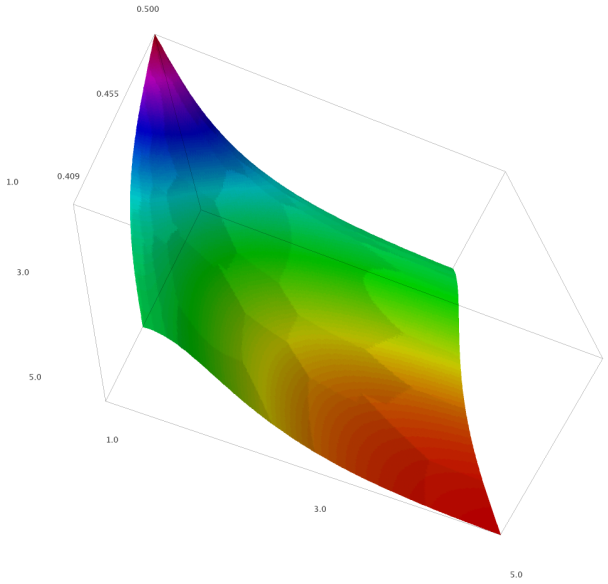


Figure 2.2: Zoom on the graph of $f_2(x, y)$ for $1 \leq x, y \leq 5$

Let $g(x) = 4^{-x}\left(x - \frac{1}{3}\right)$. Then its derivative is

$$g'(x) = \left(1 + \frac{\ln 4}{3} - \ln 4x\right) 4^{-x} \ ,$$

so that for $x \geq 0$, $g'(x) \geq 0 \Leftrightarrow x \leq \frac{1}{2\ln 2} + \frac{1}{3} = x_{\max}$.

Moreover $1 < x_{\max} \approx 1.054 < 2$ so that

$$g(x) \leq \max(g(1), g(2)) = g(1) = \frac{1}{6} \ .$$

Finally, we get that

$$f_2(x,y) \leq \frac{11}{27} + \frac{1}{27} + \frac{1}{27} + \frac{1}{54} = \frac{1}{2} \ . \qquad \square$$

It should be remarked that $f_2(x,y) \to \frac{11}{27}$ when $x, y \to \infty$ which agrees with the results for $d = 2$ of Subsection 2.6.1.

We have just proved the following theorem.

Theorem 2.4.14. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ verify the following constraints:*

- *t is made of two blocks, i.e. $d = 2$;*
- *the two blocks of `1`'s of t are of length at least $B-1$, i.e. $\alpha_1,\ \alpha_2 \geq B-1$.*

Then

$$\#S_{t,k} \leq 2^{k-1} \ .$$

2.4.6 Extremal value: $\beta_i = 1$

We now add another constraint: the `0`'s of t are isolated, that is

$$\forall i,\ \beta_i = 1 \ .$$

The previous cosntraint then becomes

$$\min_i(\alpha_i) \geq B - 1 = d - 1 \ .$$

Theorem 2.4.15. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ verify the two following constraints:*

- *$\forall i,\ \beta_i = 1$,*
- *$\min_i(\alpha_i) \geq B - 1 = d - 1$.*

Then

$$\#S_{t,k} = 2^{k-1} \ .$$

Proof. With the additional constraint, for $e_i = 0$, $P(e_i)$ is

$$P(0) = 2^{-1} \ ;$$

and for $0 < e_i < B$,

$$\begin{aligned} P(e_i) &= 2^{-|e_i - 1|}\frac{1 - 4^{M-m}}{3} \\ &= 2^{-e_i+1}\frac{1 - 4^{e_i - 1 - e_i}}{3} \\ &= 2^{-e_i-1} \ , \end{aligned}$$

so that $P(e_i) = 2^{-e_i-1}$ for all the values of e_i we are interested in.

According to Proposition 2.4.10, $P_{t,k}$ is now

$$\begin{aligned} P_{t,k} &= \sum_{E=0}^{d-1} \sum_{\substack{\sum_d e_i = E \\ 0 \le e_i}} \prod_{i=1}^{d} 2^{-e_i-1} \\ &= \sum_{E=0}^{d-1} 2^{-E-d} \sum_{\substack{\sum_d e_i = E \\ 0 \le e_i}} 1 \\ &= 2^{-d} \sum_{E=0}^{d-1} 2^{-E} \binom{E+d-1}{d-1} \\ &= \frac{2^{d-1}}{2^d} \\ &= \frac{1}{2} \ . \end{aligned}$$

In that case we can also see $\epsilon'_i = \gamma'_i + (1 - \delta'_i) = \gamma_i(1 - \delta_i)$ as the number of `0`'s at the end of each block:

$$\begin{aligned} t &= \texttt{1--10...1--10...1--10} \ , \\ a &= \texttt{?10-0...?10-0...?10-0} \ , \\ &\qquad \underbrace{\phantom{\texttt{?10-0}}}_{\epsilon'_1} \quad \underbrace{\phantom{\texttt{?10-0}}}_{\epsilon'_i} \quad \underbrace{\phantom{\texttt{?10-0}}}_{\epsilon'_d} \end{aligned}$$

and directly compute $P(\epsilon''_i = e_i) = P(\epsilon'_i = e_i) = 2^{-e_i-1}$ for the values of e_i we are interested in. □

As a byproduct, we get an interesting combinatorial equality.

Corollary 2.4.16. *Let $d \ge 1$. Then*

$$\sum_{\Gamma=0}^{d-1} 2^{-\Gamma} \sum_{\Delta=\Gamma+1}^{d} 2^{\Delta} \binom{d}{\Delta} \binom{\Gamma+d-\Delta-1}{d-\Delta-1} = 2^{2d-1} \ .$$

Proof. Indeed, using Proposition 2.4.9, $P_{t,k}$ is written

$$\begin{aligned} P_{t,k} &= \sum_{\Delta=1}^{d} \sum_{\Gamma=0}^{\Delta-1} 2^{-\Gamma+\Delta-2d} \sum_{\substack{\sum_d \delta'_i = \Delta \\ \delta'_i = 0,1}} \sum_{\substack{\sum_d \gamma'_i = \Gamma \\ 0 \le \gamma'_i}} 1_{\delta'_i=1, \gamma'_i=0} \\ &= 2^{-2d} \sum_{\Gamma=0}^{d-1} 2^{-\Gamma} \sum_{\Delta=\Gamma+1}^{d} 2^{\Delta} \binom{d}{\Delta} \binom{\Gamma+d-\Delta-1}{d-\Delta-1} \ . \end{aligned}$$

□

And using Corollary 2.3.13, we prove the conjecture in the following additional case.

Corollary 2.4.17. *Let $k \ge 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ verify the two following constraints:*

- $\forall i, \ \beta_i = 1$,

- $\min_i(\alpha_i) \geq B - 1 = d - 1$.

Then

$$\#S_{-t,k} \leq 2^{k-1} \ .$$

Proof. According to Corollary 2.3.13, $\#S_{t,k} + \#S_{-t,k} \leq 2^k$ so that $\#S_{-t,k} \leq 2^{k-1}$. □

The theoretical study of the conjecture, together with experimental results obtained with Sage [250], lead us to conjecture that the converse of Theorem 2.4.15 is also true, i.e. the numbers of Theorem 2.4.15 are the only ones reaching the bound of Conjecture 1.2.2, which is obviously stronger than the original conjecture.

Conjecture 2.4.18. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$. Then $S_{t,k} = 2^{k-1}$ if and only if t verifies the two following constraints:*

- $\forall i,\ \beta_i = 1$,
- $\min_i(\alpha_i) \geq B - 1 = d - 1$.

2.5 A closed-form expression for f_d

The main goal of this section is to describe a closed-form expression for $f_d(\beta_1, \ldots, \beta_d)$ and study its properties.

After giving some experimental results in Subsection 2.5.1, we will prove that f_d has the following "polynomial" expression.

Proposition 2.5.1. *For any $d \geq 1$, f_d can be written in the following form:*

$$f_d(\beta_1, \ldots, \beta_d) = \sum_{I \subset \{1,\ldots,d\}} 4^{-\sum_{i\in I} \beta_i} P_d^{\#I}(\{\beta_i\}_{i\in I}) \ ,$$

where P_d^n is a symmetric multivariate polynomial in n variables of total degree $d-1$ and of degree $d-1$ in each variable if $n > 0$. If $n = 0$, then $P_d^0 = \frac{1}{2}(1 - P_d)$, the value computed in Corollary 2.6.16.

The proof of this result covers three subsections:

1. in Subsection 2.5.2, we split the expression giving f_d as a sum into smaller pieces and establish a recursion relation in d;
2. in Subsection 2.5.3, we study the expression of the residual term appearing in this relation;
3. in Subsection 2.5.4, we put the pieces back together to conclude.

Once this proposition is shown, we will be allowed to denote by $a^{d,n}_{(i_1,\ldots,i_n)}$ the coefficient of $P_d^n(x_1, \ldots, x_n)$ of multi-degree $(i_1, \ldots, i_n)$ normalized by 3^d. In Subsection 2.5.5, we give simple expressions for some specific values of $a^{d,n}_{(i_1,\ldots,i_n)}$ as well as the following general expression.

Proposition 2.5.2. *Suppose that $i_1 \geq \cdots \geq i_m \neq 0 > i_{m+1} = 0 = \cdots = i_n = 0$ and $m > 0$. Let l denote the sum $l = i_1 + \ldots + i_n > 0$ (i.e. the total degree of the monomial). Then*

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \binom{l}{i_1, \ldots, i_n} b^{d,n}_{l,m} \ ,$$

where $\binom{l}{i_1,\ldots,i_n}$ *is a multinomial coefficient and* $b_{l,m}^{d,n}$ *is defined as*

$$b_{l,m}^{d,n} = \sum_{\mathtt{i}=0}^{n-m} \binom{n-m}{\mathtt{i}} \sum_{\mathtt{j}=0}^{d-n} \binom{d-n}{\mathtt{j}} \sum_{k_j \geq 0, j \in I \cup J, 1 \leq j \leq m} \frac{(l+S-m)!}{l!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ l+S-m \end{bmatrix} \right) \prod_{j \in J} \frac{A_{k_j}}{k_j!} \prod_{j \in I} \frac{A_{k_j} - 3_{k_j=0}}{k_j!} \prod_{j=1}^{m} \frac{C_{k_j-1}}{|k_j - 1|!} \ .$$

Within the above expression for $b_{l,m}^{d,n}$*, the following notation is used:*

- $I = \{m+1, \ldots, m+\mathtt{i}\}$*;*
- $J = \{n+1, \ldots, n+\mathtt{j}\}$*;*
- $S = \sum_{j \in I \cup J, 1 \leq j \leq m} k_j$*;*
- $h = d - m - \mathtt{j} - \mathtt{i}$*;*

and

$$C_j = \begin{cases} A_j + \frac{B_{j+1}}{j+1} & \text{if } j > 0 \ , \\ -\frac{13}{6} & \text{if } j = 0 \ , \\ 1 & \text{if } j = -1 \ . \end{cases}$$

Here, A_i is a sum of Eulerian numbers and B_i a Bernoulli number; both are described in Subsection 2.5.3.

Finally, we prove in Subsection 2.5.6 an additional property predicted experimentally.

Proposition 2.5.3. *For* $0 < j \leq i$*,*

$$a_{(i,j,\ldots)}^{d,n} = \frac{i+1}{j} a_{(i+1,j-1,\ldots)}^{d,n} \ ;$$

i.e. the value of $b_{l,m}^{d,n}$ *does not depend on* m*.*

2.5.1 Experimental results

For $d = 1$, by Theorem 2.4.8, we have

$$f_1(\beta_1) = \frac{2}{3} 4^{-\beta_1} + \frac{1}{3} \ .$$

The case $d = 2$ has been treated in Subsection 2.4.5 and leads to a similar expression:

$$f_2(\beta_1, \beta_2) = \frac{11}{27} + 4^{-\beta_1} \left(\frac{2}{9}\beta_1 - \frac{2}{27} \right) + 4^{-\beta_2} \left(\frac{2}{9}\beta_2 - \frac{2}{27} \right) + 4^{-\beta_1-\beta_2} \left(\frac{20}{27} - \frac{2}{9}(\beta_1 + \beta_2) \right) \ .$$

In both these cases, f_d has the correct form and has been shown to verify Conjecture 1.2.2.

The tables in Appendix A give the normalized coefficients $a_{(i_1,\ldots,i_n)}^{d,n}$ of the multivariate polynomials P_d^n for the first few d's. All of these data were computed symbolically using Sage [250], Pynac [268] and Maxima [267]. As a byproduct of this work, the interface between Sage [250]

and Maxima [267] was completely rewritten[5]. The functions used for internal comparison in Pynac [268] were also completely rewritten[6]. Graphs of some functions derived from f_d are given in Figures 2.3, 2.4 and 2.5.

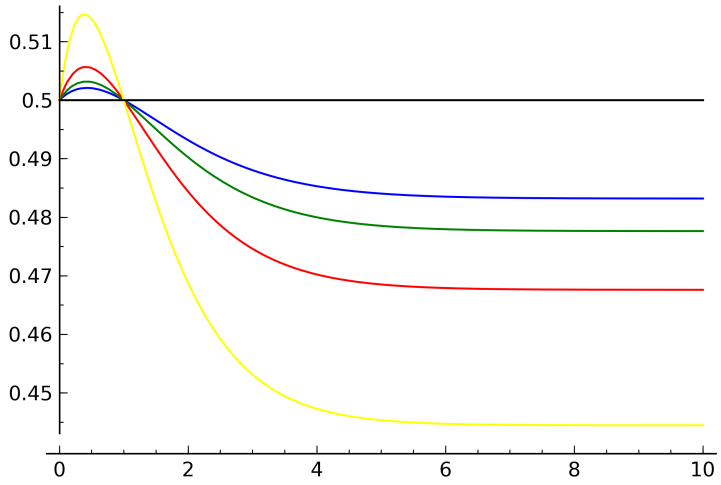


Figure 2.3: Graph of $f_d(\beta_i)$ for $\beta_i = 1$, $i \neq 1$

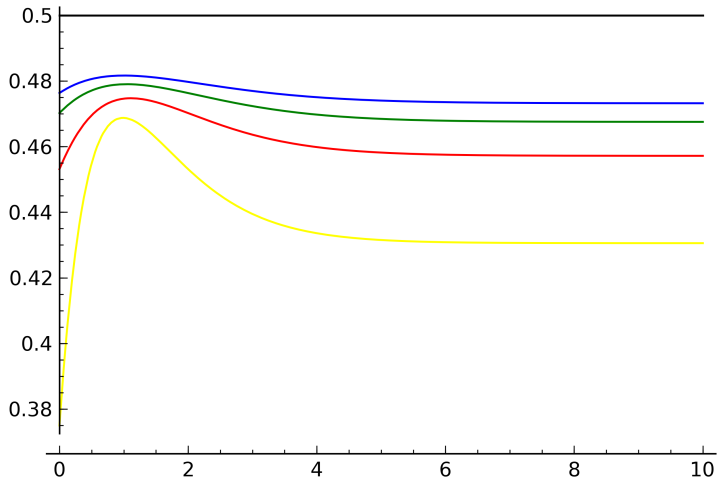


Figure 2.4: Graph of $f_d(\beta_i)$ for $\beta_i = 2$, $i \neq 1$

Moreover, looking at the tables in Appendix A, some additional properties seem to be verified. Here are some examples. The value of $a^{d,d}_{(1,\ldots,1,0)}$ is easy to predict:

$$a^{d,d}_{(1,\ldots,1,0)} = (-1)^{d+1}2 \ ;$$

[5] http://trac.sagemath.org/sage_trac/ticket/7377
[6] http://trac.sagemath.org/sage_trac/ticket/9880

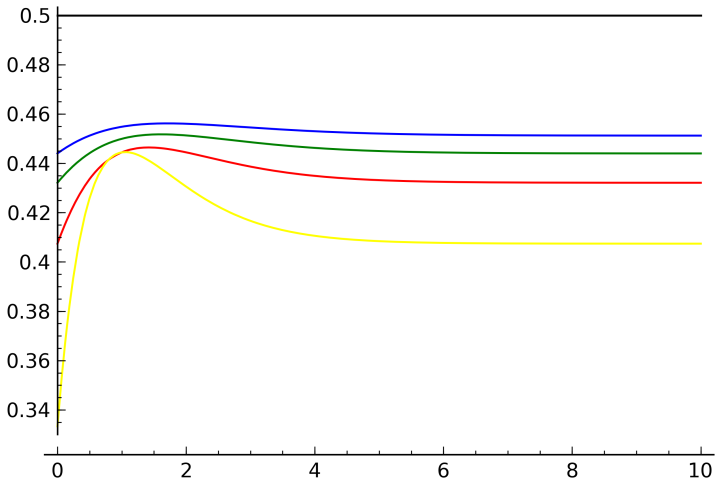


Figure 2.5: Graph of $f_d(\beta_i)$ for $\beta_i = 10$, $i \neq 1$

we prove this in Proposition 2.5.19. There is a recursion relation between coefficients with different d's:

$$a^{d,n+1}_{(i_1,\ldots,i_n,0)} + a^{d,n}_{(i_1,\ldots,i_n)} = 3a^{d-1,n}_{(i_1,\ldots,i_n)} \ ;$$

this is Corollary 2.5.18. There is a relation between coefficients with a given d:

$$a^{d,n}_{(i,j,\ldots)} = \frac{i+1}{j} a^{d,n}_{(i+1,j-1,\ldots)} \ ;$$

this is Proposition 2.5.3.

2.5.2 Splitting the sum into atomic parts

We consider a general $d \geq 1$. From Proposition 2.4.10, we have

$$f_d(\beta_1, \ldots, \beta_d) = \sum_{E=0}^{B-1} \sum_{\substack{\sum_d e_i = E \\ 0 \leq e_i}} \prod_d P(e_i) \ ,$$

where $P(e_i)$ has three different expressions according to the value of e_i:

$$P(e_i) = \begin{cases} 2^{-\beta_i} & \text{if } e_i = 0 \ , \\ \frac{2^{-\beta_i}}{3}(2^{e_i} - 2^{-e_i}) & \text{if } 0 < e_i < \beta_i \ , \\ \frac{2^{\beta_i} - 2^{-\beta_i}}{3} 2^{-e_i} & \text{if } \beta_i \leq e_i \ . \end{cases}$$

Let us denote for a vector $X \in \{0,1,2\}^d$:

- the i-th coordinate by X_i with $1 \leq i \leq d$;
- $j_k = \#\{i \mid X_i = k\}$ for $0 \leq k \leq 2$;
- $B_{0,1} = \sum_{\{i \mid X_i \neq 2\}} \beta_i$;

- $E_1 = \sum_{\{i|X_i=1\}} e_i$.

We can now define subsets S_X^d of the sum in Proposition 2.4.10 where each $P(e_i)$ has a specific behavior given by the value of the i-th coordinate of such a vector X.

$$S_X^d = \sum_{E=0}^{B-1} \sum_{\substack{\sum_d e_i = E \\ e_i=0 \text{ if } X_i=0 \\ 0<e_i<\beta_i \text{ if } X_i=1 \\ \beta_i \le e_i \text{ if } X_i=2}} \prod_{i=1}^{n} P(e_i)$$

$$= \sum_{E=0}^{B-1} \sum_{\substack{\sum_d e_i = E \\ e_i=0 \text{ if } X_i=0 \\ 0<e_i<\beta_i \text{ if } X_i=1 \\ \beta_i \le e_i \text{ if } X_i=2}} \left(\prod_{\{i|X_i=0\}} 2^{-\beta_i} \prod_{\{i|X_i=1\}} \frac{2^{-\beta_i}}{3}(2^{e_i} - 2^{-e_i}) \prod_{\{i|X_i=2\}} \frac{2^{\beta_i} - 2^{-\beta_i}}{3} 2^{-e_i} \right) ,$$

so that

$$f_d(\beta_1, \ldots, \beta_d) = \sum_{X \in \{0,1,2\}^d} S_X^d \ .$$

Here we drop the dependency on the β_i's for concision. The sum S_X^d has already some properties of f_d.

The following lemma is a direct consequence of the expression of S_X^d as a sum.

Lemma 2.5.4. *The function S_X^d is symmetric for the three sets $\{1 \le i \le d \mid X_i = k\}$ where $k \in \{0,1,2\}$, i.e. it takes the same value when two variables whose indices are in the same set are exchanged. Moreover, to compute S_Y^d where Y is any permutation of X, one has just to permute the β_i's accordingly, i.e. $S_Y^d(\beta_1, \ldots, \beta_d) = S_X^d(\beta_{\sigma(1),\ldots,\sigma(d)})$ if $Y_{\sigma(i)} = X_i$.*

The previous lemma shows that it is enough to study the X's such that

$$X = (\overbrace{0, \ldots, 0}^{j_0}, \overbrace{1, \ldots, 1}^{j_1}, \overbrace{2, \ldots, 2}^{j_2}) \ .$$

The following lemma gives the value of S_X^d for $X = 0$ and is also a trivial consequence of the expression of S_X^d as a sum.

Lemma 2.5.5. $S^d_{(0,\ldots,0)} = 2^{-\sum_{i=1}^d \beta_i}$ *and* $S^d_{(2,\ldots,2)} = 0$.

And when $j_2 = 0$, S_X^d has a simple expression.

Proposition 2.5.6. *If $j_2 = 0$ and $X = (\overbrace{0, \ldots, 0}^{j_0}, \overbrace{1, \ldots, 1}^{j_1})$, then*

$$S_X^d = \frac{2^{-\sum_{i=1}^{j_0} \beta_i}}{3^{j_1}} \prod_{i=j_0+1}^{d} (1 + 2 \cdot 4^{-\beta_i} - 3 \cdot 2^{-\beta_i}) \ .$$

Proof. This is a simple consequence of the fact that we can sum up over each e_i independently.

$$\begin{aligned} S_X^d &= \frac{2^{-B}}{3^{j_1}} \sum_{\substack{0<e_i<\beta_i \\ j_0+1\le i\le d}} \prod_{i=j_0+1}^{d} (2^{e_i} - 2^{-e_i}) = \frac{2^{-B}}{3^{\#j_1}} \prod_{i=j_0+1}^{d} \sum_{0<e_i<\beta_i} (2^{e_i} - 2^{-e_i}) \\ &= \frac{2^{-B}}{3^{j_1}} \prod_{i=j_0+1}^{d} (2^{\beta_i} + 2\cdot 2^{-\beta_i} - 3) \\ &= 2^{-\sum_{i=1}^{j_0}\beta_i} \prod_{i=j_0+1}^{d} \frac{1 + 2\cdot 4^{-\beta_i} - 3\cdot 2^{-\beta_i}}{3} \ . \end{aligned}$$

□

The next proposition is the key to our proof. It exhibits a recursion relation between S_X^d for different values of d and will reduce the proof of Proposition 2.5.1 to the case where $j_2 = 0$ and to the study of a residual term denoted by T_X^d.

Proposition 2.5.7. *For $j_2 \ge 1$ and $X = (\overbrace{0,\dots,0}^{j_0}, \overbrace{1,\dots,1}^{j_1}, \overbrace{2,\dots,2}^{j_2})$, we have*

$$S_X^d = 2\frac{1-4^{-\beta_d}}{3} S_X^{d-1} - 2T_X^d \ ,$$

where

$$T_X^d = \frac{4^{-B_{0,1}}}{3^{j_1+j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \sum_{\substack{0<e_i<\beta_i \\ j_0+1\le i\le j_0+j_1}} \prod_{i=j_0+1}^{j_0+j_1} (4^{e_i}-1) \sum_{\substack{0\le e_i, \sum e_i < B_{0,1}-E_1 \\ j_0+j_1+1\le i\le d-1}} 1 \ .$$

Proof. Replacing $P(e_i)$ by its expression, we get

$$\begin{aligned} S_X^d &= \prod_{i=1}^{j_0} 2^{-\beta_i} \sum_{\substack{0<e_i<\beta_i \\ j_0+1\le i\le j_0+j_1}} \prod_{i=j_0+1}^{j_0+j_1} \frac{2^{-\beta_i}}{3}(2^{e_i}-2^{-e_i}) \sum_{\substack{\beta_i\le e_i, \sum e_i < B-E_1 \\ j_0+j_1+1\le i\le d}} \prod_{i=j_0+j_1+1}^{d} \frac{2^{\beta_i}-2^{-\beta_i}}{3} 2^{-e_i} \\ &= \frac{2^{-B_{0,1}}}{3^{j_1+j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \sum_{\substack{0<e_i<\beta_i \\ j_0+1\le i\le j_0+j_1}} \prod_{i=j_0+1}^{j_0+j_1} (2^{e_i}-2^{-e_i}) \sum_{\substack{0\le e_i, \sum e_i < B_{0,1}-E_1 \\ j_0+j_1+1\le i\le d}} \prod_{i=j_0+j_1+1}^{d} 2^{-e_i} \ , \end{aligned}$$

letting $e_i = e_i - \beta_i$ for $j_0 + j_1 + 1 \le i \le d$. We now explicitly compute the sum on e_d.

$$\begin{aligned} S_X^d &= \frac{2^{-B_{0,1}}}{3^{j_1+j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \sum_{\substack{0<e_i<\beta_i \\ j_0+1\le i\le j_0+j_1}} \prod_{i=j_0+1}^{j_0+j_1} (2^{e_i}-2^{-e_i}) \\ &\qquad \sum_{\substack{0\le e_i, \sum e_i < B_{0,1}-E_1 \\ j_0+j_1+1\le i\le d-1}} \prod_{i=j_0+j_1+1}^{d-1} 2^{-e_i} \left(2\left(1-2^{-B_{0,1}+E_1+\sum_{i=j_0+j_1+1}^{d-1} e_i}\right)\right) \\ &= 2\frac{1-4^{-\beta_d}}{3} S_X^{d-1} - 2\frac{4^{-B_{0,1}}}{3^{j_1+j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \sum_{\substack{0\le e_i, \sum e_i < B_{0,1}-E_1 \\ j_0+j_1+1\le i\le d-1}} 1 \\ &= 2\frac{1-4^{-\beta_d}}{3} S_X^{d-1} - 2T_X^d \ . \end{aligned}$$

□

2.5.3 The residual term T_X^d

We now study the term T_X^d for $j_2 \geq 1$ and $X = (\overbrace{0,\dots,0}^{j_0},\overbrace{1,\dots,1}^{j_1},\overbrace{2,\dots,2}^{j_2})$ and show that it has the following expression.

Proposition 2.5.8. *For $j_2 \geq 1$ and $X = (\overbrace{0,\dots,0}^{j_0},\overbrace{1,\dots,1}^{j_1},\overbrace{2,\dots,2}^{j_2})$,*

$$T_X^d = \frac{1}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i})\Sigma_X^d$$

where

$$\Sigma_X^d = \frac{4^{-\sum_{i=1}^{j_0}\beta_i}}{3^{j_1}(j_2-1)!} \sum_{l=0}^{j_2-1} \begin{bmatrix} j_2-1 \\ l \end{bmatrix} \sum_{k+k_{j_0+1}+\dots+k_{j_0+j_1}=l} \binom{l}{k,k_{j_0+1},\dots,k_{j_0+j_1}} \left(\sum_{i=1}^{j_0}\beta_i\right)^k \Pi_X^d \ ,$$

$$\Pi_X^d = \prod_{\{j_0\leq j\leq j_0+j_1 | k_j=0\}} \frac{1-4^{-\beta_j}-3\beta_j 4^{-\beta_j}}{3} \prod_{\{j_0\leq j\leq j_0+j_1 | k_j\neq 0\}} \left(A_{k_j}(1-4^{-\beta_j}) - \Theta_{X,j}^d 4^{-\beta_j}\right) \ ,$$

and

$$\Theta_{X,j}^d = \frac{1}{k_j+1}\beta_j^{k_j+1} + \frac{5}{6}\beta_j^{k_j} + \sum_{i=1}^{k_j-1}\binom{k_j}{i}\left(A_i + \frac{B_{i+1}}{i+1}\right)\beta^{k_j-i} \ .$$

The quantity Σ_X^d is a sum for $I \subset \{j_0+1,\dots,j_0+j_1\}$ of terms of the form $4^{-\sum_{i=1}^{j_0}\beta_i - \sum_{i\in I}\beta_i}$ multiplied by a multivariate polynomial of degree in β_i exactly j_2 if $i \in I$, j_2-1 if $1 \leq i \leq j_0$, 0 otherwise, and of total degree $j_2 + \#I - 1$.

This subsection is devoted to the proof of that proposition. This is a quite technical part, but it is also a key step towards the proof of Proposition 2.5.2.

We denote by R_X^d the sum at the end of T_X^d:

$$R_X^d = \sum_{\substack{0\leq e_i, \sum e_i < B_{0,1}-E_1 \\ j_0+j_1+1\leq i\leq d-1}} 1 \ ,$$

which is simply the number of j_2-1-tuples of natural integers such that their sum is strictly less than $B_{0,1}-E_1$; and by Σ_X^d the sum on the e_i's for $j_0+1 \leq i \leq j_0+j_1$:

$$\Sigma_X^d = \frac{4^{-B_{0,1}}}{3^{j_1}} \sum_{\substack{0<e_i<\beta_i \\ j_0+1\leq i\leq j_0+j_1}} \prod_{i=j_0+1}^{j_0+j_1} (4^{e_i}-1) R_X^d \ ,$$

so that T_X^d is given by

$$T_X^d = \frac{1}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i})\Sigma_X^d \ .$$

We first check the proposition for $j_2 = 1$. In that case, $R_X^d = 1$ and the sum Σ_X^d to compute is

$$\Sigma_X^d = \frac{4^{-B_{0,1}}}{3^{j_1}} \sum_{\substack{0<e_i<\beta_i \\ j_0+1\leq i\leq j_0+j_1}} \prod_{i=j_0+1}^{j_0+j_1} (4^{e_i}-1) = \frac{4^{-B_{0,1}}}{3^{j_1}} \prod_{i=j_0+1}^{j_0+j_1} \frac{4^{\beta_i}-1-3\beta_i}{3}$$
$$= \frac{4^{-\sum_{i=0}^{j_0}\beta_i}}{3^{j_1}} \prod_{i=j_0+1}^{j_0+j_1} \frac{1-4^{-\beta_i}-3\beta_i 4^{-\beta_i}}{3} \ ,$$

so T_X^d becomes

$$T_X^d = \frac{1}{3}(1-4^{-\beta_d}) \frac{4^{-\sum_{i=0}^{j_0}\beta_i}}{3^{j_1}} \prod_{i=j_0+1}^{j_0+j_1} \frac{1-4^{-\beta_i}-3\beta_i 4^{-\beta_i}}{3}$$

which is what the proposition states.

Let us now proceed to a general $j_2 \geq 1$. In what follows B_i is a Bernoulli number [122, Formula 6.78] (here $B_1 = 1/2$) and $\begin{bmatrix} i \\ j \end{bmatrix}$ is an unsigned Stirling number of the first kind [122, Section 6.1]. We recall that the sum of the first n k-th powers is given as a polynomial in n by

$$\sum_{i=0}^{n} i^k = \frac{1}{k+1} \sum_{i=0}^{k} \binom{k+1}{i} B_i n^{k+1-i} \ .$$

Here is a classical combinatorial lemma.

Lemma 2.5.9. *For $n \geq 1$ and $m > 0$, the number of n-tuples of natural integers such that their sum is strictly less than m is given by*

$$\sum_{\substack{0\leq i_j, 1\leq j\leq n \\ \sum_{j=1}^{n} i_j < m}} 1 = \binom{n+m-1}{n}$$
$$= \frac{1}{n!} \sum_{l=1}^{n} \begin{bmatrix} n \\ l \end{bmatrix} m^l \ .$$

Proof. This is indeed the same quantity as the number of $n+1$-tuples of natural integers such that their sum is exactly $m-1$. □

Then, the sum R_X^d in T_X^d for $j_2 \geq 1$, which counts the number of $j_2 - 1$-tuples of natural integers such that their sum is strictly less than $B_{0,1} - E_1$, is given by the following expression

$$R_X^d = \frac{1}{(j_2-1)!} \sum_{l=0}^{j_2-1} \begin{bmatrix} j_2-1 \\ l \end{bmatrix} (B_{0,1}-E_1)^l$$
$$= \frac{1}{(j_2-1)!} \sum_{l=0}^{j_2-1} \begin{bmatrix} j_2-1 \\ l \end{bmatrix}$$
$$\sum_{k+k_{j_0+1}+\ldots+k_{j_0+j_1}=l} \binom{l}{k, k_{j_0+1}, \ldots, k_{j_0+j_1}} \left(\sum_{i=1}^{j_0} \beta_i\right)^k \prod_{i=j_0+1}^{j_0+j_1} (\beta_i - e_i)^{k_i} \ .$$

And Σ_X^d becomes

$$\Sigma_X^d = \frac{4^{-B_{0,1}}}{3^{j_1}} \sum_{\substack{0<e_i<\beta_i \\ j_0+1\le i\le j_0+j_1}} \prod_{i=j_0+1}^{j_0+j_1} (4^{e_j}-1) R_X^d$$
$$= \frac{4^{-\sum_{i=1}^{j_0}\beta_i}}{3^{j_1}(j_2-1)!} \sum_{l=0}^{j_2-1} \begin{bmatrix} j_2-1 \\ l \end{bmatrix} \sum_{k+k_{j_0+1}+\ldots+k_{j_0+j_1}=l} \binom{l}{k, k_{j_0+1}, \ldots, k_{j_0+j_1}} \left(\sum_{i=1}^{j_0}\beta_i\right)^k \Pi_X^d \ ,$$

where Π_X^d is defined as

$$\Pi_X^d = 4^{-\sum_{i=j_0+1}^{j_0+j_1}\beta_i} \prod_{i=j_0+1}^{j_0+j_1} \sum_{e_i=1}^{\beta_i-1} (\beta_i - e_i)^{k_i}(4^{e_i}-1) \ .$$

We now study the different sums on e_i according to the value of k_i. We drop the subscripts for clarity.

If $k=0$, then the sum is simply

$$\sum_{e=1}^{\beta-1}(4^e-1) = \sum_{e=0}^{\beta-1}(4^e-1) = \frac{4^\beta - 1 - 3\beta}{3} \ .$$

When $k \ge 1$, we do the change of summation variable $e = \beta - e$, so that the sum becomes

$$\sum_{e=1}^{\beta-1}(\beta-e)^k(4^e-1) = 4^\beta \sum_{e=1}^{\beta-1}(\beta-e)^k(1/4)^{\beta-e} - \sum_{e=1}^{\beta-1}(\beta-e)^k$$
$$= 4^\beta \sum_{e=1}^{\beta-1} e^k 4^{-e} - \sum_{e=1}^{\beta-1} e^k \ .$$

The second part of this difference is related to the sum of the first n k-th powers. Here we sum up to $\beta-1$ so the formula is slightly different:

$$\sum_{e=0}^{\beta-1} e^k = \frac{1}{k+1}\sum_{i=0}^{k}(-1)^{1_{i=1}}\binom{k+1}{i} B_i \beta^{k+1-i} \ .$$

For the first part, the sum $\sum_{i=1}^n i^k z^i$ is a multivariate polynomial in n, z and z^n of degree exactly k in n and 1 in z^n. More precisely the series $\sum_{i=0}^\infty i^k z^i$ is related to the Eulerian numbers $\left\langle {k \atop i} \right\rangle$ [122, Section 6.2] defined by

$$\left\langle {0 \atop i} \right\rangle = 1_{i=0} \ ,$$
$$\left\langle {k \atop i} \right\rangle = (i+1)\left\langle {k-1 \atop i} \right\rangle + (k-i)\left\langle {k-1 \atop i-1} \right\rangle \text{ for } k>0 \ ,$$

and expressed in closed form as [122, Formula 6.38]

$$\left\langle {k \atop i} \right\rangle = \sum_{j=0}^{i}(-1)^j\binom{k+1}{j}(i+1-j)^k \ .$$

The series is then given by the following classical formula for $k \geq 1$ and $|z| < 1$:

$$\sum_{i=1}^{\infty} i^k z^i = \frac{\sum_{j=0}^{k} \left\langle {k \atop j} \right\rangle z^{j+1}}{(1-z)^{k+1}} \ .$$

The formula for the truncated sum is slightly more involved as stated in the next lemma.

Lemma 2.5.10. *For $k \geq 1$ and $|z| \neq 1$,*

$$\sum_{i=1}^{n} i^k z^i = \frac{\sum_{j=0}^{k} A_0(k,j) z^{j+1}}{(1-z)^{k+1}} - \frac{\left(\sum_{i=0}^{k} \binom{k}{i} \left(\sum_{j=0}^{k} A_i(k,j) z^{j+1}\right) n^i\right) z^n}{(1-z)^{k+1}} \ ,$$

where $A_i(k,j)$ is defined by the same recursion relation as $\left\langle {k \atop j} \right\rangle$ and the initial conditions

$$A_i(i,j) = A_i(i+1,j) = (-1)^j \binom{i}{j} \ .$$

In particular, $A_0(k,j) = \left\langle {k \atop j} \right\rangle$ and we have the simple recursion formula for $i \geq 1$

$$A_i(k,j) = A_{i-1}(k-1,j) - A_{i-1}(k-1,j-1) \ .$$

We are interested in the case where $z = 1/4$, $n = \beta - 1$ and $1 \leq k \leq j_2 - 1$, which is written as (beware that we are summing up to $\beta - 1$ and not β, so the expression is slightly different from the one above)

$$\sum_{e=1}^{\beta-1} e^k 4^{-e} = \frac{\sum_{j=0}^{k} A_0(k,j) 4^{-j-1}}{(3/4)^{k+1}} - \frac{\left(\sum_{i=0}^{k-1} \binom{k}{i} \left(\sum_{j=0}^{k} A_i(k,j) 4^{-j-1}\right) \beta^i\right) 4^{-\beta}}{(3/4)^{k+1}}$$
$$- \frac{\left(\sum_{j=0}^{k} A_k(k,j) 4^{-j}\right) \beta^k 4^{-\beta}}{(3/4)^{k+1}} \ .$$

Moreover, we have the following identity.

Lemma 2.5.11. *For $0 \leq i \leq k$,*

$$3 \sum_{j=0}^{k} A_i(k,j) 4^{-j} = 4 \sum_{j=0}^{k+1} A_{i+1}(k+1,j) 4^{-j} \ .$$

Proof. Indeed,

$$\begin{aligned}
4 \sum_{j=0}^{k+1} A_{i+1}(k+1,j) 4^{-j} &= 4 \sum_{j=0}^{k+1} (A_i(k,j) - A_i(k,j-1)) 4^{-j} \\
&= 4 \sum_{j=0}^{k} A_i(k,j) 4^{-j} - 4 \sum_{j=1}^{k+1} A_i(k,j-1) 4^{-j} \\
&= 4 \sum_{j=0}^{k} A_i(k,j) 4^{-j} - 4 \sum_{j=0}^{k} A_i(k,j) 4^{-j-1} \\
&= 3 \sum_{j=0}^{k} A_i(k,j) 4^{-j} \ .
\end{aligned}$$

□

Whence the following definition.

Definition 2.5.12. *For $i \geq 0$, let us denote by A_i the quantity*

$$A_i = \frac{\sum_{j=0}^{i} A_0(i,j)4^{-j-1}}{(3/4)^{i+1}} = \frac{\sum_{j=0}^{i} \left\langle {i \atop j} \right\rangle 4^{-j-1}}{(3/4)^{i+1}} \ .$$

The first few values for A_i are given in Table 2.3.

Table 2.3: Values of A_i for $0 \leq i \leq 7$

$i =$	0	1	2	3	4	5	6	7
$A_i =$	1/3	4/9	20/27	44/27	380/81	4108/243	17780/243	269348/729

Then, the following corollary of Lemmas 2.5.10 and 2.5.11 gives a simple expression of the sum.

Corollary 2.5.13. *For $k \geq 1$,*

$$\sum_{e=1}^{\beta-1} e^k 4^{-e} = A_k - \left(\sum_{i=0}^{k-1} \binom{k}{i} A_{k-i} \beta^i \right) 4^{-\beta} - 4A_0 \beta^k 4^{-\beta} \ .$$

So, for $k \geq 1$, the sum becomes

$$\begin{aligned}
\sum_{e=1}^{\beta-1} (\beta - e)^k (4^e - 1) &= A_k 4^\beta - \sum_{i=0}^{k-1} \binom{k}{i} A_{k-i} \beta^i - 4A_0 \beta^k - \frac{1}{k+1} \sum_{i=0}^{k} (-1)^{1_{i=1}} \binom{k+1}{i} B_i \beta^{k+1-i} \\
&= A_k 4^\beta - \sum_{i=1}^{k} \binom{k}{i} A_k \beta^{k-i} - 4A_0 \beta^k \\
&\qquad - \frac{1}{k+1} \beta^{k+1} + \frac{1}{2} \beta^k - \sum_{i=2}^{k} \binom{k+1}{i} B_i \beta^{k+1-i} \\
&= A_k (4^\beta - 1) - \frac{1}{k+1} \beta^{k+1} - \frac{5}{6} \beta^k - \sum_{i=1}^{k-1} \binom{k}{i} \left(A_i + \frac{B_{i+1}}{i+1} \right) \beta^{k-i} \ .
\end{aligned}$$

According to the above discussion about the different sums on e_i, Π_X^d can be expressed as

$$\begin{aligned}
\Pi_X^d &= 4^{-\sum_{i=j_0+1}^{j_0+j_1} \beta_i} \prod_{\{j_0+1 \leq j \leq j_0+j_1 | k_j = 0\}} \frac{4^{\beta_j} - 1 - 3\beta_j}{3} \prod_{\{j_0+1 \leq j \leq j_0+j_1 | k_j \neq 0\}} \left(A_{k_j} (4^{\beta_j} - 1) - \Theta_{X,j}^d \right) \\
&= \prod_{\{j_0+1 \leq j \leq j_0+j_1 | k_j = 0\}} \frac{1 - 4^{-\beta_j} - 3\beta_j 4^{-\beta_j}}{3} \prod_{\{j_0+1 \leq j \leq j_0+j_1 | k_j \neq 0\}} \left(A_{k_j} (1 - 4^{-\beta_j}) - \Theta_{X,j}^d 4^{-\beta_j} \right) \ .
\end{aligned}$$

where

$$\Theta_{X,j}^d = \frac{1}{k_j+1} \beta_j^{k_j+1} + \frac{5}{6} \beta_j^{k_j} + \sum_{i=1}^{k_j-1} \binom{k_j}{i} \left(A_i + \frac{B_{i+1}}{i+1} \right) \beta^{k_j-i} \ .$$

Hence, Π_X^d, Σ_X^d and T_X^d are all as stated in Proposition 2.5.1. The values of the degrees of the multivariate polynomials follow from the above expressions.

2.5.4 A polynomial expression

We can now prove a first step towards Proposition 2.5.1. We show that S_X^d is a product of exponentials in basis 2 and 4 (but not only 4 yet!) by multivariate polynomials.

Proposition 2.5.14. *For $j_2 > 0$ and $X = (\overbrace{0,\dots,0}^{j_0},\overbrace{1,\dots,1}^{j_1},\overbrace{2,\dots,2}^{j_2})$,*

$$S_X^d = \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S_X^{d-j_2} - \Xi_X^d \right) \ ,$$

where

$$\begin{aligned}\Xi_X^d &= \sum_{i=0}^{j_2-1} 2^{-i} \Sigma_X^{d-j_2+1+i} \\ &= \frac{4^{-\sum_{i=1}^{j_0}\beta_i}}{3^{j_1}} \sum_{l=0}^{j_2-1} \left(\sum_{i=l}^{j_2-1} \frac{2^{-i}}{i!} \begin{bmatrix} i \\ l \end{bmatrix} \right) \sum_{k+k_{j_0+1}+\dots+k_{j_0+j_1}=l} \binom{l}{k, k_{j_0+1}, \dots, k_{j_0+j_1}} \left(\sum_{i=1}^{j_0} \beta_i \right)^k \Pi_X^d \ .\end{aligned}$$

Ξ_X^d is a sum for $I \subset \{j_0+1,\dots,j_0+j_1\}$ of terms of the form $4^{-\sum_{i=1}^{j_0}\beta_i - \sum_{i\in I}\beta_i}$ multiplied by a multivariate polynomial of degree in β_i exactly j_2 if $i \in I$, $j_2 - 1$ if $1 \le i \le j_0$, 0 otherwise, and of total degree $j_2 + \#I - 1$.

Proof. The proof goes by induction on $j_2 \ge 1$.

For $j_2 = 1$, this is Proposition 2.5.7.

Suppose now that $j_2 > 1$. From Proposition 2.5.7,

$$S_X^d = 2\frac{1-4^{-\beta_d}}{3} S_X^{d-1} - 2T_X^d \ ;$$

and by induction hypothesis on j_2,

$$\begin{aligned}S_X^d &= 2\frac{1-4^{-\beta_d}}{3} \frac{2^{j_2-1}}{3^{j_2-1}} \prod_{i=j_0+j_1+1}^{d-1} (1-4^{-\beta_i}) \left(S_X^{d-j_2} - \Xi_X^{d-1} \right) - 2T_X^d \\ &= \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S_X^{d-j_2} - \Xi_X^{d-1} \right) - 2T_X^d \ .\end{aligned}$$

Using Proposition 2.5.8, we have

$$T_X^d = \frac{1}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \Sigma_X^d \ ,$$

so that

$$\begin{aligned}S_X^d &= \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S_X^{d-j_2} - \Xi_X^{d-1} - 2^{-j_2+1}\Sigma_X^d \right) \\ &= \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S_X^{d-j_2} - \Xi_X^{d} \right) \ ,\end{aligned}$$

whence the proposition. □

In fact, as soon as we know that S_X^d is a sum of exponentials multiplied by multivariate polynomials, we know which β_i's can appear in the multivariate polynomials. Indeed, as it is a fraction of f_d, we know that S_X^d is finite and even bounded between 0 and 1 for every tuple of β_i's. But S_X^d would explode as β_i goes to infinity whereas the other ones are fixed if this β_i appeared in a multivariate polynomial and not in the exponential.

We can now prove the final step towards Proposition 2.5.1. We claim that for $I \subset \{1, \dots, d\}$, S_I^d that we define as

$$S_I^d = \sum_{\{X | X_i = 2 \text{ if } i \in I, X_i \neq 2 \text{ if } i \notin I\}} S_X$$

already has an appropriate form, whence Proposition 2.5.1 because

$$f_d(\beta_1, \dots, \beta_d) = \sum_{I \subset \{1,\dots,d\}} S_I^d \ .$$

For $I, J \subset \{1, \dots, d\}$ such that $I \cap J = \emptyset$, we define $X(I, J)$ as the only vector in $\{0, 1, 2\}^d$ such that

$$X_i = \begin{cases} 2 & \text{if } i \in I, \\ 1 & \text{if } i \in J, \\ 0 & \text{otherwise.} \end{cases}$$

We denote $S^d_{X(I,J)}$ simply by $S^d_{I,J}$ so that

$$S_I^d = \sum_{J \subset I^c} S^d_{I,J} \ .$$

We define in the same way $T^d_{I,J}$ and T^d_I and so on when $I \neq \emptyset$.

Proposition 2.5.15. *The function S_I^d is a symmetric function in the β_i's such that $i \notin I$, as well as in the β_i's such that $i \in I$.*

For $I = \emptyset$, we have

$$S_\emptyset^d = \frac{1}{3^d} \sum_{J \subset \{1,\dots,d\}} 2^{\#J} 4^{-\sum_{j \in J} \beta_j} \ :$$

and for $\{d\} \subset I = \{j_0 + j_1 + 1, \dots, d\}$, we have

$$S_I^d = \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1 - 4^{-\beta_i}) \left(S_\emptyset^{d-j_2} - \Xi_I^d \right) \ .$$

For $\{d\} \subset I = \{j_0 + j_1 + 1, \dots, d\}$, Ξ_I^d is a sum for $J \subset I^c$ of terms of the form $4^{-\sum_{j \in J} \beta_j}$ multiplied by a multivariate polynomial of degree in β_j exactly $\#I$ if $j \in J$, 0 otherwise, and of total degree $\min(d - 1, \#I\#J)$.

Proof. This assertion does not depend on the exact value of I, but only on its cardinality $\#I$, even if the value of S_I^d does: one has to permute the β_i's to deduce one from another. Hence, we can assume that $I = \{j_0 + j_1 + 1, \dots, d\}$. The symmetry of S_I^d in each subset of variables follows from its definition. The proof goes by induction on $j_2 = \#I$.

Suppose first that $j_2 = 0$, i.e. $I = \emptyset$. We go by induction on d. For $d = 1$,

$$S_\emptyset^1 = S_{(0)}^1 + S_{(1)}^1 = f_1(\beta_1) = \frac{2}{3} 4^{-\beta_1} + \frac{1}{3} \ .$$

Suppose now that $d > 1$. Then

$$\begin{aligned} S_\emptyset^d &= \sum_{J\subset\{1,\dots,d\}} S_{\emptyset,J}^d = \sum_{J\subset\{1,\dots,d-1\}} S_{\emptyset,J}^d + \sum_{\{d\}\subset J\subset\{1,\dots,d\}} S_{\emptyset,J}^d \\ &= 2^{-\beta_d} S_\emptyset^{d-1} + 2^{-\beta_d}\frac{2^{\beta_d} + 2\cdot 2^{-\beta_d} - 3}{3} S_\emptyset^{d-1} \\ &= \frac{2\cdot 4^{-\beta_d}+1}{3}\frac{1}{3^{d-1}} \sum_{J\subset\{1,\dots,d-1\}} 2^{\#J} 4^{-\sum_{j\in J}\beta_j} \\ &= \frac{1}{3^d} \sum_{J\subset\{1,\dots,d\}} 2^{\#J} 4^{-\sum_{j\in J}\beta_j} \end{aligned}$$

using the induction hypothesis on d which proves the proposition for $I = \emptyset$.

Suppose now that $I = \{j_0 + j_1 + 1, \dots, d\}$ is not empty. It implies that $d > 1$ and that

$$\begin{aligned} S_I^d &= \sum_{J\subset\{1,\dots,j_0+j_1\}} S_{I,J}^d \\ &= \sum_{J\subset\{1,\dots,j_0+j_1\}} \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S_{I,J}^{d-j_2} - \Xi_{I,J}^d\right) \\ &= \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(\sum_{J\subset\{1,\dots,j_0+j_1\}} S_{I,J}^{d-j_2} - \sum_{J\subset\{1,\dots,j_0+j_1\}} \Xi_{I,J}^d \right) \\ &= \frac{2^{j_2}}{3^{j_2}} \prod_{i=j_0+j_1+1}^{d} (1-4^{-\beta_i}) \left(S_\emptyset^{d-j_2} - \Xi_I^d\right) \quad . \end{aligned}$$

□

Proposition 2.5.1 is a simple corollary to the last proposition and hence is finally proven.

2.5.5 The coefficients $a_{(i_1,\dots,i_n)}^{d,n}$

We can now properly define the coefficients appearing in the multivariate polynomials.

Definition 2.5.16. *We denote by $a_{(i_1,\dots,i_n)}^{d,n}$ the coefficient of $P_d^n(x_1,\dots,x_n)$ of multi-degree $(i_1,\dots,i_n)$ normalized by 3^d.*

It should be remembered that d is the index of the function f_d, n represents the number of β_j's appearing in the exponential in front of the polynomial P_d^n and the i_j's the degrees (potentially 0) in each of these β_j's of a monomial appearing in P_d^n. This does not depend on the ordering of the i_j's because P_d^n is symmetric, so we can suppose that $i_1 \geq \cdots \geq i_n$. Moreover, restrictions on the degrees imply that $a_{(i_1,\dots,i_n)}^{d,n} = 0$ as soon as $\sum_{j=1}^n i_j \geq d-1$.

Lemma 2.5.17. *For $d \geq 1$,*

$$f_{d+1}(\beta_1,\dots,\beta_d,0) = f_d(\beta_1,\dots,\beta_d) \quad .$$

Proof. This is obvious from the expression of $f_d(\beta_1,\dots,\beta_d)$ as a sum. □

Hence, we obtain a simple recursion relation on the coefficients of P_d^n.

Corollary 2.5.18. *For $d \geq 2$ and $0 \leq n < d$,*

$$a^{d,n+1}_{(i_1,\ldots,i_n,0)} + a^{d,n}_{(i_1,\ldots,i_n)} = 3a^{d-1,n}_{(i_1,\ldots,i_n)} \ .$$

We now give closed-form expressions for the coefficients $a^{d,n}_{(i_1,\ldots,i_n)}$.
Here is a first simple proposition proving an experimental observation.

Proposition 2.5.19. *If $d \geq 2$, then*[7] $a^{d,d}_{(1,\ldots,1,0)} = (-1)^{d+1}2$ *and* $a^{d,d-1}_{(1,\ldots,1)} = (-1)^d 2$.

Proof. From Propositions 2.5.15 and 2.5.14, the monomials of multi-degree $(1,\ldots,1,0)$ in P_d^{d-1} and P_d^d come from $S^d_{\{d\}}$, and within it from $S^d_{(1,\ldots,1,2)}$. Moreover

$$S^d_{(1,\ldots,1,2)} = \frac{2}{3}(1-4^{-\beta_d})\left(S^{d-1}_{(1,\ldots,1)} - \Xi^d_{(1,\ldots,1,2)}\right) \ ,$$

so it is clear that $a^{d,d}_{(1,\ldots,1,0)} = -a^{d,d-1}_{(1,\ldots,1)}$. The coefficient $a^{d,d-1}_{(1,\ldots,1,0)}$ must come from $\Xi^d_{(1,\ldots,1,2)}$ which is equal to

$$\Xi^d_{(1,\ldots,1,2)} = \frac{1}{3^{d-1}}\Pi^d_{(1,\ldots,1,2)} = \frac{1}{3^{d-1}}\prod_{i=0}^{d-1}\frac{1-(1+3\beta_i)4^{-\beta_i}}{3} \ ,$$

and finally

$$a^{d,d-1}_{(1,\ldots,1,0)} = -3^d\frac{2}{3}\frac{1}{3^{d-1}}(-1)^{d-1} = (-1)^d 2 \ . \qquad \square$$

More generally, we have the following expression for a monomial of total degree $d-1$.

Proposition 2.5.20. *Suppose that $n \geq 1$ and $i_1 + \ldots + i_n = d-1$. Then*

$$a^{d,n}_{(i_1,\ldots,i_n)} = 2\frac{(-1)^{n+1}}{i_1!\ldots i_n!} \ .$$

Proof. We can suppose that $i_1 \geq \cdots \geq i_{j_1} \neq 0 > i_{j_1+1} = 0 = \cdots = i_n$. This notation is consistent because the different constraints on the degrees show that such a monomial can only appear in S^d_X when $j_1 = \#\{i_j \mid i_j \neq 0\}$ and $j_2 = d - j_1$, so that this coefficient only comes from

$$S^d_{(1,\ldots,1,2,\ldots,2)} = \frac{2^{j_2}}{3^{j_2}}\prod_{i=j_1+1}^{d}(1-4^{-\beta_i})\left(S^{d-j_2}_{(1,\ldots,1)} - \Xi^d_{(1,\ldots,1,2,\ldots,2)}\right) \ .$$

Moreover, within $\Xi^d_{(1,\ldots,1,2,\ldots,2)}$ it can only appear in $\Sigma^{d-i}_{(1,\ldots,1,2,\ldots,2)}$ when $i = 0$. Looking at the expression of Π^d_X, we have the following expression

$$\begin{aligned}
a^{d,n}_{(i_1,\ldots,i_n)} &= (-1)^{n-j_1}(-2)\frac{(-1)^{j_1}}{(j_2-1)!}\begin{bmatrix} j_2-1 \\ d-1-j_1\end{bmatrix}\binom{d-1-j_1}{i_1-1,\ldots,i_{j_1}-1}\prod_{j=1}^{j_1}\frac{1}{(i_j-1)+1} \\
&= 2\frac{(-1)^{n+1}}{(j_2-1)!}\begin{bmatrix} j_2-1 \\ j_2-1\end{bmatrix}\binom{j_2-1}{i_1-1,\ldots,i_{j_1}-1}\prod_{j=1}^{j_1}\frac{1}{(i_j-1)+1} \\
&= 2\frac{(-1)^{n+1}}{i_1!\ldots i_{j_1}!} = 2\frac{(-1)^{n+1}}{i_1!\ldots i_n!} \ . \qquad \square
\end{aligned}$$

[7] The first equality is also true for $d = 1$.

As a corollary, we get a dependence relation.

Corollary 2.5.21. *For $d \geq 2$, $1 \leq n \leq l \leq d-1$, and $\sum_{j=1}^{n} i_j = l$,*

$$\sum_{j=0}^{d-l} \binom{d-l}{j} a^{d,n+j}_{i_1,\ldots,i_n,0,\ldots,0} = 0 \ .$$

Proof. The proof goes by induction on $d-1-l$. For $l = d-1$, this is a direct consequence of the previous proposition. For $l < d-1$, one uses the induction hypothesis and Corollary 2.5.18. □

Finally, here is the general expression for $a^{d,n}_{(i_1,\ldots,i_n)}$.

Proposition 2.5.2. *Suppose that $i_1 \geq \cdots \geq i_m \neq 0 > i_{m+1} = 0 = \cdots = i_n$ and $m > 0$. Let us denote by l the sum $l = i_1 + \ldots + i_n > 0$ (i.e. the total degree of the monomial). Then*

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \binom{l}{i_1,\ldots,i_n} b^{d,n}_{l,m} \ ,$$

with

$$b^{d,n}_{l,m} = \sum_{\mathfrak{i}=0}^{n-m} \binom{n-m}{\mathfrak{i}} \sum_{\mathfrak{j}=0}^{d-n} \binom{d-n}{\mathfrak{j}} \sum_{k_j \geq 0, j \in I \cup J, 1 \leq j \leq m} \frac{(l+S-m)!}{l!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ l+S-m \end{bmatrix} \right) \prod_{j \in J} \frac{A_{k_j}}{k_j!} \prod_{j \in I} \frac{A_{k_j - 3_{k_j=0}}}{k_j!} \prod_{j=1}^{m} \frac{C_{k_j-1}}{|k_j - 1|!} \ .$$

Within $b^{d,n}_{l,m}$, the following notation is used:

- $I = \{m+1, \ldots, m+\mathfrak{i}\}$;
- $J = \{n+1, \ldots, n+\mathfrak{j}\}$;
- $S = \sum_{j \in I \cup J, 1 \leq j \leq m} k_j$;
- $h = d - m - \mathfrak{j} - \mathfrak{i}$;

and

$$C_j = \begin{cases} A_j + \frac{B_{j+1}}{j+1} & \text{if } j > 0 \ , \\ -\frac{13}{6} & \text{if } j = 0 \ , \\ 1 & \text{if } j = -1 \ . \end{cases}$$

Proof. If $X_j = 2$, then the degree of β_j in S^d_X is zero. If $X_j = 0$, then $4^{-\beta_j}$ can be factored out of S^d_X and β_j will appear in every exponential. Therefore, we can consider only X's which verify the following constraints to compute $a^{d,n}_{(i_1,\ldots,i_n)}$:

$$X_j = \begin{cases} 0,1 & \text{if } 1 \leq j \leq m \ , \\ 0,1,2 & \text{if } m+1 \leq j \leq n \ , \\ 1,2 & \text{if } n+1 \leq j \leq d \ . \end{cases}$$

From Proposition 2.5.14,

$$S^d_X = \frac{2^{j_2}}{3^{j_2}} \prod_{\{j | X_j = 2\}} (1 - 4^{-\beta_j}) \left(S^{d-j_2}_X - \Xi^d_X \right) \ ,$$

and the monomials of non-zero degree only come from Ξ_X^d.

Moreover, Ξ_X^d can be written as

$$\Xi_X^d = \frac{1}{3^{j_1}} \sum_{k_j \geq 0, \{j|X_j \neq 2\}} \left(\sum_{k=0}^{j_2-1} \frac{2^{-k}}{k!} \begin{bmatrix} k \\ \sum_{\{j|X_j \neq 2\}} k_j \end{bmatrix} \right) \frac{\left(\sum_{\{j|X_j \neq 2\}} k_j\right)!}{\prod_{\{j|X_j \neq 2\}} k_j!} \left(\prod_{\{j|X_j=0\}} \beta_j^{k_j} 4^{-\beta_j} \right) \Pi_X^d \ .$$

So, to get a multinomial of multi-degree $(i_1, \ldots, i_n)$, different choices can be made for the k_j's:

- If $X_j = 0$, then we must take $k_j = i_j$. This happens for $1 \leq j \leq n$.
- If $X_j = 1$, then we can take any $k_j \geq \min(i_j - 1, 0)$ and take into account the correct coefficient in Π_X^d. This happens for $1 \leq j \leq d$.
- If $X_j = 2$, then there is no choice to make. This happens for $m + 1 \leq j \leq d$.

In the following sum, we gathered the contributions of all X's. We denote by I the set of indices $m + 1 \leq j \leq n$ such that $X_j = 0, 1$ (the other ones are such that $X_j = 2$) and by J the set of indices $n + 1 \leq j \leq d$ such that $X_j = 1$ (the other ones are such that $X_j = 2$).

The summation variables k_j where j is in $I \cup J$ or $[1, m]$ are to be understood as the degree we choose in the above expression of Ξ_X^d. Following the above discussion on the choice of the k_j's:

- If $j \in J$, then we can choose any positive degree k_j and extract the constant coefficient A_{k_j}.
- If $j \in I$, then we can choose any positive degree k_j and we extract the constant coefficient A_{k_j} as above if $k_j > 0$, and $A_0 - 3$ if $k_j = 0$ (the -3 comes from the choice $X_j = 0$ which gives $1 = 3 \cdot 1/3$).
- Finally, if $1 \leq j \leq m$, then we have to choose $k_j \geq i_j - 1$, and the corresponding coefficient is $\frac{1}{k_j+1} = \frac{1}{i_j}$ if $k_j = i_j - 1$, $5/6 - 3 = -13/6$ if $k_j = i_j$ (as above the -3 comes from the choice $X_j = 0$) and $\binom{k_j}{i_j} \left(A_{k_j - i_j} + \frac{B_{k_j - i_j + 1}}{k_j - i_j + 1} \right)$ if $k_j > i_j$. We denote that coefficient by D_{k_j, i_j}.

We denote S and h the quantities $S = \sum_{j \in I \cup J, 1 \leq j \leq m} k_j$ and $h = d - m - \#J - \#I$. Then $a^{d,n}_{(i_1,\ldots,i_n)}$ can be expressed as

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \sum_{\substack{I \subset \{m+1,\ldots,n\} \\ J \subset \{n+1,\ldots,d\}}} \sum_{\substack{k_j \geq 0, j \in I \cup J \\ k_j \geq i_j - 1, 1 \leq j \leq m}} \frac{S!}{\prod_{j \in I \cup J} k_j! \prod_{j=1}^m k_j!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right) \prod_{j \in J} A_{k_j} \prod_{j \in I} \left(A_{k_j} - 3_{k_j = 0} \right) \prod_{j=1}^m D_{k_j, i_j} \ .$$

Extracting the binomial coefficient of D_{k_j, i_j}, we can factor out the multinomial coefficient $\binom{l}{i_1, \ldots, i_n}$ (remember that l was defined as $l = \sum_{j=1}^n i_j$):

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \binom{l}{i_1, \ldots, i_n} \sum_{\substack{I \subset \{m+1,\ldots,n\} \\ J \subset \{n+1,\ldots,d\}}} \sum_{\substack{k_j \geq 0, j \in I \cup J \\ k_j \geq i_j - 1, 1 \leq j \leq m}} \frac{S!}{l!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right) \prod_{j \in J} \frac{A_{k_j}}{k_j!} \prod_{j \in I} \frac{A_{k_j} - 3_{k_j = 0}}{k_j!} \prod_{j=1}^m \frac{C_{k_j - i_j}}{|k_j - i_j|!} \ ,$$

where

$$C_j = \begin{cases} A_j + \frac{B_{j+1}}{j+1} & \text{if } j > 0 \\ -\frac{13}{6} & \text{if } j = 0 \\ 1 & \text{if } j = -1 \end{cases} .$$

The exact values of I and J are not important, only their cardinalities are; so defining $I = \{m+1, \ldots, m+\mathfrak{i}\}$ and $J = \{n+1, \ldots, n+\mathfrak{j}\}$, we get

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \binom{l}{i_1, \ldots, i_n} \sum_{\mathfrak{i}=0}^{n-m} \binom{n-m}{\mathfrak{i}} \sum_{\mathfrak{j}=0}^{d-n} \binom{d-n}{\mathfrak{j}} \sum_{\substack{k_j \geq 0, j \in I \cup J \\ k_j \geq i_j - 1, 1 \leq j \leq m}} \frac{S!}{l!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right) \prod_{j \in J} \frac{A_{k_j}}{k_j!} \prod_{j \in I} \frac{A_{k_j} - 3_{k_j=0}}{k_j!} \prod_{j=1}^{m} \frac{C_{k_j - i_j}}{|k_j - i_j|!} .$$

We finally make the change of summation variables $k_j = k_j - i_j + 1$ to obtain the desired expression:

$$\begin{aligned} a^{d,n}_{(i_1,\ldots,i_n)} &= (-1)^{n+1} \binom{l}{i_1, \ldots, i_n} \sum_{\mathfrak{i}=0}^{n-m} \binom{n-m}{\mathfrak{i}} \sum_{\mathfrak{j}=0}^{d-n} \binom{d-n}{\mathfrak{j}} \sum_{k_j \geq 0, j \in I \cup J, 1 \leq j \leq m} \frac{(l+S-m)!}{l!} \\ &\qquad \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ l+S-m \end{bmatrix} \right) \prod_{j \in J} \frac{A_{k_j}}{k_j!} \prod_{j \in I} \frac{A_{k_j} - 3_{k_j=0}}{k_j!} \prod_{j=1}^{m} \frac{C_{k_j - 1}}{|k_j - 1|!} \\ &= (-1)^{n+1} \binom{l}{i_1, \ldots, i_n} b^{d,n}_{l,m} . \end{aligned}$$

□

2.5.6 An additional relation

In this subsection we prove the following experimental fact.

Proposition 2.5.3. *For $n \geq 2$ and $0 < j \leq i$,*

$$a^{d,n}_{(i,j,\ldots)} = \frac{i+1}{j} a^{d,n}_{(i+1,j-1,\ldots)} ;$$

i.e. the value of $b^{d,n}_{l,m}$ does not depend on m.

Proof. From Proposition 2.5.2,

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \binom{l}{i_1, \ldots, i_n} b^{d,n}_{l,m} ,$$

where $b^{d,n}_{l,m}$ only depends on d, n, l and m. Therefore if $j > 1$, this value does not vary and the theorem is a simple corollary of Proposition 2.5.2.

If there is some degree equal to zero in $(i, j, \ldots)$, i.e. if $n > m$, then we can use the result of Corollary 2.5.18:

$$a^{d,n}_{(i,j,\ldots,0)} + a^{d,n-1}_{(i,j,\ldots)} = 3a^{d-1,n-1}_{(i,j,\ldots)} ;$$

hence we can restrict ourselves to the study of tuples where $n = m$.

Finally, the only tuples we must treat are the ones such that $i > j = 1$ and $n = m$. We write the degree $i \neq 0$ in first position even if it is not the greatest one. Then

$$a^{d,n}_{(i,\dots,1)} = (-1)^{n+1}\binom{l}{i,\dots,1} b^{d,n}_{l,n} \ ,$$
$$a^{d,n}_{(i+1,\dots,0)} = (-1)^{n+1}\binom{l}{i+1,\dots,0} b^{d,n}_{l,n-1} \ ,$$

so it suffices to show that $b^{d,n}_{l,n} = b^{d,n}_{l,n-1}$.

We use the same notation as in Proposition 2.5.2 except that S and h denote the quantities $S = l + \sum_{j\in I\cup J, 1\leq j\leq n-1} k_j - n$ and $h = d - n - \mathfrak{j}$. For $b^{d,n}_{l,n}$, I must be empty:

$$\begin{aligned} b^{d,n}_{l,n} &= \sum_{\mathfrak{j}=0}^{d-n}\binom{d-n}{\mathfrak{j}} \sum_{k_j\geq 0, j\in J, 1\leq j\leq n} \frac{(S+k_n)!}{l!} \\ &\qquad \left(\sum_{k\geq 1}\frac{2^k}{(h-k)!}\begin{bmatrix} h-k \\ S+k_n\end{bmatrix}\right)\prod_{j\in J}\frac{A_{k_j}}{k_j!}\prod_{j=1}^{n}\frac{C_{k_j-1}}{|k_j-1|!} \\ &= \sum_{\mathfrak{j}=0}^{d-n}\binom{d-n}{\mathfrak{j}} \sum_{k_j\geq 0, j\in J, 1\leq j\leq n-1} \frac{1}{l!}\prod_{j\in J}\frac{A_{k_j}}{k_j!}\prod_{j=1}^{n-1}\frac{C_{k_j-1}}{|k_j-1|!} \\ &\qquad \sum_{k_n\geq 0}(S+k_n)!\left(\sum_{k\geq 1}\frac{2^k}{(h-k)!}\begin{bmatrix} h-k \\ S+k_n\end{bmatrix}\right)\frac{C_{k_n-1}}{|k_n-1|!} \ ; \end{aligned}$$

whereas for $b^{d,n}_{l,n-1}$, I can contain n:

$$\begin{aligned} b^{d,n}_{l,n-1} &= \sum_{\mathfrak{i}=0}^{1}\binom{1}{\mathfrak{i}}\sum_{\mathfrak{j}=0}^{d-n}\binom{d-n}{\mathfrak{j}} \sum_{k_j\geq 0, j\in I\cup J, 1\leq j\leq n-1} \frac{(S+1)!}{l!} \\ &\qquad \left(\sum_{k\geq 1}\frac{2^k}{(h+1-k-\mathfrak{i})!}\begin{bmatrix} h+1-k-\mathfrak{i} \\ S+1\end{bmatrix}\right)\prod_{j\in J}\frac{A_{k_j}}{k_j!}\prod_{j\in I}\frac{A_{k_j}-3_{k_j=0}}{k_j!}\prod_{j=1}^{n-1}\frac{C_{k_j-1}}{|k_j-1|!} \\ &= \sum_{\mathfrak{j}=0}^{d-n}\binom{d-n}{\mathfrak{j}} \sum_{k_j\geq 0, j\in J, 1\leq j\leq n-1} \frac{1}{l!}\prod_{j\in J}\frac{A_{k_j}}{k_j!}\prod_{j=1}^{n-1}\frac{C_{k_j-1}}{|k_j-1|!} \\ &\qquad \left[(S+1)!\left(\sum_{k\geq 1}\frac{2^k}{(h+1-k)!}\begin{bmatrix} h+1-k \\ S+1\end{bmatrix}\right)\right. \\ &\qquad\quad \left. + \sum_{k_n\geq 0}(S+k_n+1)!\left(\sum_{k\geq 1}\frac{2^k}{(h-k)!}\begin{bmatrix} h-k \\ S+k_n+1\end{bmatrix}\right)\frac{A_{k_n}-3_{k_n=0}}{|k_n-1|!}\right] \ . \end{aligned}$$

The sums on $\mathfrak{j}$ and k_j for $j \in J$ and $1 \leq j \leq n-1$ are identical, so it is sufficient to show the

equality of the remaining terms, or that Δ defined as

$$\Delta = \sum_{k_n \geq 0} \frac{(S+k_n)!}{|k_n - 1|!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} \right) C_{k_n - 1} - (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h+1-k)!} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right)$$
$$- \sum_{k_n \geq 0} \frac{(S+k_n+1)!}{|k_n - 1|!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n+1 \end{bmatrix} \right) (A_{k_n} - 3_{k_n=0})$$

is zero. We split out the first two terms of the first sum on k_n:

$$S! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right) - \frac{13}{6}(S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+1 \end{bmatrix} \right) \ ,$$

and the first one of the second sum on k_n:

$$(S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+1 \end{bmatrix} \right) \left(\frac{1}{3} - 3 \right) \ ,$$

so that Δ becomes

$$\Delta = \sum_{k_n \geq 2} \frac{(S+k_n)!}{|k_n - 1|!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} \right) \left(A_{k_n - 1} + \frac{B_{k_n}}{k_n} \right)$$
$$+ S! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right) + \frac{1}{2}(S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+1 \end{bmatrix} \right)$$
$$- (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h+1-k)!} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right)$$
$$- \sum_{k_n \geq 1} \frac{(S+k_n+1)!}{|k_n - 1|!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n+1 \end{bmatrix} \right) A_{k_n} \ .$$

Making the change of summation variable $k_n = k_n + 1$ in the second sum on k_n, the terms in A_{k_n} cancel out between the two sums on k_n and we get

$$\Delta = \sum_{k_n \geq 2} \frac{(S+k_n)!}{k_n!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} \right) B_{k_n} + B_0 S! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S \end{bmatrix} \right)$$
$$+ B_1 (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+1 \end{bmatrix} \right) - (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h+1-k)!} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right)$$
$$= \sum_{k_n \geq 0} \frac{(S+k_n)!}{k_n!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} \right) B_{k_n} - (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h+1-k)!} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right)$$
$$= S! \sum_{k \geq 1} \frac{2^k}{(h-k)!} \left(\sum_{k_n \geq 0} \binom{S+k_n}{S} B_{k_n} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} \right) - (S+1)! \left(\sum_{k \geq 1} \frac{2^k}{(h+1-k)!} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right)$$
$$= S! \sum_{k \geq 1} \frac{2^k}{(h-k)!} \left(\sum_{k_n \geq 0} \binom{S+k_n}{S} B_{k_n} \begin{bmatrix} h-k \\ S+k_n \end{bmatrix} - \frac{S+1}{h+1-k} \begin{bmatrix} h+1-k \\ S+1 \end{bmatrix} \right) \ .$$

The difference in parenthesis is shown to be zero using Lemma 2.5.22, so that $\Delta = 0$. □

Lemma 2.5.22. *For $n \geq k \geq 0$,*

$$\sum_{l=0}^{n-k} \binom{k+l}{k} B_l \begin{bmatrix} n \\ k+l \end{bmatrix} = \frac{k+1}{n+1} \begin{bmatrix} n+1 \\ k+1 \end{bmatrix} \ .$$

Proof. Let us fix $k \geq 0$. We first recall classical results about exponential generating functions.

$$\sum_{n\geq 0} B_n \frac{z^n}{n!} = \frac{z}{1-e^{-z}} \ ,$$
$$\sum_{n\geq 0} \begin{bmatrix} n \\ k \end{bmatrix} \frac{z^n}{n!} = \frac{(-\log(1-z))^k}{k!} \ .$$

We now form the exponential generating function of the coefficients of interest.

$$\begin{aligned}
\sum_{n\geq 0} \left(\sum_{l=k}^{n} \binom{l}{k} B_{l-k} \begin{bmatrix} n \\ l \end{bmatrix} \right) \frac{z^n}{n!} &= \sum_{l\geq k} \sum_{n\geq l} \binom{l}{k} B_{l-k} \begin{bmatrix} n \\ l \end{bmatrix} \frac{z^n}{n!} = \sum_{l\geq k} \binom{l}{k} B_{l-k} \sum_{n\geq l} \begin{bmatrix} n \\ l \end{bmatrix} \frac{z^n}{n!} \\
&= \sum_{l\geq k} \binom{l}{k} B_{l-k} \frac{(-\log(1-z))^l}{l!} \\
&= \frac{(-\log(1-z))^k}{k!} \sum_{l\geq k} B_{l-k} \frac{(-\log(1-z))^{l-k}}{(l-k)!} \\
&= \frac{(-\log(1-z))^k}{k!} \sum_{l\geq 0} B_l \frac{(-\log(1-z))^l}{l!} \\
&= \frac{(-\log(1-z))^k}{k!} \frac{-\log(1-z)}{1-e^{\log(1-z)}} = \frac{k+1}{z} \frac{(-\log(1-z))^{k+1}}{(k+1)!} \\
&= \frac{k+1}{z} \sum_{n\geq 0} \begin{bmatrix} n \\ k+1 \end{bmatrix} \frac{z^n}{n!} = \sum_{n\geq 0} \frac{k+1}{n+1} \begin{bmatrix} n+1 \\ k+1 \end{bmatrix} \frac{z^n}{n!} \ ,
\end{aligned}$$

whence the identity of the lemma. □

2.6 Asymptotic behavior: $\beta_i \to \infty$

2.6.1 The limit $f_d(\infty, \ldots, \infty)$

We denote the limit of f_d when all the β_i's go to infinity by $f_d(\infty, \ldots, \infty)$. The expression of f_d given in Proposition 2.5.1 shows that this value is well defined and is nothing but the constant term P_d^0 in that expression.

In this subsection we give several expressions involving Gaussian hypergeometric series which are defined as follows.

Definition 2.6.1 (Gaussian hypergeometric series [1, Formula 15.1.1])**.** *The Gaussian hypergeometric series ${}_2F_1(a, b; c; z)$ is*

$${}_2F_1(a, b; c; z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \frac{z^n}{n!} \ ,$$

where $c \notin -\mathbb{N}$ and $(x)_n = x(x+1)(x+2)\cdots(x+n-1)$ is the Pochhammer symbol and represents the rising factorial.

It should be first remarked that, as all the β_i's go to infinity, the laws of the γ'_i's and the δ'_i's converge towards laws of independent geometrically distributed variables with parameter 1/2. From now on, let $G_1, \ldots, G_d$ and $H_1, \ldots, H_d$ be $2d$ such independent random variables. Then $P_{t,k} = P\left[\sum \gamma' < \sum \delta'\right]$ converges towards

$$P\left[\sum_{i=1}^{d} G_i < \sum_{i=1}^{d} H_i\right] = \frac{1}{2}\left(1 - P\left[\sum_{i=1}^{d} G_i = \sum_{i=1}^{d} H_i\right]\right) \ .$$

This quantity is obviously strictly lower than 1/2 for any $d > 0$ and the above discussion therefore proves that the conjecture is *asymptotically* true. We have just proved the following theorem.

Theorem 2.6.2. *Let d be a strictly positive integer. There exists a constant K_d such that if*

- *$\forall i$, $\beta_i \geq K_d$ and*
- *$\min_i \alpha_i \geq B - 1$,*

then

$$P_{t,k} < \frac{1}{2} \ .$$

We now look for an explicit expression of this limit.

Definition 2.6.3. *Let X_d be the random variable*

$$X_d = \sum_{i=1}^{d} G_i - \sum_{i=1}^{d} H_i \ ,$$

and let P_d denote

$$P_d = P\left[X_d = 0\right] \ .$$

With this notation,

$$f_d(\infty, \ldots, \infty) = P_d^0 = \frac{1}{2}(1 - P_d) \ ,$$

whence the importance of the random variable X_d.

First, it is readily seen that X_d is symmetric, i.e. $P\left[X_d = k\right] = P\left[X_d = -k\right]$. So studying $P\left[X_d = k\right]$ for k a positive integer is sufficient.

Second, to get an explicit expression for $P\left[X_d = k\right]$, we need the following easy lemma giving the law of a sum of d independent geometrically distributed variables with parameter 1/2.

Lemma 2.6.4. *For $j \geq 0$,*

$$P\left[\sum_{i=1}^{d} G_i = j\right] = \binom{d-1+j}{d-1} \frac{1}{2^{j+1}} \ .$$

It is then possible to express $P\left[X_d = k\right]$ as a hypergeometric series.

Proposition 2.6.5. *For $d \geq 1$ and $k \geq 0$,*

$$P[X_d = k] = \frac{1}{4^d}\frac{1}{2^k}\sum_{j=0}^{\infty}\binom{d-1+j}{d-1}\binom{d-1+k+j}{d-1}\frac{1}{4^j}$$
$$= \frac{1}{4^d}\frac{1}{2^k}\binom{d-1+k}{d-1}{}_2F_1(d, d+k; k+1; 1/4) \ ,$$

so that

$$P_d = P[X_d = 0] = \frac{1}{4^d}\sum_{j=0}^{\infty}\binom{d-1+j}{d-1}^2\frac{1}{4^j} = \frac{1}{4^d}{}_2F_1(d, d; 1; 1/4) \ .$$

In particular $\frac{1}{3^d} \leq P_d \leq \frac{1+3\cdot 2^{d-2}}{4^d}$. Moreover, $P_1 = 1/3$ and $P_2 = 5/27$.

Proof. To get the expression of $P[X_d = k]$ as a power series, the idea is to split it according to the value of one of the two sums of d random variables (the value of the other sum is then also fixed) and to use the above lemma:

$$P[X_d = k] = \sum_{j=0}^{\infty} P\left[\sum_{i=1}^{d} G_i = j\right] P\left[\sum_{i=1}^{d} H_i = j+k\right]$$
$$= \sum_{j=0}^{\infty} P\left[\sum_{i=1}^{d} G_i = j\right] P\left[\sum_{i=1}^{d} H_i = j+k\right]$$
$$= \frac{1}{4^d}\frac{1}{2^k}\sum_{j=0}^{\infty}\binom{d-1+j}{d-1}\binom{d-1+k+j}{d-1}\frac{1}{4^j} \ .$$

This power series is easily seen to be equal to

$$\frac{1}{4^d}\frac{1}{2^k}\binom{d-1+k}{d-1}{}_2F_1(d, d+k; k+1; 1/4) \ .$$

Setting $k = 0$ in the above expressions gives

$$P_d = P[X_d = 0] = \frac{1}{4^d}\sum_{j=0}^{\infty}\binom{d-1+j}{d-1}^2\frac{1}{4^j} = \frac{1}{4^d}{}_2F_1(d, d; 1; 1/4) \ .$$

This power series can be bounded from below by

$$\frac{1}{4^d}\sum_{j=0}^{\infty}\binom{d-1+j}{d-1}\frac{1}{4^j} = \frac{1}{4^d}\frac{1}{(1-1/4)^d} = \frac{1}{3^d} \ ,$$

and from above by

$$\frac{1}{4^d}\left(1 + \sum_{j=1}^{\infty}\binom{d-1+j}{d-1}\frac{2^{d-2+j}}{4^j}\right) = \frac{1}{4^d} + \frac{2^{d-2}}{4^d}\sum_{j=0}^{\infty}\binom{d-1+j}{d-1}\frac{1}{2^j} - \frac{2^{d-2}}{4^d}$$
$$= \frac{1 + 4^{d-1} - 2^{d-2}}{4^d} = \frac{1+3\cdot 2^{d-2}}{4^d} \ ,$$

which gives the desired inequalities.

Finally, if $d = 1$, then $\binom{d-1+j}{d-1} = 1$, so that the sum becomes

$$P_1 = \frac{1}{4}\frac{1}{1-1/4} = \frac{1}{3} \ ;$$

and, if $d = 2$, then $\binom{d-1+j}{d-1} = j + 1$, so that

$$\begin{aligned} P_2 &= \frac{1}{4^2}\sum_{j=0}^{\infty}\frac{(j+1)^2}{4^j} = \frac{1}{4}\sum_{j=0}^{\infty}\frac{j^2}{4^j} \\ &= \frac{1}{4}\left(\frac{2\frac{1}{4^2}}{\left(1-\frac{1}{4}\right)^3} + \frac{\frac{1}{4}}{\left(1-\frac{1}{4}\right)^2}\right) \\ &= \frac{2}{27} + \frac{1}{9} = \frac{5}{27} \ . \end{aligned}$$

□

When the number of blocks d goes as well to infinity, $f_d(\infty, \ldots, \infty)$ converges towards $1/2$. Indeed $\frac{1}{3^d} \leq P_d \leq \frac{1}{4^d} + \frac{3}{4}\frac{1}{2^d}$ converges towards 0 as d goes to infinity. As we show below, it does so monotonically so that $f_d(\infty, \ldots, \infty)$ goes to $1/2$ monotonically as well.

A first step towards proving the monotonicity of P_d in d is to study the special case $d = 1$. In this case the value $P[X_1 = k]$ has indeed a short closed-form expression.

Lemma 2.6.6. *For $d = 1$,*

$$P[X_1 = k] = \frac{1}{3 \cdot 2^{|k|}} \ .$$

Proof. Indeed, for $k \geq 0$,

$$\begin{aligned} P[X_1 = k] &= P[G_1 = k + H_1] \\ &= \sum_{i=0}^{\infty} P[G_1 = i]\, P[H_1 = k + i] \\ &= \sum_{i=0}^{\infty}\frac{1}{2^{i+1}}\frac{1}{2^{k+i+1}} = \frac{1}{2^{k+2}}\sum_{i=0}^{\infty}\frac{1}{4^i} \\ &= \frac{1}{2^{k+2}}\frac{4}{3} = \frac{1}{3}\frac{1}{2^k} \ . \end{aligned}$$

□

In the general case $d \geq 1$, it can also be proven quite directly that the maximal value of $P[X_d = k]$ is attained for $k = 0$.

Lemma 2.6.7. *For $d \geq 1$ and $k \neq 0$,*

$$P[X_d = k] < P[X_d = 0] \ .$$

Proof. Consider the real Hilbert space $\mathcal{H} = l^2(\mathbb{Z}, \mathbb{R})$ of square-summable sequences. It is equipped with norm preserving translation operators τ_k defined by $(\tau_k u)_j = u_{j+k}$ for a sequence $u = (u_j)_{j\in\mathbb{Z}} \in \mathcal{H}$. Consider now the sequence $u^{(d)} \in \mathcal{H}$ defined by

$$u_j^{(d)} = P\left[\sum_{i=1}^{d} G_i = j\right] = P\left[\sum_{i=1}^{d} H_i = j\right]$$

whose exact values are given in Lemma 2.6.4 for $j \geq 0$, and $u_j^{(d)} = 0$ for $j < 0$.

Then, as shown at the beginning of the proof of Proposition 2.6.5, we have

$$P[X_d = k] = \sum_{j=0}^{\infty} P\left[\sum_{i=1}^{d} G_i = j\right] P\left[\sum_{i=1}^{d} H_i = j + k\right] = \langle u^{(d)}, \tau_k u^{(d)} \rangle$$

where $\langle \cdot, \cdot \rangle$ is the scalar product of $\mathcal{H}$. We now use the Cauchy–Schwarz inequality and the fact that τ_k is norm preserving to conclude that

$$P[X_d = k] = \langle u^{(d)}, \tau_k u^{(d)} \rangle < \sqrt{\langle u^{(d)}, u^{(d)} \rangle \langle \tau_k u^{(d)}, \tau_k u^{(d)} \rangle} = \langle u^{(d)}, u^{(d)} \rangle = P[X_d = 0] \ .$$

(Remark that the Cauchy–Schwarz inequality is strict here because $u^{(d)}$ and $\tau_k u^{(d)}$ are not proportional when $k \neq 0$.) □

Combining Lemmas 2.6.6 and 2.6.7, we then get the monotonicity of P_d in d.

Proposition 2.6.8. *For $d \geq 1$,*

$$P_d > P_{d+1} \ .$$

Proof.

$$\begin{aligned} P_{d+1} &= P[X_{d+1} = 0] = P[X_1 + X_d = 0] \\ &= \sum_{k=-\infty}^{+\infty} P[X_1 = -k] \, P[X_d = k] \\ &= \sum_{k=-\infty}^{+\infty} \frac{1}{3 \cdot 2^{|k|}} P[X_d = k] \\ &< \sum_{k=-\infty}^{+\infty} \frac{1}{3 \cdot 2^{|k|}} P[X_d = 0] \\ &< P[X_d = 0] = P_d \ . \end{aligned}$$

□

Corollary 2.6.9. *The limit $f_d(\infty, \ldots, \infty)$ converges monotonically towards $\frac{1}{2}$ as d goes to infinity.*

Now that $P[X_d = k]$ has been expressed as a Gaussian hypergeometric series, we can use classical transformations to obtain other closed-form expressions for it. Here is a first example.

Proposition 2.6.10.

$$\begin{aligned} P[X_d = k] &= \frac{2^k}{3^{2d+2k}} \binom{d-1+k}{d-1} {}_2F_1(k + 1/2, d + k; 2k + 1; 8/9) \ , \\ &= 3^{-2d} \sum_{j=k}^{\infty} \binom{d-1+j}{j} \binom{2j}{k+j} 2^j 3^{-2j} \ . \end{aligned}$$

Proof. It follows directly from the quadratic transformation [1, 15.3.27, p. 561]:

$${}_2F_1(a, b; a - b + 1; z) = (1 + \sqrt{z})^{-2a} {}_2F_1\left(a, a - b + \frac{1}{2}; 2a - 2b + 1; \frac{4\sqrt{z}}{(1 + \sqrt{z})^2}\right) \ ,$$

valid for $|z| < 1$. We obtain the following expression where we shift the summation index j by k:

$$P[X_d = k] = \frac{2^k}{3^{2d+2k}} \sum_{j=0}^{\infty} \binom{d-1+k+j}{d-1} \binom{2k+2j}{j} 2^j 3^{-2j}$$
$$= 3^{-2d} \sum_{j=k}^{\infty} \binom{d-1+j}{j} \binom{2j}{k+j} 2^j 3^{-2j} \ .$$

Here is an elementary proof. We know that

$$\sum_{j=0}^{\infty} P\left[\sum_{i=1}^{d} G_i = j\right] e^{ij\theta} = \frac{1}{(2-e^{i\theta})^d} \ ,$$

so, by Parseval's theorem,

$$\sum_{j=0}^{\infty} P\left[\sum_{i=1}^{d} G_i = j\right] P\left[\sum_{i=1}^{d} G_i = j+k\right] = \frac{1}{2\pi} \int_0^{2\pi} e^{ik\theta} \left|\frac{1}{(2-e^{i\theta})^d}\right|^2 d\theta$$
$$= \frac{1}{2\pi} \int_0^{2\pi} \frac{\cos(k\theta)}{(5-4\cos\theta)^d} d\theta$$
$$= \frac{1}{2\pi} \int_0^{2\pi} \frac{\cos(k\theta)}{(9-8\cos^2(\theta/2))^d} d\theta \ .$$

Moreover

$$\frac{1}{9^d} \frac{1}{\left(1-\frac{8}{9}\cos^2(\theta/2)\right)^d} = 3^{-2d} \sum_{j=0}^{\infty} \binom{d-1+j}{j} \cos^{2j}(\theta/2) 2^{3j} 3^{-2j} \ ,$$

and

$$\cos^{2j}(\theta/2) = \left(\frac{e^{i\theta/2}+e^{-i\theta/2}}{2}\right)^{2j} = 2^{-2j} \left(\binom{2j}{j} + \sum_{m=1}^{j} \binom{2j}{j+m} 2\cos(m\theta)\right) \ ,$$

so that

$$\frac{1}{2\pi} \int_0^{2\pi} \cos(k\theta) \cos^{2j}(\theta/2) d\theta = 2^{-2j} \binom{2j}{k+j} \ .$$

Hence, we have the identity

$$P[X_d = k] = 3^{-2d} \sum_{j=k}^{\infty} \binom{d-1+j}{j} \binom{2j}{k+j} 2^j 3^{-2j} \ . \qquad \square$$

This expression is interesting because it can be used to strengthen Proposition 2.6.7.

Corollary 2.6.11. *For $d \geq 1$, X_d follows a unimodal distribution centered at 0, i.e. $P[X_d = k]$ increases for $k \leq 0$ and decreases for $k \geq 0$.*

Proof. Indeed, $P[X_d = k]$ is an even function of k and for fixed $j \geq 0$ and $k \geq 0$ each summand of the expression given in the previous proposition decreases as k increases. $\square$

Moreover, specializing this expression at $k = 0$ yields an expression for P_d where d appears only twice.

Corollary 2.6.12. *For $d \geq 1$,*

$$P_d = 3^{-2d} \sum_{j=0}^{\infty} \binom{d-1+j}{j} \binom{2j}{j} 2^j 3^{-2j} \ .$$

Finally, we give other closed-form expressions for $P[X_d = k]$ which are of particular interest for actual computation because they express $P[X_d = k]$ as a finite sum.

Definition 2.6.13. *We define for $k \in \mathbb{Z}$, the polynomials*

$$h_{d,k}(z) = \sum_{j=-k}^{\infty} \binom{d-1+k+j}{d-1} z^j = \frac{z^{-k}}{(1-z)^d} \ ,$$

$$g_{d,k}(z) = \sum_{j=0}^{\infty} \binom{d-1+k+j}{d-1} z^j = h_{d,k}(z) - \sum_{j=0}^{k-1} \binom{d-1+j}{d-1} z^{j-k} \ ,$$

and

$$f_{d,k}(x,y) = g_{d,k}(x) g_{d,0}(y) \ .$$

Then, for $k \geq 0$,

$$P[X_d = k] = \frac{1}{4^d} \frac{1}{2^k} \mathcal{D}(f_{d,k})(1/4) = \frac{1}{4^d} \frac{1}{2^k} \mathcal{D}(h_{d,0}(x) h_{d,k}(y))(1/4) \ ,$$

where $\mathcal{D}$ is the diagonal of the double power series. A well-known result of Fürstenberg [105] states that

$$\mathcal{D}(f_{d,k})(t) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f_{d,k}(\epsilon e^{i\pi\theta}, t\epsilon^{-1} e^{-i\pi\theta}) d\theta = \frac{1}{2i\pi} \int_{|z|=\epsilon} f_{d,k}(z, t/z) \frac{dz}{z} \ ,$$

where $k \geq 0$ and ϵ is such that $f_{d,k}(x,y)$ is holomorphic for $|x| \leq \epsilon$ and $|y| \leq t\epsilon^{-1}$.

For $k \geq 0$ and t small enough, $\frac{f_{d,k}(z,t/z)}{z} = \frac{1}{(z-t)^d} \left(h_{d,k+1-d}(z) - \sum_{j=0}^{k-1} \binom{d-1+j}{d-1} z^{d-1-k+j} \right)$ has only a pole of order d at t near 0, so the residue theorem gives

$$\begin{aligned}
\mathcal{D}(f_{d,k})(t) &= \operatorname{Res}\left(\frac{f_{d,k}(z,t/z)}{z}, t \right) \\
&= \frac{1}{(d-1)!} \left((z-t)^d \frac{f_{d,k}(z,t/z)}{z} \right)^{(d-1)} (t) \\
&= \frac{1}{(d-1)!} \left(h_{d,k+1-d}(z) - \sum_{j=0}^{k-1} \binom{d-1+j}{d-1} z^{d-1-k+j} \right)^{(d-1)} (t) \ .
\end{aligned}$$

Finally, for $k \geq 0$,

$$P[X_d = k] = \frac{1}{4^d} \frac{1}{2^k} \frac{1}{(d-1)!} \left(h_{d,k+1-d}(z) - \sum_{j=0}^{k-1} \binom{d-1+j}{d-1} z^{d-1-k+j} \right)^{(d-1)} (1/4) \ .$$

Proposition 2.6.14. *For $d \geq 1$, $k \leq d-1$ and $i \geq 0$,*

$$h^{(i)}_{d,k+1-d}(z) = \frac{p_{d,k,i}(z)}{(1-z)^{d+i}} \ ,$$

where $p_{d,k,i}(z)$ is a polynomial in z of degree $d-1-k$ given by:

$$p_{d,k,i}(z) = i! \sum_{j=0}^{i} \binom{d-1-k}{j} \binom{k+i}{k+j} z^{d-1-k-j} \ .$$

Proof. For $i \geq 0$,

$$h^{(i+1)}_{d,k+1-d}(z) = \left(h^{(i)}_{d,k+1-d}\right)'(z) = \frac{(1-z)p'_{d,k,i-1}(z) + (d+i)p_{d,k,i-1}(z)}{(1-z)^{d+i+1}} \ .$$

The above equality shows that we can write down

$$p_{d,k,i}(z) = \sum_{j=0}^{d-1-k} a_{i,j} z^j \ ,$$

with

$$a_{i+1,j} = (j+1)a_{i,j+1} + (d+i-j)a_{i,j} \ .$$

In particular $a_{i,j} = 0$ for all $0 \leq j < d-1-k-i$ and $j > d-1-k$. We have to show that

$$a_{i,d-1-k-j} = i! \binom{d-1-k}{j} \binom{k+i}{k+j} \ .$$

The proof goes by induction on i. For $i = 0$,

$$p_{d,k,0}(z) = z^{d-1-k} = a_{0,d-1-k} z^{d-1-k} \ .$$

Suppose now that $i \geq 0$. By induction hypothesis,

$$\begin{aligned}
a_{i+1,d-1-k-j} &= (d-k-j)a_{i,d-k-j} + (k+i+1+j)a_{i,d-1-k-j} \\
&= (d-k-j)i! \binom{d-1-k}{j-1} \binom{k+i}{k+j-1} + (k+i+1+j)i! \binom{d-1-k}{j} \binom{k+i}{k+j} \\
&= \left((d-k-j)\frac{j}{d-k-j}\frac{k+j}{k+i+1} + (k+i+1+j)\frac{i-j+1}{k+i+1} \right) \\
&\qquad\qquad i! \binom{d-1-k}{j} \binom{k+i+1}{k+j} \\
&= \frac{j(k+j) + (k+i+1+j)(i-j+1)}{k+i+1} i! \binom{d-1-k}{j} \binom{k+i+1}{k+j} \\
&= (i+1)! \binom{d-1-k}{j} \binom{k+i+1}{k+j} \ .
\end{aligned}$$

□

The coefficients of $p_{d,k,i}$ are somewhat related to those of the Laguerre polynomials: $a_{i,j} = (-1)^j \frac{i!}{j!} \binom{i}{j}$ [1, 13.6.9, p. 509 and 22.2.12, p. 775].

Proposition 2.6.15. *For $d \geq 1$ and $0 \leq k \leq d-1$,*

$$P[X_d = k] = \frac{2^k}{3^{2d-1}} \sum_{j=0}^{d-1-k} \binom{d-1-k}{j} \binom{d-1+k}{j+k} 4^j \ .$$

Proof. For $d \geq 1$ and $0 \leq k \leq d-1$,

$$(z-t)^d \frac{f_{d,k}(z,t/z)}{z} = \frac{z^{d-1-k}}{(1-z)^d} - z^{d-1-k} \sum_{j=0}^{k-1} \binom{d-1+j}{d-1} z^j$$
$$= h_{d,k+1-d}(z) - \sum_{j=0}^{k-1} \binom{d-1+j}{d-1} z^{d-1-k+j} \ ,$$

where the sum on the right is a polynomial of degree less than $d-2$, so that its $d-1$-st derivative is 0 and

$$P[X_d = k] = \frac{1}{4^d} \frac{1}{2^k} \frac{1}{(d-1)!} h^{(d-1)}_{d,k+1-d}(1/4)$$
$$= \frac{1}{4^d} \frac{1}{2^k} \frac{1}{(d-1)!} \frac{(d-1)! \sum_{j=0}^{d-1-k} \binom{d-1-k}{j} \binom{d-1+k}{k+j} (1/4)^{d-1-k-j}}{(3/4)^{2d-1}}$$
$$= \frac{2^k}{3^{2d-1}} \sum_{j=0}^{d-1-k} \binom{d-1-k}{j} \binom{d-1+k}{k+j} 4^j \ . \qquad \square$$

Setting $k = 0$ in the above expression yields an expression for P_d as a finite sum.

Corollary 2.6.16. *For $d \geq 1$,*

$$P_d = \frac{1}{3^{2d-1}} \sum_{j=0}^{d-1} \binom{d-1}{j}^2 4^j \ .$$

Here is another expression for $P[X_d = k]$ for $0 \leq k \leq d-1$.

Proposition 2.6.17. *For $d \geq 1$ and $0 \leq k \leq d-1$,*

$$P[X_d = k] = \frac{2^k}{3^{d+k}} \sum_{j=0}^{d-1-k} \binom{d-1+k+j}{d-1} \binom{d-1-k}{j} 3^{-j} \ .$$

Proof. Using the binomial theorem, we have

$$h^{(i)}_{d,k+1-d}(z) = \sum_{j=0}^{i} \binom{i}{j} ((1-z)^{-d})^{(j)} (z^{d-1-k})^{(i-j)}$$
$$= \sum_{j=\max(0,i-d+1+k)}^{i} \binom{i}{j} \frac{(d-1+j)!}{(d-1)!} \frac{(d-1-k)!}{(d-1-k-i+j)!} \frac{z^{d-1-k-i+j}}{(1-z)^{d+j}} \ ;$$

for $i = d-1$, it gives,

$$h^{(d-1)}_{d,k+1-k}(z) = \sum_{j=k}^{d-1} \binom{d-1}{j} \frac{(d-1+j)!}{(d-1)!} \frac{(d-1-k)!}{(-k+j)!} \frac{z^{-k+j}}{(1-z)^{d+j}}$$
$$= \sum_{j=0}^{d-1-k} \binom{d-1}{k+j} \frac{(d-1+k+j)!}{(d-1)!} \frac{(d-1-k)!}{j!} \frac{z^j}{(1-z)^{d+k+j}}$$
$$= \sum_{j=0}^{d-1-k} (d-1)! \binom{d-1+k+j}{d-1} \binom{d-1-k}{j} \frac{z^{-j}}{(1-z)^{d+k+j}} \ ;$$

and

$$\begin{aligned} P[X_d = k] &= \frac{1}{4^d}\frac{1}{2^k}\frac{1}{(d-1)!}h^{(d-1)}_{d,d-1+k}(1/4) \\ &= \frac{1}{4^d}\frac{1}{2^k}\sum_{j=0}^{d-1-k}\binom{d-1+k+j}{d-1}\binom{d-1-k}{j}\frac{(1/4)^j}{(3/4)^{d+k+j}} \\ &= \frac{2^k}{3^{d+k}}\sum_{j=0}^{d-1-k}\binom{d-1+k+j}{d-1}\binom{d-1-k}{j}3^{-j} \ . \end{aligned}$$

□

Corollary 2.6.18. *For $d \geq 1$,*

$$P_d = \frac{1}{3^d}\sum_{j=0}^{d-1}\binom{d-1+j}{d-1}\binom{d-1}{j}3^{-j} \ .$$

It can be verified elementary that both these expressions for P_d are actually equal writing $4 = 1+3$ in the first one, developing the power using the binomial theorem, and using the identity

$$\binom{2n+k}{n+k} = \sum_{j=0}^{n}\binom{n}{j}\binom{n+k}{j+k} \ ,$$

which is a special case of the Chu–Vandermonde identity.

We now compute formulae for $k > d-1$.

Proposition 2.6.19. *For $d \geq 1$, $k > d-1$ and $i \geq 0$,*

$$h^{(i)}_{d,k+1-d}(z) = \frac{p_{d,k,i}(z)}{(1-z)^{d+i}} \ ,$$

where $p_{d,k,i}(z)$ is a polynomial in z^{-1} of degree $k-d+1+i$ given by

$$p_{d,k,i}(z) = i!\sum_{j=0}^{i}(-1)^j\binom{k+i}{k+j}\binom{k-d+j}{j}z^{d-1-k-j} \ .$$

Proof. The proof is similar to the one above. □

Proposition 2.6.20. *For $d \geq 1$ and $k > d-1$,*

$$\begin{aligned} P[X_d = k] = \frac{2^k}{3^{2d-1}}\sum_{j=0}^{d-1}(-1)^j\binom{d-1+k}{k+j}\binom{k-d+j}{j}4^j \\ + (-1)^d\frac{2^k}{4^d}\sum_{j=0}^{k-d}\binom{d-1+j}{d-1}\binom{k-1-j}{d-1}4^{-j} \ . \end{aligned}$$

Proof. For $d \geq 1$ and $k > d-1$,

$$(z-t)^d\frac{f_{d,k}(z,t/z)}{z} = h_{d,k}(z) - \sum_{j=0}^{k-1}\binom{d-1+j}{d-1}z^{d-1-k+j} \ ,$$

so that

$$\begin{aligned}
P[X_d = k] &= \frac{1}{4^d}\frac{1}{2^k}\frac{1}{(d-1)!}\left(h_{d,k+1-d}^{(d-1)}(1/4) - \sum_{j=0}^{k-d}\binom{d-1+j}{d-1}(z^{d-1-k+j})^{(d-1)}(1/4)\right)\\
&= \frac{1}{4^d}\frac{1}{2^k}\frac{1}{(d-1)!}\left(\frac{(d-1)!\sum_{j=0}^{d-1}(-1)^j\binom{d-1+k}{k+j}\binom{k-d+j}{j}(1/4)^{d-1-k-j}}{(3/4)^{2d-1}}\right.\\
&\qquad\left. - \sum_{j=0}^{k-d}(-1)^{d-1}\binom{d-1+j}{d-1}\frac{(k-1-j)!}{(k-d-j)!}(1/4)^{-k+j}\right)\\
&= \frac{2^k}{3^{2d-1}}\sum_{j=0}^{d-1}(-1)^j\binom{d-1+k}{k+j}\binom{k-d+j}{j}4^j\\
&\qquad + (-1)^d\frac{2^k}{4^d}\sum_{j=0}^{k-d}\binom{d-1+j}{d-1}\binom{k-1-j}{d-1}4^{-j}\ .
\end{aligned}$$

□

To conclude this subsection, let us mention that, using the expression of $P[X_d = k]$ as a Gaussian hypergeometric series, most of the above expressions can be directly deduced from the expression of $P[X_d = k]$ using linear transformations.

Proposition 2.6.21. *For $d \geq 1$ and $0 \leq k$,*

$$\begin{aligned}
P[X_d = k] &= \frac{4^{d-1}}{2^k 3^{2d-1}}\binom{d-1+k}{d-1}{}_2F_1(k+1-d, 1-d; k+1; 1/4)\\
&= \begin{cases} \frac{2^k}{3^{2d-1}}\sum_{j=0}^{d-1-k}\binom{d-1-k}{j}\binom{d-1+k}{j+k}4^j & \text{if } 0 \leq k \leq d-1\\ \frac{4^{d-1}}{2^k 3^{2d-1}}\sum_{j=0}^{d-1}(-1)^j\binom{d-1+k}{k+j}\binom{k-d+j}{k-d}4^{-j} & \text{if } d-1 < k \end{cases};\\
P[X_d = k] &= \frac{2^k}{3^{d+k}}\binom{d-1+k}{d-1}{}_2F_1(k+1-d, k+d; k+1; -1/3)\\
&= \begin{cases} \frac{2^k}{3^{d+k}}\sum_{j=0}^{d-1-k}\binom{d-1+k+j}{d-1}\binom{d-1-k}{j}3^{-j} & \text{if } 0 \leq k \leq d-1\\ \frac{2^k}{3^{d+k}}\sum_{j=0}^{\infty}(-1)^j\binom{d-1+k+j}{d-1}\binom{k-d+j}{k-d}3^{-j} & \text{if } d-1 < k \end{cases};\\
P[X_d = k] &= \frac{1}{2^k 3^d}\binom{d-1+k}{d-1}{}_2F_1(d, 1-d; k+1; -1/3)\\
&= \frac{1}{2^k 3^d}\sum_{j=0}^{d-1}\binom{d-1+j}{d-1}\binom{d-1+k}{k+j}3^{-j}\ .
\end{aligned}$$

Proof. The first expression comes from Euler's transformation [1, Formula 15.3.3]:

$${}_2F_1(a, b; c; z) = (1-z)^{c-a-b}{}_2F_1(c-a, c-b; c; z)\ .$$

The second one from Pfaff's transformation [1, Formula 15.3.5]:

$${}_2F_1(a, b; c; z) = (1-z)^{-b}{}_2F_1(c-a, b; c; z/(z-1))\ .$$

The third one from the other Pfaff's transformation [1, Formula 15.3.4]:

$${}_2F_1(a, b; c; z) = (1-z)^{-a}{}_2F_1(a, c-b; c; z/(z-1))\ .$$

□

We finally deduce different expressions for P_d as a finite sum.

Corollary 2.6.22. *For $d \geq 1$,*

$$P_d = \frac{1}{3^{2d-1}} {}_2F_1(1-d, 1-d; 1; 4) = \frac{1}{3^{2d-1}} \sum_{j=0}^{d-1} \binom{d-1}{j}^2 4^j \ ,$$

$$= \frac{1}{3^d} {}_2F_1(1-d, d; 1; -1/3) = \frac{1}{3^d} \sum_{j=0}^{d-1} \binom{d-1+j}{d-1} \binom{d-1}{j} 3^{-j} \ .$$

2.6.2 The limit $f_d(1, \infty, \ldots, \infty)$

In the previous subsection, we studied the behavior of $P_{t,k} = f_d(\beta_1, \ldots, \beta_d)$ as all the β_i's go to infinity. We will now fix a subset of them to 1 and let the other ones go to infinity. As was the case in the previous subsection, the expression of f_d given in Proposition 2.5.1 shows that such limits are well defined.

Recall the distribution probability for $\epsilon'_i = \gamma'_i + \beta_i - \delta'_i$ given by Proposition 2.4.6.

Proposition 2.4.6. *For $e_i \geq 0$,*

$$P(\epsilon'_i = e_i) = \begin{cases} 2^{-\beta_i} & \text{if } e_i = 0, \\ \frac{2^{-\beta_i}}{3}(2^{e_i} - 2^{-e_i}) & \text{if } 0 < e_i < \beta_i, \\ \frac{2^{\beta_i} - 2^{-\beta_i}}{3} 2^{-e_i} & \text{if } \beta_i \leq e_i. \end{cases}$$

Therefore, if we set $\beta_i = 1$ and let α_i go to infinity for some $i \in \{1, \ldots, d\}$, Proposition 2.4.10 shows that ϵ'_i has a similar behavior to the one of γ'_i and δ'_i: its law converges towards the law of a geometrically distributed variable with parameter $1/2$. Then we have a probabilistic interpretation for the limit $\lim_{\beta_j \to \infty, j>i} f_d(\overbrace{1, \ldots, 1}^{i}, \overbrace{\beta_{i+1}, \ldots, \beta_d}^{d-i})$ which we denote by $f_d(\overbrace{1, \ldots, 1}^{i}, \overbrace{\infty, \ldots, \infty}^{d-i})$.

As in the previous subsection, let $G_1, \ldots, G_d$ and $H_1, \ldots, H_d$ be $2d$ independent geometrically distributed variables with parameter $1/2$ and X_k denote the random variable $X_k = \sum_{j=1}^{k} G_j - \sum_{j=1}^{k} H_j$. Then

$$\begin{aligned} f_d(\underbrace{1, \ldots, 1}_{i}, \underbrace{\infty, \ldots, \infty}_{d-i}) &= \lim_{\beta_j \to \infty, j>i} P\left[\sum_d \gamma' < \sum_d \delta'\right] \\ &= \lim_{\beta_j \to \infty, j>i} P\left[\sum_i \epsilon' + \sum_{d-i} \gamma' < i + \sum_{d-i} \delta'\right] \\ &= P\left[\sum_{j=1}^{d} G_j < i + \sum_{j=1}^{d-i} H_j\right] \\ &= P\left[X_{d-i} + \sum_{j=i+1}^{d} G_j < i\right]. \end{aligned}$$

The first few values of such expressions, computed using explicit expressions for f_d, are given in Table 2.4.

Using the above probabilistic interpretation, it is possible to express $f_d(1, \infty, \ldots, \infty)$ with $f_d(\infty, \ldots, \infty) = P_d^0 = 1/2(1 - P_d)$, and so to compute it with the short closed-form expressions of the previous subsection.

Table 2.4: Values of $f_d(1,\dots,1,\infty,\dots,\infty)$ for $d \geq 1$

$i=$	d	$d-1$	...				
$d=1$	1/2	1/3					
$d=2$	1/2	4/9	11/27				
$d=3$	1/2	101/216	4/9	35/81			
$d=4$	1/2	619/1296	112/243	328/729	971/2187		
$d=5$	1/2	15029/31104	10969/23328	112/243	2984/6561	8881/19683	
$d=6$	1/2	90829/186624	2777/5832	1024/2187	9104/19683	9028/19683	2993/6561

Proposition 2.6.23. *For $d \geq 2$,*

$$f_d(1,\infty,\dots,\infty) = \frac{3}{2} f_d(\infty,\dots,\infty) - \frac{1}{2} f_{d-1}(\infty,\dots,\infty) \ .$$

Proof. We equivalently show that

$$f_d(\infty,\dots,\infty) = \frac{1}{3} f_{d-1}(\infty,\dots,\infty) + \frac{2}{3} f_d(1,\infty,\dots,\infty) \ ,$$

i.e. written in a probabilistic way,

$$P\left[0 < X_d\right] = \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{2}{3} P\left[X_{d-1} < 1 - G_d\right] \ .$$

The first step is then to split X_d as $X_d = X_{d-1} + X_1$ in the left hand side of that equality.

$$\begin{aligned}
P\left[0 < X_d\right] = P\left[0 < X_{d-1} + X_1\right] &= \sum_{i=-\infty}^{+\infty} P\left[X_1 = i\right] P\left[-i < X_{d-1}\right] \\
&= \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{1}{3} \sum_{i=1}^{\infty} \frac{1}{2^i} \left(P\left[i < X_{d-1}\right] + P\left[-i < X_{d-1}\right]\right) \\
&= \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{1}{3} \sum_{i=1}^{\infty} \frac{1}{2^i} \left(P\left[i < X_{d-1}\right] + P\left[X_{d-1} < i\right]\right) \\
&= \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{1}{3} \sum_{i=1}^{\infty} \frac{1}{2^i} \left(P\left[X_{d-1} \neq i\right]\right) \\
&= \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{1}{3} \sum_{i=1}^{\infty} \frac{1}{2^i} \left(1 - P\left[X_{d-1} = i\right]\right) \\
&= \frac{1}{3} P\left[0 < X_{d-1}\right] + \frac{1}{3} \left(1 - \sum_{i=1}^{\infty} \frac{1}{2^i} P\left[X_{d-1} = i\right]\right) \ .
\end{aligned}$$

Injecting this equality back into the original one, it is then enough to show that

$$2P\left[X_{d-1} < 1 - G_d\right] = 1 - \sum_{i=1}^{\infty} \frac{1}{2^i} P\left[X_{d-1} = i\right] \ ,$$

which is proved by splitting the left term of the equality according to the value of G_d:

$$\begin{aligned}
P\left[X_{d-1} < 1 - G_d\right] &= \sum_{i=0}^{\infty} \frac{1}{2^{i+1}} P\left[X_{d-1} < 1 - i\right] \\
&= \frac{1}{2} P\left[X_{d-1} < 1\right] + \frac{1}{4} \sum_{i=0}^{\infty} \frac{1}{2^i} P\left[X_{d-1} < -i\right] \\
&= \frac{1}{2} \left(1 - P\left[1 \leq X_{d-1}\right]\right) + \frac{1}{4} \sum_{i=0}^{\infty} \frac{1}{2^i} P\left[i < X_{d-1}\right] \\
&= \frac{1}{2} - \frac{1}{2} \sum_{i=1}^{\infty} P\left[X_{d-1} = i\right] + \frac{1}{4} \sum_{i=1}^{\infty} \left(\sum_{j=0}^{i-1} \frac{1}{2^j} \right) P\left[X_{d-1} = i\right] \\
&= \frac{1}{2} - \frac{1}{2} \sum_{i=1}^{\infty} P\left[X_{d-1} = i\right] + \frac{1}{2} \sum_{i=1}^{\infty} \left(1 - \frac{1}{2^i}\right) P\left[X_{d-1} = i\right] \\
&= \frac{1}{2} - \frac{1}{2} \sum_{i=1}^{\infty} \frac{1}{2^i} P\left[X_{d-1} = i\right] \ .
\end{aligned}$$

□

As a corollary of the above equality and of the monotonicity of P_d, we deduce the following inequality.

Corollary 2.6.24. *For $d \geq 2$,*

$$f_d(1, \infty, \ldots, \infty) > f_d(\infty, \infty, \ldots, \infty) \ .$$

2.7 An inductive approach

In this section we follow a different approach: $t \in \mathbb{N}$ is a fixed integer and we let k grow. We want to study the behavior of $S_{t,k}$ as k grows, adding `0`'s or `1`'s to the binary expansion of t on k bits. Obviously, as long as $2^k < t$, the binary expansion of $t \mod 2^k - 1$ has an inconsistent behavior. Whence the following definition.

Definition 2.7.1 (Length)**.** *Let t be a natural integer. Its binary length is defined to be the smallest integer k such that $t \leq 2^k$. We denote it by $l(t)$.*

We obviously have $l(t) = \lceil \log_2(t) \rceil$. Then, if $k \geq l(t)$, the binary expansion of t on $k+1$ bits is that of t on k bits with a `0` prepended, so we will suppose that k and t are such that $k \geq l(t)$.

Considering the binary string associated with a modular integer a in $\mathbb{Z}/(2^k - 1)\mathbb{Z}$, we write down `0`$a$ and `1`a for the binary string of a on k bits with a `0` or a `1` prepended. We note that $2^k - 1$ which is equal to 0 in $\mathbb{Z}/(2^k - 1)\mathbb{Z}$ but not in $\mathbb{Z}/(2^{k+1} - 1)\mathbb{Z}$ can not be described as `0`a or `1`a for $a \in \mathbb{Z}/(2^k - 1)\mathbb{Z}$.

2.7.1 Overflow and inertia

Definition 2.7.2. *We split $C_{t,k,i}$ according to the value of the sum $a + t$ in $\mathbb{Z}$:*

- $I_{t,k,i} = \left\{ a \in \mathbb{Z}/(2^k - 1)\mathbb{Z} \mid r(a,t) = \mathrm{w_H}(t) - i, a + t < 2^k - 1 \text{ in } \mathbb{Z} \right\}$*, the* inert *modular integers;*

- $O_{t,k,i} = \left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid r(a,t) = \mathrm{w_H}(t) - i, a + t \geq 2^k - 1 \text{ in } \mathbb{Z}\right\}$, *the* overflowing *modular integers.*

Remember that $r(0,t) = k$ *and that* 0 *is considered to act as the* `1...1` *binary string, so that we have* $0 \in O_{t,k,\mathrm{w_H}(t)-k}$.

We define $I_{t,k} = \bigsqcup_{i\in\mathbb{Z}} I_{t,k,i}$ *and* $O_{t,k} = \bigsqcup_{i\in\mathbb{Z}} O_{t,k,i}$.

Lemma 2.7.3. *Let* $t \in \mathbb{N}$ *and* $k \geq l(t)$. *Then*

$$\#C_{t,k,i} = \#I_{t,k,i} + \#O_{t,k,i} \ .$$

We will now study the behavior of these sets as k grows.

2.7.2 Adding `0`'s

We want to let k grow as t is fixed, i.e. add `0`'s in front of the binary string associated with t as soon as $k \geq l(t)$.

If $a \in I_{t,k,i}$, then $\mathtt{0}a$ and $\mathtt{1}a$ are in $I_{\mathtt{0}t,k+1,i}$. Unfortunately, the situation is more complicated for $O_{t,k,i}$:

- if $a \neq 0$ and $a \neq -t$ is in $O_{t,k,i}$, then $\mathtt{1}a$ is in $O_{\mathtt{0}t,k+1,i-1}$, and $\mathtt{0}a$ is in $I_{\mathtt{0}t,k+1,j}$ with $j \geq i$;
- if $a = 0$, then $a \in O_{t,k,\mathrm{w_H}(t)-k}$, $\mathtt{0}a = 0 \in O_{\mathtt{0}t,k+1,\mathrm{w_H}(t)-k-1}$, and $\mathtt{1}a = 2^k \in I_{\mathtt{0}t,k+1,\mathrm{w_H}(t)}$;
- If $a = -t$, then $a \in O_{t,k,\mathrm{w_H}(t)-k}$, $\mathtt{0}a = \mathtt{0}\bar{t}^k \in I_{\mathtt{0}t,k+1,\mathrm{w_H}(t)}$, and $\mathtt{1}a = -t \in O_{\mathtt{0}t,k+1,\mathrm{w_H}(t)-k-1}$;

Finally, $2^k - 1 = \mathtt{0}\underbrace{\mathtt{1}\ldots\mathtt{1}}_{=k} \in I_{\mathtt{0}t,k+1,j}$ with $j \leq \mathrm{w_H}(t) - k$.

The following lemma summarizes the above discussion.

Lemma 2.7.4. *Let* $t \in \mathbb{N}$ *and* $k \geq l(t)$. *Then*

$$O_{\mathtt{0}t,k+1,i-1} = \begin{cases} \mathtt{1}O_{t,k,i} & \text{if } i < \mathrm{w_H}(t) - k \\ \mathtt{1}\left(O_{t,k,i} \setminus \{0\}\right) \sqcup \{0\} & \text{if } i = \mathrm{w_H}(t) - k \end{cases},$$

$$\bigsqcup_{j\geq i} I_{\mathtt{0}t,k+1,j} \supset \begin{cases} \mathtt{0}O_{t,k,i} & \text{if } i < \mathrm{w_H}(t) - k \\ \mathtt{0}\left(O_{t,k,i} \setminus \{0\}\right) \sqcup \left\{2^k\right\} & \text{if } i = \mathrm{w_H}(t) - k \end{cases},$$

$$I_{\mathtt{0}t,k+1,i} \supset \mathtt{0}I_{t,k,i} \sqcup \mathtt{1}I_{t,k,i} \ .$$

Lemma 2.7.5. *Let* $t \in \mathbb{N}$ *and* $k \geq \mathrm{w_H}(t) + l(t)$. *If* $i \geq 0$, *then* $O_{t,k,i} = \emptyset$.

Proof. Indeed $t = \underbrace{\mathtt{0}\ldots\mathtt{0}}_{\geq \mathrm{w_H}(t)}\ldots$, so $a = {}^{\leftarrow}\underbrace{\mathtt{1}\ldots\mathtt{1}}_{\geq \mathrm{w_H}(t)}{}^{\leftarrow}\ldots$ and $r(a,t) > \mathrm{w_H}(t)$. □

Proposition 2.7.6. *Let* $t \in \mathbb{N}$ *and* $k \geq \mathrm{w_H}(t) + l(t)$. *Then*

$$\#S_{\mathtt{0}t,k+1} = 2\#S_{t,k} - 1 \ .$$

Proof. Since $k \geq \mathrm{w_H}(t) + l(t)$, $2^k - 1 \in I_{\mathtt{0}t,k+1,i}$ with $i < 0$ ($t \neq 0$) and $O_{t,k,i} = \emptyset$ for $i \geq 0$ so that

$$I_{\mathtt{0}t,k+1,i} = \begin{cases} \mathtt{0}I_{t,k,i} \sqcup \mathtt{1}I_{t,k,i} & \text{for } 0 \leq i < \mathrm{w_H}(t) \\ \mathtt{0}I_{t,k,i} \sqcup \mathtt{1}I_{t,k,i} \sqcup \left\{2^k, \bar{t}^k\right\} & \text{for } i = \mathrm{w_H}(t) \end{cases},$$

and

$$\begin{aligned}\#E_{\mathtt{0}t,k+1} \sqcup T_{\mathtt{0}t,k+1} &= \sum_{i\geq 0} \#I_{\mathtt{0}t,k+1,i} + \#O_{\mathtt{0}t,k+1,i} \\ &= \sum_{i\geq 0} \#I_{\mathtt{0}t,k+1,i} \\ &= 2\sum_{i\geq 0} \#I_{t,k,i} + 2 \\ &= 2\#E_t \sqcup T_{t,k} + 2 \ .\end{aligned}$$

Then

$$\begin{aligned}\#S_{\mathtt{0}t,k+1} &= 2^{k+1} - 1 - \#E_{\mathtt{0}t,k+1} \sqcup T_{\mathtt{0}t,k+1} \\ &= 2(2^k - 1 - \#E_t \sqcup T_{t,k}) - 1 \\ &= 2\#S_{t,k} - 1 \ .\end{aligned}$$

□

Unfortunately, that equality is not true for $l(t) \leq k < l(t) + \mathrm{w_H}(t)$, and it can even happen that $\#S_{\mathtt{0}t,k+1} > 2\#S_{t,k}$. However, experimental results suggest that, as soon as $k \geq l(t) + 2$, the following inequality is true.

Conjecture 2.7.7. *Let $t \in \mathbb{N}$. For $k \geq l(t) + 2$,*

$$\#S_{\mathtt{0}t,k+1} \leq 2\#S_{t,k} \ .$$

2.7.3 Adding 1's

In light of Theorem 2.4.15, one would also like to increase the size of the `1` subblocks, even "empty" ones, that is insert `1`'s between `0`'s. Write down t (or an equivalent one) as:

$$t = \underbrace{\mathtt{1{-}{-}{-}1}}_{\alpha_1}\mathtt{0{-}{-}{-}0}\ldots\mathtt{1{-}{-}{-}10{-}{-}{-}0} \ .$$

In contrast with the previous section, we allow $\alpha_1 = 0$, i.e. t can begin with a `0`. However we want the last `0` subblock to be non-empty. So here d will potentially denote the previous number of blocks plus one if $\alpha_1 = 0$. For the sake of clarity, d can be defined to be the number of blocks of $\mathtt{1}t$.

If $a \in O_{t,k,i}$, then $\mathtt{1}a$ and $\mathtt{0}a$ are in $O_{\mathtt{1}t,k+1,i}$ (except for $\mathtt{10{-}{-}{-}0} = 2^k$, but we get $\mathtt{01{-}{-}{-}1} = 2^k - 1$ instead). If $a \in I_{t,k,i}$, then $\mathtt{1}a \in O_{\mathtt{1}t,k+1,j}$ with $j \leq i$ and $\mathtt{0}a \in I_{\mathtt{1}t,k+1,i+1}$. Hence, it may happen that $2\#S_{t,k} > \#S_{\mathtt{1}t,k+1}$. It is not even true that

$$2^{B-1-\alpha_1}\#S_{t,k} \leq \#S_{\mathtt{1}\ldots\mathtt{1}t,k+B-1-\alpha_1}$$

where $B - 1 - \alpha_1$ `1`'s have been added in front of t.

As pointed above, it is not true in general that

$$2\#S_{t,k} \leq \#S_{\mathtt{1}t,k+1} \ ,$$

or equivalently that $\#I_{t,k,-1} < \#\{a \in I_{t,k,i}, i \geq 0 \mid \mathtt{1}a \in O_{\mathtt{1}t,k+1,j}, j < 0\}$. However, once a block is big enough, its behavior is known.

Proposition 2.7.8. *Let $t \in \mathbb{N}$ and $k \geq l(t)$. If $\alpha_1 \geq B-1$, then*

$$\#S_{1t,k+1} = 2\#S_{t,k} \ .$$

Proof. Indeed, if $a \in I_{t,k}$, then $a \notin S_{t,k}$ and neither $\mathtt{1}a$ nor $\mathtt{0}a$ are in $S_{1t,k+1}$. Then $S_{t,k} = \bigsqcup_{i<0} O_{t,k,i}$ and

$$\begin{aligned} S_{1t,k+1} &= \bigsqcup_{i<0} O_{1t,k+1,i} \\ &= \left(\mathtt{1}(O_{t,k,k-\mathrm{w_H}(t)} \setminus \{0\}) \sqcup \mathtt{0}O_{t,k,k-\mathrm{w_H}(t)} \sqcup \left\{2^k-1\right\}\right) \sqcup \bigsqcup_{\mathrm{w_H}(t)-k<i<0} \mathtt{1}O_{t,k,i} \sqcup \mathtt{0}O_{t,k,i} \ , \end{aligned}$$

whence the equality. □

Proposition 2.7.9. *Let $t \in \mathbb{N}$ and $k \geq l(t)$. If $\alpha_1 = B-2$, then*

$$\#S_{1t,k+1} = 2\#S_{t,k} + 2^{k-2B+2} = 2\#S_{t,k} + 2^{\mathrm{w_H}(t)-\alpha_1} \ .$$

Proof. If $t = 0$, then $k = 2$ and $\#S_{1,3} = 3 = 2 \cdot 1 + 1 = 2\#S_{0,2} + 1$.

Suppose now that $t \neq 0$. If a is inert, the situation is as follows:

$$\begin{aligned} t &= \overset{\times}{\overbrace{\mathtt{1}\text{---}\overset{\times}{\mathtt{1}}}}\mathtt{0}\ldots\overset{\times}{\mathtt{0}}, \\ a &= \underline{\mathtt{0}\text{---}\mathtt{0}?}\ldots\underline{?} \ , \end{aligned}$$

so at least B carries are lost (the underlined bits) and a can not be in $S_{t,k}$. Hence, $S_{t,k} = \bigsqcup_{i<0} O_{t,k,i}$ and

$$S_{1t,k+1} \supset \left(\mathtt{1}(O_{t,k,k-\mathrm{w_H}(t)} \setminus \{0\}) \sqcup \mathtt{0}O_{t,k,k-\mathrm{w_H}(t)} \sqcup \left\{2^k-1\right\}\right) \sqcup \bigsqcup_{\mathrm{w_H}(t)-k<i<0} \mathtt{1}O_{t,k,i} \sqcup \mathtt{0}O_{t,k,i} \ ,$$

so that $\#S_{1t,k+1} \geq 2\#S_{t,k}$.

If $a \in I_{t,k}$, then a must have at least a $\mathtt{0}$ in front of a $\mathtt{1}$ of t, otherwise a is in fact in $O_{t,k}$. Moreover, if such a $\mathtt{0}$ is not in front of the first $\mathtt{0}$ of t, then

$$\begin{aligned} t &= \overset{\times}{\overbrace{\mathtt{1}\text{---}\overset{\times}{\mathtt{1}}}}\mathtt{0}\ldots\overset{\times}{\mathtt{0}}\ldots\overset{\times}{\mathtt{0}}, \\ a &= \mathtt{0}\text{---}\mathtt{0}?\ldots\mathtt{0}\ldots? \ , \end{aligned}$$

and we have the following situation for $\mathtt{1}t$ and $\mathtt{1}a$:

$$\begin{aligned} \mathtt{1}t &= \mathtt{1}\overset{\leftarrow}{\overbrace{\mathtt{1}\text{---}\overset{\times}{\mathtt{1}}}}\mathtt{0}\ldots\overset{\times}{\mathtt{0}}\ldots\mathtt{0}^{\leftarrow}, \\ \mathtt{1}a &= \mathtt{1}\underline{\mathtt{0}\text{---}\mathtt{0}?}\ldots\underline{\mathtt{0}}\ldots? \ , \end{aligned}$$

so that at least B carries are lost. Finally, $a \in I_{t,k}$ is such that $\mathtt{1}a \in O_{1t,k+1,j}$ with $j \leq 0$ (in fact $j = -1$) if and only if it has only $\mathtt{1}$'s in front of the $\mathtt{0}$'s of t except for the first one. There are exactly $2^{k-(B-2)-B} = 2^{k-2B+2}$ such a's whence the equality of the proposition. □

Proposition 2.7.10. *Let $t \in \mathbb{N}$ and $k \geq l(t)$. Suppose that $\alpha_1 = B-3$. If $d = 1$, then*

$$\#S_{1t,k+1} = 2\#S_{t,k} + 3 \ .$$

If $d > 1$, then

$$\begin{aligned} \#S_{1t,k+1} &= 2\#S_{t,k} + (d + 1 + 4 \cdot 1_{\beta_1>1} - 2 \cdot 1_{\beta_d>1})2^{k-2B+2} \\ &= 2\#S_{t,k} + (d + 1 + 4 \cdot 1_{\beta_1>1} - 2 \cdot 1_{\beta_d>1})2^{\mathrm{w_H}(t)-\alpha_1-1} \ . \end{aligned}$$

Proof. If $t = 0$, then $k = 3$, i.e. $t = \texttt{000}$ and $\#S_{1,4} = 4 = 2 \cdot 1 + 3 = 2\#S_{0,3} + 1$.

If $d = 1$ and $t \neq 0$, then $t = \underbrace{\texttt{1---1}}_{\alpha_1 \geq 1}\underbrace{\texttt{0---0}}_{\alpha_1+3}$, and the formula follows from Theorem 2.4.8.

Suppose now that $d > 1$. As in the proof of the previous proposition, $I_{t,k,i}$ is empty for $i < 0$ if $\beta_d > 1$ because at least $B - 2 + \beta_d \geq B$ carries are lost. If $\beta_d = 1$, then $I_{t,k,-1}$ is not empty and consists exactly of the following a's:

$$\begin{aligned} t &= \overset{\times}{\overbrace{\texttt{1---1}}^{B-3}}\overset{\times}{\texttt{0}}\texttt{...10}^{\times}, \\ a &= \underline{\texttt{0---00}}\texttt{...1?} \ , \end{aligned}$$

with only `1`'s in front of the other `0`'s of t, so that $\#I_{t,k,-1} = 2^{k-(B-3)-B} = 2^{k-2B+3}$.

We now enumerate the $a \in I_{t,k}$ such that $\texttt{1}a \in S_{\texttt{1}t,k+1}$. As before, a must have at least a `0` in front of a `1` of t and we get $2^{k-(B-3)-B} = 2^{k-2B+3}$ different a's with only `1`'s in front of the `0`'s of t except for the first one.

There are also inert a's with that `0` and another `0` just before a block of `1`'s as depicted below:

$$\begin{aligned} t &= \overset{\times}{\overbrace{\texttt{1---1}}^{B-3}}\overset{\times}{\texttt{0}}\texttt{...1---10...0}^{\times}, \\ a &= \underline{\texttt{0---00}}\texttt{...?--?1}\underline{\texttt{0}}\texttt{...1} \ . \end{aligned}$$

For such an a, $\texttt{1}a$ will lose at least $B - 1$ carries, so it must have a `1` before the second `0` and `1`'s in front of any other `0` of t to be in $S_{\texttt{1}t,k+1}$. There are $2^{k-(B-3)-B-1} = 2^{k-2B+2}$ such a's for each choice of the second `0` and $d - 1$ such choices, so $(d-1)2^{k-2B+2}$ different a's.

If $\beta_1 > 1$, it is also possible to put that second `0` in front of the second `0` of t:

$$\begin{aligned} t &= \overset{\times}{\overbrace{\texttt{1---1}}^{B-3}}\overset{\times}{\texttt{00}}\texttt{...0}^{\times}, \\ a &= \underline{\texttt{0---000}}\texttt{...1} \ . \end{aligned}$$

For such an a, at least $B - 1$ carries are lost for a and $\texttt{1}a$ as well, so that $\texttt{1}a \in S_{\texttt{1}t,k+1}$ if and only if there are only `1`'s in front of each other `0` of t. There are exactly $2^{k-(B-3)-B} = 2^{k-2B+3}$ such a's.

If an inert a has a `1` in front of the first `0` of t and $\beta_1 = 1$, then

$$\begin{aligned} t &= \overset{\times}{\overbrace{\texttt{1---1}}^{B-3}}\texttt{01---}\overset{\times}{\texttt{1}}\texttt{..}^{\times}\texttt{0...0}^{\times}, \\ a &= \underline{\texttt{0---010---0}}\texttt{...}\underline{\texttt{0}}\texttt{...1} \ , \end{aligned}$$

so that at least $B - 1 + \alpha_2 \geq B$ carries are lost for $\texttt{1}a$ and it can not be in $S_{\texttt{1}t,k+1}$.

If however $\beta_1 > 1$ and there is a `0` in front of the second `0` of t, then

$$\begin{aligned} t &= \overset{\times}{\overbrace{\texttt{1---1}}^{B-3}}\overset{\times}{\texttt{00}}\texttt{...0}^{\times}, \\ a &= \underline{\texttt{0---010}}\texttt{...1} \ , \end{aligned}$$

so that at least $B - 1$ carries are lost for a and $\texttt{1}a$ as well. Hence, $\texttt{1}a \in S_{\texttt{1}t,k+1}$ if and only if there are only `1`'s in front of each other `0` of t. There are exactly $2^{k-(B-3)-B} = 2^{k-2B+3}$ such a's.

Adding the above quantities gives the formula of the proposition. □

2.8 Other works

We now compare our results with those of Cusick, Li and Stănică [62], and those of Carlet [37].

2.8.1 Cusick et al.

Cusick, Li and Stănică [62] proved the conjecture in some specific cases:

- $\mathrm{w_H}(t) = 1, 2$,
- $t = 2^k - t'$ with $\mathrm{w_H}(t') \leq 2$ and t' even,
- $t = 2^k - t'$ with $\mathrm{w_H}(t') \leq 4$ and t' odd,

by splitting each case in several subcases and using specific counting arguments for each one. We now compare their results with ours.

The first case is treated by different theorems:

- $\mathrm{w_H}(t) = 1$ if and only if $t \simeq 1$, so this case is taken care of by Theorem 2.4.8.
- $\mathrm{w_H}(t) = 2$ if and only if $t \simeq 3$ which is included in Theorem 2.4.8 or $d = 2$ and $\alpha_1 = \alpha_2 = 1$ which is included in the corollary of Theorem 2.4.15.

The second one reads $t = 2^k - t' = 1 + \overline{t'}$ with $\mathrm{w_H}(t') \leq 2$ and t' even. If $\mathrm{w_H}(t') = 0$, then $t = 1$. If $\mathrm{w_H}(t') = 1$, then $t = 2^k - 2^i$ is made of one block which is included in Theorem 2.4.8. If $\mathrm{w_H}(t') = 2$, then our theorems can not be used to conclude.

The last one reads $t = 2^k - t' = 1 + \overline{t'}$ with $\mathrm{w_H}(t') \leq 4$ and t' odd, i.e. $t = 0$ or $\mathrm{w_H}(t) \geq k - 3$ (and $t = 1 \pmod 2$ which is not important). If $\mathrm{w_H}(t) = k - 1$, then $t \simeq -1$. If $\mathrm{w_H}(t) = k - 2$, then $t \simeq -3$ which is made of one block and is included in Theorem 2.4.8, or t is made of two blocks with $\beta_1 = \beta_2 = 1$ which is included in Theorem 2.4.15. The only subcases not directly included in our Theorems 2.4.8, 2.4.14 and 2.4.15 when $\mathrm{w_H}(t) = k - 3$ are:

- if $d = 2$:
  - `10010`, but it is taken care of by the corollary of Theorem 2.4.15,
  - `001101` and `110010`, which can be directly computed;
- if $d = 3$:
  - `101010`, but it is taken care of by Theorem 2.3.14,
  - one or two, but not three, α_i's equal to 1, which is not treated by our theorems.

Their approach kind of lacks a general strategy to tackle the conjecture, but points out the relevance of what we denote by $r(a, t)$, the number of carries.

2.8.2 Carlet

Carlet [37] proved the conjecture in the following cases:

- $\mathrm{w_H}(t) = 0, 1$;
- and $t = 2^i - 2^j$;

using affine functions and multisets. Both these results deal with numbers made of one block and are included in Theorem 2.4.8.

2.8.3 Towards a complete proof

The numbers for which $P_{t,k}$ is the nearest to the bound of the conjecture seem to be the ones which verify the constraint $\min(\alpha_i) \geq k - \mathrm{w_H}(t) - 1$, and especially the ones which also satisfy $\beta_i = 1$ for all i. Moreover, puncturing a `1` out of a binary string seems to make $P_{t,k}$ smaller most of the time.

We consequently hope to be able to completely solve the conjecture using one of the following strategies:

- Show that any number gives a smaller set than an *extremal* one by induction (i.e. by puncturing `1`'s, even so that different blocks merge).
- Show that the conjecture is true for every number which verifies the constraint $\min(\alpha_i) \geq k - \mathrm{w_H}(t) - 1$, and then that the other numbers give smaller sets by induction (i.e. by puncturing `1`'s, but without merging different blocks).

2.9 Efficient test of the Tu–Deng conjecture

2.9.1 The Tu–Deng algorithm

In this subsection we present the reformulation of Conjecture 1.2.2 by Tu and Deng [264, Appendix] using the transfer-matrix method [249, Subsection 4.7]. Their idea is to build the automata describing the addition bit after bit of two modular integers modulo $2^k - 1$ for any integer k. Its states are given by triplets corresponding to the two current bits and the previous carry. In particular, this automata does not depend on k.

For a fixed $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, let D be the directed graph corresponding to this automata. Its vertices are the triplets[8] $(a,t,r) \in \{0,1\}^3$. There exists an edge from (a,t,r) to (a',t',r') if and only if $t + 2r' - a - r \in \{0,1\}$ and its weight is $x^{r'}$ where x is a polynomial indeterminate. In particular, all edges to a given node have the same weight, but this is also true for all the vertices from a given node.

If $(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2$ verifies $a + b = t$, we can define a closed path in D as follows. For $0 \leq j \leq k-1$, denote by v_j the vertex $v_j = (a_j, t_j, r_{j-1})$ where r_{j-1} is 1 if a carry comes from the $j-1$-st bit when adding a and b and 0 otherwise. Then, (a,b) corresponds to the closed path $\Gamma:\ v_0 \to v_1 \to \cdots \to v_{k-1} \to v_0$ of weight $\mathrm{w_H}(\Gamma) = x^{r(a,b)}$.

The vertices of D are mapped to the range of integers $[0,7]$ via the following map: $(a,t,r) \mapsto 4a + 2t + r$. The directed graph D is depicted in Figure 2.6 where edges from the nodes labeled 0, 2, 6 and 3 have weight 1 and edges from the nodes label-led 1, 5, 7 and 4 have weight x; its adjacency matrix A is given in Figure 2.7.

Let V_i be the set of vertices (a,t,r) such that $t = i \in \{0,1\}$, i.e. $V_0 = \{0,1,4,5\}$ and $V_1 = \{2,3,6,7\}$. Denote by $B_{i,j}$ the submatrices of A made of the entries at the intersection of the rows and columns respectively specified by V_i and V_j for $i,j \in \{0,1\}$. Then, $B_{0,0} = B_{0,1}$ and $B_{1,0} = B_{1,1}$ are respectively given by the following $(4,4)$-matrices B and C:

$$B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & x & 0 & x \\ 0 & x & 0 & x \\ 0 & x & 0 & x \end{pmatrix},\ C = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & x & 0 & x \end{pmatrix}\ .$$

[8] There is a slight inconsistency in our notation here: t and a denote both modular integers and one of their bits. For simplicity, we allow ourselves to make that abuse of notation.

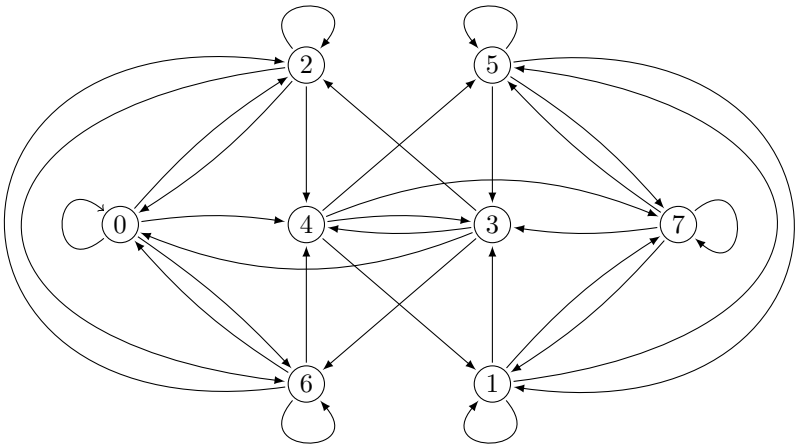


Figure 2.6: Directed graph D

$$\begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & x & 0 & x & 0 & x & 0 & x \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & x & 0 & x & 0 & x & 0 & x \\
0 & x & 0 & x & 0 & x & 0 & x \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & x & 0 & x & 0 & x & 0 & x
\end{pmatrix}$$

Figure 2.7: Adjacency matrix A of directed graph D

Recall that t (or an equivalent one) can be written down as

$$t = \underbrace{\overbrace{1\texttt{---}}^{\alpha_1}\overbrace{10\texttt{---}0}^{\beta_1}}_{t_1} \cdots \underbrace{\overbrace{1\texttt{---}}^{\alpha_i}\overbrace{10\texttt{---}0}^{\beta_i}}_{t_i} \cdots \underbrace{\overbrace{1\texttt{---}}^{\alpha_d}\overbrace{10\texttt{---}0}^{\beta_d}}_{t_d} \ .$$

Then, each integer coefficient μ_i of the polynomial

$$\begin{aligned}\sum_{i=0}^{k-1} \mu_i x^i &= \mathrm{Tr}\left(B_{0,0}^{\beta_d - 1} B_{0,1} B_{1,1}^{\alpha_d - 1} B_{1,0} \cdots B_{0,0}^{\beta_1 - 1} B_{0,1} B_{1,1}^{\alpha_1 - 1} B_{1,0}\right) \\ &= \mathrm{Tr}\left(B^{\beta_d} C^{\alpha_d} \cdots B^{\beta_1} C^{\alpha_1}\right)\end{aligned}$$

represents the number of closed paths in D with length k and weight i, i.e. the number of couples $(a, b) \in \left(\mathbb{Z}/(2^k - 1)\mathbb{Z}\right)^2$ such that $a + b = t$ and $r(a, b) = i$. Hence, we get the equality

$$\#S_{t,k} = \sum_{i=0}^{k-1-\mathrm{w_H}(t)} \mu_i \ .$$

To check the validity of the conjecture for a given t, it is therefore sufficient to compute the trace of a product of at most k $(4, 4)$-matrices.

Moreover, it is a basic result that testing one t in each cyclotomic class is enough. For example, the smallest one, which is called the *cyclotomic leader*, can be chosen.

To summarize, the algorithm devised by Tu and Deng to check the validity of their conjecture is described in Algorithm 2.1.

Algorithm 2.1: Tu–Deng algorithm

Input: A positive integer $k \geq 2$
Output: True if the conjecture is verified for k, False otherwise

```
Compute the set T of cyclotomic leaders modulo 2^k − 1
foreach t in T do
    Compute the sets {α_i} and {β_i} for t
    Compute the polynomial Σ_{i=0}^{k−1} μ_i x^i = Tr(B^{β_d} C^{α_d} ··· B^{β_1} C^{α_1})
    if Σ_{i=0}^{k−1−w_H(t)} μ_i > 2^{k−1} then
        return False
return True
```

2.9.2 Necklaces and Lyndon words

The link between cyclotomic equivalence modulo $2^k - 1$ and rotation of binary strings shows that the generation of cyclotomic leaders modulo $2^k - 1$ is nothing but the classical combinatorial problem of generation of necklaces with k beads of up to two different colors.

Definition 2.9.1 (Necklace, Lyndon word)**.** *Let k and n be two strictly positive integers.*

A k-ary necklace of length n, also called a necklace of n beads in k colors, is a string of length n on an alphabet of size k, up to rotation.

An aperiodic necklace is called a Lyndon word.

The usual representative of a necklace is its smallest element for lexicographic order. We identify equivalence classes and such elements.

An efficient iterative algorithm for the generation of necklaces has been given in the works of Fredricksen and Maiorana [100] and Fredricksen and Kessler [99]. A slight variation of it was proposed independently by Duval [77]. These algorithms have been respectively analyzed by Ruskey, Savage and Wang [225] and Berstel and Pocchiola [14]. An overview of this problem and a recursive version of the original algorithm can also be found in the monograph of Ruskey [224, Subsection 7.2]. Algorithm 2.2 describes a slight variation of the building block of the iterative version as it can be found in Ruskey's monograph [224, Algorithm 7.2]. It takes as input *any* string and returns the smallest necklace strictly greater than it, together with the largest length such that a prefix of the necklace is a Lyndon word.

Algorithm 2.2: Iterative generation of necklaces

Input: A string *word* of length n on the alphabet $\{0, \dots, k-1\}$
Output: The smallest necklace strictly greater than *word*

```
1  while True do
2      p = n
3      while word[p] == k-1 do
4          p -= p-1
5      if p == 0 then
6          return (∅, 0)
7      word[p] += 1
8      for i = 1 to n − p do
9          word[i+p] = word[i]
10     if n ≡ 0 (mod p) then
11         return (word, p)
12 return True
```

2.9.3 Implementation details

We implemented Algorithm 2.1 in C [148] using version 2.2 of the FLINT library [127] for polynomial and matrix arithmetic and version 1.5.4 of OpenMPI [106] to distribute computations. Our source code was compiled using version 4.6.1 of GCC [265]. Algorithm 2.2 was used to build the numbers to test. It is indeed particularly convenient to use that variation of the classical algorithms to distribute computations among different processes. Moreover, the knowledge of the largest length such that a prefix of a necklace is a Lyndon word allows to reduce the number of operations for periodic necklaces: the matrix corresponding to the Lyndon word is computed and then exponentiated to obtain the matrix corresponding to the necklace. Finally, the matrices powers B^i and C^i for $1 \leq i \leq k-1$ should be precomputed before looping over the necklaces. Furthermore, an easy induction shows that these matrices can be written as

$$B^i = \begin{pmatrix} 1 & P_i(x) & 1 & P_i(x) \\ 0 & 2^{i-1}x^i & 0 & 2^{i-1}x^i \\ 0 & 2^{i-1}x^i & 0 & 2^{i-1}x^i \\ 0 & 2^{i-1}x^i & 0 & 2^{i-1}x^i \end{pmatrix}, \; C^i = \begin{pmatrix} 2^{i-1} & 0 & 2^{i-1} & 0 \\ 2^{i-1} & 0 & 2^{i-1} & 0 \\ 2^{i-1} & 0 & 2^{i-1} & 0 \\ Q_i(x) & x^i & Q_i(x) & x^i \end{pmatrix},$$

where $P_i(x) = \sum_{j=0}^{i-2} 2^j x^{j+1}$ and $Q_i(x) = \sum_{j=0}^{i-2} 2^{i-2-j} x^{j+1}$.

Tu and Deng were able to check the original conjecture (Conjecture 1.2.2) for $k \leq 29$ in about fifteen days on a PC with a Pentium4 CPU cadenced at 3.2 GHz and 256 Mb of RAM [264, Appendix]. Using our implementation, we were able to check the conjecture for $k = 39$ in about twelve hours and fifteen minutes on a pool of about four hundred quite recent cores and for $k = 40$ on a subset of them. More details on the computers used are given in Tables 2.5 and 2.6. Some timings are given in Table 2.7. The complete source code of our implementation is available at the following address: `http://www.infres.enst.fr/~flori/`.

Table 2.5: Computers' description — Part I

ID	CPU	Clock rate	Cores	Number
A	Dual-Core AMD Opteron(tm) Processor 1222	3 GHz	2	20
B	Intel(R) Core(TM)2 Quad CPU Q9400	2.66 GHz	4	20
C	Intel(R) Xeon(R) CPU W3520	2.67 GHz	8	17
D	Intel(R) Core(TM)2 Duo CPU E8600	3.33 GHz	2	23
E	Intel(R) Core(TM)2 Duo CPU E8500	3.16 GHz	2	33
F	Intel(R) Xeon(R) CPU E5540	2.53 GHz	16	1
G	Intel(R) Xeon(R) CPU X5690	3.47 GHz	24	1
H	Intel(R) Core(TM)2 Quad CPU Q6600	2.40 GHz	4	1

Table 2.6: Computers' description — Part II

ID	Distribution	Linux version
A	Debian 6.0.2	`2.6.32-5-amd64`
B	Debian 6.0.2	`2.6.32-5-amd64`
C	Debian 6.0.2	`2.6.32-5-amd64`
D	Debian 6.0.2	`2.6.32-5-amd64`
E	Fedora release 15 (Lovelock)	`2.6.40.4-5.fc15.x86_64`
F	Scientific Linux CERN SLC release 6.1 beta (Carbon)	`2.6.32-71.29.1.el6.x86_64`
G	CentOS Linux release 6.0 (Final)	`2.6.32-71.29.1.el6.centos.plus.x86_64`
H	Debian wheezy/sid	`3.0.0-1-amd64`

Table 2.7: Timings for checking the Tu–Deng conjecture

	Single core implementation				OpenMPI implementation			
k	ID	Time	ID	Time	ID	Time	ID	Time
20	H	12.67	G	6.90	all A-G	0.09	all E-G + H	0.23
21	H	26.56	G	14.46	all A-G	0.15	all E-G + H	0.45
22	H	55.39	G	30.28	all A-G	0.25	all E-G + H	0.82
23	H	114.96	G	63.09	all A-G	0.57	all E-G + H	1.85
24	H	238.46	G	131.17	all A-G	1.19	all E-G + H	3.99
25	H	495.90	G	272.67	all A-G	2.38	all E-G + H	8.59
26	H	1029.27	G	565.70	all A-G	5.16	all E-G + H	13.83
27	H	2130.63	G	1174.62	all A-G	11.07	all E-G + H	29.48
28	H	4402.22	G	2424.61	all A-G	23.83	all E-G + H	56.14
29	H	9064.92	G	5002.24	all A-G	51.13	all E-G + H	119.46
30	H	18645.16	G	10267.57	all A-G	105.37	all E-G + H	240.50
31	H	38453.96	G	21213.71	all A-G	220.15	all E-G + H	511.01
32	H	78641.68	G	43644.63	all A-G	316.33	all E-G + H	1087.67
33	H	160919.01	G	89801.69	all A-G	670.45	all E-G + H	2253.70
34	H	330238.97	G	184389.28	all A-G	1408.06	all E-G + H	4715.58
35	H	671319.77	G	377472.75	all A-G	3257.02	all E-G + H	9904.41
36	H	1340319.02	G		all A-G	5842.03	all E-G + H	20105.01
37	H		G		all A-G	11797.79	all E-G + H	40665.68
38	H		G		all A-G	23729.21	all E-G + H	81862.20
39	H		G		all A-G	47553.29	all E-G + H	161199.96
40	H		G		all A-G		all E-G + H	323197.65

Part II

Bent functions and point counting on algebraic curves

Chapter 3

Bent functions and algebraic curves

> Je n'ai jamais été aſſez loin pour bien ſentir l'application de l'algebre à la géométrie. Je n'aimois point cette manière d'opérer ſans voir ce qu'on fait ; & il me ſembloit que réſoudre un problême de géométrie par les équations, c'étoit jouer un air en tournant une manivelle. La premiere fois que je trouvai par le calcul que le quarré d'un binome étoit compoſé du quarré de chacune de ſes parties & du double produit de l'une par l'autre, malgré la juſteſſe de ma multiplication, je n'en voulus rien croire juſqu'à ce que j'euſſe fait la figure. Ce n'étoit pas que je n'euſſe un grand goût pour l'algebre en n'y conſidérant que la quantité abſtraite ; mais appliquée à l'étendue je voulois voir l'opération ſur les lignes, autrement je n'y comprenois plus rien.
>
> *Les Confeſſions*
> Jean-Jacques Rousseau [223]

Contents

In Chapter 1 we emphasized the fact that a cryptographic Boolean function should verify several contradictory properties. Constructing satisfying functions is therefore a difficult task, and trade-offs between the different criteria have to be made. In the present part, our approach will be slightly different: we solely focus on one criterion — non-linearity — and more precisely on functions achieving maximum non-linearity: *bent* functions. Recall that the significance of this aspect has again been demonstrated by the recent development of linear cryptanalysis initiated by Matsui [189, 188]. It is therefore especially important when Boolean functions are used as part of S-boxes in symmetric cryptosystems.

Bent functions were introduced by Rothaus [222] in 1976. They turned out to be rather complicated combinatorial objects and a concrete description of all bent functions is elusive. The class of bent functions contains a subclass of functions introduced by Youssef and Gong [285] in 2001: the so-called hyper-bent functions. In fact, the first definition of hyper-bent functions was based on a property of the extended Walsh–Hadamard transform of Boolean functions introduced by Golomb and Gong [118]. Golomb and Gong proposed that S-boxes should not be approximated by a bijective monomial, providing a new criterion for S-box design. The classification of (hyper-)bent functions and many related problems remain open. In particular, it seems difficult to define precisely an infinite class of hyper-bent functions, as indicated by the number of open problems proposed by Charpin and Gong [46].

The purpose of this chapter is to provide the mathematical background needed in Chapter 4 where actual characterizations of such functions and efficient algorithms to generate them will be presented. In Section 3.1, an alternative representation of Boolean functions is introduced, namely the polynomial form, as well as exponential sums and polynomials classically related to it. It is indeed under that form that (hyper-)bent functions will be characterized in Chapter 4. Section 3.2 covers a completely different and at first sight unrelated topic: (hyper)elliptic curves with an emphasis on point counting and efficient algorithms addressing this problem. The main point that we need in Chapter 4 is that it is possible to count points on such curves in a very efficient manner. This introduction can also serve the reader who is not acquainted with the theory of algebraic curves and abelian varieties as an introduction to Part III. Therefore, Section 3.2 can also be seen as the beginning of the transition towards Part III which will definitely depart from the study of Boolean functions and dive into that of abelian varieties with complex multiplication.

3.1 Bent functions

3.1.1 Boolean functions in polynomial form

Let n be a positive integer. Recall that a Boolean function f in n variables is an $\mathbb{F}_2$-valued function on $\mathbb{F}_2^n$. The field $\mathbb{F}_{2^n}$ is (non-canonically) isomorphic to the vector space $\mathbb{F}_2^n$, so that a Boolean function can also be seen as a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Recall also that the Hamming weight of f, denoted by $\mathrm{w_H}(f)$, is the Hamming weight of the image vector of f, that is the cardinality of its support $\mathrm{supp}(f) = \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

We now define another classical representation of Boolean functions involving the *trace function* from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$.

Definition 3.1.1 (Field trace)**.** *For any positive integer k, and r dividing k, the trace function*

from $\mathbb{F}_{2^k}$ *to* $\mathbb{F}_{2^r}$ *is denoted by* Tr_r^k. *It can be defined as*[1]

$$\mathrm{Tr}_r^k(x) = \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}} \quad .$$

In particular, we denote the absolute trace *over* $\mathbb{F}_2$ *of an element* $x \in \mathbb{F}_{2^n}$ *by* $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

Proposition 3.1.2 (Polynomial form [38, 2.1])**.** *Every non-zero Boolean function* $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ *in* n *variables has a unique trace expansion of the form*

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^{o(j)}\left(a_j x^j\right) + \epsilon(1 + x^{2^n-1}), \quad a_j \in \mathbb{F}_{2^{o(j)}} \quad ,$$

called its polynomial form, where Γ_n *is the set of integers obtained by choosing one element in each cyclotomic coset modulo* $2^n - 1$ *(including the trivial coset containing* 0*),* $o(j)$ *is the size of the cyclotomic coset containing* j*, and* $\epsilon = \mathrm{w_H}(f)$ *modulo* 2.

The most usual choice for the coset elements is the smallest element in each cyclotomic coset, called the coset leader.

Recall that, given an integer $0 \leq j \leq 2^n - 1$ having the binary expansion $j = \sum_{i=0}^{n-1} j_i 2^i$, $j_i \in \{0, 1\}$, the Hamming or binary weight of j, denoted by $\mathrm{w_H}(j)$, is $\#\{0 \leq i \leq n-1 \mid j_i = 1\}$. The algebraic degree of f is then equal to the maximum weight of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$.

The hard problem we will try to tackle in Chapter 4 is to give efficient characterizations of bentness using the polynomial form, i.e. necessary and sufficient conditions on the coefficients a_r for the corresponding function to be bent.

3.1.2 Walsh–Hadamard transform

In this subsection we give another characterization of bentness and definitions of stronger properties.

Definition 3.1.3 (Sign function)**.** *Let* f *be a Boolean function on* $\mathbb{F}_{2^n}$. *Its* sign function *is the integer-valued function* $\chi(f) = \chi_f = (-1)^f$.

Definition 3.1.4 (Walsh–Hadamard transform)**.** *Let* f *be a Boolean function on* $\mathbb{F}_{2^n}$. *The* Walsh–Hadamard transform *of* f *is the discrete Fourier transform of* χ_f*, whose value at* $\omega \in \mathbb{F}_{2^n}$ *is defined as*

$$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(\omega x)} \quad .$$

Recall that *bent* functions are functions with maximum non-linearity. They only exist for even number of inputs and can be equivalently defined as follows.

Definition 3.1.5 (Bentness)**.** *A Boolean function* $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ *is said to be bent if* $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}$, *for all* $\omega \in \mathbb{F}_{2^n}$.

Hyper-bent functions have even stronger properties than bent functions. More precisely, hyper-bent functions can be defined as follows.

[1] This is the usual field trace. For an element $x \in \mathbb{F}_{2^k}$, it can be defined as the (linear algebra) trace of the endomorphism of multiplication by x where $\mathbb{F}_{2^k}$ is seen as a vector space over $\mathbb{F}_{2^r}$. Using Galois theory, this can also be defined as the sum of the conjugates of x in the Galois extension field $\mathbb{F}_{2^k}$ over $\mathbb{F}_{2^r}$.

Definition 3.1.6 (Hyper-bentness). *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be hyper-bent if the function $x \mapsto f(x^i)$ is bent, for every integer i co-prime to $2^n - 1$.*

Semi-bent functions exist for even or odd number of inputs. We will only be interested in even number of inputs where they can be defined as follows.

Definition 3.1.7 (Semi-bentness). *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be semi-bent if $\widehat{\chi_f}(\omega) \in \left\{0, \pm 2^{\frac{n+2}{2}}\right\}$, for all $\omega \in \mathbb{F}_{2^n}$.*

Hence, the Walsh–Hadamard transform provides a basic characterization of (hyper-)bentness. However, it can definitely not be used in practice to test efficiently bentness of a given function, especially if all its values are computed naively one at a time as exponential sums. Nevertheless, it should be noted that all the values of the Walsh–Hadamard transform can be computed *at once* using the so-called fast Walsh–Hadamard transform, a kind of Fast Fourier Transform. The complexity of the fast Walsh–Hadamard transform is $O(2^n n^2)$ bit operations and $O(2^n n)$ memory [8].

3.1.3 Binary exponential sums

The first satisfactory characterizations we will describe in Chapter 4 involve Kloosterman sums. The classical binary *Kloosterman sums* on $\mathbb{F}_{2^n}$ are defined as follows.

Definition 3.1.8 (Kloosterman sums). *The binary Kloosterman sums on $\mathbb{F}_{2^n}$ are*

$$K_n(a) = 1 + \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(ax + \frac{1}{x}\right)}, \quad a \in \mathbb{F}_{2^n} \ .$$

It is an elementary fact that $K_n(a) = K_n(a^2)$:

$$\begin{aligned} K_n(a) &= 1 + \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(ax + \frac{1}{x}\right)} = 1 + \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(a^2x^2 + \frac{1}{x^2}\right)} \\ &= 1 + \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(a^2x + \frac{1}{x}\right)} = K_n(a^2) \ . \end{aligned}$$

Some characterizations will also involve the *cubic sums* which are defined as follows.

Definition 3.1.9 (Cubic sums). *The cubic sums on $\mathbb{F}_{2^n}$ are*

$$C_n(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(ax^3 + bx\right)}, \quad a, b \in \mathbb{F}_{2^n} \ .$$

In particular, such exponential sums can be seen as the Walsh–Hadamard transforms of simple functions:

- The function $a \mapsto K_n(a)$ is the Walsh–Hadamard transform of the inverse function (we define $1/0 = 0$ or $1/x$ as x^{2^n-2} for all $x \in \mathbb{F}_{2^n}$).
- The function $b \mapsto C_n(a, b)$ is the Walsh–Hadamard transform of the cube function times a defined as $x \mapsto ax^3$.

All the values of those sums can then be computed at once using a fast Walsh–Hadamard transform. However, such an approach does not answer the problem of computing efficiently one, and only one, such exponential sum.

3.1.4 Dickson polynomials

Finally, the last classical objects we will need are the so-called *Dickson polynomials.*

Definition 3.1.10 (Binary Dickson polynomials [179])**.** *The family of binary Dickson polynomials (of the first kind) $D_r(X) \in \mathbb{F}_2[X]$ of degree r is defined by*

$$D_r(X) = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor} \frac{r}{r-i} \binom{r-i}{i} X^{r-2i}, \quad r \geq 2 \ .$$

Moreover, the family of Dickson polynomials $D_r(X)$ can also be defined by the recurrence relation

$$D_{i+2}(X) = XD_{i+1}(X) + D_i(X) \ ,$$

with initial values

$$D_0(X) = 0, \quad D_1(X) = X \ .$$

We refer the reader to the monograph of Lidl, Mullen and Turnwald [179] for many useful properties and applications of Dickson polynomials. Here is the list of the first six binary Dickson polynomials:

$$D_0(X) = 0,\ D_1(X) = X,\ D_2(X) = X^2 \ ,$$
$$D_3(X) = X + X^3,\ D_4(X) = X^4,\ D_5(X) = X + X^3 + X^5 \ .$$

3.2 Algebraic curves

3.2.1 Elliptic curves over perfect fields

Classical treatment of the theory of elliptic curves can be found for example in the textbooks of Silverman [246], Husemöller [138], Cassels [44], Washington [279] or Knapp [152]. A more cryptographic oriented point of view, and especially special treatment for even characteristic, can be found for example in the works of Koblitz [154, 155] or in several more recent textbooks [82, 18, 56, 107]

Let K be a perfect field[2]. An *elliptic curve* can be defined abstractly as follows.

Definition 3.2.1 (Elliptic curve)**.** *An elliptic curve E is a smooth projective algebraic curve[3] of genus[4] one with a rational point.*

In more down-to-earth terms, such a curve can be described by a *Weierstraß equation* [244, Section III.1]

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ ,$$

giving its affine part. There is an additional point at infinity O_E which can be seen as the only non-affine solution to the homogenized Weierstraß equation. With such an equation is associated

[2] A field is said to be perfect if every algebraic extension is separable, i.e. if every irreducible polynomial splits as a product of distinct linear factors over an algebraic closure. In particular, fields of characteristic zero and finite fields are perfect.

[3] Rigor would lead us to define now what a smooth projective algebraic curve is. Unfortunately, it would take us too far afield to define formally all these notions in a satisfactory way. Therefore, for the conciseness of exposition and because it is enough to think of such an object as "what a curve should be", we will not formally define them here. Anyhow, a concrete description of such an object is given below and more details about algebraic curves and elliptic curves will be given in Chapter 5.

[4] The remark of Footnote 3 applies here as well.

a quantity called its discriminant[5]In fact, a Weierstraß equation describes the affine part of a smooth, or non-singular, projective curve — which is then an elliptic curve — if and only if its discriminant is non-zero [244, Proposition III.1.4]. The affine parts of such curves defined over the real numbers, with discriminants zero and non-zero, are depicted in Figures 3.1, 3.2, 3.3, 3.4, and 3.5.

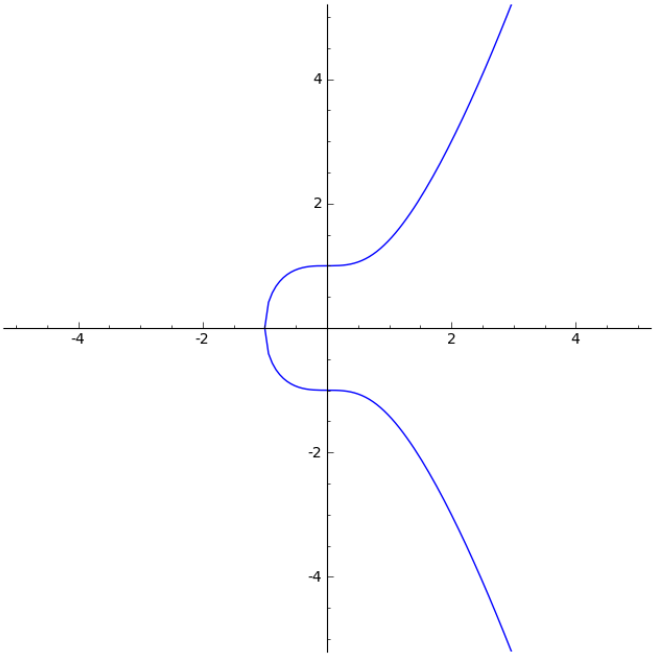


Figure 3.1: The elliptic curve $E: \ y^2 = x^3 + 1$, $\Delta = -432$

Over an algebraically closed field, elliptic curves are classified up to isomorphism by the j-invariant, which can be defined as a rational function of the coefficients of the curve[6] [244, Proposition III.1.4]. Furthermore, for any j_0 in $\overline{K}$, the algebraic closure of K, there is a curve defined over $K(j_0)$ with j-invariant j_0 [244, Proposition III.1.4].

For a given extension L of K, a point is said to be rational if its coordinates lie in L (and not in a larger extension). There is a composition law, usually additively denoted, on the set of rational points giving it a group structure [244, Section III.2]. It can be explicitly described by the so-called "chord-and-tangent" law and is depicted in Figure 3.6. The point at infinity O_E is the neutral element for the addition law. Multiplication by an integer n on E, that we denote by $[n]$, can then be naturally defined.

The following result shows that any rational map between curves is the composition of a translation and a homomorphism.

Definition 3.2.2 (Isogeny)**.** *Let E_1 and E_2 be two elliptic curves defined over K and ϕ a morphism between them. We say that ϕ is an isogeny if $\phi(O_{E_1}) = O_{E_2}$.*

[5]The expression of the discriminant using the coefficients a_1, a_3, a_2, a_4 and a_6 is quite complicated and we will not give it here. A simpler expression exists in characteristic different from 2 and 3 and is given in Definition 5.2.1.

[6]The expression of the j-invariant using the coefficients a_1, a_3, a_2, a_4 and a_6 is also quite complicated and will not be given here. A simpler expression exists as well in characteristic different from 2 and 3 and is given in Definition 5.2.2.

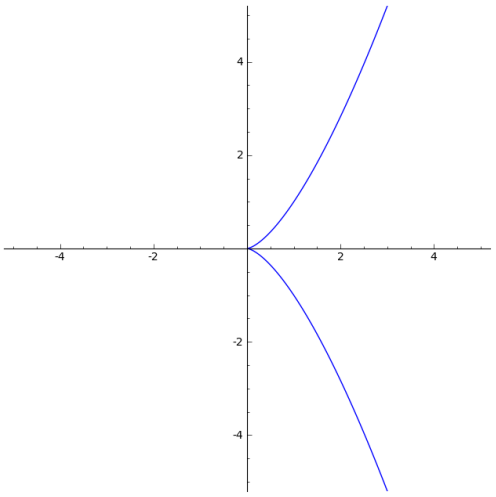


Figure 3.2: The singular curve $E: y^2 = x^3$, $\Delta = 0$

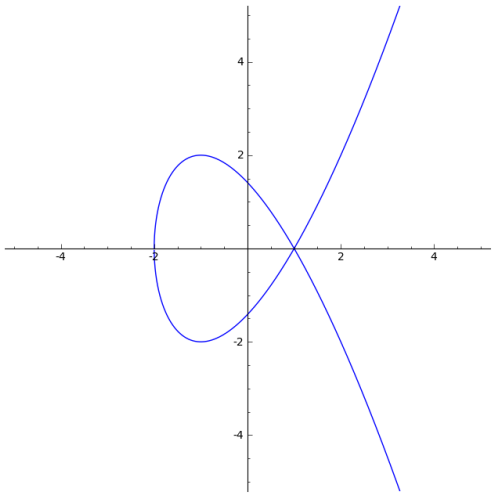


Figure 3.3: The singular curve $E: y^2 = x^3 - 3x + 2$, $\Delta = 0$

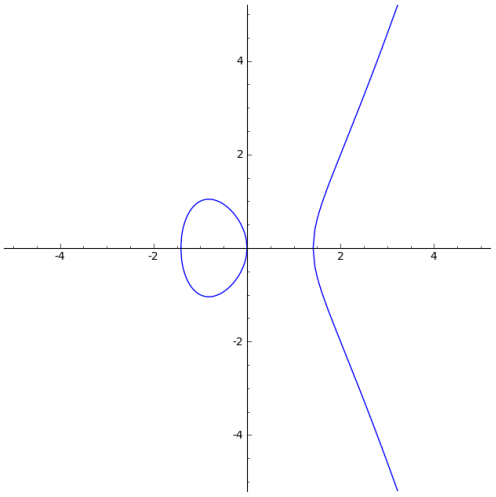


Figure 3.4: The elliptic curve $E: y^2 = x^3 - 2x$, $\Delta = 512$

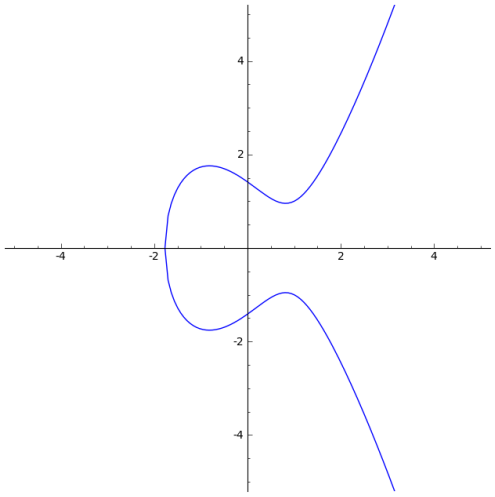


Figure 3.5: The elliptic curve $E: y^2 = x^3 - 2x + 2$, $\Delta = -1216$

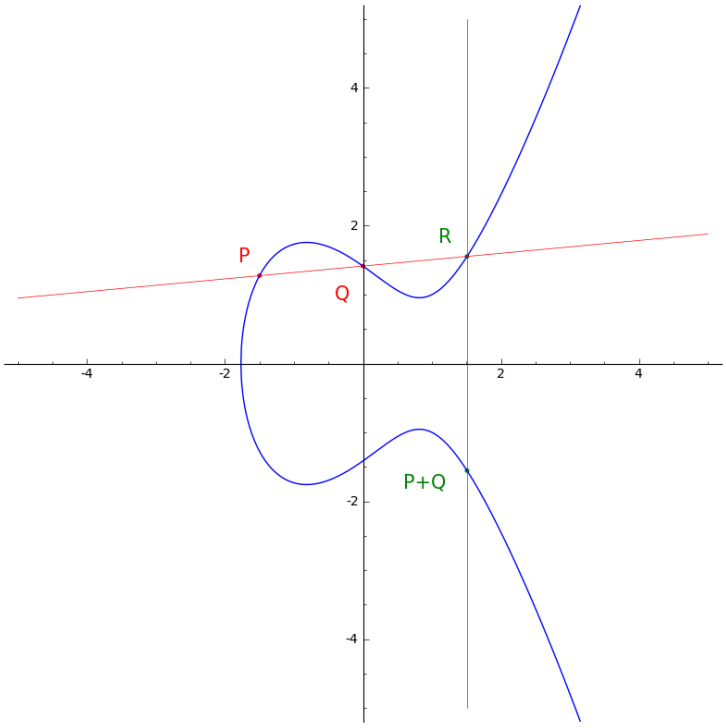


Figure 3.6: Addition law on the elliptic curve $E: \ y^2 = x^3 + 1$

Proposition 3.2.3 ([244, Theorem III.4.8]). *Let E_1 and E_2 be two elliptic curves defined over K and ϕ a map between them. If ϕ is an isogeny, then ϕ is a homomorphism.*

We denote by $\mathrm{End}_K(E)$ the ring of rational endomorphisms (i.e. homomorphisms or equivalently isogenies from E to itself) and by $\mathrm{End}(E) = \mathrm{End}_{\overline{K}}(E)$ the ring of endomorphisms of E over the algebraic closure $\overline{K}$ of K. It is possible to define the degree [244, Section II.2] and the trace [244, Proposition III.8.6] of such maps. Before stating the theorem giving the structure of $\mathrm{End}_K(E)$, we need different definitions.

Definition 3.2.4 (Order [244, Section III.9]). *Let K be a $\mathbb{Q}$-algebra finitely generated over $\mathbb{Q}$. An* order *$\mathcal{O}$ in K is a subring of K which is finitely generated and such that*[7] *$\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = K$.*

In a number field K of degree $[K : \mathbb{Q}] = n$, an order $\mathcal{O}$ is a subring which is also a lattice, i.e. a $\mathbb{Z}$-module of rank n[8].

Definition 3.2.5 (Definite quaternion algebra [244, Section III.9]). *A* definite quaternion algebra *K over $\mathbb{Q}$ is an algebra of the form*

$$K = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta \ ,$$

whose multiplication satisfies

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2, \beta^2 < 0, \quad \alpha\beta = -\beta\alpha \ .$$

Theorem 3.2.6 ([244, Corollary III.9.4]). *The endomorphism ring of an elliptic curve E over K is one of the three following objects:*

1. *the ring of natural integers $\mathbb{Z}$;*
2. *an order in an imaginary quadratic number field*[9]*;*
3. *a maximal order in a definite quaternion algebra.*

Moreover, if $\mathrm{char}(K) = 0$*, then only the first two are possible.*

In particular, $\mathrm{End}(E)$ is torsion-free. If $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, then the curve is said to have complex multiplication[10].

The group of rational points of E over an extension L of K (i.e. points with coordinates in L) is denoted by $E(L)$. For an integer n, we denote by $E[n]$ the n-torsion subgroup of the points of E over $\overline{K}$, i.e.

$$E[n] = \left\{P \in E(\overline{K}) \mid [n]P = O_E\right\} \ .$$

The subgroup of rational points of n-torsion is denoted by $E[n](K) = E[n] \cap E(K)$. The following classical result gives the structure of the groups of torsion points.

Proposition 3.2.7 ([244, Corollary III.6.4]). *Let n be a positive integer and p the characteristic of K. Then:*

- *If $p \neq 0$ and $p \nmid n$, then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*
- *One of the following is true: $E[p^e] \simeq \{0\}$ for all $e \geq 1$ or $E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$ for all $e \geq 1$.*

It can also be shown that a point of E is of n-torsion if and only if its coordinates are roots of a bivariate polynomial called the n-division polynomial of E [18, Section III.4]. In fact, one can even choose a univariate polynomial in the x-coordinate and we denote that polynomial by f_n.

[7] The operator $\otimes_{\mathbb{Z}}$ denotes a tensor product of $\mathbb{Z}$-modules.

[8] More details about such *orders* will be given in Chapters 5 and6.

[9] An imaginary quadratic number field is a number field of degree 2 whose complex embeddings are complex, i.e. their images are not included in the real numbers $\mathbb{R}$.

[10] This definition is only valid in dimension 1. For general abelian varieties, the "right" definition is given in Chapter 6.

3.2.2 Elliptic curves over finite fields

We now focus on elliptic curves defined over finite fields. Let m be a positive integer, $\mathbb{F}_q$ the finite field of characteristic p with $q = p^m$ elements and $\overline{\mathbb{F}}_q$ its algebraic closure.

The group of rational points of E over an extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ (i.e. points with coordinates in $\mathbb{F}_{q^k}$) is denoted by $E(\mathbb{F}_{q^k})$; the number of points of this group by $\#E(\mathbb{F}_{q^k})$. When the context is clear, we denote $\#E(\mathbb{F}_q)$ simply by $\#E$.

Definition 3.2.8 (Frobenius endomorphism)**.** *Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ of characteristic p. Then the q-th power map is an endomorphism of E called the q-th* Frobenius endomorphism *of the curve.*

It is a classical result that $\#E = q + 1 - t$ where t is the trace of the Frobenius endomorphism of E over $\mathbb{F}_q$ and the following theorem has been shown by Hasse.

Theorem 3.2.9 ([244, Theorem V.2.3.1])**.** *Let t be the trace of the Frobenius endomorphism of an elliptic curve defined over $\mathbb{F}_q$, then*

$$|t| \leq 2\sqrt{q} \ .$$

Here we will be interested in *ordinary* elliptic curves which can be defined as follows.

Definition 3.2.10 (Ordinary elliptic curve [244, Theorem V.3.1])**.** *Let E be an elliptic curve defined over $\mathbb{F}_q$ of characteristic p and t the trace of the Frobenius endomorphism of E. We say that E is ordinary if it verifies one of the following equivalent properties:*

- $p \nmid t$*;*
- $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$*;*
- $\mathrm{End}(E)$ *is an order in an imaginary quadratic extension of* $\mathbb{Q}$*.*

If E is not ordinary, we say it is *supersingular*.

Finally, using classical results of Deuring [68] and Waterhouse [280], the number of ordinary elliptic curves (up to isomorphism) with a given trace t of the Frobenius endomorphism (or equivalently a number of points $q + 1 - t$), verifying $|t| \leq 2\sqrt{q}$ and $p \nmid t$, can be computed as follows[11]. The conditions on t indeed imply that $\mathrm{End}(E)$ must be an order $\mathcal{O}$ in $K = \mathbb{Q}[\alpha]$ and contains the order $\mathbb{Z}[\alpha]$ of discriminant Δ where $\alpha = \frac{t+\sqrt{\Delta}}{2}$ and $\Delta = t^2 - 4q$. We denote by $H(\Delta)$ the *Kronecker class number* [232, 61]

$$H(\Delta) = \sum_{\mathbb{Z}[\alpha] \subset \mathcal{O} \subset K} h(\mathcal{O}) \ ,$$

where the sum is taken over all the orders $\mathcal{O}$ in K containing $\mathbb{Z}[\alpha]$ and $h(\mathcal{O})$ is the classical class number.

Proposition 3.2.11 ([232, 144, 61])**.** *Let t be an integer such that $|t| \leq 2\sqrt{q}$ and $p \nmid t$. The number $N(t)$ of elliptic curves over $\mathbb{F}_q$ with $q + 1 - t$ rational points is given by*

$$N(t) = H(\Delta) \ ,$$

where $\Delta = t^2 - 4q$.

[11] See Chapter 5 for details.

It should be noted that $H(\Delta)$ can be computed from the value of the classical class number of (the maximal order of) K using the following proposition.

Theorem 3.2.12 ([160, 61, 144, 54])**.** *Let $\mathcal{O}$ be the order of* conductor *f in K[12], an imaginary quadratic extension of $\mathbb{Q}$, $\mathcal{O}_K$ the maximal order of K and Δ_K the discriminant of (the maximal order of) K. Then*

$$h(\mathcal{O}) = \frac{f h(\mathcal{O}_K)}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right) \ ,$$

where $\left(\frac{\cdot}{p}\right)$ is the Kronecker symbol.

Denoting the conductor of $\mathbb{Z}[\alpha]$ by f, $H(\Delta)$ can then be written as

$$H(\Delta) = h(\mathcal{O}_K) \sum_{d|f} \frac{d}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|d} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right) \ .$$

We now give specific results to even characteristic. First, E is supersingular if and only if its j-invariant is 0. Second, if E is ordinary, then its Weierstraß equation can be chosen to be of the form

$$E: \ y^2 + xy = x^3 + bx^2 + a \ ,$$

where $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, its j-invariant is then $1/a$; moreover, its first division polynomials are given by [154, 18]

$$f_1(x) = 1, \quad f_2(x) = x, \quad f_3(x) = x^4 + x^3 + a, \quad f_4(x) = x^6 + ax^2 \ .$$

The quadratic twist of E is an elliptic curve with the same j-invariant as E, so isomorphic over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, but not over $\mathbb{F}_q$ (in fact it becomes so over $\mathbb{F}_{q^2}$). It is unique up to rational isomorphism and we denote it by $\widetilde{E}$. It is given by the Weierstraß equation

$$\widetilde{E}: \ y^2 + xy = x^3 + \widetilde{b}x^2 + a \ ,$$

where $\widetilde{b}$ is any element of $\mathbb{F}_q$ such that $\mathrm{Tr}_1^m\left(\widetilde{b}\right) = 1 - \mathrm{Tr}_1^m(b)$ [82]. The trace of its Frobenius endomorphism is given by the opposite of the trace of the Frobenius endomorphism of E, so that their number of rational points are closely related [82, 18]:

$$\#E + \#\widetilde{E} = 2q + 2 \ .$$

3.2.3 Hyperelliptic curves

The theory of hyperelliptic curves, with a cryptographic point of view, can be found for example in the classical treatments of Menezes and different coauthors [141, 194] or more recent textbooks [110, 56, 107]. We can define a *hyperelliptic curve* rather generally and abstractly as follows.

Definition 3.2.13 (Hyperelliptic curve)**.** *A hyperelliptic curve H is a smooth projective algebraic curve which is a degree 2 covering*[13] *of the projective line.*

[12] The study of orders in imaginary quadratic field is conducted in Subsection 5.2.2. The definition of the *conductor* is given there in Proposition 5.2.17. For the impatient reader, it is sufficient to know that the order $\mathcal{O}$ of conductor f can be explicitly described as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ where O_K is the ring of integers of K.

[13] The remark of Footnote 3 applies here as well.

The genus of a hyperelliptic curve will be denoted by g. The above definition includes the elliptic curves, i.e. curves of genus 1, but it is sometimes understood that a hyperelliptic curve should be of genus $g \geq 2$, hence not an elliptic curve.

A description of the different normal forms for hyperelliptic curves in even characteristic can be found in the work of Enge [83]. For cryptographic applications, the curves are often chosen to be *imaginary* hyperelliptic curves. This is also the kind of curves we will encounter in Chapter 4. An imaginary hyperelliptic curve of genus g can be described by an affine part given by the following equation[14]:

$$H: \ y^2 + h(x)y = f(x) \ ,$$

where $h(x)$ is of degree less than or equal to g and $f(x)$ is monic of degree $2g+1$. In particular, its smooth projective model has only one point at infinity. Such a curve of genus 2 is depicted in Figure 3.7.

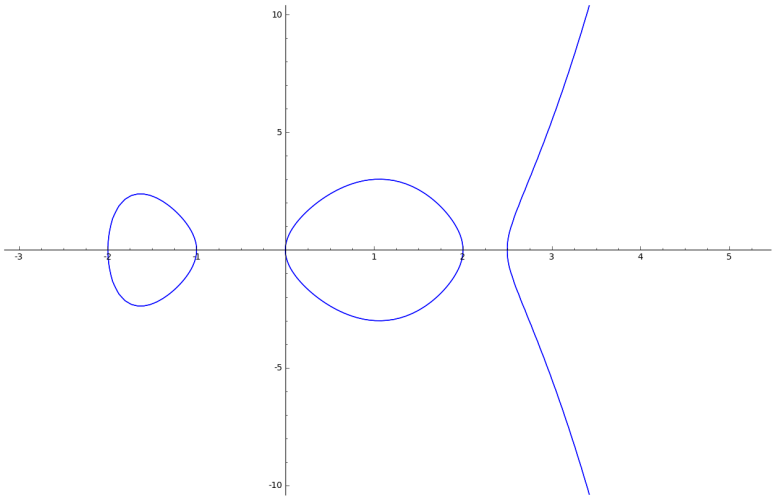


Figure 3.7: The hyperelliptic curve $H: \ y^2 = (x+2)(x+1)x(x-2)(x-5/2)$ of genus 2

We finally define an interesting subclass of hyperelliptic curves.

Definition 3.2.14 (Artin–Schreier curve)**.** *An* Artin–Schreier curve *is an imaginary hyperelliptic curve of genus g whose affine part is given by an equation of the form*

$$H: \ y^2 + x^k y = f(x) \ ,$$

where $0 \leq k \leq g$ and $f(x)$ is monic of degree $2g+1$.

3.2.4 Point counting

The main fact about elliptic and hyperelliptic curves defined over a finite field $\mathbb{F}_{q^m}$ that we will use in Chapter 4 is the existence of algorithms to compute their cardinalities in polynomial time and space in m. Moreover, those algorithms are quite efficient in small characteristic.

[14] Beware that the projective curve corresponding to the homogenization of the following equation will have a singularity at infinity as soon as $g \geq 2$. The hyperelliptic curve is therefore the desingularization of that curve. It is a fact that it also has one and only one point at infinity, and that its affine part is described by the same equation.

Let us begin our survey of such algorithms with the simplest case: elliptic curves. This is indeed the best mastered situation and there are several different algorithms to compute the cardinalities of such curves.

The most famous one is without any doubt the so-called SEA algorithm. It is named after Schoof [231] who developed in 1985 the first deterministic polynomial time algorithm for point counting, and Elkies and Atkin who subsequently proposed practical improvements [233, 81]. The overall idea of such *l-adic* algorithms is to compute the trace of the Frobenius endomorphism modulo small primes different from the characteristic of the field, and to gather this information back using the Chinese Remainder Theorem. Overviews of these algorithms, and in particular of additional practical improvements, are given in the theses of Müller [214] and Lercier [171]. These l-adic algorithms were subsequently extended to higher genera by Pila [220] and made practical, at least in genus 2, by Gaudry, Harley and Schost [111, 113].

In small characteristic, and especially in even characteristic that will be our principal interest in Chapter 4, more efficient algorithms have been developed. The first breakthrough is due to Satoh [228] who proposed in 1999 to compute the trace of the Frobenius endomorphism on a *canonical lift* of the curve over the p-adics for $p \geq 5$. This is the so-called canonical lift method. This method was extended to characteristic 2 and 3, and improved, by different authors [98, 247, 276, 200, 229, 150, 109, 172]. The main result we need relies on the AGM method described by Mestre [200] and has been given by Lercier and Lubicz [172] and further improved by Harley [126].

Theorem 3.2.15 ([126])**.** *Let E be an elliptic curve defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of E in $O(m^2(\log m)^2 \log\log m)$ time and $O(m^2)$ space.*

Mestre [201] extended the AGM method to higher genera and a quasi-quadratic algorithm was described by Lercier and Lubicz [173].

Theorem 3.2.16. *Let H be a hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of H in*

$$O(2^{4g+o(1)} g^3 m^{2+o(1)})$$

bit operations and $O(2^{3g+o(1)} m^2)$ memory.

It should be remarked that the complexity of this algorithm is exponential in the genus of the curve.

There also exist other efficient algorithms in small and medium characteristic computing the trace of the Frobenius endomorphism:

1. on Dwork cohomology groups [78] in the approach of Lauder and Wan [165, 163, 164];
2. on Monsky–Washnitzer cohomology groups [211, 208, 210, 209] in the approach initiated by Kedlaya [146, 147] and extended to even characteristic by Denef and Vercauteren [66, 67];
3. using deformation theory [79], for example in the work of Lauder [162] and Hubrechts [137, 136].

A complete description of many of the existing *p-adic* algorithms can be found in the theses of Vercauteren [275] and Hubrechts [135], or in different articles [274, 174]. Such algorithms have the advantage to extend naturally to higher genera in any characteristic.

We now state more precisely a result of Denef and Vercauteren [66, 67, 275] about hyperelliptic curves defined over a finite field of even characteristic.

Theorem 3.2.17 ([275, Theorem 4.4.1]). *Let H be an imaginary hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of H in*

$$O(g^3m^3(g^2 + \log^2 m \log\log m) \log gm \log\log gm)$$

bit operations and $O(g^4m^3)$ memory.

A slightly stronger result applies for Artin–Schreier curves.

Theorem 3.2.18 ([275, Theorem 4.3.1]). *Let H be an Artin–Schreier curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of H in*

$$O(g^3m^3(g^2 + \log^2 m \log\log m) \log gm \log\log gm)$$

bit operations and $O(g^3m^3)$ memory.

In particular, the complexities of these algorithms are polynomial in the genus of the curve.

Chapter 4

Efficient characterizations for bentness

> No constaba el nombre del heresiarca, pero sí la noticia de su doctrina, formulada en palabras casi idénticas a las repetidas por él, aunque — tal vez — literariamente inferiores. Él había recordado: *Copulation and mirrors are abominable*. El texto de la Enciclopedia decía: «Para uno de esos gnósticos, el visible universo era una ilusión o (más precisamente) un sofisma. Los espejos y la paternidad son abominables (*mirrors and fatherhood are abominable*) porque lo multiplican y lo divulgan».
>
> *Ficciones*
> Jorge Luis Borges [22]

Contents

As was already stated in the introduction to Chapter 3, characterizing (hyper-)bent functions is a difficult problem. Section 4.1 presents such characterizations for Boolean functions given in polynomial form: first for monomial functions by means of binary Kloosterman sums as originally introduced by Dillon [70] and later extended by various authors; second for functions with multiple trace terms using Dickson polynomials as presented by Charpin and Gong [46] and Mesnager [196]. Such results make a preliminary step towards efficient generation of (hyper-)bent functions: the computation of the full Walsh–Hadamard transform is typically replaced with that of only one or a finite number of exponential sums. However, computing such a sum in a naive manner still needs *exponential* time in the size of the finite field of definition.

Section 4.2 gives an elegant and efficient solution to this problem by using the classical connection between Kloosterman sums, or more generally specific exponential sums, and the number of points on (hyper)elliptic curves. These ideas go back to the works of Lachaud and Wolfmann [156] and Katz and Livné [144] in the late eighties, but the most of them was not made until quite recently and works such as those of Lisoněk [180, 182, 181]. In particular, it is shown in Section 4.2 how such results extend to the criteria proposed by Mesnager.

To actually generate an (hyper-)bent function in the monomial families, or equivalently to find binary Kloosterman sums with specific values, other criteria should be taken into account: being able to compute efficiently a Kloosterman sum is not sufficient. For example, divisibility properties of Kloosterman sums play an important role and some classical results about them are recalled in Section 4.3. As was pointed out by Lisoněk and Moisio [180, 183] among others, the connection between Kloosterman sums and elliptic curves provides once more simple and elegant proofs of such results.

To conclude this chapter we describe in Section 4.4 several algorithms which have been proposed to efficiently find zeros of Kloosterman sums, and so to generate (hyper-)bent functions, and are based on the above observations. We then show how they extend to the search for the value 4. As a byproduct of our implementation of such an algorithm, we present some experimental results on a difficult mathematical case previously studied by Mesnager about a characterization of hyper-bent functions using Kloosterman sums with value 4 in Section 4.5.

Part of the results presented in this chapter are joint work with Gérard Cohen and Sihem Mesnager [92, 93, 91].

4.1 Hyper-bentness characterizations

4.1.1 Monomial functions

A first explicit construction of monomial bent functions involving zeros of Kloosterman sums was given by Dillon [70] in 1974: those are the classical monomial functions with the Dillon exponent. We call it the *Dillon criterion*. That construction was further studied by several authors:

- Lachaud and Wolfmann [157] who actually proved that the family defined by Dillon is never empty;
- Leander [167] which refined the results of Dillon using a different point of view;
- Charpin and Gong [46] who extended the family of Dillon, implying in particular that the original functions were actually hyper-bent;
- and Mesnager [198] who characterized semi-bent functions with two or three trace terms[1] using a similar criterion;

[1] Hence, such functions are not monomials, but binomials or trinomials. However, the number of trace terms for these functions is fixed in a given family and is low, so we include them under the hood of monomials.

to cite only a few of them.

Hence, it has been shown that the zeros of binary Kloosterman sums lead to several families of bent, hyper-bent and semi-bent functions. We summarize the known results in Table 4.1 with the following conventions:

- A class of functions is given in terms of $a \in \mathbb{F}_{2^m}^*$, $b \in \mathbb{F}_4^*$, $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and r co-prime to 2^m+1; remember that $a \in \mathbb{F}_{2^m}^*$, but that the corresponding Boolean functions have $n = 2m$ inputs.
- Unless stated otherwise, the given conditions on a are necessary and sufficient for the Boolean functions to verify the given property.

Table 4.1: Families of hyper-bent and semi-bent functions for $K_m(a) = 0$

Class of functions	Property	Conditions	References
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$	hyper-bent	$K_m(a) = 0$	[70, 157, 167, 46]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$	semi-bent	$K_m(a) = 0$	[198]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$ $+ \mathrm{Tr}_1^n\left(x^{(2^m-1)\frac{1}{4}+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$, m odd	semi-bent	$K_m(a) = 0$	[198]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$ $+ \mathrm{Tr}_1^n\left(x^{(2^m-1)3+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$	semi-bent	$K_m(a) = 0$	[198]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$ $+ \mathrm{Tr}_1^n\left(x^{(2^m-1)\frac{1}{6}+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$, m even	semi-bent	$K_m(a) = 0$	[198]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(\alpha x^{2^m+1}\right)$ $+ \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{\nu-1}-1} x^{(2^m-1)\frac{i}{2^\nu}+1}\right)$; $\gcd(\nu, m) = 1$, $\alpha \in \mathbb{F}_{2^n}$, $\mathrm{Tr}_m^n(\alpha) = 1$	semi-bent	$K_m(a) = 0$	[198]

Quite surprisingly, all the aforementioned characterizations involve zeros of Kloosterman sums and it is only in 2009 that Mesnager [195] has shown that another value of such sums — the value 4 — also gives rise to bent, hyper-bent and semi-bent functions. We will call this criterion the *first Mesnager criterion*. Afterwards, other families[2] of (hyper-)bent functions and semi-bent functions were as well described by Mesnager [197, 198]. The known results about (hyper-)bent functions are summarized in Table 4.2, those about semi-bent functions in Table 4.3. The conventions are the same as for Table 4.1.

Such characterizations are obviously much more pleasant than the original definition involving the Walsh–Hadamard transform. This is also a first step towards an efficient way to explicitly build (hyper-)bent functions.

4.1.2 Functions with multiple trace terms

In fact, Charpin and Gong devised in the same article [46] a quite more general characterization of hyper-bentness for a large class of Boolean functions with multiple trace terms. In particular,

[2]The remark of Footnote 1 applies here as well

Table 4.2: Families of (hyper-)bent functions for $K_m(a) = 4$

Class of functions	Property	Conditions	References
$\mathrm{Tr}_1^n\left(a\zeta^i x^{3(2^m-1)}\right) + \mathrm{Tr}_1^2\left(\beta^j x^{\frac{2^n-1}{3}}\right)$; m odd and $m \not\equiv 3 \pmod 6$, β is a primitive element of $\mathbb{F}_4$, ζ is a generator of the cyclic group U of (2^m+1)-th roots of unity, $(i,j) \in \{0,1,2\}^2$	hyper-bent	$K_m(a) = 4$ and $\mathrm{Tr}_1^m\left(a^{1/3}\right) = 0$	[195]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; m odd	hyper-bent	$K_m(a) = 4$	[197]
$\mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; m even	bent	$K_m(a) = 4$ (necessary condition)	[197]

Table 4.3: Families of semi-bent functions for $K_m(a) = 4$

Class of functions	Property	Conditions	References
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$; m odd	semi-bent	$K_m(a) = 4$	[198]
$\mathrm{Tr}_1^n\left(ax^{3(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; m odd and $m \not\equiv 3 \pmod 6$	semi-bent	$K_m(a) = 4$	[198]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^n\left(x^{(2^m-1)\frac{1}{4}+1}\right)$; m odd	semi-bent	$K_m(a) = 4$	[198]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^n\left(x^{3(2^m-1)+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$, m odd	semi-bent	$K_m(a) = 4$	[198]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(\alpha x^{2^m+1}\right) + \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{\nu-1}-1} x^{(2^m-1)\frac{i}{2^\nu}+1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; $\gcd(\nu, m) = 1$, $\alpha \in \mathbb{F}_{2^n}$, $\mathrm{Tr}_m^n(\alpha) = 1$, m odd	semi-bent	$K_m(a) = 4$	[198]

that family includes the well-known monomial functions with the Dillon exponent as a special case. The characterization involves exponential sums and Dickson polynomials and is given below.

Theorem 4.1.1 (Charpin–Gong criterion [46]). *Let $n = 2m$ be an even integer. Let S be a set of representatives of the cyclotomic classes modulo $2^m + 1$ whose cosets have full size n. Let f_a be the function defined on $\mathbb{F}_{2^n}$ by $f_a(x) = \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r x^{r(2^m-1)}\right)$, where $R \subseteq S$ and $a_r \in \mathbb{F}_{2^m}^*$. Let g_a be the Boolean function defined on $\mathbb{F}_{2^m}$ by $g_a(x) = \sum_{r \in R} \mathrm{Tr}_1^m \left(a_r D_r(x)\right)$, where $D_r(x)$ is the Dickson polynomial of degree r. Then f_a is hyper-bent if and only if*

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_a(x)\right) = 2^m - 2\,\mathrm{w_H}(g_a) - 1 \ .$$

Finally, Mesnager [196] gave a similar characterization of hyper-bentness[3] for another large class of hyper-bent functions with multiple trace terms which do not belong to the family considered by Charpin and Gong [46]. We call it the *second Mesnager criterion* to avoid confusion with the first Mesnager criterion for binomial functions.

Theorem 4.1.2 (Second Mesnager criterion [196]). *Let $n = 2m$ be an even integer with m odd and S be a set of representatives of the cyclotomic classes modulo $2^m + 1$ whose cosets have full size n. Let $b \in \mathbb{F}_4^*$. Let $f_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by*

$$f_{a,b}(x) = \sum_{r \in R} \mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(b x^{\frac{2^n-1}{3}}\right) \ , \tag{4.1}$$

where $R \subseteq S$ and all the coefficients a_r are in $\mathbb{F}_{2^m}^*$. Let g_a be the related function defined on $\mathbb{F}_{2^m}$ by $g_a(x) = \sum_{r \in R} \mathrm{Tr}_1^m \left(a_r D_r(x)\right)$, where $D_r(x)$ is the Dickson polynomial of degree r. Then:

1. *$f_{a,b}$ is hyper-bent if and only if $f_{a,b}$ is bent.*
2. *If b is a primitive element of $\mathbb{F}_4$, then the three following assertions are equivalent:*
   - *(a) $f_{a,b}$ is hyper-bent;*
   - *(b) $\displaystyle\sum_{x \in \mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(D_3(x))\right) = -2$;*
   - *(c) $\displaystyle\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_a(D_3(x))\right) = 2^m - 2\,\mathrm{w_H}(g_a \circ D_3) + 3.$*
3. *$f_{a,1}$ is hyper-bent if and only if*

$$2 \sum_{x \in \mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(D_3(x))\right) - 3 \sum_{x \in \mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(x)\right) = 2 \ .$$

Once more, these criteria reduce the test of hyper-bentness from the computation of the full Walsh–Hadamard transform to that of a finite number of exponential sums.

[3] There was a typo in the theorem given in the original article [196] where the last term in the right hand side of Condition 2c reads 4 instead of 3. This is an unfortunate consequence of the fact that the summation set used in the statement of that condition within the theorem is $\mathbb{F}_{2^m}^*$ whereas it is $\mathbb{F}_{2^m}$ within the proof of the theorem.

4.2 Reformulation in terms of cardinalities of curves

4.2.1 Kloosterman sums and elliptic curves

The idea to connect Kloosterman sums and elliptic curves goes back to the works of Lachaud and Wolfmann [156], and Katz and Livné [144]. We recall a simple proof of their main result in a simpler and less general formulation here. Indeed, its generalizations which will be covered in the next subsection can be proved in a very similar manner.

Theorem 4.2.1 ([156, 144])**.** *Let $m \geq 3$ be any positive integer, $a \in \mathbb{F}_{2^m}^*$ and E_a the projective elliptic curve defined over $\mathbb{F}_{2^m}$ whose affine part is given by the equation*

$$E_a : \ y^2 + xy = x^3 + a \ .$$

Then

$$\#E_a = 2^m + K_m(a) \ .$$

Proof. Indeed

$$K_m(a) = 1 + \sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) \ ,$$

and

$$\begin{aligned}\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) &= \sum_{x \in \mathbb{F}_{2^m}^*} \left(1 - 2\,\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) \\ &= 2^m - 1 - 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1} + ax\right) = 1\right\} \\ &= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1} + ax\right) = 0\right\} \ .\end{aligned}$$

Using the additive version of Hilbert's Theorem 90, we get

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) = -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + t = x^{-1} + ax\right\} \ ,$$

and applying the substitution $t = t/x$ we get

$$\begin{aligned}\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) &= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ (t/x)^2 + (t/x) = x^{-1} + ax\right\} \\ &= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + xt = x + ax^3\right\} \ .\end{aligned}$$

We recognize the number of points of E_a minus the only point with x-coordinate $x = 0$ and the only point at infinity.

$$\begin{aligned}\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) &= -2^m + 1 + \#E_a - 2 \\ &= -2^m - 1 + \#E_a \ .\end{aligned}$$

□

Hence, the necessary and sufficient condition for hyper-bentness of the monomial functions with the Dillon exponent given in Table 4.2 can be reformulated as follows.

Proposition 4.2.2 (Reformulation of the Dillon criterion)**.** *The notation is as in Theorem 4.2.1. Moreover, let r be an integer such that $\gcd(r, 2^m + 1) = 1$ and f_a be the Boolean function with n inputs defined as $f_a(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$. Then f_a is hyper-bent if and only if*

$$\#E_a = 2^m \ .$$

The class of binomial functions described by Mesnager [197] can naturally be given such a treatment.

Proposition 4.2.3 (Reformulation of the first Mesnager criterion)**.** *The notation is as in Theorem 4.2.1. Suppose furthermore that m is odd and let r be an integer such that* $\gcd(r, 2^m+1) = 1$, *$b \in \mathbb{F}_4^*$ and $f_{a,b}$ be the Boolean function* $f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$. *Then $f_{a,b}$ is hyper-bent*[4] *if and only if*

$$\#E_a = 2^m + 4 \ .$$

The theory of elliptic curves is rich and quite well understood. It was subsequently used in different papers to efficiently find specific values of Kloosterman sums [180, 3], and so to build hyper-bent functions[5]. In particular, Theorem 3.2.15 shows that computing their cardinalities takes polynomial time and space in m and so is testing the hyper-bentness of such a Boolean function. This is much better than computing naively the exponential sums which would require an exponential number of operations.

4.2.2 Exponential sums and hyperelliptic curves

The characterizations of hyper-bentness given by Charpin and Gong (Theorem 4.1.1) and Mesnager (Theorem 4.1.2) can also be naturally reformulated in terms of cardinalities of hyperelliptic curves.

Lisoněk [182, 181] indeed generalized very recently this reformulation to the Charpin–Gong criterion for hyper-bentness of Boolean functions with multiple trace terms. His idea is that both sides of the equality can be reformulated in terms of cardinalities of hyperelliptic curves as in Theorem 4.2.1. We give detailed proofs because we will use similar results to reformulate the Mesnager condition.

Proposition 4.2.4. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function such that $f(0) = 0$, $g = \mathrm{Tr}_1^m(f)$ be its composition with the absolute trace and G_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by*

$$G_f : y^2 + y = f(x) \ .$$

Then

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi(g(x)) = -2^m - 1 + \#G_f \ .$$

Proof. The proof is similar as that of Theorem 4.2.1 and is summarized by the following equalities:

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{2^m}^*} \chi(g(x)) &= \sum_{x \in \mathbb{F}_{2^m}^*} (1 - 2g(x)) \\
&= 2^m - 1 - 2\#\{x \in \mathbb{F}_{2^m}^* \mid g(x) = 1\} \\
&= 2^m - 1 - 2\#\{x \in \mathbb{F}_{2^m} \mid g(x) = 1\} \\
&= 2^m - 1 - 2\left(2^m - \#\{x \in \mathbb{F}_{2^m} \mid g(x) = 0\}\right) \\
&= -2^m - 1 + 2\#\left\{x \in \mathbb{F}_{2^m} \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + t = f(x)\right\} \\
&= -2^m - 1 + \#G_f \ .
\end{aligned}$$

□

[4] In the original paper of Mesnager [197], it is first shown that the theorem is valid to characterize the bentness of $f_{a,b}$ and then that $f_{a,b}$ is bent if and only if it is hyper-bent.

[5] More details are given in Sections 4.3 and 4.4

Proposition 4.2.5. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function, $g = \mathrm{Tr}_1^m(f)$ be its composition with the absolute trace and H_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by*

$$H_f : y^2 + xy = x + x^2 f(x) \ ,$$

Then

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g(x)\right) = -2^m + \#H_f \ .$$

Proof. The proof is similar as that of Theorem 4.2.1 and is summarized by the following equalities:

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g(x)\right) &= \sum_{x \in \mathbb{F}_{2^m}^*} \left(1 - 2(\mathrm{Tr}_1^m\left(x^{-1}\right) + g(x))\right) \\
&= 2^m - 1 - 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1}\right) + g(x) = 1\right\} \\
&= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1}\right) + g(x) = 0\right\} \\
&= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + t = x^{-1} + f(x)\right\} \\
&= -2^m + 1 \\
&\qquad + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ (t/x)^2 + (t/x) = x^{-1} + f(x)\right\} \\
&= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + xt = x + x^2 f(x)\right\} \\
&= -2^m + 1 + \#H_f - \#\left\{P \in H_f \mid x = 0\right\} \\
&= -2^m + \#H_f \ .
\end{aligned}$$

□

We can now easily deduce the reformulation of the Charpin–Gong criterion given by Lisoněk.

Theorem 4.2.6 (Reformulation of the Charpin–Gong criterion [182, 181])**.** *The notation is as in Theorem 4.1.1. Moreover, let H_a and G_a be the (affine) curves defined over $\mathbb{F}_{2^m}$ by*

$$\begin{aligned}
G_a &: y^2 + y = \sum_{r \in R} a_r D_r(x) \ , \\
H_a &: y^2 + xy = x + x^2 \sum_{r \in R} a_r D_r(x) \ .
\end{aligned}$$

Then f_a is hyper-bent if and only if

$$\#H_a - \#G_a = -1 \ .$$

Proof. According to Proposition 4.2.5, the left hand side of the Charpin–Gong criterion satisfies

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_a(x)\right) = -2^m + \#H_a \ ;$$

and, according to Proposition 4.2.4, the right hand side of the Charpin–Gong criterion satisfies

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(g_a(x)\right) = -2^m - 1 + \#G_a \ .$$

□

Let us now fix a subset of indices $E \subseteq R$ and denote by r_{max} the maximal index. We can suppose r_{max} to be odd and will do so for two reasons:

1. it ensures that the smooth projective models of the curves H_a and G_a are imaginary hyperelliptic curves and such curves are way easier to manipulate than real hyperelliptic curves;

2. for efficiency reasons r_{max} should be as small as possible, so the natural choice for the the indices in a cyclotomic coset will be the coset leaders which are odd integers.

In fact, the curves H_a and G_a are even Artin–Schreier curves. As was the case for elliptic curves, Theorem 3.2.18 states that there exist efficient algorithms to compute the cardinalities of such curves. Thus, Lisoněk obtained an efficient test for hyper-bentness of Boolean functions in the class described by Charpin and Gong. The polynomial defining H_a (respectively G_a) is indeed of degree $r_{max}+2$ (respectively r_{max}), so the curve is of genus $(r_{max}+1)/2$ (respectively $(r_{max}-1)/2$). The complexity for testing a Boolean function in this family is then dominated by the computation of the cardinality of a curve of genus $(r_{max}+1)/2$, which is polynomial in m for a fixed r_{max} (and so fixed genera for the curves H_a and G_a).

We now show that a similar reformulation can be applied to the different versions of the second criterion of Mesnager for Boolean functions with multiple trace terms.

Theorem 4.2.7 (Reformulation of the second Mesnager criterion)**.** *The notation is as in Theorem 4.1.2. Moreover, let H_a and G_a be the (affine) curves defined over $\mathbb{F}_{2^m}$ by*

$$G_a : y^2 + y = \sum_{r\in R} a_r D_r(x) \ ,$$
$$H_a : y^2 + xy = x + x^2 \sum_{r\in R} a_r D_r(x) \ ;$$

and let H_a^3 and G_a^3 be the (affine) curves defined over $\mathbb{F}_{2^m}$ by

$$G_a^3 : y^2 + y = \sum_{r\in R} a_r D_r(D_3(x)) \ ,$$
$$H_a^3 : y^2 + xy = x + x^2 \sum_{r\in R} a_r D_r(D_3(x)) \ .$$

If b is a primitive element of $\mathbb{F}_4$, then $f_{a,b}$ is hyper-bent if and only if

$$\#H_a^3 - \#G_a^3 = 3 \ .$$

If $b = 1$, then $f_{a,1}$ is hyper-bent if and only if

$$\left(\#G_a^3 - \#H_a^3\right) - \frac{3}{2}\left(\#G_a - \#H_a\right) = \frac{3}{2} \ .$$

Proof. If b is a primitive element of $\mathbb{F}_4$, according to Proposition 4.2.5 the left hand side of Condition 2c in Theorem 4.1.2 satisfies

$$\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_a(D_3(x))\right) = -2^m + \#H_a^3 \ ,$$

and according to Proposition 4.2.4 the right hand side of Condition 2c in Theorem 4.1.2 satisfies

$$2^m - 2\,\mathrm{w_H}(g_a \circ D_3) + 3 = -2^m + 3 + \#G_a^3 \ ,$$

so that the criterion is equivalent to

$$\#H_a^3 - \#G_a^3 = 3 \ .$$

We could also have used Condition 2b and that its left hand side satisfies

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m\left(x^{-1}\right)=1} \chi\left(g_a \circ D_3(x)\right) &= \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g_a \circ D_3(x)\right) - \sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_a \circ D_3(x)\right)\right) \\ &= \frac{1}{2}\left(\left(-2^m - 1 + \#G_a^3\right) - \left(-2^m + \#H_a^3\right)\right) \\ &= \frac{1}{2}\left(\#G_a^3 - \#H_a^3 - 1\right) \ ;\end{aligned}$$

and decuce the same reformulation.

If $b = 1$, using the previous calculations, the first term in Condition 3 of Theorem 4.1.2 satisfies

$$2\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a \circ D_3(x)\right) = \#G_a^3 - \#H_a^3 - 1 \ ;$$

and the second term satisfies

$$3\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(x)\right) = \frac{3}{2}\left(\#G_a - \#H_a - 1\right) \ ;$$

whence the reformulation. □

Here all the curves are also Artin–Schreier curves. So, for a fixed subset of indices R, we also get a test in polynomial time and space in m. However, the complexity of the point counting algorithms also depends on the genera of the curves, and so on the degrees of the polynomials defining them. Denoting by r_{max} the maximal index as above, the genus of H_a^3 (respectively G_a^3) is $(3r_{max}+1)/2$ (respectively $(3r_{max}-1)/2$), so approximately three times that of H_a (respectively G_a). Therefore, the associated test will be much slower than for Boolean functions of the family of Charpin and Gong for a given subset R: we have to compute the cardinalities of two curves of genera $(3r_{max}+1)/2$ and $(3r_{max}-1)/2$ if b is primitive, or four curves of genera $(3r_{max}+1)/2$, $(3r_{max}-1)/2$, $(r_{max}+1)/2$ and $(r_{max}-1)/2$ if $b = 1$, instead of two curves of genera $(r_{max}+1)/2$ and $(r_{max}-1)/2$. Hence, we propose another reformulation of the Mesnager criterion involving slightly less computations.

Theorem 4.2.8 (Reformulation of the second Mesnager criterion)**.** *The notation is as in Theorem 4.2.7. If b is a primitive element of $\mathbb{F}_4$, then $f_{a,b}$ is hyper-bent if and only if*

$$\#G_a^3 - \frac{1}{2}\left(\#G_a + \#H_a\right) = -\frac{3}{2} \ .$$

If $b = 1$, then $f_{a,1}$ is hyper-bent if and only if

$$2\#G_a^3 - \frac{5}{2}\#G_a + \frac{1}{2}\#H_a = \frac{3}{2} \ .$$

Proof. We use the fact that m is odd, so that the function $x \mapsto D_3(x) = x^3 + x$ is a permutation of the set $\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1}\right) = 0\right\}$ (see the papers of Berlekamp, Rumsey and Solomon [13, Theorem 2] and Charpin, Helleseth and Zinoviev [47] for the case of D_3, or more generally the article of Dillon and Dobbertin [71]), and similar arguments as previously.

If b is a primitive element of $\mathbb{F}_4$, then the left hand side in Condition 2b of Theorem 4.1.2 satisfies

$$\begin{aligned}
\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a\circ D_3(x)\right) &= \sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g_a\circ D_3(x)\right) - \sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=0} \chi\left(g_a\circ D_3(x)\right)\\
&= \sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g_a\circ D_3(x)\right) - \sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=0} \chi\left(g_a(x)\right)\\
&= \sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g_a\circ D_3(x)\right)\\
&\quad - \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g_a(x)\right) + \sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right)+g_a(x)\right)\right)\\
&= \left(-2^m-1+\#G_a^3\right) - \frac{1}{2}\left((-2^m-1+\#G_a)+(-2^m+\#H_a)\right)\\
&= -\frac{1}{2}+\#G_a^3-\frac{1}{2}\left(\#G_a+\#H_a\right)\ .
\end{aligned}$$

If $b=1$, then the first term in Condition 3 of Theorem 4.1.2 satisfies

$$2\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a\circ D_3(x)\right) = -1+2\#G_a^3-\left(\#G_a+\#H_a\right)\ . \qquad \square$$

Here we discarded the computation of the cardinality of the curve of genus $(3r_{max}+1)/2$ and we have to compute the cardinalities of three curves of genera $(3r_{max}-1)/2$, $(r_{max}+1)/2$ and $(r_{max}-1)/2$.

4.3 Divisibility of binary Kloosterman sums

4.3.1 Classical results

Because of their cryptographic interest, divisibility properties of Kloosterman sums have been studied in several recent papers. A nice overview of such results can be found in the Ph.D. thesis of Moloney [206]. Here we cite a few of them which we will explicitly use in search algorithms for binary Kloosterman sums with specific values, especially the values 0 and 4.

The following proposition is directly obtained from the classical result of Lachaud and Wolfmann [157].

Proposition 4.3.1 ([157]). *Let $m\geq 3$ be a positive integer. The set $\{K_m(a),\ a\in\mathbb{F}_{2^m}\}$ is the set of all the multiples of 4 in the range $[-2^{(m+2)/2}+1, 2^{(m+2)/2}+1]$.*

This result states in particular that binary Kloosterman sums are always divisible by 4. Afterwards, several papers studied divisibility properties of binary Kloosterman sums by multiples of 4 and other integers.

The following result was first proved by Helleseth and Zinoviev [129] and classifies the values of $K_m(a)$ modulo 8 according to the value of the absolute trace of a.

Proposition 4.3.2 ([129]). *Let $m\geq 3$ be any positive integer and $a\in\mathbb{F}_{2^m}$. Then $K_m(a)\equiv 0 \pmod 8$ if and only if $\mathrm{Tr}_1^m(a)=0$.*

In the same article, they gave the following sufficient conditions to get certain values of $K_m(a)$ modulo 3.

Proposition 4.3.3 ([129]). *Let $m \geq 3$ be any positive integer and $a \in \mathbb{F}_{2^m}^*$. Suppose that there exists $t \in \mathbb{F}_{2^m}^*$ such that $a = t^4 + t^3$.*

- *If m is odd, then $K_m(a) \equiv 1 \pmod 3$.*
- *If m is even, then $K_m(a) \equiv 0 \pmod 3$ if $\mathrm{Tr}_1^m(t) = 0$ and $K_m(a) \equiv -1 \pmod 3$ if $\mathrm{Tr}_1^m(t) = 1$.*

Furthermore, Charpin, Helleseth and Zinoviev [48] gave additional results about values of $K_m(a)$ modulo 3.

Proposition 4.3.4 ([48]). *Let $m \geq 3$ be any positive integer and $a \in \mathbb{F}_{2^m}^*$. Then we have:*

- *If m is odd, then $K_m(a) \equiv 1 \pmod 3$ if and only if $\mathrm{Tr}_1^m\left(a^{1/3}\right) = 0$. This is equivalent to $a = \frac{b}{(1+b)^4}$ for some $b \in \mathbb{F}_{2^m}^*$.*
- *If m is even, then $K_m(a) \equiv 1 \pmod 3$ if and only if $a = b^3$ for some b such that $\mathrm{Tr}_2^m(b) \neq 0$.*

Further divisibility results exist and could be used to further refine the tests proposed in this chapter. For example, results up to 64 can be found in a paper of Göloğlu, McGuire and Moloney [124], and results up to 256 in an even more recent paper of Göloğlu, Lisoněk, McGuire and Moloney [123].

Most of these results about divisibility were first proved studying the link between exponential sums and coset weight distribution [129, 48]. However some of them can be proved in a completely different manner as we show in the next subsection.

4.3.2 Using torsion of elliptic curves

Theorem 4.2.1 giving the value of $K_m(a)$ as the cardinality of an elliptic curve can indeed be used to deduce divisibility properties of Kloosterman sums from the rich theory of elliptic curves. We recall that the quadratic twist of the ordinary elliptic curve E_a that we denote by $\widetilde{E}_a$ is given by the Weierstraß equation

$$\widetilde{E}_a : y^2 + xy = x^3 + bx^2 + a \ ,$$

where $b \in \mathbb{F}_{2^m}$ has absolute trace 1; it has cardinality:

$$\#\widetilde{E}_a = 2^m + 2 - K_m(a) \ .$$

First of all, we recall a proof of the divisibility by 4 stated in Proposition 4.3.1 as it can be found for example in the preprint of Ahmadi and Granger [3]. For $m \geq 3$, $K_m(a) \equiv \#E_a \pmod 4$, so $K_m(a) \equiv 0 \pmod 4$ if and only if $\#E_a \equiv 0 \pmod 4$. This is equivalent to E_a having a non-trivial rational point of 4-torsion. This can also be formulated as both the equation of E_a and its 4-division polynomial $f_4(x) = x^6 + ax^2$ having a rational solution. It is easily seen that $P = (a^{1/4}, a^{1/2})$ is always a non-trivial solution to this problem.

Lisoněk [180] used similar techniques to give a different proof of Proposition 4.3.2. Indeed, for $m \geq 3$, $K_m(a)$ is divisible by 8 if and only if E_a has a non-trivial rational point of 8-torsion. This is easily shown to be equivalent to $\mathrm{Tr}_1^m\left(a^{1/4}\right) = \mathrm{Tr}_1^m(a) = 0$.

Finally, it is possible to prove directly that the condition given in Proposition 4.3.3 is not only sufficient, but also necessary, using torsion of elliptic curves[6]. We use this property in Subsection 4.4.3.

[6] We were recently made aware that such a result was also proved in a different way also involving elliptic curves by Garashuck and Lisoněk [108] in the case where m is odd.

Proposition 4.3.5. *Let $a \in \mathbb{F}_{2^m}^*$.*

- *If m is odd, then $K_m(a) \equiv 1 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4+t^3$.*
- *If m is even, then:*
  - *$K_m(a) \equiv 0 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$ and $\mathrm{Tr}_1^m(t) = 0$;*
  - *$K_m(a) \equiv -1 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$ and $\mathrm{Tr}_1^m(t) = 1$.*

Proof. According to Proposition 4.3.3 we only have to show that, if a verifies the given congruence, it can be written as $a = t^4 + t^3$.

- We begin with the case m odd, so that $2^m \equiv -1 \pmod 3$. Then $K_m(a) \equiv 1 \pmod 3$ if and only if $\#E_a \equiv 0 \pmod 3$, i.e. if E_a has a non-trivial rational point of 3-torsion. It implies that the 3-division polynomial of E_a given by $f_3(x) = x^4 + x^3 + a$ has a rational solution, so that there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.
- Suppose now that m is even, so that $2^m \equiv 1 \pmod 3$.
  - If $K_m(a) \equiv -1 \pmod 3$, then $\#E_a \equiv 0 \pmod 3$, and as in the previous case we can find $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.
  - If $K_m(a) \equiv 0 \pmod 3$, then $\#E_a \equiv 1 \pmod 3$, but $\#\widetilde{E}_a \equiv 0 \pmod 3$. The 3-division polynomial of $\widetilde{E}_a$ is also given by $f_3(x) = x^4 + x^3 + a$, so that there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.

□

4.4 Finding specific values of binary Kloosterman sums

4.4.1 Generic strategy

In this subsection we present the most generic method to find specific values of binary Kloosterman sums. To this end, one picks random elements of $\mathbb{F}_{2^m}$ and computes the corresponding values until a correct one is found. Before performing any complicated computations, divisibility conditions as those stated in the previous section can be used to restrict the pool of elements to those satisfying certain conditions (but without missing any element giving the value searched for) or to filter out elements which will give inadequate values.

Then, the most naive method to check the value of a binary Kloosterman sum is to compute it as a sum. However, one test would need $O(2^m m \log^2 m \log\log m)$ bit operations and this is obviously highly inefficient. Theorem 4.2.1 tells that this costly computation can be replaced by the computation of the cardinality of an elliptic curve over a finite field of even characteristic. Using p-adic methods à la Satoh [228], also known as canonical lift methods, this can be done quite efficiently in $O(m^2 \log^2 m \log\log m)$ bit operations and $O(m^2)$ memory [126, 275, 274, 174]. Working with elliptic curves also has the advantage that one can check that the current curve is a good candidate before computing its cardinality as follows: one picks a random point on the curve and multiplies it by the targeted order; if it does not give the point at infinity, the curve does not have the targeted cardinality.

Finally, it should be noted that, if ones looks for all the elements giving a specific value, a different strategy can be adopted as noted in the paper of Ahmadi and Granger [3]. Recall

that a binary Kloosterman sum can be seen as the Walsh–Hadamard transform of the Boolean function $\mathrm{Tr}_1^m(1/x)$. Therefore, we can construct the Boolean function corresponding to the function $\mathrm{Tr}_1^m(1/x)$ and then use a fast Walsh–Hadamard transform to compute the values of all binary Kloosterman sums. Building the Boolean function costs one multiplication per element, so $O(2^m m \log m \log\log m)$ bit operations and $O(2^m)$ memory. The complexity of the fast Walsh–Hadamard transform is $O(2^m m^2)$ bit operations and $O(2^m m)$ memory [8].

4.4.2 Zeros of binary Kloosterman sums

When looking for zeros of binary Kloosterman sums, which is of high cryptographic interest as Table 4.2 emphasizes, one benefits from even more properties of elliptic curves over finite fields. Indeed, when $K_m(a) = 0$, we get that $\#E_a = 2^m$. Hence all rational points of E_a are of order some power of 2.

In fact, we know even more. As E_a is defined over a field of even characteristic, its complete 2^e-torsion (where e is any strictly positive integer) is of rank 1, whereas the complete l^e-torsion, for a prime l different from 2, is of rank 2, as stated in Proposition 3.2.7. Therefore the rational Sylow 2-subgroup is cyclic, isomorphic to $\mathbb{Z}/2^e\mathbb{Z}$ for some positive integer e. In the case where $K_m(a) = 0$, we even get that the whole group of rational points is isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$. Furthermore, basic group theory tells that E_a will then have 2^{m-1} points of order 2^m.

Finally, it should be noted that, if $2^m \mid \#E_a$, then $\#E_a$ must be equal to 2^m. This is a simple consequence of Hasse theorem (Theorem 3.2.9) giving bounds on the number of rational points of an elliptic curve over a finite field.

These facts have first been used by Lisoněk [180] to develop a probabilistic method to test whether a given a gives a binary Kloosterman zero or not: one takes a random point on E_a and tests whether its order is 2^m or not. This test involves at most m duplications on the curve, hence is quite efficient. Moreover, as soon as $\#E_a = 2^m$, half of its points are generators, so that testing one point on a correct curve gives a probability of success of $1/2$. This led Lisoněk to find zeros of binary Kloosterman sums for m up to 64 in a matter of days.

Afterwards, Ahmadi and Granger [3] proposed a deterministic algorithm to test whether an element $a \in \mathbb{F}_{2^m}$ gives a binary Kloosterman zero or not. From the above discussion, it is indeed enough to compute the size of the Sylow 2-subgroup of E_a to answer that question. This can be efficiently implemented by point halving, starting from a non-trivial point of 4-torsion (remember that such a point always exists on E_a). The complexity of each iteration of their algorithm is dominated by two multiplications in $\mathbb{F}_{2^m}$. So testing a curve with a Sylow 2-subgroup of size 2^e is of complexity $O(e \cdot m \log m \log\log m)$. Furthermore, they showed that the average size of the Sylow 2-subgroup of the curves of the form E_a is 2^3 when m goes to infinity, so that their algorithm has an asymptotic average bit complexity of $O(m \log m \log\log m)$.

4.4.3 Implementation for the value 4

As shown in Table 4.2, we have a necessary and sufficient condition to build bent functions from the value 4 of binary Kloosterman sums when m is odd and a necessary only condition when m is even. Unfortunately, the situation is more complicated than in the case of binary Kloosterman zeros.

We are indeed looking for an element $a \in \mathbb{F}_{2^m}$ such that $K_m(a) = 4$. The cardinality of E_a should then be $\#E_a = 2^m + K_m(a) = 4(2^{m-2} + 1)$ which does not ensure to have a completely fixed group structure as was the case when $\#E_a = 2^m$. Moreover, in general, the number $2^{m-2}+1$ does not verify many divisibility properties leading to an efficient test for the value 4. The

cardinality of the twist $\widetilde{E}_a$ is given by $\#\widetilde{E}_a = 2^m + 2 - K_m(a) = 2(2^{m-1} - 1)$ which does not provide more useful information.

What we can however deduce from these equalities is that, if $K_m(a) = 4$, then:

- $K_m(a) \equiv 4 \pmod 8$, so that $\mathrm{Tr}_1^m(a) = 1$;
- $K_m(a) \equiv 1 \pmod 3$, so that:
  - if m is odd, then a can be written as $t^4 + t^3$;
  - if m is even, then a can be written as t^3 with $\mathrm{Tr}_2^m(t) \neq 0$.

We can use both these conditions to filter out a to be tested as described in Algorithm 4.1 (for m odd).

Algorithm 4.1: Finding the value 4 of binary Kloosterman sums for m odd

Input: A positive odd integer $m \geq 3$
Output: An element $a \in \mathbb{F}_{2^m}$ such that $K_m(a) = 4$

1 $a \leftarrow_R \mathbb{F}_{2^m}$
2 $a \leftarrow a^3(a+1)$
3 **if** $\mathrm{Tr}_1^m(a) = 0$ **then**
4 Go to step 4.1
5 $P \leftarrow_R E_a$
6 **if** $[2^m + 4]P \neq 0$ **then**
7 Go to step 4.1
8 **if** $\#E_a \neq 2^m + 4$ **then**
9 Go to step 4.1
10 **return** a

We implemented this algorithm in Sage [250]. It was necessary to implement a relatively efficient version of point counting in even characteristic, none of them being available. The first implemented algorithm was an extension to even characteristic of Satoh's original algorithm by Fouquet, Gaudry and Harley [98]. The complexity of this algorithm is $O(m^{3+\epsilon})$ bit operations (or $O(m^5)$ with naive multiplication) and $O(m^3)$ memory, but it is quite simple and there was already an existing implementation in GP/Pari by Yeoh [284] to use as a starting point. The computations in $\mathbb{Z}_{2^m}$, the unique unramified extension of degree m of the 2-adic integers $\mathbb{Z}_2$, were done through the direct library interface to Pari [218] provided in Sage. We also implemented Harley's algorithm [126] as described in Vercauteren's thesis [275] using similar implementation details. Our implementations have both been contributed back to Sage[7][8]. As a byproduct of our work we corrected and optimized the current implementation of Boolean functions in Sage[9]. The code for manipulating binary Kloosterman sums has also been made available on the author's homepage[10].

As a result of our experiments, we found that the following value of a for $m = 55$ gives a value 4 of binary Kloosterman sum. The finite field $\mathbb{F}_{2^{55}}$ is represented as $\mathbb{F}_2[x]/(x^{55} + x^{11} + x^{10} + x^9 +$

[7] http://trac.sagemath.org/sage_trac/ticket/11448
[8] http://trac.sagemath.org/sage_trac/ticket/11548
[9] http://trac.sagemath.org/sage_trac/ticket/11450
[10] http://perso.telecom-paristech.fr/~flori/kloo/

$x^7 + x^4 + 1$); a is then given as

$$\begin{aligned} a = x^{53} + x^{52} + x^{51} + x^{50} + x^{47} + x^{43} + x^{41} + x^{38} + x^{37} + x^{35} \\ + x^{33} + x^{32} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} \\ + x^{22} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{13} + x^{12} + x^5 \ . \end{aligned}$$

4.5 Experimental results for m even

When m is even, Mesnager [197] has shown that the situation seems to be more complicated theoretically than in the case where m is odd, and that the study of the bentness of the Boolean functions given in Table 4.2 cannot be done as in the odd case. As shown in Table 4.2, we only have a necessary condition to build bent functions from the value 4 of binary Kloosterman sum when m is even. To get a better understanding of the situation we conducted some experimental investigations to check whether the Boolean functions constructed with the formula of Table 4.2 were bent or not for all the a's in $\mathbb{F}_{2^m}$ giving a Kloosterman sum with value 4.

The functions of Mesnager [197] are defined for $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$ as the Boolean functions $f_{a,b}$ with $n = 2m$ inputs given by

$$f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) \ . \tag{4.2}$$

We now show that it is enough to study the bentness of a subset of these functions to get results about all of them.

First of all, the next proposition proves that the study of the bentness of $f_{a,b}$ can be reduced to the case where $b = 1$.

Proposition 4.5.1. *Let $n = 2m$ with $m \geq 3$ even. Let $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$. Let $f_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by Equation* (4.2)*. Then $f_{a,b}$ is bent if and only if $f_{a,1}$ is bent.*

Proof. Since m is even, we have the inclusion of fields $\mathbb{F}_4^* \subset \mathbb{F}_{2^m}^*$. In particular, for every $b \in \mathbb{F}_4^*$, there exists $\alpha \in \mathbb{F}_{2^m}^*$ such that $\alpha^{\frac{2^n-1}{3}} = b$. For $x \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} f_{a,b}(x) &= \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) \\ &= \mathrm{Tr}_1^n\left(a\alpha^{2^m-1}x^{2^m-1}\right) + \mathrm{Tr}_1^2\left(\alpha^{\frac{2^n-1}{3}}x^{\frac{2^n-1}{3}}\right) \\ &= \mathrm{Tr}_1^n\left(a(\alpha x)^{2^m-1})\right) + \mathrm{Tr}_1^2\left((\alpha x)^{\frac{2^n-1}{3}}\right) \\ &= f_{a,1}(\alpha x) \ . \end{aligned}$$

Hence, for every $\omega \in \mathbb{F}_{2^n}^*$, we have

$$\begin{aligned} \widehat{\chi_{f_{a,b}}}(\omega) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_{a,b}(x) + \mathrm{Tr}_1^n(\omega x)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_{a,1}(\alpha x) + \mathrm{Tr}_1^n(\omega x)} \\ &= \widehat{\chi_{f_{a,1}}}(\omega\alpha^{-1}) \ . \end{aligned}$$

□

Second, we know that $K_m(a) = K_m(a^2)$, so the a's in $\mathbb{F}_{2^m}$ giving binary Kloosterman sums with value 4 come in cyclotomic classes. Fortunately, it is enough to check one a per class. Indeed, $f_{a,b}$ is bent if and only if f_{a^2,b^2} is, as proved in the following proposition.

Proposition 4.5.2. *Let $n = 2m$ with $m \geq 3$. Let $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$. Let $f_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by Equation (4.2). Then $f_{a,b}$ is bent if and only if f_{a^2,b^2} is bent.*

Proof.

$$\begin{aligned}
\widehat{\chi_{f_{a,b}}}(\omega) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_{a,b}(x)+\mathrm{Tr}_1^n(\omega x)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)+\mathrm{Tr}_1^n(\omega x)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(a^2x^{2\,2^m-1}\right)+\mathrm{Tr}_1^2\left(b^2x^{2\,\frac{2^n-1}{3}}\right)+\mathrm{Tr}_1^n\left(\omega^2x^2\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(a^2x^{2^m-1}\right)+\mathrm{Tr}_1^2\left(b^2x^{\frac{2^n-1}{3}}\right)+\mathrm{Tr}_1^n\left(\omega^2x\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_{a^2,b^2}(x)+\mathrm{Tr}_1^n\left(\omega^2x\right)} \\
&= \widehat{\chi_{f_{a^2,b^2}}}(\omega^2) \ .
\end{aligned}$$

□

In the specific case $b = 1$ that we are interested in, it gives that $f_{a,1}$ is bent if and only if $f_{a^2,1}$ is, which proves that checking one element of each cyclotomic class is enough.

Finally, as mentioned in Section 4.4, finding all the a's in $\mathbb{F}_{2^m}$ giving a specific value is a different problem from finding one such $a \in \mathbb{F}_{2^m}$. One can compute the Walsh–Hadamard transform of the trace of the inverse function using a fast Walsh–Hadamard transform. As long as the basis of $\mathbb{F}_{2^m}$ considered as a vector space over $\mathbb{F}_2$ is correctly chosen so that the trace corresponds to the scalar product, the implementation is straightforward.

The algorithm that we implemented is described in Algorithm 4.2.

Algorithm 4.2: Testing bentness for m even

Input: An even integer $m \geq 3$
Output: A list of couples made of one representative for each cyclotomic class of elements $a \in \mathbb{F}_{2^m}$ such that $K_m(a) = 4$ together with 1 if the corresponding Boolean functions $f_{a,b}$ are bent, 0 otherwise

```
Build the Boolean function f : x ∈ F_{2^n} ↦ Tr_1^n(1/x) ∈ F_2
Compute the Walsh–Hadamard transform of f
Build a list A made of one a ∈ F_{2^m} for each cyclotomic class such that K_m(a) = 4
Initialize an empty list R
foreach a ∈ A do
    Build the Boolean function f_{a,1}
    Compute the Walsh–Hadamard transform of f_{a,1}
    if f_{a,1} is bent then
        Append (a, 1) to R
    else
        Append (a, 0) to R
return R
```

The implementation[11] was made using Sage [250] and Cython [24], performing direct calls to Givaro [74], NTL [241] and gf2x [26] libraries for efficient manipulation of finite field elements and construction of Boolean functions.

In Table 4.4 we give the results of the computations we conducted along with different pieces of information about them. One should remark that all the Boolean functions which could be tested are bent. Evidence that our computations were correct is given by the fact that

Table 4.4: Test of bentness for m even

m	Nb. of cyclotomic classes	Time	All bent?
4	1	<1s	yes
6	1	<1s	yes
8	2	<1s	yes
10	3	4s	yes
12	6	130s	yes
14	8	3000s	yes
16	14	82000s	yes
18	20	-	-
20	76	-	-
22	87	-	-
24	128	-	-
26	210	-	-
28	810	-	-
30	923	-	-
32	2646	-	-

the number of cyclotomic classes we found is so. This can be checked using the formula of Proposition 3.2.11. We are looking for elliptic curves with trace t of the Frobenius endomorphism equal to $t = 1 - K_m(a) = -3$. Hence, the number of cycloctomic classes is $H(\Delta)/m$ where $H(\Delta)$ is the Kronecker class number and $\Delta = 9 - 4 \cdot 2^m$. Moreover, for the values we tested, except $m = 12, 30, 32$, this discriminant is fundamental, so that the order $\mathbb{Z}[\alpha]$ is maximal and $H(\Delta) = h(\Delta)$ the classical class number, a quantity even easier to compute.

Unfortunately, we were not able to check bentness of functions for $m > 16$ due to lack of memory. Constructing the Boolean functions in $n = 2m$ variables is the most time consuming part of the test, but the real bottleneck is the amount of memory needed to compute their Walsh–Hadamard transforms. One must indeed perform these computations using integers of size at least $2m + 1$ bits, so, with our implementation, integers of 64 bits as soon as $m \geq 16$. The amount of memory needed is then $64 \cdot 2^{2m} \cdot 2^{-30} = 2^{2m-24}$ GB. For $m = 16$ this represents already 32 GB of memory; for $m = 18$ it would be 512 GB of memory. Therefore, we give in Table 4.5 the fourteen values of a found for $m = 16$, the highest value that we could test. In this table the finite field $\mathbb{F}_{2^{16}}$ is represented as $\mathbb{F}_2[x]/(x^{16} + x^5 + x^3 + x^2 + 1)$. The corresponding Boolean functions in $n = 32$ variables are all bent as we already pointed out.

[11] See Footnote 10.

Table 4.5: The fourteen cyclotomic classes such that $K_{16}(a) = 4$ as elements of $\mathbb{F}_2[x]/(x^{16} + x^5 + x^3 + x^2 + 1)$

$$
\begin{array}{l}
x^{14} + x^{11} + x^8 + x^6 + x^3 + x \\
x^{15} + x^{13} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1 \\
x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^2 + x \\
x^{14} + x^{12} + x^{11} + x^9 + x^6 + x \\
x^{15} + x^{11} + x^9 + x^7 + x^6 + x^3 + x^2 + 1 \\
x^{13} + x^6 + x^4 + x^2 + x + 1 \\
x^{12} + x^{11} + x^{10} + x^9 + x^5 + x^3 + x^2 + x \\
x^{15} + x^{11} + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 \\
x^{15} + x^{13} + x^9 + x^8 + x^5 + x^4 + x^3 + x \\
x^{15} + x^{11} + x^{10} + x^3 \\
x^{13} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^3 + x^2 + x \\
x^{13} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x \\
x^{15} + x^{13} + x^{10} + x^9 + x^8 + x^7 + x^5 + x \\
x^{15} + x^{11} + x^{10} + x^3 + x + 1
\end{array}
$$

Part III

Complex multiplication and class polynomials

Chapter 5

Complex multiplication and elliptic curves

"What does it mean that those trees and mountains out there are not magic but real?" I'd yell, pointing outdoors.
"What?" they'd say.
"It means that those trees and mountains out there are not magic but real."
"Yeah?"
Then I'd say, "What does it mean that those trees and mountains aren't real at all, just magic?"
"Oh come on."
"It means that those trees and mountains aren't real at all, just magic."
"Well which is it, goddammit!"
"What does it mean that you ask, well which is it goddammit?" I yelled.
"Well what?"
"It means that you ask well which is it goddammit."

The Dharma Bums
Jack Kerouac [149]

Contents

In Part II (hyper)elliptic curves were introduced through the connections between their numbers of points and values of different exponential sums over finite fields. A particular emphasis was put on the structure of their groups of rational points and on the efficiency of point counting on such curves, thus leading to the design of efficient tests for (hyper-)bentness and efficient algorithms to generate (hyper-)bent functions. It was also brought to light that elliptic curves with complex multiplication were an important theoretical tool; the number of such curves with a given number of points was used to count the number of exponential sums with a given value.

It is a fact that (hyper)elliptic curves with complex multiplication enjoy a number of very pleasant properties, not only for the application mentioned above, but also for several applications in asymmetric cryptography. Therefore, we will now depart from the world of Boolean functions to solely concentrate our efforts on the explicit construction of such curves and the computation of class polynomials.

The theory of elliptic curves with complex multiplication is quite well understood nowadays. This chapter, which builds essentially upon a course taught at Télécom ParisTech, aims at giving an overview of this theory and the construction of class polynomials for general orders through the complex analytic method, and so at introducing the unfamiliar reader to the more general and involved theory of abelian varieties with complex multiplication which will be treated in Chapter 6. For the most of this chapter we will omit the proofs of the very classical results we introduce, but provide references to classical textbooks where they can be found. If one reference had to be chosen, we would refer the reader to the classical textbooks[1] of Silverman [244, 245] which were more than a source of inspiration for the material presented here.

Section 5.1 gives further background on the algebraic theory of elliptic curves, whereas Section 5.2 develops a completely different point of view: over the complex numbers, elliptic curves can indeed be described as complex tori. Such a description is especially useful in Section 5.3 when studying the endomorphism rings and the isomorphism classes of complex elliptic curves with complex multiplication by a given order. Moreover, this approach will not only lead to the powerful main theorem of complex multiplication, but also to the explicit construction of class polynomials and elliptic curves with complex multiplication. To conclude this chapter, some applications of elliptic curves — and particularly of elliptic curves with complex multiplication — in asymmetric cryptography are presented in Section 5.4.

5.1 Further background on elliptic curves

In this section we give further background on algebraic curves and elliptic curves. Unless stated otherwise, all curves we consider are projective.

5.1.1 Morphisms between algebraic curves

It is a basic property of projective varieties, or more generally of complete varieties, that the image of a morphism is closed. For morphisms between projective curves, this fact gives the

[1] We could not resist choosing *two* books.

following fundamental result.

Theorem 5.1.1 ([244, Theorem II.2.3], [128, Proposition II.6.8]). *Let K be a perfect field. Let $\phi : C_1 \to C_2$ be a morphism between algebraic curves defined over K. Then ϕ is constant or surjective (over $\overline{K}$).*

Basic properties of morphisms between algebraic curves are defined using the canonically associated maps on the corresponding *function fields*.

Definition 5.1.2 (Function field). *Let K be a perfect field and C algebraic curve defined on K. We denote by $K(C)$ the function field of C.*

Definition 5.1.3. *Let K be a perfect field. Let $\phi : C_1 \to C_2$ be a non-constant morphism between algebraic curves defined over K. Different homomorphisms between the function fields of the curves can be defined from a morphism between the curves:*

- $\phi^* : K(C_2) \to K(C_1),\ g \mapsto g \circ \phi$,
- $\phi_* = (\phi^*)^{-1} \circ \mathrm{N}_{K(C_1)/\phi^* K(C_2)}$.

First, these maps can be used to completely characterize a morphism.

Theorem 5.1.4 ([244, Theorem II.2.4], [128, Corollary I.6.12, Proposition II.6.8]). *Let K be a perfect field. Let C_1 and C_2 be two curves defined over K.*

1. *Let $\phi : C_1 \to C_2$ be a non-constant morphism. Then $K(C_1)$ is a finite extension of $\phi^* K(C_2)$.*
2. *Let $i : K(C_2) \to K(C_1)$ be an injection leaving K fixed. Then there exists a unique non-constant morphism $\phi : C_1 \to C_2$ such that $i = \phi^*$.*
3. *Let $K' \subset K(C_1)$ be a subfield of finite index containing K. Then there exists a smooth curve C', unique up to K-isomorphism, and a morphism $\phi : C_1 \to C'$ such that $K' = \phi^* K(C')$.*

Second, two very important quantities are defined using the function fields.

Definition 5.1.5 (Degree). *Let K be a perfect field. Let $\phi : C_1 \to C_2$ be a morphism between two algebraic curves defined over K.*

If ϕ is constant, thenwe define its degree $\deg(\phi) = 0$.

Otherwise, ϕ is surjective and its degree is defined as

$$\deg(\phi) = [K(C_1) : \phi^* K(C_2)],$$

i.e. the dimension of the $\phi^* K(C_2)$-vector space $K(C_1)$.

The morphism ϕ is said to be separable, inseparable or purely inseparable, if the extension of function fields is; the separable and inseparable degrees $\deg_s(\phi)$ *and* $\deg_i(\phi)$ *are defined accordingly.*

Definition 5.1.6 (Ramification index). *Let K be a perfect field. Let $\phi : C_1 \to C_2$ be a non-constant morphism between smooth curves defined over K. Let $P \in C_1$. The ramification index of ϕ at P is defined as*

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)})$$

where $t_{\phi(P)} \in K(C_2)$ is a uniformizer *at $\phi(P)$ (i.e.* $\mathrm{ord}_{\phi(P)}(t_{\phi(P)}) = 1$*).*

An application of these quantities is the study of the number of preimages of a point. For example, the degree is equal to the sum of ramification indices at the preimages of any point, and the separable degree is equal to the number of preimages of a point except for a finite number of them [244, Proposition 2.6].

5.1.2 Divisors of algebraic curves

The group of divisors of a curve is the free abelian group generated by its geometric points. It is a powerful tool to study the curve itself.

Definition 5.1.7 (Divisor [244, Section II.3], [128, Section II.6])**.** *Let K be a perfect field and C an algebraic curve defined over K. A* divisor *D of C is a formal finite sum of geometric points of C with integer coefficients:*

$$D = \sum_{P \in C(\overline{K})} n_P(P) \ ,$$

where only a finite number of coefficients $n_P \in \mathbb{Z}$ are non-zero. The support of a divisor is the set of points with non-zero coefficients:

$$\mathrm{supp}(D) = \left\{ P \in C(\overline{K}) \mid n_P \neq 0 \right\} \ .$$

The degree of a divisor is the sum of its coefficients:

$$\deg(D) = \sum_{P \in C(\overline{K})} n_P \ .$$

The Galois group of K naturally acts on divisors and we say that a divisor is rational over K if it is invariant by this action.

Definition 5.1.8 (Group of divisors)**.** *Let K be a perfect field and C an algebraic curve defined over K. The group of divisors on C is denoted by* $\mathrm{Div}(C)$*. The subgroup of divisors of degree* 0 *is denoted by* $\mathrm{Div}^0(C)$*.*

If $f \in \overline{K}(C)^*$ is a non-zero function on C, then one can associate a divisor with it.

Definition 5.1.9 (Divisor of a function)**.** *Let K be a perfect field and C an algebraic curve defined over K. Let $f \in \overline{K}(C)^*$ be a non-zero function on C. The divisor of f, denoted by* $\mathrm{div}(f)$*, is defined as*

$$\mathrm{div}(f) = \sum_{P \in C(\overline{K})} \mathrm{ord}_P(f)(P) \ ,$$

where $\mathrm{ord}_P(f)$ *is the order of f at P.*

These divisors form the set of *principal* divisors, which is easily seen to be a subgroup of $\mathrm{Div}(C)$.

Definition 5.1.10 (Principal divisors)**.** *Let K be a perfect field and C an algebraic curve defined over K. The group of divisors of the form* $\mathrm{div}(f)$ *for $f \in \overline{K}(C)^*$ is called the group of principal divisors and denoted by*

$$\mathrm{Prin}(C) = \left\{ \mathrm{div}(f) \in \mathrm{Div}(C) \mid f \in \overline{K}(C)^* \right\} \ .$$

We can then define an equivalence relation using them.

Definition 5.1.11 (Linear equivalence)**.** *Let K be a perfect field and C an algebraic curve defined over K. Let D and D' be two divisors on C. They are said to be linearly equivalent if $D - D' \in \mathrm{Prin}(C)$. This is an equivalence relation that we denote by*

$$D \sim D' \ .$$

And so we can define the quotient of the group of divisors by the subgroup of principal divisors: the *Picard group*.

Definition 5.1.12 (Picard group)**.** *The quotient of* $\mathrm{Div}(C)$ *by* $\mathrm{Prin}(C)$*, denoted by* $\mathrm{Pic}(C)$*, is called the divisor class group, or the Picard group, of* C*.*

For a principal divisor, the degree is always zero.

Proposition 5.1.13 ([244, Proposition II.3.1], [128, Corollary II.6.10])**.** *Let* K *be a perfect field and* C *a smooth curve defined over* K*. Let* $f \in \overline{K}(C)^*$ *be a non-zero function on* C*. Then*

1. $\mathrm{div}(f) = 0$ *if and only if* $f \in \overline{K}$*;*
2. $\deg(\mathrm{div}(f)) = 0$.

Hence, for a smooth curve, the group of principal divisors is in fact a subgroup of the group of divisors of degree zero. Therefore, we can also define the quotient of the zero degree part of the groups of divisors by the subgroup of principal divisors.

Definition 5.1.14. *Let* K *be a perfect field and* C *a smooth curve defined over* K*. We denote by* $\mathrm{Pic}^0(C)$ *the quotient of* $\mathrm{Div}^0(C)$ *by* $\mathrm{Prin}(C)$*.*

It is a general fact that this quotient group can be given the structure of an algebraic variety: the *Jacobian variety*. In the case of elliptic curve, its description as a variety is surprisingly simple.

Proposition 5.1.15 ([244, Proposition III.3.4], [128, Example II.6.10.2])**.** *Let* K *be a perfect field and* E *an elliptic curve defined over* K*. Then the following map is an isomorphism:*

$$\begin{aligned} E(\overline{K}) &\to \mathrm{Pic}^0(E) \ , \\ P &\mapsto [(P) - (O_E)] \ . \end{aligned}$$

And the following corollary is very useful.

Corollary 5.1.16 ([244, Corollary III.3.5])**.** *Let* K *be a perfect field and* E *an elliptic curve defined over* K*. Let* $D = \sum_{P \in E(\overline{K})} n_P(P)$*,* $n_P \in \mathbb{Z}$ *almost all zero, be a divisor on* E*. Then* D *is principal if and only if*

1. $\deg D = 0$*,*
2. $\sum_{P \in \overline{K}(E)} [n_P]P = O_E$.

To conclude this subsection, we should define a few more tools relating morphisms and divisors which are useful to define *pairings* on elliptic curves.

A function can be evaluated at a divisor if their support are disjoint as follows.

Definition 5.1.17 (Evaluation of a function at a divisor)**.** *Let* K *be a perfect field and* C *an algebraic curve defined on* K*. If* $f \in K(C)$ *and* $D = \sum_{P \in C(\overline{K})} n_P(P)$ *with* $\mathrm{supp}(D) \cap \mathrm{supp}(\mathrm{div}(f)) = \emptyset$*, then we define the value of* f *at* D *as*

$$f(D) = \prod_{P \in C(\overline{K})} f(P)^{n_P} \ .$$

This operation is well-behaved with regard to the group law on divisors.

Definition 5.1.18. *Let K be a perfect field. Let $\phi : C_1 \to C_2$ be a non-constant morphism between algebraic curves defined over K. Different homomorphisms between the divisors of the curves can be defined from a morphism between them:*

- $\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1),\ Q \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)P$,
- $\phi_* : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2),\ P \mapsto \sum_P \phi(P)$.

Proposition 5.1.19 ([244, Proposition II.3.6])**.** *Let K be a perfect field. Let $\phi : C_1 \to C_2$ be a non-constant morphism between algebraic curves defined over K. Then*

- $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f))$,
- $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi_*(f))$,
- $f(\phi_*(D)) = \phi^*(f)(D)$,
- $f(\phi^*(D)) = \phi_*(f)(D)$.

Proposition 5.1.20 (Weil's reciprocity [244, Exercise 2.11], [19, Theorem IX.3])**.** *Let K be a perfect field and C an algebraic curve defined over K. Let $f, g \in \overline{K}(C)^*$ be two functions with disjoint supports. Then*

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)) \ .$$

5.1.3 Pairings

There exist important bilinear applications, both for theoretical questions and practical applications, which can be defined on elliptic curves: *pairings*.

Definition 5.1.21 (Pairing)**.** *Let A be a ring and M, N and L A-modules. A pairing is an A-bilinear map from $M \times N$ into L (or equivalently an A-linear from $M \otimes_A N$ into L).*

We first define the *Tate pairing*. Let K be a perfect field and E an elliptic curve defined over K. Let $m \geq 2$ be an integer co-prime to the characteristic of K. Let $P \in E(K)[m]$ and $Q \in E(K)/mE(K)$. There exists a function $f \in K(E)$ such that

$$\mathrm{div}(f) = m(P) - m(O_E) \ .$$

We now choose a representative of Q in $E(K)$ and a divisor $D \sim (Q) - (O_E)$ with support disjoint from that of $\mathrm{div}(f)$ so that we can compute $f(D)$.

Definition 5.1.22 (Tate pairing)**.** *Let K be a perfect field and E an elliptic curve defined over K. Let $m \geq 2$ be an integer co-prime to the characteristic of K. Let $P \in E(K)[m]$ and $Q \in E(K)/mE(K)$. The Tate pairing is defined as above:*

$$\langle P, Q \rangle_m = f(D) \in K^*/(K^*)^m \ .$$

It can be shown that this map is well defined (up to m-th powers) and does not depend on the different choices we have to make [19, Lemma IX.4], [19, Lemma IX.5].

Theorem 5.1.23 ([19, Theorem IX.7])**.** *Let K be a perfect field and E an elliptic curve defined over K. Let $m \geq 2$ be an integer co-prime to the characteristic of K. Let $P, P_1, P_2, Q, Q_1, Q_2 \in E(K)$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$. The Tate pairing satisfies the following properties:*

1. *Bilinearity: $\langle P_1 + P_2, Q \rangle_m = \langle P_1, Q \rangle_m \langle P_2, Q \rangle_m$ and $\langle P, Q_1 + Q_2 \rangle_m = \langle P, Q_1 \rangle_m \langle P, Q_2 \rangle_m$.*

2. *Non-degeneracy: if K is finite and contains the m-th roots of unity, then the Tate pairing is non-degenerate.*

3. *Galois invariance: $\langle \sigma P, \sigma Q\rangle_m = \sigma\langle P, Q\rangle_m$.*

The bilinearity is a consequence of Weil's reciprocity. A proof of the non-degeneracy is given in [104]. A more elementary and specific one has been devised by Heß [130].

We now define the *Weil pairing*. With the same notation as before, let $P \in E[m]$ be an m-torsion point. There exists a function $f \in K(E)$ such that:

$$\operatorname{div}(f) = m(P) - m(O_E) \ .$$

Multiplication by m is a surjective map on $E(\overline{K})$, so we can choose P' such that $[m]P' = P$. There exists a function $g \in \overline{K}(E)$ such that

$$\operatorname{div}(g) = [m]^*((P) - (O_E)) = \sum_{R\in E[m]} (P' + R) - (R) \ ,$$

because $[m^2]P' = O_E$. Furthermore

$$\operatorname{div}(g \circ \tau_Q) = \operatorname{div}(\tau_Q^* g) = \tau_Q^* \operatorname{div}(g) = \operatorname{div}(g) \ ,$$

so that $(g \circ \tau_Q / g) \in K$. Finally

$$\operatorname{div}(f \circ [m]) = \operatorname{div}([m]^* f) = [m]^* \operatorname{div}(f) = m \operatorname{div}(g) = \operatorname{div}(g^m)$$

and so $f \circ [m] = g^m$ up to a non-zero multiplicative constant. If $Q \in E[m]$ and $S \in E(\overline{K})$, then $g((S+Q))^m = f([m](S+Q)) = f([m](S)) = g((S))^m$, so $\frac{g(S+Q)}{g(S)}$ is an m-th root of unity.

Definition 5.1.24 (Weil pairing)**.** *Let K be a perfect field and E an elliptic curve defined over K. Let $m \geq 2$ be an integer co-prime to the characteristic of K. Let $P, Q \in E(K)[m]$ be m-torsion points. We define the Weil pairing as above:*

$$e_m(P, Q) = \frac{g(S+Q)}{g(S)} \ .$$

Theorem 5.1.25 ([19, Theorem IX.10], [244, Proposition III.8.1])**.** *Let K be a perfect field and E an elliptic curve defined over K. Let $m \geq 2$ be an integer co-prime to the characteristic of K. Let $P, P_1, P_2, Q, Q_1, Q_2 \in E(K)[m]$ and $\sigma \in \operatorname{Gal}(\overline{K}/K)$. The Weil pairing satisfies the following properties:*

1. *Bilinearity:*

$$\begin{aligned} &e_m(P_1 + P_2, Q) = e_m(P_1, Q) e_m(P_2, Q) \ , \\ &\text{and } e_m(P, Q_1 + Q_2) = e_m(P, Q_1) e_m(P, Q_2) \ . \end{aligned}$$

2. *Alternance: $e_m(P, Q) = e_m(Q, P)^{-1}$.*

3. *Non-degeneracy: if $E(K)$ contains $E[m]$, then $e_m(P, Q) \neq 1$.*

4. *Galois invariance: $e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q)$.*

The Weil pairing and the Tate pairing are closely related. In fact, the following proposition is often used to define the Weil pairing.

Proposition 5.1.26 ([244, Remark III.8.5]). *Let K be a perfect field and E an elliptic curve defined over K. Let $m \geq 2$ be an integer co-prime to the characteristic of K. Let $P, Q \in E(K)[m]$.*

$$e_m(P,Q) = \langle P,Q\rangle_m / \langle Q,P\rangle_m \ ,$$

up to an m-th power.

Such a definition has the benefit to be more computational. The Tate pairing can indeed be efficiently computed in polynomial time using Miller's algorithm [203] that we now describe.

With the same notation as before, let $P \in E(K)[m]$ and $Q \in E(K)$. If we denote by f_i a function (unique up to a multiplicative constant) such that $\mathrm{div}(f_i) = i(P) - ([i]P) - (i-1)(O_E)$, then we need to compute f_m. According to the following proposition we can do it explicitly using a standard binary exponentiation.

Proposition 5.1.27 ([19, Lemma IX.17]). *Let l and v be the lines going through $\{[i]P, [j]P\}$ and $\{[i+j]P, O_E\}$. Then $f_{i+j} = f_i f_j l/v$.*

The corresponding algorithm is given in Algorithm 5.1.

Algorithm 5.1: Miller's algorithm

Input: $P \in E(K)[m]$ and $Q \in E(K)$
Output: $\langle P,Q\rangle_m$

$S \in_R E(K)$
$Q' \leftarrow Q + S$
$T \leftarrow P$
$f \leftarrow 1$
$i \leftarrow \lfloor \log m \rfloor - 1$
while $i \geq 0$ **do**
  Compute l and v to double T
  $T \leftarrow [2]T$
  $f \leftarrow f^2 l(Q')v(S)/l(S)v(Q')$
  if $b_i = 1$ **then**
    Compute l and v to add T and P
    $T \leftarrow T + P$
    $f \leftarrow f l(Q')v(S)/l(S)v(Q')$
  $i \leftarrow i - 1$
return f

5.1.4 Reduction of elliptic curves

Let K be a local field with uniformizer π and residue field k. Let E be an elliptic curve defined over K. There exist Weierstraß equations for E with integral coefficients and so it is possible to define the reduction $\widetilde{E}$ modulo π of E from such equations. The resulting curve is obviously potentially singular. In fact, it is if and only if the discriminant of the chosen Weierstraß equation is divisible by π. Moreover, there exists a "best" Weierstraß equation to use for reduction: it is called the minimal Weierstraß equation.

Proposition 5.1.28 ([244, Proposition VII.1.3]). *Let K be a local field with uniformizer π. Let E be an elliptic curve defined over K. Then E has a minimal Weierstraß equation, i.e. an equation with integral coefficients such that the valuation at π of its discriminant is minimal.*

Definition 5.1.29 ([244, Section VII.5]). *Let K be a local field. Let E an elliptic curve defined over K and $\widetilde{E}$ be the reduction of a minimal Weierstraß equation. We say that E has*

1. *good reduction if $\widetilde{E}$ is smooth,*
2. *bad reduction if $\widetilde{E}$ is singular.*

We say that E has potential good reduction if it has good reduction over an extension of K.

Reduction can also be defined for points $P \in E(K)$ in the same way. The next proposition shows that the corresponding map is injective for m-torsion points where m is co-prime to the characteristic of the residue field.

Proposition 5.1.30 ([244, Proposition VII.3.1]). *Let K be a local field with uniformizer π. Let $m \geq 1$ be an integer co-prime to the characteristic of K. Let E be an elliptic curve defined over K with good reduction. Let $\widetilde{E}$ be a non-singular reduction of E. Then the reduction map*

$$E(K)[m] \to \widetilde{E}(k)[m]$$

is injective.

Similarly, reduction can be defined for isogenies. Using the Weil pairing and the Isogeny theorem [244, Theorem III.7.7], which is valid over finite fields and number fields, it can be shown that reduction from a number field preserves degrees of isogenies.

Proposition 5.1.31 ([245, Proposition II.4.4]). *Let L be number field and $\mathfrak{p}$ a prime ideal of L. Let E_1 and E_2 be two elliptic curves with good reduction at $\mathfrak{p}$ and $\widetilde{E_1}$ and $\widetilde{E_2}$ their reductions at $\mathfrak{p}$. Then the reduction map*

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\widetilde{E_1}, \widetilde{E_2})$$

preserves degrees and is injective.

As far as endomorphisms are concerned, we have much more precise information.

Theorem 5.1.32 ([68], [160, Theorem 13.4.12]). *Let L be a number field and $\mathcal{O}$ an order in K an imaginary quadratic number field. Let E be an elliptic curve defined over L with endomorphism ring $\mathrm{End}(E) \simeq \mathcal{O}$. Let $\mathfrak{p}$ be a prime of L over the rational prime p. Suppose that E has good reduction $\widetilde{E}$ at $\mathfrak{p}$.*

Then $\widetilde{E}$ is supersingular if and only if p is inert or ramifies in K.

Otherwise, write down the conductor f of $\mathcal{O}$ as $f = p^r f_0$ where $\gcd(p, f_0) = 1$. Then $\mathrm{End}(\widetilde{E}) \simeq \mathbb{Z} + f_0\mathcal{O}_K$, the order of conductor f_0 in K. In particular, if p splits and $p \nmid f$, then the reduction map $\mathrm{End}(E) \to \mathrm{End}(\widetilde{E})$ is an isomorphism.

5.2 Elliptic curves over the complex numbers

In this section we present the basic theory of elliptic curves over the complex numbers, as well as its links with the theory of complex tori, lattices and binary quadratic forms. All curves are supposed to be defined over the complex numbers.

5.2.1 Complex tori

Over the complex numbers, a general Weierstraß equation can be simplified to yield an equivalent equation of the form[2]

$$E: \ y^2 = x^3 + ax + b \ .$$

Two important invariants have then simple definitions.

Definition 5.2.1 (Discriminant)**.** *Let E be a curve given by the Weierstraß equation*

$$E: \ y^2 = x^3 + ax + b \ .$$

The discriminant of the Weierstraß equation is given by

$$\Delta = -16(4a^3 + 27b^2) \ .$$

E is non-singular, and so is an elliptic curve, if and only if $\Delta \neq 0$.

Definition 5.2.2 (j-invariant)**.** *Let E be an elliptic curve given by the Weierstraß equation*

$$E: \ y^2 = x^3 + ax + b \ .$$

The j-invariant of E is given by

$$j = -1728\frac{(4a)^3}{\Delta} \ .$$

Two elliptic curves are isomorphic if and only if they have the same j-invariant.

We are now going to give another description of elliptic curves over the complex numbers.

Definition 5.2.3 (Lattice)**.** *A lattice Λ in $\mathbb{C}$ is a $\mathbb{Z}$-module of rank 2 such that $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{C}$.*
We denote by $\mathcal{L}$ be the set of lattices in $\mathbb{C}$.

Definition 5.2.4 (Multiplier ring)**.** *Let Λ be a lattice. The multiplier ring of Λ, denoted by $R(\Lambda)$, is the set $\{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$.*

The quotient of $\mathbb{C}$ by a lattice is called a complex torus.

Definition 5.2.5 (Complex torus)**.** *Let Λ be a lattice in $\mathbb{C}$. We say that $\mathbb{C}/\Lambda$ is a complex torus.*

Such a complex torus is depicted in Figure 5.1. It is a basic fact that two complex tori are isomorphic if and only if the corresponding lattices are homothetic.

We now relate lattices in $\mathbb{C}$ with the *Poincaré upper halfplane* through bases of a special form. Let Λ be a lattice in $\mathbb{C}$ and (ω_1, ω_2) a basis of Λ such that $\tau = \frac{\omega_1}{\omega_2}$ satisfies $\Im(\tau) > 0$. Then Λ is equivalent up to homothety to

$$\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z} \ .$$

The value of τ depends on the initial choice of the basis, but it is easy to describe the equivalence classes of such numbers.

Definition 5.2.6 (Poincaré upper halfplane)**.** *We denote by $\mathbb{H}$ the Poincaré upper halfplane, i.e. the set $\mathbb{H} = \{x \in \mathbb{C} \mid \Im(x) > 0\}$.*

[2]This is true as soon as the characteristic is different from 2 and 3.

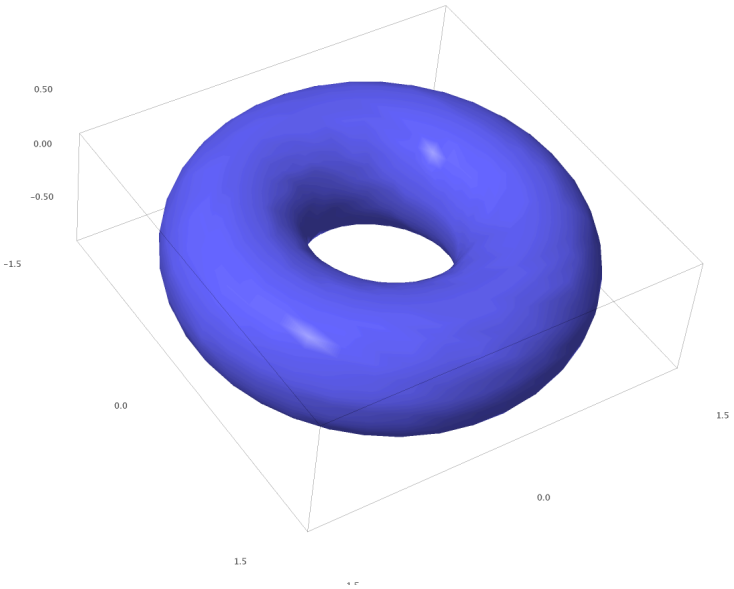


Figure 5.1: A complex torus of dimension 1

Definition 5.2.7 (Modular group)**.** *We denote by* $\mathrm{SL}_2(\mathbb{Z})$ *the* special linear group *over* $\mathbb{Z}$*, i.e.*

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}) \mid \det(\mathbb{Z}) = 1 \right\} \ .$$

We denote by $\Gamma(1)$ *the* modular group

$$\Gamma(1) = \mathrm{SL}_2(\mathbb{Z}) / \{\pm 1\} \ .$$

An action of the modular group on points of the Poincaré upper halfplane is defined as follows. A matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ acts on $\tau \in \mathbb{H}$ as

$$\gamma\tau = \frac{a\tau + b}{c\tau + d} \ .$$

Proposition 5.2.8 ([245, Lemma I.1.2])**.** *The following map is a bijection*

$$\begin{aligned} \Gamma(1)\backslash\mathbb{H} &\to \mathcal{L}/\mathbb{C}^* \ , \\ \tau &\mapsto \Lambda_\tau \ . \end{aligned}$$

In fact, a representative of each coset in $\Gamma(1)\backslash\mathbb{H}$ can be chosen in the so-called *fundamental domain.*

Proposition 5.2.9 ([245, Lemma I.1.5])**.** *Let* $\mathcal{F}$ *denote the fundamental domain*

$$\mathcal{F} = \{\tau \in \mathbb{H} \mid |\tau| \geq 1 \text{ and } |\Re(\tau)| \leq 1/2\} \ .$$

Then for every $\tau \in \mathbb{H}$*, there exists* $\gamma \in \Gamma(1)$ *such that* $\gamma\tau \in \mathcal{F}$*.*

Using the *Weierstraß $\wp$-function*, it is easily seen that a complex torus is analytically isomorphic to an elliptic curve.

Definition 5.2.10 (Weierstraß $\wp$-function [244, Section VI.3])**.** *Let Λ be a lattice in $\mathbb{C}$. The Weierstraß $\wp$-function (relative to Λ) is defined by*

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda,\ \omega\neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) \ .$$

Definition 5.2.11 (Eisenstein series [244, Section VI.3])**.** *Let Λ be a lattice in $\mathbb{C}$ and $k > 1$ be a positive integer. The Eisenstein series of weight $2k$ (for Λ) is defined by*

$$G_{2k}(\Lambda) = \sum_{\omega\in\Lambda,\omega\neq 0} \frac{1}{\omega^{2k}} \ .$$

Proposition 5.2.12 ([244, Proposition VI.3.6])**.** *Let Λ be a lattice in $\mathbb{C}$ and denote by g_2 and g_3 the quantities*

$$\begin{aligned} g_2(\Lambda) &= 60G_4(\Lambda) \ , \\ g_3(\Lambda) &= 140G_6(\Lambda) \ . \end{aligned}$$

Then $g_2^3 - 27g_3^2 \neq 0$ and the curve defined by

$$E: \ y^2 = 4x^3 - g_2x - g_3$$

is an elliptic curve. Moreover the map

$$\begin{aligned} \mathbb{C}/\Lambda &\to E(\mathbb{C}) \ , \\ z &\mapsto [\wp(z) : \wp'(z) : 1] \ , \end{aligned}$$

is a complex analytic isomorphism of complex Lie groups.

The discriminant and the j-invariant of the curve corresponding to $\tau \in \mathbb{H}$ can then be defined as complex analytic functions:

$$\begin{aligned} \Delta(\tau) &= g_2^3(\tau) - 27g_3(\tau)^2 \ , \\ j(\tau) &= 1728\frac{g_2(\tau)^3}{\Delta(\tau)} \ . \end{aligned}$$

The converse of this statement is harder to prove and is called the uniformization theorem for elliptic curves over $\mathbb{C}$. It involves studying the j-invariant as a *modular function*.

Theorem 5.2.13 (Uniformization [245, Corollary I.4.3])**.** *Let a and b be complex numbers such that $4a^3 + 27b^2 \neq 0$. Then there exists a lattice Λ in $\mathbb{C}$ such that $g_2(\Lambda) = -4a$ and $g_3(\Lambda) = -4b$. Hence, the map*

$$\begin{aligned} \mathbb{C}/\Lambda &\to E: \ y^2 = x^3 + ax + b \ , \\ z &\mapsto [\wp(z,\Lambda) : \frac{1}{2}\wp'(z,\Lambda) : 1] \ , \end{aligned}$$

is a complex analytic isomorphism.

Finally, we have an equivalence of categories between complex tori and elliptic curves over the complex numbers.

Theorem 5.2.14 ([244, Theorem VI.4.1])**.** *The following maps are bijections:*

1.
$$\{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subset \Lambda_2\} \to \{\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \mid \phi(0) = 0\} \ ,$$
$$\alpha \mapsto \phi_\alpha \ ,$$
defined by passing to the quotient;

2.
$$\{\phi : E_1 \to E_2 \mid \phi(O_{E_1}) = O_{E_2}\} \to \{\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \mid \phi(0) = 0\} \ ,$$
the natural inclusion associating an holomorphic map with an isogeny.

These results are summarized in the following theorem.

Theorem 5.2.15 ([244, Theorem VI.5.3])**.** *The following categories are equivalent:*

1. *elliptic curves over $\mathbb{C}$ up to isomorphism and isogenies;*
2. *elliptic curves over $\mathbb{C}$ up to isomorphism and complex analytic maps sending 0 onto 0;*
3. *lattices in $\mathbb{C}$ up to homothety and multiplication by a complex number.*

5.2.2 Orders in imaginary quadratic fields

Let K be an imaginary quadratic field. Recall that an order is a subring of K which is also a lattice, i.e. a $\mathbb{Z}$-module of rank 2 in this case. Moreover, all orders are subrings of the ring of integers of K, the integral closure of $\mathbb{Z}$ in K.

Proposition 5.2.16. *Let K be an imaginary quadratic field and $\mathcal{O}_K$ its ring of integers. Then $\mathcal{O}_K$ is the maximal order of K. This is the only order of K which is integrally closed. Furthermore, $\mathcal{O}_K$ is a Dedekind ring.*

Proposition 5.2.17 (Conductor [160, Theorem 8.1.3], [61, Lemma 7.2])**.** *Let K be an imaginary quadratic field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}$ an order. Then there exists an integer $f \in \mathbb{N}^*$ such that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$.*

Conversely, every integer $f \in \mathbb{N}^*$ gives a unique order.

Proposition 5.2.18. *Let K be an imaginary quadratic field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}$ an order. Then $\mathcal{O}$ is noetherian and of Krull dimension 1, i.e. all non-zero prime ideals are maximal.*

Definition 5.2.19 (Fractional ideal)**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. A fractional ideal $\mathfrak{a}$ is a non-zero $\mathcal{O}$-submodule of K such that there exist $\alpha \in K^*$ with $\alpha\mathfrak{a} \subset \mathcal{O}$. The set of fractional ideals is denoted by* $\mathrm{Frac}(\mathcal{O})$.

In particular, the zero ideal is not a fractional ideal, but every non-zero ideal is. As $\mathcal{O}$ is noetherian, its ideals are finitely generated and its fractional ideals are as well.

If Λ is a lattice in K, then its multiplier ring $R(\Lambda)$ is an order in K, and so Λ is a fractional ideal for some order. Conversely, a fractional ideal is a lattice in K. In fact, the fractional ideals of $\mathcal{O}$ are exactly the lattices in K whose multiplier rings are orders containing $\mathcal{O}$. Addition, intersection and multiplication are defined on fractional ideals as they are on usual integral ideals, and they give well defined composition laws. Moreover, we can define the *ideal quotient*, also called *ideal colon*.

Definition 5.2.20 (Ideal quotient)**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two fractional ideals. The ideal quotient, or ideal colon, of $\mathfrak{a}$ and $\mathfrak{b}$, denoted by $(\mathfrak{a} : \mathfrak{b})$, is defined as*

$$(\mathfrak{a} : \mathfrak{b}) = \{\alpha \in K \mid \alpha\mathfrak{b} \subset \mathfrak{a}\} \ .$$

It is also a fractional ideal.

We remark that $R(\mathfrak{a}) = (\mathfrak{a} : \mathfrak{a})$.

Definition 5.2.21 (Proper ideal)**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. A fractional ideal is said to be proper if its multiplier ring is exactly $\mathcal{O}$. The set of proper ideals is denoted by* $\mathrm{Prop}(\mathcal{O})$.

The ring of integers $\mathcal{O}_K$ is the maximal order of K, hence all its fractional ideals are proper.

Definition 5.2.22 (Invertible ideal)**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. A fractional ideal $\mathfrak{a}$ is said to be invertible if there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Moreover, let us define $\mathfrak{a}^{-1}$ as*

$$\mathfrak{a}^{-1} = \{\alpha \in K \mid \alpha\mathfrak{a} \subset \mathcal{O}\} = (\mathcal{O} : \mathfrak{a}) \ .$$

If $\mathfrak{a}$ is invertible, then its inverse is $\mathfrak{a}^{-1}$. The set of invertible ideals is denoted by $\mathrm{Inv}(\mathcal{O})$.

Equivalently, a fractional ideal is invertible if and only if it is projective (as a module).

An invertible ideal $\mathfrak{a}$ must verify $R(\mathfrak{a}) = \mathcal{O}$, i.e. it must be proper, and its inverse[3] $\mathfrak{a}^{-1}$ must verify the same equality $R(\mathfrak{a}^{-1}) = \mathcal{O}$, i.e. it must also be proper. Furthermore, $\mathrm{Frac}(\mathcal{O})$ is a semigroup, $\mathrm{Prop}(\mathcal{O})$ is a semigroup and $\mathrm{Inv}(\mathcal{O})$ is a group.

It is a specific feature to imaginary quadratic fields that proper ideals are always invertible.

Proposition 5.2.23 ([160, Corollary of Theorem 8.1.2], [61, Proposition 7.4])**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. If a fractional ideal is proper, then it is invertible.*

Definition 5.2.24 (Principal ideal)**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. A fractional ideal is said to be principal if there exists $\alpha \in K^*$ such that $\mathfrak{a} = \alpha\mathcal{O}$. The set of principal ideals is denoted by* $\mathrm{PF}(\mathcal{O})$.

The principal ideals are trivially invertible and so $\mathrm{PF}(\mathcal{O})$ is a subgroup of $\mathrm{Inv}(\mathcal{O})$.

Definition 5.2.25 (Class groups)**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K.*

The Picard group or class group of $\mathcal{O}$ is defined as

$$\mathrm{Pic}(\mathcal{O}) = \mathrm{Inv}(\mathcal{O})/\,\mathrm{PF}(O) \ ,$$

and its cardinality, the class number, by $h(\mathcal{O})$.

The proper class semigroup of $\mathcal{O}$ is defined as

$$\mathrm{Cl}^{prop}(\mathcal{O}) = \mathrm{Prop}(\mathcal{O})/\,\mathrm{PF}(\mathcal{O}) \ ,$$

and its cardinality, the proper class number, by $H^{prop}(\mathcal{O})$.

The class semigroup of $\mathcal{O}$ is defined as

$$\mathrm{Cl}(\mathcal{O}) = \mathrm{Frac}(\mathcal{O})/\,\mathrm{PF}(\mathcal{O}) \ ,$$

and its cardinality, the Kronecker class number, by $H(\mathcal{O})$.

[3] We use the term inverse even though $\mathfrak{a}$ could be non-invertible.

As every fractional ideal of $\mathcal{O}$ is proper and so invertible for its multiplier ring, we get the following proposition.

Proposition 5.2.26. *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K.*

$$H(\mathcal{O}) = \sum_{\mathcal{O} \subset \mathcal{O}' \subset K} h(\mathcal{O}') \ .$$

Furthermore, for the maximal order, the fractional ideals are automatically proper, whence the following proposition.

Proposition 5.2.27. *Let K be an imaginary quadratic field and $\mathcal{O}_K$ its ring of integers. Then* $\mathrm{Pic}(\mathcal{O}_K) = \mathrm{Cl}(\mathcal{O}_K)$ *and* $h(\mathcal{O}_K) = H(O_K)$.

Finally, the Picard group of an order can be described as a subgroup of the full class group of K. First, we can restrict ourselves to the classes of ideals co-prime to the conductor.

Proposition 5.2.28 ([160, Theorem 8.1.4], [61, Lemma 7.18])**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ the order of conductor f in K. Let $\mathfrak{a}$ be a non-zero integral ideal of $\mathcal{O}$ co-prime to f. Then $\mathfrak{a}$ is proper.*

We denote by $\mathrm{Frac}(\mathcal{O}, f)$ *(respectively* $\mathrm{PF}(\mathcal{O}, f)$*) the subgroups of* $\mathrm{Frac}(\mathcal{O})$ *generated by integral ideals (respectively principal integral ideals) co-prime to f.*

Proposition 5.2.29 ([160, Theorem 8.1.5], [61, Proposition 7.19])**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ the order of conductor f in K. Then*

$$\mathrm{Pic}(\mathcal{O}) \simeq \mathrm{Frac}(\mathcal{O}, f) / \mathrm{PF}(\mathcal{O}, f) \ .$$

These ideals can then be pulled back to the maximal order of K.

Proposition 5.2.30 ([160, Theorem 8.1.6], [61, Proposition 7.22])**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ the order of conductor f in K. Then*

$$\mathrm{Pic}(\mathcal{O}) \simeq \mathrm{Frac}(\mathcal{O}_K, f) / \mathrm{PF}_{\mathbb{Z}}(\mathcal{O}_K, f) \ ,$$

where $\mathrm{PF}_{\mathbb{Z}}(\mathcal{O}_K, f)$ *is the subgroup of* $\mathrm{Frac}(\mathcal{O}_K)$ *generated by principal ideals $\mathfrak{a}$ of $\mathcal{O}_K$ such that there exist $\alpha \in \mathcal{O}_K$ and $a \in \mathbb{Z}$ with $\mathfrak{a} = \alpha\mathcal{O}_K$, $\alpha \equiv a \pmod{f\mathcal{O}_K}$ and $\gcd(a, f) = 1$.*

We can deduce from the last proposition the classical expression of the class number of $\mathcal{O}$ in terms of the class number of K.

Theorem 3.2.12 ([160, Theorem 8.1.7], [61, Theorem 7.24])**.** *Let K be an imaginary quadratic field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}$ the order of conductor f in K. Denote by Δ the discriminant of K. Then*

$$h(\mathcal{O}) = \frac{f h(\mathcal{O}_K)}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p \mid f} \left(1 - \left(\frac{\Delta}{p}\right) \frac{1}{p}\right) \ ,$$

where $\left(\frac{\cdot}{p}\right)$ is the Kronecker symbol.

5.2.3 Binary quadratic forms

The theory of fractional ideals of orders in quadratic number fields is closely linked to that of binary quadratic forms. The latter one is especially convenient for computations.

Definition 5.2.31 (Binary quadratic form)**.** *A binary quadratic form is an element of* $\mathbb{Z}[X,Y]$ *of the form*

$$f = aX^2 + bXY + cY^2 \ .$$

Its discriminant is $\Delta = b^2 - 4ac$*.*

Definition 5.2.32 (Primitive form)**.** *A binary quadratic form* $f = aX^2 + bXY + cY^2$ *is said to be primitive if* $\gcd(a,b,c) = 1$*.*

Definition 5.2.33 (Definite form)**.** *A binary quadratic form is said to be positive (respectively negative) definite if* $\Delta < 0$ *and* $a > 0$ *(respectively* $a < 0$*).*

We denote by $B(\Delta)$ the set of positive definite forms of discriminant Δ, and by $b(\Delta)$ the subset of primitive forms.

Definition 5.2.34 (Reduced form)**.** *A primitive positive definite form* $f = aX^2 + bXY + cY^2$ *is said to be reduced if* $|b| \leq a \leq c$*, and* $b \geq 0$ *if either* $|b| = a$ *or* $a = c$*.*

It is possible to define an action of $\mathrm{SL}_2(\mathbb{Z})$ on binary quadratic forms, just as for points of the Poincaré upper halfplane

Definition 5.2.35. *Let* $\sigma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *and* $f = aX^2 + bXY + cY^2$ *a binary quadratic form. We define* σf *as*

$$\sigma f = a(pX+qY)^2 + b(pX+qY)(rX+sY) + c(rX+sY)^2 \ .$$

Two binary quadratic forms f *and* g *are said to be (properly) equivalent if there exists* $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ *such that* $\sigma f = g$*.*

Moreover, this action respects the discriminant of the form, its positiveness and the value of $\gcd(a,b,c)$. We also have canonical representatives for each class.

Theorem 5.2.36 ([61, Theorem 2.8], [32, Theorem 5.7.7])**.** *Every primitive positive definite form is equivalent to a unique reduced from.*

We can now define the equivalents of class groups for binary quadratic forms.

Definition 5.2.37. *Let* Δ *be a negative integer such that* $\Delta \equiv 0, 1 \pmod 4$*. The form class group is defined as*

$$\mathrm{Pic}(\Delta) = b(\Delta)/\mathrm{SL}_2(\mathbb{Z}) \ ,$$

and we denote its cardinality, the class number, by $h(\Delta)$*. The form class semigroup is defined as*

$$\mathrm{Cl}(\Delta)^* = B(\Delta)/\mathrm{SL}_2(\mathbb{Z}) \ ,$$

and we denote its cardinality, the Kronecker class number, by $H(\Delta)$*.*

The associated values are then connected by a similar equality.

Proposition 5.2.38 ([232])**.** *Let* Δ *be a negative integer such that* $\Delta \equiv 0, 1 \pmod 4$ *and* d *a positive integer such that* $d^2 | \Delta$ *and* $\Delta/d^2 \equiv 0, 1 \pmod 4$*. Then there is a one-to-one correspondence between the sets* $\{f \in B(\Delta) \mid \gcd(a,b,c) = d\} / \mathrm{SL}_2(\mathbb{Z})$ *and* $b(\Delta/d^2)/\mathrm{SL}_2(\mathbb{Z})$*.*

Corollary 5.2.39. *Let Δ be a negative integer such that $\Delta \equiv 0, 1 \pmod 4$. Then*

$$H(\Delta) = \sum_{d \in \mathbb{N},\ d^2 | \Delta,\ \Delta/d^2 \equiv 0,1 \pmod 4} h(\Delta/d^2) \ .$$

Finally, there is a well defined map between the two different kinds of class groups.

Theorem 5.2.40 ([61, Theorem 7.7], [32, Proposition 8.4.5])**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. Let Δ be the discriminant of $\mathcal{O}$. The following map*

$$b(\Delta) \to \mathrm{Prop}(\mathcal{O}) \ ,$$
$$f = aX^2 + bXY + cY^2 \mapsto \mathbb{Z}a + \mathbb{Z}(-b + \sqrt{\Delta})/2 \ ,$$

is well defined and induces an isomorphism of $\mathrm{Pic}(\Delta)$ *onto* $\mathrm{Pic}(\mathcal{O})$.

Corollary 5.2.41. *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. Let Δ be the discriminant of $\mathcal{O}$. Then*

$$h(\mathcal{O}) = h(\Delta) \ .$$

5.3 Elliptic curves with complex multiplication

In this section we describe the equivalence classes up to isomorphism of complex elliptic curves with complex multiplication by a given order in an imaginary quadratic field. We then define the Hilbert class polynomial and state the main theorem of complex multiplication.

5.3.1 Complex multiplication

Let E be an elliptic curve defined over $\mathbb{C}$ and $\tau \in \mathbb{H}$ an element of the Poincaré upper halfplane such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_\tau$. Then $\mathrm{End}(E) \simeq \mathrm{End}(\Lambda_\tau)$ and we deduce the following result on the structure of $\mathrm{End}(E)$.

Proposition 5.3.1 ([244, Theorem VI.5.5])**.** *Let E be an elliptic curve defined over $\mathbb{C}$ and $\tau \in \mathbb{H}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_\tau$. Then:*

1. *if τ is quadratic, then* $\mathrm{End}(E)$ *is an order in* $\mathbb{Q}(\tau)$*;*
2. *otherwise* $\mathrm{End}(E) = \mathbb{Z}$.

A lattice arising from a quadratic number τ is depicted in Figure 5.2.

We are interested in the first case, and more precisely in classifying curves (up to isomorphism) having complex multiplication by a given order $\mathcal{O}$ in an imaginary quadratic field K (with a fixed embedding into $\mathbb{C}$).

Definition 5.3.2. *Let $\mathcal{O}$ be an order in K an imaginary quadratic field. We denote by $\mathcal{E}ll(\mathcal{O})$ the set of elliptic curves defined over $\mathbb{C}$ such that* $\mathrm{End}(E) \simeq \mathcal{O}$.

From the results of Subsection 5.2.1, this set can also be described as the set of lattices in $\mathbb{C}$ with multiplier ring $\mathcal{O}$. For any such lattice there exists $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subset K$ and so we can choose Λ to be a fractional ideal of $\mathcal{O}$. Every such elliptic curve then comes from a proper fractional ideal of $\mathcal{O}$, i.e. we have a well defined map $\mathcal{E}ll(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O})$ which is easily seen to be injective and surjective. We can even explicitly give an action of $\mathrm{Prop}(\mathcal{O})$ on $\mathcal{E}ll(\mathcal{O})$ as follows.

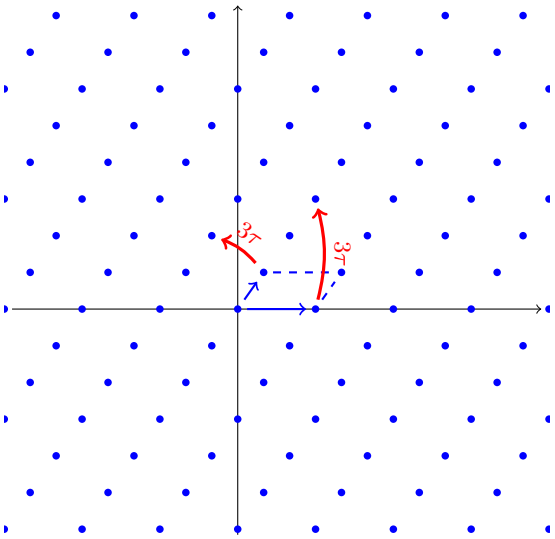


Figure 5.2: The lattice corresponding to $\tau = \frac{1+i\sqrt{2}}{3}$

Definition 5.3.3. *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. Let $E \in \mathcal{E}ll(\mathcal{O})$ and Λ a lattice in $\mathbb{C}$ such that $E \simeq E_\Lambda$. Let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$. We define $\mathfrak{a} * E$ by*

$$\mathfrak{a} * E = E_{\mathfrak{a}^{-1}\Lambda} \ .$$

The following proposition summarizes the above discussion.

Proposition 5.3.4 ([245, Proposition II.1.2])**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. Then there is a simply transitive action of* $\mathrm{Pic}(\mathcal{O})$ *on $\mathcal{E}ll(\mathcal{O})$. In particular, $\#\mathcal{E}ll(\mathcal{O}) = h(\mathcal{O})$.*

5.3.2 Hilbert class polynomial

Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ be an automorphism of $\mathbb{C}$ and E an elliptic curve defined over $\mathbb{C}$. We can define E^σ by letting σ act on the coefficients of a Weierstraß equation for E. In particular, the j-invariants of the two conjugated curves then verify $j(E^\sigma) = j(E)^\sigma$.

But σ also induces an isomorphism $\mathrm{End}(E^\sigma) \simeq \mathrm{End}(E)$. So, if K is an imaginary quadratic field (considered as a subfield of $\mathbb{C}$), $\mathcal{O}$ an order in K and E an elliptic curve defined over $\mathbb{C}$ with $\mathrm{End}(E) \simeq \mathcal{O}$, then $\mathrm{End}(E^\sigma) \simeq \mathcal{O}$.

Definition 5.3.5 (Hilbert class polynomial)**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. The* Hilbert class polynomial *$H_\mathcal{O}(X)$ of $\mathcal{O}$ is defined as*

$$H_\mathcal{O}(X) = \prod_{E \in \mathcal{E}ll(\mathcal{O})} (X - j(E)) \ .$$

There is only a finite number of elliptic curves defined over $\mathbb{C}$ with a given order as endomorphism ring, so $H_\mathcal{O}$ is well defined. The above discussion shows that $H_\mathcal{O}(X)$ has rational coefficients. In fact, it can be shown that the j-invariant of a complex elliptic curve with complex multiplication is an algebraic integer and thus that $H_\mathcal{O}(X)$ has integral coefficients.

Theorem 5.3.6 ([245, Theorem II.6.1], [160, Theorem 5.2.4])**.** *Let E be an elliptic curve defined over the complex numbers with complex multiplication. Then $j(E)$ is an algebraic integer.*

There exist three different proofs of this theorem [245, Section II.6]:

1. a complex analytic one, considering j as a modular function;
2. an l-adic one, showing that E must have good reduction at all primes;
3. a p-adic one, showing that E can not have bad reduction at a prime.

Moreover, we remark that $j(E)^\sigma$ only takes a finite number of different values, or more precisely that $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h(\mathcal{O})$.

5.3.3 The main theorem of complex multiplication

According to Proposition 5.2.30, $\mathrm{Pic}(\mathcal{O})$ is isomorphic to

$$\mathrm{Pic}(\mathcal{O}) \simeq \mathrm{Frac}(\mathcal{O}_K, f)/\,\mathrm{PF}_{\mathbb{Z}}(\mathcal{O}_K, f) \ .$$

But $\mathrm{PF}_1(\mathcal{O}_K, f) \subset \mathrm{PF}_{\mathbb{Z}}(\mathcal{O}_K, f) \subset \mathrm{Frac}(\mathcal{O}_K, f)$ where $\mathrm{PF}_1(\mathcal{O}_K, f)$ is the subgroup of $\mathrm{Frac}(\mathcal{O}_K, f)$ generated by principal ideals of the form $\alpha\mathcal{O}_K$ where $\alpha \in \mathcal{O}_K$ is such that $\alpha \equiv 1 \pmod{f\mathcal{O}_K}$. This exactly means that $\mathrm{PF}_{\mathbb{Z}}(\mathcal{O}_K, f)$ is a congruence subgroup[4] and $\mathrm{Pic}(\mathcal{O})$ is a generalized ideal class group[5]. By the Existence theorem [216, Theorem VI.6.1], [145, Theorem 2.2], there exists an abelian extension of K, called the ring class field of $\mathcal{O}$, such that

$$\mathrm{Gal}(H_{\mathcal{O}}/K) \simeq \mathrm{Pic}(\mathcal{O}) \ .$$

Definition 5.3.7 (Ring class field)**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. The ring class field of $\mathcal{O}$, denoted by $H_{\mathcal{O}}$, is defined to be the abelian extension of K such that*

$$\mathrm{Gal}(H_{\mathcal{O}}/K) \simeq \mathrm{Pic}(\mathcal{O}) \ .$$

The algebraic action of $\mathrm{Gal}(H_{\mathcal{O}}/K)$ on $\mathcal{E}ll(\mathcal{O})$ can be explicitly described in terms of the analytic action of $\mathrm{Pic}(\mathcal{O})$. The key to this description is the Kronecker congruence relation.

Proposition 5.3.8 (Kronecker congruence relation [145, Theorem 5.9], [245, Proposition II.4.2], [160, Theorem 10.1.1])**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ the order of conductor f in K. Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_h$ be representatives of the ideal classes in $\mathrm{Pic}(\mathcal{O})$. Let L be an extension of K containing $j(\mathfrak{a}_1), j(\mathfrak{a}_2), \ldots, j(\mathfrak{a}_h)$. Let p be a rational prime co-prime to f, splitting as $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$, which is not one of the finitely many primes of bad reduction of $E_1, E_2, \ldots, E_h$. Then, for any proper fractional ideal $\mathfrak{a} \in \mathrm{Prop}(\mathcal{O})$,*

$$j(\mathfrak{a})^p \equiv j(\mathfrak{p}^{-1}\mathfrak{a}) \pmod{\mathfrak{P}} \ ,$$

where $\mathfrak{P}$ is any prime ideal of L above $\mathfrak{p}\mathcal{O}_K$.

Proof. There is a canonical analytic map coming from the inclusion $\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a}$ and Theorem 5.2.14 states that there exists an isogeny λ such that the following diagram commutes:

[4] This is a notion from class field theory that we will not further describe here.
[5] The same remark as in Footnote 4 applies here.

$$\begin{array}{ccc}
\mathbb{C} & \xrightarrow{\text{id}} & \mathbb{C} \\
\downarrow & & \downarrow \\
\mathbb{C}/\mathfrak{a} & \xrightarrow{\text{can.}} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \\
\downarrow & & \downarrow \\
E(\mathbb{C}) & \xrightarrow{\lambda} & \mathfrak{p} * E(\mathbb{C})
\end{array}$$

There exists an ideal $\mathfrak{b}$ co-prime to $\mathfrak{p}$ such that $\mathfrak{p}\mathfrak{b} = (\alpha)$ is principal. We can then extend our diagram to

$$\begin{array}{ccccccc}
\mathbb{C} & \xrightarrow{\text{id}} & \mathbb{C} & \xrightarrow{\alpha} & \mathbb{C} & \xrightarrow{\text{id}} & \mathbb{C} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathbb{C}/\mathfrak{a} & \xrightarrow{\text{can.}} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} & \xrightarrow{\alpha} & \mathbb{C}/\mathfrak{b}\mathfrak{a} & \xrightarrow{\text{can.}} & \mathbb{C}/\mathfrak{a} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
E(\mathbb{C}) & \xrightarrow{\lambda} & \mathfrak{p} * E(\mathbb{C}) & \xrightarrow{\mu} & \mathfrak{b} * \mathfrak{p} * E(\mathbb{C}) = (\alpha) * E(\mathbb{C}) & \xrightarrow{\nu} & E(\mathbb{C})
\end{array}$$

for some isogeny $\mu : \mathfrak{p} * E \mapsto \mathfrak{b} * \mathfrak{p} * E$ and an isomorphism $\nu : (\alpha) * E \mapsto E$. It follows that the reduction of the composite of these maps is inseparable (this can be seen on differentials — which we will not present here — because $\widetilde{\alpha} = 0$). But the degree of $\mu \circ \nu$ is $\mathrm{N}(\mathfrak{b})$ which is co-prime to p and so the reduction of λ, which is of degree $\mathrm{N}(\mathfrak{p}) = p$, must be purely inseparable. So $\widetilde{\mathfrak{p} * E}$ is isomorphic to $\widetilde{E}^p$ and $j(\widetilde{\mathfrak{p} * E}) = j(\widetilde{E})^p$. □

As a corollary, we remark that we can now lift the Frobenius homomorphism from characteristic p to characteristic zero provided that p splits in K and does not divide the conductor of $\mathcal{O}$.

Proposition 5.3.9 ([245, Proposition II.5.3], [160, Lemma 10.1.1])**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. Let $\mathfrak{a}$ be a proper ideal of $\mathcal{O}$ and E an elliptic curve defined over $L = K(j(E))$ such that there exists an analytic representation*

$$\theta : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C}) \ .$$

For all but a finite number of primes $\mathfrak{p}$ of degree 1 in K, if σ is the Frobenius homomorphism of $\mathfrak{p}$ in L, then we can find an analytic representation

$$\theta' : \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \to E^{\sigma}(\mathbb{C})$$

and an isogeny λ such that the following diagram commutes:

$$\begin{array}{ccc}
\mathbb{C}/\mathfrak{a} & \xrightarrow{\textit{can.}} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \\
\theta \downarrow & & \downarrow \theta' \\
E(\mathbb{C}) & \xrightarrow{\lambda} & E^{\sigma}(\mathbb{C})
\end{array}$$

and such that the reduction of λ modulo any prime of L extending $\mathfrak{p}$ is the p-th Frobenius homomorphism composed with an automorphism of $\widetilde{E^\sigma}$:

$$\widetilde{\lambda} = \pi_p \circ \epsilon \ .$$

If p is prime to the conductor of $\mathcal{O}$, then that automorphism can be chosen to be the identity.

Proof. Following the proof of Proposition 5.3.8, there exists an isogeny in characteristic zero whose reduction is the composite of the p-th Frobenius homomorphism with an automorphism of $\widetilde{E^\sigma}$. If p is prime to the conductor of $\mathcal{O}$, then using Theorem 5.1.32, that automorphism (or rather its inverse) can be lifted back to characteristic zero, changing only the analytic representation in the commutative diagram. □

The Kronecker congruence relation can then be extended to every ideals.

Theorem 5.3.10 ([145, Theorem 3.16], [245, Theorem II.4.3], [160, Theorem 10.3.5])**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$ and $\mathfrak{b}$ a proper ideal whose Artin symbol on the ring class field is σ. Let $\mathfrak{a}$ be a proper ideal. Then*

$$j(\mathfrak{a})^\sigma = j(\mathfrak{b}^{-1}\mathfrak{a}) \ .$$

Proof. We describe the approach of Kedlaya [145, Proposition 4.18]. Let L be an extension large enough to contain $H_\mathcal{O}$ and all the $j(E_i)$. The Chebotarev density theorem ensures the existence of infinitely many primes $\mathfrak{p} \in \mathcal{O}$ whose Artin symbol on L is σ and for which Proposition 5.3.8 applies:

$$j(\mathfrak{a})^\sigma \equiv j(\mathfrak{a})^p \equiv j(\mathfrak{p}^{-1}\mathfrak{a}) \pmod{\mathfrak{P}} \ ,$$

where $\mathfrak{P}$ is any prime ideal of L above $\mathfrak{p}\mathcal{O}_K$. All these primes have the same Artin symbol for $H_\mathcal{O}$. Therefore, by Artin reciprocity, they must lie in the same ideal class, so that $j(\mathfrak{p}^{-1}\mathfrak{a})$ is constant. Then, the Kronecker congruence relation can be lifted back to L to obtain the desired equality. □

Corollary 5.3.11 ([145, Corollary 3.17], [61, Theorem 11.1], [245, Theorem II.4.3], [160, Theorem 10.3.5])**.** *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. Let E be an elliptic curve with complex multiplication by $\mathcal{O}$. Then $K(j(E))$ is the ring class field of $\mathcal{O}$ and $[K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}] = h(\mathcal{O})$.*

Proof. As $[K(j(E)) : K] \leq h(\mathcal{O})$, it is sufficient to prove that $H_\mathcal{O} \subset K(j(E))$.

Following Kedlaya [145, Corollary 3.17] and Cox [61, Theorem 11.1], and according to Cox [61, Proposition 8.20], it is sufficient to show that the unramified rational primes under a prime of degree 1 of $K(j(E))$ are included in those that splits completely in $H_\mathcal{O}$, except for a finite number of them.

But, except for a finite number of them, if $\mathfrak{Q}$ is a prime of degree 1 in $K(j(E))$, then $j(\mathfrak{p}\mathfrak{a})^p \equiv j(\mathfrak{p}\mathfrak{a}) \pmod{\mathfrak{Q}}$, and by the Kronecker congruence relation $j(\mathfrak{p}\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{Q}}$. If we moreover exclude the finite number of primes which divide the discriminant of the j-invariant of the curves with complex multiplication by $\mathcal{O}$, then it implies that $j(\mathfrak{p}\mathfrak{a}) = j(\mathfrak{a})$ and, so, that $\mathfrak{p}$ is principal. Hence, it has a trivial Artin symbol and splits completely in H. Therefore, $H \subset K(j(E))$, whence the equality. □

The main theorem of complex multiplication then gives an explicit analytic description of the algebraic action of the Galois group on torsion points[6].

[6]The next theorem gives the *idèlic* formulation of the main theorem of complex multiplication. Multiplication of fractional ideals by *idèles* will be defined in Subsection 6.2.3.

Theorem 5.3.12 (Main theorem of complex multiplication [245, Theorem II.8.2], [160, Theorem 10.2.3]). *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. Let E be an elliptic curve defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ be an automorphism of $\mathbb{C}$ and $s \in \mathbb{A}_K^*$ an idèle of K such that $(s, K)_{K^{ab}} = \sigma$. Fix a proper ideal $\mathfrak{a}$ of $\mathcal{O}$ and a complex analytic isomorphism*

$$\theta : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C}) \ .$$

Then there exists a unique complex analytic isomorphism

$$\theta' : \mathbb{C}/s^{-1}\mathfrak{a} \to E^{\sigma}(\mathbb{C})$$

such that the following diagram commutes:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{s^{-1}} & K/s^{-1}\mathfrak{a} \\ \theta \downarrow & & \downarrow \theta' \\ E(C) & \xrightarrow{\sigma} & E^{\sigma}(\mathbb{C}) \end{array}$$

5.3.4 Computing the Hilbert class polynomial

To conclude this section, we give the outline of the computation of the Hilbert class polynomial using the so-called *complex analytic method* in Algorithm 5.2.

Algorithm 5.2: Computation of the Hilbert class polynomial

Input: A negative discriminant $\Delta \equiv 0, 1 \pmod 4$
Output: The Hilbert class polynomial $H_\Delta(X)$ of the order of discriminant Δ

```
1 Compute a basis of the order O of discriminant Δ
2 Compute the class group Pic(O) of O
3 foreach a ∈ Pic(O) do
4     Compute j(a) with enough precision
5 Construct H(X) ∈ Z[X] from the complex approximations of its roots
6 return H(X)
```

Computation of the class group in Line 2 can be done working with binary quadratic forms.

Computation of the j-invariant in Line 4 is made considering it as a modular function and using its q-expansion [245, Proposition I.7.4], [160, Section 4.2].

The complex analytic method goes back to the work of Atkin and Morain [9]. A precise description and analysis of a sophisticated version of Algorithm 5.2 can be found in the work of Enge [85]. It is shown that, under the heuristic assumption that the correctness of the algorithm does not depend on rounding errors, the Hilbert class polynomial can be computed in $O(h^{2+\epsilon})$ operations for any $\epsilon > 0$ [85, Corollary 1.3], which is asymptotically optimal.

Finally, it should be noted that other methods have been proposed to compute the Hilbert class polynomial:

- a p-adic method, avoiding numerical instability issues and also asymptotically optimal, first described in the work of Couveignes and Hencocq [60] and analyzed in a paper of Bröker [28];

- methods using the Chinese Remainder Theorem to lift reductions at small primes of the Hilbert class polynomial back to the integers, and methods using an explicit version of the Chinese Remainder Theorem to compute modular reduction of the Hilbert class polynomial at a large prime *without* computing it over the integers, first presented in the works of Chao et al. [45] and Agashe et al. [2].

These methods were subsequently improved, for example in the works of Belding et al. [12] and Sutherland [258, 257].

5.3.5 Shimura's reciprocity law and class invariants

Finally, it should be noted that Shimura described a reciprocity law describing the Galois action on modular functions of higher level, i.e. modular functions invariant by congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. The exact statement of Shimura's reciprocity law in the elliptic case can be found in Lang's textbook [160].

This reciprocity law can then be used to study other class invariants, i.e. values of modular functions generating the ring class field. These class invariants potentially give rise to minimal polynomials with smaller coefficients than the Hilbert class polynomial. It has been shown that the ratio between the heights of the coefficient is at best constant and is bounded as follows.

Proposition 5.3.13 ([31, Theorem 4.1])**.** *The reduction factor for a modular function f satisfies*

$$r(f) \leq 32768/325 \approx 100.82 \ ;$$

if Selberg's eigenvalue conjecture [227] holds, then

$$r(f) \leq 96 \ .$$

This gain could seem useless, but is very important in practice.

The study of class invariants goes back to Weber [281]. They are classically constructed using quotients of the Dedekind η function. Such an approach is described in the works of Gee [114, 115] and Gee and Stevenhagen [116] with a view towards construction of class fields, and of Bröker [27] and Bröker and Stevenhagen [31] with a view towards construction of elliptic curves. More recent developments are due to Schertz [230], Enge and Schertz [87], and Enge and Morain [86]. The double η quotients found in [87] give the best currently known gain of 72, which is close to optimal.

An alternative approach, based on *theta functions* rather than the Dedekind η functions, can be found in the work of Leprévost, Pohst and Uzunkol [170] and Uzunkol's doctoral thesis [269].

To conclude, let us mention that, when computing minimal polynomials of a class invariant, the situation is more involved than with the j-invariant and the representatives of the class group must be normalized to compute the conjugates of the invariant. This can be done with N-systems [230].

5.4 Elliptic curves in cryptography

5.4.1 Curves with a given number of points

In this subsection we outline the different methods to obtain curves with a given number of points over a finite field. Such constructions are naturally useful to generate curves for integer factorization [169] or to build public key cryptosystems based on the difficulty of the discrete logarithm problem [69, 153, 202].

The main approaches to generate elliptic curves for cryptography are as follows [18, Chapter VI], [56, Section 23.4.2.a]:

- Generate a random curve defined over a small base field, compute the roots of its Frobenius endomorphism characteristic equation and deduce its number of points over any extension field — such curves are called *subfield curves*.
- Generate a random curve defined over the target base field and compute its number of points using generic methods, l-adic methods, or p-adic methods, as appropriate.
- Choose an endomorphism ring, look for a suitable base field, compute the corresponding curve using reduction of a class polynomial — these curves are called *CM curves*.

We give a more precise description of the last method [56, Algorithm 18.5], [84, Algorithme 1.15], which is obviously of special interest in this chapter, in Algorithm 5.3. It is called the *CM method*.

Algorithm 5.3: The CM method

Input: A discriminant Δ, the corresponding class polynomial H_Δ, and a desired bitsize
Output: A prime power q and an elliptic curve satisfying the desired properties

1 **repeat**
2 **repeat**
3 Choose a random $q = p^m$ of the desired bitsize
4 **until** *There exist integers t and u such that* $4q = t^2 - u^2\Delta$
5 **until** $n = q + 1 \pm t$ *verifies the desired properties*
6 Compute a root of the reduction modulo q of the class polynomial H_Δ
7 Build the corresponding curve E
8 **return** *(q, E)*

In Line 3, the finite field size $q = p^m$ is chosen such that:

1. p splits completely as $p\mathcal{O}_{\mathbb{Q}(\sqrt{\Delta})} = \mathfrak{p}\mathfrak{p}'$ in $\mathbb{Q}(\sqrt{\Delta})$;
2. p does not divide the conductor of $\mathcal{O}_\Delta$;
3. $\mathfrak{p}$ is of order dividing m.

The test in Line 4 is solved using Cornacchia's algorithm [56, Algorithm 18.4], [18, Algorithm VIII.1] which is described in Algorithm 5.4.

In Line 6, it is often supposed that the class polynomial is precomputed, and so the complexity of its computation is not included in that of the CM method. Usually different class polynomials such as those using double η quotients [87], mentioned in Subsection 5.3.5, are used instead of the Hilbert class polynomial.

In Line 7, the j-invariant of the curves should first be reconstructed from the root of the reduced class polynomial. This is typically done using modular polynomials which are supposed to be precomputed as well and whose computation is at least as difficult as that of class polynomials. Afterwards, there exist at least two non-isomorphic curves over $\mathbb{F}_q$ with the same j-invariant, so the right one should be chosen.

Finally, it should be noted that the curves which can be generated in practice using the CM method will have complex multiplication by an order of relatively small discriminant, which makes them somehow "special" and could lead to specific attacks against the discrete logarithm problem.

Algorithm 5.4: Cornacchia's algorithm

Input: Co-prime positive integers d and n
Output: Positive integers x and y such that $x^2 + y^2 d = n$ if they exist

Compute a solution $n/2 < r_0 < n$ to $r_0^2 \equiv -d \pmod{n}$
Write $n = qr_0 + r_1$ using the Euclidean algorithm
Set $k = 1$
while $r_k \geq \sqrt{n}$ **do**
    Write $r_k = qr_{k+1} + r_{k+2}$ using the Euclidean algorithm
    $k = k + 1$
$s = \sqrt{\frac{n - r_k^2}{d}}$
if $s \in \mathbb{Z}$ **then**
    return *(r_k, s)*
return $\emptyset$

5.4.2 The MOV/Frey–Rück attack

Pairings can be used to transport the discrete logarithm problem from the group of rational points of an elliptic curve into the multiplicative subgroup of a finite field [18, Section V.2], [19, Section IX.9]. There exist subexponential algorithms to compute the discrete logarithm in finite fields. Hence, if the size of the base field does not grow too much, it is much more efficient to solve the discrete logarithm in the target finite field rather than in the original group of points of the elliptic curve. This attack was first proposed by Menezes, Okamoto and Vanstone [192], using the Weil pairing, and by Frey and Rück [104], using the Tate pairing. It is described in Algorithm 5.5. If E is an elliptic curve defined over $\mathbb{F}_q$ of characteristic p and $P \in E(\mathbb{F}_q)$ is of prime order $l \neq p$, Q a multiple of P, we want to compute $\lambda \in \mathbb{Z}$ such that $Q = [\lambda]P$.

Algorithm 5.5: The MOV/Frey–Rück Attack

Input: $P, Q \in E(\mathbb{F}_q)$ such that P is of prime order $l \neq p$ and Q is a multiple of P
Output: $\lambda \in \mathbb{Z}$ such that $Q = [\lambda]P$

Compute k such that $l | q^k - 1$
Compute $S \in E(\mathbb{F}_{q^k})$ such that $e(P, S) \neq 1$
$\zeta_1 \leftarrow e(P, S)$
$\zeta_2 \leftarrow e(Q, S)$
Compute λ such that $\zeta_2 = \zeta_1^\lambda$ in $\mathbb{F}_{q^k}$
return λ

The following proposition shows that the Tate pairing is already faster to compute than the Weil pairing.

Proposition 5.4.1 ([10], [19, Theorem IX.12])**.** *Suppose that $l | \#E(\mathbb{F}_q)$ is prime, $l \neq p$ and $l \not| q - 1$. Then $E[l] \subset E(\mathbb{F}_{q^k})$ if and only if $l | q^k - 1$.*

To compute a Weil pairing, not only must two Tate pairings be computed, but the base field $K(E[m])$ is also larger than $K(\mu_l)$. In practice, more efficient pairing such as the *eta* or the *ate* pairings [131] are used.

It should be remarked that the discrete logarithm can be transported in a potentially strict subfield $\mathbb{F}_{p^{\mathrm{ord}_l(p)}}$ of $\mathbb{F}_{q^k}$ [133]. The integer $\mathrm{ord}_l(p)$ is the smallest integer such that $\mathbb{F}^*_{p^{\mathrm{ord}_l(p)}}$

contains the l-th roots of unity, i.e. the smallest integer such that $l|p^{\mathrm{ord}_l(p)} - 1$, or equivalently the multiplicative order of p in $(\mathbb{Z}/l\mathbb{Z})^*$. Then $k = \mathrm{ord}_l(p)/\gcd(\mathrm{ord}_l(p), n)$ if $q = p^n$. Therefore, it is $\mathrm{ord}_l(p)$ rather than k which should be considered for the difficulty of the discrete logarithm. For cryptographic applications however, the base field is often chosen to be prime so that both these values are equal.

Finally, it should be noted that supersingular curves can not be used for classical public key cryptography.

Proposition 5.4.2 ([192]). *Let E be a supersingular curve. Then its embedding degree k verifies $k \leq 6$.*

This is not a concern for ordinary curves. Indeed, for a random curve the embedding degree is relatively large, typically of the size of l.

Proposition 5.4.3 ([10]). *Let (p, E) be a random couple made of a prime number $p \in [M/2, M]$ and of an elliptic curve defined over $\mathbb{F}_p$ with a prime number of points l. Then the probability that $l|p^k - 1$ for $k \leq (\log p)^2$ is smaller than*

$$c(\log M)^9(\log\log M)^2/M$$

where c is an effectively computable positive constant.

5.4.3 Identity-based cryptography

The idea of identity-based cryptography, proposed by Shamir [235], is to use any binary string (e.g. an email address) as a public key.

A trusted third party, the *Public Key Generator*, publishes a master public key from which all public keys are derived using only public data, and keeps a master secret key to compute the secret keys corresponding to the public data. This scheme allows to encrypt messages, or check digital signatures, without prior distribution of public keys as in the classical public key cryptography model. However, the users must highly trust the Public Key Generator, because it can compute *any* private key, which is not the case in the classical infrastructure. Nonetheless, different variants exist where this pitfall is avoided.

The first instantiation of such an encrypting scheme appeared only many years later: in 2001 in the works of Cocks [52], using quadratic residues, and of Boneh and Franklin [20, 21], using the Weil pairing.

Elliptic curves used in such schemes should not only be resistant to attacks against the discrete logarithm, but also have a small enough embedding degree so that the pairing is efficiently computable. Hence, supersingular curves are natural candidates, but their embedding degrees being always really small may not be sufficient and discards them for several applications. Testing random curves will definitely not yield suitable curves. Using the CM method it is however possible to find ordinary curves which not only have a prime, or nearly prime, number of points, but also have a controlled embedding degree. More precisely, for a given discriminant Δ, we want to find a couple (t, q) where q is a prime power, $t^2 - 4q = \Delta$ and $q + 1 - t$ has large prime divisor l which divides $q^k - 1$ for a suitable k, but not $q^i - 1$ for $i < l$. This last condition can be rephrased as l dividing $\Phi_k(q)$ where Φ_k is the k-th cyclotomic polynomial. To summarize the above discussion, the following conditions are needed:

1. $t^2 - 4q = \Delta$ where q is a prime power;
2. $l \mid q + 1 - t$ where l is a large prime;

3. $l \mid \Phi_k(q)$ where Φ_k is the k-th cyclotomic polynomial.

Different methods and families of curves verifying such conditions have been proposed. Overviews of these constructions can be found in the survey of Freeman, Scott and Teske [101], the Master's thesis of Bisson [17], or the Ph.D. thesis of Naehrig [215].

Chapter 6

Complex multiplication in higher genera

We trusted in the God who created the integers
and created what we call *arithmetic invariants*.

Arithmetic Variety of Moduli for Genus Two
Jun-Ichi Igusa [139]

Contents

The theory of elliptic curves with complex multiplication was developed in the previous chapter. The explicit computation of class polynomials, together with some applications in asymmetric cryptography, were especially highlighted. The purpose of this chapter is to expose the natural generalization of these constructions to higher dimensions: the theory of abelian varieties with complex multiplication and the construction of the corresponding class polynomials. This chapter was first thought to be the very core of this thesis, but — and the reader should obviously have already remarked if he was patient enough to go through the previous chapters of this thesis — its preparation followed a quite different way. Most of the contribution of the author here is bibliographical — except for the description of the non-maximal order case. Nevertheless, a Sage [250] implementation is planned as well[1], and this chapter should be thought as an invitation to future works.

In Section 6.1 we quickly review the general theory of abelian varieties from an algebraic point of view, drawing inspiration from the more than classical textbook of Mumford [213], but also from the freely available course notes of Milne [204]. Contrary to the approach which was undertaken in Chapter 5, in this section, and more generally throughout this chapter, the analytic approach over the complex numbers is blended with the algebraic one, and we enlighten as much as possible the connections between both approaches, much inspired by the textbook of Debarre [65]. For the analytic approach the reader is also referred to the textbook of Birkenhake and Lange [16].

Section 6.2 deals with the theory of fractional ideals in general orders of number fields, a natural continuation to the exposition of Subsection 5.2.2. The situation in higher dimension is far less well understood for non-maximal orders than for maximal orders[2]. Here we stress out how the explicit computation of Picard groups for non-maximal orders can be performed efficiently following the work of Klüners and Pauli [151].

The general theory of complex multiplication is presented in Section 6.3. The content of this section is mainly restricted to characteristic zero which is the main topic of that theory. Nevertheless, some digressions are to be made and we will wander in positive characteristic. The main reference for this section are the textbook of Shimura[3] [238] who originally developed the whole theory, the textbook of Lang [159], and the course notes of Milne[4] [205]. If the reader is more inclined to a schematic approach, we refer him to the seminar notes of Conrad [57] which we will basically not treat here.

Section 6.4 follows the works of Spallek [248], van Wamelen [273], Weng [283] and Streng [252] to describe the construction of classical class polynomials in dimension 2 — the Igusa class polynomials. We show in particular how such a construction can be naturally extended to non-maximal orders. Even though this description of the non-maximal order case is the sole innovation of the author in this part, it is also the theoretical basis of a future Sage [250] implementation.

[1] A draft and quite dysfunctional implementation is available at `http://www.infres.enst.fr/~flori/cm/`. It implements arithmetic for fractional ideals of non-maximal orders, basic computation of Igusa class polynomials, but mainly lacks a full computation of the class group of a non-maximal orders although some bricks are provided.

[2] For example, Waterhouse declared in 1969 [280]: "This theorem is a good example of the way in which facts about maximal orders can be transformed into facts about varieties, and shows why the absence of theory for non-maximal orders makes the general case much more complicated." In the meantime, the interest for such a theory seems to have always been fluctuating and the situation is not much better nowadays.

[3] The reader can also refer to the previous textbook published under the names of Shimura and Taniyama [239]. The content of the first sixteen chapters is exactly the same. Chapter 17 of the first textbook, entitled "The case of non-principal orders" and which does not appear in the second one, might seem important enough with regard to the work presented in the present chapter to have been elected the reference of choice. However, most of its content is essentially treated, although in a different way, in the additional chapters of that second textbook. Therefore, we prefer to refer the reader to that more recent and complete textbook.

[4] As noted by Milne on his webpage, these are actually not course notes, and come in quite unpolished form.

6.1 Abelian varieties

6.1.1 Definition and first properties

Definition 6.1.1 (Abelian variety)**.** *An abelian variety is a connected and complete algebraic group variety.*

For example, elliptic curves are abelian varieties of dimension 1. We usually denote by g the dimension of an abelian variety.

The rigidity lemma [204, Proposition I.1.1], [132, Lemma A.7.1.1] implies that every morphism between abelian varieties is the composite of a homomorphism and a translation and that the group law on an abelian variety is commutative.

Proposition 6.1.2 (Commutativity [213, II.4], [204, Corollary I.1.4], [132, Corollary A.7.1.3])**.** *Let A be an abelian variety. Then its group law is commutative.*

It is a consequence of the more difficult theorem of the cube [213, II.6], [204, Theorem I.5.1], [132, Corollary A.7.2.2] that every abelian variety is projective.

Theorem 6.1.3 (Projectivity [213, II.6], [204, Theorem I.6.4], [132, Corollary A.7.2.1])**.** *Let A be an abelian variety. Then A is projective.*

Hence, we could have just defined abelian varieties as projective varieties with a commutative group law. Nonetheless, this is not the historical approach.

As was the case for elliptic curves, complex abelian varieties are also isomorphic to complex tori. Indeed, over the complex numbers, an abelian variety A is a compact connected complex Lie group and is equipped with the so-called exponential map exp from the tangent space $V \simeq \mathbb{C}^{2g}$ at the zero element to itself [168, 15.4]:

$$\exp : \ V \to A \ .$$

A fundamental fact is that this map is surjective and its kernel is a lattice Λ in V.

Theorem 6.1.4 ([213, I.1], [204, Proposition I.2.1])**.** *Let A be a complex abelian variety and V the tangent space at 0. Then the exponential map is a surjective homomorphism of complex Lie groups with kernel Λ a lattice in V.*

Hence

$$A \simeq V/\Lambda$$

is a complex torus.

As soon as $g > 1$, the converse of this theorem is however not true anymore. All complex tori are indeed not projective anymore [65, Exercice III.3], [242].

6.1.2 Theta functions and Riemann forms

To characterize the complex tori which are projective, and so are actually complex abelian varieties a powerful tool is *theta functions*.

Definition 6.1.5 (Theta function [213, I.3], [65, Définition 1.1])**.** *Let V be a vector space and Λ a lattice in V. A theta function θ associated with Λ is a non-zero function such that there exist linear forms a_λ and constants b_λ for every $\lambda \in \Lambda$ verifying*

$$\theta(z+\lambda) = e^{2i\pi(a_\lambda(z)+b_\lambda)}\theta(z)$$

for every $z \in V$. The theta function is said to be of type $(a_\lambda, b_\lambda)_{\lambda\in\Lambda}$.

A theta function of the form $z \mapsto e^{Q(z)}$ where Q is a polynomial of degree at most two is said to be trivial and two theta functions are said to be equivalent if their quotient is a trivial theta function.

The application

$$\begin{aligned} \Lambda \times V &\to \mathbb{C} \\ (\lambda, z) &\mapsto a_\lambda(z) \end{aligned}$$

can be uniquely extended to an application $a : V \times V \to \mathbb{R}$ which is $\mathbb{R}$-linear in the first variable and $\mathbb{C}$-linear in the second one. The $\mathbb{R}$-bilinear alternating form

$$\omega(x, y) = a(x, y) - a(y, x)$$

is called the *Riemann form* associated with θ.

Proposition 6.1.6 ([65, Propositions IV.1.3, IV.1.5])**.** *With the above notation, the Riemann form ω is real valued, integer valued on Λ and satisfies*

$$\omega(ix, iy) = \omega(x, y)$$

for all x and y in V. Moreover $\omega(x, ix) \geq 0$ for all $x \in V$; we say that ω is positive.

If $\omega(x, ix) > 0$ for all $x \in V$ different from O, then we say that ω is positive definite or non-degenerate.

A Hermitian form, or symmetric sesquilinear form, H is associated with the Riemann form ω:

$$H(x, y) = \omega(x, iy) + i\omega(x, y) \ .$$

It is $\mathbb{C}$-antilinear in the first variable and $\mathbb{C}$-linear in the second one[5]. Then ω is nothing but $\omega = \Im(H)$ and there is a one-to-one correspondence between this two kinds of forms.

It is easily seen that any theta function can be normalized, i.e. multiplied by a trivial theta function, to satisfy

$$\theta(z + \lambda) = \alpha(\lambda) e^{\pi H(\lambda, z) + \frac{\pi}{2} H(\lambda, \lambda)} \theta(z)$$

where $\alpha : \Lambda \to \mathbb{C}_1 = \{z \in \mathbb{C} \mid |z| = 1\}$ is a semicharacter:

$$\alpha(\lambda_1 + \lambda_2) = \alpha(\lambda_1)\alpha(\lambda_2)(-1)^{\omega(\lambda_1, \lambda_2)} \ ,$$

called the multiplicator, or canonical factor of automorphy, of θ. The theta function θ is said to be of type (H, α).

It can be shown that any complex embedding of a complex torus

$$u : V/\Lambda \to \mathbb{P}^n$$

can be described by $n + 1$ theta functions of the same type $u = (\theta_0, \ldots, \theta_n)$. Hence there exists a Riemann form on Λ whose kernel must be trivial, i.e. the form is positive definite, or equivalently non-degenerate.

A theta function θ on the complex torus $X = V/\Lambda$, or the associated hermitian form H and multiplicator α, can be used to construct a line bundle $L(H, \alpha)$ as the quotient of $V \times \mathbb{C}$ by the action of Λ given by

$$\lambda \cdot (z, t) = (z + \lambda, \alpha(\lambda) e^{\pi H(\lambda, z) + \frac{\pi}{2} H(\lambda, \lambda)} t) \ .$$

The Appel–Humbert theorem states that the converse is true: every line bundle can be constructed in this way.

[5] This is the convention of Debarre [65, III.1.1]. Mumford [213, I.2], Lang [159, 1], Birkenhake and Lange [16, Lemma 2.1.7], and Hindry and Silverman [132, A.5] swap x and y, i.e. set $\omega(ix, x)$ positive and $H(x, y) = \omega(ix, y) + i\omega(x, y)$. Shimura [238, I.3.1] sets $\omega(x, ix)$ positive and $2iH(x, y) = \omega(x, iy) + i\omega(x, y)$ which is skew-hermitian. Milne [205, I.2.3] sets $\omega(x, ix)$ positive and $H(x, y) = \omega(x, iy) - i\omega(x, y)$.

Theorem 6.1.7 (Appel–Humbert theorem [213, I.2], [65, Théorème V.5.10]). *Every line bundle on a complex torus is isomorphic to a line bundle $L(H, \alpha)$ where H and α are uniquely determined.*

A theorem of Lefschetz [213, I.3], [65, Théorème VI.3.5] then shows that the existence of a Riemann form on a complex torus is not only a necessary condition to be projective, but also a sufficient one.

Theorem 6.1.8 ([204, Theorem I.2.8]). *A complex torus is projective if and only if it admits a non-degenerate Riemann form.*

We now would like to give a simple description of polarizable complex tori up to isomorphism. In dimension 1, this was achieved by choosing a pleasant basis of the lattice Λ and an associated element τ in the Poincaré upper halfplane. In higher dimension a similar treatment is achieved using the Siegel upper half-space of genus g.

Definition 6.1.9 (Siegel upper half-space). *The Siegel upper half-space $\mathbb{H}_g$ of genus g is the set of $g \times g$ symmetric matrices with imaginary part positive definite:*

$$\mathbb{H}_g = \left\{\Omega \in \mathrm{Mat}_g \mid {}^t\Omega = \Omega,\ \Im(\Omega) > 0\right\} \ .$$

The existence of a Riemann form on the lattice Λ is then conveniently translated into the so-called Riemann conditions on V and Λ.

Theorem 6.1.10 (Riemann conditions [65, Théorème VI.1.3]). *Let $X = V/\Lambda$ be a complex torus of dimension g. There exists a Riemann form ω on X if and only if there exist a basis $\{e_1, \dots, e_g\}$ of V, strictly positive integers $d_1, \dots, d_g$ verifying $d_1 | \dots | d_g$ and a matrix $\Omega \in \mathbb{H}_g$, called the* period matrix*, such that Λ is written with regards to the basis $\{e_1, \dots, e_g\}$*

$$\Lambda = \Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$$

where Δ is the diagonal matrix with coefficients $d_1, \dots, d_g$.

In the basis given by the above decomposition, called a *Frobenius* or *symplectic basis*, the matrix of ω is given by

$$\begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix} \ .$$

The squareroot of the determinant of ω, called its *pfaffian* and denoted by $\mathrm{pf}(\omega)$, is then

$$\mathrm{pf}(\omega) = d_1 \cdots d_g \ .$$

6.1.3 Isogenies

Definition 6.1.11 (Isogeny [213, II.6 Application 3], [204, I.7]). *A homomorphism $\phi : A \to B$ between abelian varieties is called an isogeny if it is surjective and has a finite kernel.*

Two abelian varieties are said to be isogenous if there exists an isogeny between them. This can be shown to be an equivalence relation.

Definition 6.1.12 (Simple abelian variety). *Let A be an abelian variety. A is said to be simple*[6] *if there exists no abelian variety B verifying*

$$\{0\} \subsetneq B \subsetneq A \ .$$

[6] Waterhouse use the term *elementary* [280] which is used elsewhere to denote isotypic abelian varieties [270, Definition 12.4].

Poincaré reducibility theorem [213, Theorem IV.19.1], [205, Theorem I.2.12], [65, Théorème VI.8.1] shows that any abelian variety can be decomposed into a product of simple abelian varieties.

Proposition 6.1.13 ([213, Corollary IV.19.1], [65, VI.8.2]). *Let A be an abelian variety. Then there exist abelian varieties $A_1, \ldots, A_n$ non isogenous to each other and positive integers $r_1, \ldots, r_n$ such that*

$$A \sim A_1^{r_1} \times A_n^{r_n} \ .$$

The abelian varieties $A_1, \ldots, A_n$ are unique up to isogeny and the integers $r_1, \ldots, r_n$ are unique.

6.1.4 Picard variety and polarizations

Let A be an abelian variety. Let $\mathrm{Div}(A)$ denote the group of divisors of A, $\mathrm{Div}^a(A)$ the subgroup of those algebraically equivalent to zero and $\mathrm{Div}^l(A)$ the subgroup of those linearly equivalent to zero. The *Picard group* of A is $\mathrm{Pic}(A) = \mathrm{Div}(A)/\mathrm{Div}^l(A)$. The subgroup of equivalence classes of divisors algebraically equivalent to zero is denoted by $\mathrm{Pic}^0(A) = \mathrm{Div}^a(A)/\mathrm{Div}^l(A)$.

The theorem of the square [213, Corollary II.6.4], [65, Théorème VI.3.3] implies that a group homomorphism between an abelian variety and its Picard group can be constructed from any line bundle.

Theorem 6.1.14 ([213, Corollary II.6.4], [65, Théorème VI.4.2]). *Let A be an abelian variety and L a line bundle. Then the map ψ_L defined as*

$$\begin{aligned} A &\to \mathrm{Pic}^0(A) \\ x &\mapsto \left[\tau_x^* L \otimes L^{-1}\right] \end{aligned}$$

is a group homomorphism. It only depends on the algebraic equivalence class of L. If L is ample, then the kernel $K(L)$ of ψ_L is finite.

The group $\mathrm{Pic}^0(A)$ can then be given the structure of an abelian variety[7].

Theorem 6.1.15 (Picard variety [159, Section 3.4]). *Let A be an abelian variety. There exists an abelian variety $\widehat{A}$ called the* Picard variety[8] *and a group isomorphism*

$$\widehat{A} \simeq \mathrm{Pic}^0(A) \ .$$

The Picard variety is also called the dual abelian variety of A. Indeed, there is a canonical isomorphism

$$A \simeq \widehat{\widehat{A}} \ .$$

Moreover, if u is a homomorphism between two abelian varieties A and B, then there exists a dual homomorphism, or transpose, $\widehat{u} : \widehat{B} \to \widehat{A}$ which verifies $\widehat{\widehat{u}} = u$, $\widehat{u+v} = \widehat{u} + \widehat{v}$ for $u, v \in \mathrm{Hom}(A, B)$ and $\widehat{vu} = \widehat{u}\widehat{v}$ if $u \in \mathrm{Hom}(A, B)$ and $v \in \mathrm{Hom}(B, C)$. If u is an isogeny, then $\widehat{u}$ is an isogeny of the same degree. On divisors, this is described by taking inverse image, i.e. by u^*. In particular, A and $\widehat{A}$ have isomorphic endomorphism rings.

[7] This is done by quotienting A by the kernel of ψ_L where L is an ample line bundle. The fact that the quotient is an abelian variety is definitely non-trivial.

[8] In fact, the Picard variety is defined together with a divisor on $A \times \widehat{A}$, but we will not use this fact here.

A homomorphism ψ_L with L ample as above is then an isogeny between A and $\widehat{A}$ and is called a *polarization* of the abelian variety[9]. If ψ_L is of degree one, it is called a *principal polarization*. A morphism λ of polarized abelian varieties between (A, ψ) and (B, ψ') is a morphism of abelian varieties such that[10]

$$\lambda^*(\psi') \ (= \widehat{\lambda}\psi'\lambda) = \psi \ .$$

Over the complex numbers, an analytic description of the dual complex torus $\widehat{X}$ can be given for any complex torus X.

Proposition 6.1.16 ([213, II.9], [65, Proposition V.5.9], [16, Proposition 2.4.1]). *Let $X = V/\Lambda$ be a complex torus. Let $\overline{V}^* = \mathrm{Hom}_{\overline{C}}(V, \mathbb{C})$ be the set of $\mathbb{C}$-antilinear forms and $\widehat{\Lambda} = \left\{ l \in \overline{V}^* \mid \Im(l) \subset \mathbb{Z} \right\}$. Then the map*

$$\begin{aligned} \overline{V}^*/\widehat{\Lambda} &\to \mathrm{Pic}^0(X) \ , \\ l &\mapsto L(0, e^{2i\pi\Im l(\cdot)}) \ , \end{aligned}$$

is an isomorphism. Moreover, $Pic^0(X)$ is isomorphic to the group of characters $\Lambda_1^* = \mathrm{Hom}(\Lambda, \mathbb{C}_1)$.

The real vector space $\overline{V}^*$ is canonically isomorphic to $\mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ using a similar correspondence as for the forms ω and H: if $l \in \overline{V}^*$, then we define $k = \Im l$; if $k \in V_{\mathbb{R}}^* = \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$, then we define $l(z) = -k(iz) + ik(z)$ [65, Proposition 5.9], [16, 2.4]. Finally, $V_{\mathbb{R}}^*$ is isomorphic to Λ_1^*, both being defined by their values on a basis of Λ.

If $u : X \to Y$ is a homomorphism of complex tori, then its dual is analytically represented by $\widehat{u} : l \mapsto l \circ u$.

Furthermore, every line bundle L is of the form $L(H, \alpha)$ and it can be shown that the polarization ψ_L associated with L only depends on H, or equivalently on the Riemann form $\omega = \Im(H)$ associated with H. Therefore, on a complex abelian variety the polarization can be defined as the choice of a Riemann form.

The following proposition implies the theorem of the square over the complex numbers and describes the homomorphism from X into $\mathrm{Pic}^0(X)$ associated with a Riemann form.

Proposition 6.1.17 ([213, II.9], [65, Lemme 3.2]). *Let X be a complex torus, $L(H, \alpha)$ a line bundle on X and $x \in X$. Then*

$$\tau_x^* L(H, \alpha) \simeq L(H, \alpha e^{2i\pi\Im H(\cdot, \widetilde{x})}) \ .$$

More precisely, the homomorphism ϕ_L corresponding to ω is given analytically by

$$\begin{aligned} X = V/\Lambda &\to \widehat{X} = \overline{V}^*/\widehat{\Lambda} \ , \\ x &\mapsto H(\cdot, \widetilde{x}) \ , \end{aligned}$$

[9] This is neither the more general definition of Milne [204, I.11] where it is only required that ϕ can be described as above over an extension of the base field, nor that of Shimura [238, 4.1] or Lang [159, 3.4] which only consider them up to the existence of positive integers m and m' such that mL and $m'L'$ are algebraically equivalent, i.e. if the associated Riemann forms are proportional. In the latter case, there exists a so-called basic polar divisor Y in the polarization $\mathcal{C}$ such that any divisor X in the polarization is algebraically equivalent to a multiple of Y: $X \equiv mY$.

[10] This is once again more restrictive than the definitions of Shimura [238, 4.1] and Lang [159, 3.4] which only set $\lambda^*(\mathcal{C}') \subset \mathcal{C}$. Lang [159, 3.5] says that the polarizations correspond to each other for the above definition. However, for automorphisms of polarized abelian varieties, both definitions coincide.

where $\widetilde{x}$ is any element of V over x and $H(\cdot,\widetilde{x})$ is indeed a $\mathbb{C}$-antilinear map [65, VI.4.3], [213, II.9], [16, Lemma 2.4.5]. The kernel of ϕ_L is $K(L)=\Lambda(L)/\Lambda$ where

$$\Lambda(L)=\{x\in V \mid \omega(\Lambda,x)\subset\mathbb{Z}\} \ .$$

If L is non degenerate, then the matrix of ω in a symplectic basis is

$$\begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix} \ ,$$

and

$$\#K(L)=\deg(\psi_L)=\mathrm{pf}(\omega)^2=(d_1\cdots d_g)^2 \ .$$

To conclude this section let us mention that, as was pointed out by Weil [282], the correct generalization of elliptic curves to higher dimensions are *polarized* abelian varieties. They have indeed finite automorphism groups and are well suited for moduli problems.

Theorem 6.1.18 ([213, Theorem IV.21.5], [204, Proposition I.14.4])**.** *Let A be an abelian variety and ψ a polarization. Then the automorphism group of (A,ψ) is finite.*

Over the complex numbers, isomorphism classes of polarized abelian variety of a given type can be classified using the fact that an element $\Omega\in\mathbb{H}_g$ can be associated with every polarized abelian variety of a given type.

Definition 6.1.19 (Symplectic group)**.** *Let J be the $2g\times 2g$ matrix*

$$J=\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \ .$$

The symplectic group $\mathrm{SP}_{2g}(\mathbb{Q})$ is the set of $2g\times 2g$ matrices M such that $MJ^tM=J$:

$$\mathrm{SP}_{2g}(\mathbb{Q})=\left\{M\in\mathrm{GL}_{2g}(\mathbb{Q}) \mid MJ^tM=J\right\} \ .$$

As was the case in dimension 1, there is an action of the symplectic group $\mathrm{SP}_{2g}(\mathbb{Q})$ on $\mathbb{H}_g$ given for $M=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\mathrm{SP}_{2g}(\mathbb{Q})$ and $\Omega\in\mathbb{H}_g$ by [65, Proposition VII.1.1]

$$M\cdot\Omega=(a\Omega+b)(c\Omega+d)^{-1} \ .$$

Proposition 6.1.20 ([65, VII.1], [16, Proposition 8.1.3])**.** *Let A and B be two complex polarized abelian varieties of type Δ. Then A and B are isomorphic if and only if there exists $M\in G_\Delta$ such that $M\cdot A=B$ where G_Δ is the following subgroup of $\mathrm{SP}_{2g}(\mathbb{Q})$:*

$$G_\Delta=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\mathrm{SP}_{2g}(\mathbb{Q}) \mid a,b\Delta^{-1},\Delta c,\Delta d\Delta^{-1}\in\mathrm{Mat}_g(\mathbb{Z})\right\} \ .$$

In particular the moduli space of complex polarized abelian varieties of a given type is of dimension $\frac{g(g+1)}{2}$.

6.1.5 Homomorphisms and the Rosati involution

If A is a simple abelian variety, then every non zero endomorphism is surjective so that it is an isogeny and is invertible in $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, the *endomorphism algebra* of A. Thus, $\mathrm{End}^0(A)$ is a division algebra when A is simple.

Moreover, if A and B are isogenous simple abelian varieties, then $\mathrm{End}^0(A) \simeq \mathrm{End}^0(B)$.

Finally, if A is not simple, using the decomposition of an abelian variety A into a product of simple abelian varieties $A_1^{n_1} \times \cdots \times A_r^{n_r}$ not isogenous to each other, we get [213, Corollary IV.19.2], [65, Théorème VI.10.1]

$$\mathrm{End}^0 A \simeq \mathrm{Mat}_{n_1}\left(\mathrm{End}^0(A_1)\right) \times \cdots \times \mathrm{Mat}_{n_r}\left(\mathrm{End}^0(A_r)\right) \ .$$

Over the complex numbers, if A and B are two abelian varieties, they can be described as complex tori $A \simeq V/\Lambda$ and $B \simeq V'/\Lambda'$. Moreover, as a consequence of the GAGA principle [234], or more precisely of a theorem of Chow [49], every complex analytic map between two complex abelian varieties is in fact given by rational maps and so is a morphism of abelian varieties. So it is enough to study homomorphisms between complex tori.

Furthermore, a homomorphism ϕ between two complex tori $X = V/\Lambda$ and $X' = V'\Lambda'$ can be lifted to a map $\widetilde{\phi}$ between the complex vector spaces V and V' which sends Λ into Λ' so that the following diagram is commutative:

$$\begin{array}{ccc} V & \xrightarrow{\widetilde{\phi}} & V' \\ \downarrow & & \downarrow \\ V/\Lambda & \xrightarrow{\phi} & V'/\Lambda' \end{array}$$

Therefore, we get different representations of $\mathrm{Hom}(X, X')$ [159, 1.1], [16, 1.2]:

- a complex or analytic representation $\rho_a : \mathrm{Hom}(X, X') \to \mathrm{Hom}_{\mathbb{C}}(V, V')$, $\phi \mapsto \widetilde{\phi}$,
- and a rational representation $\rho_r : \mathrm{Hom}(X, X') \to \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda')$.

Moreover, for the endomorphism algebra $\mathrm{End}^0(X) = \mathrm{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ of a complex torus X, the rational representation $\rho_r \otimes_{\mathbb{Z}} 1 : \mathrm{End}^0(X) \otimes_{\mathbb{Z}} \mathbb{C} \to \mathrm{End}_{\mathbb{C}}(\Lambda \otimes_Z \mathbb{C})$ is equivalent to the sum of the complex representation and its complex conjugate [16, Proposition 1.2.3]:

$$\rho_r \otimes_{\mathbb{Z}} 1 \simeq \rho_a \oplus \overline{\rho_a} \ .$$

In positive characteristic $p > 0$, the l-adic Tate module for any l co-prime to p, which is a free $\mathbb{Z}_l$-module of rank $2g$, plays the same role as Λ for the complex numbers [213, IV.19], [280].

It can be shown that the $\mathbb{Z}$-module of homomorphisms between two abelian varieties, and in particular the endomorphism ring of an abelian variety, is always a free $\mathbb{Z}$-module of finite rank.

Theorem 6.1.21 ([213, Corollary IV.19.1], [204, Theorem I.10.15])**.** *Let A and B be two abelian varieties. Then* $\mathrm{Hom}(A, B)$ *is a free $\mathbb{Z}$-module of rank $\leq 4\dim(A)\dim(B)$.*

Over the complex numbers, if $A \simeq V/\Lambda$ is simple, then $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ is a vector space over $\mathrm{End}^0(A)$ so that the rank of $\mathrm{End}(A)$ is in fact at most $2g$ [213, IV.19].

Definition 6.1.22 (Rosati involution [213, IV.20], [204, I.14], [65, Définition VI.10.2]). *Let (A, ψ) be a polarized abelian variety. The Rosati involution † is defined as*

$$u^\dagger = \psi^{-1}\widehat{u}\psi \ ,$$

for $u \in \mathrm{End}^0(A)$.

The Rosati involution satisfies $u^{\dagger\dagger} = u$, $(u+v)^\dagger = u^\dagger + v^\dagger$ and $(uv)^\dagger = v^\dagger u^\dagger$. So this is indeed an anti-involution of the $\mathbb{Q}$-algebra $\mathrm{End}^0(A)$.

Theorem 6.1.23 (Positivity [213, Theorem IV.21.1], [204, Theorem I.14.3]). *Let (A, ψ) be a polarized abelian variety. Then the map $(u, v) \mapsto \mathrm{Tr}(u^\dagger v)$ is a rational positive definite quadratic form on $\mathrm{End}^0(A)$.*

As was the case in dimension 1, the existence of the Rosati involution can be used to classify all the possible structures of the endomorphism algebra $\mathrm{End}^0(A)$ for A simple. Most of the classification was conducted by Albert [5, 4, 7, 6] and can be found e.g. in [213, Application IV.21.I] or [270, 12.27].

Over the complex numbers, the Rosati involution can be explicitly described in terms of the Riemann form associated with the polarization.

Theorem 6.1.24 ([159, Theorem 3.4.3]). *Let (A, ψ) be a polarized abelian variety defined over the complex numbers and ω the Riemann form associated with ψ via the analytic parametrization $\theta : V/\Lambda \xrightarrow{\sim} A$. Then the transpose with respect to ω corresponds via θ to the Rosati involution associated with ψ.*

6.2 Class groups and units

In this section we generalize the discussion of Subsection 5.2.2 to class groups of orders in number fields of any degree.

6.2.1 Description

Let K be a number field of degree n over $\mathbb{Q}$. We denote by $\mathcal{O}_K$ the ring of integers of K. Recall that $\mathcal{O}_K$ is maximal, i.e. any order $\mathcal{O}$ of K is a subring of $\mathcal{O}_K$; in fact, it is the integral closure of any order $\mathcal{O}$ of K. We denote the integral closure, or normalization, using a tilde.

Theorem 6.2.1 ([251, Theorem 3.20]). *Let K be a number field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}$ an order. Then*

$$\widetilde{\mathcal{O}} = \mathcal{O}_K \ .$$

To avoid double subscripts, we indifferently use the notation $\mathcal{O}_K$ and $\widetilde{\mathcal{O}}$. As in the quadratic case, the maximal order $\mathcal{O}_K$ is a Dedekind ring and general orders are noetherian and of Krull dimension 1.

The definitions of fractional, proper and invertible ideals are the same as in Subsection 5.2.2. Note that it is not true anymore that a proper ideal is always invertible. In fact, counterexamples arise as soon as $n \geq 3$ [63, 1.4]. However, every fractional ideal becomes invertible for some order when raised to the power $n-1$ [63, Theorem C].

Necessary conditions for a fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ to be invertible are still that it is proper, i.e. its multiplier ring $R(\mathfrak{a}) = (\mathfrak{a} : \mathfrak{a})$ is exactly $\mathcal{O}$ and that its inverse $\mathfrak{a}^{-1} = (R(a) : \mathfrak{a})$ is also proper.

The set of fractional ideals of $\mathcal{O}$ is stable under addition, multiplication, quotient and intersection, but the set of proper ideals is not. Nonetheless, we can define an action of invertible ideals on proper ideals by multiplication. For $\mathfrak{a}, \mathfrak{b} \in \mathrm{Prop}(\mathcal{O})$, $\mathfrak{a} * \mathfrak{b}$ is defined as

$$\mathfrak{a} * \mathfrak{b} = \mathfrak{a}^{-1}\mathfrak{b} \ .$$

The four basic operations on fractional ideals: addition, multiplication, quotient and intersection, are compatible with localization at a maximal ideal. Moreover, an ideal is invertible if and only if it is locally invertible, or equivalently locally principal, at each maximal ideal.

Proposition 6.2.2 ([216, Satz I.12.4], [251, Theorem 2.7], [63, Corollary 2.1.7])**.** *Let K be a number field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}$ an order. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. Then $\mathfrak{a}$ is invertible if and only if $\mathfrak{a}_\mathfrak{p}$ is a principal fractional ideal of $\mathcal{O}_\mathfrak{p}$ for every maximal ideal $\mathfrak{p}$ of $\mathcal{O}$.*

Definition 6.2.3 (Singular ideal)**.** *Let K be a number field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}$ an order. A maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ is said to be singular if it is non invertible. Otherwise it is said to be regular.*

Equivalently, a maximal ideal is singular if the local ring $\mathcal{O}_\mathfrak{p}$ is not a discrete valuation ring [251, Theorem 2.17].

Definition 6.2.4 (Conductor [216, I.12], [25, 9.1])**.** *Let K be a number field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}$ an order. The conductor of $\mathcal{O}$, denoted by $\mathfrak{f}(\mathcal{O})$, is the largest ideal of $\mathcal{O}_K$ contained in $\mathcal{O}$.*

The conductor can also be described as

$$\mathfrak{f}(\mathcal{O}) = \{x \in K \mid x\mathcal{O}_K \subset \mathcal{O}\} = (\mathcal{O} : \mathcal{O}_K) \ .$$

The maximal ideals dividing $\mathfrak{f}$ are exactly the singular maximal ideals of $\mathcal{O}$ [216, Satz I.12.10], [251, Exercise 4.25]. Moreover, if $\mathfrak{p}$ is regular, then $\mathfrak{p}\mathcal{O}_K$ is a maximal ideal. Finally, every fractional ideal co-prime to the conductor can be uniquely written as a product of maximal ideals co-prime to the conductor.

If $m = [\mathcal{O}_K : \mathcal{O}]$ is the index of $\mathcal{O}$ in $\mathcal{O}_K$, then $m\mathcal{O}_K \subset \mathfrak{f}(\mathcal{O})$. Furthermore, the rational primes $p \in \mathbb{Q}$ dividing m are exactly those above which $\mathcal{O}$ is singular. Contrary to the case of quadratic fields, orders are not classified anymore by their indices in $\mathcal{O}_K$.

Finally, for an order $\mathcal{O}$, we define as in Subsection 5.2.2 the Picard or class group $\mathrm{Pic}(\mathcal{O})$ of classes of invertible ideals, the proper class semigroup $\mathrm{Prop}(\mathcal{O})$ of classes of proper ideals, and the class semigroup of classes of fractional ideals modulo principal ideals. As in the quadratic case, the set of fractional ideals co-prime to the conductor modulo principal fractional ideals is isomorphic to the Picard group [217].

We also have the following fundamental exact sequence relating the Picard group of an order with that of the maximal order.

Proposition 6.2.5 ([216, Satz I.12.9], [25, Proposition 9.9])**.** *Let K be a number field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}$ an order of conductor $\mathfrak{f}$. The following canonical exact sequence is exact:*

$$1 \to \mathcal{O}^* \to \widetilde{\mathcal{O}}^* \to \bigoplus_{\mathfrak{p}\mid\mathfrak{f}} \widetilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^* \to \mathrm{Pic}(\mathcal{O}) \to \mathrm{Pic}(\widetilde{\mathcal{O}}) \to 1 \ ,$$

where $\mathfrak{p}$ ranges over the prime ideals of $\mathcal{O}$ dividing the conductor $\mathfrak{f}$.

Proposition 6.2.6 (Normalization kernel [216, Satz I.12.11], [25, Proposition 9.14])**.** *Let K be a number field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}$ an order. The normalization kernel $S_{\mathcal{O}}$ is the kernel of the map*

$$\begin{aligned} \mathrm{Frac}(\mathcal{O}) &\to \mathrm{Frac}(\mathcal{O}_K) \ , \\ \mathfrak{a} &\mapsto \mathfrak{a}\mathcal{O}_K \ . \end{aligned}$$

The group of its invertible elements $S_{\mathcal{O}}^*$ is isomorphic to

$$S_{\mathcal{O}}^* \simeq \bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \simeq \bigoplus_{\mathfrak{f}\subset\mathfrak{p}} (\widetilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}\widetilde{\mathcal{O}}_{\mathfrak{p}})^*/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{f}\mathcal{O}_{\mathfrak{p}})^* \simeq (\widetilde{\mathcal{O}}/\mathfrak{f})^*/(\mathcal{O}/\mathfrak{f})^* \ ,$$

where $\mathfrak{f} = \mathfrak{f}(\mathcal{O})$ is the conductor of $\mathcal{O}$.

As a consequence, a formula for $\#\operatorname{Pic}(\mathcal{O})$ in function of $\#\operatorname{Pic}(\widetilde{\mathcal{O}})$ can be deduced.

Theorem 6.2.7 ([216, Satz 12.12])**.** *Let K be a number field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}$ an order. Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Then*

$$\#\operatorname{Pic}(\mathcal{O}) = \frac{\#\operatorname{Pic}(\widetilde{\mathcal{O}})}{[\widetilde{\mathcal{O}}^* : \mathcal{O}^*]} \frac{\#(\widetilde{\mathcal{O}}/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*} \ .$$

Bounds on the size of the class semigroup can be found in Brakenhoff's Ph.D. thesis [25, Chapter 9].

6.2.2 Computation of the Picard and unit groups

Algorithms for computations with finite abelian groups are described in Cohen's textbooks [54, Chapter 2] and [55, Chapter 1, Section 4.1]. Factorization of fractional ideals of maximal orders is described in [55, Subsection 2.3.5]. The computation of Picard groups and unit groups of maximal orders is a classical problem and algorithms to compute them are described in the same textbooks [54, Section 6.5]. It is worth noting that most of these algorithms are implemented in Pari [218].

However, except for the case of quadratic fields, the computation of Picard groups was not efficiently addressed until the recent work of Klüners and Pauli [151] that we describe in this subsection.

Using the right part of the exact sequence of Proposition 6.2.5:

$$\widetilde{\mathcal{O}}^* \to \bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \to \operatorname{Pic}(\mathcal{O}) \to \operatorname{Pic}(\widetilde{\mathcal{O}}) \to 1 \ ,$$

one can indeed compute $\operatorname{Pic}(\mathcal{O})$ if $\bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$ is known. The explicit description of the different maps is easy, and the computations of $\widetilde{\mathcal{O}}^*$ and $\operatorname{Pic}(\widetilde{O})$ are assumed to be well-known.

Using the group isomorphism of Proposition 6.2.6, the direct sum can be described as

$$\bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \simeq \bigoplus_{\mathfrak{f}\subset\mathfrak{p}} (\widetilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}\widetilde{\mathcal{O}}_{\mathfrak{p}})^*/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{f}\mathcal{O}_{\mathfrak{p}})^* \ ,$$

so it is enough to compute the quotient $(\widetilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}\widetilde{\mathcal{O}}_{\mathfrak{p}})^*/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{f}\mathcal{O}_{\mathfrak{p}})^*$ for each maximal ideal $\mathfrak{p}$ containing $\mathfrak{f}$. The computation of the conductor is just the computation of an ideal quotient and is described

in [151, Section 6]. The computation of the set $\mathcal{P}$ of maximal ideals of $\mathcal{O}$ containing the conductor is done by factoring $\mathfrak{f} = \mathfrak{f}\widetilde{\mathcal{O}}$ in $\widetilde{\mathcal{O}}$:

$$\mathfrak{f}\widetilde{\mathcal{O}} = \mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_r^{n_r} \ ,$$

and then computing intersections of the $\mathfrak{q}_i$ with $\mathcal{O}$:

$$\mathcal{P} = \{\mathfrak{q}_i \cap \mathcal{O}\}_{1 \le i \le r} \ .$$

The first quotient to compute is nothing but

$$(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\widetilde{\mathcal{O}}_\mathfrak{p})^* \simeq \prod_{\mathfrak{q}|\mathfrak{p}\widetilde{\mathcal{O}}} (\widetilde{\mathcal{O}}_\mathfrak{q}/\mathfrak{f}\widetilde{\mathcal{O}}_\mathfrak{q})^* \simeq \prod_{\mathfrak{q}|\mathfrak{p}\widetilde{\mathcal{O}}} (\widetilde{\mathcal{O}}_\mathfrak{q}/\mathfrak{q}^{n_\mathfrak{q}}\widetilde{\mathcal{O}}_\mathfrak{q})^* \ .$$

It is not necessary to compute completely the second quotient. Indeed if $\mathfrak{p}\mathcal{O}_\mathfrak{p} \supset \mathfrak{f}\mathcal{O}_\mathfrak{p} \supset \mathfrak{p}^m\mathcal{O}_\mathfrak{p}$, computing generators of $(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^m\mathcal{O}_\mathfrak{p})^*$ is enough to deduce the structure of $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\widetilde{\mathcal{O}}_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/\mathfrak{f}\mathcal{O}_\mathfrak{p})^*$ [151, Section 8]. The integer m is easily deduced from the factorization of $\mathfrak{f}\widetilde{\mathcal{O}}$ and $\mathfrak{p}\widetilde{\mathcal{O}}$ [151, Lemma 7.4].

It now remains to explain the computation of $(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^m\mathcal{O}_\mathfrak{p})^*$ for any order $\mathcal{O}$, for a maximal ideal $\mathfrak{p}$ and a positive integer m. The first step is to get back to the global ring $\mathcal{O}$ with the following classical result.

Lemma 6.2.8 ([151, Theorem 4.1.i])**.** *Let K be a number field and $\mathcal{O}$ an order. Let $\mathfrak{p}$ be a maximal ideal and $\mathfrak{a}$ a $\mathfrak{p}$-primary ideal. Then*

$$\mathcal{O}/\mathfrak{a} \simeq \mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p} \ .$$

Afterwards, the structure of the *unit group* in the residue ring is given by the following lemma.

Lemma 6.2.9 ([151, Lemma 4.3])**.** *Let K be a number field and $\mathcal{O}$ an order. Let $\mathfrak{p}$ be a maximal ideal. Then*

$$(\mathcal{O}/\mathfrak{p}^m)^* \simeq (\mathcal{O}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{p}^m) \ .$$

The computation of a generator of the finite field $\mathcal{O}/\mathfrak{p}$ is classical. It can then be lifted back to $\mathcal{O}/\mathfrak{p}^m$ using Hensel's lemma. The computation of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ is done using a binary decomposition and the following lemma.

Lemma 6.2.10 ([151, Lemma 4.4])**.** *Let K be a number field and $\mathcal{O}$ an order. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of $\mathcal{O}$ such that $\mathfrak{a} \supset \mathfrak{b} \supset \mathfrak{a}^2$. Then the map $\psi : \ (1+\mathfrak{a})/(1+\mathfrak{b}) \to \mathfrak{a}/\mathfrak{b}, \ [1+\gamma] \mapsto [\gamma]$ is a group isomorphism.*

To summarize the above discussion, we finally recall the complete algorithm of Klüners and Pauli [151, Algorithm 8.1] in Algorithm 6.1.

The unit group is computed in a similar way using the fact that it is the kernel of the left part of the exact sequence

$$1 \to \mathcal{O}^* \to \widetilde{\mathcal{O}}^* \to \bigoplus_\mathfrak{p} \widetilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^* \ .$$

It is then realized as the kernel of the map $\widetilde{\mathcal{O}}^* \to \bigoplus_\mathfrak{p} \widetilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^*$.

6.2.3 Multiplication of fractional ideals by finite idèles

The main theorems of complex multiplication are expressed using the action of finite idèles on lattices which we describe in this subsection.

The *finite adèles* and *idèles* are defined as follows.

Algorithm 6.1: Computation of the Picard group of a non-maximal order

Input: An order $\mathcal{O}$ in a number field K
Output: Generators and relations for $\mathrm{Pic}(\mathcal{O})$

Compute the conductor $\mathfrak{f}$ of $\mathcal{O}$
Factorize $\mathfrak{f}\widetilde{\mathcal{O}} = \mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_r^{n_r}$
Compute $\mathcal{P} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_u\} = \{\mathfrak{q}_i \cap \mathcal{O}\}_{1 \leq i \leq r}$
foreach $\mathfrak{p}$ *in* $\mathcal{P}$ **do**
    foreach $\mathfrak{q}$ *dividing* $\mathfrak{p}\widetilde{\mathcal{O}}$ **do**
        Compute generators and relations for $(\widetilde{\mathcal{O}}_\mathfrak{q}/\mathfrak{q}^{n_\mathfrak{q}}\widetilde{\mathcal{O}}_\mathfrak{q})^*$
    Compute generators and relations for $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\widetilde{\mathcal{O}}_\mathfrak{p})^*$
    Compute m such that $\mathfrak{f}\mathcal{O}_\mathfrak{p} \supset \mathfrak{p}^m\mathcal{O}_\mathfrak{p}$
    Compute generators for $(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^m\mathcal{O}_\mathfrak{p})^*$
    Compute generators and relations for $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\widetilde{\mathcal{O}}_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/\mathfrak{f}\mathcal{O}_\mathfrak{p})^*$
Compute generators and relations for $\bigoplus_\mathfrak{p} \widetilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^*$
Compute generators and relations for $\mathrm{Pic}(\widetilde{\mathcal{O}})$
Compute generators and relations for $\widetilde{\mathcal{O}}^*$
Compute generators and relations for $\mathrm{Pic}(\mathcal{O})$
return *Generators and relations for* $\mathrm{Pic}(\mathcal{O})$

Definition 6.2.11 (Finite adèles and idèles)**.** *Let K be a number field. A finite adèle s is an element of the restricted product $\mathbb{A}_{K,f} = \prod'_\mathfrak{P} K_\mathfrak{P}$ over the completions of K at the maximal ideals $\mathfrak{P}$. A finite idèle is an invertible finite adèle.*

It can be shown that $\mathbb{A}_{K,f} \simeq K \otimes_\mathbb{Q} \mathbb{A}_{\mathbb{Q},f} \simeq K \otimes_\mathbb{Z} \widehat{Z}$ where $\widehat{\mathbb{Z}}$ is the ring of integral adèles $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p = \varprojlim \mathbb{Z}/n\mathbb{Z}$.

Furthermore, if $\mathcal{O}$ is an order in K, then the completion $\mathcal{O}_\mathfrak{p}$ of $\mathcal{O}$ is embedded in $\prod_{\mathfrak{P}|\mathfrak{p}\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{P}}$. We denote by $K_\mathfrak{p}$ the product $K_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}\mathcal{O}_K} K_\mathfrak{P}$. If $s \in \mathbb{A}_{K,f}$ is a finite idèle, we define its $\mathfrak{p}$-part as $s_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}\mathcal{O}_K} s_\mathfrak{P}$.

Now let $\mathfrak{a}$ of be a fractional ideal of $\mathcal{O}$. If we denote by $\mathfrak{a}_{(\mathfrak{p})}$ the localization of $\mathfrak{a}$ at $\mathfrak{p}$, then we have an isomorphism [160, 8.2]

$$K/\mathfrak{a}_{(\mathfrak{p})} \simeq K_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} \ .$$

Moreover, a fundamental fact is that there is a canonical isomorphism

$$K/\mathfrak{a} \simeq \bigoplus_\mathfrak{p} K_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$$

where $K_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$ is naturally identified with the $\mathfrak{p}$-primary part of $K/\mathfrak{a}$.

Now for any finite idèle $s \in \mathbb{A}_{K,f}^\times$ and proper ideal $\mathfrak{a}$ of the order $\mathcal{O}$ in K, it can be shown that there exists a unique proper ideal denoted by $s\mathfrak{a}$ such that $(s\mathfrak{a})_\mathfrak{p} = s_\mathfrak{p}\mathfrak{a}_\mathfrak{p}$ for every maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ [57, Lemma 6.1], [159, 3.6] and multiplication by s yields an isomorphism $s: \ K/\mathfrak{a} \to K/s\mathfrak{a}$.

If the order $\mathcal{O}$ is the maximal order $\mathcal{O}_K$ of K, then multiplication by s is nothing but multiplication by the ideal $[s]_{\mathcal{O}_K}$ associated with s, i.e.

$$[s]_{\mathcal{O}_K} = \prod_\mathfrak{p} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}\, s} \ .$$

If the order $\mathcal{O}$ is non-maximal, then we can also associate to s the fractional ideal $[s]_{\mathcal{O}}$ such that $([s]_{\mathcal{O}})_{\mathfrak{p}} = s_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$. Then $[s]_{\mathcal{O}}$ is locally principal, and so is an invertible ideal of $\mathcal{O}$. If $s \equiv 1 \mod \mathfrak{f}$ where $\mathfrak{f}$ is the conductor of $\mathcal{O}$, then we have $[s]_{\mathcal{O}} = [s]_{\mathcal{O}_K} \cap \mathcal{O}$.

6.3 Complex multiplication

6.3.1 CM field

Definition 6.3.1 (CM field)**.** *A CM field is a totally imaginary extension of a totally real number field.*

Definition 6.3.2 (CM algebra)**.** *A CM algebra is a finite product of CM fields.*

An order in a CM algebra is nothing but a product of orders in the associated CM fields. When we speak of ideals in such an order, we mean lattices-ideals, i.e. ideals which are also lattices, unless explicitly stated otherwise.

If E is a CM algebra, then complex conjugation induces a positive involution on E which does not depend on the complex embedding. We denote both the complex conjugation and this involution by $\bar{\cdot}$. Then, for any complex embedding ϕ, we have the identity $\overline{\phi} = \phi(\bar{\cdot})$. Moreover, the complex embeddings of E come in pairs of complex conjugates whence the following definition.

Definition 6.3.3 (CM type)**.** *Let E be a CM algebra. A CM type Φ on E is a subset of* $\mathrm{Hom}(E, \mathbb{C})$ *such that*

$$\mathrm{Hom}(E, \mathbb{C}) = \Phi \sqcup \overline{\Phi} \ .$$

We say that two CM types Φ and Φ' are equivalent if there exists an automorphism $\sigma \in \mathrm{Aut}(E)$ such that

$$\Phi\sigma = \Phi' \ .$$

If E' is a CM subalgebra of E and Φ is a CM type on E, then it induces a CM type Φ' on E'. We then say a CM type is primitive, or simple, if E is a CM field and there exists no such CM subfield and induced type.

Proposition 6.3.4 ([205, Proposition I.1.9], [159, Lemma 1.2.2])**.** *For every CM pair (F, Φ) where F is a CM field, there exists a unique primitive pair (K, Ψ) which extends to (F, Φ).*

Moreover, K is the fixed field of

$$H = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \mid \Phi_L\sigma = \Phi_L\}$$

where L is the Galois closure of F and Φ_L is extended from Φ.

A quartic CM field is either non-Galois, normal with cyclic Galois group — in which cases all CM types are primitive with respectively two and one equivalence classes of types — or normal with Galois group isomorphic to $C_2 \times C_2$ — in which case all types are non-primitive [252, Lemma I.3.4]. Hence we will speak of primitive, or non-primitive, quartic CM field.

6.3.2 Reflex field

Definition 6.3.5 (Reflex field [205, Proposition I.1.16])**.** *Let E be a CM algebra and Φ a CM type. The reflex field E^r of (E, Φ) is the fixed field of*

$$H = \left\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid \sigma\Phi = \Phi\right\} \ .$$

Equivalently, E^r is generated by the elements of the form

$$\sum_{\phi\in\Phi} \phi(a),\ a \in E\ .$$

The reflex field is a CM field and is left invariant by extension of CM algebra and type; moreover, if $(E,\Phi) = \prod_{i=1}^{n}(E_i,\Phi_i)$, then $E^r = E_1^r \cdots E_n^r$ [205, Proposition I.1.18].

If F is a CM field and Φ a CM type, then Φ can be extended to the Galois closure L of F. Denote by (K,Ψ) the primitive CM subpair of (L,Φ^{-1}). Then $K = E^r$ and Ψ is called the reflex CM type of Φ [204, Example I.1.19], [159, Theorem 1.5.1].

Definition 6.3.6 (Type trace [159, 1.5])**.** *Let (E,Φ) be a CM pair and E^r its reflex field. The type trace Tr_Φ is defined as*

$$\begin{aligned} E &\to E^r\ , \\ x &\mapsto \sum_{\phi\in\Phi} \phi(x)\ . \end{aligned}$$

Definition 6.3.7 (Type norm [159, 1.5], [205, I.1.5])**.** *Let (E,Φ) be a CM pair and E^r its reflex field. The type norm N_Φ is defined as*

$$\begin{aligned} E &\to E^r\ , \\ x &\mapsto \prod_{\phi\in\Phi} \phi(x)\ . \end{aligned}$$

The type norm naturally extends to fractional ideals and induces a map between class groups.

6.3.3 CM abelian varieties

Definition 6.3.8 (CM abelian variety [205, I.3])**.** *Let A be an abelian variety of dimension g. We say that A is an abelian variety with complex multiplication or is a CM abelian variety*[11] *if there exists a commutative semisimple $\mathbb{Q}$-algebra E of dimension $2g$ and an embedding $i:\ E \to \mathrm{End}^0(A)$.*

The CM abelian variety A, or the pair (A,i), is also said to have complex multiplication by E or $R = i^{-1}(\mathrm{End}^0(A))$ an order in E. If (A,i) has complex multiplication by R, then we say that it is defined over k, or that (A,i) has complex multiplication over k, if A is and if every homomorphism $i(R)$ is. If R is the maximal order of E, then we say that A is *principal*.

Using the decomposition of A into a product of simple abelian varieties it can be shown that an abelian variety has complex multiplication if and only if each simple factor has. Moreover, the endomorphism algebra of a simple abelian variety is a division algebra, so it has complex multiplication if and only if it contains a field of degree $2g$.

Tate has shown that every abelian variety defined over a finite field has complex multiplication [261].

Not only over the complex numbers, but over any field, the maximal commutative algebra can be chosen to be a CM algebra [286].

Over the complex numbers, a CM abelian variety is then characterized as follows.

Proposition 6.3.9 ([205, Proposition I.3.6])**.** *Let A be a complex abelian variety of dimension g:*

- *If A is simple, then it has complex multiplication if and only if its endomorphism algebra is a CM field K.*

[11] One also says that the abelian variety has sufficiently many complex multiplication or is of CM type.

- *If A is* isotypic*, i.e. $A \sim B^s$ where B is a simple abelian variety, then it has complex multiplication*[12] *if and only if* $\mathrm{End}^0(A)$ *contains a CM field F of degree $2g$.*
- *A has complex multiplication if and only if* $\mathrm{End}^0(A)$ *contains a CM subalgebra.*

In fact, if A is a complex CM abelian variety and $\mathrm{End}^0(A)$ contains a CM field F of degree $2g$, then $A \sim B^s$ is isotypic. Moreover, the commutant of F in $\mathrm{End}^0(A)$ is F [159, Theorem 3.1] and the center of $\mathrm{End}^0(A)$ is $\mathrm{End}^0(B) = K$ [159, Theorem 1.3.3]. Finally, the center of $\mathrm{End}_{\mathbb{Q}}(A)$ can also be described as $(F^r)^r$ [159, Theorem 1.5.3].

We have a more precise result about the commutant of R in $\mathrm{End}(A)$ valid in any characteristic.

Proposition 6.3.10 ([205, Corollary II.7.4])**.** *Let A be an abelian variety with complex multiplication by R. Then the commutant of R in* $\mathrm{End}(A)$ *is R.*

Working over the tangent space at zero of a complex CM abelian variety A, it can be shown that the embedding i induces a rational representation and can in fact be given by a CM type Φ, i.e. $i(a)$ acts as $\Phi(a)$ [205, I.3.11], [159, 1.3]. We say that (A, i) is of type (E, Φ) or (R, Φ). Furthermore, if $\sigma \in \mathrm{Aut}(\mathbb{C})$, then (A^σ, i^σ) is of type $(R, \sigma\Phi)$.

If A is an isotypic complex CM abelian variety, then there exists a CM field F of degree $2g$ and an embedding $i : F \to \mathrm{End}^0(A)$ which can be described by a CM type Φ and we also say that (A, i) is of type (F, Φ), or $(\mathcal{O}, \Phi)$ where $\mathcal{O}$ is an the order in F such that $\mathcal{O} = i(F) \cap \mathrm{End}(A)$. If $\sigma \in \mathrm{Aut}(F)$, then $(A, i \circ \sigma)$ is of type $(\mathcal{O}, \Phi\sigma)$.

Proposition 6.3.11 ([205, Proposition I.3.13], [159, Theorem 1.3.5])**.** *Let (A, i) be a complex CM abelian variety of type (E, Φ). Then A is simple if and only if E is a CM field and the type Φ is primitive.*

Moreover, if (A, i) is a simple complex CM abelian variety of type $(\mathcal{O}, \Phi)$ where $\mathcal{O}$ is an order in the CM field K, then i is an isomorphism:

$$i(K) = \mathrm{End}^0(A) \ ,$$

and

$$i(\mathcal{O}) = \mathrm{End}(A) \ .$$

Finally, as was the case in dimension 1, complex CM abelian varieties can be described by lattices in their CM algebra.

Theorem 6.3.12 ([205, I.3.11], [159, Theorem 1.4.1])**.** *Let E be a CM algebra of degree $2g$ and R an order in E. Let (A, i) be a complex abelian variety with complex multiplication by R. Then there exists a lattice $\mathfrak{a}$ in E which is a proper ideal of R, a CM type Φ and an analytic isomorphism θ such that*

$$V/\Phi(\mathfrak{a}) \overset{\theta}{\simeq} A$$

where $V = \mathbb{C}^{2g}$.

We say that the pair (A, i) is of type $(E, \Phi, \mathfrak{a})$ or $(R, \Phi, \mathfrak{a})$ with respect to θ.

It can also be shown that the converse of Theorem 6.3.12 is true: every complex torus of the form $V/\Phi(\mathfrak{a})$ admits a polarization and so is an abelian variety.

Proposition 6.3.13 ([205, Example I.2.9], [159, Theorem 1.4.4])**.** *Let E be a CM algebra, Φ a CM type, and $\mathfrak{a}$ a lattice in E. Then the complex torus $V/\Phi(\mathfrak{a})$ is polarizable.*

[12] This is the more restrictive definition of Mumford [213, IV.22] and Lang [159, 1.2].

We now restrict to the case where (A, i) is a simple complex CM abelian variety of type $(\mathcal{O}, \Phi, \mathfrak{a})$. Then, it should be noted that the ideal $\mathfrak{a}$ can be non invertible. However, if we let $\sigma \in \mathrm{Aut}(\mathbb{C})$ act on A, then we get a commutative diagram on the torsion points:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\theta \circ \Phi} & A_{tor} \\ \phi \downarrow & & \downarrow \sigma \\ K/\mathfrak{b} & \xrightarrow{\theta' \circ \sigma\Phi} & A^{\sigma}_{tor} \end{array}$$

where $\mathfrak{b}$ is another proper ideal of $\mathcal{O}$. But the left isomorphism commutes with the action of $\mathcal{O}$ and so must be described by multiplication by an idèle[13] [159, 7.3]. Hence, there exists an idèle s such that $\mathfrak{b} = s\mathfrak{a}$. This can also be described as multiplication by an invertible ideal of $\mathcal{O}$ and implies that $\mathfrak{b}$ is in the same orbit as $\mathfrak{a}$. Another point of view is to look at the multiplication locally at each maximal ideal: if $\mathfrak{a}$ is locally principal, then so is $s\mathfrak{a}$. In particular, if $\mathfrak{a}$ is invertible, then so is $\mathfrak{b}$.

Finally, complex CM abelian varieties have models over any algebraically closed subfield of $\mathbb{C}$ [205, Corollary II.7.10].

Proposition 6.3.14 ([205, Proposition II.7.11], [159, Theorem 3.1.1])**.** *Let (A, i) be a complex CM abelian variety of type (E, Φ) and suppose that A is defined over k. If (A, i) is defined over k, then $E^r \subset k$. Moreover, if A is simple, then the converse is true.*

6.3.4 Homomorphisms

If (A, i) and (B, j) are two abelian varieties with complex multiplication by E, then a homomorphism λ between them is understood to be a usual homomorphism commuting with the action of $i(E)$, i.e. $\lambda \circ i(\alpha) = i(\alpha) \circ j$ for all $\alpha \in E$.

If (A, i) and (B, j) are two isotypic abelian varieties of the same type (F, Φ) where F is a CM field of degree $2g$, then every homomorphism commuting with the action of F induces an endomorphism of $\Phi(F)$ and so an F-endomorphism of F. Hence, it is given by multiplication by an element $\gamma \in F$ [159, Theorem I.4.2].

Theorem 6.3.15 ([159, Theorem I.4.2])**.** *Let F be a CM field of degree $2g$ and Φ a CM type. Let (A, i) and (B, j) be two abelian varieties of type $(F, \Phi, \mathfrak{a})$ and $(F, \Phi, \mathfrak{b})$. Then $\mathrm{Hom}((A, i), (B, j))$ is represented by $(\mathfrak{b} : \mathfrak{a})$.*

In particular, if A and B are defined over the complex numbers and simple, then every homomorphism comes from $(\mathfrak{b} : \mathfrak{a})$ and A and B are isomorphic in the usual sense if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are in the same ideal class[14].

6.3.5 Dual abelian variety

Definition 6.3.16 (Trace dual)**.** *Let $\mathfrak{a}$ be a R lattice in E. We denote by $\mathfrak{a}^*$ the trace dual, or complementary lattice, of $\mathfrak{a}$:*

$$\mathfrak{a}^* = \{x \in E \mid \mathrm{Tr}(x\mathfrak{a}) \subset \mathbb{Z}\} \quad .$$

[13] This is also a consequence of the main theorem of complex multiplication over the rationals stated in Section 6.3.7.

[14] A similar result can be shown for $\mathfrak{a}$-transform of principal abelian varieties defined over any field [159, Proposition 3.2.5].

We have the obvious inclusion

$$\mathfrak{a}^{-1}R^* \subset \mathfrak{a}^*$$

where R^* is the trace dual or codifferent of R. It is a proper ideal of R, but in general it is not invertible. It is invertible if and only if every proper ideal is [125, Theorem 5.2]. If R is the maximal order $\mathcal{O}_K$ of a number field K, then $\mathcal{O}_K^* = \mathfrak{d}_{K/\mathbb{Q}}^{-1}$ is the usual absolute codifferent of K; moreover, the above inclusion becomes an equality [238, IV.14.3]:

$$\mathfrak{a}^* = \mathfrak{a}^{-1}\mathfrak{d}_{K/\mathbb{Q}}^{-1} \ .$$

Every $\mathbb{R}$-linear form k on V considered as a real vector space can be described as [238, I.3.3]

$$k: \ w \mapsto \langle z, w\rangle = \langle z, w\rangle_{\mathbb{C}} + \overline{\langle z, w\rangle_{\mathbb{C}}} = \sum_{i=1}^{g} (z_i\overline{w_i} + \overline{z_i}w_i)$$

for some $z \in V$. If (A, i) is a complex CM abelian variety of type $(E, \Phi, \mathfrak{a})$ and $k \in \widehat{\Lambda}$, then z must be equal to $\Phi(\xi)$ for $\xi \in E$ and hence k corresponds to $\mathrm{Tr}(\xi\cdot)$ on E [238, II.6.3]. Thus, $\widehat{\Lambda}$ corresponds to $\overline{\mathfrak{a}}^*$ and the dual abelian variety $\widehat{A}$ is analytically described by $V/\Phi(\overline{\mathfrak{a}}^*)$ using the above identification between V and $V_{\mathbb{R}}^*$. Moreover, for $\alpha \in E$, the dual endomorphism $\widehat{i(\alpha)}: \ l \mapsto l \circ i(\alpha)$ is given by $i(\overline{\alpha})$ on V. Hence, if we define $\widehat{i}(\alpha) = i(\overline{\alpha})$, then $(\widehat{A}, \widehat{i})$ is of type $(E, \Phi, \overline{\mathfrak{a}}^*)$.

Finally, if λ is a homomorphism from (A, i) of type $(E, \Phi, \mathfrak{a})$ to (B, j) of type $(E, \Phi, \mathfrak{b})$ described by $\alpha \in E$ such that $\alpha\mathfrak{a} \subset \mathfrak{b}$, then the dual homomorphism $\widehat{\lambda}$ from $(\widehat{B}, \widehat{j})$ to $(\widehat{A}, \widehat{i})$ is described by $\overline{\alpha}$.

6.3.6 Polarizations

Until the end of this subsection, all CM abelian varieties are defined over the complex numbers. Let (A, i) be a CM abelian variety of type (E, Φ). If ψ is a polarization on A, then we say that it is compatible with i if the Rosati involution associated with ψ leaves $i(E)$ stable. In particular, if A is simple, then any polarization is compatible with i.

Furthermore, if ψ is a compatible polarization on (A, i) and $\sigma \in \mathrm{Aut}(\mathbb{C})$, then ψ^σ is a compatible polarization of the same degree on (A^σ, i^σ). In particular, if (A, i) is principally polarized, then so is (A^σ, i^σ). From now on, we write *p.p.a.v.* for "principally polarized CM abelian variety defined over the complex numbers".

Theorem 6.3.17 ([205, Example I.2.9], [159, Theorem I.4.5])**.** *Let (A, i, ψ) be a polarized complex CM abelian variety of type $(E, \Phi, \mathfrak{a})$ with respect to some analytic parametrization θ. Then there exists an invertible element $\xi \in E^\times$ verifying $\overline{\xi} = -\xi$ and $\Im(\phi(\xi)) > 0$ for all $\phi \in \Phi$ such that the Riemann form ω associated with ψ can be described on $\Phi(E)$ as*

$$\omega(\Phi(x), \Phi(y)) = \mathrm{Tr}(\xi x\overline{y})$$

and extended by $\mathbb{R}$-linearity to V:

$$\omega(z, w) = \sum_{i=1}^{g} (\phi_i\xi)(z_i\overline{w}_i - \overline{z}_i w_i) = \langle \Phi(\xi)z, w\rangle \ .$$

With the above notation, the polarized complex CM abelian variety (A, i, ψ) is said to be of type $(E, \Phi, \mathfrak{a}, \xi)$ with respect to θ.

Conversely, every such element $\xi \in E^\times$ defines a form with rational values on Λ which have bounded denominators, so a rational multiple of it is a Riemann form. We call such a form a rational Riemann form.

From the results of Subsection 6.3.5, we see that the polarization induced by ξ between $\mathbb{C}^g/\Phi(\mathfrak{a})$ and $\mathbb{C}^g/\Phi(\overline{\mathfrak{a}}^*)$ is analytically described by multiplication by ξ. In particular, we have $\xi\mathfrak{a} \subset \overline{\mathfrak{a}}^*$, i.e. $\xi \in (\overline{\mathfrak{a}}^* : \mathfrak{a})$. Its kernel is included in $\Phi(E)$ and given by $K(\xi) = \Lambda(\xi)/\mathfrak{a}$ where

$$\Lambda(\xi) = \{x \in V \mid \mathrm{Tr}(\xi x\overline{\mathfrak{a}}) \subset \mathbb{Z}\} \ .$$

Hence $\Lambda(\xi) = \xi^{-1}\overline{\mathfrak{a}}^*$ and $K(\xi) = (\xi^{-1}\overline{\mathfrak{a}}^*)/\mathfrak{a}$. The degree of the polarization is therefore $\#K(\xi) = [\xi^{-1}\overline{\mathfrak{a}}^* : \mathfrak{a}]$. This is summarized in the following proposition.

Proposition 6.3.18 ([30, 4.3], [273, Theorem 3])**.** *Let (A, i, ψ) be a polarized complex CM abelian variety of type $(E, \Phi, \mathfrak{a}, \xi)$. Then*

$$\xi \in (\overline{\mathfrak{a}}^* : \mathfrak{a}) \ .$$

The degree of the polarization is $[\overline{\mathfrak{a}}^* : \xi\mathfrak{a}]$. In particular, the polarization is principal if and only if the following equality holds:

$$\xi\mathfrak{a} = \overline{\mathfrak{a}}^* \ .$$

If A is simple and principal, then the last equality reads

$$\xi\mathfrak{a}\overline{\mathfrak{a}}\mathfrak{d}_{K/\mathbb{Q}} = \mathcal{O}_K \ .$$

A homomorphism from (A, i, ψ) of type $(E, \Phi, \mathfrak{a}, \xi)$ to (B, j, ψ') of type $(E, \Phi, \mathfrak{b}, \zeta)$ is described by an element $\alpha \in E$ such that $\alpha\mathfrak{a} \subset \mathfrak{b}$. If ω_1 and ω_2 are the Riemann forms corresponding to the polarizations, then $\omega_2(z, w) = \alpha_*\omega_1(z, w) = \omega_1(\Phi(\alpha)z, \Phi(\alpha)w)$, so that we have $\xi = \alpha\overline{\alpha}\zeta$ [159, 3.5], [238, Proposition IV.14.3].

In particular, two triples (A, i, ψ) of type $(E, \Phi, \mathfrak{a}, \xi)$ and (B, j, ψ') of type $(E, \Phi, \mathfrak{b}, \zeta)$ are isomorphic if and only if there exists $\alpha \in E^\times$ such that $\mathfrak{b} = \alpha\mathfrak{a}$ and $\xi = \alpha\overline{\alpha}\zeta$. Moreover, it is readily seen that $[\overline{\mathfrak{a}}^* : \xi\mathfrak{a}] = [\overline{\mathfrak{b}}^* : \zeta\mathfrak{b}]$ so that such an isomorphism preserves the degree of the polarization. To summarize, we get the following classification up to isomorphism.

Proposition 6.3.19 (Classification of polarized CM abelian varieties over the complex numbers up to isomorphism [205, I.3.4], [237, 5.5.B])**.** *The triples (A, i, ψ) of type (E, Φ) are classified up to isomorphism by the quadruples $(E, \Phi, \mathfrak{a}, \xi)$ up to a change by an element $\alpha \in E^\times$ as above.*

If the abelian varieties are simple, then every homomorphism necessarily commutes with the action of $i(E)$ and we can drop the dependency on i.

This classification can be made more precise if we fix the couple (A, i) and the analytic parametrization θ, and so the type $(E, \Phi, \mathfrak{a})$. First, if ξ and ζ define two polarizations on (A, i) of type $(E, \Phi, \mathfrak{a})$, then $\xi\zeta^{-1}$ is left invariant by complex conjugation and so is a totally positive invertible element α_0 of E_0, the subalgebra of E fixed by its involution [238, Proposition IV.14.2]. Conversely, if α_0 is a totally positive invertible element of E_0 and ξ defines a compatible polarization on (A, i), so does some positive multiple of $\alpha_0^{-1}\xi$. Second, if $\alpha \in E^\times$ defines an automorphism of (A, i), then $\mathfrak{a} = \alpha\mathfrak{a}$ and α must be a unit in R, i.e. $\alpha \in R^\times$. If moreover α defines an isomorphism between polarized abelian varieties, then $\alpha\overline{\alpha}$ is a totally positive unit of E_0. This leads to the following proposition.

Proposition 6.3.20 ([238, Proposition IV.14.5])**.** *Let U_0 be the group of totally positive units of E_0, and U_1 the subgroup of units of the form $\alpha\overline{\alpha}$ for $\alpha \in R^\times$. Suppose that there exists a*

polarized complex CM abelian variety (A, i, ψ) of type $(E, \Phi, \mathfrak{a})$. Then there are exactly $[U_0 : U_1]$ isomorphism classes[15] *of polarized complex CM abelian varieties of the same type.*

The above discussion also implies that, if α defines an automorphism of (A, i, ψ) for some compatible polarization ψ, then $\alpha\overline{\alpha} = 1$ and consequently that α is a root of unity [238, IV.14.2].

Finally, Streng gave the following criterion for complex CM abelian varieties with complex multiplication by the same CM field but different types.

Proposition 6.3.21 ([252, Lemma I.5.6])**.** *Let (A, i) and (B, j) be two complex abelian varieties of types (K, Φ) and (K, Ψ). If Φ is primitive and Φ and Ψ are not equivalent, then A and B are not isogenous.*

6.3.7 The main theorems of complex multiplication

As was the case in dimension 1, the main theorems of complex multiplication describe the action of automorphisms of $\mathbb{C}$ analytically. The proofs of the theorems, although they are more involved and technical, are quite similar. We sketch the main steps of the proofs in this subsection.

The classical proofs involve the theory of $\mathfrak{a}$-*multiplications* and $\mathfrak{a}$-*transforms* defined below.

Definition 6.3.22 ($\mathfrak{a}$-multiplication [205, Definition II.7.17], [159, 3.2], [238, II.7])**.** *Let (A, i) be an abelian variety with complex multiplication by an order R. Let $\mathfrak{a}$ be an ideal in R. A surjective homomorphism $\lambda : A \to A^{\mathfrak{a}}$ is an $\mathfrak{a}$-multiplication if every homomorphism $\alpha : A \to A$ for $\alpha \in \mathfrak{a}$ factors through λ and it is universal for that property. An abelian variety B such that there exists an $\mathfrak{a}$-multiplication $\lambda : A \to B$ is called an $\mathfrak{a}$-transform*[16]*.*

For example, if (A, i) is a complex CM abelian variety of type $(R, \Phi, \mathfrak{a})$ and $\mathfrak{b}$ is an ideal in R, then the quotient map $\mathbb{C}^g/\Phi(\mathfrak{a}) \to \mathbb{C}^g/\Phi(\mathfrak{b}^{-1}\mathfrak{a})$ is a $\mathfrak{b}$-multiplication [205, Example II.7.18.b]. Conversely, if (A, i) and (B, j) are isogenous, then there exists an $\mathfrak{a}$-multiplication between them [205, Proposition II.7.29], [159, Proposition 3.2.6].

In any characteristic, it can be shown that an $\mathfrak{a}$-multiplication exists for every ideal $\mathfrak{a}$[17] [238, Proposition II.7], [205, Proposition II.7.20], [159, 3.2].

The classical proofs of the main theorems of complex multiplication first prove them in the principal case and are then extended to a general abelian variety using commutative diagrams. Indeed, the theory of maximal orders is far better understood than that of non-maximal ones. The situation for non-maximal orders is more subtle and similar direct proofs seem more arduous to obtain.

The Shimura–Taniyama formula, or congruence relation, then express a lift of the Frobenius endomorphism in characteristic zero as an $\mathfrak{a}$-multiplication.

Theorem 6.3.23 ([205, Corollary II.8.7], [159, Theorem 3.3.4], [238, Theorem III.13.1])**.** *Let (A, i) be an abelian variety defined over a number field k with complex multiplication by the maximal order R of the CM algebra E. Let $\mathfrak{P}$ be a prime of k where A has good reduction and such that $p = \mathfrak{P} \cap \mathbb{Z}$ is unramified in E and let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{E^r}$. Let $\sigma \in \mathrm{Gal}(l/E^r)$ be the Frobenius endomorphism of $\mathfrak{P}$ in l, a Galois extension of $\mathbb{Q}$ containing k. Then there exists an $\mathfrak{a}$-multiplication $\lambda : (A, i) \to (A^\sigma, i^\sigma)$ such that $\widetilde{\lambda}$ is the q-th power Frobenius endomorphism where $q = [\mathcal{O}_{E^r} : \mathfrak{p}]$ and $\mathfrak{a} = \mathrm{N}_{\Phi^r}(\mathfrak{p})$.*

[15] Here an isomorphism between (A, i, ψ) and (A, i, ψ') is understood as an isomorphism in the sense of Shimura [238, 4.1] or Lang [159, 3.4]: it is an isomorphism of abelian varieties such that the polarizations ψ and $\lambda^*\psi'$ are proportional. In particular, degree is not preserved.

[16] Waterhouse defines the related notion of kernel ideals [280, 3.2].

[17] In fact, $A^{\mathfrak{a}}$ can even be directly defined as the quotient of A by the finite group scheme $\ker(\mathfrak{a}) = \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha)$.

For a polarized principal CM abelian variety (A, i, ψ) of type $(E, \Phi, \mathfrak{a}, \xi)$ defined over the complex numbers, it is then relatively easy to show that $(A^\sigma, i^\sigma, \psi^\sigma)$ is of type $(E, \Phi, \mathrm{N}_{\Phi^r}(\mathfrak{p})^{-1}, \mathrm{N}(\mathfrak{p})\xi)$ and that the following diagram is commutative:

$$\begin{array}{ccc} \mathbb{C}^g/\Phi(\mathfrak{a}) & \xrightarrow{\theta \circ \Phi} & A \\ \Big\downarrow \text{can.} & & \Big\downarrow \lambda \\ \mathbb{C}^g/\Phi(\mathrm{N}_{\Phi^r}(\mathfrak{p})^{-1}\mathfrak{a}) & \xrightarrow{\theta' \circ \Phi} & A^\sigma \end{array}$$

Using the same method as in dimension 1 one then shows the main theorem over the reflex field. This first version of the main theorems of complex multiplication deals with the action of the absolute Galois group of the reflex field on complex abelian varieties with complex multiplication.

Theorem 6.3.24 (Over the reflex field [238, Theorems IV.18.6 and IV.18.8], [159, Theorem 3.6.1], [205, Theorem II.9.17], [57, Theorem 6.3])**.** *Let (A, i, ψ) be a polarized complex CM abelian variety of type $(E, \Phi, \mathfrak{a}, \xi)$ with respect to θ. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/E^r)$ and s be an idèle of E^r such that $\sigma = (s, E^r)_{E^{rab}}$. Then there exists a unique uniformization θ' such that $(A^\sigma, i^\sigma, \psi^\sigma)$ is of type $(E, \Phi, \mathrm{N}_{\Phi^r}(s^{-1})\mathfrak{a}, \mathrm{N}_{\mathbb{Q}}(s)\xi)$ with respect to θ' and the following diagram commutes:*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\theta \circ \Phi} & A_{tor} \\ \Big\downarrow \mathrm{N}_{\Phi^r}(s^{-1}) & & \Big\downarrow \sigma \\ K/\mathrm{N}_{\Phi^r}(s^{-1})\mathfrak{a} & \xrightarrow{\theta' \circ \Phi} & A_{tor}^\sigma \end{array}$$

The previous theorem can then be extended to arbitrary types of conjugations for a CM field K. It is much more involved and uses the cyclotomic character $\chi_{cyc} : \mathrm{Aut}_{\mathbb{C}} \to \widehat{Z}^\times = \mathbb{A}_{\mathbb{Q},f}^\times$ and a map $f_\Phi : \mathrm{Aut}(\mathbb{C}) \to \mathbb{A}_{K,f}^\times/K^\times$ verifying $f_\Phi(\sigma)\overline{f_\Phi(\sigma)} = \chi_{cyc}(\sigma)K^\times$ extending the map induced by the reflex norm $\mathrm{N}_\Phi : \mathrm{Aut}(\mathbb{C}/K^r) \to \mathbb{A}_{K,f}^\times/K^\times$ and called the type transfer [159, 7], [205, II.10].

Theorem 6.3.25 (Over the rationals [159, Theorem 7.3.1], [205, Theorem II.10.1])**.** *Let (A, i, ψ) be a polarized complex CM abelian variety of type $(K, \Phi, \mathfrak{a}, \xi)$ with respect to θ. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ and $s \in f_\Phi(\sigma) \subset \mathbb{A}_{K,f}^\times$. Then there exists a unique uniformization θ' such that $(A^\sigma, i^\sigma, \psi^\sigma)$ is of type $(K, \sigma\Phi, s\mathfrak{a}, \frac{\chi(\sigma)}{s\bar{s}})$ with respect to θ' and the following diagram commutes:*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\theta \circ \Phi} & A_{tor} \\ \Big\downarrow s & & \Big\downarrow \sigma \\ K/s\mathfrak{a} & \xrightarrow{\theta' \circ \sigma\Phi} & A_{tor}^\sigma \end{array}$$

6.4 Class polynomials for genus 2

In this section we extend the construction of the Hilbert class polynomial to curves of genus 2.

6.4.1 Jacobian variety

Definition 6.4.1 (Jacobian variety)**.** *Let C be an algebraic curve*[18] *of genus g defined over k; There exists an abelian variety of dimension g called the* Jacobian variety[19] *of C and denoted by* $\mathrm{Jac}(C)$ *such that* $\mathrm{Jac}(C)(l) \simeq \mathrm{Pic}^0_l(C)$ *for every extension l of k such that $C(l) \neq \emptyset$.*

The Jacobian variety is equipped with a canonical principal polarization.

Over the complex numbers, the Jacobian variety can be defined analytically as [204, III.2]

$$\mathrm{Jac}(C) = H^0(C, \Omega^1)^* / H_1(C, \mathbb{Z})$$

where $H_1(C, \mathbb{Z})$ is embedded into $H^0(C, \Omega^1)^*$ through the map $\gamma \mapsto \int_\gamma \cdot$.

If $P \in C(l)$, then there is a well defined map

$$\begin{aligned} C(l) &\to \mathrm{Jac}(C)(l) \\ Q &\mapsto [Q - P] \end{aligned}$$

and the Riemann–Roch theorem implies that the g-fold product of C is a cover of $\mathrm{Jac}(C)$[20].

A theorem of Torelli states that classifying curves is equivalent to classifying their Jacobian varieties.

Theorem 6.4.2 (Torelli's theorem [204, Theorem III.12.1])**.** *Let C and C' be two algebraic curves of genus g. Then C and C' are isomorphic if and only if their Jacobian varieties, together with their canonical polarizations, are.*

We say that a curve has complex multiplication by a CM algebra E or an order R within it if its Jacobian variety has.

Finally, it should be noted that over the complex numbers:

- in dimension 2, every simple p.p.a.v. is the Jacobian variety of a curve which is necessarily hyperelliptic;
- in dimension 3, every simple p.p.a.v. is the Jacobian of a curve, but it is not necessarily a hyperelliptic curve anymore;
- in dimension greater than or equal to 4, consideration of dimension shows that there exist simple p.p.a.v. which are not Jacobian varieties.

Classifying the simple p.p.a.v. which arise as Jacobian varieties is an unsolved question known as the Schottky problem. However, it is possible to characterize period matrices of hyperelliptic curves among those of p.p.a.v., but for a general number field there will not be any such matrices in the set of isomorphism classes of complex abelian varieties with complex multiplication by K [56, 18.3.1].

6.4.2 Igusa invariants

The moduli space of hyperelliptic curves of genus 2 is of dimension 3, so three invariants are needed to classify them up to isomorphism. Igusa defined such invariants which are valid in any characteristic [139], based on invariants defined by Clebsch [51]. In a field k of characteristic different from 2, every hyperelliptic curve of genus 2 can be given by an equation of the form

[18] Here a curve is a projective geometrically irreducible smooth scheme of dimension 1 over a perfect field.

[19] This is obviously a simplified definition which will be more than enough for our purposes.

[20] This can in fact be used to actually construct the Jacobian variety [204, III.7].

$y^2 = f(x)$ where $f(x)$ is a separable polynomial of degree 6. If we denote its root by $\alpha_1, \ldots, \alpha_6$, then the homogeneous Igusa invariants can be defined using the compact notation of Streng [252, II.2.1] as

$$\begin{aligned} I_2 &= a_6^2 \sum_{15} (12)^2 (34)^2 (56)^2 \ , \\ I_4 &= a_6^4 \sum_{10} (12)^2 (23)^2 (31)^2 (45)^2 (56)^2 (64)^2 \ , \\ I_6 &= a_6^6 \sum_{60} (12)^2 (23)^2 (31)^2 (45)^2 (56)^2 (64)^2 (14)^2 (25)^2 (36)^2 \ , \\ I_{10} &= a_6^{10} \prod_{i<j} (\alpha_i - \alpha_j)^2 \ . \end{aligned}$$

Different sets of absolute *Igusa invariants* can be defined from them. Streng chose the following ones for efficiency reasons:

$$i_1 = \frac{I_4 I_6'}{I_{10}}, \quad i_2 = \frac{I_2 I_4^2}{I_{10}}, \quad i_3 = \frac{I_4^5}{I_{10}^2} \ ,$$

where $I_6' = \frac{1}{2}(I_2 I_4 - 3 I_6)$. These triples classify the hyperelliptic curves up to isomorphism over $\overline{k}$ and, if the characteristic is not 3 and (i_1, i_2, i_3) is a triple where $i_3 \neq 0$, then there exists a curve whose invariants is that triple. The curve corresponding to such a triple can be reconstructed using an algorithm of Mestre [199].

Over the complex numbers these invariants can be computed from *theta constants*, or *theta null values*, which are the values of *Riemann theta functions* on the corresponding Jacobian variety. A Riemann theta function is nothing but a theta function for the lattice $\Lambda_\tau = \tau\mathbb{Z}^g \oplus \mathbb{Z}^g$ with a different normalization from the one we considered in Subsection 6.1.2.

Definition 6.4.3 (Riemann theta function [65, Exemple IV.1.2.3])**.** *Let a and b be two real column matrices with g rows. The Riemann theta function $\theta \begin{bmatrix} a \\ b \end{bmatrix} (\cdot, \tau)$ is defined by*

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau) = \sum_{m \in \mathbb{Z}^g} e^{i\pi[{}^t(m+a)\tau(m+a) + 2^t(m+a)(z+b)]} \ .$$

A theta constant with characteristic $c \in \{0, 1/2\}^{2g}$ is just $\theta[c](\tau) = \theta[c](0, \tau)$. The Igusa invariants can then be computed using these values [252, II.7.1].

A similar treatment was performed by Shioda [240] for hyperelliptic curves of genus 3 using nine invariants. The reconstruction of the curve corresponding to a tuple of invariants was recently described by Lercier and Ritzenthaler [176, 175].

6.4.3 Igusa class polynomials

We are now ready to describe an algorithm to compute *Igusa class polynomials* for a general order $\mathcal{O}$ in a primitive CM field, that is polynomials $H_1(X)$, $H_2(X)$ and $H_3(X)$ whose roots are the Igusa invariants i_1, i_2 and i_3 of hyperelliptic curves of genus 2 with CM by $\mathcal{O}$. These polynomials can then be used to extend the CM method to genus 2 and build hyperelliptic curves suitable for cryptographic use. The reader is refered to the Ph.D. theses of Spallek [248], Weng [283]

and Streng [252] for details; and to the paper of Freeman, Stevenhagen and Streng [102] for the ordinary case, and that of Hitt O'Connor et al. [134] for the p-rank one case.

We have seen that the CM order is preserved by the Galois action, so the corresponding Igusa class polynomials computed over all isomorphism classes of complex abelian varieties with complex multiplication by a given order will have rational coefficients. Moreover, invertible ideals are sent onto invertible ideals, so that we can restrict ourselves to such ideals, even though the following algorithms can be naturally extended to orbits of non-invertible proper ideals, and get factors of the Igusa class polynomials.

The first algorithm we propose is thus a straightforward generalization of the construction of the Hilbert class polynomial in dimension 1: one first enumerates all isomorphism classes of p.p.a.v. for a given order $\mathcal{O}$ and given by an invertible ideal and then computes the corresponding invariants analytically with sufficient precision. The Igusa class polynomials, which have rational coefficients, can then be recognized from their approximations. Precise description and analysis of such an algorithm have been done by Streng in his Ph.D. thesis [252] in the case of maximal orders and readily extend to the case of non-maximal orders. The enumeration of isomorphism classes is described in Algorithm 6.2 which corresponds to the algorithm proposed by Streng in the case of maximal orders [252, Algorithm II.3.1]. Its correctness is a consequence of the results presented in Section 6.3. A high-level description of the algorithm is given in Algorithm 6.3

Algorithm 6.2: Computation of representatives of the isomorphism classes of p.p.a.v. with CM by an order $\mathcal{O}$ in a primitive CM quartic field and given by invertible ideals

Input: A primitive quartic CM field K and an order $\mathcal{O}$
Output: A triple $(\Phi, \mathfrak{a}, \xi)$ for each isomorphism class of p.p.a.v. with CM by $\mathcal{O}$

```
Compute a complete set T of representatives of the CM types Φ on K
Compute a complete set U of representatives of O*_{K_0} / N_{K/K_0}(O*)
Compute a complete set I of representatives of the Picard group of O
Initialize an empty list L = []
foreach Ideal a ∈ I do
    if ā*a^{-1} is principal and generated by an element ξ ∈ K such that ξ^2 ∈ K_0 and ξ is
    totally negative then
        Append (a, ξ) to A
Initialize an empty list M = []
foreach Pair (a, ξ) ∈ L and unit u ∈ U do
    Append (Φ, a, uξ) to M where Φ is the unique CM type Φ such that ℑ(φuξ) > 0
return The triples (Φ, a, uξ) ∈ M such that Φ ∈ T
```

which is nothing but an extension of the algorithm of Streng [252, Algorithm II.11.1].

A second version of this algorithm using the explicit description of the main theorem of complex multiplication over the reflex field was developed by Streng [252, Chapter III]. The idea is that, if $\sigma \in \mathrm{Aut}(\mathbb{C}/K^r)$, then it does not modify the type Φ and acts as multiplication by the reflex norm $\mathrm{N}_{\Phi^r}(s^{-1})$ of the corresponding idèle s. This action can be explicitly described as multiplication by $\mathrm{N}_{\Phi^r}(\mathfrak{a}^{-1})$ where $\mathfrak{a}$ is an ideal of $\mathcal{O}_{K^r}$. Therefore, it is enough to find a triple $(\Phi, \mathfrak{a}, \xi)$ and then to compute the action of $\mathrm{Pic}(\mathcal{O}_{K^r})$ on it to build irreducible components of the Igusa class polynomials over K^r corresponding to a single orbit under $\mathrm{Aut}(\mathbb{C}/K^r)$. In fact, it can be shown that any K_0^r-conjugate of an Igusa invariant is also a K^r-conjugate [252, Corollary I.9.3]. Therefore, these irreducible components of the Igusa class polynomials have coefficients in K_0^r. One should then recognize the coefficients in K_0^r.

Algorithm 6.3: Computation of the Igusa class polynomials of a non-maximal order

Input: An order $\mathcal{O}$ in a CM quartic number field K
Output: The Igusa class polynomials $H_1(X)$, $H_2(X)$ and $H_3(X)$ corresponding to the Picard group of $\mathcal{O}$

1 Compute a set M of representatives of the isomorphism classes of p.p.a.v. with CM by $\mathcal{O}$ given by invertible ideals
2 **foreach** *Triple* $(\Phi, \mathfrak{a}, \xi) \in M$ **do**
3 Compute a symplectic basis of $\mathfrak{a}$ with respect to the polarization defined by ξ
4 Reduce the corresponding period matrix Ω into a fundamental domain
5 Evaluate the Igusa invariants i_1, i_2 and i_3 with sufficient precision through analytic evaluation of theta constants on Ω
6 Reconstruct the polynomials $H_1(X)$, $H_2(X)$ and $H_3(X)$ with rational coefficients from their respective roots
7 **return** $H_1(X)$, $H_2(X)$, $H_3(X)$

This method can as well be extended to the case of non-maximal orders. Indeed, we know that $\sigma \in \mathrm{Aut}(\mathbb{C}/K^r)$ also acts as multiplication by the idèle $\mathrm{N}_{\Phi^r}(s^{-1})$ for general orders. To describe that action explicitly as multiplication by an invertible ideal, it is sufficient that $\mathrm{N}_{\Phi^r}(s^{-1}) \equiv 1 \bmod \mathfrak{f}$, which can always be achieved up to multiplication by a principal idèle. Equivalently, the action of an ideal $\mathfrak{a}$ of $\mathcal{O}_{K^r}$ is given by multiplication $\mathrm{N}_{\Phi^r}(\mathfrak{a}^{-1}) \cap \mathcal{O}$ provided that $\mathrm{N}_{\Phi^r}(\mathfrak{a}^{-1})$ is co-prime to $\mathfrak{f}$. This can also always be achieved up to multiplication by a principal ideal.

6.4.4 Going further

The previous description of the algorithms is very scarce and many details are omitted. The missing steps for the principal case can be found in the Ph.D. thesis of Streng [252] and extend naturally to the non-principal case. We now list a few of them as well as some practical optimizations.

A first concrete complication in comparison with the genus 1 case is that Igusa class polynomials are no more integral, but only rational. Moreover, computing bounds on the value of the denominator is a hard problem. It was recently achieved by Goren and Lauter [119, 120] even thogh their result is not very sharp.

Furthermore, once the isomorphisms classes and the corresponding period matrices have been computed, they should be reduced, i.e. moved to a fundamental domain, to obtain faster convergence as is done for genus 1 [252, II.5].

Then, the theta constants should be computed using Borchardt sequences as proposed by Dupont [75]. This led to some record computations made by Dupont, Enge and Thomé [76].

The *complex analytic method* is not the only one which extends from genus 1. Eisenträger and Lauter developed a *CRT method* [80], implemented by Freeman [103] and later improved by Bröker, Gruenewald and Lauter [29] and Lauter and Robert [166]. As far as the *p-adic methods* are concerned, Gaudry et al. [112] developed a 2-adic one and Carls, Kohel and Lubicz [43] a 3-adic one.

To conclude, it should be mentioned that it is possible to define smaller class invariants than the Igusa invariants as was already the case in dimension 1. Such an approach, based on the higher-dimensional Shimura reciprocity, is being conducted by Streng [254, 255, 253]. Related ideas can also be found in the Ph.D. thesis of Uzunkol [269].

Appendices

Appendix A

Coefficients of f_d

> In another dream, I had a chlorophyll habit. Me and about five other chlorophyll addicts are waiting to score on the landing of a cheap Mexican hotel. We turn green and no one can kick a chlorophyll habit. One shot and you're hung for life. We are turning into plants.
>
> *Junky*
> William S. Burroughs [33]

In this section, we give the normalized coefficients $a^{d,n}_{(i_1,\dots,i_n)}$ of the multivariate polynomials P^n_d for the first few d's. In the following tables, $4\hat{}\,n$ means an exponential where the exponent is the opposite of the sum of n different β_i's. The total degree of the correpsonding multivariate polynomial is exactly $d-1$, except for $n=0$. The n-tuples then indicate the multi-exponent of the monomials and are followed by the corresponding coefficients. The omitted coefficients are obtained from the previous ones by permuting the β_i's. These coefficients were obtained using Sage [250], Pynac [268] and Maxima [267].

Table A.1: Coefficients for $d=1$, normalized by $(1/3)=(1/3^1)$

4^ 1	4^ 0
(0,) 2	() 1

Table A.2: Coefficients for $d=2$, normalized by $(1/9)=(1/3^2)$

4^ 2	4^ 1	4^ 0
(1,0) −2	(1,) 2	
(0,0) 20/3	(0,) −2/3	() 11/3

Table A.3: Coefficients for $d = 3$, normalized by $(1/27) = (1/3^3)$

4^ 3	4^ 2	4^ 1	4^ 0
$(2,0,0)$ 1	$(2,0)$ -1	$(2,)$ 1	
$(1,1,0)$ 2	$(1,1)$ -2		
$(1,0,0)$ -11	$(1,0)$ 5	$(1,)$ 1	
$(0,0,0)$ $64/3$	$(0,0)$ $-4/3$	$(0,)$ $-2/3$	() $35/3$

Table A.4: Coefficients for $d = 4$, normalized by $(1/81) = (1/3^4)$

4^ 4	4^ 3	4^ 2	4^ 1	4^ 0
$(3,0,0,0)$ $-1/3$	$(3,0,0)$ $1/3$	$(3,0)$ $-1/3$	$(3,)$ $1/3$	
$(2,1,0,0)$ -1	$(2,1,0)$ 1	$(2,1)$ -1		
$(1,1,1,0)$ -2	$(1,1,1)$ 2			
$(2,0,0,0)$ $23/3$	$(2,0,0)$ $-14/3$	$(2,0)$ $5/3$	$(2,)$ $4/3$	
$(1,1,0,0)$ $46/3$	$(1,1,0)$ $-28/3$	$(1,1)$ $10/3$		
$(1,0,0,0)$ $-416/9$	$(1,0,0)$ $119/9$	$(1,0)$ $16/9$	$(1,)$ $11/9$	
$(0,0,0,0)$ $1808/27$	$(0,0,0)$ $-80/27$	$(0,0)$ $-28/27$	$(0,)$ $-26/27$	() $971/27$

Table A.5: Coefficients for $d = 5$, normalized by $(1/243) = (1/3^5)$

4^ 5	4^ 4	4^ 3	4^ 2	4^ 1	4^ 0
$(4,0,0,0,0)$ $1/12$	$(4,0,0,0)$ $-1/12$	$(4,0,0)$ $1/12$	$(4,0)$ $-1/12$	$(4,)$ $1/12$	
$(3,1,0,0,0)$ $1/3$	$(3,1,0,0)$ $-1/3$	$(3,1,0)$ $1/3$	$(3,1)$ $-1/3$		
$(2,2,0,0,0)$ $1/2$	$(2,2,0,0)$ $-1/2$	$(2,2,0)$ $1/2$	$(2,2)$ $-1/2$		
$(2,1,1,0,0)$ 1	$(2,1,1,0)$ -1	$(2,1,1)$ 1			
$(1,1,1,1,0)$ 2	$(1,1,1,1)$ -2				
$(3,0,0,0,0)$ $-59/18$	$(3,0,0,0)$ $41/18$	$(3,0,0)$ $-23/18$	$(3,0)$ $5/18$	$(3,)$ $13/18$	
$(2,1,0,0,0)$ $-59/6$	$(2,1,0,0)$ $41/6$	$(2,1,0)$ $-23/6$	$(2,1)$ $5/6$		
$(1,1,1,0,0)$ $-59/3$	$(1,1,1,0)$ $41/3$	$(1,1,1)$ $-23/3$			
$(2,0,0,0,0)$ $161/4$	$(2,0,0,0)$ $-69/4$	$(2,0,0)$ $13/4$	$(2,0)$ $7/4$	$(2,)$ $9/4$	
$(1,1,0,0,0)$ $161/2$	$(1,1,0,0)$ $-69/2$	$(1,1,0)$ $13/2$	$(1,1)$ $7/2$		
$(1,0,0,0,0)$ $-9421/54$	$(1,0,0,0)$ $1933/54$	$(1,0,0)$ $209/54$	$(1,0)$ $79/54$	$(1,)$ $119/54$	
$(0,0,0,0,0)$ $16832/81$	$(0,0,0,0)$ $-560/81$	$(0,0,0)$ $-160/81$	$(0,0)$ $-92/81$	$(0,)$ $-142/81$	() $8881/81$

Table A.6: Coefficients for $d = 6$, normalized by $(1/729) = (1/3^6)$

4^ 6		4^ 5		4^ 4		4^ 3		4^ 2		4^ 1		4^ 0	
(5,0,0,0,0,0)	−1/60	(5,0,0,0,0)	1/60	(5,0,0,0)	−1/60	(5,0,0)	1/60	(5,0)	−1/60	(5,)	1/60		
(4,1,0,0,0,0)	−1/12	(4,1,0,0,0)	1/12	(4,1,0,0)	−1/12	(4,1,0)	1/12	(4,1)	−1/12				
(3,2,0,0,0,0)	−1/6	(3,2,0,0,0)	1/6	(3,2,0,0)	−1/6	(3,2,0)	1/6	(3,2)	−1/6				
(3,1,1,0,0,0)	−1/3	(3,1,1,0,0)	1/3	(3,1,1,0)	−1/3	(3,1,1)	1/3						
(2,2,1,0,0,0)	−1/2	(2,2,1,0,0)	1/2	(2,2,1,0)	−1/2	(2,2,1)	1/2						
(2,1,1,1,0,0)	−1	(2,1,1,1,0)	1	(2,1,1,1)	−1								
(1,1,1,1,1,0)	−2	(1,1,1,1,1)	2										
(4,0,0,0,0,0)	1	(4,0,0,0,0)	−3/4	(4,0,0,0)	1/2	(4,0,0)	−1/4	(4,0)	0	(4,)	1/4		
(3,1,0,0,0,0)	4	(3,1,0,0,0)	−3	(3,1,0,0)	2	(3,1,0)	−1	(3,1)	0				
(2,2,0,0,0,0)	6	(2,2,0,0,0)	−9/2	(2,2,0,0)	3	(2,2,0)	−3/2	(2,2)	0				
(2,1,1,0,0,0)	12	(2,1,1,0,0)	−9	(2,1,1,0)	6	(2,1,1)	−3						
(1,1,1,1,0,0)	24	(1,1,1,1,0)	−18	(1,1,1,1)	12								
(3,0,0,0,0,0)	−745/36	(3,0,0,0,0)	391/36	(3,0,0,0)	−145/36	(3,0,0)	7/36	(3,0)	23/36	(3,)	55/36		
(2,1,0,0,0,0)	−745/12	(2,1,0,0,0)	391/12	(2,1,0,0)	−145/12	(2,1,0)	7/12	(2,1)	23/12				
(1,1,1,0,0,0)	−745/6	(1,1,1,0,0)	391/6	(1,1,1,0)	−145/6	(1,1,1)	7/6						
(2,0,0,0,0,0)	4840/27	(2,0,0,0,0)	−6319/108	(2,0,0,0)	365/54	(2,0,0)	323/108	(2,0)	61/27	(2,)	485/108		
(1,1,0,0,0,0)	9680/27	(1,1,0,0,0)	−6319/54	(1,1,0,0)	365/27	(1,1,0)	323/54	(1,1)	122/27				
(1,0,0,0,0,0)	−83909/135	(1,0,0,0,0)	26503/270	(1,0,0,0)	1246/135	(1,0,0)	643/270	(1,0)	271/135	(1,)	1243/270		
(0,0,0,0,0,0)	640	(0,0,0,0,0)	−448/27	(0,0,0,0)	−112/27	(0,0,0)	−16/9	(0,0)	−44/27	(0,)	−98/27	()	2993/9

Table A.7: Coefficients for $d = 7$, normalized by $(1/2187) = (1/3^7)$

4^ 7		4^ 6		4^ 5		4^ 4		4^ 3		4^ 2		4^ 1		4^ 0	
(6,0,0,0,0,0,0)	1/360	(6,0,0,0,0,0)	−1/360	(6,0,0,0,0)	1/360	(6,0,0,0)	−1/360	(6,0,0)	1/360	(6,0)	−1/360	(6,)	1/360		
(5,1,0,0,0,0,0)	1/60	(5,1,0,0,0,0)	−1/60	(5,1,0,0,0)	1/60	(5,1,0,0)	−1/60	(5,1,0)	1/60	(5,1)	−1/60				
(4,2,0,0,0,0,0)	1/24	(4,2,0,0,0,0)	−1/24	(4,2,0,0,0)	1/24	(4,2,0,0)	−1/24	(4,2,0)	1/24	(4,2)	−1/24				
(3,3,0,0,0,0,0)	1/18	(3,3,0,0,0,0)	−1/18	(3,3,0,0,0)	1/18	(3,3,0,0)	−1/18	(3,3,0)	1/18	(3,3)	−1/18				
(3,2,1,0,0,0,0)	1/6	(3,2,1,0,0,0)	−1/6	(3,2,1,0,0)	1/6	(3,2,1,0)	−1/6	(3,2,1)	1/6						
(2,2,2,0,0,0,0)	1/4	(2,2,2,0,0,0)	−1/4	(2,2,2,0,0)	1/4	(2,2,2,0)	−1/4	(2,2,2)	1/4						
(2,2,1,1,0,0,0)	1/2	(2,2,1,1,0,0)	−1/2	(2,2,1,1,0)	1/2	(2,2,1,1)	−1/2								
(2,1,1,1,1,0,0)	1	(2,1,1,1,1,0)	−1	(2,1,1,1,1)	1										
(1,1,1,1,1,1,0)	2	(1,1,1,1,1,1)	−2												
(5,0,0,0,0,0,0)	−17/72	(5,0,0,0,0,0)	67/360	(5,0,0,0,0)	−49/360	(5,0,0,0)	31/360	(5,0,0)	−13/360	(5,0)	−1/72	(5,)	23/360		
(4,1,0,0,0,0,0)	−85/72	(4,1,0,0,0,0)	67/72	(4,1,0,0,0)	−49/72	(4,1,0,0)	31/72	(4,1,0)	−13/72	(4,1)	−5/72				
(3,2,0,0,0,0,0)	−85/36	(3,2,0,0,0,0)	67/36	(3,2,0,0,0)	−49/36	(3,2,0,0)	31/36	(3,2,0)	−13/36	(3,2)	−5/36				
(3,1,1,0,0,0,0)	−85/18	(3,1,1,0,0,0)	67/18	(3,1,1,0,0)	−49/18	(3,1,1,0)	31/18	(3,1,1)	−13/18						
(2,2,1,0,0,0,0)	−85/12	(2,2,1,0,0,0)	67/12	(2,2,1,0,0)	−49/12	(2,2,1,0)	31/12	(2,2,1)	−13/12						
(2,1,1,1,0,0,0)	−85/6	(2,1,1,1,0,0)	67/6	(2,1,1,1,0)	−49/6	(2,1,1,1)	31/6								
(1,1,1,1,1,0,0)	−85/3	(1,1,1,1,1,0)	67/3	(1,1,1,1,1)	−49/3										
(4,0,0,0,0,0,0)	1595/216	(4,0,0,0,0,0)	−947/216	(4,0,0,0,0)	461/216	(4,0,0,0)	−137/216	(4,0,0)	−25/216	(4,0)	25/216	(4,)	137/216		
(3,1,0,0,0,0,0)	1595/54	(3,1,0,0,0,0)	−947/54	(3,1,0,0,0)	461/54	(3,1,0,0)	−137/54	(3,1,0)	−25/54	(3,1)	25/54				
(2,2,0,0,0,0,0)	1595/36	(2,2,0,0,0,0)	−947/36	(2,2,0,0,0)	461/36	(2,2,0,0)	−137/36	(2,2,0)	−25/36	(2,2)	25/36				
(2,1,1,0,0,0,0)	1595/18	(2,1,1,0,0,0)	−947/18	(2,1,1,0,0)	461/18	(2,1,1,0)	−137/18	(2,1,1)	−25/18						
(1,1,1,1,0,0,0)	1595/9	(1,1,1,1,0,0)	−947/9	(1,1,1,1,0)	461/9	(1,1,1,1)	−137/9								
(3,0,0,0,0,0,0)	−23021/216	(3,0,0,0,0,0)	9611/216	(3,0,0,0,0)	−2573/216	(3,0,0,0)	−37/216	(3,0,0)	163/216	(3,0)	251/216	(3,)	739/216		
(2,1,0,0,0,0,0)	−23021/72	(2,1,0,0,0,0)	9611/72	(2,1,0,0,0)	−2573/72	(2,1,0,0)	−37/72	(2,1,0)	163/72	(2,1)	251/72				
(1,1,1,0,0,0,0)	−23021/36	(1,1,1,0,0,0)	9611/36	(1,1,1,0,0)	−2573/36	(1,1,1,0)	−37/36	(1,1,1)	163/36						
(2,0,0,0,0,0,0)	130997/180	(2,0,0,0,0,0)	−11399/60	(2,0,0,0,0)	1301/90	(2,0,0,0)	262/45	(2,0,0)	63/20	(2,0)	653/180	(2,)	443/45		
(1,1,0,0,0,0,0)	130997/90	(1,1,0,0,0,0)	−11399/30	(1,1,0,0,0)	1301/45	(1,1,0,0)	524/45	(1,1,0)	63/10	(1,1)	653/90				
(1,0,0,0,0,0,0)	−173017/81	(1,0,0,0,0,0)	109904/405	(1,0,0,0,0)	18719/810	(1,0,0,0)	3709/810	(1,0,0)	1039/405	(1,0)	280/81	(1,)	8387/810		
(0,0,0,0,0,0,0)	476416/243	(0,0,0,0,0,0)	−9856/243	(0,0,0,0,0)	−2240/243	(0,0,0,0)	−784/243	(0,0,0)	−512/243	(0,0)	−676/243	(0,)	−1970/243	()	244403/243

Table A.8: Coefficients for $d = 8$, normalized by $(1/6561) = (1/3^8)$

4^	8	4^	7	4^	6	4^	5	4^	4	4^	3	4^	2	4^	1	4^	0
(7, 0, 0, 0, 0, 0, 0, 0)	−1/2520	(7, 0, 0, 0, 0, 0, 0, 0)	1/2520	(7, 0, 0, 0, 0, 0, 0)	−1/2520	(7, 0, 0, 0, 0, 0)	1/2520	(7, 0, 0, 0)	−1/2520	(7, 0, 0)	1/2520	(7, 0)	−1/2520	(7,)	1/2520		
(6, 1, 0, 0, 0, 0, 0, 0)	−1/360	(6, 1, 0, 0, 0, 0, 0, 0)	1/360	(6, 1, 0, 0, 0, 0, 0)	−1/360	(6, 1, 0, 0, 0, 0)	1/360	(6, 1, 0, 0)	−1/360	(6, 1, 0)	1/360	(6, 1)	−1/360				
(5, 2, 0, 0, 0, 0, 0, 0)	−1/120	(5, 2, 0, 0, 0, 0, 0, 0)	1/120	(5, 2, 0, 0, 0, 0, 0)	−1/120	(5, 2, 0, 0, 0, 0)	1/120	(5, 2, 0, 0)	−1/120	(5, 2, 0)	1/120	(5, 2)	−1/120				
(4, 3, 0, 0, 0, 0, 0, 0)	−1/72	(4, 3, 0, 0, 0, 0, 0, 0)	1/72	(4, 3, 0, 0, 0, 0, 0)	−1/72	(4, 3, 0, 0, 0, 0)	1/72	(4, 3, 0, 0)	−1/72	(4, 3, 0)	1/72	(4, 3)	−1/72				
(4, 2, 1, 0, 0, 0, 0, 0)	−1/24	(4, 2, 1, 0, 0, 0, 0, 0)	1/24	(4, 2, 1, 0, 0, 0, 0)	−1/24	(4, 2, 1, 0, 0, 0)	1/24	(4, 2, 1, 0)	−1/24	(4, 2, 1)	1/24						
(3, 3, 1, 0, 0, 0, 0, 0)	−1/18	(3, 3, 1, 0, 0, 0, 0, 0)	1/18	(3, 3, 1, 0, 0, 0, 0)	−1/18	(3, 3, 1, 0, 0, 0)	1/18	(3, 3, 1, 0)	−1/18	(3, 3, 1)	1/18						
(3, 2, 2, 0, 0, 0, 0, 0)	−1/12	(3, 2, 2, 0, 0, 0, 0, 0)	1/12	(3, 2, 2, 0, 0, 0, 0)	−1/12	(3, 2, 2, 0, 0, 0)	1/12	(3, 2, 2, 0)	−1/12	(3, 2, 2)	1/12						
(3, 2, 1, 1, 0, 0, 0, 0)	−1/6	(3, 2, 1, 1, 0, 0, 0, 0)	1/6	(3, 2, 1, 1, 0, 0, 0)	−1/6	(3, 2, 1, 1, 0, 0)	1/6	(3, 2, 1, 1)	−1/6								
(2, 2, 2, 1, 0, 0, 0, 0)	−1/4	(2, 2, 2, 1, 0, 0, 0, 0)	1/4	(2, 2, 2, 1, 0, 0, 0)	−1/4	(2, 2, 2, 1, 0, 0)	1/4	(2, 2, 2, 1)	−1/4								
(2, 2, 1, 1, 1, 0, 0, 0)	−1/2	(2, 2, 1, 1, 1, 0, 0, 0)	1/2	(2, 2, 1, 1, 1, 0, 0)	−1/2	(2, 2, 1, 1, 1, 0)	1/2										
(2, 1, 1, 1, 1, 1, 0, 0)	−1	(2, 1, 1, 1, 1, 1, 1, 0)	1	(2, 1, 1, 1, 1, 1, 1)	−1												
(1, 1, 1, 1, 1, 1, 1, 0)	−2	(1, 1, 1, 1, 1, 1, 1, 1)	2														
(6, 0, 0, 0, 0, 0, 0, 0)	49/1080	(6, 0, 0, 0, 0, 0, 0, 0)	−1/27	(6, 0, 0, 0, 0, 0)	31/1080	(6, 0, 0, 0, 0)	−11/540	(6, 0, 0, 0)	13/1080	(6, 0, 0)	−1/270	(6, 0)	−1/216	(6,)	7/540		
(5, 1, 0, 0, 0, 0, 0, 0)	49/180	(5, 1, 0, 0, 0, 0, 0, 0)	−2/9	(5, 1, 0, 0, 0, 0, 0)	31/180	(5, 1, 0, 0, 0)	−11/90	(5, 1, 0, 0)	13/180	(5, 1, 0)	−1/45	(5, 1)	−1/36				
(4, 2, 0, 0, 0, 0, 0, 0)	49/72	(4, 2, 0, 0, 0, 0, 0, 0)	−5/9	(4, 2, 0, 0, 0, 0, 0)	31/72	(4, 2, 0, 0, 0)	−11/36	(4, 2, 0, 0)	13/72	(4, 2, 0)	−1/18	(4, 2)	−5/72				
(4, 1, 1, 0, 0, 0, 0, 0)	49/36	(4, 1, 1, 0, 0, 0, 0, 0)	−10/9	(4, 1, 1, 0, 0, 0, 0)	31/36	(4, 1, 1, 0, 0)	−11/18	(4, 1, 1, 0)	13/36	(4, 1, 1)	−1/9	(3, 3)	−5/54				
(3, 3, 0, 0, 0, 0, 0, 0)	49/54	(3, 3, 0, 0, 0, 0, 0, 0)	−20/27	(3, 3, 0, 0, 0, 0, 0)	31/54	(3, 3, 0, 0, 0)	−11/27	(3, 3, 0, 0)	13/54	(3, 3, 0)	−2/27						
(3, 2, 1, 0, 0, 0, 0, 0)	49/18	(3, 2, 1, 0, 0, 0, 0, 0)	−20/9	(3, 2, 1, 0, 0, 0, 0)	31/18	(3, 2, 1, 0, 0)	−11/9	(3, 2, 1, 0)	13/18	(3, 2, 1)	−2/9						
(3, 1, 1, 1, 0, 0, 0, 0)	49/9	(3, 1, 1, 1, 0, 0, 0, 0)	−40/9	(3, 1, 1, 1, 0, 0, 0)	31/9	(3, 1, 1, 1, 0)	−22/9	(3, 1, 1, 1)	13/9	(2, 2, 2)	−1/3						
(2, 2, 2, 0, 0, 0, 0, 0)	49/12	(2, 2, 2, 0, 0, 0, 0, 0)	−10/3	(2, 2, 2, 0, 0, 0, 0)	31/12	(2, 2, 2, 0, 0)	−11/6	(2, 2, 2, 0)	13/12								
(2, 2, 1, 1, 0, 0, 0, 0)	49/6	(2, 2, 1, 1, 0, 0, 0, 0)	−20/3	(2, 2, 1, 1, 0, 0, 0)	31/6	(2, 2, 1, 1, 0)	−11/3	(2, 2, 1, 1)	13/6								
(2, 1, 1, 1, 1, 0, 0, 0)	49/3	(2, 1, 1, 1, 1, 0, 0, 0)	−40/3	(2, 1, 1, 1, 1, 0, 0)	31/3	(2, 1, 1, 1, 1)	−22/3										
(1, 1, 1, 1, 1, 1, 0, 0)	98/3	(1, 1, 1, 1, 1, 1, 1, 0)	−80/3	(1, 1, 1, 1, 1, 1, 1)	62/3												
(5, 0, 0, 0, 0, 0, 0, 0)	−719/360	(5, 0, 0, 0, 0, 0, 0, 0)	58/45	(5, 0, 0, 0, 0, 0)	−263/360	(5, 0, 0, 0, 0)	29/90	(5, 0, 0, 0)	−23/360	(5, 0, 0)	−2/45	(5, 0)	1/360	(5,)	17/90		
(4, 1, 0, 0, 0, 0, 0, 0)	−719/72	(4, 1, 0, 0, 0, 0, 0, 0)	58/9	(4, 1, 0, 0, 0, 0, 0)	−263/72	(4, 1, 0, 0, 0)	29/18	(4, 1, 0, 0)	−23/72	(4, 1, 0)	−2/9	(4, 1)	1/72				
(3, 2, 0, 0, 0, 0, 0, 0)	−719/36	(3, 2, 0, 0, 0, 0, 0, 0)	116/9	(3, 2, 0, 0, 0, 0, 0)	−263/36	(3, 2, 0, 0, 0)	29/9	(3, 2, 0, 0)	−23/36	(3, 2, 0)	−4/9	(3, 2)	1/36				
(3, 1, 1, 0, 0, 0, 0, 0)	−719/18	(3, 1, 1, 0, 0, 0, 0, 0)	232/9	(3, 1, 1, 0, 0, 0, 0)	−263/18	(3, 1, 1, 0, 0)	58/9	(3, 1, 1, 0)	−23/18	(3, 1, 1)	−8/9						
(2, 2, 1, 0, 0, 0, 0, 0)	−719/12	(2, 2, 1, 0, 0, 0, 0, 0)	116/3	(2, 2, 1, 0, 0, 0, 0)	−263/12	(2, 2, 1, 0, 0)	29/3	(2, 2, 1, 0)	−23/12	(2, 2, 1)	−4/3						
(2, 1, 1, 1, 0, 0, 0, 0)	−719/6	(2, 1, 1, 1, 0, 0, 0, 0)	232/3	(2, 1, 1, 1, 0, 0, 0)	−263/6	(2, 1, 1, 1, 0)	58/3	(2, 1, 1, 1)	−23/6								
(1, 1, 1, 1, 1, 0, 0, 0)	−719/3	(1, 1, 1, 1, 1, 1, 0, 0)	464/3	(1, 1, 1, 1, 1, 1, 0)	−263/3	(1, 1, 1, 1, 1)	116/3										
(4, 0, 0, 0, 0, 0, 0, 0)	3113/72	(4, 0, 0, 0, 0, 0, 0, 0)	−253/12	(4, 0, 0, 0, 0, 0)	571/72	(4, 0, 0, 0, 0)	−55/36	(4, 0, 0, 0)	−3/8	(4, 0, 0)	1/36	(4, 0)	23/72	(4,)	19/12		
(3, 1, 0, 0, 0, 0, 0, 0)	3113/18	(3, 1, 0, 0, 0, 0, 0, 0)	−253/3	(3, 1, 0, 0, 0, 0, 0)	571/18	(3, 1, 0, 0, 0)	−55/9	(3, 1, 0, 0)	−3/2	(3, 1, 0)	1/9	(3, 1)	23/18				
(2, 2, 0, 0, 0, 0, 0, 0)	3113/12	(2, 2, 0, 0, 0, 0, 0, 0)	−253/2	(2, 2, 0, 0, 0, 0, 0)	571/12	(2, 2, 0, 0, 0)	−55/6	(2, 2, 0, 0)	−9/4	(2, 2, 0)	1/6	(2, 2)	23/12				
(2, 1, 1, 0, 0, 0, 0, 0)	3113/6	(2, 1, 1, 0, 0, 0, 0, 0)	−253	(2, 1, 1, 0, 0, 0, 0)	571/6	(2, 1, 1, 0, 0)	−55/3	(2, 1, 1, 0)	−9/2	(2, 1, 1)	1/3						
(1, 1, 1, 1, 0, 0, 0, 0)	3113/3	(1, 1, 1, 1, 1, 0, 0, 0)	−506	(1, 1, 1, 1, 1, 0, 0)	571/3	(1, 1, 1, 1, 0)	−110/3	(1, 1, 1, 1)	−9								
(3, 0, 0, 0, 0, 0, 0, 0)	−789649/1620	(3, 0, 0, 0, 0, 0, 0, 0)	543353/3240	(3, 0, 0, 0, 0, 0)	−55429/1620	(3, 0, 0, 0, 0)	−4927/3240	(3, 0, 0, 0)	1631/1620	(3, 0, 0)	4073/3240	(3, 0)	3611/1620	(3,)	26033/3240		
(2, 1, 0, 0, 0, 0, 0, 0)	−789649/540	(2, 1, 0, 0, 0, 0, 0, 0)	543353/1080	(2, 1, 0, 0, 0, 0, 0)	−55429/540	(2, 1, 0, 0, 0)	−4927/1080	(2, 1, 0, 0)	1631/540	(2, 1, 0)	4073/1080	(2, 1)	3611/540				
(1, 1, 1, 0, 0, 0, 0, 0)	−789649/270	(1, 1, 1, 0, 0, 0, 0, 0)	543353/540	(1, 1, 1, 0, 0, 0, 0)	−55429/270	(1, 1, 1, 0, 0)	−4927/540	(1, 1, 1, 0)	1631/270	(1, 1, 1)	4073/540						
(2, 0, 0, 0, 0, 0, 0, 0)	375892/135	(2, 0, 0, 0, 0, 0, 0, 0)	−64919/108	(2, 0, 0, 0, 0, 0)	8411/270	(2, 0, 0, 0, 0)	1649/135	(2, 0, 0, 0)	709/135	(2, 0, 0)	2267/540	(2, 0)	361/54	(2,)	6169/270		
(1, 1, 0, 0, 0, 0, 0, 0)	751784/135	(1, 1, 0, 0, 0, 0, 0, 0)	−64919/54	(1, 1, 0, 0, 0, 0, 0)	8411/135	(1, 1, 0, 0, 0)	3298/135	(1, 1, 0, 0)	1418/135	(1, 1, 0)	2267/270	(1, 1)	361/27				
(1, 0, 0, 0, 0, 0, 0, 0)	−60917648/8505	(1, 0, 0, 0, 0, 0, 0, 0)	6417293/8505	(1, 0, 0, 0, 0, 0)	506659/8505	(1, 0, 0, 0, 0)	165979/17010	(1, 0, 0, 0)	33844/8505	(1, 0, 0)	31613/8505	(1, 0)	56587/8505	(1,)	415207/17010		
(0, 0, 0, 0, 0, 0, 0, 0)	4360960/729	(0, 0, 0, 0, 0, 0, 0, 0)	−73216/729	(0, 0, 0, 0, 0, 0)	−15488/729	(0, 0, 0, 0, 0)	−4672/729	(0, 0, 0, 0)	−2384/729	(0, 0, 0)	−2224/729	(0, 0)	−3860/729	(0,)	−13870/729	()	2213497/729

Bibliography

[1] Milton Abramowitz and Irene Anne Stegun. *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, volume 55 of *National Bureau of Standards Applied Mathematics Series*. For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 1964. (Cited on pages 67, 71, 74, and 77.)

[2] Amod Agashe, Kristin Estella Lauter, and Ramarathnam Venkatesan. Constructing elliptic curves with a known number of points over a prime field. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 1–17. Amer. Math. Soc., Providence, RI, 2004. (Cited on page 153.)

[3] Omran Ahmadi and Robert Granger. An efficient deterministic test for Kloosterman sum zeros. *CoRR*, abs/1104.3882, 2011. (Cited on pages 115, 120, 121, and 122.)

[4] Abraham Adrian Albert. On the construction of Riemann matrices. I. *Ann. of Math. (2)*, 35(1):1–28, 1934. (Cited on page 168.)

[5] Abraham Adrian Albert. A solution of the principal problem in the theory of Riemann matrices. *Ann. of Math. (2)*, 35(3):500–515, 1934. (Cited on page 168.)

[6] Abraham Adrian Albert. Involutorial simple algebras and real Riemann matrices. *Ann. of Math. (2)*, 36(4):886–964, 1935. (Cited on page 168.)

[7] Abraham Adrian Albert. On the construction of Riemann matrices. II. *Ann. of Math. (2)*, 36(2):376–394, 1935. (Cited on page 168.)

[8] Jörg Arndt. *Matters Computational: Ideas, Algorithms, Source Code*. Springer, 2010. (Cited on pages 98, 122, and 232.)

[9] Arthur Oliver Lonsdale Atkin and François Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993. (Cited on page 152.)

[10] Ramachandran Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *J. Cryptology*, 11(2):141–145, 1998. (Cited on pages 155 and 156.)

[11] Samuel Beckett. *En attendant Godot : pièce en deux actes*. Charles Massin et Cie, Editions, 1952. (Cited on pages xi and 218.)

[12] Juliana Belding, Reinier Martijn Bröker, Andreas Enge, and Kristin Estella Lauter. Computing Hilbert class polynomials. In van der Poorten and Stein [271], pages 282–295. (Cited on page 153.)

[13] Elwyn Ralph Berlekamp, Victor Henry Rumsey, and Hannah Greenebaum Solomon. On the solution of algebraic equations over finite fields. *Information and Control*, 10:553–564, 1967. (Cited on page 118.)

[14] Jean Berstel and Michel Pocchiola. Average cost of Duval's algorithm for generating Lyndon words. *Theor. Comput. Sci.*, 132(2):415–425, 1994. (Cited on page 89.)

[15] Eli Biham, editor. *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*. Springer, 2003. (Cited on pages 195 and 202.)

[16] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004. (Cited on pages 160, 162, 165, 166, and 167.)

[17] Gaëtan Bisson. On the generation of pairing-friendly elliptic curves. Master's thesis, Université Paris-Sud 11, 2007. `http://www.normalesup.org/~bisson/res/memm2.pdf`. (Cited on page 157.)

[18] Ian Fraser Blake, Gadiel Seroussi, and Nigel Paul Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original. (Cited on pages 99, 103, 105, 154, and 155.)

[19] Ian Fraser Blake, Gadiel Seroussi, and Nigel Paul Smart, editors. *Advances in elliptic curve cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2005. (Cited on pages 136, 137, 138, and 155.)

[20] Dan Boneh and Matthew Keith Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001. (Cited on page 156.)

[21] Dan Boneh and Matthew Keith Franklin. Identity-based encryption from the Weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003. (Cited on page 156.)

[22] Jorge Luis Borges. *Ficciones*. Works. Emecé Editores, 1973. (Cited on page 109.)

[23] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). (Cited on pages 2 and 3.)

[24] Robert Bradshaw, Craig Citro, and Dag Sverre Seljebotn. Cython: the best of both worlds. *CiSE 2011 Special Python Issue*, page 25, 2010. (Cited on pages 2 and 126.)

[25] Johannes Franciscus Brakenhoff. *Counting problems for number rings*. PhD thesis, Universiteit Leiden, 2009. (Cited on pages 169 and 170.)

[26] Richard Peirce Brent, Pierrick Gaudry, Emmanuel Thomé, and Paul Zimmermann. Faster multiplication in GF(2)[x]. In van der Poorten and Stein [271], pages 153–166. (Cited on page 126.)

[27] Reinier Martijn Bröker. *Constructing elliptic curves of prescribed order*. PhD thesis, Universiteit Leiden, 2006. (Cited on page 153.)

[28] Reinier Martijn Bröker. A p-adic algorithm to compute the Hilbert class polynomial. *Math. Comput.*, 77(264):2417–2435, 2008. (Cited on page 152.)

[29] Reinier Martijn Bröker, David Gruenewald, and Kristin Estella Lauter. Explicit CM-theory in dimension 2. *0910.1848*, October 2009. (Cited on page 184.)

[30] Reinier Martijn Bröker, Kristin Estella Lauter, and Marco Streng. Abelian surfaces admitting an (l, l)-endomorphism. *1106.1884*, June 2011. (Cited on pages 178 and 240.)

[31] Reinier Martijn Bröker and Peter Stevenhagen. Elliptic curves with a given number of points. In Duncan Alan Buell, editor, *ANTS*, volume 3076 of *Lecture Notes in Computer Science*, pages 117–131. Springer, 2004. (Cited on page 153.)

[32] Johannes Buchmann and Ulrich Vollmer. *Binary quadratic forms*, volume 20 of *Algorithms and Computation in Mathematics*. Springer, Berlin, 2007. An algorithmic approach. (Cited on pages 146 and 147.)

[33] William Seward Burroughs and Oliver C. G. Harris. *Junky: the definitive text of "Junk"*. Penguin Books, 2003. (Cited on page 187.)

[34] Christian Cachin and Jan Camenisch, editors. *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*. Springer, 2004. (Cited on pages 198 and 203.)

[35] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbf{F}_{2^m}$, and crosscorrelation of maximum-length sequences. *SIAM J. Discrete Math.*, 13(1):105–138 (electronic), 2000. (Cited on page 21.)

[36] Claude Carlet. On a weakness of the Tu-Deng function and its repair. Cryptology ePrint Archive, Report 2009/606, 2009. `http://eprint.iacr.org/`. (Cited on page 15.)

[37] Claude Carlet. Private communication, 2009. (Cited on page 85.)

[38] Claude Carlet. Boolean functions for cryptography and error correcting codes. In Yves Crama and Peter Ladislaw Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 257–397. Cambridge University Press, June 2010. (Cited on pages 8, 9, 10, 11, 97, and 219.)

[39] Claude Carlet. Comments on "Constructions of cryptographically significant Boolean functions using primitive polynomials". *Information Theory, IEEE Transactions on*, 57(7):4852 –4853, july 2011. (Cited on page 12.)

[40] Claude Carlet, Deepak Kumar Dalai, Kishan Chand Gupta, and Subhamoy Maitra. Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction. *IEEE Transactions on Information Theory*, 52(7):3105–3121, 2006. (Cited on page 11.)

[41] Claude Carlet and Keqin Feng. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In Josef Pieprzyk, editor, *ASIACRYPT*, volume 5350 of *Lecture Notes in Computer Science*, pages 425–440. Springer, 2008. (Cited on pages 8, 12, 220, and 221.)

[42] Claude Carlet, Xiangyong Zeng, Chunlei Li, and Lei Hu. Further properties of several classes of Boolean functions with optimum algebraic immunity. *Des. Codes Cryptography*, 52(3):303–338, 2009. (Cited on page 11.)

[43] Robert Carls, David Russell Kohel, and David Lubicz. Higher-dimensional 3-adic CM construction. *J. Algebra*, 319(3):971–1006, 2008. (Cited on page 184.)

[44] John William Scott Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991. (Cited on page 99.)

[45] Jinhui Chao, Osamu Nakamura, Kohji Sobataka, and Shigeo Tsujii. Construction of secure elliptic cryptosystems using CM tests and liftings. In Kazuo Ohta and Dingyi Pei, editors, *ASIACRYPT*, volume 1514 of *Lecture Notes in Computer Science*, pages 95–109. Springer, 1998. (Cited on page 153.)

[46] Pascale Charpin and Guang Gong. Hyperbent functions, Kloosterman sums, and Dickson polynomials. *IEEE Transactions on Information Theory*, 54(9):4230–4238, 2008. (Cited on pages 96, 110, 111, 113, and 232.)

[47] Pascale Charpin, Tor Helleseth, and Victor Zinoviev. Divisibility properties of Kloosterman sums over finite fields of characteristic two. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 2608 –2612, july 2008. (Cited on pages 118 and 234.)

[48] Pascale Charpin, Tor Helleseth, and Victor Zinoviev. Divisibility properties of classical binary Kloosterman sums. *Discrete Mathematics*, 309(12):3975–3984, 2009. (Cited on page 120.)

[49] Wei-Liang Chow. On compact complex analytic varieties. *Amer. J. Math.*, 71:893–914, 1949. (Cited on page 167.)

[50] Marcus Tullius Cicero, Jules Martha, and Carlos Lévy. *Des termes extrêmes des biens et des maux: Livres I-II*. Collection des universités de France. Série latine. Les Belles Lettres, 1990. (Cited on page 1.)

[51] Alfred Clebsch. Zur Theorie der binären algebraischen Formen. *Math. Ann.*, 3(2):265–267, 1870. (Cited on page 181.)

[52] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *IMA Int. Conf.*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363. Springer, 2001. (Cited on page 156.)

[53] Gérard Denis Cohen and Jean-Pierre Flori. On a generalized combinatorial conjecture involving addition $\mod 2^k - 1$. Cryptology ePrint Archive, Report 2011/400, 2011. `http://eprint.iacr.org/`. (Cited on page 20.)

[54] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993. (Cited on pages 105 and 170.)

[55] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. (Cited on page 170.)

[56] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006. (Cited on pages 99, 105, 154, and 181.)

[57] Brian Conrad. Main theorem of complex multiplication. Talk given at the CM Seminar of the VIGRE number theory working group, notes available at `http://math.stanford.edu/~conrad/vigregroup/vigre04/mainthm.pdf`, 2004. (Cited on pages 160, 172, 180, and 241.)

[58] Nicolas Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In Dan Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 176–194. Springer, 2003. (Cited on pages 10 and 220.)

[59] Nicolas Courtois and Willi Meier. Algebraic attacks on stream ciphers with linear feedback. In Biham [15], pages 345–359. (Cited on pages 10 and 220.)

[60] Jean-Marc Couveignes and Thierry Henocq. Action of modular correspondences around CM points. In Fieker and Kohel [90], pages 234–243. (Cited on page 152.)

[61] David Archibald Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication. (Cited on pages 104, 105, 143, 144, 145, 146, 147, and 151.)

[62] Thomas William Cusick, Yuan Li, and Pantelimon Stănică. On a combinatorial conjecture. *Integers*, 11(2):185–203, May 2011. (Cited on page 85.)

[63] Everett Clarence Dade, Olga Taussky, and Hans Julius Zassenhaus. On the theory of orders, in paricular on the semigroup of ideal classes and genera of an order in an algebraic number field. *Math. Ann.*, 148:31–64, 1962. (Cited on pages 168 and 169.)

[64] Deepak Kumar Dalai, Subhamoy Maitra, and Sumanta Sarkar. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. *Des. Codes Cryptography*, 40(1):41–58, 2006. (Cited on page 11.)

[65] Olivier Debarre. *Tores et variétés abéliennes complexes*, volume 6 of *Cours Spécialisés [Specialized Courses]*. Société Mathématique de France, Paris, 1999. (Cited on pages 160, 161, 162, 163, 164, 165, 166, 167, 168, 182, and 238.)

[66] Jan Denef and Frederik Vercauteren. An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2. In Fieker and Kohel [90], pages 308–323. (Cited on page 107.)

[67] Jan Denef and Frederik Vercauteren. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. *J. Cryptology*, 19(1):1–25, 2006. (Cited on page 107.)

[68] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941. (Cited on pages 104 and 139.)

[69] Whitfield Diffie and Martin Edward Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976. (Cited on page 153.)

[70] John Francis Dillon. *Elementary Hadamard Difference Sets*. ProQuest LLC, Ann Arbor, MI, 1974. Thesis (Ph.D.)–University of Maryland, College Park. (Cited on pages 8, 11, 12, 13, 110, 111, and 230.)

[71] John Francis Dillon and Hans Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004. (Cited on page 118.)

[72] Cunsheng Ding, Guozhen Xiao, and Weijuan Shan. *The Stability Theory of Stream Ciphers*, volume 561 of *Lecture Notes in Computer Science*. Springer, 1991. (Cited on pages 11 and 220.)

[73] Hans Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In Bart Preneel, editor, *FSE*, volume 1008 of *Lecture Notes in Computer Science*, pages 61–74. Springer, 1994. (Cited on page 14.)

[74] Jean-Guillaume Dumas, Thierry Gautier, Pascal Giorgi, Jean-Louis Roch, and Gilles Villard. *Givaro-3.2.13rc1: C++ library for arithmetic and algebraic computations*, September 2008. `http://ljk.imag.fr/CASYS/LOGICIELS/givaro/`. (Cited on page 126.)

[75] Régis Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications*. PhD thesis, École Polytechnique, 2006. (Cited on page 184.)

[76] Régis Dupont, Andreas Enge, and Emmanuel Thomé. Computation of Igusa class polynomials with the complex analytic method. Talk given at GeoCrypt 2011, slides available at `http://iml.univ-mrs.fr/ati/GeoCrypt2011`, June 2011. (Cited on page 184.)

[77] Jean-Pierre Duval. Génération d'une section des classes de conjugaison et arbre des mots de Lyndon de longueur bornée. *Theor. Comput. Sci.*, 60:255–283, 1988. (Cited on page 89.)

[78] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.*, 82:631–648, 1960. (Cited on page 107.)

[79] Bernard Dwork. A deformation theory for the zeta function of a hypersurface. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 247–259. Inst. Mittag-Leffler, Djursholm, 1963. (Cited on page 107.)

[80] Kirsten Eisenträger and Kristin Estella Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. *math/0405305*, May 2004. (Cited on page 184.)

[81] Noam David Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998. (Cited on page 107.)

[82] Andreas Enge. *Elliptic Curves and Their Applications to Cryptography: An Introduction*. Springer, 1st edition, August 1999. (Cited on pages 99 and 105.)

[83] Andreas Enge. How to distinguish hyperelliptic curves in even characteristic. In *Public-key cryptography and computational number theory (Warsaw, 2000)*, pages 49–58. de Gruyter, Berlin, 2001. (Cited on page 106.)

[84] Andreas Enge. *Courbes Algébriques et Cryptologie*. Hdr, Université Paris-Diderot - Paris VII, December 2007. (Cited on page 154.)

[85] Andreas Enge. The complexity of class polynomial computation via floating point approximations. *Math. Comput.*, 78(266):1089–1107, 2009. (Cited on page 152.)

[86] Andreas Enge and François Morain. Generalised Weber functions. I. *0905.3250*, May 2009. (Cited on page 153.)

[87] Andreas Enge and Reinhard Schertz. Constructing elliptic curves over finite fields using double eta-quotients. *J. Théor. Nombres Bordeaux*, 16(3):555–568, 2004. (Cited on pages 153 and 154.)

[88] Michel Fabrikant. *Guide des montagnes corses*. Guides et cartes Didier et Richard. Didier et Richard, 1982. (Cited on page xi.)

[89] Keqin Feng, Qunying Liao, and Jing Yang. Maximal values of generalized algebraic immunity. *Des. Codes Cryptography*, 50(2):243–252, 2009. (Cited on pages 8, 12, and 221.)

[90] Claus Fieker and David Russell Kohel, editors. *Algorithmic Number Theory, 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002, Proceedings*, volume 2369 of *Lecture Notes in Computer Science*. Springer, 2002. (Cited on pages 195 and 201.)

[91] Jean-Pierre Flori and Sihem Mesnager. An efficient characterization of a family of hyperbent functions with multiple trace terms. Cryptology ePrint Archive, Report 2011/373, 2011. `http://eprint.iacr.org/`. (Cited on page 110.)

[92] Jean-Pierre Flori, Sihem Mesnager, and Gérard Denis Cohen. Binary Kloosterman sums with value 4. In Liqun Chen, editor, *IMA Int. Conf.*, volume 7089 of *Lecture Notes in Computer Science*, pages 61–78. Springer, 2011. (Cited on page 110.)

[93] Jean-Pierre Flori, Sihem Mesnager, and Gérard Denis Cohen. The value 4 of binary Kloosterman sums. Cryptology ePrint Archive, Report 2011/364, 2011. `http://eprint.iacr.org/`. (Cited on page 110.)

[94] Jean-Pierre Flori and Hugues Randriam. On the number of carries occurring in an addition mod $2^k - 1$. To appear in Integers journal, 2011. `http://www.integers-ejcnt.org/`. (Cited on page 20.)

[95] Jean-Pierre Flori and Hugues Randriam. On the number of carries occurring in an addition mod $2^k - 1$. Cryptology ePrint Archive, Report 2011/245, 2011. `http://eprint.iacr.org/`. (Cited on page 20.)

[96] Jean-Pierre Flori, Hugues Randriam, Gérard Denis Cohen, and Sihem Mesnager. On a conjecture about binary strings distribution. In Claude Carlet and Alexander Pott, editors, *SETA*, volume 6338 of *Lecture Notes in Computer Science*, pages 346–358. Springer, 2010. (Cited on page 20.)

[97] Jean-Pierre Flori, Hugues Randriam, Gérard Denis Cohen, and Sihem Mesnager. On a conjecture about binary strings distribution. Cryptology ePrint Archive, Report 2010/170, 2010. `http://eprint.iacr.org/`. (Cited on page 20.)

[98] Mireille Fouquet, Pierrick Gaudry, and Robert Harley. An extension of Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, 15(4):281–318, 2000. (Cited on pages 107 and 123.)

[99] Harold Fredricksen and Irving J. Kessler. An algorithm for generating necklaces of beads in two colors. *Discrete Mathematics*, 61(2-3):181–188, 1986. (Cited on page 89.)

[100] Harold Fredricksen and James Maiorana. Necklaces of beads in k colors and k-ary de Bruijn sequences. *Discrete Math.*, 23(3):207–210, 1978. (Cited on page 89.)

[101] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *J. Cryptology*, 23(2):224–280, 2010. (Cited on page 157.)

[102] David Freeman, Peter Stevenhagen, and Marco Streng. Abelian varieties with prescribed embedding degree. In van der Poorten and Stein [271], pages 60–73. (Cited on page 183.)

[103] David Mandell Freeman. *Constructing Abelian Varieties for Pairing-Based Cryptography.* PhD thesis, University of California, Berkeley, 2008. (Cited on page 184.)

[104] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206):865–874, 1994. (Cited on pages 137 and 155.)

[105] Harry Furstenberg. Algebraic functions over finite fields. *J. Algebra*, 7:271–277, 1967. (Cited on page 73.)

[106] Edgar Gabriel, Graham Edward Fagg, George Bosilca, Thara Angskun, Jack J. Dongarra, Jeffrey Michael Squyres, Vishal Sahay, Prabhanjan Kambadur, Brian Barrett, Andrew Lumsdaine, Ralph Henri Castain, David J. Daniel, Richard Lewis Graham, and Timothy S. Woodall. Open MPI: Goals, concept, and design of a next generation MPI implementation. In *Proceedings, 11th European PVM/MPI Users' Group Meeting*, pages 97–104, Budapest, Hungary, September 2004. (Cited on pages 89 and 227.)

[107] Steven D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, 2011. `http://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html`. (Cited on pages 99 and 105.)

[108] Kseniya Garaschuk and Petr Lisoněk. On binary Kloosterman sums divisible by 3. *Des. Codes Cryptography*, 49(1-3):347–357, 2008. (Cited on page 120.)

[109] Pierrick Gaudry. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. In Yuliang Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 311–327. Springer, 2002. (Cited on page 107.)

[110] Pierrick Gaudry. Hyperelliptic curves and the HCDLP. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 133–150. Cambridge Univ. Press, Cambridge, 2005. (Cited on page 105.)

[111] Pierrick Gaudry and Robert Harley. Counting points on hyperelliptic curves over finite fields. In Wieb Bosma, editor, *ANTS*, volume 1838 of *Lecture Notes in Computer Science*, pages 313–332. Springer, 2000. (Cited on page 107.)

[112] Pierrick Gaudry, Thomas Houtmann, David Russell Kohel, Christophe Ritzenthaler, and Annegret Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In Lai and Chen [158], pages 114–129. (Cited on page 184.)

[113] Pierrick Gaudry and Éric Schost. Construction of secure random curves of genus 2 over prime fields. In Cachin and Camenisch [34], pages 239–256. (Cited on page 107.)

[114] Alice Chia Ping Gee. Class invariants by Shimura's reciprocity law. *J. Théor. Nombres Bordeaux*, 11(1):45–72, 1999. Les XXèmes Journées Arithmétiques (Limoges, 1997). (Cited on page 153.)

[115] Alice Chia Ping Gee. *Class fields by Shimura reciprocity.* PhD thesis, Universiteit Leiden, 2001. (Cited on page 153.)

[116] Alice Chia Ping Gee and Peter Stevenhagen. Generating class fields using Shimura reciprocity. In Joe Buhler, editor, *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 441–453. Springer, 1998. (Cited on page 153.)

[117] Johann Wolfgang von Goethe. *Faust. Eine Tragödie von Goethe.* J. G. Cotta, 1808. (Cited on page 217.)

[118] Guang Gong and Solomon Wolf Golomb. Transform domain analysis of DES. *IEEE Transactions on Information Theory*, 45(6):2065–2073, 1999. (Cited on page 96.)

[119] Eyal Zvi Goren and Kristin Estella Lauter. Class invariants for quartic CM fields. *Ann. Inst. Fourier (Grenoble)*, 57(2):457–480, 2007. (Cited on page 184.)

[120] Eyal Zvi Goren and Kristin Estella Lauter. Genus 2 curves with complex multiplication. *International Mathematics Research Notices*, 2011. (Cited on page 184.)

[121] Aline Gouget and Hervé Sibert. Revisiting correlation-immunity in filter generators. In Carlisle Michael Adams, Ali Miri, and Michael James Wiener, editors, *Selected Areas in Cryptography*, volume 4876 of *Lecture Notes in Computer Science*, pages 378–395. Springer, 2007. (Cited on page 10.)

[122] Ronald Lewis Graham, Donald Ervin Knuth, and Oren Patashnik. *Concrete mathematics.* Addison-Wesley Publishing Company, Reading, MA, second edition, 1994. A foundation for computer science. (Cited on pages 34, 54, and 55.)

[123] Faruk Göloğlu, Petr Lisoněk, Gary McGuire, and Richard Moloney. Binary Kloosterman sums modulo 256 and coefficients of the characteristic polynomial. *Information Theory, IEEE Transactions on*, PP(99):1, 2012. (Cited on page 120.)

[124] Faruk Göloğlu, Gary McGuire, and Richard Moloney. Binary Kloosterman sums using Stickelberger's theorem and the Gross-Koblitz formula. *Acta Arith.*, 148(3):269–279, 2011. (Cited on page 120.)

[125] Franz Halter-Koch. Ideal semigroups of Noetherian domains and Ponizovski decompositions. *J. Pure Appl. Algebra*, 209(3):763–770, 2007. (Cited on page 177.)

[126] Robert Harley. Asymptotically optimal p-adic point-counting. Email to NMBRTHRY list, December 2002. `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L=nmbrthry&T=0&P=1343`. (Cited on pages 107, 121, 123, and 230.)

[127] William Hart, Sebastian Pancratz, Andy Novocin, Fredrik Johansson, and David Harvey. *FLINT: Fast Library for Number Theory – Version 2.2*, june 2011. `www.flintlib.org`. (Cited on pages 89 and 227.)

[128] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. (Cited on pages 133, 134, and 135.)

[129] Tor Helleseth and Victor Zinoviev. On Z_4 linear Goethals codes and Kloosterman sums. *Des. Codes Cryptography*, 17(1-3):269–288, 1999. (Cited on pages 119, 120, and 231.)

[130] Florian Heß. A note on the Tate pairing of curves over finite fields. *Arch. Math. (Basel)*, 82(1):28–32, 2004. (Cited on page 137.)

[131] Florian Heß, Nigel Paul Smart, and Frederik Vercauteren. The eta pairing revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006. (Cited on page 155.)

[132] Marc Hindry and Joseph Hillel Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction. (Cited on pages 161 and 162.)

[133] Laura Hitt. On the minimal embedding field. In Tsuyoshi Takagi, Tatsuaki Okamoto, Eiji Okamoto, and Takeshi Okamoto, editors, *Pairing*, volume 4575 of *Lecture Notes in Computer Science*, pages 294–301. Springer, 2007. (Cited on page 155.)

[134] Laura Hitt O'Connor, Gary McGuire, Michael Naehrig, and Marco Streng. A CM construction for curves of genus 2 with p-rank 1. *J. Number Theory*, 131(5):920–935, 2011. (Cited on page 183.)

[135] Hendrik Hubrechts. *Computing zeta functions of curves over finite fields*. PhD thesis, Katholieke Universiteit Leuven, 2003. (Cited on page 107.)

[136] Hendrik Hubrechts. Point counting in families of hyperelliptic curves in characteristic 2. *LMS J. Comput. Math.*, 10:207–234, 2007. (Cited on page 107.)

[137] Hendrik Hubrechts. Point counting in families of hyperelliptic curves. *Foundations of Computational Mathematics*, 8(1):137–169, 2008. (Cited on page 107.)

[138] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. (Cited on page 99.)

[139] Jun-ichi Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960. (Cited on pages 159 and 181.)

[140] The OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. `http://oeis.org`. (Cited on page 26.)

[141] Michael Jacobson, Jr., Alfred John Menezes, and Andreas Stein. Hyperelliptic curves and cryptography. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 255–282. Amer. Math. Soc., Providence, RI, 2004. (Cited on page 105.)

[142] Qingfang Jin, Zhuojun Liu, and Baofeng Wu. 1-resilient Boolean function with optimal algebraic immunity. Cryptology ePrint Archive, Report 2011/549, 2011. `http://eprint.iacr.org/`. (Cited on pages 17 and 20.)

[143] Qingfang Jin, Zhuojun Liu, Baofeng Wu, and Xiaoming Zhang. A general conjecture similar to T-D conjecture and its applications in constructing Boolean functions with optimal algebraic immunity. Cryptology ePrint Archive, Report 2011/515, 2011. `http://eprint.iacr.org/`. (Cited on pages 8, 16, 17, 23, 221, and 222.)

[144] Nicholas Katz and Ron Livné. Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989. (Cited on pages 104, 105, 110, 114, and 230.)

[145] Kiran Sridhara Kedlaya. Complex multiplication and explicit class field theory, April 1996. (Cited on pages 149, 151, and 237.)

[146] Kiran Sridhara Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001. (Cited on page 107.)

[147] Kiran Sridhara Kedlaya. Errata for: "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology" [J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338; mr1877805]. *J. Ramanujan Math. Soc.*, 18(4):417–418, 2003. Dedicated to Professor Karaikurichi Srinivasan Padmanabhan. (Cited on page 107.)

[148] Brian Wilson Kernighan and Dennis MacAlistair Ritchie. *C Programming Language*. Prentice Hall, 2 edition, April 1988. (Cited on pages 2, 89, and 227.)

[149] Jean-Louis Kerouac. *The Dharma Bums*. Penguin classics. Penguin Books, 2000. (Cited on page 131.)

[150] Hae Young Kim, Jung Youl Park, Jung Hee Cheon, Je Hong Park, Jae Heon Kim, and Sang Geun Hahn. Fast elliptic curve point counting using Gaussian normal basis. In Fieker and Kohel [90], pages 292–307. (Cited on page 107.)

[151] Jürgen Klüners and Sebastian Pauli. Computing residue class rings and Picard groups of orders. *J. Algebra*, 292(1):47–64, 2005. (Cited on pages 160, 170, and 171.)

[152] Anthony William Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992. (Cited on page 99.)

[153] Neal Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987. (Cited on page 153.)

[154] Neal Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. In Alfred John Menezes and Scott Alexander Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 156–167. Springer, 1990. (Cited on pages 99 and 105.)

[155] Neal Koblitz. *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. With an appendix by Alfred John Menezes, Yi-Hong Wu and Robert Joseph Zuccherato. (Cited on page 99.)

[156] Gilles Lachaud and Jacques Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(20):881–883, 1987. (Cited on pages 110, 114, and 230.)

[157] Gilles Lachaud and Jacques Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Transactions on Information Theory*, 36(3):686Ð692, 1990. (Cited on pages 110, 111, and 119.)

[158] Xuejia Lai and Kefei Chen, editors. *Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3-7, 2006, Proceedings*, volume 4284 of *Lecture Notes in Computer Science*. Springer, 2006. (Cited on pages 198 and 203.)

[159] Serge Lang. *Complex multiplication*, volume 255 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983. (Cited on pages 160, 162, 164, 165, 167, 168, 172, 173, 174, 175, 176, 177, 178, 179, 180, 240, and 241.)

[160] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate. (Cited on pages 105, 139, 143, 144, 145, 149, 150, 151, 152, 153, 172, and 237.)

[161] Philippe Langevin, Nils-Gregor Leander, Gary Mcguire, and Eugen Zalinescu. Analysis of Kasami-Welch functions in odd dimension using Stickelberger's theorem. *Journal of Combinatorics and Number Theory*, 2(1):55 – 72, 2011. (Cited on page 21.)

[162] Alan George Beattie Lauder. Deformation theory and the computation of zeta functions. *Proc. London Math. Soc. (3)*, 88(3):565–602, 2004. (Cited on page 107.)

[163] Alan George Beattie Lauder and Daqing Wan. Computing zeta functions of Artin-Schreier curves over finite fields. *LMS J. Comput. Math.*, 5:34–55, 2002. (Cited on page 107.)

[164] Alan George Beattie Lauder and Daqing Wan. Computing zeta functions of Artin-Schreier curves over finite fields II. *J. Complexity*, 20(2-3):331–349, 2004. (Cited on page 107.)

[165] Alan George Beattie Lauder and Daqing Wan. Counting points on varieties over finite fields of small characteristic. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 579–612. Cambridge Univ. Press, Cambridge, 2008. (Cited on page 107.)

[166] Kristin Estella Lauter and Damien Robert. About the CRT method to compute class polynomials in dimension 2. Talk given at the "Journées Codage et Cryptographie 2011", slides available at `http://www2.lirmm.fr/c2/programme.html`, April 2011. (Cited on page 184.)

[167] Nils-Gregor Leander. Monomial bent functions. *IEEE Transactions on Information Theory*, 52(2):738–743, 2006. (Cited on pages 110 and 111.)

[168] John Marshall Lee. *Introduction to smooth manifolds*, volume 218 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003. (Cited on page 161.)

[169] Hendrik Willem Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987. (Cited on page 153.)

[170] Franck Leprévost, Michael Pohst, and Osmanbey Uzunkol. On the computation of class polynomials with "thetanullwerte" and its applications to the unit group computation, 2009. To appear in Experimental Mathematics. (Cited on page 153.)

[171] Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. PhD thesis, École Polytechnique, June 1997. (Cited on page 107.)

[172] Reynald Lercier and David Lubicz. Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time. In Biham [15], pages 360–373. (Cited on page 107.)

[173] Reynald Lercier and David Lubicz. A quasi quadratic time algorithm for hyperelliptic curve point counting. *Ramanujan J.*, 12(3):399–423, 2006. (Cited on page 107.)

[174] Reynald Lercier, David Lubicz, and Frederik Vercauteren. Point counting on elliptic and hyperelliptic curves. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 407–453. Chapman & Hall/CRC, Boca Raton, FL, 2006. (Cited on pages 107 and 121.)

[175] Reynald Lercier and Christophe Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *arXiv:1111.4152*, November 2011. (Cited on page 182.)

[176] Reynald Lercier and Christophe Ritzenthaler. Reconstruction of genus 3 hyperellitpic curve. Talk given at GeoCrypt 2011, slides available at `http://iml.univ-mrs.fr/ati/GeoCrypt2011/`, June 2011. (Cited on page 182.)

[177] Na Li and Wen-Feng Qi. Construction and analysis of Boolean functions of $2t + 1$ variables with maximum algebraic immunity. In Lai and Chen [158], pages 84–98. (Cited on page 11.)

[178] Na Li, Longjiang Qu, Wen-Feng Qi, GuoZhu Feng, Chao Li, and DuanQiang Xie. On the construction of Boolean functions with optimal algebraic immunity. *IEEE Transactions on Information Theory*, 54(3):1330–1334, 2008. (Cited on page 11.)

[179] Rudolf Lidl, Gary Lee Mullen, and Gerhard Turnwald. *Dickson polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow, 1993. (Cited on pages 99 and 228.)

[180] Petr Lisoněk. On the connection between Kloosterman sums and elliptic curves. In Solomon Wolf Golomb, Matthew Geoffrey Parker, Alexander Pott, and Arne Winterhof, editors, *SETA*, volume 5203 of *Lecture Notes in Computer Science*, pages 182–187. Springer, 2008. (Cited on pages 110, 115, 120, 122, and 231.)

[181] Petr Lisoněk. An efficient characterization of a family of hyperbent functions. *IEEE Transactions on Information Theory*, 57(9):6010–6014, 2011. (Cited on pages 110, 115, 116, and 233.)

[182] Petr Lisoněk. Hyperbent functions and hyperelliptic curves. Talk given at Arithmetic, Geometry, Cryptography and Coding Theory (AGCT-13), slides available at `http://iml.univ-mrs.fr/~ritzenth/AGCT/talks/lisonek.pdf`, March 2011. (Cited on pages 110, 115, 116, and 233.)

[183] Petr Lisoněk and Marko J. Moisio. On zeros of Kloosterman sums. *Des. Codes Cryptography*, 59(1-3):223–230, 2011. (Cited on page 110.)

[184] Mikhail Sergeevich Lobanov. Exact relations between nonlinearity and algebraic immunity. *Diskretn. Anal. Issled. Oper.*, 15(6):34–47, 95, 2008. (Cited on page 11.)

[185] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes. I.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16. (Cited on page 13.)

[186] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes. II.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16. (Cited on page 13.)

[187] James Lee Massey. Shift-register synthesis and BCH decoding. *Information Theory, IEEE Transactions on*, 15(1):122 – 127, jan 1969. (Cited on pages 10 and 219.)

[188] Mitsuru Matsui. Linear cryptoanalysis method for DES cipher. In *EUROCRYPT*, pages 386–397, 1993. (Cited on page 96.)

[189] Mitsuru Matsui and Atsuhiro Yamagishi. A new method for known plaintext attack of FEAL cipher. In *EUROCRYPT*, pages 81–91, 1992. (Cited on page 96.)

[190] Willi Meier, Enes Pasalic, and Claude Carlet. Algebraic attacks and decomposition of Boolean functions. In Cachin and Camenisch [34], pages 474–491. (Cited on page 10.)

[191] Willi Meier and Othmar Staffelbach. Fast correlation attacks on stream ciphers (extended abstract). In *EUROCRYPT*, pages 301–314, 1988. (Cited on pages 11 and 220.)

[192] Alfred John Menezes, Tatsuaki Okamoto, and Scott Alexander Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993. (Cited on pages 155 and 156.)

[193] Alfred John Menezes, Paul C. van Oorschot, and Scott Alexander Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. (Cited on pages 8, 10, and 219.)

[194] Alfred John Menezes, Yi-Hong Wu, and Robert Joseph Zuccherato. An elementary introduction to hyperelliptic curves. In *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. (Cited on page 105.)

[195] Sihem Mesnager. A new family of hyper-bent Boolean functions in polynomial form. In Matthew Geoffrey Parker, editor, *IMA Int. Conf.*, volume 5921 of *Lecture Notes in Computer Science*, pages 402–417. Springer, 2009. (Cited on pages 111, 112, and 231.)

[196] Sihem Mesnager. Hyper-bent Boolean functions with multiple trace terms. In Mohammed Anwar Hasan and Tor Helleseth, editors, *WAIFI*, volume 6087 of *Lecture Notes in Computer Science*, pages 97–113. Springer, 2010. (Cited on pages 110, 113, and 232.)

[197] Sihem Mesnager. A new class of bent and hyper-bent Boolean functions in polynomial forms. *Des. Codes Cryptography*, 59(1-3):265–279, 2011. (Cited on pages 111, 112, 115, and 124.)

[198] Sihem Mesnager. Semibent functions from Dillon and Niho exponents, Kloosterman sums, and Dickson polynomials. *Information Theory, IEEE Transactions on*, 57(11):7443 –7458, nov. 2011. (Cited on pages 110, 111, and 112.)

[199] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991. (Cited on page 182.)

[200] Jean-François Mestre. Lettre addressée à Gaudry et Harley, December 2000. `http://www.math.jussieu.fr/~mestre`. (Cited on page 107.)

[201] Jean-François Mestre. Applications de l'AGM au calcul du nombre de points d'une courbe de genre 1 ou 2 sur $\mathbb{F}_{2^n}$, March 2002. Talk given to the Séminaire de Cryptographie de l'Université de Rennes, slides available at `http:/www.maths.univ-rennes1.fr/crypto/2001-02/Mestre2203.html`. (Cited on page 107.)

[202] Victor Saul Miller. Use of elliptic curves in cryptography. In Hugh Cowie Williams, editor, *CRYPTO*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1985. (Cited on page 153.)

[203] Victor Saul Miller. Short programs for functions on curves. *Unpublished manuscript*, 1986. (Cited on page 138.)

[204] James Stuart Milne. Abelian varieties. `http://www.jsmilne.org/math/`. (Cited on pages 160, 161, 163, 165, 166, 167, 168, 174, 181, and 238.)

[205] James Stuart Milne. Complex multiplication. `http://www.jsmilne.org/math/`. (Cited on pages 160, 162, 164, 173, 174, 175, 176, 177, 178, 179, 180, 239, 240, and 241.)

[206] Richard Moloney. *Divisibility Properties of Kloosterman Sums and Division Polynomials for Edward Curves*. PhD thesis, University College Dublin, may 2011. (Cited on page 119.)

[207] Michael Burnett Monagan, Keith Oliver Geddes, K. Michael Heal, George Labahn, Stefan M. Vorkoetter, James McCarron, and Paul DeMarco. *Maple 10 Programming Guide*. Maplesoft, Waterloo ON, Canada, 2005. (Cited on page 2.)

[208] Paul Monsky. Formal cohomology. II. The cohomology sequence of a pair. *Ann. of Math. (2)*, 88:218–238, 1968. (Cited on page 107.)

[209] Paul Monsky. *p-adic analysis and zeta functions*, volume 4 of *Lectures in Mathematics, Department of Mathematics, Kyoto University*. Kinokuniya Book-Store Co. Ltd., Tokyo, 1970. (Cited on page 107.)

[210] Paul Monsky. Formal cohomology. III. Fixed point theorems. *Ann. of Math. (2)*, 93:315–343, 1971. (Cited on page 107.)

[211] Paul Monsky and Gerard Washnitzer. Formal cohomology. I. *Ann. of Math. (2)*, 88:181–217, 1968. (Cited on page 107.)

[212] Charles Mugler. *Œuvres : Des corps flottants. Stomachion. Le méthode. Le livre des lemmes. Le problème des bœufs*. Œuvres. Les Belles lettres, 2002. (Cited on page 19.)

[213] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970. (Cited on pages 160, 161, 162, 163, 164, 165, 166, 167, 168, and 175.)

[214] Volker Müller. *Ein Algorithmus zur Bestimmung der Punktzahl elliptischer Kurven über endlischen Körpern der Charakteristik größer drei*. PhD thesis, Üniversität des Saarlandes, 1995. (Cited on page 107.)

[215] Michael Naehrig. *Constructive and Computational Aspects of Cryptographic Pairings*. PhD thesis, Eindhoven University of Technology, 2009. (Cited on page 157.)

[216] Jürgen Neukirch. Algebraische Zahlentheorie. In *Ein Jahrhundert Mathematik 1890–1990*, volume 6 of *Dokumente Gesch. Math.*, pages 587–628. Vieweg, Braunschweig, 1990. (Cited on pages 149, 169, 170, and 237.)

[217] Brian Osserman. Orders and their class groups. `http://www.math.ucdavis.edu/~osserman/seminar/orders.ps`. (Cited on page 169.)

[218] The PARI Group, Bordeaux. *PARI/GP, version* `2.4.3`, October 2010. available from `http://pari.math.u-bordeaux.fr/`. (Cited on pages 123 and 170.)

[219] Birgit Pfitzmann, editor. *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, volume 2045 of *Lecture Notes in Computer Science*. Springer, 2001. (Cited on page 209.)

[220] Jonathan S. Pila. *Frobenius maps of Abelian varieties and finding roots of unity in finite fields*. ProQuest LLC, Ann Arbor, MI, 1988. Thesis (Ph.D.)–Stanford University. (Cited on page 107.)

[221] Marcel Proust and Thierry Laget. *Le côté de Guermantes*. À la recherche du temps perdu. Gallimard, 1994. (Cited on page 7.)

[222] Oscar Seymour Rothaus. On "bent" functions. *J. Comb. Theory, Ser. A*, 20(3):300–305, 1976. (Cited on pages 13 and 96.)

[223] Jean-Jacques Rousseau. *Les confessions*. Les confessions. s.n., 1782. (Cited on page 95.)

[224] Frank Ruskey. *Combinatorial Generation*. Unpublished manuscript, 2003. Working Version (1j-CSC 425/520). (Cited on page 89.)

[225] Frank Ruskey, Carla Diane Savage, and Terry Min Yih Wang. Generating necklaces. *J. Algorithms*, 13(3):414–430, 1992. (Cited on page 89.)

[226] Sondre Rønjom and Tor Helleseth. A new attack on the filter generator. *IEEE Transactions on Information Theory*, 53(5):1752–1758, 2007. (Cited on pages 10 and 219.)

[227] Peter Sarnak. Selberg's eigenvalue conjecture. *Notices Amer. Math. Soc.*, 42(11):1272–1277, 1995. (Cited on page 153.)

[228] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000. (Cited on pages 107 and 121.)

[229] Takakazu Satoh, Berit Skjernaa, and Yuichiro Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields Appl.*, 9(1):89–101, 2003. (Cited on page 107.)

[230] Reinhard Schertz. Weber's class invariants revisited. *J. Théor. Nombres Bordeaux*, 14(1):325–343, 2002. (Cited on page 153.)

[231] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985. (Cited on page 107.)

[232] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Comb. Theory, Ser. A*, 46(2):183–211, 1987. (Cited on pages 104 and 146.)

[233] René Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993). (Cited on page 107.)

[234] Jean-Pierre Serre. Géométrie algébrique et géométrie analytique. *Ann. Inst. Fourier, Grenoble*, 6:1–42, 1955–1956. (Cited on page 167.)

[235] Adi Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pages 47–53, 1984. (Cited on page 156.)

[236] Claude Elwood Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28:656–715, 1949. (Cited on page 8.)

[237] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1. (Cited on pages 178 and 240.)

[238] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998. (Cited on pages 160, 162, 165, 177, 178, 179, 180, and 241.)

[239] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961. (Cited on page 160.)

[240] Tetsuji Shioda. On the graded ring of invariants of binary octavics. *Amer. J. Math.*, 89:1022–1046, 1967. (Cited on page 182.)

[241] Victor Shoup. NTL 5.4.2: A library for doing number theory, March 2008. `www.shoup.net/ntl`. (Cited on page 126.)

[242] Carl Ludwig Siegel. *Analytic functions of several complex variables*. Lectures delivered at the Institute for Advanced Study, 1948–1949, With notes by Paul Trevier Bateman, Reprint of the 1950 edition. Kendrick Press, Heber City, UT, 2008. (Cited on page 161.)

[243] Thomas Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, 30(5):776–, 1984. (Cited on pages 9 and 10.)

[244] Joseph Hillel Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original. (Cited on pages 99, 100, 103, 104, 132, 133, 134, 135, 136, 137, 138, 139, 142, 143, 147, 228, and 230.)

[245] Joseph Hillel Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. (Cited on pages 132, 139, 141, 142, 148, 149, 150, 151, 152, 235, and 237.)

[246] Joseph Hillel Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. (Cited on page 99.)

[247] Berit Skjernaa. Satoh's algorithm in characteristic 2. *Math. Comput.*, 72(241):477–487, 2003. (Cited on page 107.)

[248] Anne-Monika Spallek. *Kurven von Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Universität Gesamthochschule Essen, 1994. (Cited on pages 160 and 182.)

[249] Richard Peter Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original. (Cited on page 86.)

[250] William Arthur Stein et al. *Sage Mathematics Software (Version 4.7)*. The Sage Development Team, 2011. `http://www.sagemath.org`. (Cited on pages 2, 26, 43, 47, 48, 123, 126, 160, 187, 219, and 231.)

[251] Peter Stevenhagen. Number rings. `http://websites.math.leidenuniv.nl/algebra/ant.pdf`. (Cited on pages 168 and 169.)

[252] Marco Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Universiteit Leiden, 2010. (Cited on pages 160, 173, 179, 182, 183, 184, and 241.)

[253] Marco Streng. An explicit version of Shimura's reciprocity law for Siegel modular functions. *arXiv:1201.0020*, December 2011. (Cited on page 184.)

[254] Marco Streng. Smaller class invariants for constructing curves of genus 2. Talk given at GeoCrypt 2011, slides available at `http://iml.univ-mrs.fr/ati/GeoCrypt2011`, June 2011. (Cited on page 184.)

[255] Marco Streng. Smaller class invariants for constructing curves of genus 2. Talk given at ECC 2011, slides available at `http://ecc2011.loria.fr/program.html`, September 2011. (Cited on page 184.)

[256] Stupeflip. Stupeflip, January 2003. (Cited on page 1.)

[257] Andrew Victor Sutherland. Accelerating the CM method. *1009.1082*, September 2010. (Cited on page 153.)

[258] Andrew Victor Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem. *Math. Comput.*, 80(273):501–538, 2011. (Cited on page 153.)

[259] Deng Tang, Claude Carlet, and Xiaohu Tang. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. Cryptology ePrint Archive, Report 2011/366, 2011. `http://eprint.iacr.org/`. (Cited on pages 3, 8, 12, 15, 16, 17, 21, 23, 24, 25, 221, and 222.)

[260] Xiaohu Tang, Deng Tang, Xiangyong Zeng, and Lei Hu. Balanced Boolean functions with (almost) optimal algebraic immunity and very high nonlinearity. Cryptology ePrint Archive, Report 2010/443, 2010. `http://eprint.iacr.org/`. (Cited on pages 14 and 16.)

[261] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966. (Cited on page 174.)

[262] Ziran Tu and Yingpu Deng. Boolean functions with all main cryptographic properties. Cryptology ePrint Archive, Report 2010/518, 2010. `http://eprint.iacr.org/`. (Cited on pages 14 and 17.)

[263] Ziran Tu and Yingpu Deng. A class of 1-resilient function with high nonlinearity and algebraic immunity. Cryptology ePrint Archive, Report 2010/179, 2010. `http://eprint.iacr.org/`. (Cited on page 14.)

[264] Ziran Tu and Yingpu Deng. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. *Des. Codes Cryptography*, 60(1):1–14, 2011. (Cited on pages 8, 12, 13, 14, 15, 16, 21, 29, 86, 90, 221, and 222.)

[265] `http://gcc.gnu.org`. *GCC, the GNU Compiler Collection – Version 4.6.1*, 2011. `http://gcc.gnu.org`. (Cited on page 89.)

[266] `http://python.org`. *Python Programming Language – Version 2.6*, 2011. `http://python.org`. (Cited on page 2.)

[267] `Maxima.sourceforge.net`. *Maxima, a Computer Algebra System (Version 5.23.2)*, 2011. `http://maxima.sourceforge.net`. (Cited on pages 48, 49, and 187.)

[268] `Pynac.sagemath.net`. *Pynac, symbolic computation with Python objects (Version 0.2.2)*, 2011. `http://pynac.sagemath.org`. (Cited on pages 48, 49, and 187.)

[269] Osmanbey Uzunkol. *Über die Konstruktion algebraischer Kurven mittels komplexer Multiplikation*. PhD thesis, Technischen Universität Berlin, 2010. (Cited on pages 153 and 184.)

[270] Gerard van der Geer and Ben Moonen. *Abelian Varieties*. None, 2011. `http://staff.science.uva.nl/~bmoonen/boek/BookAV.html`. (Cited on pages 163 and 168.)

[271] Alfred Jacobus van der Poorten and Andreas Stein, editors. *Algorithmic Number Theory, 8th International Symposium, ANTS-VIII, Banff, Canada, May 17-22, 2008, Proceedings*, volume 5011 of *Lecture Notes in Computer Science*. Springer, 2008. (Cited on pages 191, 192, and 198.)

[272] Jacobus Hendrikus van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 1999. (Cited on page 13.)

[273] Paul Bastiaan van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comput.*, 68(225):307–320, 1999. (Cited on pages 160, 178, and 240.)

[274] Frederik Vercauteren. Advances in point counting. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 103–132. Cambridge Univ. Press, Cambridge, 2005. (Cited on pages 107 and 121.)

[275] Frederik Vercauteren. *Computing zeta functions of curves over finite fields*. PhD thesis, Katholieke Universiteit Leuven, 2007. (Cited on pages 107, 108, 121, 123, and 230.)

[276] Frederik Vercauteren, Bart Preneel, and Joos Vandewalle. A memory efficient version of Satoh's algorithm. In Pfitzmann [219], pages 1–13. (Cited on page 107.)

[277] Qichun Wang and Thomas Johansson. A note on fast algebraic attacks and higher order nonlinearities. In Xuejia Lai, Moti Yung, and Dongdai Lin, editors, *Information Security and Cryptology*, volume 6584 of *Lecture Notes in Computer Science*, pages 404–414. Springer Berlin / Heidelberg, 2011. 10.1007/978-3-642-21518-6-28. (Cited on page 15.)

[278] Qichun Wang, Jie Peng, Haibin Kan, and Xiangyang Xue. Constructions of cryptographically significant Boolean functions using primitive polynomials. *IEEE Transactions on Information Theory*, 56(6):3048–3053, 2010. (Cited on page 12.)

[279] Lawrence Clinton Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography. (Cited on page 99.)

[280] William Charles Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969. (Cited on pages 104, 160, 163, 167, and 179.)

[281] Heinrich Weber. *Lehrbuch der Algebra*. Chelsea Pub Co, 3rd reprint edition, July 1979. (Cited on page 153.)

[282] André Weil. On the theory of complex multiplication. In *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955*, pages 9–22, Tokyo, 1956. Science Council of Japan. (Cited on page 166.)

[283] Annegret Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*. PhD thesis, Universität GH Essen, 2001. (Cited on pages 160 and 182.)

[284] Kim-Ee Yeoh. GP/Pari implementation of point counting in characteristic 2. `http://pages.cs.wisc.edu/~yeoh/nt/satoh-fgh.gp`. (Cited on page 123.)

[285] Amr Mohamed Youssef and Guang Gong. Hyper-bent functions. In Pfitzmann [219], pages 406–419. (Cited on page 96.)

[286] Chia-Fu Yu. The isomorphism classes of abelian varieties of CM-type. *J. Pure Appl. Algebra*, 187(1-3):305–319, 2004. (Cited on page 174.)

Index

D

E

Résumé long

Faust.

Werd' ich beruhigt je mich auf ein Faulbett legen,
So sey es gleich um mich gethan!
Kannst du mich schmeichelnd je belügen,
Daß ich mir selbst gefallen mag,
Kannst du mich mit Genuß betrügen;
Das sey für mich der letzte Tag!
Die Wette biet' ich!

Mephistopheles.

Top!

Faust.

Und Schlag auf Schlag!
Werd' ich zum Augenblicke sagen:
Verweile doch! du bist so schön!
Dann magst du mich in Fesseln schlagen,
Dann will ich gern zu Grunde gehn!
Dann mag die Todtenglocke schallen,
Dann bist du deines Dienstes frey,
Die Uhr mag stehn, der Zeiger fallen,
Es sey die Zeit für mich vorbey!

Mephistopheles.

Bedenk' es wohl, wir werden's nicht vergessen.

ESTRAGON. — Alors, adieu.
POZZO. — Adieu.
VLADIMIR. — Adieu.
ESTRAGON. — Adieu.
Silence. Personne ne bouge.
VLADIMIR. — Adieu.
POZZO. — Adieu.
ESTRAGON. — Adieu.
Silence.
POZZO. — Et merci.
VLADIMIR. — Merci à vous.
POZZO. — De rien.
ESTRAGON. — Mais si.
POZZO. — Mais non.
VLADIMIR. — Mais si.
ESTRAGON. — Mais non.
Silence.
POZZO. — Je n'arrive pas... (*il hésite*) ...à partir.
ESTRAGON. — C'est la vie.

En attendant Godot
Samuel Beckett [11]

Sommaire

La cryptologie est l'art du secret et de la protection de l'information. Une de ses applications classiques est l'échange d'informations confidentielles entre deux entités. Pour ce faire, deux solutions quelque peu différentes sont possibles : la cryptographie symétrique où les deux entités partagent un même secret et la cryptographie asymétrique où un dissymétrie existe.

Un autre dichotomie est habituelle en cryptologie : les cryptographes conçoivent les systèmes ; les cryptanalystes cherchent à les attaquer. Plus les attaques des seconds sont efficaces, plus le travail des premiers est difficile. La plupart des cryptosystèmes, tout comme les attaques les ébranlant, reposent sur les propriétés mathématiques des objets mis en jeu, et ce, que le système soit symétrique ou asymétrique. Il est donc nécessaire de bien comprendre ces objets et leurs propriétés aussi bien en théorie qu'en pratique. En effet, une étude purement abstraite ne saurait être suffisante pour s'assurer de la robustesse d'un système. Démontrer l'existence d'objets intéressants, mais ne pas savoir les construire n'apportera pas grand chose non plus ; inversement, savoir construire des objets en petites dimensions, mais ne pas savoir démontrer leur existence en général, est tout aussi peu satisfaisant.

Une fois de plus, deux approches sont possibles pour implémenter les objets étudiés : utiliser des logiciels puissants, mais propriétaires, ou se tourner vers le monde du logiciel libre où les solutions sont parfois moins abouties, mais présentent souvent d'autres avantages. C'est cette seconde approche qui a été choisie avec l'utilisation et la contribution au logiciel libre Sage [250].

Dans la Section 1, nous nous intéressons à une conjecture combinatoire dont la validité assure l'existence de fonctions booléennes avec de bonnes propriétés cryptographiques. La première sous-section présente les différentes propriétés attendues d'une fonction booléenne pour un usage cryptographique, ainsi que certaines familles infinies de fonctions les satisfaisant, à condition que la conjecture mentionnée ci-dessus soit vérifiée ; la seconde sous-section donne un certain nombre de résultats concernant cette conjecture, en particulier sa validité dans divers cas. Dans la Section 2, nous concentrons notre attention sur une propriété des fonctions booléennes : la non-linéarité. Et plus particulièrement sur les fonctions courbes et hyper-courbes, c'est-à-dire les fonctions booléennes qui atteignent la non-linéarité maximum. Pour ce faire, un certain nombre d'objets mathématiques sont présentés dans la première sous-section. C'est en particulier le cas des courbes elliptiques et hyperelliptiques qui seront utilisées dans la sous-section suivante. Nous montrerons en effet dans cette seconde sous-section, comment l'utilisation de ces courbes permet de caractériser, mais aussi de construire efficacement, des fonctions courbes. Dans la Section 3, nous étudions les courbes elliptiques et hyperelliptiques d'un point de vue différent : nous cherchons à construire des polynômes de classes à partir de courbes à multiplication complexe. La première sous-section présente le cas classique des courbes elliptiques et du polynôme de classes de Hilbert ; la seconde sous-section les extensions de cette méthode aux courbes hyperelliptiques et en particulier aux courbes de genre deux et aux polynômes d'Igusa dans le cas d'ordre non-maximaux.

1 Des fonctions booléennes et d'une conjecture combinatoire

Dans cette première section, nous nous intéressons à l'utilisation des fonctions booléennes en cryptographie symétrique et plus particulièrement à une conjecture d'ordre combinatoire assurant l'existence de fonctions intéressantes d'un point de vue cryptographique.

1.1 Fonctions booléennes en cryptographie

Une fonction booléenne est une fonction du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_2^n$ de dimension n vers le corps $\mathbb{F}_2$ à deux éléments. Les fonctions booléennes sont une brique fondamentale des systèmes cryptographiques symétriques. Elles sont par exemple utilisées pour construire des boîtes–S dans les systèmes de chiffrement par blocs et pour filtrer, ou combiner, des registres à décalage à rétroaction linéaire (LFSR) dans les systèmes de chiffrement à flot. C'est cette dernière utilisation qui nous intéresse ici et qui est schématisée dans les Figures 1 et 2

Afin d'assurer la sécurité du système cryptographique reposant sur une telle construction, les fonctions booléennes utilisées doivent vérifier un certain nombre de propriétés. Ainsi, elles doivent être :

- équilibrées, i.e. prendre aussi souvent les valeurs 0 et 1, afin d'éviter l'apparition de dépendances statistiques entre les entrées et les sorties du système et la possibilité de concevoir un distingueur ;
- avoir un haut degré algébrique, qui est le multi-degré de la forme polynomiale multivariée de la fonction, afin de résister aux attaques à la Berlekamp–Massey [187], [193, 6.2.3], [38, 4.1.1] et à la Rønjom–Helleseth [226] ;

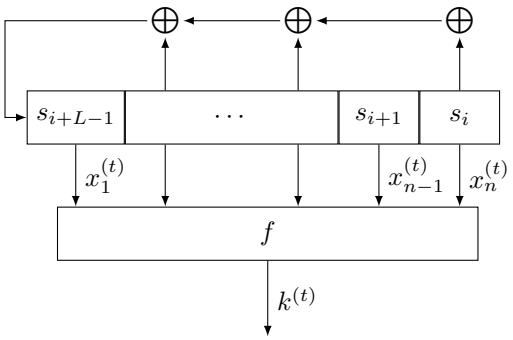


FIGURE 1 – Filtrage de LFSR

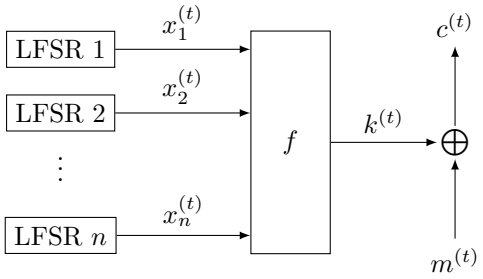


FIGURE 2 – Combinaison de LFSR

- avoir une haute immunité algébrique, c'est-à-dire qu'il n'existe pas de fonction booléenne de petit degré de support disjoint, afin de résister aux attaques algébriques [59] ;
- résister aux attaques algébriques rapides [58], c'est-à-dire qu'il n'existe pas de fonction booléenne de petit degré telle que le produit avec la fonction concernée donne une nouvelle fonction de petit degré ;
- être hautement non-linéaire, i.e. éloignée des fonctions affines, afin de résister aux attaques par corrélation rapide [191] et aux attaques par approximation linéaire [72].

Des propriétés plus fines peuvent être demandées. Par exemple que la fonction soit m-résiliente, c'est-à-dire que toute restriction de la fonction où m entrées ont été fixées doit rester équilibrée. Cette propriété permet de résister aux attaques par corrélation et n'est pas requise dans le modèle filtré.

Construire des fonctions satisfaisant ces critères, voire prouver leur existence est une tâche ardue. De plus, ces critères sont dans un sens incompatibles. Ainsi, le degré algébrique d'une fonction m-résiliente vérifie

$$m + \deg(f) \leq n - 1 \ .$$

Ou encore, une fonction courbe, i.e. possédant une non-linéarité maximum, n'est jamais équilibrée. Bien souvent, l'apparition d'un nouveau type d'attaque, et l'introduction d'un critère de résistance associé, rendent caduques toutes les familles de fonctions connues. Par exemple, parmi les fonctions connues avant l'apparition des attaques algébriques, celles qui possédaient une immunité algébrique optimale avaient toutes une piètre non-linéarité. C'est seulement en 2008 que Carlet et Feng [41]

mirent à jour une famille de fonctions booléennes et ses bonnes propriétés cryptographiques au sein de familles de fonctions booléennes précédemment étudiées par Feng, Liao et Yang [89].

Définition 1.1 (Construction de Carlet et Feng [41, Section 3]). *Soient $n \geq 2$ un entier positif et α un élément primitif de $\mathbb{F}_{2^n}$. La fonction booléenne f en n variables est définie par*

$$\mathrm{supp}(f) = \left\{0, 1, \alpha, \ldots, \alpha^{2^{n-1}-2}\right\} \ .$$

Carlet et Feng ont montré que ces fonctions sont

1. équilibrées,
2. de degré algébrique optimal $n-1$ pour une fonction équilibrée,
3. d'immunité algébrique optimale $\lceil n/2 \rceil$,
4. assez résistantes aux attaques algébriques rapides,
5. et munies d'une bonne non-linéarité

$$\mathrm{nl}(f) \geq 2^{n-1} + \frac{2^{n/2+1}}{\pi} \ln\left(\frac{\pi}{2^n - 1}\right) - 1 \approx 2^{n-1} - \frac{2\ln 2}{\pi} n 2^{n/2} \ .$$

Cette famille fut en suite modifiée par Tu et Deng [264], puis étendue par divers auteurs dont Tang, Carlet et Tang [259], et finalement Jin et al., pour donner la famille suivante.

Définition 1.2 (Construction de Jin et al. [143]). *Soient $n = 2k \geq 4$ un entier pair, α un élément primitif de $\mathbb{F}_{2^n}$, $A = \left\{1, \alpha, \ldots, \alpha^{2^{k-1}-1}\right\}$ et $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ un fonction booléenne en k variables définie par*

$$\mathrm{supp}(g) = \alpha^s A \ ,$$

pour tout $0 \leq s \leq 2^k - 2$, et $u \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^\times$. La fonction booléenne $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ en n variables est définie par

$$f(x, y) = g\left(xy^{2^k-1-u}\right) \ .$$

Jin et al. ont prouvé que ces fonctions sont

1. de degré algébrique compris entre $n/2$ et $n-2$ selon la valeur de u,
2. d'immunité algébrique optimale $n/2$ à condition qu'une conjecture soit vérifiée,
3. d'une non-linéarité supérieure à

$$2^{n-1} - \frac{2}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/2} - 1 \approx 2^{n-1} - \frac{\ln 2}{\pi} n 2^{n/2} \ .$$

La preuve de l'optimalité de l'immunité algébrique dépend de la validité d'une conjecture combinatoire qui est l'objet de la sous-section suivante.

1.2 D'une conjecture sur l'addition modulo $2^k - 1$

La version la plus générale de cette conjecture est la suivante.

Conjecture 1.3 (Conjecture de Jin et al. [143])**.** *Soient $k \geq 2$ un entier, $t, u, v \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ tels que $\gcd(u, 2^k-1) = \gcd(v, 2^k-1) = 1$. Alors*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua + vb = t; \mathrm{w_H}(a) + \mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

Elle recouvre la conjecture originale de Tu et Deng pour $u = v = 1$ et celle de Tang, Carlet et Tang pour $u = -v = 1$. Ce dernier cas est particulièrement intéressant car Tang, Carlet et Tang [259] ont prouvé que les fonctions booléennes correspondantes sont résistantes aux attaques algébriques rapides, ce qui n'est pas le cas de celles de Tu et Deng [264].

Cette conjecture s'exprime naturellement à l'aide du nombre de retenues qui se produisent lors d'une addition modulo $2^k - 1$. Si a et t sont deux entiers modulo $2^k - 1$, le nombre de retenues $r(a,t)$ qui se produisent lors de leur addition peut être défini comme suit.

Définition 1.4. *Pour $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, $a \neq 0$, posons*

$$r(a,t) = \mathrm{w_H}(a) + \mathrm{w_H}(t) - \mathrm{w_H}(a+t) \ ,$$

i.e. $r(a,t)$ est le nombre de retenues qui se produisent lors de l'addition modulaire. Par convention, posons

$$r(0,t) = k \ ,$$

i.e. 0 se comporte comme la chaîne de caractères $\underbrace{1\ldots1}_{k}$. Remarquons aussi que $r(-t,t) = k$.

Malheureusement, une telle quantité est difficile à appréhender et une structure algébrique agréable permettant d'attaquer le problème reste à trouver. Des considérations d'ordre combinatoire, ainsi que probabiliste dans certains cas, permettent toutefois d'apporter un certain nombre de réponses au problème initial. Ainsi, quelques propriétés sont faciles à déduire de la définition. Par exemple,

- $\#S_{t,v,u,k} = \#S_{2t,v,u,k}$, i.e. le cardinal de $S_{t,v,u,k}$ ne dépend que de la classe cyclotomique de t modulo $2^k - 1$;
- les entiers u et v peuvent être échangé, i.e. $\#S_{t,v,u,k} = \#S_{t,u,v,k}$;
- si c est inversible, alors $\#S_{t,v,u,k} = \#S_{ct,cv,cu,k}$;
- la relation suivante est vérifiée

$$\#S_{t,v,u,k} = \#S_{(uv)^{-1}t,v^{-1},u^{-1},k} \ .$$

Ces considérations permettent de prouver la validité de la conjecture de Tang, Carlet et Tang.

Théorème 1.5. *Soient $k \geq 2$ un entier, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ et $u = 2^i$ pour un entier i quelconque. Alors*

$$\#S_{t,-1,u,k} \leq 2^{k-1} \ .$$

Ainsi, les bonnes propriétés des fonctions booléennes correspondantes ne sont plus conjecturales.

Intéressons nous maintenant à la conjecture originale de Tu et Deng. La conjecture s'énonce de la façon suivante en termes de retenues.

Conjecture 1.6. *Soient $k \geq 2$ un entier, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, $S_{t,k}$ l'ensemble*

$$S_{t,k} = \left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid r(a,t) > \mathrm{w_H}(t)\right\} \ ,$$

et $P_{t,k}$ le nombre

$$P_{t,k} = \#S_{t,k}/2^k \ .$$

Alors

$$P_{t,k} \leq \frac{1}{2} \ .$$

Les considérations précédentes ne permettent malheureusement plus de conclure aussi facilement. Un approche similaire indique en effet simplement que

$$S_{t,k} + S_{-t,k} \leq 2^k$$

en général. Elles permettent cependant de conclure dans quelques cas dégénérés ; par exemple si $t = 0$, ou si t et $-t$ sont dans la même classe cyclotomique.

Pour continuer notre étude, décomposons t, qui sera maintenant considéré comme fixe, de la façon suivante.

Définition 1.7.

$$t = \underbrace{\overbrace{\texttt{1}^{\alpha_1}\texttt{0}^{\beta_1}}^{\texttt{1---10---0}}\cdots\overbrace{\texttt{1}^{\alpha_i}\texttt{0}^{\beta_i}}^{\texttt{1---10---0}}\cdots\overbrace{\texttt{1}^{\alpha_d}\texttt{0}^{\beta_d}}^{\texttt{1---10---0}}}_{t}$$
$$\underbrace{\qquad\qquad}_{t_1}\qquad\underbrace{\qquad\qquad}_{t_i}\qquad\underbrace{\qquad\qquad}_{t_d}$$

avec d le nombre de blocs, α_i et β_i les nombres de `1` *et de* `0` *dans le i-ième bloc et $B = \sum_{i=1}^{d} \beta_i = k - \mathrm{w_H}(t)$.*

Pour un entier modulaire a, nous définissons les quantités correspondantes de la façon suivante.

Définition 1.8.

$$t = \overbrace{\texttt{1}^{\alpha_1}\texttt{0}^{\beta_1}}^{\texttt{1---10---0}}\cdots\overbrace{\texttt{1}^{\alpha_i}\texttt{0}^{\beta_i}}^{\texttt{1---10---0}}\cdots\overbrace{\texttt{1}^{\alpha_d}\texttt{0}^{\beta_d}}^{\texttt{1---10---0}} \ ,$$
$$a = \underbrace{\texttt{?}^{\gamma_1}\texttt{1}^{\delta_1}}_{\texttt{?10-01-1}}\cdots\underbrace{\texttt{?}^{\gamma_i}\texttt{1}^{\delta_i}}_{\texttt{?10-01-1}}\cdots\underbrace{\texttt{?}^{\gamma_d}\texttt{1}^{\delta_d}}_{\texttt{?10-01-1}} \ ,$$

La première étape est alors de traiter le cas où t est composé d'un unique bloc. Dans cette situation, il est encore possible d'expliciter le nombre de retenues produites lors de l'addition d'un entier modulaire a.

Proposition 1.9. *La proportion $P(e)$ d'entiers a tels que $k - r(a,t) = e$ est*

$$P(e) = \begin{cases} 2^{-\beta} & \text{pour } e = 0 \ , \\ 2^{-|e-\beta|}\frac{1-4^{M-m}}{3} & \text{pour } 0 < e < \alpha+\beta \ , \\ 2^{-\alpha} - 2^{-\alpha-\beta} & \text{pour } e = \alpha+\beta \ , \end{cases}$$

où

$$m = \min(e, \alpha) \text{ et } M = \max(0, e-\beta) \ .$$

Cette proposition permet de conclure dans le cas où $d = 1$ et exprime $\#S_{t,k}$ de façon explicite.

Théorème 1.10. *Soient $k \geq 2$ et $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ fait d'un unique bloc. Alors*

$$P_{t,k} = \begin{cases} 2^{-\alpha-\beta}\frac{1-2^{-2\alpha}}{3} & \text{si } 1 \leq \alpha \leq \frac{k-1}{2} \ , \\ \frac{1+2^{-2\beta+1}}{3} & \text{si } \frac{k-1}{2} \leq \alpha \leq k-1 \ . \end{cases}$$

Afin d'utiliser les résultats ci-dessus pour des nombres t composés de plusieurs blocs il est nécessaire de poser l'hypothèse

$$\min_i(\alpha_i) \geq \sum_{i=1}^{d} \beta_i - 1 = B - 1 = k - \mathrm{w_H}(t) - 1 \ .$$

Ceci assure que tous les blocs de t se comportent de la même façon quand un entier $a \in S_{t,k}$ est ajouté : ils débordent, i.e. une retenue se propage toujours d'un bloc à l'autre. De plus, la valeur exacte de $\#S_{t,k}$ ne dépend plus de l'ordre des blocs, ni de la valeur des α_i, d'où la définition suivante.

Définition 1.11. *Soient $k \geq 2$ et $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ tels que*

$$\min_i(\alpha_i) \geq \sum_{i=1}^{d} \beta_i - 1 = B - 1 = k - \mathrm{w_H}(t) - 1 \ .$$

La fonction $f_d(\beta_1, \ldots, \beta_d)$ est définie par

$$f_d(\beta_1, \ldots, \beta_d) = P_{t,k} \ .$$

Il est également possible d'exprimer $\#S_{t,k}$ en utilisant les valeurs de $P(e)$ ci-dessus.

Proposition 1.12. *La fonction f_d s'exprime comme*

$$\begin{aligned} f_d(\beta_1, \ldots, \beta_d) &= \sum_{E=0}^{B-1} \sum_{\substack{\sum_d e_i = E \\ 0 \leq e_i}} \prod_d P(e_i) \\ &= 2^{-B} 3^{-d} \sum_{E=0}^{B-1} 2^{-E} \sum_{\substack{\sum_d e_i = E \\ 0 \leq e_i}} \prod_d \left(4^{\max(1, \min(e_i, \beta_i))} - 1\right) \ . \end{aligned}$$

Cette expression permet de construire un famille d'entiers qui atteignent la borne de la conjecture.

Théorème 1.13. *Pour $k \geq 2$, on a*

$$f_d(1, \ldots, 1) = \frac{1}{2} \ .$$

Une étude analytique permet de conclure dans le cas où t est composé de deux blocs.

Théorème 1.14. *Soient $k \geq 2$ et $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ tels que $d = 2$ et $\alpha_1, \alpha_2 \geq B - 1$. Alors*

$$\#S_{t,k} \leq 2^{k-1} \ .$$

La fonction f_2 s'exprime en effet explicitement de la façon suivante.

Proposition 1.15. *La fonction f_2 est donnée par*

$$\begin{aligned} f_2(x, y) = \frac{11}{27} &+ 4^{-x}\left(\frac{2}{9}x - \frac{2}{27}\right) \\ &+ 4^{-y}\left(\frac{2}{9}y - \frac{2}{27}\right) + 4^{-x-y}\left(\frac{20}{27} - \frac{2}{9}(x+y)\right) \ . \end{aligned}$$

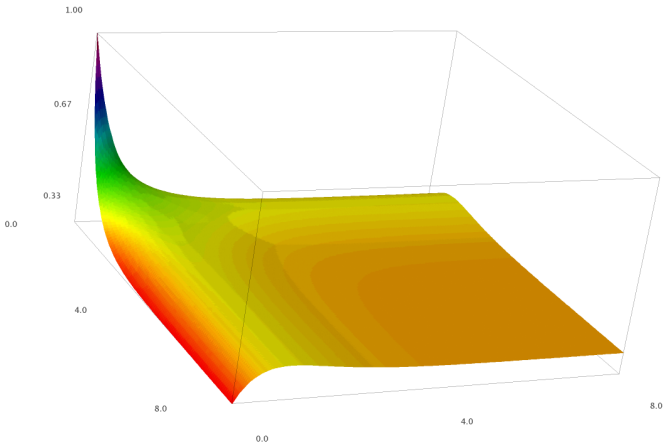


Figure 3 – Graphe de $f_2(x, y)$ pour $0 \leq x, y \leq 8$

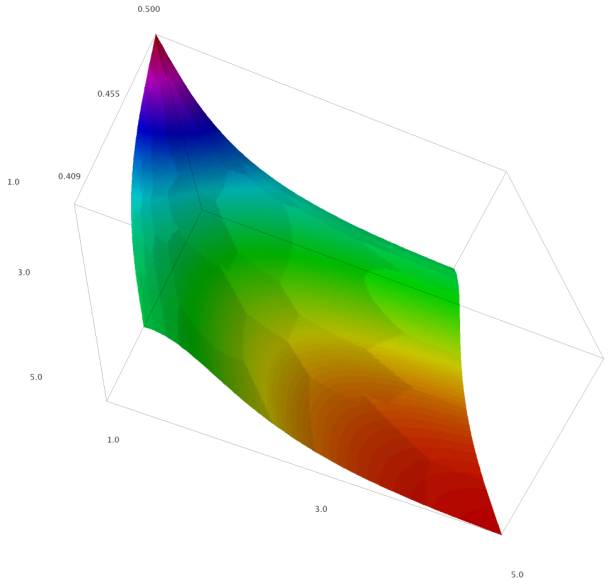


Figure 4 – Graphe de $f_2(x, y)$ pour $1 \leq x, y \leq 5$

Son graphe est représenté dans les Figures 3 et 4.

Une telle approche peut se généraliser à un nombre de blocs supérieur. Une étude plus poussée de l'expression de f_d sous forme de somme donnée plus haut permet d'obtenir la forme close suivante.

Proposition 1.16. *Pour tout $d \geq 1$, f_d peut s'écrire*

$$f_d(\beta_1, \ldots, \beta_d) = \sum_{I \subset \{1,\ldots,d\}} 4^{-\sum_{i\in I} \beta_i} P_d^{\#I}(\{\beta_i\}_{i\in I}) \ ,$$

où P_d^n est un polynôme multivarié symétrique en n variables de degré total $d-1$ et de degré $d-1$ en chaque variable pour $n > 0$ et 0 pour $n = 0$.

Les coefficients $a^{d,n}_{(i_1,\ldots,i_n)}$ des polynômes multivariés sont donnés par la formule suivante.

Proposition 1.17. *Supposons que $i_1 \geq \ldots \geq i_m \neq 0 > i_{m+1} = 0 = \ldots = i_n = 0$ et que $m > 0$. Notons l la somme $l = i_1 + \ldots + i_n > 0$ (i.e. le degré total du monôme). Alors*

$$a^{d,n}_{(i_1,\ldots,i_n)} = (-1)^{n+1} \binom{l}{i_1, \ldots, i_n} b^{d,n}_{l,m} \ ,$$

où $\binom{l}{i_1,\ldots,i_n}$ est un coefficient multinomial et $b^{d,n}_{l,m}$ est défini par

$$b^{d,n}_{l,m} = \sum_{\mathfrak{i}=0}^{n-m} \binom{n-m}{\mathfrak{i}} \sum_{\mathfrak{j}=0}^{d-n} \binom{d-n}{\mathfrak{j}} \sum_{k_j \geq 0, j \in I \cup J, 1 \leq j \leq m} \frac{(l+S-m)!}{l!} \left(\sum_{k \geq 1} \frac{2^k}{(h-k)!} \begin{bmatrix} h-k \\ l+S-m \end{bmatrix} \right) \prod_{j\in J} \frac{A_{k_j}}{k_j!} \prod_{j\in I} \frac{A_{k_j} - 3_{k_j=0}}{k_j!} \prod_{j=1}^{m} \frac{C_{k_j-1}}{|k_j - 1|!} \ .$$

Dans cette expression de $b^{d,n}_{l,m}$, les notations sont :

- $I = \{m+1, \ldots, m+\mathfrak{i}\}$;
- $J = \{n+1, \ldots, n+\mathfrak{j}\}$;
- $S = \sum_{j \in I \cup J, 1 \leq j \leq m} k_j$;
- $h = d - m - \mathfrak{j} - \mathfrak{i}$;

et

$$C_j = \begin{cases} A_j + \frac{B_{j+1}}{j+1} & si\ j > 0 \ , \\ -\frac{13}{6} & si\ j = 0 \ , \\ 1 & si\ j = -1 \ , \end{cases}$$

où A_i est une somme de nombres eulériens et B_i est un nombre de Bernoulli.

Enfin, il est possible d'exprimer la limite de f_d quand les β_i tendent vers l'infini à l'aide de séries hypergéométriques.

Proposition 1.18. *Pour $d \geq 1$ et $k \geq 0$, notons $P_d = 1 - 2f_d(\infty, \ldots, \infty)$. Alors*

$$P_d = \frac{1}{4^d} \sum_{j=0}^{\infty} \binom{d-1+j}{d-1}^2 \frac{1}{4^j} = \frac{1}{4^d} {}_2F_1(d, d; 1; 1/4) \ .$$

En particulier, $\frac{1}{3^d} \leq P_d \leq \frac{1+3\cdot 2^{d-2}}{4^d}$. Qui plus est, $P_1 = 1/3$ et $P_2 = 5/27$.

De simples considérations d'ordre probabiliste permettent alors de prouver la validité de la conjecture de Tu et Deng dans un cadre asymptotique.

Théorème 1.19. *Soit $d \geq 1$ un entier. Il existe une constante K_d telle que, si $\forall i$, $\beta_i \geq K_d$, on a alors*

$$f_d(\beta_1, \ldots, \beta_d) < \frac{1}{2} \ .$$

Pour conclure cette section, notons qu'une approche inductive naïve semble difficile à mettre en place ; de nombreuses données expérimentales soutiennent cette affirmation. Enfin, d'un point de vue calculatoire, nous avons étendu les résultats de Tu et Deng, qui avaient vérifié la validité de leur conjecture pour $k \leq 29$, jusqu'à $k = 40$. Notre implémentation en C [148] s'appuie sur la version 2.2 de la bibliothèque FLINT [127] pour l'arithmétique et la version 1.5.4 de la bibliothèque OpenMPI [106] pour distribuer les calculs.

2 Fonctions courbes et comptage de points sur les courbes algébriques

Dans cette section nous nous concentrons sur une propriété bien précise des fonctions booléennes : la non-linéarité ; et plus particulièrement aux fonctions qui atteignent la non-linéarité maximum. Ce sont les fonctions courbes et nous les étudierons au travers de leur forme polynomiale. De plus, nous nous efforcerons de décrire des algorithmes efficaces permettant de générer de telles fonctions. Ces algorithmes font intervenir de façon quelque peu inattendue des objets rencontrés habituellement en cryptographie asymétrique : les courbes elliptiques et hyperelliptiques.

2.1 Fonctions courbes et courbes algébriques

Rappelons que le corps fini $\mathbb{F}_{2^n}$ à 2^n éléments est (non-canoniquement) isomorphe au $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_2^n$ de dimension n. Toute fonction booléenne peut donc s'écrire de façon unique sous forme d'une somme de traces de monômes :

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^{o(j)}\left(a_j x^j\right) + \epsilon(1 + x^{2^n-1}), \quad a_j \in \mathbb{F}_{2^{o(j)}} \ ,$$

où Γ_n est un ensemble de représentants des classes cyclotomiques modulo $2^n - 1$ (incluant la classe triviale de 0), $o(j)$ est la taille du coset cyclotomique contenant j, et $\epsilon = \mathrm{w_H}(f)$ modulo 2.

C'est ce qu'on appelle la forme polynomiale. Un problème difficile consiste alors à donner des conditions nécessaires et suffisantes sur les coefficients a_j pour que la fonction booléenne correspondante soit courbe.

Afin d'attaquer ce problème, une première étape consiste à exprimer le caractère courbe à l'aide de la transformée de Walsh–Hadamard.

Définition 2.1. *Soit f une fonction booléenne définie sur $\mathbb{F}_{2^n}$. La transformée de Walsh–Hadamard de f est la transformée de Fourier discrète de $\chi_f = (-1)^f$. Pour $\omega \in \mathbb{F}_{2^n}$, elle est explicitement donnée par*

$$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(\omega x)} \ .$$

Une fonction est courbe si et seulement si sa transformée de Walsh–Hadamard ne prend que les valeurs $\pm 2^{n/2}$. Si de plus toute fonction de la forme $f(x^k)$ avec k premier avec $2^n - 1$ est encore courbe, la fonction est dite hyper-courbe.

La caractérisation ci-dessus n'est pas satisfaisante : elle implique un nombre exponentiel de sommes exponentielles. Avant de pouvoir décrire de meilleures caractérisations dans la sous-section suivante, définissons différents objets mathématiques classiques.

Les premiers sont les sommes de Kloosterman binaires. Ce sont les valeurs de la transformée de Walsh–Hadamard de la fonction inverse.

Définition 2.2 (Somme de Kloosterman)**.** *La somme de Kloosterman associée à $a \in \mathbb{F}_{2^n}$ est*

$$K_n(a) = 1 + \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(ax + \frac{1}{x}\right)} \ .$$

Les seconds les polynômes de Dickson binaires.

Définition 2.3 (Polynôme de Dickson [179])**.** *Le polynôme de Dickson de degré r sur $\mathbb{F}_2[X]$ est*

$$D_r(X) = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor} \frac{r}{r-i} \binom{r-i}{i} X^{r-2i}, \quad r \geq 2 \ .$$

Enfin, nous aurons besoin d'un certain nombre de résultats sur les courbes algébriques. Une courbe elliptique E est une courbe algébrique lisse de genre 1 donnée par une équation de Weierstraß [244, Section III.1]

$$E : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ .$$

Deux telles courbes sont tracées dans les Figures 5 et 6. Une propriété fondamentale est que les

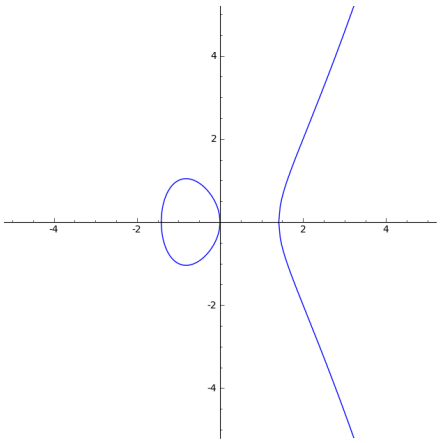


FIGURE 5 – La courbe elliptique E : $y^2 = x^3 - 2x$

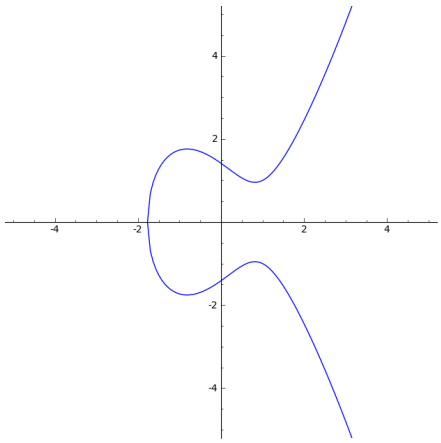


FIGURE 6 – La courbe elliptique E : $y^2 = x^3 - 2x + 2$

points rationnels d'une courbe elliptique forment un groupe. La loi d'addition est illustrée dans la Figure 7.

Si une courbe elliptique est définie sur un corps fini $\mathbb{F}_q$, il est toujours possible de parler de son nombre de points rationnels. Calculer efficacement ce nombre de points est un problème mathématique difficile. Cette quantité s'exprime en fonction de la trace t de l'endomorphisme de Frobenius :

$$\#E = q + 1 - t \ .$$

Un théorème classique borne cette trace.

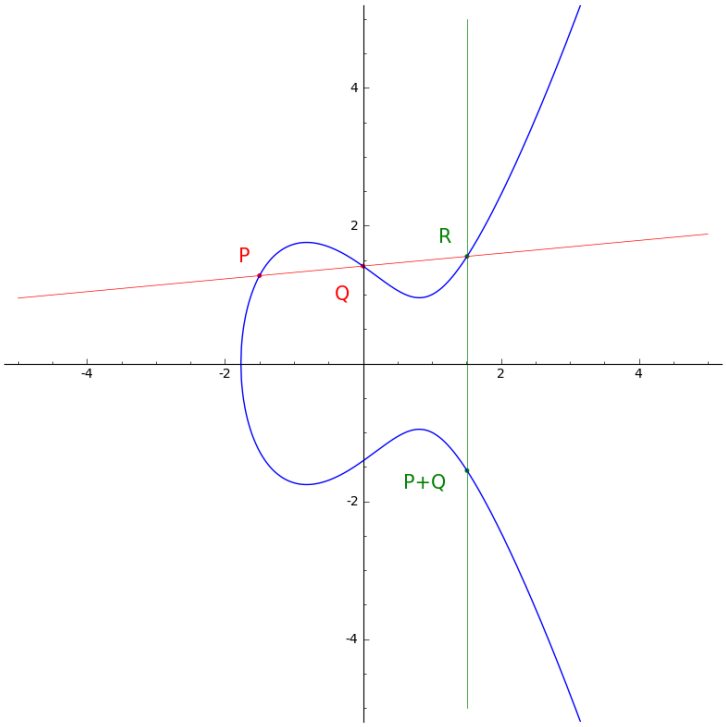


Figure 7 – Loi d'addition sur la courbe elliptique $E : \ y^2 = x^3 + 1$

Théorème 2.4 (Théorème d'Hasse–Weil [244, Theorem V.2.3.1]). *Soit t la trace de l'endomorphisme de Frobenius d'une courbe elliptique sur $\mathbb{F}_q$. Alors*

$$|t| \leq 2\sqrt{q} \ .$$

En ce qui concerne les courbes elliptiques définies sur un corps de caractéristique paire, il a été montré qu'il est possible de calculer la valeur de t en temps quasi-quadratique, ce qui est optimal.

Théorème 2.5 ([126]). *Soit E une courbe elliptique définie sur $\mathbb{F}_{2^m}$. Il existe un algorithme calculant la trace du Frobenius avec une complexité temporelle en $O(m^2(\log m)^2 \log\log m)$ et spatiale en $O(m^2)$.*

Les courbes hyperelliptiques sont une généralisation des courbes elliptiques. Celles qui nous intéresseront sont plus précisément des courbes hyperelliptiques imaginaires, et même des courbes d'Artin–Schreier. Une telle courbe H de genre g est définie par une équation de la forme

$$H : \ y^2 + x^k y = f(x) \ ,$$

où $0 \leq k \leq g$ et $f(x)$ est unitaire de degré $2g+1$.

Théorème 2.6 ([275, Theorem 4.3.1]). *Soit H une courbe d'Artin–Schreier de genre g sur $\mathbb{F}_{2^m}$. Il existe un algorithme calculant le nombre de points de H avec une complexité temporelle en*

$$O(g^3 m^3 (g^2 + \log^2 m \log\log m) \log gm \log\log gm)$$

et spatiale en $O(g^3 m^3)$.

2.2 Caractérisations efficaces de fonctions courbes

Le problème qui nous intéresse à présent est le suivant : donner des conditions nécessaires et suffisantes sur les coefficients de la forme polynomiale pour que la fonction booléenne correspondante soit courbe.

Une première réponse à cette question a été apportée par Dillon [70] qui a prouvé que les fonctions monomiales avec l'exposant de Dillon

$$f_a(x) = \mathrm{Tr}_1^n \left(a x^{r(2^m-1)} \right)$$

définies sur $\mathbb{F}_{2^n}$ et où r est premier avec $2^m - 1$ sont courbes si et seulement si la somme de Kloosterman $K_m(a)$ associée à a est nulle. Il a ensuite été démontré que ces fonctions sont en fait hyper-courbes. Dillon conjectura qu'il existait toujours des coefficients $a \in \mathbb{F}_{2^m}$ tels que $K_m(a) = 0$. Ce résultat a été démontré par Lachaud et Wolfmann [156] qui reformulèrent ce problème en termes de courbes elliptiques. Les sommes de Kloosterman peuvent en effet être exprimées à l'aide du nombre de points sur une courbe elliptique.

Théorème 2.7 ([156, 144]). *Soient $m \geq 3$ un entier positif, $a \in \mathbb{F}_{2^m}^*$ et E_a la courbe elliptique projective définie sur $\mathbb{F}_{2^m}$ par l'équation*

$$E_a : \ y^2 + xy = x^3 + a \ .$$

Alors

$$\#E_a = 2^m + K_m(a) \ .$$

Cette reformulation implique non seulement que les sommes de Kloosterman sont toujours divisibles par 4, mais bien plus encore. Cependant, ce n'est qu'au début des années 2000 que ce résultat fut exploité plus avant. Par exemple, Lisoněk [180] l'utilisa pour fournir une démonstration alternative et particulièrement élégante de la caractérisation des valeurs des sommes de Kloosterman modulo 8.

Proposition 2.8 ([129]). *Soient $m \geq 3$ un entier positif et $a \in \mathbb{F}_{2^m}$. Alors $K_m(a) \equiv 0 \pmod 8$ si et seulement si $\mathrm{Tr}_1^m(a) = 0$.*

Cette correspondance lui permit également de générer des zéros de Kloosterman pour m jusqu'à 64 en seulement quelques jours. Si la somme de Kloosterman $K_m(a)$ est nulle, la courbe elliptique E_a a en effet exactement 2^m points. Ceci implique en particulier que son groupe de points rationnels est cyclique, isomorphe à

$$E_a(\mathbb{F}_{2^m}) \simeq \mathbb{Z}/2^m\mathbb{Z} \ .$$

Cette identité permet entre autres de tester les zéros de Kloosterman encore plus efficacement qu'en comptant les points de E_a.

Plus récemment, Mesnager [195] a montré que la valeur 4 des sommes de Kloosterman caractérise les fonctions courbes de la forme

$$f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^4\left(bx^{(2^n-1)/3}\right)$$

quand m est impair. L'approche précédente s'étend partiellement à cette valeur. Par exemple, il est possible de montrer la réciproque d'un résultat de Helleseth et Zinoviev [129] concernant la valeur des sommes de Kloosterman modulo 3.

Proposition 2.9. *Soit $a \in \mathbb{F}_{2^m}^*$.*

- *Si m est impair, alors $K_m(a) \equiv 1 \pmod 3$ si et seulement s'il existe $t \in \mathbb{F}_{2^m}$ tel que $a = t^4 + t^3$.*
- *Si m est pair, alors*
  - *$K_m(a) \equiv 0 \pmod 3$ si et seulement s'il existe $t \in \mathbb{F}_{2^m}$ tel que $a = t^4 + t^3$ and $\mathrm{Tr}_1^m(t) = 0$;*
  - *$K_m(a) \equiv -1 \pmod 3$ si et seulement s'il existe $t \in \mathbb{F}_{2^m}$ tel que $a = t^4 + t^3$ and $\mathrm{Tr}_1^m(t) = 1$.*

Malheureusement, la situation n'est pas aussi idéale que pour les zéros de Kloosterman. En particulier, le cardinal d'une courbe elliptique E_a correspondant à une somme de Kloosterman $K_m(a) = 4$ est

$$\#E_a = 2^m + 4$$

et cet entier ne jouit pas des mêmes propriétés de divisibilité qu'avant. Toutefois, les considérations précédentes permettent de générer efficacement des éléments a tels que $K_m(a) = 4$ et notre implémentation pour le logiciel Sage [250] nous a permis de trouver de tels éléments pour m jusqu'à 55.

Dans le cas où m est pair, le critère de Mesnager est nécessaire, mais il n'a pas été démontré qu'il est suffisant. En utilisant les outils développés précédemment, nous avons étudié le caractère courbe des fonctions booléennes de la famille de Mesnager pour tous les $a \in \mathbb{F}_{2^m}$ tels que $K_m(a) = 4$ pour des petites valeurs de m. Il est bon de noter que trouver *tous* les éléments $a \in \mathbb{F}_{2^m}$ correspondant à une certaine somme de Kloosterman est un problème différent du

précédent. Dans cette situation, mieux vaut en effet calculer *toutes* les sommes de Kloosterman sur $\mathbb{F}_{2^m}$ à l'aide d'une transformée de Walsh–Hadamard rapide [8] de la fonction inverse. La vérification du caractère courbe d'un fonction associée à un tel élément se fait ensuite par un nouveau calcul de transformée de Walsh–Hadamard rapide. Le résultat de nos expérimentations est que tous les éléments $a \in \mathbb{F}_{2^m}$ tels que $K_m(a) = 4$ pour $4 \leq m \leq 16$ sont associés à des fonctions courbes. Ces résultats sont résumés dans la Table 1.

TABLE 1 – Test du caractère courbe pour m pair

m	Nb. de classes cyclotomiques	Temps	Toutes courbes ?
4	1	<1s	oui
6	1	<1s	oui
8	2	<1s	oui
10	3	4s	oui
12	6	130s	oui
14	8	3000s	oui
16	14	82000s	oui
18	20	-	-
20	76	-	-
22	87	-	-
24	128	-	-
26	210	-	-
28	810	-	-
30	923	-	-
32	2646	-	-

La caractérisation de Dillon a également été étendue par Charpin et Gong [46] à des fonctions booléennes avec plusieurs termes de trace.

Théorème 2.10 (Critère de Charpin et Gong [46])**.** *Soit $n = 2m$. Soit S un ensemble de représentants des classes cyclotomiques modulo $2^m + 1$ de taille maximale n. Soit f_a la fonction booléenne définie sur $\mathbb{F}_{2^n}$ par*

$$f_a(x) = \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r x^{r(2^m-1)} \right) \ ,$$

où $R \subseteq S$ et $a_r \in \mathbb{F}_{2^m}$. Soit g_a la fonction booléenne définie sur $\mathbb{F}_{2^m}$ par

$$g_a(x) = \sum_{r \in R} \mathrm{Tr}_1^m \left(a_r D_r(x) \right) \ ,$$

où $D_r(x)$ est le polynôme de Dickson de degré r. Alors f_a est hyper-courbe si et seulement si

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi \left(\mathrm{Tr}_1^m \left(x^{-1} \right) + g_a(x) \right) = 2^m - 2\, \mathrm{w_H}(g_a) - 1 \ .$$

Mesnager [196] a ensuite décrit un critère similaire pour des fonctions booléennes avec plusieurs termes de trace et un terme de trace additionnel sur $\mathbb{F}_4$.

Théorème 2.11 (Critère de Mesnager [196])**.** *Soient $n = 2m$ avec m impair et S un ensemble de représentants des classes cyclotomiques modulo $2^m + 1$ de taille maximale n. Soit $b \in \mathbb{F}_4^*$. Soit*

$f_{a,b}$ la fonction définie sur $\mathbb{F}_{2^n}$ par

$$f_{a,b}(x) = \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) \ ,$$

où $R \subseteq S$ et $a_r \in \mathbb{F}_{2^m}$. Soit g_a la fonction booléenne définie sur $\mathbb{F}_{2^m}$ par

$$g_a(x) = \sum_{r\in R} \mathrm{Tr}_1^m\left(a_r D_r(x)\right) \ ,$$

où $D_r(x)$ est le polynôme de Dickson de degré r. Alors :

1. *Si b est un élément primitif de $\mathbb{F}_4$, alors les trois conditions suivantes sont équivalentes :*
   (a) *$f_{a,b}$ est hyper-courbe ,*
   (b) $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(D_3(x))\right) = -2$,
   (c) $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_a(D_3(x))\right) = 2^m - 2\,\mathrm{w_H}(g_a \circ D_3) + 3$;
2. *$f_{a,1}$ est hyper-courbe si et seulement si*

$$2\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(D_3(x))\right) - 3\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(x)\right) = 2 \ .$$

Lisoněk [182, 181] a ensuite montré comment étendre la reformulation des sommes de Kloosterman en termes de courbes elliptiques pour exprimer le critère de Charpin et Gong à l'aide du nombre de points sur des courbes hyperelliptiques et a obtenu le critère suivant.

Théorème 2.12 (Reformulation du critère de Charpin et Gong [182, 181])**.** *Soient H_a et G_a les courbes affines définies sur $\mathbb{F}_{2^m}$ par*

$$G_a : y^2 + y = \sum_{r\in R} a_r D_r(x) \ ,$$
$$H_a : y^2 + xy = x + x^2 \sum_{r\in R} a_r D_r(x) \ .$$

Alors f_a est hyper-courbe si et seulement si

$$\#H_a - \#G_a = -1 \ .$$

L'intérêt d'une telle reformulation est double. D'un point de vue théorique, elle relie des problèmes concernant les sommes exponentielles et les fonctions courbes à des problèmes concernant le nombre de points de courbes hyperelliptiques. D'un point de vue pratique, elle permet de tester le caractère courbe d'une fonction en temps polynomial.

Cependant, un étude fine du résultat de Lachaud et Wolfmann montre qu'il est possible de faire beaucoup mieux. Sommes exponentielles et cardinaux de courbes d'Artin–Schreier sont en effet reliés de la façon suivante.

Proposition 2.13. *Soient $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ une fonction telle que $f(0) = 0$, g la fonction booléenne $g = \mathrm{Tr}_1^m(f)$ et G_f et H_f les courbes affines définies sur $\mathbb{F}_{2^m}$ par*

$$G_f : y^2 + y = f(x) \ ,$$
$$H_f : y^2 + xy = x + x^2 f(x) \ .$$

Alors

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi(g(x)) = -2^m - 1 + \#G_f \ ,$$
$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g(x)\right) = -2^m + \#H_f \ .$$

Il est donc possible d'étendre l'approche précédente au critère de Mesnager.

Théorème 2.14 (Reformulation du second critère de Mesnager)**.** *Soient H_a et G_a les courbes affines définies sur $\mathbb{F}_{2^m}$ par*

$$G_a : y^2 + y = \sum_{r \in R} a_r D_r(x) \ ,$$
$$H_a : y^2 + xy = x + x^2 \sum_{r \in R} a_r D_r(x) \ ;$$

et H_a^3 et G_a^3 les courbes affines définies sur $\mathbb{F}_{2^m}$ par

$$G_a^3 : y^2 + y = \sum_{r \in R} a_r D_r(D_3(x)) \ ,$$
$$H_a^3 : y^2 + xy = x + x^2 \sum_{r \in R} a_r D_r(D_3(x)) \ .$$

Si b est un élément primitif de $\mathbb{F}_4$, alors $f_{a,b}$ est hyper-courbe si et seulement si

$$\#H_a^3 - \#G_a^3 = 3 \ .$$

Si $b = 1$, alors $f_{a,1}$ est hyper-courbe si et seulement si

$$\left(\#G_a^3 - \#H_a^3\right) - \frac{3}{2}\left(\#G_a - \#H_a\right) = \frac{3}{2} \ .$$

Enfin, en utilisant le fait [47] que la fonction $x \mapsto D_3(x)$ induit une permutation de

$$\{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}_1^m(1/x) = 0\} \ ,$$

il est possible d'obtenir une reformulation plus efficace.

Théorème 2.15 (Reformulation du second critère de Mesnager)**.** *Si b est un élément primitif de $\mathbb{F}_4$, alors $f_{a,b}$ est hyper-courbe si et seulement si*

$$\#G_a^3 - \frac{1}{2}\left(\#G_a + \#H_a\right) = -\frac{3}{2} \ .$$

Si $b = 1$, alors $f_{a,1}$ est hyper-courbe si et seulement si

$$2\#G_a^3 - \frac{5}{2}\#G_a + \frac{1}{2}\#H_a = \frac{3}{2} \ .$$

Le genre des courbes utilisées est en effet moindre, conduisant donc à des tests plus efficaces.

3 Multiplication complexe et polynômes de classes

Dans cette dernière section nous approfondissons un aspect quelque peu différent des courbes elliptiques et des variétés abéliennes — une autre généralisation en dimensions supérieures de ces dernières — : la multiplication complexe et la construction de polynômes de classes. De telles constructions ont cette fois-ci des applications en cryptographie asymétrique.

3.1 Multiplication complexe et courbes elliptiques

Dans la section précédente nous avons considéré les courbes elliptiques sur des corps finis. Dans celle-ci nous considérons principalement les objets sur le corps des nombres complexes.

Sur le corps des nombres complexes $\mathbb{C}$, une courbe elliptique peut toujours être décrite par une équation de Weierstraß de la forme

$$E:\ y^2 = x^3 + ax + b\ .$$

Dans cette situation, le j-invariant d'une courbe elliptique, qui les classifie à isomorphisme près sur un corps algébriquement clos, a une expression particulièrement simple :

$$j = -1728\frac{(4a)^3}{\Delta}\ ,$$

où $\Delta \neq 0$ est le discriminant de la courbe

$$\Delta = -16(4a^3 + 27b^2)$$

et caractérise sa non-singularité.

Sur le corps des nombres complexes $\mathbb{C}$, il existe une autre description d'une courbe elliptique en tant que tore complexe, c'est-à-dire comme le plan complexe quotienté par un réseau. Un tel objet est représenté dans la Figure 8. Le théorème d'uniformisation assure que la réciproque de cette affirmation est également vraie.

Théorème 3.1 (Uniformisation [245, Corollary I.4.3])**.** *Soient a et b deux nombres complexes tels que $4a^3 + 27b^2 \neq 0$. Alors il existe un réseau Λ dans $\mathbb{C}$ tel que l'application*

$$\begin{aligned} \mathbb{C}/\Lambda &\to E:\ y^2 = x^3 + ax + b\ ,\\ z &\mapsto [\wp(z,\Lambda) : \frac{1}{2}\wp'(z,\Lambda) : 1]\ , \end{aligned}$$

où $\wp$ est la fonction $\wp$ de Weierstraß, est un isomorphisme analytique complexe.

Le choix d'une base du réseau Λ conduit à une seconde bijection avec l'ensemble des éléments τ du domaine fondamental du demi-plan de Poincaré $\mathbb{H}$. Ce résultat peut aussi être raffiné pour montrer que la catégorie des courbes elliptiques complexes à isomorphisme près et celle des réseaux à homothétie près sont équivalentes.

Les courbes qui nous intéressent maintenant sont les courbes à multiplication complexe, i.e. les courbes elliptiques qui ont strictement plus d'endomorphismes que les multiplications par un entier qui proviennent de la loi de groupe sur la courbe elliptique et que nous avons déjà évoquées dans la section précédente. Sur un corps fini, toute courbe a multiplication complexe. L'endomorphisme de Frobenius ne correspond en effet à aucun endomorphisme de multiplication. Sur le corps des nombres complexes, la situation est inverse et une courbe générique n'a pas d'endomorphismes supplémentaires. Le nom de multiplication complexe provient de l'identification

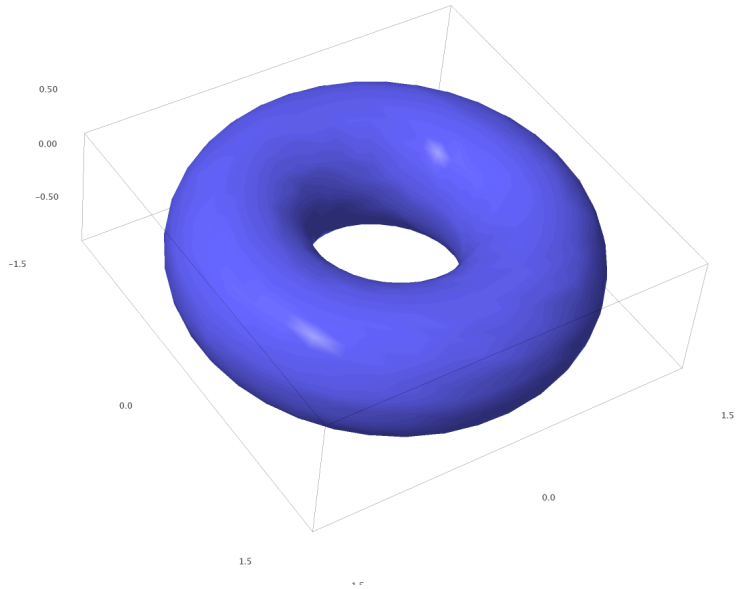


FIGURE 8 – Un tore complexe de dimension 1

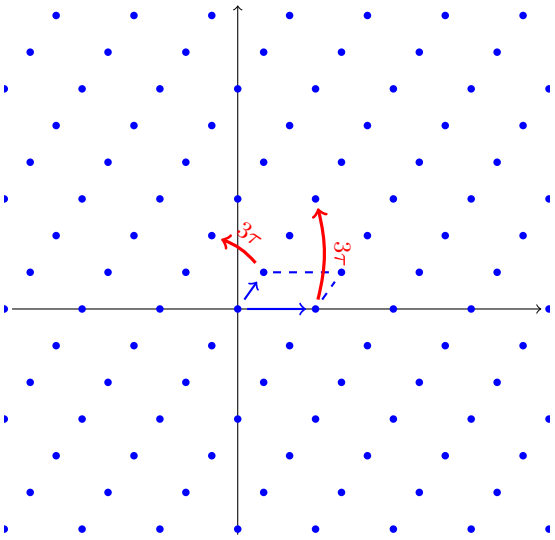


FIGURE 9 – Le réseau correspondant à $\tau = \frac{1+i\sqrt{2}}{3}$

des endomorphismes de la courbe avec ceux du réseau : une multiplication complexe est la multiplication par un nombre complexe non réel qui envoie le réseau dans lui-même. Un tel endomorphisme existe si et seulement si le nombre τ du demi-plan de Poincaré correspondant au réseau est quadratique. Un exemple de ce type de réseaux est donné dans la Figure 9

Si τ est quadratique et appartient au corps quadratique imaginaire K, alors l'anneau des endomorphismes de la courbe correspondante $E = E_\tau$ est un ordre $\mathcal{O}$ dans K, i.e. un réseau qui est aussi un sous-anneau de l'anneau des entiers $\mathcal{O}_K$ de K. Notons $\mathcal{E}ll(\mathcal{O})$ l'ensemble des courbes elliptiques complexes à multiplication complexe par $\mathcal{O}$. À homothétie près, Λ_τ est un $\mathcal{O}$-idéal. Plus précisément, $\mathcal{O}$ est le plus grand ordre pour lequel cette propriété est vraie. Un idéal fractionnaire vérifiant cette propriété est dit propre. Pour un corps quadratique, être propre est équivalent à être inversible. En utilisant la structure de $\mathcal{O}$-idéal de Λ_τ une action de $\mathrm{Prop}(\mathcal{O})$ sur $\mathcal{E}ll(\mathcal{O})$ peut être définie de la façon suivante : pour $\mathfrak{a}$ un idéal fractionnaire propre de $\mathcal{O}$, définissons $\mathfrak{a} * \Lambda_\tau$ comme l'idéal

$$\mathfrak{a} * \Lambda_\tau = \mathfrak{a}^{-1}\Lambda_\tau \ .$$

Modulo l'action triviale des idéaux fractionnaires principaux, cette action est propre et transitive.

Proposition 3.2 ([245, Proposition II.1.2])**.** *Soient K un corps quadratique imaginaire et $\mathcal{O}$ un ordre dans K. Alors l'action du groupe de Picard $\mathrm{Pic}(\mathcal{O})$ sur $\mathcal{E}ll(\mathcal{O})$ est simple et transitive. En particulier, $\#\mathcal{E}ll(\mathcal{O}) = h(\mathcal{O})$ le nombre de classes de $\mathcal{O}$.*

Définissons maintenant le polynôme de classes de Hilbert.

Définition 3.3 (Polynôme de classes de Hilbert)**.** *Soient K un corps quadratique imaginaire et $\mathcal{O}$ un ordre dans K. Le polynôme de classes de Hilbert $H_\mathcal{O}(X)$ de $\mathcal{O}$ est*

$$H_\mathcal{O}(X) = \prod_{E \in \mathcal{E}ll(\mathcal{O})} (X - j(E)) \ .$$

Il est possible de définir une autre action sur $\mathcal{E}ll(\mathcal{O})$. Si $\sigma \in \mathrm{Aut}(\mathbb{C})$ est un automorphisme de $\mathbb{C}$, la courbe E^σ associée à E par l'action de σ a également multiplication complexe par $\mathcal{O}$ et appartient donc a $\mathcal{E}ll(\mathcal{O})$. Les considérations précédentes montrent que l'ensemble $\{j(\tau)^\sigma\}_{\sigma \in \mathrm{Aut}(\mathbb{C})}$ est fini et que $H_\mathcal{O}(X)$ est à coefficients rationnels. Il est en réalité possible de montrer que $j(E)$ est un entier algébrique quand E a multiplication complexe [245, Theorem II.6.1], [160, Theorem 5.2.4] et que $H_\mathcal{O}(X)$ est donc à coefficients entiers.

Il est possible de relier les deux actions décrites ci-dessus. Le groupe $\mathrm{Pic}(\mathcal{O})$ est un groupe de classes d'idéaux généralisé. Par le théorème d'existence [216, Theorem VI.6.1], [145, Theorem 2.2], il existe une extension abélienne de K, appelée corps de classes d'anneaux de $\mathcal{O}$, telle que

$$\mathrm{Gal}(H_\mathcal{O}/K) \simeq \mathrm{Pic}(\mathcal{O}) \ .$$

Théorème 3.4 ([145, Theorem 3.16], [245, Theorem II.4.3], [160, Theorem 10.3.5])**.** *Soient K un corps quadratique imaginaire et $\mathcal{O}$ un ordre dans K. Soient $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$ et $\mathfrak{b}$ un idéal propre de $\mathcal{O}$ dont le symbole d'Artin sur le corps de classes d'anneaux est σ. Soit $\mathfrak{a}$ un idéal propre de $\mathcal{O}$. Alors*

$$j(\mathfrak{a})^\sigma = j(\mathfrak{b} * \mathfrak{a}) \ .$$

En particulier, $K(j(E))$ est le corps de classes d'anneaux de $\mathcal{O}$ et $[K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}] = h(\mathcal{O})$. Enfin, le théorème principal de la multiplication complexe se déduit assez aisément du théorème précédent et décrit l'action de σ sur les points de torsion de E.

La construction du polynôme de classes de Hilbert est décrite dans l'Algorithme 1. La connaissance du polynôme de Hilbert d'un ordre permet de construire, par réduction, des courbes

Algorithme 1 – Calcul du polynôme de classes de Hilbert

Données: Un discriminant négatif $\Delta \equiv 0, 1 \pmod 4$
Résultat: Le polynôme de classes de Hilbert $H_\Delta(X)$ de l'ordre de discriminant Δ
1 Calculer une base de l'ordre $\mathcal{O}$ de discriminant Δ
2 Calculer le groupe de classes $\mathrm{Pic}(\mathcal{O})$ de $\mathcal{O}$
3 **pour chaque** $\mathfrak{a} \in \mathrm{Pic}(\mathcal{O})$ **faire**
4 Calculer $j(\mathfrak{a})$ avec suffisamment de précision
5 Construire $H(X) \in \mathbb{Z}[X]$ à partir des approximations complexes de ses racines
6 **retourner** $H(X)$

elliptiques sur un corps fini qui ne pourraient être obtenues par recherche aléatoire. Sous certaines contraintes, l'anneau des endomorphismes de la courbe ne change pas et son Frobenius est donc connu, tout comme son nombre de points. De plus, cette connaissance préalable peut également permettre de s'assurer que le degré de plongement de la courbe réduite sera petit, chose impossible en tirant des courbes au hasard. De telles courbes sont particulièrement utiles dans le cadre de la cryptographie fondée sur l'identité.

3.2 Multiplication complexe en genre supérieur

Passons maintenant au cas de la dimension supérieure. Dans la section précédente nous avons généralisé les courbes elliptiques, qui sont des courbes de genre 1, par les courbes hyperelliptiques. Il est possible d'adopter un point de vue plus général en considérant la structure de groupe algébrique projectif de dimension 1 des courbes elliptiques. L'extension naturelle est alors de considérer les groupes algébriques projectifs de dimension supérieure : ce sont les variétés abéliennes. Le lien entre ces deux approches peut se faire à l'aide de la jacobienne d'une courbe qui est une variété abélienne dont le groupe des points est isomorphe au sous-groupe de degré zéro du groupe de Picard de la courbe.

Sur le corps des nombres complexes $\mathbb{C}$, une variété abélienne A de dimension g est à nouveau isomorphe à un tore complexe $X = V/\Lambda$ où V est un $\mathbb{C}$-espace vectoriel de dimension g et Λ est un réseau dans V. Cependant, la réciproque n'est plus vraie dès que $g \geq 2$: il existe des tores complexes qui ne sont pas des variétés abéliennes. Une condition nécessaire et suffisante pour qu'un tore complexe soit une variété abélienne est l'existence d'une forme de Riemann non-dégénérée pour le réseau Λ.

Théorème 3.5 ([204, Theorem I.2.8]). *Un tore complexe $X = V/\Lambda$ est projectif si et seulement s'il admet une forme de Riemann non-dégénérée, i.e. une forme $\mathbb{R}$-bilinéaire alternée réelle $\omega(x, y)$ à valeurs entières sur Λ telle que*

$$\omega(ix, iy) = \omega(x, y)$$

pour tous x et y dans V et telle que $\omega(x, ix) > 0$ pour tout $x \in V$ non-nul.

L'existence d'une forme de Riemann permet en effet de construire suffisamment de fonctions thêta pour plonger le tore dans un espace projectif. Les conditions de Riemann donnent un critère simple pour l'existence d'une telle forme.

Théorème 3.6 (Conditions de Riemann [65, Théorème VI.1.3]). *Soit $X = V/\Lambda$ un tore complexe de dimension g. Il existe une forme de Riemann ω sur X si et seulement s'il existe un base $\{e_1, \ldots, e_g\}$ de V, des entiers strictement positifs $d_1, \ldots, d_g$ vérifiant $d_1 | \ldots | d_g$ et une matrice*

$\Omega \in \mathbb{H}_g$, *appelée matrice des périodes, telle que* Λ *s'écrit vis-à-vis de la base* $\{e_1, \ldots, e_g\}$

$$\Lambda = \Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$$

où Δ *est la matrice diagonale de coefficients* $d_1, \ldots, d_g$.

La racine carrée du déterminant de ω est appelé pfaffien et vaut

$$\mathrm{pf}(\omega) = d_1 \cdots d_g \ .$$

La donnée d'une forme de Riemann sur le corps des nombres complexes $\mathbb{C}$ est équivalente à la donnée d'une polarisation. De notre point de vue, la généralisation correcte des courbes elliptiques est une variété abélienne polarisée. Le choix d'une polarisation assure en effet que le groupe des automorphismes d'une variété abélienne est fini. La polarisation est dite principale si le pfaffien de la forme de Riemann est égal à 1. L'existence d'une polarisation principale équivaut à l'existence d'un isomorphisme entre la variété abélienne et sa duale. La jacobienne d'une courbe est canoniquement munie d'une polarisation principale.

Une variété abélienne A de dimension g est dite avoir multiplication complexe si son algèbre des endomorphismes contient un corps CM, i.e. une extension quadratique totalement imaginaire d'une extension totalement réelle de $\mathbb{Q}$, de degré $2g$. Si l'injection correspondante est notée $i : \ K \to \mathrm{End}^0(A)$, alors le couple (A, i) est appelé variété abélienne CM. L'image inverse de l'anneau des endomorphismes de A dans K est un ordre $\mathcal{O} = i^{-1}(\mathrm{End}(A))$. Si cet ordre est maximal, i.e. s'il est égal à l'anneau des entiers $\mathcal{O}_K$ de K, alors la variété abélienne est dite principale. Si A est isotypique et définie sur un corps fini, alors elle a toujours multiplication complexe. Si A est définie sur le corps des nombres complexes, l'injection i peut être décrite sur l'espace tangent à A en 0 par le choix de g plongements distincts de K dans $\mathbb{C}$ non deux à deux conjugués par la conjugaison complexe. Un tel ensemble Φ est appelé type CM. Il vérifie

$$\mathrm{Hom}(K, \mathbb{C}) = \Phi \sqcup \overline{\Phi} \ .$$

Le type CM est dit primitif s'il ne provient pas de l'extension d'un type CM d'un sous-corps CM strict de K. Une variété abélienne CM est simple si et seulement si le type CM associé est primitif. Le choix d'un type CM permet également de définir le corps réflexe de K.

Définition 3.7 (Corps réflexe [205, Proposition I.1.16])**.** *Soient* K *un corps CM et* Φ *un type CM. Le corps réflexe* K^r *de la paire CM* (K, Φ) *est le corps fixé par le groupe*

$$H = \left\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid \sigma\Phi = \Phi\right\} \ .$$

De façon équivalente, K^r *est engendré par l'ensemble des éléments de la forme*

$$\sum_{\phi \in \Phi} \phi(a), \ a \in K \ .$$

Il est possible de munir K^r d'un type CM Φ^r associé à Φ et appelé type réflexe. La norme réflexe N_{Φ^r} est alors définie de la façon suivante

$$\begin{aligned} K^r &\to K \ , \\ x &\mapsto \prod_{\phi \in \Phi^r} \phi(x) \ . \end{aligned}$$

Si (A, i) est une variété abélienne complexe CM de type $(\mathcal{O}, \Phi)$, alors elle peut être décrite par un réseau de K et même par un $\mathcal{O}$-idéal propre.

Théorème 3.8 ([205, I.3.11], [159, Theorem 1.4.1]). *Soient K un corps CM de degré $2g$ et $\mathcal{O}$ un ordre de K. Soit (A, i) un variété abélienne complexe à multiplication complexe par $\mathcal{O}$. Il existe un idéal fractionnaire propre $\mathfrak{a}$ de $\mathcal{O}$, un type CM Φ et un isomorphisme analytique complexe θ tels que*

$$V/\Phi(\mathfrak{a}) \overset{\theta}{\simeq} A \ .$$

La variété abélienne CM (A, i) est dite de type $(\mathcal{O}, \Phi, \mathfrak{a})$ vis-à-vis de θ. Tous les tores complexes de ce type sont polarisables et leurs polarisations s'expriment toutes de la façon suivante.

Théorème 3.9 ([205, Example I.2.9], [159, Theorem I.4.5]). *Soit (A, i, ψ) une variété abélienne complexe CM polarisée de type $(\mathcal{O}, \Phi, \mathfrak{a})$ vis-à-vis d'une paramétrisation analytique θ. Il existe un élément inversible $\xi \in K^*$ vérifiant $\overline{\xi} = -\xi$ et $\Im(\phi(\xi)) > 0$ pour tout $\phi \in \Phi$ tel que la forme de Riemann ω associée à ψ peut-être décrite sur $\Phi(K)$ par*

$$\omega(\Phi(x), \Phi(y)) = \mathrm{Tr}(\xi x \overline{y}) \ .$$

La variété abélienne complexe CM polarisée (A, i, ψ) est dite de type $(\mathcal{O}, \Phi, \mathfrak{a}, \xi)$ vis-à-vis de θ. Inversement, tout élément inversible $\xi \in K^*$ définit une forme de Riemann rationnelle, d'où la proposition suivante.

Proposition 3.10 ([30, 4.3], [273, Theorem 3]). *Soit (A, i, ψ) une variété abélienne complexe CM polarisée de type $(\mathcal{O}, \Phi, \mathfrak{a}, \xi)$. Alors*

$$\xi \in (\overline{\mathfrak{a}}^* : \mathfrak{a}) \ .$$

Le degré de la polarisation est $[\overline{\mathfrak{a}}^* : \xi\mathfrak{a}]$. En particulier, la polarisation est principale si et seulement si

$$\xi\mathfrak{a} = \overline{\mathfrak{a}}^* \ ,$$

où $\mathfrak{a}^*$ est le dual de $\mathfrak{a}$ pour la forme trace :

$$\mathfrak{a}^* = \{x \in E \mid \mathrm{Tr}(x\mathfrak{a}) \subset \mathbb{Z}\} \ .$$

Si A est simple et principale, alors la condition sur ξ devient

$$\xi\mathfrak{a}\overline{\mathfrak{a}}\mathfrak{d}_{K/\mathbb{Q}} = \mathcal{O}_K \ .$$

Supposons maintenant que A et B sont deux variétés abéliennes complexes CM simples du même type (K, Φ) et décrites par deux réseaux $\mathfrak{a}$ et $\mathfrak{b}$. L'ensemble des isogénies $\mathrm{Hom}(A, B)$ entre A et B est alors décrit par l'idéal quotient

$$(\mathfrak{b} : \mathfrak{a}) = \{\alpha \in K \mid \alpha\mathfrak{a} \subset \mathfrak{b}\} \ .$$

Pour les variétés abéliennes complexes CM simples polarisées, la classification à isomorphisme près est décrite ci-dessous.

Proposition 3.11 (Classification des variétés abéliennes complexes CM simples polarisées à isomorphisme près [205, I.3.4], [237, 5.5.B]). *Les triplets (A, i, ψ) de type $(\mathcal{O}, \Phi)$ sont classifiés à isomorphisme près par les quadruplets $(\mathcal{O}, \Phi, \mathfrak{a}, \xi)$ à un changement de la forme*

$$\xi \mapsto \frac{\xi}{\alpha\overline{\alpha}} \ ,$$
$$\mathfrak{a} \mapsto \alpha\mathfrak{a} \ ,$$

où $\alpha \in K^*$, près.

Le théorème principal de la multiplication complexe décrit ensuite l'action du groupe de Galois absolu du corps réflexe sur un triplet (A, i, ψ).

Théorème 3.12 (Théorème principal de la multiplication complexe sur le corps réflexe [238, Theorems IV.18.6 and IV.18.8], [159, Theorem 3.6.1], [205, Theorem II.9.17], [57, Theorem 6.3])**.** *Soit (A, i, ψ) une variété abélienne complexe CM polarisée de type $(\mathcal{O}, \Phi, \mathfrak{a}, \xi)$ vis-à-vis d'une paramétrisation analytique θ. Soient $\sigma \in \mathrm{Aut}(\mathbb{C}/K^r)$ et s une idèle de K^r telle que $\sigma = (s, K^r)_{K^{rab}}$. Il existe une unique paramétrisation analytique θ' telle que $(A^\sigma, i^\sigma, \psi^\sigma)$ est de type $(K, \Phi, \mathrm{N}_{\Phi^r}(s^{-1})\mathfrak{a}, \mathrm{N}_{\mathbb{Q}}(s)\xi)$ vis-à-vis de θ' et telle que le diagramme suivant est commutatif :*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\theta \circ \Phi} & A_{tor} \\ \Big\downarrow{\scriptstyle \mathrm{N}_{\Phi^r}(s^{-1})} & & \Big\downarrow{\scriptstyle \sigma} \\ K/\,\mathrm{N}_{\Phi^r}(s^{-1})\mathfrak{a} & \xrightarrow{\theta' \circ \Phi} & A_{tor}^{\sigma} \end{array}$$

Nous pouvons associer à l'idèle s un $\mathcal{O}$-idéal fractionnaire inversible $[s]_{\mathcal{O}}$ afin de décrire l'action de s et donc de σ. Cette action peut être étendue à $\mathrm{Aut}(\mathbb{C})$, mais il n'est alors plus possible de la décrire de façon suffisamment explicite en termes d'idéaux.

Nous pouvons maintenant étendre la construction de polynômes de classes aux courbes hyperelliptiques de genre 2 en suivant les travaux de Streng [252]. Les courbes hyperelliptiques de genre 2 sont classifiées à isomorphisme près par trois invariants appelés invariants d'Igusa. Sur le corps des nombres complexes, toute surface abélienne simple principalement polarisée est isomorphe à la jacobienne d'une courbe et toute courbe de genre 2 est hyperelliptique. De plus, le théorème de Torelli assure que deux courbes sont isomorphes si et seulement leurs jacobiennes, munies de leurs polarisations principales canoniques, le sont. Les surfaces abéliennes simples principalement polarisées peuvent donc être classifiées par les invariants d'Igusa des courbes associées. Ces invariants peuvent se calculer directement à partir de la matrice des périodes d'une surface abélienne en utilisant les fonctions thêta. Il est donc possible d'étendre l'approche de la sous-section précédente de différentes façons pour construire les polynômes de classes d'Igusa par approximation complexe :

- calculer les invariants de l'orbite d'un idéal de $\mathcal{O}$ sous l'action du groupe de Galois du corps réflexe en utilisant le groupe de classes de son anneau des entiers, le théorème principal de la multiplication complexe et la norme réflexe — dans ce cas le polynôme est à coefficients dans le sous-corps fixé par la conjugaison complexe du corps réflexe — ;
- calculer les invariants pour l'orbite d'un idéal de $\mathcal{O}$ sous l'action du groupe de Picard de $\mathcal{O}$, i.e. du groupe des idéaux fractionnaires inversibles de $\mathcal{O}$;
- calculer les invariants pour l'ensemble du semi-groupe de classes de $\mathcal{O}$, i.e. toutes les classes d'idéaux propres de $\mathcal{O}$.

Enfin, une méthode de Mestre permet de retrouver l'équation d'une courbe hyperelliptique de genre 2 à partir de ses invariants d'Igusa. Les polynômes de classes d'Igusa peuvent donc être utilisés pour construire des courbes hyperelliptiques de genre 2 intéressantes d'un point de vue cryptographique.