ON BINARY AND TERNARY KLOOSTERMAN SUMS

by

Kseniya Garaschuk

B.Sc., Simon Fraser University, 2005

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
in the Department
of
Mathematics

SIMON FRASER UNIVERSITY
Fall 2007

APPROVAL

Name: Kseniya Garaschuk

Degree: Master of Science

Title of thesis: On binary and ternary Kloosterman sums

Examining Committee: Dr. Cedric Chauve
Chair

Dr. Petr Lisoněk, Senior Supervisor

Dr. Jonathan Jedwab, Supervisor

Dr. Michael Monagan, Examiner

Date Approved: November 26, 2007

Abstract

We study certain exponential sums $K(a)$, known as Kloosterman sums, when $a \in \mathbb{F}_{2^m}$ or $a \in \mathbb{F}_{3^m}$.

For the binary case we establish the exact spectrum of the number of coset leaders of cosets of weight 3 of the binary Melas code. We derive a family of elliptic curves that allows us to characterize all $a \in \mathbb{F}_{2^m}$ for which $K(a)$ is divisible by 3. As an application we construct so-called "caps with many free pairs of points" in $\mathrm{PG}(n, 2)$ and describe their use in statistical experimental designs.

In the ternary case we use a similar method. By transforming a certain system of equations over $\mathbb{F}_{3^m}^*$ into a parametrized family of elliptic curves, we classify and count those $a \in \mathbb{F}_{3^m}$ for which $K(a) \equiv 0, 2 \pmod 4$.

We also present a result which is of independent interest, namely a generalization of the well known fact that $\mathrm{Tr}(a) = 0$ $(a \in \mathbb{F}_{2^m})$ if and only if $a = t^2 + t$ for some $t \in \mathbb{F}_{2^m}$.

Acknowledgments

I would like to express my sincere gratitude to Simon Fraser University and the Department of Mathematics for having me as a student and supporting me with Graduate Fellowships and teaching appointments. I would also like to thank NSERC for the funding I received through them that allowed me to attend numerous conferences and meet many interesting people that I now call my friends.

On the personal note, first and foremost, I would like to thank my supervisor Dr. Petr Lisoněk. Thank you for being patient and encouraging and for guiding me through this entire process; I could not ask for a better advisor.

To my committee members for reading this thesis and making truly helpful suggestions.

To Jordan for everything that you mean to me.

To Ira for keeping me in your heart.

To Mahdad for inspiring me, $\lim_{t\to 2.5^-} \mathcal{HR} = \infty$.

Thanks to all of my friends for sharing your life experiences with me.

To my officemates for frequent coffee breaks and sleepless nights at the conferences.

To all of my family for believing in me and for making me what I am today.

Finally, I would like to thank my Мама and Папа for never ceasing to spoil me.

Contents

List of Tables

Chapter 1

Background

Throughout this thesis we assume a knowledge of finite fields and linear codes. We ask the reader to refer to [20], [22], [30] and [17] for more details on these subjects if needed. In this chapter we will state the essential facts and definitions which will be used later on. We will also present a new result which is of independent interest, namely a generalization of the well known fact that $\mathrm{Tr}(a) = 0$ ($a \in \mathbb{F}_{2^m}$) if and only if $a = t^2 + t$ for some $t \in \mathbb{F}_{2^m}$.

1.1 Results on finite fields

Throughout the thesis let $\mathbb{F}_{p^m}$ denote the finite field of order p^m, where p is prime, $q = p^m$, and let $\mathbb{F}_{p^m}^* := \mathbb{F}_{p^m} \setminus \{0\}$. We will often use the fact that $\mathbb{F}_{p^m}$ can be viewed as an m-dimensional vector space over $\mathbb{F}_p$.

Let $\mathrm{Tr} : \mathbb{F}_{p^m} \to \mathbb{F}_p$ denote the trace mapping given by

$$\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{p^i} = x + x^p + \cdots + x^{p^{m-1}}.$$

Lemma 1.1.1. [20, p. 55] *Let $x, y \in \mathbb{F}_{p^m}$. Then the trace mapping satisfies the following properties:*

1. $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$,
2. $\mathrm{Tr}(x^p) = \mathrm{Tr}(x)$,
3. $\mathrm{Tr}(cx) = c\mathrm{Tr}(x)$ *for all* $c \in \mathbb{F}_p$,
4. *Trace mapping is a $\mathbb{F}_p$-linear transformation from $\mathbb{F}_{p^m}$ onto $\mathbb{F}_p$.*

The following result is well known and easy to prove:

Proposition 1.1.2. [20, p. 56] *Let $a \in \mathbb{F}_{p^m}$. $\mathrm{Tr}(a) = 0$ if and only if $a = t^p - t$ for some $t \in \mathbb{F}_{p^m}$.*

Proof. For all $t \in \mathbb{F}_{p^m}$ we have $\mathrm{Tr}(t^p - t) = \mathrm{Tr}(t^p) - \mathrm{Tr}(t) = 0$.

On the other hand, let ϕ denote a mapping from $\mathbb{F}_{p^m}$ to itself defined by $\phi(t) = t^p - t$. Notice that ϕ is $\mathbb{F}_p$-linear. Then $\mathrm{Ker}(\phi) = \mathbb{F}_p$ and since $\mathbb{F}_{p^m} \cong \mathbb{F}_p^m$, we can consider $\mathrm{Im}(\phi)$ as a vector subspace of $\mathbb{F}_p^m$ of dimension $m-1$. Every element in $\mathrm{Im}(\phi)$ is of trace zero and the set of elements of trace zero forms a proper subspace of $\mathbb{F}_p^m$ by Lemma 1.1.1. Therefore the elements of $\mathrm{Im}(\phi)$ are precisely the elements of trace zero. □

Corollary 1.1.3. *Let $a \in \mathbb{F}_p$. Then $\mathrm{Tr}(x) = a$ for exactly p^{m-1} elements $x \in \mathbb{F}_{p^m}$.*

Proof. It follows from the proof of Proposition 1.1.2 that there are p^{m-1} elements of $\mathbb{F}_{p^m}$ of trace zero. Then Lemma 1.1.1 (1, 4) implies the general statement. □

The following result can be found, for example, in [17, p. 8].

Lemma 1.1.4. *Let $f(x) = ax^2 + bx + c$ be a polynomial of degree 2 over $\mathbb{F}_{2^m}$ with $b \neq 0$ and let $\delta = ac/b^2$. Then $f(x)$ has 2 roots in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}(\delta) = 0$.*

Proof. Since $b \neq 0$, let $y = ax/b$. Then $ax^2 + bx + c = 0$ becomes

$$y^2 + y + \delta = 0. \tag{1.1}$$

Then by Proposition 1.1.2 equation (1.1), and hence $f(x)$, has solutions in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}(\delta) = 0$. To see that it has two solutions, note that if $y = y_0$ is a solution to (1.1), then so is $y = y_0 + 1$. □

Lemma 1.1.5. *Let s be a positive integer. Then $f(x) = x^s$ is injective on $\mathbb{F}_{2^m}$ if and only if $\gcd(s, 2^m - 1) = 1$.*

Proof. Since $f(x) = 0$ if and only if $x = 0$, we have to consider all the non-zero elements of $\mathbb{F}_{2^m}$. Let α be a primitive element of $\mathbb{F}_{2^m}$ and let $x_1 = \alpha^a$, $x_2 = \alpha^b$ for some $a, b \in \mathbb{Z}_{2^m-1}$, $a \neq b$. Then

$$x_1^s = x_2^s \iff \alpha^{as} = \alpha^{bs} \iff as \equiv bs \pmod{2^m - 1},$$

so that

$$f(x_1) = f(x_2) \iff s(a-b) \equiv 0 \pmod{2^m - 1}. \tag{1.2}$$

If the inverse of s exists, that is $\gcd(s, 2^m - 1) = 1$, then $a = b$ and $f(x)$ is injective. Otherwise, if $\gcd(s, 2^m - 1) \neq 1$, then $st \equiv 0 \pmod{2^m - 1}$ for some non-zero $t \in \mathbb{Z}_{2^m-1}$ and hence by (1.2) $f(x)$ is not injective. □

It is surprising that the following natural generalization of Proposition 1.1.2 for $p = 2$ to the case $\mathrm{Tr}(a^{1/(2^k-1)}) = 0$ has not been noted before. It is an interesting result and we will also use it later on, however it does not generalize further to the case $p > 2$.

Theorem 1.1.6. *Let $m > 1$ and let k be such that $\gcd(2^k - 1, 2^m - 1) = 1$. Then for each $a \in \mathbb{F}_{2^m}$ we have $\mathrm{Tr}(a^{1/(2^k-1)}) = 0$ if and only if $a = t^{2^k} + t^{2^k-1}$ for some $t \in \mathbb{F}_{2^m}$.*

Proof. Since $\gcd(2^k-1, 2^m-1) = 1$, there exists a unique $x \in \mathbb{Z}_{2^m-1}$ such that $y^{1/(2^k-1)} = y^x$ for all $y \in \mathbb{F}_{2^m}$.

($\Leftarrow$) Let $a = t^{2^k} + t^{2^k-1}$ for some $t \in \mathbb{F}_{2^m}$. Then

$$\begin{aligned}
a^{1/(2^k-1)} &= (t^{2^k} + t^{2^k-1})^{1/(2^k-1)} \\
&= (t^{2^k-1}(t+1))^{1/(2^k-1)} \\
&= t(t+1)^{1/(2^k-1)} \\
&= (t+1)(t+1)^{1/(2^k-1)} + (t+1)^{1/(2^k-1)} \\
&= (t+1)^{2^k/(2^k-1)} + (t+1)^{1/(2^k-1)} \\
&= (t^{2^k}+1)^{1/(2^k-1)} + (t+1)^{1/(2^k-1)} \\
&= \sum_{j=0}^{x} \binom{x}{j} (t^{2^k j} + t^j).
\end{aligned}$$

Therefore

$$\begin{aligned}
\mathrm{Tr}(a^{1/(2^k-1)}) &= \mathrm{Tr}\left(\sum_{j=0}^{x} \binom{x}{j} (t^{2^k j} + t^j) \right) \\
&= \sum_{j=0}^{x} \binom{x}{j} \mathrm{Tr}(t^{2^k j} + t^j) \\
&= 0.
\end{aligned}$$

($\Rightarrow$) We shall show that the equation

$$t^{2^k} + t^{2^k-1} = a \tag{1.3}$$

has 0 or 2 solutions in $\mathbb{F}_{2^m}$ (not counting solution multiplicities) for each $a \in \mathbb{F}_{2^m}$. If $a = 0$, then (1.3) has 2 solutions $t = 0, 1$. If $a \neq 0$, then by substituting $\bar{t} = 1/t$ into (1.3) and setting $z = 1/a$ we arrive at

$$\bar{t}^{2^k} + z\bar{t} + z = 0. \tag{1.4}$$

Let t_0 be a solution to (1.4), i.e. $t_0^{2^k} + zt_0 + z = 0$. We will show that there exists a unique $d \neq 0$ such that $t_0 + d$ is also a solution to (1.4). Substituting $\bar{t} = t_0 + d$ into (1.4) we get:

$$\begin{aligned}
(t_0 + d)^{2^k} + z(t_0 + d) + z = 0 &\Leftrightarrow t_0^{2^k} + d^{2^k} + zt_0 + zd + z = 0 \\
&\Leftrightarrow d^{2^k} + zd = 0 \\
&\Leftrightarrow d^{2^k - 1} = z \\
&\Leftrightarrow d = z^{1/(2^k-1)}.
\end{aligned}$$

Recall that $z^{1/(2^k-1)}$ exists and therefore d is unique, and $z \neq 0$ implies $d \neq 0$, so if we have one solution to (1.4), then we have exactly two of them. Therefore exactly one half of the elements $a \in \mathbb{F}_{2^m}$ can be written in the form $a = t^{2^k} + t^{2^k-1}$ and from the first part of the proof we know that $\mathrm{Tr}(a^{1/(2^k-1)}) = 0$ for all such a. There cannot be any other elements a for which $\mathrm{Tr}(a^{1/(2^k-1)}) = 0$. This is because $a \mapsto a^{1/(2^k-1)}$ is a bijection on $\mathbb{F}_{2^m}$ by the assumption on k, and $\mathrm{Tr}(b) = 0$ holds for exactly one half of the elements $b \in \mathbb{F}_{2^m}$. □

The following result will be needed in Chapter 3.

Corollary 1.1.7. *Let m be odd. The mapping $t \mapsto t^4 + t^3$ is two-to-one on $\mathbb{F}_{2^m}$. Furthermore, for each $d \in \mathbb{F}_{2^m}$ such that $\mathrm{Tr}(d) = 1$ there is exactly one pair $\{u, v\}$ with $u, v \in \mathbb{F}_{2^m}$ such that $u - v = d$ and $u^4 + u^3 = v^4 + v^3$.*

Proof. The fact that $t \mapsto t^4 + t^3$ is two-to-one on $\mathbb{F}_{2^m}$ follows from the second part of the proof of Theorem 1.1.6 and from the fact that $\gcd(2^2 - 1, 2^m - 1) = 1$ (since m is odd).

Let d be an arbitrary element of $\mathbb{F}_{2^m}$ of trace 1. The equation $u^4 + u^3 = (u+d)^4 + (u+d)^3$ simplifies to

$$d(u^2 + du + d^3 + d^2) = 0.$$

The second factor on the right-hand side, viewed as a quadratic in u, has exactly two roots in $\mathbb{F}_{2^m}$ by applying Lemma 1.1.4 where we get $\delta = (d^3 + d^2)/d^2 = d + 1$ and so $\mathrm{Tr}(\delta) = 0$ by the assumption $\mathrm{Tr}(d) = 1$. These two roots are the pair $\{u, v\}$ from the statement of the corollary.

□

1.2 Almost perfect nonlinear functions

Most widely used secret-key block ciphers, such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES), have a relatively simple structure [31]. The encryption process consists of a certain number of iterations. Within each round a given bitstring is xor-ed with a round key, transformed using substitution boxes, or S-boxes, and then permuted. The security of these ciphers therefore heavily relies on S-boxes, since they are the only nonlinear components of such cryptosystems. When DES was proposed by IBM in the 1970's, there were a lot of concerns regarding its mysteriously chosen S-boxes. There were even suspicions that the National Security Agency of the US had modified them. While the majority of IBM researchers confirmed that NSA did not tamper with the security of the system, Konheim, one of the designers of DES, was quoted as saying, "We sent the S-boxes off to Washington. They came back and were all different. We ran our tests and they passed."[28, p. 280] When comparing DES S-boxes with randomly chosen ones, it becomes clear that they were specifically designed and finely tuned to prevent certain types of attacks. In particular, the concept of differential cryptanalysis, introduced by Eli Biham and Adi Shamir in 1990, was known to both NSA and IBM before DES became a standard. Although DES S-boxes do not appear to have any algebraic structure, it was not until 2001 that a new standard (AES) was adopted. Due to its structured S-boxes, among other things, AES is proven secure against differential attacks. Its S-boxes are defined algebraically using the function $f(x) = x^{-1}$ over $\mathbb{F}_{2^8}$, a function that is close to one particular instance of a class of so-called almost perfect nonlinear (APN) functions; it is APN for most of $(a, b) \in (\mathbb{F}_{2^m}^*, \mathbb{F}_{2^m})$, except for a small finite number of constants $a \in \mathbb{F}_{2^m}^*$, $b \in \mathbb{F}_{2^m}$ for which $\nabla_f = 4$ as introduced later in Section 1.2.1.

APN functions are useful not only in cryptography. They can also be used to construct different combinatorial structures such as distance regular graphs, association schemes, uniformly packed codes [9] and binary caps in $\mathrm{PG}(n, 2)$ with many free pairs of points.

It is hard to trace who was the first person to introduce the notion of highly nonlinear functions with some references going as far back as 1967. In this section we will start with the definitions first presented by Nyberg and Knudsen [27], [26] and use the notation of [15]. We distinguish between three different classes of highly nonlinear functions, namely almost perfect nonlinear (APN), almost bent (AB) and crooked functions (CR), whose classes we shall denote by $\mathcal{APN}$, $\mathcal{AB}$, $\mathcal{CR}$ correspondingly. Although the definitions can be extended to more general domains, all of the known constructions of these functions are done over

finite fields and their associated vector spaces, and this is what we will limit ourselves to. All known examples of APN functions are given as polynomial functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$. We will state alternative definitions for APN and AB functions and show some of their properties, but will not go into discussion regarding crooked functions. From now on we will freely switch between $\mathbb{F}_2^m$ and $\mathbb{F}_{2^m}$.

1.2.1 Highly nonlinear functions

Let f be a mapping from $\mathbb{F}_{p^m}$ to itself. For all $a, b \in \mathbb{F}_{p^m}$ let $N(a,b)$ denote the number of solutions $x \in \mathbb{F}_{p^m}$ of $f(x+a) - f(x) = b$. Consider

$$\nabla_f = \max\{N(a,b) : a \in \mathbb{F}_{p^m}^*, b \in \mathbb{F}_{p^m}\}.$$

The smaller the value of ∇_f, the further f is from being linear. To see this consider a linear function $f(x) = cx + d$ where $c, d \in \mathbb{F}_{p^m}$. Then for $a \in \mathbb{F}_{p^m}^*, b \in \mathbb{F}_{p^m}$

$$f(x+a) - f(x) = b \iff ca = b,$$

so that $N(a,b) = p^m$ or $N(a,b) = 0$ and hence $\nabla_f = p^m$.

Therefore any function with $\nabla_f < p^m$ is called nonlinear. A more precise measure of non-linearity was introduced in [26].

Definition 1.2.1 (Differentially k-uniform Function, Perfect Nonlinear Function). *A mapping f from $\mathbb{F}_{p^m}$ to itself is called differentially k-uniform if $\nabla_f = k$. Differentially 1-uniform mappings over $\mathbb{F}_{p^m}$ are known as perfect nonlinear functions.*

From now on we will work with functions over $\mathbb{F}_{2^m}$ unless otherwise specified. The 2-uniform mappings over $\mathbb{F}_{2^m}$ are known as almost perfect nonlinear functions:

Definition 1.2.2 (Almost Perfect Nonlinear Function). *A mapping f from $\mathbb{F}_{2^m}$ to itself is called almost perfect nonlinear (APN) if for each $a \in \mathbb{F}_{2^m}^*$, $b \in \mathbb{F}_{2^m}$ the equation*

$$f(x+a) - f(x) = b \tag{1.5}$$

has at most two solutions in $\mathbb{F}_{2^m}$.

Notice that the solutions to (1.5) in $\mathbb{F}_{2^m}$ occur in pairs $\{x_0, x_0 + a\}$, which is why these functions are called *almost* perfect nonlinear.

Definition 1.2.3 (Fourier Transform). [9] *The Fourier transform of f (also called Walsh or Hadamard transform) $\mu_f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{Z}$ is defined as follows:*

$$\mu_f(a,b) = \sum_{x \in \mathbb{F}_2^m} (-1)^{\langle a,x \rangle} (-1)^{\langle b,f(x) \rangle},$$

where $a, b \in \mathbb{F}_{2^m}$ and $\langle \cdot, \cdot \rangle$ denotes the standard inner product on $\mathbb{F}_2^m$.

In [22] the Fourier transform of a Boolean function $F : \mathbb{F}_2^m \to \{0,1\}$ is given by

$$\bar{F}(a) = \sum_{x \in \mathbb{F}_2^m} (-1)^{\langle a,x \rangle} F(x),$$

with $a \in \mathbb{F}_2^m$. The function F is called *bent* if $\bar{F}(a) = \pm 2^{m/2}$ for every $a \in \mathbb{F}_{2^m}$. Bent functions are furthest away than any other Boolean function from any linear function. More precisely, they are at the distance at least $2^{m-1} \pm 2^{m/2-1}$ from any codeword of a $[2^m, m+1, 2^{m-1}]$-code, known as the first-order Reed-Muller code [22].

Definition 1.2.4 (Almost Bent Function). [9] *A mapping f from $\mathbb{F}_2^m$ to itself is called almost bent (AB) if $\mu_f(a,b) \in \{0, \pm 2^{(m+1)/2}\}$ for all $(a,b) \neq (0,0)$.*

Note that AB functions exist only for m odd simply because $\pm 2^{(m+1)/2}$ has to be an integer.

There are connections between AB functions and bent Boolean functions [5], however we will not explore them here.

Definition 1.2.5 (Crooked Function). [9] *A function f from $\mathbb{F}_2^m$ to itself is called crooked if $f(0) = 0$ and*

1. *$f(x) + f(y) + f(z) + f(x+y+z) \neq 0$ when x, y, z are distinct*
2. *$f(x) + f(y) + f(z) + f(x+a) + f(y+a) + f(z+a) \neq 0$ when $a \neq 0$.*

1.2.2 Alternative definitions of APN functions

Apart from the most classical definitions given in the previous section, both APN and AB functions have various alternative definitions. They can be characterized using sets $H_a(f)$, the number of solutions to a certain system of equations, as well as in terms of binary linear codes and the Fourier transforms.

Let f be a mapping from $\mathbb{F}_2^m$ to itself, $q = 2^m$. For $a \in \mathbb{F}_2^m$, $a \neq \mathbf{0}$ denote by $H_a(f)$, or simply H_a, the set $H_a(f) = \{f(x+a) - f(x) | x \in \mathbb{F}_2^m\}$.

Lemma 1.2.6. *A function f is APN if $|H_a(f)| = \frac{1}{2}q$ for all non-zero $a \in \mathbb{F}_2^m$.*

Lemma 1.2.7. *A function f is APN if and only if the system of equations*

$$\begin{aligned} x &+ y &= a \\ f(x) &+ f(y) &= b \end{aligned}$$

has 0 or 2 solutions (x, y) for every $(a, b) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$, $a \neq \mathbf{0}$. The system has precisely 2 solutions when $b \in H_a(f)$.

Both Lemma 1.2.6 and Lemma 1.2.7 follow directly from Definition 1.2.2. Using these Lemmas we can prove that APN property of functions is preserved under linear transformations.

Proposition 1.2.8. *Let f be an APN function from $\mathbb{F}_{2^m}$ to itself, then given $a \in \mathbb{F}_{2^m}^*$, $b \in \mathbb{F}_{2^m}$, the function $\bar{f}(x) = f(ax + b)$ is also APN.*

Proof. Consider $H_c(\bar{f})$ for all non-zero $c \in \mathbb{F}_{2^m}$:

$$\begin{aligned} H_c(\bar{f}) &= \{\bar{f}(x + c) + \bar{f}(x) | x \in \mathbb{F}_{2^m}\} \\ &= \{f(a(x + c) + b) + f(ax + b) | x \in \mathbb{F}_{2^m}\} \\ &= \{f(y + ac) + f(y) | y \in \mathbb{F}_{2^m}\} \\ &= H_{ac}(f). \end{aligned}$$

The mapping $c \mapsto ac$ is a bijection on $\mathbb{F}_{2^m}$ for all $a \in \mathbb{F}_{2^m}^*$, therefore $|H_c(\bar{f})| = |H_{ac}(f)| = \frac{1}{2}q$ and $\bar{f}(x)$ is APN by Definition 1.2.6. □

APN functions can be defined in many different ways, and although we will not use the following result, it is interesting to note that, similarly to AB functions, APN functions can be defined in terms of the Fourier transform.

Theorem 1.2.9. [9] *For any function $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$*

$$\sum_{a,b \in \mathbb{F}_{2^m}} (\mu_f(a, b))^4 \geq 3 \cdot (2^m)^4 - 2 \cdot (2^m)^3$$

with equality if and only if f is APN.

Just like APN functions, AB functions can be defined in terms of the number of solutions to certain systems of equations. The following theorem is also due to van Dam and Fon-Der-Flaass [9].

Theorem 1.2.10. [9] *A function $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is almost bent if and only if the system*

$$\begin{array}{ccccccc} x & + & y & + & z & = & a \\ f(x) & + & f(y) & + & f(z) & = & b \end{array} \tag{1.6}$$

has $q-2$ or $3q-2$ solutions (u,v,w) for every (a,b), where $q = 2^m$. If so, then the system has $3q-2$ solutions if $b = f(a)$ and $q-2$ solutions otherwise.

The proof is technical and is done in terms of matrices. The full version of it can be found in [9] and [23].

There are proper inclusions between the classes of highly nonlinear functions, namely:

$$\mathcal{CR} \subset \mathcal{AB} \subset \mathcal{APN}.$$

The second inclusion is easy to see: if f is not APN, then equation (1.5) has more than two solutions, say $x = u, v$ such that $f(u+a) + f(u) = b = f(v+a) + f(v)$. Then the system

$$\begin{array}{ccccccc} x & + & y & + & z & = & v \\ f(x) & + & f(y) & + & f(z) & = & f(v) \end{array}$$

has an additional solution $x = u$, $y = u + a$, $z = v + a$. Therefore by Theorem 1.2.10 the function $f(x)$ is not AB.

Until recently, every known APN function was known to be equivalent to one of the families of power mappings from $\mathbb{F}_{2^m}$ to itself, i.e. $f(x) = x^k$, as summarized in Tables 1.1 and 1.2. It has been shown that for $m \leq 15$ there are no more power APN mappings apart from those and so it was believed that this list is exhaustive. However, in 2005 the first example of a new APN function that is not equivalent to any power mapping was found [12]. This new function is a mapping $F(x)$ from $\mathbb{F}_{2^{10}}$ to itself defined by $F(x) = x^3 + ux^{36}$, where u is a suitable element of $\mathbb{F}_{2^{10}}^*$.

There are several notions of equivalence between highly nonlinear functions, including equivalence in the general sense known as CCZ-equivalence first introduced in [5] by Carlet, Charpin and Zinoviev and named after its authors. Given just two functions it is hard to decide whether they are CCZ-equivalent or not - there is no known theoretical approach to this problem. In fact, there is no reference showing that some of the classical families of APN and AB functions as in Tables 1.1 and 1.2 are not CCZ-equivalent. Today, with constantly emerging new results [4, 2], it becomes more and more difficult to prove that a given function is not equivalent in some way to any of the known ones. In [12] tools such as dimension arguments (via computer assistance) and Fourier spectra were used and the search for more invariants for CCZ-equivalence is ongoing.

Name	Exponent k	Type
Gold	$2^i + 1$, $(i, m) = 1$, $1 \leq i < n$	CR
Kasami	$2^{2i} - 2^i + 1$, $(i, m) = 1$, $2 \leq i < n$	AB
Field inverse (Kloosterman)	$2^m - 2 \equiv -1 \pmod{2^m - 1}$	APN
Welch	$2^n + 3$	AB
Niho	$2^n + 2^{n/2} - 1$ for even n $2^n + 2^{(3n+1)/2} - 1$ for odd n	AB AB
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$, $m = 5i$	APN

Table 1.1: Known APN functions $f(x) = x^k$ over $\mathbb{F}_{2^m}$ where $m = 2n + 1$

Name	Exponent k	Type
Gold	$2^i + 1$, $(i, m) = 1$, $1 \leq i < n$	APN
Kasami	$2^{2i} - 2^i + 1$, $(i, m) = 1$, $2 \leq i < n$	APN
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$, $m = 5i$	APN

Table 1.2: Known APN functions $f(x) = x^k$ over $\mathbb{F}_{2^m}$ where $m = 2n$

1.3 Linear codes

In this section we introduce binary linear codes and show their correspondence to almost perfect non-linear functions and binary caps in PG$(n, 2)$.

1.3.1 Definitions and preliminary facts

We use standard definitions and notation for linear codes [22].

Definition 1.3.1 (Hamming Distance). *For all $x, y \in \mathbb{F}_q^n$ the Hamming distance $d(x, y)$ is defined by*

$$d(x, y) = |\{i | 1 \leq i \leq n, x_i \neq y_i\}|,$$

i.e. $d(x, y)$ is the number of coordinates in which x and y differ.

Definition 1.3.2 (Linear Code, Binary Linear Code). *A linear $[n, k, d]_q$-code C is a k-dimensional linear subspace of $\mathbb{F}_q^n$ such that any two different elements of the code are at Hamming distance at least d and there exists a pair that is at Hamming distance exactly d.*

The block length of C is n, the redundancy is $r = n - k$, the minimum distance is d and its elements are called codewords. If $q = 2$, then C is called binary $[n, k, d]$-code.

The minimum distance of a code determines its error-correction capabilities. Given a received vector, the decoder will try to find the codeword closest to it. However, if too many errors have occurred (over $\lfloor (d-1)/2 \rfloor$ to be precise), the received vector might be equidistant from two codewords or even be closer to a codeword different from the correct one.

Definition 1.3.3 (Hamming Weight). *For $x \in \mathbb{F}_q^n$ the Hamming weight $w(x)$ is defined by*

$$w(x) = d(x, \mathbf{0}),$$

where $\mathbf{0}$ is the zero vector in $\mathbb{F}_q^n$. The weight of a linear code C is the minimum weight among all of its non-zero codewords.

From now on by weight and distance we shall mean Hamming weight and Hamming distance, and by code or $[n, k, d]$-code we mean binary linear $[n, k, d]$-code, unless otherwise specified.

Remark 1.3.4. Let C be a linear code. If $x, y \in C$, then $x - y \in C$. Then $d(x, y) = d(x - y, \mathbf{0})$ and therefore the minimum distance of the code C is always equal to its weight.

Definition 1.3.5 (Generator Matrix). *Let C be an $[n, k, d]$-code. A $k \times n$ matrix G is called a generator matrix for C if its rows form a basis for C.*

Definition 1.3.6 (Dual Code). *For an $[n, k, d]_q$-code C, the dual code $C^\perp$ is defined as follows:*

$$C^\perp = \{y \in \mathbb{F}_q^n : \langle x, y \rangle = 0 \quad \forall x \in C\},$$

where $\langle \cdot, \cdot \rangle$ denotes the standard inner product on $\mathbb{F}_q^n$.

Clearly the dual of a linear k-dimensional code is a linear code of dimension $n - k$.

Definition 1.3.7 (Parity Check Matrix, Syndrome). *Let C be an $[n, k, d]_q$-code with generator matrix G. An $r \times n$ generator matrix H for $C^\perp$ is called a parity check matrix for C and Hx^T is called a syndrome of x with respect to H for all $x \in \mathbb{F}_q^n$.*

Since $GH^T = 0$ by the definition of the dual code, we have

$$x \in C \iff Hx^T = \mathbf{0}.$$

Theorem 1.3.8. [22, p. 33] *Let H be a parity check matrix of an $[n, k, d]_q$-code C. Then C has minimum distance d if and only if every $d-1$ columns of H are linearly independent and some d columns of H are linearly dependent.*

Proof. Suppose C has block length n and let $h_1, \ldots, h_n$ be columns of H. Then $w = (w_1, \ldots, w_n)$ is a codeword of C if and only if

$$Hw^T = \sum_{i=1}^{n} w_i h_i = \mathbf{0}.$$

Hence w is of weight u if and only if some u columns of H are linearly dependent. □

Definition 1.3.9 (Coset, Coset leader, Weight of a coset). *Let C be a linear $[n, k, d]_q$-code. For any vector $y \in \mathbb{F}_q^n$, the set $C + y = \{x + y | x \in C\}$ is called a coset of C. A coset leader of $C + y$ is its element (not necessarily unique) with the smallest Hamming weight. The weight of a coset is the weight of its coset leader(s).*

Proposition 1.3.10. *Two vectors are in the same coset if and only if they have the same syndrome.*

Proof. Let $D = C + y$ be a coset of a code C, $y \in \mathbb{F}_q^n$. Then w_1 and w_2 belong to D if and only if $w_1 = x_1 + y$ and $w_2 = x_2 + y$ for some $x_1, x_2 \in C$. Therefore $w_1 - w_2$ is a codeword in C, or, equivalently, $H(w_1 - w_2)^T = \mathbf{0}$ and so $Hw_1^T = Hw_2^T$. □

Thus there is a one-to-one correspondence between cosets and syndromes, giving rise to so-called "syndrome decoding". Suppose we are transmitting information over a noisy channel, and suppose that a codeword $x \in \mathbb{F}_q^n$ of an $[n, k, d]$-code C is sent and the vector $y \in \mathbb{F}_q^n$, $y = x + e$ is received. Then the vector e is called an *error vector* or an *error pattern*. The decoder then calculates the syndrome of the received vector, which depends only on the error pattern (hence the name). The possible error vectors are exactly the vectors in the coset D containing y. The decoder assumes that the probability of an error is low and therefore chooses a coset leader of D as an error vector. If there is more than one coset leader, the decoding is not unique and the decoder either outputs an error message or any one (or all) of the suitable codewords.

We now can move on to see how codes correspond to almost perfect nonlinear functions and binary caps.

1.3.2 Correspondence between codes and APN functions

Recall the definition of APN functions from Section 1.2. We have the following result due to Carlet, Charpin and Zinoviev [5].

Theorem 1.3.11. [5] *Let f be a function from $\mathbb{F}_{2^m}$ to itself such that $f(0) = 0$ and let α be a primitive element of $\mathbb{F}_{2^m}$. View α^i and $f(\alpha^i)$ as m-dimensional binary column vectors. Let C_f be the $[n = 2^m - 1, k, d]$ binary code defined by the parity check matrix*

$$\mathcal{H}_f = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{n-1}) \end{pmatrix}.$$

Then f is APN if and only if $d = 5$.

Proof. First notice that we can always apply a shift to get $f(0) = 0$. Since $\mathcal{H}_f$ is a $(2m) \times (2^m - 1)$ matrix, the dimension k of the code is such that $k \geq 2^m - 1 - 2m$. Since $\mathcal{H}_f$ doesn't contain zero columns or two equal columns, by Theorem 1.3.8 we have $d \geq 3$. Now let $c = (c_0, \ldots, c_{n-1})$ be a binary vector. Then by definition of a parity check matrix, $c \in C_f$ if and only if $\mathcal{H}_f c^T = \mathbf{0}$ or, equivalently,

$$\sum_{i=0}^{n-1} c_i \alpha_i = 0, \quad \sum_{i=0}^{n-1} c_i f(\alpha_i) = 0.$$

Therefore C_f has minimum distance 3 or 4 if and only if there are four distinct elements $x, x', y, y' \in \mathbb{F}_{2^m}$ such that

$$\begin{cases} x + y + x' + y' = 0, \\ f(x) + f(y) + f(x') + f(y') = 0. \end{cases} \tag{1.7}$$

Since $f(0) = 0$, the minimum distance is 3 when one of those elements is zero, otherwise it's four. These equations can also be re-written as follows:

$$\begin{cases} x + y = a, \\ f(x) + f(y) = b, \end{cases} \tag{1.8}$$

where $a, b \in \mathbb{F}_{2^m}$ and $a \neq 0$. If there exist two distinct pairs $\{x, y\}$ and $\{x', y'\}$ that satisfy (1.8), then there exist four distinct elements $x, x', y, y' \in \mathbb{F}_{2^m}$ that satisfy (1.7) and vise versa. Therefore by Lemma 1.2.7 $f(x)$ is APN if and only if C_f has minimum distance at least 5.

To see that d is at most 5, first assume that $d \geq 6$. If there exists a linear $[n, k, d]$ code, then there exists a linear $[n-1, k, d-1]$ code (simply delete one coordinate). So in our case if C_f has parameters $[2^m - 1, k, 6]$, with $k \geq 2^m - 1 - 2m$, then there is a linear $[2^m - 2, k, 5]$-code. However, such codes do not exist [3]. Therefore $d \leq 5$. Together with the first part of the proof we now see that $d = 5$. □

Observation 1.3.12. Since a linear $[2^m - 1, 2^m - 2m, 5]$-code does not exist [11], the code C_f as defined in Theorem 1.3.11 in the case $d = 5$ has dimension $k = 2^m - 1 - 2m$.

Theorem 1.3.11 is useful when showing certain properties of APN functions.

Proposition 1.3.13. *If f is a one-to-one APN function from $\mathbb{F}_{2^m}$ to itself, then f^{-1} is also APN.*

Proof. Once again, without loss of generality we can assume that $f(0) = 0$. By Theorem 1.3.11 f is APN if and only if the $[n = 2^m - 1, k, d]$ binary code C defined by the parity check matrix whose columns are of the form

$$\begin{pmatrix} \alpha^i \\ f(\alpha^i) \end{pmatrix}$$

has minimum distance 5. By swapping the horizontal blocks of $\mathcal{H}_f$ we get a parity check matrix $\bar{\mathcal{H}}_f$ with columns of the form

$$\begin{pmatrix} f(\alpha^i) \\ \alpha^i \end{pmatrix} = \begin{pmatrix} f(\alpha^i) \\ f^{-1}(f(\alpha^i)) \end{pmatrix}.$$

However, $\bar{\mathcal{H}}_f$ also defines C and, since f is one-to-one, by Theorem 1.3.11 f^{-1} is APN. □

One special case of the above proposition is the following:

Corollary 1.3.14. *Let $s, t \in \mathbb{Z}_{2^m-1}$ be such that $st \equiv 1 \pmod{2^m - 1}$. If $f(x) = x^s$ is APN, then so is $\bar{f}(x) = x^t$.*

1.3.3 Codes and binary caps

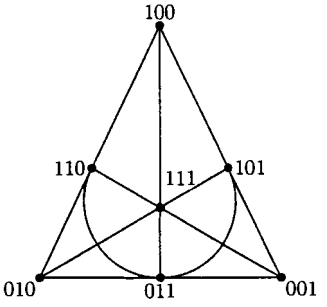
Let $\mathbb{F}_q^{n+1}$ be an $(n+1)$-dimensional vector space over the field $\mathbb{F}_q$. An $(m+1)$-dimensional subspace of $\mathbb{F}_q^{n+1}$ with zero deleted is called an *m-flat*. The *n-dimensional projective space over $\mathbb{F}_q$*, denoted by $\mathrm{PG}(n, q)$, is the set of all m-flats for $m = -1, 0, \ldots, n$. Incidence is

defined by containment of the corresponding subspaces, so on every m-flat we have the structure of $\mathrm{PG}(m,q)$. A *point*, a *line* and a *plane* are 0-flat, 1-flat and 2-flat respectively. An $(n-1)$-flat is called a *hyperplane*. By $(x_0 : \ldots : x_n)$ we denote a point of $\mathrm{PG}(n,q)$ corresponding to a 1-dimensional subspace of $\mathbb{F}_q^{n+1}$ spanned by $(x_0,\ldots,x_n) \in \mathbb{F}_q^{n+1} \setminus \{\mathbf{0}\}$. Therefore the points in the projective space are equivalence classes with the equivalence relation defined as follows:

$$(x_0,\ldots,x_n) \sim (\lambda x_0,\ldots,\lambda x_n), \lambda \in \mathbb{F}_q^*.$$

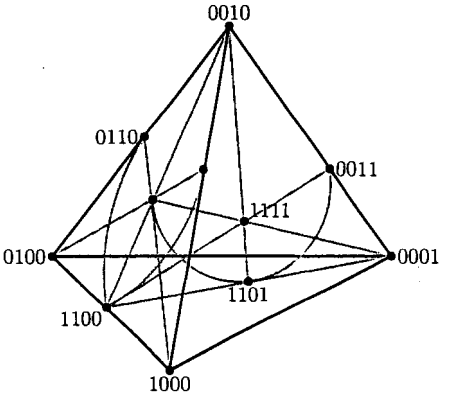
Since this representation is unique up to scalar multiplication, it will usually be right-normalized, i.e. scaled to make the right-most non-zero coordinate equal to one.

Let u, v be distinct points of $\mathrm{PG}(n,2)$. Since every point in $\mathrm{PG}(n,2)$ is a 1-dimensional subspace of $\mathbb{F}_2^{n+1}$, the third point on the line determined by u and v is $u+v$. The smallest example of a projective plane is $\mathrm{PG}(2,2)$, known as the *Fano plane*:



Note that in the figures for convenience we use $x_0x_1\ldots x_n$ instead of $(x_0 : x_1 : \ldots : x_n)$ to denote points in $\mathrm{PG}(n,2)$.

With 15 points and 35 lines, $\mathrm{PG}(3,2)$ has a copy of the Fano plane in each of its 15 hyperplanes (note that not all of the points are depicted in the following picture):



Definition 1.3.15 (Cap). *A cap is a set of points in $PG(n, q)$ that does not contain any collinear triples. An s-cap is a cap with s points.*

Example 1.3.16. Consider the set S of points in $\mathrm{PG}(3, 2)$ with $x_0 = 1$:

$$S = \{1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}.$$

Then S is an 8-cap in $\mathrm{PG}(3, 2)$.

Proposition 1.3.17. *H is a parity check matrix of an $[n, k, d]_q$-code C with minimum distance at least 4 if and only if H contains no repeated columns and the columns of H form an n-cap in $PG(r - 1, q)$, where $r = n - k$.*

Proof. If the minimum distance of C is at least 4, then by Theorem 1.3.8 the columns of H are all non-zero, no two of them are multiples of each other and no three of them are linearly dependent. Therefore the columns of H viewed as points in $\mathrm{PG}(r-1, q)$ form a cap in $\mathrm{PG}(r - 1, q)$. Similarly we can easily see the converse. □

Chapter 2

Elliptic curves and binary Kloosterman sums

In this chapter we work with elliptic curves over fields of characteristic 2 and binary Kloosterman sums. In Section 2.1 we survey the known results. We ask the reader to refer to [32] and [30] for more details on these topics. In Section 2.2 we study certain elliptic curves associated with binary Kloosterman sums $K(a)$ ($a \in \mathbb{F}_{2^m}$) where m is odd. In Section 2.2.2 we give a characterization of those a for which $K(a)$ is divisible by 3. In one direction this result was proved earlier; we give a shorter proof that shows the result in both directions. New results due to Charpin, Helleseth and Zinoviev then provide a connection to a characterization of all $a \in \mathbb{F}_{2^m}$ such that $\mathrm{Tr}(a^{1/3}) = 0$.

2.1 Basic definitions and properties of elliptic curves

In this section we will use standard definitions and notation. We follow the notation of [30] and ask the reader to refer to [30] for a more thorough introduction to elliptic curves.

Recall that the points in the projective plane $\mathrm{PG}(2, p^m)$ are equivalence classes denoted by $(X : Y : Z)$ and this representation is right-normalized, i.e. scaled to make the right-most non-zero coordinate equal to one. The *affine points* are the points with $Z = 1$ and *points at infinity* are those with $Z = 0$.

Definition 2.1.1 (Elliptic Curve, Generalized Weierstrass Equation). [30] *Let $\overline{\mathbb{F}}_{p^m}$ be the algebraic closure of $\mathbb{F}_{p^m}$. An elliptic curve $\mathcal{E}(\mathbb{F}_{p^m})$ over the finite field $\mathbb{F}_{p^m}$ is the set of*

points $(X : Y : Z)$, $(X, Y, Z) \in (\overline{\mathbb{F}}_{p^m})^3$ *given by the generalized Weierstrass equation:*

$$\mathcal{E}(\mathbb{F}_{p^m}) : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{2.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_{p^m}$ *are constants. The rational (or* $\mathbb{F}_{p^m}$*-rational) points on* $\mathcal{E}(\mathbb{F}_{p^m})$ *are points* $(X : Y : Z)$ *on* $\mathcal{E}(\mathbb{F}_{p^m})$ *such that* $(X, Y, Z) \in (\mathbb{F}_{p^m})^3$. *By* $\#\mathcal{E}(\mathbb{F}_{p^m})$ *we denote the number of rational points on* $\mathcal{C}$.

We will write $\mathcal{E}$ and $\#\mathcal{E}$ when the underlying field is understood.

Definition 2.1.2 (Singular Point, Singular Curve). *Let* $P = (X_0 : Y_0 : Z_0)$ *be a point on an elliptic curve* $\mathcal{E}$ *defined by* $F(X, Y, Z) = 0$. *Then* P *is called singular if and only if*

$$\frac{\partial F}{\partial X}(X_0 : Y_0 : Z_0) = \frac{\partial F}{\partial Y}(X_0 : Y_0 : Z_0) = \frac{\partial F}{\partial Z}(X_0 : Y_0 : Z_0) = 0.$$

A curve is called singular if it contains a singular point and non-singular otherwise.

If the characteristic of the field is not 2 or 3, then the Weierstrass equation can be further simplified to include only two constants. However, since we will be working with elliptic curves over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$, we need equation (2.1) in its most general form. Notice that in (2.1) $Z = 0$ implies $X^3 = 0$, so the only point at infinity on $\mathcal{E}$ is $\mathcal{O} = (0 : 1 : 0)$.

Since all the affine points can be written in the form $(X : Y : 1)$, for convenience we will use (X, Y) when describing them. We will normally use the Weierstrass equation in its non-homogenized form, which can be obtained by setting $x = X/Z$ and $y = Y/Z$ in (2.1):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.2}$$

Then an elliptic curve $\mathcal{E}$ in Definition 2.1.1 is the set of points (x, y) satisfying equation (2.2) together with the point at infinity.

We define the following quantities:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

Proposition 2.1.3. [30] *The value* Δ *defined above is called the discriminant of an elliptic curve* $\mathcal{E}$. *Then the curve* $\mathcal{E}$ *is singular if and only if* $\Delta = 0$.

Group Law. Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_{p^m}$ given by the generalized Weierstrass equation. The group of $\mathcal{E}$ is $(E, +)$, where E is the set of all $\mathbb{F}_{p^m}$-rational affine points on $\mathcal{E}$ (including the point at infinity). Let $P = (x, y)$ be an affine point on $\mathcal{E}$. The inverse of P is defined to be $-P = -(x, y) = (x, -a_1x - a_3 - y)$. For the point at infinity we have $-\mathcal{O} = \mathcal{O}$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be rational points on $\mathcal{E}$ different from $\mathcal{O}$. The group operation '+' arises naturally from the geometry of elliptic curves: to add two points P_1 and P_2, we first draw a line through them (it will be tangent to $\mathcal{E}$ if $P_1 = P_2$). This line intersects $\mathcal{E}$ in a third point $-P_3$ which we then "reflect" in the x-axis to get $P_3 = P_1 + P_2$. Algebraically, the group operation '+' is defined as follows:

- $P + \mathcal{O} = P$, $\mathcal{O} + \mathcal{O} = \mathcal{O}$, so $\mathcal{O}$ is the identity of the group $(\mathcal{E}, +)$
- If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 + P_2 = \mathcal{O}$
  Otherwise, if $x_1 \neq x_2$ let

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \ \mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

  and if $x_1 = x_2$ let

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \ \mu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

  Then

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - \mu - a_3. \end{aligned}$$

For details on isomorphism between any two non-singular curves see [30].

Definition 2.1.4. [24] *Two elliptic curves $\mathcal{E}_1$ and $\mathcal{E}_2$ over a field $\mathbb{F}_{p^m}$ given by*

$$\begin{aligned} \mathcal{E}_1 &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \\ \mathcal{E}_2 &: y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6 \end{aligned}$$

are isomorphic over $\mathbb{F}_{p^m}$ if and only if there exist $u, r, s, t \in \mathbb{F}_{p^m}$ such that the change of variables

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$$

transforms equation $\mathcal{E}_1$ to equation $\mathcal{E}_2$.

We would like to emphasize that the number of rational points on a curve is invariant under an isomorphism as we will later often use this fact.

2.2 Binary Kloosterman sums

Definition 2.2.1. *The Kloosterman map is the mapping* $K : \mathbb{F}_{p^m} \to \mathbb{R}$ *defined by*

$$K(a) := \sum_{x \in \mathbb{F}_{p^m}^*} \omega^{\mathrm{Tr}(x^{-1}+ax)}, \tag{2.3}$$

where ω *is* p^{th} *root of unity, i.e.* $\omega = e^{2\pi i/p}$.

These sums were first introduced in 1926 by the Dutch mathematician Hendrik Kloosterman and turn out to be fundamental for many problems in analytic number theory and in the theory of modular functions. Recently, Kloosterman sums have been shown to have close connections to coding theory. They are used when counting the number of coset leaders for cosets of a certain weight of some linear binary codes. Moreover, we can express the number of rational points on a parametrized family of elliptic curves, now known as Kloosterman curves, in terms of Kloosterman sums. We can therefore transform the problem of studying the spectrum of Kloosterman sums into counting the number of rational points on elliptic curves. This allows us to approach the problem from a different angle as well as run more extensive computations, since Schoff algorithm used by Magma for calculating the number of rational points on elliptic curves is quite fast and efficient.

One property of general Kloosterman sums that will be used later on is the following:

Lemma 2.2.2. $K(a) = K(a^p)$ *for all* $a \in \mathbb{F}_{p^m}$.

Proof. Since the mapping $x \mapsto x^p$ is bijective on $\mathbb{F}_{p^m}$ and since

$$\mathrm{Tr}(x^{-1} + ax) = \mathrm{Tr}((x^{-1} + ax)^p) = \mathrm{Tr}(x^{-p} + a^p x^p),$$

$K(a) = K(a^p)$ by definition. □

In this chapter we will study Kloosterman sums over $\mathbb{F}_{2^m}$, $m \geq 3$. In this case $\omega = -1$ and $K(a)$ is an integer for all $a \in \mathbb{F}_{2^m}$.

2.2.1 Kloosterman curves

Lauchaud and Wolfmann [19] provide a direct connection between a certain family of elliptic curves and binary Kloosterman sums. This enables them to discuss the distribution of the values of Kloosterman sums. We state their results below and include detailed proofs of their statements.

Definition 2.2.3 (Supersingular Curve, Ordinary Curve). *An elliptic curve is called supersingular if in the generalized Weierstrass form $a_1 = 0$. Otherwise it is said to be ordinary.*

Theorem 2.2.4. [19] *An ordinary elliptic curve $\mathcal{E}$ over $\mathbb{F}_{2^m}$ is isomorphic to one of the following curves:*

$$\begin{aligned} \mathcal{E}_a^+ : y^2 + xy &= x^3 + a, \\ \mathcal{E}_a^- : y^2 + xy &= x^3 + \tau x^2 + a, \end{aligned}$$

where $a \in \mathbb{F}_{2^m}$ and τ is a fixed element of $\mathbb{F}_{2^m}$ of trace 1.

Proof. Let $\mathcal{E}$ be given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Since $\mathcal{E}$ is ordinary, $a_1 \neq 0$ and we can apply the following substitution:

$$\begin{cases} x = a_1^2x + \dfrac{a_3}{a_1}, \\ y = a_1^3(y + sx) + \dfrac{a_4^{'}}{a_1}, \end{cases} \tag{2.4}$$

where $a_4^{'} = \dfrac{a_1^2a_4 + a_3^2}{a_1^2}$ and $s \in \mathbb{F}_{2^m}$. After normalizing to make the coefficient of x^3 equal to 1 we obtain:

$$y^2 + xy = x^3 + (\bar{a}_2 + s^2 + s)x^2 + \bar{a}_6.$$

If $\mathrm{Tr}(\bar{a}_2) = 0$, by Proposition 1.1.2 we can find $s \in \mathbb{F}_{2^m}$ such that $\bar{a}_2 = s^2 + s$. If $\mathrm{Tr}(\bar{a}_2) = 1$, we can find $s \in \mathbb{F}_{2^m}$ such that $\bar{a}_2 + \tau = s^2 + s$. Therefore $\mathcal{E}$ is isomorphic to $\mathcal{E}_a^+$ if $\mathrm{Tr}(\bar{a}_2) = 0$ and to $\mathcal{E}_a^-$ otherwise. □

Corollary 2.2.5. [19] *An ordinary elliptic curve $\mathcal{E}$ over $\mathbb{F}_{2^m}$ can be transformed into one of the Kloosterman curves:*

$$\begin{aligned} \mathcal{K}l_a^+ : y^2 + y &= ax + \frac{1}{x}, \\ \mathcal{K}l_a^- : y^2 + y &= ax + \frac{1}{x} + \tau, \end{aligned}$$

where $a \in \mathbb{F}_{2^m}$.

Proof. Theorem 2.2.4 and its proof imply that $\mathcal{E}$ is isomorphic to an elliptic curve with homogeneous equation

$$Y^2Z + XYZ = X^3 + bX^2Z + \bar{a}_6Z^3,$$

where b is either 0 or τ, depending on trace of $\bar{a}_2$. Let $a \in \mathbb{F}_{2^m}$ be such that $a^2 = \bar{a}_6$. Then apply the following substitutions in the listed order:

$$\begin{aligned} Y &= y + aZ, \\ X &= 1, \\ Z &= x. \end{aligned}$$

We obtain the equation

$$y^2x + yx = ax^2 + 1 + bx.$$

Since $x = 0$ does not lead to any solutions in the equation above, we can divide by x to get:

$$y^2 + y = ax + \frac{1}{x} + b,$$

which completes the proof. □

Consider the following equations over $\mathbb{F}_{2^m}$:

$$\begin{aligned} E_a^+ &: \mathrm{Tr}(x^{-1} + ax) = 0, \\ E_a^- &: \mathrm{Tr}(x^{-1} + ax) = 1, \end{aligned}$$

where $a \in \mathbb{F}_{2^m}$ is a fixed constant. Let $N^{\pm}(a)$ denote the number of solutions in $\mathbb{F}_{2^m}^*$ to $E_a^{\pm}$ respectively.

Proposition 2.2.6. [19] *Let $\#\mathcal{K}l_a^{\pm}$ denote the number of $\mathbb{F}_{2^m}$-rational points on $\mathcal{K}l_a^{\pm}$, $a \in \mathbb{F}_{2^m}$ respectively. Then $\#\mathcal{K}l_a^{\pm} = 2N^{\pm}(a) + 2$.*

Proof. The homogeneous equations corresponding to $\mathcal{K}l_a^{\pm}$ are

$$\begin{aligned} XY^2 + XYZ &= aX^2Z + Z^3 \\ XY^2 + XYZ &= aX^2Z + Z^3 + \tau XZ^2. \end{aligned}$$

We can now see that the curves $\mathcal{K}l_a^{\pm}$ are non-singular and have 2 points at infinity each, namely $(1:0:0)$ and $(0:1:0)$. By Lemma 1.1.4 if x is a solution to $E_a^{\pm}$, then there are exactly two values y such that (x, y) are affine $\mathbb{F}_{2^m}$-rational points on $\mathcal{K}l_a^{\pm}$. Since there are $N^{\pm}(a)$ solutions to $E_a^{\pm}$, the statement follows. □

Proposition 2.2.7. [19] *Let $a \in \mathbb{F}_{2^m}$. Then $2N^{\pm}(a) = 2^m - 1 \pm K(a)$.*

Proof. Since $N^+(a) + N^-(a) = 2^m - 1$ we have:

$$K(a) = N^+(a) - N^-(a) = 2N^+(a) - 2^m + 1. \tag{2.5}$$

This implies that $2N^+(a) = 2^m - 1 + K(a)$. The expression for $2N^-(a)$ follows similarly. □

The following proposition now follows easily:

Proposition 2.2.8. [19] *Let $a \in \mathbb{F}_{2^m}$. Then $\#\mathcal{K}l_a^{\pm} = 2^m + 1 \pm K(a)$.*

Proposition 2.2.9. [19] *Let $a \in \mathbb{F}_{2^m}$. The number $N^+(a)$ is odd and the number $N^-(a)$ is even.*

Proof. It's enough to show one of the assertions since $N^+(a) + N^-(a) = 2^m - 1$ and the other one will follow. First let $a \in \mathbb{F}_{2^m}^*$. Notice that if x is a solution to E_a^+, then so is $\frac{1}{ax}$ and so we can pair up the solutions except when $x = \frac{1}{ax}$. However, the equation $x = \frac{1}{ax}$ has exactly one root in $\mathbb{F}_{2^m}^*$ for any non-zero a, namely $x = \sqrt{1/a}$. Hence we have an odd number of solutions to E_a^+.

Since the mapping $x \mapsto x^{-1}$ is a bijection on $\mathbb{F}_{2^m}^*$, it follows immediately from Corollary 1.1.3 that $N^+(0)$ is odd. □

The following theorem holds for both even and odd m.

Theorem 2.2.10. [19] *Let $m \geq 3$. The set of $K(a)$, $a \in \mathbb{F}_{2^m}^*$ is the set of all the integers congruent to $-1 \pmod 4$ in the range*

$$[-2^{m/2+1}, 2^{m/2+1}].$$

Proof. For every odd s in the interval $[-2^{m/2+1}, 2^{m/2+1}]$ there is an ordinary elliptic curve C_s with $\#C_s = 2^m + 1 + s$ [18]. Corollary 2.2.5 implies that C_s can be transformed into one of $\mathcal{K}l_a^{\pm}$ and so $s = \pm K(a)$ by Proposition 2.2.8. We know from Proposition 2.2.9 that $N^+(a)$ is odd. Then by equation (2.5)

$$K(a) = 2N^+(a) - 2^m + 1 \equiv -1 \pmod 4.$$

Therefore if $s \equiv -1 \pmod 4$, we must have $s = K(a)$, otherwise if $s \equiv 1 \pmod 4$, then $s = -K(a)$. □

2.2.2 Kloosterman sums divisible by 3

We will refer to results of Charpin, Helleseth and Zinoviev on the divisibility modulo 24 of Kloosterman sums [7]. For that reason we need to point out that the Kloosterman sum $\mathcal{K}(a)$ as defined in [7] relates to our Definition 2.2.1 by $\mathcal{K}(a) = K(a) + 1$ for all $a \in \mathbb{F}_{2^m}$. Also notice that in [7] the authors only consider the cases of odd $m \geq 5$, since $m = 3$ does not suit their purposes. However, all of the following statements hold for $m \geq 3$, m odd.

Let $t \in \mathbb{F}_{2^m}$, $t \notin \{0, 1\}$, and consider the following elliptic curve over $\mathbb{F}_{2^m}$:

$$\mathcal{E}_t : \quad y^2 + xy = x^3 + a_2 x^2 + (t^8 + t^6), \tag{2.6}$$

where

$$a_2 = s^2 + s + t,$$

with $s \in \mathbb{F}_{2^m}$ chosen in such a way that

$$a_2 = \mathrm{Tr}(t).$$

Let $\#\mathcal{E}_t$ denote the number of points on $\mathcal{E}_t$ over $\mathbb{F}_{2^m}$. In the next chapter we will show that $\mathcal{E}_t$ arises naturally in the problem of counting coset leaders for the Melas code. Before coming to that, let us first note that $\mathcal{E}_t$ can be used to give a new proof of the characterization of those $a \in \mathbb{F}_{2^m}$ for which $3|K(a)$. This strengthens the first part of Theorem 5 of [16], where only the right-to-left implication of the following theorem is stated:

Theorem 2.2.11. *Let $m \geq 3$ be odd, and let a be a nonzero element of $\mathbb{F}_{2^m}$. Then $K(a)$ is divisible by 3 if and only if $a = t^4 + t^3$ for some $t \in \mathbb{F}_{2^m}$.*

Proof. ($\Leftarrow$) The discriminant of $\mathcal{E}_t$ is

$$\Delta = t^8 + t^6 = t^6(t + 1)^2,$$

so $\mathcal{E}_t$ is non-singular since $t \notin \{0, 1\}$. It is not hard to verify that the point $P = (t^2 + t : t^4 + t^3 + s(t^2 + t) : 1)$ lies on $\mathcal{E}_t$. Moreover (see Appendix C),

$$\begin{aligned} 2P &= (t^2 : t^4 + t^3 + st^2 : 1), \\ 3P &= 2P + P = (0 : t^4 + t^3 : 1). \end{aligned}$$

Since the affine x-coordinate of $3P$ is zero, and $a_3 = 0$ in the generalized Weierstrass equation of the curve, we have $3P = -3P$ and hence $6P = 3P + 3P = \mathcal{O}$. Therefore the order of P in

the group of $\mathcal{E}_t$ is equal to 6. By Lagrange's Theorem the order of a group element divides the order of the group and hence 6 divides $\#\mathcal{E}_t$. Since $(t^4+t^3)^2 = t^8+t^6$, we deduce from Proposition 2.2.8 and the proof of Corollary 2.2.5 that

$$\#\mathcal{E}_t = \begin{cases} 2^m + 1 + K(t^4+t^3) & \text{if } \mathrm{Tr}(t) = 0, \\ 2^m + 1 - K(t^4+t^3) & \text{if } \mathrm{Tr}(t) = 1. \end{cases} \tag{2.7}$$

Since $3|(2^m+1)$ for odd m, it follows that $3|K(t^4+t^3)$.

($\Rightarrow$) Assume that $3|K(a)$, then by Theorem 3 in [7] $\mathrm{Tr}(a^{1/3}) = 0$. Now apply Theorem 1.1.6 with $k = 2$. □

Remark 2.2.12. A more combinatorial proof of the fact that 6 divides $\#\mathcal{E}_t$ arises from the proof of Theorem 3.2.3 in the next chapter, in which we find that $\#\mathcal{E}_t - 6$ is the number of solutions to a certain system of equations over $\mathbb{F}_{2^m}^*$, and this number is easily seen to be divisible by 6.

Chapter 3

Melas codes

In this chapter we establish the exact spectrum of the number of coset leaders for cosets of weight 3 of the binary Melas code. In Section 3.2 we transform this problem to counting points on a certain parametrized family of elliptic curves. Similar techniques have been used before, see for example [29]. We provide a connection to Theorem 2.2.11 of Chapter 2 thus giving a combinatorial interpretation (and a second proof) of it. In Section 3.3 we use the results of the previous section to construct caps with many free pairs of points in PG$(n, 2)$, that have recently proved useful in statistical experimental design.

3.1 Definitions and preparatory facts

Definition 3.1.1 (Cyclic Code). *A code C is called cyclic if it is linear and any cyclic shift of a codeword is also a codeword. Equivalently, a cyclic code of block length n over a field $\mathbb{F}_q$ is an ideal in $\mathbb{F}_q[x]/(x^n - 1)$.*

Every ideal in $\mathbb{F}_q[x]/(x^n - 1)$ is a principal ideal, that is it consists of all multiples of a fixed polynomial $g(x)$ by elements of $\mathbb{F}_q[x]/(x^n - 1)$. The polynomial $g(x)$ is then called a *generator polynomial* and therefore every cyclic code of length n has a generator polynomial.

Definition 3.1.2 (Minimal Polynomial). *The minimal polynomial of β over the field $\mathbb{F}_{p^m}$ is a monic polynomial $m(x)$ of the lowest degree with coefficients in $\mathbb{F}_{p^m}$ with β as a root.*

Definition 3.1.3 (Melas Code). *Let α be a primitive element of $\mathbb{F}_{2^m}$. The Melas code $\mathcal{M}_m$ is the binary cyclic code of length $n = 2^m - 1$ with generator polynomial $m_+(x)m_-(x)$, where $m_+(x)$ and $m_-(x)$ are the minimal polynomials of α and α^{-1} respectively.*

The redundancy of $\mathcal{M}_m$ is $2m$. It is known [6, p. 1021] that the minimum distance of $\mathcal{M}_m$ is five when m is odd and three when m is even. Since we are primarily motivated by the application described in Section 3.3, we only consider the case when m is odd. Consider $\mathbb{F}_{2^m}$ as an m-dimensional vector space over $\mathbb{F}_2$ and view α^s and α^{-s} as m-dimensional binary column vectors. Then by Theorem 5.4 of [6] the standard parity check matrix of the Melas code is

$$\mathcal{H}_{\mathcal{M}} = \begin{pmatrix} \alpha & \dots & \alpha^i & \dots & \alpha^{2^m-1} \\ \alpha^{-1} & \dots & \alpha^{-i} & \dots & \alpha^{-(2^m-1)} \end{pmatrix}.$$

That is, $c \in \mathcal{M}_m$ if and only if $\mathcal{H}_{\mathcal{M}} c^T = \mathbf{0}$.

3.2 Counting coset leaders for the Melas code

We assume that $\mathcal{H}_{\mathcal{M}}$ as defined in the previous section is used to produce syndromes and we wish to study the number of coset leaders for a coset D of $\mathcal{M}_m$ of weight 3 corresponding to a given syndrome. As discussed in Chapter 1, there is a one-to-one correspondence between cosets and syndromes. The number of coset leaders is the number of different error patterns of weight 3 resulting in the same syndrome and we would like to minimize this quantity as will be explained in the next section.

Let $d = (d_1, \dots, d_{2^m-1})$ be a coset leader of a coset D of $\mathcal{M}_m$ of weight 3 corresponding to a given syndrome $(a, b)^T \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Then

$$\mathcal{H}_{\mathcal{M}} d^T = \begin{pmatrix} \alpha & \dots & \alpha^i & \dots & \alpha^{2^m-1} \\ \alpha^{-1} & \dots & \alpha^{-i} & \dots & \alpha^{-(2^m-1)} \end{pmatrix} d^T = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Let the three non-zero coordinates of d be in positions i, j and k, $0 < i < j < k \leq 2^m - 1$. We then have the following system:

$$\begin{cases} \alpha^i + \alpha^j + \alpha^k = a, \\ \alpha^{-i} + \alpha^{-j} + \alpha^{-k} = b. \end{cases}$$

If $a \neq 0$, then we may assume without loss of generality that $a = 1$. We are then led to counting the number of solutions to the following system of equations over $\mathbb{F}_{2^m}^*$:

$$\begin{cases} u + v + w = 1, \\ u^{-1} + v^{-1} + w^{-1} = r, \end{cases} \tag{3.1}$$

where $r \in \mathbb{F}_{2^m}$ is a fixed constant.

Definition 3.2.1. *Let $S(r)$ denote the total number of solutions (ordered triples (u, v, w)) to (3.1) when r is the right-hand side of the second equation in (3.1).*

Let us first consider the general case when $r \notin \{0, 1\}$. The special cases $a = 0$ or $r = 0, 1$ will be treated separately at the end of this section.

Lemma 3.2.2. *For each $r \notin \{0, 1\}$, 6 divides $S(r)$.*

Proof. Suppose that in (3.1) two variables are equal, without loss of generality let $u = v$. Then (3.1) becomes:

$$\begin{cases} w = 1, \\ w^{-1} = r, \end{cases}$$

which has no solutions under the assumption $r \neq 1$. Hence the assumption $r \neq 1$ forces u, v, w to be distinct in any solution (u, v, w) to (3.1). Thus $S(r)$ is divisible by $3! = 6$. □

Theorem 3.2.3. *Let $m \geq 3$ be odd and let $r \in \mathbb{F}_{2^m} \setminus \{0, 1\}$. The number of solutions $(u, v, w) \in (\mathbb{F}_{2^m}^*)^3$ of (3.1) is an integer T such that*

- $T \in [2^m + 1 - 2^{m/2+1} - 6, 2^m + 1 + 2^{m/2+1} - 6]$
- *6 divides T.*

Conversely, each T satisfying these two conditions occurs as the number of solutions for at least one $r \in \mathbb{F}_{2^m} \setminus \{0, 1\}$.

Proof. Please see Appendix A for all the upcoming calculations.

Without loss of generality we choose to eliminate w from the first equation in (3.1) and substitute the result into the second equation; we then clear the denominators. So far we have:

$$ru^2v + ruv^2 + u^2 + v^2 + u + v + uv(r + 1) = 0.$$

After introducing the homogenization variable Z by setting $u = U/Z$, $v = V/Z$ and clearing the denominators we arrive at the equation

$$rU^2V + rUV^2 + UZ^2 + VZ^2 + U^2Z + V^2Z + UVZ(r + 1) = 0. \tag{3.2}$$

We shall first transform (3.2) into Weierstrass form by setting

$$\begin{cases} U = \dfrac{r+1}{r^4}x, \\ V = \dfrac{(r+1)^2}{r^6}y, \\ Z = \dfrac{r+1}{r^3}x + rz. \end{cases} \tag{3.3}$$

Then, to make the computations easier, let

$$r = 1 + \frac{1}{t}. \tag{3.4}$$

Note that the assumption $r \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ implies $t \in \mathbb{F}_{2^m} \setminus \{0, 1\}$. After dehomogenizing and scaling to make the coefficient of y^2 to be equal to one we get an elliptic curve in standard Weierstrass form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_1 = \dfrac{(t+1)^2}{t^2}$, $a_3 = \dfrac{(t+1)^7}{t^5}$, $a_2 = \dfrac{(t+1)^4}{t^2}$, $a_4 = \dfrac{(t+1)^9}{t^6}$ and $a_6 = 0$ (please refer to Appendix D.1 to see how this substitution was obtained).

Next we apply the substitutions that Lachaud and Wolfmann used to obtain their canonical form of elliptic curves as given in (2.4). Combining (3.3) and (2.4) we get:

$$\begin{cases} U = \dfrac{1}{t}x + (t+1)z, \\ V = \dfrac{1}{t^2}(y + sx) + (t^2 + t)z, \\ Z = \dfrac{t+1}{t^2}x + (t+1)z. \end{cases} \tag{3.5}$$

From now on we will denote by $\mathcal{E}_t$ the elliptic curve obtained by applying the substitution (3.5) to the equation (3.2):

$$\mathcal{E}_t : \quad y^2z + xyz = x^3 + a_2x^2z + (t^8 + t^6)z^3,$$

or, after dehomogenization (set $z = 1$),

$$y^2 + xy = x^3 + a_2x^2 + (t^8 + t^6), \tag{3.6}$$

where

$$a_2 = s^2 + s + t.$$

We will now introduce the specific choice $\tau = 1$ in Theorem 2.2.4. Recall that $\mathrm{Tr}(1) = 1$ since m is odd and thus τ satisfies the condition of Theorem 2.2.4. We then fix s such that in (3.6) we have

$$a_2 = \mathrm{Tr}(t).$$

Note that, with this choice of s, the equation (3.6) is precisely the equation (2.6) of the curve $\mathcal{E}_t$ in Chapter 2.

First, let us consider the points on $\mathcal{E}_t$ that do *not* correspond to a solution of (3.1) (please see Appendix A.2).

The points on $\mathcal{E}_t$ are $(x : y : 1)$ where x, y satisfy equation (3.6) together with the point at infinity $\mathcal{O} = (0 : 1 : 0)$. There are three types of points that we need to consider:

- point at infinity;
- points that correspond to (u, v, w) being a permutation of $(0, 0, 1)$ (since we count triples $(u, v, w) \in (\mathbb{F}_{2^m}^*)^3$);
- points that lead to $Z = 0$.

The point $\mathcal{O}$ leads to $U = Z = 0$, and hence it does not correspond to a solution of (3.1). It remains to consider the affine points of $\mathcal{E}_t$. Thus from now on we will consider the substitution (3.5) in its dehomogenized form, meaning that we set $z = 1$.

Next consider the affine points on $\mathcal{E}_t$ that lead to $Z = 0$ and hence do not give a solution to (3.1). From (3.5) we see that in this case $x = t^2$. Substituting this into (3.6) results in

$$\begin{cases} y^2 + t^2 y = t^8 & \text{if } \mathrm{Tr}(t) = 0, \\ y^2 + t^2 y = t^8 + t^4 & \text{if } \mathrm{Tr}(t) = 1. \end{cases} \tag{3.7}$$

Viewing (3.7) as quadratic equations in y, from Lemma 1.1.4 we obtain:

$$\delta = \begin{cases} t^4 & \text{if } \mathrm{Tr}(t) = 0, \\ t^4 + 1 & \text{if } \mathrm{Tr}(t) = 1. \end{cases}$$

Recall that by Lemma 1.1.1 $\mathrm{Tr}(a^{2^i}) = \mathrm{Tr}(a)$ for all $a \in \mathbb{F}_{2^m}$, so $\mathrm{Tr}(t) = 0$ implies $\mathrm{Tr}(t^4) = 0$ and $\mathrm{Tr}(t) = 1$ implies $\mathrm{Tr}(t^4 + 1) = 0$. Hence by Lemma 1.1.4 both equations of (3.7) will have 2 solutions each in $\mathbb{F}_{2^m}$ and so for each $t \notin \{0, 1\}$ there are exactly 2 affine points on $\mathcal{E}_t$ that correspond to $Z = 0$.

Consider the ideals I_i for $i = 0, 1$ in $\mathbb{F}_{2^m}[x, y, s, t, U, V, Z]$ generated by the polynomials corresponding to the equations (3.5) and (3.6), where to each equation $A = B$ corresponds the polynomial $A - B$ with denominators cleared:

$$I_i = \langle tU + x + t(t+1), t^2V + (y + sx) + t^2(t^2 + t), t^2Z + (t+1)x + t^2(t+1), \\ y^2 + xy + x^3 + (s^2 + s + t)x^2 + t^8 + t^6, g_i(s,t)\rangle,$$

where $g_0(s,t) = s^2 + s + t$ and $g_1(s,t) = s^2 + s + t + 1$ depending on the trace of t.

To explicitly find the y-coordinates of the two points that make the homogenization variable $Z = 0$, first notice that if $x = t^2$, then (3.5) implies $U = 1$. We now only need to compute Gröbner bases $G_{1,i}$ for I_i with $Z = 0$, $U = 1$ and $x = t^2$ with lexicographic ordering $y > s > t > V$. We obtain:

$$G_{1,i} = \{Vt^4(V+1), y + t^4 + t^3 + t^2V + st^2, g_i(s,t)\}.$$

The first polynomial in $G_{1,i}$ implies $V = 0$ or $V = 1$ and substituting it back in we obtain $y = t^2(t^2 + t + s)$ and $y = t^2(t^2 + t + s + 1)$, respectively.

The other case when a point on $\mathcal{E}_t$ does not yield a solution to (3.1) is when one of u, v, w is equal to 0, because then its inverse does not exist. Either u or v equal to 0 lead to U or V being 0, whereas $w = 0$ implies $u = v + 1$ and so $U = V + Z$. Let us now determine the affine points on $\mathcal{E}_t$ which lead to one of these three cases.

We will first compute Gröbner bases $G_{2,i}$ with lexicographic ordering $x > y > s > t > V > Z$ for the above ideals with $U = 0$. We get:

$$G_{2,i} = \{Vt(V+Z), t(Zt + t + 1), y + t^4 + t^3 + t^2V + st^2 + st, x + t^2 + t, g_i(s,t)\}.$$

Therefore $U = 0$ implies that either $V = 0$ or $V = Z$ and in both cases $x = t^2 + t$. Next, let $G_{3,i}$ denote Gröbner bases for I_i together with $V = 0$ and lexicographic ordering $x > y > s > t > U > Z$. Then both $G_{3,i}$ contain the polynomial

$$t(U+1)^4U(U+Z).$$

Therefore $V = 0$ implies either $U = 0$, $U = Z$ or $U = 1$. However, by (3.5) $U = 1$ leads to $Z = 0$. Finally, compute Gröbner bases $G_{4,i}$ with lexicographic ordering $x > y > s > t > V > Z$ for the ideals I_i with $U = V + Z$. This time, both bases contain the polynomial

$$tV(V+Z)(V+Z+1)^4.$$

Hence for $U = V + Z$ we have that $V = 0$ or $V = Z$ or $V = Z + 1$. Notice that $U = V + Z$ and $V = Z + 1$ together imply $U = 1$ and so $Z = 0$.

We have just shown the following implications for each affine point on $\mathcal{E}_t$ ($\wedge$ and $\vee$ are the logical "and" and the logical "or", respectively:

$$\begin{aligned} U = 0 &\Rightarrow (V = 0) \vee (V = Z) \\ V = 0 &\Rightarrow (U = 0) \vee (U = Z) \\ U = V + Z &\Rightarrow (V = 0) \vee (V = Z) \end{aligned}$$

Consequently, it is sufficient to consider the three cases $(U = 0) \wedge (V = 0)$, $(U = 0) \wedge (V = Z)$ and $(U = Z) \wedge (V = 0)$. Again by computing Gröbner bases with respect to some obvious lexicographic monomial orderings we see that to each case there corresponds exactly one affine point on $\mathcal{E}_t$:

Condition	Affine point on $\mathcal{E}_t$
$(U = 0) \wedge (V = 0)$	$(t^2 + t : t(t+1)(t^2+s) : 1)$
$(U = 0) \wedge (V = Z)$	$(t^2 + t : t(t+1)(t^2+s+1) : 1)$
$(U = Z) \wedge (V = 0)$	$(0 : t^3(t+1) : 1)$

We therefore summarize that for each $t \notin \{0, 1\}$ there are precisely 6 points on $\mathcal{E}_t$ that do not produce a solution to (3.1):

Description	**Points on $\mathcal{E}_t$**
Point at infinity $\mathcal{O}$	$(0 : 1 : 0)$
Points that make $Z = 0$	$(t^2 : t^2(t^2+t+s) : 1)$ $(t^2 : t^2(t^2+t+s+1) : 1)$
Points that correspond to (u, v, w) being a permutation of $(0, 0, 1)$	$(t^2 + t : t(t+1)(t^2+s) : 1)$ $(t^2 + t : t(t+1)(t^2+s+1) : 1)$ $(0 : t^3(t+1) : 1)$

Since $t \notin \{0, 1\}$, all six exceptional points found so far are clearly distinct.

We will now prove that for $z = 1$, the mapping $(x, y) \mapsto (u, v)$, defined by (3.5) composed with $u = U/Z$, $v = V/Z$, is injective, that is, distinct affine points on $\mathcal{E}_t$ produce distinct solutions to (3.1), if any. Let $u = u(x)$, $v = v(x, y)$ be this mapping. Towards a

contradiction assume that there are two distinct affine points (x_1, y_1) and (x_2, y_2) on $\mathcal{E}_t$ so that $(u(x_1), v(x_1, y_1)) = (u(x_2), v(x_2, y_2))$ (see Appendix A.3). Then $u(x_1) = u(x_2)$ gives

$$\frac{t^2(x_1 + x_2)}{(x_1 + t^2)(x_2 + t^2)(t + 1)} = 0,$$

and since $t \neq 0, 1$, it must be that $x_1 = x_2$. Substituting $x_1 = x_2$ into $v(x_1, y_1) = v(x_2, y_2)$ results in

$$\frac{y_1 + y_2}{(x_1 + t^2)(t + 1)} = 0,$$

which implies that $y_1 = y_2$. Since the two points on $\mathcal{E}_t$ with the x-coordinate equal to t^2 do not produce solutions to (3.1), the two values displayed above are well defined.

Recall that $S(r)$ denotes the total number of ordered triples (u, v, w) satisfying (3.1) where r is the right-hand side of the second equation in (3.1). We just proved that

$$S(r) = \#\mathcal{E}_t - 6, \tag{3.8}$$

where $\#\mathcal{E}_t$ denotes the number of points on $\mathcal{E}_t$ over $\mathbb{F}_{2^m}$ and t and r are related via (3.4).

By the Hasse Theorem [17, p. 56] and Lemma 3.2.2 equation (3.8) implies

$$\{S(r) \, : \, r \in (\mathbb{F}_{2^m} \setminus \{0, 1\})\} \subseteq [2^m + 1 - 2^{m/2+1} - 6, 2^m + 1 + 2^{m/2+1} - 6] \cap 6\mathbb{Z},$$

where $6\mathbb{Z}$ denotes the integers divisible by 6.

Now we need to show the inclusion in the other direction: for each $k \in [2^m + 1 - 2^{m/2+1}, 2^m + 1 + 2^{m/2+1}] \cap 6\mathbb{Z}$, there exists $t \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ so that $\#\mathcal{E}_t = k$. Let $k = \#\mathcal{E}_t = 2^m + 1 + s$, then $s \in [-2^{m/2+1}, 2^{m/2+1}]$. Notice that $6|k$ implies $3|s$ (because m is odd) and $s \equiv 1 \pmod 2$.

Since $(t^4 + t^3)^2 = t^8 + t^6$, it follows from Proposition 2.2.8 that

$$\#\mathcal{E}_t = \begin{cases} 2^m + 1 + K(t^4 + t^3) & \text{if } \mathrm{Tr}(t) = 0, \\ 2^m + 1 - K(t^4 + t^3) & \text{if } \mathrm{Tr}(t) = 1. \end{cases}$$

Then by Theorem 2.2.10

$$\{K(a) \, : \, a \in \mathbb{F}_{2^m}\} = \{u \, : \, u \in [-2^{m/2+1}, 2^{m/2+1}], \, u \equiv -1 \pmod 4\}.$$

Theorem 2.2.11 together with Corollary 1.1.7 imply that for each $s \in [-2^{m/2+1}, 2^{m/2+1}] \cap 3\mathbb{Z}$ such that $s \equiv -1 \pmod 4$ we can find $t \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ such that $s = K(t^4 + t^3)$ and $\mathrm{Tr}(t) = 0$. If on the other hand $s \equiv 1 \pmod 4$, then we can find $t \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ such that $-s = K(t^4 + t^3)$ and $\mathrm{Tr}(t) = 1$. In either case applying equation (2.7) then completes the second part of the proof of Theorem 3.2.3. □

Theorem 3.2.3 immediately translates to the following result for the number of coset leaders of the Melas code.

Corollary 3.2.4. *Let $m \geq 3$ be an odd integer. Let $a, b \in \mathbb{F}_{2^m}^*$, $a \neq b$. Suppose that the syndrome $(a, b)^T$ corresponds to a coset D of weight 3 of $\mathcal{M}_m$. Then the number of coset leaders of D is an integer L such that*

$$6L \in [2^m + 1 - 2^{m/2+1} - 6, 2^m + 1 + 2^{m/2+1} - 6].$$

Conversely, each such L occurs as the number of coset leaders for at least one such coset D.

Since $\#\mathcal{E}_t = S(r) + 6$ and $S(r)$ is divisible by $3! = 6$, it follows that $6|\#\mathcal{E}_t$. This gives one of several possible combinatorial interpretations of Theorem 2.2.11. Another such interpretation is the aforementioned Theorem 5 of [16], where the proof is also of a combinatorial (counting) nature. However, if one is only interested in proving $6|\#\mathcal{E}_t$ *without* considering the implications for the cosets of the Melas code, then the (probably) easiest way to achieve that is to consider the point of order 6 mentioned in the proof of Theorem 2.2.11.

The following theorem is important for the application outlined in Section 3.3.

Theorem 3.2.5. *For $S(r)$ introduced in Definition 3.2.1, let $N(k)$ denote the number of those $r \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ for which $S(r) = k$. Then for each $l \in \mathbb{N}$ we have $N(2^m - 5 + l) = N(2^m - 5 - l)$, that is, the values $N(k)$ are symmetric about $k = 2^m - 5$.*

Proof. Recall that $S(r) = \#\mathcal{E}_t - 6$, where r and t are related via (3.4). The substitution (3.4) defines a one-to-one correspondence between the values r and t on the set $\mathbb{F}_{2^m} \setminus \{0, 1\}$. Corollary 1.1.7 implies that for each $t \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ there exists a unique $u \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ such that $\{\mathrm{Tr}(t), \mathrm{Tr}(u)\} = \{0, 1\}$ and $u^4 + u^3 = t^4 + t^3$. The statement now follows from equation (2.7). □

The special cases $r = 0, 1$ not covered in Theorems 3.2.3 and 3.2.5 are of no interest for us because the number of solutions to (3.1) is too high for them (in particular, this number is greater than the average number of solutions $2^m - 5$ implied by Theorem 3.2.5) or because they do not produce cosets of weight 3.

Consider first the case when $r = 1$. Then $\mathcal{H}_{\mathcal{M}}$ contains a column of the form

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

implying that the corresponding coset of weight 1. Nonetheless, let us count the number of solutions to (3.1) in this case. As in the proof of Theorem 3.2.3 we first eliminate w from the system to get:

$$u^2 + v^2 + u^2v + uv^2 + u + v = 0, \tag{3.9}$$

or, equivalently,

$$(u + v)(u + 1)(v + 1) = 0. \tag{3.10}$$

Since both u and v must be nonzero, the first factor gives $2^m - 1$ solutions, while the other two result in another $2^m - 2$ solutions each. Therefore for $r = 1$ the number of solutions $(u, v, w) \in (\mathbb{F}_{2^m}^*)^3$ to (3.1) is $3 \cdot 2^m - 5$.

Now consider syndromes of the form $(0, a)^T$, so we are working with a different system of equations over $\mathbb{F}_{2^m}^*$:

$$\begin{cases} u + v + w = 0 \\ u^{-1} + v^{-1} + w^{-1} = a \end{cases} \tag{3.11}$$

where $a \in \mathbb{F}_{2^m}$ is a fixed constant. For the syndromes of the form $(a, 0)^T$ (i.e. corresponding to $r = 0$ in (3.1)) we simply use the substitution $(u, v, w) \mapsto (u^{-1}, v^{-1}, w^{-1})$ to get the system (3.11).

A scaling argument shows that it is enough to consider the case $a = 1$. After eliminating w from the second equation and clearing the denominators we arrive at the following equation viewed as a quadratic equation in u:

$$u^2(1 + v) + u(v + v^2) + v^2 = 0. \tag{3.12}$$

From Lemma 1.1.4 we get $\delta = 1/(1 + v)$. For $v \neq 0, 1$ (3.12) has two solutions in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}(\delta) = 0$. Now, since the mapping $v \mapsto 1/(1 + v)$ is one-to-one on the set $S := \mathbb{F}_{2^m} \setminus \{0, 1\}$, $\mathrm{Tr}(\delta) = 0$ for $2^{m-1} - 1$ elements of S and the number of solutions $(u, v, w) \in (\mathbb{F}_{2^m}^*)^3$ is $2 \cdot (2^{m-1} - 1) = 2^m - 2$.

3.3 Application to caps with free pairs

In this section we outline one particular motivation for counting coset leaders for the Melas code. Given the size of a cap and its projective dimension, our objective is to maximize the number of pairs of points in the cap that are not contained in any coplanar quadruple.

In Section 3.3.1 we explain the motivation that comes from statistical experimental design, and in Section 3.3.2 we survey the known results and present a construction that improves the known lower bound on the number of free pairs of points in binary caps for odd m.

3.3.1 Introduction and motivation

In statistical terms, a factorial design is obtained when two or more experimental factors are used and each of them has a number of possible values, known as levels. Consider a (i-level) factorial design consisting of f factors at i possible levels each. Clearly, if the number of factors increases, it becomes impractical to run all possible i^f experiments and we turn to *fractional* factorial designs, meaning that we reduce the number of experiments. The main defining property of fractional factorial designs is their resolution, which is a measure of the amount of information lost. In practice the most common fractional designs are of so-called resolution IV, since they provide a reasonable trade-off between the number of runs and the amount of information lost. The major drawback of these designs is the fact that some two-factor interactions are indistinguishable, meaning that certain pairs of factors cannot be estimated independently of each other. Therefore in the construction of experiments we would like to minimize the number of two-factor interactions that are statistically aliased, or, alternatively, maximize the number of pairs of factors that are independent.

Example 3.3.1. Suppose you wish to run an experiment consisting of 4 factors (A, B, C, and D) at two levels each (+ and −). Instead of 16 experiments, we choose to run only 8 and the following table summarizes the results (for full explanation please refer to Section 5.3.3.4 of [1]):

A	B	C	D	AB	CD	BC	Outcome
−	−	−	−	+	+	+	success
+	−	−	+	−	−	+	failure
−	+	−	+	−	−	−	failure
+	+	−	−	+	+	−	success
−	−	+	+	+	+	−	success
+	−	+	−	−	−	−	failure
−	+	+	−	−	−	+	failure
+	+	+	+	+	+	+	success

As can be seen from the table, $AB = CD$, hence these two interactions are statistically aliased and it is impossible to say which one caused the outcome. Since $AB \neq BC$, this pair of factors is independent. Notice, that although $ABC = D$, interaction of three or more factors are considered unlikely to happen in practice.

Let C be a cap in PG$(n, 2)$ as defined in Section 1.3.3.

Definition 3.3.2 (Free pair of points). *We say that $\{s, t\} \subset C$ is a free pair of points of C if $\{s, t\}$ is not contained in any coplanar quadruple of C.*

If a cap C is used as a fractional factorial design, then its points are viewed as random variables and if a set of points lies in the same plane of PG$(n, 2)$, that means that the corresponding random variables are statistically dependent. Then a free pair of points in a cap corresponds to two random variables such that any set of 4 variables containing this pair is independent. This explains why in statistics free pairs of points are called *clear two-factor interactions.* Given the cardinality of a cap and the projective dimension, it is therefore desired to maximize the number of free pairs of points in the cap by choice of a cap.

3.3.2 A construction of caps with many free pairs of points

Let H_C be a matrix whose columns are points of a cap C in PG$(r-1, 2)$ with no repeated columns. Recall that by Proposition 1.3.17 H_C defines a parity check matrix of a binary linear $[n, k, d]$-code with minimum distance at least 4. Clearly, *all* pairs of points of C are free if and only if H_C defines a code of minimum distance at least 5, since in that case there are no dependent, that is coplanar, quadruples. Thus one way of obtaining caps with a large number of free pairs is as follows: start with the parity check matrix H^* of a binary linear code of distance 5, and carefully add columns to it so that as many free pairs as possible are retained, and no dependent triples are created. First of all, notice that adding a syndrome corresponding to a coset of weight 2 would create a dependent triple and therefore destroy the cap property. If d is a newly added column and if x, y, z are three columns of $\mathcal{H}^*$ such that $x + y + z = d$, then the free pairs $\{x, y\}$, $\{x, z\}$ and $\{y, z\}$ are destroyed.

Recall the matrix from Theorem 1.3.11:

$$\mathcal{H}_f = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{2^m-2}) \end{pmatrix}. \tag{3.13}$$

The statement of the theorem implies that we can construct caps with many free pairs of points by extending parity check matrices of the form (3.13) using any APN function.

In [21] this approach was worked out for the case when H^* is the parity check matrix of the primitive double-error correcting BCH code with one particular APN function, namely $f(x) = x^3$. As in Chapter 3, the corresponding system of equations is

$$\begin{cases} u + v + w = 1, \\ u^3 + v^3 + w^3 = r, \end{cases}$$

where $r \in \mathbb{F}_{2^m}$ is a fixed constant. After eliminating w, homogenizing the equation and applying substitution (3.3), we get a supersingular elliptic curve. In [21] the previously known bounds were improved, but the right-hand side of the first equation was zero, making the counting easier.

For a cap S, let $g(S)$ denote the number of those subsets $\{x, y\} \subset S$ that are free pairs. Then for positive integers n and r such that $n \leq 2^{r-1}$, let $F(n, r)$ denote the maximum of $g(S)$ over all n-caps S in PG$(r-1, 2)$. Let n be such that $2^{\lfloor r/2 \rfloor} \leq n \leq 2 \cdot 2^{\lfloor r/2 \rfloor} - 4$.

Theorem 3.3.3. [21] *Let $n = (2^m - 1) + k$, where $m \in \{2, 3\}$ or $m \geq 6$, and let $0 \leq k < 0.234 \cdot 2^m$. Then*

$$F(n, 2m) > \binom{2^m - 1}{2} - k \cdot 2^{m-1} > \frac{n^2}{4}. \tag{3.14}$$

Since $f(x) = x^3$ is not only APN, but AB when m is odd, by Theorem 1.2.10 the corresponding system of equations has $q - 2$ solutions over $\mathbb{F}_{2^m}$ whenever $b \neq a^3$, where $q = 2^m$. On the other hand, if we take f to be the inverse function $f(x) = x^{-1}$, which for m odd is APN *but not* AB, then the matrix (3.13) becomes the parity check matrix of the Melas code. Then by Theorem 3.2.3 the number of solutions can be as low as roughly $q - 2\sqrt{q}$ compared to roughly q solutions for any AB function (Theorem 1.2.10). We skip the details, however, one can easily reproduce the proof of Theorem 3.3.3 using the inverse function to get the same result and even slightly improve the lower bound on $F(n, 2m)$ in equation (3.14) for m odd.

Observation 3.3.4. Since the distribution of the number of solutions to (3.1) has been shown to be symmetric about $q - 5$ in Theorem 3.2.5, we see that when using the parity check matrix of the Melas code with m odd, roughly one half of the choices for syndromes yield better results than can be achieved by using the primitive double-error correcting BCH code, for which the number of solutions is $q - 2$ (or higher).

Chapter 4

Ternary Kloosterman sums

In Chapter 2 we studied binary Kloosterman sums using results by Lachaud and Wolfmann [19]. The authors transformed the problem of determining the spectrum of binary Kloosterman sums into counting points on elliptic curves. Recently Moisio [25] has proved an analogous result for the ternary case. In this chapter we will use this connection to classify and count those $a \in \mathbb{F}_{3^m}$ for which $K(a) \equiv 0, 2 \pmod 4$.

4.1 Odd Kloosterman sums over $\mathbb{F}_{3^m}$

Let $\mathbb{F}_{3^m}$ be a finite field of characteristic 3, $q = 3^m$, and let $a \in \mathbb{F}_{3^m}$. Recall Definition 2.2.1. In this case $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, so that Kloosterman sums over $\mathbb{F}_{3^m}$ are defined as follows:

$$K(a) := \sum_{x \in \mathbb{F}_{3^m}^*} \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i \right)^{\mathrm{Tr}(x^{-1}+ax)} . \tag{4.1}$$

Let us first introduce some notation. Consider the following equations over $\mathbb{F}_{3^m}^*$:

$$\begin{aligned} E_0 &: \mathrm{Tr}(x^{-1} + ax) = 0, \\ E_1 &: \mathrm{Tr}(x^{-1} + ax) = 1, \\ E_{-1} &: \mathrm{Tr}(x^{-1} + ax) = -1, \end{aligned}$$

where $a \in \mathbb{F}_{3^m}$ is a fixed constant. Let $N_0(a)$, $N_1(a)$ and $N_{-1}(a)$ denote the number of solutions $x \in \mathbb{F}_{3^m}^*$ to E_0, E_1 and E_{-1} respectively.

Lemma 4.1.1. *$K(a)$ is an integer for all $a \in \mathbb{F}_{3^m}$.*

Proof. Fix an element $a \in \mathbb{F}_{3^m}$. Then each solution of E_1 contributes $-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ to the sum in $K(a)$, and each solution of E_{-1} contributes $\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)^{-1} = -\frac{1}{2}-\frac{\sqrt{3}}{2}i$. Let x be a solution to E_1, that is $\mathrm{Tr}(x^{-1}+ax)=1$. Then

$$\mathrm{Tr}((-x)^{-1}+a(-x)) = -\mathrm{Tr}(x^{-1}+ax) = -1,$$

and hence $-x$ is a solution to E_{-1}. Therefore $N_1(a) = N_{-1}(a)$ and

$$\begin{aligned} K(a) &= N_0(a) + N_1(a)\cdot\omega + N_{-1}(a)\cdot\omega^2 \\ &= N_0(a) + N_1(a)(\omega+\omega^2) \\ &= N_0(a) - N_1(a). \end{aligned}$$

□

Since $N_0(a) + N_1(a) + N_{-1}(a) = 3^m - 1$ and $N_1(a) = N_{-1}(a)$ we have:

$$N_0(a) = 3^m - 1 - 2N_1(a).$$

Hence

$$K(a) = N_0(a) - N_1(a) = 3^m - 1 - 3N_1(a). \tag{4.2}$$

Lemma 4.1.2. *Let $a \in \mathbb{F}_{3^m}$. Then $K(a) \equiv N_1(a) \pmod 2$.*

Lemma 4.1.3. *Let $a \in \mathbb{F}_{3^m}$. Then $K(a) \equiv 2 \pmod 3$.*

Both Lemma 4.1.2 and Lemma 4.1.3 follow directly from equation (4.2).

Our research on this topic was motivated by the following result:

Theorem 4.1.4. [25] *Let $c \in \mathbb{F}_{3^m}^*$ and let Φ be an elliptic curve over $\mathbb{F}_{3^m}$ defined by*

$$\Phi: \quad y^2 = x^3 + x^2 - c.$$

Then $\#\Phi = 3^m + 1 + K(c)$, where $\#\Phi$ denotes the number of $\mathbb{F}_{3^m}$-rational points on Φ.

We can now apply techniques similar to the ones in Chapter 2 to study the divisibility of ternary Kloosterman sums modulo 4.

Before we proceed, let us note that by $\sqrt{a}$ we will denote an element $x \in \mathbb{F}_{3^m}$ such that $x^2 = a$. If this equation has a solution, then it has two of them, unless $a = 0$. In all of the statements to follow it will not matter which square root is under consideration as long as it is consistent (we will arbitrarily pick one of them to be denoted by $\sqrt{a}$).

Theorem 4.1.5. *$N_1(a)$ is odd if and only if $a = 0$ or a is a square and $\mathrm{Tr}(\sqrt{a}) \neq 0$.*

Proof. First let $a \in \mathbb{F}_{3^m}^*$. Consider the mapping κ_a from $\mathbb{F}_{3^m}^*$ to itself defined by

$$\kappa_a(x) = x^{-1} + ax.$$

Then for $x, y \in \mathbb{F}_{3^m}^*$

$$\kappa_a(x) = \kappa_a(y) \iff (x-y)(a - \frac{1}{xy}) = 0 \iff y = x \quad \text{or} \quad y = \frac{1}{ax}.$$

Therefore κ_a maps x and $1/ax$ to the same element. Since $x = \dfrac{1}{ax}$ if and only if $x = \pm\sqrt{1/a}$, we have to consider two cases: $1/a$ is a non-square and $1/a$ is a square.

If $1/a$ is a non-square, then the mapping $x \mapsto x^{-1} + ax$ is two-to-one and hence $N_1(a)$ is even since if x_0 is a solution to E_1, then so is $\dfrac{1}{ax_0}$.

If $1/a$ is a non-zero square, or equivalently a is a non-zero square, then the equation $x = \dfrac{1}{ax}$ has two solutions $x_{1,2} = \pm\sqrt{1/a}$. If $x = \sqrt{1/a}$, then

$$(\sqrt{1/a})^{-1} + a(\sqrt{1/a}) = -\sqrt{a}.$$

So for $x = \sqrt{1/a}$ we have $\mathrm{Tr}(x^{-1} + ax) = 1$ if and only if $\mathrm{Tr}(-\sqrt{a}) = 1$. Similarly for $x = -\sqrt{1/a}$ we have $\mathrm{Tr}(x^{-1}+ax) = 1$ if and only if $\mathrm{Tr}(\sqrt{a}) = 1$. Therefore $\mathrm{Tr}(x^{-1}+ax) = 1$ for exactly one of $x = x_1, x_2$.

Now let $a = 0$, then the mapping $x \mapsto x^{-1}$ is one-to-one on $\mathbb{F}_{3^m}^*$. Therefore $\mathrm{Tr}(x^{-1}) = 1$ for one third of the elements $x \in \mathbb{F}_{3^m}$, implying that $N_1(0)$ is odd. □

Corollary 4.1.6. *$K(a)$ is odd for $3^{m-1} + 1$ elements $a \in \mathbb{F}_{3^m}$.*

Proof. By Corollary 1.1.3 two thirds of the elements of $\mathbb{F}_{3^m}$ have non-zero trace. Because $b^2 = (-b)^2$, those elements will yield 3^{m-1} non-zero squares. Since $K(0) = -1$, altogether $K(a)$ is odd for $3^{m-1} + 1$ elements of $\mathbb{F}_{3^m}$. □

4.2 Counting the number of solutions

Consider the following system of equations over $\mathbb{F}_{3^m}^*$:

$$\begin{cases} u + v + w = 1, \\ u^{-1} + v^{-1} + w^{-1} = \dfrac{1}{t}, \end{cases} \tag{4.3}$$

where $t \in \mathbb{F}_{3^m}^*$ is a fixed constant.

Although we will later work with this system of equations with $r = 1/t$, for now having $1/t$ in (4.3) makes the upcoming computations easier.

Definition 4.2.1. *Let $S(1/t)$ denote the total number of solutions (ordered triples (u, v, w)) to (4.3).*

Let $t \in \mathbb{F}_{3^m} \setminus \{0, 1\}$. Consider solutions to (4.3) as ordered triples $(u, v, w) \in \mathbb{F}_{3^m}^*$. Notice that we can pair up the solution (u, v, w) with the solution $(\frac{t}{u}, \frac{t}{v}, \frac{t}{w})$. We wish to see how many distinct ordered solutions there are in the set composed of all permutations of (u, v, w) and all permutations of $(\frac{t}{u}, \frac{t}{v}, \frac{t}{w})$. We will say that such a set is generated by the solution (u, v, w). In most cases there will be 12 triples in total except when $|\{u, v, w\}| < 3$ or $(\frac{t}{u}, \frac{t}{v}, \frac{t}{w})$ is a permutation of (u, v, w). We therefore have the following four cases:

1. $|\{u, v, w\}| = 1$
2. $|\{u, v, w\}| = 2$
3. $u = t/u, v = t/v, w = t/w$
4. $u = t/v, w = t/w$ up to a permutation

If $u = v = w$, then the first equation of (4.3) is not satisfied. If $u = t/u, v = t/v, w = t/w$, then $u^2 = t, v^2 = t, w^2 = t$, so that t must be a square. Since all three values cannot be the same, suppose that $u = v = \sqrt{t}, w = -\sqrt{t}$. Then either equation of (4.3) implies that $t = 1$. Therefore Cases 1 and 3 never occur. We now only need to consider the other two cases.

We will say that a set generated by the solution (u, v, w) is of type 1 if $|\{u, v, w\}| = 2$ and it is of type 2 if $u = t/v, w = t/w$. Notice that a set cannot be of type 1 and 2 simultaneously, since otherwise we must have $u^2 = t, v^2 = t, w^2 = t$. Therefore both type 1 and type 2 sets are of size 6.

Lemma 4.2.2. *Let $t \in \mathbb{F}_{3^m} \setminus \{0, 1\}$. There is exactly one set of type 1 if and only if $1 - t$ is a square in $\mathbb{F}_{3^m}$. Otherwise there are no sets of type 1.*

Proof. Without loss of generality suppose that $u = v$, then solving the first equation of (4.3) for w and substituting it back into the second one yields

$$u^2 + u + t = 0. \tag{4.4}$$

Since the characteristic of the field is not 2, we can use the standard formula for solving quadratic equations. This equation has two roots if and only if $1-t$ is a square and they are distinct, unless $t = 1$ which is excluded in the statement. Now, if u_0 is a root of equation (4.4), then the other root is t/u_0 so both of these roots generate the same set of type 1. □

Lemma 4.2.3. *Let $t \in \mathbb{F}_{3^m} \setminus \{0, 1\}$. There is one set of type 2 if and only if t is a square and exactly one of $1 \pm \sqrt{t}$ is a square. There are two sets of type 2 if and only if t is a square and both $1 \pm \sqrt{t}$ are squares. If t is not a square, then there are no sets of type 2.*

Proof. Without loss of generality assume that $u = t/v, v = t/u$ and $w^2 = t$, so that t must be a square, and $|\{u, v, w\}| = 3$.

Equation $w^2 = t$ has two solutions $w_{1,2} = \pm\sqrt{t}$. Once again, we will simply pick one of $w_{1,2}$ to be denoted by $\sqrt{t}$. If $w = \sqrt{t}$, then substituting it together with $u = t/v, v = t/u$ into (4.3) results in the following quadratic equation in u:

$$u^2 + (\sqrt{t} - 1)u + t = 0. \tag{4.5}$$

This equation has roots in $\mathbb{F}_{3^m}$ if and only if $1 + \sqrt{t}$ is a square and they are distinct, unless $t = 1$. If u_0 is a root of (4.5), then so is t/u_0 and hence both roots of (4.5) generate the same set of type 2. Similarly, if $w = -\sqrt{t}$, then the corresponding quadratic equation is

$$u^2 - (\sqrt{t} + 1)u + t = 0 \tag{4.6}$$

and it has roots in $\mathbb{F}_{3^m}$ if and only if $1 - \sqrt{t}$ is a square. Once again roots are distinct, unless $t = 1$; they are of the form u_0 and t/u_0 and so they generate the same set of type 2.

Therefore there is one set of type 2 if and only if exactly one of $1 \pm \sqrt{t}$ is a square. If both $1 \pm \sqrt{t}$ are squares, then there are two sets of type 2, one corresponding to $w = \sqrt{t}$ and the other one corresponding to $w = -\sqrt{t}$. □

Theorem 4.2.4. *Let $t \in \mathbb{F}_{3^m} \setminus \{0, 1\}$. If $1 - t$ is a square or t is a square, then $S(1/t) \equiv 6 \pmod{12}$, otherwise $S(1/t) \equiv 0 \pmod{12}$.*

Proof. We have the following four disjoint cases and we draw conclusions by repeatedly using Lemmas 4.2.2 and 4.2.3:

Case 1. $1 - t$ is a square, t is a non-square.
Since $1 - t$ is a square, there is exactly one set of type 1. Since t is a non-square, there are no sets of type 2.

Case 2. $1-t$ **is a non-square,** t **is a square.**
Since $1-t=(1-\sqrt{t})(1+\sqrt{t})$ and $1-t$ is a non-square, exactly one of $1\pm\sqrt{t}$ is a square. Therefore there is one set of type 2. There are no sets of type 1.

Case 3. $1-t$ **is a square,** t **is a square.**
Since $1-t=(1-\sqrt{t})(1+\sqrt{t})$ either both $1\pm\sqrt{t}$ are squares or they are both non-squares.

If both $1\pm\sqrt{t}$ are squares, then there are two sets of type 2. However, since $1-t$ is also a square, there is one set of type 1. Hence there are 3 distinct sets of size 6.

If both $1\pm\sqrt{t}$ are non-squares, then there are no sets of type 2, so the only set of size 6 is one set type 1.

Case 4. $1-t$ **is a non-square,** t **is a non-square.**
There are no sets of type 1 or type 2.

In the first 3 cases there was an odd number of sets of size 6 and hence $S(1/t)\equiv 6 \pmod{12}$. Otherwise $S(1/t)\equiv 0 \pmod{12}$. □

4.3 Correspondence between solutions and points on the elliptic curve

Let $\bar{\mathcal{E}}_t$ denote the following elliptic curve over $\mathbb{F}_{3^m}$:

$$\bar{\mathcal{E}}_t: \quad y^2=x^3+x^2-(t^6-t^9).$$

Theorem 4.3.1. *Let* $t\in\mathbb{F}_{3^m}\setminus\{0,1\}$. *Then*

$$\#\bar{\mathcal{E}}_t=S(1/t)+6,$$

where $\#\bar{\mathcal{E}}_t$ *denotes the number of points on* $\bar{\mathcal{E}}_t$ *over* $\mathbb{F}_{3^m}$.

Proof. Let $r=1/t$ be the right-hand side of the second equation of (4.3), so that

$$\begin{cases} u+v+w=1, \\ u^{-1}+v^{-1}+w^{-1}=r. \end{cases} \tag{4.7}$$

Then the assumption $t\in\mathbb{F}_{3^m}\setminus\{0,1\}$ implies that $r\in\mathbb{F}_{3^m}\setminus\{0,1\}$.

We eliminate w from the first equation in (4.7), substitute the result into the second equation, clear the denominators, and introduce the homogenization variable Z. We now

use the following substitution to obtain an elliptic curve in Weierstrass form (please refer to Appendix D.2 to see how this substitution was obtained):

$$\begin{cases} U = \dfrac{2}{r^2+2r}x \\ V = y \\ Z = \dfrac{2}{r+2}x + \dfrac{2}{r^2(r+2)^2}z \end{cases} \tag{4.8}$$

We get the following elliptic curve (see Appendix B.1):

$$\bar{\mathcal{E}}_r : y^2z + a_3yz^2 + a_1xyz = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{4.9}$$

where

$$\begin{cases} a_1 = \dfrac{1}{r} \\ a_2 = \dfrac{2r+2}{r^2(r+2)^2} \\ a_3 = \dfrac{1}{r^2(r+2)^2} \\ a_4 = \dfrac{1}{r^3(r+2)^3} \\ a_6 = 0. \end{cases} \tag{4.10}$$

First of all let us determine the points on $\bar{\mathcal{E}}_r$ that do *not* correspond to a solution of (4.7).

The discriminant of $\bar{\mathcal{E}}_r$ is $\Delta = \dfrac{1}{r^9(r+2)^9}$, so the curve is non-singular except for $r = 0, 1$, which are excluded in the assumption. We will now find the exact number of the points on $\bar{\mathcal{E}}_r$ that do not correspond to a solution of (4.7).

The first candidate is the point at infinity $\mathcal{O} = (0 : 1 : 0)$, which leads to $U = Z = 0$ and hence does not correspond to a solution of (4.7). From now on we will only deal with affine points on $\bar{\mathcal{E}}_r$, and so will consider substitution (4.8) in its dehomogenized form with $z = 1$.

The other cases when a point on $\bar{\mathcal{E}}_r$ does not correspond to a solution of (4.7) is when $Z = 0$, or when one of u, v or w is equal to zero, which is equivalent to $U = 0$, $V = 0$ and $Z = U + V$. Consider the ideal I in $\mathbb{F}_{3^m}[x, y, r, U, V, Z]$ generated by the polynomials corresponding to the equations (4.8,4.9), where to each equation $A = B$ corresponds the polynomial $A - B$ with denominators cleared. Since the polynomials in I have coefficients in $\mathbb{F}_3$, and the Buchberger algorithm preserves this property, we can consider I to be an ideal in $\mathbb{F}_3[x, y, r, U, V, Z]$ and compute the corresponding Gröbner basis over $\mathbb{F}_3$.

First compute the Gröbner basis G_1 for the above ideal with $Z = 0$ with lexicographical ordering $x > y > r > U > V$. It contains the polynomial

$$V(U + V),$$

so $Z = 0$ implies $V = 0$ or $U = -V$. In the similar fashion we compute all other corresponding Gröbner bases with respect to some obvious lexicographical ordering. We find the following implications (see Appendix B.2):

$$\begin{aligned} Z = 0 &\Rightarrow (V = 0) \vee (U = -V) \\ U = 0 &\Rightarrow (V = 0) \vee (Z = V) \\ V = 0 &\Rightarrow (U = 0) \vee (Z = 0) \vee (U = Z) \\ Z = U + V &\Rightarrow (U = 0) \vee (V = 0) \vee (U = -V) \end{aligned}$$

Consequently, it is sufficient to consider the five cases $(U = 0) \wedge (V = 0)$, $(V = 0) \wedge (Z = 0)$, $(U = 0) \wedge (V = Z)$, $(V = 0) \wedge (U = Z)$, and $(Z = 0) \wedge (U = -V)$. By computing Gröbner bases (see Appendix B.2) we find that there are exactly 5 affine points on $\bar{\mathcal{E}}_r$ that do not correspond to a solution of (4.7):

Condition	Affine point on $\bar{\mathcal{E}}_r$
$(U = 0) \wedge (V = 0)$	$(0 : 0 : 1)$
$(V = 0) \wedge (Z = 0)$	$\left(\frac{2}{r^2(r+2)} : 0 : 1\right)$
$(U = 0) \wedge (V = Z)$	$\left(0 : \frac{2}{r^2(r+2)^2} : 1\right)$
$(V = 0) \wedge (U = Z)$	$\left(\frac{2}{r(r+2)^2} : 0 : 1\right)$
$(Z = 0) \wedge (U = -V)$	$\left(\frac{2}{r^2(r+2)} : \frac{2}{r^3(r+2)^2} : 1\right)$

Notice that all the points in the table above are distinct for $r \neq 0, 1$.

We now only need to prove that for $z = 1$, the mapping $(x, y) \mapsto (u, v)$, defined by (4.8) composed with $u = U/Z$, $v = V/Z$, is injective, that is, distinct affine points on $\bar{\mathcal{E}}_r$ produce distinct solutions to (4.7), if any. Let $u = u(x, y)$, $v = v(x, y)$ be this mapping. Towards a contradiction assume that there are two distinct affine points (x_1, y_1) and (x_2, y_2) on $\bar{\mathcal{E}}_r$ so that $(u(x_1, y_1), v(x_1, y_1)) = (u(x_2, y_2), v(x_2, y_2))$. By computing the Gröbner basis

containing all of the above conditions together with the fact that $Z(x_1, y_1)$ and $Z(x_2, y_2)$ (according to (4.8)) cannot be zero, we get $x_1 = x_2$ and $y_1 = y_2$ (see Appendix B.3).

Therefore there are 6 points on $\bar{\mathcal{E}}_r$ that do not correspond to a solution of (4.7): 5 affine points summarized in the table above and the point at infinity. We have just proved that $S(r) = \#\bar{\mathcal{E}}_r - 6$.

Given the curve $\bar{\mathcal{E}}_r$, we will now apply the following substitution (see Appendix B.4):

$$\begin{cases} r = \dfrac{1}{t} \\ x = \dfrac{t^2}{(t+2)^2}x + \dfrac{t^3(t+1)}{t+2} \\ y = \dfrac{2t^3}{(t+2)^3}y + tx + \dfrac{t^4}{(t+2)^2} \end{cases} \tag{4.11}$$

to get:

$$\bar{\mathcal{E}}_t : \quad y^2 = x^3 + x^2 - (t^6 - t^9). \tag{4.12}$$

The curves $\bar{\mathcal{E}}_r$ and $\bar{\mathcal{E}}_t$ are isomorphic by Theorem 2.1.4, and therefore $\#\bar{\mathcal{E}}_r = \#\bar{\mathcal{E}}_t$, so $S(1/t) = \#\bar{\mathcal{E}}_t - 6$. □

4.4 Kloosterman sums modulo 4

Proposition 4.4.1. *Let $t \in \mathbb{F}_{3^m} \setminus \{0, 1\}$ and let $a = t^2 - t^3$. We have the following:*

- *If $1 - t$ is a square or t is a square, then $K(a) \equiv 2m + 2 \pmod 4$, i.e. $K(a) \equiv 0 \pmod 4$ for odd m and $K(a) \equiv 2 \pmod 4$ for even m;*
- *If both t and $1 - t$ are non-squares, then $K(a) \equiv 2m \pmod 4$, i.e. $K(a) \equiv 2 \pmod 4$ for odd m and $K(a) \equiv 0 \pmod 4$ for even m.*

Proof. Recall the elliptic curve $\bar{\mathcal{E}}_t$ and system (4.3). Theorem 4.3.1 together with Theorem 4.2.4 imply that if at least one of t and $1 - t$ is a square, then $S(1/t) \equiv 6 \pmod{12}$ and so $\#\bar{\mathcal{E}}_t \equiv 0 \pmod{12}$. Otherwise $S(1/t) \equiv 0 \pmod{12}$ and $\#\bar{\mathcal{E}}_t \equiv 6 \pmod{12}$. By Theorem 4.1.4 we can express the number of points on $\#\bar{\mathcal{E}}_t$ as follows:

$$\#\bar{\mathcal{E}}_t = 3^m + 1 + K(t^6 - t^9) = 3^m + 1 + K(t^2 - t^3),$$

since $K(a) = K(a^3)$ by Lemma 2.2.2.

Since $3^m + 1 \equiv 0 \pmod 4$ for m odd and $2 \pmod 4$ for m even, the result now follows.

□

Lemma 4.4.2. [17] *Let $f(x) = x^3 - bx - c$ be a polynomial of degree 3 over $\mathbb{F}_{3^m}$. Then $f(x)$ has zero, one or three roots in $\mathbb{F}_{3^m}$. If b is a non-zero square in $\mathbb{F}_{3^m}$, such that $b = s^2$ for some $s \in \mathbb{F}_{3^m}$, then $f(x)$ has three roots in $\mathbb{F}_{3^m}$ when $\mathrm{Tr}(c/s^3) = 0$ and no roots in $\mathbb{F}_{3^m}$ if $\mathrm{Tr}(c/s^3) \neq 0$. If b is a non-square, then $f(x)$ has exactly one root in $\mathbb{F}_{3^m}$.*

Theorem 4.4.3. *Let $m \geq 3$ and let*

$$A_1 = \{a \in \mathbb{F}_{3^m} | a = 0 \text{ or } a \text{ is a square and } \mathrm{Tr}(\sqrt{a}) \neq 0\},$$

$$A_2 = \{a \in \mathbb{F}_{3^m} | a = t^2 - t^3 \text{ for some } t \in \mathbb{F}_{3^m} \setminus \{0,1\}, \ t \text{ or } 1-t \text{ is a square}\},$$

$$A_3 = \{a \in \mathbb{F}_{3^m} | a = t^2 - t^3 \text{ for some } t \in \mathbb{F}_{3^m} \setminus \{0,1\}, \text{ both } t \text{ and } 1-t \text{ are non-squares}\}.$$

Then the sets A_1, A_2 and A_3 partition $\mathbb{F}_{3^m}$.

Proof. Consider the cubic polynomial $f(t) = t^3 - t^2 + a$. For $a \neq 0$, $f(t)$ has no zero roots and $f(t^{-1}) = \frac{a}{t^3}\bar{f}(t)$, where

$$\bar{f}(t) = t^3 - \frac{1}{a}t - \frac{1}{a}.$$

By Lemma 4.4.2 the cubic polynomial $\bar{f}(t)$, and consequently $f(t)$, has no roots in $\mathbb{F}_{3^m}$ if and only if $1/a$ is a square and $\mathrm{Tr}(\sqrt{a}) \neq 0$. Therefore $\mathbb{F}_{3^m} \setminus A_1$ consists of those elements $a \in \mathbb{F}_{3^m}$ for which $f(t)$ has at least one root, or equivalently, $a = t^2 - t^3$ for some $t \in \mathbb{F}_{3^m} \setminus \{0,1\}$. Hence A_1 is disjoint from both A_2 and A_3 and $A_2 \cup A_3 = \mathbb{F}_{3^m} \setminus A_1$. It only remains to see that A_2 and A_3 are disjoint. Choose $a \in A_3$. Then $a = t^2 - t^3 = t^2(1-t)$, $t \notin \{0,1\}$, $1-t$ is a non-square and so a is a non-square. Lemma 4.4.2 implies that $f(t)$ has exactly one root and hence this representation of a is unique. Therefore a cannot be an element of A_2 by the condition on t.

□

Corollary 4.4.4. *Let $m \geq 3$ and $a \in \mathbb{F}_{3^m}$. Then exactly one of the following cases occurs:*

- *$a \in A_1$ and $K(a) \equiv 1 \pmod 2$,*
- *$a \in A_2$ and $K(a) \equiv 2m+2 \pmod 4$,*
- *$a \in A_3$ and $K(a) \equiv 2m \pmod 4$.*

Having characterized those $a \in \mathbb{F}_{3^m}$ for which $K(a) \equiv 0, 2 \pmod 4$, we will now count them.

For all $t \in \mathbb{F}_{3^m}$ define the mapping $\chi : \mathbb{F}_{3^m} \mapsto \{-1, 0, 1\}$ as follows: $\chi(0) = 0$, $\chi(t) = 1$ if t is a square and $\chi(t) = -1$ if t is a non-square. This implies that χ is multiplicative, i.e. $\chi(st) = \chi(s)\chi(t)$ for all $s, t \in \mathbb{F}_{3^m}$.

Recall that $q = 3^m$.

Lemma 4.4.5. *The set* $S_q = \{t \in \mathbb{F}_{3^m} | \chi(t) = 1, \chi(1-t) = -1\}$ *is of the size* $\frac{1}{4}(q-3)$ *if* m *is odd and* $\frac{1}{4}(q-1)$ *if* m *is even.*

Proof. Consider the function $\kappa(t) : \mathbb{F}_{3^m} \mapsto \mathbb{R}$

$$\kappa(t) := \frac{1}{4}(1 + \chi(t))(1 - \chi(1-t))$$

so that for $t \in \mathbb{F}_{3^m} \setminus \{0, 1\}$ we have $\kappa(t) = 1$ if $t \in S_q$ and $\kappa(t) = 0$ if $t \notin S_q$. We have:

$$\begin{aligned}
|S_q| = \sum_{t \in \mathbb{F}_{3^m} \setminus \{0,1\}} \kappa(t) &= \sum_{t \in \mathbb{F}_{3^m} \setminus \{0,1\}} \frac{1}{4}(1 + \chi(t))(1 - \chi(1-t)) \\
&= \frac{1}{4}\left(q - 2 + 1 - 1 - \sum_{t \in \mathbb{F}_{3^m} \setminus \{0,1\}} \chi(t)\chi(t)\chi(t^{-1} - 1)\right) \\
&= \frac{1}{4}\left(q - 2 - \sum_{t \in \mathbb{F}_{3^m} \setminus \{0,1\}} \chi(t^{-1} - 1)\right) \\
&= \begin{cases} \frac{1}{4}(q-3) & \text{if } m \text{ is odd,} \\ \frac{1}{4}(q-1) & \text{if } m \text{ is even.} \end{cases}
\end{aligned}$$

□

Theorem 4.4.6. *The number of* $a \in \mathbb{F}_{3^m}^*$ *such that* $K(a) \equiv 0 \pmod 4$ *is* $\frac{1}{4}q - \frac{1}{4}$ *if* m *is even and* $\frac{5}{12}q - \frac{5}{4}$ *if* m *is odd. The number of* $a \in \mathbb{F}_{3^m}^*$ *such that* $K(a) \equiv 2 \pmod 4$ *is* $\frac{5}{12}q - \frac{3}{4}$ *if* m *is even and* $\frac{1}{4}q + \frac{1}{4}$ *if* m *is odd.*

Proof. Corollary 4.1.6 implies that $K(a)$, $a \neq 0$ is even for $\frac{2}{3}q - 1$ elements of $\mathbb{F}_{3^m}$, i.e. $|A_2| + |A_3| = \frac{2}{3}q - 1$. Hence it is enough to find the cardinality of A_2.

Recall the cubic polynomial from the proof of Theorem 4.4.3. By Lemma 4.4.2 we have the following two disjoint cases:

- $1 - t$ is a square and $f(t)$ has three distinct roots

- $1-t$ is a non-square, t is a square and $f(t)$ has exactly one root.

The number of $t \in \mathbb{F}_{3^m} \setminus \{0,1\}$ such that $1-t$ is a square is $\frac{q-1}{2} - 1 = \frac{q-3}{2}$. Since in this case $f(t)$ has three distinct roots, the number of the corresponding $a \in \mathbb{F}_{3^m}^*$ is $\frac{q-3}{2} \cdot \frac{1}{3} = \frac{q-3}{6}$. If $1-t$ is a non-square and t is a square, then by Lemma 4.4.5 the number of such $a \in \mathbb{F}_{3^m}^*$ is $\frac{1}{4}(q-1)$ if m is even and $\frac{1}{4}(q-3)$ if m is odd. Hence altogether for m even we get:

$$\frac{q-3}{6} + \frac{1}{4}(q-1) = \frac{5}{12}q - \frac{3}{4}.$$

Similarly for m odd the number of such $a \in \mathbb{F}_{3^m}^*$ is $\frac{5}{12}q - \frac{5}{4}$. Combining all the facts above we have the following table:

Parity of m	$K(a) \pmod 4$	Number of a
m is even	$0 \pmod 4$	$\frac{1}{4}q - \frac{1}{4}$
	$2 \pmod 4$	$\frac{5}{12}q - \frac{3}{4}$
m is odd	$0 \pmod 4$	$\frac{5}{12}q - \frac{5}{4}$
	$2 \pmod 4$	$\frac{1}{4}q + \frac{1}{4}$

□

4.5 New ternary quasi-perfect codes

Danev and Dodunekov recently constructed [10] a new family of ternary quasi-perfect codes with minimum distance 5 and covering radius 3. A major step in their proof of the covering radius value is showing that the system (4.3) is solvable over $\mathbb{F}_{3^m}^*$ for any $t \in \mathbb{F}_{3^m}^*$. In [10] this is done by explicitly finding one solution. By applying Theorem 4.3.1 together with the Hasse Theorem, we offer an alternative proof of the solvability of (4.3) over $\mathbb{F}_{3^m}$.

Appendix A

Maple code for the binary case

A.1 Substitution for the elliptic curve

```
maple binary-thesis
    |\^/|     Maple 11 (IBM INTEL LINUX)
._|\|   |/|_. Copyright (c) Maplesoft, a division of Waterloo Maple Inc.
 \  MAPLE  /  All rights reserved. Maple is a trademark of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.
# ========================================================
#     u  +  v  +  w    =  1
#    1/u + 1/v + 1/w   =  r
# ========================================================
> with(Groebner):
> eq:=1/u+1/v+1/w+r:
> eq:=subs(w=1+u+v,eq):
> eq:=numer(Normal(expand(eq)) mod 2):
> eq:=numer(Normal(expand(subs({u=U/Z, v=V/Z}, eq))) mod 2);
           2     2       2     2                          2     2
    eq := V  Z + U  Z + V Z  + U Z  + V U Z + r V U Z + r V U  + r V  U

> sb:= { U=(r+1)/r^4*x, V=(r+1)^2/r^6*y, Z=(r+1)/r^3*x+r*z }:
> fact:= f -> (Factor(numer(f)) mod 2)/(Factor(denom(f)) mod 2);
```

```
# ========================================================
# Weierstrass form
# ========================================================
> g := subs( sb  , eq) mod 2:  g := subs( r=1+1/t  , g) mod 2:
> g:=subs( z=1  , g) mod 2:
> c:=Normal(coeff(coeff(g,y,2),x,0)) mod 2:
> g:= Normal(expand(g/c)) mod 2:
> Normal(coeff(coeff(g,y,0),x,3)) mod 2;
                                    1

> Normal(coeff(coeff(g,y,2),x,0)) mod 2;
                                    1

> a1:=Normal(coeff(coeff(g,y,1),x,1)) mod 2: fact(%);
                                      2
                                 (t + 1)
                                 --------
                                     2
                                    t

> a3:=Normal(coeff(coeff(g,y,1),x,0)) mod 2: fact(%);
                                      7
                                 (t + 1)
                                 --------
                                     5
                                    t

> a2:=Normal(coeff(coeff(g,y,0),x,2)) mod 2: fact(%);
                                      4
                                 (t + 1)
                                 --------
                                     2
                                    t
```

```
> a4:=Normal(coeff(coeff(g,y,0),x,1)) mod 2: fact(%);
                                        9
                                   (t + 1)
                                   --------
                                       6
                                      t

> a6:=Normal(coeff(coeff(g,y,0),x,0)) mod 2;
                                   a6 := 0

# ========================================================
# Lauchaud-Wolfmann substitution
# ========================================================
> g:= expand(subs( x=a1^2*x+a3/a1, g)) mod 2:
> g:= expand(subs( y=a1^3*(y+s*x)+(a1^2*a4+a3^2)/a1^3, g)) mod 2:
> c:=Normal(coeff(coeff(g,y,0),x,3)) mod 2:
> g:= Normal(expand(g/c)) mod 2;
                  2  2      2    3      2          8    6    2
           g := s  x  + s x  + x  + t x  + y x + t  + t  + y

> Normal(coeff(coeff(g,y,0),x,3)) mod 2;
                                      1

> Normal(coeff(coeff(g,y,2),x,0)) mod 2;
                                      1

> a1:=Normal(coeff(coeff(g,y,1),x,1)) mod 2;
                                   a1 := 1

> a3:=Normal(coeff(coeff(g,y,1),x,0)) mod 2;
                                   a3 := 0
```

```
> a2:=Normal(coeff(coeff(g,y,0),x,2)) mod 2;
                                    2
                           a2 := s  + s + t

> a2s:=Normal(coeff(coeff(coeff(g,y,0),x,2),s,0)) mod 2;
                                a2s := t

> a4:=Normal(coeff(coeff(g,y,0),x,1)) mod 2;
                                 a4 := 0

> a6:=Normal(coeff(coeff(g,y,0),x,0)) mod 2;
                                     8    6
                              a6 := t  + t

# ============================================================
# check combined substitution
# ============================================================
> sb:={U=1/t*x+(t+1)*z,V=1/t^2*(y+s*x)+(t^2+t)*z,Z=(t+1)/t^2*x+(t+1)*z}:
> Et := subs( sb   , eq) mod 2:
> c:=Normal(coeff(coeff(Et,y,0),x,3)) mod 2:
> gh := Normal(expand(Et/c)) mod 2:
##Dehomogenize
> Et := subs( z=1   , gh) mod 2:
> Et:=collect(Et,x^2);
                    3     2           2          8    6    2
            Et := x  + (s  + s + t) x  + y x + t  + t  + y

> Normal(coeff(coeff(Et,y,0),x,3)) mod 2;
                                     1

> Normal(coeff(coeff(Et,y,2),x,0)) mod 2;
                                     1
```

```
> a1:=Normal(coeff(coeff(Et,y,1),x,1)) mod 2;
                                  a1 := 1

> a3:=Normal(coeff(coeff(Et,y,1),x,0)) mod 2;
                                  a3 := 0

> a2:=Normal(coeff(coeff(Et,y,0),x,2)) mod 2;
                                     2
                             a2 := s  + s + t

> a2s:=Normal(coeff(coeff(coeff(Et,y,0),x,2),s,0)) mod 2;
                                 a2s := t

> a4:=Normal(coeff(coeff(Et,y,0),x,1)) mod 2;
                                  a4 := 0

> a6:=Normal(coeff(coeff(Et,y,0),x,0)) mod 2;
                                       8    6
                               a6 := t  + t

> d2:=a1^2: d4:=a1*a3: d6:=a3^2: d8:=a1^2*a6+a1*a3*a4+a2*a3^2+a4^2:
> discriminant:=d2^2*d8+d6^2+d2*d4*d6;
                                            8    6
                        discriminant := t  + t
```

A.2 Special points

```
> sb:=[
> t*U+x+t*(t+1)*z,
> t^2*V+(y+s*x)+t^2*(t^2+t)*z,
> t^2*Z+(t+1)*x+t^2*(t+1)*z]:
> Et:=y^2+x*y+x^3+(s^2+s+t)*x^2+t^8+t^6:
```

```
> Tr0:=s^2+s+t:
> Tr1:=s^2+s+t+1:
>
#########  Z=0,  Tr(t)=0
> G10:=Basis(subs({Z=0,U=1,x=t^2,z=1},[op(sb),Et,Tr0]),plex(y,s,t,V),
> characteristic=2):
> map(po -> (Factor(po) mod 2), G10);
              4          2           2          2     4    3
         [V t  (V + 1), s  + s + t, t  V + y + t  s + t  + t ]

> map(po -> (Factor(po) mod 2), subs(V=0,G10));
                        2                 2     4    3
                   [0, s  + s + t, y + t  s + t  + t ]

> map(po -> (Factor(po) mod 2), subs(V=1,G10));
                     2          2         2     4    3
                [0, s  + s + t, t  + y + t  s + t  + t ]

#########  Z=0,  Tr(t)=1
> G11:=Basis(subs({Z=0,U=1,x=t^2,z=1},[op(sb),Et,Tr1]),plex(y,s,t,V),
> characteristic=2):
> map(po -> (Factor(po) mod 2), G11);
            4          2                 2            2     4    3
       [V t  (V + 1), s  + s + t + 1, t  V + y + t  s + t  + t ]

> map(po -> (Factor(po) mod 2), subs(V=0,G11));
                      2                     2     4    3
                 [0, s  + s + t + 1, y + t  s + t  + t ]

> map(po -> (Factor(po) mod 2), subs(V=1,G11));
                   2                2         2     4    3
              [0, s  + s + t + 1, t  + y + t  s + t  + t ]
```

```
# ========================================================
# First phase
# ========================================================
#########  U=0,  Tr(t)=0
> G20:=Basis(subs({U=0,z=1},[op(sb),Et,Tr0]),plex(x,y,s,t,V,Z),
> characteristic=2):
> map(po -> (Factor(po) mod 2), G20);
                                    2
[V t (Z + V), t ((Z + 1) t + 1), s  + s + t,

        2      4    3    2                2
    y + t  V + t  + t  + t  s + s t, x + t  + t]

#########  U=0,  Tr(t)=1
> G21:=Basis(subs({U=0,z=1},[op(sb),Et,Tr1]),plex(x,y,s,t,V,Z),
> characteristic=2):
> map(po -> (Factor(po) mod 2), G21);
                                    2
[V t (Z + V), t ((Z + 1) t + 1), s  + s + t + 1,

        2      4    3    2                2
    y + t  V + t  + t  + t  s + s t, x + t  + t]

#########  V=0,  Tr(t)=0
> G30:=Basis(subs({V=0,z=1},[op(sb),Et,Tr0]),plex(x,y,s,t,U,Z),
> characteristic=2):
> Factor(G30[1]) mod 2;
                                              4
                          U t (U + Z) (U + 1)

> map(po -> (Factor(po) mod 2), subs(U=1,G30[3]));
                                    2
                                   t  Z
```

```
#########  V=0,  Tr(t)=1
> G31:=Basis(subs({V=0,z=1},[op(sb),Et,Tr1]),plex(x,y,s,t,U,Z),
> characteristic=2):
> Factor(G31[1]) mod 2;
                                                4
                              U t (U + Z) (U + 1)

> map(po -> (Factor(po) mod 2), subs(U=1,G31[3]));
                                        2
                                       t  Z

#########  U=V+Z,  Tr(t)=0
> G40:=Basis(subs({U=V+Z,z=1},[op(sb),Et,Tr0]),plex(x,y,s,t,V,Z),
> characteristic=2):
> Factor(G40[1]) mod 2;
                                                 4
                             t (V + Z) V (Z + V + 1)

> expand(subs(V=Z+1,G40[3])) mod 2;
                                        2
                                       t  Z

#########  U=V+Z,  Tr(t)=1
> G41:=Basis(subs({U=V+Z,z=1},[op(sb),Et,Tr1]),plex(x,y,s,t,V,Z),
> characteristic=2):
> Factor(G41[1]) mod 2;
                                                 4
                             t (V + Z) V (Z + V + 1)

> Factor(G41[1]) mod 2;
                                                 4
                             t (V + Z) V (Z + V + 1)
```

```
# ========================================================
# Second phase
# ========================================================
####################  U=0, V=0
> G7:=Basis(subs({U=0,V=0,z=1},[op(sb),Et]),plex(Z,s,t,x,y),
> characteristic=2);
           2            2              2                    2
G7 := [x + t  + t, x s + x  + x t + y, Z y  + y s t + y x t + y  + s y,

                           2           2
    Z y x + y x + t y + y, x  + x t + Z x  + x, Z x + Z t + x]

> Factor( subs(x=t^2+t,G7[2]) - y ) mod 2;
                                          2
                           t (t + 1) (s + t )

> expand( subs( { y=%, x=t^2+t} , Et) ) mod 2;
                                    0


####################  U=0, V=Z
> G8:=Basis(subs({U=0,V=Z,z=1},[op(sb),Et]),plex(Z,s,t,x,y),
> characteristic=2);
           2            2
G8 := [x + t  + t, x s + x  + x t + y + x,

       2                   2
    Z y  + y s t + y x t + y  + s y + t y + y, Z y x + y x + t y + y,

     2           2
    x  + x t + Z x  + x, Z x + Z t + x]
```

```
> Factor( subs(x=t^2+t,G8[2]) - y ) mod 2;
                                          2
                          t (t + 1) (s + t  + 1)

> expand( subs( { y=%, x=t^2+t} , Et) ) mod 2;
                                    0

#################### U=Z, V=0
> G9:=Basis(subs({U=Z,V=0,z=1},[op(sb),Et]),plex(Z,s,t,x,y),
>
> characteristic=2);
                       4    3                              2
           G9 := [x, t  + t  + y, Z y + t y + y, Z t + t  + t]

> expand( subs( { y=t^3+t^4, x=0} , Et) ) mod 2;
                                    0
```

A.3 Injectivity of the mapping

```
# ======================================================
# 1-1 correspondence between (u,v) and (x,y)
# ======================================================
> sb:=[U=1/t*x+(t+1)*z,V=1/t^2*(y+s*x)+(t^2+t)*z,Z=(t+1)/t^2*x+(t+1)*z]:
> U1:=subs({x=x1,y=y1,z=1},rhs(sb[1])):
> Z1:=subs({x=x1,y=y1,z=1},rhs(sb[3])):
> U2:=subs({x=x2,y=y2,z=1},rhs(sb[1])):
> Z2:=subs({x=x2,y=y2,z=1},rhs(sb[3])):
> V1:=subs({x=x1,y=y1,z=1},rhs(sb[2])):
> V2:=subs({x=x2,y=y2,z=1},rhs(sb[2])):
> fv:=V1/Z1-V2/Z2:
> fu:=U1/Z1-U2/Z2:
> fact(fu);
```

$$\frac{t^2 (x1 + x2)}{(t + 1)^2 (t^2 + x1) (t^2 + x2)}$$

```
> fv:=subs(x1=x2,fv):
> fact(fv);
```

$$\frac{y1 + y2}{(t + 1)^2 (t^2 + x2)}$$

Appendix B

Maple code for the ternary case

B.1 Substitution for the elliptic curve

```
maple ternary-thesis
    |\^/|     Maple 11 (IBM INTEL LINUX)
._|\|   |/|_. Copyright (c) Maplesoft, a division of Waterloo Maple Inc.
 \  MAPLE  /  All rights reserved. Maple is a trademark of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.
# ============================================================
#     u  +  v  +  w    =  1
#    1/u + 1/v + 1/w   =  r
# ============================================================
> with(Groebner):
> eq:=1/u+1/v+1/w-r:
> f:=numer(subs(w=1-u-v,eq));
                          2       2             2         2
        f := -v + u v + v  - u + u  + r u v - r u  v - r u v

> F:=numer( eval(f, {u=U/Z, v=V/Z}) ):
> C:= expand(eval( F , {
> U=2/(r^2 + 2*r)*x,
> V=y,
```

```
> Z=2/(r + 2)*x + 2/(r^4 + r^3 + r^2)*z}))  mod 3:
> fact:= f -> (Factor(numer(f)) mod 3)/(Factor(denom(f)) mod 3);
> E:=eval(C, { z=1} ):
> lc:=Normal( coeff(E,x,3) ) mod 3:
> Er:=E/lc:
> Normal(coeff(coeff(Er,y,0),x,3)) mod 3;
                                  1

> a2:=Normal(coeff(coeff(Er,y,0),x,2)) mod 3: fact(%);
                                 2 r + 2
                                -----------
                                 2        2
                                r  (r + 2)

> a1:=-Normal(coeff(coeff(Er,y,1),x,1)) mod 3;
                                 a1 := 1/r

> a3:=-Normal(coeff(coeff(Er,y,1),x,0)) mod 3: fact(%);
                                     1
                                -----------
                                 2        2
                                r  (r + 2)

> a4:=Normal(coeff(coeff(Er,y,0),x,1)) mod 3: fact(%);
                                     1
                                -----------
                                 3        3
                                r  (r + 2)

> -Normal(coeff(coeff(Er,y,2),x,0)) mod 3;
                                  1

> a6:=Normal(coeff(coeff(Er,y,0),x,0)) mod 3;
```

```
                              a6 := 0

> d2:=a1^2+a2: d4:=2*a4+a1*a3: d6:=a3^2+a6:
> d8:=a1^2*a6+a2*a6+2*a1*a3*a4+a2*a3^2+2*a4^2:
> discriminant:=2*d2^2*d8+d4^3:
> Factor(numer(discriminant)) mod 3;
                                        10
                              r (r + 2)

> Factor(denom(discriminant)) mod 3;
                               10        19
                              r   (r + 2)
```

B.2 Special points

```
> Er:=Normal(numer(E/lc)) mod 3:
> sb:=[U*(r^2 + 2*r)-2*x,V-y,Z*(r^4 + r^3 + r^2)-2*r^2*(r + 2)*x - 2*z]:
# ============================================================
# First phase
# ============================================================
#########  Z=0
> G1:=
> Basis(subs({Z=0,z=1},[op(sb),Er]),plex(x,y,r,U,V),characteristic=3):
> Factor(G1[1]) mod 3;
                               V (U + V)

#########  U=0
> G2:=
> Basis(subs({U=0,z=1},[op(sb),Er]),plex(x,y,r,V,Z),characteristic=3):
> Factor(G2[1]) mod 3;
                              V (V + 2 Z)
```

```
#########  V=0
> G3:=
> Basis(subs({V=0,z=1},[op(sb),Er]),plex(x,y,r,U,Z),characteristic=3):
> Factor(G3[1]) mod 3;
                              Z U (2 Z + U)

#########  Z=U+V
> G5:=
> Basis(subs({Z=U+V,z=1},[op(sb),Er]),plex(x,y,r,V,U),characteristic=3):
> Factor(G5[1]) mod 3;
                               U V (U + V)

# ========================================================
# Second phase
# ========================================================
####################  U=0, V=0
> G7:=
> Basis(subs({U=0,V=0,z=1},[op(sb),Er]),plex(Z,r,x,y),characteristic=3):
> map(po -> (Factor(po) mod 3), G7);
                                4          3      2
                    [y, x, Z r  + 1 + Z r  + Z r ]

####################  V=0, Z=0
> G8:=
> Basis(subs({V=0,Z=0,z=1},[op(sb),Er]),plex(U,r,x,y),characteristic=3):
> map(po -> (Factor(po) mod 3), G8);
                               3        2     2
                  [y, 1 + x r  + 2 x r , 2 x  r + U]

####################  U=0, V=Z
> G9:=
> Basis(subs({U=0,V=Z,z=1},[op(sb),Er]),plex(Z,r,x,y),characteristic=3):
> map(po -> (Factor(po) mod 3), G9);
```

```
                          4          3      2
                [x, y r  + 1 + y r  + y r , Z + 2 y]
################### V=0, U=Z
> G10:=
> Basis(subs({V=0,U=Z,z=1},[op(sb),Er]),plex(Z,r,x,y),characteristic=3):
> map(po -> (Factor(po) mod 3), G10);
                     3          2           2      2
             [y, x r  + 1 + x r  + x r, 2 x  r + x  + Z]

################### Z=0, U=-V
> G11:=
> Basis(subs({Z=0,U=-V,z=1},[op(sb),Er]),plex(V,x,y,r),characteristic=3):
> map(po -> (Factor(po) mod 3), G11);
                   5      4      3       2
          [1 + y r  + y r  + y r , 2 y r  + y r + x, V + 2 y]
```

B.3 Injectivity of the mapping

```
# ==========================================================
# correspondence between (u,v) and (x,y)
# ==========================================================
#take distinct (x1,y1) and (x2,y2), assume they produce the same (u,v)
> sb:=[U=2/(r^2 + 2*r)*x,V=y,Z=2/(r + 2)*x + 2/(r^4 + r^3 + r^2)*z]:
>
> U1:=subs({x=x1,y=y1,z=1},rhs(sb[1])):
> Z1:=subs({x=x1,y=y1,z=1},rhs(sb[3])):
> U2:=subs({x=x2,y=y2,z=1},rhs(sb[1])):
> Z2:=subs({x=x2,y=y2,z=1},rhs(sb[3])):
> fu:=U1/Z1-U2/Z2:
> fu:=numer(fu) mod 3:
> V1:=subs({x=x1,y=y1,z=1},rhs(sb[2])):
> V2:=subs({x=x2,y=y2,z=1},rhs(sb[2])):
```

```
> fv:=V1/Z1-V2/Z2:
> fv:=numer(fv) mod 3:
>
> G:=Basis([
> fu,fv,subs({x=x1,y=y1,z=1},Er) mod 3,subs({x=x2,y=y2,z=1},Er) mod 3,
> numer(1-k*Z1*Z2) mod 3],
> plex(k,x1,x2,y1,y2,r),characteristic=3):
> Factor(G[1]) mod 3;
                                        2        4
                          (y1 + 2 y2) r  (r + 2)

> Factor(G[3]) mod 3;
                                         2        4
                        2 (2 x1 + x2) r  (r + 2)
```

B.4 Second substitution

```
# ============================================================
# Second substitution
# ============================================================
> Er:=x^3+a2*x^2-a1*x*y+a4*x-a3*y-y^2:
> Et:=expand(subs({r=1/t, y=2*t^3/(t+2)^3*y+t*x+t^4/(t+2)^2},Er)) mod 3:
> Et:=expand(subs(x=t^2/(t+2)^2*x+t^3*(t+1)/(t+2),Et)) mod 3:
> Et:=Et*((2*t+1)/t)^6:
> Normal(coeff(coeff(Et,y,0),x,3)) mod 3;
                                      1

> a2:=Normal(coeff(coeff(Et,y,0),x,2)) mod 3;
                                   a2 := 1

> a1:=-Normal(coeff(coeff(Et,y,1),x,1)) mod 3;
                                   a1 := 0
```

```
> a4:=Normal(coeff(coeff(Et,y,0),x,1)) mod 3;
                                  a4 := 0

> -Normal(coeff(coeff(Et,y,2),x,0)) mod 3;
                                    1

> a3:=-Normal(coeff(coeff(Et,y,1),x,0)) mod 3;
                                  a3 := 0

> a6:=Normal(coeff(coeff(Et,y,0),x,0)) mod 3;
                                     9      6
                             a6 := t  + 2 t
```

Appendix C

Point of order 6

```
    |\^/|     Maple 11 (IBM INTEL LINUX)
._|\|   |/|_. Copyright (c) Maplesoft, a division of Waterloo Maple Inc.
 \  MAPLE  /  All rights reserved. Maple is a trademark of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.
> Et:=x^3+(s^2+s+t)*x^2+x*y+y^2+t^8+t^6;
                        3     2           2          2    8    6
                 Et := x  + (s  + s + t) x  + x y + y  + t  + t

> expand(subs({x=t^2+t, y=t^4+t^3+s*t^2+s*t},Et)) mod 2;
                                        0

> a1:=Normal(coeff(coeff(Et,y,1),x,1)) mod 2;
                                     a1 := 1

> a3:=Normal(coeff(coeff(Et,y,1),x,0)) mod 2;
                                     a3 := 0

> a2:=Normal(coeff(coeff(Et,y,0),x,2)) mod 2;
                                       2
                                a2 := s  + s + t
```

```
> a4:=Normal(coeff(coeff(Et,y,0),x,1)) mod 2;
                                    a4 := 0

> a6:=Normal(coeff(coeff(Et,y,0),x,0)) mod 2;
                                        8    6
                                  a6 := t  + t

#Adding points on the elliptic curve in characteristic 2.
> AddPt:=proc(P::list,Q::list)
>  global a1,a2,a3,a4,a6;
>  local lam,mu,x3,y3,x1,y1,x2,y2;
>  x1:=P[1]: y1:=P[2]: x2:=Q[1]: y2:=Q[2]:
>  if (x1 mod 2 = x2 mod 2) and (y1+y2+a1*x2+a3 mod 2 =0 mod 2)
>    then return "PtAtInfinity";
>  elif x1<>x2 and x1<>-x2 then
>   lam:=(y2-y1)/(x2-x1): mu:=(y1*x2-y2*x1)/(x2-x1):
>  else lam:=(x1^2+a4+a1*y1)/(a1*x1+a3): mu:=(x1^3+a4*x1-a3*y1)/(a1*x1+a3):
>  fi;
>  x3:=lam^2+a1*lam-a2-x1-x2:
>  y3:=-(lam+a1)*x3-mu-a3;
>  return [Factor(Normal(x3) mod 2) mod 2, Factor(Normal(y3) mod 2) mod 2];
> end:
>
> P:=[t^2+t, t^4+t^3+s*t^2+s*t];
                              2       4    3       2
                    P := [t  + t, t  + t  + s t  + s t]

#Doubling the point P
> P2:=AddPt(P,P);
                                   2        2       2
                          P2 := [t , (s + t  + t) t ]

> expand(subs({x=P2[1], y=P2[2]},Et)) mod 2;
```

```
                                    0

#Tripling the point 3P=2P+P.
> P3:=AddPt(P2, P);
                                     3
                          P3 := [0, t  (1 + t)]

> expand(subs({x=P3[1], y=P3[2]},Et)) mod 2;
                                    0

#4P=2P+2P.
> P4:=AddPt(P2, P2);
                                2        2          2
                      P4 := [t , (s + t  + t + 1) t ]

> expand(subs({x=P4[1], y=P4[2]},Et)) mod 2;
                                    0

#5P=2P+3P.
> P5:=AddPt(P2, P3);
                                          2
                 P5 := [t (1 + t), (s + t  + 1) t (1 + t)]

> expand(subs({x=P5[1], y=P5[2]},Et)) mod 2;
                                    0

#6P=3P+3P.
> P6:=AddPt(P3, P3);
                          P6 := "PtAtInfinity"
```

Appendix D

Magma code: Creation of the elliptic curves

D.1 Binary case

```
Magma V2.14-1     Mon Nov  5 2007 11:14:48 on ella
Type ? for help.  Type <Ctrl>-D to quit.
> k<r>:=RationalFunctionField( GF(2), 1 );
> A2<u,v>:=AffineSpace(k,2);
> // u+v+w = 1
> // 1/u+1/v+1/w = r
> C:=Curve(A2, v*(1-u-v) + u*(1-u-v) + u*v - r*u*v*(1-u-v) );
> Genus(C);
1
> Dp:=ProjectiveClosure(C);
> _<U,V,Z>:=Dp;
> E,m:=EllipticCurve(Dp,Dp![0,1,0]);
> _<x,y,z> := E;
> E;
Elliptic Curve defined by y^2 + r^2*x*y + r^7/(r^2 + 1)*y = x^3 +
r^4/(r^2 + 1)*x^2 + r^9/(r^3 + r^2 + r + 1)*x over Multivariate
rational function field of rank 1 over GF(2)
> d:= Discriminant(E);
```

```
> Factorization(Numerator(d));
[
    <r, 26>
]
> Factorization(Denominator(d));
[
    <r + 1, 8>
]
> AllDefiningPolynomials(Extend(m))[2];
[
    r^4/(r + 1)*U,
    r^6/(r^2 + 1)*V,
    U + 1/r*Z
]
```

```
    |\^/|     Maple 11 (X86 64 LINUX)
._|\|   |/|_. Copyright (c) Maplesoft, a division of Waterloo Maple Inc.
 \  MAPLE  /  All rights reserved. Maple is a trademark of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.
> fact:= proc(f) (Factor(numer(f)) mod 2)/(Factor(denom(f)) mod 2);
end proc;
> E:=y^2 + r^2*x*y + r^7/(r^2 + 1)*y + x^3 +
> r^4/(r^2 + 1)*x^2 + r^9/(r^3 + r^2 + r + 1)*x;
```

$$E := y^2 + r^2 x y + \frac{r^7}{r^2+1} y + x^3 + \frac{r^4}{r^2+1} x^2 + \frac{r^9}{r^3+r^2+r+1} x$$

```
> E := subs( r=1+1/t  , E) mod 2:
> E:=subs( z=1  , E) mod 2:
> c:=Normal(coeff(coeff(E,y,2),x,0)) mod 2:
```

```
> E:= Normal(expand(E/c)) mod 2:
> Normal(coeff(coeff(E,y,0),x,3)) mod 2;
                                        1

> Normal(coeff(coeff(E,y,2),x,0)) mod 2;
                                        1

> a1:=Normal(coeff(coeff(E,y,1),x,1)) mod 2: fact(%);
                                          2
                                    (t + 1)
                                    --------
                                        2
                                       t

> a3:=Normal(coeff(coeff(E,y,1),x,0)) mod 2: fact(%);
                                          7
                                    (t + 1)
                                    --------
                                        5
                                       t

> a2:=Normal(coeff(coeff(E,y,0),x,2)) mod 2: fact(%);
                                          4
                                    (t + 1)
                                    --------
                                        2
                                       t

> a4:=Normal(coeff(coeff(E,y,0),x,1)) mod 2: fact(%);
                                          9
                                    (t + 1)
                                    --------
                                        6
```

t

```
> a6:=Normal(coeff(coeff(E,y,0),x,0)) mod 2;
                                        a6 := 0
```

D.2 Ternary case

```
magma < ternary-thesis-magma
Magma V2.14-1     Mon Nov  5 2007 14:19:46 on ella
Type ? for help.  Type <Ctrl>-D to quit.
> k<r>:=RationalFunctionField( GF(3), 1 );
> A2<u,v>:=AffineSpace(k,2);
> // u+v+w = 1
> // 1/u+1/v+1/w = r
> C:=Curve(A2, v*(1-u-v) + u*(1-u-v) + u*v - r*u*v*(1-u-v) );
> Genus(C);
1
> Dp:=ProjectiveClosure(C);
> _<U,V,Z>:=Dp;
> E,m:=EllipticCurve(Dp);
> _<x,y,z> := E;
> E;
Elliptic Curve defined by y^2 + 1/r*x*y + 1/(r^4 + r^3 + r^2)*y =
x^3 + (2*r + 2)/(r^4 + r^3 + r^2)*x^2 + 1/(r^6 + 2*r^3)*x over
Multivariate rational function field of rank 1 over GF(3)
> d:= Discriminant(E);
> Factorization(Numerator(d));
[]
> Factorization(Denominator(d));
[
    <r, 9>,
    <r + 2, 9>
]
```

```
> minv:=Inverse(m);
> AllDefiningPolynomials(Extend(minv));
[
    [
        y,
        2/(r^2 + 2*r)*x,
        2/(r + 2)*x + 2/(r^4 + r^3 + r^2)*z
    ]
]
```

Bibliography

[1] *NIST/SEMATECH e-Handbook of Statistical Methods.* Available on-line at http://www.itl.nist.gov/div898/handbook/. November 30, 2007.

[2] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Elsevier.* Submitted on August 17, 2007.

[3] A. E. Brouwer and L. M. G. M. Tolhuizen. A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters. *Des. Codes Cryptogr.*, 3(2):95–98, 1993.

[4] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications.* Submitted on May 22, 2007.

[5] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[6] Pascale Charpin. Open problems on cyclic codes. In *Handbook of coding theory, Vol. I, II*, pages 963–1063. North-Holland, Amsterdam, 1998.

[7] Pascale Charpin, Tor Helleseth, and Victor Zinoviev. The divisibility modulo 24 of Kloosterman sums on GF(2^m), m odd. *J. Combin. Theory Ser. A*, 114(2):322–338, 2007.

[8] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra.* Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007.

[9] E. R. van Dam and D. Fon-Der-Flaass. Codes, graphs, and schemes from nonlinear functions. *European J. Combin.*, 24(1):85–98, 2003.

[10] D. Danev and S. Dodunekov. A family of ternary quasi-perfect codes. In *Workshop on Coding and Cryptography 2007, 16–20 April 2007, Versailles, France*, pages 109–115, 2007.

[11] S. Dodunekov and V.A. Zinoviev. A note on Preparata codes. In *Proceedings of Sixth Intern. Symp. on Information Theory*, pages 78–80. Moscow - Tashkent, 1984.

[12] Yves Edel, Gohar Kyureghyan, and Alexander Pott. A new APN function which is not equivalent to a power mapping. *IEEE Trans. Inform. Theory*, 52(2):744–747, 2006.

[13] Kseniya Garaschuk and Petr Lisoněk. On Kloosterman sums divisible by 3. *Accepted to Special issue of Designs, Codes and Cryptography*, 2007.

[14] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography.* Springer Professional Computing. Springer-Verlag, New York, 2004.

[15] Tor Helleseth and Daniel Sandberg. Some power mappings with low differential uniformity. *Appl. Algebra Engrg. Comm. Comput.*, 8(5):363–370, 1997.

[16] Tor Helleseth and Victor Zinoviev. On Z_4-linear Goethals codes and Kloosterman sums. *Des. Codes Cryptogr.*, 17(1-3):269–288, 1999.

[17] J. W. P. Hirschfeld. *Projective geometries over finite fields.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[18] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.

[19] Gilles Lachaud and Jacques Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Trans. Inform. Theory*, 36(3):686–692, 1990.

[20] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge, second edition, 1997.

[21] Petr Lisoněk. Binary caps with many free pairs of points. *J. Combin. Des.*, 14(6):490–499, 2006.

[22] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[23] M.S. Maxwell. *Almost perfect nonlinear functions and related combinatorial structures.* PhD thesis, Iowa State University, 2005.

[24] Alfred Menezes and Scott Vanstone. Isomorphism classes of elliptic curves over finite fields of characteristic 2. *Utilitas Math.*, 38:135–153, 1990.

[25] Marko Moisio. Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm. *Finite Fields and Their Applications.* Submitted on 14 June 2007.

[26] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, volume 765 of *Lecture Notes in Comput. Sci.*, pages 55–64. Springer, Berlin, 1994.

[27] Kaisa Nyberg and Lars Ramkilde Knudsen. Provable security against differential cryptanalysis. In *Advances in cryptology—CRYPTO '92 (Santa Barbara, CA, 1992)*, volume 740 of *Lecture Notes in Comput. Sci.*, pages 566–574. Springer, Berlin, 1993.

[28] Bruce Schneier. *Applied cryptography (2nd ed.): protocols, algorithms, and source code in C.* John Wiley & Sons, Inc., New York, NY, USA, 1995.

[29] René Schoof. Families of curves and weight distributions of codes. *Bull. Amer. Math. Soc. (N.S.)*, 32(2):171–183, 1995.

[30] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[31] Douglas R. Stinson. *Cryptography: Theory and practice.* CRC Press Series on Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, second edition, 2002.

[32] Lawrence C. Washington. *Elliptic curves: Number theory and Cryptography.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2003.