Exponential Sums, Gauss Sums and Cyclic Codes

by

Marko Moisio

University of Oulu
Department of Mathematical Sciences
90570 Oulu
Finland
1997

Moisio, Marko, Exponential sums, Gauss sums and cyclic codes
Department of Mathematics and Statistics, University of Vaasa, P.O. Box 700, FIN 65101 Vaasa, Finland
Acta Univ. Oul. A 306, 1998
Oulu, Finland

Abstract

The dissertation consists of three articles in which the evaluation of certain exponential sums and Gauss sums and bounds for the absolute values of exponential sums are considered. The summary part of the thesis provides interpretations in terms of coding theory for the results obtained in the articles.

Keywords: character sums, Kloosterman sums, error correcting codes

Acknowledgements

I wish to express my deepest gratitude to my advisor Associate Professor Keijo Väänänen for his careful reading of my writings and for his encouragement to write the dissertation based on them. I am also indebted to him for his constructive criticism and for his valuable advice.

I am very grateful to Professor Victor Zinoviev and Ph.D. Hannu Tarnanen for refereeing the manuscript.

I am indebted to the Graduate school *Mathematical Modelling and Computing* of the University of Oulu for giving me an opportunity to concentrate completely on my investigations and for its financial support.

I also wish to thank the staff of the Department of Mathematical Sciences, University of Oulu, and the staff of the Department of Mathematics and Statistics, University of Vaasa, for the good and inspirational working atmosphere that exist there.

Finally, my warmest thanks to my wife Tuula for her support and patience. I also wish to thank my parents Aino and Juhani as well as my sister Soile and her husband Jari for their support.

Vaasa, March 1998 Marko Moisio

List of original articles

I M. Moisio, On relations between certain exponential sums and multiple Kloosterman sums and some applications to coding theory, Math. Univ. Oulu, Preprint, January 1997, pp. 1-11.

II M. Moisio, Exponential Sums, Gauss sums, and irreducible cyclic codes, Math. Univ. Oulu, Preprint, June 1997, pp. 1-19.

III M. Moisio and K. Väänänen, Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes, Math. Univ. Oulu, Preprint, November 1997, pp. 1-15.

Contents

1. Introduction

Let $\mathbb{F}$ be a finite field with r elements and let e be the canonical additive character of $\mathbb{F}$. An exponential sum over $\mathbb{F}$ is of the form $S(f) := \sum_{x\in\mathbb{F}} e(f(x))$ with $f \in \mathbb{F}[X]$. Exponential sums are important tools for studying the number of solutions to equations over finite fields and also for some coding theoretical applications. Bounds for the absolute value of $S(f)$, for example, can be used to estimate the number of solutions to equations of the form $\sum f_i(x_i) = \alpha$, with $\alpha \in \mathbb{F}$, $f_i \in \mathbb{F}[X_i]$, and the weights of the codewords of binary cyclic codes. Furthermore, the determination of the weight distribution of a binary cyclic code is a task equivalent to the determination of the distribution of the values of $S(f)$ when $S(f)$ is interpreted as a function from an additive subgroup of $\mathbb{F}[X]$ into $\mathbb{Z}$.

In general terms, the distribution of the values of S is very difficult to determine, and we have to be satisfied with considering the bounds for the absolute values of exponential sums, which is also difficult to do. Let $f \in \mathbb{F}[X]$. The classical bound for $|S(f)|$ is that proved by A. Weil [26] by deep methods taken from algebraic geometry:

$$|S(f)| \leq (\deg f - 1)\sqrt{r},$$

provided that r and the degree of f are relatively prime. Although the original proof of Weil has been simplified, the known proofs of the Weil bound are still difficult for arbitrary $f \in \mathbb{F}[X]$ (see [15], [24]). On the other hand, we can give an easy proof for monomial $S(\alpha X^N)$ by means of Gauss sums of the form $\sum_{x\in\mathbb{F}^*} e(x)\chi(x)$, where χ is a multiplicative character of $\mathbb{F}$. Gauss sums have been studied extensively from the 19th century up to present days at least in [7], [1], [2], [3], [6], [8], [19], [25] and [14] and it is known that their explicit evaluation is in general difficult. On the other hand, $G(e, \chi)$ can be evaluated more or less explicitly by suitably restricting the order of χ

The aim of the dissertation is to study the interplay between Gauss sums and monomial sums in certain special cases, i.e. when N has certain special properties. Assume, for example, that the multiplicative order of the characteristic of $\mathbb{F}$ is $\phi(N)/2$, where ϕ is the Euler function, and that -1 is not a power of the characteristic of $\mathbb{F}$ modulo N. We shall develop a recursive method with respect to the divisors of N for computing the distribution of the values of $s(\alpha X^N)$. In terms of coding theory this means that we can recursively compute the weight distribution of irreducible cyclic codes of length $(r-1)/N$ from those of irreducible cyclic codes of length $(r-1)/D$ with $D \mid N$. The method allows us to generalize previous results obtained by Baumert and Mykkeltveit [2] and van der Vlugt [25].

From the computational point of view, the recursion formulae together with a superb algorithm developed in [9] for solving certain Diophantine equations open up a possibility for determining the weight distributions of the codes involved in less than $\mathcal{O}(\log^2 r)$ elementary arithmetical operations.

The investigation also leads us to a relation between certain monomial sums and multiple Kloosterman sums of the form

$$\sum_{x_1,\ldots,x_n\in\mathbb{F}^*} e(x_1+\cdots+x_n+\alpha x_1^{-1}\ldots x_n^{-1})$$

with $\alpha\neq 0$.

The Weil bound is often too weak for the absolute values of monomial sums with large exponents (with respect to $\sqrt{r}$), and we get better estimates by the bounds for multiple Kloosterman sums proved by Deligne in [5]. In particular, if the degree of extension of $\mathbb{F}$ over the prime field of $\mathbb{F}$ is even, we obtain for all divisors N of $r-1$ estimates for $|S(\alpha X^N)|$ which are in many cases better than the Weil bound.

As Gauss sums have shown their usefulness in the study of monomial sums, it is natural to try to use their properties with binomial sums $S(\alpha X^N+\beta X^T)$, $T>0$. It will turn out that Gauss sums can enable some binomial sums, for which the Weil bound is too weak, to be converted to multiple Kloosterman sums and again we obtain sharp upper bounds by using the deep results of Deligne.

Results obtained in the manner described above are used to construct some coding theoretical examples. More precisely, we study the dimensions, weight distributions and minimum distances of some binary cyclic codes. We construct a binary $[2^{3t}-1, 4t]$-subcode of the 3rd order punctured Reed-Muller code, for example, and using a deep result concerning the distribution of the values of Kloosterman sums proved by Lachaud and Wolfman in [13], we are able to determine the set of weights of the code.

2. Summary of the original articles

2.1. Preliminaries

In this subsection we shall fix some notations and list the most important properties of characters of finite fields and Gauss sums needed later. For proofs, we refer to [15], [22] and [11].

A character of a finite group $(G, *)$ is a homomorphism Φ from G to the group of the non-zero complex numbers $\mathbb{C}^*$. The set $\widehat{G}$ of all characters on G takes on a group structure with respect to the operation $\cdot : \widehat{G} \times \widehat{G} \longrightarrow \widehat{G}$ defined by

$$\Phi_1, \Phi_2 \in \widehat{G} \Longrightarrow (\Phi_1 \cdot \Phi_2)(a) = \Phi_1(a)\Phi_2(a) \qquad \forall\ a \in G,$$

when we define the inverse Φ^{-1} of $\Phi \in \widehat{G}$ and the identity element Φ_0 by setting

$$\Phi^{-1}(a) = \overline{\Phi(a)}\ \forall\ a \in G,$$
$$\Phi_0(a) = 1 \qquad \forall\ \ a \in G,$$

where the bar denotes the complex conjugation. It is proved in [22], for example, that $\widehat{G}$ is isomorphic to G and that the following character relations are valid

$$\sum_{a \in G} \Phi(a) = \begin{cases} |G| & \text{if } \Phi = \Phi_0, \\ 0 & \text{otherwise,} \end{cases}$$

$$\sum_{\Phi \in \widehat{G}} \Phi(a) = \begin{cases} |G| & \text{if } a = 1_G, \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

where 1_G is the identity element of G.

Let $\mathbb{F}$ be the finite field with $r = p^m$ elements, and let $\mathbb{F}^*$ denote the multiplicative group of $\mathbb{F}$. The character group of the multiplicative (resp. additive) group of $\mathbb{F}$ is called the multiplicative (resp. additive) character group of $\mathbb{F}$. Let γ be a primitive

element of $\mathbb{F}$. The multiplicative character group $\widehat{\mathbb{F}}$ of $\mathbb{F}$ consists of the mappings χ_j, $j = 0, 1, \ldots, r-2$, defined by

$$\chi_j(\gamma^k) = \exp(2\pi ijk/(r-1)), \qquad k = 0, \ldots, r-2,$$

where $i = \sqrt{-1}$.

Let Tr denote the trace mapping from $\mathbb{F}$ to its prime field $\mathbb{F}_p$. i.e.

$$Tr(x) = x + x^p + \cdots + x^{p^{m-1}} \qquad \forall\ x \in \mathbb{F}.$$

The additive character group of $\mathbb{F}$ consists of the mappings e_a, $a \in \mathbb{F}$, defined by

$$e_a(x) = \exp(2\pi i Tr(ax)/p) \qquad \forall\ a \in \mathbb{F}.$$

We denote the character e_1 by e and call it the canonical additive character of $\mathbb{F}$.

Exponential sums or additive character sums (over $\mathbb{F}$) are of the form

$$S(f) := \sum_{x \in \mathbb{F}} e(f(x)),$$

where $f \in \mathbb{F}[X]$. If f is a monomial, i.e. of the form αX^n, or a binomial, i.e. of the form $\alpha X^n + \beta X^t$ with $n, t \in \mathbb{Z}_+$, $\alpha, \beta \in \mathbb{F}^*$, we refer to these sums as monomial and binomial sums, respectively.

Let ψ and χ be an additive character and a multiplicative character of $\mathbb{F}$, respectively. The Gauss sum $G(\chi, \psi)$ over $\mathbb{F}$ is defined by

$$G(\psi, \chi) = \sum_{x \in \mathbb{F}^*} \psi(x)\chi(x).$$

If $\psi = e$ we also write $G(\chi) = G(\psi, \chi)$. Let α be a fixed element of $\mathbb{F}$ and let ψ_α denote the additive character defined by $\psi_\alpha(x) = \psi(\alpha x)$ for $x \in \mathbb{F}$.

The Gauss sum $G(\psi, \chi)$ satisfies

$$G(\psi, \chi) = \begin{cases} r-1 & \text{if } \psi = e_0,\ \chi = \chi_0, \\ -1 & \text{if } \psi \neq e_0,\ \chi = \chi_0, \\ 0 & \text{if } \psi = e_0,\ \chi \neq \chi_0. \end{cases} \tag{2}$$

If $\psi \neq e_0$ and $\chi \neq \chi_0$ then

$$|G(\psi, \chi)| = \sqrt{r}. \tag{3}$$

In addition, Gauss sums have the following properties

$$\begin{aligned}
&(a)\ G(\psi_{ab}, \chi) = \overline{\chi(a)} G(\psi_b, \chi) \qquad \text{for } a \in \mathbb{F}^*, b \in \mathbb{F};\\
&(b)\ G(\overline{\psi}, \chi) = \chi(-1) G(\psi, \chi);\\
&(c)\ G(\psi, \overline{\chi}) = \chi(-1) \overline{G(\psi, \chi)};\\
&(d)\ G(\psi, \chi) G(\psi, \overline{\chi}) = \chi(-1) r \qquad \text{for } \chi \neq \chi_0,\ \psi \neq e_0;\\
&(e)\ G(\psi_b, \chi^p) = G(\psi_{b^p}, \chi) \qquad \text{for } b \in \mathbb{F}.
\end{aligned} \tag{4}$$

It follows easily from the character relations that we have a Fourier expansion of the restriction of ψ to $\mathbb{F}^*$ in terms of the multiplicative characters of $\mathbb{F}$ with Gauss sums as coefficients:

$$\psi(x) = \frac{1}{r-1} \sum_{\chi \in \widehat{\mathbb{F}}} G(\psi, \overline{\chi}) \chi(x) \qquad \forall\ x \in \mathbb{F}^*. \tag{5}$$

Let $\mathbb{E}$ be the extension field of $\mathbb{F}$ of degree n. A deep theorem of Davenport and Hasse [4] (see also [15] for an elementary proof) relates certain Gauss sums over $\mathbb{E}$ to the Gauss sums over $\mathbb{F}$:

The Davenport-Hasse theorem. *Let $Tr_{\mathbb{E}/\mathbb{F}}$ and $\mathbb{N}_{\mathbb{E}/\mathbb{F}}$ be the trace and norm mappings from $\mathbb{E}$ into $\mathbb{F}$, respectively. Then*

$$G(\psi \circ Tr_{\mathbb{E}/\mathbb{F}}, \chi \circ N_{\mathbb{E}/\mathbb{F}}) = (-1)^{n-1} G(\psi, \chi)^n,$$

provided that not both of ψ and χ are trivial.

We shall also need the prime ideal decomposition of some Gauss sums in the ring of integers of certain cyclotomic fields. Let $n \in \mathbb{Z}_+$ and denote $\zeta_n = \exp(2\pi i/n)$. Let $\mathcal{P}$ be a fixed prime divisor of the ideal (p) in the ring of integers $\mathbb{Z}[\zeta_{p(r-1)}]$ of $E := \mathbb{Q}(\zeta_{p(r-1)})$, and consider the residue class field $\mathbb{K} := \{0, 1, g, \ldots, g^{r-2}\}$, where $g = \zeta_{r-1} + \mathcal{P}$. Let $a \in \{1, \ldots, r-2\}$. A theorem of Stickelberger [23] (see also [11, Ch. 14]) states that the highest power of $\mathcal{P}$ dividing the ideal generated by the Gauss sum

$$\sum_{i=0}^{r-2} \zeta_p^{Tr(g^i)} \zeta_{r-1}^{-ai}$$

is equal to the digit sum $S_p(a)$ in the p-base expansion of a. Since $\mathbb{F}$ and $\mathbb{K}$ are isomorphic fields, there exists a primitive element γ in $\mathbb{F}$ which maps onto g under the isomorphism. Now the character χ defined by $\chi(\gamma) = \zeta_{r-1}$ is a multiplicative character of order $r-1$ of $\mathbb{F}$. Thus, the highest power of $\mathcal{P}$ dividing $(G(\overline{\chi}^a))$ is equal to $S_p(a)$.

Assume now that $a = (r-1)/N$ for some divisor N of $r-1$, and that $G(\overline{\chi}^a) \in F := \mathbb{Q}(\zeta_N)$. Since $G(\overline{\chi}^a)\overline{G(\overline{\chi}^a)} = p^m$ the only possible prime divisors of $(G(\overline{\chi}^a))$ in $\mathbb{Z}[\zeta_N]$ are prime divisors of (p). Let $\prod_{i=1}^{t} P_i$ and $\prod_{i=1}^{t'} \mathcal{P}_i^{p-1}$, with $t = \phi(N)/\operatorname{ord}_N(p)$ and $t' = \phi(r-1)/m$, be the prime ideal decompositions of (p) in $\mathcal{O}_F := \mathbb{Z}[\zeta_N]$ and in $\mathcal{O}_E := \mathbb{Z}[\zeta_{p(r-1)}]$, respectively (see [11]). It then follows that $\operatorname{ord}_{\mathcal{P}_i}(P_i\mathcal{O}_E) = p-1$ for $i = 1, \ldots, t$. Now, by lifting the prime ideal decomposition of the ideal $G(\overline{\chi}^a)\mathcal{O}_F$ into $\mathcal{O}_E$, we obtain $(p-1)\operatorname{ord}_P(G(\overline{\chi}^a)) = \operatorname{ord}_{\mathcal{P}}(G(\overline{\chi}^a))$ for some $P \in \{P_1, \ldots, P_g\}$, since $P_i\mathcal{O}_E$ and $P_j\mathcal{O}_E$ are relatively prime if $i \neq j$. Consequently, $\operatorname{ord}_P(G(\overline{\chi}^a)) = S_p(a)/(p-1)$. Let P' be another prime divisor of $(G(\overline{\chi}^a))$ in $\mathcal{O}_F$. We know that $P' = \sigma_i^{-1}(P)$ for some $\sigma_i \in Gal(F/\mathbb{Q})$ (see [11, Ch. 12]). Further, $\sigma_1(P) = \sigma_2(P)$ if and only if $\sigma_2^{-1}\sigma_1 \in G_p := \{\sigma \in Gal(F/\mathbb{Q}) \mid \sigma(P) = P\} < Gal(F/\mathbb{Q})$. Thus $P' = \sigma(P)$ if and only if $\sigma \in \sigma_i^{-1}G_p$.

Let $S \subset \mathbb{Z}_N^*$ be a complete set of representatives of cosets of $< p >$ in $\mathbb{Z}_N^*$. Since the mapping $[\mathbb{Z}_N^* \longrightarrow Gal(F/\mathbb{Q}), i \mapsto \sigma_i]$ with $\sigma_i : \zeta_N \mapsto \zeta_N^i$ is an isomorphism and $G_p =< \sigma_p >$ (see [11, Ch. 13]) we have

$$(G(\overline{\chi}^a)) = \prod_{i \in S} \sigma_i^{-1}(P)^{b_i},$$

where $b_i = \operatorname{ord}_{\sigma_i^{-1}(P)}(G(\overline{\chi}^a))$. Obviously $b_i = \operatorname{ord}_P(\sigma_i(G(\overline{\chi}^a)))$, and it is easy to see that $\operatorname{ord}_{\mathcal{P}}(\sigma_i(G(\overline{\chi}^a))) = S_p(ai)$ (see [11, Ch. 14]). Now, by similar reasoning to the above, we get $b_i = S_p(ai)/(p-1)$.

Thus the highest power of p dividing $G(\overline{\chi}^{\frac{r-1}{N}i})$ is

$$h := \frac{1}{p-1}\min\{S_p(\frac{r-1}{N}i) \mid i \in S\}. \tag{7}$$

We may replace S by $\mathbb{Z}_N^*$ since $S_p(j) = S_p(pj)$ for all $j \in \mathbb{Z}_+$. It also follows that the highest power of p dividing $G(\chi^{\frac{r-1}{N}i}) = G(\overline{\chi}^{(N-i)\frac{r-1}{N}})$ is equal to h, since $(N-i, N) = 1$ if and only if $(i, N) = 1$.

2.2. Gauss sums and monomial sums

Let $\mathbb{F}$ be the finite field with r elements and let γ be a fixed primitive element of $\mathbb{F}$. In this subsection we consider a relation between Gauss sums and monomial sums $s(\alpha, N, r) := \sum_{x\in\mathbb{F}^*} e(\alpha x^N)$. Since $s(\alpha, N, r) = s(\alpha, d, r)$ with $d = (N, r-1)$, we may assume that N is a divisor of $r-1$.

Summing both sides of (5) over $\mathbb{F}_r^*$ we obtain

$$s(\alpha, N, r) = \frac{1}{r-1}\sum_{\chi\in\widehat{\mathbb{F}}} G(\overline{\chi})\chi(\alpha)\sum_{x\in\mathbb{F}_r^*}\chi^N(x).$$

By (1), the inner sum is equal to $r-1$ or 0 depending, respectively, on whether or not χ is $(r-1)/N$:th power in $\widehat{\mathbb{F}}$. Thus

$$s(\alpha, N, r) = \sum_{\chi\in H} G(\overline{\chi})\chi(\alpha) = \sum_{\chi\in H} G(\chi)\overline{\chi}(\alpha), \tag{8}$$

where H is the subgroup of order N of $\widehat{F}$.

The equations above are obtained at least in [15], and are the starting points for all the considerations concerning monomial sums in this dissertation.

Let us consider the determination of the distribution of the values of $s(\alpha, N, r)$ with N a fixed divisor of $r-1$. Let p denote the characteristic of $\mathbb{F}$ and let $k = \mathrm{ord}_N(p)$, $N > 2$.

Assume that -1 is a power of p modulo N and let $\chi \in H$. Since $\chi^i(\alpha) = \chi^j(\alpha)$ for all $\alpha \in \mathbb{F}^*$ if $i \equiv j\ (N)$, it follows from (4c) and (4e) that $G(\chi) = G(\chi^{-1}) = \chi(-1)\overline{G(\chi)}$ for all $\chi \in H$. If $p = 2$ then $\chi(-1) = \chi(1) = 1$, and therefore $G(\chi) \in \mathbb{R}$ for all $\chi \in H$. Assume that $p > 2$. Since $p^t \equiv -1\ (N)$ for some $t \in \mathbb{Z}_+$, we have $k \mid 2t$, and consequently $2 \mid k$. Now $p^{k/2} \equiv -1\ (N)$, and therefore N is a divisor of $\sqrt{r}-1$ or $\sqrt{r}+1$. Thus N divides $(r-1)/2$ which implies that $\chi(-1) = 1$ and $G(\chi) \in \mathbb{R}$ for all $\chi \in H$. It can also be proved that if $G(\chi) \in \mathbb{R}$ for all $\chi \in H$ then -1 is a power of p modulo N. A short version of this is given in [6].

Assume now that $r = p^{2s}$ and $d \mid p^s + 1$. Let χ be of order $d > 1$ in $\widehat{\mathbb{F}}$. Stickelberger proved in [23] (see also [15]) that

$$G(\chi) = \begin{cases} p^s & \text{if } d \text{ odd or } \dfrac{p^s+1}{d} \text{ even,} \\ -p^s & \text{if } d \text{ even and } \dfrac{p^s+1}{d} \text{ odd.} \end{cases} \tag{9}$$

By combining the result with the Davenport-Hasse theorem it is easy to evaluate $G(\chi)$ when $r = p^{2sl}$, upon which we obtain

Theorem 1 (Theorem 2.5 in I)**.** *Let γ be a primitive element of $\mathbb{F}$ and assume that $N \mid p^s + 1$, $N > 1$. Then*

$$\sum_{x\in\mathbb{F}} e(\gamma^a x^N) = \begin{cases} (-1)^l\sqrt{r} & \text{if } a \not\equiv t \ (N), \\ (-1)^{l-1}(N-1)\sqrt{r} & \text{if } a \equiv t \ (N), \end{cases}$$

where $t = 0$ if
(1) $p = 2$, or $p > 2$ and $2 \mid l$, or $p > 2$, $2 \nmid l$ and $2 \mid (p^s + 1)/N$;
and $t = N/2$ if
(2) $p > 2$, $2 \nmid l$ and $2 \nmid (p^s + 1)/N$.

For odd N there is no need to use the Davenport-Hasse theorem to evaluate $G(\chi)$ and the related monomial sums (see Theorem 1 in II).

Assume now that N is odd and -1 is not a power of p modulo N. Write $r = p^m$ with $m \geq 1$ and assume that the order of χ is N. If $p = 2$, it follows from (4e) that $G(\chi)$ belongs to the fixed field of the subgroup of $Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ that is isomorphic to $< 2 > \subseteq \mathbb{Z}_N^*$. This fixed field is a subfield of $\mathbb{Q}(\zeta_N)$ whose degree of extension over $\mathbb{Q}$ is $\phi(N)/k$ where $k = \mathrm{ord}_N(2)$ i.e. the multiplicative order of 2 modulo N. Suppose that $k = \phi(N)/2$. Now $G(\chi)$ belongs to a quadratic subfield of $\mathbb{Q}(\zeta_N)$, and we can write $G(\chi) = (b + c\sqrt{-f})/2$ with $b \equiv c \ (2)$, $f \in \mathbb{Z}_+$. Thus (b, c) is a solution of a relatively simple Diophantine equation

$$x^2 + fy^2 = 4r. \tag{10}$$

More precisely, it follows from (7) that we can convert the equation (10) into a form from which we are able to evaluate $G(\chi)$ up to an ambiguity in the signs of b and c. The sign of b can also be determined from a simple congruence (see II).

It is straightforward to verify that all that we said in the case $p = 2$ also holds if $p > 2$, $k = \phi(N)/2$: all we have to do is to show that $G(\chi) \in \mathbb{Q}(\zeta_N)$. For this, let σ be any automorphism of $\mathbb{Q}(\zeta_p)$. Since the Galois group of $\mathbb{Q}(\zeta_{pN})$ is isomorphic to the direct product of the Galois groups of $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_N)$, there exists an

automorphism of $\mathbb{Q}(\zeta_{pN})$, say ψ, whose restrictions to $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_N)$ are σ and $id_{\mathbb{Q}(\zeta_N)}$, respectively. Since $\psi(\zeta_p) = \zeta_p^j$, for some $j \in \mathbb{Z}_p^*$, we have

$$\psi(G(\chi)) = \sum_{x\in\mathbb{F}^*} \zeta_p^{jTr(x)}\chi(x) = \sum_{x\in\mathbb{F}^*} e(jx)\chi(x) = \overline{\chi(j)}G(\chi),$$

by (4a). Since the lemmas 2 and 6, proved in II, also holds in the case $p > 2$, it follows from them that $p-1$ is not divisible by any divisor of N which is greater than 1, and therefore N divides $(r-1)/(p-1)$, if $N > 3$. Thus $\chi(j) = 1$, and consequently $G(\chi)$ is invariant under ψ. It follows that $G(\chi)$ belongs to the fixed field of $<\psi>< Gal(\zeta_{pN})$, i.e. to the extension field of $\mathbb{Q}$ of degree $\phi(pN)/\phi(p)$, i.e. to $\mathbb{Q}(\zeta_N)$. From now on we assume that $N > 3$ if $p > 2$.

Despite the ambiguity in the sign of c, Baumert and Mykkeltveit [2] succeeded in determining the distribution of the values of $s(\alpha, N, r)$ when N is a prime, and van der Vlugt [25] succeeded when N is the product of two different primes. Consider next a more general N. Assume that N is divisible by at least three primes, say p_1, p_2 and p_3, and write $N = p_1^{u_1}p_2^{u_2}p_3^{u_3}N'$ where $p_i \nmid N'$ for $i = 1, 2, 3$. Since $\mathrm{ord}_{p_i^{u_i}}(p)$ and $\mathrm{ord}_{N'}(p)$ divide $\phi(N)/4$, it follows from

$$\mathrm{ord}_N(p) = l.c.m(\mathrm{ord}_{p_1^{u_1}}(p), \mathrm{ord}_{p_2^{u_2}}(p), \mathrm{ord}_{p_3^{u_3}}(p), \mathrm{ord}_{N'}(p))$$

that $\mathrm{ord}_N(p)$ divides $\phi(N)/4$. Thus the most general form for N is: $N = p_1^u p_2^v$ with $u, v \geq 0$, $N > 1$.

As N can have at most two prime divisors, we can try to convert the sum $\sum_{\chi\in H} G(\overline{\chi})\chi(\alpha)$ to a form in which the summing is done over the factors of N. We then use the Möbius inversion formula to the identity $s(\alpha, N, r) = \sum_{\chi\in H} G(\overline{\chi})\chi(\alpha)$ to obtain a simple relation between the sum of the sums $s(\alpha, D, r)$ corresponding to the square-free factors N/D of N and a possible evaluable quantity depending on χ and α. This is the key idea which is used to obtain a recursive algorithm for computing the distribution of the values of $s(\alpha, N, r)$ in II. To state the main results of II, we first fix some notations.

Let $r = p^{lk}$ with $k = \mathrm{ord}_N(p)$ and $l \geq 1$. Let D be a divisor of N and define

$$h = \frac{1}{p-1} min\{S_p((r-1)/D), lk - S_p((r-1)/D)\}.$$

We choose $\zeta = \exp(2\pi i/N)$ and normalize the character χ by defining $\chi(\gamma) = \zeta$. Let

$$S(a, D) := \sum_{x \in \mathbb{F}^*} e(\gamma^a x^D),$$

and let C_a^D denote the p-cyclotomic coset modulo D defined by a.

It is shown in II that if $k = \phi(N)/2$ and $-1 \notin < 2 > \subset \mathbb{Z}_N^*$, we have three cases to deal with:

A. $N = p_1^u$, $p_1 \equiv 3 \ (4)$;

B. $N = p_1^u p_2^v$, $p_1 \equiv 1 \ (4), \mathrm{ord}_{p_1^u}(p) = \phi(p_1^u)$ and $p_2 \equiv 3 \ (4), \mathrm{ord}_{p_2^v}(p) = \phi(p_2^v)$;

C. $N = p_1^u p_2^v$, $p_1 \equiv 1, 3 \ (4), \mathrm{ord}_{p_1^u}(p) = \phi(p_1^u)$ and $p_2 \equiv 3 \ (4), \mathrm{ord}_{p_2^v}(p) = \phi(p_2^v)/2$.

This result also holds if $p > 2$, by the proof of lemma 6 in II.

Theorem 2 (Theorem 2 in II)**.** *Assume that the case A is valid and let $D > 1$. Then*

$$G(\chi^{N/D}) = \frac{b + c\sqrt{-p_1}}{2} p^h, \ b, c \not\equiv 0 \quad (p).$$

Also, the distribution of the values of $S(a, D)$ can be computed recursively by the following relations:

$$(1) \qquad S(a, D) = \begin{cases} \dfrac{\phi(D)}{2} b p^h + S(0, D/p_1) & \text{if } a = 0, \\ -\dfrac{D(b - \epsilon c p_1) p^h}{2p_1} + S(0, D/p_1) & \text{if } a \in C^D_{\epsilon D/p_1}, \\ S(a, D/p_1) & \text{otherwise,} \end{cases}$$

where $\epsilon \in \{-1, 1\}$,

(2) $b^2 + p_1 c^2 = 4p^{m-2h}$,

(3) $\phi(D) b p^h \equiv -2 S(0, D/p_1) \ (D)$,

(4) $S(0, 1) = -1$.

We can replace the congruence (3) with (3'), which is easier to use in practical calculations and implies that $G(\chi^{N/D})$ is not a real number (see III):

(3) $bp^h \equiv -2 \ (p_1)$.

Theorem 3 (Theorem 3 in II)**.** *Assume that the case B is valid and let* $D = p_1^s p_2^t$ *with* $1 \le s \le u$, $1 \le t \le v$. *Then*

$$G(\chi^{N/D}) = \frac{b + c\sqrt{-p_1 p_2}}{2} p^h, \ b, c \not\equiv 0 \quad (p).$$

Also, the distribution of the values of $S(a, D)$ *can be computed recursively by the following relations:*

(1) $S(a, D)$

$$= \begin{cases} \dfrac{\phi(D)}{2} bp^h + S(0, D/p_1) + S(0, D/p_2) - S\Big(0, \dfrac{D}{p_1 p_2}\Big) & \text{if } a = 0, \\ -\dfrac{\phi(D)}{2(p_1-1)} bp^h + S(0, D/p_1) + S\Big(\dfrac{D}{p_1 p_2}, D/p_2\Big) - S\Big(0, \dfrac{D}{p_1 p_2}\Big) & \text{if } a \in C^D_{D/p_1}, \\ -\dfrac{\phi(D)}{2(p_2-1)} bp^h + S\Big(\dfrac{D}{p_1 p_2}, D/p_1\Big) + S(0, D/p_2) - S\Big(0, \dfrac{D}{p_1 p_2}\Big) & \text{if } a \in C^D_{D/p_2}, \\ \dfrac{D(b + \epsilon c p_1 p_2)p^h}{2p_1 p_2} + S\Big(\dfrac{D}{p_1 p_2}, \dfrac{D}{p_1}\Big) + S\Big(\dfrac{D}{p_1 p_2}, \dfrac{D}{p_2}\Big) - S\Big(0, \dfrac{D}{p_1 p_2}\Big) & \text{if } a \in C^D_{\epsilon \frac{D}{p_1 p_2}}, \\ S(a, D/p_1) & \text{if } a \in C^D_{\epsilon \frac{D}{p_1^i p_2^j}}, \\ S(a, D/p_2) & \text{if } a \in C^D_{\epsilon \frac{D}{p_1^j p_2^i}}, \\ S(a, D/p_1) = S(a, D/p_2) & \text{otherwise,} \end{cases}$$

where $i \ge 2$, $j \in \{0, 1\}$, *and* $\epsilon \in \{-1, 1\}$.

(2) $b^2 + p_1 p_2 c^2 = 4p^{m-2h}$,

(3) $\phi(D) bp^h \equiv -2(S(0, \frac{D}{p_1 p_2}) - S(0, D/p_1) - S(0, D/p_2)) \ (D)$,

$$S(a, D') = \begin{cases} (-1)^{l'-1}(D' - 1)\sqrt{r} - 1 & \text{if } D' \mid a, \\ (-1)^{l'}\sqrt{r} - 1 & \text{if } D' \nmid a, \end{cases} \tag{4}$$

where $l' \equiv l \ (2)$ *if* $D' = p_1^m$, $m > 0$, *and* $l' \equiv 0 \ (2)$ *if* $D' = p_2^n$, $n > 0$.

(5) $S(0, 1) = -1$.

We can replace the congruence (3) with (3'), which is easier to use in practical calculations and which implies that $G(\chi^{N/D})$ is not a real number (see III):

(3') $bp^h \equiv (-1)^{l-1} 2 \ (p_1 p_2)$.

Theorems 2 and 3 imply that we can compute the distribution of the values of $S(a, D)$ for all divisors D of N (see II and III). We note that van der Vlugt [25]

was able to determine the distribution of the values of $S(a, N)$ in the case C with $N = pq$, but we are not able to generalize on this result.

The algorithms in Theorems 2 and 3 are easy to implement, e.g. using MATHEMATICA (see Appendix). The critical step from the computational point of view is the solving of the Diophantine equations. Fortunately, a fast algorithm for that was developed in [9], and this together with our algorithms allows us to compute the exponential sums involved in the $\mathcal{O}(u \log r)$ and $\mathcal{O}(uv \log r)$ steps, depending on whether the case is A or B, respectively. We used these algorithms in III to obtain the weight distributions of certain irreducible cyclic codes.

We finish the discussion concerning monomial sums by considering the absolute values of $s(\alpha, N, r)$. First we note that taking the absolute values of both sides of (8) and using (2) and (3), we obtain the Weil bound:

$$|s(\alpha, N, r)| \leq (N-1)\sqrt{r} + 1.$$

This simple observation is made at least in [15] and [22]. Theorem 1 shows that the Weil bound is obtained for certain divisors $N < \sqrt{r}$ of $r - 1$. On the other hand Theorems 3 and 4 imply that the Weil bound is never obtained if one of the cases A or B above is valid, since the Gauss sums involved are not real.

We next consider the sums $s(\alpha, N, r)$, for which the Weil bound is often too weak, i.e. when N is large with respect to $\sqrt{r}$. We shall first fix some notations.

Let F denote the finite field with q elements and let E denote the extension field of F with $r = q^m$ elements. Let e and ψ denote the canonical additive characters of E and F, respectively. Let $n \in \mathbb{Z}_+$, $\beta \in F^*$ and define an n-dimensional (or multiple) Kloosterman sum over F

$$K_n(\beta) = \sum_{x \in F^*} \psi(x_1 + \cdots + x_n + \beta x_1^{-1} \ldots x_n^{-1}).$$

We obtain from the Davenport-Hasse theorem the following relation between monomial sums and $(m-1)$-dimensional Kloosterman sums.

Theorem 4 (Theorem 2.2 in I). *For all* $\alpha \in \mathbb{E}^*$

$$s(\alpha, q-1, r) = (-1)^{m-1} \sum_{\chi \in \widehat{F}} g(\overline{\chi})^m \chi(N_{E/F}(\alpha)) = (-1)^{m-1}(q-1)K_{m-1}(N_{E/F}(\alpha)),$$

where $g(\chi)$ *is a Gauss sum over* $\mathbb{F}$ *and* $N_{E/F}$ *is the norm mapping from* E *to* F.

Let N be a divisor of $q-1$. Since we have a partition of the group of the N-th powers of E^* into the cosets of the subgroup of $(q-1)$:th powers we can convert the sum $s(\alpha, N, r)$ into a sum of $(m-1)$-dimensional Kloosterman sums over F. The Deligne bound

$$|K_n(\alpha)| \leq (n+1)q^{n/2}$$

now implies

Corollary 1 (Corollary 2.4 in I)**.** *Let* $\alpha \in E^*$ *and* $N \mid q-1$. *Then*

$$\left|s(\alpha, N, r)\right| \leq m(q^{1/2} - q^{-1/2})\sqrt{r}.$$

Deligne's difficult proof is contained in [5].

Theorem 4 also implies

Corollary 2 (Corollary 2.3 in I)**.** *Let* $\beta \in \mathbb{F}^*$. *Then*

$$|K_n(\beta)| \leq q^{\frac{n+1}{2}} - \frac{q^{\frac{n+1}{2}} - 1}{q-1}.$$

The bound in corollary 2 is practically the same as the bound

$$|K_n(\beta)|^2 \leq q^{n+1} - \frac{q^{n+1}-1}{q-1}$$

obtained in [12], and is a generalizion and a slight improvement of the classical bound $|K_n(\beta)| \leq q^{\frac{n+1}{2}}$ proved by Mordell for the prime q in [21].

Assume now that $r = p^m$ with $m > 0$ even and consider the sums $s(\alpha, N, r)$, $\alpha \neq 0$. We may write $N = dt$ where $d \mid q+1$ and $t \mid q-1$ with $q = p^{m/2}$. We have

already dealt with the cases where $d = 1$ or $t = 1$, and so we assume that $d, t > 1$. Because of the partition $< \gamma^{dt} >= \bigcup_{i=0}^{\frac{q+1}{d}-1} \gamma^{dti} < \gamma^{(q+1)t} >$, we have

$$\begin{aligned} s(\alpha, N, r) &= dt \sum_{i=0}^{\frac{q+1}{d}-1} \sum_{j=0}^{\frac{q-1}{t}-1} e(\alpha\gamma^{dti}\gamma^{(q+1)t}) \\ &= d \sum_{i=0}^{\frac{q+1}{d}-1} \sum_{x\in\mathbb{K}^*} \psi(Tr_{\mathbb{F}/\mathbb{K}}(\alpha\gamma^{dti})x^t), \end{aligned}$$

where $\mathbb{K}$ is the subfield of $\mathbb{F}$ with q elements and ψ is the canonical additive character of $\mathbb{K}$.

If $\alpha \in \mathbb{K}$ then $s(\alpha, N, r) = r - 1$. Assume $\alpha \notin \mathbb{K}$.

If $p = 2$ and $\alpha \notin \mathbb{K}$, then $Tr_{\mathbb{E}/\mathbb{K}}(\alpha\gamma^{dti}) = 0$ if and only if $dti \equiv -ind_\gamma(\alpha)\ (q+1)$. Also, the congruence is solvable if and only if $d \mid \mathrm{ind}_\gamma(\alpha)$, and so there exists at most one $i \in \{0, \ldots, (q+1)/d - 1\}$ for which the congruence is solvable. Now, by the Weil bound, we have

Theorem 5.

$$|s(\alpha, dt, r)| \leq \begin{cases} ((t-1)r^{1/4} + d + 1)\sqrt{r} - (d-1)(t-1)r^{1/4} - 2d + 1 & \text{if } ind_\gamma(\alpha) \equiv 0\ (d), \\ (t-1)r^{1/4}\sqrt{r} + (t-1)r^{1/4} + 1 & \text{if } ind_\gamma(\alpha) \not\equiv 0\ (d). \end{cases}$$

If $p > 2$, then $Tr_{\mathbb{E}/\mathbb{K}}(\alpha\gamma^{dti}) = 0$ if and only if $dti \equiv (q+1)/2 - ind_\gamma(\alpha)\ (q+1)$. It is easy to see that $(dt, q+1)$ is equal to $2d$ if $2 \mid t$ and $d < q+1$ (Case 1). Otherwise it equals d (Case 2). Now we have

Theorem 5'. *If $ind_\gamma(\alpha) \equiv (q+1)/2\ (nd)$ then*

$$|s(\alpha, dt, r)| \leq ((t-1)r^{1/4} + nd + 1)\sqrt{r} - (nd-1)(t-1)r^{1/4} - 2nd + 1;$$

otherwise

$$|s(\alpha, dt, r)| \leq (t-1)r^{1/4}\sqrt{r} + (t-1)r^{1/4} + 1,$$

where $n = 1$ or 2 depending on whether Case 1 or Case 2 is valid, respectively.

We observe that our bounds are better than the Weil bound if $d > r^{1/4}$, for example.

2.3. Gauss sums and binomial sums

Let $f = \alpha X^N + \beta X \in \mathbb{F}[X]$, $\alpha, \beta \in \mathbb{F}$, $\alpha \neq 0$. Let us denote

$$s(\alpha, \beta, N, r) := \sum_{x \in \mathbb{F}^*} e(\alpha x^N + \beta x).$$

Two methods come to mind for studying the sums $s(\alpha, \beta, N, r)$ with $\beta \neq 0$ using Gauss sums. First, expanding $e(\alpha x^N)$ using (5), we arrive at the relation

$$s(\alpha, \beta, N, r) = \frac{1}{r-1} \sum_{\chi \in \widehat{\mathbb{F}}} G(\overline{\chi}) G(\chi^N) \chi(\alpha \beta^{-N}). \tag{11}$$

On the other hand, expanding $e(\beta x)$ using (5) leads us to the relation

$$s(\alpha, \beta, N, r) = \frac{1}{r-1} \sum_{\chi \in \widehat{\mathbb{F}}} G(\overline{\chi}) \chi(\beta) \sum_{x \in \mathbb{F}^*} \chi(x) e(\alpha x^N). \tag{12}$$

We see that we can convert the sum $s(\alpha, \beta, N, r)$ into a simpler form if we can evaluate $G(\chi^N)$ or the product of the Gauss sums $G(\overline{\chi})G(\chi^N)$ or hybrid sums $\sum_{x \in \mathbb{F}^*} \chi(x) e(\alpha x^N)$. These are in general hard tasks, but as we shall see, they can be achieved in certain special cases.

If $(N, r-1) = 1$, the substitution $x \mapsto x^t$ makes the inner sum in (12) to be $\chi(\alpha^{-t}) G(\chi^t)$ by (4a), if t is the inverse of N modulo $r-1$. Thus, no matter whether the starting point is (11) or (12), we have to analyze the sums of the products of two Gauss sums.

Assume now that $N \mid r-1$, $N > 1$. Let F denote the finite field with q elements and let E denote the extension field of F with $r = q^m$ elements. Let e and ψ denote the canonical additive characters of E and F, respectively.

Let us first consider (11). Let H be the subgroup of order N of $\widehat{E}$. Let us fix a generator of $\widehat{E}$, say λ. Denote $J := \{0, \ldots, (r-1)/N - 1\}$. Now $\{\lambda^j \mid j \in J\}$ is a complete set of representatives of the cosets of H, and we have

$$s(\alpha, \beta, N, r) = \frac{1}{r-1} \Big(\sum_{j \in J \setminus \{0\}} G(\lambda^{Nj}) \sum_{\chi \in H} G(\overline{\lambda^j \chi})(\lambda^j \chi)(\alpha \beta^{-N}) - \sum_{\chi \in H} G(\overline{\chi}) \chi(\alpha \beta^{-N}) \Big).$$

We see that it may be possible to convert the above sum into a simpler form if we can evaluate $G(\lambda^{Nj})$. We assume that $N = (r-1)/(q+1)$ and m is even, since we can then use (9). Let M denote the field satisfying $F \subseteq M \subseteq E$, $[M : F] = 2$.

Let us fix a generator of $\widehat{M}$, say λ_M, by setting $\lambda_M(\mathbb{N}_{E/M}(\gamma)) = \lambda^t(\gamma)$, where $t = (r-1)/(q^2-1)$ and γ is a primitive element of E. It follows from the Davenport-Hasse theorem that $G(\lambda^{Nj}) = (-1)^{m/2-1} g(\lambda_M^{(q-1)j})^{m/2}$, where $g(\lambda_M^{(q-1)j})$ is a Gauss sum over M. Denote $\epsilon = (-1)^{m/2-1}$. Since $ord(\lambda_M^{(q-1)j}) = (q+1)/(q+1,j)$, it follows from (9) that $g(\lambda_M^{(q-1)j}) = -q$ if and only if j and q are odd. Thus $G(\lambda^{Nj}) = \epsilon\sqrt{r}$ if $2 \mid q$ or $2 \mid m/2$, and otherwise $G(\lambda^{Nj}) = \epsilon(-1)^j\sqrt{r}$. In the latter case we also have $(-1)^j(\lambda^j\chi)(\alpha\beta^{-N}) = (\lambda^j\chi)(-\alpha\beta^{-N})$, since $\chi(-1) = 1$ for all $\chi \in H$. Now, by (8), we obtain

$$\begin{aligned} s(\alpha,\beta,N,r) &= \frac{1}{r-1}\Big(\epsilon\sqrt{r}\sum_{j\in J\setminus\{0\}}\sum_{\chi\in H} G(\overline{\lambda^j\chi})(\lambda^j\chi)(\pm\alpha\beta^{-N}) - \sum_{\chi\in H} G(\overline{\chi})\chi(\alpha\beta^{-N})\Big) \\ &= \frac{1}{r-1}\Big(\epsilon\sqrt{r}\sum_{\chi\in\widehat{E}} G(\overline{\chi})\chi(\pm\alpha\beta^{-N}) - (\epsilon\sqrt{r}+1)\sum_{x\in E^*} e(\alpha\beta^{-N}x^N)\Big). \end{aligned}$$

It follows from (5) that

$$s(\alpha,\beta,N,r) = \epsilon\sqrt{r}e(\pm\alpha\beta^{-N}) - \frac{1}{\epsilon\sqrt{r}-1}\sum_{x\in E^*} e(\alpha\beta^{-N}x^N), \tag{13}$$

where the $+$ sign holds if and only if $2 \mid q$ or $m \equiv 0$ (4). To handle the monomial sum in (13) we need a simple

Lemma (Proposition 2.6 in I)**.**

$$\sum_{x\in E^*} e(\alpha x^{\frac{r-1}{q+1}}) = \begin{cases} r-1 & \text{if } Tr_{E/M}(\alpha) = 0, \\ -\dfrac{r-1}{q+1}K_1\big(\mathbb{N}_{M/F}(Tr_{E/M}(\alpha))\big) & \text{if } Tr_{E/M}(\alpha) \neq 0. \end{cases}$$

Now, by (13) and this lemma, we have

Theorem 6 (Theorem 2.7 in I)**.** *Let $\alpha,\beta \in E$, $\beta \neq 0$ and assume that m is even. Then*

$$s(\alpha,\beta,\frac{r-1}{q+1},r) = \begin{cases} -1 & \text{if } Tr_{E/M}(\alpha) = 0, \\ (-1)^{m/2-1}e(\pm\delta)\sqrt{r} + \dfrac{(-1)^{m/2-1}\sqrt{r}+1}{q+1}K_1(\nu) & \text{if } Tr_{E/M}(\alpha) \neq 0, \end{cases}$$

where $\delta = \alpha\beta^{-\frac{r-1}{q+1}}$, $\nu = N_{M/F}(Tr_{E/M}(\delta))$ and the $-$ sign holds if and only if $m \equiv 2$ (4).

Corollary 3. *Let $\alpha,\beta \in E$, $\beta \neq 0$ and assume that m is even. Then*

$$|s(\alpha,\beta,\frac{r-1}{q+1},r)| \leq \Big(\frac{2r^{\frac{1}{2m}}}{r^{\frac{1}{m}}+1}+1\Big)\sqrt{r} + \frac{2r^{\frac{1}{2m}}}{r^{\frac{1}{m}}+1}$$

We shall next consider (12):

$$s(\alpha,\beta,N,r)=\frac{1}{r-1}\sum_{\chi\in\widehat{E}}G(\overline{\chi})\chi(\beta)\sum_{x\in E^*}\chi(x)e(\alpha x^N).$$

Let us fix a primitive element of E, say γ. Let T be a subgroup of order N of E^* and denote $J:=\{0,\ldots,(r-1)/N-1\}$. The set $S:=\{\gamma^j\mid j\in J\}$ is now a complete set of representatives of cosets of T in E^*. Obviously

$$\sum_{x\in E^*}\chi(x)e_E(\alpha x^N)=\sum_{j\in J}\chi(\gamma^j)e(\alpha\gamma^{Nj})\sum_{x\in T}\chi(x),$$

and $\sum_{x\in T}\chi(x)=N$ or 0 depending on whether $\mathrm{ord}(\chi)$ divides $(r-1)/N$ or not. Let λ denote a generator of $\widehat{E}$. Now

$$s(\alpha,\beta,N,r)=\frac{N}{r-1}\sum_{i\in J}G(\overline{\lambda}^{Ni})\lambda^{Ni}(\beta)\sum_{j\in J}\lambda^{Ni}(\gamma^j)e(\alpha\gamma^{Nj}).$$

Let us fix a generator of $\widehat{F}$, say λ_F, by setting $\lambda_F(\mathbb{N}_{E/F}(\gamma))=\lambda^t(\gamma)$, where $t=(r-1)/(q-1)$. Assume that $N=t$. The inner sum is now nothing more than a Gauss sum $g(\lambda_F^i,\psi_\delta)$ over F where ψ is the canonical additive character of F and $\delta=Tr_{E/F}(\alpha)$. By the Davenport-Hasse theorem, we now have

$$\begin{aligned}s(\alpha,\beta,N,r)&=\frac{(-1)^{m-1}}{q-1}\sum_{i\in J}g(\overline{\lambda}_F^i)^m g(\lambda_F^i,\psi_\delta)\lambda_F^i(\mathbb{N}_{E/F}(\beta))\\&=\frac{(-1)^{m-1}}{q-1}\sum_{\chi\in\widehat{F}}g(\overline{\chi})^m g(\chi,\psi_\delta)\chi(\mathbb{N}_{E/F}(\beta)).\end{aligned}$$

Assume that $\delta=0$. Now $g(\chi,\psi_\delta)=q-1$ or 0, depending on whether χ is trivial or not. Thus

$$s(\alpha,\beta,N,r)=\frac{(-1)^{m-1}}{q-1}(-1)^m(q-1)=-1.$$

Assume that $\delta\neq 0$. Now $g(\chi,\psi_\delta)=\overline{\chi}(\delta)g(\chi)$. We also have $g(\chi)g(\overline{\chi})=\chi(-1)q$, if χ is not the trivial character χ_0. Consequently,

$$\begin{aligned}s(\alpha,\beta,N,r)&=\frac{(-1)^{m-1}q}{q-1}\sum_{\chi\in\widehat{F}\setminus\{\chi_0\}}g(\overline{\chi})^{m-1}\chi(-N_{E/F}(\beta)Tr_{E/F}(\alpha)^{-1})+\frac{1}{q-1}\\&=\frac{(-1)^{m-1}q}{q-1}\sum_{\chi\in\widehat{F}}g(\overline{\chi})^{m-1}\chi(-N_{E/F}(\beta)Tr_{E/F}(\alpha)^{-1})-1.\end{aligned}$$

If $m=2$, we obtain by (5)

Theorem 7 (Theorem 2.8 in I). *If $\alpha, \beta \in E$, $\beta \neq 0$. Then*

$$\sum_{x \in \mathbb{E}^*} e(\alpha x^{q+1} + \beta x) = \begin{cases} -1 & \text{if } \alpha + \alpha^q = 0, \\ -q\psi(-\beta^{q+1}(\alpha + \alpha^q)^{-1}) - 1 & \text{if } \alpha + \alpha^q \neq 0, \end{cases}$$

Assume that $m > 2$. Let E' be an extension field of degree $m-1$ over F. Because of the surjectivity of the norm mapping, we can choose $\nu \in E'$ such that $N_{E'/F}(\nu) = -N_{E/F}(\beta)Tr_{E/F}(\alpha)^{-1}$. By Theorem 4, we now obtain

$$\sum_{x \in E'^*} e_{E'}(\nu x^{q-1}) = (-1)^{m-2} \sum_{\chi \in \widehat{F}} g(\overline{\chi})^{m-1} \chi(-N_{E/F}(\beta)Tr_{E/F}(\alpha)^{-1}).$$

We have thus proved

Theorem 8 (Theorem 2.9 in I). *Let $\alpha, \beta \in E$, $\beta \neq 0$. If $m > 2$ then*

$$s(\alpha, \beta, \frac{r-1}{q-1}, r) = \begin{cases} -1 & \text{if } Tr_{E/F}(\alpha) = 0, \\ (-1)^{m-1} q K_{m-2}(-N_{E/F}(\beta)Tr_{E/F}(\alpha)^{-1}) - 1 & \text{if } Tr_{E/F}(\alpha) \neq 0. \end{cases}$$

Corollary 4. *Let $\alpha, \beta \in E$, $\beta \neq 0$. Then*

$$|s(\alpha, \beta, \frac{r-1}{q-1}, r)| \leq (m-1)\sqrt{r} + 1.$$

The case $\beta = 0$ is easy to deal with:

$$\sum_{x \in E^*} e(\alpha x^{\frac{r-1}{q-1}}) = \frac{r-1}{q-1} \sum_{y \in F^*} \psi(Tr_{E/F}(\alpha)y) = \begin{cases} r-1 & \text{if } Tr_{E/F}(\alpha) = 0, \\ -\dfrac{r-1}{q-1} & \text{if } Tr_{E/F}(\alpha) \neq 0. \end{cases} \quad (14)$$

Thus our study of $s(\alpha, \beta, (r-1)/(q-1), r)$ is completed.

Now that we have found these results, we may try to find simpler proofs for them. This is done in I by starting from the equation

$$s(\alpha, \beta, N, r) = \sum_{i=0}^{t-1} e(\alpha\gamma^{Ni}) \sum_{x \in \gamma^i < \gamma^T >} e(\beta x), \quad (15)$$

where $T = (r-1)/N$.

We conclude the discussion of binomial sums by considering the sums

$$s(\alpha,\beta,N,T,r) := \sum_{x\in\mathbb{F}^*} e(\alpha x^N + \beta x^T),$$

where N is a divisor of $r-1$ greater than 1 and $NT = r-1$. We could proceed as in the proof of Theorem 8, but instead of that we start from (15).

Since we have a partition $\mathbb{F}^* = \bigcup_{i=0}^{N-1} \gamma^i < \gamma^N >$, we obtain

$$s(\alpha,\beta,N,T,r) = \sum_{i=0}^{N-1} e(\beta\gamma^{Ti}) \sum_{x\in<\gamma^N>} e(\alpha\gamma^{Ni}x^N).$$

Assume now that $(N,T) = 1$. It follows that the mapping $x \mapsto x^N$ is a permutation of $< \gamma^N >$, and therefore

$$\sum_{x\in<\gamma^N>} e(\alpha\gamma^{Ni}x^N) = \sum_{x\in<\gamma^N>} e(\alpha\gamma^{Ni}x) = \sum_{x\in<\gamma^N>} e(\alpha x).$$

Thus

$$s(\alpha,\beta,N,T,r) = (\sum_{x\in<\gamma^N>} e(\alpha x))(\sum_{x\in<\gamma^T>} e(\beta x)),$$

and we have

Theorem 9. *Let $NT = r-1$ with $N > 1$. If $(N,T) = 1$, then*

$$s(\alpha,\beta,N,T,r) = \frac{s(\alpha,N,r)s(\beta,T,r)}{r-1}.$$

Corollary 5. *Let $r = 2^{2n}$. Then*

$$|s(\alpha,\beta,2^n-1,2^n+1,r)| \le \begin{cases} 2r^{1/4} & \text{if } \beta \neq \beta^{2^n}, \\ 2r^{1/4}(\sqrt{r}-1) & \text{if } \beta = \beta^{2^n}, \end{cases}$$

Proof. Since $(2^n-1, 2^n+1) = 1$, the bound follows from Theorems 1 and 9 and corollary 1. □

2.4. Coding theoretic applications

In this subsection we give interpretations in terms of coding theory for the results obtained so far. We first state some preliminaries concerning binary cyclic codes. For more complete descriptions, see [17] and [10].

Let $\mathbb{F}_2^n$ denote the n-dimensional vector space over $\mathbb{F}_2$, and let $\mathcal{C}$ be a k-dimensional subspace of $\mathbb{F}_2^n$. We call $\mathcal{C}$ a linear $[n,k]$-code over $\mathbb{F}_2$, and an element of $\mathcal{C}$ a codeword (of $\mathcal{C}$). The weight $w(c)$ of a codeword $c \in \mathcal{C}$ is the sum of the coordinates of c. Let N_i denote the number of codewords of $\mathcal{C}$ of weight i. The weight distribution of $\mathcal{C}$ is the set $W(\mathcal{C}) := \{(i, N_i) \mid i = 0, 1, \ldots n, N_i \neq 0\}$ and the minimum distance of $\mathcal{C}$ is the weight of the non-zero codeword with smallest weight.

Assume now that $\mathcal{C}$ is invariant under the cyclic shift of the coordinates of every codeword of $\mathcal{C}$. Such a code is called cyclic. There is a one to one correspondence between the cyclic $[n,k]$-codes $\mathcal{C}$ and the ideals I of the residue class ring $R_n := \mathbb{F}_2[X]/ < X^n+1 >$ (see [17]). Furthermore, we may think a codeword $(a_0, \ldots, a_{n-1})$ of $\mathcal{C}$ as an element $a_0 + a_1X + \ldots, a_{n-1}X^{n-1} + < X^n + 1 >$ of I, and conversely.

Let I be an ideal of R_n and let $\mathcal{C}$ be the corresponding cyclic code. We know that I is generated by an element $g(X) + < X^n + 1 >$, where $g(X)$ is a divisor of $X^n + 1$ in $\mathbb{F}_2[X]$ (see [17]). We call $g(X)$ the generator polynomial of $\mathcal{C}$ and the zeros of $g(X)$ in the splitting field of $X^n + 1$ the zeros of $\mathcal{C}$. The cyclic code with the generator polynomial $X^{\deg h(X)}h(X^{-1})$ with $h(X) = (X^n + 1)/g(X)$ is called the dual of $\mathcal{C}$.

Let $r = 2^m$ and $nN = r - 1$. Let $\mathbb{F}$ denote the field with r elements and let γ be a primitive element of $\mathbb{F}$. Any cyclic code of length n has a very simple description by means of the trace function. In fact, let P be an additive subgroup of $\mathbb{F}_2[X]$ and define a linear code $\mathcal{C}$ of length n by setting

$$\mathcal{C} = \mathcal{C}(P) = \{c(f) \mid f \in P\},$$

where

$$c(f) = (Tr(f(1)), Tr(f(\gamma)), \ldots, Tr(f(\gamma^{n-1}))).$$

It is shown in [10] that the dual of a cyclic code $\mathcal{B}$ of length n with zeros $\gamma^{Ns_1}, \ldots, \gamma^{Ns_u}$

is the code $\mathcal{C}(P)$ with $P = \{\sum_{i=1}^{u} a_i X^{Ns_i} \mid a_i \in \mathbb{F}\}$. Since the dual of the dual of $\mathcal{B}$ is $\mathcal{B}$, every cyclic code has the above description.

Let us consider the weight of a word $c(f)$ of the cyclic code $\mathcal{C}(P)$ with $P = \{\sum_{i=1}^{u} a_i X^{Ns_i} \mid a_i \in \mathbb{F}\}$. Clearly

$$\begin{aligned} w(c(f)) &= \frac{1}{2}\sum_{j=0}^{n-1}(1 - e(\sum_{i=1}^{u} a_i \gamma^{Ns_i j})) \\ &= \frac{1}{2}(n - \sum_{j=0}^{n-1} e(\sum_{i=1}^{u} a_i \gamma^{Ns_i j})) \\ &= \frac{1}{2N}(r - \sum_{x\in\mathbb{F}} e(\sum_{i=1}^{u} a_i x^{Ns_i})). \end{aligned} \tag{16}$$

Thus the determination of the weight distribution of $\mathcal{C}$ is an equivalent task to the determination of the distribution of the values of $\sum_{x\in\mathbb{F}} e(f(x))$ with $f(X) \in P$.

Let us now consider more closely the cyclic code $\mathcal{C}(P)$ with all s_i's in the same 2-cyclotomic coset modulo n defined by $s := s_1$. In other words $\mathcal{C} := \mathcal{C}(P)$ is the dual of the code $\mathcal{B}$ with an irreducible generator polynomial $g(X)$ (see [17]). Consequently, the generator polynomial of $\mathcal{C}$ is $h(X) := (X^n+1)/f(X)$ with $f(X) = X^{\deg g(X)} g(X^{-1})$. Since $f(X)$ is irreducible, it follows that the ideal generated by $h(X) + < X^n+1 >$ is a minimal ideal of R_n. In other words, $\mathcal{C}$ contains no subspace $\neq 0$ which is closed under the cyclic shift operator. Code $\mathcal{C}$ is called an irreducible cyclic code, since the ideal corresponding to $\mathcal{C}$ cannot be written non-trivially as the sum of its subideals.

The dimension $\dim \mathcal{C}(P)$ of $\mathcal{C}$ over $\mathbb{F}_2$ is easy to determine. Since the number of elements on the 2-cyclotomic coset modulo n defined by s is equal to $\mathrm{ord}_{n'}(2)$ with $n' = n/(n,s)$, $\deg g(X) = \mathrm{ord}_{n'}(2)$. Since $\dim \mathcal{C} = n - \deg h(X)$ (see [17]), $\dim \mathcal{C}(P) = \mathrm{ord}_{n'}(2)$.

As $Tr(\alpha x^2) = Tr(\sqrt{\alpha} x)$ for all $\alpha \in \mathbb{F}_r$ we arrive at the following result proved by van Lint in [16]: The set

$$\mathcal{C} = \{c(\alpha) := (Tr(\alpha), Tr(\alpha\gamma^N), \ldots, Tr(\alpha\gamma^{(n-1)N})) \mid \alpha \in \mathbb{F}\}$$

is an irreducible cyclic code of dimension $\mathrm{ord}_n(2)$ over $\mathbb{F}_2$.

Let F be a homomorphism from $(\mathbb{F},+)$ to $\mathcal{C}$ defined by $\alpha \mapsto c(\alpha)$. Each codeword occurs $|Ker(F)| = 2^{m-\mathrm{ord}_{n'}(2)}$ times in $\mathcal{C}$. We call $\mathcal{C}$ a degenerate code if $m > \mathrm{ord}_{n'}(2)$. Otherwise we call $\mathcal{C}$ a non-degenerate code. Denote $d = (n,s)$. A sufficient condition for the bijectivity of F is $Nd < \sqrt{r}+1$, since for $\alpha \neq 0$, $|\sum_{x\in\mathbb{F}} e(\alpha x^{Ns})| \leq (Nd-1)\sqrt{r}$. Furthermore, this condition holds if $m/\mathrm{ord}_{Nd}(2) \geq 2$, since then $Nd \leq \sqrt{r}-1$.

Example 1. Let $N = 1$. The code $\mathcal{C}(P)$ with $P = \{\alpha x \mid \alpha \in \mathbb{F}\}$ is now the dual of the Hamming code of length $2^m - 1$ i.e. the dual of a $[2^m-1, n-\mathrm{ord}_n(2)] = [2^m-1, 2^m-m-1]$ code. The $[2^m-1,m]$ code $\mathcal{C}(P)$ is called the Simplex code. The weight distribution of $\mathcal{C}(P)$ is $\{(0,1),(2^{m-1},2^m-1)\}$, by (1) and (16).

Example 2. Let $N > 1$ and $-1 \in <2> \subset \mathbb{Z}_N^*$. Now the code $\mathcal{C}(P)$ with $P = \{\alpha x^N \mid \alpha \in \mathbb{F}\}$ is an irreducible cyclic $[(2^m-1)/N, m]$ code. The dimension is m, since $N < \sqrt{r}+1$ (see the discussion after (8)). The weight distribution of the code is $\{(0,1),(w_1,(r-1)/N),(w_2,(N-1)(r-1)/N)\}$, where

$$w_1 = \frac{1}{2N}(r + (-1)^l(N-1)2^{m/2}), w_2 = \frac{1}{2N}(r + (-1)^{l-1}2^{m/2}),$$

with $l = m/\mathrm{ord}_N(2)$, by Theorem 1 and (16).

Example 3. Let $\mathrm{ord}_N(2) = \phi(N)/2$ and assume that $-1 \notin <2> \subset \mathbb{Z}_N^*$. Suppose that case A or B is valid (see Theorems 2 and 3). The code $\mathcal{C}(P)$ with $P = \{\alpha X^N \mid \alpha \in \mathbb{F}\}$ is an irreducible cyclic $[(2^m-1)/N, \mathrm{ord}_n(2)]$-code. The weight distribution of the code can be computed by Theorems 2 and 3. See also III, where algorithms for the computation of the weight distributions and also some weight distributions are presented, and the Appendix for the implementation of these algorithms using MATHEMATICA .

Denote $q = 2^t$, $t > 1$ and $r = q^m$, $m > 1$.

Example 4. Let $N = q-1$. The code $\mathcal{C}(P)$ with $P = \{\alpha X^N \mid \alpha \in \mathbb{F}\}$ is an irreducible cyclic $[(q^m-1)/(q-1), mt]$ code, since $mt/ord_N(2) \geq 2$. The weight of any word $c := c(\alpha) \in \mathcal{C}(P), \alpha \neq 0$, satisfies the inequality

$$|2w(c) - n| \leq \min\{mq^{(m-1)/2}, \sqrt{q}q^{(m-1)/2} - \frac{q^{m/2}-1}{q-1}\},$$

by corollary 1 and the Weil bound.

The first two examples are well known (see e.g. [17]). Example 4 is from I. If $m = 2$, the dual in example 4 is the dual of the Zetterberg code (see [17]), in which case it has been studied at least in [13] and [20].

Let us again consider $\mathcal{C} := \mathcal{C}(P)$ with $P = \{\sum_{i=1}^{u} a_i X^{Ns_i} \mid a_i \in \mathbb{F}\}$. Let us assume that all s_i's lie in different 2-cyclotomic cosets modulo n. It follows from the linearity of the trace map that the ideal corresponding to $\mathcal{C}$ is the sum of the ideals corresponding to $\mathcal{C}_i := \mathcal{C}(P_i)$ with $P_i = \{\alpha X^{Ns_i} \mid \alpha \in \mathbb{F}\}$. Since the ideals corresponding to $\mathcal{C}_i$ are minimal, it follows that the sum is direct. We say that the cyclic code $\mathcal{C}$ is the direct sum of irreducible cyclic codes $\mathcal{C}_i$. Clearly the dimension of $\mathcal{C}$ is $\sum_{i=1}^{u} \mathrm{ord}_{n_i'}(2)$ with $n_i' = n/(n, s_i)$. Furthermore, $\dim \mathcal{C} = um$ if $NM \leq \sqrt{r} + 1$ with $M = \max\{(n, s_i)\}$, and this condition is satisfied if $m/\mathrm{ord}_{NM}(2) \geq 2$.

Example 5. Let $N = 1$ and $m = 2$. The code $\mathcal{C}(P)$ with $P = \{\alpha X^{q+1} + \beta X \mid \alpha, \beta \in \mathbb{F}\}$ is a cyclic $[q^2 - 1, 3t]$ code since $\mathrm{ord}_{q^2-1}(2) = 2t$ and $\mathrm{ord}_{q-1}(2) = t$. The code is the direct sum of the Simplex code of length $q^2 - 1$ and the irreducible cyclic code obtained by pasting together $q + 1$ copies of the Simplex code of length $q - 1$. The weight distribution of the code is

$$\{(0,1), (2^{2t-1} - 2^{t-1}, 2^{t-1}(2^{2t} - 1)), (2^{2t-1}, 2^{2t} - 1), (2^{2t-1} + 2^{t-1}, 2^{3t-1} - 2^{2t} + 2^{t-1})\}$$

by the following discussion.

Denote

$$c(\alpha, \beta) = \big(Tr(\alpha + \beta), Tr(\alpha\gamma^{2^t+1} + \beta\gamma), \ldots, Tr(\alpha\gamma^{(2^t+1)(r-2)} + \beta\gamma^{r-2})\big) \in \mathcal{C}(P).$$

If $c(\alpha', \beta') \in \mathcal{C}(P)$ it follows from the linearity of the trace map and from Theorems 1 and 7 that $c(\alpha, \beta) = c(\alpha', \beta')$ if and only if $T(\alpha) = T(\alpha')$ and $\beta = \beta'$, where T is the trace map from $\mathbb{F}$ to its subfield with 2^t elements, say $\mathbb{K}$. Let β be a fixed element of $\mathbb{F}^*$. If α runs over all elements of $\mathbb{F}$ satisfying $T(\alpha) \neq 0$, then $T(\beta^{2^t+1}(\alpha + \alpha^{2^t})^{-1})$ runs over all elements of $\mathbb{K}^*$. There exist $2^{t-1} - 1$ elements $\delta \in \mathbb{K}^*$ satisfying $Tr_{\mathbb{K}/\mathbb{F}_2}(\delta) = 0$ and 2^{t-1} elements $\delta \in \mathbb{K}^*$ satisfying $Tr_{\mathbb{K}/\mathbb{F}_2}(\delta) = 1$.

We now let β vary over $\mathbb{F}^*$ and it follows from Theorem 7 that there are $2^{t-1}(2^{2t}-1)$ codewords of weight $2^{2t-1}-2^{t-1}$, $(2^{t-1}-1)(2^{2t}-1)$ words of weight $2^{2t-1}+2^{t-1}$, and $2^{2t}-1$ words of weight 2^{2t-1} in $\mathcal{C}(P)$. Let $\beta=0$. It now follows from Theorem 1 that there are 2^t-1 words more of weight $2^{2t-1}+2^{t-1}$ and the zero word in $\mathcal{C}(P)$.

Example 6. Let $N=1$ and $m>2$. The code $\mathcal{C}(P)$ with $P=\{\alpha X^d+\beta x \mid \alpha,\beta\in \mathbb{F}_r\}$, $d=(q^m-1)/(q-1)$, is a cyclic $[q^m-1,(m+1)t]$-code. It follows from Theorem 8, Corollary 2, Corollary 4 and (14) that there are

(1) q^m-1 words of weight $q^m/2$ and

(2) $q-1$ words of weight $(q^m-1+(q^m-1)/(q-1))/2$

in the code $\mathcal{C}(P)$. For the remaining $(q^m-1)(q-1)$ words $c\neq(0,\ldots,0)$ we have

(3) $q-1\leq |2w(c)-n|\leq \min\{\sqrt{q}q^{m/2}-\frac{\sqrt{q}q^{m/2}-q}{q-1}+1,(m-1)q^{m/2}+1\}$.

This code is a small subcode of m-th order punctured Reed-Muller code $\mathcal{R}^*(m,tm)$ (see [10] for the trace function description of Reed-Muller codes). We note that the weights in Cases 2 and 3 are exactly divisible by 2^{t-1} which is in accordance with the divisibility result of McEliece [18] (see also [17]) which states that the weights of an arbitrary Reed-Muller code $\mathcal{R}(l,u)$ are divisible by $2^{\lceil \frac{u}{l}\rceil-1}$, but not necessarily exactly. This example also shows us that it may be difficult to determine the weight distribution of $\mathcal{R}(l,u)$ if $l>2$ and $l\mid u$, since we the have to be able to compute the distribution of the values of multiple Kloosterman sums (see Research Problem 15.1 in [17]). We can go further in the example if we assume that $m=3$, i.e. the code under consideration is a $[2^{3t}-1,4t]$ subcode of $\mathcal{R}^*(3,3t)$. It is proved in [13] that the set of values of Kloosterman sum $K_1(\alpha)$ over the field of order q is equal to the set $\{i \mid i\in[-2\sqrt{q},2\sqrt{q}], i\equiv -1 \pmod 4\}$. Thus we can replace (3) by

(3') The set of the weights of the remaining $(q^3-1)(q-1)$ non-zero codewords is equal to the set

$$\{\frac{1}{2}q(q^{m-1}-i) \mid i\in[-2\sqrt{q},2\sqrt{q}], i\equiv -1 \pmod 4\}.$$

3. References

1. Baumert LD & McEliece RJ (1972) Weights of irreducible cyclic codes. Inform. and Control 20: 158-175.
2. Baumert LD & Mykkeltveit J (1973) Weight distributions of some irreducible cyclic codes. JPL Tech. Report 32-1526: 128-131.
3. Berndt BC & Evans RJ (1981) The determination of Gauss sums. Bull. Am. Math. Soc. 5: 107-129.
4. Davenport H & Hasse H (1935) Die Nullstellen der Kongruenz Zetafunktion in gewissen zyklischen Fällen. J. Reine und Angew. Math. 172: 151-182.
5. Deligne P (1977) Applications de la formule des traces aux sommes trigonometriques. SGA 4 1/2 Springer Lecture Notes in Math 569: 168-232. Springer, New York.
6. Evans RJ (1981) Pure Gauss sums over finite fields. Mathematika 28: 239-248.
7. Gauss CF (1965) Arithmetische Untersuchungen. Chelsea, New York.
8. Hardy K, Muskat JB & Williams KS (1990) A deterministic algorithm for solving $n = fu^2 + gv^2$ in coprime integers u and v. Math. Comp. 55: 327-343.
9. Hasse H (1964) Vorlesungen über Zahlentheorie. Grudl. der Math. Wiss. Vol. 59. Springer-Verlag, Berlin.
10. Honkala I & Tietäväinen A (to appear) Codes and Number Theory. In: Brualdi RA, Huffman WC & Pless V (eds) Handbook of Coding Theory. Elsevier Science Publisher, Amsterdam.
11. Ireland K & Rosen M (1982) A Classical Introduction to Modern Number Theory. Grad. Texts in Math. Vol. 84. Springer-Verlag, New York.
12. Katz NM (1980) Sommes Exponentielles. Soc. Math. France 79. Paris.
13. Lachaud G & Wolfman J (1990) The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Trans. Inform. Theory 36: 686-692.
14. Langevin P (1997) Calculus de certaines sommes de Gauss. J. Number Theory 32: 59-64.
15. Lidl R & Niederreiter H (1984) Finite Fields. Cambridge Univ. Press, Cambridge.
16. van Lint J. H. (1982) Introduction to Coding Theory. Springer-Verlag, New York.
17. MacWilliams FJ & Sloane NJA (1978) The Theory of Error-Correcting Codes. North-Holland, Amsterdam.
18. McEliece RJ (1972) Weight congruences for p-adic cyclic codes. Discrete Math. 3: 177-192.
19. McEliece RJ (1974) Irreducible cyclic codes and Gauss sums. In: Hall M Jr & van Lint JH (eds) Combinatorics (Part 1): 179-196. Mathematical Centre Tracts 55, Mathematical Centre, Amsterdam.
20. McEliece RJ (1980) Correlation properties of sets of sequences derived from irreducible cyclic codes. Inform. and Control 45: 18-25.
21. Mordell LJ (1963) On a special polynomial congruence and exponential sums. In: Calcutta Math. Soc. Golden Jubilee Commemoration Volume, Part 1: 29-32. Calcutta Math. Soc., Calcutta.
22. Schmidt WM (1976) Equations over Finite Fields: An Elementary Approach. Springer, Berlin.
23. Stickelberger L (1890) Über eine Verallgemeinerung von der Kreistheilung. Math. Ann. 37: 321-367.
24. Stichtenoth H (1993) Algebraic Function Fields and Codes. Springer-Verlag, Universitext, New York.
25. van der Vlugt M (1995) Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes. J. Number Theory 55: 145-159.

26. Weil A (1948) On some exponential sums. Proc. Natl. Acad. Sci. 34: 204-207.

Appendix: Computer programs

Original articles

See my homepage.