2005

Sums of Gauss Sums and Weights of Irreducible Codes

Robert W. Fitzgerald
Southern Illinois University Carbondale, rfitzg@math.siu.edu

Joseph L. Yucas
Southern Illinois University Carbondale

Published in *Finite Fields and Their Applications*, 11, 89-110.

Sums of Gauss Sums and Weights of Irreducible Codes

Robert W. Fitzgerald
and
Joseph L. Yucas

Abstract

We develop a matrix approach to compute a certain sum of Gauss sums which arises in the study of weights of irreducible codes. A lower bound on the minimum weight of certain irreducible codes is given.

KEYWORDS: Gauss sums, codes, weights.

1 Introduction

Let d be a positive odd integer and set $e = ord_d(2)$, the order of 2 mod d. We will let L denote the field $\mathbb{F}_{2^e}$, and for a positve integer s, we set $K = \mathbb{F}_{2^{se}}$.

For a multiplicative character, $\chi : K^* \to \mathbb{C}$, the *Gauss sum* of χ is defined as

$$g_K(\chi) = \sum_{\beta \in K^*} (-1)^{tr(\beta)} \chi(\beta),$$

where tr denotes the usual trace map $tr_{K/\mathbb{F}_2}$. Basic results on Gauss sums may be found in [8] and [6].

Computing Gauss sums over K can be reduced to computing them over L via the Hasse-Davenport Theorem [5].

Theorem 1.1. *(***Hasse-Davenport**) Suppose λ is a multiplicative character on L. Let χ be the multiplicative character on K defined by $\chi = \lambda \circ N$ where N is the usual norm map $N_{K/L}$. Then

$$g_K(\chi) = (-1)^{s-1} g_L(\lambda)^s.$$

Generally, it is hard to determine Gauss sums explicitly. They have only been computed when the subgroup generated by 2 in $(\mathbb{Z}/d\mathbb{Z})^*$ has index 2 or contains -1, see [15], [2], [11] and [7]. For applications of these computations to irreducible codes see [2], [4], [3], [12] and [14].

Let $c(x)$ be an irreducible polynomial over $\mathbb{F}_2$ of degree se and order $n = (2^{se} - 1)/d$. The *irreducible code* $\mathbf{C}$ based on $c(x)$ is the cyclic code generated by $(x^n - 1)/c(x)$ over F. For background information on irreducible codes see [9].

The code $\mathbf{C}$ may be described explicitly. Let θ be a primitive n^{th} root of unity in K. There is one code word for each $\beta \in K$, namely,

$$cw(\beta) = (tr(\beta), tr(\beta\theta), \ldots, tr(\beta\theta^{n-1})).$$

In [14], Van Der Vlugt has shown that

$$wt(cw(\beta^{-1})) = \frac{1}{2d}[2^{se} - \sum \chi(\beta) g_K(\chi)],$$

where wt denotes the weight of the code word and where the sum is over all non-trivial characters χ satisfying $\chi^d = \epsilon$.

The sum

$$\sum \chi(\beta) g_K(\chi)$$

will be the main concern of this paper. In section 2 we develop a matrix approach for computing this sum. We then use this matrix technique in section 3 to obtain a lower bound for the minimal weight of $\mathcal{C}$ in the case $s = 2$ and $d = 2^k - 1$ for some positive integer k. In section 4 we discuss applications of this sum in linear recurrences and diagonal equations.

Although we restrict our attention to binary codes, the methods of this paper can also be applied to codes in odd characteristic.

2 The Matrix Approach

2.1 The sum

Define an equivalence relation on $\mathbb{Z}/d\mathbb{Z}$ by: $a \sim b$ iff $a = b2^t$ for some $t \in \mathbb{Z}$. Let H be the subgroup of $(\mathbb{Z}/d\mathbb{Z})^*$ generated by 2. The equivalence classes of $\sim$ have the form $cH = \{ch : h \in H\}$, for $c \in \mathbb{Z}/d\mathbb{Z}$. These are the well-studied *cyclotomic cosets* .

The following theorem is well known. It follows for example from Theorem 2.47 of [8].

Theorem 2.1. *(1) The number of equivalence classes of $\sim$ is given by*

$$NC(d) = \sum_{f|d} \frac{\phi(f)}{ord_f(2)}.$$

When $f = 1$ we take $\phi(f)/ord_f(2)$ to be 1.

(2) For any $0 \neq c \in \mathbb{Z}/d\mathbb{Z}$, $|cH| = ord_f(2)$, where $f = d/(c,d)$.

(3) For any $b, c \in \mathbb{Z}/d\mathbb{Z}$, $|bcH|$ divides $|cH|$.

Lemma 2.2. *Let χ be a multiplicative character of K. Then $g_K(\chi^2) = g_K(\chi)$.*

Proof:

$$g_K(\chi^2) = \sum_{x \in K^*} (-1)^{\mathrm{tr}x} \chi^2(x) = \sum_{x \in K^*} (-1)^{\mathrm{tr}(x^2)} \chi(x^2) = g_K(\chi),$$

since $K^2 = K$.

■

Throughout, we fix a primitive root α of L and a primitive d^{th} root of unity, ω. Let λ denote the multiplicative character of L sending α to ω. Then the list of multiplicative characters of L with trivial d^{th} power is: $\epsilon, \lambda, \lambda^2, \ldots, \lambda^{d-1}$.

Pick a primitive root δ of K such that $N_{K/L}(\delta) = \alpha$. Set $\chi = \lambda \circ N_{K/L}$. Then $\chi^i = \lambda^i \circ N_{K/L}$ and the characters of K with trivial dth power are χ^i for $0 \leq i \leq d-1$. The sums we want to compute then become

$$\sum_{i=1}^{d-1} \chi^i(\delta^j) g_K(\chi^i).$$

We will let $\mathcal{C}$ denote a fixed and ordered set of representatives of the cyclotomic cosets mod d.

For $s \geq 0$, define $Sum(j,s)$ by

$$Sum(j,s) = \sum_{0 \neq c \in \mathcal{C}} \left[\sum_{i \in cH} \lambda^i(\alpha^j) \right] g_L(\lambda^c)^s.$$

Lemma 2.3.

$$\sum_{i=1}^{d-1} \chi^i(\delta^j) g_K(\chi^i) = (-1)^{s-1} Sum(j,s).$$

Proof:

$$\sum_{i=1}^{d-1} \chi^i(\delta^j) g_K(\chi^i) = \sum_{0 \neq c \in \mathcal{C}} \left[\sum_{i \in cH} \chi^i(\delta^j) \right] g_K(\chi^c) \quad \text{by Lemma 2.2}$$

$$= (-1)^{s-1} \sum_{0 \neq c \in \mathcal{C}} \left[\sum_{i \in cH} \chi^i(\delta^j) \right] g_L(\lambda^c)^s,$$

by the Hasse-Davenport Theorem. Now,

$$\chi^j(\delta^j) = \lambda^i(N_{K/L}(\delta^j)) = \lambda^i(\alpha^j).$$

■

Proposition 2.4. $Sum(2j,s) = Sum(j,s)$.

Proof: Let

$$C(j,c) = \sum_{i \in cH} \lambda^i(\alpha^j).$$

Notice that

$$C(2j,c) = \sum_{i \in cH} \lambda^i(\alpha^{2j}) = \sum_{i \in cH} \omega^{2ij} = \sum_{i \in cH} \lambda^{2i}(\alpha^j) = C(j,c),$$

since the sum is over cH and $2i \in cH$ if and only if $i \in cH$. Hence, by the Lemma 2.3 we have,

$$Sum(2j,s) = \sum_{0 \neq c \in \mathcal{C}} C(2j,c) g_L(\lambda^{cs}) = \sum_{0 \neq c \in \mathcal{C}} C(j,c) g_L(\lambda^{cs}) = Sum(j,s).$$

■

Consequently, we have now reduced the computation of the sums down to computing just $Sum(c,s)$ for $c \in \mathcal{C}$.

Theorem 2.5. *Let $c(x)$ be an irreducible polynomial over $\mathbb{F}_2$ of degree se and order $n = (2^{se}-1)/d$. Further, let $\mathbf{C}$ be the irreducible code based on $c(x)$.*

(1) The maximum number of distinct non-zero weights of $\mathbf{C}$ is $NC(d)$.

(2)Assume that $\mathbf{C}$ has exactly $NC(d)$ many distinct weights. Then the number of codewords of weight

$$\frac{1}{2d}\left(2^{se} + (-1)^s Sum(c,s)\right)$$

is $|cH|n$.

Proof: (1) is by Proposition 2.4. For (2) note that $\chi^d = \epsilon$ implies $\chi(\delta^d) = 1$. Then for any integers c, h, j we have $Sum(ch+jd, s) = Sum(ch, s)$, which is in turn equal to $Sum(c, s)$ by Proposition 2.4. Then for each $ch \in cH$ and each $0 \leq j < n$, the codeword $cw(\delta^{-(ch+jd)})$ has weight

$$w_c = \frac{1}{2d}(2^{se} - (-1)^{s-1} Sum(c,s)),$$

by van der Vlugt's formula and Lemma 2.3. Let $N(w_c)$ denote the number of codewords of weight w_c. We have just shown $N(w_c) \geq n|cH|$. Suppose the w_c's, as c runs through $\mathcal{C}$, are distinct. Then

$$2^{se} - 1 = \sum_{c \in \mathcal{C}} N(w_c) \geq \sum_{c \in \mathcal{C}} n|cH| = nd = 2^{se} - 1$$

We thus have equality throughout: $N(w_c) = n|cH|$.

■

The reason for the hypothesis in Theorem 2.5(2) is simply that sometimes, for small s, it can happen that $Sum(b, s) = Sum(c, s)$ for distinct $b, c \in \mathcal{C}$. Then the frequency is the sum $|bH|n + |cH|n$.

2.2 The matrix

As before, fix a primitive d^{th} root of unity $\omega \in \mathbb{C}$. For $b \in \mathbb{Z}/d\mathbb{Z}$, set

$$\beta_b = \sum_{x \in bH} \omega^x.$$

Lemma 2.6. *For $b, c \in \mathbb{Z}/d\mathbb{Z}$*

$$\frac{|cH|}{|bcH|}\beta_{bc} = \sum_{x \in cH} \omega^{bx}.$$

Proof Map $\psi : cH \to bcH$ by $x \mapsto bx$. We **Claim** that if $y, y' \in bcH$ then $|\psi^{-1}(y)| = |\psi^{-1}(y')|$. Namely, suppose $\psi^{-1}(y) = \{x_1, x_2, \ldots, x_r\}$. Now $y' = yh_0$ for some $h_0 \in H$. Then $x_1h_0, x_2h_0, \ldots, x_rh_0$ are distinct elements of cH and each is mapped to $yh_0 = y'$. Hence $|\psi^{-1}(y)| \leq |\psi^{-1}(y')|$. Reversing the roles of y and y' gives the other inequality and proves the **Claim**.

Let Y be the common value of the $|\psi^{-1}(y)|$'s. Then $|bcH| = Y|cH|$. Thus:

$$\sum_{x \in cH} \omega^{bx} = \sum_{y \in bcH} \sum_{x \in \psi^{-1}(y)} \omega^{bx} = \frac{|cH|}{|bcH|} \sum_{y \in bcH} \omega^{y} = \frac{|cH|}{|bcH|}\beta_{bc}.$$

■

Corollary 2.7. *For $b \in \mathbb{Z}/d\mathbb{Z}$*

$$Sum(b, s) = \sum_{0 \neq c \in \mathcal{C}} \frac{|cH|}{|bcH|}\beta_{bc} g_L(\lambda^c)^s.$$

Proof: By Lemma 2.3 we have

$$Sum(b, s) = \sum_{0 \neq c \in \mathcal{C}} \left[\sum_{i \in cH} \lambda^i(\alpha^b) \right] g_L(\lambda^c)^s.$$

Now $\lambda^i(\alpha^b) = \omega^{ib}$ so the result follows from Lemma 2.6.

■

Set, for $c \in \mathbb{Z}$,

$$A_c = \sum_{i=0}^{\frac{2^e-1}{d}-1} (-1)^{\mathrm{tr}(\alpha^{c+id})}.$$

We will write the range of summation in A_c more simply as $m \equiv t \pmod{d}$.

Lemma 2.8. *For each non-zero $b \in \mathcal{C}$ we have*

$$g_L(\lambda^b) = \sum_{c \in \mathcal{C}} \frac{|cH|}{|bcH|} A_c \beta_{bc}.$$

Proof: Let α generate L^* and let $\omega \in \mathbb{C}$ be a primitive d root of unity. We have

$$\begin{aligned} g_L(\lambda^b) &= \sum_{i=0}^{2^e-2} (-1)^{\mathrm{tr}(\alpha^i)} \lambda^b(\alpha^i) = \sum_{i=0}^{2^e-2} (-1)^{\mathrm{tr}(\alpha^i)} \omega^{bi} \\ &= \sum_{t=0}^{d-1} \left[\sum_{m=0}^{\frac{2^e-1}{d}-1} (-1)^{\mathrm{tr}(\alpha^{t+md})} \right] \omega^{bt} = \sum_{t=0}^{d-1} A_t \omega^{bt}. \end{aligned}$$

We **Claim** that $A_t = A_{2t}$, with the subscripts taken modulo d. Namely,

$$\begin{aligned} A_t &= \sum_{m \equiv t \pmod d} (-1)^{\mathrm{tr}(\alpha^m)} = \sum_{2m \equiv 2t \pmod d} (-1)^{\mathrm{tr}(\alpha^m)} \\ &= \sum_{2m \equiv 2t \pmod d} (-1)^{\mathrm{tr}(\alpha^{2m})} = \sum_{\ell \equiv 2t \pmod d} (-1)^{\mathrm{tr}(\alpha^\ell)} = A_{2t}. \end{aligned}$$

Thus there are at most $|\mathcal{C}|$ distinct A_t's, namely the A_c for $c \in \mathcal{C}$. Then

$$\begin{aligned} g_L(\lambda^b) &= \sum_{t=0}^{d-1} A_t \omega^{bt} = \sum_{c \in \mathcal{C}} \sum_{j \in cH} A_j \omega^{jb} \\ &= \sum_{c \in \mathcal{C}} A_c \sum_{j \in cH} \omega^{jb} = \sum_{c \in \mathcal{C}} A_c \frac{|cH|}{|bcH|} \beta_{bc}, \end{aligned}$$

by Lemma 2.6.

■

For $a, b, c \in \mathcal{C}$ define

$$D(a, b, c) = N(x + y = c),$$

the number of solutions to $x + y = c$ where $x \in aH$ and $y \in bH$.

Lemma 2.9.

$$\frac{|aH|}{|amH|} \frac{|bH|}{|bmH|} \beta_{am} \beta_{bm} = \sum_{c \in \mathcal{C}} \frac{|cH|}{|cmH|} D(a, b, c) \beta_{cm}.$$

Proof: From Lemma 2.6 we have

$$\begin{aligned}\frac{|aH|}{|amH|}\beta_{am}\frac{|bH|}{|bmH|}\beta_{bm} &= \sum_{x\in aH}\omega^{mx}\sum_{y\in bH}\omega^{my}\\ &= \sum_{x\in aH}\sum_{y\in bH}\omega^{m(x+y)}\\ &= \sum_{c\in\mathcal{C}}\sum_{z\in cH}N(x+y=z)\omega^{mz},\end{aligned}$$

where $N(x+y=z)$ is the number of solutions with $x\in aH$ and $y\in bH$. For each $z\in cH$, $N(x+y=z)$ equals $N(x+y=c)$. We thus have

$$\frac{|aH|}{|amH|}\beta_{am}\frac{|bH|}{|bmH|}\beta_{bm} = \sum_{c\in\mathcal{C}}D(a,b,c)\sum_{z\in cH}\omega^{mz} = \sum_{c\in\mathcal{C}}D(a,b,c)\frac{|cH|}{|cmH|}\beta_{cm},$$

using Lemma 2.6 again.

■

Let $r=|\mathcal{C}|$. Define the $r\times r$ matrix E by

$$E(a,c) = \frac{|cH|}{|aH|}\sum_{b\in\mathcal{C}}A_bD(a,b,c).$$

Lemma 2.10.

$$\beta_{am}g_L(\lambda^m) = \sum_{c\in\mathcal{C}}\frac{|amH|}{|cmH|}E(a,c)\beta_{cm}.$$

Proof: Each of the following sums is over $\mathcal{C}$.

$$\begin{aligned}\beta_{am}g_L(\lambda^m) &= \beta_{am}\sum_b\frac{|bH|}{|bmH|}A_b\beta_{bm} \quad \text{by Lemma 2.8}\\ &= \sum_b\frac{|amH|}{|aH|}A_b\frac{|aH|}{|amH|}\frac{|bH|}{|bmH|}\beta_{am}\beta_{bm}\\ &= \sum_b\frac{|amH|}{|aH|}A_b\sum_c\frac{|cH|}{|cmH|}D(a,b,c)\beta_{cm} \quad \text{by Lemma 2.9}\\ &= \sum_c\frac{|amH|}{|aH|}\frac{|cH|}{|cmH|}\left(\sum_b A_bD(a,b,c)\right)\beta_{cm}\\ &= \sum_c\frac{|amH|}{|aH|}\frac{|cH|}{|cmH|}\frac{|aH|}{|cH|}E(a,c)\beta_{cm},\end{aligned}$$

which gives the result.

■

Theorem 2.11.

$$Sum(a, s+1) = \sum_{c \in \mathcal{C}} E(a,c) Sum(c,s).$$

Proof Again each sum is over $\mathcal{C}$.

$$\begin{aligned} Sum(a,s+1) &= \sum_{b \neq 0} \frac{|bH|}{|abH|} \beta_{ab} g_L(\lambda^b) \cdot g_L(\lambda^b)^s \quad \text{by Corollary 2.7} \\ &= \sum_{b \neq 0} \frac{|bH|}{|abH|} g_L(\lambda^b)^s \sum_c \frac{|abH|}{|bcH|} E(a,c) \beta_{bc} \quad \text{by Lemma 2.10} \\ &= \sum_c E(a,c) \sum_{b \neq 0} \frac{|bH|}{|bcH|} \beta_{bc} g_L(\lambda^b)^s \\ &= \sum_c E(a,c) Sum(c,s), \end{aligned}$$

by Corollary 2.7 again.

■

Let $\mathcal{S}_s$ be the (column) vector with entries $Sum(c,s)$, over $c \in \mathcal{C}$ (including $c = 0$). Further, let $v_0 = (1-d, 1, \ldots 1)$.

Corollary 2.12. *For all $s \geq 0$ we have*

$$\mathcal{S}_s = -E^s v_0,$$

Proof: By Theorem 2.11, it suffices to check only that $v_0 = \mathcal{S}_0$. By our definition of $Sum(j,s)$ we have

$$Sum(b,0) = \sum_{0 \neq c \in \mathcal{C}} \sum_{i \in cH} \lambda^i(\alpha^j) = \sum_{0 \neq c \in \mathcal{C}} \sum_{i \in cH} \omega^{bi} = \sum_{y=1}^{d-1} \omega^{bi}$$

which is $d-1$ if $b = 0$ and -1 otherwise.

■

Combining this with Theorem 2.5 yields

Theorem 2.13. *Let $c(x)$ be an irreducible polynomial over $\mathbb{F}_2$ of degree se and order $n = (2^{se} - 1)/d$. Further, let $\mathbf{C}$ be the irreducible code based on $c(x)$. The non-zero weights of $\mathbf{C}$ are given by*

$$\frac{1}{2d}\left(2^{se}j - (-1)^s E^s v_0\right).$$

where j is the vector consisting of r 1's.

2.3 Properties of E

Lemma 2.14. *For a, b and $c \in \mathcal{C}$, $D(a, b, c) = |(c - aH) \cap bH|$.*

Proof: $D(a, b, c)$ is the number of pairs, $x \in aH$, $y \in bH$, such that $x + y = c$. Thus $D(a, b, c) = |(c - aH) \cap bH|$.

■

Lemma 2.15. *For a fixed pair $a, c \in \mathcal{C}$,*

$$\sum_{b \in \mathcal{C}} D(a, b, c) = |aH|.$$

Proof: By the previous lemma,

$$\sum_{b \in \mathcal{C}} D(a, b, c) = \sum_{b \in \mathcal{C}} |(c - aH) \cap bH|.$$

For each $ah \in aH$, $c - ah$ is in exactly one bH hence the result follows.

■

For a, b and $c \in \mathcal{C}$, set

$$T(a, b, c) = |(a + bH) \cap cH|.$$

Lemma 2.16. *For a, b, and c in $\mathcal{C}$, $T(a, b, c) = T(a, -c, -b)$*

Proof: $T(a, b, c)$ is the number of solutions to $a + y = z$, with $y \in bH$ and $z \in cH$. $T(a, -c, -b)$ is the number of solutions to $a - z = -y$, with $z \in cH$ and $y \in bH$. These are clearly the same.

■

Proposition 2.17. *For a, b and $c \in \mathcal{C}$, we have*

$$E(a,c) = \sum_{b \in \mathcal{C}} A_b T(a,b,c)$$

. In particular, the entries of E are integers.

Proof; Let $M(a,b,c) = |\{(x,y,z) : x+y=z, x \in aH, y \in bH, z \in cH\}|$. Say $aH = \{ah_1, ah_2, \ldots, ah_{t_1}\}$. Then given $z \in (a+bH) \cap cH$, multiply by each $h_i, 1 \leq i \leq t_1$, to get a solution $x+y=z$ counted by $M(a,b,c)$. We obtain

$$M(a,b,c) = |aH| T(a,b,c)$$

Similarly, if $cH = \{ch_1, ch_2, \ldots, ch_{t_2}\}$, then given $z \in (a-cH) \cap bH$, multiply by each $h_i, 1 \leq i \leq t_2$, to get a solution $x+y=z$ counted by $M(a,b,c)$. Hence,

$$M(a,b,c) = |cH| D(a,b,c).$$

Now,

$$E(a,c) = \frac{|cH|}{|aH|} \sum_{b \in \mathcal{C}} A_b D(a,b,c) = \frac{1}{|aH|} \sum_{b \in \mathcal{C}} A_b M(a,b,c) = \sum_{b \in \mathcal{C}} A_b T(a,b,c).$$

■

Let j be the vector consisting of r 1's.

Proposition 2.18. *j is an eigenvector of E^s corresponding to the eigenvalue $(-1)^s$.*

Proof: It suffices to show that j is an eigenvector of E with eigenvalue -1. The a^{th} coordinate of Ej is

$$(Ej)_a = \sum_{c \in \mathcal{C}} E(a,c) = \sum_{c \in \mathcal{C}} \sum_{b \in \mathcal{C}} A_b T(a,b,c) = \sum_{b \in \mathcal{C}} A_b \sum_{c \in \mathcal{C}} T(a,b,c).$$

Now consider the sets $\{(a+bH) \cap cH\}$ for $c \in \mathcal{C}$. These are disjoint since the cH's are. Further,

$$\bigcup_{c \in \mathcal{C}} [(a+bH) \cap cH] = (a+bH) \cap \bigcup_{c \in \mathcal{C}} cH = a + bH.$$

Hence,

$$\sum_{c \in \mathcal{C}} T(a,b,c) = \sum_{c \in \mathcal{C}} |(a+bH) \cap cH| = |a+bH| = |bH|.$$

We thus have,

$$(Ej)_a = \sum_{b\in\mathcal{C}} A_b|bH| = \sum_{b\in\mathcal{C}} |bH| \sum_{i=0}^{\frac{2^e-1}{d}-1} (-1)^{tr(\alpha^{b+di})}$$
$$= \sum_{b\in\mathcal{C}} \sum_{y\in bH} \sum_{i=0}^{\frac{2^e-1}{d}-1} (-1)^{tr(\alpha^{y+di})} = \sum_{\beta\in L^*} (-1)^{tr(\beta)} = -1.$$

■

Corollary 2.19. $E^s v_0 = (-d[E^s(a,0)]_{a\in\mathcal{C}} + (-1)^s j)^T$.

Proof: Let u be the vector with first entry $-d$ and 0 elsewhere.

$$E^s v_0 = E^s(u+j) = E^s(u) + E^s(j) = (-d[E^s(a,0)]_{a\in\mathcal{C}} + (-1)^s j)^T$$

by the previous proposition.

■

Example 1: Using these techniques it was relatively straight forward to write a computer program to compute the weights of the codewords of an irreducible code. We ran this program for all $d < 400$ with $e < 18$ and the program ran quickly. But of course the time increases as e does. Here is the output for $d = 51$.

$$d = 51$$
$$H = \{1, 2, 4, 8, 16, 32, 13, 26\}$$
$$e = 8$$

$$\mathcal{C} = \begin{array}{cc} \underline{c} & \underline{|cH|} \\ 0 & 1 \\ 1 & 8 \\ 3 & 8 \\ 5 & 8 \\ 9 & 8 \\ 11 & 8 \\ 17 & 2 \\ 19 & 8 \end{array}$$

$$v = [5, 1, 1, -3, -3, 1, 5, 1]$$

$$E = \begin{bmatrix} 5 & 8 & 8 & -24 & -24 & 8 & 10 & 8 \\ 1 & 4 & 4 & 0 & 0 & -12 & -2 & 4 \\ 1 & -4 & -4 & 8 & -8 & 4 & -2 & 4 \\ 1 & 4 & 4 & 0 & 0 & 4 & -2 & -12 \\ -3 & 8 & -8 & 0 & 0 & 0 & 2 & 0 \\ -3 & -8 & 8 & 0 & 0 & 0 & 2 & 0 \\ 5 & -8 & -8 & 8 & 8 & -8 & 10 & -8 \\ 1 & -4 & -4 & -8 & 8 & 4 & -2 & 4 \end{bmatrix}$$

With $s = 2$ the vector of non-zero weights, $2^{se}j - (-1)^s E^s v_0$, is

$$[704, 664, 648, 632, 640, 640, 672, 616]$$

and with $s = 3$ it is

$$[163584, 164448, 164768, 164064, 164480, 164736, 163968, 164640].$$

Note that when $s = 2$, one weight (640) occurs for two cyclotomic cosets while for $s = 3$, the cyclotomic cosets have distinct weights. Hence, when $s = 2$, we have $n = 1285$ and $\mathbf{C}$ has

# of codewords	weight
$1n = 1285$	704
$8n = 10280$	664
$8n = 10280$	648
$8n = 10280$	632
$16n = 20560$	640
$2n = 2570$	672
$8n = 10280$	616

Similarly, when $s = 3$, we have $n = 328965$ and $\mathbf{C}$ has

# of codewords	weight
$1n = 328965$	163584
$8n = 2631720$	164448
$8n = 2631720$	164768
$8n = 2631720$	164064
$8n = 2631720$	164480
$8n = 2631720$	164736
$2n = 657930$	163968
$8n = 2631720$	164640 .

■

Next, we illustrate the use this matrix technique in deriving a formula for the weights of $\mathbf{C}$ in the case $d = 2^k + 1$. This formula also follows from the work in [4].

Set $L_0 = \{\beta \in L : tr(\beta) = 0\}$.

Lemma 2.20. *Let $d = 2^k + 1$, for some positive integer k. For $c \in \mathcal{C}$, set $V_c = \{\alpha^{c+md}\} \cup \{0\}$ for $m = 0, \ldots, 2^k - 1$. Then V_0 is a subfield of L contained in L_0 and V_c, for $c \neq 0$, is a subspace of L with $|V_c \cap L_0| = 2^{k-1}$.*

Proof: First notice that $2^{2k} - 1 = (2^k - 1)(2^k + 1) = 0 \pmod{d}$, hence $e = 2k$. Next we show that V_0 is a subfield of L contained in L_0. Suppose $0 \leq m \leq 2^k - 1$. $(\alpha^{md})^{2^k-1} = \alpha^{m(2^e-1)} = (\alpha^{2^e-1})^m = 1$. Hence, V_0 is a subfield of L isomorphic to $\mathbb{F}_{2^k}$.

$$\begin{aligned} tr(\alpha^{md}) &= \alpha^{md} + (\alpha^{md})^2 + \cdots + (\alpha^{md})^{2^{k-1}} + (\alpha^{md})^{2^k} + \cdots + (\alpha^{md})^{2^{e-1}} \\ &= \alpha^{md} + (\alpha^{md})^2 + \cdots + (\alpha^{md})^{2^{k-1}} + (\alpha^{md}) + \cdots + (\alpha^{md})^{2^{k-1}} = 0, \end{aligned}$$

and thus $V_0 \subset L_0$. To show V_c is a subspace of L for $c \neq 0$, suppose $0 \leq m, m' \leq 2^k - 1$. $\alpha^{c+md} + \alpha^{c+m'd} = \alpha^c(\alpha^{md} + \alpha^{m'd}) = \alpha^c\alpha^{m''d}$ for some $0 \leq m'' \leq 2^k - 1$ since V_0 is a subspace of L. Hence, $\alpha^{c+md} + \alpha^{c+m'd} = \alpha^{c+m''d}$ and V_c is a subspace of L. Finally notice that since L_0 is a hyperplane in L, either $V_c \subset L_0$ or $| V_c \cap L_0 | = 2^{k-1}$. If $V_c \subset L_0$ then since $V_c \cap V_0 = \{0\}$, we would have the $2k$-dimensional space $V_c + V_0$ contained inside the $(2k-1)$-dimensional space L_0, a contradiction.

■

Corollary 2.21. *Let $d = 2^k + 1$, for some positive integer k. For $c \in \mathcal{C}$, we have*

$$A_c = \begin{cases} 2^k - 1 & \text{if } c = 0 \\ -1 & \text{otherwise} \end{cases}.$$

Proof: Recall that

$$A_c = \sum_{i=0}^{\frac{2^e-1}{d}-1} (-1)^{tr(\alpha^{c+md})}.$$

In this case $(2^e - 1)/d = 2^k - 1$. The result now follows from the previous lemma.

■

Theorem 2.22. *Let $d = 2^k + 1$ for some positive integer k. Suppose $c(x)$ is an irreducible polynomial over $\mathbb{F}_2$ of degree $2ks$ and order $n = (2^{2ks} - 1)/d$. Then the irreducible code $\mathbf{C}$ based on $c(x)$ has two non-zero weights given by*

$$\frac{1}{2d}(2^{2sk} - (-1)^s 2^{sk}) \text{ and } \frac{1}{2d}(2^{2sk} + (-1)^s(d-1)2^{sk}).$$

Proof: We use the previous corollary in the following computation.

$$\begin{aligned} E(a,c) &= \frac{|cH|}{|aH|}\sum_{b\in\mathcal{C}} A_b D(a,b,c) \\ &= \frac{|cH|}{|aH|}[2^k D(a,0,c) - \sum_{b\in\mathcal{C}} D(a,b,c)] \\ &= \frac{|cH|}{|aH|}(2^k D(a,0,c) - |aH|), \end{aligned}$$

by Lemma 2.15. Since

$$D(a,0,c) = \begin{cases} 1 & \text{if } a = c \\ 0 & \text{otherwise} \end{cases}$$

we have

$$E(a,c) = \begin{cases} 2^k - |cH| & \text{if } a = c \\ -|cH| & \text{otherwise} \end{cases}.$$

Now, for $s \geq 0$ set

$$F(s) = \sum_{i=0}^{s} (-1)^i 2^{(s-i)k}.$$

Notice that

$$2^k F(s) = \sum_{i=0}^{s} (-1)^i 2^{(s-i+1)k} = F(s+1) - (-1)^{s+1},$$

so that

$$(2^k - 1)F(s) + 2^k F(s-1) = F(s+1) - (-1)^{s+1} - F(s) + F(s) - (-1)^s = F(s+1).$$

That is, for $s \geq 1$, F satisfies the recurrence

$$F(s+1) = (2^k - 1)F(s) + 2^k F(s-1).$$

We **Claim** that the first column of E^s, for $s \geq 1$, is given by $[F(s), -F(s-1), \ldots, -F(s-1)]^T$. We prove this claim by induction on s. If $s = 1$, the result is easy to check. For $s > 1$, notice that

$$\begin{aligned} E^{s+1}(0,0) &= (2^k - |0H|)F(s) + \sum_{c \in C \setminus \{0\}} |cH| F(s-1) \\ &= (2^k - 1)F(s) + 2^k F(s-1) = F(s+1), \end{aligned}$$

and for $a \neq 0$,

$$\begin{aligned} E^{s+1}(a,0) &= -|0H|F(s) - 2^k F(s-1) + \sum_{c \in C \setminus \{0\}} |cH| F(s-1) \\ &= -F(s) - 2^k F(s-1) + 2^k F(s-1) = F(s). \end{aligned}$$

This proves the **Claim**.

Next, notice that

$$\begin{aligned} 2^k F(s) &= \sum_{i=0}^{s} (-1)^i 2^{(s-i+1)k} = 2^{(s+1)k} + \sum_{i=1}^{s} (-1)^i 2^{(s-i+1)k} \\ &= 2^{(s+1)k} + \sum_{i=0}^{s-1} (-1)^{i-1} 2^{(s-i)k} = 2^{(s+1)k} - F(s) + (-1)^s, \end{aligned}$$

so that

$$dF(s) = 2^{(s+1)k} + (-1)^s.$$

By Corollary 2.19, we have

$$\begin{aligned} E^s v_0 &= [-d[E^s(a,0)]_{a \in \mathcal{C}} + (-1)^s j]^T \\ &= [-dF(s) + (-1)^s, dF(s-1) + (-1)^s, \ldots, dF(s-1) + (-1)^s]^T \\ &= [-2^{(s+1)k}, 2^{sk}, \ldots, 2^{sk}]^T. \end{aligned}$$

The result now follows from Theorem 2.13.

■

3 Minimal Weights

3.1 Some results of Niederreiter

In this subsection we generalize some results of Niederreiter. These generalizations will be needed in the next subsection to obtain a lower bound on the minimal weight of $\mathbf{C}$ in the case $d = 2^k - 1$.

We begin with p being a prime and q being a power of p. For a non-trivial additive character χ of F_q, let $\chi^{(s)}$ denote the additive character obtained by lifting χ to an extension field F_{q^s}.

For $a, b \in F_q$, with $ab \neq 0$, and $\beta \in F_q^*$, define

$$K_\beta(\chi; a, b) = \sum_{c \in F_q^*} \chi(ac\beta + bc^{-1}).$$

Theorem 3.1. *There exist complex numbers ω_1 and ω_2(only depending on χ, a and b) that are either complex conjugates or both real such that for any positive integer s we have*

$$K_\beta(\chi^{(s)}; a, b) = -\omega_1^s - \omega_2^s.$$

Proof: Note that if $\beta = 1$, this theorem is precisely Theorem 5.43 of [8]. The proof of [8] Theorem 5.43 will work here as well. Just replace line 6 of page 277 with $\gamma_\beta(g) = \chi(ac_1\beta + bc_{k-1}c_k^{-1})$, if $c_k \neq 0$.

■

Corollary 3.2. *The complex numbers ω_1 and ω_2 of Theorem 3.1 satisfy $|\omega_1 + \omega_2| \leq 2\sqrt{q}$.*

Proof: As in the proof of Theorem 5.43 of [8], we have

$$L(z) = 1 + K_\beta z + qz^2 = (1 - \omega_1 z)(1 - \omega_2 z).$$

Hence $\omega_1\omega_2 = q$ and

$$|\omega_1 + \omega_2| \leq |\omega_1| + |\omega_2| = \sqrt{\omega_1\omega_2} + \sqrt{\omega_2\omega_1} = 2\sqrt{q}.$$

■

We will need these results only in the case when $q = 2^e$, $a = b = s = 1$ and χ is the character on L defined by $\chi(\beta) = (-1)^{tr(\beta)}$. In this case we have

Corollary 3.3. *There exists complex numbers ω_1 and ω_2 that are complex conjugates or both real such that*

$$\sum_{\gamma \in L^*} (-1)^{tr(\beta\gamma + \gamma^{-1})} = -\omega_1 - \omega_2.$$

Further, $|\omega_1 + \omega_2| \leq 2\sqrt{2^e}$.

For $\beta \in L$, let Ψ_β denote the linear map $\Psi_\beta : L \to F$, defined by $\Psi_\beta(\gamma) = tr(\beta\gamma)$. Further, let $L_0^{-1} = \{\beta^{-1} \in L^* : \beta \in L_0\}$.

The next proposition was inspired by the proof of [13] Theorem 2.

Proposition 3.4. *For $\beta \in L^*$, we have*

$$|L_0^{-1} \cap Ker\Psi_\beta| \geq \frac{1}{4}(2^e - 3 - 2\sqrt{2e}).$$

Proof:

$$\begin{aligned}
|L_0^{-1} \cap Ker\Psi_\beta| &= \sum_{\gamma \in L^*}(\frac{1}{2}\sum_{a \in \mathbb{F}_2}(-1)^{\gamma tr(\gamma\beta)})(\frac{1}{2}\sum_{b \in \mathbb{F}_2}(-1)^{btr(\gamma^{-1})}) \\
&= \frac{1}{4}\sum_{\gamma \in L^*}[(-1)^0 + (-1)^{tr(\gamma\beta)}][(-1)^0 + (-1)^{tr(\gamma^{-1})}] \\
&= \frac{1}{4}(\sum_{\gamma \in L^*} 1 + \sum_{\gamma \in L^*}(-1)^{tr(\gamma\beta)} + \sum_{\gamma \in L^*}(-1)^{tr(\gamma^{-1})} + \sum_{\gamma \in L^*}(-1)^{tr(\gamma\beta+\gamma^{-1})} \\
&= \frac{1}{4}[(2^e - 1) + (-1) + (-1) - (\omega_1 + \omega_2)] \\
&\geq \frac{1}{4}(2^e - 3 - |\omega_1 + \omega_2|) \geq \frac{1}{4}(2^e - 3 - 2\sqrt{2^e})
\end{aligned}$$

by Corollary 3.3.

■

3.2 The bound

We begin this section with d arbitrary but will later restrict $d = 2^k - 1$, for some positive integer k. This is a case where the Gauss sums have not been computed.

For each $a \in \mathcal{C}$, define the $r \times r$ matrix ST_a by $ST_a(b, c) = T(a, b, -c)$. Notice that $ST_a(c, b) = T(a, c, -b) = T(a, b, -c) = ST_a(b, c)$, by Lemma 2.16. Hence ST_a is a symmetric matrix. Consider the quadratic form $Q_a(x) = x^T ST_a x$ and recall that $v = [A_b]_{b \in \mathcal{C}}$.

Proposition 3.5. *The first column of E is given by $E(a, 0) = A_{-a}$ and the first column of E^2 is given by $E^2(a, 0) = Q_a(v)$.*

Proof: First notice that $|0H| = 1$ and

$$D(a,b,0) = |(0 - aH) \cap bH| = \begin{cases} |-aH| & \text{if } b \in -aH \\ 0 & \text{otherwise} \end{cases}.$$

Consequently,

$$E(a,0) = \frac{|0H|}{|aH|} \sum_{b \in \mathcal{C}} A_b D(a,b,0) = \frac{1}{|aH|}(A_{-a}|-aH|) = A_{-a}.$$

For the second part notice that

$$E^2(a,0) = \sum_{c \in \mathcal{C}} E(a,c)E(c,0) = \sum_{c \in \mathcal{C}} \sum_{b \in \mathcal{C}} A_b A_{-c} T(a,b,c)$$

by the first part of this proposition and Propostion 2.17. Consequently,

$$\begin{aligned} E^2(a,0) &= \sum_{c \in \mathcal{C}} \sum_{b \in \mathcal{C}} A_b A_{-c} T(a,b,c) = \sum_{c \in \mathcal{C}} \sum_{b \in \mathcal{C}} A_b A_{-c} ST_a(b,-c) \\ &= \sum_{c \in \mathcal{C}} \sum_{b \in \mathcal{C}} A_b ST_a(b,c) A_c = v^T ST_a v = Q_a(v). \end{aligned}$$

■

Lemma 3.6. $Q_a(j) = d$.

Proof: First notice that the b^{th} entry of $ST_a j$ is

$$\begin{aligned} (ST_a j)_b &= \sum_{c \in \mathcal{C}} ST_a(b,c) = \sum_{c \in \mathcal{C}} T(a,b,-c) = \sum_{c \in \mathcal{C}} T(a,b,c) \\ &= \sum_{c \in \mathcal{C}} |(a + bH) \cap cH| = |a + bH| = |bH|. \end{aligned}$$

Hence,

$$Q_a(j) = j^T ST_a j = \sum_{b \in \mathcal{C}} (ST_a j)_b = \sum_{b \in \mathcal{C}} |bH| = d.$$

■

Now consider the case when $d = 2^k - 1$ for some positive interger k. It is easy to see that $e = k$ in this case.

Proposition 3.7. $v = [(-1)^{tr(\alpha^b)}]_{b \in \mathcal{C}}$.

Proof:

$$A_b = \sum_{i=0}^{[(2^e-1)/d]-1} (-1)^{tr(\alpha^{b+di})} = \sum_{i=0}^{0} (-1)^{tr(\alpha^{b+di})} = (-1)^{tr(\alpha^b)}.$$

■

Write $v = j + 2v_1$, where $v_1 = [-tr(\alpha^b)]_{b\in\mathcal{C}}$. Further, set $\mathcal{C}_0 = \{c \in \mathcal{C} : tr(\alpha^c) = 0\}$ and $\mathcal{C}_1 = \{c \in \mathcal{C} : tr(\alpha^c) = 1\}$.

Theorem 3.8. *The first column of E^2 becomes:*

$$E^2(a,0) = 4(|L_0^{-1} \cap Ker\Psi_{\alpha^{-a}}| - 2^{k-2}) + 3.$$

Proof:

$$E^2(a,0) = Q_a(v) = Q_a(j+2v_1) = Q_a(j) + 4B_a(j,v_1) + 4Q_a(v_1)$$

$$= d + 4(j^T ST_a v_1 + v_1^T ST_a v_1) = d + 4((j^T + v_1^T)ST_a v_1) \qquad (*)$$

where we have used Lemma 3.6 for the fourth equality above. Now $j^T + v_1^T = [1 - tr(\alpha^b)]_{b\in\mathcal{C}}$ and

$$1 - tr(\alpha^b) = \begin{cases} 0 & \text{if } tr(\alpha^b) = 1 \\ 1 & \text{if } tr(\alpha^b) = 0 \end{cases}$$

hence

$$(j^T + v_1^T)ST_a = [\sum_{b\in\mathcal{C}_0} ST_a(b,c)]_{c\in\mathcal{C}}$$

and

$$(j^T + v_1^T)ST_a v_1 = -\sum_{c\in\mathcal{C}_1}\sum_{b\in\mathcal{C}_0} ST_a(b,c) = \sum_{c\in\mathcal{C}_1}\sum_{b\in\mathcal{C}_0} |(a+bH)\cap -cH|$$

$$= |\{bh : tr(\alpha^b) = 0, a + bh \in -cH \text{ for some } c \text{ with } tr(\alpha^c) = 1\}|$$
$$= |\{\beta \in L_0^* : \alpha^{-a}\beta^{-1} = \gamma \text{ for some } \gamma \notin L_0\}| = |\{\beta \in L_0^* : tr(\alpha^{-a}\beta^{-1}) = 1\}|$$
$$= 2^{k-1} - 1 - |\{\beta \in L_0^* : tr(\alpha^{-a}\beta^{-1}) = 0\}|$$
$$= 2^{k-1} - 1 - |L_0^{-1} \cap Ker\Psi_{\alpha^{-a}}|. \qquad (**)$$

Combining (*) and (**) we obtain

$$\begin{aligned} E^2(a,0) &= d - 4(2^{k-1} - |L_0^{-1} \cap Ker\Psi_{\alpha^{-a}}| - 1) \\ &= 2^k - 1 - 2^{k+1} + 4|L_0^{-1} \cap Ker\Psi_{\alpha^{-a}}| + 4 \\ &= -2^k + 4|L_0^{-1} \cap Ker\Psi_{\alpha^{-a}}| + 3 \\ &= 4(|L_0^{-1} \cap Ker\Psi_{\alpha^{-a}}| - 2^{k-2}) + 3. \end{aligned}$$

■

Theorem 3.9. *Let $c(x)$ be an irreducible polynomial over $\mathbb{F}_2$ of degree $2k$ and order 2^k+1. The minimal weight of the irreducible code $\mathbf{C}$ based on $c(x)$ is no smaller than the ceiling of $2^{k-1} - 2^{k/2} + 1/2$.*

Proof: From Theorem 2.14, we have that the non-zero weights of $\mathbf{C}$ are given by $\frac{1}{2d}(2^{se}j - E^s v_0)$. Using Corollary 2.19 and Theorem 3.8 we obtain

$$\begin{aligned} \frac{1}{2d}(2^{se}j - E^s v_0) &= \frac{1}{2d}(2^{2k}j + d[E^2(a,0)]_{a\in\mathcal{C}} - j) = \frac{1}{2}((2^k+1)j + [E^2(a,0)]_{a\in\mathcal{C}}) \\ &= [\frac{1}{2}(2^k + 1 + 4|L_0^{-1} \cap Ker\Psi_{\alpha^{-a}}| - 2^k + 3)]_{a\in\mathcal{C}} \\ &= [2 + 2|L_0^{-1} \cap Ker\Psi_{\alpha^{-a}}|]_{a\in\mathcal{C}}. \end{aligned}$$

Hence, the minimal weight of $\mathbf{C}$ is $2(|L_0^{-1} \cap Ker\Psi_\beta| + 1)$, for some $\beta \in L^*$. But by Proposition 3.4, $2(|L_0^{-1} \cap Ker\Psi_\beta| + 1) \geq 2(\frac{1}{4}(2^e - 3 - 2\sqrt{2^e}) + 1) = \frac{1}{2}2^e - \sqrt{2^e} + \frac{1}{2} = 2^{k-1} - 2^{k/2} + \frac{1}{2}$. Since the minimal weight is an integer, the result follows.

■

Let B be the ceiling of $2^{k-1} - 2^{k/2} + 1/2$. We have computed the exact minimal weight of $\mathbf{C}$ for $k = 2, \ldots, 10$. For $k = 3, 5, 7, 9$, the minimal weight is B. For $k = 2, 4, 6, 8, 10$, the minimal weight is $B + 1$. Hence, we make the following

Conjecture: The minimal weight of $\mathbf{C}$ is

$$\begin{cases} B & \text{if } k \text{ is odd} \\ B+1 & \text{if } k \text{ is even} \end{cases}.$$

4 Other Applications

A kth order linear recurrence

$$(s) \qquad s_{m+k} = a_{k-1}s_{m+k-1} + \cdots + a_1 s_{m+1} a_0 s_m$$

(each $a_i \in \mathbb{F}_2$) together with a vector of initial values $I = (s_0, s_1, \ldots, s_{k-1})$ determine an infinite sequence (s, I). We assume that the characteristic polynomial $c(x)$ of (s) is irreducible. Then (s, I) is periodic with period $n = \mathrm{ord}(c(x))$. We denote the terms of one period by $\pi(s, I)$.

Let $m(x)$ be the reciprocal of $c(x)$ and let $\mathbf{C}$ be the irreducible code generated by $(x^n - 1)/m(x)$. Then the codewords of $\mathbf{C}$ are precisely the periods $\pi(s, I)$ as I runs over $\mathbb{F}_2^k$, a result that goes back at least to [1] and can be found in [8], p. 485. We get immediately:

Theorem 4.1. *Let (s) be an irreducible linear recurrence of order se and period $n = (2^{se} - 1)/d$ and let I be a non-zero vector of intial values. Then the number of occurrences of 0 in one period of (s, I) is $n - \alpha$, where α is a non-zero weight of $\mathbf{C}$.*

Remark: [8] has bounds on $Z_s(0)$, the number of zeros in one period of (s), namely,

$$\left| Z_s(0) - \frac{(2^{se-1} - 1)n}{2^k - 1} \right| \leq \frac{1}{2}(1 - \frac{n}{2^{se} - 1})2^{se/2}.$$

This bound is excellent in the sense that both the upper and lower bounds are achieved. However, relatively few of the values in this range arise as $Z_s(0)$.

Example 2: Suppose $se = 10$ and $n = 341$. Then $d = 3, e = 2$ and $s = 5$. By Theorem 2.22, the non-zero weights of $\mathbf{C}$ are 176 and 160. Then by Theorem 4.1, $Z_s(0)$ is 165 or 181. Compare this with the bound from [8], which gives

$$159.7 \leq Z_s(0) \leq 181.$$

Of the 22 values in this range, only two can occur as $Z_s(0)$. In fact, both values of 165, 181 do occur. For

$$c(x) = x^{10} + x^3 + x^2 + x + 1$$

(which is irreducible of order 341) we get $Z_s(0) = 165$. And for

$$c(x) = x^{10} + x^4 + x^3 + x^2 + 1$$

(also irreducible of order 341) we get $Z_s(0) = 181$.

Now we consider diagonal equations. Let N denote the number of solution in K to the diagonal equation

$$\sum_{i=1}^{s} x_i^d = 0.$$

In [16] and [17], Wolfman gives a direct connection between diagonal equations and irreducible codes. His result may be stated as:

Theorem 4.2. *Let $c(x)$ be an irreducible polynomial over $\mathbb{F}_2$ of degree se and order $n = (2^{se} - 1)/d$. Further, let $\mathbf{C}$ be the irreducible code based on $c(x)$ and let n_i be the number of codewords in $\mathbf{C}$ of weight i. Then*

$$N = \frac{1}{2^{se}} \sum_{i=0}^{n} n_i (2^{se} - 2di)^s.$$

Example 3: From Example 1 we see that the number of solutions in $\mathbb{F}_{2^{16}}$ to the equation

$$x_1^{51} + x_2^{51}$$

is then

$$\begin{aligned} &\frac{1}{2^{16}}[1285(2^{16} - 102 \cdot 704)^2 + 10280(2^{16} - 102 \cdot 664)^2 \\ &+10280(2^{16} - 102 \cdot 648)^2 + 10280(2^{16} - 102 \cdot 632)^2 \\ &+20560(2^{16} - 102 \cdot 640)^2 + 2570(2^{16} - 102 \cdot 672)^2 \\ &+10280(2^{16} - 102 \cdot 616)^2] = 3276750, \end{aligned}$$

and the number of solutuions in $\mathbb{F}_{2^{24}}$ to the equation

$$x_1^{51} + x_2^{51} + x_3^{51}$$

is 25735845156840.

References

[1] N. M. Abramson, *Error-correcting codes from linear sequential circuits*, 1961 Information Theory (Symposium, London, 1960) Butterworths, Washington DC, 22-40.

[2] L. D. Baumert and R. J. McEliece, *Weights of irreducible codes*, Information and Control **20** (1972), 158-175.

[3] L. D. Baumert and J. Mykkelveit, *Weight distribution of some irreducible cyclic codes*, D.S.N. Report **16** (1973), 128-131.

[4] P. Delsarte and J.-M. Goethals, *Irreducible binary codes of even dimension*, 1970 Proc. Second Chapel Hill Conf. on Combinatorial Mathematics and its Applications, Univ. North Carolina, Chapel Hill, NC,(1970), 100-113.

[5] H. Hasse and H. Davenport, *Die Nullstellen der Konguenzzetafunktion in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 151-182.

[6] L. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory (second edition)*, Graduate Texts in Math. **84** , Springer-Verlag, New York/Berlin 1992.

[7] P. Langevin, *Calculs de certaines sommes de Gauss*, J. Number Theory **63** (1997), 59-64.

[8] R. Lidl and H. Niederreiter, *Finite Fields (second edition)*, Encyclopedia of Mathematics **20** , Cambridge University Press, Cambridge, 1997.

[9] J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, Amsterdam/New York, 1977.

[10] R. J. McEliece, *On periodic sequences from GF(q)*, J. Combinatorial Theory Ser. A **10** (1971), 80-91.

[11] R. J. McEliece, *Irreducible cyclic codes and Gauss sums*, Math Centre Tracts **55** (1974), 179-196.

[12] R. J. McEliece and H. Rumsey, Jr., *Euler products, cyclotomy and coding*, J. Number Theory **4** (1972), 302-311.

[13] H. Niederreiter, *An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary field*, AAECC **1** (1990), 119-124.

[14] M. Van Der Vlugt, *Hasse-Davenport curves, Gauss sums and weight distributions of irreducible cyclic codes*, J. Number Theory **55** (1995), 145-159.

[15] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. **83** , Springer-Verlag, New York, 1980.

[16] J. Wolfmann, *The number of solutions of certain diagonal equations over finite fields*, J. Number Theory **42** (1992), 247-257.

[17] J. Wolfmann, *New results on diagonal equations over finite fields from cyclic codes*, Finite Fields: Theory, Applications and Algorithms (Las Vegas, NV 1993), Contemp. Math. **168** Amer. Math. Soc., Providence, RI, 1994, 387-395.

Department of Mathematics, Southern Illinois University, Carbondale, IL 62901, Email: rfitzg@math.siu.edu, jyucas@math.siu.edu