All Two-Weight Irreducible Cyclic Codes?

Bernhard Schmidt
Mathematisches Institut
Universität Augsburg
Universitätsstasse 15
86135 Augsburg
Germany
email: schmidt@math.uni-augsburg.de

and

Clinton White
Department of Mathematics
California Institute of Technology
Pasadena, CA 91125
email: cwhite@its.caltech.edu

Proposed running head:
Two-weight irreducible cyclic codes

Mailing address:

Clinton White
Department of Mathematics, 253-37
California Institute of Technology
Pasadena, CA 91125
email: cwhite@its.caltech.edu
fax: (626) 585-1728

Abstract

The aim of this paper is the classification of two-weight irreducible cyclic codes. Using Fourier transforms and Gauss sums, we obtain necessary and sufficient numerical conditions for an irreducible cyclic code to have at most two weights. This gives a unified explanation for all two-weight irreducible cyclic codes and allows a conjecturally complete classification. Aside from the two known infinite families of two-weight irreducible cyclic codes, a computer search reveals eleven sporadic examples. We conjecture that these are already all two-weight irreducible cyclic codes and give a partial proof of our conjecture conditionally on GRH.

1991 Mathematics Subject Classification: 51E20 (primary), 11L03 (secondary). *Key words and phrases*: irreducible cyclic codes, Gauss sums, Stickelberger's theorem, class numbers, generalized Riemann hypothesis.

1 Introduction

The determination of the weight distribution of irreducible cyclic codes is a fascinating problem which can be tackled by an interplay of number theoretic and combinatorial techniques. Important contributions in this direction can be found in [2, 4, 10, 15]. A basic identity due to McEliece shows that the weights of an irreducible cyclic code can be expressed by linear combinations of Gauss sums via the Fourier transform. This makes number theoretic techniques available for the determination of the weights of irreducible cyclic codes. However, McEliece's identity also indicates that this problem is extremely difficult in general since the same is true for the evaluation of Gauss sums.

Even the *two-weight* irreducible cyclic codes have not yet been classified. Two infinite families of two-weight irreducible cyclic codes and seven sporadic examples are known, see Section 4. In our paper, we will give a unified explanation for all these two-weight codes, find four new sporadic examples and provide evidence that there are no further examples.

The main point of our approach is to find "simple" necessary and sufficient numerical conditions for an irreducible cyclic code to have at most two weights. In Section 3, we will derive these conditions without evaluating the corresponding Gauss sums in McEliece's identity; we only need to use the factorization of Gauss sums given by Stickelberger's theorem and Parseval's identity for Fourier transforms. What makes the analysis of our "simple" conditions complicated is that they involve a parameter θ coming from Stickelberger's theorem which behaves as irregularly as class numbers of imaginary quadratic number fields. Nevertheless, we believe we have found *all* two-weight irreducible cyclic codes. The classification is described in detail in Section 4.

In Section 5, we prove the completeness of our classification in some cases by resorting to a class number estimate conditionally on GRH due to Louboutin [12]. We also use recent results on Gauss sums due to Mbodj [14].

Two-weight irreducible cyclic codes can also be studied in terms of two-intersection sets in finite projective spaces and in terms of difference sets. Since these viewpoints are enlightening sometimes, we explain them in Section 6. The two-intersection sets corresponding to the eleven sporadic two-weight codes all have the interesting property that the square of the difference of their intersection numbers is not the order of the underlying geometry. Examples of such sets are rare and have received some recent interest.

Turning to the difference set interpretation, we arrive at the most elegant way to phrase our results: subject to our conjecture, there are exactly eleven sub-difference sets of Singer difference sets which are neither trivial nor another Singer difference set. We will identify these eleven examples among the known difference sets.

Some background material on irreducible cyclic codes and Gauss sums will be given in the next section. The necessary results of Fourier analysis on finite abelian groups are appended in Section 7 for the convenience of the reader.

2 Background

We begin with the definition of irreducible cyclic codes. We first give the usual definition and then switch to an alternative which is more useful for our purposes. For the necessary coding terminology, see [19].

Definition 2.1 *Let f be an irreducible divisor of $x^n - 1$ over $GF(q)$ where $(q, n) = 1$. The cyclic code of length n over $GF(q)$ generated by $(x^n - 1)/f$ is called a* **minimal cyclic code** *or an* **irreducible cyclic code**.

The following definition is narrower, but essentially equivalent to Definition 2.1, see Remark 2.3 below.

Definition 2.2 *Let L/K be an extension of finite fields of degree m where K has order q. Let n be a divisor of $q^m - 1$, write $u = (q^m - 1)/n$, and let ω be a primitive nth root of unity in L. Then*

$$c(q, m, u) := \left\{ c(y) := \Big(Tr_{L/K}(y\omega^i) \Big)_{i=0}^{n-1} \;\middle|\; y \in L \right\}.$$

is called an **irreducible cyclic code** *over K.*

We note that the dimension of $c(q, m, u)$ is $\mathrm{ord}_n(q)$, cf. [19, Thm. 6.3.1].

Remark 2.3 If we allowed ω to be an arbitrary nth root of unity in Definition 2.2, then by the argument of [19, Thm. 6.5.1], the two definitions above would be equivalent. However, in the case where ω is a non-primitive nth root of unity, the codewords of $c(q, m, u)$ are periodic with period $\mathrm{ord}(\omega)$. Thus it suffices to consider the case where ω is a *primitive* nth root of unity.

Definition 2.4 *Let $w(y)$ denote the Hamming weight of $c(y) \in c(q,m,u)$. If w takes at most two nonzero values, we call $c(q,m,u)$ a* **two-weight irreducible cyclic code**.

For a description of all known two-weight irreducible cyclic codes, see Section 4. We first show that we can restrict our attention to the case where $q-1$ divides n.

Lemma 2.5

(a) Write $u' = u(q-1,n)/(q-1)$ and $n' = n(q-1)/(q-1,n)$. The code $c(q,m,u)$ is a two-weight code if and only if $c(q,m,u')$ is a two-weight code.

(b) If $q-1$ divides n, then $q-1$ divides all weights of $c(q,m,u)$.

Proof (a) Any primitive n' root of unity is product of a primitive nth root of unity and an element of K^*. Thus, because of the K-linearity of the trace, the weights of the words of $c(q,m,u')$ differ just by the constant factor $(q-1)/(q-1,n)$.
(b) Also follows from the K-linearity of the trace. □

An identity of McEliece [15] expresses the weights of irreducible cyclic codes as linear combinations of Gauss sums. Before we state it, we recall the definition of Gauss sums and their most basic property. For a proof, see [11, Thm. 5.11]. We use the notation $\xi_t = e^{2\pi i/t}$.

Definition 2.6 *Let $r = p^a$ be a prime power, $F = GF(r)$, and let χ be a character of F^*. We define*

$$G_F(\chi) := \sum_{x \in F} \chi(x) \xi_p^{Tr(x)}$$

where Tr denotes the absolute trace map from F to $GF(p)$.

Lemma 2.7 *If χ is nontrivial, then*

$$|G_F(\chi)|^2 = r.$$

Now we are ready to state McEliece's identity from [15]. For the convenience of the reader, we give a proof.

Lemma 2.8 (McEliece) *Let L/K be an extension of finite fields of degree m where $K = GF(q)$. Let u be a divisor of $(q^m - 1)/(q - 1)$ and $n := (q^m - 1)/u$. Let U be the subgroup of L^* of index u and let Γ be the subgroup of characters of L^* which are trivial on U. For $a \in L^*$, the weight of the codeword $c(a) \in c(q, m, u)$ is given by*

$$w(a) = \frac{q-1}{qu}\Big(q^m - \sum_{\chi \in \Gamma \setminus \{1\}} G_L(\chi)\overline{\chi}(a)\Big); \tag{1}$$

for $\chi \in \Gamma \setminus \{1\}$,

$$G_L(\chi) = \frac{-q}{q-1} \sum_{a \in L^*/U} w(a)\chi(a). \tag{2}$$

Proof We only need to prove (2) and calculate $\sum_{a \in L^*/U} w(a)$ since (1) then follows by Fourier inversion, see Lemma 7.3 of the Appendix. We define $R_a := \{x \in U : \mathrm{Tr}_{L/K}(ax) = 0\}$. Note $|R_a| = n - w(a)$ and

$$\sum_{a \in L^*/U} |R_a| = |\{y \in L^* : \mathrm{Tr}_{L/K}(y) = 0\}| = q^{m-1} - 1,$$

so $\sum_{a \in L^*/V} w(a) = (q-1)q^{m-1}$. Using Lemma 7.1 of the Appendix, we get

$$\begin{aligned}
G_L(\chi) &= \sum_{x \in L^*} \chi(x)\xi_p^{\mathrm{Tr}(x)} \\
&= \sum_{a \in L^*/U} \chi(a) \sum_{x \in U} \xi_p^{\mathrm{Tr}(ax)} \\
&= \sum_{a \in L^*/U} \chi(a)\Big((n - w(a)) + \sum_{x \in U \setminus R_a} \xi_p^{\mathrm{Tr}(ax)}\Big) \\
&= \sum_{a \in L^*/U} \chi(a)\Big(- w(a) + \frac{w(a)}{q-1} \cdot (-1)\Big) \\
&= \frac{-q}{q-1} \sum_{a \in L^*/U} w(a)\chi(a)
\end{aligned}$$

□

Corollary 2.9 *Let q, m, u, n be as in Lemma 2.8, and write $q = p^t$ where p is a prime. Then $c(q, m, u)$ is a two-weight code if and only if $c(p, mt, u)$ is a two-weight code.*

Proof By (1), the weights of these two codes differ only by the constant factor $(q-1)p/(p-1)q$. $\square$

Remark 2.10 In view of Lemma 2.5 (a) and Corollary 2.9, for the classification of two-weight irreducible cyclic codes $c(q, m, u)$, it is enough to consider the case where q is prime and $q-1$ divides $n = (q^m - 1)/u$.

Now we list some facts on Gauss sums needed later. A well known result of Stickelberger [18] completely determines the factorization of Gauss sums into prime ideals. As a preparation for the formulation of Stickelberger's theorem, we recall the factorization of rational primes in certain cyclotomic fields. A proof of this result can be found in [9, pp. 196-198]. Let φ denote the Euler totient function.

Result 2.11 *Let p be a prime, and $q = p^f$ be a power of p. Then p factors in $\mathbb{Q}(\xi_{q-1})$ as*

$$(p) = \prod_{i=1}^{t} \pi_i$$

where $t = \varphi(q-1)/f$ and the π_i are prime ideals. Furthermore, in $\mathbb{Q}(\xi_{q-1}, \xi_p)$, each π_i is the $(p-1)$th power of a prime ideal.

Now we state Stickelberger's theorem. For a proof, see [20, Prop. 6.13]. For a positive integer x, let $S_p(x)$ denote the sum of the p-digits of x.

Result 2.12 *Let p be a prime, and $q = p^a$ be a power of p. Let π be a prime ideal of $\mathbb{Q}(\xi_{q-1})$ above p, let $\tilde{\pi}$ be the prime ideal of $\mathbb{Q}(\xi_{q-1}, \xi_p)$ above π. By $\nu_{\tilde{\pi}}$ we denote the $\tilde{\pi}$-adic evaluation. Let $\omega = \omega(\pi)$ be the Teichmüller character of $\mathbb{F}_q^*$ corresponding to π (see* [20, p. 96] *for the definition of ω). Then*

$$\nu_{\tilde{\pi}}(G(\omega^j)) = S_p(j)$$

for $1 \le j < q-1$.

We will also need the Davenport-Hasse Theorem, see [11, Thm. 5.14], which we recall in the following.

Result 2.13 *Let r be a prime power and let E be an extension field of $F = GF(r)$ of degree s. Let χ be a character of F^* and define a character χ' of E^* by $\chi'(x) = \chi(\mathrm{N}_{E/F}(x))$ where $\mathrm{N}_{E/F}$ denotes the norm function of E relative to F. Then*

$$G_E(\chi') = (-1)^{s-1} G_F(\chi)^s.$$

Corollary 2.14 *Let p be a prime u be a positive integer with $(u, p) = 1$. Write $f := ord_u(p)$. Define*

$$\theta(u,p) := \frac{1}{p-1} \min\{S_p(\tfrac{j(p^f-1)}{u}) : 1 \le j < u\}.$$

Let s be a positive integer. If u divides $(p^{sf}-1)/(p-1)$, then $p^{s\theta(u,p)}$ is the largest p-power dividing $G(\chi)$ for every nontrivial character χ of $GF(p^{sf})^*$ such that χ^u is trivial.

Proof By (2), we have $G(\chi) \in Z[\xi_u]$. Thus Stickelberger's theorem and Result 2.11 imply that $\theta(u,p)$ is an integer. Now the assertion follows from Stickelberger's theorem together with the Davenport-Hasse theorem. □

3 The main result

We now state and prove the necessary and sufficient numerical conditions on the parameters of an irreducible cyclic code to have at most two nonzero weights. In view of Remark 2.10, it suffices to consider the codes $c(p, m, u)$ where p is a prime and u divides $(p^m - 1)/(p - 1)$.

Theorem 3.1 *Let p be a prime, and let u, m be positive integers such that u divides $(p^m - 1)/(p - 1)$. Write $\theta = \theta(u, p)$ and $m = fs$ with $f := ord_u(p)$. Then $c(p, m, u)$ is a two-weight code if and only if there exists a positive integer k satisfying*

$$\left.\begin{array}{l} k \mid u-1 \\ kp^{s\theta} \equiv \pm 1 (\mathrm{mod}\ u) \\ k(u-k) = (u-1)p^{s(f-2\theta)} \end{array}\right\} \quad (3)$$

Proof L denotes $\mathrm{GF}(p^m)$. Let U be the subgroup of L^* of index u and let Γ be the subgroup of characters of L^* which are trivial on U. Let $G = L^*/U$.

Necessity. Define $\nu(a) = p(w(a) - w(1))/(p-1)$. Note that we may consider ν as a function on G and also that Γ is isomorphic to the character group of G. Calculate the Fourier transform of ν:

$$\hat{\nu}(\chi) = \begin{cases} \frac{1}{\sqrt{u}} G(\chi) & \text{if } \chi \neq 1, \\ \frac{p^{sf}}{\sqrt{u}} - \frac{p\sqrt{u}\ w(1)}{p-1} & \text{if } \chi = 1. \end{cases}$$

The latter uses the fact that $\sum_{a \in G} w(a) = (p-1)p^{sf-1}$. If $c(p, fs, u)$ has at most two weights, then $\nu(a) \in \{0, \delta\}$ for some nonzero integer δ. By Lemmas 2.7 and 2.8 and Proposition 2.14 it follows that $\delta = \pm p^{s\theta}$. Now define $D = \{a \in G \mid \nu(a) = \delta\}$ and $d = |D|$. Then

$$\hat{\nu}(1) = \frac{1}{\sqrt{u}} \sum_{a \in G} \nu(a) = \frac{\pm d p^{s\theta}}{\sqrt{u}}.$$

Compare with the previous expression for $\hat{\nu}(1)$ to obtain

$$dp^{s\theta} \equiv \pm 1 (\mathrm{mod}\ u).$$

Finally, from the Parseval identity we have

$$udp^{2s\theta} = d^2 p^{2s\theta} + (u-1)p^{sf},$$

or $d(u-d) = (u-1)p^{s(f-2\theta)}$. If $f = 2\theta$ then take $k = u - 1$. Otherwise p divides exactly one of d and $u - d$, and thus the other divides $u - 1$. Let k equal the latter.

Sufficiency. Let

$$x = \frac{(p-1)p^{s\theta-1}(p^{s(f-\theta)} - \varepsilon k)}{u},$$

where $\varepsilon = \pm 1$ is determined by $kp^{s\theta} \equiv \varepsilon (\mathrm{mod}\ u)$. Define

$$\gamma(a) = \frac{w(a) - x}{(p-1)p^{s\theta-1}}.$$

Note that γ is integer-valued as $(p-1)p^{s\theta-1}$ divides $w(a)$ for every $a \in G$ and u divides $\varepsilon k - p^{s(f-\theta)}$.

Since $\sum_{a\in G} w(a) = (p-1)p^{sf-1}$, then $\sum_{a\in G}\gamma(a) = \varepsilon k$. Also,

$$\hat{\gamma}(\chi) = \begin{cases} \varepsilon k u^{-\frac{1}{2}} & \text{if } \chi = 1 \\ p^{-s\theta}u^{-\frac{1}{2}}G(\chi) & \text{if } \chi \neq 1 \end{cases}$$

Applying the Parseval identity we obtain,

$$\sum_{a\in G}\gamma(a)^2 = \frac{k^2}{u} + \frac{u-1}{u}p^{s(f-2\theta)}.$$

Since $k(u-k) = (u-1)p^{s(f-2\theta)}$, it follows that $\sum_{a\in G}\gamma(a)^2 = k$. Therefore $\gamma(a) \in \{0, \varepsilon\}$ for every $a \in G$ and hence the weight function w is two-valued. □

Corollary 3.2 *Suppose the irreducible cyclic code $c(p, fs, u)$ has at most two weights and let k, ε be as in Theorem* 3.1. *Then these weights are*

$$w_1 = (p-1)p^{s\theta-1}(p^{s(f-\theta)} - \varepsilon k)/u,$$
$$w_2 = w_1 + \varepsilon(p-1)p^{s\theta-1}.$$

4 All two-weight irreducible cyclic codes?

Using Theorem 3.1 we can attempt to classify all two-weight irreducible cyclic codes by finding all solutions to (3). In the following, we only consider codes $c(p, m, u)$ with p prime, see Remark 2.10.

4.1 Subfield and semiprimitive codes

There are two known infinite families of two-weight irreducible cyclic codes: the subfield codes and the semiprimitive codes. We now describe the corresponding solutions of (3). We use the notation of Definition 2.2. The most obvious two-weight codes $c(p, m, u)$ arise if ω generates a subfield of L.

Proposition 4.1 *If ω is a primitive element for a subfield $F \cong GF(p^a)$ of $L = GF(p^m)$, then $c(p, m, u)$ has only one nonzero weight.*

Proof Let $y \in L^*$. If $\mathrm{Tr}_{L/F}(y) = 0$, then $\mathrm{Tr}_{L/K}(y\omega^i) = 0$ for all i. If $\mathrm{Tr}_{L/F}(y) \neq 0$, then $\{\omega^i : \mathrm{Tr}_{L/K}(y\omega^i) = 0\} \cup \{0\}$ is a K-vector space of dimension $a-1$. Thus the only nonzero weight of $c(p, m, u)$ is $p^a - p^{a-1}$. □

We call the codes appearing in Proposition 4.1 **subfield codes**. From the proofs of Theorem 3.1 and Proposition 4.1 we see that $k = (p^{m-a}-1)/(p^a-1)$ in (3) and thus $\theta(u,p) = a$ for a subfield code $c(p,m,u)$. Thus we have the following.

Proposition 4.2 *The subfield codes $c(p,m,u)$ exactly correspond to the solutions of (3) of the form*

$$\begin{aligned} u &= (p^m-1)/(p^a-1) \\ k &= (p^{m-a}-1)/(p^a-1) \\ s &= 1. \end{aligned}$$

Now we come to the semiprimitive codes. A prime p is called **semiprimitive** modulo u if -1 is power of p modulo u. Note that (3) has a solution with $k \in \{1, u-1\}$ if and only if $\theta(u,p) = f/2$. By [3, Thms. 1,4], we have $\theta(u,p) = f/2$ if and only if p is semiprimitive modulo u. Thus we have the following.

Proposition 4.3 *There is a solution of (3) with $k \in \{1, u-1\}$ if and only if p is semiprimitive modulo u. The corresponding two-weight codes $c(p,m,u)$ are called* **semiprimitive codes**.

4.2 The exceptional codes

Two-weight irreducible cyclic irreducible codes which are neither subfield nor semiprimitive codes will be called **exceptional**. The corresponding solutions of (3) will also be called **exceptional**. Theorem 3.1 makes possible a computer search for exceptional codes. This can be done as follows. For every proper divisor $k > 1$ of $u-1$ compute $k(u-k)/(u-1)$. If it is a prime power, say p^r, check whether $f - 2\theta$ divides r. If so and the quotient is s, then as long as the congruence condition of (3) holds, $c(p, fs, u)$ is a two-weight irreducible cyclic code. The following table lists all exceptional solutions of (3) with $u \leq 100,000$.

u	p	s	f	θ	k	ε
11	3	1	5	2	5	$+1$
19	5	1	9	4	9	$+1$
35	3	1	12	5	17	$+1$
37	7	1	9	4	9	$+1$
43	11	1	7	3	21	$+1$
67	17	1	33	16	33	$+1$
107	3	1	53	25	53	$+1$
133	5	1	18	8	33	-1
163	41	1	81	40	81	$+1$
323	3	1	144	70	161	$+1$
499	5	1	249	123	249	$+1$

The two-weight codes from above with $u \in \{11, 19, 67, 107, 163, 499\}$ were already found by Langevin [10]. His proof relies on the fact that the Gauss sums in McEliece's indentity can be evaluated if u is prime and $f = (u-1)/2$. Batten and Dover [1] verified by computer that $c(7, 9, 37)$ is a two-weight code. The result in [1] is presented as a certain two-intersection set in $\mathrm{PG}(2, 7^3)$; see Section 6 for more on the correspondence between two-weight codes and two-intersection sets. We believe that $c(3, 12, 35)$, $c(11, 7, 43)$, $c(5, 18, 133)$ and $c(3, 144, 323)$ are new two-weight codes.

The fact that there are no exceptional solutions with $500 \leq u \leq 100,000$ and the results of the next section provide evidence for the following.

Conjecture 4.4 *An irreducible cyclic code $c(p, m, u)$ is a two-weight code if and only if it is a subfield code, a semiprimitive code or appears in the above table of exceptional codes.*

5 Partial proof of Conjecture 4.4

Conditionally on GRH, we give a partial proof of Conjecture 4.4. Again we only consider codes $c(p, m, u)$ with p prime, see Remark 2.10.

One of the tools we will need is a bound on class numbers of imaginary quadratic fields due to Louboutin [12]. Let K be an imaginary quadratic number field, and let $\zeta_K(s)$ denote its Dedekind zeta function, see [6, p. 309]. We recall that the generalized Riemann hypothesis (GRH) for K asserts that $\Re s = 1/2$ for all zeros s of $\zeta_K(s)$ with $0 < \Re s < 1$.

Result 5.1 (Louboutin [12]) *Let d be a square-free positive integer and let $h(-d)$ denote the class number of $K = \mathbb{Q}(\sqrt{-d})$. Assuming GRH for K, we have*

$$h(-d) \geq \frac{\pi\sqrt{d}}{3e\log d}.$$

To prove the following Theorem, we combine Louboutin's bound with work of Baumert and Mykkelveit [4] and recent work of Mbodj [14] on Gauss sums

Theorem 5.2 *Conditionally on GRH, there are no two-weight irreducible cyclic codes $c(p,m,u)$ for which the triple (p,m,u) satisfies any of the following conditions.*

(a) $u \equiv 0 \pmod 3$, $u \neq 3$, $p \equiv 1 \pmod 3$ and

$$m > \frac{3\log((u+1)/4)}{\log p}. \tag{4}$$

(b) There is a prime divisor $r \equiv 3 \pmod 4$ of u with $r > 3$,

$$ord_r(p) = (r-1)/2 \tag{5}$$

and

$$m > \frac{3e(r-1)\log r \log((u+1)/4)}{2\pi\sqrt{r}\log p}. \tag{6}$$

(c) There are two odd prime divisors $r,\ s > 3$ of u such that

$$ord_r(p) = r-1,\, ord_{rs}(p) = (r-1)(s-1)/2 \tag{7}$$

and

$$m > \frac{3e(r-1)(s-1)\log rs \log((u+1)/4)}{2\pi\sqrt{rs}\log p}. \tag{8}$$

Proof (b) Assume that $c(p,m,u)$ is a two-weight code. Write $f = \mathrm{ord}_u(p)$, $m = ft$, $g = (r-1)/2$, and let χ be a character of $\mathrm{GF}(p^g)$ of order r. By [4], the exact power of p dividing the Gauss sum $G(\chi)$ is $p^{(g-h)/2}$ where h is the class number of $\mathbb{Q}(\sqrt{-r})$. Thus, by the Davenport-Hasse theorem and

Corollary 2.14, $2\theta(u,p) \le f - hf/g$. Recall that $k(u-k) = (u-1)p^{t(f-2\theta(u,p))}$ for some divisor k of $u-1$ by Theorem 3.1. Note that $k(u-k)/(u-1) \le (u+1)/4$. Putting this together, we get

$$\frac{u+1}{4} \ge p^{t(f-2\theta(u,p))} \ge p^{mh/g}.$$

Now assertion (b) follows by taking logarithms and using Result 5.1.

The proof of part (c) is similar. If $s \equiv 3 \pmod 4$ and $\mathrm{ord}_s(p) = (s-1)/2$ then the bound from part (b), with s in place of r, implies the bound in (c). Otherwise, we may use Proposition 3.8 of [14] applied to a character of $\mathrm{GF}(p^g)$ of order rs in the estimation of $\theta(u,p)$. Here $g = (r-1)(s-1)/2$. Proceed as in part (b).

To prove (a), note that $s_p(\frac{p^f-1}{3}) = f(p-1)/3$. By Corollary 2.14, $t\theta(u,p) \le m/3$. As in part (b), the result follows by Theorem 3.1. □

Following Mbodj [14], we say that the pair (u,p) falls under the **index 2 case** if u is odd and $\mathrm{ord}_u(p) = \varphi(u)/2$. Note that u can have at most two distinct prime divisors in this case. The corresponding codes $c(p,m,u)$ will be called **index 2 codes**. Index 2 codes are promising candidates for two-weight codes because of the following.

Proposition 5.3 *The number of different nonzero weights of a code $c(p,m,u)$ is at most the number of orbits of $x \mapsto x^p$ on $\mathbb{Z}_u^*$.*

Proof The weight of a codeword $c(y)$ only depends on the coset $\langle\omega\rangle y$. This implies the assertion since the Frobenius automorphism $y \mapsto y^p$ of $\mathrm{GF}(p^m)$ is trace-preserving. □

In particular, an index 2 code with u prime has at most three different nonzero weights. Note that eight of the eleven exceptional two-weight codes listed in Section 4.2 are index 2 codes. Thus it is desirable to verify Conjecture 4.4 for index 2 codes.

Theorem 5.4 *Conditionally on GRH, Conjecture 4.4 is true for all index 2 codes.*

Proof Let $C = c(p,m,u)$ be a two-weight index 2 code. If C is a semiprimitive code, then there is nothing to show. Thus assume that p is not semiprimitive modulo u. First suppose 3 divides u and $p \equiv 1 \pmod 3$ If $u = 3^a s^b$, for

a prime $s > 3$, then Theorem 5.2 (a) implies

$$3^{a-1}(s-1)s^{b-1} \leq \frac{3\log((u+1)/4)}{\log p}.$$

Hence,

$$\frac{u\log 7}{12} \leq \log\frac{u+1}{4},$$

a contradiction. The case u is a power of 3 is similar and once again there are no admissible values of u by Theorem 5.2(a).

Next suppose that $(u,3)=1$. We claim that

$$\frac{\pi\sqrt{u}\log p}{3e\log u} \leq \log\frac{u+1}{4}. \tag{9}$$

We carry out the proof of (9) only for the case where u has two distinct prime divisors s, r. The case where u is a prime power is similar. Write $u = r^a s^b$ where $a, b \geq 1$. As $\mathrm{ord}_u(p) = \varphi(u)/2$, (5) or (7) holds for the pair (u,p). If (5) holds, then

$$\frac{r^{a-1}s^{b-1}(s-1)}{2} \leq \frac{3e\log r\log(u+1)/4}{2\pi\sqrt{r}\log p}$$

by Theorem 5.2. If (7) holds, then

$$\frac{r^{a-1}s^{b-1}}{2} \leq \frac{3e\log rs\log(u+1)/4}{2\pi\sqrt{rs}\log p}$$

by Theorem 5.2. Each of these implies (9).

Note that (9) implies $u < 86,909$ if $p > 2$. Since the table in Section 5 contains all exceptional codes with $u \leq 100,000$, this shows that Theorem 5.4 is true for $p > 2$. If $p = 2$, then (9) implies $u < 125,383$. A computer search shows that there are no exceptional codes with $p = 2$ in this range. □

6 Two-intersection sets and sub-difference sets

In this section we will discuss the connections between two-weight irreducible cyclic codes, two-intersection sets in finite projective spaces and sub-difference sets of Singer difference sets.

6.1 Two-intersection sets in PG(m − 1, q)

Let $K = \mathrm{GF}(q)$, L an extension of K of degree m, and q a power of a prime p. Consider the model of $\mathrm{PG}(m-1,q)$ in the m-dimensional K-vector space L. Multiplication with elements of L^* induces a cyclic automorphism group $G \cong L^*/K^*$ called the **Singer cycle** acting regularly on the points and hyperplanes of $\mathrm{PG}(m-1,q)$.

Definition 6.1 *A subset X consisting of h points of $PG(m-1,q)$ such that every hyperplane meets X in h_1 or h_2 points is called a* **projective (h, m, h_1, h_2) set**. *Other common terms for X are a* **set of type $(\mathbf{h_1}, \mathbf{h_2})$** *or* **projective two-intersection set**.

It is well-known that projective two-weight codes are equivalent to two-intersection sets in finite projective geometries. We refer the reader to the survey [7] of Calderbank and Kantor for a thorough treatment of this fact, as well as connections to other objects.

The following simple fact establishes the equivalence of two-weight irreducible cyclic codes and certain two-intersection sets. The proof is staightforward and left to the reader.

Proposition 6.2 *Let G be the Singer cycle of $PG(m-1,q)$. Suppose u divides $(q^m-1)/(q-1)$ and let let U be the subgroup of G of index u. Then $c(q,m,u)$ has at most two nonzero weights if and only if each orbit of U on the points of $PG(m-1,q)$ is a two-intersection set.*

Our main theorem gives a necessary and sufficient condition for an orbit of a subgroup of the Singer group of $\mathrm{PG}(m-1,q)$ to be a two-intersection set and thus furnishes a proof for the examples recently found by Dover and Batten [1] in $\mathrm{PG}(2,5^3)$ and $\mathrm{PG}(2,7^3)$. Those two examples appear on our list of exceptional solutions as $u = 19$ and $u = 37$, respectively.

The problem of finding two-intersection sets in projective planes has received special attention. Until recently, all known examples of sets of type (h_1, h_2) in projective planes (except those with $h_i = 1$ or $h_i = q+1$) had the property that $(h_1 - h_2)^2 = q$, the order of the plane. In particular, these planes all had square order. The examples of Batten and Dover are interesting in that they do not share this property. In fact none of the exceptional two-intersection sets has the property that the square of the difference of the intersection numbers equals the order of the underlying geometry.

6.2 Sub-difference sets of Singer difference sets

A third point of view for the question we have all along been considering is that of difference sets and we include here a few remarks on the problem in this context.

Recall that a $(\mathbf{v}, \mathbf{k}, \lambda)$-**difference set** in a finite group G of order v is a k-subset D of G such that every element $g \neq 1$ of G has exactly λ representations $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. The parameter $k - \lambda$ is called the order of D. For a detailed treatment of difference sets, see [5].

Let L, K, G be as before. It is well-known that $H_0 = \{K^* x \mid \mathrm{Tr}(x) = 0\}$ is a difference set in G with parameters

$$(v, k, \lambda) = \left(\frac{q^m - 1}{q - 1}, \frac{q^{m-1} - 1}{q - 1}, \frac{q^{m-2} - 1}{q - 1} \right),$$

called the **Singer** or **trace zero** difference set.

The following observation is basically due to McFarland [16].

Proposition 6.3 *Let D be a (v, k, λ)-difference set in a group G, and let N be a normal subgroup of G. If $|D \cap Ng| \in \{a, b\}$ for some nonnegative integers a, b and all $g \in G$, then*

$$E := \{Ng : |D \cap Ng| = a\}$$

is a difference set in G/N

In the situation of Proposition 6.3, we will call E a **sub-difference set** of D in G/N. It is straightforward to prove the following.

Corollary 6.4 *Let q be a power of a prime p, let G be the Singer cycle of $\mathrm{PG}(m-1, q)$ and let $H_0 \subset G$ be the Singer difference set. The point orbits of a subgroup V of G are projective two-intersection sets in $\mathrm{PG}(m-1, q)$ if and only if H_0 has a sub-difference set E in G/V. Furthermore, p is a multiplier of E.*

We conclude this section by identifying the sub-difference sets corresponding to the known two-weight irreducible cyclic codes among the known difference sets. We find it remarkable that not less than five different types of difference sets correspond to the eleven exceptional codes, see the table below.

From the proof of Theorem 3.1, we have that E is a (u, k, λ)-difference set in L^*/U, where k comes from equation (3). It follows immediately that the sub-difference sets corresponding to the semi-primitive codes are trivial. Similarly, it is straightforward to check that the sub-difference sets corresponding to the subfield codes are again Singer difference sets.

The following table lists the sub-difference sets corresponding to the known exceptional codes. Each of the difference sets on this list except the $(43, 21, 10)$ Hall difference set is determined up to equivalence by its parameters (u, k, λ) and the condition that it admits p as a multiplier.

u	k	λ	name	p
11	5	2	QR	3
19	9	4	QR	5
35	17	8	Twin	3
37	9	2	4th	7
43	21	10	Hall	11
67	33	16	QR	17
107	53	26	QR	3
133	33	8	Hall Sp.	5
163	81	40	QR	41
323	161	80	Twin	3
499	249	124	QR	5

Here **QR** stands for the quadratic residues modulo u; **Twin** denotes the twin-prime power difference sets due to Stanton and Sprott [17]; **4th** denotes the set of fourth powers modulo u; **Hall Sp.** is the $(133, 33, 8)$ sporadic example found by M. Hall [8].

There are two inequivalent $(43, 21, 10)$ difference sets in $\mathbb{Z}/43\mathbb{Z}$ admitting the multiplier 11, the quadratic residues and the so-called Hall difference set. Note that 19 is a primitive element and $19^6 \equiv 11 (\mathrm{mod}\ 43)$. Let

$$C_i = \{19^{i+6j} \mid j = 0, \ldots, 6\},$$

for $i = 0, \ldots, 5$. The quadratic residues are $QR = C_0 \cup C_2 \cup C_4$ and the Hall difference set is $H = C_0 \cup C_1 \cup C_3$. Pick $y \in C_4$. Consider $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_{43})/\mathbb{Q})$ defined by $\sigma : \xi_{43} \mapsto \xi_{43}^y$. Let $L = \mathrm{GF}(11^7)$ and let χ be a character of L^* of order 43. By (2) and Corollary 3.2,

$$G_L(\chi) = 11^3 \chi(E)$$

where E is a sub-difference set of the Singer difference set in $L^*/\mathrm{GF}(11)^*$. Furthermore, using Result 2.12 one checks that

$$(G_L(\chi))^\sigma \neq (G_L(\chi)).$$

It follows that the E cannot be equivalent to QR and therefore is equivalent to the Hall difference set.

The following is equivalent to Conjecture 4.4.

Conjecture 6.5 *Any nontrivial sub-difference set of a Singer difference set is equivalent either to a Singer difference set or to one of the eleven difference sets in the above table.*

7 Appendix: Fourier analysis

We list some facts about Fourier analysis on finite abelian groups. See [13] for proofs. For an abelian group G, we denote its character group by G^*, and for a subgroup W of G, we write $W^\perp$ for the subgroup of all characters which are trivial on W. We identify G with $(G^*)^*$ by $g \leftrightarrow \tau_g$ where τ_g is the character of G^* with $\tau_g(\chi) = \overline{\chi(g)}$. The following **orthogonality relations** are extremely useful.

Lemma 7.1 *Let G be an abelian group, let U be a subgroup of G, and let W be a subgroup of G^*. Then*
a) $\sum_{g\in U} \chi(g) = 0$ *for all* $\chi \in G^* \setminus U^\perp$ *and*
b) $\sum_{\chi\in W} \chi(g) = 0$ *for all* $g \in G \setminus W^\perp$.

As a consequence of the orthogonality relations, one gets the so-called **Fourier inversion formula**.

Lemma 7.2 *Let G be an abelian group, and let $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$. Then*

$$a_g = \frac{1}{|G|} \sum_{\chi\in G^*} \chi(Ag^{-1})$$

for all $g \in G$.

Sometimes it is convenient to express Lemma 7.2 in terms of *Fourier transforms*. Let G be an abelian group, and let $f : G \to \mathbb{C}$ be a function. The **Fourier transform** $\hat{f} : G^* \to \mathbb{C}$ of f is defined by

$$\hat{f}(\chi) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} f(g)\chi(g).$$

Lemma 7.3 *Let G be an abelian group, and let $f : G \to \mathbb{C}$. Then $\hat{\hat{f}} = f$.*

As a consequence of Lemma 7.2, we get **Parseval's identity**. Note that $\sum_{g \in G} |f(g)|^2$ is the coeffient of 1 in $AA^{(-1)}$ if we let $A = \sum_{g \in G} f(g)g$.

Lemma 7.4 *Let G be an abelian group, and let $f : G \to \mathbb{C}$ be a function. Then*

$$\sum_{g \in G} |f(g)|^2 = \sum_{\chi \in G^*} |\hat{f}(\chi)|^2.$$

Acknowledgement The authors would like to thank the referee for several helpful suggestions and for bringing to our attention the recent work on the index two Gauss sums.

References

[1] L. Batten, J.M. Dover: Some sets of type (m, n) in cubic order planes. Designs, Codes and Cryptography 16 (1999) 211-213.

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

[3] L. D. Baumert, W.H. Mills, R.L. Ward: Uniform cyclotomy. J. Number Theory 14 (1982), 67-82.

[4] L. D. Baumert, J. Mykkelveit: Weight Distribution of Some Irreducible Cyclic Codes. D.S.N. report, vol. 11 (1973), 128-131.

[5] T. Beth, D. Jungnickel, H. Lenz: Design Theory. Cambridge University Press, Cambridge (1986).

[6] Z.I. Borevich, I.R. Shafarevich, "Number Theory," Academic Press, New York/San Francisco/London, 1966.

[7] R. Calderbank, W.M. Kantor: The geometry of two-weight codes. Bull. London Math. Soc. 18 (1986), 97-122.

[8] M. Hall: A survery of difference sets. Proc. Amer. Math. Soc. 7 (1956), 975-986.

[9] K. Ireland, M. Rosen, "A Classical Introduction to Modern Number Theory," Graduate Texts in Math. No. 84. Springer Verlag, Berlin/New York/Heidelberg, 1990.

[10] P. Langevin: A new class of two weight codes. Finite fields and their applications (Glasgow, 1995), 181–187, London Math. Soc. Lecture Note Ser., 233, Cambridge Univ. Press, Cambridge, 1996.

[11] R. Lidl, H. Niederreiter: "Introduction to finite fields and their applications". Revision of the 1986 first edition. Cambridge University Press, Cambridge, 1994.

[12] S. Louboutin: Minorations (sous l'hypothèse de Riemann généralisée) des nombres de classes des corps quadratiques imaginaires. Application. C.R. Acad. Sci. Paris Sr. I Math. 310 (1990), no. 12, 795-800.

[13] H.B. Mann: Addition Theorems. Wiley, New York (1965).

[14] O.D. Mbodj: Quadratic Gauss Sums. Finite Fields and Their Applications 4 (1998), 347-361.

[15] R. J. McEliece: Irreducible cyclic codes and Gauss sums. Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: Theory of designs, finite geometry and coding theory, pp. 179–196. Math. Centre Tracts, No. 55, Math. Centrum, Amsterdam, 1974.

[16] R.L. McFarland: Sub-Difference Sets of Hadamard Difference Sets. J. Combin. Theory A 54 (1990), 112-122.

[17] R.G. Stanton, D.A. Sprott: A family of difference sets. Canadian J. Math. 10 (1958), 73-77.

[18] L. Stickelberger: Über eine Verallgemeinerung der Kreistheilung. Math. Annalen 37 (1890), 321-367.

[19] J. H. van Lint: Coding Theory. Lecture Notes in Mathematics, No. 201. Springer-Verlag, Berlin/Heidelberg/New York, 1971.

[20] L.C. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Math. No. 83. Springer Verlag, Berlin/New York/Heidelberg, 1997.