The lengths of Hermitian Self-Dual Extended Duadic Codes

Lilibeth Dicuangco[*], Pieter Moree[**], Patrick Solé[§]

Abstract

Duadic codes are a class of cyclic codes that generalizes quadratic residue codes from prime to composite lengths. For every prime power q, we characterize integers n such that there is a duadic code of length n over $\mathbb{F}_{q^2}$ with an Hermitian self-dual parity-check extension. We derive asymptotic estimates for the number of such n as well as for the number of lengths for which duadic codes exist.

Keywords: Duadic codes, Splittings.
Mathematics Subject Classification: 11N64, 94B15, 11N37

1 Introduction

Duadic codes are a family of cyclic codes over fields that generalize quadratic residue codes to composite lengths. For a general introduction, see [2], [6] and [15]. It can be determined when an extended duadic code is self-dual for the Euclidean scalar product ([2]). In this work, we study for which n there exist duadic codes over $\mathbb{F}_{q^2}$ of length n the extension of which by a suitable parity-check is self-dual for the Hermitian scalar product $\sum_{i=1}^{n+1} x_i y_i^q$.

First, we characterize the Hermitian self-orthogonal cyclic codes by their defining sets (Theorem 3.6), then the duadic codes (Theorem 4.4). Next, we study under what conditions the extension by a parity-check of a duadic code is Hermitian self-dual (Theorem 4.8). Finally, we derive by elementary means an arithmetic condition bearing on the divisors of n (Theorem 5.7) for the previous situation. This condition was arrived at in [9] using

[*]Mathematics Department, University of the Philippines, Diliman, Quezon City, 1101 Philippines, `ldicuangco@math.upd.edu.ph`

[**]Max-Planck-Institut, Vivatsgasse 7, D-53111 Bonn, Germany, `moree@mpim-bonn.mpg.de`

[§]CNRS, I3S ESSI, BP 145, Route des Colles, 06 903 Sophia Antipolis, France, `sole@essi.fr`

representation theory of groups. In an appendix, we derive asymptotic estimates for x large on $A_q(x)$, the number of integers $\leq x$ that are split by the multiplier μ_{-q}, and on $D_q(x)$, the number of possible lengths $\leq x$ of a duadic code. The proofs are based on analytic number theory.

2 Preliminaries

We assume the reader is familiar with the theory of cyclic codes (see e.g., [1], [2]). Let q be a power of a prime p and let $\mathbb{F}_q$ denote the Galois field with q elements. Let n be a positive integer such that $\gcd(n, q) = 1$. Let $\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - 1)$. We view a cyclic code over $\mathbb{F}_q$ of length n as an ideal in $\mathcal{R}_n$.

Let $0 < s < n$ be a nonnegative integer. Let $C_s = \{s, sq, sq^2, \ldots, sq^{r_s - 1}\}$, where r_s is the smallest positive integer such that $sq^{r_s} \equiv s \pmod{n}$. The coset C_s is called the *q-cyclotomic coset of s modulo n*. The subscript of C_s is usually taken to be the smallest number in the set and is also taken as the coset representative. The distinct q-cyclotomic cosets modulo n partition the set $\{0, 1, 2, \ldots, n-1\}$.

Let α be a primitive nth root of unity in some extension field of $\mathbb{F}_q$. A set $T \subseteq \{0, 1, 2, \ldots, n-1\}$ is called the *defining set* (relative to α) of a cyclic code C whenever $c(x) \in C$ iff $c(\alpha^i) = 0 \ \forall i \in T$. In this paper, we assume implicitly that an nth root of unity has been fixed when talking of defining sets.

A ring element e such that $e^2 = e$ is called an idempotent. Since $\gcd(n, q) = 1$, the ring $\mathcal{R}_n$ is semi-simple. Thus, by invoking the Wedderburn Structure theorems, we can say that each cyclic code in $\mathcal{R}_n$ contains a unique idempotent element which generates the ideal. Alternatively, this fact has also been proven directly in [2, Theorem 4.3.2]. We call this idempotent element the *generating idempotent* (or *idempotent generator*) of the cyclic code.

Let a be an integer such that $\gcd(a, n) = 1$. We define the function μ_a, called a *multiplier*, on $\{0, 1, 2, \cdots, n-1\}$ by $i\mu_a \equiv ia \pmod{n}$. Clearly, μ_a gives a permutation of the coordinate positions of a cyclic code of length n. Note that this is equivalent to the action of μ_a on $\mathcal{R}_n$ by $f(x)\mu_a \equiv f(x^a) \pmod{x^n - 1}$.

If C is a code of length n over $\mathbb{F}_q$, we define a *complement of C* as a code C^c such that $C + C^c = \mathbb{F}_q^n$ and $C \cap C^c = \{\mathbf{0}\}$. In general, a complement of a code is not unique. But it is easy to show that if C is cyclic, then C^c is unique and that it is also cyclic (see e.g., Exercise 243, [2]). In this case, we call C^c *the cyclic complement of C*.

3 Cyclic Codes over $\mathbb{F}_{q^2}$

We now consider cyclic codes over the Galois field $\mathbb{F}_{q^2}$, where q is a power of a prime p. In this case, we note that $\mathcal{R}_n = \mathbb{F}_{q^2}[x]/(x^n - 1)$.

3.1 Idempotents in $\mathcal{R}_n$

Consider the involution $^-$: $z \mapsto z^q$ defined on $\mathbb{F}_{q^2}$. We extend this map component-wise to $\mathbb{F}_{q^2}^n$. For an element $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ in $\mathcal{R}_n$, we set $\overline{a(x)} = a_0^q + a_1^qx + \cdots + a_{n-1}^qx^{n-1}$.

Let C be a code of length n over $\mathbb{F}_{q^2}$. We define the *conjugate of* C to be the code $\overline{C} = \{\overline{\mathbf{c}} \mid \mathbf{c} \in C\}$. It can easily be shown that if C is a cyclic code with generating idempotent $e(x)$, then $\overline{C}$ is also cyclic and its generating idempotent is $\overline{e(x)}$.

Suppose we list all the distinct q^2-cyclotomic cosets modulo n in the following way:

$$C_1, C_2, \ldots, C_k, D_1, D_2, \ldots, D_l, E_1, E_2, \ldots, E_l$$

such that

$$C_i = qC_i \quad \text{for } 1 \le i \le k \qquad \text{and} \qquad E_i = qD_i \quad \text{for } 1 \le i \le l.$$

By Corollary 4.3.15 of [2], an idempotent in $\mathcal{R}_n$ has the form

$$e(x) = \sum_{j=1}^{k} a_j \sum_{i \in C_j} x^i + \sum_{j=1}^{l} b_j \sum_{i \in D_j} x^i + \sum_{j=1}^{l} c_j \sum_{i \in E_j} x^i. \tag{1}$$

Thus,

$$\begin{aligned} e(x) &= e(x)^q \\ &= \sum_{j=1}^{k} a_j^q \sum_{i \in C_j} x^{qi} + \sum_{j=1}^{l} b_j^q \sum_{i \in D_j} x^{qi} + \sum_{j=1}^{l} c_j^q \sum_{i \in E_j} x^{qi} \\ &= \sum_{j=1}^{k} a_j^q \sum_{i \in C_j} x^{i} + \sum_{j=1}^{l} b_j^q \sum_{i \in E_j} x^{i} + \sum_{j=1}^{l} c_j^q \sum_{i \in D_j} x^{i}. \end{aligned}$$

Hence,

$$\begin{aligned} a_j^q &= a_j \quad 1 \le j \le k\,; \\ b_j^q &= c_j \quad 1 \le j \le l\,, \end{aligned}$$

which implies

$$e(x) = \sum_{j=1}^{k} a_j \sum_{i \in C_j} x^i + \sum_{j=1}^{l} b_j \sum_{i \in D_j} x^i + \sum_{j=1}^{l} b_j^q \sum_{i \in D_j} x^{qi}. \tag{2}$$

Thus,

$$\begin{aligned} \overline{e(x)} &= \sum_{j=1}^{k} a_j^q \sum_{i \in C_j} x^i + \sum_{j=1}^{l} b_j^q \sum_{i \in D_j} x^i + \sum_{j=1}^{l} b_j^{q^2} \sum_{i \in D_j} x^{qi} \\ &= \sum_{j=1}^{k} a_j \sum_{i \in C_j} x^{qi} + \sum_{j=1}^{l} c_j \sum_{i \in E_j} x^{qi} + \sum_{j=1}^{l} b_j \sum_{i \in D_j} x^{qi} \\ &= e(x)\mu_q. \end{aligned}$$

And hence, by Theorem 4.3.13 of [2], $\overline{C} = \langle \overline{e(x)} \rangle = \langle e(x)\mu_q \rangle = C\mu_q$.

The discussion above is summarized in the following theorem.

Theorem 3.1 *Let C be a cyclic code over $\mathbb{F}_{q^2}$ with generating idempotent $e(x)$. The following hold:*

1. *$e(x)$ has the form given in (2).*
2. *$\overline{C}$ is cyclic with generating idempotent $\overline{e(x)}$.*
3. *$\overline{e(x)} = e(x)\mu_q$.*
4. *$\overline{C} = C\mu_q$.*

3.2 Euclidean and Hermitian Duals

Let $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ and $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1})$ be any vectors in $\mathbb{F}_{q^2}^n$. Consider the involution $^- : z \mapsto z^q$ defined on $\mathbb{F}_{q^2}$. The *Hermitian scalar product* is given by $x \cdot \overline{y} = \sum_{i=0}^{n-1} x_i \overline{y_i}$. If C is a linear code over $\mathbb{F}_{q^2}$, the *Euclidean dual of* C is denoted $C^{\perp_E}$. The *Hermitian dual of* C is $C^{\perp_H} = \{\mathbf{u} \in \mathbb{F}_{q^2}^n \mid \mathbf{u} \cdot \overline{\mathbf{w}} = 0 \text{ for all } \mathbf{w} \in C\}$. We say that a code C is *Euclidean self-orthogonal* if $C \subseteq C^{\perp_E}$, and that C is *Euclidean self-dual* if $C = C^{\perp_E}$. Similarly, C is said to be *Hermitian self-orthogonal* if $C \subseteq C^{\perp_H}$, and that C is *Hermitian self-dual* if $C = C^{\perp_H}$.

Let $f(x) = f_0 + f_1 x + \cdots + f_r x^r \in \mathbb{F}_{q^2}[x]$. The *reciprocal polynomial* of $f(x)$ is the polynomial $f^*(x) = x^r f(x^{-1}) = x^r (f(x)\mu_{-1}) = f_r + f_{r-1}x + \cdots + f_0 x^r$.

Lemma 3.2 *Let $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$, $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$ be vectors in $\mathbb{F}_{q^2}^n$ with associated polynomials $a(x)$ and $b(x)$. Then $\mathbf{a}$ is Hermitian orthogonal (similarly Euclidean orthogonal) to $\mathbf{b}$ and all its cyclic shifts iff $a(x)\overline{b^*(x)} = 0$ (similarly $a(x)b^*(x) = 0$) in $\mathcal{R}_n$.*

Proof: Denote by $\mathbf{b}^{(i)}$ the i^{th} cyclic shift of the vector $\mathbf{b}$. Since the Euclidean case appears as Lemma 4.4.8 of [2], we only prove the result for the Hermitian case. Note that $\mathbf{a} \cdot \overline{\mathbf{b}^{(i)}} = \sum_{k=0}^{n-1} a_k \overline{b_{k-i}}$, where the subscripts are read modulo n. Let $a(x)\overline{b^*(x)} = A_0 + A_1 x + A_2 x^2 + \cdots + A_{n-1}x^{n-1}$. Then

$$\begin{aligned}
A_0 &= a_0 b_{n-1}^q + a_1 b_0^q + a_2 b_1^q + \cdots + a_{n-1} b_{n-2}^q &&= \mathbf{a} \cdot \overline{\mathbf{b}^{(1)}}\,; \\
A_1 &= a_0 b_{n-2}^q + a_1 b_{n-1}^q + a_2 b_0^q + \cdots + a_{n-1} b_{n-3}^q &&= \mathbf{a} \cdot \overline{\mathbf{b}^{(2)}}\,; \\
&\vdots \\
A_{n-1} &= a_0 b_0^q + a_1 b_1^q + a_2 b_2^q + \cdots + a_{n-1} b_{n-1}^q &&= \mathbf{a} \cdot \overline{\mathbf{b}}\,.
\end{aligned}$$

Thus $a(x)\overline{b^*(x)} = 0$ iff $A_i = 0$ for all $i = 0, 1, \ldots, n-1$ iff $\mathbf{a}$ is orthogonal to $\mathbf{b}$ and all its cyclic shifts. □

Recall that a vector $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ of $\mathbb{F}_{q^2}^n$ is called an *even-like vector* if $\sum_{i=0}^{n-1} a_i = 0$. A code C is called an *even-like code* if all its codewords are even-like, otherwise it is called *odd-like.*

Lemma 3.3 *Let C be a cyclic code over $\mathbb{F}_{q^2}$ with defining set T and generator polynomial $g(x)$. Let C_e be the subcode of C consisting of all the even-like vectors in C. Then:*

1. *C_e is cyclic and has defining set $T \cup \{0\}$.*
2. *$C = C_e$ iff $0 \in T$ iff $g(1) = 0$.*
3. *If $C \neq C_e$, then the generator polynomial of C_e is $(x-1)g(x)$.*

Proof: Let $a(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in C$. Clearly $xa(x) \in C$. By definition, $a(x) \in C_e$ iff $\sum_{i=0}^{n-1} a_i = 0$ iff $a(1) = 0$. If $a(x) \in C_e$ then clearly $xa(x) \in C_e$. Hence part 1 holds.

Note that $C = C_e$ iff $a(1) = 0$ for all $a(x) \in C$ iff $g(1) = 0$ iff $0 \in T$. Thus part 2 holds.

To prove part 3, notice that $(x-1)g(x)$ generates a cyclic subcode of C which contains all $a(x) \in C$ such that $a(1) = 0$. Clearly this cyclic subcode must be C_e. $\square$

The following theorems generalize some results on Euclidean duals of cyclic codes over an arbitrary finite field to Hermitian duals of cyclic codes over $\mathbb{F}_{q^2}$.

Theorem 3.4 *Let C be a cyclic code of length n over $\mathbb{F}_{q^2}$ with generating idempotent $e(x)$ and defining set T. The following hold:*

1. *$C^{\perp_H}$ is a cyclic code and $C^{\perp_H} = C^c \mu_{-q}$.*
2. *$C^{\perp_H}$ has generating idempotent $1 - e(x)\mu_{-q}$.*
3. *If $\mathcal{N} = \{0, 1, 2, \ldots, n-1\}$, then $\mathcal{N} \setminus (-q)T \bmod n$ is the defining set for $C^{\perp_H}$.*
4. *Precisely one of C and $C^{\perp_H}$ is odd-like and the other is even-like.*

Proof: Let $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in C$. Denote by $\mathbf{a}^{(i)}$ the i^{th} cyclic shift of $\mathbf{a}$. By assumption $\mathbf{a}^{(i)} \in C$ for all i. Let $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1}) \in C^{\perp_H}$. For $i = 0, 1, \ldots, n-1$, we have $\mathbf{b}^{(i)} \cdot \overline{\mathbf{a}} = \mathbf{b} \cdot \overline{\mathbf{a}^{n-i}} = 0$. Thus $C^{\perp_H}$ contains all the cyclic shifts of $\mathbf{b}$. Hence it is cyclic. Note that $C^{\perp_H} = \overline{C}^{\perp_E}$. By Theorem 4.4.9 of [2], $\overline{C}^{\perp_E} = \overline{C}^c \mu_{-1}$. By the definition of a cyclic complement, $\mathbb{F}_{q^2}^n = \overline{C} + \overline{C}^c$ and $\overline{C} \cap \overline{C}^c = \{0\}$. Similarly $\mathbb{F}_{q^2}^n = C + C^c$ and $C \cap C^c = \{0\}$. Thus $\mathbb{F}_{q^2}^n = \overline{\mathbb{F}_{q^2}^n} = \overline{C + C^c} = \overline{C} + \overline{C^c}$ and $\overline{C} \cap \overline{C^c} = \{0\}$. Hence $\overline{C^c}$ is also a cyclic complement of $\overline{C}$. By the uniqueness of complements of cyclic codes, we must have $\overline{C}^c = \overline{C^c}$. Also, by Theorem 3.1 we have $\overline{C^c} = C^c \mu_q$. Hence $C^{\perp_H} = \overline{C}^c \mu_{-1} = \overline{C^c} \mu_{-1} = C^c \mu_q \mu_{-1} = C^c \mu_{-q}$, proving part 1.

By Theorem 4.4.6 in [2], the idempotent generator for C^c is $1-e(x)$. Hence, by Theorem 4.3.13 of [2], the generating idempotent for $C^{\perp_H} = C^c\mu_{-q}$ is $(1-e(x))\mu_{-q} = 1-e(x)\mu_{-q}$. Thus part 2 holds.

To prove part 3, note that Theorem 4.4.6 of [2] implies that the defining set for C^c is $\mathcal{N} \setminus T$. Applying Corollary 4.4.5 of [2], the defining set for $C^{\perp_H}$ is $(-q)^{-1}(\mathcal{N} \setminus T) = \mathcal{N} \setminus (-q)^{-1}T \bmod n$. Note that $\mu_{-q}^2 = \mu_{(-q)^2} = \mu_{q^2}$ and μ_{q^2} fixes each q^2-cyclotomic coset. Hence $(-q)^{-1}T = (-q)^2(-q)^{-1}T = (-q)T \bmod n$. Thus the defining set for $C^{\perp_H}$ is $\mathcal{N} \setminus (-q)T \bmod n$. This proves part 3.

Lastly, since exactly one of T and $\mathcal{N} \setminus (-q)T$ contains 0, part 4 follows from part 3 and Lemma 3.3 . $\square$

The proof of the following lemma is left as an exercise to the reader.

Lemma 3.5 *Let C_i be a cyclic code of length n over $\mathbb{F}_{q^2}$ with defining sets T_i for $i = 1, 2$. Then:*

1. *$C_1 \cap C_2$ has defining set $T_1 \cup T_2$.*
2. *$C_1 + C_2$ has defining set $T_1 \cap T_2$.*
3. *$C_1 \subseteq C_2 \iff T_2 \subseteq T_1$.*

Theorem 3.6 *Let C be a Hermitian self-orthogonal cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set T. Let $C_1, C_2, \ldots, C_k$, $D_1, D_2, \ldots, D_l$, $E_1, E_2, \ldots, E_l$ be all the distinct q^2-cyclotomic cosets modulo n partitioned such that $C_i = C_i\mu_{-q}$ for $1 \le i \le k$ and $D_i = E_i\mu_{-q}$ for $1 \le i \le l$. Then the following hold:*

1. *$C_i \subseteq T$ for $1 \le i \le k$, and at least one of D_i or E_i is contained in T for each $1 \le i \le l$.*
2. *C is even-like.*
3. *$C \cap C\mu_{-q} = \{0\}$.*

Conversely, if C is a cyclic code with defining set T that satisfies part 1, then C is an Hermitian self-orthogonal code.

Proof: Let $\mathcal{N} = \{0, 1, 2, \ldots, n-1\}$.

Let $T^\perp$ be the defining set for $C^{\perp_H}$. By Theorem 3.4, $T^\perp = \mathcal{N} \setminus (-q)T \bmod n$. By assumption, $C \subseteq C^{\perp_H}$. Thus $\mathcal{N} \setminus (-q)T \subseteq T$ by Lemma 3.5. If $C_i \not\subseteq T$ for some i, then $C_i\mu_{-q} \not\subseteq (-q)T$. Since $C_i = C_i\mu_{-q}$, it follows that $C_i \subseteq \mathcal{N} \setminus (-q)T \subseteq T$, a contradiction. Thus $C_i \subseteq T$ for all i. If $D_i \not\subseteq T$, then $E_i = D_i\mu_{-q} \not\subseteq (-q)T \bmod n$. Thus $E_i \subseteq \mathcal{N}\setminus(-q)T \subseteq T$. Hence part 1 holds.

To prove part 2, note that $\{0\} = C_i$ for some i. Hence $0 \in T$ by part 1. By Lemma 3.3, C is even-like.

By Corollary 4.4.5 of [2], $C\mu_{-q}$ has defining set $(-q)^{-1}T$. Notice that $(-q)^{-1}T = (-q)^2(-q)^{-1}T = (-q)T \bmod n$ since $\mu_{-q}^2 = \mu_{(-q)^2} = \mu_{q^2}$ fixes each q^2-cyclotomic coset mod n. Thus $C\mu_{-q}$ has defining set $(-q)T$. Clearly $T \cup (-q)T = \mathcal{N}$. By Lemma 3.5, $T \cup (-q)T$ is the defining set for $C \cap C\mu_{-q}$. Thus $C \cap C\mu_{-q} = \{0\}$, which proves part 3.

For the converse, assume T satisfies part 1. We will show that $T^\perp \subseteq T$ which will imply that C is Hermitian self-orthogonal. By Theorem 3.4, $T^\perp = \mathcal{N} \setminus (-q)T \bmod n$. Note that $C_i \subseteq T \implies C_i = C_i\mu_{-q} \subseteq (-q)T \implies C_i \nsubseteq T^\perp$. Hence $T^\perp$ is a union of some E_i's and D_i's. If $D_i \subseteq T^\perp = \mathcal{N} \setminus (-q)T$, then $D_i \nsubseteq (-q)T \bmod n$, implying that $(-q)D_i \nsubseteq T$. Since $(-q)D_i = E_i$, it follows that $E_i \nsubseteq T$. By part 1, $D_i \subseteq T$. By a similar argument, it can be shown that if $E_i \subseteq T^\perp$, then $E_i \subseteq T$. □

4 Duadic Codes

Let n be an odd positive integer. We let $\overline{j}(x) = \frac{1}{n}(1 + x + x^2 + \cdots + x^{n-1})$, the generating idempotent for the repetition code of length n over $\mathbb{F}_q$.

We first define duadic codes over arbitrary finite fields. Then we proceed to examine duadic codes over finite fields of square order. The goal of this section is to present some results concerning Hermitian orthogonality of duadic codes over such finite fields.

4.1 Definitions and Basic Properties

Definition 4.1 *Let $e_1(x)$ and $e_2(x)$ be a pair of even-like idempotents and let $C_1 = \langle e_1(x)\rangle$ and $C_2 = \langle e_2(x)\rangle$. The codes C_1 and C_2 form a pair of* even-like duadic codes *if the following properties are satisfied: a.) the idempotents satisfy $e_1(x) + e_2(x) = 1 - \overline{j}(x)$; and b.) there is a multiplier μ_a such that $C_1\mu_a = C_2$ and $C_2\mu_a = C_1$.*

To the pair of even-like codes C_1 and C_2, we associate a pair of odd-like duadic codes *$D_1 = \langle 1 - e_2(x)\rangle$ and $D_2 = \langle 1 - e_1(x)\rangle$.*

We say that the multiplier μ_a gives a splitting *for the even-like duadic codes or for the odd-like duadic codes.*

Theorem 4.2 ([2].) *Let C_1 and C_2 be cyclic codes over $\mathbb{F}_q$ with defining sets $T_1 = \{0\} \cup S_1$ and $T_2 = \{0\} \cup S_2$, respectively, where $0 \notin S_1$ and $0 \notin S_2$. Then C_1 and C_2 form a pair of even-like duadic codes if and only if the following conditions are satisfied: a.) S_1 and S_2 satisfy $S_1 \cup S_2 = \{1, 2, \ldots, n-1\}$ and $S_1 \cap S_2 = \emptyset$; and b.) there is a multiplier μ_b such that $S_1\mu_b = S_2$ and $S_2\mu_b = S_1$.*

If the conditions in the preceding theorem are satisfied, we say that S_1 and S_2 gives a *splitting of n by μ_b over $\mathbb{F}_q$*. This gives us another way of describing duadic codes.

Note that for a fixed pair of duadic codes over $\mathbb{F}_q$ of length n, we can use the same multiplier for the splitting in Definition 4.1 and the splitting of n in Theorem 4.2.

Theorem 4.3 ([2].) *Duadic codes of length n over $\mathbb{F}_q$ exist iff q is a square mod n.*

4.2 Hermitian Orthogonality of Duadic Codes over $\mathbb{F}_{q^2}$

From this point onwards, we consider codes over the Galois field $\mathbb{F}_{q^2}$, where q is a power of some prime p. Again we assume that n is an odd positive integer and $\gcd(n, q) = 1$. Thus duadic codes of length n over $\mathbb{F}_{q^2}$ always exist by Theorem 4.3. The following theorem is the Hermitian analogue of Theorem 6.4.1 of [2], where the Euclidean self-orthogonality of duadic codes over $\mathbb{F}_q$ are considered.

Theorem 4.4 *Let C be any $[n, \frac{n-1}{2}]$ cyclic code of length n over $\mathbb{F}_{q^2}$. Then C is Hermitian self-orthogonal if and only if C is an even-like duadic code whose splitting is given by μ_{-q}.*

Proof: ($\Leftarrow$) Suppose $C = C_1$ is an even-like duadic code whose splitting is given by μ_{-q}. Let $e(x)$ be the generating idempotent for C. By Theorem 3.4, the generating idempotent for $C^{\perp_H}$ is $1 - e(x)\mu_{-q}$. By definition, $D_1 = \langle 1 - e(x)\mu_{-q}\rangle$. Thus $C^{\perp_H} = D_1$. By Theorem 6.1.3 (vi) of [2], $C = C_1 \subseteq D_1$. Thus C is Hermitian self-orthogonal.

($\Rightarrow$) Let $C = C_1$ be a Hermitian self-orthogonal cyclic code. Let $e_1(x)$ be the generating idempotent for C_1 and T_1 its defining set. Since C_1 is Hermitian self-orthogonal and $\overline{j}(x)$ is not orthogonal to itself, it follows that $\overline{j}(x) \notin C_1$. Hence by Lemma 6.1.2 (iii) of [2], C_1 is even-like. Let $e_2(x) = e_1(x)\mu_{-q}$ and let $C_2 = \langle e_2(x)\rangle$. By Theorem 4.3.13 of [2], $C_2 = C_1\mu_{-q}$.

Let $(a_0, a_1, \ldots, a_{n-1}) \in C_1$. Since C_1 is even-like, it follows that $\sum_{i=0}^{n-1} a_i = 0$. Thus $(1, 1, \ldots, 1) \cdot \overline{(a_0, a_1, \ldots, a_{n-1})} = (1, 1, \ldots, 1) \cdot (a_0^q, a_1^q, \ldots, a_{n-1}^q) = \sum_{i=0}^{n-1} a_i^q = \left(\sum_{i=0}^{n-1} a_i\right)^q = 0$ which implies that $\overline{j}(x) \in C_1^{\perp_H}$. Since $C_1^{\perp_H}$ has dimension $\frac{n+1}{2}$ and $C_1 \subseteq C_1^{\perp_H}$, we have $C_1^{\perp_H} = C_1 + \langle\overline{j}(x)\rangle$. By Theorem 4.3.7 of [2], the code $C_1^{\perp_H}$ has generating idempotent $e_1(x) + \overline{j}(x) - e_1(x)\overline{j}(x)$. However by Lemma 6.1.2 (i) of [2], $e_1(x)\overline{j}(x) = 0$. Thus $C_1^{\perp_H}$ has generating idempotent $e_1(x) + \overline{j}(x)$.

By Theorem 3.4, the generating idempotent for $C_1^{\perp_H}$ is $1 - e_1(x)\mu_{-q}$ and so by the uniqueness of the idempotent generator, we must have $1 - e_1(x)\mu_{-q} = e_1(x) + \overline{j}(x)$ which implies $1 - \overline{j}(x) = e_1(x) + e_1(x)\mu_{-q} = e_1(x) + e_2(x)$. Clearly, $e_1(x) = e_2(x)(\mu_{-q})^{-1} = e_2(x)(\mu_{-q})$. Therefore, C_1 and C_2 form a pair of even-like codes whose splitting is given by μ_{-q}. $\square$

Lemma 4.5 *Let C be a cyclic code. Then $(C\mu_a)^{\perp_H} = C^{\perp_H}\mu_a$.*

Proof: Let $e(x)$ be the idempotent generator for C. By Theorem 3.4 above and Theorem 4.3.13 of [2], $(C\mu_a)^{\perp_H}$ has idempotent generator $1 - e(x)\mu_a\mu_{-q}$ and $C^{\perp_H}$ has idempotent generator $1 - e(x)\mu_{-q}$. And therefore by Theorem 4.3.13 of [2], $C^{\perp_H}\mu_a$ has idempotent generator $(1 - e(x)\mu_{-q})\mu_a = 1 - e(x)\mu_a\mu_{-q}$. $\square$

Theorem 4.6 *Suppose that C_1 and C_2 are a pair of even-like duadic codes over $\mathbb{F}_{q^2}$, having D_1 and D_2 as their associated odd-like duadic codes. Then the following are equivalent.*

1. $C_1^{\perp_H} = D_1$

2. $C_2^{\perp_H} = D_2$

3. $C_1\mu_{-q} = C_2$

4. $C_2\mu_{-q} = C_1$

Proof: From the definition of duadic codes and Theorem 6.1.3 (vii) of [2], we obtain $C_1\mu_a = C_2$, $C_2\mu_a = C_1$, $D_1\mu_a = D_2$ and $D_2\mu_a = D_1$ for some a. Hence by Lemma 4.5, if part 1 holds, then

$$C_2^{\perp_H} = (C_1\mu_a)^{\perp_H} = C_1^{\perp_H}\mu_a = D_1\mu_a = D_2$$

and if part 2 holds, then

$$C_1^{\perp_H} = (C_2\mu_a)^{\perp_H} = C_2^{\perp_H}\mu_a = D_2\mu_a = D_1.$$

Hence parts 1 and 2 are equivalent.

Part 3 is equivalent to part 4 since $(\mu_{-q})^{-1} = \mu_{-q}$.

If part 1 holds, then by Theorem 6.1.3 (vi) of [2], C_1 is Hermitian self-orthogonal. Hence by Theorem 4.4, part 3 holds.

If part 3 holds, then μ_{-q} gives a splitting for C_1 and C_2. Let $e_i(x)$ be the generating idempotent for C_i. By Theorem 4.3.13 of [2], $e_1(x)\mu_{-q} = e_2(x)$. Hence by Theorem 3.4, the generating idempotent for $C_1^{\perp_H}$ is $1 - e_1(x)\mu_{-q} = 1 - e_2(x)$. Thus, part 1 holds, completing the proof. □

Theorem 4.7 *Suppose that C_1 and C_2 are a pair of even-like duadic codes over $\mathbb{F}_{q^2}$, having D_1 and D_2 as their associated odd-like duadic codes. Then the following are equivalent.*

1. $C_1^{\perp_H} = D_2$

2. $C_2^{\perp_H} = D_1$

3. $C_1\mu_{-q} = C_1$

4. $C_2\mu_{-q} = C_2$

Proof: From the definition of duadic codes and Theorem 6.1.3 (vii) of [2], we obtain $C_1\mu_a = C_2$, $C_2\mu_a = C_1$, $D_1\mu_a = D_2$ and $D_2\mu_a = D_1$ for some a. Hence, by Lemma 4.5, if part 1 holds, then

$$C_2^{\perp_H} = (C_1\mu_a)^{\perp_H} = C_1^{\perp_H}\mu_a = D_2\mu_a = D_1$$

and if part 2 holds, then

$$C_1^{\perp_H} = (C_2\mu_a)^{\perp_H} = C_2^{\perp_H}\mu_a = D_1\mu_a = D_2.$$

Hence parts 1 and 2 are equivalent.

Let $e_i(x)$ be the generating idempotent for C_i. By Theorem 3.4, $C_1^{\perp_H}$ has generating idempotent $1 - e_1(x)\mu_{-q}$. Thus $C_1^{\perp_H} = D_2$ iff $1 - e_1(x)\mu_{-q} = 1 - e_1(x)$ iff $e_1(x)\mu_{-q} = e_1(x)$ iff $C_1\mu_{-q} = C_1$ by Theorem 4.3.13 of [2]. Hence parts 1 and 3 are equivalent. It can be shown by an analogous argument that parts 2 and 4 are equivalent. □

4.3 Extensions of Odd-like Duadic Codes

Odd-like duadic codes have parameters $[n, \frac{n+1}{2}]$. Hence it is interesting to consider extending such codes because such extensions could possibly be Hermitian self-dual codes. The goal of this section is to give a way of extending odd-like duadic codes and to give conditions under which these extensions are Hermitian self-dual.

Let D be an odd-like duadic code. Then D can be obtained from its even-like subcode C by adding $\overline{j}(x)$ to a basis of C (Theorem 6.1.3 (ix), [2]). Hence it is natural to define an extension for which the all-one vector $\mathbf{1}$ is Hermitian orthogonal to itself.

Consider the equation

$$1 + \gamma^{q+1}n = 0. \tag{3}$$

Since $n^{q+1} = n^2$ in $\mathbb{F}_{q^2}$, the equation above is equivalent to

$$n + \gamma^{q+1} = 0. \tag{4}$$

Note that

$$\{a^{q+1} \mid a \in \mathbb{F}_{q^2}\} = \mathbb{F}_q.$$

Thus (4) will always have a solution in $\mathbb{F}_{q^2}$, which implies that (3) is solvable in $\mathbb{F}_{q^2}$.

We are now ready to describe the extension.

Let γ be a solution to (3).

Let $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in D$.

Define the extended codeword $\widetilde{\mathbf{c}} = (c_0, c_1, \dots, c_{n-1}, c_\infty)$, where

$$c_\infty = -\gamma \sum_{i=0}^{n-1} c_i.$$

Let $\widetilde{D} = \{\widetilde{\mathbf{c}} \mid \mathbf{c} \in D\}$ be the extended code of D.

Theorem 4.8 *Let D_1 and D_2 be a pair of odd-like duadic codes of length n over $\mathbb{F}_{q^2}$. The following hold:*

1. *If μ_{-q} gives the splitting for D_1 and D_2, then $\widetilde{D_1}$ and $\widetilde{D_2}$ are Hermitian self-dual.*

2. If $D_1\mu_{-q} = D_1$, then $\widetilde{D_1}$ and $\widetilde{D_2}$ are Hermitian duals of each other.

Proof: Let C_1 and C_2 be the even-like duadic codes associated to D_1 and D_2.

Note that

$$\begin{aligned}
\widetilde{\overline{j}(x)}\overline{\widetilde{\overline{j}(x)}} &= \left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}, -\gamma\right) \cdot \overline{\left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}, -\gamma\right)} \\
&= \left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}, -\gamma\right) \cdot \left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}, (-\gamma)^q\right) \\
&= \frac{1}{n} + \gamma^{q+1} \\
&= \frac{1}{n}(1 + \gamma^{q+1}n) \\
&= 0,
\end{aligned}$$

by our choice of γ. This shows that $\widetilde{\overline{j}(x)}$ is Hermitian orthogonal to itself.

Also, since C_i is even-like, $\widetilde{C_i}$ is obtained by adding a zero coordinate to C_i. Hence it follows that $\widetilde{\overline{j}(x)}$ is orthogonal to $\widetilde{C_i}$.

We first prove part 1. Theorem 4.4 ensures that C_1 is Hermitian self-orthogonal, and so $\widetilde{C_1}$ is Hermitian self-orthogonal. Since $\widetilde{\overline{j}(x)}$ is orthogonal to $\widetilde{C_1}$, the code spanned by $\langle \widetilde{C_1}, \widetilde{\overline{j}(x)} \rangle$ is Hermitian self-orthogonal. However, by Theorem 6.1.3 (ix) of [2], $D_1 = \langle C_1, \overline{j}(x) \rangle$. Clearly $\widetilde{D_1} = \langle \widetilde{C_1}, \widetilde{\overline{j}(x)} \rangle$. Thus $\widetilde{D_1}$ is Hermitian self-orthogonal. On the other hand, Theorem 6.1.3 (v) of [2] says that $\widetilde{D_1}$ has dimension $\frac{n+1}{2}$. Therefore $\widetilde{D_1}$ is Hermitian self dual. Analogous arguments will prove that $\widetilde{D_2}$ is Hermitian self-dual.

We now prove part 2. Suppose $D_1\mu_{-q} = D_1$. It follows that $C_1\mu_{-q} = C_1$. By Theorem 4.7, $C_2^{\perp_H} = D_1$. Also, $C_1 \subseteq D_1$ by Theorem 6.1.3 (vi) of [2]. Hence $C_1 \subseteq C_2^{\perp_H}$. Thus C_1 and C_2 are orthogonal to each other. Therefore $\widetilde{C_1}$ and $\widetilde{C_2}$ are orthogonal to each other and consequently the codes spanned by $\langle \widetilde{C_1}, \widetilde{\overline{j}(x)} \rangle$ and $\langle \widetilde{C_2}, \widetilde{\overline{j}(x)} \rangle$ are orthogonal. By Theorem 6.1.3 (v) & (vi) of [2], these codes must be $\widetilde{D_1}$ and $\widetilde{D_2}$ of dimension $\frac{n+1}{2}$. Therefore $\widetilde{D_1}$ and $\widetilde{D_2}$ are duals of each other. $\square$

5 Lengths with Splittings By μ_{-q}

All throughout this section, we let q be a power of a prime p and we assume that n is an odd integer with $gcd(n, q) = 1$. Define $ord_r(q)$ to be the smallest positive integer t such that $q^t \equiv 1 \pmod{r}$.

In view of Theorem 4.4 and Theorem 4.8, it is natural to ask under what conditions do we get a splitting of n by μ_{-q}. We note that the study of the feasibility of an integer in [7] becomes a special case of this with $q = 2$.

The main result of this section is the following theorem.

Theorem 5.1 *The permutation map μ_{-q} gives a splitting of n iff $ord_r(q) \not\equiv 2 \pmod 4$ for every prime r dividing n.*

Our proof of this theorem will be based on several lemmas. Lemma 5.2 is a well-known fact from elementary number theory, see e.g. Proposition 3 in [10], and we leave its proof as an exercise to the reader.

Lemma 5.2 *Let r be a prime distinct from p. Then r divides q^k+1 for some positive integer k iff $ord_r(q)$ is even.*

Lemma 5.3 *Let r be a prime distinct from p. Then r divides $q^{2i-1}+1$ for some integer $i \geq 1$ iff $ord_r(q) \equiv 2 \pmod 4$.*

Proof: By Lemma 5.2, r divides q^k+1 for some positive integer k iff $ord_r(q)$ is even.
If $ord_r(q)$ is even, then

$$\begin{aligned} r \mid q^k+1 &\iff q^k \equiv -1 \pmod r \\ &\iff k \equiv \frac{ord_r(q)}{2} \pmod{ord_r(q)}. \end{aligned}$$

Thus r divides $q^{2i-1}+1$ iff $ord_r(q)$ is even and

$$2i-1 \equiv \frac{ord_r(q)}{2} \pmod{ord_r(q)}. \tag{5}$$

But (5) has a solution i iff $ord_r(q) \equiv 2 \pmod 4$. □

Proposition 5.4 *Assume $gcd(n,q)=1$. Then*
$gcd(n, q^{2i-1}+1) = 1 \ \forall i \in \mathbb{Z}^+$ iff $ord_r(q) \not\equiv 2 \pmod 4$ for every prime r dividing n.

Proof: Write $n = r_1^{e_1} r_2^{e_2} \cdots r_s^{e_s}$. Then, using Lemma 5.3,

$$\begin{aligned} ord_{r_j}(q) \not\equiv 2 \pmod 4 \ \ \forall j=1,\dots,s &\iff \forall j=1,\dots,s, \ \ r_j \text{ does not divide } q^{2i-1}+1 \ \ \forall i \in \mathbb{Z}^+ \\ &\iff \forall j=1,2,\dots,s, \ \ gcd(r_j, q^{2i-1}+1) = 1 \ \ \forall i \in \mathbb{Z}^+ \\ &\iff gcd(n, q^{2i-1}+1) = 1 \ \ \forall i \in \mathbb{Z}^+. \end{aligned}$$

□

Proposition 5.5 *Let t be an integer such that $t \not\equiv (q^2)^j \pmod n$ and $t^2 \equiv (q^2)^j \pmod n$ for some non-negative integer j. Suppose $gcd(t,n)=1$. Then μ_t gives a splitting of n iff $gcd(n, q^{2i}-t) = 1$ for all $i = 1,2,3,\dots$.*

Proof: Clearly by the assumptions on t, $(\mu_t)^2(C_s) = C_s$ for every q^2-cyclotomic coset C_s.

Thus μ_t gives a splitting of n if and only if it does not fix any q^2-cyclotomic coset.

Let C_a be a q^2-cyclotomic coset. Then μ_t fixes C_a if and only if $ta \equiv (q^2)^i a \pmod{n}$ for some positive integer i. Thus μ_t gives a splitting of n iff $ta \not\equiv (q^2)^i a \pmod{n}$ for all $i = 1, 2, 3, \ldots$ iff $gcd(n, q^{2i} - t) = 1$ for all $i = 1, 2, 3, \ldots$. □

Theorem 9 of [14] is a special case of Proposition 5.5 with $q = 2$.

Corollary 5.6 *The permutation map* μ_{-q} *gives a splitting of* n *iff* $gcd(n, q^{2i-1} + 1) = 1$ *for all* $i = 1, 2, 3, \ldots$.

Proof: This follows immediately from Proposition 5.5 since $gcd(n, q) = 1$ by assumption. □

We are now ready to prove the main theorem of this section.

Proof of Theorem 5.1:

By Corollary 5.6, the permutation map μ_{-q} gives a splitting of n iff $gcd(n, q^{2i-1} + 1) = 1$ for all $i = 1, 2, 3, \ldots$.

By Proposition 5.4, $gcd(n, q^{2i-1} + 1) = 1$ iff $ord_r(q) \not\equiv 2 \pmod{4}$ for every prime r dividing n. □

Finally, we remark that Theorem 5.1 says that μ_{-q} gives a splitting of n if and only if for all prime r dividing n, either $ord_r(q)$ is odd or $ord_r(q)$ is doubly even. However, it is easy to show that $ord_r(q)$ is doubly even if and only if $ord_r(q^2)$ is even. Thus we can restate Theorem 5.1 as:

Theorem 5.7 *The permutation map* μ_{-q} *gives a splitting of* n *iff for every prime* r *dividing* n*, either* $ord_r(q)$ *is odd or* $ord_r(q^2)$ *is even.*

The table below enumerates all the splittings (up to symmetry between S_1 and S_2) of n by μ_{-q} over $\mathbb{F}_{q^2}$ for $n \leq 45$ and $q = 2$ and $q = 3$ by listing all the possible sets for the S_1 in Theorem 4.2. The C_i's are q^2-cyclotomic cosets modulo n. We omit those n for which no such splitting exists for both values of q.

n	S_1	
	$q=2$	$q=3$
5	$C_1{}^{\clubsuit}$	$C_1{}^{\clubsuit}$
7	$C_1{}^{\clubsuit}$	——
11	——	$C_1{}^{\clubsuit}$
13	$C_1{}^{\clubsuit}$	$C_1 \cup C_2,\ C_1 \cup C_7$
17	$C_1 \cup C_3,\ C_1 \cup C_6$	$C_1{}^{\clubsuit}$
23	$C_1{}^{\clubsuit}$	$C_1{}^{\clubsuit}$
25	$C_1 \cup C_5,\ C_1 \cup C_{10}$	$C_1 \cup C_5,\ C_1 \cup C_{10}$
29	$C_1{}^{\clubsuit}$	$C_1{}^{\clubsuit}$
31	$C_1 \cup C_3 \cup C_5,\ C_1 \cup C_3 \cup C_{11},$ $C_1 \cup C_5 \cup C_7{}^{\clubsuit},\ C_1 \cup C_7 \cup C_{11}$	——
35	$C_1 \cup C_2 \cup C_5 \cup C_7,$ $C_1 \cup C_2 \cup C_5 \cup C_{14},$ $C_1 \cup C_2 \cup C_7 \cup C_{15},$ $C_1 \cup C_2 \cup C_{14} \cup C_{15},$ $C_1 \cup C_5 \cup C_6 \cup C_7,$ $C_1 \cup C_5 \cup C_6 \cup C_{14},$ $C_1 \cup C_6 \cup C_7 \cup C_{15},$ $C_1 \cup C_6 \cup C_{14} \cup C_{15},$	——
37	$C_1{}^{\clubsuit}$	——
41	$C_1 \cup C_3,\ C_1 \cup C_6$	$C_1 \cup C_2 \cup C_4 \cup C_7 \cup C_8,$ $C_1 \cup C_2 \cup C_4 \cup C_7 \cup C_{11},$ $C_1 \cup C_2 \cup C_4 \cup C_8 \cup C_{16}{}^{\clubsuit},$ $C_1 \cup C_2 \cup C_4 \cup C_{11} \cup C_{16},$ $C_1 \cup C_2 \cup C_7 \cup C_8 \cup C_{12},$ $C_1 \cup C_2 \cup C_7 \cup C_{11} \cup C_{12},$ $C_1 \cup C_2 \cup C_8 \cup C_{12} \cup C_{16},$ $C_1 \cup C_2 \cup C_{11} \cup C_{12} \cup C_{16},$ $C_1 \cup C_4 \cup C_6 \cup C_7 \cup C_8,$ $C_1 \cup C_4 \cup C_6 \cup C_7 \cup C_{11},$ $C_1 \cup C_4 \cup C_6 \cup C_8 \cup C_{16},$ $C_1 \cup C_4 \cup C_6 \cup C_{11} \cup C_{16},$ $C_1 \cup C_6 \cup C_7 \cup C_8 \cup C_{12},$ $C_1 \cup C_6 \cup C_7 \cup C_{11} \cup C_{12},$ $C_1 \cup C_6 \cup C_8 \cup C_{12} \cup C_{16},$ $C_1 \cup C_6 \cup C_{11} \cup C_{12} \cup C_{16},$

Table 1: Splittings of n by μ_{-q} ($\clubsuit$ denotes splittings of Quadratic Residue codes)

A Quantitative Aspects

A.1 Counting integers that are split by μ_{-q}

Theorem 5.1 raises the question of counting the number of integers $n \leq x$ such that μ_{-q} gives a splitting of n. In other words, we are interested in counting those integers n such that n is coprime with the sequence $S(q) := \{q^{2i-1}+1\}_{i=1}^{\infty}$. We let $A_q(x)$ denote the associated counting function. We are interested in sharp estimates for $A_q(x)$ as x gets large. We use the shorthand GRH to denote the Generalized Riemann Hypothesis. The best we can do in this respect is stated in the following theorem:

Theorem A.1 *Let $q = p^t$ be a prime power. Put $\lambda = \nu_2(t)$.*

1. *For some positive constant c_q we have*

$$A_q(x) = c_q \frac{x}{\log^{\delta(q)} x} + O_q\left(\frac{x(\log\log x)^5}{\log^{1+\delta(q)} x}\right),$$

   where the implicit constant depends at most on q.

2. *Let $\epsilon > 0$ and $v \geq 1$ be arbitrary. Assuming GRH we have that*

$$A_q(x) = \sum_{0 \leq j < v} \frac{b_j x}{\log^{\delta(q)+j} x} + O_{\epsilon,q}\left(\frac{x}{\log^{\delta(q)+v-\epsilon} x}\right),$$

   where the implied constant depends at most on ϵ and q, and $b_0(= c_q), \ldots, b_v$ are constants that depend at most on q.

The constant $\delta(q)$ is the natural density of primes r such that $ord_r(q) \equiv 2 \pmod 4$ and is given as follows:

$$\delta(p^t) = \begin{cases} 7/24 & \text{if } p = 2 \text{ and } \lambda = 0; \\ 1/3 & \text{if } p = 2 \text{ and } \lambda = 1; \\ 2^{-\lambda-1}/3 & \text{if } p = 2 \text{ and } \lambda \geq 2; \\ 2^{-\lambda}/3 & \text{if } p \neq 2. \end{cases}$$

Our proof of Theorem A.1 rests on various lemmas. Let $\chi_q(n)$ be the characteristic function of the integers n that are coprime with the sequence $S(q)$, i.e.

$$\chi_q(n) = \begin{cases} 1 & \text{if } (n, S(q)) = 1; \\ 0 & \text{otherwise.} \end{cases}$$

Clearly $A_q(x) = \sum_{n \leq x} \chi_q(n)$. Note that $\chi_q(n)$ is a completely multiplicative function in n, i.e., $\chi_q(nm) = \chi_q(n)\chi_q(m)$ for all natural numbers n and m. This observation reduces the study of $\chi_q(n)$ to that of $\chi_q(r)$ with r a prime. Using Lemma 5.3 we infer the following lemma.

Lemma A.2 *We have $\chi_q(r) = 1$ iff $r = p$ or $ord_r(q) \not\equiv 2 \ (mod\ 4)$ in case $r \neq p$.*

This result allows one to count the number of primes $r \leq x$ such that $(r, S(q)) = 1$. Recall that $\mathrm{Li}(x)$, the logarithmic integral, is defined as $\int_2^x dt/\log t$.

Lemma A.3 *Write $q = p^t$. Let $\lambda = \nu_2(t)$.*

1. *We have*

$$\sum_{r \leq x,\ (r,S(q))=1} 1 = \sum_{r \leq x} \chi_q(r) = (1 - \delta(q))\mathrm{Li}(x) + O_q\left(\frac{x(\log\log x)^4}{\log^3 x}\right). \tag{6}$$

2. *Assuming GRH the estimate (6) holds with error term $O_q(\sqrt{x}\log^2 x)$, where the index q indicates that the implied constant depends at most on q.*

Proof: 1.) The number of primes $r \leq x$ such that $\mathrm{ord}_r(q) \equiv 2 \pmod 4$ is counted in Theorem 2 of [10]. On invoking the Prime Number Theorem in the form $\pi(x) = \mathrm{Li}(x) + O(x \log^{-3} x)$, the proof of part 1 is then completed.

2.) The proof of this part follows from Theorem 3 of [11] together with the well-known result (von Koch, 1901) that the Riemann Hypothesis is equivalent with $\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x)$. □

We are now ready to prove Theorem A.1.

Proof of Theorem A.1: 1.) This is a consequence of part 1 of Lemma A.3, Theorem 4 of [10] and the fact that $\chi_q(n)$ is multiplicative in n.

2.) By part 2 of Lemma A.3 we have $\sum_{r \leq x} \chi_q(r) = (1 - \delta(p^t))\mathrm{Li}(x) + O_q\left(x \log^{-1-v} x\right)$. Now invoke Theorem 6 of [12] with $f(n) = \chi_q(n)$. □

A.2 Counting duadic codes

Theorem 4.3 allows one to study how many duadic codes of length $n \leq x$ (with $(n, q) = 1$) over $\mathbb{F}_q$ exist as x gets large. We let $D_q(x)$ be the associated counting function. Indeed, we will study the more general function $D_a(x)$ which is defined similarly, but where a is an arbitrary integer. The trivial case arises when a is a square and thus we assume henceforth that a is not a square.

At first glance it seems that

$$D_a(x) = \frac{1}{2} \sum_{n \leq x,\ (n,a)=1} \left(1 + (\frac{a}{n})\right),$$

with (a/n) the Jacobi symbol. However, it is not true that $(a/n) = 1$ iff a is a square modulo n, e.g., $(2/15) = (2/3)(2/5) = (-1)(-1) = 1$, but 2 is not a square modulo 15. It is possible, however, to develop a criterium for a to be a square modulo n in terms of Legendre symbols. To this effect first note that if a is a square modulo n, then a must be a square modulo all prime powers in the factorisation of n. This is a consequence of the following lemma.

Lemma A.4 *Let n and m be coprime integers. Then a is a square modulo mn iff it is a square modulo m and a square modulo n.*

Proof: By the Chinese Remainder Theorem $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m \oplus \mathbb{Z}/n$ is an isomorphism of rings and hence a is a square in the ring on the left iff a is is square in the ring on the right. Now note that the multiplication in the second ring is coordinatewise. □

It is a well-known result from elementary number theory that if p is an odd prime and if $x^2 \equiv a \pmod{p}$ is solvable, so is $x^2 \equiv a \pmod{p^e}$ for all $e \geq 1$, see e.g. [4, Proposition 4.2.3]. Using this observation together with Lemma A.4 one arrives at the following criterium for a to be a square modulo n.

Lemma A.5 *Let a and n be coprime integers. Put*

$$g_a(n) = \prod_{p|n} \left(\frac{1 + (\frac{a}{p})}{2} \right).$$

Let $e = \nu_2(n)$. Put

$$f_a(n) = \begin{cases} 0 & \textit{if } a \equiv 3 \pmod 4 \textit{ and } e \geq 2; \\ 0 & \textit{if } a \equiv 5 \pmod 8 \textit{ and } e \geq 3; \\ g_a(n) & \textit{otherwise.} \end{cases}$$

Then

$$f_a(n) = \begin{cases} 1 & \textit{if } a \textit{ is a square modulo } n; \\ 0 & \textit{otherwise.} \end{cases}$$

By Lemma A.5 we have that $D_a(x) = \sum_{n \leq x,\, (n,a)=1} f_a(n)$. Note that $g_a(n)$ is a multiplicative function, but that $f_a(n)$ is a multiplicative function only on the odd integers n (generically). For this reason let us first consider

$$G_a(x) := \sum_{n \leq x,\, (n,a)=1} g_a(n).$$

As a consequence of the law of quadratic reciprocity, the primes p for which $g_a(p) = 1$ are precisely the primes p in certain arithmetic progressions with modulus dividing $4q$. On using the prime number theorem for arithmetic progressions one then infers that for every $v > 0$ the following estimate holds true:

$$\sum_{p \leq x} g_a(p) = \frac{1}{2}\mathrm{Li}(x) + O_q\left(\frac{x}{\log^v x}\right), \tag{7}$$

On using this one sees that the conditions of Theorem 6 of [12] are satisfied and this yields the truth of the following assertion.

Lemma A.6 *Let $\epsilon > 0$ and $v \geq 1$ be arbitrary. Suppose that a is not a square. We have*

$$G_a(x) = \sum_{0 \leq j < v} \frac{d_j x}{\log^{1/2+j} x} + O_{\epsilon,q}\left(\frac{x}{\log^{1/2+v-\epsilon} x}\right),$$

where the implied constant depends at most on ϵ and a, and d_0 $(> 0), \ldots, d_v$ are constants that depend at most on a.

Now it is straightforward to derive an asymptotic for $D_a(x)$. Using Lemma A.5 one infers that

$$D_a(x) = \begin{cases} G_{2a}(x) + G_{2a}(x/2) & \text{if } a \equiv 3 \pmod 4; \\ G_{2a}(x) + G_{2a}(x/2) + G_{2a}(x/4) & \text{if } a \equiv 5 \pmod 8; \\ G_a(x) & \text{otherwise.} \end{cases} \tag{8}$$

From this and Lemma A.6 it then follows that we have the following asymptotic for $D_a(x)$.

Theorem A.7 *Let $\epsilon > 0$ and $v \geq 1$ be arbitrary. Suppose that a is not a square. We have*

$$D_a(x) = \sum_{0 \leq j < v} \frac{e_j x}{\log^{1/2+j} x} + O_{\epsilon,q}\left(\frac{x}{\log^{1/2+v-\epsilon} x}\right),$$

where the implied constant depends at most on ϵ and a, and e_0 $(> 0), \ldots, e_v$ are constants that depend at most on a.

In particular we have, as x tends to infinity,

$$D_a(x) \sim D_a \frac{x}{\sqrt{\log x}} \text{ and } G_a(x) \sim G_a \frac{x}{\sqrt{\log x}},$$

where D_a and G_a are positive constants. We now consider the explicit evaluation of these constants. Note that by (8) it suffices to find an explicit formula for the constant G_a.

In case $a = D$ is a negative discriminant of a binary quadratic form this constant can be easily computed using results from the analytic theory of binary quadratic forms. We say an integer D is a discriminant if it arises as the discriminant of a binary quadratic form. This implies that either $4|D$ or $D \equiv 1 \pmod 4$. On the other hand, it can be shown that any number D satisfying $4|D$ or $D \equiv 1 \pmod 4$ arises as the discriminant of a binary quadratic form. Now let D be a discriminant and ξ_D be the multiplicative function defined as follows:

$$\xi_D(p^e) = \begin{cases} 1 & \text{if } (\frac{D}{p}) = 1; \\ 1 & \text{if } (\frac{D}{p}) = -1 \text{ and } 2|e; \\ 0 & \text{otherwise.} \end{cases}$$

Let n be any integer coprime to D. Then $\xi_D(n) = 1$ iff n is represented by some primitive positive integral binary quadratic form of discriminant D. Let $B_D(x)$ denote the number of positive integers $n \leq x$ which are coprime to D and which are represented by some primitive integral form of discriminant $D \leq -3$. Note that $B_D(x) = \sum_{n \leq x} \xi_D(n)$. It was proved by James [5] that

$$B_D(x) = J(D)\frac{x}{\sqrt{\log x}} + O\left(\frac{x}{\log x}\right),$$

where $J(D)$ is the positive constant given by

$$\pi J(D)^2 = \frac{\varphi(|D|)}{|D|} L(1, \chi_D) \prod_{(\frac{D}{p})=-1} \frac{1}{1 - \frac{1}{p^2}}, \tag{9}$$

and p runs over all primes such that $(D/p) = -1$. (Recall that the Dirichlet L-series $L(s, \chi_D)$ is defined by $L(s, \chi_D) = \sum_{n=1}^{\infty} \chi_D(n) n^{-s}$.) Since the behaviour of ξ_D is so similar to that of f_D, James' result can in fact be used to determine the asymptotic behaviour of $G_D(x)$ for negative discriminants D and, in particular, to determine G_D. Using a classical result of Wirsing, see e.g. Theorem 3 of [12], one infers that

$$\frac{G_D(x)}{B_D(x)} \sim \prod_{\substack{p \leq x \\ (\frac{D}{p})=-1}} \left(1 - \frac{1}{p^2}\right).$$

From this and the identity (9) it follows that G_D is the positive solution of

$$\pi G_D^2 = \frac{\varphi(|D|)}{|D|} L(1, \chi_D) \prod_{(\frac{D}{p})=-1} \left(1 - \frac{1}{p^2}\right). \tag{10}$$

For more details on $B_D(x)$ and related counting functions the reader is referred to a paper (in preparation) by Moree and Osburn [13]. In [13] it is also pointed out that $B_D(x)$ in fact satisfies an asymptotic result similar to the one given for $D_a(x)$ in Theorem A.7.

The fact that the characteristic functions ξ_d and f_D are so closely connected, can be exploited to give a criterium for the existence of duadic codes in terms of representability by quadratic forms.

Lemma A.8 *Let q be an odd prime power, say $q = p_1^e$ with $p_1 \equiv 3 \pmod 4$. Let n be an odd squarefree integer satisfying $(n, q) = 1$ and suppose, moreover, that n can be written as a sum of two integer squares. A duadic code of length n over $\mathbb{F}_q$ exists iff n can be represented by some primitive positive integral binary quadratic form of discriminant $-p_1$*

Proof: By assumption $-p_1 \equiv 1 \pmod 4$ and hence is a discriminant. The assumption that n is odd and squarefree ensures that $\xi_{-p_1}(n) = f_{-p_1}(n) = f_{-p_1^e}(n)$. The assumption that n can be represented as a sum of two squares, together with the assumption that n is squarefree ensures that n is a product of primes p satisfying $p \equiv 1 \pmod 4$. For every prime $p \equiv 1 \pmod 4$ we have $(-p_1^e/p) = (p_1^e/p)$. It thus follows that $\xi_{-p_1}(n) = f_{-p_1^e}(n) = f_{p_1^e}(n)$.

The result then follows on invoking Theorem 4.3, Lemma A.5 and the fact that, for $(n, D) = 1$, $\xi_D(n) = 1$ iff n is represented by some primitive positive integral binary quadratic form of discriminant D. $\square$

It remains, however, to determine G_a for a general number a. It is well-known from Tauberian theory that one has

$$G_a = \frac{1}{\Gamma(1/2)} \lim_{s \downarrow 1} \sqrt{s-1} F(s),$$

where $F(s) = \sum_{n=1}^{\infty} g_a(n) n^{-s}$. An easy computation shows that

$$(s-1)F(s)^2 = (s-1)\zeta(s) \frac{\varphi(|a|)}{|a|} L(s, \chi_a) \prod_{(\frac{a}{p})=-1} \left(1 - \frac{1}{p^2}\right).$$

On using that the Riemann zeta-function $\zeta(s)$ has a simple pole at $s = 1$ of residue 1, one obtains that

$$\pi G_a^2 = \frac{\varphi(|a|)}{|a|} L(1, \chi_a) \prod_{(\frac{a}{p})=-1} \left(1 - \frac{1}{p^2}\right).$$

Notice that equation (10) is a special case of this.

Acknowledgements. The first author gratefully acknowledges financial support from the University of the Philippines and from the Philippine Council for Advanced Science and Technology Research and Development through the Department of Science and Technology.

The second author likes to thank I. Shparlinski for suggesting Lemma A.5 and D. Gurevich for some helpful remarks.

References

[1] R. A. Brualdi, W. C. Huffman, V. S. Pless, *An Introduction to Algebraic Codes*, in *Handbook of Coding Theory*, V. S. Pless & W. C. Huffman (Editors), Elsevier Science, Amsterdam (1998), pp. 3-139.

[2] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press (2003).

[3] T. W. Hungerford, *Algebra*. Springer-Verlag New York (1974).

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory (Second Edition)*. Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1990.

[5] R.D. James, *The Distribution of Integers Represented by Quadratic Forms*. American Journal of Mathematics, **60** (1938), pp. 737-744.

[6] J. S. Leon, J. M. Masley, V. Pless, *Duadic Codes*. IEEE Transactions on Information Theory, Vol. **IT-30**, No. 5 (1984), pp. 709-714.

[7] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, H. N. Ward, *Self-Dual Codes over GF(4)*. Journal of Combinatorial Theory, Series **A 25** (1978), pp. 288-318.

[8] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North Holland Publishing Company, Amsterdam (1983).

[9] C. Martínez-Pérez, W. Willems, *Self-Dual Extended Cyclic Codes*. Preprint (2004)

[10] P. Moree, *On the divisors of* $a^k + b^k$. Acta Arithmetica **80**, No. 3 (1997), pp. 197-212.

[11] P. Moree, *On primes* p *for which* d *divides* $ord_p(g)$. Funct. Approx. Comment. Math. **33** (2005), pp. 85-95.

[12] P. Moree and J. Cazaran, *On a claim of Ramanujan in his first letter to Hardy*. Exposition. Math. **17**, no. 4, (1999), pp. 289-311.

[13] P. Moree and R. Osburn, *Two-dimensional lattices with few distances*. In preparation.

[14] V. Pless, *Q-Codes*. Journal of Combinatorial Theory, Series **A 43** (1986), pp. 258-276.

[15] M. Smid, *Duadic Codes*. IEEE Transactions on Information Theory, Vol. **IT-33** No. 3 (1987), pp. 432-433.

[16] K.S. Williams, *Note on integers representable by binary quadratic forms*. Canad. Math. Bull. **18** (1975), pp. 123-125.