MATIMYÁS MATEMATIKA
ISSN 0115-6926

Journal of the Mathematical Society of the Philippines
Vol. 40 Nos. 1-2 (2017) pp. 19-30

Ternary Duadic Codes of Prime Lengths

Geronimo L. Magcanta III
Institute of Mathematics
University of the Philippines-Diliman
Quezon City, Philippines
—-

Lilibeth D. Valdez
Institute of Mathematics
University of the Philippines-Diliman
Quezon City, Philippines
ldicuangco@math.upd.edu.ph

Abstract

In 1999, Ding and Pless [2] presented a cyclotomic approach to the construction of all binary duadic codes of prime lengths. They have also calculated the number of all binary duadic codes for a given prime length and the number of those binary duadic codes that are not quadratic residue codes. In 2000, Xin Li et.al [5] constructed and enumerated all binary duadic codes of length $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ where each p_i is a prime.

In this paper, we use the results in [2] and [5] to give a formula for the number of ternary duadic codes for a given prime length. We also illustrate the results by enumerating all ternary duadic codes of lengths $p = 13$ and $p = 61$.
Keywords:

2010 MSC:

1 Introduction

Duadic codes are an important class of cyclic codes. They include the quadratic residue codes which are known for their good error-correcting capabilities. Whereas quadratic residue codes exist only for prime lengths, duadic codes can be defined for composite lengths.

Binary duadic codes were first introduced by Leon, Masley, and Pless in 1984 (see [4]). A cyclotomic approach in constructing binary duadic codes of prime lengths was introduced by Ding and Pless [2]. This was used to count the number of all binary duadic codes for a given prime length. In 2000, Xin Li et.al [5] extended the results in [2] and enumerated all binary duadic codes of length $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ where each p_i is a prime. Then in 2010, Tada, Nishimura and Hiramitsu [6] proved the conjecture of Ding and Pless that there are infinitely many cyclotomic duadic codes of prime lengths that are not quadratic residue codes of prime length p.

In this paper, we consider ternary duadic codes of prime lengths. Following the techniques in [2] and [5], we count the number of ternary duadic codes of length p where p is prime. The paper is organized as follows. We present preliminary results on cyclic codes

and duadic codes over finite fields in the subsequent section. In section 3, we show that every ternary duadic code of prime length is cyclotomic. In the last section, we describe a construction of ternary duadic codes of prime lengths and calculate the number of such codes. Some example are presented at the end of this section.

2 Preliminaries

The basic results discussed in this section can be found in [3]. We assume that the reader is familiar with the theory of cyclic codes (see e.g. [1], [3]).

Let $\mathbb{F}_q$ denote a field with q elements. An $[n, k]$ linear code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The elements of C are called codewords. A code C is cyclic if for every codeword $c_0c_1 \cdots c_{n-1} \in C$, its cyclic shift $c_{n-1}c_0c_1 \cdots c_{n-2}$ is a codeword in C. Using the natural bijective correspondence between codewords $c_0c_1 \cdots c_{n-1} \in C$ and polynomials $c_0 + c_1x + \cdots c_{n-1}x^{n-1} \in \mathbb{F}_q[x]$, cyclic codes over $\mathbb{F}_q$ are seen as ideals in $\mathcal{R}_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$.

The ring $\mathcal{R}_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ is a principal ideal. For a cyclic code C, the unique monic polynomial which divides $x^n - 1$ and which generates the ideal C is called the *generator polynomial* of C. Furthermore, when $\gcd(n, q) = 1$, the ring $\mathcal{R}_n$ is a semi-simple ring. It follows then from the Wedderburn Structure Theorems that each cyclic code C in $\mathcal{R}_n$ contains a unique idempotent which generates the code C. We call this the *generating idempotent* of C.

We equip $\mathbb{F}_q^n$ with the usual inner product $x \cdot y = \sum_{i=1}^{n} x_iy_i$. The dual of a code C over $\mathbb{F}_q$ is $C^\perp = \{y \in \mathbb{F}_q^n | x \cdot y = 0 \ \forall x \in C\}$. It can be shown that if C is a cyclic code, then so is $C^\perp$.

A vector $x = x_0x_1 \ldots x_{n-1}$ in $\mathbb{F}_q^n$ is *even-like* if $\sum_{i=0}^{n-1} x_i = 0$. A code C is said to be even-like if all its vectors are even-like. Otherwise, C is said to be odd-like. Let ε_n denote the subcode of all even-like vectors in $\mathbb{F}_q^n$. The code ε_n is an $[n, n-1]$ cyclic code with generating idempotent $1 - \overline{j}(x)$ where $\overline{j}(x) = \frac{1}{n}(1 + x + x^2 + \ldots x^{n-1})$.

Let C be a cyclic code with generator polynomial $g(x)$. Then the following are equivalent:

1. C is an even-like code.
2. $\overline{j}(x) \notin C$.
3. $(x - 1) \mid g(x)$.

Let a be an integer such that $\gcd(a, n) = 1$. A *multiplier* is a permutation $\mu_a : i \mapsto ai \pmod n$ defined on $\{0, 1, \ldots, n-1\}$. The multiplier μ_a is a permutation of the coordinate positions of a cyclic code in $\mathbb{F}_q^n$. Equivalently, the multiplier μ_a acts on $\mathcal{R}_n$ by $\mu_a(f(x)) \equiv f(x^a) \pmod{x^n - 1}$.

Let C_1 and C_2 be a pair of even-like cyclic codes in $\mathbb{F}_q^n$ with associated even-like generating idempotents $e_1(x)$ and $e_2(x)$, respectively. Then C_1 and C_2 form a pair of *even-like duadic codes* if

1. $e_1(x) + e_2(x) = 1 - \overline{j}(x)$, and
2. there is a multiplier μ_a such that $\mu_a(C_1) = C_2$ and $\mu_a(C_2) = C_1$.

In this case, we say that μ_a gives a splitting for the even-like duadic codes C_1 and C_2. Associated to the pair C_1 and C_2 is the pair of odd-like duadic codes $D_1 = \langle 1 - e_2(x)\rangle$ and $D_2 = \langle 1 - e_1(x)\rangle$.

Theorem 1. *[3] Let $C_1 = \langle e_1(x) \rangle$ and $C_2 = \langle e_2(x) \rangle$ be a pair of even-like duadic codes in $\mathbb{F}_q^n$ given by the splitting μ_a. Then:*

1. $e_1(x)e_2(x) = 0$.
2. $C_1 \cap C_2 = \{0\}$ *and* $C_1 + C_2 = \varepsilon_n$.
3. n *is odd and* C_1 *and* C_2 *each have dimension* $\frac{n-1}{2}$.
4. D_1 *and* D_2 *each have dimension* $\frac{n+1}{2}$.
5. C_i *is the even-like subcode of* D_i *for* $i = 1, 2$.
6. $\mu_a(D_1) = D_2$ *and* $\mu_a(D_2) = D_1$.
7. $D_i \cap D_2 = \langle \overline{j}(x) \rangle$ *and* $D_1 + D_2 = R_n$.
8. $D_i = C_i + \langle \overline{j}(x) \rangle = \langle \overline{j}(x) + e_i(x) \rangle$ *for* $i = 1, 2$.

Let $\gcd(n, q) = 1$ and let s be a non-negative integer less than n. The *q-cyclotomic coset of s modulo n* is the set $\mathcal{C}_s = \{s, sq, sq^2, \ldots, sq^{r-1}\}$ where each element is computed modulo n and r is the smallest positive integer such that $sq^r \equiv s \pmod{n}$. The element s is usually taken as the smallest number in the set. Note that the distinct q-cyclotomic cosets modulo n partition the set $\{0, 1, \ldots, n-1\}$.

Fix a primitive nth root of unity α in some extension of $\mathbb{F}_q$. Then $x^n - 1 = \prod_{i=0}^{n-1} x - \alpha^i$. Let C be a cyclic code with generator $g(x)$. It can be shown that $g(x) = \prod_{i \in T}(x - \alpha^i)$ for some set T which is a union of q-cyclotomic cosets. We refer to the set T as the *defining set* of C. It should be noted that C is an even-like code if and only if $0 \in T$.

Duadic codes can also be described in terms of their defining sets. Let C_1 and C_2 be a pair of even-like cyclic codes in $\mathbb{F}_q^n$ 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

1. $S_1 \cup S_2 = \{1, 2, \ldots, n\}$ and $S_1 \cap S_2 = \emptyset$, and
2. there is a multiplier μ_a such that $\mu_a(S_1) = S_2$ and $\mu_a(S_2) = S_1$.

In this case, we say that the pair of subsets S_1 and S_2 of $\{1, 2, ..., n-1\}$ forms *a splitting of n given by μ_a*. Note that $|S_1| = |S_2| = (n-1)/2$.

3 Cyclotomic Duadic Codes

In this section, we generalize the methods in [2] and [5] to show that all ternary duadic codes of prime length are cyclotomic. Throughout the rest of the paper, we consider the ternary field $\mathbb{F}_3$.

Fix an odd prime $p = 2ef + 1$, and let g be a primitive root modulo p. The *cyclotomic classes of order* $2e$ are defined as

$$D_0 = \left\langle g^{2e} \right\rangle$$

$$D_i = g^i D_0, \qquad i = 1, 2, ..., 2e - 1,$$

where $\left\langle g^{2e} \right\rangle$ denotes the multiplicative group generated by g^{2e}.

Note that $|D_0| = |D_i|, i = 1, 2, ..., 2e - 1$. If $D_i \neq D_j$, then $D_i \cap D_j = \varnothing$.

Let $\mathbb{Z}_{2e}$ denote the ring $\{0, 1, .., 2e - 1\}$ with integer addition and integer multiplication modulo $2e$. For our aim of enumerating the ternary duadic codes of prime lengths, we need to find all pairs (I_1, I_2), where I_1 and I_2 are subsets of $\mathbb{Z}_{2e}$, such that

1) $|I_1| = e$;

2) there exists nonzero $z \in \mathbb{Z}_{2e}$ satisfying

$$I_1 + z = I_2 \text{ and } I_2 + z = I_1 \tag{1}$$

where $I_2 = \mathbb{Z}_{2e} \setminus I_1$.

Such a pair (I_1, I_2) is called a *splitting of* $\mathbb{Z}_{2e}$ *given by* z.

Set

$$S_1 = \bigcup_{i \in I_1} D_i, \qquad S_2 = \bigcup_{i \in I_2} D_i.$$

Then Lemma 1 of [2] states that $g^z S_1 = S_2$ and $g^z S_2 = S_1$.

Lemma 2. *If* $D_i = D_j$ *then* $i = j$.

Proof: Suppose $D_i = D_j$ for some $i, j \in \{0, 1, 2, ..., 2e - 1\}$. Then for each $x_2 = 0, 1, 2, ..., f - 1$, $g^i g^{2ex_2} \equiv g^j g^{2ex_1}$ for some $x_1 \in \{0, 1, 2, ..., f - 1\}$. Thus p divides $i + 2ex_2 - (j + 2ex_1)$. Letting $x = x_2 - x_1$ and $h = i - j$, we see that $2ef + 1$ divides $2ex + h$. Note that $|x| \leq f - 1$, and so $|2ex| \leq 2ef - 2e$. Also, $|h| \leq 2e - 1$. Hence $|2ex + h| \leq 2ef - 1|$. But $2ef + 1$ divides $2ex + h$, and so $2ex + h = 0$. Noting that $|h| < 2e \leq |2ex|$ if $x \neq 0$, we see that $2ex + h = 0$ will only hold if $x = 0$. Thus $h = 0$ and $i = j$.

Lemma 3. *S is the union of 3-cyclotomic cosets if and only if $3S = S$.*

Proof:

($\Rightarrow$) This is clear.

($\Leftarrow$) Suppose that $3S = S$. For any $a \in S$, we have $3^i a \in S$ for any positive integer i. Hence $a = 3^k a$ for some positive integer k. Thus the 3-cyclotomic coset $\mathcal{C}_a$ is a subset of S for each $a \in S$. Hence $S = \bigcup_{a \in S} \mathcal{C}_a$.

For the rest of the sections, we let (I_1, I_2) be a splitting of $\mathbb{Z}_{2e}$ given by z. Let $S_1 = \cup_{i \in I_1} D_i$ and $S_2 = \cup_{i \in I_2} D_i$.

The next results show that the methods in [2] for the binary case also works for the ternary case.

Lemma 4. *Assume* $3 \equiv g^h \pmod{p}$ *where* $1 \leq h \leq p-1$. *Then* S_i *is a union of* 3*-cyclotomic cosets for* $i = 1, 2$ *if and only if*

$$I_1 + h = I_1 \text{ and } I_2 + h = I_2. \tag{2}$$

Proof: By the preceding lemma, S_i is the union of 3-cyclotomic cosets if and only if $3S_i = S_i$. Note that

$$S_i = \bigcup_{j \in I_i} D_j, \text{ and } \qquad 3S_i = g^h S_i = \bigcup_{j \in I_i + h} D_j.$$

Clearly, if $I_i = I_i + h$ then $3S_i = S_i$.

Suppose that $3S_i = S_i$, then

$$\bigcup_{j \in I_i} D_j = \bigcup_{k \in I_i + h} D_k.$$

Let $a \in D_j$ then $a \in D_k$ for some $k \in I_i + h$. Thus $D_j = D_k$. By Lemma 2, for all $j \in I_i$, $j = k$ for some $k \in I_i + h$. Hence $I_i \subseteq I_i + h$. Analogous arguments show that $I_i + h \subseteq I_i$.

Lemma 5. *If* $3 \in D_0$ *then* $3D_i = D_i$ *and* $3S_i = S_i$ *for* $i = 1, 2$.

Proof: The proof is straightforward.

Theorem 6. *If* (1) *and* (2) *are satisfied or* (1) *and* $3 \in D_0$ *are satisfied, then* (S_1, S_2) *is a splitting of* p *given by* μ_{g^z}. *(These codes are called cyclotomic duadic codes of order* $2e$*).*

Proof: By the previous lemmas, $3 \in D_0$ implies $3S_i = S_i$, which means that S_i is a union of 3-cyclotomic cosets. Invoking Lemma 4, we see that $3 \in D_0$ if and only if equation (2) holds. Now (1) implies $g^z S_1 = S_2$ and $g^z S_2 = S_1$, while (2) implies S_i is a union of 3-cyclotomic cosets by Lemma 5.

Now since $I_1 \cap I_2 = \varnothing$ then $D_i \neq D_j$. Hence $D_i \cap D_j = \varnothing$. Thus

$$S_1 \cap S_2 = (\bigcup_{i \in I_1} D_i) \cap (\bigcup_{j \in I_2} D_j) = \varnothing.$$

Also,

$$S_1 \cup S_2 = (\bigcup_{i \in I_1} D_i) \cup (\bigcup_{j \in I_2} D_j) = \bigcup_{k \in I_1 \bigcup I_2} D_k = \bigcup_{k \in \mathbb{Z}_{2e}} D_k \subset \mathbb{Z}_p^*.$$

Note that if $i \neq j$ then $D_i \neq D_j$. Thus for any fixed $j \in I_1$,

$$|S_1| = |\bigcup_{i \in I_1} D_i| = |I_1||D_j| = |I_1||D_0| = ef.$$

Similarly, $|S_2| = ef$. Since $S_1 \cap S_2 = \varnothing$, then

$$|S_1 \cup S_2| = |S_1| + |S_2| = ef + ef = 2ef = p - 1 = |\mathbb{Z}_p^*|.$$

Hence $S_1 \cup S_2 = \mathbb{Z}_p^* = \{1, 2, ..., p-1\}$.

Lemma 7. *Let* p *be a prime such that* $p \equiv \pm 1 \pmod{12}$. *Then* $(p-1)/ord_p(3)$ *is even, where* $ord_p(3)$ *denotes the multiplicative order of* 3 *modulo* p.

Proof:

By the Law of Quadratic Reciprocity, 3 is a quadratic residue modulo p. Let Q be the set of quadratic residues modulo p. Then Q is a multiplicative group of order $(p-1)/2$. Since $3 \in Q$, $ord_p(3) \mid (p-1)/2$. Hence

$$\frac{p-1}{ord_p(3)} = 2\left[\frac{(p-1)/2}{ord_p(3)}\right].$$

Thus $(p-1)/ord_p(3)$ is even.

Lemma 8. *Let p be a prime such that $p \equiv \pm 1 \pmod{12}$ and $f = ord_p(3)$. Then $\{\mathcal{C}_a\}$ forms the set of cyclotomic classes of order $2e$, where $\mathcal{C}_a$ is the 3-cyclotomic coset containing a for $1 \leq a \leq p-1$.*

Proof: By Lemma 7, we can let $p - 1 = 2ef$. Let g be a primitive root of unity modulo p, i.e., $\mathbb{Z}_p^* = \langle g \rangle$ and $ord_p(g) = p-1$. Then $g^b \equiv 3 \pmod{p}$ for some integer b with $1 \leq b \leq p-2$. Since $ord_p(3) = f$, we have

$$g^{bf} \equiv 3^f \equiv 1 \equiv g^{p-1} \pmod{p}.$$

Hence $(p-1) \mid bf$, which implies $2ef \mid bf$. That is, $2e \mid b$. Hence $b = 2ex$, for some $x \in \mathbb{Z}$.

Define $D_0 = \langle g^{2e} \rangle$, the subgroup generated by g^{2e}. Then $3 \in D_0$ since $3 \equiv g^b \pmod{p}$. But $g^b = g^{2ex} = (g^{2e})^x$. Thus

$$\mathcal{C}_1 = \{1, 3, 3^2, ..., 3^{f-1}\} \subseteq D_0.$$

But $|\langle g^{2e} \rangle| = f = D_0$, hence $\mathcal{C}_1 = D_0$. Note that $\mathcal{C}_a = a\mathcal{C}_1$ for each $a \in \mathbb{Z}_p^*$. Therefore,

$$\mathcal{C}_a = a\mathcal{C}_1 = aD_0 = g^i D_0 = D_i$$

where $a \equiv g^i \pmod{p}$.

Theorem 9. *Each ternary duadic code of prime length is cyclotomic.*

Proof: Duadic codes of prime length p exist if and only if there exists a multiplier which gives a splitting of p. Let (S_1, S_2) be that splitting of $p = 2ef + 1$ given by μ_a, where $a \in \mathbb{Z}_p^* = \langle g \rangle$. Then $S_1 \cup S_2 = \{1, 2, ..., p-1\}$, $S_1 \cap S_2 = \varnothing$, $|S_1| = |S_2| = (p-1)/2 = ef$, $g^z S_1 = S_2$ and $g^z S_2 = S_1$, where $g^z \equiv a \pmod{p}$.

Let $S_1 = \bigcup_{a \in A_0} \mathcal{C}_a$, where $\mathcal{C}_a$ is a cyclotomic coset containing a and A_0 is a set of representatives of distinct cyclotomic cosets. We have

$$ef = |S_1| = |\bigcup_{a \in A_0} \mathcal{C}_a| = |\bigcup_{a \in A_0} aC_1| = |\bigcup_{a \in A_0} aD_0| = |\bigcup_{i \in I_1} g^i D_0|$$

$$= |\bigcup_{i \in I_1} D_i| = |I_1||D_j| = |I_1||D_0| = |I_1||C_1| = |I_1|f,$$

where $j \in I_1$, $a \equiv g^i \pmod{p}$ and $i = 1, 2, ..., 2e-1$. Thus $|I_1| = e$. Similarly, $S_2 = \bigcup_{i \in I_2} D_i$ and $|I_2| = e$. Now,

$$\mu_a(S_1) = \mu_a(\bigcup_{i \in I_1} D_i) = g^z(\bigcup_{i \in I_1} D_i) = \bigcup_{i \in I_1} g^z D_i = \bigcup_{i \in I_1} D_{i+z} = \bigcup_{i \in I_1 + z} D_i.$$

Hence $\bigcup_{i \in I_1 + z} D_i = \bigcup_{j \in I_2} D_j$ since $\mu_a(S_1) = S_2$. Thus $I_1 + z = I_2$. Similarly, $I_2 + z = I_1$.

By Lemma 4, S_i is a union of 3-cyclotomic cosets for $i = 1, 2$ if and only if $I_i + h = I_i$, where $3 \equiv g^h \pmod{p}, i \leq h \leq p-1$.

Thus (S_1, S_2) is a splitting of p given by g^z and gives cyclotomic duadic codes.

4 Constructing ternary duadic codes of prime lengths

We will now present a cyclotomic construction of all ternary duadic codes of odd prime lengths and then calculate the number of such codes. In this section, the methods for constructing binary duadic codes of prime length in [2] are shown to also hold true for the ternary case. By invoking the results in the previous section, most of the proofs follow exactly the same arguments as those in [2] and are hence omitted.

Note that we need to consider only cyclotomic classes instead of 3-cyclotomic cosets. In our case, each cyclotomic class is the union of some 3-cyclotomic cosets.

It is well-known that duadic codes of length n over $\mathbb{F}_q$ exist if and only if q is a square modulo n (see for example [3]). Moreover, ternary duadic codes of length $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ exist if and only if $p_i \equiv \pm 1 \pmod{12}$ for $1 \leq i \leq r$.

Let p be a prime such that $p \equiv \pm 1 \pmod{12}$. Note that 3 is a quadratic residue (mod p) and $(p-1)/ord_p(3)$ is even. Define

$$P_e = \{p \mid (p-1)/ord_p(3)) = 2e\}$$

for each $e \geq 1$.

Our discussion in the previous section shows that for all primes p within the same class P_e, we get the same number of duadic codes. Hence we need only to determine all pairs (I_1, I_2) which are splittings of $\mathbb{Z}_{2e}$ given by z. That is, we need to determine all pairs (I_1, I_2) such that

1) $I_1 \subset \mathbb{Z}_{2e}$ with $|I_1| = e$;

2) $\exists z \in \mathbb{Z}_{2e}$ satisfying (1), where $I_2 = \mathbb{Z}_{2e} \setminus I_1$.

Let $N(e)$ denote the number of such pairs.

Ternary duadic codes of length p exist if and only if there is a multiplier which gives a splitting of p. Hence it is sufficient to calculate the number of splittings of p to determine the number of ternary duadic codes of length p.

Lemma 10. *If $I_1 + z = I_2$ and $I_2 + z = I_1$ then*

$$\begin{array}{llll} I_1 + \alpha z = I_1 & \text{and} & I_2 + \alpha z = I_2 & \text{if } \alpha \text{ is even;} \\ I_1 + \alpha z = I_2 & \text{and} & I_2 + \alpha z = I_1 & \text{if } \alpha \text{ is odd.} \end{array}$$

Proof: Note that $I_1 + 2z = I_1 + z + z = I_2 + z = I_1$. Similarly, $I_2 + 2z = I_2$. Hence $I_i + \alpha z = I_i$ if α is even for $i = 1, 2$.

If α is odd then $\alpha = 2n + 1$ for some integer n. Thus,

$$I_1 + \alpha z = I_1 + (2n+1)z = I_1 + 2nz + z = I_1 + z = I_2.$$

Similarly, $I_2 + \alpha z = I_1$ if α is odd.

Lemma 11. *Suppose that the subgroups $\langle d \rangle$ and $\langle d_1 \rangle$ of $\mathbb{Z}_{2e}$ are equal. Then*

$$I_1 + d_1 = I_2 \quad \text{and} \quad I_2 + d_1 = I_1$$

if and only if

$$I_1 + d = I_2 \text{ and } I_2 + d = I_1.$$

Proof: Assume $I_1 + d = I_2$ and $I_2 + d = I_1$. Since $\langle d \rangle = \langle d_1 \rangle$, then

$$d_1 \equiv \alpha d \,(\text{mod } 2e) \quad \text{and} \quad d \equiv \beta d_1 \,(\text{mod } 2e).$$

Suppose that α is even. Then $I_1 + \alpha d = I_1$ and $I_2 + \alpha d = I_2$ by Lemma 10. Note that if $I_1 + x = I_1$ and $I_2 + x = I_2$ then for all α, $I_1 + \alpha x = I_1$ and $I_2 + \alpha x = I_2$. Hence $I_1 + \beta\alpha d = I_1$ and $I_2 + \beta\alpha d = I_2$ for all β. Thus $I_1 + \beta d_1 = I_1$ and $I_2 + \beta d_1 = I_2$, which implies that $I_1 + d = I_1$ and $I_2 + d = I_2$, a contradiction. So α must be odd. By Lemma 10, $I_1 + \alpha d = I_2$ *and* $I_2 + \alpha d = I_1$, and so $I_1 + d_1 = I_2$ and $I_2 + d_1 = I_1$.

Conversely, suppose $I_1 + d_1 = I_2$ and $I_2 + d_1 = I_1$. By a similar argument, we can also show that β is odd. By Lemma 10, $I_1 + \beta d_1 = I_2$ and $I_2 + \beta d_1 = I_1$. Hence $I_1 + d = I_2$ and $I_2 + d = I_1$.

Theorem 12. *Let $e = 2^s e_1$, where e_1 is odd. Then*

$$N(e) = \sum_{j=0}^{s} 2^{2^j e_1 - 1} \geq 2^{e-1}.$$

Proof:
Consider the equation

$$I_1 + d = I_2, \qquad I_2 + d = I_1. \tag{3}$$

Let $I(d)$ denote the set of solutions (I_1, I_2) of (3).

If $d_1 \in \mathbb{Z}_{2e}$, then $\langle d \rangle = \langle d_1 \rangle$ for some d dividing $2e$. Hence when counting pairs (I_1, I_2) satisfying Equation (3), it suffices to assume that $d \mid 2e$ by Lemma 11. Suppose $d \mid 2e$ but $d \nmid e$. Then $\alpha = 2e/d$ is odd and so $\alpha d \equiv 0\,(\text{ mod } 2e)$ for some odd α. Hence by Lemma 10, $I_1 + d = I_2$ and $I_2 + d = I_1$ implies $I_1 + \alpha d = I_2$ and $I_2 + \alpha d = I_1$. Hence $I_1 + 0 = I_2$ and $I_2 + 0 = I_1$, a contradiction. Thus $d \mid e$. It follows that we only need to consider Equation (3) for values of d dividing e.

Let $d \in \mathbb{Z}_{2e}$ divide e. We first calculate the cardinality of $I(d)$. Define $h = e/d$. By Equation (3), we have $I_i + 2d = I_i$ for $i = 1, 2$. Thus there are d integers $a_0, a_1, ..., a_{d-1}$ of $\mathbb{Z}_{2e}$ such that

$$a_i \not\equiv a_j + d \,(mod\ 2e) \qquad \forall i, j$$

and

$$I_1 = \bigcup_{i=0}^{d-1} A_1^{(i)} \qquad I_2 = \bigcup_{i=0}^{d-1} A_2^{(i)}$$

where

$$A_1^{(i)} = \{a_i + 2dk \mid k = 0, 1, ..., h-1\}, \quad \text{and}$$

$$A_2^{(i)} = \{a_i + 2dk + d \mid k = 0, 1, ..., h-1\}.$$

Thus $\mathbb{Z}_{2e}$ is partitioned into d pairs

$$(A_1^{(i)}, A_2^{(i)}), \qquad i = 0, 1, ..., d-1$$

where

$$A_1^{(i)} + d = A_2^{(i)} \quad \text{and} \quad A_1^{(i)} + d = A_0^{(i)}.$$

Hence I_1 includes one and only one of each pair $(A_1^{(i)}, A_2^{(i)})$, and there are 2^d choices for I_1. But we regard (I_1, I_2) and (I_2, I_1) as the same. It follows that

$$|I(d)| = 2^d/2 = 2^{d-1}. \tag{4}$$

Let d_1 and d_2 be two divisors of e such that $d_1 \mid d_2$. We now investigate the relationship between $I(d_1)$ and $I(d_2)$. Define $m = d_2/d_1$.

Suppose m is odd. Let $(I_1, I_2) \in I(d_1)$, then $I_1 + d_1 = I_2$ and $I_2 + d_1 = I_1$. Hence $I_1 + md_1 = I_2$ and $I_2 + md_1 = I_1$, which implies $I_1 + d_2 = I_2$ and $I_2 + d_2 = I_1$. Thus $(I_1, I_2) \in I(d_2)$ and hence $I(d_1) \subseteq I(d_2)$.

Suppose m is even. Let $(I_1, I_2) \in I(d_1)$, then $I_1 + d_1 = I_2$ and $I_2 + d_1 = I_1$. Thus $I_1 + md_1 = I_1$ and $I_2 + md_1 = I_2$. This implies $I_1 + d_2 = I_1$ and $I_2 + d_2 = I_2$. And so $(I_1, I_2) \notin I(d_2)$ Thus $I(d_1) \cap I(d_2) = \varnothing$.

We then consider the divisors of e. For each pair (d_1, d_2) from the set

$$H = \{e_1, 2e_1, 2^2e_1, ..., 2^se_1\}$$

where $d_1 \leq d_2$, we see that d_2/d_1 is even. Thus $I(d_1) \cap I(d_2) = \varnothing$. On the other hand, for any divisor d_1 of e, there exists $d_2 \in H$ such that d_2/d_1 is odd. In this case, $I(d_1) \subseteq I(d_2)$. Hence the set of solutions of Equation (3) for all d is

$$\bigcup_{j=0}^{s} I(2^j e_1).$$

Thus

$$N(e) = \sum_{j=0}^{s} \left|I(2^j e_1)\right| = \sum_{j=0}^{s} 2^{2^j e_1 - 1} = 2^{e-1} + \sum_{j=0}^{s-1} 2^{2^j e_1 - 1} \geq 2^{e-1}.$$

Corollary 13. *$N(e) = 2^{e-1}$ if and only if e is odd.*

Example 14. *Let $p = 13$. Then*

$$2e = \frac{p-1}{ord_p(3)} = \frac{12}{3} = 4.$$

Therefore, $e = 2$.

Applying Theorem 12 to solve for $N(e)$, where $e = 2$, we have $e = 2^s e_1 = 2$, where e_1 is odd. Hence, $e_1 = 1$ and $s = 1$. Thus,

$$N(2) = \sum_{j=0}^{s} 2^{2^j e_1 - 1} = \sum_{j=0}^{1} 2^{2^j (1) - 1} = 1 + 2 = 3.$$

The 3-cyclotomic cosets modulo 13 are $\mathcal{C}_0 = \{0\}$, $\mathcal{C}_1 = \{1, 3, 9\}$, $\mathcal{C}_2 = \{2, 6, 5\}$, $\mathcal{C}_4 = \{4, 12, 10\}$, $\mathcal{C}_7 = \{7, 8, 11\}$. The splittings are

$$(\mathcal{C}_1 \cup \mathcal{C}_2, \mathcal{C}_4 \cup \mathcal{C}_7)$$

$$(\mathcal{C}_1 \cup \mathcal{C}_4, \mathcal{C}_2 \cup \mathcal{C}_7)$$

$$(\mathcal{C}_1 \cup \mathcal{C}_7, \mathcal{C}_2 \cup C_4),$$

showing that there are indeed three splittings.

Example 15. *Let $p = 61$. Then*

$$2e = \frac{p-1}{ord_p(3)} = \frac{60}{10} = 6.$$

Therefore, $e = 3$. *By Corollary 13,*

$$N(3) = 2^{3-1} = 4.$$

The 3*-cyclotomic cosets modulo* 61 *are*

$$\mathcal{C}_0 = \{0\},$$
$$\mathcal{C}_1 = \{1, 3, 9, 27, 20, 60, 58, 52, 34, 41\},$$
$$\mathcal{C}_2 = \{2, 6, 18, 54, 40, 59, 55, 43, 7, 21\},$$
$$\mathcal{C}_4 = \{4, 12, 36, 47, 19, 57, 49, 25, 14, 42\},$$
$$\mathcal{C}_5 = \{5, 15, 45, 13, 39, 56, 46, 16, 48, 22\},$$
$$\mathcal{C}_8 = \{8, 24, 11, 33, 38, 53, 37, 50, 28, 23\},$$
$$\mathcal{C}_{10} = \{10, 30, 29, 26, 17, 51, 31, 32, 35, 44\}.$$

The splittings are

$$(\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_4, \mathcal{C}_5 \cup \mathcal{C}_8 \cup \mathcal{C}_{10})$$
$$(\mathcal{C}_1 \cup \mathcal{C}_4 \cup \mathcal{C}_5, \mathcal{C}_2 \cup \mathcal{C}_8 \cup \mathcal{C}_{10})$$
$$(\mathcal{C}_1 \cup \mathcal{C}_5 \cup \mathcal{C}_{10}, \mathcal{C}_8 \cup \mathcal{C}_2 \cup \mathcal{C}_4)$$
$$(\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_{10}, \mathcal{C}_8 \cup \mathcal{C}_5 \cup \mathcal{C}_4),$$

which shows that there are indeed four splittings.

Next we give an explicit description of the construction of ternary duadic codes of prime length. The construction follows from the proof of Theorem 12 and is taken from the methods explicitly described in [2] for the binary case.

To construct all ternary duadic codes of prime length $p \in P_e$, we let $e = 2^s e_1$, where e_1 is odd, and let $H = \{e_1, 2e_1, 2^2 e_1, ..., 2^s e_1\}$. The procedure of this construction is as follows.

Step 1 : For each $d \in H$ do the following:

1. Partition $\mathbb{Z}_{2e}$ into d pairs $(A_0^{(i)}, A_1^{(i)})$ as described in the proof of Theorem 12 of [2].
2. Without loss of generality, we require that $0 \in A_0^{(0)}$. Then fix $A_0^{(0)}$ as the root of a complete binary tree of depth d. Write $A_0^{(i)}$ and $A_1^{(i)}$ as the two children of each node at level $i-1$ for all i. This completes the binary tree associated with $d \in H$. Taking the union of all subsets of each branch gives an I_0 and therefore a splitting $(I_0, I_1) \in I(d)$.

Step 2 : Form the union $\bigcup_{d \in H} I(d)$.

When e is odd, the above procedure is simplified as follows.

Step 1 : Divide the elements of $\mathbb{Z}_{2e}$ into the following groups:

$$(0, e), (1, e+1), \ldots, (e-1, 2e-1).$$

Step 2 : Fix $a_0 = 0$ as the root of a binary tree. Each a_i takes i and $i + e$ for $i \geq 1$, and the values are written at level i. Doing this at each level completes the binary tree. The branches of the binary tree give all 2^{e-1} possible $I_0 s$.

The next examples illustrate how we can construct ternary duadic codes of prime length $p \in P_e$.

Example 16. *We will construct the* 2^2 *ternary duadic codes of length* $p \in P_3$. *This includes the case when* $p = 61$ *(see Example 15). Here* $e = 3$, *so we partition* $\mathbb{Z}_{2e}$ *into the following groups:* $(0, 3), (1, 4), (2, 5)$. *Thus* (I_0, z) *can be one of* $(\{0, 1, 2\}, 3), (\{0, 1, 5\}, 3), (\{0, 2, 4\}, 3)$ *or* $(\{0, 4, 5\}, 3)$.

For instance, when $p = 61$, *each* (I_0, z) *corresponds to a desired splitting of* 61 *as given in Example 15.*

Example 17. *We will construct the 3 ternary duadic codes of length* $p \in P_2$. *(This includes* $p = 13$ *as in Example 14). In this case,* $H = \{1, 2\}$.

If $d = 2$ *then* $h = 1$, *so we have*

$$A_0^0 = \{0\}, \qquad A_1^0 = \{2\}$$

$$A_0^1 = \{1\}, \qquad A_1^1 = \{3\}$$

Thus $(I_0, 2) = (\{0, 1\}, 2), (\{0, 3\}, 2)$.

If $d = 1$ *then* $h = 2$, *so we have*

$$A_0^0 = \{0, 2\}, \qquad A_1^0 = \{1, 3\}$$

Thus $(I_0, 1) = (\{0, 2\}, 1)$.

Therefore (I_0, z) *can be any of* $(\{0, 1\}, 2), (\{0, 3\}, 2)$ *or* $(\{0, 2\}, 1)$.

When $p = 13$, *the three possible* $(I_0, z)s$ *correspond to the three splittings of* $p = 31$ *as in Example 14.*

5 References

[1] *R.A. Brualdi, W.C. Huffman and V. Pless, An introduction to algebraic codes, in Handbook of Coding Theory, V. Pless, W.C. Huffman (Eds.), Elsevier Science, Amsterdam, 1998, pp. 3139.*

[2] *C. Ding and V. Pless, "Cyclotomy and Duadic Codes of Prime Lengths", IEEE Transactions on Information Theory, Vol. 45, No.2 pp. 453-466, 1999.*

[3] *W. C. Huffman and V. Pless, "Fundamentals of Error-Correcting Codes", Cambridge University Press 2003.*

[4] *J. Leon, J. Masley and V. Pless, "Duadic Codes", IEEE Transactions on Information Theory, pp. 709-714, September 1984.*

[5] *X. Li, W. Sun, Y. Yang, and Z. Zhang, "Enumeration and Construction of All Binary Duadic Codes", ISIT, Sorrento, Italy, June 25-30, 2000.*

[6] *H. Tada, S. Nishimura, and T. Hiramatsu, "Cyclotomy and its application to duadic codes", Finite Fields and Their Applications, Elsevier Science, Vol 16, pp. 413, 2010.*

This page is intentionally left blank