The Minimum Distance of the Duals of Binary Irreducible Cyclic Codes

Cunsheng Ding, *Member, IEEE*, Tor Helleseeth, *Fellow, IEEE*, Harald Niederreiter, and Chaoping Xing

Abstract—Irreducible cyclic codes have been an interesting subject of study for many years. The weight distribution of some of them have been determined. In this paper, we determine the minimum distance and certain weights of the duals of binary irreducible cyclic codes. We show that the weight distribution of these codes is determined by the cyclotomic numbers of certain order. As a byproduct, we describe a class of double-error correcting codes.

Index Terms—Codes, cyclotomy, irreducible cyclic codes.

I. INTRODUCTION

IRREDUCIBLE cyclic codes have been an interesting subject of study for many years due to several facts. First, the weight distribution of some of them is relatively easy to determine partly because they have small dimensions. In fact, some irreducible cyclic codes have only two weights [9], [1]. In the semiprimitive cases and several special cases, the weight distribution of irreducible cyclic codes has been determined (see Baumert and McEliece [1], Delsarte and Goethals [9], Helleseeth, Kløve, and Mykkeltveit [14]). Second, in certain cases such as the semiprimitive cases, powerful mathematical tools, such as cyclotomy and exponential sums, can be applied to determine the weight distributions (see, for example, Niederreiter [20]). Numerical examples of the weight distribution of certain minimal cyclic codes are given by MacWilliams and Seery [17]. However, it should be noted that the weight distribution of only a few classes of irreducible cyclic codes is known.

In contrast, little has been done on the determination of the weight distribution of the duals of irreducible cyclic codes. The purpose of this paper is to determine the minimum distance and some weights of the duals of certain classes of binary irreducible cyclic codes. We show that the weight distribution of the duals of binary irreducible cyclic codes is totally determined by the cyclotomic numbers of certain order. This demonstrates

again that cyclotomy could be quite useful in studying certain codes (see [11], [10], [12] for some recent applications of cyclotomy in coding theory). As a byproduct, we describe a class of double-error correcting codes obtained from some of the duals of binary irreducible cyclic codes. We also present a number of open problems on these codes.

II. A CYCLOTOMIC APPROACH TO THE CODES

Let α be a primitive element of $\text{GF}(2^m)$, and let $\ell = (2^m - 1)/e$, where the integer e with $1 \leq e < 2^m - 1$ divides $2^m - 1$. We use $m_e(x)$ to denote the minimum polynomial of α^i over $\text{GF}(2)$.

Lemma 1: Let $\text{ord}_\ell(2)$ denote the order of 2 modulo ℓ . Then $\deg(m_e(x)) = \text{ord}_\ell(2)$.

Proof: Consider the cyclotomic coset modulo $2^m - 1$ containing e

$$S_e = \{e, e2, e2^2, \dots, e2^{r-1}\} \subseteq \mathbf{Z}_{2^m-1},$$

where r is the least positive integer such that

$$e \equiv e2^r \pmod{2^m - 1}.$$

Note that $e\ell = 2^m - 1$. Obviously, $e(2^i - 1) \equiv 0 \pmod{2^m - 1}$ if and only if $2^i - 1 \equiv 0 \pmod{\ell}$. Hence, $r = \text{ord}_\ell(2)$. It follows that

$$m_e(x) = \prod_{j \in S_e} (x - \alpha^j).$$

The conclusion then follows. $\square$

Clearly, $m_e(x) | (x^\ell - 1)$ as all the roots of $m_e(x)$ are roots of $x^\ell - 1$. Define

$$R_\ell = \text{GF}(2)[x]/(x^\ell - 1).$$

As usual, we identify a vector

$$c = (c_0, c_1, \dots, c_{\ell-1}) \in \text{GF}(2)^\ell$$

with the polynomial

$$c(x) = c_0 + c_1x + \dots + c_{\ell-1}x^{\ell-1} \in R_\ell.$$

Consider the binary cyclic code of length ℓ defined by

$$\mathcal{C}_e = \{c(x) \in R_\ell | c(\alpha^e) = 0\}.$$

This code is cyclic and generated by the irreducible polynomial $m_e(x)$. Also $c(x) = 1 + x + x^2 + \dots + x^{\ell-1} \in \mathcal{C}_e$. Hence, $\mathcal{C}_e$ is self-complementary. As usual, let A_i denote the number

Manuscript received September 27, 2001; revised May 20, 2002. This work was supported by a grant from the Research Grants Council of the Hong Kong Special Administration Region, China (Project HKUST6179/01E), by the Singapore MOE-ARF under Grant R-146-000-029-112, and by a grant from The Norwegian Research Council. The main part of this work was carried out when the authors were attending the Research Program on Coding Theory and Data Integrity at the Institute for Mathematical Sciences of the National University of Singapore in 2001.

C. Ding is with the Department of Computer Science, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (e-mail: cding@cs.ust.hk).

T. Helleseeth is with the Department of Informatics, University of Bergen, 5020 Bergen, Norway (e-mail: torh@ii.uib.no).

H. Niederreiter and C. Xing are with the Department of Mathematics, National University of Singapore, Singapore 117543 (e-mail: nied@math.nus.edu.sg; matxcp@nus.edu.sg).

Communicated by P. Solé, Associate Editor for Coding Theory.
Publisher Item Identifier 10.1109/TIT.2002.802593.

of codewords of Hamming weight i in the code $\mathcal{C}_e$. Since $\mathcal{C}_e$ is self-complementary, $A_i = A_{\ell-i}$ for each i .

Let $\mathbf{F} = \text{GF}(2^{\text{ord}_\ell(2)})$ be the splitting field of $x^\ell - 1$ over $\text{GF}(2)$ and let $\beta = \alpha^e$. Define

$$\mathcal{C}_e^\perp = \{ (\text{Tr}(\lambda), \text{Tr}(\lambda\beta), \dots, \text{Tr}(\lambda\beta^{\ell-1})) \mid \lambda \in \mathbf{F} \}$$

where $\text{Tr}(\cdot)$ is the trace function from $\mathbf{F} = \text{GF}(2^{\text{ord}_\ell(2)})$ to $\text{GF}(2)$. $\mathcal{C}_e^\perp$ is called an *irreducible cyclic code* with length ℓ and dimension $\text{ord}_\ell(2)$. It is easy to prove that $\mathcal{C}_e^\perp$ and $\mathcal{C}_e$ are duals of each other.

Proposition 2: The code $\mathcal{C}_e$ has parameters $[\ell, \ell - \text{ord}_\ell(2), d \geq 3]$, i.e., length ℓ , dimension $\ell - \text{ord}_\ell(2)$, and minimum distance $d \geq 3$.

Proof: It is clear that $c(x) \in \mathcal{C}_e$ if and only if $m_e(x) \mid c(x)$. Then by Lemma 1, the dimension of $\mathcal{C}_e$ is $\ell - \text{ord}_\ell(2)$. Since the multiplicative order of α^e is $\ell > 1$, the minimum distance of the code is at least 3. $\square$

Proposition 3: If an integer $h > 1$ divides ℓ , then the minimum distance d of $\mathcal{C}_e$ is at most h .

Proof: Note that $(\alpha^{e(\ell/h)})^h = 1$ gives

$$1 + \alpha^{e(\ell/h)} + \alpha^{2e(\ell/h)} + \dots + \alpha^{(h-1)e(\ell/h)} = 0.$$

Thus, $\mathcal{C}_e$ has a codeword of weight h . $\square$

Let $D_0^{(e)}$ be the multiplicative subgroup of $\mathbf{F}^*$ generated by α^e . Define $D_i^{(e)} = \alpha^i D_0^{(e)}$ to be the cosets for all i with $1 \leq i \leq e-1$. These $D_i^{(e)}$ are called the *cyclotomic classes* of order e . The *cyclotomic numbers* of order e are defined as

$$(i, j)_e = \left| \left((1 + D_i^{(e)}) \cap D_j^{(e)} \right) \right|$$

where $0 \leq i \leq e-1$ and $0 \leq j \leq e-1$.

Theorem 4: The code $\mathcal{C}_e$ has parameters $[\ell, \ell - \text{ord}_\ell(2), 3]$ if and only if $(0, 0)_e \neq 0$.

Proof: If $\mathcal{C}_e$ has a codeword of weight 3, then

$$\alpha^{ei_1} + \alpha^{ei_2} + \alpha^{ei_3} = 0$$

for three integers $0 \leq i_1 < i_2 < i_3 \leq \ell - 1$. Therefore,

$$1 + \alpha^{e(i_2-i_1)} + \alpha^{e(i_3-i_1)} = 0.$$

Hence, $\alpha^{e(i_3-i_1)} \in (1 + D_0^{(e)}) \cap D_0^{(e)}$ and $(0, 0)_e \neq 0$. On the other hand, if $(0, 0)_e \neq 0$, then $\alpha^{ej} \in (1 + D_0^{(e)}) \cap D_0^{(e)}$ and

$$1 + \alpha^{ei} + \alpha^{ej} = 0$$

for some $0 < i < j < \ell$. Hence, $\mathcal{C}_e$ has a codeword of weight 3. $\square$

In the case $(0, 0)_e \neq 0$, we are interested in determining the number A_3 of codewords of weight 3 in $\mathcal{C}_e$.

Theorem 5: If $(0, 0)_e \neq 0$, then for the $[\ell, \ell - \text{ord}_\ell(2), 3]$ cyclic code $\mathcal{C}_e$ we have

$$A_3 = A_{\ell-3} = \frac{\ell(0, 0)_e}{3!}.$$

Proof: Set $\beta = \alpha^e$. Then for any $0 \leq j \leq \ell - 1$

$$\beta^j \in (1 + D_0^{(e)}) \cap D_0^{(e)}$$

if and only if there is an $i \neq j$ with $0 \leq i \leq \ell - 1$ such that $1 + \beta^i = \beta^j$. Such a $(0, i, j) \in \mathbf{Z}_\ell^3$ is called a *cyclotomic triple*. Obviously, if $(0, i, j)$ is a cyclotomic triple, so is $(0, j, i)$. In view of this, we now consider only cyclotomic triples $(0, i, j)$ with $0 < i < j < \ell$.

Two cyclotomic triples $(0, i_1, j_1)$ and $(0, i_2, j_2)$ are called *equivalent* if the triple $(0, i_2, j_2)$ is some cyclic shift of $(a, i_1 + a, j_1 + a)$ for some integer $0 \leq a \leq \ell - 1$, where these additions are modulo ℓ . Clearly, this is an equivalence relation among the set of cyclotomic triples.

If $(0, i, j)$ is a cyclotomic triple, so are

$$(0, j - i, \ell - i), \quad (0, \ell - j, \ell - j + i).$$

In fact, the three form an equivalence class, denoted $\overline{(0, i, j)}$. It is easy to check that

$$|\overline{(0, i, j)}| = \begin{cases} 1, & \text{if } 3 \mid \ell \text{ and } (i, j) = (\ell/3, 2\ell/3) \\ 3, & \text{otherwise.} \end{cases}$$

Each codeword

$$\begin{aligned} c(x) &= x^{i_1} + x^{i_2} + x^{i_3} \\ &= x^{i_1} (1 + x^{i_2-i_1} + x^{i_3-i_1}) \end{aligned}$$

of weight 3 in $\mathcal{C}_e$ gives a unique cyclotomic triple $(0, i_2 - i_1, i_3 - i_1)$, where $0 \leq i_1 < i_2 < i_3 < \ell$. On the other hand, if $(i, j) \neq (\ell/3, 2\ell/3)$, the equivalence class $\overline{(0, i, j)}$ gives ℓ different codewords of weight 3

$$c(x) = x^h (1 + x^i + x^j)$$

where $0 \leq h \leq \ell - 1$, and this equivalence class contributes exactly 6 to the cyclotomic number $(0, 0)_e$.

If $3 \mid \ell$, then $(\alpha^{e\ell/3})^3 - 1 = 0$ gives

$$1 + \beta^{\ell/3} + \beta^{2\ell/3} = 0.$$

Hence in this case $(0, 0)_e \neq 0$ and $(0, \ell/3, 2\ell/3)$ is indeed a cyclotomic triple, and the equivalence class $\overline{(0, \ell/3, 2\ell/3)}$ has only one element. Note that the triple $(0, \ell/3, 2\ell/3)$ contributes exactly 2 to the cyclotomic number $(0, 0)_e$ and gives $\ell/3$ different codewords of $\mathcal{C}_e$.

We use $\mathcal{C}[\overline{(0, i, j)}]$ to denote the codewords of weight 3 of the form $x^h (1 + x^i + x^j)$. It is easily seen that

$$\mathcal{C}[\overline{(0, i_1, j_1)}] \cap \mathcal{C}[\overline{(0, i_2, j_2)}] = \emptyset$$

if the cyclotomic triples $(0, i_1, j_1)$ and $(0, i_2, j_2)$ are not equivalent. Hence, in the case $3 \mid \ell$, we have

$$A_3 = \frac{\ell[(0, 0)_e - 2]}{3!} + \frac{\ell}{3} = \frac{\ell(0, 0)_e}{3!}.$$

In the case $\ell \not\equiv 0 \pmod{3}$,

$$A_3 = \frac{\ell(0, 0)_e}{3!}. \quad \square$$

The proof of Theorem 5 also proves the following conclusion.

Corollary 6: Let m be even and let $\ell \equiv 0 \pmod{3}$. Then the cyclotomic number $(0, 0)_e \neq 0$ and the cyclic code $\mathcal{C}_e$ has parameters $[\ell, \ell - \text{ord}_\ell(2), 3]$ with

$$A_3 = A_{\ell-3} = \frac{\ell(0, 0)_e}{3!}.$$

Remark: It is easily seen that $\mathcal{C}_1$ is a $[2^m-1, 2^m-1-m, 3]$ code, which is equivalent to the $[2^m-1, 2^m-1-m, 3]$ Hamming code. So we are interested only in the case $e > 1$.

It is possible that the minimum distance d of $\mathcal{C}_e$ is 4. One natural question is whether it is possible in this case to express the total number of codewords of weight 4 in terms of cyclotomic numbers of order e . The answer is positive. We give such an expression later in Theorem 8.

Lemma 7: The number N_t of solutions $(z_1, z_2, \dots, z_t)$ of the equation

$$z_1^e + z_2^e + \dots + z_t^e = 0 \quad (1)$$

in $\text{GF}(2^m)$ is given by

$$N_t = 2^{-m} \left(2^{mt} + \ell \sum_{i=0}^{e-1} (1 + ey_i)^t \right)$$

where the y_i satisfy the following system of equations:

$$\begin{aligned} -1 &= \sum_{i=0}^{e-1} y_i \\ y_i^2 - \ell &= \sum_{j=0}^{e-1} (i-j, i-j)_e y_j, \quad i = 0, 1, \dots, e-1 \\ y_i y_j &= \sum_{h=0}^{e-1} (i-h, j-h)_e y_h, \quad 0 \leq i \neq j \leq e-1 \end{aligned}$$

and the $(i, j)_e$ are cyclotomic numbers of order e .

Proof: Let $D_i^{(e)}$ denote the cyclotomic classes of order e . Note that

$$\begin{aligned} N_t 2^m &= \sum_{z_1, \dots, z_t \in \text{GF}(2^m)} \sum_{u \in \text{GF}(2^m)} (-1)^{\text{Tr}_1^m(u \sum_{i=1}^t z_i^e)} \\ &= \sum_{u \in \text{GF}(2^m)} \prod_{i=1}^t \left(\sum_{z_i \in \text{GF}(2^m)} (-1)^{\text{Tr}_1^m(uz_i^e)} \right) \\ &= \sum_{u \in \text{GF}(2^m)} \left(\sum_{z \in \text{GF}(2^m)} (-1)^{\text{Tr}_1^m(uz^e)} \right)^t \\ &= 2^{mt} + \sum_{0 \neq u \in \text{GF}(2^m)} \left(\sum_{z \in \text{GF}(2^m)} (-1)^{\text{Tr}_1^m(uz^e)} \right)^t \\ &= 2^{mt} + \sum_{i=0}^{e-1} \sum_{u \in D_i^{(e)}} \left(\sum_{z \in \text{GF}(2^m)} (-1)^{\text{Tr}_1^m(uz^e)} \right)^t \end{aligned}$$

$$\begin{aligned} &= 2^{mt} + \sum_{i=0}^{e-1} \sum_{u \in D_i^{(e)}} \left(1 + e \sum_{z \in D_0^{(e)}} (-1)^{\text{Tr}_1^m(uz)} \right)^t \\ &= 2^{mt} + \ell \sum_{i=0}^{e-1} \left(1 + e \sum_{z \in D_i^{(e)}} (-1)^{\text{Tr}_1^m(z)} \right)^t \\ &= 2^{mt} + \ell \sum_{i=0}^{e-1} (1 + ey_i)^t, \end{aligned}$$

where

$$y_i = \sum_{z \in D_i^{(e)}} (-1)^{\text{Tr}_1^m(z)}$$

and are called the *Gaussian periods*. We now prove that these y_i satisfy the system of equations in the theorem.

We define for each $i = 0, 1, \dots, e-1$ the multiset

$$D(i) = \{x - y : x, y \in D_i^{(e)}, x \neq y\}$$

where an element a appears in $D(i)$ as many times as $x - y$ takes on the value a . We now calculate $\sum_{x \in D(i)} (-1)^{\text{Tr}_1^m(x)}$ in two different ways.

First, $D_i^{(e)}$ is partitioned into two parts, $D_i^{(e)} \cap T_0$ and $D_i^{(e)} \cap T_1$, where

$$T_j = \{x \in \text{GF}(2^m) : \text{Tr}_1^m(x) = j\}, \quad j = 0, 1.$$

Define $a_i = |D_i^{(e)} \cap T_0|$. Then $|D_i^{(e)} \cap T_1| = \ell - a_i$. It follows that

$$\begin{aligned} \sum_{x \in D(i)} (-1)^{\text{Tr}_1^m(x)} &= a_i(a_i - 1) + (\ell - a_i)(\ell - a_i - 1) - 2a_i(\ell - a_i) \\ &= (2a_i - \ell)^2 - \ell. \end{aligned}$$

Second, by the definition of cyclotomic numbers and classes,

$$|(D_i^{(e)} + x) \cap D_j^{(e)}| = (i - h, j - h)_e, \quad \text{for all } x \in D_h^{(e)}.$$

Thus, each element of $D_j^{(e)}$ appears in $D(i)$ exactly $(i-j, i-j)_e$ times, where $(i-j, i-j)_e$ denotes the cyclotomic number of order e . It follows that

$$\begin{aligned} \sum_{x \in D(i)} (-1)^{\text{Tr}_1^m(x)} &= \sum_{j=0}^{e-1} \left[\sum_{x \in D_j^{(e)}} (-1)^{\text{Tr}_1^m(x)} \right] (i-j, i-j)_e \\ &= \sum_{j=0}^{e-1} (i-j, i-j)_e y_j. \end{aligned}$$

It is easily seen that $y_i = 2a_i - \ell$ for each i . Therefore,

$$y_i^2 - \ell = \sum_{j=0}^{e-1} (i-j, i-j)_e y_j$$

for all i with $0 \leq i \leq e-1$. In addition

$$\sum_{i=0}^{e-1} y_i = \sum_{z \neq 0} (-1)^{\text{Tr}_1^m(x)} = -1.$$

Define now for each ordered pair (i, j) with $i \neq j$ the multiset

$$D(i, j) = \{x - y : x \in D_j^{(e)}, y \in D_i^{(e)}\}.$$

We similarly compute $\sum_{x \in D(i, j)} (-1)^{\text{Tr}_1^m(x)}$ in two different ways.

On the one hand

$$\begin{aligned} \sum_{x \in D(i, j)} (-1)^{\text{Tr}_1^m(x)} &= a_i a_j + (\ell - a_i)(\ell - a_j) - a_i(\ell - a_j) - a_j(\ell - a_i) \\ &= (2a_i - \ell)(2a_j - \ell) = y_i y_j. \end{aligned}$$

On the other hand, each element of $D_h^{(e)}$ appears in $D(i, j)$ exactly $(i - h, j - h)_e$ times. It follows that

$$\begin{aligned} \sum_{x \in D(i, j)} (-1)^{\text{Tr}_1^m(x)} &= \sum_{h=0}^{e-1} \left[\sum_{x \in D_h^{(e)}} (-1)^{\text{Tr}_1^m(x)} \right] (i - h, j - h)_e \\ &= \sum_{h=0}^{e-1} (i - h, j - h)_e y_h. \end{aligned}$$

This completes the proof. $\square$

Theorem 8: If $\mathcal{C}_e$ has minimum distance $d \geq 4$, then

$$A_4 = \frac{2^{3m} + 2^{-m} \sum_{i=0}^{e-1} (1 + e y_i)^4}{4! e^4} - \frac{3e^4 \ell^2 - 2e^4 \ell + 6e^2 \ell + 1}{4! e^4}.$$

Proof: By Lemma 7, the number N_4 of the solutions to

$$z_1^e + z_2^e + z_3^e + z_4^e = 0 \quad (2)$$

in $\text{GF}(2^m)$ is

$$N_4 = 2^{-m} \left(2^{4m} + \ell \sum_{i=0}^{e-1} (1 + e y_i)^4 \right).$$

However, some solutions of (2) correspond to a codeword of weight 4, others do not give such a codeword.

To determine the number A_4 of codewords of weight 4, we divide the solutions of (2) into the following disjoint classes.

A) Those (z_1, z_2, z_3, z_4) with z_1^e, z_2^e, z_3^e , and z_4^e being pairwise distinct.

B) Those (z_1, z_2, z_3, z_4) with

- $z_1^e = z_2^e = a \in D_0^{(e)}$ and $z_3^e = z_4^e = b \in D_0^{(e)}$, $a \neq b$;
- $z_1^e = z_2^e = 0$ and $z_3^e = z_4^e = b \in D_0^{(e)}$;
- $z_1^e = z_2^e = a \in D_0^{(e)}$ and $z_3^e = z_4^e = 0$;
- $z_1^e = z_3^e = a \in D_0^{(e)}$ and $z_2^e = z_4^e = b \in D_0^{(e)}$, $a \neq b$;

- $z_1^e = z_3^e = 0$ and $z_2^e = z_4^e = b \in D_0^{(e)}$;
- $z_1^e = z_3^e = a \in D_0^{(e)}$ and $z_2^e = z_4^e = 0$;
- $z_1^e = z_4^e = a \in D_0^{(e)}$ and $z_2^e = z_3^e = b \in D_0^{(e)}$, $a \neq b$;
- $z_1^e = z_4^e = 0$ and $z_2^e = z_3^e = b \in D_0^{(e)}$;
- $z_1^e = z_4^e = a \in D_0^{(e)}$ and $z_2^e = z_3^e = 0$.

The total number of solutions within class B) is

$$3(e^4 \ell(\ell - 1) + e^2 \ell + e^2 \ell).$$

C) Those (z_1, z_2, z_3, z_4) with

- $z_1^e = z_2^e = z_3^e = z_4^e \in D_0^{(e)}$;
- $z_1^e = z_2^e = z_3^e = z_4^e = 0$.

The total number of solutions within class C) is $e^4 \ell + 1$.

The total number of solutions of classes C) and B) is thus

$$3e^4 \ell^2 - 2e^4 \ell + 6e^2 \ell + 1.$$

No solution in Class B) or C) yields a codeword of weight 4.

If (z_1, z_2, z_3, z_4) is a solution of class A), then each z_i is nonzero (since $d \geq 4$), and $(z_1 \alpha^{k_1 \ell}, z_2 \alpha^{k_2 \ell}, z_3 \alpha^{k_3 \ell}, z_4 \alpha^{k_4 \ell})$ is also a solution for any $0 \leq k_i \leq e-1$, and any permutation of the coordinates of (z_1, z_2, z_3, z_4) is also a solution. These $4!e^4$ solutions give the same codeword of weight 4. On the other hand, any codeword of weight 4 gives $4!e^4$ solutions. Hence, the number of solutions in class A) is $4!e^4 A_4$. Hence,

$$N_4 = 3e^4 \ell^2 - 2e^4 \ell + 6e^2 \ell + 1 + 4!e^4 A_4.$$

The conclusion then follows. $\square$

Corollary 9: If the minimum distance $d \geq 4$ and

$$e^4 + (2^{m+1} - 4) e^3 - 3(2^{2m} - 2^m - 2) e^2 - (3 \times 2^{m+1} + 4) e + 1 + 2^m + 2^{2m} + 2^{3m} > 0 \quad (3)$$

then $d = 4$.

Proof: By definition, y_i must be odd. Hence,

$$(1 + e y_i)^4 \geq (e - 1)^4.$$

The conclusion then follows from Theorem 8. $\square$

If one can prove that the minimum distance d of some $\mathcal{C}_e$ is at least 4, Corollary 9 could be used to show that d is exactly 4.

Theorem 10: If $\mathcal{C}_e$ has minimum distance $d = 3$ then

$$\begin{aligned} A_4 &= \frac{2^{3m} + 2^{-m} \sum_{i=0}^{e-1} (1 + e y_i)^4}{4! e^4} \\ &\quad - \frac{(3e^4 \ell^2 - 2e^4 \ell + 6e^2 \ell + 1) + 4\ell e^3 (0, 0)_e}{4! e^4}. \end{aligned}$$

Proof: A slight extension of the proof of Theorem 8 yields

$$N_4 = 3e^4 \ell^2 - 2e^4 \ell + 6e^2 \ell + 1 + 4!e^4 A_4 + 4!e^3 A_3.$$

On the other hand, by Theorem 5 we have $A_3 = \frac{\ell(0, 0)_e}{3!}$. The conclusion then follows. $\square$

Theorem 11: If $\mathcal{C}_e$ has minimum distance $d \geq 5$ then

$$A_5 = \frac{2^{4m} + 2^{-m} \ell \sum_{i=0}^{e-1} (1 + ey_i)^5}{5!e^5} - \frac{30e^4\ell^2 - 25e^4\ell + 70e^2\ell + 1}{5!e^5}.$$

Proof: Similarly to the proof of Theorem 8, we can obtain

$$N_4 = 30e^4\ell^2 - 25e^4\ell + 70e^2\ell + 1 + 5!e^5 A_5.$$

The conclusion then follows. $\square$

III. THE CODES $\mathcal{C}_e$ WITH $e|(2^i + 1)$ FOR SOME i

The following result is due to Baumert, Mills, and Ward [2]. It seems that the determination of the cyclotomic numbers of order e , where $e|(2^i + 1)$, is equivalent to that of the weight distribution of the binary semiprimitive irreducible cyclic codes.

Lemma 12: Let $m \equiv 0 \pmod{2}$ with $m \geq 4$ and let $2^m - 1 = e\ell$, where e divides $2^i + 1$ for some $1 \leq i \leq m/2$ and $e \geq 3$. Then

$$\begin{aligned} (0, 0)_e &= \mu^2 + 3\mu - r \\ (0, i)_e &= (i, 0)_e = (i, i)_e = \mu^2 + \mu, & \text{for } i \neq 0 \\ (i, j)_e &= \mu^2, & \text{for } 0 \neq i \neq j \neq 0 \end{aligned}$$

where $\mu = \frac{r-1}{e}$, $r = \pm 2^{m/2}$, and the sign is determined by $r \equiv 1 \pmod{e}$. In addition, there is an integer $0 \leq c \leq e-1$ such that $y_c = \mu - r$, and $y_i = \mu$ for any other $i \neq c$. Here the y_i 's are the Gaussian periods defined earlier.

Theorem 13: Let $m \equiv 0 \pmod{2}$ with $m \geq 6$ and let $2^m - 1 = e\ell$, where e divides $2^i + 1$ for some $1 \leq i \leq m/2$ and $e \geq 3$. Then $\mathcal{C}_e$ has parameters

- 1) $[2^{m/2} - 1, 2^{m/2} - 1 - m/2, 3]$, if $e = 2^{m/2} + 1$;
- 2) $[\ell, \ell - m, 3]$, if $e < 2^{m/2} + 1$.

In both cases

$$A_3 = A_{\ell-3} = \frac{\ell(\mu^2 + 3\mu - r)}{3!}$$

where μ and r are defined as in Lemma 12.

Proof: Since $3 \leq e \leq 2^{m/2} + 1$, we have $\ell \geq 2^{m/2} - 1$. If $\ell = 2^{m/2} - 1$, then $\text{ord}_\ell(2) = m/2$. If $\ell > 2^{m/2} - 1$, then $\text{ord}_\ell(2) > m/2$. But $\text{ord}_\ell(2)$ divides m . Hence, in this case, $\text{ord}_\ell(2) = m$. Therefore, the conclusions about the dimension of $\mathcal{C}_e$ then follow from Proposition 2.

By Lemma 12

$$e^2(0, 0)_e = (r-1)^2 + 3(r-1)e - re^2$$

where $e|(r-1)$. If

$$(r-1)^2 + 3(r-1)e - re^2 \neq 0$$

then $(0, 0)_e \neq 0$, and so $\mathcal{C}_e$ has minimum distance $d = 3$ by Theorem 4. If

$$(r-1)^2 + 3(r-1)e - re^2 = 0$$

then

$$(r-1) \frac{r-1}{e} + 3(r-1) - re = 0.$$

Hence $r-1$ divides e , and so $e = \pm(r-1)$. But then

$$0 = (r-1)^2 + 3(r-1)e - re^2 = (b-r)(r-1)^2$$

with $b = 4$ or -2 , and this is a contradiction to $r = \pm 2^{m/2}$ and $m \geq 6$. Hence the minimum distance is always $d = 3$.

The formula for A_3 then follows from Theorems 4 and 5 and Lemma 12. $\square$

For the special case $e = 3$, we have the following result, which may be known.

Corollary 14: If $m = 4$, then the code $\mathcal{C}_3$ has parameters $[5, 1, 5]$ with only two codewords $\{(00000), (11111)\}$. If $m \geq 6$ is even, then the code $\mathcal{C}_3$ has parameters

$$\left[\frac{2^m - 1}{3}, \frac{2^m - 3m - 1}{3}, 3 \right]$$

with

$$A_3 = \begin{cases} \frac{(2^m - 1)(2^m - 8 - 2^{(m+2)/2})}{162}, & \text{if } m \equiv 0 \pmod{4} \\ \frac{(2^m - 1)(2^m - 8 + 2^{(m+2)/2})}{162}, & \text{if } m \equiv 2 \pmod{4} \end{cases}$$

and $A_{\ell-3} = A_3$.

Proof: It follows from Lemma 12 and Theorem 13. $\square$

Example 1: Let $m = 6$. Then $\mathcal{C}_3$ has parameters $[21, 15, 3]$. The best binary linear codes known with length 21 and dimension 15 have minimum distance 4 [4].

Let $m = 8$. Then $\mathcal{C}_3$ has parameters $[85, 77, 3]$. The best binary linear codes known with length 85 and dimension 77 have minimum distance 4 [4].

As mentioned earlier, the weight distribution of several classes of irreducible cyclic codes is known. By using the MacWilliams identity, the weight distribution of the dual code is also known in principle. However, it could even be hard in practice to determine the minimum distance of the dual code, not to mention other weights. To justify this, we look at the following example.

Let e divide $2^{m/2} + 1$. In this case, $\mathcal{C}_e^\perp$ is called a *semiprimitive code* and has parameters

$$\left[\frac{2^m - 1}{e}, m, \frac{2^{m-1} - (e-1)2^{m/2-1}}{e} \right].$$

In fact, $\mathcal{C}_e^\perp$ is a two-weight code with weight enumerator $A(z)$ [1], where

$$A(z) = 1 + \frac{2^m - 1}{e} z^{(2^{m-1} - (e-1)2^{m/2-1})/e} + \frac{(e-1)(2^m - 1)}{e} z^{(2^{m-1} + 2^{m/2-1})/e}.$$

By the MacWilliams identity, the weight enumerator $B(z)$ of $\mathcal{C}_e$ is

$$\begin{aligned} B(z) &= 2^{-m}(1+z)^{(2^m-1)/e} A\left(\frac{1-z}{1+z}\right) \\ &= 2^{-m}(1+z)^{(2^m-1)/e} \\ &\quad + \frac{2^m-1}{2^m e} (1-z^2)^{(2^m-1-(e-1)2^{m/2-1})/e} \\ &\quad \times (1+z)^{((e-1)2^{m/2}-1)/e} + \frac{(e-1)(2^m-1)}{2^m e} \\ &\quad \times (1-z^2)^{(2^m-1-2^{m/2-1}-1)/e} (1-z)^{(2^{m/2}+1)/e}. \end{aligned}$$

It is possible to find the coefficients of $B(z)$ and prove that $\mathcal{C}_e$ has minimum distance 3. But the expression for $B(z)$ is quite complicated.

IV. THE ZETTERBERG CODES $\mathcal{C}_{2^{m/2}-1}$

Let $m \equiv 0 \pmod{4}$. Then $\mathcal{C}_{2^{m/2}-1}$ is the Zetterberg code [23]. In this case, $e = 2^{m/2} - 1$ and $\ell = 2^{m/2} + 1$. Zetterberg [23] proved that the minimum distance d is at least 5. Here we point out that $d = 5$ or $d = 6$, and show that in certain cases $d = 5$ exactly.

Before looking at the Zetterberg codes, we prove the following general result.

Lemma 15: As before, let $2^m - 1 = e\ell$. If ℓ divides $2^h + 1$ for some positive integer h , then $\mathcal{C}_e$ has no codewords of weight 4.

Proof: Let $\beta = \alpha^e$. Then $\beta^\ell = 1$ and thus $\beta^{2^h+1} = 1$. Assume there is a codeword of weight 4. Then there are three distinct integers $0 < u_i < \ell$ such that

$$1 + \beta^{u_1} + \beta^{u_2} + \beta^{u_3} = 0. \quad (4)$$

Whence

$$(1 + \beta^{u_1} + \beta^{u_2})^{2^h+1} = \beta^{(2^h+1)u_3} = 1$$

which gives

$$\beta^{u_1} + \beta^{u_2} + \beta^{u_1 2^h} + \beta^{u_2 2^h} + \beta^{u_1 2^h + u_2} + \beta^{u_2 2^h + u_1} = 0. \quad (5)$$

Multiplying both sides of (5) with $\beta^{u_1+u_2}$ yields

$$(\beta^{u_1} + \beta^{u_2})\beta^{u_1+u_2} + (\beta^{u_1} + \beta^{u_2}) + (\beta^{u_1} + \beta^{u_2})^2 = 0. \quad (6)$$

Note that $\beta^{u_1} + \beta^{u_2} = 1 + \beta^{u_3} \neq 0$. It follows from (6) that

$$\beta^{u_1+u_2} + \beta^{u_1} + \beta^{u_2} + 1 = 0. \quad (7)$$

Combining (4) and (7) yields

$$\beta^{u_3} = \beta^{u_1+u_2}.$$

Hence,

$$u_3 - u_1 - u_2 \equiv 0 \pmod{\ell}. \quad (8)$$

By symmetry, we have

$$\begin{cases} u_2 - u_1 - u_3 \equiv 0 \pmod{\ell} \\ u_1 - u_2 - u_3 \equiv 0 \pmod{\ell}. \end{cases} \quad (9)$$

Combining (8) and (9) gives

$$u_1 = u_2 = u_3 \equiv 0 \pmod{\ell}$$

which contradicts the fact that $0 < u_i < \ell$. Thus, $\mathcal{C}_e$ has no codeword of weight 4. $\square$

Theorem 16: If $m \equiv 2 \pmod{4}$, then $\mathcal{C}_{2^{m/2}-1}$ has parameters

$$\left[2^{m/2} + 1, 2^{m/2} + 1 - m, 3 \right]$$

with

$$A_3 = A_{2^{m/2}-2} = \frac{2^{m/2} + 1}{3} \quad \text{and} \quad A_4 = A_{2^{m/2}-3} = 0.$$

If $m \equiv 0 \pmod{4}$, then $\mathcal{C}_{2^{m/2}-1}$ has parameters

$$\left[2^{m/2} + 1, 2^{m/2} + 1 - m, 5 \leq d \leq 6 \right].$$

Proof: First of all, 3 divides ℓ if and only if $m \equiv 2 \pmod{4}$. We now determine the cyclotomic number $(0, 0)_{2^{m/2}-1}$. Suppose that $(0, 0)_{2^{m/2}-1} \neq 0$. Then there are two distinct integers u and v with $0 < u < v < \ell$ such that

$$1 + \alpha^{eu} + \alpha^{ev} = 0.$$

It follows that

$$(1 + \alpha^{eu})^\ell = (\alpha^{ev})^\ell = 1$$

which gives

$$(1 + \alpha^{eu})^{2^{m/2}} (1 + \alpha^{ev}) = 1.$$

Hence,

$$1 + \alpha^{eu} = \alpha^{ev 2^{m/2}}.$$

Multiplying both sides with α^{eu} yields

$$1 + \alpha^{eu} + (\alpha^{eu})^2 = 0.$$

By symmetry

$$1 + \alpha^{ev} + (\alpha^{ev})^2 = 0.$$

Thus, α^{eu} and α^{ev} both are solutions over $\text{GF}(2^m)$ of the equation

$$1 + x + x^2 = 0.$$

Hence, they are multiplicative inverses of each other and hence $u + v = \ell$.

On the other hand, $\alpha^{3eu} = \alpha^{3ev} = 1$. Hence

$$3eu \equiv 0 \pmod{e\ell} \quad \text{and} \quad 3e(\ell - u) \equiv 0 \pmod{e\ell}.$$

Note that $0 < u < \ell$ and $0 < \ell - u < \ell$. The only possible solutions are

$$3eu = e\ell \quad \text{and} \quad 3e(\ell - u) = 2e\ell$$

and

$$3eu = 2e\ell \quad \text{and} \quad 3e(\ell - u) = e\ell.$$

Hence, there is no solution if $\ell \not\equiv 0 \pmod{3}$, and there are exactly two solutions

$$(u, v) = \left(\frac{\ell}{3}, \frac{2\ell}{3}\right) \quad \text{and} \quad (u, v) = \left(\frac{2\ell}{3}, \frac{\ell}{3}\right)$$

if $3|\ell$. Hence,

$$(0, 0)_{2^{m/2}-1} = \begin{cases} 2, & \text{if } 3|\ell \\ 0, & \text{otherwise.} \end{cases}$$

By Theorem 5, if $3|\ell$, then $\mathcal{C}_{2^{m/2}-1}$ has parameters

$$[2^{m/2} + 1, 2^{m/2} + 1 - m, 3]$$

with $A_3 = (2^{m/2} + 1)/3$. Otherwise, the minimum distance satisfies $d \geq 4$ by Theorem 4. By Lemma 15, we have $d \geq 5$.

We now prove that $d \leq 6$ for $m \equiv 0 \pmod{4}$. Note that the length of the code is $\ell = 2^{m/2} + 1$ and

$$\sum_{i=0}^3 \binom{\ell}{i} = \frac{2^{m/2} + 3}{3} 2^{m-1} + \frac{4}{3} 2^{m/2} + 2 > 2^m$$

due to $m \geq 4$. Since $\mathcal{C}_e$ has dimension $\ell - m$, the sphere-packing bound implies $d < 7$. Hence, $d = 5$ or 6 . $\square$

Example 2: Let $m = 8$. Theorem 16 gives a $[17, 9, 5 \leq d \leq 6]$ binary cyclic code. The best binary linear codes known with length 17 and dimension 9 have minimum distance 5 [4].

Let $m = 10$. Theorem 16 gives a $[33, 23, 3]$ binary cyclic code. The best binary linear codes known with length 33 and dimension 23 have minimum distance 5 [4].

The following result is a consequence of Proposition 3 and Theorem 16.

Corollary 17: Let $m \equiv 4 \pmod{8}$. Then $\mathcal{C}_{2^{m/2}-1}$ has parameters

$$[2^{m/2} + 1, 2^{m/2} + 1 - m, 5].$$

Example 3: Let $m = 12$. Corollary 17 gives a $[65, 53, 5]$ binary cyclic code. The best binary linear codes known with length 65 and dimension 53 have the same minimum distance 5 [4].

V. SOME CODES $\mathcal{C}_e$ WITH $d = 3$

Lemma 18 [16, Example 6.38]: Let $N_{e,1}$ denote the number of solutions $(x_1, x_2) \in \text{GF}(q)^2$ of the diagonal equation

$$x_1^e + x_2^e = 1.$$

Then

$$|N_{e,1} - q| \leq (e-1)(e-2)\sqrt{q} + e - 1.$$

Theorem 19: The code $\mathcal{C}_e$ has minimum distance $d = 3$ if

$$e < \frac{3}{2} \left(1 - \frac{1}{2^{m/2}}\right) + \sqrt{2^{m/2} + \frac{1}{4} - \frac{7}{2^{m/2+1}} + \frac{9}{2^{m+2}}}.$$

Proof: Let $q = 2^m$ and consider the solutions of

$$x_1^e + x_2^e = 1 \tag{10}$$

over $\text{GF}(q)^2$. By Lemma 18

$$N_{e,1} \geq q + 1 - (e-1)(e-2)\sqrt{q} - e.$$

Note that (10) has $2e$ solutions of the form $(0, x_2)$ and $(x_1, 0)$. Any solution of other forms gives a codeword of weight 3 in $\mathcal{C}_e$. Hence, as long as

$$q + 1 - 3e - (e-1)(e-2)\sqrt{q} > 0$$

$\mathcal{C}_e$ must have a codeword of weight 3. The conclusion then follows. $\square$

Remark: This theorem shows that $\mathcal{C}_e$ must have minimum distance 3 if $e < 2^{m/4}$. So it is a useful and general result.

The following theorem gives a class of codes with minimum distance 3.

Theorem 20: Let $m = 6h$ with an integer $h \geq 1$, $e = 2^{2h} - 2^h + 1$, and $\ell = 2^{4h} + 2^{3h} - 2^h - 1$. Then $\mathcal{C}_e$ has parameters

$$[2^{4h} + 2^{3h} - 2^h - 1, 2^{4h} + 2^{3h} - 2^h - 1 - 6h, 3].$$

Proof: We first prove that $\text{ord}_\ell(2) = 6h$. It is easily seen that

$$\text{ord}_{2^h+1}(2) = 2h, \quad \text{ord}_{2^{3h}-1}(2) = 3h.$$

On the other hand, $\gcd(2^h + 1, 2^{3h} - 1) = 1$. By the Chinese Remainder Theorem

$$\text{ord}_\ell(2) = \text{lcm}(\text{ord}_{2^h+1}(2), \text{ord}_{2^{3h}-1}(2)) = \text{lcm}(2h, 3h) = 6h.$$

This proves the dimension of this code. Finally, it follows from $\ell \equiv 0 \pmod{3}$ that $d = 3$ (see Propositions 2 and 3). $\square$

Remark: Theorem 20 is related to [7, Proposition 5 and Theorem 5] in the sense that they all involve exponents of the form $2^u - 2^v + 1$. The difference is that our code of Theorem 20 has a length of the form $2^{4h} + 2^{3h} - 2^h - 1$, while the code in [7, Theorem 5] has length of the form $2^m - 1$. So the code of Theorem 20 and the code in [7, Theorem 5] must be different.

We now describe another class of codes $\mathcal{C}_e$. Let $h \geq 2$ and $t \geq 2$ be integers and let $m = th$. In this case, we write $2^m - 1 = e\ell$, where $e = 2^h - 1$ and $\ell = \sum_{i=0}^{t-1} 2^{ih}$.

Theorem 21: For any $t \geq 3$, the code $\mathcal{C}_{2^h-1}$ has parameters

$$\left[\sum_{i=0}^{t-1} 2^{ih}, \left(\sum_{i=0}^{t-1} 2^{ih} \right) - th, 3 \right].$$

Proof: Recall that $\ell = \sum_{i=0}^{t-1} 2^{ih}$. We first prove that $\text{ord}_\ell(2) = th$. Note that ℓ divides $2^{\text{ord}_\ell(2)} - 1$. So

$$2^{\text{ord}_\ell(2)} \geq \ell + 1 = 2^{(t-1)h} + 2^{(t-2)h} + \dots + 2^h + 2.$$

Hence $\text{ord}_\ell(2) > (t-1)h$. On the other hand, $\text{ord}_\ell(2)$ divides th . It follows that $\text{ord}_\ell(2) = th$.

The proof of $d = 3$ is carried out by distinguishing the two cases $t = 3$ and $t \geq 4$. We first prove that $d = 3$ for the case $t = 3$.

By Proposition 2 we have $d \geq 3$. To prove $d = 3$, it suffices to prove that $\mathcal{C}_{2^h-1}$ has a codeword of weight 3. We first prove that there is an element $b \in \text{GF}(2^h)$ such that the polynomial

$$B(x) = x^3 + bx^2 + (b+1)x + 1$$

is irreducible over $\text{GF}(2^h)$. To this end, we define for each $a \in \text{GF}(2^h)$ the set

$$S(a) = \{y \in \text{GF}(2^h) : y^3 + ay^2 + (a+1)y + 1 = 0\}.$$

It is easily proved that $S(a) \cap S(b) = \emptyset$ if $a \neq b$. On the other hand, neither 0 nor 1 belongs to $S(a)$ for any $a \in \text{GF}(2^h)$. In addition, for any $y \notin \{0, 1\}$, $y \in S((1+y+y^3)/(y^2+y))$. Hence,

$$\bigcup_{b \in \text{GF}(2^h)} S(b) = \text{GF}(2^h) \setminus \{0, 1\}.$$

Therefore, for at least one $b \in \text{GF}(2^h)$ we have $S(b) = \emptyset$. This means that $B(x) = x^3 + bx^2 + (b+1)x + 1$ is irreducible over $\text{GF}(2^h)$.

Now suppose that $B(x) = x^3 + bx^2 + (b+1)x + 1$ is irreducible over $\text{GF}(2^h)$. Let γ be a root of $B(x)$ in $\text{GF}(2^{3h})$. Then $\gamma, \gamma^{2^h}, \gamma^{2^{2h}}$ are all the roots of $B(x)$ in $\text{GF}(2^{3h})$. Hence, the norm of γ is

$$N_h^{3h}(\gamma) = \gamma^{\sum_{i=0}^{2^h-1} 2^{ih}} = 1. \quad (11)$$

We now define another polynomial

$$\begin{aligned} A(x) &= B(x+1) \\ &= (x+1)^3 + b(x+1)^2 + (b+1)(x+1) + 1 \\ &= x^3 + (b+1)x^2 + bx + 1. \end{aligned}$$

Since $B(x)$ is irreducible over $\text{GF}(2^h)$, so is $A(x)$. Clearly, $\gamma+1$ is a root of $A(x)$, as γ is a root of $B(x)$. Thus,

$$N_h^{3h}(\delta) = \delta^{\sum_{i=0}^{2^h-1} 2^{ih}} = 1 \quad (12)$$

where $\delta = \gamma + 1$. By (11) and (12) there are two integers i and j such that

$$\gamma = \alpha^{(2^h-1)i}, \quad \delta = \alpha^{(2^h-1)j}$$

where α is the primitive element of $\text{GF}(2^{3h})$. Then we have

$$1 + \alpha^{(2^h-1)i} + \alpha^{(2^h-1)j} = 0.$$

This gives a codeword of weight 3 in $\mathcal{C}_{2^h-1}$. This completes the proof of $d = 3$ for the case $t = 3$.

When $t \geq 4$, it follows directly from Theorem 19 that $d = 3$. $\square$

Theorem 22: Let q be an odd positive integer such that $\gcd(3, q) = 1$. Define $m = \text{lcm}(2, \text{ord}_q(2))$ and $e = (2^m - 1)/3q$ and $\ell = 3q$. Then $\mathcal{C}_e$ has parameters

$$[3q, 3q - m, 3].$$

In particular, we have the following results.

1) If $q = 2^t - 1$, t odd, then $\mathcal{C}_e$ has parameters

$$[3(2^t - 1), 3(2^t - 1) - 2t, 3].$$

2) If $q = 2^t + 1$, t even, then $\mathcal{C}_e$ has parameters

$$[3(2^t + 1), 3(2^t + 1) - 2t, 3].$$

Proof: Since $\gcd(3, q) = 1$, by the Chinese Remainder Theorem

$$\text{ord}_\ell(2) = \text{lcm}(\text{ord}_3(2), \text{ord}_q(2)) = m.$$

Hence, $\mathcal{C}_e$ has dimension $3q - m$ by Proposition 2. Because 3 divides ℓ , $\mathcal{C}_e$ has minimum distance 3 by Propositions 2 and 3.

If $q = 2^t - 1$ and t is odd, then $m = \text{lcm}(2, \text{ord}_q(2)) = 2t$ and $\gcd(3, 2^t - 1) = 1$. If $q = 2^t + 1$ and t is even, then $m = \text{lcm}(2, \text{ord}_q(2)) = 2t$ and $\gcd(3, 2^t + 1) = 1$. Then the conclusion for the two special cases follows. $\square$

Theorem 23: Let $h \geq 2$ and $t \geq 2$ be integers with $h(t-1) \equiv 0 \pmod{2}$. Define $m = 2ht$, $e = (2^{ht} - 1)/(2^h - 1)$, and $\ell = (2^h - 1)(2^{ht} + 1)$. Then the code $\mathcal{C}_e$ has parameters

$$[(2^h - 1)(2^{ht} + 1), (2^h - 1)(2^{ht} + 1) - 2ht, 3].$$

Proof: Clearly, $\gcd(2^h - 1, 2^{ht} + 1) = 1$. Hence, by the Chinese Remainder Theorem

$$\text{ord}_\ell(2) = \text{lcm}(\text{ord}_{2^h-1}(2), \text{ord}_{2^{ht}+1}(2)) = \text{lcm}(h, 2ht) = 2ht.$$

This proves the dimension of $\mathcal{C}_e$. Since 3 divides ℓ , we have $d = 3$ by Propositions 2 and 3. $\square$

Similar to Theorem 23, we have the following result.

Theorem 24: Let $h \geq 1$ and $t \geq 3$ be integers with t odd. Define $m = 2ht$, $e = (2^{ht} + 1)/(2^h + 1)$, and $\ell = (2^h + 1)(2^{ht} - 1)$. Then the code $\mathcal{C}_e$ has parameters

$$[(2^h + 1)(2^{ht} - 1), (2^h + 1)(2^{ht} - 1) - 2ht, 3].$$

VI. SOME CODES $\mathcal{C}_e$ WITH LENGTH OF SPECIAL FORMS

As before, let $2^m - 1 = e\ell$. As shown before, if $3 \nmid \ell$, then the minimum distance of $\mathcal{C}_e$ must be 3. Thus, $\ell \not\equiv 0 \pmod{3}$ is a necessary condition for $d \geq 4$. Intuitively, this is not a sufficient condition. In this section, we describe several classes of codes $\mathcal{C}_e$ whose minimum distance is at least 4.

Theorem 25: Let $2^m - 1 = e\ell$, where $\ell = 2^{h_2} + 2^{h_1} - 1$ for some integers $h_2 > h_1 \geq 1$. If $\gcd(h_1 + 1, h_2 + 1) = 1$, then the code $\mathcal{C}_e$ has parameters $[\ell, \ell - \text{ord}_\ell(2), d \geq 4]$.

Proof: By Proposition 2 we have $d \geq 3$. We need only to prove that $d \neq 3$. Assume that $d = 3$. Then there are two distinct integers $0 < u < \ell$ and $0 < v < \ell$ such that

$$1 + \alpha^{eu} + \alpha^{ev} = 0.$$

Define $\gamma = \alpha^{eu}$. It follows that $(1 + \gamma)^\ell = 1$ and thus

$$(1 + \gamma)^{\ell+1} = 1 + \gamma.$$

Hence, $\gamma^{2^{h_2}} = \gamma^{2^{h_1}}$, which leads to $\alpha^{(2^{h_2}-2^{h_1})eu} = 1$. It follows that

$$(2^{h_2} - 2^{h_1})eu \equiv 0 \pmod{e\ell}$$

and

$$(2^{h_2} - 2^{h_1})u \equiv 0 \pmod{\ell}.$$

Note that $\ell = 2^{h_1}(2^{h_2-h_1} - 1) + 2^{h_1+1} - 1$. We have

$$\begin{aligned} \gcd(2^{h_2-h_1} - 1, \ell) &= \gcd(2^{h_2-h_1} - 1, 2^{h_1+1} - 1) \\ &= 2^{\gcd(h_2-h_1, h_1+1)} - 1 \\ &= 2^{\gcd(h_1+1, h_2+1)} - 1 \\ &= 1. \end{aligned}$$

Hence $u \equiv 0 \pmod{\ell}$, which is a contradiction to $0 < u < \ell$. Thus, $d \geq 4$. $\square$

Corollary 26: Let $t \equiv 2 \pmod{4}$ and $h \equiv 1 \pmod{4}$ be positive integers with $\gcd(h+1, t-1) = 1$. Define

$$\ell = 2^{th} + 2^h - 1 \quad \text{and} \quad e = \left(2^{\text{ord}_\ell(2)} - 1\right) / \ell.$$

Then the code $\mathcal{C}_e$ has parameters

$$[2^{th} + 2^h - 1, 2^{th} + 2^h - 1 - \text{ord}_{2^{th}+2^h-1}(2), 4 \leq d \leq 5].$$

Proof: It can be proved that $\ell \equiv 0 \pmod{5}$. The conclusion then follows from Proposition 3 and Theorem 25. $\square$

If $h = 1$, the codes of Corollary 26 have indeed minimum distance 5 by Lemma 15. The following open problem would be interesting.

Open Problem 1: Prove or disprove that all the codes of Corollary 26 have minimum distance 5. In addition, determine $\text{ord}_{2^{th}+2^h-1}(2)$.

Theorem 27: Let $2^m - 1 = e\ell$, where $\ell = 2^{h_2} - 2^{h_1} + 1$ for some integers $h_2 > h_1 \geq 1$. If $\gcd(h_2, h_1 - 1) = 1$, then the code $\mathcal{C}_e$ has parameters $[\ell, \ell - \text{ord}_\ell(2), d \geq 4]$.

Proof: By Proposition 2 we have $d \geq 3$. We need only to prove that $d \neq 3$. Assume that $d = 3$. Then there are two distinct integers $0 < u < \ell$ and $0 < v < \ell$ such that

$$1 + \alpha^{eu} + \alpha^{ev} = 0.$$

Define $\gamma = \alpha^{eu}$. It follows that $(1 + \gamma)^\ell = 1$ and thus

$$(1 + \gamma)^{2^{h_2}+1} = (1 + \gamma)^{2^{h_1}}.$$

Hence, $\gamma^{2^{h_1}-1} = \gamma$. It follows that $(2^{h_1} - 2)u \equiv 0 \pmod{\ell}$. Since

$$\gcd(2^{h_1-1} - 1, \ell) = 2^{\gcd(h_2, h_1-1)} - 1 = 1$$

we get $u \equiv 0 \pmod{\ell}$. This is a contradiction to $0 < u < \ell$. Thus, $d \geq 4$. $\square$

Corollary 28: Let $t \equiv 3 \pmod{4}$ and $h \equiv 3 \pmod{4}$, and let both t and h be positive integers with $\gcd(t, h-1) = 1$. Define $\ell = 2^{th} - 2^h + 1$ and $e = (2^{\text{ord}_\ell(2)} - 1)/\ell$. Then the code $\mathcal{C}_e$ has parameters

$$[2^{th} - 2^h + 1, 2^{th} - 2^h + 1 - \text{ord}_{2^{th}-2^h+1}(2), 4 \leq d \leq 5].$$

Proof: Under the given conditions, it can be proved that 5 divides ℓ . The conclusion then follows from Proposition 3 and Theorem 27. $\square$

Theorem 29: Let $m = 6h$ with an even integer $h \geq 4$ and let

$$e = 2^{4h} + 2^{3h} - 2^h - 1, \quad \ell = 2^{2h} - 2^h + 1.$$

The $\mathcal{C}_e$ has parameters $[\ell, \ell - 6h, 5 \leq d \leq 8]$.

Proof: Similarly to the proof of Theorem 20, we can prove that $\text{ord}_\ell(2) = 6h$. This proves the dimension of this code.

Since h is even, we have $\gcd(2h, h-1) = 1$. It then follows from Theorem 27 that $d \geq 4$. By Lemma 15 we get $d \geq 5$. For $h \geq 4$ it can be checked that

$$\sum_{i=0}^4 \binom{\ell}{i} > 2^{6h}.$$

By the sphere-packing bound, $d \leq 8$. $\square$

Example 4: Taking $h = 4$ and $h = 6$ in Theorem 29, we obtain two codes with parameters

$$[241, 217, 5 \leq d \leq 8] \quad \text{and} \quad [4033, 3997, 5 \leq d \leq 8]$$

respectively.

Open Problem 2: Determine or establish better bounds for the minimum distance of the codes of Theorem 29.

The proof of the following theorem is similar to that of Theorem 27.

Theorem 30: Let $2^m - 1 = e\ell$, where $\ell = 2^{h_2} - 2^{h_1} - 1 \geq 3$ for some integers $h_2 > h_1 \geq 1$. If $\gcd(h_1, h_2 - 1) = 1$, then the code $\mathcal{C}_e$ has parameters $[\ell, \ell - \text{ord}_\ell(2), d \geq 4]$.

Corollary 31: Let t and h be positive integers. Define

$$\ell = 2^{th} - 2^h - 1 \quad \text{and} \quad e = (2^{\text{ord}_\ell(2)} - 1)/\ell.$$

Then the code $\mathcal{C}_e$ has parameters

$$[2^{th} - 2^h - 1, 2^{th} - 2^h - 1 - \text{ord}_{2^{th}-2^h-1}(2), 4 \leq d \leq 5]$$

if

- 1) $h \equiv 1 \pmod{4}$ and $t \equiv 3 \pmod{4}$ or
- 2) $h \equiv 3 \pmod{4}$ and $t \equiv 2 \pmod{4}$.

Proof: It can be proved that $\ell \equiv 0 \pmod{5}$. The conclusion then follows from Proposition 3 and Theorem 30. $\square$

Open Problem 3: Determine the minimum distance of the codes of Corollary 31. In addition, determine $\text{ord}_{2^{th}-2^h-1}(2)$.

VII. SOME SPECIAL CLASSES OF CODES $\mathcal{C}_e$

Let $p \geq 5$ be a prime. Then p divides $2^{p-1} - 1$. We now consider the finite field $\text{GF}(2^m)$, where $m = p - 1$. Let $2^m - 1 = e\ell$, where $e = (2^{p-1} - 1)/p$ and $\ell = p$. Then, the code $\mathcal{C}_e$ has parameters $[p, p - \text{ord}_p(2), d \geq 3]$. This forms a subclass of codes with prime length.

Theorem 32: If $p \geq 7$ is a Mersenne prime, i.e., of the form $2^r - 1$ for some r , then $\mathcal{C}_{(2^{p-1}-1)/p}$ is equivalent to a $[p, p - \log_2(p+1), 3]$ Hamming code.

The proof of Theorem 32 is straightforward. The theorem shows that the class of codes $\mathcal{C}_e$ with $e > 1$ does contain codes equivalent to Hamming codes.

Theorem 33: Let $p \geq 5$ be a Fermat prime, i.e., of the form $2^r + 1$ for some r . Then $\mathcal{C}_{(2^{p-1}-1)/p}$ has parameters

$$[p, p - 2\log_2(p-1), 5 \leq d \leq 6].$$

Proof: It can be easily proved that $\mathcal{C}_e$ has no codeword of weight 3. The proof of Theorem 16 also applies to the proof of $5 \leq d \leq 6$. $\square$

Theorem 34: Let $p \equiv \pm 1 \pmod{8}$ be a prime with

$$\text{ord}_p(2) = (p-1)/2.$$

Then $\mathcal{C}_{(2^{p-1}-1)/p}$ has parameters $[p, (p+1)/2, d \geq \sqrt{p}]$ and is a quadratic residue code.

Proof: Since $\text{ord}_p(2) = (p-1)/2$, there are only two nonzero cyclotomic classes. Hence, $x^p - 1 = (x-1)f_1(x)f_2(x)$, where f_i is an irreducible polynomial of degree $(p-1)/2$ over $\text{GF}(2)$. The code $\mathcal{C}_e$ must have generator polynomial $f_1(x)$ or $f_2(x)$, and thus must be a quadratic residue code. Thus, we have the square-root bound for the minimum distance. $\square$

This theorem shows that the class of codes $\mathcal{C}_e$ contains also some quadratic residue codes. When $p = 23$, we have a $[23, 12]$ quadratic residue code, which is equivalent to the $[23, 12]$ Golay code.

VIII. DOUBLE-ERROR CORRECTING CODES FROM $\mathcal{C}_e$

As shown earlier, some codes $\mathcal{C}_e$ have minimum distance 3 and may not be optimal linear codes. In this section, we use some of them to construct some optimal double-error correcting codes.

Let ℓ and a be positive integers. If there is a positive integer m such that $a^m \equiv -1 \pmod{\ell}$, the smallest such m is called the negative order (negord) of a modulo ℓ , and is denoted $\text{nord}_\ell(a)$ [8, p. 46].

An integer a may have a negord modulo an integer ℓ or not. For example, 1, 2, 4, 8, 16, 9, 18, 13, and 12 have no negord modulo 23, but 17, 11, 22, 21, 19, 15, 7, and 14 have the negord.

Let ℓ be a positive integer. If an integer a , where $1 \leq a \leq \ell-1$ and $\gcd(a, \ell) = 1$, has the negord modulo ℓ , then [8, p. 46]

$$\text{ord}_\ell(a) = 2\text{nord}_\ell(a).$$

Let $\ell \geq 9$ be an integer such that $3|\ell$ and $\text{nord}_\ell(2)$ exists. In this case, $\text{nord}_\ell(2)$ must be odd. Define $e = (2^{2\text{nord}_\ell(2)} - 1)/\ell$. Then, $\mathcal{C}_e$ is an $[\ell, \ell - 2\text{nord}_\ell(2), 3]$ cyclic code. Since $3|\ell$ and $\ell \geq 9$, $1 + x^{\ell/3} + x^{2\ell/3}$ and $x + x^{1+\ell/3} + x^{1+2\ell/3}$ both are codewords of $\mathcal{C}_e$, and thus

$$1 + x + x^{\ell/3} + x^{1+\ell/3} + x^{2\ell/3} + x^{1+2\ell/3}$$

is a codeword of $\mathcal{C}_e$ with weight 6. By definition, ℓ divides $2^{2\text{nord}_\ell(2)} + 1$. It follows from Lemma 15 that $\mathcal{C}_e$ has no codeword of weight 4.

Let $\mathcal{C}_e^{(0)}$ denote the even-weight subcode of $\mathcal{C}_e$. Then $\mathcal{C}_e^{(0)}$ is a cyclic code with parameters $[\ell, \ell - 1 - 2\text{nord}_\ell(2), 6]$ code. Let $\mathcal{C}_e^{(0P)}$ denote the punctured code obtained by deleting the last coordinate of all the codewords in $\mathcal{C}_e^{(0)}$. We have then proved the following conclusion.

Theorem 35: $\mathcal{C}_e^{(0P)}$ is a linear code with parameters $[\ell - 1, \ell - 1 - \text{ord}_\ell(2), 5]$.

Some of the codes in Theorem 35 have the following parameters:

$$[8, 2, 5]^*, [26, 8, 5], [32, 22, 5]^*, [56, 38, 5], [98, 68, 5], [128, 114, 5]^*, [170, 152, 5].$$

Those with the mark $*$ are the best codes known and are optimal in the sense that their dimension cannot be increased, given the

TABLE I
PARAMETERS OF THE CODES STUDIED IN THIS PAPER

e	ℓ	k	d
$e (2^i + 1), i < m/2$ $m \equiv 0 \pmod{2}$	$\frac{2^m - 1}{e}$	$\ell - m$	3
$2^{m/2} + 1$, $m \equiv 0 \pmod{2}$	$2^{m/2} - 1$	$\ell - m/2$	3
$2^{2h} - 2^h + 1$	$2^{4h} + 2^{3h} - 2^h - 1$	$\ell - 6h$	3
$2^{m/2} - 1$, $m \equiv 2 \pmod{4}$	$2^{m/2} + 1$	$\ell - m$	3
$2^h - 1$	$\frac{2^{th} - 1}{2^h - 1}$	$\frac{2^{th} - 1}{2^h - 1} - th$	3
$\frac{2^{ht} - 1}{2^h - 1}$, $t \geq 2, h \geq 2$ $h(t-1) \equiv 0 \pmod{2}$	$(2^h - 1)(2^{ht} + 1)$	$\ell - 2ht$	3
$\frac{2^{ht} + 1}{2^h + 1}$, $t \geq 3$ odd, $h \geq 1$	$(2^h + 1)(2^{ht} - 1)$	$\ell - 2ht$	3
$(2^{\text{ord}_\ell(2)} - 1)/\ell$	$2^{th} + 2^h - 1$, where $t \equiv 2 \pmod{4}$, $h \equiv 1 \pmod{4}$	$\ell - \text{ord}_\ell(2)$	$d = 4, 5$
$(2^{\text{ord}_\ell(2)} - 1)/\ell$, $h \equiv 1 \pmod{4}$, $h \equiv 3 \pmod{4}$	$2^{th} - 2^h - 1$, where $t \equiv 3 \pmod{4}$ or $t \equiv 2 \pmod{4}$	$\ell - \text{ord}_\ell(2)$	$d = 4, 5$
$2^{m/2} - 1$, $m \equiv 0 \pmod{4}$	$2^{m/2} + 1$	$\ell - m$	$d = 5, 6$
$2^{4h} + 2^{3h} - 2^h - 1$	$2^{2h} - 2^h + 1$, $h > 4$ even	$\ell - 6h$	$5 \leq d \leq 8$

minimum distance 5 and length. However, it is clear that some of the codes $\mathcal{C}_e^{(0P)}$ in Theorem 35 are bad.

The following is a special case of Theorem 35.

Corollary 36: Let $\ell = 2^t + 1$, where $t \geq 3$ is odd. Then $\mathcal{C}_e^{(0P)}$ is a linear code with parameters $[2^t, 2^t - 2t, 5]$.

The codes in Corollary 36 are optimal in the sense that the dimension is maximal with respect to the length and minimum distance. The smallest three codes have parameters $[8, 2, 5]$, $[32, 22, 5]$, and $[128, 114, 5]$.

IX. SUMMARY AND CONCLUDING REMARKS

In this paper, we have demonstrated that the weight distribution of the codes $\mathcal{C}_e$ is, in principle, determined by the cyclotomic numbers of certain orders or the corresponding Gaussian periods. We determined the minimum distance of a number of classes of codes $\mathcal{C}_e$ and showed that the codes $\mathcal{C}_e$ contain certain classes of known good codes such as some quadratic residue codes. The parameters of the special classes of codes studied in this paper are summarized in Table I. It is noted that for certain classes of codes $\mathcal{C}_e$, determining the dimension could be very hard as it needs the determination of cyclotomic polynomials. We have studied only several special classes of codes $\mathcal{C}_e$. Much work in this direction needs to be done. In Section VIII, we described a class of double-error correcting codes which contains some subclass of optimal codes. We mention that the purpose of this paper is to study the parameters of some codes $\mathcal{C}_e$, not to search for optimal codes. We draw the reader's attention to the recent work of Charpin, Tietäväinen, and Zinoviev on certain binary cyclic codes with small minimum distance and large dimension [6]. Finally, information about the weight enumerators of cyclic codes may be found in Charpin [5], Honkala and Tietäväinen [15], and Pless, Huffman, and Brualdi [21].

ACKNOWLEDGMENT

The authors thank the referee and Xuesong Wang for their helpful comments and suggestions that improved this paper.

REFERENCES

- [1] L. D. Baumert and R. J. McEliece, "Weights of irreducible cyclic codes," *Inform. Contr.*, vol. 20, pp. 158–175, 1972.
- [2] L. D. Baumert, W. H. Mills, and R. L. Ward, "Uniform cyclotomy," *J. Number Theory*, vol. 14, pp. 67–82, 1982.
- [3] L. D. Baumert and J. Mykkeltveit, "Weight distribution of some irreducible cyclic codes," *DSN Progr. Rep.*, vol. 16, pp. 128–131, 1973.
- [4] A. E. Brouwer, "Bounds on the size of linear codes," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: North-Holland, 1998, vol. I, pp. 295–461.
- [5] P. Charpin, "Open problems on cyclic codes," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: North-Holland, 1998, vol. I, pp. 963–1063.
- [6] P. Charpin, A. Tietäväinen, and V. Zinoviev, "On binary cyclic codes with codewords of weight three and binary sequences with the trinomial property," *IEEE Trans. Inform. Theory*, vol. 47, pp. 421–425, Jan. 2001.
- [7] —, "On binary cyclic codes with minimum distance $d = 3$," *Probl. Inform. Transm.*, vol. 33, no. 4, pp. 287–296, 1997.
- [8] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. Amsterdam, The Netherlands: North-Holland, 1998.
- [9] P. Delsarte and J.-M. Goethals, "Irreducible cyclic codes of even dimension," in *Proc. 2nd Chapel Hill Conf. Combinatorial Mathematics and Applications*. Chapel Hill, NC: Univ. North Carolina Press, 1970.
- [10] C. Ding and T. Helleseeth, "New generalized cyclotomy and its applications," *Finite Fields Their Applic.*, vol. 4, pp. 140–166, 1998.
- [11] —, "Generalized cyclotomic codes of length $p_1^{e_1} \cdots p_t^{e_t}$," *IEEE Trans. Inform. Theory*, vol. 45, pp. 467–474, Mar. 1999.
- [12] C. Ding and V. Pless, "Cyclotomy and duadic codes of prime lengths," *IEEE Trans. Inform. Theory*, vol. 45, pp. 453–466, Mar. 1999.
- [13] J. M. Goethals, "Factorization of cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 242–246, Apr. 1967.
- [14] T. Helleseeth, T. Kløve, and J. Mykkeltveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l - 1)/N)$," *Discr. Math.*, vol. 18, pp. 179–211, 1977.
- [15] I. Honkala and A. Tietäväinen, "Codes and number theory," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam: North-Holland, 1998, vol. II, pp. 1141–1194.
- [16] R. Lidl and H. Niederreiter, *Finite Fields*. Reading, MA: Addison-Wesley, 1983.
- [17] F. J. MacWilliams and J. Seery, "The weight distributions of some minimal cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 796–806, Nov. 1981.
- [18] R. J. McEliece, "Irreducible cyclic codes and Gauss sums," in *Combinatorics, Part I*, M. Hall, Jr. and J. H. van Lint, Eds. Amsterdam, The Netherlands: Mathematisch Centrum, 1974, Mathematical Center Tracts 55.
- [19] R. J. McEliece and H. Rumsey, Jr., "Euler products, cyclotomy, and coding," *J. Number Theory*, vol. 4, pp. 302–311, 1972.
- [20] H. Niederreiter, "Weights of cyclic codes," *Inform. Contr.*, vol. 34, no. 2, pp. 130–140, 1977.
- [21] V. S. Pless, W. C. Huffman, and R. A. Brualdi, "An introduction to algebraic codes," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: North-Holland, 1998, vol. I, pp. 3–139.
- [22] T. Storer, *Cyclotomy and Difference Sets*. Chicago, IL: Markham, 1967.
- [23] L.-H. Zetterberg, "Cyclic codes from irreducible polynomials for correction of multiple errors," *IEEE Trans. Inform. Theory*, vol. IT-8, pp. 13–20, Jan. 1962.