FINITE FIELDS AND THEIR APPLICATIONS **4,** 140–166 (1998)
ARTICLE NO. FF980207

New Generalized Cyclotomy and Its Applications

Cunsheng Ding

Department of Information Systems and Computer Science, and National University of Singapore, Lower Kent Ridge Road, Singapore 119260
E-mail: dingcs@iscs.nus.edu.sg

and

Tor Helleseth

Department of Informatics, University of Bergen, N-5020 Bergen, Norway
E-mail: Tor.Helleseth@ii.uib.no

Communicated by Dieter Jungnickel

Received February 14, 1997; revised September 26, 1998

In this paper we first introduce a new generalized cyclotomy of order 2 with respect to $p_1^{e_1} \cdots p_t^{e_t}$, then we calculate the new cyclotomic numbers of order 2. Some applications of the new cyclotomy in sequences, cryptography, and coding theory are also discussed. In the last section of this paper, we introduce more generalized cyclotomies and point out their applications. The major motivation behind the new generalized cyclotomies is the construction of binary duadic codes. © 1998 Academic Press

1. INTRODUCTION

Let $n \geq 2$ be a positive integer. A partition $\{D_0, D_1, \ldots, D_{d-1}\}$ of Z_n^* is a family of sets with

$$D_1 \cap D_j = \emptyset \quad \text{for all } i \neq j, \qquad \bigcup_{i=0}^{d-1} D_i = Z_n^*.$$

If D_0 is a multiplicative subgroup of Z_n^*, and there are elements $g_1, \ldots, g_{d-1}$ of Z_n^* such that $D_i = g_i D_0$ for all i, the D_i are called *generalized cyclotomic classes* of order d when n is composite, and *classical cyclotomic classes* of order d when n is prime. The (generalized) cyclotomic numbers of order d are

1071-5797/98 $25.00

defined by

$$(i,j) = |(D_i + 1) \cap D_j|, \qquad i,j = 0,1, \ldots, d-1.$$

Note that there could exist many multiplicative subgroups D_0 of index d of Z_n^*. Different D_0 give different generalized cyclotomies and cyclotomic numbers of order d.

Cyclotomy is an old topic of elementary number theory. Cyclotomic and generalized cyclotomic numbers are related to Waring's problem [6], difference sets [3, 16, 17], sequences [4, 5, 10], coding theory [14, 15], and cryptography [7].

Classical cyclotomy was dealt to a good extent by Gauss in his "Disquisitiones Arithmeticae" [9], where he introduced the so called *Gaussian periods*, and *cyclotomic numbers*. Both Gaussian periods and some cyclotomic numbers are related to some cyclic codes [13, 15].

Cyclotomic numbers of order up to 24 with respect to primes have been calculated with various kinds of character sums. Generalized cyclotomic numbers of order 2 with respect to p^2 were presented in [7] for cryptographic purpose, but no proof was given. A generalized cyclotomy with respect to pq was introduced by Whiteman [17], where the motivation is to search for residue difference sets. Whiteman's Generalized cyclotomic numbers of orders 2, 4, and 6 with respect to pq are known now. However, his generalized cyclotomy is not consistent with classical cyclotomy.

In this paper, we first introduce a new generalized cyclotomy with respect to $p_1^{e_1} \cdots p_t^{e_t}$, which includes classical cyclotomy as a special case. Then we compute the generalized cyclotomic numbers of order 2, and investigate some applications of the new generalized cyclotomy in sequences, cryptography, and coding theory. Finally, we introduce more new generalized cyclotomies and point out their applications.

2. NEW GENERALIZED CYCLOTOMY w.r.t. $p_1^{e_1} \cdots p_t^{e_t}$

For a positive integer $n \geq 2$, we use Z_n to denote the ring $Z_n = \{0, 1, 2, \ldots, n-1\}$ with integer addition modulo n and integer multiplication modulo n as the ring operations. Here and hereafter $a \bmod n$ denotes the least nonnegative integer that is congruent to a modulo n. As usual, we use Z_n^* to denote all the invertible elements of Z_n.

Let S be a subset of Z_n and a an element of Z_n, define

$$a + S = S + a = \{s + a : s \in S\}, \qquad aS = Sa = \{as : s \in S\},$$

where addition and multiplication refer to those of Z_n.

Let $p_1, p_2, \ldots, p_t$ be pairwise distinct odd primes satisfying

$$\gcd(p_i^{e_i-1}(p_i-1), p_j^{e_j-1}(p_j-1)) = 2 \qquad \text{for all } i \neq j. \tag{1}$$

Thus, there is at most one p_i such that $p_i \equiv 1 \pmod 4$.

Let $e_1 \geq 1, \ldots, e_t \geq 1$ be integers. Define

$$n = \prod_{i=1}^{t} p_i^{e_i}, \qquad e = 2^{1-t} \prod_{i=1}^{t} p_i^{e_i-1}(p_i-1).$$

The group Z_n^* of all invertible elements of Z_n has cardinality

$$\phi(n) = \prod_{i=1}^{t} (p_i-1)p_i^{e_i-1},$$

where $\phi(x)$ denotes the Euler function.

An integer a is said to be a *primitive root* of (or modulo) n if the multiplicative order of a modulo n is $\phi(n)$, where $\gcd(a, n) = 1$. It is well-known that the only integers having primitive roots are p^e, $2p^e$, 1, 2, and 4, where p is an odd prime.

If g is a primitive root of p^2, then it is one of p. g is a primitive root of p^2 if and only if it is one of all p^i for $i \geq 1$ [1]. That g is a primitive root of p does not necessarily imply that it is one of p^2, but such a case is rare.

Let g_i be a primitive root of $p_i^{e_i}$. Define g to be the unique solution of the following set of congruences

$$g \equiv g_i \pmod{p_i^{e_i}}, \qquad i = 1, 2, \ldots, t,$$

where $0 \leq g \leq n-1$. Then g is a common primitive root of $p_1^{e_1} \cdots p_t^{e_t}$.

The following Generalized Chinese Remainder Theorem is frequently used in the sequel. For a proof of the Generalized Chinese Remainder Theorem and a comprehensive treatment of applications of the Chinese Remainder Theorem in computing, coding, and cryptography, we refer to [8].

LEMMA 1. *Let $m_1, \ldots, m_t$ be positive integers. For a set of integers $a_1, \ldots, a_t$, the system of congruences*

$$x \equiv a_i \pmod{m_i}, \qquad i = 1, \ldots, t$$

has solutions if and only if

$$a_i \equiv a_j \pmod{\gcd(m_i, m_j)}, \qquad i \neq j,\ 1 \leq i, j \leq t. \tag{2}$$

If (2) *is satisfied, the solution is unique modulo* $\operatorname{lcm}(m_1, \ldots, m_t)$.

To introduce the generalized cyclotomy, we need a set of elements $\{y_1, \ldots, y_t\}$. For each $1 \le i \le t$, let y_i be the unique solution of the set of congruences

$$\begin{aligned} y_i &\equiv g \pmod{p_i^{e_i}}, \\ y_i &\equiv 1 \pmod{p_j^{e_j}}, \qquad j \ne i, \end{aligned} \tag{3}$$

where $0 \le y_i \le n-1$. The existence and uniqueness of y_i are guaranteed by the Chinese Remainder Theorem.

LEMMA 2. $\operatorname{ord}_n(g) = e$.

Proof. By the Chinese Remainder Theorem and (1)

$$\begin{aligned} \operatorname{ord}_n(g) &= \operatorname{lcm}\{\operatorname{ord}_{p_1^{e_1}}(g), \ldots, \operatorname{ord}_{p_t^{e_t}}(g)\} \\ &= \operatorname{lcm}\{\phi(p_1^{e_1}), \ldots, \phi(p_t^{e_t})\} \\ &= \operatorname{lcm}\{p_1^{e_1-1}(p_1-1), \ldots, p_t^{e_t-1}(p_t-1)\} \\ &= e. \qquad \blacksquare \end{aligned}$$

For $t \ge 2$, define

$$Y = \{y_1^{a_1} y_2^{a_2} \cdots y_{t-1}^{a_{t-1}} : a_i \in \{0,1\}\}.$$

For $t = 1$, we define $Y = \{1\}$. Let $G = (g^2)$ be the subgroup of Z_n^*, generated by g^2. By Lemma 2, $|G| = e/2$.

LEMMA 3. *$y^2 \in G$ for each $y \in Y$.*

Proof. By definition, every element $y \in Y$ must be of the form

$$y = y_1^{a_1} y_2^{a_2} \cdots y_{t-1}^{a_{t-1}},$$

where $a_i \in \{0,1\}$. It follows that

$$y^2 = y_1^{2a_1} y_2^{2a_2} \cdots y_{t-1}^{2a_{t-1}}.$$

We want to prove now that there is an even s with $0 \le s \le e-1$ such that $y^2 = g^s$. By the Chinese Remainder Theorem, it is equivalent to solving the following system of congruences

$$\begin{aligned}
&g^s \equiv g^{2a_1} && (\mathrm{mod}\ p_1^{e_1}),\\
&\vdots\\
&g^s \equiv g^{2a_{t-2}} && (\mathrm{mod}\ p_{t-2}^{e_{t-2}}),\\
&g^s \equiv g^{2a_{t-1}} && (\mathrm{mod}\ p_{t-1}^{e_{t-1}}),\\
&g^s \equiv 1 && (\mathrm{mod}\ p_t^{e_t}).
\end{aligned}$$

This has a solution if and only if

$$\begin{aligned}
&s \equiv 2a_1 && (\mathrm{mod}\ p_1^{e_1-1}(p_1-1)),\\
&\vdots\\
&s \equiv 2a_{t-2} && (\mathrm{mod}\ p_{t-2}^{e_{t-2}-1}(p_{t-2}-1)),\\
&s \equiv 2a_{t-1} && (\mathrm{mod}\ p_{t-1}^{e_{t-1}-1}(p_{t-1}-1)),\\
&s \equiv 0 && (\mathrm{mod}\ p_t^{e_t-1}(p_t-1))
\end{aligned} \tag{4}$$

has a solution. By (1) and the above Generalized Chinese Remainder Theorem, there is a unique solution s modulo e of (4). By the last congruence of (4), s is even. Again by the Chinese Remainder Theorem $g^s = y^2$. ■

Define

$$D_0^{(n)} = \{g^{2s}y : s = 0, 1, \ldots, (e-2)/2;\ y \in Y\}.$$

LEMMA 4. *$D_0^{(n)}$ is a subgroup of Z_n^* with $|D_0^{(n)}| = 2^{t-2}e$.*

Proof. Let

$$a = g^{s_1}y_1^{a_1}y_2^{a_2}\cdots y_{t-1}^{a_{t-1}},$$
$$b = g^{s_2}y_1^{b_1}y_2^{b_2}\cdots y_{t-1}^{b_{t-1}}$$

be two elements of $D_0^{(n)}$, where s_1 and s_2 are even. By Lemma 3,

$$y_i^{a_i+b_i} = \begin{cases} 1, & \text{if } a_i + b_i = 0;\\ y_i, & \text{if } a_i + b_i = 1;\\ g^s, & \text{if } a_i + b_i = 2, \end{cases}$$

where s is an even integer. Thus, $ab \in D_0^{(n)}$.

Let the above a be a fixed element of $D_0^{(n)}$. Let the described b above be a variable. We wish to find an even integer $0 \le s_2 \le e-1$, and $b_i \in \{0, 1\}$

such that $ab = 1$. These b_i are defined as follows:

$$b_i = \begin{cases} 0, & \text{if } a_i = 0; \\ 1, & \text{if } a_i = 1. \end{cases}$$

By Lemma 3, define

$$u_i = \begin{cases} 0, & \text{if } a_i = 0; \\ u, & \text{if } a_i = 1, \end{cases}$$

where u is the unique one such that $g^u = y_i^2$, by Lemma 3 u is even. By defining

$$s_2 = -(s_1 + u_1 + \cdots + u_{t-1}) \bmod e,$$

the corresponding b satisfies $ab \equiv 1 \pmod{n}$. Note that since $s_1, u_1, \ldots, u_{t-1}$ and e are even, the obtained s_2 must be even. Hence, $a \in D_0^{(n)}$ implies that $a^{-1} \in D_0^{(n)}$. This proves that $D_0^{(n)}$ is a group.

It is obvious that $|D_0^{(n)}| \leq 2^{t-2}e$. Assume that two elements

$$a = g^{s_1} y_1^{a_1} y_2^{a_2} \cdots y_{t-1}^{a_{t-1}},$$

$$b = g^{s_2} y_1^{b_1} y_2^{b_2} \cdots y_{t-1}^{b_{t-1}}$$

of $D_0^{(n)}$ are equal, where s_1 and s_2 are even. Modulo $p_i^{e_i}$ this implies $s_1 + a_i \equiv s_2 + b_i \pmod 2$ and therefore $a_i = b_i$ for $1 \leq i \leq t-1$. Hence, $g^{s_1} = g^{s_2}$ and $s_1 = s_2$. This proves that $|D_0^{(n)}| = 2^{t-2}e$. ■

LEMMA 5. $g \notin D_0^{(n)}$.

Proof. Suppose that $g = g^s y_1^{a_1} \cdots y_{t-1}^{a_{t-1}}$, where $0 \leq s \leq e-1$ is even, $a_i \in \{0, 1\}$. This can be written as

$$g^{-s+1} = y_1^{a_1} \cdots y_{t-1}^{a_{t-1}}.$$

Modulo $p_t^{e_t}$ this gives $g^{-s+1} = 1$, which implies that $-s+1$ is even, contradicting that s was even. ■

Define

$$D_1^{(n)} = gD_0^{(n)},$$

where the arithmetic is that of Z_n. Combining Lemmas 2, 4 and 5 yields the following result.

LEMMA 6. *$D_0^{(n)} \cap D_1^{(n)} = \emptyset$, $D_0^{(n)} \cup D_1^{(n)} = Z_n^*$, where $\emptyset$ denotes the empty set.*

We call $D_0^{(n)}$ and $D_1^{(n)}$ the new *generalized cyclotomic classes* of order 2 with respect to n. Our generalized cyclotomy is rather different from Whiteman's [17]. In the following $D_i^{(n)}$ will denote $D_{i \bmod 2}^{(n)}$.

LEMMA 7. *Let $a \in D_j^{(n)}$. Then $aD_i^{(n)} = D_{i+j}^{(n)}$.*

Proof. Note that $a \in D_j^{(n)}$ can be expressed as

$$a = g^{s+j} y_1^{a_1} \cdots y_{t-1}^{a_{t-1}},$$

where s is even. Any $b \in D_i^{(n)}$ can be expressed as

$$b = g^{t+i} y_1^{b_1} \cdots y_{t-1}^{b_{t-1}},$$

where t is even. Hence,

$$ab = g^{t+s+i+j} y_1^{a_1+b_1} \cdots y_{t-1}^{a_{t-1}+b_{t-1}}.$$

By Lemma 3, $ab \in D_{i+j}$. ■

3. NEW GENERALIZED CYCLOTOMIC NUMBERS

Let p be an odd prime and let $(i,j)^{(p)}$ denote the cyclotomic numbers of order 2 with respect to p. The following conclusion is well-known [16].

LEMMA 8. *If $p \equiv 3 \pmod 4$, then*

$$(1,0)^{(p)} = (0,0)^{(p)} = (1,1)^{(p)} = \frac{p-3}{4}, \qquad (0,1)^{(p)} = \frac{p+1}{4}.$$

If $p \equiv 1 \pmod 4$, then

$$(0,1)^{(p)} = (1,0)^{(p)} = (1,1)^{(p)} = \frac{p-1}{4}, \qquad (0,0)^{(p)} = \frac{p-5}{4}.$$

Recall the generalized cyclotomic classes introduced in Section 2 and the generalized cyclotomic numbers defined in Section 1. Before calculating the generalized cyclotomic numbers of order 2 with respect to n, we first compute those with respect to p^m.

Let g be a primitive root of p^m, $D_0^{(p^m)} = (g^2)$, and $D_1^{(p^m)} = gD_0^{(p^m)}$, where the arithmetic is that of Z_{p^m}. Define

$$R^{(p^m)} = \{0, p, 2p, \ldots, (p^{m-1} - 1)p\}.$$

Then

$$Z_{p^m} = R^{(p^m)} \cup D_0^{(p^m)} \cup D_1^{(p^m)}.$$

LEMMA 9.

$$|R^{(p^m)} \cap (D_1^{(p^m)} + 1)| = \begin{cases} 0, & p \equiv 1 \pmod 4, \\ p^{m-1}, & p \equiv 3 \pmod 4. \end{cases}$$

$$|R^{(p^m)} \cap (D_0^{(p^m)} + 1)| = \begin{cases} p^{m-1}, & p \equiv 1 \pmod 4, \\ 0, & p \equiv 3 \pmod 4. \end{cases}$$

Proof. $g^{2s} + 1 \in R^{(p^m)}$ if and only if $g^{2s} \equiv -1 \pmod p$. Since g is a primitive root of p, $g^{2s} \equiv -1 \pmod p$ if and only if $2s \equiv (p-1)/2 \pmod{p-1}$. This is impossible if $p \equiv 3 \pmod 4$. If $p \equiv 1 \pmod 4$, then $(p-1)/2$ is even. So $2s = (p-1)/2 + a(p-1)$ for some a. It follows that

$$0 \le 2s = (p-1)\frac{1+2a}{2} \le p^{m-1}(p-1).$$

Hence, $0 \le a \le p^{m-1} - 1$. This proves the second part of the lemma, and the first part then follows easily. ■

The relations between the cyclotomic numbers $(i,j)^{(p^m)}$ are described by the following lemma:

LEMMA 10.

1. $(0,0)^{(p^m)} + (1,0)^{(p^m)} = \dfrac{p^{m-1}(p-3)}{2}$.

2. $(0,1)^{(p^m)} + (1,1)^{(p^m)} = \dfrac{p^{m-1}(p-1)}{2}$.

3. $(1,0)^{(p^m)} + (1,1)^{(p^m)} = \begin{cases} \frac{p^{m-1}(p-1)}{2}, & p \equiv 1 \pmod 4, \\ \frac{p^{m-1}(p-3)}{2}, & p \equiv 3 \pmod 4. \end{cases}$

4. $(0,0)^{(p^m)} + (0,1)^{(p^m)} = \begin{cases} \frac{p^{m-1}(p-3)}{2}, & p \equiv 1 \pmod 4, \\ \frac{p^{m-1}(p-1)}{2}, & p \equiv 3 \pmod 4. \end{cases}$

Proof. We prove only part four, and the rest can be similarly proved. Note that

$$D_0^{(p^m)} \cup D_1^{(p^m)} \cup R^{(p^m)} = Z_{p^m}.$$

By definition and Lemma 9

$$\begin{aligned}(0,0)^{(p^m)} + (0,1)^{(p^m)} &= |D_0^{(p^m)} \cap (D_0^{(p^m)} + 1)| + |D_1^{(p^m)} \cap (D_0^{(p^m)} + 1)| \\ &= p^{m-1}(p-1)/2 - |R^{(p^m)} \cap (D_0^{(p^m)} + 1)| \\ &= \begin{cases} \frac{p^{m-1}(p-3)}{2}, & p \equiv 1 \pmod 4, \\ \frac{p^{m-1}(p-1)}{2}, & p \equiv 3 \pmod 4. \end{cases}\end{aligned}$$

THEOREM 1. *If* $p \equiv 3 \pmod 4$, *then*

$$(1,0)^{(p^m)} = (0,0)^{(p^m)} = (1,1)^{(p^m)} = \frac{p^{m-1}(p-3)}{4}, \qquad (0,1)^{(p^m)} = \frac{p^{m-1}(p+1)}{4}.$$

If $p \equiv 1 \pmod 4$, *then*

$$(0,1)^{(p^m)} = (1,0)^{(p^m)} = (1,1)^{(p^m)} = \frac{p^{m-1}(p-1)}{4}, \qquad (0,0)^{(p^m)} = \frac{p^{m-1}(p-5)}{4}.$$

Proof. Since g is a primitive root of p^m,

$$D_i^{(p^m)} \bmod p = \{\underbrace{x, \ldots, x}_{p^{m-1}} : x \in D_i^{(p)}\}. \tag{5}$$

It follows that

$$\begin{aligned}(i,j)^{(p^m)} &= |(D_i^{(p^m)} + 1) \cap D_j^{(p^m)}| \\ &= p^{m-1}|(D_i^{(p)} + 1) \cap D_j^{(p)}| \\ &= p^{m-1}(i,j)^{(p)}.\end{aligned}$$

The conclusions of this theorem then follows from Lemma 8. ■

This theorem can also be proved by considering some character sums or some Gaussian periods, but we prefer this straightforward approach here.

THEOREM 2. *For any* $r \in R^{(p^m)}$,

$$|(D_i^{(p^m)} + r) \cap D_j^{(p^m)}| = \begin{cases} p^{m-1}(p-1)/2, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Note that $r \bmod p = 0$. It follows from (5) that

$$|(D_i^{(p^m)} + r) \cap D_j^{(p^m)}| = p^{m-1} |D_i^{(p)} \cap D_j^{(p)}|.$$

The conclusion then follows. ■

Now we are ready to compute the new cyclotomic numbers of order 2 with respect to $n = p_1^{e_1} \cdots p_t^{e_t}$.

THEOREM 3.

$$(i,j)^{(n)} = (i,j)^{(p_t^{e_t})} \prod_{k=1}^{t-1} (p_k^{e_k} - 2p_k^{e_k - 1}),$$

where $(i,j)^{(p_t^{e_t})}$ *are given in Theorem* 1.

Proof. Recall the definition of $D_i^{(n)}$ and $D_i^{(p_i^{e_i})}$. The Chinese Remainder Theorem says that the mapping

$$\tau : Z_n \to Z_{p_1^{e_1}} \times \cdots \times Z_{p_t^{e_t}},$$
$$\tau(x) = (x \bmod p_1^{e_1}, \ldots, x \bmod p_t^{e_t})$$

is an isomorphism between the two rings. We now prove that τ is a one-to-one mapping between the following two sets:

$$\tau : D_i^{(n)} \mapsto \bigcup_{a_1, \ldots, a_{t-1} \in \{0,1\}} D_{i+a_1}^{(p_1^{e_1})} \times \cdots \times D_{i+a_{t-1}}^{(p_{t-1}^{e_{t-1}})} \times D_i^{(p_t^{e_t})}. \tag{6}$$

By definition, every $x \in D_i^{(n)}$ must be of the form

$$x = g^{2s+i} y_1^{a_1} \cdots y_{t-1}^{a_{t-1}}.$$

By the definition of y_i, we have

$$\tau(x) = (g^{2s+i+a_1} \bmod p_1^{e_1}, \ldots, g^{2s+i+a_{t-1}} \bmod p_{t-1}^{e_{t-1}}, g^{2s+i} \bmod p_t^{e_t}).$$

Hence,

$$\tau(x) \in D_{i+a_1}^{(p_1^{e_1})} \times \cdots \times D_{i+a_{t-1}}^{(p_{t-1}^{e_{t-1}})} \times D_i^{(p_t^{e_t})}.$$

On the other hand, for any

$$(x_1, \ldots, x_t) \in D_{i+a_1}^{(p_1^{e_1})} \times \cdots \times D_{i+a_{t-1}}^{(p_{t-1}^{e_{t-1}})} \times D_i^{(p_t^{e_t})},$$

by the Chinese Remainder Theorem there is an $x \in Z_n$ such that $\tau(x) = (x_1, \ldots, x_t)$. Obviously, x is not a zero divisor of Z_n. Thus, it must belong to $D_i^{(n)} \cup D_{i+1}^{(n)}$. By the proof above, $x \in D_i^{(n)}$. Hence, τ is surjective. The Chinese Remainder Theorem says that τ is injective.

It is straightforward to see that

$$\bigcup_{a_1, \ldots, a_{t-1} \in \{0,1\}} D_{i+a_1}^{(p_1^{e_1})} \times \cdots \times D_{i+a_{t-1}}^{(p_{t-1}^{e_{t-1}})} \times D_i^{(p_t^{e_t})} = Z_{p_1^{e_1}}^* \times \cdots \times Z_{p_{t-1}^{e_{t-1}}}^* \times D_i^{(p_t^{e_t})}.$$

Hence

$$\tau : D_i^{(n)} \to Z_{p_1^{e_1}}^* \times \cdots \times Z_{p_{t-1}^{e_{t-1}}}^* \times D_i^{(p_t^{e_t})}$$

is a group isomorphism.

Note that

$$|(Z_{p_i^{e_i}}^* + 1) \cap Z_{p_i^{e_i}}^*| = p_i^{e_i} - 2p_i^{e_i - 1}.$$

It then follows that

$$\begin{aligned}(i,j)^{(n)} &= |(D_i^{(n)} + 1) \cap D_j^{(n)}| \\ &= |[Z_{p_1^{e_1}}^* \times \cdots \times Z_{p_{t-1}^{e_{t-1}}}^* \times D_i^{(p_t^{e_t})} + (1, 1, \ldots, 1)] \\ &\quad \cap [Z_{p_1^{e_1}}^* \times \cdots \times Z_{p_{t-1}^{e_{t-1}}}^* \times D_j^{(p_t^{e_t})}]| \\ &= (i,j)^{(p_t^{e_t})} \prod_{k=1}^{t-1} (p_k^{e_k} - 2p_k^{e_k - 1}).\end{aligned}$$

This theorem and Theorem 1 determine the new cyclotomic numbers of order 2 with respect to n completely.

4. APPLICATIONS IN SEQUENCES AND CRYPTOGRAPHY

In this section we show how to construct binary sequences and some cryptographic mappings based on this new generalized cyclotomy. To this end, we need to do some preparations.

For any divisor $d = \prod_{k=1}^{m} p_{i_k}^{l_{i_k}}$ of n, where m is any integer with $1 \le m \le t$, $1 \le i_1 < \cdots < i_m \le t$, we can similarly define the cyclotomic classes $D_0^{(d)}$ and $D_1^{(d)}$ with respect to d using the parameters $y_{i_1}, \ldots, y_{i_m}$.

Similar to Lemmas 4 and 6, we have the following conclusion (the proof is exactly the same).

LEMMA 11. *Let $d > 1$ be a divisor of n. Then*

1. *$D_0^{(d)}$ is a subgroup of Z_d^* with*

$$|D_0^{(d)}| = \phi(d)/2.$$

2. *The two $D_i^{(d)}$ form a partition of Z_d^**, i.e.,

$$D_0^{(d)} \cap D_1^{(d)} = \emptyset, \qquad D_0^{(d)} \cup D_1^{(d)} = Z_d^*.$$

The following result allows us to get a partition of Z_n for the purpose of constructing our binary sequences.

LEMMA 12.

$$Z_n \setminus \{0\} = \bigcup_{d|n,\, d>1} \left[\frac{n}{d} (D_0^{(d)} \cup D_1^{(d)}) \right].$$

Proof. Note that every a with $1 \le a \le n-1$ can be written in the form

$$a = \frac{n}{d} a_1,$$

where $d > 1$ is a divisor of n, $1 \le a_1 \le d-1$, and $\gcd(a_1, n) = 1$. It follows that

$$a_1 \in D_0^{(d)} \cup D_1^{(d)}$$

and

$$a \in \frac{n}{d} (D_0^{(d)} \cup D_1^{(d)}).$$

Hence

$$Z_n \setminus \{0\} \subseteq \left[\bigcup_{d|n,\, d>1} \frac{n}{d} (D_0^{(d)} \cup D_1^{(d)}) \right].$$

We now calculate the cardinality of the set described above. By Lemma 11 we have

$$|D_0^{(d)} \cup D_1^{(d)}| = \phi(d).$$

It follows that the cardinality of the set, denoted by Δ, is

$$\Delta = \sum_{d|n,\, d>1} \phi(d) = n - 1,$$

which is a well-known result in number theory. This completes the proof. ■

With this lemma, we are now ready to define the binary sequence based on this new generalized cyclotomy. Let

$$C_1 = \{0\} \cup \left[\bigcup_{d|n,\, d>1} \frac{n}{d} D_1^{(d)} \right] \tag{7}$$

and

$$C_0 = \bigcup_{d|n,\, d>1} \frac{n}{d} D_0^{(d)}. \tag{8}$$

By Lemma 12, $\{C_0, C_1\}$ is a partition of Z_n, i.e.,

$$C_0 \cap C_1 = \emptyset, \qquad C_0 \cup C_1 = Z_n.$$

The binary periodic sequence s^∞ is then defined by

$$s_i = a \text{ if and only if } (i \bmod n) \in C_a,$$

where $i \bmod n$ denotes the least nonnegative integer that is congruent to i modulo n. Lemma 12 ensures that the sequence is well defined.

The sequence s^∞ has least period n. In one cycle of this sequence there are $(n-1)/2$ zeros and $(n+1)/2$ ones. Thus, the balance between 0 and 1 are optimal since n is odd. The autocorrelation of this sequence partly depends on the cyclotomic numbers of order 2, and should be ideal if n is properly chosen.

As an example, we consider the case $n = 3 \times 7 = 21$. It is easy to check that

$$D_0^{(3)} = \{1\}, \qquad D_0^{(7)} = \{1, 2, 4\}, \qquad D_0^{(21)} = \{1, 2, 4, 8, 11, 16\}.$$

If follows that

$$C_0 = 7D_0^{(3)} \cup 3D_0^{(7)} \cup D_0^{(21)} = \{1, 2, 3, 4, 6, 7, 8, 11, 12, 16\}.$$

Hence, the corresponding sequence is

$$s^{\infty} = \underbrace{10000100011001101111}\ \underbrace{10000100011001101111}\cdots$$

The periodic autocorrelation function of a binary sequence s^{∞} of period N is defined by

$$C_s(a) = \sum_{i=0}^{N-1} (-1)^{s_i + s_{i+a}}.$$

The autocorrelation values of this special sequence are described as follows:

$$C_s(a) = \begin{cases} -3, & \text{if } a \in \{2,3,6,8,9,10,11,12,13,15,18,19\}; \\ 5, & \text{if } a \in \{1,4,5,16,17,20\}; \\ -7, & \text{if } a \in \{7,14\}. \end{cases}$$

It is essential to note that for many odd n there are no $(n,(n-1)/2,\lambda)$ residue difference sets on Z_n. This means that it is impossible to construct sequences s^{∞} such that

- in a cycle of the sequence the difference between the number of ones and that of zeros is one; and
- its autocorrelation function is two-valued.

Thus, the above sequence based on this new generalized cyclotomy could be the best, as far as autocorrelation property is concerned. We also mention that the linear complexity (linear span) of these sequences should be quite good. We will compute the exact linear complexity in a separate work.

This new generalized cyclotomy has also applications in cryptography. Let $f(x)$ be a mapping from Z_n to Z_2. The differentiality and nonlinearity of $f(x)$ are measured by

$$p(a,b) = \Pr(f(x+a) - f(x) = b),$$

where Pr denotes the probability and $0 \neq a \in Z_n$ and $b \in Z_2$. The flatter the values $p(a,b)$ for all $a \in Z_n^*$ and all $b \in Z_2$, the better the differentiality and nonlinearity of this mapping. In some cryptographic applications, such as the construction of keystream generators, we need such mappings $f(x)$ with good nonlinearity.

With this new generalized cyclotomy we can construct mappings from Z_n to Z_2 with ideal nonlinearity with respect to the additions of Z_n and Z_2, provided that n is chosen properly. This is done as follows.

Let C_1 and C_0 be the subsets defined in (7) and (8) respectively. We define the mapping $f(x)$ by

$$f(x) = i \text{ if } x \in C_i, \qquad i = 0, 1.$$

Its differentiability and nonlinearity depend partly on the generalized cyclotomic numbers of order 2. An interesting case is $n = pq$, the product of two different primes. The most interesting case is when $n = p(p+2)$, where p and $p+2$ are twin primes. Here the application of this new generalized cyclotomy in cryptography is similar to that of Whiteman's described in [7]. We refer to [7] for details.

5. APPLICATION IN CODING THEORY

Quadratic residue codes [14, Chapter 16] of prime lengths are a class of interesting error-correcting codes due to a high minimum distance. Those codes have a "square root bound" [2], which roughly asserts that the square of the minimum distance is greater than the block length. Those codes are special cases of the duadic codes discovered by Leon, Masley and Pless [12]. It should be noted that it is not known how many duadic codes of length $n = p_1^{e_1} \cdots p_t^{e_t}$ there are and how to construct them. Using the new generalized cyclotomy of order 2, we can give a constructive approach to a large number of the duadic error-correcting codes as follows.

Let θ be an nth primitive root of unity over a field F containing $GF(2)$. For any positive integer $d|n$ and $d \neq 1$, we define the new generalized cyclotomic polynomials of order 2 with respect to d by

$$d_k^{(d)}(x) = \prod_{a \in D_k^{(d)}} (x - \theta^{\frac{na}{d}}), \qquad k = 0, 1.$$

Whether these polynomials belong to $GF(2)[x]$ or not depends on the primes p_i. We shall come to this problem later. Now we consider the factorization of $x^n - 1$ over F.

By Lemma 12 we have the following result.

LEMMA 13.

$$\frac{x^n - 1}{x - 1} = \prod_{d|n,\, d>1} d_0^{(d)}(x) d_1^{(d)}(x).$$

LEMMA 14. *For any $1 \leq a \leq p-1$, $a \in D_i^{(p)}$ if and only if $a \in D_i^{(p^l)}$ for all $l \geq 1$, where p is an odd prime.*

Proof. The proof is straightforward and is omitted.

LEMMA 15. *$2 \in D_0^{(n)}$ if and only if $p_t \equiv \pm 1 \pmod 8$.*

Proof. Assume that $2 \in D_0^{(n)}$, there exists an even s with $1 \le s \le e-1$ and $a_i \in \{0,1\}$ such that

$$2 = g^s y_1^{a_1} \cdots y_{t-1}^{a_{t-1}}.$$

In particular $g^s \equiv 2 \pmod{p_t^{e_t}}$, since s is even, the last congruence implies that 2 is a quadratic residue of p_t. Thus, $p_t \equiv \pm 1 \pmod 8$ by the Law of Quadratic Reciprocity.

Assume that $p_t \equiv \pm 1 \pmod 8$, by Lemma 14 we can find integers $s_1, \ldots, s_t$ satisfying $g^{s_i} \equiv 2 \pmod{p_i^{e_i}}$ for $i = 1, 2, \ldots, t$, where s_t is even. We choose $a_i = 0$ if s_i is even, and choose $a_i = 1$ if s_i is odd for $i = 1, 2, \ldots, t-1$. Consider now the following set of congruences

$$\begin{aligned}
&s \equiv s_1 - a_1 && (\bmod\, p_1^{e_1-1}(p_1-1)),\\
&\vdots\\
&s \equiv s_{t-2} - a_{t-2} && (\bmod\, p_{t-2}^{e_{t-2}-1}(p_{t-2}-1)),\\
&s \equiv s_{t-1} - a_{t-1} && (\bmod\, p_{t-1}^{e_{t-1}-1}(p_{t-1}-1)),\\
&s \equiv s_t && (\bmod\, p_t^{e_t-1}(p_t-1)).
\end{aligned} \tag{9}$$

Since $s_i - a_i$ is even for $i = 1, 2, \ldots, t-1$ and s_t is also even, by the Generalized Chinese Remainder Theorem, (9) has a unique solution $0 \le s \le e-1$. Clearly s is even. By the Chinese Remainder Theorem, the element $g^s y_1^{a_1} \cdots y_{t-1}^{a_{t-1}}$ is equal to 2, and is an element of $D_0^{(n)}$. ■

LEMMA 16. *Let $d > 1$ be a positive integer and $d|n$. Then $d_i^{(d)}(x) \in GF(2)[x]$ if and only if $2 \in D_0^{(d)}$.*

Proof. By Lemma 7,

$$\begin{aligned}
d_i^{(d)}(x)^2 &= \prod_{a \in D_i^{(d)}} (x - \theta^{\frac{na}{d}})^2\\
&= \prod_{a \in D_i^{(d)}} (x^2 - \theta^{\frac{2na}{d}})\\
&= \prod_{a \in 2D_i^{(d)}} (x^2 - \theta^{\frac{na}{d}})\\
&= \begin{cases} d_i^{(d)}(x^2), & \text{if } 2 \in D_0^{(d)};\\ d_{(i+1) \bmod 2}^{(d)}(x^2), & \text{if } 2 \in D_1^{(d)}. \end{cases}
\end{aligned}$$

This completes the proof. ■

We are now only interested in the case that all the generalized cyclotomic polynomials $d_i^{(d)}(x)$ belong to $GF(2)[x]$. This is ensured if $p_i \equiv \pm 1 \pmod 8$ for all i. In the sequel we consider only the case $p_i \equiv \pm 1 \pmod 8$ for all i.

By the definition of our new generalized cyclotomy of order 2, the following result is obvious.

LEMMA 17. *Let $d > 1$ be a positive integer and $d|n$. Then the element $g \in D_1^{(n)}$ satisfies*

$$g \bmod d \in D_1^{(d)}.$$

With all the preparations above, we are ready to describe the generalized cyclotomic codes. We begin by defining some polynomials.

For $i = 1, 2$, define

$$g_i(x) = \prod_{d|n,\, d>1} d_i^{(d)}(x).$$

Let $\mathscr{C}_i$ denote the cyclic code of length n with generator polynomial $g_i(x)$.

THEOREM 4. *$\mathscr{C}_i$ is an $[n,(n+1)/2]$ code with minimum odd weight $d \geq \sqrt{n}$. In particular, if $p_i \equiv -1 \pmod 8$ for all i, then $d^2 - d + 1 \geq n$.*

Proof. Let $u(x)$ be a codeword with Hamming weight h of $\mathscr{C}_0$ (resp. $\mathscr{C}_1$), then the polynomial $v(x) = u(x^g) \bmod (x^n - 1)$ is a codeword with Hamming weight h of $\mathscr{C}_1$ (resp. $\mathscr{C}_0$) by Lemmas 7 and 17. Thus, the two codes $\mathscr{C}_0$ and $\mathscr{C}_1$ have the same minimum distance.

Let $a(x)$ be a codeword of minimum odd Hamming weight d of $\mathscr{C}_0$, then the polynomial $b(x)$ defined by

$$b(x) = a(x)a(x^g) \bmod (x^n - 1)$$

is a codeword with odd Hamming weight of both $\mathscr{C}_0$ and $\mathscr{C}_1$. It follows that $b(x)$ is a multiple of $g_0(x)g_1(x)$. But

$$\begin{aligned} g_0(x)g_1(x) &= \frac{x^n - 1}{x - 1} \\ &= 1 + x + x^2 + \cdots x^{n-1}. \end{aligned}$$

Hence, $b(x) = 1 + x + x^2 + \cdots + x^{n-1}$. Since there are at most d^2 terms in $b(x)$, we have $d^2 \geq n$.

If $p_i \equiv -1 \pmod 8$ for all i, then it is not hard to see that $-1 \in D_1^{(d)}$ for any integer $d > 1$ with $d|n$. Thus, replacing g with -1 in the above proof yields

$$d^2 - d + 1 \geq n,$$

since in this case, there are at most $d^2 - d + 1$ terms in $b(x)$. ■

For any integer $d > 1$ with $d|n$, let $u(d) \in \{0, 1\}$. Then $u(x)$ is a mapping from the set of divisors of n to $\{0, 1\}$. Define

$$h_u(x) = \prod_{d|n,\, d>1} d_{u(d)}^{(d)}(x).$$

Let $\mathscr{H}_u$ denote the cyclic code of length n with generator polynomial $h_u(x)$.

The proof of Theorem 4 also proves the following conclusion:

THEOREM 5. *For any mapping u above, $\mathscr{H}_u$ is an $[n,(n+1)/2]$ code with minimum odd Hamming weight $d \geq \sqrt{n}$. In particular, if $p_i \equiv -1 \pmod 8$ for all i, then $d^2 - d + 1 \geq n$.*

Since the number of distinct divisors $d > 1$ of n is

$$w =: (e_1 + 1)(e_2 + 1) \cdots (e_t + 1) - 1,$$

for one set of polynomials $\{d_i^{(d)}(x) : d|n,\ d > 1,\ i = 0, 1\}$ the number of $[n,(n+1)/2]$ binary cyclic codes described by Theorem 5 is 2^w. Let v denote the number of distinct such sets $\{d_i^{(d)}(x) : d|n, d > 1, i = 0, 1\}$, then the number of codes described by the generalized cyclotomic approach is $v2^w$. Thus, the generalized cyclotomic approach gives a large number of such duadic codes described by Leon, Masley and Pless [12].

6. MORE GENERALIZED CYCLOTOMIES AND THEIR APPLICATIONS

In the foregoing sections we have introduced a new generalized cyclotomy and considered its applications in the design of sequences, cryptography, and the construction of a large class of duadic codes. As pointed out at the beginning of this paper, by finding different multiplicative subgroups of index 2 of Z_n^*, we can obtain different generalized cyclotomies of order 2. In this section we introduce more new generalized cyclotomies of order 2 and compute the corresponding cyclotomic numbers of order 2.

For any nonzero vector $a = (a_1, a_2, \ldots, a_t) \in (Z_2)^t$, the equation

$$\sum_{k=1}^{t} i_k a_k = 0$$

over $(Z_2)^t$ has 2^{t-1} solutions $(i_1, i_2, \ldots, i_t) \in (Z_2)^t$. Define

$$I_0^{(a,n)} = \left\{(i_1, i_2, \ldots, i_t) \in (Z_2)^t : \sum_{k=1}^{t} i_k a_k = 0\right\},$$
$$I_1^{(a,n)} = (Z_2)^t \setminus I_0^{(a,n)}.$$

We further define

$$E_0^{(a,n)} = \bigcup_{(i_1, i_2, \ldots, i_t) \in I_0^{(a,n)}} D_{i_1}^{(p_1^{e_1})} \times \cdots \times D_{i_t}^{(p_t^{e_t})}$$

and

$$E_1^{(a,n)} = Z_{p_1^{e_1}}^* \times \cdots \times Z_{p_t^{e_t}}^* \setminus E_0^{(a,n)}.$$

Since τ is an isomorphism from Z_n^* to $Z_{p_1^{e_1}}^* \times \cdots \times Z_{p_t^{e_t}}^*$, let

$$D_i^{(a,n)} = \tau^{-1}(E_i^{(a,n)}), \qquad i = 0, 1.$$

It is straightforward to prove that $E_0^{(a,n)}$ is a multiplicative subgroup of index 2 of $Z_{p_1^{e_1}}^* \times \cdots \times Z_{p_t^{e_t}}^*$. So $D_0^{(a,n)}$ is a subgroup of index 2 of Z_n^*. Clearly there is an element $b \in Z_n^*$ such that $D_1^{(a,n)} = bD_0^{(a,n)}$. The $D_1^{(a,n)}$ and $D_0^{(a,n)}$ are called *generalized cyclotomic classes* of order 2 with respect to a and n. Our generalized cyclotomy introduced before is the special case $a = (0, 0, \ldots, 0, 1)$. The corresponding cyclotomic numbers of order 2 with respect to a and n are similarly defined as before, and denoted by $(i, j)^{(a,n)}$.

THEOREM 6.

$$(l, m)^{(a,n)} = \sum_{(i_1, \ldots, i_t) \in I_l^{(a,n)}} \sum_{(j_1, \ldots, j_t) \in I_m^{(a,n)}} \prod_{k=1}^{t} (i_k, j_k)^{(p_k^{e_k})},$$

where $(i_k, j_k)^{(p_k^{e_k})}$ *are given in Theorem* 1.

Proof. From the definition we have,

$$(l, m)^{(a,n)} = |(D_l^{(a,n)} + 1) \cap D_m^{(a,n)})|$$

$$= \sum_{(i_1, \ldots, i_t) \in I_l^{(a,n)}} \sum_{(j_1, \ldots, j_t) \in I_m^{(a,n)}} \prod_{k=1}^{t} |(D_{i_k}^{(p_k^{e_k})} + 1) \cap D_{j_k}^{(p_k^{e_k})}|$$

$$= \sum_{(i_1, \ldots, i_t) \in I_l^{(a,n)}} \sum_{(j_1, \ldots, j_t) \in I_m^{(a,n)}} \prod_{k=1}^{t} (i_k, j_k)^{(p_k^{e_k})}. \quad \blacksquare$$

We next give an explicit expression for the new generalized cyclotomic numbers of order two.

THEOREM 7. *Let* $a = (a_1, a_2, \ldots, a_t)$, *where we also use the notation* $a_i = a_{p_i}$. *Let* r *denote the number of prime divisors of* n *with* $a_p = 1$ *and* $p \equiv 1 \pmod 4$. *Let* s *denote the number of prime divisors of* n *with* $a_p = 1$ *and* $p \equiv 3 \pmod 4$. *Then*,

$$(l, m)^{(a,n)} = \frac{n}{4} \prod_{p|n} \frac{p-2}{p} \left[1 + \frac{\delta}{\prod_{p|n, a_p = 1} (p-2)} \right]$$

where

$$\delta = \begin{cases} 3(-1)^r, & \text{if } l = 0 \text{ and } m \equiv s \pmod 2, \\ (-1)^{r+1}, & \text{otherwise.} \end{cases}$$

Proof. Let

$$t_{i,j} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \text{ and } (i,j) = (0,0), \\ 0, & \text{if } p \equiv 1 \pmod 4 \text{ and } (i,j) \neq (0,0), \end{cases}$$

then by Lemma 8,

$$(i,j)^{(p_k)} = A_k - t_{i,j}, \qquad \text{where } A_k = \frac{p_k - 1}{4} \text{ and } p_k \equiv 1 \pmod 4.$$

Similarly, let

$$s_{i,j} = \begin{cases} -1, & \text{if } p \equiv 3 \pmod 4 \text{ and } (i,j) = (0,1), \\ 0, & \text{if } p \equiv 3 \pmod 4 \text{ and } (i,j) \neq (0,1), \end{cases}$$

then by Lemma 8,

$$(i,j)^{(p_k)} = B_k - s_{i,j}, \qquad \text{where } B_k = \frac{p_k - 3}{4} \text{ and } p_k \equiv 3 \pmod 4.$$

We divide the prime divisors of n into three sets $P_0 = \{p | a_p = 0\}$, $P_1 = \{p | a_p = 1,\ p \equiv 1 \pmod 4\}$ and $P_3 = \{p | a_p = 1,\ p \equiv 3 \pmod 4\}$. Without loss of generality we assume that the first r components of a correspond to P_1, the next s components to P_3, and the remaining components to P_0. Note that $(i,k)^{(p^k)} = p^{k-1}(i,j)^{(p)}$, and that the indices (i_k, j_k) for $k > r+s$, corresponding to P_0 take on all possible combinations in $Z_2 \times Z_2$. Since, $\sum_{i_k, j_k \in \{0,1\}} (i_k, j_k)^{(p_k)} = p_k - 2$, it follows from Theorem 6 that

$$\begin{aligned}
(l,m)^{(a,n)} &= \frac{n}{\prod_{k=1}^{t} p_k} \sum_{(i_1, \ldots, i_t) \in I_l^{(a,n)}} \sum_{(j_1, \ldots, j_t) \in I_m^{(a,n)}} \prod_{k=1}^{t} (i_k, j_k)^{(p_k)} \\
&= \frac{n}{\prod_{k=1}^{t} p_k} \sum_{i_1 + \cdots + i_{r+s} = l} \sum_{j_1 + \cdots + j_{r+s} = m} \prod_{k=1}^{r+s} (i_k, j_k)^{(p_k)} \\
&\quad \times \prod_{k=r+s+1}^{t} \sum_{i_k, j_k \in \{0,1\}} (i_k, j_k)^{(p_k)} \\
&= \frac{n}{\prod_{k=1}^{t} p_k} \prod_{p \in P_0} (p-2) \sum_{i_1 + \cdots + i_{r+s} = l} \sum_{j_1 + \cdots + j_{r+s} = m} \prod_{k=1}^{r+s} (i_k, j_k)^{(p_k)} \\
&= \frac{n}{\prod_{p|n} p} \prod_{p|n,\, a_p = 0} (p-2)\, T \qquad (10)
\end{aligned}$$

where

$$T = \sum_{i_1 + \cdots + i_{r+s} = l} \sum_{j_1 + \cdots + j_{r+s} = m} \prod_{k=1}^{r+s} (i_k, j_k)^{(p_k)}. \qquad (11)$$

Let

$$L_1 = \{(i_1, i_2, \ldots, i_{r+s}) | \, i_1 + i_2 + \cdots + i_{r+s} = l\}$$

and

$$L_3 = \{(j_1, j_2, \ldots, j_{r+s}) | \, j_1 + j_2 + \cdots + j_{r+s} = m\}.$$

For any subsets S_1 of $\{1, 2, \ldots, r\}$ and S_3 of $\{r+1, r+2, \ldots, r+s\}$, let $\tilde{S}_1$ and $\tilde{S}_3$ denote their respective complements. Expanding the expression for T leads to,

$$\begin{aligned}
T &= \sum_{(i_1, \ldots, i_{r+s}) \in L_1} \sum_{(j_1, \ldots, j_{r+s}) \in L_3} \prod_{k=1}^{r} (A_k - t_{i_k, j_k}) \prod_{k=r+1}^{r+s} (B_k - s_{i_k, j_k}) \\
&= \sum_{S_1} \sum_{S_3} (-1)^{r - |S_1|} \prod_{k \in S_1} A_k \prod_{k \in S_3} B_k (-1)^{s - |S_3|} \sum_{L_1} \sum_{L_3} \prod_{k \in \tilde{S}_1} t_{i_k, j_k} \prod_{k \in \tilde{S}_3} s_{i_k, j_k}.
\end{aligned}$$

Let K_{S_1,S_3} denote the inner double sum over L_1 and L_3. The terms that contribute have $t_{i_k,j_k}=1$ and therefore, $i_k=j_k=0$ for $k\in\tilde{S}_1$ and similarly $s_{i_k,j_k}=-1$ which means $i_k=0, j_k=1$ for $k\in\tilde{S}_3$. The contribution to K_{S_1,S_3} is therefore $(-1)^{s-|S_3|}$ times the number of elements in L_1 and L_3 obeying these restrictions. Therefore,

$$(-1)^{s-|S_3|}K_{S_1,S_3}=\begin{cases}4^{|S_1|+|S_3|-1}, & \text{if } |S_1|+|S_3|>0,\\ 1, & \text{if } |S_1|+|S_3|=0,\ l=0 \text{ and } m\equiv s \pmod 2,\\ 0, & \text{otherwise.}\end{cases}$$

Hence,

$$T=\sum_{(S_1,S_3)\neq(\emptyset,\emptyset)}(-1)^{r-|S_1|}4^{|S_1|+|S_3|-1}\prod_{k\in S_1}A_k\prod_{k\in S_3}B_k+\gamma,$$

where γ corresponds to $S_1=S_3=\emptyset$, i.e.,

$$\gamma=\begin{cases}(-1)^r & \text{if } l=0 \text{ and } m\equiv s \pmod 2,\\ 0 & \text{otherwise.}\end{cases}$$

Therefore,

$$\begin{aligned}T&=\frac{1}{4}\left[\sum_{(S_1,S_3)\neq(\emptyset,\emptyset)}(-1)^{r-|S_1|}\prod_{k\in S_1}(4A_k)\prod_{k\in S_3}(4B_k)+4\gamma\right]\\&=\frac{1}{4}\left[\prod_{k=1}^{r}(4A_k-1)\prod_{k=r+1}^{r+s}(4B_k+1)-(-1)^r+4\gamma\right]\\&=\frac{1}{4}\left[\prod_{k=1}^{r+s}(p_k-2)+(-1)^{r+1}+4\gamma\right]\\&=\frac{1}{4}\left[\prod_{p|n,\,a_p=1}(p-2)+\delta\right],\end{aligned}\tag{12}$$

where δ is as given in the theorem. Substituting this value of T in (10) completes the proof. ■

In the next theorem we show that $|(D_l^{(a,n)}+\tau)\cap D_m^{(a,n)}|$ can be calculated similarly as the cyclotomic numbers in the previous theorem. This result is useful to find the autocorrelation function of the large variety of binary

sequences that can be constructed from the new generalized cyclotomy using the same techniques as in Section 4. For practical applications one would like sequences where the maximum value of the out-of-phase autocorrelation is as small as possible (see [11] for further results on sequences).

Let

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

THEOREM 8. *Let* $\tau_k = \tau \pmod{p_k}$, *where we also use the notation* $\tau_k = \tau_{p_k}$. *Let* r *denote the number of prime divisors of* n *with* $a_p = 1$, $\tau_p \neq 0$, *and* $p \equiv 1 \pmod 4$. *Let* s *denote the number of prime divisors of* n *with* $a_p = 1$, $\tau_p \neq 0$, *and* $p \equiv 3 \pmod 4$, *and let* w *denote the number of prime divisors of* n *with* $a_p = 1$ *and* $\tau_p = 0$. *Then,*

$$|(D_l^{(a,n)} + \tau) \cap (D_m^{(a,n)})| = \frac{n}{4} \prod_{p|n} \frac{p - 2 + \delta_{\tau_p, 0}}{p} \left[1 + \frac{\mu}{\prod_{p|n, a_p = 1, \tau_p \neq 0} (p-2)} \right],$$

where $\tau_p \in D_{u_p}^{(p)}$ *for* $\tau_p \neq 0$ *and* $u = \sum_{p|n, a_p = 1, \tau_p \neq 0} u_p$.

In the case $w \geq 1$, *then*

$$\mu = \begin{cases} (-1)^r, & \text{if } l \equiv u \pmod 2 \text{ and } m \equiv u + s \pmod 2, \\ (-1)^{r+1}, & \text{if } l \equiv u \pmod 2 \text{ and } m \equiv u + s + 1 \pmod 2, \\ (-1)^{r+1}, & \text{if } l \equiv u + 1 \pmod 2 \text{ and } m \equiv u + s \pmod 2, \\ (-1)^r, & \text{if } l \equiv u + 1 \pmod 2 \text{ and } m \equiv u + s + 1 \pmod 2. \end{cases}$$

In the case $w = 0$, *then*

$$\mu = \begin{cases} 3(-1)^r, & \text{if } l \equiv u \pmod 2 \text{ and } m \equiv u + s \pmod 2, \\ (-1)^{r+1}, & \text{otherwise.} \end{cases}$$

Proof. Since, $|(D_i^{(p^e)} + \tau) \cap D_j^{(p^e)}| = p^{e-1} |(D_i^{(p)} + \tau_p) \cap D_j^{(p)}|$, we get by definition,

$$\begin{aligned} |(D_l^{(a,n)} + \tau) \cap D_m^{(a,n)}| &= \sum_{(i_1, \ldots, i_t) \in I_l^{(a,n)}} \sum_{(j_1, \ldots, j_t) \in I_m^{(a,n)}} \prod_{k=1}^{t} |(D_{i_k}^{(p_k^{e_k})} + \tau) \cap D_{j_k}^{(p_k^{e_k})}| \\ &= \frac{n}{\prod_{p|n} p} \sum_{(i_1, \ldots, i_t) \in I_l^{(a,n)}} \sum_{(j_1, \ldots, j_t) \in I_m^{(a,n)}} \prod_{k=1}^{t} |(D_{i_k}^{(p_k)} + \tau_k) \cap D_{j_k}^{(p_k)}|. \end{aligned}$$

For the prime divisors p_k with $a_{p_k} = 0$, we obtain a contribution

$$\sum_{i_k, j_k \in \{0,1\}} |(D_{i_k}^{(p_k)} + \tau_k) \cap D_{j_k}^{(p_k)}| = |(Z_{p_k}^* + \tau_k) \cap Z_{p_k}^*| = p_k - 2 + \delta_{\tau_{p_k}, 0}.$$

Further,

$$|(D_{i_k}^{(p_k)} + \tau_k) \cap D_{j_k}^{(p_k)}| = \begin{cases} 0, & \text{if } \tau_k = 0,\ i_k \neq j_k, \\ (p_k - 1)/2, & \text{if } \tau_k = 0,\ i_k = j_k, \\ (i_k + u_k, j_k + u_k)^{(p_k)}, & \text{if } \tau_k \in D_{u_k}^{(p_k)}. \end{cases}$$

Assume that $p_1, p_2, \ldots, p_v$ are all the prime divisors of n corresponding to $a_i = 1$ and $\tau_i \neq 0$. Then by the assumption of this theorem, $v = r + s$. Further we assume that $p_{v+1}, \ldots, p_{v+w}$ are all the prime divisors of n corresponding to $a_i = 1$ and $\tau_i = 0$. Then the rest of the prime divisors of n correspond to $a_i = 0$.

Case I. $w \geq 1$.

Let H denote the set of all solutions $(i_1, \ldots, i_{v+w}, j_1, \ldots, j_{v+w}) \in (Z_2)^{2(v+w)}$ of the following set of equations

$$\begin{aligned} &i_1 + \cdots + i_v + i_{v+1} + \cdots + i_{v+w} = l, \\ &j_1 + \cdots + j_v + j_{v+1} + \cdots + j_{v+w} = m, \\ &i_{v+1} = j_{v+1}, \\ &\vdots \\ &i_{v+w} = j_{v+w}. \end{aligned}$$

For each $a \in \{0, 1\}$, let H_a denote the set of solutions $(i_1, \ldots, i_{v+w}, j_1, \ldots, j_{v+w}) \in (Z_2)^{2(v+w)}$ of the following set of equations

$$\begin{aligned} &i_1 + \cdots + i_v = l - a, \\ &j_1 + \cdots + j_v = m - a, \\ &i_{v+1} + \cdots + i_{v+w} = a, \\ &i_{v+1} = j_{v+1}, \\ &\vdots \\ &i_{v+w} = j_{v+w}. \end{aligned}$$

Then it is straightforward to see that

$$H = H_0 \cup H_1.$$

Note that the contributing terms, where $\tau_k = 0$, have $i_k = j_k = 0$ and $i_k = j_k = 1$. Hence

$$|(D_l^{(a,n)} + \tau) \cap D_m^{(a,n)}| = \frac{n}{\prod_{p|n} p} \prod_{p|n,\, a_p = 0} (p - 2 + \delta_{\tau_p, 0}) \times V,$$

where

$$V = \sum_{i_1 + \cdots + i_{v+w} = l} \sum_{j_1 + \cdots + j_{v+w} = m} \prod_{k=1}^{v+w} |(D_{i_k}^{(p_k)} + \tau_k) \cap D_{j_k}^{(p_k)}|.$$

Since $H = H_0 \cup H_1$, we have

$$\begin{aligned} V &= \sum_{a=0}^{1} \sum_{i_1 + \cdots + i_v = l-a} \sum_{j_1 + \cdots + j_v = m-a} \left(\prod_{k=1}^{v} |(D_{i_k}^{(p_k)} + \tau_k) \cap D_{j_k}^{(p_k)}| \right) \\ &\quad \times \left(\sum_{i_{v+1} + \cdots + i_{v+w} = a} \prod_{k=v+1}^{v+w} |D_{i_k}^{(p_k)}| \right) \\ &= \frac{1}{2} \prod_{i=v+1}^{v+w} (p_i - 1) \sum_{a=0}^{1} \sum_{i_1 + \cdots + i_v = l-a} \sum_{j_1 + \cdots + j_v = m-a} \left(\prod_{k=1}^{v} |(D_{i_k}^{(p_k)} + \tau_k) \cap D_{j_k}^{(p_k)}| \right) \\ &= \frac{1}{2} \prod_{i=v+1}^{v+w} (p_i - 1)(U_0 + U_1), \end{aligned}$$

where

$$U_a = \sum_{i_1 + \cdots + i_v = l-a} \sum_{j_1 + \cdots + j_v = m-a} \prod_{k=1}^{v} (i_k + u_k, j_k + u_k)^{(p_k)}.$$

With the same technique used to calculate the T of (11), we get

$$U_a = \frac{1}{4} \left[\prod_{p|n,\, a_p = 1,\, \tau_p \neq 0} (p - 2) + \delta_a \right],$$

where

$$\delta_a = \begin{cases} 3(-1)^r, & \text{if } \ l \equiv u + a \pmod 2 \ \text{ and } \ m \equiv u + s + a \pmod 2, \\ (-1)^{r+1}, & \text{otherwise.} \end{cases}$$

Therefore

$$U_0 + U_1 = \frac{1}{2} \prod_{p|n, a_p = 1, \tau_p \neq 0} (p-2) + \frac{\delta_0 + \delta_1}{4}$$
$$= \frac{1}{2} \prod_{p|n, a_p = 1, \tau_p \neq 0} (p-2) + \frac{\mu}{2},$$

where μ is defined before in this theorem. Combining the above results proves the first case.

Case II. $w = 0$.

In this case, we have

$$V = \sum_{i_1 + \cdots + i_v = l} \sum_{j_1 + \cdots + j_v = m} \prod_{k=1}^{v} |(D_{i_k}^{(p_k)} + \tau_k) \cap D_{j_k}^{(p_k)}|$$
$$= \sum_{i_1 + \cdots + i_v = l} \sum_{j_1 + \cdots + j_v = m} \prod_{k=1}^{v} (i_k + u_k, j_k + u_k)^{(p_k)}$$
$$= U_0,$$

where U_0 is calculated before. Combining this with the above results proves the second case. ■

Once the nonzero vector $a = (a_1, a_2, \ldots, a_t)$ is chosen, the generalized cyclotomy and the two sets $I_0^{(a,n)}$ and $I_1^{(a,n)}$ are determined, so the formulae for the cyclotomic numbers $(l, m)^{(a,n)}$ are clear.

It should be noted that the constructive approach used to introduce the new generalized cyclotomy of Section 2 has the restriction (1), while the approach of this section does not have such a restriction. This shows the advantage of this general approach.

These generalized cyclotomies and cyclotomic numbers introduced in this section have similar applications in coding theory, cryptography, and sequences as the new cyclotomy introduced before.

ACKNOWLEDGMENT

The authors are grateful to the two anonymous referees for their valuable and constructive comments and suggestions that much improved this paper. In fact the more new generalized cyclotomies described in Section 6 were suggested by one of the referees.

REFERENCES

1. T. M. Apostol, "Introduction to Analytic Number Theory," Springer-Verlag, New York, 1976.

2. E. F. Assmus, Jr., H. F. Mattson, Jr., and W. E. Sachar, A new form of the square root bound, *SIAM J. Appl. Math.* **30** (1976), 352–354.
3. L. D. Baumert, "Cyclic Difference Sets," Lecture Notes in Mathematics, Vol. 182, Springer-Verlag, New York, 1971.
4. A. M. Boehmer, Binary pulse compression codes, *IEEE Trans. Inform. Theory* **IT-13** (1967), 156–166.
5. N. B. Chakrabarti and M. Tomlinson, Design of sequences with specified autocorrelation and cross correlation, *IEEE Trans. Commun.* (November 1976), 1246–1252.
6. L. E. Dickson, Cyclotomy, higher congruences, and Waring's problem, *Amer. J. Math.* **57** (1935), 391–424, 463–474.
7. C. Ding, Binary cyclotomic generators, *in* "Fast Software Encryption" (B. Preneel, Ed.), LNCS **1008** (1995), 29–60.
8. C. Ding, D. Pei, and A. Salomaa, "Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography," World Scientific, Singapore, 1996, Chapters 2 and 6.
9. C. F. Gauss, "Disquisitiones Arithmeticae," 1801. English translation, Yale, New Haven, 1966. (Reprinted by Springer-Verlag, Berlin/Heidelberg/New York, 1986).
10. E. R. Hauge and T. Helleseth, DeBruijn sequences, irreducible codes and cyclotomy, *Discrete Math.* **159** (1996), 143–154.
11. T. Helleseth and P. V. Kumar, Sequences with low correlation, to appear in "Handbook of Coding Theory" (V. Pless, W. C. Huffman, and R. A. Brualdi, Eds.), Elsevier, Amsterdam, 1998, to appear.
12. J. S. Leon, J. M. Masley, and V. Pless, Duadic codes, *IEEE Trans. Inform. Theory* **IT-30** (1984), 709–714.
13. F. J. MacWilliams, Cyclotomic numbers, coding theory and orthogonal polynomials, *Discrete Math.* **3** (1972), 133–151.
14. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1978.
15. R. J. McEliece and H. Rumsey, Jr., Euler products, cyclotomy, and coding, *J. Number Theory* **4** (1972), 302–311.
16. T. Storer, "Cyclotomy and Difference Sets," Markham, Chicago, 1967.
17. A. L. Whiteman, A family of difference sets, *Illinois J. Math.* **6** (1962), 107–121.