IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 24, 2020, accepted December 7, 2020, date of publication December 17, 2020, date of current version January 5, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3045611

Frequency-Hopping Sequences With Optimal Average Hamming Correlation and Their Applications in Energy and Spectrum Harvesting Technologies Area

MINGYUE FAN
School of Information Engineering, China Jiliang University, Hangzhou 310018, China
e-mail: mingyue_fan@163.com

ABSTRACT The research of cyclotomy theory can be traced to Gauss and it has been applied to many fields such as cryptography, coding theory, and combinatorics. According to v prime numbers or compound words, the incision on the residue-like ring $\mathbb{Z}_v$ can be separated to classic incision or general incision. In this work, a kind of extended generalized cyclotomic classes is introduced. Based on this tangent method, a class of frequency hopping sequence set with the best average Hamming correlation is proposed.

INDEX TERMS Frequency-hopping, hamming correlation, generalized cyclotomy, energy and spectrum harvesting technologies.

I. INTRODUCTION

Suppose $\mathbb{Z}_v$ is an integer ring modulo v. Let $\mathbb{Z}_v^*$ be all reversible elements of $\mathbb{Z}_v$. $\{D_0, D_1, \ldots, D_{d-1}\}$ is a partition of $\mathbb{Z}_v^*$, which is a family set with

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

Suppose that $\mathbb{Z}_v^*$ has a multiplicative sub-group D_0, and $h_1, \ldots, h_{d-1}$ is the elements of $\mathbb{Z}_v^*$ so that for all i, $D_i = h_i D_0$ and the cosets D_i can be called as *generalized cyclotomic classes* when v is composite, and *classical cyclotomic classes* when v is prime. For all $0 \leq i, j \leq d-1$, the (generalized) ring number of d is set as $(i, j) = |(D_i + 1) \cap D_j|$. There may be many multiplication subgroups D_0 for index d in $\mathbb{Z}_v^*$. There will be give different numbers of generalized incision and circumcision with Different subgroups D_0.

In the book "*Disquisitiones Arithmeticae*" [2]–[4], [12], Gauss first presented the detailed classical secant technique. The so-called *cyclotomic numbers* and *Gaussian periods* were also introduced, and they are associated with some loop codes [10].

In order to find the residual set, Whiteman presented the generalized segmentation method of order d in [21] on $p_1 p_2$, where p_1, p_2 satisfy the rule of $\gcd(p_1 - 1, p_2 - 1) = d$. After that, it has been applied to several research fields, such as cyclic codes, sequence construction, and codebooks. Ding [10] introduced *extended generalized cyclotomic classes of order two* by extending the concept of generalized circumsection of Whiteman, and studied their basic characteristics. Facts have proved that the extended generalized cyclic tangent method in [10] can be used to generate cyclic codes with good parameters.

The first objective of this work is to study an approach of extended generalized cyclotomic classes of order n and their basic properties and their cyclotomic numbers. This generalizes the study of order two' cyclotomic classes. Another objective is using order n's extended generalized cyclotomic classes to obtain highly Hamming correlational frequency-hopping sequence sets.

The following symbols can conclude the first section and the remained content will use these notations.

- p and q are two distinct odd primes.
- $P = \{p, 2p, \ldots, (q-1)p\}$, $Q = \{q, 2q, \ldots, (p-1)q\}$, $R = \{0\}$.
- $\mathbb{Z}_{pq}^*$ is the $\mathbb{Z}_{pq}$'s invertible elements.
- $d = \gcd(p-1, q-1)$, $e = \frac{(p-1)(q-1)}{d}$ and $\kappa = \frac{(p-1)(q-1)}{d^2}$.
- positive integer n satisfies $n|d$.

II. GENERALIZED CYCLOTOMY

In the following, the properties of order d's generalized generalized segmentation of Whiteman is introduced, and we will utilize them next sections.

The associate editor coordinating the review of this manuscript and approving it for publication was Guangjie Han.

When the multiplicative order of an integer a modulo v equals $\phi(v)$ ($\phi(v)$ is Euler function and $\gcd(a, v) = 1$), a can be named a *primitive root* modulo v.

According to the Chinese Remainder Theorem, since p and q are relative prime numbers, there is a universal primitive root g. Then the integer x should satisfy

$$x \equiv g \pmod{p}, \quad x \equiv 1 \pmod{q}.$$

Whiteman proved that [21]

$$\mathbb{Z}_{pq}^* = \left\{ g^s x^i : s = 0, 1, \ldots, e-1, i = 0, 1, \ldots, d-1 \right\}.$$

The order d's *generalized cyclotomic classes* can be denoted as

$$D_i = \left\{ g^s x^i : s = 0, 1, \ldots, e-1 \right\}, \; i = 0, 1, \ldots, d-1$$

and the *generalized cyclotomic numbers* $(i, j)_d$ are denoted as

$$(i, j)_d = |(D_i + 1) \cap D_j|, \; 0 \le i, j \le d-1.$$

Lemmas shown as follows summarizes many properties of order d's generalized ring number of Whiteman [21].

Lemma 1: Let the notations be used as afore-mentioned. Then

(1) $\mathbb{Z}_{pq}^* \cup P \cup Q \cup R = \mathbb{Z}_{pq}$.

(2) $\mathbb{Z}_{pq}^* = \bigcup_{i=0}^{d-1} D_i$, $D_i \cap D_j = \emptyset$ *for* $i \neq j$.

(3) The order of g *modulo* pq *is* e.

(4) D_0 *is a subgroup of* $\mathbb{Z}_{pq}^*$.

(5) The order of x *modulo* pq *is* $p-1$.

(6) $x^d = g^u$ *for some* u *with* $0 \le u \le e-1$.

(7) If $a \in D_j$, $aD_i = D_{(i+j) \pmod{d}}$.

(8) $-1 = \begin{cases} g^{\frac{e}{2}} \pmod{v}, & \text{if } \kappa \text{ is odd} \\ g^{\mu} x^{\frac{d}{2}} \pmod{v}, & \text{if } \kappa \text{ is even} \end{cases}$, *for some* μ *with* $0 \le \mu \le e-1$.

Lemma 2: Let the notations be used as afore-mentioned. Then

(A0) $(i, j)_d = (i', j')_d$, *when* $i \equiv i' \pmod{d}$ *and* $j \equiv j' \pmod{d}$.

(A1) $(i, j)_d = (d-i, j-i)_d = \begin{cases} (j, i)_d, & \text{if } \kappa \text{ is odd,} \\ (j+\frac{d}{2}, i+\frac{d}{2})_d, & \text{if } \kappa \text{ is even.} \end{cases}$

(A2) $\sum_{j=0}^{d-1} (i, j)_d = \frac{(p-2)(q-2)-1}{d} + \delta_i$, *where*

$$\delta_i = \begin{cases} 1, & \text{if } i \equiv 0 \pmod{d} \text{ and } \kappa \text{ is odd,} \\ 1, & \text{if } i \equiv \dfrac{d}{2} \pmod{d} \text{ and } \kappa \text{ is even,} \\ 0, & \text{otherwise.} \end{cases}$$

(A3) $\sum_{i=0}^{d-1} (i, j)_d = \frac{(p-2)(q-2)-1}{d} + \epsilon_j$, *where*

$$\epsilon_j = \begin{cases} 1, & \text{if } j \equiv 0 \pmod{d}, \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 3: Let the notations be used as afore-mentioned. Then for any $\omega \in \mathbb{Z}_{pq}$,

$$|(D_i + \omega) \cap D_j| = \begin{cases} \dfrac{(p-1)(q-1)}{d^2}, & i \neq j, \; \omega \in P \cup Q, \\ \dfrac{(p-1)(q-1-d)}{d^2}, & i = j, \; \omega \in P, \omega \notin Q, \\ \dfrac{(p-1-d)(q-1)}{d^2}, & i = j, \; \omega \notin P, \omega \in Q, \\ (i-k, j-k)_d, & \omega \in D_k \; (0 \le k \le d-1). \end{cases}$$

$$|(D_i + \omega) \cap (Q \cup R)| = \begin{cases} 0, & \omega \in Q \cup R, \\ \dfrac{p-1}{d}, & \omega \in P \cup \mathbb{Z}_{pq}^*. \end{cases}$$

$$|(D_i + \omega) \cap (P \cup R)| = \begin{cases} 0, & \omega \in P \cup R, \\ \dfrac{q-1}{d}, & \omega \in Q \cup \mathbb{Z}_{pq}^*. \end{cases}$$

III. EXTENDED GENERALIZED CYCLOTOMY

In [10], Ding introduced the *order two's extended generalized cyclotomic classes*:

$$C_0^{(2)} = \bigcup_{i=0}^{(d-2)/2} D_{2i}, \; C_1^{(2)} = \bigcup_{i=0}^{(d-2)/2} D_{2i+1},$$

which is different from Whiteman's generalized cyclotomic classes if $d > 2$. We will generalize this concept, and define *order n's extended generalized cyclotomic classes* and *order n's extended cyclotomic numbers* as follows:

$$A_i^{(n)} = \bigcup_{s=0}^{\frac{d}{n}-1} D_{sn+i}, \quad 0 \le i \le n-1,$$

$$(i, j)_n = |(A_i^{(n)} + 1) \cap A_j^{(n)}|, \; 0 \le i, j \le n-1.$$

Remark 4: For the extended generalized cyclotomy defined above, we have the following comments.

(1) When $n = d$, the extended generalized cyclotomy is identical to the generalized cyclotomy of Whiteman.

(2) When $n = 2$, the extended generalized cyclotomy is indeed the cyclotomy introduced by Ding [10].

We summarize some properties of order n's extended cyclotomy in the following lemmas.

Lemma 5: Let the notations be used as afore-mentioned. Then

(1) $\mathbb{Z}_{pq}^* = \bigcup_{i=0}^{n-1} A_i^{(n)}$, $A_i^{(n)} \cap A_j^{(n)} = \emptyset$ *for* $i \neq j$.

(2) $A_0^{(n)}$ *is a subgroup of order* $\frac{(p-1)(q-1)}{n}$ *of* $\mathbb{Z}_{pq}^*$.

(3) If $a \in A_j^{(n)}$, $aA_i^{(n)} = A_{(i+j) \pmod{n}}^{(n)}$.

(4) $-1 \in \begin{cases} A_0^{(n)}, & \text{if } \kappa \text{ is odd,} \\ A_0^{(n)}, & \text{if } \kappa \text{ is even and } \frac{d}{n} \text{ is even,} \\ A_{\frac{n}{2}}^{(n)}, & \text{if } \kappa \text{ is even and } \frac{d}{n} \text{ is odd.} \end{cases}$

Proof: The properties can be easily obtained by Lemma 1. We omit the details here. □

Lemma 6: Let the notations be the same as before. Then

(B0) $(j, i)_n = (j', i')_n$, *where* $j \equiv j' \pmod{n}$ *and* $i \equiv i' \pmod{n}$.

(B1) $(j, i)_n = (n-j, i-j)_n$.

(B2) $$(j, i)_n = \begin{cases} (i, j)_n, & \text{if } \kappa \text{ is odd,} \\ (i, j)_n, & \text{if } \kappa \text{ is even and } \frac{d}{n} \text{ is even,} \\ (i+\frac{n}{2}, j+\frac{n}{2})_n, & \text{if } \kappa \text{ is even and } \frac{d}{n} \text{ is odd.} \end{cases}$$

(B3) $\sum_{j=0}^{n-1}(i, j)_n = \frac{(p-2)(q-2)-1}{n} + \overline{\delta}_i$, *where*

$$\overline{\delta}_i = \begin{cases} 1, & \text{if } i \equiv 0 \pmod{n} \text{ and } \kappa \text{ is odd,} \\ 1, & \text{if } i \equiv 0 \pmod{n}, \kappa \text{ is even and } \dfrac{d}{n} \text{ is even,} \\ 1, & \text{if } i \equiv \dfrac{n}{2} \pmod{n}, \kappa \text{ is even and } \dfrac{d}{n} \text{ is odd,} \\ 0, & \text{otherwise.} \end{cases}$$

(B4) $\sum_{i=0}^{n-1}(i, j)_n = \frac{(p-2)(q-2)-1}{n} + \overline{\epsilon}_j$, *where*

$$\overline{\epsilon}_j = \begin{cases} 1, & \text{if } j \equiv 0 \pmod{n}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof: It can be seen that Property (B0) is obvious. Property (B1) will be first proved. We can learn from Lemma 2's Property (A1):

$$\begin{aligned} (i, j)_n &= \sum_{s',t'=0}^{\frac{d}{n}-1} |(D_{s'n+i}+1) \cap D_{t'n+j}| && (1) \\ &= \sum_{s',t'=0}^{\frac{d}{n}-1} (s'n+i, t'n+j)_d && (2) \\ &= \sum_{s',t'=0}^{\frac{d}{n}-1} ((\frac{d}{n}-s')n-i, (t'-s')n+j-i)_d && (3) \\ &= \sum_{s,t=0}^{\frac{d}{n}-1} (sn-i, tn+j-i)_d && (4) \\ &= (n-i, j-i)_n. && (5) \end{aligned}$$

Then Property (B2) is easily proved by $(i, j)_n = |((-1)A_j^{(n)}+1) \cap (-1)A_i^{(n)}|$ and Lemma 5 (3), (4).

Property (B3) will be then proved. It follows from Property (A2) in Lemma 2 that

$$\begin{aligned} \sum_{j=0}^{n-1}(i, j)_n &= \sum_{j=0}^{n-1}\sum_{s,t=0}^{\frac{d}{n}-1} |(D_{sn+i}+1) \cap D_{tn+j}| \\ &= \sum_{s=0}^{\frac{d}{n}-1}\left(\sum_{t=0}^{\frac{d}{n}-1}\sum_{j=0}^{n-1}(sn+i, tn+j)_d\right) \\ &= \sum_{s=0}^{\frac{d}{n}-1}\sum_{j'=0}^{d-1}(sn+i, j')_d \\ &= \sum_{s=0}^{\frac{d}{n}-1}\left(\frac{(p-2)(q-2)-1}{d} + \delta_{sn+i}\right) \\ &= \frac{(p-2)(q-2)-1}{n} + \overline{\delta}_i. \end{aligned}$$

We can prove Property (B4) in similar. The detailed process is omitted here. □

Lemma 7: For any $0 \leq i, j \leq n-1$ *and* $\omega \neq 0$,

$$|(A_i^{(n)}+\omega) \cap A_j^{(n)}| = \begin{cases} (i-k, j-k)_n, & \omega \in A_k^{(n)}, \\ \dfrac{(p-1)(q-1)}{n^2}, & i \neq j, \ \omega \in P \cup Q, \\ \dfrac{(p-1)(q-1-n)}{n^2}, & i = j, \ \omega \in P, \omega \notin Q, \\ \dfrac{(p-1-n)(q-1)}{n^2}, & i = j, \ \omega \notin P, \omega \in Q. \end{cases}$$

Proof: (1) The first equality is easily proved by Lemma 5 (3).

(2) When $\omega \in P \cup Q$ and $i \neq j$, $A_i^{(n)} \cap A_j^{(n)} = \emptyset$. Then by Lemma 3,

$$\begin{aligned} |(A_i^{(n)}+\omega) \cap A_j^{(n)}| &= \sum_{s,t=0}^{\frac{d}{n}-1} |(D_{sn+i}+\omega) \cap D_{tn+j}| \\ &= \sum_{s,t=0}^{\frac{d}{n}-1} \frac{(p-1)(q-1)}{d^2} = \frac{(p-1)(q-1)}{n^2}. \end{aligned}$$

(3) When $\omega \in P, \ \omega \notin Q$ and $i = j$, by Lemma 3,

$$\begin{aligned} |(A_i^{(n)}+\omega) \cap A_i^{(n)}| &= \sum_{s,t=0}^{\frac{d}{n}-1} |(D_{sn+i}+\omega) \cap D_{tn+i}| \\ &= \sum_{s=0}^{\frac{d}{n}-1} |(D_{sn+i}+\omega) \cap D_{sn+i}| \\ &\quad + \sum_{\substack{s,t=0 \\ s \neq t}}^{\frac{d}{n}-1} |(D_{sn+i}+\omega) \cap D_{tn+i}| \\ &= \frac{(p-1)(q-1-d)}{dn} \\ &\quad + \frac{(d-n)(p-1)(q-1)}{dn^2} \\ &= \frac{(p-1)(q-1-n)}{n^2}. \end{aligned}$$

(4) When $\omega \notin P, \ \omega \in Q$ and $i = j$, the result is similarly proved. We omit the details here. □

Lemma 8: For i in $[0, n-1]$, $j \neq 0$ *and* $\omega \neq 0$,

$$\sum_{i=0}^{n-1} |(A_i^{(n)}+\omega) \cap A_i^{(n)}| = \begin{cases} \dfrac{(p-1)(q-1-n)}{n}, & \omega \in P, \\ \dfrac{(p-1-n)(q-1)}{n}, & \omega \in Q, \\ \dfrac{(p-2)(q-2)-1}{n}+1, & \omega \in Z_{pq}^{*}. \end{cases}$$

$$\sum_{i=0}^{n-1}|(A_{i+j}^{(n)}+\omega)\cap A_i^{(n)}|=\begin{cases}\frac{(p-1)(q-1)}{n}, & \omega\in P\cup Q,\\ \frac{(p-2)(q-2)-1}{n}, & \omega\in Z_{pq}^{*}.\end{cases}$$

Proof: The results can be obtained by Lemma 6 (B1), (B4) and Lemma 7. We only proved the last equality here, and leave the rest to the readers.

For $\omega\in A_k^{(n)}$ $(0\le k\le n-1)$, we have

$$\begin{aligned}&\sum_{i=0}^{n-1}|(A_{i+j}^{(n)}+\omega)\cap A_i^{(n)}|\\ &\quad=\sum_{i=0}^{n-1}(i+j-k,\,i-k)_n=\sum_{i=0}^{n-1}(k-i-j,\,n-j)_n\\ &\quad=\sum_{i'=0}^{n-1}(i',\,n-j)_n=\frac{(p-2)(q-2)-1}{n}.\end{aligned}$$

The last equality comes true since $n-j\not\equiv 0\pmod{n}$. □

Lemma 9: For i in $[0,n-1]$ *and* $\omega\in\mathbb{Z}_{pq}$,

$$|(A_i^{(n)}+\omega)\cap(Q\cup R)|=\begin{cases}0, & \omega\in Q\cup R,\\ \frac{p-1}{n}, & \omega\in P\cup Z_{pq}^{*}.\end{cases}$$

$$|(A_i^{(n)}+\omega)\cap(P\cup R)|=\begin{cases}0, & \omega\in P\cup R,\\ \frac{q-1}{n}, & \omega\in Q\cup Z_{pq}^{*}.\end{cases}$$

$$|A_i^{(n)}\cap(P+\omega)|=\begin{cases}0, & \omega\in P,\\ \frac{q-1}{n}-1, & \omega\in A_i^{(n)}.\\ \frac{q-1}{n}, & \omega\in Q\cup Z_{pq}^{*}\setminus A_i^{(n)}.\end{cases}$$

$$|A_i^{(n)}\cap(P\cup Q\cup R+\omega)|=\begin{cases}\frac{p-1}{n}, & \omega\in P,\\ \frac{q-1}{n}, & \omega\in Q,\\ \frac{p-1}{n}+\frac{q-1}{n}-1, & \omega\in A_i^{(n)}.\\ \frac{p-1}{n}+\frac{q-1}{n}, & \omega\in Z_{pq}^{*}\setminus A_i^{(n)}.\end{cases}$$

$$|(P\cup Q\cup R+\omega)\cap(P\cup Q\cup R)|=\begin{cases}q, & \omega\in P,\\ p, & \omega\in Q.\\ 2, & \omega\in Z_{pq}^{*}.\end{cases}$$

Proof: The results are easily obtained by Lemma 3. We only notice the last equality is proved by the following trivial facts:

$$|(P+\omega)\cap Q|=\begin{cases}0, & \omega\in P\cup Q\cup R,\\ 1, & \omega\in Z_{pq}^{*}.\end{cases}$$

$$|(P+\omega)\cap P|=\begin{cases}0, & \omega\in Q\cup Z_{pq}^{*},\\ q-2, & \omega\in P.\end{cases}$$

$$|(Q+\omega)\cap Q|=\begin{cases}0, & \omega\in P\cup Z_{pq}^{*},\\ p-2, & \omega\in Q.\end{cases}$$

Thus, we get all the conclusions. □

IV. AN APPLICATION OF EXTENDED CYCLOTOMY IN FHS DESIGN

Frequency-hopping sequence (FHS) has been broadly utilized in nowadays communication systems, such as ultra-wide bandwidth radios, blue tooth, and wearable sense network [11], [20]. The using of FHS sets with lower Hamming correlation and larger sets is very important in these systems. In the FHS spectrum (FHSS) communication systems, average error performance was evaluated by the average Hamming correlation (AHC), and the worst-case performance is represented by the maximum Hamming correlation (MHC). We only discuss the sets of FHS with the best AHC in the article. For the construction of the sets of FHS with the best MHC in terms of Peng-Fan bound [17], readers can refer to [1], [5]–[7], [9], [13], [14], [16] and its references.

We can denote a available frequencies set as $\mathcal{F}=\{f_0,f_1,\ldots,f_{\ell-1}\}$. The array $X=(x_0,x_1,\ldots,x_{L-1})$ is defined as an L-length FHS over $\mathcal{F}$ when $x_t\in\mathcal{F}$ for $t\in[0,L-1]$. For L-length FHSs Y and X over $\mathcal{F}$, the *periodic Hamming correlation* between Y and X can be written as

$$H_{Y,X}(\tau)=\sum_{k=0}^{L-1}h[y_k,x_{k+\tau}],\ 0\le\tau<L,$$

where $h[y,x]=0$ when $y\neq x$, and 1 when $y=x$. If $Y=X$, $H_{Y,X}(\tau)$ is Y's *Hamming autocorrelation*, and is defined as $H_Y(\tau)$.

Let $\mathcal{U}$ be a set of M L-length FHSs over $\mathcal{F}$ with $|\mathcal{F}|=\ell$. Define

$$S_a(\mathcal{U})=\sum_{X\in\mathcal{U},1\le\tau<L}H_X(\tau),$$

$$S_c(\mathcal{U})=\frac{1}{2}\sum_{X,Y\in\mathcal{U},X\neq Y,0\le\tau<L}H_{X,Y}(\tau).$$

The *average Hamming autocorrelation and crosscorrelation* of $\mathcal{U}$ are defined by

$$A_a(\mathcal{U})=\frac{S_a(\mathcal{U})}{M(L-1)},$$

$$A_c(\mathcal{U})=\frac{2S_c(\mathcal{U})}{LM(M-1)},$$

respectively [19]. A bound on an FHS set's AHCs is created in lemma [19] as follows.

Lemma 10: For an L-length and M-size FHS set $\mathcal{U}$ over $\mathcal{F}$ with $|\mathcal{F}|=\ell$, the average Hamming auto-correlation and cross-correlation of $\mathcal{U}$ can be denoted as $A_a(\mathcal{U})$and $A_c(\mathcal{U})$. Then,

$$\frac{A_a(\mathcal{U})}{L(M-1)}+\frac{A_c(\mathcal{U})}{L-1}\ge\frac{LM-\ell}{\ell(L-1)(M-1)}.\qquad(6)$$

When the pair $(A_a(\mathcal{U}),A_c(\mathcal{U}))$ keeps (6) with equality, the set $\mathcal{U}$ of an FHS is considered having *optimal* AHC.

After the AHC's concept was introduced [19], we have known several constructions of FHS with the best AHC. The boundary in the above lemma was first proposed by Peng, Niu and Tang [19], and some FHS sets based on cubic polynomials with the best AHC were also proposed. According to the power residual theory, they [19] construct a type of FHS set, which are the best for AHC and MHC binding [18]. Chung and Yang analyzed some FHS sets' AHC known to have the best MHC, and showed that the best MHC cannot ensure the best AHC. The segmentation method [8] constructed the best AHC and was close to the best MHC New FHS set. Through utilizing the theory of generalized circumcision of Whiteman [21], the FHS set with the best AHC was also constructed [15].

In what follows, we shall construct a class of FHS sets with best AHC property based upon the extended generalized cyclotomy defined in the above section.

We follow the notations in sections above. Define

$$\begin{aligned} E_0 &= A_0^{(n)} \cup P \cup Q \cup R, \\ E_i &= A_i^{(n)},\ 1 \le i \le n-1. \end{aligned}$$

Then $\sum_{i=0}^{n-1} E_i = \mathbb{Z}_{pq}$ and $E_i \cap E_j = \emptyset$ for $i \ne j$.

Let $X = (x_0, x_1, \ldots, x_{L-1})$ be an L-length sequence over a frequency set $\mathcal{F}$. Then $supp_X(k) = \{t | x_t = k,\ t = 0, 1, \ldots, L-1\}$ is called as $k \in \mathcal{F}$'s support.

Theorem 11: Let

$$supp_{X^{(i)}}(j) = E_{j+i},\ 0 \le j \le n-1,$$

where $j+i$ is reduced modulo n, then $\mathcal{X} = \{X^{(i)} : i = 0, 1, \ldots, n-1\}$ is a family of n sequences with length pq, and alphabet size n which is best in terms of the bound of AHC in (6).

Proof: The length, family size, and alphabet size of $\mathcal{X}$ follows directly from its definition. We now prove that it has optimal average Hamming correlation. We only consider the condition that n is odd, since the condition that n is even is similar. By Lemmas 8 and 9, for any $0 \le k, l \le n-1$ and $k \ne l$, we have

$$H_{X^{(k)}}(\omega) = \begin{cases} \frac{p+pq-q-1}{n}+q-p+1, & \omega \in P, \\ \frac{q+pq-p-1}{n}+p-q+1, & \omega \in Q, \\ \frac{pq-1}{n}+1, & \omega \in A_0^{(n)}. \\ \frac{pq-1}{n}+3, & \omega \in A_i^{(n)} \text{ for } i \ne 0, \end{cases}$$

$$H_{X^{(k)},X^{(l)}}(\omega) = \begin{cases} 0, & \omega = 0, \\ \frac{p+pq-q-1}{n}, & \omega \in P, \\ \frac{q+pq-p-1}{n}, & \omega \in Q, \\ \frac{pq-1}{n}-1, & \omega \in A_{k-l}^{(n)} \cup A_{l-k}^{(n)}, \\ \frac{pq-1}{n}, & \omega \in A_i^{(n)} \text{ for } i \ne k-l, l-k. \end{cases}$$

Therefore, according to the definition of S_a and S_c, we have

$$\begin{aligned} S_a &= \sum_{k=0}^{n-1}\sum_{\omega=1}^{L-1} H_{X^{(k)}}(\omega) \\ &= n\Bigg\{(q-1)\left(\frac{pq-1}{n}+\frac{p-q}{n}+q-p+1\right) \\ &\quad +(p-1)\left(\frac{q+pq-p-1}{n}+p-q+1\right) \\ &\quad +\frac{(p-1)(q-1)}{n}\left(\frac{pq-1}{n}+1\right) \\ &\quad +(n-1)\frac{(p-1)(q-1)}{n}\left(\frac{pq-1}{n}+3\right)\Bigg\} \\ &= (pq-1)^2+(n-1)(q-1)^2+(n-1)(p-1)^2+n(pq-1). \end{aligned}$$

$$\begin{aligned} 2S_c &= \sum_{0 \le k \ne l \le n-1}\ \sum_{\omega=0}^{L-1} H_{X^{(k)},X^{(l)}}(\omega) \\ &= (n-1)[(pq-1)^2-(p-1)^2-(q-1)^2]. \end{aligned}$$

It then follows that the average Hamming auto-correlation and average Hamming cross-correlation of the FHS set $\mathcal{X}$ are respectively in the following:

$$A_a(\mathcal{X}) = \frac{(pq-1)^2+(n-1)(q-1)^2+(n-1)(p-1)^2+n(pq-1)}{n(pq-1)}$$

$$A_c(\mathcal{X}) = \frac{2S_c(\mathcal{X})}{LM(M-1)} = \frac{(pq-1)^2-(p-1)^2-(q-1)^2}{pqn}.$$

Note that

$$\begin{aligned} &\frac{A_a}{L(M-1)}+\frac{A_c}{L-1} \\ &= \frac{(pq-1)^2+(n-1)(q-1)^2+(n-1)(p-1)^2+n(pq-1)}{n(n-1)pq(pq-1)} \\ &\quad +\frac{(pq-1)^2-(p-1)^2-(q-1)^2}{pqn(pq-1)} \\ &= \frac{1}{n-1}. \end{aligned}$$

and

$$\frac{LM-\ell}{\ell(L-1)(M-1)} = \frac{pqn-n}{n(pq-1)(n-1)} = \frac{1}{n-1}.$$

Therefore, FHS set $\mathcal{X}$ is best in terms of the bound of AHC in (6). □

V. CONCLUSION

For any positive integer $n|\gcd(q-1, p-1)$, an extended generalized ring number class and order n's ring number are introduced, where q and p are two different Odd prime numbers. The name "extended generalized circumcision" was first proposed by Ding [10], which discussed the basic characteristics of second-order extended circumcision. They are the non-trivial generalizations of Whiteman generalized ring atom classification and ring number. Then Some basic characteristics of them are derived. We construct a kind of FHS set that is most ideal relative to AHC constraints. We will consider the application of extended generalized ring atom classification in theory of coding, cryptography and direct-spread sequence design in the future work.

REFERENCES

[1] W. Chu and C. J. Colbourn, ''Optimal frequency-hopping sequences via cyclotomy,'' *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1139–1141, Mar. 2005.

[2] G. Han, X. Long, C. Zhu, M. Guizani, and W. Zhang, ''A high-availability data collection scheme based on multi-AUVs for underwater sensor networks,'' *IEEE Trans. Mobile Comput.*, vol. 19, no. 5, pp. 1010–1022, May 2020.

[3] G. Han, Z. Tang, Y. He, J. Jiang, and J. A. Ansere, ''District partition-based data collection algorithm with event dynamic competition in underwater acoustic sensor networks,'' *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5755–5764, Oct. 2019.

[4] G. Han, S. Shen, H. Song, T. Yang, and W. Zhang, ''A stratification-based data collection scheme in underwater acoustic sensor networks,'' *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10671–10682, Nov. 2018.

[5] G. Cui, J. Yang, S. Lu, X. Yu, and L. Kong, ''Dual-use unimodular sequence design via frequency nulling modulation,'' *IEEE Access*, vol. 6, pp. 62470–62481, 2018.

[6] J.-H. Chung, Y. K. Han, and K. Yang, ''New classes of optimal frequency-hopping sequences by interleaving techniques,'' *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5783–5791, Dec. 2009.

[7] J.-H. Chung and K. Yang, ''*k*-fold cyclotomy and its application to frequency-hopping sequences,'' *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2306–2317, Apr. 2011.

[8] J.-H. Chung and K. Yang, ''On the average Hamming correlation of frequency-hopping sequence sets with good maximum Hamming correlation,'' in *Proc. 5th Int. Workshop Signal Design Appl. Commun.*, Oct. 2011, pp. 118–121.

[9] C. Ding and J. Yin, ''Sets of optimal frequency-hopping sequences,'' *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3741–3745, Aug. 2008.

[10] C. Ding, ''Cyclic codes from the two-prime sequences,'' *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3881–3891, Jun. 2012.

[11] P. Z. Fan and M. Darnell, *Sequence Design for Communications Applications*. London, U.K.: Wiley, 1996.

[12] C. F. Gauss, *Disquisitiones Arithmeticae*. New Haven, CT, USA: Yale, 1966.

[13] Y. K. Han and K. Yang, ''On the Sidel'nikov sequences as frequency-hopping sequences,'' *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4279–4285, Sep. 2009.

[14] P. V. Kumar, ''Frequency-hopping code sequence designs having large linear span,'' *IEEE Trans. Inf. Theory*, vol. 34, no. 1, pp. 146–151, Jun. 1988.

[15] F. Liu, D. Peng, Z. Zhou, and X. Tang, ''A new frequency-hopping sequence set based upon generalized cyclotomy,'' *Designs, Codes Cryptogr.*, vol. 69, no. 2, pp. 247–259, Nov. 2013.

[16] A. Lempel and H. Greenberger, ''Families of sequences with optimal Hamming-correlation properties,'' *IEEE Trans. Inf. Theory*, vol. IT-20, no. 1, pp. 90–94, Jan. 1974.

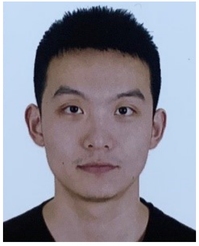
[17] D. Peng and P. Fan, ''Lower bounds on the Hamming auto- and cross correlations of frequency-hopping sequences,'' *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2149–2154, Sep. 2004.

[18] D. Peng, T. Peng, X. Tang, and X. Niu, ''A class of optimal frequency hopping sequences based upon the theory of power residues,'' in *Proc. Int. Conf. Sequences Appl.* Berlin, Germany: Springer, 2008.

[19] D. Peng, X. Niu, and X. Tang, ''Average Hamming correlation for the cubic polynomial hopping sequences,'' *IET Commun*, vol. 4, no. 15, pp. 1775–1786, 2010.

[20] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. New York, NY, USA: McGraw-Hill, 1994.

[21] A. L. Whiteman, ''A family of difference sets,'' *Illinois J. Math.*, vol. 6, no. 1, pp. 107–121, Mar. 1962.



MINGYUE FAN received the B.Eng. degree from the Wuhan Polytechnic University of Food Science and Engineering, in 2018. He is currently pursuing the master's degree in control engineering with China Jiliang University. His research interests include the security of industrial Internet of Things and data aggregation.