mathematics

MDPI

Article

New Constructions of One-Coincidence Sequence Sets over Integer Rings

Jin-Ho Chung *, Daehan Ahn and Daehwan Kim

Department of Electrical, Electronic, and Computer Engineering, University of Ulsan, Ulsan 44610, Republic of Korea; daehan@ulsan.ac.kr (D.A.); daehwankim@ulsan.ac.kr (D.K.)
* Correspondence: jinho@ulsan.ac.kr

Abstract: In this paper, we introduce new constructions of one-coincidence frequency-hopping sequence (OC-FHS) sets over integer rings. These OC-FHSs are designed to minimize interference in frequency-hopping multiple access (FHMA) systems, which are widely used in various communication applications. By leveraging the properties of primitive elements in integer ring $\mathbb{Z}_{p^n}$, we develop OC-FHS sets with lengths mp^{n-1} for m dividing $(p-1)$, along with constructions with composite lengths based on linear functions. The proposed OC-FHS sets include parameters not previously addressed in the literature and encompass some known cases as special cases.

Keywords: frequency-hopping; hamming correlation; primitive root; pseudorandom sequence

MSC: 94A55; 94B05

1. Introduction

The primary challenge in frequency-hopping multiple access (FHMA) systems lies in enabling multiple users to share the same frequency band without experiencing interference [1]. In such systems, interference occurs when signals from different users overlap, especially when they transmit on the same frequency at the same time. This type of interference, known as multiple-access interference or "hits", can severely degrade system performance, leading to communication breakdowns, data loss, or transmission errors. Addressing this issue requires the use of frequency-hopping sequences (FHSs) that are carefully structured to exhibit low correlation properties, which reduces the probability of users transmitting on the same frequency simultaneously. The design of FHS is pivotal in minimizing collisions or overlaps, ensuring that each user hops between frequencies in a manner that avoids interference. This structured frequency allocation over time optimizes the use of the available spectrum, making the system more efficient and reliable. By reducing the likelihood of collisions, FHS significantly improves the overall communication quality and system performance, even in environments with high user density. FHMA systems, supported by well-designed FHS, are integral to a variety of modern applications. For instance, in Bluetooth communication, frequency-hopping helps to reduce interference from nearby devices using the same frequency band. In military communications and secure transmissions, FHSs are employed to prevent interception and jamming, ensuring the confidentiality and integrity of transmitted information [2–5]. Additionally, radar systems utilize frequency-hopping to avoid detection and countermeasures, enhancing the reliability of signals in complex environments. By providing robust communication solutions across these diverse fields, FHSs continue to be a cornerstone in the development of FHMA systems.

To address the need for low-correlation FHS sets, numerous algebraic and combinatorial methods have been developed [6–18]. These constructions aim to produce optimal FHS sets that adhere to established theoretical bounds, such as the Lempel–Greenberger bound [19] and the Peng–Fan bound [20]. These bounds provide criteria for evaluating the

check for updates

Citation: Chung, J.-H.; Ahn, D.; Kim, D. New Constructions of One-Coincidence Sequence Sets over Integer Rings. *Mathematics* **2024**, *12*, 3316. https://doi.org/10.3390/math12213316

Academic Editors: Li Guo, Xinchao Zhao, Jesus Requena-Carrión, Xingquan Zuo and Patrick Solé

Received: 12 September 2024
Revised: 24 September 2024
Accepted: 22 October 2024
Published: 22 October 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

performance and efficiency of FHS sets in minimizing interference. Among the various types of FHS sets, the one-coincidence FHS (OC-FHS) set is of particular interest. An OC-FHS set is characterized by sequences where the maximum Hamming autocorrelation is 0, indicating that there is no self-interference within a sequence, and the maximum Hamming cross-correlation is 1, meaning that the sequences are designed to have minimal overlap with each other [21,22]. These properties make OC-FHS sets highly effective in reducing interference in FHMA systems, ensuring that the communication between different users remains as clear and uninterrupted as possible. Consequently, the study and development of OC-FHS sets have been the focus of extensive research, resulting in a wide range of methods and constructions aimed at achieving these desirable properties.

There have been some significant advances in design of OC-FHS sets. The sequences constructed in [23] can be interpreted as an OC-FHS set with a prime power length. In [21,22], Shaar and Davies developed the basic concept of OC-FHS sets for use in FHMA systems. Then, several OC-FHS sets over the finite field or the integer ring have been presented. Cao, Ge, and Miao provided a combinatorial framework to understand OC-FHS sets, together with some new OC-FHS sets [24]. Lee, Jung, and Chung presented an OC-FHS set of length $p^2 - p$ on $\mathbb{Z}_{p^2}$ [25]. Recently, Niu and Xing presented a new OC-FHS set based on the integer ring in the process of developing an extension method for general FHS sets [26].

In this paper, we present some new classes of OC-FHS sets constructed over integer rings. By using the primitive element of the integer ring $\mathbb{Z}_{p^n}$, we construct an OC-FHS set of length mp^{n-1} for $m \mid (p-1)$. We also present two constructions of OC-FHS sets with composite lengths constructed based on linear functions over integer rings. The new OC-FHS sets have parameters that are not covered in the literature and include some previously known parameters as special cases, as shown in Table 1. The organization of this paper is as follows. In Section 2, we present some preliminary knowledge on OC-FHS sets. In Section 3, we introduce three new constructions of OC-FHS sets based on integer rings. Section 4 provides examples of these new OC-FHS sets and compares our constructions with previously known methods. Finally, we conclude the paper in Section 5 with a discussion of the implications of our results and potential directions for future research.

Table 1. Some known classes of OC-FHS sets and OC-FHS sets from Constructions I, II, and III.

References	Parameter of FHS Sets $(N,M,1;L)$	Constraints
[21,22]	$(p-1, p, 1; p)$	p is a prime
	$(p, p, 1; p-1)$	p is a prime
[23]	$(p^n-1, p^n, 1; p^n)$	p is a prime
[24]	$(N, N, 1; k-1)$	k is size of the difference unit set modulo N
	$\left(\frac{p^n-1}{e}, p^n, 1; e\right)$	p is a prime
[25]	$(p^2-p, p^2, 1; p)$	p is a prime
[26]	$(p^n-p^{n-1}, p^n, 1; p)$	p is a prime
This paper	$(mp^{n-1}, p^n, 1; Kp)$	p is a prime, $mK = p-1$
	$(p^{n-1}, p^n, 1; p^2-p)$	p is a prime
	$(N', N, 1; p_1^2-p_1)$	$N = p_1p_2\cdots p_k$, $N' = p_2\cdots p_k$, $p_1, p_2, \cdots, p_k$: odd primes

2. Preliminaries

In mathematical terms, the effectiveness of a frequency-hopping sequence can be analyzed using Hamming correlation. This concept refers to the similarity between two se-

quences, where a high correlation indicates significant overlap between the sequences, and a low correlation means they are distinct. The Hamming auto-correlation measures the similarity of a sequence with a cyclically shifted version of itself. Ideally, in frequency-hopping systems, the auto-correlation should be zero for all shifts, meaning that there are no repetitions of frequencies within the sequence. The Hamming cross-correlation, on the other hand, measures the overlap between two different sequences. In FHMA systems, sequences with low cross-correlation are desirable because they reduce the likelihood of interference between users. The bounds established by Lempel–Greenberger and Peng–Fan provide theoretical limits on the minimum Hamming correlation that can be achieved for a given sequence length and alphabet size. These bounds guide the design of FHS sets that are optimal in terms of minimizing interference in FHMA systems.

An FHS $X = \{X(t)\}_{t=0}^{N-1}$ of length N is defined over an alphabet $F = \{f_0, \ldots, f_{M-1}\}$, in which each letter corresponds to a distinct available frequency. If we have two FHSs X and Y, the Hamming correlation is defined as the number of the coincidence of frequencies in X and the cyclic shift of Y, that is, the Hamming correlation $H_{X,Y}(\tau)$ for $0 \leq \tau \leq N-1$ is calculated as

$$H_{X,Y}(\tau) = \sum_{t=0}^{N-1} h[X(t), X(t+\tau \bmod N)] \tag{1}$$

where $h[x, y] = 1$ if $x = y$ and $h[x, y] = 0$ if $x \neq y$. If $X(t) = Y(t)$ for all t, then it is called the Hamming auto-correlation. Otherwise, it is called the Hamming cross-correlation. Lempel and Greenberger established a bound on the maximum Hamming auto-correlation of an FHS with respect to the length and the alphabet size [19].

Theorem 1 (Lempel–Greenberger bound [19]). *An FHS of length N defined over an alphabet of size M with maximum auto-correlation λ_a satisfies*

$$\lambda_a \geq \left\lceil \frac{(N-r)(N+r-M)}{(N-1)M} \right\rceil \tag{2}$$

where r is the remainder of N divided by M

Let $\mathbf{X} = \{X_0, \ldots, X_{L-1}\}$ be a set of FHSs of length N defined over an alphabet of size M. The maximum Hamming auto-correlation value $H_a(\mathbf{X})$ of $\mathbf{X}$ is defined as the maximum among all the Hamming auto-correlation values of FHSs in $\mathbf{X}$, except for $\tau = 0$ cases. $H_{X,Y}(\tau)$ for a nonzero τ is called an out-of-phase Hamming auto-correlation value. In a similar way, the maximum Hamming cross-correlation value $H_c(\mathbf{X})$ of $\mathbf{X}$ is defined as the maximum among all the Hamming cross-correlation values between two distinct FHSs in $\mathbf{X}$.

We denote $\mathbf{X}$ by an $(N, M, \lambda_s; L)$ FHS set. If N is the length of each FHS, M is the alphabet size, λ_s is the maximum between $H_a(\mathbf{X})$ and $H_c(\mathbf{X})$, and L is the number of FHSs in $\mathbf{X}$. In particular, if $H_a(\mathbf{X}) = 0$ and $H_c(\mathbf{X}) = 1$, then it is called a $(N, M, 1; L)$ one-coincidence FHS (OC-FHS) set. Note that $H_a(\mathbf{X}) = 0$ implies the non-repeating property of each FHS, that is, each symbol appears at most once in each FHS.

Peng and Fan established an important bound on the Hamming correlation values of an FHS set in the following theorem [20].

Theorem 2 (Peng–Fan bound [20]). *An $(N, M, \lambda_s; L)$ FHS set $\mathbf{X}$ satisfies*

$$\lambda_s \geq \left\lceil \frac{(NL-M)N}{(NL-1)M} \right\rceil \tag{3}$$

and

$$\lambda_s \geq \left\lceil \frac{2INL-(I+1)IM}{(NL-1)L} \right\rceil \tag{4}$$

where $I = \lfloor NL/M \rfloor$, and consequently satisfies.

Note that an OC-FHS set satisfies (3) with equality.

3. Three Constructions for New OC-FHS Sets

Integer rings, denoted $\mathbb{Z}_n$, are a mathematical structure where the set of integers is considered under modulo-n arithmetic. This structure plays an important role in the design of FHS sets because it allows for sequences that exhibit desirable properties such as non-repetition and low correlation. In this section, we utilize the properties of primitive elements of integer rings, which are numbers that generate all the nonzero elements in the multiplicative sense. These elements provide the characteristics of the OC-FHS sets from our constructions, ensuring that the resulting sequences are both non-repeating and minimally correlated with one another. On the other hand, the use of linear functions of composite lengths further enhances the flexibility of constructions, allowing for a wide range of sequence parameters that can be applied to various environments. The first and the second constructions in this section are based on the structure of the integer ring $\mathbb{Z}_{p^n}$, while the third construction is based on the product of the integer rings of prime sizes.

3.1. OC-FHS Sets of Length mp^{n-1}

For an odd prime p and a positive integer n, there exists a primitive root α of $\mathbb{Z}_{p^n}$, that is, the multiplicative group $\mathbb{Z}_{p^n}^* = \mathbb{Z}_{p^n} \setminus p\mathbb{Z}_{p^n}$ satisfies

$$\mathbb{Z}_{p^n}^* = \left\{\alpha^l \ : 0 \le l \le (p-1)p^{n-1} - 1\right\}. \tag{5}$$

It is also known that if α is a primitive root of $\mathbb{Z}_{p^2}$, then it is also a primitive root of $\mathbb{Z}_{p^n}$ for $n \ge 2$ in almost all cases [27].

Construction I. *Assume that α is a primitive root of $\mathbb{Z}_{p^n}$ and m is a positive divisor of $p-1$, that is, $p-1 = mK$ for some positive integer. For $0 \le i \le K-1$ and $r \in \{0, 1, \ldots, p-1\}$, define an FHS $X_{i,r} = \{X_{i,r}(t)\}_{t=0}^{mp^{n-1}-1}$ over $\mathbb{Z}_{p^n}$ as*

$$X_{i,r}(t) = \alpha^{Kt+i} + r. \tag{6}$$

Then, construct an FHS set as

$$\mathbf{A} = \{X_{i,r} \ : 0 \le i \le K-1 \text{and} r \in \{0, 1, \ldots, p-1\}\}. \tag{7}$$

Theorem 3. *The set $\boldsymbol{A}$ in Construction I is an $\left(mp^{n-1}, p^n, 1; Kp\right)$ OC-FHS set.*

Proof. The length, the alphabet size, and the set size of $\boldsymbol{A}$ are clear from the definition, and so they are enough to prove the auto- and cross-correlation properties.

(i) Autocorrelation: the Hamming auto-correlation $H_{i,r}(\tau)$ of $X_{i,r}$ can be calculated as

$$\begin{aligned} H_{i,r}(\tau) &= \sum_{t=0}^{mp^{n-1}-1} h\left[\alpha^{Kt+i} + r, \alpha^{K(t+\tau)+i} + r\right] \\ &= \sum_{t=0}^{mp^{n-1}-1} h\left[\alpha^{Kt+i}\left(1 - \alpha^{K\tau}\right), 0\right]. \end{aligned} \tag{8}$$

When $\tau = 0$,

$$H_{i,r}(\tau) = \sum_{t=0}^{mp^{n-1}-1} h[0,0] = mp^{n-1}. \tag{9}$$

When $\tau \neq 0$, it is clear that $h\left[\alpha^{Kt+i}\left(1 - \alpha^{K\tau}\right), 0\right] = 0$ for all τ because α^{Kt+i} is a unit in $\mathbb{Z}_{p^n}$, and $1 - \alpha^{K\tau} \neq 0$. That is, the out-of-phase auto-correlation value is always 0.

(ii) Cross-correlation: the Hamming cross-correlation $H_{(i,r),(j,s)}(\tau)$ between $X_{i,r}$ and $X_{j,s}$ can be expressed as

$$\begin{aligned} H_{(i,r),(j,s)}(\tau) &= \sum_{t=0}^{mp^{n-1}-1} h\left[\alpha^{Kt+i}+r, \alpha^{K(t+\tau)+j}+s\right] \\ &= \sum_{t=0}^{mp^{n-1}-1} h\left[\alpha^{Kt}\left(\alpha^{i}-\alpha^{K\tau+j}\right), s-r\right]. \end{aligned} \tag{10}$$

When $s = r$,

$$H_{(i,r),(j,s)}(\tau) = \sum_{t=0}^{mp^{n-1}-1} h\left[\alpha^{Kt}\left(\alpha^{i}-\alpha^{K\tau+j}\right), 0\right]. \tag{11}$$

Note that $0 \le i \ne j \le K-1$, and so $\alpha^i - \alpha^{K\tau+j} \ne 0$ in $\mathbb{Z}_{p^n}$. Thus,

$$H_{(i,r),(j,s)}(\tau) = \sum_{t=0}^{mp^{n-1}-1} 0 = 0. \tag{12}$$

When $s \ne r$, it is clear that $s-r$ is a unit in $\mathbb{Z}_{p^n}$. Then, $H_{(i,r),(j,s)}(\tau)$ is equal to the number of t with $0 \le t \le mp^{n-1}-1$ satisfying

$$\alpha^{-Kt} = \frac{\alpha^i - \alpha^{K\tau+j}}{s-r}. \tag{13}$$

If $\alpha^i - \alpha^{K\tau+j}$ is a unit in $\mathbb{Z}_{p^n}$, then $H_{(i,r),(j,s)}(\tau) \le 1$ since $\left(\alpha^i - \alpha^{K\tau+j}\right)/(s-r) = \alpha^l$ for some l with $0 \le l \le (p-1)p^{m-1}-1$. Otherwise, $H_{(i,r),(j,s)}(\tau) = 0$. Therefore, $H_{(i,r),(j,s)}(\tau) \le 1$ for all (i,r), (j,s), and $0 \le \tau \le mp^{n-1}-1$.

By summarizing the results of (i) and (ii), we get the assertion. □

3.2. OC-FHS Sets of Prime-Power Lengths

For an odd prime p and a positive integer n, the following construction gives a non-repeating sequence set of length p^{n-1} over $\mathbb{Z}_{p^n}$.

Construction II. *Let the FHS* $Y_{a,b} = \left\{Y_{a,b}(t)\right\}_{t=0}^{p^{n-1}-1}$ *be defined over* $\mathbb{Z}_{p^n}$ *as*

$$Y_{a,b}(t) = apt + b \bmod p^n.$$

where $1 \le a \le p-1$ *and* $0 \le b \le p-1$. *Then, construct an FHS set as*

$$\mathbf{B} = \left\{Y_{a,b} : 1 \le a \le p-1 \text{and} 0 \le b \le p-1\right\}. \tag{14}$$

Theorem 4. *The set* ***B*** *in Construction II is an optimal* $\left(p^{n-1}, p^n, 1; p^2-p\right)$ *OC-FHS set*.

Proof. The length, the alphabet size, and the set size of **B** is clear from the definition. The Hamming correlation $H_{(a,b),(a',b')}(\tau)$ between two sequences $Y_{a,b}$ and $Y_{a',b'}$ in **B** can be written as

$$\begin{aligned} H_{(a,b),(a',b')}(\tau) &= \sum_{t=0}^{p^{n-1}-1} h[atp+b,\ a'(t+\tau)p+b'] \\ &= \sum_{t=0}^{p^{n-1}-1} h[(a-a')tp, a'\tau p + (b'-b)] \end{aligned} \tag{15}$$

where every argument is computed modulo p^n.

(i) $a = a'$: When $b = b'$, $H_{(a,b),(a',b')}(\tau)$ becomes an auto-correlation, and

$$H_{(a,b),(a,b)}(\tau) = \sum_{t=0}^{p^{n-1}-1} h[0, a\tau p)] = \begin{cases} p^{n-1}, & \text{if } \tau = 0 \\ 0, & \text{if } \tau \neq 0. \end{cases} \tag{16}$$

When $b \neq b'$, we have

$$H_{(a,b),(a,b')}(\tau) = \sum_{t=0}^{p^{n-1}-1} h\big[-a\tau p, b' - b\big)\big] = 0 \tag{17}$$

where the second equality comes from the fact that $-a\tau p$ is not a unit in $\mathbb{Z}_{p^n}$, while $b' - b$ is a unit.

(ii) $a \neq a'$: When $b = b'$, the Hamming correlation is given by

$$\begin{aligned} H_{(a,b),(a',b)}(\tau) &= \sum_{t=0}^{p^{n-1}-1} h[(a - a')tp,\ a'\tau p] \\ &= \left|\left\{t \in \mathbb{Z}_{p^{n-1}} \ : (a - a')t \equiv a'\tau \bmod p^{n-1}\right\}\right| \end{aligned} \tag{18}$$

because $a - a'$ is a unit in $\mathbb{Z}_{p^{n-1}}$. When $b \neq b'$, $H_{(a,b),(a',b')}(\tau)$ is always zero, since, in (15), $(a - a')tp$ is not unit in $\mathbb{Z}_{p^n}$ while $a'\tau p + (b' - b)$ is a unit.

By summarizing the results of (i) and (ii), we can conclude that the Hamming auto-correlation values are zero for all nonzero τ, and the Hamming cross-correlation values are always less than or equal to 1. □

3.3. OC-FHS Sets of a Composite Length

In a similar way to Construction II, it is possible to construct an FHS set whose length is a product of distinct primes. For distinct odd primes, $p_1 < p_2 < \ldots < p_k$, let $N = p_1 p_2 \cdots p_k$ and $N' = p_2 \cdots p_k$.

Construction III. *Let the FHS* $Z_{c,d} = \left\{Z_{c,d}(t)\right\}_{t=0}^{N'-1}$ *be defined over* $\mathbb{Z}_N$ *as*

$$Z_{c,d}(t) = cp_1 t + d \ mod\ N. \tag{19}$$

where $1 \leq c \leq p_1 - 1$ *and* $0 \leq d \leq p_1 - 1$. *Then, construct an FHS set as*

$$\mathbf{C} = \left\{Z_{c,d} \ : 1 \leq c \leq p_1 - 1 \text{and} 0 \leq d \leq p_1 - 1\right\}. \tag{20}$$

Theorem 5. *The set* $\boldsymbol{C}$ *in Construction I is an optimal* $\left(N', N, 1; p_1^2 - p_1\right)$ *OC-FHS set.*

Proof. The length, the alphabet size, and the set size of **C** are clear from the definition. The Hamming correlation $H_{(c,d),(c',d')}(\tau)$ between two sequences $Z_{c,d}$ and $Z_{c',d'}$ in **C** can be expressed as

$$\begin{aligned} H_{(c,d),(c',d')}(\tau) &= \sum_{t=0}^{N'-1} h[ctp_1 + d,\ c'(t + \tau)p_1 + d'] \\ &= \sum_{t=0}^{p^{n-1}-1} h[(c - c')tp_1, c'\tau p_1 + (d' - d)] \end{aligned} \tag{21}$$

where every argument is computed modulo N.

(i) $c = c'$: When $d = d'$, $H_{(c,d),(c',d')}(\tau)$ becomes an auto-correlation, and

$$\begin{aligned} H_{(c,d),(c,d)}(\tau) &= \sum_{t=0}^{N'-1} h[0, c\tau p_1)] \\ &= \begin{cases} N', & \text{if } \tau = 0 \\ 0, & \text{if } \tau \neq 0. \end{cases} \end{aligned} \tag{22}$$

When $d \neq d'$, we have

$$H_{(c,d),(c,d')}(\tau) = \sum_{t=0}^{N'-1} h\left[-c\tau p_1, d' - d\right]. \tag{23}$$

Note that $-c\tau p_1$ is a multiple of p_1 while $d' - d$ cannot be a multiple of p_1. Thus, the correlation value is always zero.

(ii) $c \neq c'$: When $d = d'$, the Hamming correlation is given by

$$\begin{aligned} H_{(c,d),(c',d)}(\tau) &= \sum_{t=0}^{N'-1} h[(c-c')tp_1,\ c'\tau p_1] \\ &= |\{t \in \mathbb{Z}_{N'} : (c-c')t \equiv c'\tau \bmod N'\}| \\ &= 1 \end{aligned} \tag{24}$$

because $1 \leq |c - c'| \leq p_1 - 1 < p_2$, and so $c - c'$ has an inverse modulo N'. When $d \neq d'$, $H_{(c,d),(c',d')}(\tau)$ is always zero, for in (21), $d\prime - d$ is not divided by p_1.

By summarizing the results of (i) and (ii), we can conclude that the out-of-phase Hamming auto-correlation values are always 0, and the Hamming cross-correlation values are upper-bounded by 1. □

4. Examples and Discussion

An OC-FHS set is clearly optimal with respect to the Peng–Fan bound in Theorem 1, since its maximum Hamming auto- and cross-correlation values are upper-bounded by 0 and 1, respectively. In this section, we present some examples of the OC-FHS sets presented in Section 3 and compare the parameters with the previously known ones in the literature.

4.1. Examples of Construction

In this subsection, we provide examples of the three constructions in Section 3. Detailed versions of the constructed sequences are included in Appendices A–C.

Example 1 (Construction I). *Let $p = 5$,$n = 2$, and $m = 2$ in Construction I. By using a primitive root 2 modulo 25, we can construct*

$$\boldsymbol{A} = \{X_{i,r} : 0 \leq i \leq 1 \text{ and } 0 \leq i \leq 4\}$$

where $X_{i,r}(t) = 2^{2t+i} + r \bmod 25$ for $0 \leq t \leq 19$ (Refer to Appendix A *for the actual generated FHS set). The set is an $(10, 25, 1; 10)$ OC-FHS set.*

Example 2 (Construction II). *Let $p = 5$ and $n = 2$ in Construction II. We can construct*

$$\boldsymbol{B} = \{Y_{a,b} : 1 \leq a \leq 4 \text{ and } 0 \leq b \leq 4\}$$

where $Y_{a,b}(t) = 5at + b \bmod 25$ for $0 \leq t \leq 4$ (Refer to Appendix B *for the actual generated FHS set). The set is a $(5, 25, 1; 20)$ OC-FHS set.*

Example 3 (Construction III). *Let $p_1 = 5$ and $p_2 = 7$ in Construction III. We can construct*

$$\boldsymbol{C} = \{Z_{c,d} : 1 \leq c \leq 4 \text{ and } 0 \leq d \leq 4\}$$

where $Z_{c,d}(t) = 5at + b \bmod 35$ for $0 \leq t \leq 6$ (Refer to Appendix C *for the actual generated FHS set). The set is a $(7, 35, 1; 20)$ OC-FHS set.*

4.2. Comparison to Known OC-FHS Sets

The parameter of **A** in Construction I, as shown in Table 1, includes some parameters of the previously known OC-FHS sets as special cases. In the case $m = p - 1$, **A** becomes an $(p^n - p^{n-1}, p^n, 1; p)$ OC-FHS set, which is given in Lemma 6 of [24]. Moreover, the parameter in [23] corresponds to the case $m = p - 1$ and $n = 2$ in Construction I. In terms of the ratio between length and alphabet size, the parameters of Constructions II and III are similar to that in [22]. In Construction II, the length divides the alphabet size, whereas in the construction in [22], the length does not divide the alphabet size, which marks a difference between them. Furthermore, the parameters of Construction III also differ in terms of the alphabet size.

4.3. Parameters of New OC-FHS Sets

Depending on the specific type of the FHMA system, the relationship between the length of the FHSs and the alphabet size can vary significantly. In practical applications such as systems with limited power resources, real-time communication constraints, or environments with low interference, a shorter FHS can offer distinct advantages. For example, shorter sequences enhance power efficiency by reducing the number of hops, minimize synchronization complexity, and allow faster data transmission where low latency is essential. Additionally, in bandwidth-constrained environments, shorter sequences optimize spectrum utilization without compromising performance, making them highly effective in scenarios requiring a balance between efficiency, speed, and system complexity. When the frequency-hopping sequence is short, users may end up utilizing limited frequency bands. However, this issue can be mitigated by exchanging the hopping sequences between users in subsequent hopping periods. By rotating or swapping sequences among users, the system ensures more balanced frequency usage over time, reducing the chances of prolonged interference or congestion on certain frequencies. Note that new FHS sets from our constructions have larger alphabet size than the length of the FHSs. To the best of our knowledge, the only known construction for the case where the length can be significantly smaller than the alphabet size is presented in [24], as shown in Table 1.

4.4. Balance Property of New OC-FHS Sets

When the alphabet size in an FHS is larger than the length of the sequence, frequencies tend to be used in an unbalanced way. Therefore, when designing an FHS set, it is essential to ensure that all the available frequencies are used in a balanced manner. From this perspective, we aim to check whether the frequencies in the OC-FHS sets from Constructions I, II, and III satisfy the balance criterion. This analysis may help ensure that the system makes efficient use of the available frequencies.

The number of appearances of a symbol a in an FHS set $\mathbf{X} = \{X_0, \ldots, X_{L-1}\}$ of FHSs $X_i = \{X_i(t)\}_{t=0}^{N-1}$ of length N defined over an alphabet $\mathbf{F}$ of size M can be defined as

$$N_{\mathbf{X}}(a) = \sum_{i=0}^{L-1} |\{0 \le t \le N-1 : X_i(t) = a\}|$$

for $a \in \mathbf{F}$. If $N_{\mathbf{X}}(a)$ is constant for all $a \in \mathbf{F}$, we call $\mathbf{X}$ a balanced FHS set. The balance properties of the OC-FHS sets **A, B**, and **C** can be checked as follows:

- **A** (Construction I): For all $a \in \mathbb{Z}_{p^n}$, we have

$$N_{\mathbf{A}}(a) = p - 1$$

- **B** (Construction II): For all $b \in \mathbb{Z}_{p^n}$, we have

$$N_{\mathbf{B}}(b) = p - 1.$$

- **C** (Construction III): For all $c \in \mathbb{Z}_N$, we have

$$N_{\mathbf{C}}(c) = p_1 - 1.$$

Therefore, every OC-FHS set from our constructions satisfies the balance property, which is related to the balanced use of available frequencies in practical situations.

5. Conclusions

In this paper, we have introduced new constructions of OC-FHS sets over integer rings, which are designed to minimize interference in FHMA systems. By leveraging the properties of primitive elements and linear functions in integer rings, we have developed three classes of OC-FHS sets. Moreover, the new OC-FHS sets satisfies the balance property. These new constructions encompass parameters not previously addressed in the literature and include some known cases as special instances. Future research could explore further generalizations of these constructions, including the investigation of other algebraic structures or the application of these sequences in different communication scenarios.

Author Contributions: Conceptualization, J.-H.C. and D.K.; methodology, J.-H.C. and D.A.; validation, D.K. and D.A.; writing—original draft preparation, J.-H.C.; writing—review and editing, D.K. and D.A.; project administration, J.-H.C.; funding acquisition, J.-H.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the 2022 Research Fund of University of Ulsan.

Data Availability Statement: No new data were created or analyzed in this study.

Acknowledgments: The authors would like to thank the anonymous reviewers and the academic editor for their valuable comments that helped to improve the quality of the paper.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Full Sequence Set of Example 1

Table A1. A $(10, 25, 1; 10)$ OC-FHS Set from Construction I.

(i,r)	$X_{i,r}$
(0,0)	{1, 4, 16, 14, 6, 24, 21, 9, 11, 19}
(0,1)	{2, 5, 17, 15, 7, 0, 22, 10, 12, 20}
(0,2)	{3, 6, 18, 16, 8, 1, 23, 11, 13, 21}
(0,3)	{4, 7, 19, 17, 9, 2, 24, 12, 14, 22}
(0,4)	{5, 8, 20, 18, 10, 3, 0, 13, 15, 23}
(1,0)	{2, 8, 7, 3, 12, 23, 17, 18, 22, 13}
(1,1)	{3, 9, 8, 4, 13, 24, 18, 19, 23, 14}
(1,2)	{4, 10, 9, 5, 14, 0, 19, 20, 24, 15}
(1,3)	{5, 11, 10, 6, 15, 1, 20, 21, 0, 16}
(1,4)	{6, 12, 11, 7, 16, 2, 21, 22, 1, 17}

Appendix B. Full Sequence Set of Example 2

Table A2. A $(5, 25, 1; 20)$ OC-FHS Set from Construction II.

(a,b)	$Y_{a,b}$
1,0)	{0, 5, 10, 15, 20}
(1,1)	{1, 6, 11, 16, 21}
(1,2)	{2, 7, 12, 17, 22}

Table A2. *Cont.*

(a,b)	$Y_{a,b}$
(1,3)	{3, 8, 13, 18, 23}
(1,4)	{4, 9, 14, 19, 24}
(2,0)	{0, 10, 20, 5, 15}
(2,1)	{1, 11, 21, 6, 16}
(2,2)	{2, 12, 22, 7, 17}
(2,3)	{3, 13, 23, 8, 18}
(2,4)	{4, 14, 24, 9, 19}
(3,0)	{0, 15, 5, 20, 10}
(3,1)	{1, 16, 6, 21, 11}
(3,2)	{2, 17, 7, 22, 12}
(3,3)	{3, 18, 8, 23, 13}
(3,4)	{4, 19, 9, 24, 14}
(4,0)	{0, 20, 15, 10, 5}
(4,1)	{1, 21, 16, 11, 6}
(4,2)	{2, 22, 17, 12, 7}
(4,3)	{3, 23, 18, 13, 8}
(4,4)	{4, 24, 19, 14, 9}

Appendix C. Full Sequence Set of Example 3

Table A3. A $(7, 35, 1; 20)$ OC-FHS Set from Construction III.

(c,d)	$Z_{c,d}$
(1,0)	{0, 5, 10, 15, 20, 25, 30}
(1,1)	{1, 6, 11, 16, 21, 26, 31}
(1,2)	{2, 7, 12, 17, 22, 27, 32}
(1,3)	{3, 8, 13, 18, 23, 28, 33}
(1,4)	{4, 9, 14, 19, 24, 29, 34}
(2,0)	{0, 10, 20, 30, 5, 15, 25}
(2,1)	{1, 11, 21, 31, 6, 16, 26}
(2,2)	{2, 12, 22, 32, 7, 17, 27}
(2,3)	{3, 13, 23, 33, 8, 18, 28}
(2,4)	{4, 14, 24, 34, 9, 19, 29}
(3,0)	{0, 15, 30, 10, 25, 5, 20}
(3,1)	{1, 16, 31, 11, 26, 6, 21}
(3,2)	{2, 17, 32, 12, 27, 7, 22}
(3,3)	{3, 18, 33, 13, 28, 8, 23}
(3,4)	{4, 19, 34, 14, 29, 9, 24}
(4,0)	{0, 20, 5, 25, 10, 30, 15}
(4,1)	{1, 21, 6, 26, 11, 31, 16}
(4,2)	{2, 22, 7, 27, 12, 32, 17}
(4,3)	{3, 23, 8, 28, 13, 33, 18}
(4,4)	{4, 24, 9, 29, 14, 34, 19}

References

1. Simon, M.K.; Omura, J.K.; Scholtz, R.A.; Levitt, B.K. *Spread Spectrum Communications Handbook*; McGraw-Hill: New York, NY, USA, 2002.
2. Sarwate, D.V. Reed-Solomon codes and the design of sequences for spread-spectrum multiple-access communications. In *Reed-Solomon Codes and Their Applications*; Wicker, S.B., Bharagava, V.K., Eds.; IEEE Press: Piscataway, NJ, USA, 1994.
3. Fan, P.; Darnell, M. *Sequence Design for Communications Applications*; Research Studies Press, John Wiley & Sons: London, UK, 1996.
4. Yang, L.; Giannakis, G.B. Ultra-wideband communications: An idea whose time has come. *IEEE Sig. Proc. Mag.* **2004**, *21*, 26–54. [CrossRef]
5. Wi-Fi and Bluetooth-Interference Issues. Available online: http://www.hp.com (accessed on 25 August 2024).
6. Kumar, P.V. Frequency-hopping code sequence designs having large linear span. *IEEE Trans. Inf. Theory* **1988**, *34*, 146–151. [CrossRef]
7. Udaya, P.; Siddiqi, M.U. Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings. *IEEE Trans. Inf. Theory* **1998**, *44*, 1492–1503. [CrossRef]
8. Fuji-Hara, R.; Miao, Y.; Mishima, M. Optimal frequency hopping sequences: A combinatorial approach. *IEEE Trans. Inf. Theory* **2004**, *50*, 2408–2420. [CrossRef]
9. Chu, W.; Colbourn, C.J. Optimal frequency-hopping sequences via cyclotomy. *IEEE Trans. Inf. Theory* **2005**, *51*, 1139–1141. [CrossRef]
10. Ding, C.; Moisio, M.J.; Yuan, J. Algebraic constructions of optimal frequency-hopping sequences. *IEEE Trans. Inf. Theory* **2007**, *53*, 2606–2610. [CrossRef]
11. Ge, G.; Miao, Y.; Yao, Z. Optimal frequency hopping sequences: Auto- and cross-correlation properties. *IEEE Trans. Inf. Theory* **2009**, *55*, 867–879. [CrossRef]
12. Chung, J.-H.; Han, Y.K.; Yang, K. New classes of optimal frequency-hopping sequences by interleaving techniques. *IEEE Trans. Inf. Theory* **2009**, *55*, 783–5791. [CrossRef]
13. Yang, Y.; Tang, X.; Parampalli, U.; Peng, D. New bound on frequency hopping sequence sets and its optimal constructions. *IEEE Trans. Inf. Theory* **2011**, *57*, 7605–7613. [CrossRef]
14. Zeng, X.Y.; Cai, H.; Tang, X.H.; Yang, Y. A class of optimal frequency hopping sequences with new parameters. *IEEE Trans. Inf. Theory* **2012**, *58*, 4899–4907. [CrossRef]
15. Chung, J.-H.; Yang, K. A new class of balanced near-perfect nonlinear mappings and its application to sequence design. *IEEE Trans. Inf. Theory* **2013**, *59*, 1090–1097. [CrossRef]
16. Zeng, X.Y.; Cai, H.; Tang, X.H.; Yang, Y. Optimal frequency hopping sequences of odd length. *IEEE Trans. Inf. Theory* **2013**, *59*, 3237–3248. [CrossRef]
17. Ren, W.; Fu, F.-W.; Zhou, Z. New sets of frequency-hopping sequences with optimal Hamming correlation. *Des. Codes Cryptogr.* **2014**, *72*, 423–434. [CrossRef]
18. Niu, X.; Xing, C.; Liu, Y.; Zhou, L. A construction of optimal frequency hopping sequence set via combination of multiplicative and additive groups of finite fields. *IEEE Trans. Inf. Theory* **2020**, *66*, 5310–5315. [CrossRef]
19. Lempel, A.; Greenberger, H. Families of sequences with optimal Hamming correlation properties. *IEEE Trans. Inf. Theory* **1974**, *20*, 90–94. [CrossRef]
20. Peng, D.; Fan, P. Lower bounds on the Hamming auto- and cross-correlations of frequency-hopping sequences. *IEEE Trans. Inf. Theory* **2004**, *50*, 2149–2154. [CrossRef]
21. Shaar, A.A.; Davies, P.A. Prime sequences: Quasi-optimal sequences for OR channel code division multiplexing. *Electron. Lett.* **1983**, *9*, 888–889. [CrossRef]
22. Shaar, A.A.; Davies, P.A. A survey of one-coincidence sequences for frequency-hopped spread-spectrum systems. *IEE Proc. F* **1984**, *131*, 719–724. [CrossRef]
23. Reed, I.S. kth-order near-orthogonal codes. *IEEE Trans. Inf. Theory* **1971**, *17*, 116–117. [CrossRef]
24. Cao, Z.; Ge, G.; Miao, Y. Combinatorial characterizations of one-coincidence frequency-hopping sequences. *Des. Codes Crypt.* **2006**, *41*, 177–184. [CrossRef]
25. Lee, T.H.; Jung, H.H.; Chung, J.-H. A new one-coincidence frequency-hopping sequence set of length $p^2 - p$. In Proceedings of the 2018 IEEE Information Theory Workshop, Guangzhou, China, 25–29 November 2018. [CrossRef]
26. Niu, X.; Xing, C. New extension constructions of optimal frequency hopping sequence sets. *IEEE Trans. Inf. Theory* **2019**, *65*, 5846–5855. [CrossRef]
27. Rosen, K.H. *Elementary Number Theory and Its Applications*; Addison-Wesley: Reading, MA, USA, 1988.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.