Master's Thesis

Design of One-Coincidence Frequency Hopping Sequence Sets for FHMA Systems

Tae-Hwan Lee

Department of Electrical Engineering

Graduate School of UNIST

2019

Design of One-Coincidence Frequency Hopping Sequence Sets for FHMA Systems

Tae-Hwan Lee

Department of Electrical Engineering

Graduate School of UNIST

Design of One-Coincidence Frequency Hopping Sequence Sets for FHMA Systems

A thesis/dissertation
submitted to the Graduate School of UNIST
in partial fulfillment of the
requirements for the degree of
Master of Science

Tae-Hwan Lee

June 7, 2019
Approved by

_____

Advisor
Jin-Ho Chung

Design of One-Coincidence Frequency Hopping Sequence Sets for FHMA Systems

Tae-Hwan Lee

This certifies that the thesis/dissertation of Tae-Hwan Lee is approved.

June 7, 2019

signature

_____

Advisor: Jin-Ho Chung

signature

_____

Hyoil Kim

signature

_____

Hyun Jong Yang

Abstract

In the thesis, we discuss frequency hopping multiple access (FHMA) systems and construction of optimal frequency hopping sequence and applications. Moreover, FHMA is widely used in modern communication systems such as Bluetooth, ultrawideband (UWB), military, etc. For these systems, it is desirable to employ frequency-hopping sequences (FHSs) having low Hamming correlation in order to reduce the multiple-access interference.

In general, optimal FHSs with respect to the Lempel-Greenberger bound do not always exist for all lengths and frequency set sizes. Therefore, it is an important problem to verify whether an optimal FHS with respect to the Lempel-Greenberger bound exists or not for a given length and a given frequency set size.

I constructed FHS satisfying optimal with respect to the Lempel-Greenberger bound and Peng-Fan bound for efficiency of available frequency. Parameters of a new OC-FHS set are length $p^2 - p$ over $\mathbb{Z}_{p^2}$ by using a primitive element of $\mathbb{Z}_p$. The new OC-FHS set with $H_a(\mathcal{X}) = 0$ and $H_c(\mathcal{X}) = 1$ can be applied to several recent applications using ISM band (e.g. IoT) based on BLE and Zigbee.

In the construction and theorem, I used these mathematical back grounds in preliminaries (i.e., finite field, primitive element, primitive polynomial, frequency hopping sequence, multiple frequency shift keying, DS/CDMA) in order to prove mathematically.

The outline of thesis is as follows. In preliminaries, we explain algorithm for minimal polynomial for sequence, linear complexities, Hamming correlation and bounds for FHSs and some applications are presented. In section Ⅲ, algorithm for complexity, correlation and bound for FHSs and some applications are presented. In section Ⅳ, using information in section Ⅱ and Ⅲ, a new construction of OC-FHS is presented. In order to prove the optimality of FHSs, all cases of Hamming autocorrelation and Hamming cross-correlation are mathematically calculated.

Moreover, in order to raise data rate or the number of users, a new method is presented. Using this method, sequences are divided into two times of length and satisfies Lempel-Greenberger bound and Peng-Fan bound.

Contents

List of Figures

List of Tables

Ⅰ. Introduction

We use a kind of specific sequence for error correcting code, parity check in communication system, data storage (HDD, SDD), BlueBee, etc. Especially, BlueBee uses mapping of two different module between Zigbee and Bluetooth. When we use electronic device, thermal noise or power decrease is unavoidable.

In order to have robustness to noise, time delay, fading, or other disturbance, we make information bits sequence of n-tuple to longer sequence bits of m-tuple, $m > n$. Note that each sequence bit is over $\mathbb{F}_p$.

For example, in the case of transmitting signals, we map information bits using one-to-one mapping from specific symbol into predefined sequence which has maximized hamming distance within fixed sequence. At the receiver, received sequence is decoded to each symbol meaning information. In these processes, each symbol which is mapped to sequence by using predefined generator matrix G. Moreover, at receiver, by using inverse matrix of $H = G^{-1}$, we decode transmitted signal.

We use pseudo-random sequence made by Linear Feedback Shift Register (LFSR) in stream cipher, Monte Carlo method, Frequency Hopping Sequence (FHS) which is implemented to FHMA (Frequency Hopping Multiple Access). We show pros and cons of the pseudo-random sequence as follows:

- Pros
  1. It is generated fast by using LFSR.
  2. Because of high data rate, we need it.
  3. We can generate a kind of sequences by choosing initial state.

- Cons
  1. If consecutive sequences are exposed with the length which is 2 times of LFSR length, whole sequences can be known.

To make pseudo-random sequence which is k-tuples over $\mathbb{F}_p$, we use LFSR which consists of a cascade of L unit delay cells, or stages, with provision to form a linear combination of the cell contents, which serves as the input to the first stage. The output of the LFSR is assumed to be taken from the last stage. The initial contents of the L stages coincide with the first L output digits, and the remaining output digits are uniquely determined by the recursion.

In stream cipher, we usually use LFSR to encrypt plain-text to cipher-text. Because we need high speed with low delay for data communication, we want fast process of encryption and decryption by using LFSR and XOR operation.

Moreover, for a secure of the LFSR, it needs to be hard to presume complexity, also it must not make overlapped sequence during large period. This complexity is a significant measure for security. If twice the length of complexity is known, entire sequences could be exposed according to Berlekamp-Massey algorithm. Therefore, we need complexity which makes large period.

For these properties, we use a finite field or Galois field which contains a finite number of elements. The most common examples of finite fields are given by the integers mod p when p is a prime number.

The number of elements of a finite field is called its order. A finite field of order q exists if and only if the order q is a prime power p^k (where p is a prime number and k is a positive integer). All finite fields of a given order are isomorphic. In a field of order p^k, adding p copies of any element always results in zero; that is, the characteristic of the field is p.

In a finite field of order q, the polynomial $x^q - x$ has all q elements of the finite field as roots. The non-zero elements of a finite field form a multiplicative group. This group is cyclic, so all non-zero elements can be expressed as powers of a single element called a primitive element of the field. (In general, there will be several primitive elements for a given field.)

For these purposes, we get, first, minimal polynomial of a value α which is the polynomial of lowest degree having coefficients of a specified type. If the minimal polynomial of exists, it is unique. The coefficient of the highest-degree term in the polynomial is required to be 1, and the specified type for the remaining coefficients could be integers, rational numbers, real numbers, or others

Furthermore, we choose a primitive polynomial is the minimal polynomial of a primitive element of the finite extension field $GF(p^m)$. In other words, a polynomial $F(x)$ with coefficients in $GF(p)$ is a primitive polynomial if its degree is m and it has a root α in $GF(p^m)$ such that $\{0,1,\alpha,\alpha^2,\alpha^3,\dots,\alpha^{p^m-2}\}$ is the entire field $GF(p^m)$. This means that α is a primitive (p^m-1)-root of unity in $GF(p^m)$.

In the case of FHS, we use an FHS for diversity of the frequency and low correlation of sequence set. An FSK modulation map each information to one frequency. If some frequency lost its properties, we

cannot receive or classify signal. Therefore, we use an FHS set occupying wide frequency bandwidth. In the bandwidth of FHS, each sequence mapped to an information symbol is designed to have low correlation with other sequences in the same set. The sequence construction usually uses mathematical and combinatorial methods for distinctive array.

Furthermore, by using an LFSR, we obtain property of secure and wide bandwidth which robust to noise. Correlation is the important measure for sequence about time delay. Therefore, our purpose is to design construction which makes sequence with minimal correlation.

In this thesis, we investigate an OC (One-Coincidence) FHS Construction and calculate correlation in the *Theorem*. Moreover, we divide each sequence to make half period in FHS set and we double the number of sequences for double symbol or users.

The outline of this paper is as follows. In chapter 2, we give some preliminaries for finite field and LFSR and FHS. In chapter 3, we investigate stream cipher and block cipher with examples. In chapter 4, we inform FHS *Construction* which is used in FHMA and Theorem. In chapter 5, we suggest OC-FHS *Construction* and *Theorem* using mathematical and combinational methods. In chapter 6, we summarize results and present expected applications.

Ⅱ. Preliminaries

In this chapter, we discuss some preliminaries about primitive in finite field, LFSR, FHS.

Primitive polynomial is important factor when we design an LFSR. By using a prime field F_p and an mth degree irreducible polynomial $p(x)$ in $F_p[x]$, we can construct a field with p elements. To construct the specific degree of primitive polynomial, we need some conditions. In order to define finite field, we start with integral domain and Euclidean domain.

2.1 Integral domain and Euclidean Domains

An integral domain is a set *D*, together with two binary operations, $+$ and $\cdot$, such that:

- The elements of *D* form an abelian group under $+$; the additive identity element is denoted by 0.
- The multiplication is associative and commutative, and has an identity element, denoted by 1.
- The cancellation law holds. That is, if $ab = ac$ and $a \neq 0$, then $b = c$.
- The distributive law holds. That is, if *a, b,* and *c* belong to *D*, then $a(b + c) = ab + ac$.

A *Euclidean domain* is an integral domain with an added feature: a notion of ”size” among its elements. The ”size” of $a \neq 0$, denoted $g(a)$, is a nonnegative integer such that

$$g(a) \leq g(ab) \qquad if\ \ b \neq 0;$$

and

For all $a, b \neq 0$, there exist q and r (”quotient” and ”remainder”) such that $a = qb + r$, with $r = 0\ \ or\ \ g(r) \leq g(b)$.

Lemma 2.1. If *a* and *b* are relatively prime, then there exist *s* and *t* such that $as + bt = 1$.

Lemma 2.2. If $p \in D$ is prime, and if $p \nmid a$ then *p* and a are relatively prime.

Lemma 2.3. If $p \nmid a$ then there exist elements $s, t \in D$, such that $ps + at = 1$.

In order to check whether D mod m is a field, there exist multiplicative inverses., i.e., if for any $a \neq 0$ there exist a b such that

$$a \cdot b = 1.$$

Theorem 2.4. If p is prime, D mod p is a field.

Proof. Let a be an element of D mod $p, a \neq 0$; we must show that there exist an element *b* such that $a \cdot b = 1$ holds. $a \neq 0$ means that $p \nmid a$. Thus, by Lemma 2.3, there exist element *b* and *t* in *D* such that $ab + pt = 1$. Thus $ab \equiv 1 \pmod{p}$, and this in turn is equivalent to (2.1). Thus, b is the inverse of a.

Example 2.1 We calculate the first new powers of x modulo $p(x) = x^3 + x + 1$:

$$\begin{aligned}
x^0 &\equiv 1 \\
x^1 &\equiv x \\
x^2 &\equiv x^2 \\
x^3 &\equiv x + 1 \\
x^4 &\equiv x^2 + x \\
x^5 &\equiv x^3 + 2 \equiv x^2 + x + 1 \\
x^6 &\equiv x^3 + x^2 + x \equiv x^2 + 1 \\
x^7 &\equiv x^3 + x \equiv 1,
\end{aligned}$$

all mod $x^3 + x + 1$.

2.2 Properties of Finite Fields

We can construct a field with p^m elements given a prime field F_p and an mth degree irreducible polynomial $p(x)$ in $F_p[x]$. We assume the existence of a finite field F with q elements and investigate the logical consequences. We already know that for some values of *q* there are finite fields, e.g. if q is a prime, or if $q = 8$ (Example 2.1).

Theorem 2.5. The number of elements *q* must be a power of a prime: $q = p^m$, p prime.

Theorem 2.6. If t is the order of α, then t divides $q - 1$.

Proof. Order is the smallest positive integer *t* such that $a^t = e$ (where *e* denotes the identity element of the group). Let F^* denotes the set of nonzero elements of F. Then F^* is a multiplicative group with $q - 1$ elements, and $\{1, \alpha, \alpha^2, \ldots, \alpha^{t-1}\}$ is a subgroup with t elements. Lagrange's theorem shows that the number of elements in a subgroup is always a divisor of the number of elements in the

group. Therefore, t divides $q-1$.

Corollary 2.7. In every finite field, there exists at least one element (in fact, exactly $\phi(q-1)$ elements) of order $q-1$. Hence, the multiplicative group of any finite field is cyclic.

2.3 Primitive Polynomial in Finite Field

The definition of primitive polynomial is as follows.

Definition 2.8. An element of multiplicative order $q-1$, i.e., a generator of the cyclic group $\mathrm{F}^* = \mathrm{F} - \{0\}$, is called a primitive root of the field F.

Example 2.1. Consider the field $F_7 = \mathrm{mod}\ 7$, whose elements we take to be $\{0,1,2,3,4,5,6\}$. Neither 2 nor any of its powers is a primitive root in F_7. The powers of 3 are summarized in the following table:

Table 2.1: Table of order

i	3^i	Ord(3^i)
0	1	1
1	3	6
2	2	3
3	6	2
4	4	3
5	5	6
6	1	(repeats)

The minimal polynomial of a value α is the polynomial of lowest degree having coefficients of a specified type, such that α is a root of the polynomial. If the minimal polynomial of α exists, it is unique. The coefficient of the highest-degree term in the polynomial is required to be 1, and the specified type for the remaining coefficients could be integers, rational numbers, real numbers, or others.

Theorem 2.9. Suppose F is a field with p m elements. Associated with each $\alpha \in F$, there is a unique monic polynomial $p(x) \in F_p(x)$, with the following properties:

- $p(\alpha) = 0$
- $deg(p) \leq m$
- If $f(x)$ is another polynomial in $F_p(x)$ with $f(\alpha) = 0$, then $p(x)|f(x)$

The polynomial described in Theorem 2.9 is called the minimal polynomial of α with respect to the

subfield F_p of F.

Example 2.2. If α satisfies equation as follows, $\alpha^2 - 2 = 0$, and the minimal polynomial for α is $x^2 - 2$

$$1 = (0, 1)$$
$$\alpha = (1, 0)$$
$$\alpha^2 = (0, 2)$$

We get the following table of minimal polynomials.

Table 2.2: Table of minimal polynomial

i	α^i	Minimal polynomial
0	(0,1)	$x - 1$
1	(1,0)	$x^2 - 2$
2	(0,2)	$x - 2$
3	(2,0)	$x^2 - 3$
4	(0,4)	$x - 4$
5	(4,0)	$x^2 - 2$
6	(0,3)	$x - 3$
7	(3,0)	$x^2 - 3$

A primitive polynomial is the minimal polynomial of a primitive element of the finite extension field $GF(p^m)$. In other words, a polynomial $F_p[x]$ over $GF(p)$ is a primitive polynomial if its degree is m and it has a root α in $GF(p^m)$ such that $\{0,1,\alpha,\alpha^2,\alpha^3,\dots,\alpha^{p^m-2}\}$ is the entire field $GF(p^m)$. This means also that α is a primitive $(p^m - 1)$-root of unity in $GF(p^m)$.

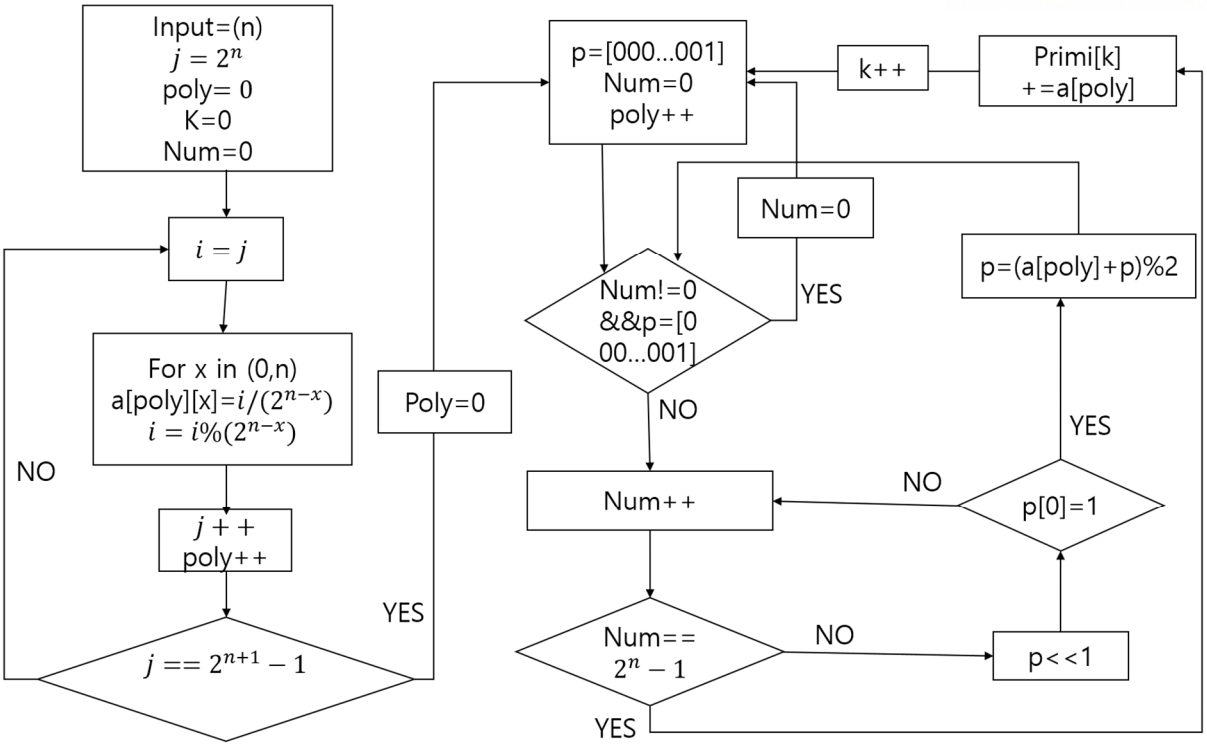


Figure 2.1 : Algorithm of producing coefficient of primitive polynomial

After we decide the number of complexity *n*, we find primitive polynomial using algorithm in Figure 2.1. Because primitive polynomial makes all non-zero elements, we make maximum period in LFSR. In the **Example 2.1**, we construct sequences as 3-tuple.

Example 2.1 Let $p = 2$ and $f(x) = x^3 + x + 1$. Then $f(x)$ is irreducible over $GF(2)$. Let α be a root of $f(x)$; that is, $f(x) = 0$. The finite field $GF(2^3)$ is defined by

$$GF(2^3) = \{a_0 + a_1\alpha + a_2\alpha^2 | a_i \in GF(2)\}$$
$$GF(2^3), \text{defined by } f(x) = x^3 + x + 1 \text{ and } f(\alpha) = 0$$

Table 2.3: Polynomial Table of Example 2.1

As a 3-tuple	As a polynomial	As a Power of α
000	0	$= 0$
100	1	$= 1$
010	α	$= \alpha$
001	α^2	$= \alpha^2$
110	$1 + \alpha$	$= \alpha^3$
011	$\alpha + \alpha^2$	$= \alpha^4$
111	$1 + \alpha + \alpha^2$	$= \alpha^5$
101	$1 + \alpha^2$	$= \alpha^6$
$\alpha^7 = 1$		

2.4 Frequency Hopping Systems

Frequency-hopping spread spectrum (FHSS) is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver Figure 2.2. It is used as a multiple access method in the code division multiple access (CDMA) scheme frequency-hopping code division multiple access (FH-CDMA).

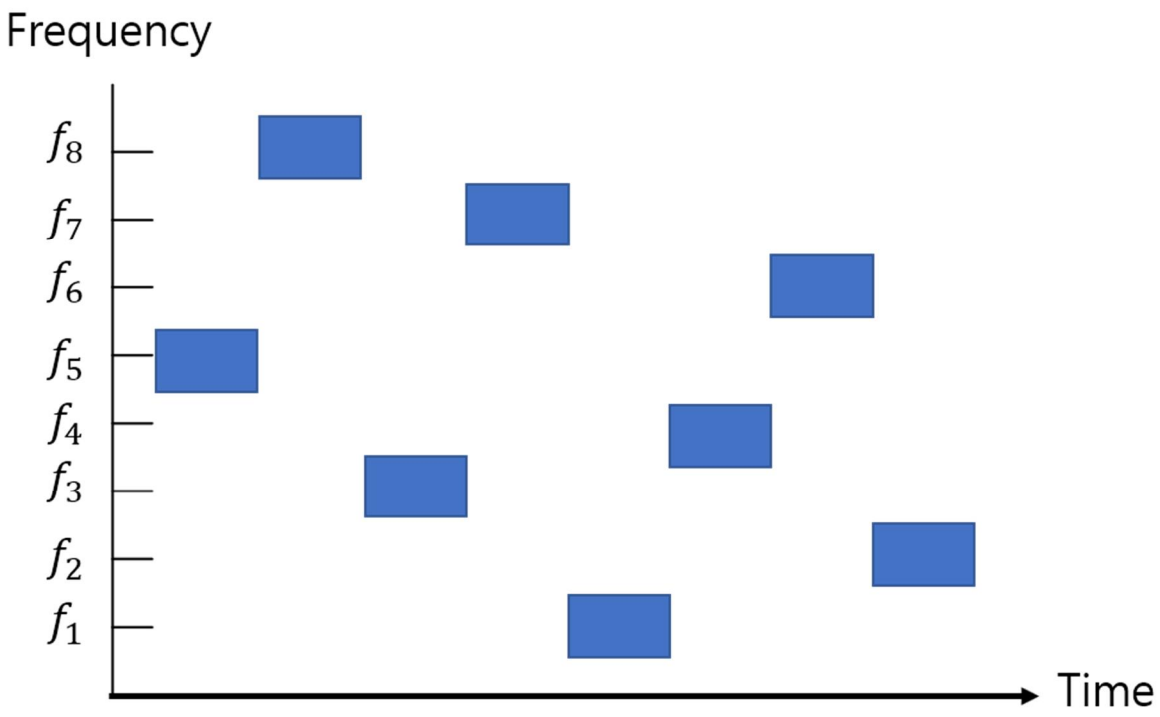


Figure 2.2 Frequency Hopping

Each available frequency band is divided into sub-frequencies. Signals rapidly change (”hop”) among these in a predetermined order. Interference at a specific frequency will only affect the signal during that short interval.

A sub-type of FHSS used in Bluetooth wireless data transfer is adaptive frequency-hopping spread spectrum (AFH).

Adaptive Frequency-hopping spread spectrum (AFH) (as used in Bluetooth) improves resistance to radio frequency interference by avoiding crowded frequencies in the hopping sequence. This sort of adaptive transmission is easier to implement with FHSS than with DSSS.

The key idea behind AFH is to use only the good frequencies, by avoiding the ”bad” frequency channels perhaps those ”bad” frequency channels are experiencing frequency selective fading, or

perhaps some third party is trying to communicate on those bands or perhaps those bands are being actively jammed. Therefore, AFH should be complemented by a mechanism for detecting good/bad channels.

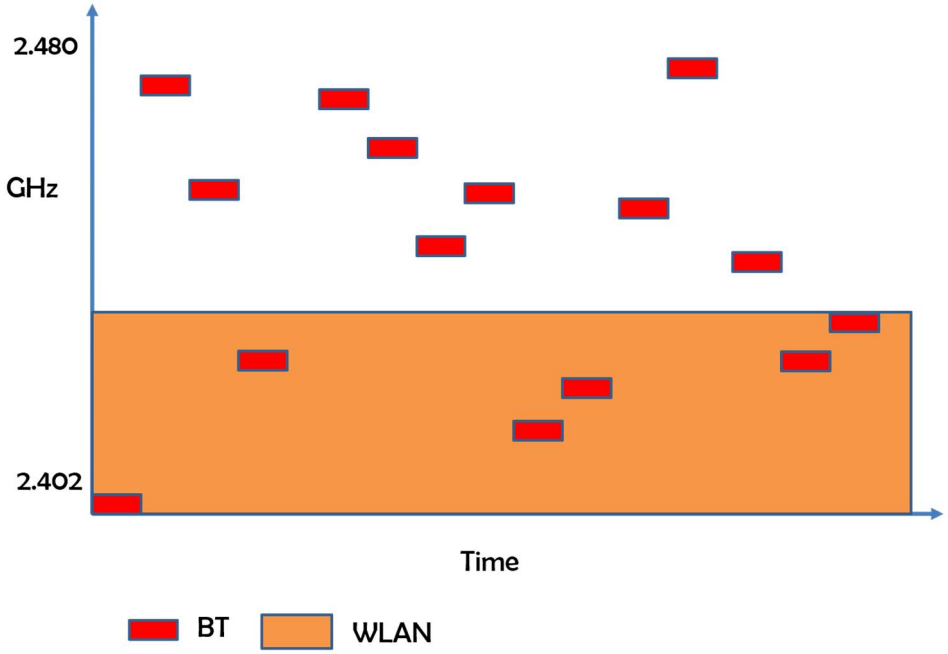


Figure 2.3 Without AFH

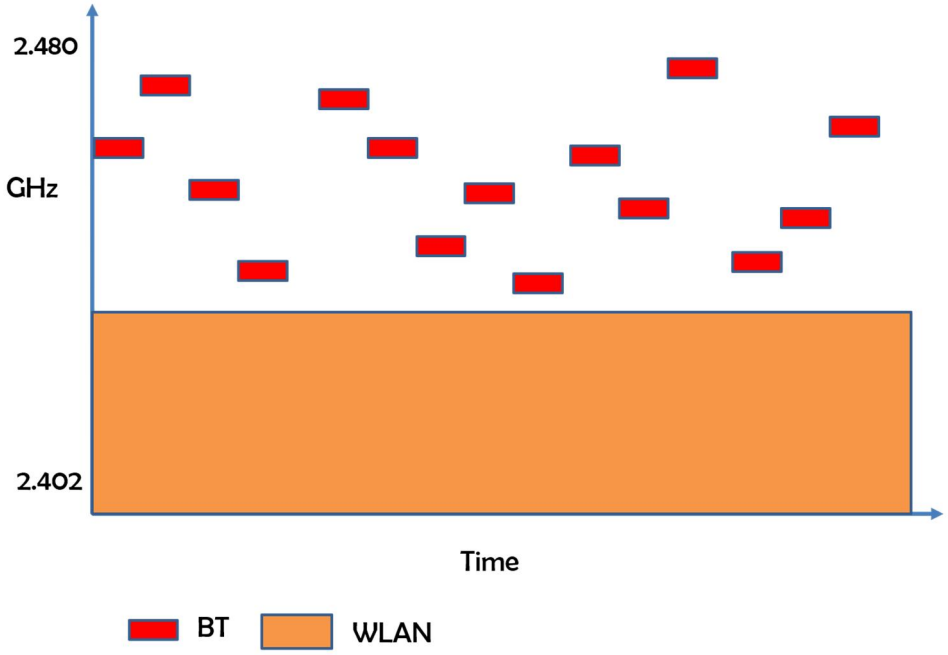


Figure 2.4 With AFH

However, if the radio frequency interference is itself dynamic, then the strategy of bad channel removal, applied in AFH might not work well. For example, if there are several co-located frequency-

hopping networks (as Bluetooth Piconet), then they are mutually interfering and the strategy of AFH fails to avoid this interference.

2.5 Multiple frequency-shift keying

The modulation most commonly used with spread-spectrum technique is *M*-ary frequency shift keying (MFSK), where $k = log_2 M$ which information bits are used to determine which one of M frequencies is to be transmitted. The position of the *M*-ary signal set is mapped pseudo-randomly by the LFSR over a hopping bandwidth W_{ss}. A typical FH/MFSK system block diagram is shown in Figure 2.5.

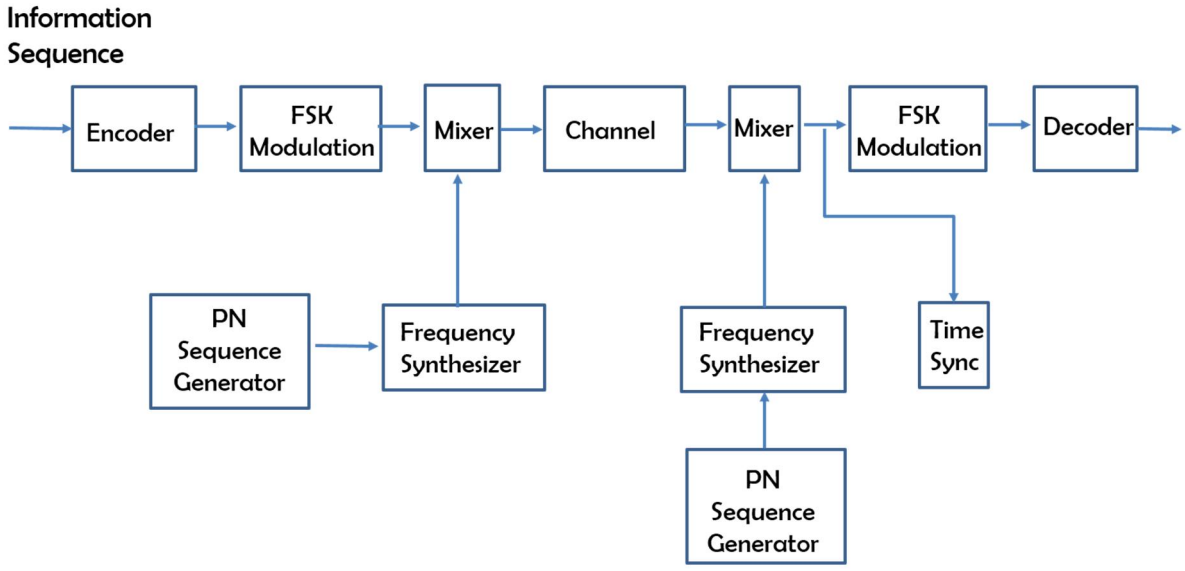


Figure 2.5 Mapping of Frequency Hopping Sequence

In a conventional MFSK system, the data symbol modulates a fixed frequency carrier. In the case of an FH/MFSK system, the data symbol modulates a carrier frequency which is pseudo-randomly determined by LFSR. In either case, a one frequency is transmitted. At each frequency hop time, an output sequence of PN generator feeds the frequency synthesizer a frequency word (a sequence of l chips), which dictates one of 2^l symbol-set. We denote the frequency-hopping bandwidth W_{ss}, and the minimum frequency spacing between each hopping position Δf.

For a given system, the occupied frequency bandwidth is identical to the bandwidth of conventional MFSK, which is typically much smaller than W_{ss}. The FH/MFSK spectrum occupies the entire

spread-spectrum bandwidth. Since frequency hopping techniques work over such wide bandwidths, it is difficult to maintain phase coherence from hop to hop. Therefore, such systems usually use non-coherent demodulation. Nevertheless, consideration has been given to coherent FH in [33].

In Figure 2.5, we know that the receiver is the reverse of the signal processing of the transmitter. The received signal is first FH demodulated (dehopped) by XOR it with the same sequence of pseudo-randomly selected frequency which was used for hopping. Then the dehopped signal is applied to a conventional bank of *M* non-coherent energy detectors to select the most likely symbol.

In the Figure 2.6, there is an example of Frequency-hopping. A dashed line f_0 is a center frequency which is not fixed and changed according to tone.

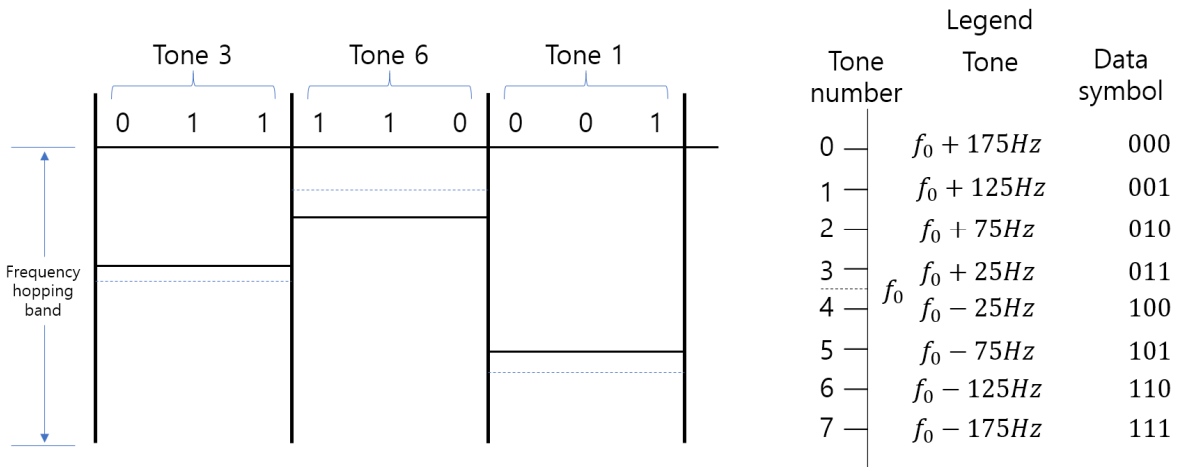


Figure 2.6 Frequency-hopping example using 8-ary FSK modulation

2.6 Properties of Frequency Hopping

Robustness is a signal's ability to resist own information from the channel, such as noise, jamming, fading, and so on. A signal with multiple duplicate, each transmitted on a different frequency, has a greater probability of correct than the one which transmitted on a single frequency with equal power. The greater the diversity (multiple transmissions, at different frequencies, spread in time), the more robust the signal against random interference, i.e. noise, fading, etc.

The following example clarify what is diversity. Consider a message consisting of four symbols: s_1, s_2, s_3, s_4. The introduction of diversity starts with repeating the message *N* times. Let us choose $N = 8$. Then, the repeated symbols, called chips, can be written as follows.

$$s_1s_1s_1s_1s_1s_1s_1s_1s_2s_2s_2s_2s_2s_2s_2s_2s_3s_3s_3s_3s_3s_3s_3s_3s_4s_4s_4s_4s_4s_4s_4s_4$$

Each chip is mapped to a different hopping frequency (the center frequency of the data bandwidth is changed for each chip). The resulting transmissions at frequencies $f_i, f_j, f_k, \ldots$ yield a more robust signal than without such diversity. A target-shooting analogy is that a pellet from a barrage of shotgun pellets has a better chance of hitting a target, compared with the action of a single bullet.

In Figure 2.7 we extend the example illustrated in Figure 2.6, with the additional feature of a chip repeat factor of *N = 4*. During each 20-ms symbol interval, there are now four columns, corresponding to the four separate chips to be transmitted for each symbol. At the top of the figure we see the same data sequence, with $R = 150$ bps, as in the earlier example; and we see the same 3-bit partitioning to form the 8-ary symbols. Each symbol is transmitted four times, and for each transmission the center frequency of the data band is hopped to a new region of the hopping band, under the control of a PN code generator. Therefore, for this example, each chip interval, T_c is equal to $T/N = 20ms/4 = 5ms$ in duration, and the hopping rate is now

$$\frac{NR}{log_2 8} = \frac{200hops}{s}.$$

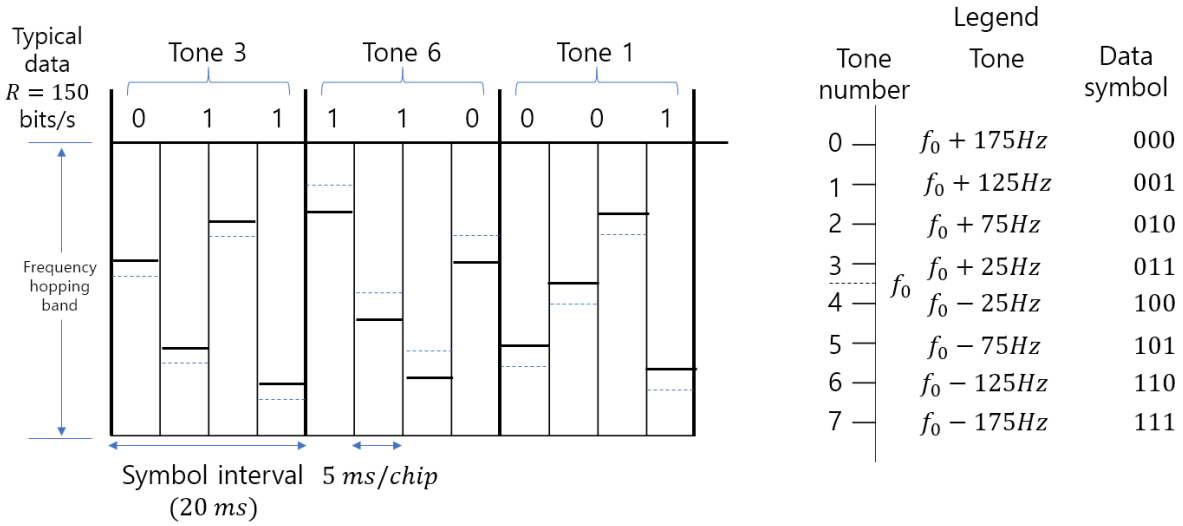


Figure 2.7 Frequency-hopping example with diversity $(\boldsymbol{N = 4})$

Notice that the spacing between frequency tones must change to meet the changed requirement for orthogonality. Since the duration of each FSK tone is now equal to the chip duration, that is, $T_c = T/N$, the minimum separation between tones is $1/Tc = N/T = 200Hz$. As in the earlier example, Figure 2.7 illustrates that the center of the data band is shifted at each new chip time. The position of the solid line has the same relationship to the dashed line for each of the chips associated with a given symbol.

In the case of direct-sequence spread-spectrum systems, the term ”chip” refers to the PN (Pseudo-random Number) code symbol (the symbol of shortest duration in a DS system). In a similar sense for frequency hopping systems, the term ”chip” is used to characterize the shortest uninterrupted waveform in the system. Frequency hopping systems are classified as slow-frequency hopping (SFH), which means there are several modulation symbols per hop, or as fast-frequency hopping (FFH), which means that there are several frequency hops per modulation symbol. For SFH, the shortest uninterrupted waveform in the system is that of the data symbol; however, for FFH, the shortest uninterrupted waveform is that of the hop.

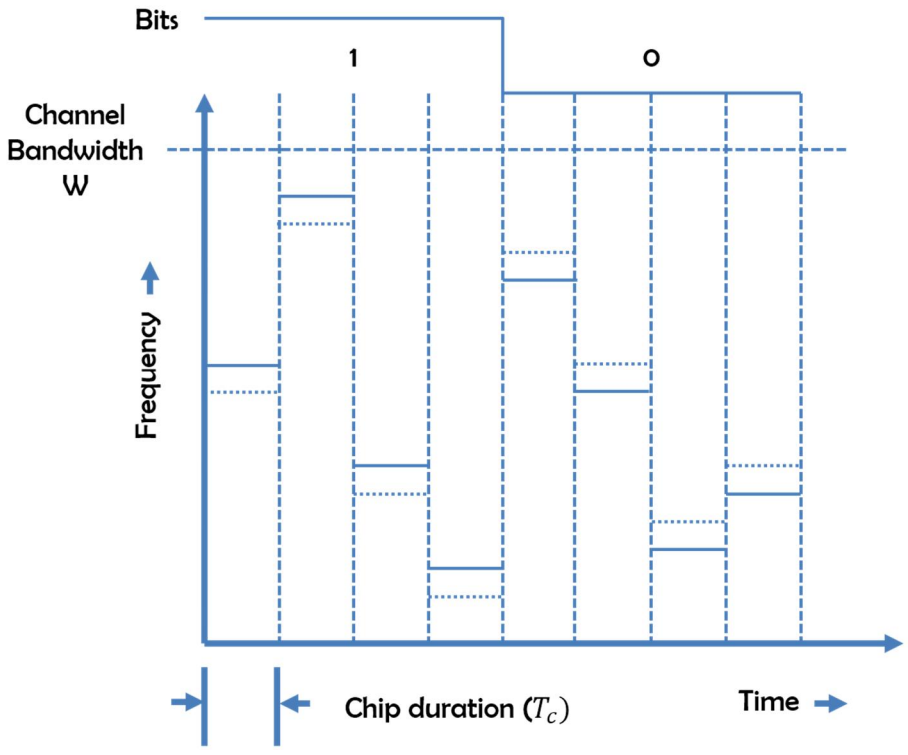


Figure 2.8 Fast hopping

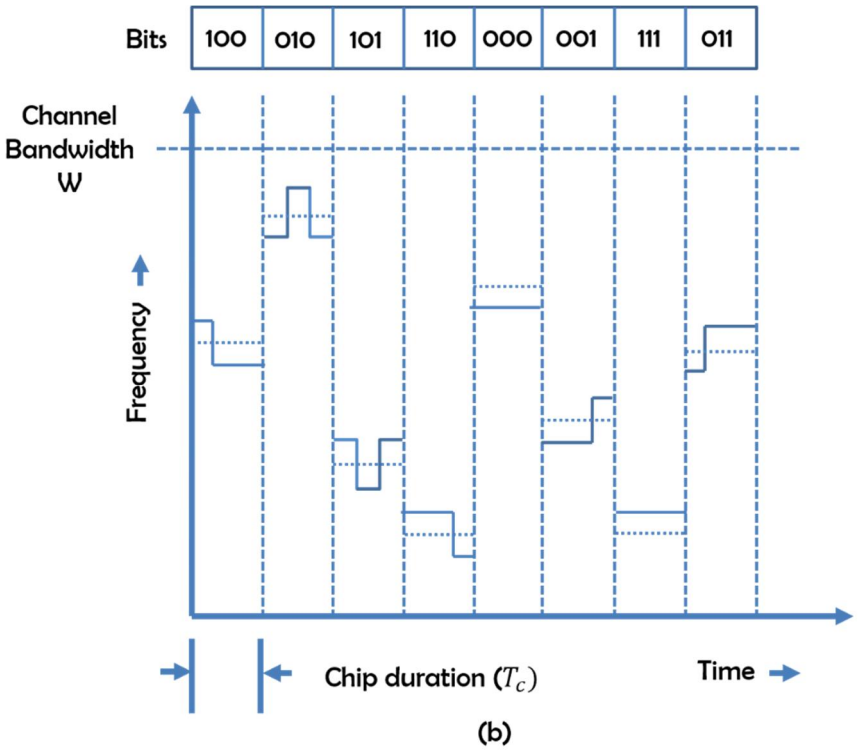


Figure 2.9 Slow hopping

Figure 2.8 illustrates an FFH example of a binary FSK system. The diversity is $N = 4$. There are 4 chips transmitted per bit. As in Figure 2.7, the dashed line in each column corresponds to the center of the data band and the solid line corresponds to the symbol frequency. Here, for FFH, the chip duration is the hop duration. Figure 2.9 illustrates an example of an SFH binary FSK system. In this case, there are 3 bits transmitted during the time duration of a single hop. Here, for SFH, the chip duration is the bit duration. If this SFH example were changed from a binary system to an 8-ary system, what would then be the same, and the chip duration, the hop duration, and the symbol duration would be the same.

2.7 DS/CDMA

In Direct Sequence spread spectrum transmission, the user data signal is multiplied by a code sequence. Mostly, binary sequences are used. The duration of an element in the code is called the ”chip time”. The ratio between the user symbol time and the chip time is called the spread factor. The transmit signal occupies a bandwidth that equals the spread factor times the bandwidth of the user data.

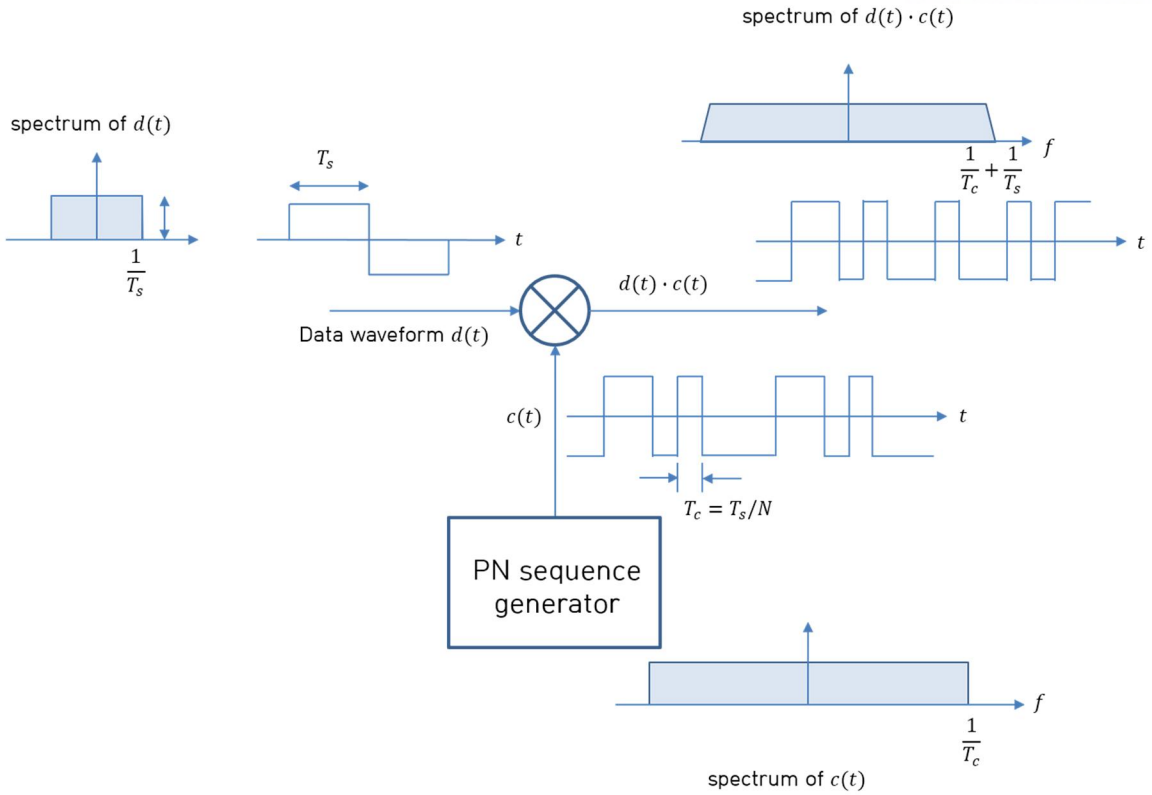


Figure 2.10 Scheme of DS/CDMA

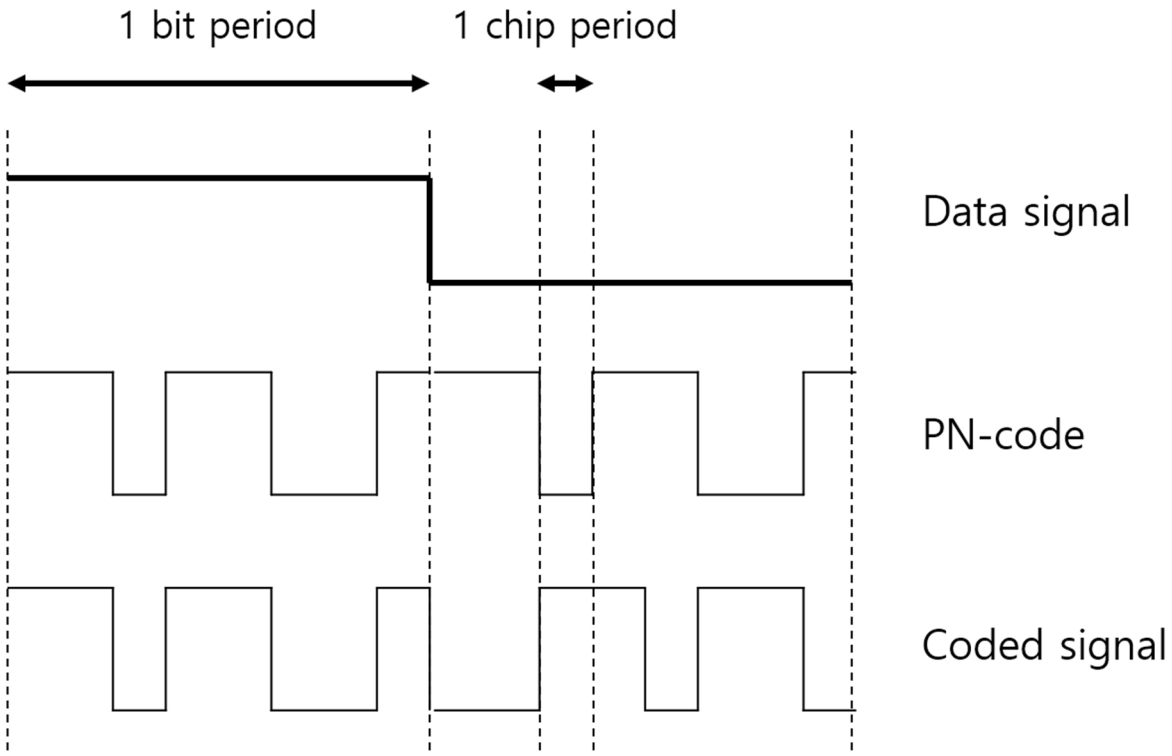


Figure 2.11 Sequence for DS

Ⅲ. Frequency Hopping Sequence

We discussed a kind of properties and preliminaries in Chapter 1 and Chapter 2. In Chapter 3, we introduce frequency hopping sequence and table of FHS constructions. Moreover, we discuss some methods of constructing FHSs over $\mathbb{Z}_{p^k}$ with k-tuples of sequences over $\mathbb{Z}_p$.

Frequency-hopping sequences (FHSs) are widely used in frequency-hopping multiple access (FHMA) systems such as Bluetooth, secure, military or radar applications, and so on [1]-[6]. For an FHMA system, interference caused by other signal is unavoidable, when two users occupy the same frequency. To reduce such multiple-access interferences (hits), an FHS set with low correlation is required. There exist several algebraic and combinatorial constructions of optimal FHS sets [7]-[23] with respect to the Lempel-Greenberger bound [3] and the Peng-Fan bound [6].

Interleaving techniques are used to construct a sequence of length kN from k sequences of length N, which are not necessarily distinct for some positive integers k and N. They are classified into two types. One employs the Chinese Remainder Theorem (CRT) [44], [45], and the other uses the concept of column sequences [46], [47]. They have been widely applied to construction of sequences with good correlation (but, not Hamming correlation) [44], [47], [48], [45], [49], [50] as well as to construction of complementary sequences [46], [51].

In next section, we investigate minimal polynomial used for LFSR.

3.1 Sequence with minimal polynomial over finite field

We discussed a kind of properties and preliminaries in Chapter 1 and Chapter 2. In Chapter 3, we introduce frequency hopping sequence and table of FHS constructions. Moreover, we discuss some methods of constructing FHSs over $\mathbb{Z}_{p^k}$ with k-tuples of sequences over $\mathbb{Z}_p$.

Frequency-hopping sequences (FHSs) are widely used in frequency-hopping multiple access (FHMA) systems such as Bluetooth, secure, military or radar applications, and so on [1]-[6]. For an FHMA system, interference caused by other signal is unavoidable, when two users occupy the same frequency. To reduce such multiple-access interferences (hits), an FHS set with low correlation is required. There exist several algebraic and combinatorial constructions of optimal FHS sets [7]-[23] with respect to the Lempel-Greenberger bound [3] and the Peng-Fan bound [6].

Interleaving techniques are used to construct a sequence of length kN from k sequences of length

N, which are not necessarily distinct for some positive integers k and N. They are classified into two types. One employs the Chinese Remainder Theorem (CRT) [44], [45], and the other uses the concept of column sequences [46], [47]. They have been widely applied to construction of sequences with good correlation (but, not Hamming correlation) [44], [47], [48], [45], [49], [50] as well as to construction of complementary sequences [46], [51].

In next section, we investigate minimal polynomial used for LFSR.

3.2 A fast algorithm for complexity of binary sequence with period 2^n

In the case that N is power of 2, we could know complexity of LFSR with the number of $logN$. The algorithm is as follows.

This condition makes fast to choose a complexity. However, as we reduce time to confirm period, it could be more dangerous. Eavesdropper could know complexity of LFSR, if he or she knows only x steps.

In this case, $c(s) \leq N$. In general, $\mathrm{c(s)}$ can be determined using an algorithm developed by Massey [43]. In the case that N is a power of 2, the complexity can be determined in $logN$ steps using a much simpler algorithm presented in this correspondence. Let $a = (a_0, a_1, \dots, a_{N-1})$ be a vector of length $N = 2n,\ n > 0$.

$$L(\boldsymbol{a}) = (a_0, a_1, \dots, a_{N/2-1})$$
$$R(\boldsymbol{a}) = (a_{N/2}, a_{N/2+1}, \dots, a_{N-1}).$$

and write $\boldsymbol{a} = (L(\boldsymbol{a})|R(\boldsymbol{a}))$

$$s_i + \sum_{k=1}^{r} c_k s_{i-k} = 0\,, \qquad i \geq r.$$

$$\left(E^r + \sum_{k=1}^{r} c_k E^{r-k}\right) s_{i-r} = 0, \qquad i \geq r$$

where E is the shift operator; that is, $Es_i = s_{i+1}$.

For a given sequence of arbitrary period N, the Massey algorithm [43] accepts the sequence sequentially and at each stage computes the connection polynomial for the shortest LFSR that generates the encountered portion of the sequence. The Massey algorithm may have to run through more than one period of length N of the sequence before it stabilizes on the correct connection polynomial. In practice, additional iterations are required to ensure that the algorithm has in fact stabilized. The algorithm given in this correspondence works only for a sequence with period of length $N = 2^n$ and computes the complexity c in $logN = n$ steps. The connection polynomial $f(E)$ then must be $(E-1)^c$ in this case. The storage requirements of the Massey algorithm depend directly on the eventual complexity of the sequence, while the present algorithm must always store a single period of the sequence, making the algorithm inappropriate for very long periods.

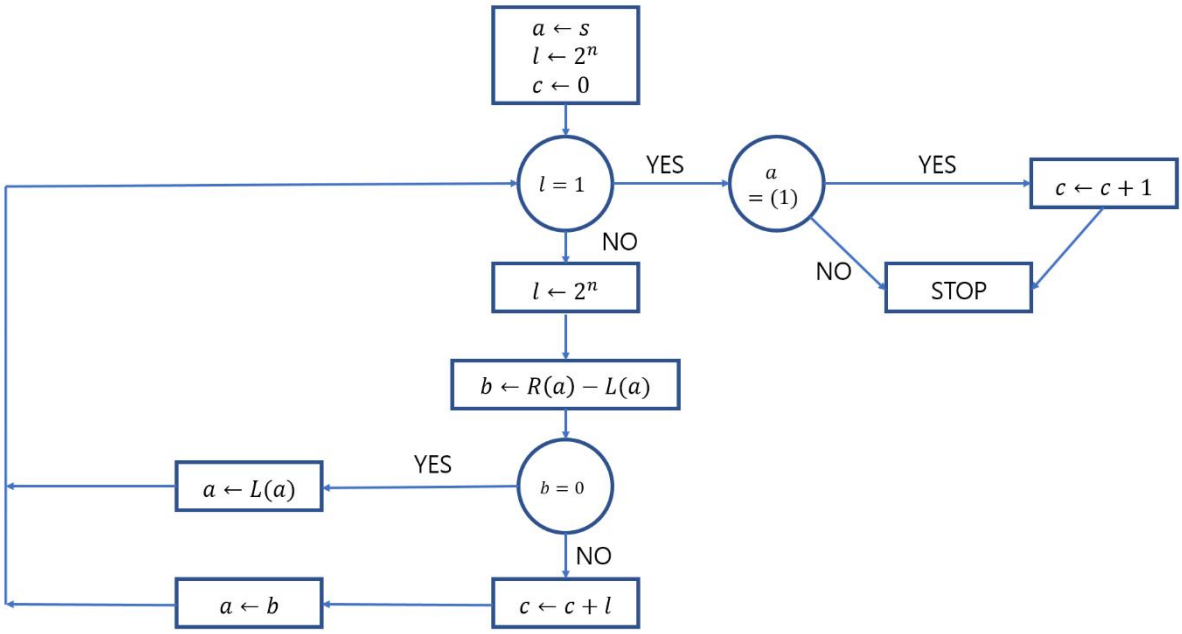


Figure 3. 1 The flowchart of the algorithm

3.3 Correlation and Bound

Let $\mathcal{F} = \{f_1, f_2, \ldots, f_n\}$ be a set of frequencies. For two FHSs X and Y of length L over $\mathcal{F}$, the $periodic\ Hamming\ correlation$ between X and Y is defined as

$$H_{X,Y}(\tau) = \sum_{t=0}^{L-1} h[X(t), Y(\langle t+\tau \rangle_L)], \qquad 0 \le \tau \le L-1 \tag{3.4}$$

where

$$h[x,y] = \begin{cases} 1, & \text{if } x = y \\ 0, & \text{otherwise} \end{cases}$$

and $\langle x \rangle_L$ is x modulo L. When $X = Y$, $H_{X,Y}(\tau)$ is called the $Hamming\ autocorrelation$, $H_X(\tau)$.

Let $\mathcal{S}$ be the set of all FHSs of length L over $\mathcal{F}$. For an FHS X in $\mathcal{S}$, let

$$H(X) = \max_{1 \le \tau \le L-1} \{H_X(\tau)\}.$$

For any two distinct FHSs X and Y in $\mathcal{S}$, let

$$H(X,Y) = \max_{0 \le \tau \le L-1} \{H_{X,Y}(\tau)\}.$$

An FHS $X \in \mathcal{S}$ is said to be optimal if $H(X) \le H(X')$ for all $X' \in \mathcal{S}$ [3]. The following lemma is well-known as the $Lempel - Greenburger\ bound$.

Lemma 3.4 [3]: For any FHS X of length L over $\mathcal{F}$ with $|\mathcal{F}| = M$

$$H(X) \ge \left\lceil \frac{(L-b)(L+b-M)}{M(L-1)} \right\rceil$$

where $b = \langle L \rangle_M$, $\lceil x \rceil$ be the smallest number bigger than or equal to x.

Let $\mathcal{U}$ be a subset of $\mathcal{S}$. The $maximum\ out-of-phase\ Hamming-autocorrelation$ $H_a(\mathcal{U})$ and the $maximum\ Hamming\ crosscorrelation$ $H_c(\mathcal{U})$ of $\mathcal{U}$ are defined as

$$H_a(\mathcal{U}) = \max_{X \in \mathcal{U}} \{H(X)\}$$
$$H_c(\mathcal{U}) = \max_{X,Y \in \mathcal{U}, X \ne Y} \{H(X,Y)\}.$$

Moreover, the $maximum\ Hamming\ correlation$ of $\mathcal{U}$ is denoted by

$$H(\mathcal{U}) = \max\{H_a(\mathcal{U}), H_c(\mathcal{U})\}.$$

Note that τ corresponds to time delay in practical situations. Thus, $H_a(\mathcal{U})$ and $H_c(\mathcal{U})$ are important measures for multiple-access interference. To minimize such interference, it is required to design an FHS set with low $H_a(\mathcal{U})$ and $H_c(\mathcal{U})$. Therefore, we need to minimize $H_a(\mathcal{U})$ and $H_c(\mathcal{U})$.

When we have $H(\mathcal{U}) = \lambda$, $|\mathcal{F}| = M$, length=L and $|\mathcal{U}| = N$, we use a notation for an FHS set $\mathcal{U}$, subset of $\mathcal{S}$, as an $(L, M, \lambda; N)$-FHS set. Peng and Fan established a bound on the $H_a(\mathcal{U})$ and $H_c(\mathcal{U})$ with parameters of an FHS [6].

Lemma 3.5 ([6]): Let a subset $\mathcal{U}$ be an $(L, M, \lambda; N)$-FHS set and $K = \lfloor NL/M \rfloor$. Then

$$M(L-1)H_a(\mathcal{U}) + LM(N-1)H_c(\mathcal{U}) \geq L(LN - M)$$
$$N(L-1)H_a(\mathcal{U}) + LM(N-1)H_c(\mathcal{U}) \geq 2KLN - LM(K+1).$$

We call $\mathcal{U}$, an FHS set, optimal if $H(\mathcal{U})$ achieves one of the bounds in Lemma 3.5, that is, $\mathcal{U}$ is optimal with respect to the Peng–Fan bound.

3.4 Optimal Frequency-Hopping Sequences

In this section, we introduce a method to construct FHSs. There are some kinds of construction method which are interleaving techniques, for some positive integers k and N covered in [53].

Moreover, we construct FHS sets with FHSs. There are some kinds of construction method which are interleaving using a priory constructed FHS, and method in Table 3.2[52].

Construction A1: Consider an $(L, M, \lambda; N)$-FHS set $\mathcal{V} = \{V_l | 0 \leq l \leq L-1\}$, where $V_l = \{V_l(t)\}_{t=0}^{N-1}$. For an integer $k, 1 \leq k \leq L$, which is relatively prime to N, we define the FHS set $\mathcal{Q}_{\mathrm{k}}(\mathcal{V}) = \{R_i | 0 \leq i \leq \lfloor L/k \rfloor - 1\}$, where $Q_i = \{Q_i(t)\}_{t=0}^{kN-1}$ is the FHS of length kN, given by

$$\mathrm{Q_i}(t) \coloneqq Q_i(t_0, t_1) = V_{ki+t_0}(t_1), \qquad 0 \leq t \leq kN-1.$$

The above interleaved construction is based on the information that any integer x in $\mathbb{Z}_{kN}$ can be uniquely represented as $(x)_k$ and $(x)_N$ when k and N are relatively prime. On the other hand, the following interleaved construction can be applied even when k and N are not relatively prime.

Table 3.1: Optimal (kN, N, k)-FHSs

Subcases of Constructions B1 and B2		Constructions in [53]	
(kN, N, k)	Constrains	(kN, N, k)	Constrains
(2N, N, 2)	$N \geq 2$	-	-
(3N, N, 3)	$N \equiv 1{,}5 \mod 6$ and $N \geq 5$	$(3N, N, 3)$	$N \equiv 1 \mod 6$ or $N \geq 3$ is prime.
(kp, p, k)	p is prime and any integer k, $2 \leq k \leq p-1$.	$(4p, p, 4)$	$p = 12f + 1$ is prime and f is odd
		$(5p, p, 5)$	$p > 15$ is prime.
		$(7p, p, 7)$	$p = 42f + 1$ is prime
		(p_1p_2, p_2, p_1)	p_1, p_2 are primes and $p_1 < p_2$
$(k(2^m - 1), 2^m - 1, k)$	$k = 3$ or 4, and m is odd	-	-

Table 3.2: Optimal FHS Sets with Respect to the Lempel-Green and Peng-Fan Bound

Parameters		Optimality	
$(L, M, \lambda; N)$	Constrains	L-G bound	P-F bound
$\left(k\frac{q^m-1}{d}, q, k\frac{q^{m-1}-1}{d}; \left\lfloor\frac{d}{f}\right\rfloor\right)$	$d \mid q-1$, $gcd\left(\frac{q^m-1}{q-1}, d\right) = 1$, and $2 \leq k \leq d$	optimal	optimal
$(kp^2, p, kp; \left\lfloor\frac{p}{k}\right\rfloor)$	$2 \leq k \leq p$	optimal	optimal
$(2p, M, 2f+1; M/2)$	$p = Mf + 1, M \geq 4$, and f is odd	near optimal	optimal
$(kp, p, k; \left\lfloor\frac{p-1}{k}\right\rfloor)$	$2 \leq k \leq p-1$	optimal	optimal

Construction A2: Consider an $(L, M, \lambda; N)$-FHS set $\mathcal{V} = \{V_l | 0 \leq l \leq L-1\}$, where $V_l = \{V_l(t)\}_{t=0}^{N-1}$. For an integer $k, 1 \leq k \leq L$, we define the FHS set $\mathcal{R}_k(\mathcal{V}) = \{R_i | 0 \leq i \leq \lfloor L/k \rfloor - 1\}$, where $R_i = \{R_i(t)\}_{t=0}^{kN-1}$ t=0 } is the FHS of length kN, given by

$$R_i(t) \coloneqq V_{ki+(t)_k}(\lfloor t/k \rfloor), \qquad 0 \leq t \leq kN-1.$$

In the following propositions and corollaries, we calculate the Hamming correlation between two FHSs of FHS set in Construction A1 or A2. Moreover, we derive an upper bound on their maximum Hamming correlation.

Proposition 3.6: Let *k* and *N* be positive integers such that $gcd(k, N) = 1$. Let $X = \{X(t)\}_{t=0}^{kN-1}$ and $Y = \{Y(t)\}_{t=0}^{kN-1}$ be two FHSs of length *kN* obtained from Construction A1. The Hamming correlation $H_{X,Y}(\tau)$ between *X* and *Y* is given by

$$H_{X,Y}(\tau) \coloneqq H_{X,Y}(\tau_0, \tau_1) = \sum_{t_0=0}^{k-1} \sum_{t_1=0}^{N-1} h[X(t_0, t_1), Y((t_0 + \tau_0)_k, (t_1 + \tau_1)_N)] \quad (3.5)$$

where $x_0 = (x)_k$ and $x_1 = (x)_N$ for any integer $x, 0 \le x \le kN - 1$.

Corollary 3.7: The FHS set $\mathcal{Q}_k(\mathcal{V})$ in Construction A1 satisfies

$$H\left(\mathcal{Q}_k(\mathcal{V})\right) \le k\lambda.$$

Proof. Because Hamming correlation of FHSs is defined in equation 3.4, the maximum of inner sum in equation 3.5 is λ. Therefore, it is bounded by $k\lambda$.

Proposition 3.8: Let k and N be positive integers. Let $X = \{X(t)\}_{t=0}^{kN-1}$ and $Y = \{Y(t)\}_{t=0}^{kN-1}$ be two FHSs of length kN obtained from Construction A2. The Hamming correlation $H_{X,Y}(\tau)$ between X and Y is given by

$$H_{X,Y}(\tau) \coloneqq H_{X,Y}(k\tau_0, \tau_1) = \sum_{t_0=0}^{k-1} \sum_{t_1=0}^{N-1} h\left[X(kt_1 + t_0), Y\left(k\left(t_1 + \tau_1 + \left\lfloor \frac{t_0 + \tau_0}{k} \right\rfloor\right) + (t_0 + \tau_0)_k\right)\right] \quad (3.5)$$

where $t = kt_1 + t_0$ such that $0 \le t_0 \le k - 1$ and $0 \le t_1 \le N - 1$ for any integer $t, 0 \le t \le kN - 1$.

Corollary 3.9: The FHS set $\mathcal{R}_k(\mathcal{V})$ in Construction A2 satisfies

$$H\left(\mathcal{R}_k(\mathcal{V})\right) \le k\lambda.$$

Proof. Similar to the Proof of Corollary 3.7

3.5 BlueBee (BLE and Zigbee)

Cross-Technology Communication is a promising solution proposed recently to the coexistence problem of heterogeneous wireless technologies in the ISM bands. The existing works use only the coarse-grained packet-level information for cross-technology modulation, suffering from a low throughput (e.g., 10bps). Our approach, called BlueBee, proposes a new direction by emulating legitimate Zig- Bee frames using a Bluetooth radio. Uniquely, BlueBee achieves dual-standard compliance and transparency by selecting only the payload of Bluetooth frames, requiring neither hardware nor firmware changes at the Bluetooth senders and ZigBee receivers.[34]

3.6 BlueBee design

Key point of BlueBee is as follows.

1. BLE Transmitter: BLE uses Gaussian Frequency Shift Keying (GFSK) modulation, which is normally realized by phase shift over time. Note that a frequency shift keying $s(t) = Acos(2\pi(f \pm \Delta f)t)$ is equivalent to a phase shift keying of $s(t) = Acos(2\pi ft \pm \Phi(t))$, where $\Phi(t) = 2\pi\Delta ft$.

2. ZigBee Receiver: BlueBee enables BLE to transmit emulated ZigBee packets which can be demodulated by any commodity ZigBee device through the standard Offset Quadrature Phase Shift Keying (OQPSK) demodulation procedure.

3. The narrower bandwidth of BLE (1MHz) compared to ZigBee (2MHz).

4. BlueBee enables BLE to transmit emulated ZigBee packets which can be demodulated by any commodity ZigBee device through the standard Offset Quadrature Phase Shift Keying (OQPSK) demodulation procedure.

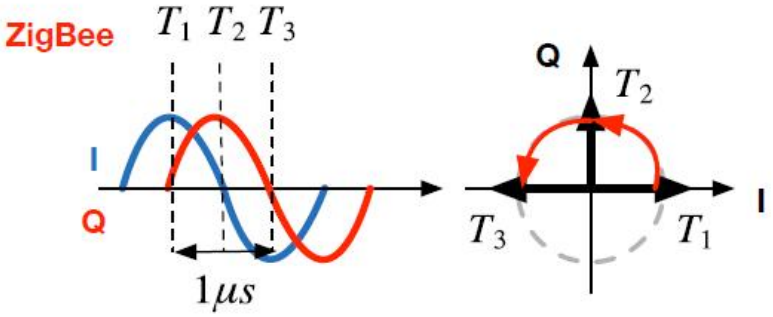
5. Finally, 32 ZigBee chips are mapped to a ZigBee symbol, by looking up a symbol-to-chip mapping table (Table 3.1) predefined in DSSS. There are 16 different symbols where each represents $\log_2 16 = 4$ bits

Table 3.3: Symbol-to-chip mapping in ZigBee (802.15.4)

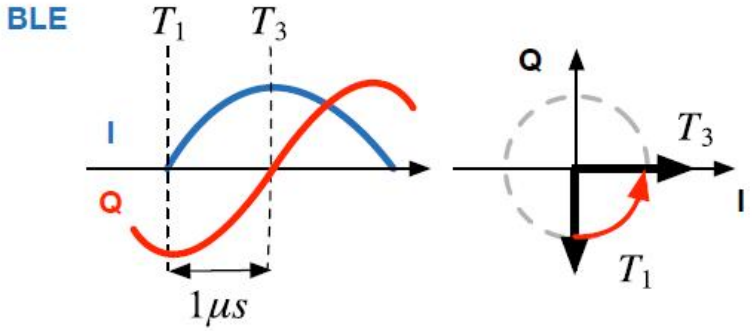
Symbol (4 bits)	Chip Sequence (32 bits)
0000	11011001110000110101001000101110
0001	11101101100111000011010100100010
...	…
1111	11001001011000000111011110111000

3.7 GFSK and OQPSK

As mentioned in key point of BlueBee, the difference is bandwidth in Figure 3.4. The time duration of ZigBee is 0.5us, and the one of BLE is 1us. Because of the difference of these sampling frequency, the signal '1' is translated into '11' in ZigBee. Then, we map 'Chip Sequence' in Table 3.3 to shortest binary sequence that consists of '11' and '00'. As a result, the sequences consisting of '00' and '11' are matched to sequence in Table 3.3, and it is translated to symbol. These sequence makes that different module can communicate each other.



(a) ZigBee signal with two chips, '11'.



(b) Emulation of (a) by BLE

Figure 3.2 Signal of two modulations

IV. One-Coincidence Frequency Hopping Sequence

4.1 Definition of OC-FHS

A one-coincidence FHS (OC-FHS) set consists of FHSs whose maximum Hamming autocorrelation is 0 and maximum Hamming cross-correlation is 1. They possess the following properties [24]-[32]:

1. All the sequences are of the same length.
2. All the sequences are non-repeating, that is, each frequency is used at most once within one sequence period.
3. The maximum number of hits between any pair of sequences for any time shift equals one.

4.2 New Construction of OC-FHS Sets

An OC-FHS set is defined as follows.

Definition 4.1. [26] An OC-FHS set $\mathcal{U}$ is a set of non-repeating FHSs for which $H_a(\mathcal{U}) = 0$ and $H_c(\mathcal{U}) = 1$. Clearly, any OC-FHS set is optimal with respect to the Peng-Fan bound.

When N is a prime, there is a primitive element β in $\mathbb{Z}_N$ such that $\mathbb{Z}_N\backslash\{0\} = \{\beta^0, \beta^1, \dots, \beta^{N-2}\}$. We will design an OC-FHS of length $p^2 - p$ over $\mathbb{Z}_{p^2}$ by using a primitive element β of $\mathbb{Z}_p$.

Construction A: For $0 \le t \le p(p-1) - 1$, let $t_0 = \langle t \rangle_{p-1}$ and $t_1 = \langle t \rangle_p$. Define an FHS $X_i \triangleq \{X_i(t)\}_{t=0}^{p^2-p-1}$ over $\mathbb{Z}_{p^2}$ as

$$X_i(t) = \langle \beta^{t_0} + i \rangle_p p + \left\langle \langle t_0 + 1 \rangle_p t_1 \right\rangle_p$$

where β is a primitive element of $\mathbb{Z}_p$. Then, construct an FHS set as

$$\mathcal{O} = \{X_i | 0 \le i \le N - 1\}.$$

4.3 Calculation of Hamming Correlation Values

In this section, the Hamming correlation values of $\mathcal{O}$ in Construction A will be calculated in order to show that $\mathcal{O}$ is an OC-FHS set.

***Theorem* 4.2** The set $\mathcal{O}$ in Construction A satisfies

$$H_a(\mathcal{O}) = 0 \quad \text{and} \quad H_c(\mathcal{O}) = 1.$$

Moreover, $\mathcal{O}$ is an $(p^2 - p, p^2, 1; p)$-FHS set which is optimal with respect to the Peng-Fan bound.

Proof. Clearly, the set size of $\mathcal{O}$ is p. Let $\tau_0 = \langle \tau \rangle_{p-1}$ and $\tau_1 = \langle \tau \rangle_p$. For $\tau \neq 0$, the Hamming autocorrelation $H_i(\tau)$ of X_i is given by

$$\begin{aligned} H_i(\tau) &= H_i(\tau_0, \tau_1) \\ &= \sum_{t_0=0}^{p-2} \sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} + i \rangle_p p + \langle (t_0+1)t_1 \rangle_p, \langle \beta^{t_0+\tau_0} + i \rangle_p p + \left\langle \left(\langle t_0 + \tau_0 \rangle_{p-1} + 1\right)(\tau_1 + t_1) \right\rangle_p\right] \\ &= \sum_{t_0=0}^{p-2} \sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} + i - \beta^{t_0+\tau_0} - i \rangle_p p, \left\langle \left(\langle t_0 + \tau_0 \rangle_{p-1} + 1\right)(\tau_1 + t_1) - (t_0+1)t_1 \right\rangle_p\right] \\ &= \sum_{t_0=0}^{p-2} \sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} - \beta^{t_0+\tau_0} \rangle_p p, \left\langle \left(\langle t_0 + \tau_0 \rangle_{p-1} + 1\right)\tau_1 + \tau_0 t_1 \right\rangle_p\right]. \end{aligned}$$

Case 1-1) $\tau_0 = 0$ and $\tau_1 \neq 0$: We have

$$H_i(\tau) = \sum_{t_0=0}^{p-2} \sum_{t_1=0}^{p-1} h\left[0, \left\langle \left(\langle t_0 + \tau_0 \rangle_{p-1} + 1\right)\tau_1 \right\rangle_p\right].$$

Since $\left\langle \langle t_0 + 1 \rangle_p \tau_1 \right\rangle_p \neq 0$ and $\tau_1 \neq 0$, we obtain

$$H_i(\tau) = 0.$$

Case 1-2) $\tau_0 \neq 0$ and $\tau_1 = 0$: Note that $p \leq \langle \beta^{t_0} - \beta^{t_0+\tau_0} \rangle_p p \leq p^2 - p$ and $0 \leq \langle \tau_0 t_1 \rangle_p < p$. Thus,

$$H_i(\tau) = 0.$$

Case 1-3) $\tau_0 \neq 0$ and $\tau_1 \neq 0$: Since $p \leq \langle \beta^{t_0} - \beta^{t_0+\tau_0} \rangle_p p \leq p^2 - p$ and $0 \leq \left\langle \left(\langle t_0 + \tau_0 \rangle_{p-1} + 1 \right) \tau_1 + \tau_0 t_1 \right\rangle_p < p$. We obtain

(1)

$$H_i(\tau) = 0.$$

By summarizing the results of Cases 1-1), 1-2), and 1-3), we have

$$H_a(\mathcal{O}) = 0.$$

For $i \neq j$, the Hamming cross correlation $H_{i,j}(\tau)$ between X_i and X_j is written as

$$H_{i,j}(\tau) = \sum_{t_0=0}^{p-2} \sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} + i \rangle_p p + \langle (t_0+1) t_1 \rangle_p, \langle \beta^{t_0+\tau_0} + j \rangle_p p + \left\langle \left(\langle t_0 + \tau_0 \rangle_{p-1} + 1 \right) (\tau_1 + t_1) \right\rangle_p \right].$$

Case 2-1) $\tau = 0$ and $i \neq j$: In this case,

$$\begin{aligned} H_{i,j}(\tau) &= \sum_{t_0=0}^{p-2} \sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} + i \rangle_p p + \langle (t_0+1) t_1 \rangle_p, \langle \beta^{t_0} + j \rangle_p p + \left\langle \langle t_0 + 1 \rangle_p t_1 \right\rangle_p \right] \\ &= \sum_{t_0=0}^{p-2} \sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} + i - \beta^{t_0} - j \rangle_p p, \left\langle \langle t_0 + 1 \rangle_p t_1 - \langle t_0 + 1 \rangle_p t_1 \right\rangle_p \right] \\ &= \sum_{t_0=0}^{p-2} \sum_{t_1=0}^{p-1} h\left[\langle i - j \rangle_p p, 0 \right] \end{aligned}$$

For $i \neq j$,

$$H_{i,j}(\tau) = 0.$$

Case 2-2) $\tau_0 = 0, \tau_1 \neq 0$ and $i \neq j$: We have

$$\begin{aligned} H_{i,j}(\tau) &= \sum_{t_0=0}^{p-2}\sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} + i\rangle_p p + \langle (t_0+1)t_1\rangle_p, \langle \beta^{t_0} + j\rangle_p p + \langle (t_0+1)(t_1+\tau_1)\rangle_p\right] \\ &= \sum_{t_0=0}^{p-2}\sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} - \beta^{t_0} + i - j\rangle_p p, \langle (t_0+1)(t_1+\tau_1) - (t_0+1)t_1\rangle_p\right] \\ &= \sum_{t_0=0}^{p-2}\sum_{t_1=0}^{p-1} h\left[\langle i-j\rangle_p p, \langle (t_0+1)\tau_1\rangle_p\right]. \end{aligned}$$

Since $p^2 - p \geq \langle i-j\rangle_p p \geq p$ and $p > \langle (t_0+1)\tau_1\rangle_p > 0$,

$$H_{i,j}(\tau) = 0.$$

Case 2-3) $\tau_0 \neq 0, \tau_1 = 0$ and $i \neq j$: We have

$$\begin{aligned} H_{i,j}(\tau) &= \sum_{t_0=0}^{p-2}\sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} + i\rangle_p p + \langle (t_0+1)t_1\rangle_p, \langle \beta^{t_0+\tau_0} + j\rangle_p p + \left\langle \left(\langle t_0+\tau_0\rangle_{p-1} + 1\right)t_1\right\rangle_p\right] \\ &= \sum_{t_0=0}^{p-2}\sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} - \beta^{t_0+\tau_0} + i - j\rangle_p p, \left\langle \left(\langle t_0+\tau_0\rangle_{p-1} + 1\right)t_1 - (t_0+1)t_1\right\rangle_p\right] \\ &= \sum_{t_0=0}^{p-2}\sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} - \beta^{t_0+\tau_0} + i - j\rangle_p p, \left\langle \left(\langle t_0+\tau_0\rangle_{p-1} - t_0\right)t_1\right\rangle_p\right] \\ &= \sum_{t_0=0}^{p-2}\sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} - \beta^{t_0+\tau_0} + i - j\rangle_p p, 0\right] \cdot h\left[\left\langle \left(\langle t_0+\tau_0\rangle_{p-1} - t_0\right)t_1\right\rangle_p, 0\right]. \end{aligned}$$

Only when $t_1 = 0$ and $\beta^{t_0}(1-\beta^{\tau_0}) = j - i$, we have $\langle \beta^{t_0} - \beta^{t_0+\tau_0} + i - j\rangle_p p = 0$ and $\left\langle \left(\langle t_0+\tau_0\rangle_{p-1} - t_0\right)t_1\right\rangle_p = 0$. Therefore,

$$H_{i,j}(\tau) = 1.$$

Case 2-4) $\tau_0 \neq 0, \tau_1 \neq 0$ and $i \neq j$:

$$H_{i,j}(\tau) = \sum_{t_0=0}^{p-2}\sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} - \beta^{t_0+\tau_0} + i - j\rangle_p p, \left\langle \left(\langle t_0+\tau_0\rangle_{p-1} + 1\right)(t_1+\tau_1) - (t_0+1)t_1\right\rangle_p\right]$$

$$= \sum_{t_0=0}^{p-2} \sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} - \beta^{t_0+\tau_0} + i - j\rangle_p p, \left\langle \left(\langle t_0 + \tau_0\rangle_{p-1} - t_0\right)t_1 + \left(\langle t_0 + \tau_0\rangle_{p-1} + 1\right)\tau_1 \right\rangle_p\right]$$

$$= \sum_{t_0=0}^{p-2} \sum_{t_1=0}^{p-1} h\left[\langle \beta^{t_0} - \beta^{t_0+\tau_0} + i - j\rangle_p p, 0\right]$$

$$\cdot\, h\left[\left\langle \left(\langle t_0 + \tau_0\rangle_{p-1} - t_0\right)t_1 + \left(\langle t_0 + \tau_0\rangle_{p-1} + 1\right)\tau_1 \right\rangle_p, 0\right].$$

There exists exactly one pair of t_0 and t_1 satisfying $\langle \beta^{t_0} - \beta^{t_0+\tau_0} + i - j\rangle_p p = 0$ and $\left\langle \left(\langle t_0 + \tau_0\rangle_{p-1} - t_0\right)t_1 + \left(\langle t_0 + \tau_0\rangle_{p-1} + 1\right)\tau_1 \right\rangle_p = 0$. Consequently,

$$H_{i,j}(\tau) = 1.$$

Summarizing the results of Cases 2-1), 2-2), 2-3) and 2-4), we obtain

$$H_c(\mathcal{O}) = 1.$$

It is obvious that $\mathcal{O}$ is optimal with respect to the Peng-Fan bound

According to Theorem 4.2, the set $\mathcal{O}$ in Construction A is an OC-FHS set of length $p^2 - p$. Furthermore, the Hamming cross-correlation value for each τ is exactly 1 except for the case $\tau_0 = 0$.

Example 4.1: Let $p = 5$ and $\beta = 2$ in Construction A. Then FHS $X_i \triangleq \{X_i(t)\}_{t=0}^{t=19}$ for $0 \le i \le 4$ is written as $X_i(t) = \langle 2^{t_0} + i\rangle_5 5 + \langle\langle t_0 + 1\rangle_5 t_1\rangle_5$ where $\mathrm{t}_0 = \langle t\rangle_4$ and $\mathrm{t}_1 = \langle t\rangle_5$. Consequently, the FHS set $\mathcal{X} \triangleq \{X_0, X_1, \ldots, X_4\}$ of period 20 over $\mathbb{Z}_{25}$ is given by

$$\{\mathrm{X}_0(t)\}_{t=0}^{19} = \{5,12,21,17,9,10,23,18,8,13,20,19,7,11,22,15,6,14,24,16\},$$
$$\{\mathrm{X}_1(t)\}_{t=0}^{19} = \{10,17,1,22,14,15,3,23,13,18,0,24,12,16,2,20,11,19,4,21\},$$
$$\{\mathrm{X}_2(t)\}_{t=0}^{19} = \{15,22,6,2,19,20,8,3,18,23,5,4,17,21,7,0,16,24,9,1\},$$
$$\{\mathrm{X}_3(t)\}_{t=0}^{19} = \{20,2,11,7,24,0,13,8,23,3,10,9,22,1,12,5,21,4,14,6\},$$
$$\{\mathrm{X}_4(t)\}_{t=0}^{19} = \{0,7,16,12,4,5,18,13,3,8,15,14,2,6,17,10,1,9,19,11\}.$$

It is easily checked that the $H_c(\mathcal{X}) = 1$ and $H_a(\mathcal{X}) = 0$.

Table 4.1: Table of correlation

i, j	0	1	2	3	4
0	0	1	1	1	1
1	1	0	1	1	1
2	1	1	0	1	1
3	1	1	1	0	1
4	1	1	1	1	0

4.4 Separating of Sequence

If we have a good SNR, we could reduce time period and increase the number of sequences. From Example 4.1, we change time period, t, and the number of sequences, i.

Example 4.2: $X_i \triangleq X_i(t)_{t=0}^{9}$ for $0 \le i \le 9$ is written by $X_i(t) = \langle 2^{t_0} + i \rangle_5 5 + \langle \langle t_0 + 1 \rangle_5 t_1 \rangle_5$ where $\mathrm{t}_0 = \langle t \rangle_4$ and $\mathrm{t}_1 = \langle t \rangle_5$. Consequently, the FHS set $\mathcal{X} \triangleq \{X_0, X_1, \dots, X_8, X_9\}$ of period 10 over $\mathbb{Z}_{25}$ is given by

$$
\begin{aligned}
\{\mathrm{X}_0(t)\}_{t=0}^{9} &= \{12, 17, 10, 18, 13, 19, 11, 15, 14, 16\} \\
\{\mathrm{X}_1(t)\}_{t=0}^{9} &= \{17, 22, 15, 23, 18, 24, 16, 20, 19, 21\}, \\
\{\mathrm{X}_2(t)\}_{t=0}^{9} &= \{22, 2, 20, 3, 23, 4, 21, 0, 24, 1\}, \\
\{\mathrm{X}_3(t)\}_{t=0}^{9} &= \{2, 7, 0, 8, 3, 9, 1, 5, 4, 6\}, \\
\{\mathrm{X}_4(t)\}_{t=0}^{9} &= \{7, 12, 5, 13, 8, 14, 6, 10, 9, 11\}, \\
\{\mathrm{X}_5(t)\}_{t=0}^{9} &= \{5, 21, 9, 23, 8, 20, 7, 22, 6, 24\}, \\
\{\mathrm{X}_6(t)\}_{t=0}^{9} &= \{10, 1, 14, 3, 13, 0, 12, 2, 11, 4\}, \\
\{\mathrm{X}_7(t)\}_{t=0}^{9} &= \{15, 6, 19, 8, 18, 5, 17, 7, 16, 9\}, \\
\{\mathrm{X}_8(t)\}_{t=0}^{9} &= \{20, 11, 24, 13, 23, 10, 22, 12, 21, 14\}, \\
\{\mathrm{X}_9(t)\}_{t=0}^{9} &= \{0, 16, 4, 18, 3, 15, 2, 17, 1, 19\}.
\end{aligned}
$$

Conclusions

Through this thesis, we studied finite field, primitive element, minimal polynomial, multiple frequency-shift keying, DS/CDMA, BlueBee, which is used for many applications, frequency hopping sequence, One-Coincidence frequency-hopping sequence. Moreover, we investigated a new construction of OC-FHSs.

FHMA is widely used in modern communication systems such as Bluetooth, ultrawideband (UWB), military, etc. For these systems, it is desirable to employ frequency-hopping sequences (FHSs) having low Hamming correlation in order to reduce the multiple-access interference.

In general, optimal FHSs with respect to the Lempel-Greenberger bound do not always exist for all lengths and frequency set sizes. Therefore, it is an important problem to verify whether an optimal FHS with respect to the Lempel-Greenberger bound exists or not for a given length and a given frequency set size.

Therefore, we constructed a new OC-FHS set of length $p^2 - p$ over $\mathbb{Z}_{p^2}$ by using a primitive element of $\mathbb{Z}_p$. The new OC-FHS set with $H_a(X) = 0$ and $H_c(X) = 1$ can be applied to several recent applications using ISM band (e.g. IoT) based on BLE and Zigbee. In order to prove the optimality of FHSs, all cases of Hamming autocorrelation and Hamming cross-correlation are mathematically calculated.

Moreover, in order to raise data rate or the number of users, a new method is presented. Using this method, sequences are divided into two times of length and satisfies Lempel-Greenberger bound and Peng-Fan bound.

REFERENCES

1. Specification of the Bluetooth Systems-Core. The Bluetooth Special Interest Group (SIG). [Online]. Available: http://www.bluetooth.com

2. Wi-Fi and Bluetooth - Interference Issues. [Online]. Available: http://www.hp.com

3. A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming correlation properties," *IEEE Trans. Inf. Theory*, vol. 20, no. 1, pp. 90–94, Jan. 1974.

4. D. V. Sarwate, "Reed-Solomon codes and the design of sequences for spread spectrum multiple-access communications," *Reed-Solomon Codes and Their Applications*, S. B. Wicker and V. K. Bhargava, Eds. Piscataway, NJ: IEEE Press, 1994.

5. M. K. Simon, J. K. Omura, R. A. Scholtz, B. K. Levitt, *Spread Spectrum Communications Handbook*, revised ed. New York: McGraw-Hill, 1994.

6. 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, Sept., pp. 2149– 2154, 2004.

7. P. V. Kumar, "Frequency-hopping code sequence designs having large linear span," *IEEE Trans. Inf. Theory*, vol. 34, no. 1, pp. 146–151, Jan. 1988.

8. P. Udaya and M. U. Siddiqi, "Optimal large linear complexity frequency hopping patterns derived from polynomials residue class rings," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1492–1503, July. 1998.

9. R. Fuji-Hara, Y. Miao, and M. Mishima, "Optimal frequency hopping sequences: a combinatorial approach," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2408–2420, Oct. 2004.

10. 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.

11. G. Ge, R. Fuji-Hara, and Y. Miao, "Further combinatorial constructions for optimal frequency hopping sequences," *J. Combin. Theory, Ser. A*, vol. 113, pp. 1699–1718, 2006.

12. C. Ding, M. J. Miosio, and J. Yuan, "Algebraic constructions of optimal frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2606–2610, Jul. 2007.

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

14. C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo, and M. Mishima, "Sets of frequency hopping sequences: bounds and optimal constructions," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3297–3304, Jul. 2009.

15. J. H. Chung, Y. K. Han, and K. Yang, "New classes of optimal frequency-hopping sequences by interleaving techniques," *IEEE Trans. Inf. Theory*, vol. 45, no. 12, pp. 5783–5791, Dec. 2009.

16. G. Ge, Y. Miao, and Z. Yao, "Optimal frequency hopping sequences: auto- and cross-correlation properties," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 867–879, Feb. 2009.

17. 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.

18. Y. Yang, X. Tang, P. Udaya, and D. Y. Peng, "New bound on frequency hopping sequence sets and its optimal constructions," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7605–7613, Nov. 2011.

19. Z. Zhou, X. Tang, X. Niu, and U. Parampalli, "New classes of frequency-hopping sequences with optimal partial correlation," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 453–458, Jan. 2012.

20. X. Zeng, H. Cai, X. Tang, and Y. Yang, "A class of optimal frequency hopping sequences with new parameters," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4899– 4907, Jul. 2012.

21. J.-H. Chung, G. Gong, and K. Yang, "New families of optimal frequency-hopping sequences of composite lengths," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3688– 3697, Jun. 2014.

22. H. Cai, Y. Yang, Z. Zhou, and X. Tang, "Strictly optimal frequency-hopping sequence sets with optimal family sizes," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 1087–1093, Feb. 2016.

23. J. Bao and L. Ji, "New families of optimal frequency hopping sequence sets," *IEEE Trans. Inf. Theory*, vol. 62, no. 9, pp. 5209–5224, Sep. 2016.

24. I. S. Reed, "*k*th-order near-orthogonal codes," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 116–117, Jan. 1971.

25. G. Solomon, "Optimal frequency hopping for multiple access," in *Proc. Symp. Spread Spectrum Commun*, San Diego, CA, pp. 13-16, Mar. 1977.

26. G. R. Cooper and R. W. Nettleton, "A spread spectrum technique for high capacity mobile communications," *IEEE Trans. Veh. Technol.*, vol. VT-27, pp. 264-275, NOV. 1978.

27. E. L. Titlebaum, "Time-frequency hop signals Part I: Coding based upon the theory of linear congruences," *IEEE Trans. Aerospace Electron. Syst.*, vol. AES-17, no. 4, pp. 490-493, Jul. 1981.

28. A. A. Shaar and P. A. Davies, "Prime sequences: Quasi-optimal sequences for OR channel code division multiplexing," *Electron. Lett.*, vol. 19, no. 21, pp. 888-890, 1983.

29. A. A. Shaar and P.A. Davies, "A survey of one-coincidence sequences for frequencyhopped spread spectrum systems," *IEE Proc*, vol. 131, no.7, pp.719- 726, Dec. 1984.

30. P. Fan and M. Darnell, "Sequence Design for Communications Applications." New York, 1996.

31. Z. Cao, G. Ge, and Y. Miao, "Combinatorial characterizations of one-coincidence frequency-hopping sequences", *Des. Codes Crypt.*, vol. 41, no. 2, pp. 177-184, Nov. 2006.

32. A. A. Shaar and L. Fukshansky, "A new family of one-coincidence sets of sequences with dispersed elements for frequency hopping cdma systems", Jan. 2017. [Online]. Available https://arxiv.org/abs/1701.05209.

33. M. K. Simon and A. Polydoros, "Coherent detection of frequency-hopped quadrature modulations in the presence of jamming-Part I: QPSK and QASK; Part II: QPR class I modulation," *IEEE Trans.Commun*., vol. 29, pp. 1644-1660, Nov. 1981.

34. W. Jiang, Z Yin, R Liu, "BlueBee: a 10,000x Faster Cross-Technology Communication via PHY Emulation," in *Proc. of ACM SenSys*, 2017.

35. ETSI/SAGE Specification: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 1: UEA2 and UIA2 Specification" [Online]. Available: http://www.3gpp.org

36. T. W. Cusick, P Stanica, *Cryptographic Boolean functions and applications*. New York: Academic, 2009.

37. M. Bellare and P. Rogaway, "Introduction to modern cryptography." 2005, Available at: http://www-cse.ucsd.edu/~mihir/cse207/ classnotes.html.

38. D. Chakraborty, F. Rodriguez-Henriquez, "Block Cipher Modes of Operation from a Hardware Implementation Perspective," *Cryptographic Engineering*, C.K. Koc, ed., pp. 321-363, Springer, 2009.

39. J. Katz, A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*. Boca Raton, FL: CRC Press, 1997.

40. L. Hathaway, *National policy on the use of the advanced encryption standard (AES) to protect national security systems and national security information*. National Security Agency, 2003.

41. E. L. Key, "An analysis on the structure and complexity of non-linear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 732-736, Nov. 1976.

42. S. W. Golomb, *Shift Register Sequences*. Laguna Hills, CA, USA: Aegean Park Press, 1982.

43. J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122-1127, Jan. 1969

44. C. Ding, T. Helleseth, and H. M. Martinsen, "New families of binary sequences with optimal three-level autocorrelation," *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 428433, Jan. 2001.

45. V. P. Ipatov, "Contribution to the theory of sequences with perfect periodic autocorrelation properties," *Radio Eng. Electron. Phys*., vol. 25, pp. 31-34, Apr. 1980.

46. M. J. E. Golay, "Complementary series," *IEEE Trans. Inf. Theory*, vol. IT-7, pp. 82-87, Apr. 1961.

47. G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Trans. Inf. Theory*, vol. 41, pp. 400-411, Mar. 1995.

48. G. Gong, "New designs for signal sets with low cross correlation, balance property, and large linear span: $\mathbf{GF}(p)$ case," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2847-2867, Nov. 2002.

49. P. Udaya and M. U. Siddiqi, "Optimal biphase sequences with large linear complexity derived from sequences over Z_4," *IEEE Trans. Inf. Theory*, vol. 42, no. 1, pp. 206-216, Jan. 1996.

50. Z. Zhou, X. H. Tang, and G. Gong, "A new class of sequences with zero or low correlation zone based on interleaving technique," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4267-4273, Sep. 2008.

51. C. C. Tseng and C. L. Liu, "Complementary sets of sequences," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 5, pp. 644-652, Sep. 1972.

52. J. H. Chung, Y. K. Han, and K. Yang, "New classes of optimal frequency-hopping sequences by interleaving techniques," *IEEE Trans. Inf. Theory*, vol. 45, no. 12, pp. 5783-5791, Dec. 2009.

53. R. Fuji-Hara, Y. Miao, and M. Mishima, "Optimal frequency hopping sequences: A combinatorial approach," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2408-2420, Oct. 2004.