論 文

A NEW FAMILY OF FREQUENCY HOPPING PATTERNS WITH GOOD HAMMING AUTOCORRELATION AND CROSSCORRELATION

Jong-Seon No* *Regular Member*

우수한 해밍 자기상관성 및 타 상관성을 갖는 새로운 주파수 도약 패턴 군

正會員 盧 宗 善*

ABSTRACT

New family of frequency hopping patterns with long period and good Hamming autocorrelation and Hamming crosscorrelation properties which can be used for frequency hopped multiple access communication systems is introduced. Period of frequency hopping patterns is q^k-1, the alphabet size of frequency hoppng patterns is q, and the size of family of frequency hopping patterns is q, where k is arbitrary integer and q is power of prime number. The maximum value of out-of-phase Hamming autocorrelation function of any frequency hopping pattern and Hamming crosscorrelation function of any two frequency hopping patterns in the family is q^{k-1}, which corresponds to optimal Hamming correlation properties. And the average number of hits per $q \times q$ square in one frequency hopping pattern and its time shifted version or two frequency hopping patterns in the frequency hopped multiple access communication systems is less than 1.

要 約

주파수 도약 다원접속 통신시스템에 사용될 수 있는 우수한 해밍자기상관성 및 타 상관성 그리고 긴주기를 갖는 새로운 주파수 도약 패턴군이 소개되었다. 주파수 도약 패턴군의 주기는 q^k-1, 알파벳 크기는 q, 주파수 도약 패턴군의 크기는 q인데, 여기서 k는 임의의 양의정수 그리고 q는 소수의 정수승이다. 자기상관함수 및 타 상관함수의 최대값은 q^{k-1}(trivial경우 제외)인데 이것은 최적의 해밍 상관함수에 해당된다. 그리고 주파수 도약 패턴에 있어서 $q \times q$ 스퀘어당 평균 충돌의수는 1보다 작다.

*建國大學校 電子工學科
Dept. of Elec. Eng., Kon-Kuk Univ.
論文番號 : 93-175

Ⅰ. Introduction

In the frequency hopped multiple access communication systems, family of frequency hopping patterns with good Hamming autocorrelation and good Hamming crosscorrelation properties is needed. Lots of work has been done for searching the family of frequency hopping patterns with good Hamming autocorrelation and good Hamming crosscorrelation properties [1, 2, 3, 4].

In this paper, new family of frequency hopping patterns with optimal Hamming correlation properties generated by using m-sequences with alphabet size q is presented. The period of frequency hopping patterns is q^k-1, their alphabet sizes are q, and the size of family of frequency hopping patterns is q, where k is arbitrary integer and q is power of prime number. The maximum value of out-of-phase Hamming autocorrelation function of any frequency hopping patterns and Hamming crosscorrelation function of any two frequency hopping patterns in the family is q^{k-1}, which corresponds to optimal Hamming correlation properties in terms of lower bound derived by Lempel and Greenberger [4]. The number of hits per $q\times q$ square in the multiple access environment of one frequency hopping pattern and its time shifted version or two frequency hopping patterns is less than 1. Therefore, the Hamming correlation properties of new family of frequency hopping patterns in terms of maximum value of Hamming correlation function and number of hits per $q\times q$ square is almost the same as those of ideal matrices.

Ⅱ. Construction of Frequency Hopping Patterns

We can construct a family of frequency hopping patterns with period q^k-1 and alphabet size q which have the optimal Hamming correlation properties in terms of lower bound derived by Lempel and Greenberger [4], by using m-sequences with alphabet size q.

Let $s(t)$ be an m-sequence with period q^k-1 over the finite field, $GF(q)$ [5, 6, 8],

$$s(t)=tr_q^{q^k}(\alpha^t), \tag{1}$$

where q is a power of prime number p, p^m, and α and β are primitive elements of $GF(q^k)$ and $GF(q)$, respectively and trace function is defined as [7]

$$tr_q^{q^k}(x)=\sum_{i=1}^{k-1}x^{q^i}. \tag{2}$$

Then the family of frequency hopping patterns is defined as follows :

DEFINITION 1 : The family of frequency hopping patterns with period $N=q^k-1$ and alphabet size q is given by

$$S=\{s(t),\ s(t)+\beta^0,\ s(t)+\beta^1,\ s(t)+\beta^2,\cdots,\ s(t)+\beta^{q-2}\}$$
$$=\{s_i(t)\mid i=-\infty,\ 0,\ 1,\ 2,\cdots,q-2\}, \tag{3}$$

where for $i=-\infty,\ 0,\ 1,\ 2,\cdots,q-2$,

$$s_i(t)=s(t)+\beta^i,\ \beta^{-\infty}=0 \tag{4}$$

and the size of family of frequency hopping patterns is given by

$$|S|=q. \tag{5}$$

The values which are taken by $s_i(t)$ are the elements of $GF(q)$, that is, 0 or β^j, $0\le j\le q-2$. The elements of $GF(q)$, where q is a power of prime number p, p^m, can be expressed by p-ary m-tuple vectors and these vectors map into the set of decimal numbers $\{0,\ 1,\ 2,\cdots,q-1\}$, which means the different frequencies in the frequency hopping patterns. In case of $p=2$, that is, $q=2^m$, zero element of $GF(2^m)$ maps into the decimal number 0, which corresponds to frequency f_0 and the other elements of $GF(2^m)$, β^j, map into one of decimal numbers between 1 and $q-1$, which corresponds to the frequency f_j. By this mapping,

the other expression of the family of frequency hopping patterns of period q^k-1 and alphabet, {0, 1, 2,⋯,$q-1$}, i.e., {f_0, f_1, f_2,⋯, f_{q-1}} for frequency hopped multiple access communication systems can be generated.

Ⅲ. Correlation Properties of Frequency Hopping Patterns

In this section, we can consider property of m-sequences with alphabet size q, which will be used in the proof of theorem below. Let $s(t)$ be an m-sequence defined in (1), where p is prime number and $q=p^m$. Then, the characteristic of $GF(q)$ is p. Therefore,

$$\begin{aligned} s(t)-s(t+\tau) &= s(t)-s(t+\tau)+p\cdot s(t+\tau) \\ &= s(t)+(p-1)\cdot s(t+\tau) \\ &= s(t)+s(t+\tau)+(p-2)\cdot s(t+\tau) \end{aligned} \quad (6)$$

and from the shift and add property of m-sequence, the following equation is true.

$$s(t)+s(t+\tau)=s(t+\tau_1). \quad (7)$$

Therefore, (6) can be rewritten in the form

$$s(t)-s(t+\tau)=s(t+\tau_1)+(p-2)\cdot s(t+\tau). \quad (8)$$

Applying (6) and (7) to (8) successively, the following equation can be easily derived.

$$s(t)-s(t+\tau)=s(t+\tau') \quad (9)$$

Next, the definition of Hamming correlation function of the sequences is given as follows [4]. Let $H_s(\tau)$ and $H_{s,r}(\tau)$ be Hamming autocorrelation function of the sequence, $s(t)$, and Hamming crosscorrelation function of the sequences, $s(t)$, $r(t)$, repectively. Then

$$H_s(\tau)=\sum_{t=0}^{N-1} h(s(t), s(t+\tau)), \quad (10)$$

and

$$H_{s,r}(\tau)=\sum_{t=0}^{N-1} h(s(t), r(t+\tau)), \quad (11)$$

where $h(a, b)=\begin{cases} 1, & \text{if } a=b \\ 0, & \text{if } a\neq b \end{cases}$

and the period of sequences, $s(t)$ and $r(t)$, is $N=q^k-1$.

Thus Hamming autocorrelation and crosscorrelation properties of frequency hopping patterns defined in the previous section are given as follows :

THEOREM 1 : Hamming autocorrelation function, $H_{s_i}(\tau)$, of the frequency hopping pattern, $s_i(t)$, in S is given by

$$H_{s_i}(\tau)=\begin{cases} q^{k-1}-1, & \text{if } \tau\neq 0 \ mod\ N \\ q^k-1, & \text{if } \tau=0 \ mod\ N, \end{cases} \quad (12)$$

where N is a period of sequence, $s_i(t)$.

PROOF : For all i and $\tau\neq 0$ *mod* N,

$$\begin{aligned} H_{s_i}(\tau) &= \text{no. of occurrences of } [s_i(t)-s_i(t+\tau)=0] \\ &= \text{no. of occurrences of } [s(t)+\beta^i-s(t+\tau)-\beta^i=0] \\ &= \text{no. of occurrences of } [s(t)-s(t+\tau)=0]. \end{aligned}$$

From (9), the number of occurrences of $[s(t)-s(t+\tau)=0]$ is the number of occurrences of $[s(t+\tau')=0]$. By the balance property of the m-sequences, for $0\le t\le q^k-2$ and all j [6, 8],

no. of occurrences of $[s(t)=\beta^j]=q^{k-1}$, $0\le j\le q-2$

no. of occurrences of $[s(t)=0]=q^{k-1}-1$.

Therefore,

$H_{s_i}(\tau)=q^{k-1}-1$.

Clearly, for $\tau=0$ *mod* N,

$H_{s_i}(\tau)=q^k-1$. *Q.E.D.*

THEOREM 2 : Hamming crosscorrelation function of the frequency hopping patterns, $s_i(t)$ and $s_j(t)$, $i\neq j$, in S is by

$$H_{s_i, s_j}(\tau) = \begin{cases} q^{k-1}, & \text{if } \tau \neq 0 \bmod N \\ 0, & \text{if } \tau = 0 \bmod N. \end{cases} \quad (13)$$

PROOF : Assume that

$$s_i(t) = s(t) + \beta^i$$
$$s_j(t) = s(t) + \beta^j,$$

where $i \neq j$ and β^i can be replaced by zero element of finite field, $GF(q)$.
For $\tau \neq 0 \bmod N$, Hamming crosscorrelation function becomes

$$\begin{aligned} H_{s_i, s_j}(\tau) &= \text{no. of occurrences of } [s_i(t) - s_j(t+\tau) = 0] \\ &= \text{no. of occurrences of } [s(t) + \beta^i - s(t+\tau) - \beta^j = 0] \\ &= \text{no. of occurrences of } [s(t) - s(t+\tau) - \beta^d = 0]. \end{aligned}$$

From (9),

$$\begin{aligned} H_{s_i, s_j}(\tau) &= \text{no. of occurrences of } [s(t+\tau') = \beta^d] \\ &= q^{k-1}, \end{aligned}$$

where

$$\beta^d = \beta^j - \beta^i.$$

For $\tau = 0 \bmod N$, Hamming crosscorrelation function is

$$\begin{aligned} H_{s_i, s_j}(\tau) &= \text{no. of occurrences of } [s_i(t) - s_j(t+\tau) = 0] \\ &= \text{no. of occurrences of } [s(t) + \beta^i - s(t) - \beta^j = 0] \\ &= \text{no. of occurrences of } [\beta^d = 0] \\ &= 0. \end{aligned} \quad (Q.E.D.)$$

From theorem 1 and 2, the maximum values of Hamming autocorrelation function of any frequency hopping pattern and Hamming crosscorrelation function of any two frequency hopping patterns in the family can be rewritten as follows.

THEOREM 3 : Maximum value of out-of-phase Hamming autocorrelation function, $H_{max/a}$, and maximum value of Hamming crosscorrelation function, $H_{max/c}$, in the new family of frequency hopping patterns given as

$$H_{max/a} = q^{k-1} - 1 \quad (14)$$
$$H_{max/c} = q^{k-1}. \quad (15)$$

And the maximum value of Hamming correlation functions in the new family of frequency hopping patterns, H_{max}, is given as

$$\begin{aligned} H_{max} &= MAX\{H_{max/a}, H_{max/c}\} \\ &= q^{k-1}. \end{aligned} \quad (16)$$

From the lower bounds derived by Lempel and Greenberger [4], the lower bounds to the maximum value of out-of-phase Hamming autocorrelation function and the maximum value of Hamming crosscorrelation function for the family of frequency hopping patterns in (3) can be restated as below ;

$$H_{max/a} \geq q^{k-1} - 1 \quad (17)$$
$$H_{max/c} \geq q^{k-1}. \quad (18)$$

Therefore, the maximum value of out-of-phase Hamming autocorrelation function and the maximum value of Hamming crosscorrelation function derived in theorem 3 are optimal in terms of lower bound derived by Lempel and Greenberger as in (17) and (18).

Now, we consider the average number of hits per $(q \times q)$ square between one frequency hopping pattern and its time shifted version in the environment of frequency hopped multiple access communication systems, $H_{a/sq}$, or the average number of hits per $(q \times q)$ square between two frequency hopping patterns in the environment of frequency hopped multiple access communication systems, $H_{c/sq}$. The number of $q \times q$ squares which contains in each frequency hopping patterns with period $q^k - 1$ is $\frac{q^k - 1}{q}$. From the above theorem 1

and 2, the average numbers of hits per $(q \times q)$ square, $H_{a/sq}$ and $H_{c/sq}$, can be derived as follows,

$$H_{a/sq} = (q^{k-1}-1) \cdot \frac{q^k-2}{q^k-2} / \frac{q^k-1}{q} = \frac{q^k-q}{q^k-1} < 1 \quad (19)$$

$$H_{c/sq} = q^{k-1} \cdot \frac{q^k-2}{q^k-1} / \frac{q^k-1}{q} = \frac{q^{2k}-2 \cdot q^k}{q^{2k}-2 \cdot q^k+1} < 1. \quad (20)$$

Therefore, the performances of these frequency hopping patterns are almost the same as those of square matrices.

Further, $s_i(t)$'s except $s(t)$ in S are not m-sequences. Thus, the linear spans of $s_i(t)$'s except $s(t)$ are larger than those of m-sequences, k.

Ⅳ. Example

Let $q=8$ and $k=2$. Consider the finite fields $GF(8)$ and $GF(64)$. Then, there exist 8 frequency hopping patterns with period 63 and alphabet size 8 as follows ;

$$s(t) = tr_8^{8^2}(\alpha^t)$$

$$S = \{s(t),\ s(t)+\beta^0,\ s(t)+\beta^1, \cdots, s(t)+\beta^6\},$$

where α and β are primitive elements of $GF(8)$ and $GF(64)$, respectively. Assume that the minimal polynomials of α and β are chosen as

$$M_\alpha(x) = x^6+x^5+x^2+x+1 \quad (21)$$

$$M_\beta(x) = x^3+x+1. \quad (22)$$

From (22), the mapping from $GF(8)$ to the set of decimal numbers, {0, 1, 2, 3, 4, 5, 6, 7}, can be given as

$0 \rightarrow (0, 0, 0) \rightarrow 0$
$\beta^0 \rightarrow (0, 0, 1) \rightarrow 1$
$\beta^1 \rightarrow (0, 1, 0) \rightarrow 2$
$\beta^2 \rightarrow (1, 0, 0) \rightarrow 4$
$\beta^3 \rightarrow (0, 1, 1) \rightarrow 3$
$\beta^4 \rightarrow (1, 1, 0) \rightarrow 6$
$\beta^5 \rightarrow (1, 1, 1) \rightarrow 7$
$\beta^6 \rightarrow (1, 0, 1) \rightarrow 5.$

Then, the frequency hopping patterns, $s_i(t)$, can be expressed in the other form as follows ;

$s_{-\infty}(t) = s(t) = tr_8^{8^2}(\alpha^t)$

0577313650155626710211747520422535140344161230633272460766454 37

$s_0(t) = s(t)+\beta^0 = tr_8^{8^2}(\alpha^t)+\beta^0$

1466202741044737601300656431533424051255070321722363571677545 26

$s_1(t) = s(t)+\beta^1 = tr_8^{8^2}(\alpha^t)+\beta^1$

2755131472377404532033565702600717362166343012411050642544676 15

$s_2(t) = s(t)+\beta^2 = tr_8^{8^2}(\alpha^t)+\beta^2$

4133757214511262354655303164066171504700525674277636024322010 73

$s_3(t) = s(t)+\beta^3 = tr_8^{8^2}(\alpha^t)+\beta^3$

3644020563266515423122474613711606273077252103500141175345576704

$s_4(t) = s(t)+\beta^4 = tr_8^{8^2}(\alpha^t)+\beta^4$

6311575036733040176477121346244353726522707456055414206100232 51

$s_5(t) = s(t)+\beta^5 = tr_8^{8^2}(\alpha^t)+\beta^5$

7200464127622151067566030257355242637433616547144505315701132340

$s_6(t) = s(t)+\beta^6 = tr_8^{8^2}(\alpha^t)+\beta^6$

5022646305400373245744212075177060415611434765366727135233101 62

where the decimal number, i, $0 \le i \le 7$, corresponds to the frequency, f_i in the set $\{f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7\}$. Clearly, there exist 8 frequency hopping patterns with period 63 and alphabet size 8, that is,

$|S|=8$.

The family of frequency hopping patterns in this example has the following correlation properties. The Hamming autocorrelation and Hamming crosscorrelation functions are given by

$$H_{s_i}(\tau)=\begin{cases}7, & \text{if } \tau\neq 0 \ mod\ 63\\ 63, & \text{if } \tau=0 \ mod\ 63,\end{cases} \tag{23}$$

$$H_{s_i,s_j}(\tau)=\begin{cases}8, & \text{if } \tau\neq 0 \ mod\ 63\\ 0, & \text{if } \tau=0 \ mod\ 63,\end{cases} \tag{24}$$

and the average number of hits per 8×8 square in out-of-phase Hamming autocorrelation and the average number of hits per 8×8 square in Hamming crosscorrelation are given by

$H_{a/sq}=0.888\cdots$

$H_{c/sq}=0.984\cdots$.

V. Conclusion

New family of frequency hopping patterns with long period and optimal Hamming correlation properties generated by using m-sequences is introduced. The period of frequency hopping patterns is q^k-1, their alphabet sizes are q, and the size of family of frequency hopping patterns is q, where k is arbitrary integer and q is power of prime number. The maximum value of out-of-phase Hamming autocorrelation function of any frequency hopping patterns and Hamming crosscorrelation function of any two frequency hopping patterns in the family is q^{k-1}, which corresponds to optimal Hamming correlation properties in terms of lower bound derived by Lempel and Greenberger. As the family of frequency hopping patterns introduced in this paper has the desirable properties, such as long period, good Hamming autocorrelation, and good Hamming crosscorrelation, they can be used as the code sequences in the frequency hopped multiple access communication systems.

References

1. D.V. Sarwate and M.B. Pursley, "Hopping patterns for frequency hopped multiple-access communication," *in IEEE* 1978 ICC Conference Record, pp. 7.4.1-7.4.3, 1978.
2. P.V. Kumar, "Frequency hopping code sequence designs having large linear span," *in IEEE* 1984 *Global Telecommunications Conference Record*, pp. 29.4.1-29.4.5, November 1984.
3. D.Jevtic and H. Alkhatib, "Frequency-hopping codes for multiple-access channels : A geometric approach," *IEEE Trans. Inform. Theory*, vol. IT-35, no.2, pp. 477-481, Mar. 1989.
4. A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming correlation properties," *IEEE Inform. Theory*, vol IT-20, no. 1, pp. 90-94, Jan. 1974.
5. J.S. No and P.V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Inform. Theroy*, vol. IT-35, no.2, pp. 371-379, Mar. 1989.
6. S. W. Golomb, *Shift Register Sequences*, San Francisco, CA : Holden-Day, 1967 ; revised edition, Laguna Hills, CA : Aegean Park Press, 1982.
7. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, the Netherlands : North-Holland, 1977.
8. D. V. Sarwarte and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593-620, May 1980.

盧 宗 善(Jong-Seon No) 정회원

1981년 2월 : 서울대학교 공과대학 전자공학과 학사

1984년 2월 : 서울대학교 대학원 전자공학과 석사

1988년 5월 : (미국)남가주대학교 전자공학과 박사

1988년 2월 ~ 1990년 7월 : (미국)메릴랜드 소재 Hughes Network Systems 연구개발부 책임연구원

1990년 9월 1일 : 건국대학교 공과대학 전자공학과 조교수