論文 94-19-5-18

Periodic Binary Sequence Time Offset Calculation Based on Number Theoretic Approach for CDMA System

正會員 韓 榮 烈*

CDMA 시스템을 위한 정수론 접근 방법에 의한 주기이진부호의 사건옵셑 계산

Young Yearl Han* *Regular Member*

ABSTRACT

In this paper a method calculates the time offset between a binary sequence and its shifted sequence based on the number theoretic approach is presented. Using this method the time offset between a binary sequence and its shifted sequence can be calculated. It has been recognized that the defining the reference (zero-offset) sequence is important in synchronous code division multiple access(CDMA) system since the same spreading sequence are used by the all base stations. The time offset of the sequence with respect to the zero offset sequence are used to distinguish signals received at a mobile station from different base stations. This paper also discusses a method that defines the reference sequence.

요 약

본 논문에서 정수론에 기초한 이진부호와 이전된 이진부호 사이의 시간옵셑을 계산하는 방법을 제시한다. 이 방법을 이용하여 이진부호 사이의 시간옵셑을 계산할 수 있다. 모든 기지국은 동일한 확산부호를 사용하므로써 동기 부호분할 다원접속 시스템에서 기준(영 옾셑)부호를 정의하는 것은 중요하다. 다른 기지국으로부터 이동국에 수신되는 신호를 구별하기 위하여 영옵셑부호에 대한 시간옵셑을 사용하고 있다. 본 논문은 기준부호를 정의하는 방법을 제시한다.

*漢陽大學校 電子通信工學科
Dept. of Electronic Communication Engineering Han Yang University.
論文番號 : 9436
接受日字 : 1994年 2月 2日

I. INTRODUCTION

In the recent years, direct-sequence ocde divison multiple access (CDMA) technology has been considered for digital mobile system and personal communication network applications. In CDMA systems spreading sequence is used to spread and despread information data. In the proposed CDMA system, the time offset of the spreading sequence is important since the same spreading sequences with different time offset are assigned to each base station[1]. When the sequence length is short the relative time offset between two sequences can be found by comparing the two sequences. However as the sequence length increases it is not easy to find the relative time offset between two sequences.

In this paper we present a method that calculates the time offset two binary sequences of length p-1, where p is a prime number. This method exploits the fact that every integer which is relatively prime to p possesses a unique index among the integres of the set {0, 1, 2,⋯,p-2}. Definition of reference sequence (zero offset sequence) will be discussed. This paper is organized follows.

Section 2 provides the description of method which can be used to calculate the relative time offset between two binary sequences. sequences. Section 3 is devoted to the implementation of the method described in section 2. The sequence patterns that can be applied to the proposed method are anayzed in section 4. And section 5 states concluding remarks.

II. DESCRIPTION OF THE METHOD

We define a periodic $\varphi(p)$-tuple sequence

$$C^0 = (C_0, C_1, \cdots, C_{\varphi(p)-1})$$
$$C^1 = (C_{\varphi(p)-1}, C_0, \cdots, C_{\varphi(p)-2})$$
$$\vdots$$
$$C^i = (C_{\varphi(p)-i}, C_{\varphi(p)-i+1}, \cdots, C_{\varphi(p)-i-1}) \quad (1)$$
$$\vdots$$
$$C^{\varphi(p)-1} = (C_1, C_2, \cdots, C_0)$$

p is a prime unmber. $\varphi(p)$ is an Euler's phi function and is the number of positive integers less than p that are relatively prime to p. If a prime number, 1, 2,⋯,p-1 are relatively prime to p. Thus we have $\varphi(p) = p-1$. Observe that $C_i = C_{i+\varphi(p)}$ and $C^i = C^{i+\varphi(p)}$, $0 \le i \le \varphi(p)-1$.

Once C^0 is defined, C^i, $0 \le i \le p-1$, can be obtained by shifting C^0 cyclically i units to the right. Each element symbol is chosen from the symbol set {1, −1} or {1, 0}. We define $A_g(C^i)$ as follows

$$A_g(C^i) = (C_{\varphi(p)-i} \cdot g^0 + C_{\varphi(p)-i+1} \cdot g^1 + \cdots + C_{\varphi(p)-i-1} \cdot g^{\varphi(p)-1}) \quad (2)$$

which is a weighted sum of sequence elements. g is a primitive root modulo p. By a primitive root modulo p we mean an integer g such that $g^0, g^1, \cdots, g^{\varphi(p)-1}$ form a reduced residue system modulo p. That is, the integers, $g^0 \pmod p$, $g^1 \pmod p$,⋯, $g^{\varphi(p)-1} \pmod p$ are a rearrangement of 1, 2,⋯,p-1. The sequence $g^0, g^1, \cdots \pmod p$ is periodic and the period of this sequence is $\varphi(p)$. It can be shown that there exists $\varphi(p-1)$ primitive roots modulo p [2, 3] and we will use the least primitive root modulo p throughout this paper. In order to show that equation (2) is related with shift of the periodic $\varphi(p)$-tuple sequence, we prove some properties of equation (2).

【Theorem 1】 If $A_g(C^i) \neq 0 \pmod p$, $0 \le i \le \varphi(p)-1$, $A_g(C^i)$, $0 \le i \le \varphi(p)-1$ form a reduced residue system of modulo p.

Proof : Since $g^i \equiv g^{i+\varphi(p)} \pmod p$[2], we have

$$A_g(C^0) \equiv (C_0 \cdot g^0 + C_1 \cdot g^1 + \cdots + C_{\varphi(p)-1} \cdot g^{\varphi(p)-1})$$
$$\equiv g^0 \cdot (C_0 + C_1 \cdot g^1 + \cdots + C_{\varphi(p)-1} \cdot g^{\varphi(p)-1}) \pmod p$$
$$A_g(C^1) \equiv (C_0 \cdot g^1 + C_1 \cdot g^2 + \cdots + C_{\varphi(p)-1} \cdot g^0)$$
$$\equiv g^1 \cdot (C_0 + C_1 \cdot g^1 + \cdots + C_{\varphi(p)-1} \cdot g^{\varphi(p)-1}) \pmod p$$
$$\vdots$$

$$A_g(C^{\varphi(p)-1}) \equiv (C_0 \cdot g^{\varphi(p)-1} + C_1 \cdot g^0 + \cdots + C_{\varphi(p)-1} \cdot g^{\varphi(p)-2})$$
$$\equiv g^{\varphi(p)-1} \cdot (C_0 + C_1 \cdot g^1 + \cdots + C_{\varphi(p)-1} \cdot g^{\varphi(p)-1}) \pmod{p} \quad (3)$$

Let $a = C_0 + C_1 \cdot g^1 + \cdots + C_{\varphi(p)-1} \cdot g^{\varphi(p)-1} \neq 0$ and the greatest common divisor of a and p be 1, gcd (a, p) = 1, then the set $a \cdot g^0$, $a \cdot g^1, \cdots, a \cdot g^{\varphi(p)-1}$ forms a reduced residue system modulo p. Consequenctly $A_g(C^i)$, $0 \le i \le \varphi(p)-1$, forms a reduced residue system modulo p.

【Theorem 2】 If $A_g(C^i) \pmod{p}$, $0 \le i \le \varphi(p)-1$, do not form a reduced residue system modulo p then $A_g(C^i) \equiv 0 \pmod{p}$ for $0 \le i \le \varphi(p)-1$.

Proof : If $A_g(C^i) \pmod{p}$ do not form reduced residue system modulo p for $0 \le i \le \varphi(p)-1$, then there exists an integer j, $0 \le j \le \varphi(p)-1$ and $i \neq j$, such that

$$A_g(C^i) \pmod{p} = A_g(C^{i+j}) \pmod{p}$$

Hence

$$A_g(C^i) \equiv g^i \cdot (C_0 + C_1 \cdot g^1 + \cdots + C_{\varphi(p)-1} \cdot g^{\varphi(p)-1})$$
$$\equiv g^{i+j} \cdot (C_0 + C_1 \cdot g^1 + \cdots + C_{\varphi(p)-1} \cdot g^{\varphi(p)-1})$$
$$\equiv A_g(C^{i+j}) \pmod{p}$$

Since $g^i \neq g^{i+j}$, we have

$$(C_0 + C_1 \cdot g^i + \cdots + C_{\varphi(p)-1} \cdot g^{\varphi(p)-1}) \equiv 0 \pmod{p}$$

Consequently

$$A_g(C^i) \equiv 0 \pmod{p} \text{ for } 0 \le i \le \varphi(p)-1.$$

Let p be a prime with primitive root g. If b is a positive integer with gcd(b, p) = 1, then the least nonnegative integer i such that $g^i = b \pmod{p}$ is called the index of the integer b to base g modulo p and is denoted by $i = \mathrm{ind}_g\, b$. It follows that every b which is relatively prime to p, possesses a unique index i among the integers of the set $\{0, 1, \cdots, \varphi(p)-1\}$.

For example consider the primitive root g = 2 of p = 5, we have $g^0 \equiv 1$, $g^1 \equiv 2$, $g^2 \equiv 4$ and $g^3 \equiv 3 \pmod{5}$ hence $\mathrm{ind}_2\, 1 = 0$, $\mathrm{ind}_2\, 2 = 1$, $\mathrm{ind}_2\, 4 = 2$ and $\mathrm{ind}_2\, 3 = 3$. We will use the relationship $g^i \equiv A_g(C) \pmod{p}$ in finding the index of $A_g(C)$ modulo p. Using he primitive root g = 2 of p = 5, we can construct the following table of least indices.

$A_g(C) \pmod 5$	1	2	4	3
$\mathrm{ind}_2\, A_g(C)$	0	1	2	3

We introduce the definition of a reference sequence. Assuming $A_g(C^i) \pmod{p}$, $0 \le i \le \varphi(p)-1$, form a reduced residue system modulo p, we define the reference sequence (zero offset sequence), C^0, which satisfies the following equation.

$$\mathrm{ind}_g\,[A_g(C^0)] = 0 \quad (4)$$

If $A_g(C^i \pmod{p})$, $0 \le i \le \varphi(p)-1$, form a reduced residue system modulo p, there always exists an unique index corresponding to an $A_g(C)$. Next we prove a theorem which enables us to find the time offset between two binary sequences.

【Theorem 3】. If $A_g(C^i) \neq 0 \pmod{p}$, then for the sequence C^{i+j} and C^i

$$\{\mathrm{ind}_g\,[A_g(C^{i+j}) \pmod{p}] - \mathrm{ind}_g[A_g(C^i) \pmod{p}]\}$$
$$\equiv j \pmod{\varphi(p)},\ 0 \le i \le \varphi(p)-1,\ 0 \le j \le j\varphi(p)-1 \quad (5)$$

Proof : If $i, j, b \in \{0, 1, \cdots, p-1\}$, we have

$$\mathrm{ind}_g\,[A_g(C^{i+j}) \pmod{p}] \equiv \mathrm{ind}_g\,[g^{i+j} \cdot (C_0 + C_1 \cdot g^1$$
$$+ \cdots + C_{\varphi(p)-1} \cdot g^{\varphi(p)-1} \pmod{p}]$$
$$\equiv \mathrm{ind}_g\,[g^{i+j} \cdot g^b \pmod{p}]$$
$$\equiv \mathrm{ind}_g\,[g^{i+j+b} \pmod{p}]$$

and

$$\mathrm{ind}_g\,[A_g(C^i) \pmod{p}] \equiv \mathrm{ind}_g\,[g^{i+b} \pmod{p}]$$

Hence, we have

$$[(i+j+b) - (i+b)] \equiv j \pmod{\varphi(p)}$$

This gives the stated formula.

We illustrate the use of the result of theorem 3 with an example.

Example 1. Suppose that $p = 11.2 (= g)$ is a least primitive root modulo 11 and the period of sequence is $10 (= \varphi(11))$. Table 1 shows three cases for binary Hamming weight, w(C) is the number of 1's in the periodic $\varphi(p)$-tuple sequece. We used the relationship $g^i \equiv A_g(C) \pmod{11}$ in finding the index of $A_g(C)$ modulo 11

Table 1. The value of $A_s(C)$ (mod 11) and its index for p=11 and w(C)=1, 2, 3

a) In the case of p=11, w(C)=1

p = 11 w(C)=1						
C^i	$C_i, C_{i+1}, \cdots, C_{i-1}$	$A_s(C)$ (mod 11)	$ind_2\ A_s(C)$	$C_i, C_{i+1}, \cdots, C_{i-1}$	$A_s(C)$ (mod 11)	$ind_2\ A_s(C)$
C^0	1 0 0 0 0 0 0 0 0 0 0	1	0	1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1	2	1
C^1	0 1 0 0 0 0 0 0 0 0 0	2	1	-1 1 -1 -1 -1 -1 -1 -1 -1 -1 -1	4	2
C^2	0 0 1 0 0 0 0 0 0 0 0	4	2	-1 -1 1 -1 -1 -1 -1 -1 -1 -1 -1	8	3
C^3	0 0 0 1 0 0 0 0 0 0 0	8	3	-1 -1 -1 1 -1 -1 -1 -1 -1 -1 -1	5	4
C^4	0 0 0 0 1 0 0 0 0 0 0	5	4	-1 -1 -1 -1 1 -1 -1 -1 -1 -1 -1	10	5
C^5	0 0 0 0 0 1 0 0 0 0 0	10	5	-1 -1 -1 -1 -1 1 -1 -1 -1 -1 -1	9	6
C^6	0 0 0 0 0 0 1 0 0 0 0	9	6	-1 -1 -1 -1 -1 -1 1 -1 -1 -1 -1	7	7
C^7	0 0 0 0 0 0 0 1 0 0 0	7	7	-1 -1 -1 -1 -1 -1 -1 1 -1 -1 -1	3	8
C^8	0 0 0 0 0 0 0 0 1 0 0	3	8	-1 -1 -1 -1 -1 -1 -1 -1 1 -1 -1	6	9
C^9	0 0 0 0 0 0 0 0 0 1 0	6	9	-1 -1 -1 -1 -1 -1 -1 -1 -1 1 -1	1	0
C^{10}	0 0 0 0 0 0 0 0 0 0 1	6	9	-1 -1 -1 -1 -1 -1 -1 -1 -1 -1 1	1	0

b) In the case of p=11, w(C)=2.

p = 11 , w(C)=2						
C^i	$C_i, C_{i+1}, \cdots, C_{i-1}$	$A_s(C)$ (mod 11)	$ind_2\ A_s(C)$	$C_i, C_{i+1}, \cdots, C_{i-1}$	$A_s(C)$ (mod 11)	$ind_2\ A_s(C)$
C^0	0 0 0 0 0 0 1 0 1 0	1	0	-1 -1 -1 -1 -1 -1 1 -1 1 -1	2	1
C^1	0 0 0 0 0 0 0 1 0 1	2	1	-1 -1 -1 -1 -1 -1 -1 1 -1 1	4	2
C^2	1 0 0 0 0 0 0 0 1 0	4	2	1 -1 -1 -1 -1 -1 -1 -1 1 -1	8	3
C^3	0 1 0 0 0 0 0 0 0 1	8	3	-1 1 -1 -1 -1 -1 -1 -1 -1 1	5	4
C^4	1 0 1 0 0 0 0 0 0 0	5	4	1 -1 1 -1 -1 -1 -1 -1 -1 -1	10	5
C^5	0 1 0 1 0 0 0 0 0 0	10	5	-1 1 -1 1 -1 -1 -1 -1 -1 -1	9	6
C^6	0 0 1 0 1 0 0 0 0 0	9	6	-1 -1 1 -1 1 -1 -1 -1 -1 -1	7	7
C^7	0 0 0 1 0 1 0 0 0 0	7	7	-1 -1 -1 1 -1 1 -1 -1 -1 -1	3	8
C^8	0 0 0 0 1 0 1 0 0 0	3	8	-1 -1 -1 -1 1 -1 1 -1 -1 -1	6	9
C^9	0 0 0 0 0 1 0 1 0 0	6	9	-1 -1 -1 -1 -1 1 -1 1 -1 -1	1	0
C^{10}	0 0 0 0 0 0 1 0 1 0	1	0	-1 -1 -1 -1 -1 -1 1 -1 1 -1	2	1

c) In the case of p=11, w(C)=3

p = 11 , w(C)=3						
C^i	$C_i, C_{i+1}, \cdots, C_{i-1}$	$A_s(C)$ (mod 11)	$ind_2\ A_s(C)$	$C_i, C_{i+1}, \cdots, C_{i-1}$	$A_s(C)$ (mod 11)	$ind_2\ A_s(C)$
C^0	0 1 1 0 0 0 0 0 0 0 1	1	0	-1 1 1 -1 -1 -1 -1 -1 -1 1	2	1
C^1	1 0 1 1 0 0 0 0 0 0 0	2	1	1 -1 1 1 -1 -1 -1 -1 -1 -1	4	2
C^2	0 1 0 1 1 0 0 0 0 0 0	4	2	-1 1 -1 1 1 -1 -1 -1 -1 -1	8	3
C^3	0 0 1 0 1 1 0 0 0 0 0	8	3	-1 -1 1 -1 1 1 -1 -1 -1 -1	5	4
C^4	0 0 0 1 0 1 1 0 0 0 0	5	4	-1 -1 -1 1 -1 1 1 -1 -1 -1	10	5
C^5	0 0 0 0 1 0 1 1 0 0 0	10	5	-1 -1 -1 -1 1 -1 1 1 -1 -1	9	6
C^6	0 0 0 0 0 1 0 1 1 0 0	9	6	-1 -1 -1 -1 -1 1 -1 1 1 -1	7	7
C^7	0 0 0 0 0 0 1 0 1 1 0	7	7	-1 -1 -1 -1 -1 -1 1 -1 1 1	3	8
C^8	1 0 0 0 0 0 0 1 0 1 1	3	8	1 -1 -1 -1 -1 -1 -1 1 -1 1	6	9
C^9	1 1 0 0 0 0 0 0 1 0 1	6	9	1 1 -1 -1 -1 -1 -1 -1 1 1 -1	1	0
C^{10}	1 1 1 0 0 0 0 0 0 1 0	1	0	1 1 1 -1 -1 -1 -1 -1 -1 1	2	1

We can take C^0 as a reference sequence in applications. We used difinition of zero offset sequence from equation (4). To calculate the time offset between reference sequence and its shifted sequence, we need only calculate $ind_g[A_g(C) \pmod p]$ of the shifted sequence to find the time offset with respect to the zero sequence.

Ⅲ. REALIZATION OF THE METHOD

In this section we describe the realization of theorem 3. The realization of $A_g(C)$ calculator is illustrated in Fig. 1.

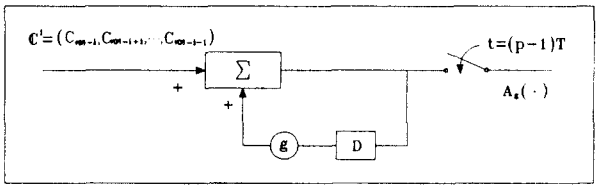


Figure 1. $A_g(C)$ calculator.

D is a symbol delayer. In calculating the value of $A_g(\cdot)$, $C_{\varphi(p)-i-1}$ is fed into the $A_g(\cdot)$ calculator. Next $C_{\varphi(p)-i-2}$ enters the $A_g(\cdot)$ calculator. The added value become $C_{\varphi(p)-i-2}+C_{\varphi(p)-i-1}\cdot g$. After all symbols arrive, the value of $A_g(\cdot)$ becomes

$$A_g(\cdot)=C_{\varphi(p)-i}+g\cdot(C_{\varphi(p)-i+1}+C_{\varphi(p)-i+2}\cdot g+\cdots+C_{\varphi(p)-i-1}\cdot g^{\varphi(p)-2})$$

which is extracted out at the time $t=(p-1)T$. $p-1$ is the sequence length and T is the symbol duration.

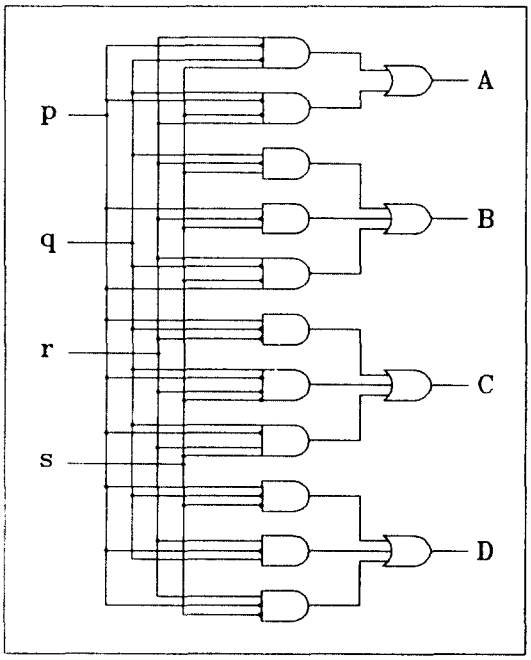
We have a one-to-one correspondence between $A_g(C^i) \pmod p$, $0\le i\le\varphi(p)-1$ and index of $A_g(C^i)$ modulo p. This relationship provides us to design a logic circuit that convert $A_g(C^i) \pmod p$ to index of $A_g(C^i) \pmod p$. Table 2 shows the value of $A_g(C^i) \pmod{11}$, $0\le i\le 9$, ad corresponding value of index in decimal and binary digits.

Table 2. The truth table of $A_g(\cdot)$ and its index in case of $p=11$.

$A_g(\cdot) \pmod{11}$	p q r s	A B C D	index
1	0 0 0 1	0 0 0 0	0
2	0 0 1 0	0 0 0 1	1
3	0 0 1 1	1 0 0 0	8
4	0 1 0 0	0 0 1 0	2
5	0 1 0 1	0 1 0 0	4
6	0 1 1 0	1 0 0 1	9
7	0 1 1 1	0 1 1 1	7
8	1 0 0 0	0 0 1 1	3
9	1 0 0 1	0 1 1 0	6
10	1 0 1 0	0 1 0 1	5

The boolena expressions for A, B, C, D, obtained from Table 2 are

$$A=\bar{p}\,\bar{q}\,rs+\bar{p}\,qr\bar{s}$$
$$B=q\bar{r}s+q\bar{r}\bar{s}+p\bar{q}\,r\bar{s}$$
$$C=p\,\bar{q}\,\bar{r}+\bar{p}q\bar{r}\bar{s}+\bar{p}qrs$$
$$D=p\bar{q}\bar{s}+\bar{p}qr+\bar{p}r\bar{s} \qquad (6)$$



where $\bar{p}$ is a complement of p. The logic circuit that implement the boolean expressions is given in Fig. 2. The logic circuit can be constructed by using OR-gate and decoder.

Ⅳ. PATIERN ANALYSIS

We now investigate the patterns and number of ways of the (p-1) tuple sequence $(C_i, C_{i+1},\cdots,C_{i-1})$ for which equation $A_g(C^i) \equiv 0 \pmod p$ holds. The numbers g^0, $g^1,\cdots,g^{\varphi(p)-1}$ form a reduced residue system of modulo p as described before. But it is convenient to use numbers $g^0 \pmod p$, $g^1 \pmod p,\cdots,g^{\varphi(p)-1} \pmod p$ which are rearrangement of 1, 2,⋯,p-1. In order to find the patterns that we must avoid in applying theorem 3 consider following equation

$$n = d_i + d_{i+1} + \cdots + d_{i+r} \equiv 0 \pmod p,$$
$$d_j \in \{1, 2,\cdots,p-1\},\ r \le p-1 \tag{7}$$

The equation (7) indicates that the sum of distinct positive integers with summands from {1, 2,⋯, p−1} equals to k·p, k = 1, 2⋯.

The generating function for patterns and number of way for which equation (7) hlods can be wrtten as follows

$$G_{p-1}(n \equiv 0 \pmod p) = \prod_{i=1}^{p-1} (1 + x^i) \tag{8}$$

where n is the sum of distinct positive integers that is zero modulo p. Subscript (p−1) of G indicates summands less than or equal to p−1. If we multiply p−1 times, the power series is of the form $1 + a_1 x + a_2 x^2 + \cdots + a_{p(p-1)/2} x^{p(p-1)/2}$. The coefficient of x^q is the number of ways that q is a sum of distinct positive integers with summands {1, 2,⋯,p−1}.

Example 2. Suppose that p=5. The generating function is

$$G_4(n \equiv 0 \pmod 5) = \prod_{i=1}^{4} (1 + x^i)$$
$$= (1+x)(1+x^2)(1+x^3)(1+x^4)$$
$$= (1+x+x^2+x^{1+2})(1+x^3)(1+x^4)$$
$$= (1+x+x^2+x^{1+2}+x^3+x^{1+3}+x^{2+3}+x^{1+2+3})(1+x^4)$$
$$= 1+x+x^2+(x^{1+2}+x^3)+(x^{1+3}+x^4)$$
$$+(x^{2+3}+x^{1+4})+(x^{1+2+3}+x^{2+4})$$
$$+(x^{1+2+4}+x^{3+4})+x^{1+3+4}+x^{2+3+4}+x^{1+2+3+4} \tag{9}$$
$$= 1+x+x^2+2x^3+2x^4+2x^5+2x^6+2x^7+x^8+x^9+x^{10} \tag{10}$$

Each coefficient of x^q in equation (10), is the number of ways such that q is a sum of distinct positive integers with summands {1, 2,⋯,p−1}. Each power of x in equation (9) corresponds to a sum pattern of distinct possible integers with summands {1, 2,⋯, p−1}.

There are two n's, namely n=5, 10, that holds equation n=0(mod 5) and corresponding patterns are (2+3), (1+4) and (1+2+3+4). With p=5 we have following equation

$$(C_i \cdot g^0 + C_{i+1} \cdot g^i + C_{i+2} \cdot g^2 + C_{i+3} \cdot g^3) \equiv 0 \pmod 5 \tag{11}$$

With g=2 which is a least primitive root of modulo 5 we can write equivalently

$$(C_i \cdot 1 + C_{i+1} \cdot 2 + C_{i+2} \cdot 4 + C_{i+3} \cdot 3) \equiv 0 \pmod 5 \tag{12}$$

By applying equation (12) the three patterns becomes (0, 1, 0, 1), (1, 0, 1, 0) and (1, 1, 1, 1) in the form of binary sequence. It is noted that sequence (0, 1, 0, 1) is the one step cyclic shift of sequence (1, 0, 1, 0). Trivial solution (0, 0, 0, 0) satisfies the equation (12), but it is excluded since the summands are from the set {1, 2,⋯,p−1}.

The ratio of total pattern and the number of pattern that the suggested method can be applied to is 1 for p=5, 1 for p=7 and 0.939 for p=11. In the total pattern we have excluded the all zero, one sequence

and sequences that don't have the period $\varphi(p)$ when shifted.

V. CONCLUSION

In this paper the relative time/phase offset between two binary sequences of length $\varphi(p)$ is investigated. The proposed method that calculates the time offset between two binary sequences is based on number theoretic approach. The method exploits the fact that every integer which is relatively prime to p possesses a unique index in number theory. The zero offset (reference) sequence is defined and circuit realization is described to calculate the time offset between two sequences effectively. However there is a restriction in applying this method. The number of restricting patterns which were analyzed and found was small compared with the number of the total patterns.

韓 榮 烈(Young Yearl Han) 正會員
1938年 6月 10日生
1960年 2月 : 서울대학교 전자공학사
1976年 5月 : 미주리주립대학교 대학원 공학석사
1979年 5月 : 미주리주립대학교 대학원 공학박사
1980年 ~ 現在 : 한양대학교 전자통신공학과 교수
1980年 ~ 1991年 : 본학회이사, 상임이사
1991年 ~ 現在 : 본학회 부회장

REFERENCES

1. S. Nanda and D. J. Goodman, *Third Generation Wireless Information Networks*, Kluwer Academic Publishers, 1992.
2. K. H. Rosen, *Elementary Number Theory and Its Applications*, Bell Telephone Laboratories : Addison-Wesley Publishing Company, 1988.
3. I. Niven and H. S. Zukerman, *An Introduction to the Theory of Number*, John Wiley & Sons, 1980.
4. Y. Y. Han and J. S. Jun, "Analysis of Time Offset of PN Sequence in CDMA System," *IEEE Globecom'93*, Vol.1, pp.48-53, Houston, 1993.