Numerical Algorithm for Phase Offsets of Binary Codes in the Code Division Multiple Access System

Hong Goo Park

ABSTRACT—There has been a growing need for increased capacity in cellular systems. This has resulted in the adoption of the code division multiple access (CDMA) system as a multiple channel access method. Thus, it is important to obtain the phase offsets of binary codes in the CDMA system because distinct phase offsets of the same code are used to distinguish signals received at the mobile station from different base stations. This letter proposes an efficient algorithm to compute the phase offset of a binary code in the CDMA system through the use of the basic facts of number theory and a new notion of the subcodes of a given code. We also formulate the algorithm in a compact form.

Keywords—Binary code, phase offset, code division multiple access system, subcode.

I. Introduction

Let $S=\{\alpha,\beta \mid \alpha=1,\beta=0 \text{ or } -1\}$, and B^n the set of all n-tuple binary codes $C=(c_0,c_1,...,c_{n-1})$, where $c_i \in S$ for each i with $0 \le i \le n-1$. We define a cyclic shift to the left operator $L:B^n \to B^n$ by $L(C)=(c_1, c_2, \ldots, c_{n-1}, c_0)$ for all C in B^n. For each nonnegative integer i, we define by L^i the i-times function composition of L, where L^0 is defined as the identity function on B^n. Note that if m and t are integers with $m \equiv t \pmod n$, then $L^m(C)=L^t(C)$ for a code C in B^n. We denote $L^i(C)$ by C^i for each nonnegative integer i, and define $C^0=C$ and $(C^s)^t = C^{s+t}$ for any two integers s, t. For each pair of $C, D \in B^n$, we define the relation $\sim$ on B^n as $C \sim D$ iff there exists an integer i with $0 \le i \le n-1$ such that $C^i = D$. Then, it can be shown that the relation $\sim$ is an equivalent relation on B^n. Thus, B^n can be partitioned into cells, so-called equivalent classes, induced from the relation. If $C \in B^n$, then the equivalent class $\overline{C}$ containing C can be written as

$$\overline{C}=\{C^i \mid C \in B^n,\ 0 \le i \le n-1\}.$$

Next, we define a function $\sigma : B^n \to \mathbb{Z}$ by

$$\sigma(C)=\sum_{i=0}^{n-1}(n-i)c_i \qquad (1)$$

for the set $\mathbb{Z}$ of integers and all C in B^n. Such a function σ will be called a σ-function on B^n. Let R be a binary code in $\overline{C}$. Then, the phase offset $P_R(C)$ of a binary code C in $\overline{C}$ with respect to R is defined as the least nonnegative integer m such that

$$R^m = C. \qquad (2)$$

Such a code R will be called a (zero offset) reference code in $\overline{C}$. Note that the phase offset of the reference code with respect to itself is equal to zero, and can be chosen arbitrarily in $\overline{C}$.

Willet [3] proposed a method to calculate the phase offset of a maximal length sequence with minimum period 2^n-1, so-called an m-sequence, over a Galois field GF(2) of order 2 as an application. That is, if $u=(u_i)_0^\infty=(u_0,u_1,...)$ is a pseudo-random noise (PN) code with minimum period 2^n-1 over GF(2), then the phase offset M of u can be obtained by

$$\mathrm{M} \equiv \left[\sum_{i\in J_k} i\right]-\left[\sum_{i\in I_k} i\right] \equiv -2\left[\sum_{i\in I_k} i\right] \pmod{2^n-1}, \qquad (3)$$

where $I_k=\{i \mid 0\le i\le 2^n-1, u_{i+k}=0\}$ and $J_k=\{i \mid 0\le i\le 2^n-1, u_{i+k}=1\}$.

In [1], we can see a method to calculate the value of the phase offset of a binary code $C \in B^n$ by computing the reduction of $a\sigma(C) \pmod n$ for a proper integer a, provided

Manuscript received June 08, 2005; revised Dec. 23, 2005.

Hong Goo Park (phone: +82 2 2220 0907, email: hpark@hanyang.ac.kr) is with the Department of Mathematics, Hanyang University, Seoul, Korea.

$\gcd(n,(\alpha-\beta)v_C(\beta))=1$ for $\alpha,\beta\in S$, where $v_C(\beta)$ is the number of β's in C. Note that the phase offsets (3) of the above m-sequences can also be calculated using the reduction.

In this letter, we propose a new numerical algorithm for the phase offset (NAPO) of an n-tuple binary code C in the case of $\gcd(n,(\alpha-\beta)v_C(\beta))\neq 1$. It will be done by investigating the value of the σ -function defined in (1) for a given binary code $C\in B^n$ and the phase offsets of the subcodes of C as a new notion.

II. A Modified NAPO Based on a σ -Function

We can easily modify and simplify the main results of [1] as in Theorem 1. We have omitted the proofs because they are almost the same as the proofs of the main results in [1].

Theorem 1. Let C be a binary code in B^n satisfying $\gcd(n,(\alpha-\beta)v_C(\beta))=1$ for α,β in C. If σ is a σ -function on B^n, then the following hold:
(a) For each fixed s, $t\in\mathbb{Z}$ with $0\le s,t\le n-1$,

$$\sigma(C^t)-\sigma(C^s)\equiv-(\alpha-\beta)v_C(\beta)(t-s)(\mathrm{mod}\,n). \tag{4}$$

(b) If there exists an integer $a\in\mathbb{Z}$ such that $a(\alpha-\beta)\,v_C(\beta)\equiv -1(\mathrm{mod}\ n)$, then $a(\sigma(C^i)-\sigma(C^i))\equiv i(\mathrm{mod}\ n)$ for each fixed integer i with $0\le i\le n-1$.
(c) If a is an integer defined in (b), then a set

$$\{a\sigma(C^i)(\mathrm{mod}\ n)\,|\,0\le i\le n-1\} \tag{5}$$

forms a complete system of residues modulo n.

The set $\{\sigma(C^i)(\mathrm{mod}\,n)\,|\,0\le i\le n-1\}$ also forms a complete system of residues modulo n with the same condition in Theorem 1. However, the set in (5) gives us a nice ordering of residues modulo n; that is, it becomes

$$\{n-j+1,n-j+2,\ldots,n-1,0,1,\ldots,n-j\}$$

for an integer j with $0\le j\le n-1$ such that $\sigma(C^j)\equiv 0\ (\mathrm{mod}\ n)$. In this case, we can have distinct and ordered phase offsets of the binary codes in $\overline{C}$. For each fixed i with $0\le i\le n-1$, the phase offset $P_R(C^i)$ of C^i's with respect to a reference code R is a nonnegative integer defined by

$$P_R(C^i)\equiv a\sigma(C^i)(\mathrm{mod}\,n) \tag{6}$$

for an integer a with $a(\alpha-\beta)\,v_C(\beta)\equiv -1(\mathrm{mod}\ n)$.

For example, if

$$C=(\alpha,\beta,\alpha,\alpha,\beta,\alpha,\beta,\beta,\beta,\alpha,\beta,\alpha,\beta,\alpha,\beta)\in B^{15},$$

then $\sigma(C^4)\equiv\sum_{i=0}^{14}(15-i)c_i\equiv 0(\mathrm{mod}\,15)$, where each c_i is an i-th component of C. So, C^4 becomes a reference code of C. Tables 1 and 2 illustrate the values of distinct phase offsets $P_{C^4}(C^i)$ of C^i's with respect to C^4 for all i with $0\le i\le n-1$.

Table 1. $P_R(C^i)$ with $\alpha=1$, $\beta=0$, gcd(15, $v_C(0)$)=1, and $a=1$.

i	$C^i=(c_i, c_{i+1},\ldots,c_{i-1})$	$\sigma(C^i)$	$\sigma(C^i)$ (mod n)	$P_R(C^i)$
0	(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)	62	2	11
1	(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)	54	9	12
2	(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)	61	1	13
3	(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)	53	8	14
4	(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)	45	0	0
5	(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)	52	7	1
6	(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)	44	14	2
7	(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)	51	6	3
8	(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)	58	13	4
9	(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0,. 0, 0)	65	5	5
10	(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0,. 0, 0, 1)	57	12	6
11	(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0,. 0, 0, 1, 0)	64	4	7
12	(0, 1, 0, 1, 0, 1, 1, 0, 1, 0,. 0, 0, 1, 0, 1)	56	11	8
13	(1, 0, 1, 0, 1, 1, 0, 1, 0,. 0, 0, 1, 0, 1, 0)	63	3	9
14	(0, 1, 0, 1, 1, 0, 1, 0,. 0, 0, 1, 0, 1, 0, 1)	55	10	10

Table 2. $P_R(C^i)$ with $\alpha=1$, $\beta=-1$, gcd(15, $2v_C(-1)$)=1, and $a=14$.

i	$C^i=(c_i, c_{i+1},\ldots,c_{i-1})$	$\sigma(C^i)$	$\sigma(C^i)$ (mod n)	$P_R(C^i)$
0	(1, –1,1,1,–1,1,–1,–1,–1,1,–1,1,–1,1,–1)	4	4	11
1	(–1,1,1,–1,1,–1,–1,–1,1,–1,1,–1,1,–1,1)	-12	3	12
2	(1,1,–1,1,–1,–1,–1,1,–1,1,–1,1,–1,1,–1)	2	2	13
3	(1,–1,1,–1,–1,–1,1,–1,1,–1,1,–1,1,–1,1)	-14	1	14
4	(–1,1,–1,–1,–1,1,–1,1,–1,1,–1,1,–1,1,1)	-30	0	0
5	(1,–1,–1,–1,1,–1,1,–1,1,–1,1,–1,1,1,–1)	-16	14	1
6	(–1,–1,–1,1,–1,1,–1,1,–1,1,–1,1,1,–1,1)	-32	13	2
7	(–1,–1,1,–1,1,–1,1,–1,1,–1,1,1,–1,1,–1)	-18	12	3
8	(–1,1,–1,1,–1,1,–1,1,–1,1,1,–1,1,–1,–1)	-4	11	4
9	(1,–1,1,–1,1,–1,1,–1,1,1,–1,1,–1,–1,–1)	10	10	5
10	(–1,1,–1,1,–1,1,–1,1,1,–1,1,–1,–1,–1,1)	-6	9	6
11	(1,–1,1,–1,1,–1,1,1,–1,1,–1,–1,–1,1,–1)	8	8	7
12	(–1,1,–1,1,–1,1,1,–1,1,–1,–1,–1,1,–1,1)	-8	7	8
13	(1,–1,1,–1,1,1,–1,1,–1,–1,–1,1,–1,1,–1)	6	6	9
14	(–1,1,–1,1,1,–1,1,–1,–1,–1,1,–1,1,–1,1)	-10	5	10

III. Definitions of d-Subcodes and Reference Codes Based on a σ_d-Function

If $\gcd(n,(\alpha-\beta)v_C(\beta)) \neq 1$ in Theorem 1, then we fail to obtain the distinct phase offsets of C^i's since there does not exist an integer a such that $a(\alpha-\beta)v_C(\beta) \equiv -1 \pmod n$. Now, we need to find a possible method to have the distinct phase offsets of binary codes in $\overline{C}$ with respect to a proper reference code. As an example, see Table 3.

Let $C = (c_0, c_1, \ldots, c_{n-1})$ be a binary code in B^n with $\gcd(n,(\alpha-\beta)v_C(\beta)) = d$. Then, a code

$$(c_0, c_{n/d}, c_{2n/d}, \ldots, c_{(d-1)n/d})$$

is called a d-subcode of C, denoted by $S_d(C)$. It is easy to see that $S_d(C^{jn/d}) = (c_{jn/d}, c_{(j+1)n/d}, \ldots, c_{(j+d-1)n/d})$ for each j with $0 \le j \le d-1$, where $c_{(j+k)n/d} = c_t$ with $0 \le j,k \le d-1$ for $t \equiv (j+k)n/d \pmod d$. It follows from Theorem 1 that if $\gcd(d,(\alpha-\beta)v_{S_d(C^{jn/d})}(\beta)) = 1$, then a set

$$\{s \in [[d]] \,|\, \sigma(S_d(C^{jn/d})) \equiv s \pmod d,\ 0 \le j \le d-1\}$$

forms a complete system of residues modulo d, where $[[d]] = \{0, 1, \ldots, d-1\}$.

For example, consider a code $C = (\beta,\alpha,\beta,\alpha,\beta,\alpha,\alpha,\beta,\beta,\beta,\beta,\alpha,\beta,\alpha) \in B^{15}$. $\gcd(15,(\alpha-\beta)v_C(\beta)) = 3$, and therefore, $S_3(C^{j5}) = (c_{j5}, c_{(j+1)5}, c_{(j+2)5})$ for $j = 0, 1, 2$. Thus,

$$\sigma(S_3(C^{j5})) = \sum_{i=0}^{2}(3-i)c_{(j+i)5}.$$

Hence, for $j = 0, 1, 2$, the values of the σ-function are either $\{2+\beta, 0, 2\beta+1\} = \{2, 0, 1\}$ if $\beta = 0$, or $\{2+\beta, 0, 2\beta+1\} = \{1, 0, 2\}$ if $\beta = -1$, which is a complete system of residues modulo $d = 3$.

As the third column in Table 3, we cannot use the former definition given in (6) if $\gcd(n,(\alpha-\beta)v_C(\beta)) \neq 1$. Thus, we need to find an efficient reference code in $\overline{C}$ to distinguish among the phase offsets of binary codes in $\overline{C}$.

For a given binary code $C \in B^n$, suppose that $\sigma(C) \equiv \gamma \pmod d$, where $d = \gcd(n,(\alpha-\beta)v_C(\beta))$ and γ is an integer with $0 \le \gamma \le d-1$. Then, we define a σ_d-function by $\sigma_d(C) = \sigma(C) - \gamma$ for the σ-function on B^n. Let s be a nonnegative integer with $a\sigma_d(R) \equiv ds \pmod{n/d}$ for the integer a such that $a(\alpha-\beta)v_R(\beta) \equiv -d \pmod{n/d}$. If a code $R \in \overline{C}$ satisfies the next two properties,

$$\sigma_d(R) \equiv 0 \pmod{n/d},\quad \sigma(S_d(R^{-s})) \equiv 0 \pmod d, \tag{7}$$

then we choose such a code R as a reference code of C in $\overline{C}$. Note that there always exists a unique R satisfying two conditions in (7) since $\gcd(n/d, d) \mid 0$. In fact, we will see that the required reference code can be determined naturally by the new NAPO given in the next section.

IV. A New NAPO Based on a σ_d-Function

We choose a binary code $C \in B^n$ and suppose that the binary code C satisfies the following two conditions:

(a) $\gcd(n,(\alpha-\beta)v_C(\beta)) = d$, and

(b) $\gcd(d,(\alpha-\beta)v_{S_d(C)}(\beta)) = 1$.

Then, consider a set $\overline{C} = \{C^i \,|\, 0 \le i \le n-1\}$ and a unique integer X_0 with $0 \le X_0 \le (n/d)-1$ satisfying

$$dX_0 \equiv a\sigma_d(C^i) \pmod{n/d} \tag{8}$$

for the integer a such that $a(\alpha-\beta)v_C(\beta) \equiv -d \pmod{n/d}$.

Also, consider a unique integer Y_0 with $0 \le Y_0 \le d-1$ satisfying

$$Y_0 \equiv b\sigma(S_d(C^{i-X_0})) \pmod d \tag{9}$$

for the integer b such that $b(\alpha-\beta)v_{S_d(C)}(\beta) \equiv -1 \pmod d$.

If R is a reference code of $C \in \overline{C}$ satisfying (7), then we can choose unique nonnegative integers q and r with $0 \le r \le (n/d)-1$ such that

$$P_R(C^i) = (n/d)q + r \tag{10}$$

for each fixed $C^i \in \overline{C}$ with $0 \le i \le n-1$.

Then, we will show that $r = X_0$ and $q = Y_0$. It is clear that $\sigma_d(C^i) = \sigma_d(C^i) - \sigma_d(R) \equiv \sigma(C^i) - \sigma(R) \pmod d$. Since $\sigma_d(C^i) \equiv -(\alpha-\beta)v_C(\beta)P_R(C^i) \pmod n$ by Theorem 1, $\sigma_d(C^i) + (\alpha-\beta)v_C(\beta)P_R(C^i) = nt$ for some nonnegative integers t. Hence,

$$\begin{aligned}\sigma_d(C^i) &\equiv -(\alpha-\beta)v_C(\beta)P_R(C^i)\\ &\equiv -(\alpha-\beta)v_C(\beta)X_0 \pmod{n/d}.\end{aligned}$$

So,

$$\begin{aligned}X_0 &\equiv a\sigma_d(C^i)/d\\ &\equiv [-a(\alpha-\beta)v_C(\beta)/d]r\\ &\equiv r \pmod{n/d}.\end{aligned} \tag{11}$$

On the other hand, it is clear that $P_R(C^{i-X_0}) = nq/d$. Thus, $C^{i-X_0} = C^{nq/d}$. This implies that

$$\begin{aligned}Y_0 &\equiv b\sigma(S_d(C^{i-X_0}))\\ &\equiv b\sigma(S_d(C^{nq/d}))\\ &\equiv [-b(\alpha-\beta)v_{S_d(C^i)}(\beta)]q\\ &\equiv q \pmod d.\end{aligned} \tag{12}$$

According to (8) through (12), the required phase offsets $P_R(C^i)$ of C^i's with respect to R can be obtained by

$$P_R(C^i)=(n/d)q+r=X_0+(n/d)Y_0. \quad (13)$$

It is easy to see that if we choose $R=C^t$ for an integer t with $0 \le t \le n-1$, then $P_R(C^i) \equiv i-t \pmod n$ for $i = 0, 1, \ldots, n-1$. Therefore $\{P_R(C^i) \mid i = 0,1,\ldots,n-1\}$ forms a complete well-ordering system of residues modulo n. If $d = 1$ in (13), then we can easily see that $P_R(C^i) \equiv a\sigma(C^i) \pmod n$, which indicates the phase offset given in (6).

For a given code

$$C = (\beta,\alpha,\beta,\alpha,\beta,\alpha,\alpha,\beta,\beta,\beta,\beta,\beta,\alpha,\beta,\alpha) \in B^{15},$$

the distinct phase offsets $P_R(C^i)$ of C^i's with respect to a reference code $R = C^{12}$ are calculated in Table 3 through the use of (7) and the algorithm given in (13). As the results from the table show, the new algorithm is very efficient to obtain distinct and well-ordering phase offsets of the shifted binary codes given in $\overline{C}$.

Table 3. $P_R(C^i)$ with α =1, β =0, gcd(15, $v_C(0)$)=3, a =3, and b=1. $P_R(C^i)$ with α =1, β =-1, gcd(15, $2v_C(-1)$)=3, a =4, and b=2.

C^i	$\sigma(C^i)$		$\sigma(C^i) \pmod n$		$\sigma_d(C^i) \pmod n$		X_0	Y_0	$P_R(C^i)$
	$\beta=0$	$\beta=-1$	$\beta=0$	$\beta=-1$	$\beta=0$	$\beta=-1$			
C^0	49	–22	4	8	3	6	3	0	3
C^1	55	–10	10	5	9	3	4	0	4
C^2	46	–28	1	2	0	0	0	1	5
C^3	52	–16	7	14	6	12	1	1	6
C^4	43	–34	13	11	12	9	2	1	7
C^5	49	–22	4	8	3	6	3	1	8
C^6	40	–40	10	5	9	3	4	1	9
C^7	31	–58	1	2	0	0	0	2	10
C^8	37	–46	7	14	6	12	1	2	11
C^9	43	–34	13	11	12	9	2	2	12
C^{10}	49	–22	4	8	3	6	3	2	13
C^{11}	55	–10	10	5	9	3	4	2	14
C^{12}	61	2	1	2	0	0	0	0	0
C^{13}	52	–16	7	14	6	12	1	0	1
C^{14}	58	–4	13	11	12	9	2	0	2

V. Conclusion

Interim Standard 95 (IS-95) [6] uses two PN generators to spread the signal power uniformly over a physical bandwidth of about 1.25 MHz, and the generated PN codes are referred to as the reference codes whose characteristic polynomials are primitive polynomials with degree 15 over a Galois field of order 2, and which have the same initial state code (000000000000001) of length 15. The phase offsets of the shifted binary codes in a signal set produced by each reference PN code play an important part in distinguishing between the received signal and locally generated signals in a mobile station of each cell, as well as in the acquisition of the received signals. Note that in this system, the start of the reference PN code is chosen arbitrarily without any background of the systematic and mathematical elaboration. In this letter, we developed an exact definition of a reference code in an arbitrary signal set $\overline{C}$, and described a numerical algorithm for phase offsets based on a σ-function modified from the results in [1] with the condition $\gcd(n,(\alpha-\beta)v_C(\beta)) = 1$. Furthermore, in the case of $\gcd(n,(\alpha-\beta)v_C(\beta)) \neq 1$, we proposed a new numerical algorithm to obtain the distinct and well-ordered phase offsets of shifted binary codes with respect to a reference code based on the σ_d-function in section IV.

In the CDMA system of IS-95, if we consider a reference PN code C generated by a PN generator such that the number of 0's in the given C is equal to 16383 and the signal set is $\overline{C}=\{C^i \mid 0 \le i < 2^{15}-1\}$, then $P_R(C^i) \equiv 2\sigma(C^i) \pmod{2^{15}-1}$ by (13). Thus, it follows from this that if we choose C^i satisfying $2\sigma(C^i) \equiv 0 \pmod{2^{15}-1}$ as a reference PN code in $\overline{C}$, then the number of shifted times in $\overline{C}$ with respect to the reference PN code is identical with the value of the required phase offset.

References

[1] Y. Han and Y. Song, "Phase Offset of Binary Code and Its Application to the CDMA Mobile Communications," *IEICE Trans. Fundamentals*, vol. E81-A, no. 6, 1998, pp. 1145-1151.

[2] Y. Song, *Enumeration of Phase Offsets for Binary Sequence*, Doctoral Dissertation, Hanyang University, 1998.

[3] M. Willet, "The Index of an M-Sequence," *SIAM J. Appl. Math.*, vol. 25, no. 1, 1973, pp. 24-27.

[4] D. M. Burton, *Elementary Number Theory,* 3rd ed., Wm. C. Brown, 1989.

[5] K. H. Rosen, *Elementary Number Theory and Its Applications*, 2nd ed., Addison-Wesley, 1988.

[6] TIA/EIA/IS95, *Mobile Station-Base Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System*, Telecommunication Industry Assoc., July 1993.