

論文98-35S-10-1

이원부호의 위상 오프셋과 CDMA 이동 통신에의 응용

(Phase Offset of Binary Code and Its Application to the CDMA Mobile Communications)

宋寧俊*, 韓榮烈**

(Song Young Joon and Han Young Yearl)

요 약

Code division multiple access (CDMA) 이동 통신 시스템에서는 각 기지국을 동일 확산 부호의 위상 오프셋 (phase offset)을 이용하여 구분하고 있으므로, 이 시스템에서 확산부호의 위상 오프셋을 안다는 것은 매우 중요하다. 부호의 주기가 길지 않을 경우는 한 부호와 이전된 부호 사이의 위상 오프셋은 두 부호를 비교하여 구할 수 있지만, 부호의 주기가 길어지면 이러한 방법으로는 어려움이 따른다. 본 논문은 정수론에 근거한 이원부호의 위상 오프셋 계산 방법을 제안한다. 본 논문에서 중심적 역할을 하는 누산함수를 정의하고, 그들의 관계를 규명한다. 이러한 정수론적 접근 방법에 의하여 유도된 결과들을 이용하여 이원부호의 위상 오프셋 계산이 매우 쉽게 이루어짐을 보인다. CDMA (code division multiple access) 이동 통신에의 응용과 위상 오프셋 산출 회로 구현도 논의된다.

Abstract

It is important to know phase offsets of a spreading code in the code division multiple access (CDMA) mobile communication systems because different phase offsets of the same spreading code are used to distinguish each base station. When the period of the code is not that long, the relative phase offset between the code and its shifted code can be found by comparing them, but as the period of the code increases it becomes difficult to find the phase offset. This paper describes a method to calculate the phase offset of a binary code based on the number theoretical approach. We define an accumulator function which plays a central role in this paper, and relationships between the functions are clarified. This number theoretical approach and their results show that this method is very easy for the phase offset calculation. Its application to the CDMA system and circuit realization of the phase offset calculation are also discussed.

I. 서 론

셀룰라 이동 통신에서의 용량 증가 필요성으로 인하여, 부호분할다원접속 (code division multiple access : CDMA) 시스템이 채택되게 되었다.

TIA/EIA/IS-95 CDMA 시스템^[1]에서 가입자와 기지국은 유용한 채널 대역폭에서 각 송신 신호를 확산하기 위한 부호와 가입자를 구분하기 위한 부호를 두어 통신한다. 대역 확산을 위한 두 가지의 부호는 각각 다른 특성다항식 (characteristic polynomial)을

* 正會員, LG電子미디어 通信研究所
(Media Communications Research Lab., LG Electronics Inc.)

** 正會員, 漢陽大學校 電子通信工學科

(Dept. of Electronics Communication Eng., Hanyang Univ.)

接受日字: 1997年10月13日, 수정완료일: 1998年7月29日

가지며, 다른 기능을 한다. 두 부호 중 한 가지는 한 셀 (cell) 내에서 모든 신호가 공유하는 I 와 Q 채널 PN (pseudo noise) 부호이며, 나머지 한 가지는 가입자를 구분하기 위한 long PN 부호이다. 이 시스템에서는 각 기지국을 동일 I, Q 채널 PN 확산 부호의 위상 오프셋을 이용하여 구분하고 있다. 그러므로 각 기지국 사이의 PN 부호의 위상 오프셋을 맞추어 주는 소프트 핸드오프 (soft handoff)가 가능해지며, 한 셀에 속한 이동국은 다른 기지국에서 수신된 신호를 동일한 I 와 Q 채널 PN 부호의 위상 오프셋을 이용하여 구분할 수 있다. 그러므로 CDMA 시스템에서 확산부호의 위상 오프셋 (phase offset)을 안다는 것은 매우 중요하다. 확산부호의 위상 오프셋을 구하기 위해서는 기준부호를 설정하여야 하는데, CDMA 시스템에서는 $r-1$ 개의 연속적인 '0'이 나온 후 처음으로 '1'이 나오는 부호를 기준부호로 설정하고 있다. 여기서 r 은 PN 부호 발생기의 쉬프트 레지스터(shift register) 수를 나타낸다. 이는 쉬프트 레지스터의 r 번째 초기 상태를 '1'로 두고 나머지 쉬프트 레지스터의 초기 상태는 '0'로 놓는 것을 의미한다. PN 부호의 주기가 길지 않을 경우는 한 부호에서 이전된 부호 사이의 위상 오프셋은 두 부호를 비교하여 구할 수 있지만, PN 부호의 주기가 길어지면 이러한 방법으로는 어려움이 따른다.

수학자 Willet은 제안된 방법과는 다른 방법으로 유한체 $GF(2)=(0,1)$ 의 최장부호 (maximal length sequence : m -sequence)의 인덱스 (index) 또는 위상 오프셋 (phase offset)을 계산하는 방법을 제안하였다^[2]. 그러나 Willet은 위상 오프셋을 계산하는 회로구성 방법에 관하여서는 제안하지 않았다. 본 논문에서는 정수론적 접근 방법에 근거하여, 이원부호의 주기가 n 이고 이원부호에 포함된 '0' 또는 '-1'의 개수가 k 일 때, n 과 k 가 서로 소의 조건을 만족하는 이원부호에 대한 위상 오프셋을 계산할 수 있는 보다 더 일반화된 위상 오프셋 산출 방법을 제시한다. 또한, 제안된 방법의 회로 구현에 관하여서도 논하며, 낮은 복잡도의 회로 구성으로 구현될 수 있음을 보인다. 위상 오프셋이 계산되어지기 위해서는 먼저, 이원부호의 각 비트에 연속적인 정수를 곱하고, 이렇게 가중치가 곱해진 값들을 모두 더한다. 그 다음, 법 (modulo) n 에 대한 대수적 역원을 산출하여 곱한다. 여기서, n 은 이원부호의 길이를 나타낸다. 마지막으로, 계산된 값에

법 n 연산을 취함으로써 원하는 위상 오프셋 값을 얻게 된다. 일단 기준부호가 정해지면, 계산된 수신 이원부호의 위상 오프셋 값은 기준부호에 대하여 계산된 위상 오프셋 값만큼 순회된 부호임을 나타낸다. 예를 들어, $(0,0,0,1,1,1,1)$ 을 기준부호로 설정하자. 그러면, 기준부호보다 4비트 오른쪽으로 순회된 부호 $(1,1,1,0,0,0)$ 는 기준부호에 대하여 4의 위상 오프셋 값을 가진다. 이러한 위상 오프셋 산출 방법에 근거하여, CDMA 시스템에서의 PN (pseudo noise) 부호에 대한 기준부호 설정에 관하여서도 논한다.

본 논문은 다음과 같이 구성된다. II장에서는 본 논문에서 사용될 정의와 보조정리에 대하여 설명하며, III장에서는 이원부호의 위상 오프셋 계산에 적용되는 주요 결과들을 도출한다. 그리고, IV장에서는 이원부호의 위상 오프셋 산출 알고리즘, 회로 구현, 그리고 CDMA 시스템에 있어서 PN 부호의 기준부호 설정에 관하여 논한다. 마지막으로 V장에서 결론을 맺는다.

II. 정의와 보조정리

먼저 n 쌍 (n -tuple)의 부호 C 와 순회 연산자 T 를 다음과 같이 정의한다.

$$\begin{aligned} C &= (C_0, C_1, \dots, C_{n-2}, C_{n-1}) \\ TC &= (C_{n-1}, C_0, \dots, C_{n-3}, C_{n-2}) \\ &\vdots \\ T^i C &= (C_{n-i}, C_{n-i+1}, \dots, C_{n-i-2}, C_{n-i-1}) \\ &\vdots \\ T^{n-1} C &= (C_1, C_2, \dots, C_{n-1}, C_0) \end{aligned} \quad (1)$$

그리고 $i \equiv j \pmod{n}$ 이면,

$T^i C = T^j C = (C_{n-j}, C_{n-j+1}, \dots, C_{n-j-1})$ 의 관계가 성립한다. 여기서 i, j 는 정수이다. 또한, $T^0 C = C$ 라고 정의한다. 부호 C 는 다음과 같은 다항식으로 표시된다.

$$C(x) = C_0 + C_1 x + \dots + C_{n-1} x^{n-1} = \sum_{i=0}^{n-1} C_i x^i \quad (2)$$

가중치가 1인 누산합수를 다음과 같이 정의한다.

$$A'(C) = \left. \frac{d}{dx} x^i C(x) \right|_{x=1} \quad (3)$$

여기서, l 은 임의의 정수이다. 부호 C 가 $A^l(C) \equiv 0 \pmod{n}$ 의 조건을 만족한다면, 이 부호를 가중치가 l 인 누산함수의 기준부호 (reference code) 또는 영 오프셋 부호 (zero offset code)라고 정의한다. 또한, 두 정수 l 과 m 이 $l \equiv m \pmod{n}$ 의 조건을 만족하면, $A^l(C) \equiv A^m(C) \pmod{n}$ 의 합동식 (congruence equation)이 성립한다. 누산함수 $A^l(C)$ 는 n 쌍의 이원부호 C 의 원소가 $C_i \in \{-1, 1\}$ 이면 $A^l_1(C)$ 로 표기하고, $C_i \in \{0, 1\}$ 이면 $A^l_0(C)$ 로 표기한다. 아래 첨자 없이 $A^l(C)$ 로 표기한 경우는 이원부호 C 의 원소가 두가지 집합 중 어디에 속하더라도 무관한 경우를 나타낸다.

다음의 누산함수와 관련된 보조정리는 이원부호의 위상 오프셋 계산에 사용된다.

보조정리 1 : 정수 i, l, m 에 대하여 다음이 성립한다.

$$A^l(T^i C) \equiv A^{l+i}(C) \pmod{n} \tag{4}$$

$$A^l(T^i C) - A^m(T^i C) = (l-m)C(1) \tag{5}$$

여기서 $C(1) = \sum_{i=0}^{n-1} C_i$ 이다.

증명 : 식 (4)는 누산함수의 정의 식 (3)과 식 (1), (2)에 의하여 다음과 같이 증명된다.

$$\begin{aligned} A^l(T^i C) &= \frac{d}{dx} x^l (C_{n-i} + C_{n-i+1}x + \dots + C_{n-1}x^{n-1}) \Big|_{x=1} \\ &= lC_{n-i} + (l+1)C_{n-i+1} + \dots + (l+i-1)C_{n-1} \\ &\quad + (l+i)C_0 + \dots + (l+n-1)C_{n-1} \\ &= (l+i)C_0 + \dots + (l+n-1)C_{n-1} + lC_{n-i} \\ &\quad + (l+1)C_{n-i+1} + \dots + (l+i-1)C_{n-1} \\ &\equiv [(l+i)C_0 + \dots + (l+n-1)C_{n-1} + (l+n)C_{n-i} \\ &\quad + (l+n+1)C_{n-i+1} + \dots + (l+i+n-1)C_{n-1}] \pmod{n} \\ &= \frac{d}{dx} x^{l+i} C(x) \Big|_{x=1} \pmod{n} \\ &= A^{l+i}(C) \pmod{n} \end{aligned} \tag{6}$$

그리고 누산함수의 정의 식 (3)과 식 (2)에 의하여 다음 식이 주어진다.

$$\begin{aligned} A^l(T^i C) &\equiv \frac{d}{dx} x^l C(x) \Big|_{x=1} \\ &\equiv \frac{d}{dx} x^l (C_{n-i} + C_{n-i+1}x + \dots + C_{n-1}x^{n-1}) \Big|_{x=1} \\ &\equiv lC_{n-i} + (l+1)C_{n-i+1} + \dots + (l+n-1)C_{n-1} \\ &\equiv l(C_{n-i} + C_{n-i+1} + \dots + C_{n-1}) + 0 + C_{n-i+1} + \dots + (n-1)C_{n-1} \\ &\equiv lC(1) + \frac{d}{dx} x^0 (C_{n-i} + C_{n-i+1}x + \dots + C_{n-1}x^{n-1}) \Big|_{x=1} \\ &\equiv lC(1) + A^0(T^i C) \end{aligned} \tag{7}$$

그리고, 식 (7)로부터 $A^l(T^i C) = lC(1) + A^0(T^i C)$ 와 $A^m(T^i C) = mC(1) + A^0(T^i C)$ 의 두 식이 얻어지므로, $A^l(T^i C) - A^m(T^i C) = (l-m)C(1)$ 의 결과 식을 얻을 수 있다.

보조정리 2 : k 를 n 쌍의 이원부호 C 에 포함된 '-1' 또는 '0' 원소의 개수라 할 때, 정수 i, j, l 에 대하여 다음이 성립한다.

$$A^l_1(T^{i+j} C) - A^l_1(T^i C) \equiv -2jk \pmod{n} \tag{8}$$

$$A^l_0(T^{i+j} C) - A^l_0(T^i C) \equiv -jk \pmod{n} \tag{9}$$

증명 : k 가 n 쌍의 이원부호 C 에 포함된 '-1'의 개수이면, '1'의 개수는 $n-k$ 이고 $C(1) = \sum_{i=0}^{n-1} C_i \equiv -2k \pmod{n}$ 이다. 그러면, 보조정리 1의 식(4), (5)에 의하여

$$\begin{aligned} A^l_1(T^{i+j} C) - A^l_1(T^i C) &\equiv (A^{l+i+j}_1(C) - A^{l+i}_1(C)) \pmod{n} \\ &= jC(1) \pmod{n} \\ &\equiv -2jk \pmod{n} \end{aligned} \tag{10}$$

이므로, 합동식 (8)이 성립한다.

유사한 방법으로, k 가 n 쌍의 이원부호 C 에 포함된 '0'의 개수이면, $C(1) \equiv -k \pmod{n}$ 이고 보조정리 1에 의하여

$$\begin{aligned} A^l_0(T^{i+j} C) - A^l_0(T^i C) &\equiv (A^{l+i+j}_0(C) - A^{l+i}_0(C)) \pmod{n} \\ &= jC(1) \pmod{n} \\ &\equiv -jk \pmod{n} \end{aligned} \tag{11}$$

이므로, 합동식 (9)가 성립한다.

III. 누산함수의 성질

이 장에서는 이원부호의 위상 오프셋을 계산하고 누산함수 사이의 관계를 규명하는 수학적 결과를 제시한다.

정리 1 : k 가 n 쌍의 이원부호 C 내에 포함된 '-1' 또는 '0'의 개수이고, $I = \{0, 1, \dots, n-1\}$ 라 할 때, $I = \{0, 1, \dots, n-1\}$ 에 대하여 $2k$ 와 n 의 최대공약수가 $(2k, n) = 1$ 이고, $C_i \in \{0, 1\}$ 에 대하여 k 와 n 의 최대공약수가 $(k, n) = 1$ 인 것은, 함수 $A_i(\bullet) \pmod{n}$ 와 $A_0(\bullet) \pmod{n}$ 가 집합 $B = \{T^i C \mid i \in I\}$ 을 집합 $\{0, 1, \dots, n-1\}$ 로 일대일 대응시키기 위한 필요충분조건이다. 즉, $C_i \in \{-1, 1\}$ 에 대하여 $(2k, n) = 1$ 이고 $C_i \in \{0, 1\}$ 에 대하여 $(k, n) = 1$ 인 것은 집합 $\{A_i(T^i C) \pmod{n} \mid i \in I\}$ 와 집합 $\{A_0(T^i C) \pmod{n} \mid i \in I\}$ 가 법 n 에 대하여 완전잉여계(complete residue system modulo n)이기 위한 필요충분조건이다.

증명 : 먼저 $C_i \in \{-1, 1\}$ 에 대하여 $(2k, n) = 1$ 이면 집합 $\{A_i(T^i C) \pmod{n} \mid i \in I\}$ 이 법 n 에 대하여 완전잉여 계임을 증명한다. 보조정리 2의 합동식 (8)에 의하여 다음 식이 성립한다.

$$\begin{aligned} A_1(T^{i+1}C) &\equiv (-2k + A_1(T^i C)) \pmod{n} \\ A_1(T^{i+2}C) &\equiv (-2k(2) + A_1(T^i C)) \pmod{n} \\ &\vdots \\ A_1(T^{i+n-1}C) &\equiv (-2k(n-1) + A_1(T^i C)) \pmod{n} \\ A_1(T^{i+n}C) &\equiv (-2kn + A_1(T^i C)) \pmod{n} \\ &\equiv A_1(T^i C) \pmod{n} \end{aligned} \quad (12)$$

$A_1(T^i C)$ 를 b 라 할 때, 집합 $\{b, -2k + b, \dots, -2k(n-1) + b\}$ 에는 집합 I 와 같은 수의 원소가 존재한다. 따라서, x_i 와 x_j 가 집합 I 의 원소일 때, $0 \leq i, j \leq n-1$ 인 두 정수 i, j 에 대하여, $i \neq j$ 이면 $2kx_i \not\equiv 2kx_j \pmod{n}$ 인 것을 보이면 된다. $(2k, n) = 1$ 인 가정으로부터, $2kx_i \equiv 2kx_j \pmod{n}$ 이면 $x_i \equiv x_j \pmod{n}$ 의 합동식이 성립하며 $i = j$ 이다.¹³ 그러므로 집합 $\{A_i(T^i C) \pmod{n} \mid i \in I\}$ 는 법 n 에 대하여 완전잉여계이다.

역으로, $2k$ 와 n 이 서로 소가 아니라고 가정할 때,

$$2kx_i + b \equiv 2kx_j + b \pmod{n} \text{ 이면 } x_i \equiv x_j \left(\pmod{\frac{n}{(2k, n)}} \right) \text{ 이다}$$

[3]. 그리고 $(2k, n) > 1$ 이므로 $(2k, n)$ 는 n 을 나누며, 이는 집합 $\{b, 2k + b, \dots, 2k(n-1) + b\}$ 에는 법 n 에 대하여 쌍으로 합동인 원소가 존재함을 의미한다.

유사한 방법으로, 집합 $\{A_0(T^i C) \pmod{n} \mid i \in I\}$ 에 대하여서도 위의 정리가 성립함을 보일 수 있다.

정리 2 : n 쌍의 이원부호 C 의 원소가 $C_i \in \{-1, 1\}$ 인 경우 $(2k, n) = 1$ 이고, $C_i \in \{0, 1\}$ 인 경우 $(k, n) = 1$ 이면

$$a^* [A_i(T^{i+j}C) - A_i(T^i C)] \equiv j \pmod{n} \quad (13)$$

$$a^* [A_0(T^{i+j}C) - A_0(T^i C)] \equiv j \pmod{n} \quad (14)$$

이다. 여기서, a^* 는 다음을 만족하는 법 n 에 대한 a 의 대수적 역원(arithmetic inverse)이다.

$$-2ka^* \equiv 1 \pmod{n} \text{ for } C_i \in \{-1, 1\} \quad (15)$$

$$-ka^* \equiv 1 \pmod{n} \text{ for } C_i \in \{0, 1\} \quad (16)$$

증명 : 먼저 합동식 (13)이 성립함을 보인다. 보조정리 2의 식 (8)에 의하여 $a^* [A_i(T^{i+j}C) - A_i(T^i C)] \equiv -2kia^* \pmod{n}$ 이다. n 쌍의 이원부호 C 의 원소가 $C_i \in \{-1, 1\}$ 이면 $(2k, n) = 1$ 이므로 $2kx + ny = 1$ 인 선형 방정식을 만족하는 두 정수 x 와 y 가 존재한다^[4]. 그리고, $2kx + ny = -2k(-x) + ny = 1$ 이고 $-2k(-x) \equiv 1 \pmod{n}$ 이다. 따라서 $a = -2k$ 라 할 때, 법 n 에 대한 a 의 대수적 역원 $a^* = -x$ 을 구할 수 있으므로, 식 (13)이 성립한다.

유사한 방법으로, n 쌍의 이원부호 C 의 원소가 $C_i \in \{0, 1\}$ 인 경우에도 식 (14)가 성립함을 보일 수 있다.

따름정리 1 : 이원부호 C 의 길이 n 이 $C_i \in \{-1, 1\}$ 인 경우 1보다 큰 홀수이고, $C_i \in \{-1, 1\}$ 인 경우 1보다 큰 정수일 때, 이원부호 C 가 정리 2의 (13) 또는 (14) 식을 만족하기 위한 k 의 개수는 오일러의 ϕ 함수(Euler ϕ -function), $\phi(n)$ 이다. 여기서, $k \in \{1, 2, \dots, n-1\}$ 이다.

증명 : 먼저 $C_i \in \{-1, 1\}$ 인 경우를 고려하자. 정리 2에 의하여 식 (13)이 n 쌍의 이원부호에 대하여 성립하기 위하여, $2k$ 는 n 과 서로 소이어야 한다. 가정에 의하여 n 은 1보다 큰 홀수이므로 2는 n 과 서로 소이다. 그리고 $2k$ 와 n 이 서로 소이기 위하여 k 는 n 과 서로 소이어야 한다. 그러므로, n 이 1보다 큰 홀수이고 $k \in \{1, 2, \dots, n-1\}$ 일 때, 식 (13)을 만족하는 k 의 개수는 $\phi(n)$ 이다.

$C_i \in \{0, 1\}$ 인 경우 정리 2에 의하여 식 (14)가 만족되기 위하여 k 와 n 은 서로 소이어야 한다. 그리고 n 이 1보다 큰 정수이므로 식 (14)를 만족하는 k 의 개수도 $\phi(n)$ 이다.

따름정리 2 : 이원부호 C 가 주기 n 인 PN 부호일 때, 다음이 성립한다.

$$A_i'(T^{i+j}C) - A_i'(T^iC) \equiv j \pmod{n} \quad (17)$$

$$2[A_0'(T^{i+j}C) - A_0'(T^iC)] \equiv j \pmod{n} \quad (18)$$

증명 : 이원부호 C 가 주기가 n 인 PN 부호이면, C 내에 포함된 '-1' 또는 '0'의 원소의 개수는 모두 $k = \frac{n-1}{2}$ 이다 [5]. $C_i \in \{-1, 1\}$ 인 경우, 식 (15)에 의하여 $a = -2k = -2\left(\frac{n-1}{2}\right) \equiv 1 \pmod{n}$ 이고 $a^* = 1$ 이다. 그리고 $C_i \in \{0, 1\}$ 인 경우, 식 (16)에 의하여 $a = -k \equiv n-k = \frac{n+1}{2} \pmod{n}$ 이므로, $a^* = 2$ 이다. 따라서, 정리 2의 식 (13)과 (14)에 의하여 식 (17)과 (18)이 성립한다.

정리 3 : n 쌍의 이원부호 C 의 원소가 $C_i \in \{-1, 1\}$ 인 경우 $(2k, n) = 1$ 이고 $C_i \in \{0, 1\}$ 인 경우 $(k, n) = 1$ 일 때, $a^*A^i(C) \equiv j \pmod{n}$ 이면 다음 식이 성립한다.

$$a^*A^m(T^{l-m+i-j}C) \equiv i \pmod{n} \quad (19)$$

증명 : $C_i \in \{-1, 1\}$ 에 대하여 $(2k, n) = 1$ 이고 $C_i \in \{0, 1\}$ 에 대하여 $(k, n) = 1$ 이므로, 정리 2에 의하여 $a^*[A^i(C) - A^i(T^{i-j}C)] \equiv (j-i) \pmod{n}$ 이다. 여기서 $a^*A^i(C) \equiv j \pmod{n}$ 이므로, $a^*A^i(T^{i-j}C) \equiv i \pmod{n}$ 임을 알 수 있다. 따라서, 보조정리 1의 합동식 (4)에 의하

여 다음이 성립한다.

$$\begin{aligned} a^*A^i(T^{i-j}C) &\equiv a^*A^{m-m+i}(T^{i-j}C) \pmod{n} \\ &\equiv a^*A^m(T^{l-m+i-j}C) \pmod{n} \\ &\equiv i \pmod{n} \end{aligned} \quad (20)$$

예를 들어 $C = (C_0, C_1, C_2, C_3, C_4) = (0, 0, 0, 1, 1)$ 인 경우, $n = 5$ 이고 $k = 3$ 이므로 $(n, k) = 1$ 이다. 그리고 법 5에 대한 $a = -3$ 의 대수적 역원은 $a^* = 3$ 이므로 표 1을 얻을 수 있다. 표 1의 각 열의 값은 가중치가 정해졌을 때 이원부호가 순회함에 따른 누산함수 값의 변화를 나타내고 있으며 법 5에 관하여 완전잉여계임을 알 수 있다. 그리고 표 1의 각 행의 값은 가중치의 변화에 따른 누산함수 값의 변화를 나타내고 있으며, 이도 또한 법 5에 대하여 완전 잉여계임을 알 수 있다. 그리고 정리 3의 누산함수들 간의 관계도 성립함을 확인할 수 있다.

표 1. $C = (C_0, C_1, C_2, C_3, C_4) = (0, 0, 0, 1, 1)$ 인 경우 $a^*A_0^i(\bullet) \pmod{5}$ 의 값
Table 1. Values of $a^*A_0^i(\bullet) \pmod{5}$ when $C = (C_0, C_1, C_2, C_3, C_4) = (0, 0, 0, 1, 1)$.

	$a^*A_0^0(\bullet) \pmod{5}$	$a^*A_0^1(\bullet) \pmod{5}$	$a^*A_0^2(\bullet) \pmod{5}$	$a^*A_0^3(\bullet) \pmod{5}$	$a^*A_0^4(\bullet) \pmod{5}$
C	1	2	3	4	0
T ¹ C	2	3	4	0	1
T ² C	3	4	0	1	2
T ³ C	4	0	1	2	3
T ⁴ C	0	1	2	3	4

IV. 응용

Willet은 다음과 같은 방법에 의하여 PN부호가 $\{0, 1\}$ 로 구성되었을 때 위상 오프셋을 아는 방법을 제시하였다 [2]. 유한체 $GF(2) = \{0, 1\}$ 에서 계열 $u = (u_i)_{i=0}^{\infty} = (u_0, u_1, u_2, \dots)$ 은 부호주기가 $t = 2^n - 1$ 인 PN 부호일 때, $I_k = \{i | 0 \leq i < 2^n - 1, u_{i+k} = 0\}$, $J_k = \{i | 0 \leq i < 2^n - 1, u_{i+k} = 1\}$, 즉, I_k 와 J_k 가 $\{u_k, u_{k+1}, \dots, u_{k-1}\}$ 의 '0'과 '1'의 위치를 나타낸다. 이 때, 위상 오프셋 M 은 $M \equiv \left\{ \sum_{i \in I_k} i - \sum_{i \in J_k} i \right\} \pmod{t} \equiv -2 \sum_{i \in I_k} i \pmod{t}$ 가 됨을 증명하였다. 이는 PN부호의 '0'의 위치를 더하여 (-2)를 곱함으로써 PN부호의 위상 오프셋을 구할 수 있음을 의미

한다. 예로써, PN부호가 (1,1,1,0,1,0,0)일 때, 위상 오프셋을 구하면 다음 표와 같다.

표 2. Willet의 방법에 의한 PN부호 (1,1,1,0,1,0,0)와 순회된 동일 PN부호의 위상 오프셋 값

Table 2. Phase offset values of PN code (1,1,1,0,1,0,0) and its shifted replicas using Willet's method.

위치							$-2\sum_{i=1}^7 i = A$	$A(\text{mod } 7)$
0	1	2	3	4	5	6		
1	1	1	0	1	0	0	-28	0
0	1	1	1	0	1	0	-20	1
0	0	1	1	1	0	1	-12	2
1	0	0	1	1	1	0	-18	3
0	1	0	0	1	1	1	-10	4
1	0	1	0	0	1	1	-16	5
1	1	0	1	0	0	1	-22	6

위의 방법은 {0,1}로 구성된 부호가 PN부호일 때 위상 오프셋을 알 수 있다. 그러나 Willet은 위 계산을 할 수 있는 회로구성 방법은 제시하지 않고 있다. 이 장에서는 II장과 III장에서 유도된 중요한 결과들을 이용하여 보다 더 일반화된 이원부호의 위상 오프셋 계산 방법과 회로구성 방법을 제시한다. 그리고 CDMA 시스템^[1]의 I와 Q 채널 PN 부호의 기준부호 설정에 관하여 논한다.

그림 1은 정리 2의 결과를 이용하여 이원부호의 주기가 n이고, 이원부호의 '0' 또는 '-1' 원소의 개수가 k일 때 $(k, n)=1$ 또는 $(2k, n)=1$ 의 조건을 만족하는 이원부호의 위상 오프셋을 산출하는 알고리즘을 나타내고 있다. 그림 1의 흐름도에 나타난 것과 같이, 먼저 주기가 n인 수신 이원부호 T'C를 계산하기 위한 누산함수의 가중치 l을 정하여 누산함수 $A'(T'C)$ 을 구한다. 그 다음, 이원부호의 원소가 {0,1}이면 $a^*(n-k) \equiv 1(\text{mod } n)$ 인 법 n에 대한 (n-k)의 대수적 역원 a^* 을 설정하고, {-1,1}이면 $a^*(n-2k) \equiv 1(\text{mod } n)$ 인 a^* 를 설정하여, 계산된 누산함수의 값에 곱하여 $a^*A'(T'C)$ 를 산출한다. 이어 modulo n 연산을 수행한 후 수신 이원부호의 위상 오프셋 값을 출력한다. 이 값은 수신 이원부호가 가중치가 l인 누산함수의 기준부호에 대하여 몇 비트 오른쪽으로 순회된 부호인지를 나타낸다. 예를 들어, 이원부호 C가 가중치가 l인

누산함수의 기준부호라고 가정하자. 그러면, 수신 이원부호 T'C는 기준부호 C에 대하여 오른쪽으로 i비트 순회된 동일 이원부호가 되는 것이다.

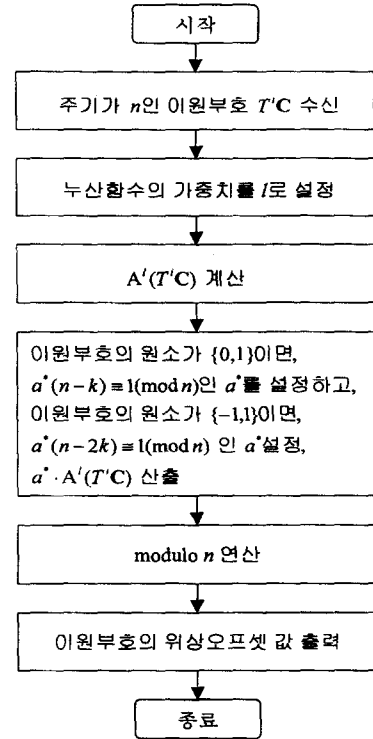


그림 1. 이원부호의 위상 오프셋 계산 흐름도
Fig. 1. Flow chart for calculating the phase offset of a binary code.

그림 2는 그림 1의 알고리즘에 기반하여 수신 이원부호의 위상 오프셋을 산출하는 구성도를 나타내고 있으며, II장의 누산함수의 정의식과 보조정리를 이용하여 구현할 수 있다.

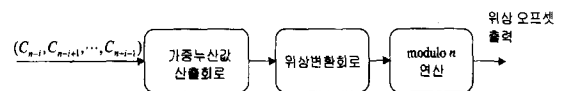


그림 2. 누산함수를 이용한 이원부호의 위상 오프셋 계산 구성도
Fig. 2. Block Diagram to calculate the phase offset of the binary code.

식 (5)에 의한 가중치가 l인 누산함수에 대한 보조정리에 의하여, 다음 식이 주어진다.

$$A'(T'C) = A'(T'C) + (l-1)C(l) \tag{21}$$

누산함수의 정의 식 (3)에 의하여, 식 (21)의 첫번째 항은 식 (22)로 주어지며, 그림 3의 회로 구성을 이용하여 계산할 수 있다.

$$\begin{aligned}
 A^1(T^iC) &= \frac{d}{dx} xC(x) \Big|_{x=1} \\
 &= \frac{d}{dx} (xC_{n-i} + x^2C_{n-i+1} + \dots + x^{n-1}C_{n-i-2} + x^nC_{n-i-1}) \Big|_{x=1} \\
 &= C_{n-i} + 2C_{n-i+1} + \dots + (n-1)C_{n-i-2} + nC_{n-i-1} \\
 &= C_{n-i-1} \\
 &\quad + (C_{n-i-1} + C_{n-i-2}) \\
 &\quad \vdots \\
 &\quad + (C_{n-i-1} + C_{n-i-2} + \dots + C_{n-i+1}) \\
 &\quad + (C_{n-i-1} + C_{n-i-2} + \dots + C_{n-i+1} + C_{n-i})
 \end{aligned} \tag{22}$$

그림 3에서 T_b 는 입력 이원부호의 한 비트 시간 간격을 나타낸다. 그림 3의 회로에서 이원부호 T^iC 의 첫번째 비트 C_{n-i-1} 는 시간 $t=T_b$ 에서 회로에 입력되어 누산기에 저장된다. 그리고, 그 값은 다시 1비트 지연기를 통하여 두번째 입력 비트인 C_{n-i-2} 와 더해진다. 이제, 더해진 값 ($C_{n-i-1} + C_{n-i-2}$)는 시간 $t=2T_b$ 에 다시 누산기의 새로운 입력 값이 된다. 회로의 동작 원리를 보다 더 명확히 설명하기 위하여, 여기서는 회로의 처리 시간 지연은 고려하지 않고 있다. 유사한 방법으로, 마지막 입력 비트 C_{n-i} 가 입력되면, 시간 $t=(n-1)T_b$ 에서 누산기의 입력 값인 ($C_{n-i-1} + C_{n-i-2} + \dots + C_{n-i+1}$)이 1비트 지연기를 통과한 후 C_{n-i} 와 더해진다. 그리고, 더해진 값은 시간 $t=nT_b$ 에서 누산기의 새로운 입력 값이 된다. 따라서 시간 $t=nT_b$ 에서 누산기의 출력 값은 식 (22)의 가중치가 1인 누산함수 값과 동일하게 된다. 식 (21)의 두번째 항은 그림 4를 이용하여 간단히 구현할 수 있다. 그러므로, 그림 3과 4를 합한 그림 5을 이용하여 식 (21)의 가중치가 1인 누산함수를 계산하는 회로를 구현할 수 있으며, 이 회로는 그림 2의 가중누산값 산출 회로가 된다.

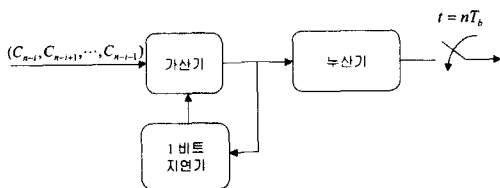


그림 3. $A^1(T^iC)$ 계산 회로 구성도
Fig. 3. Circuit block diagram to calculate $A^1(T^iC)$.

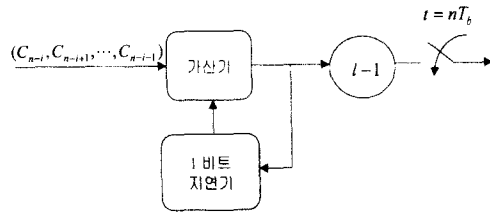


그림 4. $(l-1)C(l)$ 계산 회로 구성도
Fig. 4. Circuit block diagram to calculate $(l-1)C(l)$.

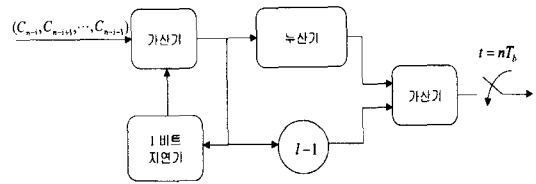


그림 5. $A^1(T^iC)$ 계산 회로 구성도
Fig. 5. Circuit block diagram to calculate $A^1(T^iC)$.

그림 2의 가중누산값 산출회로에 의하여 출력되는 값은 위상변환 회로를 통과하게 되는데, 이 위상변환 회로는 정리 2의 식 (15)와 (16)에 의하여 구해진 a^k 를 가중누산값 산출회로의 출력에 곱하는 역할을 한다. 그리고 a^k 은 식 (15)와 (16)에 언급된 것과 같이 이원부호의 원소가 $C_i \in \{0,1\}$ 인 경우는 $a^k(n-k) \equiv 1 \pmod{n}$ 인 대수적 역원이며, $C_i \in \{-1,1\}$ 인 경우는 $a^k(n-2k) \equiv 1 \pmod{n}$ 인 대수적 역원이다. 이렇게 수신 이원부호가 가중누산값 산출회로와 위상변환 회로를 거치고 나서, 마지막 막으로 modulo n 연산회로를 거치고 나면 원하는 수신 이원부호의 위상오프셋 값을 얻게 된다.

그림 6은 III장의 정리 3의 결과를 이용하여, 가중치가 다른 두 누산함수를 이용하여, 다른 경로를 통하여 입력된 부호들 사이의 위상 오프셋을 산출하거나, 수신되는 이원부호와 수신기내에 내장된 이원부호 발생기에서 생성된 이원부호와의 위상 오프셋을 산출하는 알고리즘의 흐름도로 나타내고 있다. 그리고, 그림 7은 가중치가 다른 두 누산함수를 이용하여, 다른 위상 오프셋을 가지는 두 동일 이원부호의 위상 오프셋을 계산하는 회로 구성을 나타내고 있다.

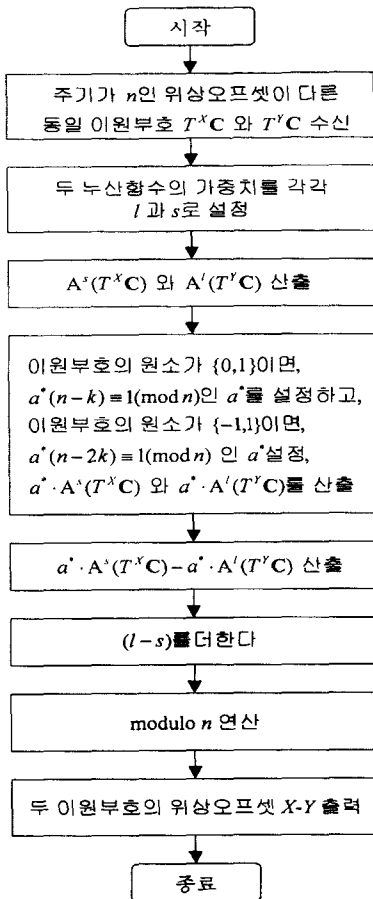


그림 6. 가중치가 다른 두 누산함수를 이용한 이원부호의 위상 오프셋 계산 흐름도
Fig. 6. Flow chart to find phase offset between the code and its shifted replica using two accumulator functions with different weights.

먼저 주기가 n 이고 위상 오프셋 X 와 Y 를 가지는 두 동일 이원부호 $T^X C$ 와 $T^Y C$ 에 대한 누산함수의 가중치 l 과 s 를 각각 설정하여, 누산함수의 값 $A^l(T^X C)$ 및 $A^s(T^Y C)$ 를 구한다. 그 다음, 이원부호의 원소가 $\{0,1\}$ 이면 $a^*(n-k) \equiv 1(\text{mod } n)$ 인 법 n 에 대한 $(n-k)$ 의 대수적 역원 a^* 를 설정하고, $\{-1,1\}$ 이면 $a^*(n-2k) \equiv 1(\text{mod } n)$ 인 a^* 를 설정하여, 계산된 누산함수 값에 곱하여 $a^*A^l(T^X C)$ 및 $a^*A^s(T^Y C)$ 를 산출한다. 이어 $a^*A^l(T^X C) - a^*A^s(T^Y C)$ 를 계산하여, 가중치의 차 $l-s$ 를 더하고, modulo n 연산을 수행한 후 두 이원부호의 위상 오프셋 $X-Y$ 를 출력한다. 만약, 그림 7에서

두 누산함수의 가중치를 동일하게 두고, $T^Y C$ 를 기준 부호로 설정한다면, $l-s=0$ 가 되어 그림 7은 그림 2가 됨을 알 수 있다.

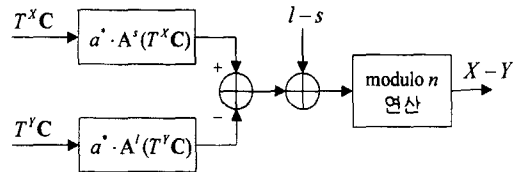


그림 7. 가중치가 다른 두 누산함수를 이용한 이원부호의 위상 오프셋 계산 회로 구성도
Fig. 7. Circuit block diagram to calculate the phase offset of the binary code and its shifted replica using two accumulator functions with different weights.

CDMA [1] [5] 이동통신 시스템에서는 이원부호의 자기상관 함수가 지연이 없을 때는 '1'이고 그 외의 자기상관 함수 값은 부호의 주기가 N 일 때 $-1/N$ 의 값을 갖는 최장부호가 중요한 역할을 한다. 이 최장 부호는 선형 쉬프트 레지스터 (shift register)를 사용하여 발생시킬 수 있는 주기가 최대가 되는 이원 부호이다. 이 부호는 수신기에서는 수신기의 동기, 채널의 임펄스 응답 (impulse response) 측정, 거리 측정, 암호화등에 사용된다.

TIA/EIA/IS-95 CDMA [1] 시스템에서는 부호 길이가 $2^{15}-1$ 인 short PN 부호와 $2^{42}-1$ 인 long PN 부호를 두어 통신한다. 대역 확산을 위한 두 가지의 부호는 각기 다른 특성다항식 (characteristic polynomial)을 가지며, 다른 기능을 한다. 두 부호 중 한 가지는 한 셀(cell) 내에서 모든 신호가 공유하는 (23), (24)의 특성다항식을 가지며, 그림 8의 발생기로부터 생성되는 I 와 Q 채널 short PN 부호이며, 나머지 한 가지는 가입자를 구분하기 위한 long PN 부호이다. CDMA 시스템에서는 식 (23)과 (24)의 생성 다항식으로 발생된 I 와 Q PN 동일 확산부호를 모든 셀에 할당하면서 각각 다른 위상 오프셋 값을 주어 셀을 구분하고 있다.

$$P_I(x) = x^{15} + x^{13} + x^9 + x^8 + x^7 + x^5 + 1 \quad (23)$$

$$P_Q(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^6 + x^5 + x^4 + x^3 + 1 \quad (24)$$

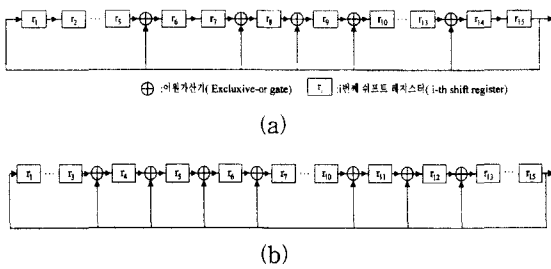


그림 8. (a) I 채널 PN 부호 발생기 (b) Q 채널 PN 부호 발생기

Fig. 8. (a) Sequence generator for I channel PN code. (b) Sequence generator for Q channel PN code.

그러므로 각 기지국 사이의 PN 부호의 위상 오프셋을 맞추어 주는 소프트 핸드 오프(soft handoff)가 가능해지며, 한 셀에 속한 이동국은 다른 기지국에서 수신된 신호를 동일한 PN 부호의 위상 오프셋을 이용하여 구분할 수 있으므로, CDMA 시스템에서 확산 부호의 인덱스 또는 위상 오프셋을 안다는 것은 매우 중요하다. 현재 CDMA 시스템에서 이동국은 순방향 파일럿 채널 (Pilot Channel)의 I, Q PN 확산 부호를 이용하여 15초 이내에 초기 동기기를 이룬 후 동기 채널 (Sync Channel)을 수신한다. 그리고 이동국은 이 동기 채널을 통하여 SID (System identification), NID (Network identification), PILOT_PN (Pilot PN sequence offset index), LC_STATE (Long code state), SYS_TIME (System time) 등의 CDMA 시스템 정보를 받아서, 이동국 자신의 long code timing과 system time을 CDMA 시스템에 맞춘다^[11]. 여기서 PILOT_PN은 자기가 속한 기지국의 PN 확산 부호의 위상 오프셋 정보를 나타낸다. 이렇게 이동국은 파일럿 채널과 동기 채널을 통하여 충분히 CDMA 시스템 타이밍 정보를 획득한 후, 페이징 채널 (Paging channel)을 통하여, System Parameter Message, Access Parameter Message, Neighbor List Message, Page Message, Channel Assignment Message 등의 제어 정보를 수신한다. 페이징 채널의 많은 제어정보 중 Neighbor List Message에는 인접 기지국의 PN 확산 부호 위상 오프셋 정보가 포함되어 있다^[11]. 따라서, 본 논문에서 제안된 수학적으로 명확한 방법으로 기준부호를 설정하고 그림 2의 구성을 이용하여 수신 확산 부호의 위상 오프셋을 계산한다면, 단말기는 기지국에서 인접

기지국의 확산부호 위상 오프셋 정보 없이, 스스로 인접 기지국에서 수신된 확산부호의 위상 오프셋을 산출하고, 신호를 복조할 수 있어 기지국의 업무를 그만큼 경감시킬 수 있음을 알 수 있다.

다음은 CDMA 시스템에 있어서 PN 확산부호의 기준부호 설정에 관하여 논한다. 임의의 기준부호가 설정되면, 이 기준부호의 위상 오프셋을 0으로 하고 이 부호를 m 번 순회시킨 부호의 위상 오프셋을 m 으로 정의한다. PN 부호의 주기가 길지 않을 경우는 한 부호에서 이전된 부호 사이의 위상 오프셋은 두 부호를 1대 1로 대응시켜 비교하여 구할 수 있지만, 부호의 길이가 길어지면 이원부호의 위상 오프셋을 알기란 용이치 않다. 우선 기준부호의 설정이 임의가 아니라 논리적이고 명확한 수학적 근거가 있어야 하며 또한 공학적으로 회로 구성이 용이하여야 한다. 하지만, 이 기준부호를 정하는 방법이 아직까지 존재하고 있지 않으므로, CDMA 시스템에서는 $r-1$ 개의 연속적인 '0'이 나온 후 처음으로 '1'이 나오는 부호를 기준 부호로 설정하고 있다. 이는 쉬프트 레지스터의 r 번째 초기 상태를 '1'로 두고 나머지 쉬프트 레지스터의 초기 상태는 '0'로 놓는 것을 의미한다. 여기서 r 은 PN 부호 발생기의 쉬프트 레지스터 수를 나타낸다. CDMA 시스템에서 정의한 방법으로 그림 8의 I와 Q 채널 확산부호의 초기상태를 정하면, 모두 $(r_1 r_2 \dots r_{15}) = (000000000000001)$ 이다. 이렇게 발생된 기준부호는 초기 상태를 용이하게 정하는 장점이 있지만 임의로 정한 것이다. 식 (23)과 (24)의 특성다항식으로 생성된 I와 Q 채널 확산부호의 주기는 모두 $n=32767$ 이며, 부호에 포함된 '0'의 개수 k 는 16383이다. 그리고 따름정리 2의 식 (18)에 의하여 $a = -k \equiv n - k \pmod{n} \equiv 16384$ 의 법 n 에 대한 a 의 대수적 역원은 $a^{-1} = 2$ 이다. C_1 와 C_0 가 PN 부호 발생기의 쉬프트 레지스터 초기 상태를 (000000000000001) 로 가지며, 각각 식 (23)과 (24)의 특성 다항식으로 생성된 PN 부호라 할 때, 가중치가 영인 누산합수로부터 다음을 구할 수 있다.

$$\begin{aligned} a^{-1} A_0^0(C_1) &\equiv 28287 \pmod{n} \\ a^{-1} A_0^0(C_0) &\equiv 30858 \pmod{n} \end{aligned} \quad (25)$$

그리고 정리 3에 의하여

$$\begin{aligned} a^* A_0^0 (T^{-28287} C_1) &\equiv 0 \pmod{n} \\ a^* A_0^0 (T^{-30858} C_0) &\equiv 0 \pmod{n} \end{aligned} \quad (26)$$

이다. 그러므로 식 (26)으로부터 C_1 와 C_0 를 각각 오른쪽으로 $(n - 28287) = 4480$ 번, $(n - 30858) = 1909$ 번 순회시킨 부호는 가중치가 영인 누산함수의 기준부호임을 알 수 있다. 그리고 $T^{4480} C_1$ 와 $T^{1909} C_0$ 두 부호는 각각 I 와 Q 채널 PN 부호 발생기의 쉬프트 레지스터 초기 상태를 (000010101000101)와 (001010000010001)로 두어 발생된다. 또한 보조정리 1의 식 (4)에 의하여

$$\begin{aligned} a^* A_0^{4480} (C_1) &\equiv 0 \pmod{n} \\ a^* A_0^{1909} (C_0) &\equiv 0 \pmod{n} \end{aligned} \quad (27)$$

이므로, 그림 8의 PN 부호 발생기의 쉬프트 레지스터 초기 상태를 (000000000000001)로 발생하는 PN 부호 C_1 와 C_0 는 각각 가중치가 4480이고 1909인 누산함수의 기준부호가 됨을 알 수 있다.

V. 결 론

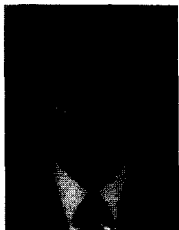
본 논문은 PN 부호를 포함하는 이원부호의 위상 오프셋 계산 방법을 정수론에 근거하여 제안하였다. 위상 오프셋의 해석에서는 누산함수가 중심적 역할을 하였으며, 가중치가 다른 두 누산함수의 관계도 규명하였다. 이러한 유도된 결과를 이용하여, 수신 이원부호의 원소가 $C_i \in \{0, 1\}$ 인 경우 $(k, n) = 1$ 이고, $C_i \in \{-1, 1\}$

인 경우 $(2k, n) = 1$ 의 조건을 만족하는 모든 이원부호에 대한 위상 오프셋을 매우 효율적으로 구할 수 있는 알고리즘을 제안하였다. 수신 이원부호의 위상 오프셋 계산에는 기준부호의 설정이 중요하므로, 본 논문에서 제안된 수학적이고 체계적인 방법으로, CDMA 시스템의 PN 확산부호 기준부호설정 방법에 관하여 논하였다. 또한 제안된 위상 오프셋 계산 방법을 구현할 수 있는 회로 구현에 대하여서도 논하였다.

참 고 문 헌

- [1] TIA/EIA/IS-95 Interim Standard, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System", July 1993.
- [2] M. Willet, "The Index of an M-sequence", SIAM J. Appl. Math. Vol. 25, No. 1, pp.24-27, July 1973.
- [3] I. Niven and H. S. Zuckerman, "An Introduction to the Theory of Number", John Wiley & Sons, 1980.
- [4] K. H. Rosen, "Elementary Number Theory and Its Applications", Bell Telephone Laboratories : Addison-Wesley Publishing Company, 1988.
- [5] R. E. Ziemer and R. L. Peterson, "Digital Communications and Spread Spectrum Systems", Macmillan, 1985.

저 자 소 개



宋寧俊(正會員)
1987년 2월 한양대학교 전자통신공학과 공학사. 1994년 2월 한양대학교 전자통신공학과 공학석사. 1994년 3월 ~ 현재 한양대학교 전자통신공학과 박사과정. 1994년 10월 ~ 현재 LG전자 미디어통신연구소 선임연구원. 주관 심분야는 디지털 이동통신

韓榮烈(正會員) 第34卷 S編 第11號 參照