論文 94-19-5-20

CDMA 시스템에서의 PN 부호 시간차 측정 기법

正會員 全 正 植* 正會員 韓 榮 烈**

Analysis for Time Offset of PN Sequence in CDMA System

Jung-Sig Jun*, Young Yearl Han** *Regular Members*

요 약

현존하는 셀룰라 이동통신의 가입자 수용 한계로 부호분할다원접속(CDMA) 방식을 사용하는 디지틀 셀룰라 통신 방식이 거론되고 있다. EIA/TIA 잠정 표준안인 CDMA 시스템에서는 동일한 확산부호를 전체 시스템에 사용하지만 각 기지국에 확산부호의 위상옵셉(phase-offset)을 다르게 배분함으로써 이동국은 기지국으로 송신된 신호를 구별하도록 하고 있다. 그러나 확산부호의 위상옵셉의 기준이 되는 영옵셉(zero-offset) 부호를 임의로 설정하고 있다.

본 논문은 확산부호의 기준 부호를 정하는 방법을 제시하고, 기준 부호로부터 위상을 이전(shift)시킨 부호 사이의 위상옵셉을 쉽게 계산하는 방법을 제시한다.

abstract

The need increased capacity in the cellular system has resulted in the adoption of digital technology with CDMA as the channel access method. It has been recognized that the distinction of the base station is important for its performance in CDMA, since the same spreading sequences are used by the all base stations. Time offset of the pseudo-random noise binary code are used to distinguish signals received at a mobile station from different base stations. But the start of the zero offset PN sequence is chosen arbitrary without the background of the systematic and mathematical elaboration.

This paper proposes a mothed that define the start of the zero offset PN sequence mathematically. This paper also discusses a methed that can easily calculate the time offset of the received spreading sequence with respect to the zero offset PN sequence.

*金星社 영상미디어 연구소
Goldstar
**漢陽大學校 電子通信工學科
Dept. of Electronic Communication Engineering Han Yang University.
論文番號 : 9449
接受日字 : 1994年 2月 17日

Ⅰ. 서 론

현재의 아나로그 통신 방식을 이용한 셀룰라 이동 통신 방식은 멀리 않아 무선 회선 용량이 포화 상태에 이를 것으로 예상되며, 모든 통신망의 종합 정보 통신망화 추세에 따라 음성뿐만 아니라 데이타, 영상 정보등 다양한 비음성계 서비스가 요구되고 있어, 디지탈 이동통신 시스템에 대한 개발이 활발히 추진 되고 있다.

부호분할다원접속 방식을 이용한 직접확산 통신 방식은 확산부호를 이용하여 대역을 확산시켜 통신하는 방식으로 기존의 아나로그 방식보다 수용용량이 증대하고 매 셀(cell)마다 동일한 주파수를 사용하여 주파수 배치 방법이 간단하고, 각 셀 사이의 핸드오프(handoff)도 PN 부호의 위상을 맞추어 주는 소프트 핸드오프(soft handoff)를 이용할 수 있으며 다중로에 의한 페이딩의 영향을 감소시킬 수 있는 장점을 가지고 있다. EIA/TIA CDMA 시스템에서는 동일한 확산부호의 위상옵셉을 갖는 확산부호를 각 기지국에 배당함으로써 이동국은 각 기지국으로부터 수신된 신호를 구별하고 있다. 확산부호의 위상옵셉을 주기 위해서는 영옵셉의 부호를 설정하여야 하는데, r을 쉬프트 레지스터(shift register)의 수라 할 때 EIA/TIA CDMA 잠정 표준안에서는 처음에(r-1)번 '0'이 나온 후 '1'이 나오는 부호를 영옵셉 부호로 정의하고 있다. 이것은 쉬프트 레지스트의 r번째 초기상태를 '1'로 놓고 나머지 쉬프트 레지스터의 초기상태는 '0'으로 놓는 것을 의미한다. 이러한 영옵셉 부호의 설정은 임의로 정한 것으로 단지 PN 부호 발생기의 쉬피트 레지스터의 초기 상태는 쉽게 만들 수 있다.

본 논문에서는 PN 부호뿐만 아니라 다른 부호의 영옵셉 부호를 정의하는 방법을 제시하고, 한 부호에서 이전(shift)된 부호 사이의 위상차를 쉽게 구하는 방법을 제시한다. 다음 장에서는 본 논문에 사용될 기호와 정의를 설명하고, 3장에서 영옵셉 부호를 설정하는 이론적 근거를 제시한다. 아울러 두 부호 사이의 위상차를 쉽게 찾아 내는 과정을 설명한다.

Ⅱ. 기초와 종의

먼저 n쌍(n-tuple)의 부호(sequence)를 다음과 같이 정의한다.

$$C^0=(C_0, C_1, \cdots, C_{n-2}, C_{n-1}) \tag{1}$$

$$C^1=(C_1, C_2, \cdots, C_{n-1}, C_0) \tag{2}$$

$$\vdots$$

$$C^i=(C_i, C_{i+1}, \cdots, C_{i-2}, C_{i-1}) \tag{3}$$

$$\vdots$$

$$C^{n-1}=(C_{n-1}, C_0, \cdots, C_{n-3}, C_{n-2}) \tag{4}$$

C^0가 정의되면 C^i, $0\le 0\le i\le n-1$,는 C^0를 왼쪽으로 i번 순환이전(cyclic shift)시켜서 얻을 수 있다. 또한 $C^i=C^{i+n}$인 주기성을 갖는다. 각 부호의 원소들은 {1, 0} 또는 {1, −1}로 구성되는 이진 심볼로 가정한다.

본 논문에서 새로이 정의하는 $A(C^i)$를 다음과 같이 정의한다.

$$A(C^i)=\int_0^n [C_i\cdot u(t)+C_{i+1}\cdot u(t-1)+\cdots+ C_{i-1}\cdot u(t-n+1)]\,dt \tag{5}$$

여기서 u(t)는 단위 계단 함수(unit step function)이고, 부호의 비트(bit) 길이는 1초로 가정하고 있지만 비트 길이는 임의의 값을 가질 수 있다. $A(C^i)$를 다른 표현으로 쓰면 다음과 같다.

$$A(C^i)=C_i+\sum_{j=0}^{1} C_{i+j}+\sum_{j=0}^{2} C_{i+j}+\cdots+\sum_{j=0}^{n-1} C_{i+j}$$

$$=n\cdot C_i+(n-1)\cdot C_{i+1}+\cdots+1\cdot C_{i-1} \tag{6}$$

$A(C^i)$는 부호열 내의 n개의 원소 각각에 '1~n' 사이의 다른 부가치(weight)를 곱한 합이라 볼 수 있다. 부호가 {1, 0}로 구성된 부호에서 구한 $A(C^i)$를 $A_0(C^i)$로 표시하고, {1, −1}의 부호로 구성된 부호에서 구한 $A(C^i)$ 값은 $A_1(C^i)$로 표시한다. 첨자 없이 A(C)와 C로 표기한 것은 첨자의 값이 어떠한 값을 가지더라도 만족할 때를 나타낸다. 따라서 A(C)와 C는 n 쌍의 부호를 대표하는 표기이다. 또한 부호어가 {1, 0}로 구성된 부호인 경우를 case 0, {1, −1}로 구성된 경우를 case 1이라 하자. A(C)에 대한 자세한 설명은 3장에서 다루고 있다.

n쌍의 부호에서 C^0를 기준 부호(reference sequence) 또는 영옵셉 부호라 정의하고 다음을 만족한다.

$$A(C^0) \pmod n = 0 \pmod n \tag{7}$$

기준 부호 C^0는 n 쌍의 부호 중 서로 다른 두 부호의 위상차를 구하는데 기준이 되며, 부호의 길이 n과 부호 내의 원소 중 '0'의 수가 k일때 〈case 0〉

$$\gcd((n-k), n)=1 \tag{8}$$

이고, 부호 길이 n과 부호 내의 '−1'의 갯수 k〈case 1〉의 관계가 다음과 같을 때

$$\gcd(2\cdot(n-k), n)=1 \tag{9}$$

식 (8)과 (9)를 만족하는 n 쌍의 부호는 모두 기준 부호 C^0를 갖는다. (PN 부호도 이 경우에 해당한다.)

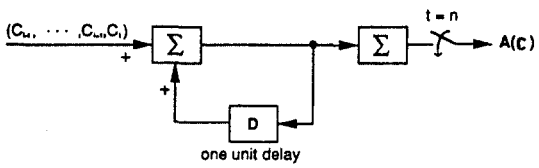


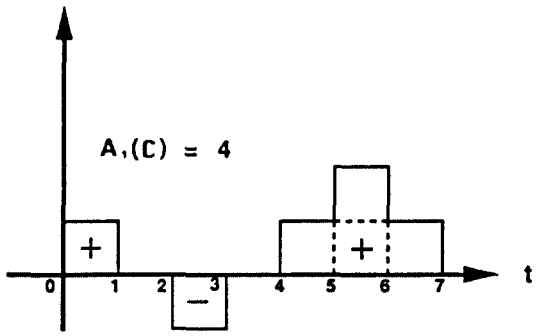
그림 1. A(C) 발생기.
Fig 1. Realization of A(C) calculation.

그림 1은 A(C)를 구하는 블록도로써 식(6)과 같은 값을 출력한다.

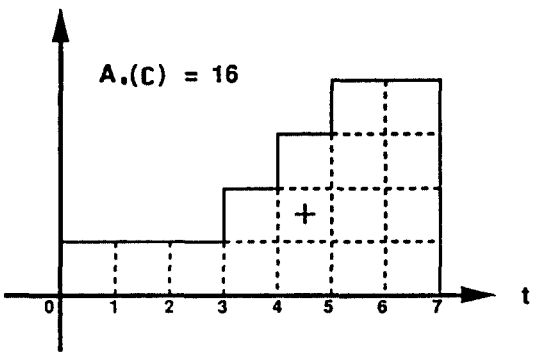
1비트가 1심볼 일 때 {1, 0} 또는 {1, −1}의 원소를 가지는 부호의 각 심볼은 앞 심볼까지의 결과인 1 심볼 지연기(1 symbol delay)의 출력과 더해지고 이 결과가 적분기 입력된다. 한 주기의 모든 심볼이 도착하면 스위치를 닫아 적분기의 값을 출력한다. 이때의 값이 A(C)의 값이다. 여기서 한 심볼은 1초의 길이를 갖는다.

주기가 7인 부호 C=(1, −1, −1, 1, 1, 1, −1) 또는 C=(1, 0, 0, 1, 1, 1, 0)가 그림 1의 덧셈기에 입력된다고 하자. 두 부호에 대한 적분기의 입력이 그림 2에 그려져 있다.

한 심볼의 길이가 1초라고 할 때 이들 부호의 한 주기, 즉 7초가 지난 다음 스위치를 닫아서 얻는 최종 출력은 그림 2의 함수 값을 7초 동안 적분해서 얻은 값이 된다.



(a) $A_1(C)$의 값, C = (1, -1, -1, 1, 1, 1, -1).



(b) $A_0(C)$의 값, C = (1, 0, 0, 1, 1, 1, 0).

그림 2. A(C)의 값.
Fig 2. Values of A(C).

Ⅲ. A(C)의 성질

2장에서 정의된 A(C)와 영옵셉 부호에 대해 자세히 살펴보자.

$A(C^i)$는 식 (6) 또는 그림 1에 의해 쉽게 구할 수 있다.

【정리 1】 k를 n 쌍의 부호 원소내에 포함되어 있는 '−1' 또는 '0'의 갯수라 할 때

$$A_1(C^{i+1}) - A_1(C^i) = -2\cdot k \text{ or } 2\cdot(n-k) \quad 0<k\le n-1,\ n\ge 2 \tag{10}$$

$$A_0(C^{i+1}) - A_0(C^i) = -k \text{ or } (n-k) \quad 0<k\le n-1,\ n\ge 2 \tag{11}$$

이다.

〈증명〉 먼저 식 (10)을 증명해 보자 식(6)에서 다음을 얻을 수 있다.

$$A_1(C^{i+1})-A_1(C^i)=[n\cdot C_{i+1}+(n-1)\cdot C_{i+2}+\cdots+C_i]$$
$$-[n\cdot C_i+(n-1)\cdot C_{i+1}+\cdots+C_{i-1}]$$
$$=\underbrace{C_{i+1}+C_{i+2}+\cdots+C_{i-2}+C_{i-1}}_{(n-1)\text{ elements}}+(1-n)\cdot C_i$$

① $C_i=1$이면 $(n-1)$개의 중 부호 내에 k개의 '-1'이 있으므로 밑줄친 $(n-1)$개의 원소 중 $(n-k-1)$개의 '1'과 k개의 '-1'이 있다. 따라서

$$A_1(C^{i+1})-A_1(C^i)=(n-k-1)\cdot 1+k\cdot(-1)+(1-n)\cdot 1=-2\cdot k$$

② $C_i=-1$이면 밑줄친$(n-1)$개의 원소 중 $(k-1)$개의 '-1'과 $(n-k)$개의 '1'이 있으므로

$$A_1(C^{i+1})-A_1(C^i)=(n-k)\cdot 1+(k-1)\cdot(-n)$$
$$+(1-n)\cdot(-1)=2\cdot(n-k)$$

따라서 식 (10)이 성립한다.
식(11)은 식(10)의 경우와 유사하게 다음과 같이 증명된다.

$$A_0(C^{i+1})-A_0(C^i)=-k \text{ or } (n-k),\ 0<k\le n-1,\ n\ge 2$$
$$A_0(C^{i+1})-A_0(C^i)=[n\cdot C_{i+1}+(n-1)\cdot C_{i+2}+\cdots+C_i]$$
$$-[n\cdot C_i+(n-1)\cdot C_{i+1}+\cdots+C_{i-1}]$$
$$=\underbrace{C_{i+1}+C_{i+2}+\cdots+C_{i-2}+C_{i-1}}_{(n-1)\text{ elements}}+(1-n)\cdot C_i$$

① $C_i=1$, 밑줄친 $(n-1)$개의 원소 중 k개의 '1'이 존재하므로

$$A_1(C^{i+1})-A_1(C^i)=(n-k-1)\cdot 1+k\cdot 0+(1-n)\cdot 1=-k$$

② $C_i=0$, 이 경우는 $(k-1)$개의 '0'과 $(n-k)$개의 '1'이 밑줄친 $(n-1)$개의 원소 중에 포함되어

$$A_1(C^{i+1})-A_1(C^i)=(n-k)\cdot 1+(k-1)\cdot 0+(1-n)\cdot 0=(n-k)$$

이 된다.

식(10)과 식(11)의 성질을 4장의 예제 1이 잘 예시하고 있다.

【정리 2】

$$-2\cdot k\ (\mathrm{mod}\ n)=2\cdot(n-k)\ (\mathrm{mod}\ n)=2\cdot(n-k) \quad (12)$$

$$-k\ (\mathrm{mod}\ n)=(n-k)\ (\mathrm{mod}\ n)=(n-k) \quad (13)$$

성질 2의 증명은 정수론을 다룬 책[2][4]에서 쉽게 찾아볼 수 있으므로 생략한다.

【정리 3】 k를 부호내의 '-1' 또는 '0'의 갯수하고 n을 부호의 길이라 하자. 또한 k와 n의 최대공약수(greatest common divisor)를 1, 즉 $\gcd(n, k)=1$이라 하자.

이때 홀수 n에 대한 집합 $B\in\{A_1(C^i),\ i=0, 1, \cdots, n-1\}$〈case 1〉과 양의 정수 n에 대한 집합 $B'\in\{A_0(C^i),\ i=0, 1, \cdots, n-1\}$〈case 0〉는 '0'과 '$n-1$' 사이의 정수 집합 $I\in\{0, 1, \cdots, n-1\}$에 일대일 대응한다. 즉 $A(C^i)\ (\mathrm{mod}\ n)$, $0\le i\le n-1$, 은 법(modulo) n에 대한 완전 잉여계이다.

〈증명〉 case 1의 경우를 먼저 증명해 보자
식 (10)에 의해

$$A_1(C^{i+1})\ (\mathrm{mod}\ n)-A_1(C^i)\ (\mathrm{mod}\ n)\equiv -2\cdot k\ (\mathrm{mod}\ n)$$

이다. $A_1(\cdot)\ (\mathrm{mod}\ n)$을 우변으로 옮기면

$$A_1(C^{i+1})\ (\mathrm{mod}\ n)\equiv -2\cdot k\ (\mathrm{mod}\ n)+A_1(C^i)\ (\mathrm{mod}\ n) \quad (14)$$

또 식 (14)의 i에 $i+1$을 대입하면

$$A_1(C^{i+2})\ (\mathrm{mod}\ n)\equiv -2\cdot k\ (\mathrm{mod}\ n)-A_1(C^{i+1})\ (\mathrm{mod}\ n) \quad (15)$$

식 (15)에서 식 (14)를 빼면

$$A_1(C^{i+2})\ (\mathrm{mod}\ n)\equiv -2\cdot(2\cdot k)\ (\mathrm{mod}\ n)+A_1(C^i)\ (\mathrm{mod}\ n) \quad (16)$$

이고, 식(14), (15) 그리고 (16)의 관계를 이용하여 다음을 얻는다.

$$A_1(C^{i+1})\ (\mathrm{mod}\ n)\equiv -2\cdot(1\cdot k)\ (\mathrm{mod}\ n)+A_1(C^i)\ (\mathrm{mod}\ n) \quad (17)$$
$$A_1(C^{i+2})\ (\mathrm{mod}\ n)\equiv -2\cdot(2\cdot k)\ (\mathrm{mod}\ n)+A_1(C^i)\ (\mathrm{mod}\ n) \quad (18)$$
$$\vdots$$
$$A_1(C^{i+j})\ (\mathrm{mod}\ n)\equiv -2\cdot(j\cdot k)\ (\mathrm{mod}\ n)+A_1(C^i)\ (\mathrm{mod}\ n) \quad (19)$$

$$\vdots$$

$$A_1(C^{i+n}) \pmod n \equiv -2\cdot(n\cdot k) \pmod n + A_1(C^i) \pmod n \quad (20)$$

n과 k는 서로소 즉 gcd(n, k)=1,이므로 $-1\cdot k \pmod n$, $-2\cdot k \pmod n$, …, $-n\cdot k \pmod n$는 n개의 서로 다른 값을 가진다. 이들 n개의 서로 다른 값들은 n보다 작고, 음의 정수가 아닌 값, 0~(n−1) 사이의 서로 다른 값을 가지므로 완전 잉여계를 형성한다. n이 홀수이고, x가 법 n에 대한 완전 잉여계의 원소일 때 2·x+b(b는 정수)는 완전 잉여계를 형성한다[2]. 이는 법 n에 대한 완전 잉여계의 원소에 n과 서로소인 값을 곱하여도 완전 잉여계를 이탈하지 않으며 완전 잉여계의 원소에 임의의 정수를 더하여도 완전 잉여계를 형성함을 보여준다.

이 성질에 의하여 $A_1(C^i)$가 정수일 때 $A_1(C^{i+1})$, … , $A_1(C^{i+(n-1)})$는 법 n에 대한 완전 잉여계를 형성한다. 따라서 홀수인 정수인 n에 대한 집합 $B \in \{A_1(C^i),\ i=0,\ 1,\cdots,\ n-1\}$는 정수 집합 $I \in \{0,\ 1,\ \cdots,\ n-1\}$에 일대일 대응 한다.

case 0의 경우도 case 1과 비슷하게 다음과 같이 증명할 수 있다.

식(11)에 의해

$$A_0(C^{i+1}) \pmod n - A_0(C^i) \pmod n \equiv -k \pmod n$$

를 얻고, 이 식을 이용하여 다음 식을 구할 수 있다.

$$A_0(C^{i+1}) \pmod n \equiv -1\cdot k \pmod n + A_0(C^i) \pmod n \quad (21)$$

$$A_0(C^{i+2}) \pmod n \equiv -2\cdot k \pmod n + A_0(C^i) \pmod n \quad (22)$$

$$\vdots$$

$$A_0(C^{i+j}) \pmod n \equiv -j\cdot k \pmod n + A_0(C^i) \pmod n \quad (23)$$

$$\vdots$$

$$A_0(C^{i+n}) \pmod n \equiv -n\cdot k \pmod n + A_0(C^i) \pmod n \quad (24)$$

이다. $-1\cdot k$, $-2\cdot k$, … , $n\cdot k$는 k와 n이 서로소이므로 법 에 대한 완전 잉여계를 형성한다. 또한 $A_0(C^i)$가 정수이므로 $-1\cdot k + A_0(C^i)$, … m $-n\cdot k + A_0(C^i)$도 법 n에 대한 완전 잉여계를 형성한다. 따라서 집합 $B' \in \{A_0(C^i),\ i=0,\ 1,\ \cdots,\ n-1\}$는 집합 $I \in \{0,\ 1,\ \cdots,\ n-1\}$에 일대일 대응 한다.

정리 3은 $A(C^i)$가 부호의 위상차를 구할 수 있는 이론적 근거를 제시한다. n이 2가 아닌 소수이고, k가 '1'과 'n−1' 사이의 정수일 때 $A(C^i) \pmod n$은 완전 잉여계를 형성한다. 그러나 k가 '0'이나 'n'이면, $A(C^i) \pmod n$은 항상 같은 값을 가져 완전 잉여계를 형성하지 않는다.

【정리 4】 주기가 n인 PN 부호일 때

$$[A_1(C^{i+1}) - A_1(C^i)] \pmod n \equiv j \quad 0 \le i \le n-1,\ 0 \le j \le n-1 \quad (25)$$

이다.

〈증명〉 case 1인 경우 PN 부호의 주기가 n일 때 부호의 원소 중 '−1'의 갯수 k는 (n−1)/2이다[3]. 정리 3의 식(19)로 부터 다음을 구할 수 있다.

$$A_1(C^{i+1}) \pmod n - A_1(C^i) \pmod n \equiv [A_1(C^{i+j}) - A_1(C^i)] \pmod n$$

$$\equiv -2\cdot(j\cdot k) \pmod n \equiv -2\cdot[j\cdot(n-1)/2] \pmod n \equiv j$$

【정리 5】 $\gcd(2\cdot(n-k),\ n)=1$〈case 1〉이거나, $\gcd(n-k),\ n)=1$〈case 0〉일 때 다음이 성립한다.

$$a^*\cdot[A_1(C^{i+j}) - A_1(C^i)] \pmod n \equiv j \quad (26)$$

$$a^*\cdot[A_0(C^{i+j}) - A_0(C^i)] \pmod n \equiv j \quad (27)$$

여기서 a^*는 다음 식을 만족하는 법 n에 대한 대수적 역원(arithmetic inverse)이다.

$$2\cdot(n-k)\cdot a^* \equiv 1 \pmod n \quad \text{for } C_i \in \{1,\ -1\} \quad (28)$$

$$(n-k)\cdot a^* \equiv 1 \pmod n \quad \text{for } C_i \in \{1,\ 0\} \quad (29)$$

〈증명〉 식 (19)에서 다음을 얻을 수 있다.

$$a^*\cdot[A_1(C^{i+j}) \pmod n - A_1(C^i) \pmod n] \pmod n$$

$$\equiv a^*\cdot[A_1(C^{i+j}) - A_1(C^i)] \pmod n$$

$$\equiv -2\cdot(j\cdot k)\cdot a^* \pmod n \equiv j\cdot 2\cdot(n-k)\cdot a^* \pmod n$$

식 (28)에서

$$2\cdot(n-k)\cdot a^* = 1 \pmod n$$

이므로

$$a^* \cdot [A_1(C^{i+j}) - A_1(C^i)] \pmod n = j$$

가 성립한다. 또한 식 (23)으로 부터

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

을 얻고, 식(29)를 이용하여

$$(n-k) \cdot a^* \equiv 1 \pmod n$$

을 얻고,

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

가 성립함을 알 수 있다.
$2 \cdot (n-k)$를 a로 두고 gcd(a, n)=1이라 할 때 $a \cdot x + n \cdot y = 1$을 만족하는 x와 y가 존재한다[4]. 또한

$$(a \cdot x + n \cdot y) \pmod n \equiv a \cdot x \pmod n \equiv 1 \pmod n \quad (30)$$

을 만족한다. a의 대수적 역원을 a^*라 하면

$$a \cdot a^* \pmod n \equiv 1 \pmod n \quad (31)$$

을 만족한다. 식 (31)에 의해 x는 법 n에 대한 대수적 역원이다. 따라서 gcd(2·(n-k), n)=1일때 2·(n-k)는 법 n에 역원을 가진다. 또한 (n-k)를 a로 두고 gcd(a, n)=1인 경우에도 식(30)과 식(31)을 만족하므로 gcd((n-k), n)=1일 때도 (n-k)는 법 n에 대한 대수적 역원을 가진다.

양의 정수 a의 법 n에 대한 대수적 역원이나 다음 식과 같이 Euler 정리를 사용한다.

$$a \cdot a^* = a \cdot a^{\phi(n-1)} = a^{\phi(n)} = 1 \pmod n \quad (32)$$

여기서 $\phi(n)$은 Euler의 ϕ 함수 $\phi(n)$가 n보다 작은 양의 정수 j라 할 때 $A(C) \pmod n$이 집합 $B \in \{A(C^i),\ i=0, 1, \cdots, n-1\}$에서 집합 $I \in \{0, 1, \cdots, n-1\}$에 일대일 대응될 수 있는 k의 값은 Euler의 ϕ 함수 값 j이다.
표 1은 $n \le 25$인 $\phi(n)$의 값을 보여준다.

표 1. $n \le 25$인 $\phi(n)$의 값.
Table 1. Values of $\phi(n)$ for $n \le 25$.

n	2	3	4	5	6	7	8	9	10	11	12	13
$\phi(n)$	1	2	2	4	2	6	4	6	4	10	4	12
n	14	15	16	17	18	19	20	21	22	23	24	25
$\phi(n)$	6	8	8	16	6	18	8	12	10	22	8	20

위와 같은 정리들에 의해 함수 $A_1(C)$ 또는 $A_0(C)$와 기준 부호 $[A(C^i \equiv 0 \pmod n)]$ 사이의 시간차를 구할 수 있고, 또한 시간차가 d인 두 부호의 시간차를 구할 수 있다.

길이가 n이고, 부호 내의 '-1', 또는 '0'인 원소들의 갯수가 k일 때, n, k가 gcd(2·(n-k), n)=1〈case 1〉또는 gcd((n-k), n)=1〈case 0〉을 만족하는 경우(PN 부호는 항상이 조건을 만족한다), A(C)를 이용하여 수신기에 저장되어 있는 부호의 함수값 $A(C)_S$와 수신된 부호의 함수 값 $A(C)_R$로 부터 두 부호 사이의 위상차를 구하여 수신기의 동기에 응용할 수 있는데 절차는 다음과 같다.

(1) 수신기에 저장되어 있는 부호에서 $A(C)_S \pmod n$을 얻고,

(2) 수신된 부호로부터 $A(C)_R \pmod n$을 구하여,

(3) $[A(C)_R \pmod n - A(C)_S \pmod n] \pmod n$을 계산한다.

(4) 법 n에 대한 2·(n-k)의 대수적 역원〈case 1〉또는 (n-k)의 대수적 역원〈case 0〉을 다음과 같이 구한다.

$$2 \cdot (n-k) \cdot a^* \equiv 1 \pmod n \langle \text{case } 1 \rangle$$
$$(n-k) \cdot a^* \equiv 1 \pmod n \quad \langle \text{case } 0 \rangle$$

(5) $[A(C)_R \pmod n - A(C)_S \pmod n] \pmod n$
$\equiv a^* [A(C)_R - A(C)_S] \pmod n$을 계산한다.

이러한 절차를 거쳐서 얻은 값이 수신기에 저장되어 있는 부호와 수신된 부호 사이의 시간차가 된다.

만약 수신기에 저장되어 있는 부호가 기준 부호인 경우는 $a^* \cdot A(C)_R \pmod n$이 곧 두 부호 사이의 시간차가 된다. 또한 {1, -1}로 구성된 PN 부호의 법 n에 대한 대수적 역원 a^*는 '1'이다.

Ⅳ. 예 제

〈예제 1〉 원시 다항식이 $g(x) = 1 + x + x^4$이고, 초기조건이 (1111)인 15 bit의 PN 부호가 그림 3으로

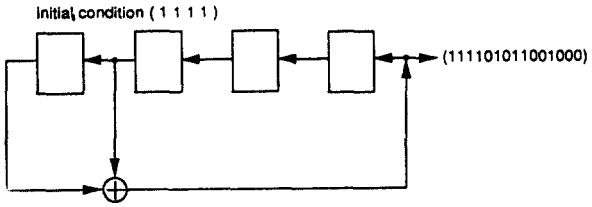


그림 3. 4단 PN 부호 발생기.
Fig 3. PN sequence generated by 4 shift register.

부터 생성된다.

부호의 원소들을 왼쪽으로 순환 이전시켜서 n 쌍의 부호열을 만들고 각 부호에 대한 $A_1(C^i)$, $[A_1(C^{i+1}) - A_1(C^i)]$, $A_0(C^i)$ 및 $[A_0(C^{i+1}) - A_0(C^i)]$가 표 2에 주어져 있다.

표 2에서 부호 내의 원소중 $C_i = -1$인 경우

$$[A_1(C^{i+1}) - A_1(C^i)] = 2 \cdot (n-k)$$

를 만족하고, $C_i = 1$인 경우

$$[A_1(C^{i+1}) - A_1(C^i)] = -2 \cdot k$$

를 만족함을 알 수 있고, $A_0(C)$의 경우 부호 내의 원소중 $C_i = 0$일 때

$$[A_0(C^{i+1}) - A_0(C^i)] = (n-k)$$

그리고 $C_i = 1$일 때

$$[A_0(C^{i+1}) - A_0(C^i)] = -k$$

를 만족함을 알 수 있다.

표 3. n = 15, k = 7인 부호의 $A_1(C)$와 $A_1(C)$ (mod 15).
Table 3. Shifted sequence and its $A_1(C)$ and $A_1(C)$ (mod 15) with n = 15 and k = 7.

C^i	C_i C_{i+1} . . . C_{i-2} C_{i-1}	$A_1(C)$	$A_1(C)$ (mod 15)
C^0	-1-1-1 1-1-1 1 1-1 1-1 1 1 1 1	-30	0
C^1	-1-1 1-1-1 1 1-1 1-1 1 1 1 1-1	-14	1
C^2	-1 1-1-1 1 1-1 1-1 1 1 1 1-1-1	2	2
C^3	1-1-1 1 1-1 1-1 1 1 1 1-1-1-1	18	3
C^4	-1-1 1 1-1 1-1 1 1 1 1-1-1-1 1	4	4
C^5	-1 1 1-1 1-1 1 1 1 1-1-1-1 1-1	20	5
C^6	1 1-1 1-1 1 1 1 1-1-1-1 1-1-1	36	6
C^7	1-1 1-1 1 1 1 1-1-1-1 1-1-1 1	22	7
C^8	-1 1-1 1 1 1 1-1-1-1 1-1-1 1 1	8	8
C^9	-1 1-1 1 1 1 1-1-1-1 1-1-1 1 1	24	9
C^{10}	-1 1 1 1 1-1-1-1 1-1-1 1 1-1 1	10	10
C^{11}	1 1 1 1-1-1-1 1-1-1 1 1-1 1-1	26	11
C^{12}	1 1 1-1-1-1 1-1-1 1 1-1 1-1 1	12	12
C^{13}	1 1-1-1-1 1-1-1 1 1-1 1-1 1 1	-2	13
C^{14}	1-1-1-1 1-1-1 1 1-1 1-1 1 1 1	-16	14
C^{15}	-1-1-1 1-1-1 1 1-1 1-1 1 1 1 1	-30	15 ≡ 0

표 2. n = 15, k = 7인 PN 부호의 A(C)와 $A(C^{i+1}) - A(C^i)$ 값.
Table 2. Example with PN sequence generated by 4 shift registers (n = 15, k = 7).

C^i	C_i C_{i+1} C_{i+2} . . . C_{i-2} C_{i-1}	$A_1(C)$	$A_1(C^{i+1}) - A_1(C^i)$ $= -2 \cdot k$ or $2 \cdot (n-k)$	$A_0(C)$	$A_0(C^{i+1}) - A_0(C^i)$ $= -k$ or $n-k$
C^i	-1-1-1 1-1-1 1 1-1 1-1 1 1 1 1	-30	16 ≡ 2·(15 - 7)	45	8
C^{i+1}	-1-1 1-1-1 1 1-1 1-1 1 1 1 1-1	-14	16 ≡ 2·(15 - 7)	53	8
C^{i+2}	-1 1-1-1 1 1-1 1-1 1 1 1 1-1-1	2	16 ≡ 2·(15 - 7)	61	8
C^{i+3}	1-1-1 1 1-1 1-1 1 1 1 1-1-1-1	18	-14 ≡ -2·7	69	-7
C^{i+4}	-1-1 1 1-1 1-1 1 1 1 1-1-1-1 1	4	16 ≡ 2·(15 - 7)	62	8
C^{i+5}	-1 1 1-1 1-1 1 1 1 1-1-1-1 1-1	20	16 ≡ 2·(15 - 7)	70	8
C^{i+6}	1 1-1 1-1 1 1 1 1-1-1-1 1-1-1	36	-14 ≡ 2·7	78	-7
C^{i+7}	1-1 1-1 1 1 1 1-1-1-1 1-1-1 1	22	-14 ≡ 2·7	71	-7
C^{i+8}	-1 1-1 1 1 1 1-1-1-1 1-1-1 1 1	8	16 ≡ 2·(15 - 7)	64	8
C^{i+9}	1-1 1 1 1 1-1-1-1 1-1-1 1 1-1	24	-14 ≡ 2·7	72	-7
C^{i+10}	-1 1 1 1 1-1-1-1 1-1-1 1 1-1 1	10	16 ≡ 2·(15 - 7)	80	8
C^{i+11}	1 1 1 1-1-1-1 1-1-1 1 1-1 1-1	26	-14 ≡ 2·7	73	-7
C^{i+12}	1 1 1-1-1-1 1-1-1 1 1-1 1-1 1	12	-14 ≡ 2·7	66	-7
C^{i+13}	1 1-1-1-1 1-1-1 1 1-1 1-1 1 1	-2	-14 ≡ 2·7	59	-7
C^{i+14}	1-1-1-1 1-1-1 1 1-1 1-1 1 1 1	-16	-14 ≡ 2·7	52	-7
C^{i+15}	-1-1-1 1-1-1 1 1-1 1-1 1 1 1 1	-30	16 = 2·(15 - 7)	45	8

예제 1은 정리 1을 잘 설명한다.

〈예제 2〉 예제 1의 그림 3에서 생성된 PN 부호 C^1에서 구한 n 쌍의 부호와 함수 값 $A_1(C)$, $A_1(C)$ (mod n)이 표 3에서 보여준다.

예제 2에서 CDMA에 사용되는 영옵셋 PN 부호 또는 기준 PN 부호 C^0를 얻을 수 있다. 여기서 영옵셋 PN 부호는 식(7)에서 정의한 것과 같이

$$A(C^0) \pmod n \equiv 0 \pmod n \qquad (7)$$

이다.

위의 예제는 정리 3과 정리 4를 잘 예시하고 있다.

〈예제 3〉 주기가 7인 부호이고, k가 1, 2, 3, 4, 5 그리고 6인 경우를 생각하자.

대수식 역원은 $C_i \in \{1, -1\}$의 경우는 식(28)로 부터 구할 수 있고, $C_i \in \{1, 0\}$인 경우는 식(29)로 부터 얻을 수 있다. 표 4는 $C_i \in \{1, -1\}$ 그리고 $C_i \in \{1, 0\}$로 구성된 7쌍의 부호의 A(C), A(C^t) (mod 7) 그리고 $a^* \cdot A(C^t)$ (mod 7)을 나타내고 있다.

〈예제 7〉 표 3의 15 쌍의 부호 중 $C^7 = (1, -1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1, -1, -1, 1)$이 수신기에 저장 되어 있고, $C^2 = (-1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, -1, -1)$가 수신된 부호라 할 때 다음 절차에 따라 두 부호 사이의 시간차를 구할 수 있다.

표 4. n=7인 부호의 A(C), A(C) (mod 7) 그리고 $a^* \cdot A(C)$ (mod 7) k=1 (a), k=2 (b), k=3 (c), k=4 (d), k=5 (e) and k=6 (f).

Table 4. 7-tuple sequence and its A(C), A(C) (mod 7) and $a^* \cdot A(C)$ (mod 7) with k=1 (a), k=2 (b), k=3 (c), k=5 (e) and k=6 (f).

(a) n = 7, k = 1

C^t	$C_t, C_{t+1}, \cdots, C_{t-1}$	$A_1(C)$	$A_1(C)$(mod 7)	$3 \cdot A_1(C)$ (mod 7)	$A_0(C)$	$A_0(C)$(mod 7)	$6 \cdot A_0(C)$ (mod 7)
C^0	0 1 1 1 1 1 1	14	0	0	21	0	0
C^1	1 1 1 1 1 1 0	26	5	1	27	6	1
C^2	1 1 1 1 1 0 1	24	3	2	26	5	2
C^3	1 1 1 1 0 1 1	22	1	3	25	4	3
C^4	1 1 1 0 1 1 1	20	6	4	24	3	4
C^5	1 1 0 1 1 1 1	18	4	5	23	2	5
C^6	1 0 1 1 1 1 1	16	2	6	22	1	6

(b) n = 7, k = 2

C^t	$C_t, C_{t+1}, \cdots, C_{t-1}$	$A_1(C)$	$A_1(C)$(mod 7)	$5 \cdot A_1(C)$ (mod 7)	$A_0(C)$	$A_0(C)$(mod 7)	$3 \cdot A_0(C)$ (mod 7)
C^0	1 0 1 1 1 1 0	14	0	0	21	0	0
C^1	0 1 1 1 1 0 1	10	3	1	19	5	1
C^2	1 1 1 1 0 1 0	20	6	2	24	3	2
C^3	1 1 1 0 1 0 1	16	2	3	22	1	3
C^4	1 1 0 1 0 1 1	12	5	4	20	6	4
C^5	1 0 1 0 1 1 1	8	1	5	18	4	5
C^6	0 1 0 1 1 1 1	4	4	6	16	2	6

(c) n = 7, k = 3

C^t	$C_t, C_{t+1}, \cdots, C_{t-1}$	$A_1(C)$	$A_1(C)$(mod 7)	$1A_1(C)$ (mod 7)	$A_0(C)$	$A_0(C)$(mod 7)	$2A_0(C)$ (mod 7)
C^0	1 1 1 0 1 0 0	14	0	0	21	0	0
C^1	1 1 0 1 0 0 1	8	1	1	18	4	1
C^2	1 0 1 0 0 1 1	2	2	2	15	1	2
C^3	0 1 0 0 1 1 1	-4	3	3	12	5	3
C^4	1 0 0 1 1 1 0	4	4	4	16	2	4
C^5	0 0 1 1 1 0 1	-2	5	5	13	6	5
C^6	0 1 1 1 0 1 0	6	6	6	17	3	6

(d) n = 7, k = 4

C^t	$C_t, C_{t+1}, \cdots, C_{t-1}$	$A_1(C)$	$A_1(C) \pmod 7$	$6 \cdot A_1(C) \pmod 7$	$A_0(C)$	$A_0(C) \pmod 7$	$5 \cdot A_0(C) \pmod 7$
C^0	0 1 1 0 1 0 0	0	0	0	14	0	0
C^1	1 1 0 1 0 0 0	6	6	1	17	3	1
C^2	1 0 1 0 0 0 1	-2	5	2	13	6	2
C^3	0 1 0 0 0 1 1	-10	4	3	9	2	3
C^4	1 0 0 0 1 1 0	-4	3	4	12	5	4
C^5	0 0 0 1 1 0 1	-12	2	5	8	1	5
C^6	0 0 1 1 0 1 0	-6	1	6	11	4	6

(e) n = 7, k = 5

C^t	$C_t, C_{t+1}, \cdots, C_{t-1}$	$A_1(C)$	$A_1(C) \pmod 7$	$2 \cdot A_1(C) \pmod 7$	$A_0(C)$	$A_0(C) \pmod 7$	$4 \cdot A_0(C) \pmod 7$
C^0	0 0 1 0 0 1 0	-14	0	0	7	0	0
C^1	0 1 0 0 1 0 0	-10	4	1	9	2	1
C^2	1 0 0 1 0 0 0	-6	1	2	11	4	2
C^3	0 0 1 0 0 0 1	-16	5	3	6	6	3
C^4	0 1 0 0 0 1 0	-12	2	4	8	1	4
C^5	1 0 0 0 1 0 0	-8	6	5	10	3	5
C^6	0 0 0 1 0 0 1	-18	3	6	5	5	6

(f) n = 7, k = 6

C^t	$C_t, C_{t+1}, \cdots, C_{t-1}$	$A_1(C)$	$A_1(C) \pmod 7$	$4 \cdot A_1(C) \pmod 7$	$A_0(C)$	$A_0(C) \pmod 7$	$1 \cdot A_0(C) \pmod 7$
C^0	1 0 0 0 0 0 0	-14	0	0	7	0	0
C^1	0 0 0 0 0 0 1	-26	2	1	1	1	1
C^2	0 0 0 0 0 1 0	-24	4	2	2	2	2
C^3	0 0 0 0 1 0 0	-22	6	3	3	3	3
C^4	0 0 0 1 0 0 0	-20	1	4	4	4	4
C^5	0 0 1 0 0 0 0	-18	3	5	5	5	5
C^6	0 1 0 0 0 0 0	-16	5	6	6	6	6

(1) 수신기에 저장되어 있는 부호 C^7로 부터

$A(C^7)_S \pmod{15} \equiv 7$

를 얻고, (2) 수신된 부호로 부터

$A(C^2)_R \pmod{15} \equiv 2$

를 구하고, (3)

$[A(C^2)_R \pmod{15} - A(C^7)_S \pmod{15}] \pmod{15}$
$\equiv 10$

(4) 법 15에 대한 $2 \cdot (n-k)$의 역원 a^*을

$2 \cdot (15-7) \cdot a^* \equiv 1 \pmod{15}$ 〈case 1 이므로〉

로 부터

$a^* \equiv 1 \pmod{15}$

를 얻는다.(5)

$a^* \cdot [A(C)_R \pmod n - A(C)_S \pmod n] \pmod n$
$\equiv 1 \cdot [2-7] \pmod{15}$
$\equiv 10 \pmod{15}$

를 얻어 수신기에 저장되어 있는 부호 C^7과 수신된 신호 C^2의 시간차가 '10'임을 알 수 있다. 이는 C^7의 원소들을 오른쪽으로 10번 순환이전 시켜서 C^2를 얻을 수 있음을 알려준다. 다르게 표현하면 수신기에 저장되어 있는 신호를 오른쪽으로 10회 순화이전시

키면 수신된 신호와 동기가 맞음을 알 수 있다.

V결 론

본 논문에서는 통신 시스템의 동기에 사용되는 PN 부호의 기준 PN 부호를 결정하는 방법을 제시하고 있다. 이 방법으로 수신된 PN 부호 사이의 시간 또는 위상차를 구할 수 있다. 또한 기존의 동기 방법들은 PN 부호나 Gold 부호등 특정한 부호를 사용하고 있으나, 본 논문에서 제시하는 방법을 이용하여 n 쌍 부호의 주기 n과 부호 내의 '0'의 갯수 k 사이의 최대 공약수가 '1' 〈case 0〉, 그리고 부호의 주기가 홀수인 n과 부호 내의 '-1'의 갯수 k의 최대공약수가 '1'〈case 1〉인 경우에는 부호의 구성원소의 배치에 상관 없이 동기에 응용할 수 있는 장점이 있다.

본 논문의 정리들은 쉽게 이해할 수 있으며 정수론과 밀접한 관계가 있다. 또한 PN 부호의 기준을 결정하는 것 외에도 여러 분야에 응용될 것으로 기대된다.

全 正 植(Jung-Sig Jun) 정회원
1991년 2월 : 한양대학교 공과대학 전자통신공학과(공학사)
1993년 2월 : 한양대학교 공과대학 전자통신공학과(공학석사)
현재 : (주)금성사 영상미디어연구소 ATV Gr. 재직

REFERENCES

1. Proposed EIA/TIA INTERIM STANDARD Wideband Spread Spectrum Digital Cellular System Dual-Mode Mobile Station-Base Station Compatibility Standard, April 1992.
2. I.Niven, H.S.Zuckerman, An Introduction to the Theory of Number, John Wiley & Sons, 1980.
3. R.E. Ziemer and R.L.Peterson, Digital Communications and Spread Sprectrum Systems, Macmillan Publishing Company, 1985.
4. K.H.Rosen, Elementary Number Theory and Its Applications, Bell Telephone Laboratories : Addison-Wesley Publishing Company, 1988.