論文99-36S-9-4

이원부호의 위상오프셋 오류 검출

(Error Detection of Phase Offsets for Binary Sequences)

宋 寧 俊 *, 韓 榮 烈 **

(Young Joon Song and Young Yearl Han)

요 약

본 논문은 정수론에 기반하여, PN (Pseudo Noise) 확산부호를 포함한 이원부호의 위상오프셋 오류검출 방법을 제안한다. 부호분할다원접속 (code division multiple access : CDMA) 이동 통신 시스템에서는 확산부호의 위상오프셋을 이용하여, 각 기지국을 구분하고 있으므로 위상오프셋을 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. 제안된 방법의 오류검출실패확률 식을 유도하고 시뮬레이션 결과를 이용하여 검증한다. 그리고 회로 구현 방법에 관하여서도 논하며, 간단한 회로로 구현할 수 있음을 보인다.

Abstract

In this paper, we propose an error detection scheme of phase offsets for binary sequences including PN (Pseudo Noise) sequences based on the number theoretical approach. It is important to know phase offsets of spreading sequences in the CDMA (Code Division Multiple Access) mobile communication systems because phase offsets of the same spreading sequence are used to achieve the acquisition and are used to distinguish each base station. When the period of the sequence is not very long, the relative phase offset between the sequence and its shifted replica can be found by comparing them, but as the period of the sequence increases it becomes difficult to find the phase offset. The error detection failure probability of the proposed method is derived, and it is confirmed by the simulation results. We also discuss the circuit realization of the proposed method and show it can be easily implemented.

Ⅰ. 서 론

일반적으로 q개의 원소를 갖는 부호 중 $q=2$인 이원부호는 디지털 통신에서 정보 전송을 위하여 주로 사용되어지고 있다[1]-[2]. 음성, 화상과 같은 연속 신호는 아나로그-디지털 변환기(Analog-to-Digital Converter : ADC)를 거쳐 이원부호화 되고 이 이원부호는 변조라는 주파수 천이 과정을 거쳐 무선이나 유선으로 전송되며 수신측에서는 아나로그 신호를 다시 이원부호로 복원하게 된다. 이와 같이 이원부호는 정보화되어 전송될 뿐 아니라 이동 통신의 부호분할 다중접속(Code Division Multiple Access : CDMA) 방식[3]에서는 확산부호로 사용되기도 한다. 이 시스템에서는 이원부호의 자기상관 함수가 지연이 없을 때는 '1'이고 그 외의 자기상관 함수 값은 부호의 주기가 N일 때 '$-1/N$'의 값

* 正會員, LG 情報通信
(Next Generation Communications Research Lab, LG Information and Communications Inc.)

** 正會員, 漢陽大學校 電子通信工學科
(Dept. Of Electronics Communciation Eng., Hanyang Univ.)

接受日字:1999年1月15日, 수정완료일:1999年8月23日

을 갖는 최장부호가 중요한 역할을 한다. 이 최장 부호는 선형 쉬프트 레지스터 (shift register)를 사용하여 발생시킬 수 있는 주기가 최대가 되는 이원 부호이다[4] [10]. 이 부호는 수신기에서는 수신기의 동기, 채널의 임펄스 응답 (impulse response) 측정, 거리 측정, 암호화등에 사용된다[11]-[15].

임의의 기준 부호가 설정되면, 이 기준부호의 위상오프셋을 '0'으로 하고 m 번 순회된 동일 이원부호의 위상오프셋을 m 으로 정의한다. 부호 길이가 2^r-1인 확산 부호에는 다른 위상오프셋을 갖는 부호가 부호길이 2^r-1와 동일한 수 만큼 존재한다. 부호의 주기가 길지 않을 경우는 한 부호에서 이전된 부호 사이의 위상오프셋은 두 부호를 비교하여 구할 수 있지만, 부호의 길이가 길어지면 이원부호의 위상오프셋을 알기란 용이치 않다. 우선 기준부호의 설정이 임의가 아니라 논리적이고 명확한 수학적 근거가 있어야 하며 또한 공학적으로 회로 구성이 용이하여야 한다.

Willet[16]이 최장 이원부호에만 적용되는 위상오프셋 계산 방법을 제안하였다. 그러나 오류검출 방법과 회로 구성 방법에 대하여서는 제안하지 않고 있다. 그 후 [17]에서는 이원부호의 주기가 n이고, 이원부호에 포함된 '0'의 개수가 k일 때, n과 k가 서로 소의 조건을 만족하는 이원부호에 대한 위상 오프셋을 계산할 수 있는, 보다 더 일반화된 회로 구성이 용이한 위상오프셋 계산 방법을 제안하였다.

주기가 $n=2^L-1$인 PN부호 내에 포함된 '0' 원소의 개수는 $k=(n-1)/2=2^{L-1}-1$이다[8]-[10]. 여기서 L은 PN부호 특성다항식의 차수이다. 그리고 두 정수 n과 k의 최대공약수는 $(n, k)=2^{(L, L-1)}-1=1$[9]이므로, [17]의 방법은 [16]의 방법을 보다 더 일반화한 것이다. 하지만 수신 이원부호의 위상오프셋 계산 오류 검출 방법은 제안하지 않고 있다.

수신 이원부호에 오류가 포함된 경우, 계산된 위상오프셋 값은 송신 이원부호의 위상오프셋 값과 다른 값을 가지게 되며, 이러한 경우 계산된 위상오프셋 값이 오류가 포함된 이원부호의 위상오프셋 값인지 아닌지를 판단하여, 오류가 포함된 값이 아닌 경우에 대하여서만 위상오프셋을 산출하는 것이 요구된다.

본 논문은 패리티검사비트 (parity-check bit) 없이 수신 이원부호의 오류를 검출하고, 효율적으로 이원부호의 위상오프셋을 산출할 수 있는 알고리듬을 제안한다. 그리고 제안된 방법의 오류검출실패 확률 식을 유도하고 시뮬레이션 결과와 비교한다. 또한 제안된 방법의 회로 구현 방법에 관하여서도 논한다.

본 논문은 다음과 같이 구성된다. Ⅱ장에서는 본 논문에서 사용될 이원부호의 위상오프셋 관련 정의에 대하여 설명하며, Ⅲ장에서는 이원부호의 위상오프셋 계산과 오류 검출에 이용되는 주요한 결과를 유도한다. 그리고, Ⅳ장에서는 이원부호의 위상오프셋 오류검출 알고리듬, 오류검출실패 확률에 관하여 논하며, Ⅴ장에서는 제안된 방법의 회로구현에 관하여 논한다. 마지막으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. 위상오프셋 관련 정의

먼저 S를 n쌍(n-tuple) 이원부호의 전체 집합이라 정의하고, $\mathbf{C}\in\mathbf{S}$인 n쌍의 이원부호 C에 대하여 순회연산자 T를 다음과 같이 정의한다.

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

두 정수 i와 j에 대하여 $i\equiv j(\bmod n)$이면, $T^i\boldsymbol{C}=T^j\boldsymbol{C}=(C_{n-j}, C_{n=j+1}, \cdots, C_{n-j-1})$의 관계가 성립하며, $T^0\boldsymbol{C}=\boldsymbol{C}$로 정의한다. 그리고 $T^j\boldsymbol{C}\in\boldsymbol{S}$인 이원부호는 다음과 같은 다항식으로 표시된다.

$$C(x)=C_{n-j}+C_{n-j+1}x+\cdots\cdots+C_{n-j-1}x^{n-1}\tag{2}$$

$\boldsymbol{Z}$를 정수 전체의 집합이라고 하자. 그러면, 정수 l을 가중치로 갖는 위상오프셋 산출함수 A^l: $\boldsymbol{S}\rightarrow\boldsymbol{Z}$는 이원부호 $T^j\boldsymbol{C}\in\boldsymbol{S}$에 대하여 다음과 같이 정의한다.

$$\mathrm{A}^l(T^j\mathbf{C})=\frac{d}{dx}x^lC(x)\Big|_{x=1}\tag{3}$$

부호 $T^j\boldsymbol{C}$가 $A^l(T^j\boldsymbol{c})\equiv 0(\bmod n)$의 조건을 만족한다면, 이 부호를 가중치가 l인 위상오프셋 산출함수의 기준부호(reference sequence) 또는 영 오프셋 부호

(zero offset sequence)라 정의한다. 위상오프셋 산출함수 $A^l(T^i\mathbf{C})$는 n쌍의 이원부호 $\mathbf{C}$의 원소가 $C_i \in \{-1, 1\}$이면 $A_1^l(T^i\mathbf{C})$로 표기하고, $C_i \in \{0, 1\}$이면 $A_0^l(T^i\mathbf{C})$로 표기한다. 아래 첨자 없이 $A^l(T^i\mathbf{C})$로 표기한 경우는 이원부호 $\mathbf{C}$의 원소가 두 가지 집합 중 어디에 속하더라도 무관한 경우를 나타낸다.

Ⅲ. 위상오프셋 산출함수의 성질

다음은 계산된 이원부호의 위상오프셋 값의 오류를 검출하는 방법을 유도하는데 사용되는 정리와 따름 정리이다.

정리 1 : n쌍의 이원부호 $\mathbf{C}$내에 포함된 원소가 $C_i \in \{-1, 1\}$인 경우 $(2k, n)=1$의 조건을 만족하고, $C_i \in \{0, 1\}$인 경우 $(k, n)=1$의 조건을 만족하며, n쌍의 이원부호 $\mathbf{C}$와 $\hat{\mathbf{C}}$내에 포함된 '-1' 또는 '0' 원소의 개수를 각각 k와 $\hat{k}$이라 하자. 그러면, $k \neq \hat{k}$이고 정수 ξ와 n이 서로 소이면

$$a^*[A^l(T^\xi\hat{\mathbf{C}}) - A^l(\hat{\mathbf{C}})] \neq \xi \pmod n \tag{4}$$

$$a^*\hat{C}(1) \neq 1 \pmod n \tag{5}$$

이다. 여기서 l과 ξ는 정수이며, a^*는 다음을 만족하는 법 n에 대한 a의 대수적 역원(arithmetic inverse)이다.

$$-2ka^* \equiv 1 \pmod n \text{ for } C_i \in \{1,1\} \tag{6}$$

$$-ka^* \equiv 1 \pmod n \text{ for } C_i \in \{0,1\} \tag{7}$$

그리고 $\hat{C}(1)$은 다음과 같이 정의된다.

$$\hat{C}(1) = \sum_{i=0}^{n-1} \hat{C}_i \tag{8}$$

증명 : 이원부호 $\mathbf{C}$와 $\hat{\mathbf{C}}$을 각각 $\mathbf{C}=(C_0, C_1, \cdots, C_{n-1})$와 $\hat{\mathbf{C}}=(\hat{C}_0, \hat{C}_1, \cdots, \hat{C}_{n-1})$라 하자. 그리고 $\mathbf{C}$와 $\hat{\mathbf{C}}$내에 포함된 '-1' 또는 '0' 원소의 개수를 각각 k와 $\hat{k}$이라 하자. $\hat{k}=0$인 경우와 $\hat{k}=n$인 경우는, 식 (4)와 (5)가 성립함을 쉽게 알 수 있으므로, $1 \le \hat{k} \le n-1$인 경우에 대하여 증명한다. 그러면 $k \neq \hat{k}$인 가정과 k의 정의에 의하여 $1 \le k, \hat{k} \le n-1$이다. $\hat{k}=k+k'$으로 정하면, $k \neq \hat{k}$이므로 k'은 $k' \neq 0, |k'| \le n-2$인 정수이다.

식 (3)의 위상오프셋 산출함수의 정의 식에 의하여

$$\begin{aligned}
A^l(T^\xi\hat{\mathbf{C}}) &= \frac{d}{dx}x^l\left(\hat{C}_{n-\xi} + \hat{C}_{n-\xi+1}x + \cdots + \hat{C}_{n-1}x^{n-1}\right)\Big|_{x=1} \\
&= l\hat{C}_{n-\xi} + (l+1)\hat{C}_{n-\xi+1} + \cdots + (l+\xi-1)\hat{C}_{n-1} + (l+\xi)\hat{C}_0 + \cdots + (l+n-1)\hat{C}_{n-\xi-1} \\
&= (l+\xi)\hat{C}_0 + \cdots + (l+n-1)\hat{C}_{n-\xi-1} + l\hat{C}_{n-\xi} + (l+1)\hat{C}_{n-\xi+1} + \cdots + (l+\xi-1)\hat{C}_{n-1} \\
&\equiv \left\{(l+\xi)\hat{C}_0 + \cdots + (l+n-1)\hat{C}_{n-\xi-1} + (l+n)\hat{C}_{n-\xi} + (l+n+1)\hat{C}_{n-\xi+1} + \cdots \right. \\
&\quad \left. + (l+\xi+n-1)\hat{C}_{n-1}\right\} \pmod n \\
&= \frac{d}{dx}x^{l+\xi}\hat{C}(x)\Big|_{x=1} \pmod n \\
&= A^{l+\xi}(\hat{\mathbf{C}}) \pmod n
\end{aligned} \tag{9}$$

$$\begin{aligned}
A^{l+\xi}(\hat{\mathbf{C}}) &= \frac{d}{dx}x^{l+\xi}\left(\hat{C}_0 + \hat{C}_1x + \cdots + \hat{C}_{n-1}x^{n-1}\right)\Big|_{x=1} \\
&= (l+\xi)\hat{C}_0 + (l+\xi+1)\hat{C}_1 + \cdots + (l+\xi+n-1)\hat{C}_{n-1} \\
&= (l+\xi)(\hat{C}_0 + \hat{C}_1 + \cdots + \hat{C}_{n-1}) + 0 + \hat{C}_1 + \cdots + (n-1)\hat{C}_{n-1} \\
&= (l+\xi)\hat{C}(1) + \frac{d}{dx}x^0\left(\hat{C}_0 + \hat{C}_1x + \cdots + \hat{C}_{n-1}x^{n-1}\right)\Big|_{x=1} \\
&= (l+\xi)\hat{C}(1) + A^0(\hat{\mathbf{C}})
\end{aligned} \tag{10}$$

이 성립한다. 그리고 식 (9)와 (10)을 이용하여

$$\begin{aligned}
A^l(T^\xi\hat{\mathbf{C}}) &\equiv A^{l+\xi}(\hat{\mathbf{C}}) \pmod n \\
&= [(l+\xi)\hat{C}(1) + A^0(\hat{\mathbf{C}})] \pmod n
\end{aligned} \tag{11}$$

이 성립함을 확인할 수 있다. 그러면 식 (11)에 의하여, 이원부호 $\hat{\mathbf{C}}$와 ξ번 순회된 동일 이원부호 $T^\xi\hat{\mathbf{C}}$ 사이의 위상오프셋은 다음과 같이 된다.

$$a^*[A^l(T^\xi\hat{\mathbf{C}}) - A^l(\hat{\mathbf{C}})] \equiv a^*\xi\hat{C}(1) \pmod n \tag{12}$$

그리고 $\hat{C}(1)$은 식 (8)의 정의에 의하여

$$\hat{C}(1) = \begin{cases} n-2\hat{k}, & \text{for } C_i \in \{-1,1\} \\ n-\hat{k}, & \text{for } C_i \in \{0,1\} \end{cases} \tag{13}$$

으로 주어진다.

$C_i \in \{-1, 1\}$인 경우, 식 (12)는 다음과 같다.

$$\begin{aligned}
a^*[A_1^l(T^\xi\hat{\mathbf{C}}) - A_1^l(\hat{\mathbf{C}})] &\equiv a^*\xi\hat{C}(1) \pmod n \\
&\equiv a^*(-2\hat{k}\xi) \pmod n \\
&= a^*(-2\xi(k+k')) \pmod n \\
&\equiv (\xi + bk') \pmod n
\end{aligned} \tag{14}$$

여기서 $b \equiv -2\xi a^* \pmod n$으로 정의하였다. 식 (6)에 의하여, $a^*(-2k) \equiv 1 \pmod n$이고, 가정에 의하여 $(2k, n)=1$이므로 $(a^*, n)=1$이다[18]-[19]. 그리고 정수 n은 짝수 $2k$와 서로 소이기 위하여 홀수이다.

$(a^*, n)=1$, $k'\neq 0$, $|k'|\leq n-2$이므로, $(\xi, n)=1$이면 $(b, n)=1$, $bk'\neq 0 \pmod n$이고

$$a^*\xi\hat{C}(1)\equiv(\xi+bk')\pmod n \neq \xi \pmod n \quad (15)$$

이 되어 식 (4)가 성립함을 알 수 있다. 그리고 $a^*\hat{C}(1)\equiv 1\pmod{(n/(\xi,n))}$은 $a^*\xi\hat{C}(1)\equiv\xi\pmod n$이 성립하기 위한 필요충분조건이므로[18]-[19], 식 (15)에서 $a^*\hat{C}(1)\neq 1\pmod n$이 성립함을 알 수 있다.

유사한 방법으로 $C_i\in\{0, 1\}$인 경우에 대하여서도 위의 관계가 성립함을 증명할 수 있다. □

따름정리 1 : $\hat{k}$을 n쌍의 이원부호 $\hat{\mathbf{C}}$내에 포함된 '-1' 또는 '0' 원소의 개수라 하자. 그리고 이원부호 C내에 포함된 원소가 $C_i\in\{-1, 1\}$인 경우 $(2k, n)=1$의 조건을 만족하고, $C_i\in\{0, 1\}$인 경우 $(k, n)=1$의 조건을 만족한다고 가정하자. 그러면, $k=\hat{k}$인 것은 $a^*\hat{C}(1)\equiv 1\pmod n$이기 위한 필요충분조건이다.

증명 : 정리 1에 의하여, $\xi=1$인 경우 $(\xi, n)=1$이므로, $k=\hat{k}$이면 $a^*\hat{C}(1)\neq 1\pmod n$이다. 역으로, 식 (14)에 의하여 $k=\hat{k}$이면 $k'=0$이므로 $a^*\hat{C}(1)\equiv 1\pmod n$이 된다. □

위의 따름정리에 의하면, 수신 이원부호의 한 주기를 수신하여 $\hat{C}(1)$을 계산한 후, 법 n에 대한 대수적 역원을 곱한 값이 법 n에 대하여 '1'이면, 수신 이원부호 내의 '0' 또는 '-1' 원소의 개수가 원래 송신한 것과 동일한 것을 의미하며, 그렇지 않으면 동일하지 않은 것을 의미한다.

예제 : $n=7$인 이원부호 $\mathbf{C}=(1,1,1,0,0,0,0)$ 또는 $\mathbf{C}=(1,1,1,-1,-1,-1,-1)$의 이원부호를 고려하면, $\mathbf{C}=(1,1,1,0,0,0,0)$인 경우, $k=4$, $a^*=5$, $C(1)=3$, $a^*C(1)=1\pmod 7$이 며, $\mathbf{C}=(1,1,1,-1,-1,-1,-1)$인 경우, $k=4$, $a^*=6$, $C(1)=-1$, $a^*C(1)=1\pmod 7$이 된다. 수신되는 이원부호의 세 번째 비트에 오류가 발생하여, $\hat{\mathbf{C}}=(1,1,0,0,0,0,0)$ 또는 $\hat{\mathbf{C}}=(1,1,-1,-1,-1,-1,-1)$라 가정하자. 표 1은 $(\xi, n)=1$, $a^*[A^3(T^\xi\hat{\mathbf{C}})-A^3(\hat{\mathbf{C}}))\pmod 7$의 계산 결과를 나타내며, 정리 1의 식 (4)가 성립함을 확인할 수 있다. 그리고 표 2는 $k\neq\hat{k}$인 경우의 $a^*\hat{C}(1)\pmod n$의 값이 법 n에 대하여 항상 '1'이 아님을 나타내고 있으므로 식 (5)와 따름정리 1이 성립함을 확인할 수 있다. □

표 1. $\mathbf{C}=(1,1,1,0,0,0,0)$와 $\hat{\mathbf{C}}=(1,1,0,0,0,0,0)$에 대한 $a^*[A^3(T^\xi\hat{\mathbf{C}})-A^3(\hat{\mathbf{C}}))\pmod 7$의 값.

Table 1. $a^*[A^3(T^\xi\hat{\mathbf{C}})-A^3(\hat{\mathbf{C}}))\pmod 7$ for (1,1,1,0,0,0,0) and (1,1,0,0,0,0,0).

ξ	$T^\xi\hat{\mathbf{C}}$	$5[A_0^3(T^\xi\mathbf{C})-A_0^3(\mathbf{C})]\pmod 7$	$6[A_1^3(T^\xi\mathbf{C})-A_1^3(\mathbf{C})]\pmod 7$
1	(0,1,1,0,0,0,0)	3	3
2	(0,0,1,1,0,0,0)	6	6
3	(0,0,0,1,1,0,0)	2	2
4	(0,0,0,0,1,1,0)	5	5
5	(0,0,0,0,0,1,1)	1	1
6	(1,0,0,0,0,0,1)	4	4

표 2. $\mathbf{C}=(1,1,1,0,0,0,0)$인 경우, $k\neq\hat{k}$, $0\leq\hat{k}\leq 7$인 $\hat{\mathbf{C}}$에 대한 $a^*\hat{C}(1)\pmod 7$의 값.

Table 2. The values of $a^*\hat{C}(1)\pmod 7$ with $k\neq\hat{k}$ and $0\leq\hat{k}\leq 7$ when $\mathbf{C}=(1,1,1,0,0,0,0)$.

$\hat{\mathbf{C}}$	$\hat{k}$	$5\hat{C}(1)\pmod 7$	$\hat{\mathbf{C}}$	$\hat{k}$	$6\hat{C}(1)\pmod 7$
(1,1,1,1,1,1,1)	0	0	(1,1,1,1,1,1,1)	0	0
(1,1,1,1,1,1,0)	1	2	(1,1,1,1,1,1,-1)	1	2
(1,1,1,1,1,0,0)	2	4	(0,0,1,1,0,0,0)	2	4
(1,1,1,1,0,0,0)	3	6	(1,1,1,1,1,-1,-1)	3	6
(1,1,0,0,0,0,0)	5	3	(1,1,1,1,-1,-1,-1)	5	3
(1,0,0,0,0,0,0)	6	5	(1,1,-1,-1,-1,-1,-1)	6	5
(0,0,0,0,0,0,0)	7	0	(1,-1,-1,-1,-1,-1,-1)	7	0

Ⅳ. 이원부호의 위상오프셋 오류검출 알고리듬과 오류검출실패 확률

수신 이원부호 $\hat{\mathbf{C}}$에 오류가 포함된 경우, 계산된 위상오프셋 값은 송신 이원부호 $\mathbf{C}$의 위상오프셋 값과 다른 값을 가지게 되며, 이러한 경우 수신 이원부호의 오류를 검출한 다음, 오류가 포함되지 않은 경우에 한하여 위상오프셋을 산출하는 것이 요구된다.

다음은 패리티검사비트 없이 수신 이원부호의 오류를 검출할 수 있는 위상오프셋 오류 검출 방법을 제안하며,

제안된 방법의 오류검출 실패확률에 관하여 논한다.

1. 이원부호의 위상오프셋 오류검출 알고리듬

n 쌍의 이원부호 $\mathbf{C}$의 원소가 $C_i \in \{-1,1\}$인 경우 $(2k, n)=1$이고, $C_i \in \{0,1\}$인 경우 $(k, n)=1$의 조건을 만족하면 다음이 성립한다 [17].

$$a^*[\mathrm{A}^l(T^{i+j}\mathbf{C}) - \mathrm{A}^l(T^i\mathbf{C})] \equiv j \pmod n \tag{16}$$

위의 식을 이용하면 위상오프셋이 다른 두 동일 이원부호 $T^{i+j}\mathbf{C}$와 $T^i\mathbf{C}$의 위상오프셋 j를 산출할 수 있음을 알 수 있다. 하지만 이원부호에 오류가 포함된 경우 식 (16)을 이용하여 계산된 위상오프셋 값은 원래의 것과 다르므로, 이러한 경우 계산된 위상오프셋 값을 무시하고 새로이 한 주기의 이원부호를 수신하여 위상오프셋을 계산하는 것이 요구된다.

이는 따름정리 1의 $a^*\hat{C}(1) \pmod n$값을 이용한 그림 1의 위상오프셋 오류 검출 알고리듬을 이용하여 가능해진다. $a^*\hat{C}(1) \pmod n$의 값이 '1'이 아니면, $k \neq \hat{k}$이고 수신된 이원부호에 오류가 포함되어 있으므로, 다시 한 주기의 이원부호를 수신하여 위상오프셋을 계산한다. 만약 $a^*\hat{C}(1) \pmod n$의 값이 '1'이면, $k \neq \hat{k}$이므로, 수신된 이원부호에는 오류가 포함되어 있지 않다고 판단하고 계산된 위상오프셋 값을 출력한다.

다음은 $(n, 2k)=1$일 때 법 n에 대한 $(n-2k)$의 대수적 역원, $(n, k)=1$일 때 법 n에 대한 $(n-k)$의 대수적 역원을 유클리드의 알고리듬(Euclidean algorithm)[20]-[21]을 이용하여 쉽게 구하는 방법을 설명한다. 먼저 $(n, 2k)=1$인 경우, $n=a$, $-2k \equiv b \pmod n$이라 하면, 유크리드의 알고리듬에 의하여 다음의 관계식과 절차가 성립한다.

$$r_i = s_i a + t_i b \tag{17}$$

$$t_i = t_{i-2} - q_i t_{i-1} \tag{18}$$

$$s_i = s_{i-2} - q_i s_{i-1} \tag{19}$$

i	s_i	t_i	r_i	q_i
-1	1	0	a	-
0	0	1	b	-
1	1	$-q_1$	r_1	q_1
2	$-q_2$	$1+q_1q_2$	r_2	q_2
⋮	⋮	⋮	⋮	⋮
m	s_m	t_m	r_m	q_m
$m+1$	s_{m+1}	t_{m+1}	0	q_{m+1}

그리고 $(a, b)=(n, -2k)=r_m=1$이고 $s_m n + t_m b = 1$이므로 $t_m b \equiv 1 \pmod n$이다. 따라서 t_m은 법 n에 대한 $(n-2k)$의 대수적 역원임을 알 수 있다. 유사한 방법으로 $(n-k)=1$일 때 법 n에 대한 $(n-k)$의 대수적 역원도 위의 절차를 이용하여 쉽게 구할 수 있다.

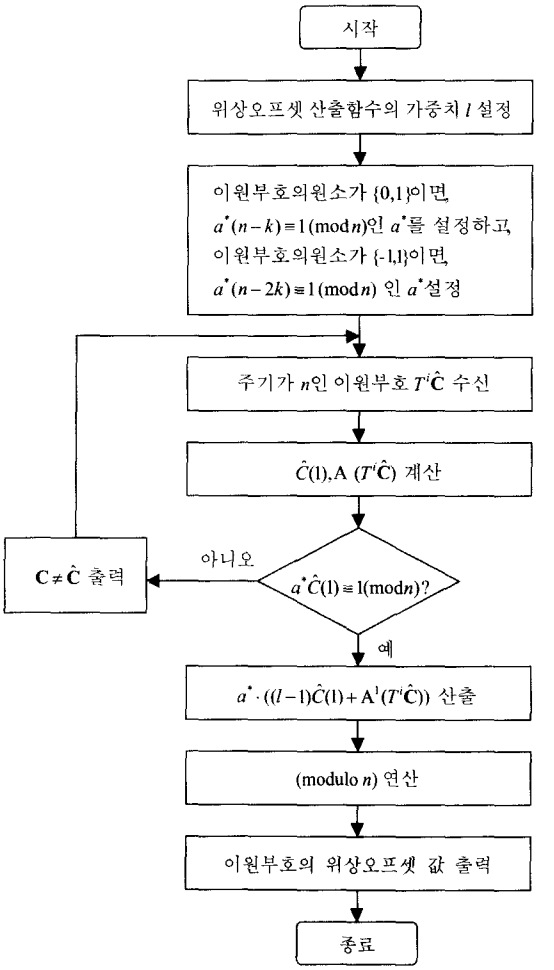

그림 1. 이원부호의 위상오프셋 오류검출 알고리듬
Fig. 1. Error detection algorithm for phase offsets of binary sequences.

2. 오류검출실패 확률

다음의 세 가지 조건을 동시에 만족하는 유형의 오류가 n 쌍의 수신 이원부호에 발생하면, $\mathbf{C} \neq \hat{\mathbf{C}}$이지만 $k=\hat{k}$인 경우에 해당하므로, 그림 1의 알고리듬으로는 오류를 검출할 수 없다.

① 수신 이원부호에 짝수개의 오류 발생.

② 수신 이원부호내의 k개의 '0' 또는 '1'의 위치에 발생한 오류의 개수와 $(n-k)$개의 '1'의 위치에 발생한 오류의 개수는 동일.

③ 수신 이원부호에 $2\min(n-k, k)$이하의 오류 발생.

여기서, $\min(n-k, k)$는 $(n-k)$와 k의 두 정수 중 작은 정수를 나타낸다. 수신 비트 오류확률 또는 수신 비트의 평균 오류발생 확률을 p라 정의하면, 위의 세 가지 조건을 동시에 만족하는 오류검출 실패확률 또는 평균 오류검출 실패확률은 다음과 같다.

$$P_u = \sum_{i=1}^{\min(n-k,k)} \binom{n-k}{i}\binom{k}{i} p^{2i}(1-p)^{n-2i} \qquad (20)$$

가산성 백색 가우시안 잡음 (Additive White Gaussian Noise : AWGN) 채널에서 동기 BPSK (Coherent Binary Phase Shift Keying)인 경우 비트 오류확률은 $p=\frac{1}{2}[1-\mathrm{erf}(\sqrt{\frac{E_b}{N_0}})]$으로 주어지며, E_b는 수신 이원부호의 비트 에너지, N_0는 단측 전력 스펙트럼 밀도 (single-sided noise power spectral density), $\mathrm{erf}(x)=\frac{2}{\sqrt{\pi}}\int_0^x e^{-u^2}du$을 나타낸다[12]. 그리고 레일리 페이딩 (Rayleigh fading) 채널에서 동기 BPSK인 경우, 수신 비트의 평균 오류발생 확률은 $p=\frac{1}{2}\left(1-\sqrt{\frac{\overline{\gamma_b}}{1+\overline{\gamma_b}}}\right)$으로 주어지며, $\overline{r_b}$는 평균 신호대 잡음비 (Signal-to-Noise Ratio : SNR)를 나타낸다[12].

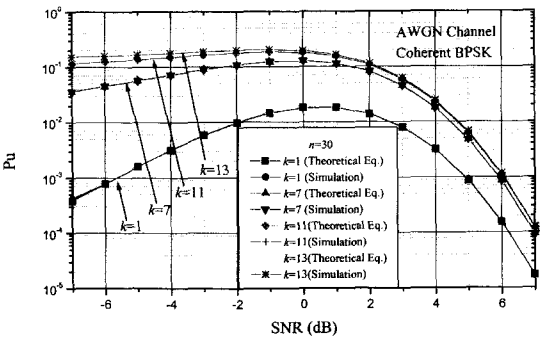

그림 2. AWGN 채널에서 동기 BPSK인 경우 $n=30$, $k=1,7,11,13$인 이원부호에 대한 오류검출 실패확률

Fig. 2. Error detection failure probability for binary sequences with $n=30$, $k=1,7,11,13$, and the coherent BPSK over the AWGN channel.

그림 2는 AWGN 채널에서 $n=30$, $k=1,7,11,13$인 이원부호에 식 (20)으로 주어지는 이론적인 오류검출실패 확률과 컴퓨터 시뮬레이션 값을 나타내고 있으며, 그림 3 레일리 페이딩 채널에서 $n=30$, $k=1,7,11,13$인 이원부호에 대한 이론적 P_u와 시뮬레이션 값을 나타내고 있다. 식 (20)의 이론적 계산 값과 시뮬레이션 값이 매우 근사적으로 일치함을 확인할 수 있다.

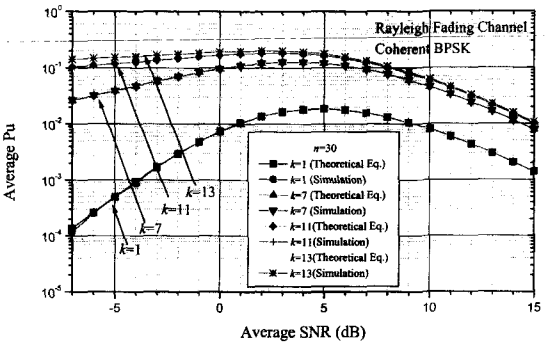

그림 3. 레일리 페이딩 채널에서 동기 BPSK인 경우 $n=30$, $k=1,7,11,13$인 이원부호에 대한 평균 오류검출 실패확률

Fig. 3. Average error detection failure probability for binary sequences with $n=30$, $k=1,7,11,13$ and the coherent BPSK over the Rayleigh fading channel.

오류검출이 실패하기 위한 위의 세 가지의 조건 중에서 k가 작으면 ②와 ③의 경우가 발생할 확률이 작아짐을 알 수 있다. 이는 k가 작아지면 P_u가 감소하고, k가 커지면 P_u가 증가하는 그림 2와 3의 오류검출실패 확률 곡선에서 확인할 수 있다. 또한 SNR이 매우 작아지면, 한 주기의 수신 이원부호에 $2\min(n-k, k)$ 이상의 많은 오류가 발생할 확률이 증가하므로 ③의 경우가 발생할 확률이 감소한다. 그리고 SNR이 높아지면 수신 이원부호에 오류 자체가 발생할 확률이 감소하게 되므로, 이 경우에도 $\mathbf{C}\neq\hat{\mathbf{C}}$이면서 $k=\hat{k}$인 확률은 작아진다. 이러한 현상은 SNR이 아주 높거나 낮은 영역에서 오류검출실패 확률이 감소하는 그림 2와 3의 오류검출 실패확률 곡선에서 확인할 수 있다. 그림 2의 AWGN 채널에서의 오류검출실패 확률은 SNR이 높아지면 급격히 감소하는 반면, 그림 3의 레일리 페이딩 채널의 평균 오류검출실패 확률은 평균 SNR이 증가하더라도 완만히 감소함을 알 수 있다.

식 (20)에 의하면, 일단 n과 p가 정해지면, P_u는 단지 k의 값에 의하여 결정되어진다. 여기서

$\min(n-k,k)$는 두 값 $n-k$와 k중 작은 값을 나타내며, $\lfloor n/2 \rfloor$는 n 2을 초과하지 않는 최대 정수를 나타낸다. 따라서 n이 짝수이면, $\min(n-k,k)$의 최대값은 $n/2$가 되며, n이 홀수이면 $(n-1)/2$가 되므로, P_u의 최대값은 식 (21)로 표시된다. PN부호인 경우 n은 홀수이고 $\min(n-k,k)=k=(n-1)/2$이 되므로[4] [10], 모든 PN부호의 P_u는 식 (21)의 n이 홀수인 경우가 된다.

$$= \begin{cases} \sum_{=}^{n-2} \binom{n}{\quad}^{2} \; ^{2} \; - \; ^{n-2} \; n & \text{경우} \\ \sum_{=}^{n-} \; ^{2} \binom{n+}{} \binom{n-}{} \; ^{2} \; - \; ^{n-2} \; n & \text{경우} \end{cases} \tag{21}$$

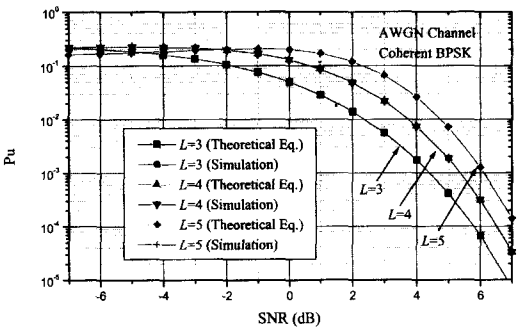

그림 4. AWGN 채널에서 동기 BPSK인 경우 $n=2^L-1$, $L=3,4,5$인 PN부호에 대한 오류검출 실패확률

Fig. 4. Error detection failure probability for PN sequences with $n=2^L-1$, $L=3,4,5$ and the coherent BPSK over the AWGN channel.

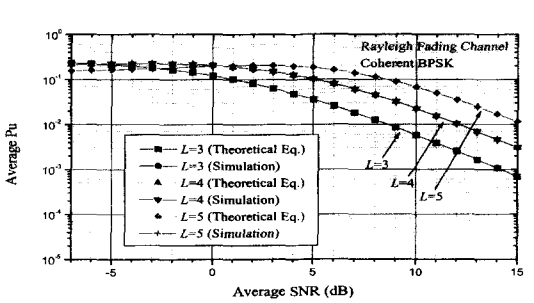

그림 5. 레일리 페이딩 채널에서 동기 BPSK인 경우 $n=2^L-1$, $L=3,4,5$인 PN부호에 대한 평균 오류검출 실패확률

Fig. 5. Average error detection failure probability for PN sequences with $n=2^L-1$, $L=3,4,5$ and the coherent BPSK over the Rayleigh fading channel.

그림 4는 AWGN 채널에서 동기 BPSK인 경우, 주기가 2^l-1, $L=3\sim5$인 PN부호에 대한 식 (21)의 이론적 계산 값과 컴퓨터 시뮬레이션 값을 나타내고 있다. 그리고 그림 5는 레일리 페이딩 채널에서 동기 BPSK인 경우, 주기가 2^L-1, $L=3\sim5$인 PN부호에 대한 이론적 계산 값과 시뮬레이션 값을 나타내고 있다. 식 (21)의 이론적 계산 값과 컴퓨터 시뮬레이션 값이 근사적으로 매우 근접함을 확인할 수 있다.

V. 회로 구성

1. 위상오프셋 산출함수의 회로

가중치가 l인 위상오프셋 산출함수는 다음과 같은 성질을 갖는다 [17].

$$\mathrm{A}^l(T^i\mathbf{C}) = \mathrm{A}^1(T^i\mathbf{C}) + (l-1)C(1) \tag{22}$$

그리고 식 (22)의 첫번째 항, 두번째 항은 각각 그림 6과 7을 이용하여 구현되며, 식 (22)의 위상오프셋 산출함수는 그림 6과 그림 7의 두 회로를 합한 그림 8로 구현된다[17].

2. 오류검출 회로

그림 9는 위상오프셋 오류검출 회로를 나타내고 있으며, 그림 8의 위상오프셋 산출 함수의 회로의 일부를 사용하여 구현된다. 수신 이원부호 $T^i\hat{\mathbf{C}}$는 그림 9의 위상오프셋 오류 검출 회로에 입력이 된다. 그리고 시간 nT_b에 위상오프셋 오류검출 회로의 출력 값 'Validity'는 $a^*\hat{C}(1)\,(\mathrm{mod}\,n)$이 되므로, 이 값이 '1'이 아니면 계산된 위상오프셋의 값은 오류라고 판단하고, 이 값이 '1'이면 계산된 위상오프셋의 값은 오류가 아니라고 판단한다.

3. 오류검출능력을 보유한 위상오프셋 산출 회로

그림 10은 그림 1의 알고리듬에 기반하여 수신 이원부호의 위상오프셋을 산출하는 회로 구성도를 나타내고 있으며, 그림 8과 9의 회로를 이용하여 구현된다.

회로의 'Validity' 값이 '1'이 아니면, $\hat{k} \neq k$이고 수신된 이원부호에는 오류가 발생한 경우이므로, 계산된 위상오프셋 값을 출력하지 않고, 한 주기의 이원부호를 다

시 수신하여 위상오프셋을 계산한다. 만약 'Validity' 값이 '1'이면, 수신 이원부호에 오류가 발생하지 않았다고 판단하고 계산된 위상오프셋 값을 출력한다.

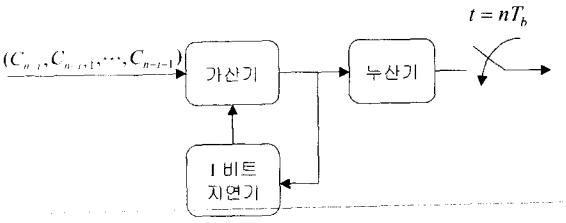

그림 6. $A^1(T^iC)$ 계산 회로 구성도
Fig. 6. Circuit block diagram to calculate $A^1(T^iC)$.

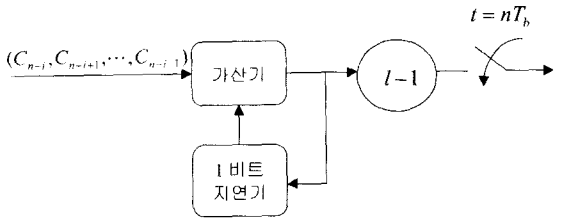

그림 7. $(l-1)C(1)$ 계산 회로 구성도
Fig. 7. Circuit block diagram to calculate $(l-1)C(1)$.

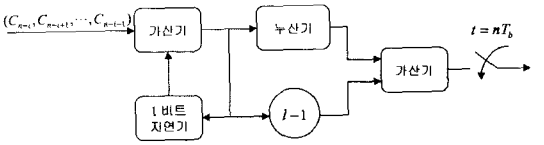

그림 8. $A^l(T^iC)$ 계산 회로 구성도
Fig. 8. Circuit block diagram to calculate $A^l(T^iC)$.

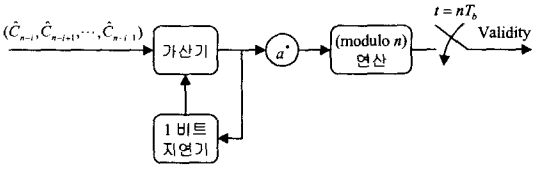

그림 9. 위상오프셋 오류 검출 회로
Fig. 9. Phase offset error detection circuit.

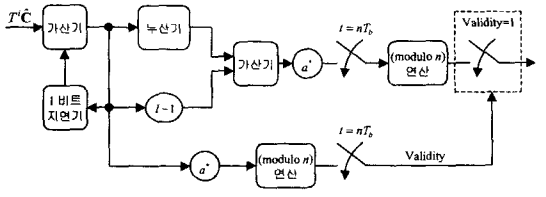

그림10. 오류검출 능력을 보유한 위상오프셋 산출 회로
Fig.10. Phase offset calculation circuit with error detection.

Ⅵ. 결 론

이원부호의 주기가 n이고, 이원부호에 포함된 '0'의 개수가 k일 때, n과 k가 서로 소인 조건을 만족하는 이원부호의 위상오프셋 산출과 패리티검사비트를 사용하지 않고 위상오프셋의 오류검출을 동시에 수행할 수 있는 효율적인 알고리듬을 정수론에 기반하여 제안하였다.

제안된 오류검출방법은 비교적 양호한 SNR 환경이나, 매우 낮은 SNR 환경에서는 오류검출실패확률이 감소하며, $\min(n-k,k)$의 값에 비례하여 오류검출실패확률이 증가하는 특성을 가지고 있으며, 이는 시뮬레이션을 통하여 이론치와 매우 근사적으로 일치함을 알 수 있었다. 그리고 이원부호의 위상오프셋 산출 회로의 일부를 이용하여 제안된 오류검출 방법을 구현할 수 있으므로, 회로의 복잡도가 증가하지 않는 장점이 있다.

제안된 방법은 패리티검사비트가 필요하지 않으며, 간단한 회로로 구현되는 장점이 있으나, 낮은 SNR에서 오류검출실패 확률이 증가하는 단점이 있다. 따라서, 이러한 단점을 보완하는 연구가 계속 진행되어져야 할 것이다.

참 고 문 헌

[1] B. Sklar, *Digital Communications*, Prentice-Hall, 1988.

[2] J. M. Wozencraft and I. M. Jacobs, *Principle of Communication Engineering*, John Willy, New York, 1965.

[3] TIA/EIA Interim Standard, *Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System*, July 1993.

[4] N. Zieler, "Linear Recurring Sequence," *J.Soc. Appl. Math.*, pp.31-48, July 1959.

[5] S.W. Golomb, *Shift Register Sequences*, Holden Day, San Francisco, 1967.

[6] D. V. Sarwate and M. B. Pursely, "Crossco-rrelation Properties of Pseudo random and Related Sequences," *Proc. IEEE*, vol. 68, no.5, pp.593-619, May 1980.

[7] A. J. Viterbi, *CDMA-Principles of Spread*

Spectrum Communication, Addition-Wesley, 1995.

[8] R. E. Ziemer and R. L. Peterson, Digital *Communications and Spread Spectrum Systems*, Macmillan ,1985.

[9] M. K. Simon, J. K. Omura, R. A. Scholtz and B. K. Levit, *Spread Spectrum Communications Handbook*, McGraw-Hill, 1994.

[10] J. K. Holmes, *Coherent Spread Spectrum Systems*, John Willy, New York, 1982.

[11] Y. Y. Han, "On the Minimization of Overhead in Channel Impulse Response Measurement," *IEEE Trans. on Veh. Technol.*, vol. 47, no.2, pp.631-636, May, 1998.

[12] J. G. Proakis, *Digital Communications*, McGraw-Hill, 2nd edition, 1989.

[13] A. Polydoros and C. L. Weber, "A Unified Approach to Serial Search Spread-Spectrum Code Acquisition-Part I : General Theory," *IEEE Trans. on Comm.*, vol. COM-32, no.5, pp.542-549, May, 1984.

[14] A. Polydoros and C. L. Weber, "A Unified Approach to Serial Search Spread-Spectrum Code Acquisition-Part II : A Matched-Filter Receiver," *IEEE Trans. on Comm.*, vol. COM-32, no.5, pp.550-560, May, 1984.

[15] P. M. Hopkins, "A Unified Analysis of Pseudonoise Synchronization by Envelope Correlation," *IEEE Trans. Comm.*, vol COM-25, no.8, pp.770-777, Aug., 1977.

[16] M. Willet, "The index of an m-sequence," *SIAM J, Appl.*, vol 25, no.1, pp.24-27, July 1973.

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

[18] I. Niven and H. S. Zukerman, *An Introduction to the Theory of Number*, John Wiley & Sons, 1980.

[19] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1990.

[20] I. N. Herstein, *Abstract Algebra*, Maxwell Macmillan, 1990.

[21] R. A. Dean, *Classical Abstract Algebra*, Harper & Row, 1990.

저 자 소 개

宋 寧 俊(正會員)

1987년 2월 : 한양대학교 전자통신공학과 공학사. 1994년 2월 : 한양대학교 전자통신공학과 공학석사. 1999년 2월 : 한양대학교 전자통신공학과 공학박사. 1994년 10월~현재 : LG정보통신 차세대 통신연구소 책임연구원. 주관심 분야 : 이동통신 시스템, 부호이론

韓 榮 烈(正會員) 第 34券 S編 第 11號 參照