새로운 주기 확장된 코드에 관한 연구

임 지 형, 김 운 경, *이 경 록
통신 신호처리 연구실
고려대학교 전파공학과, *(주)현대전자
전화 : 02-3290-3901 / 핸드폰 : 016-254-3246

Design and Investigation of new composite code

Ji-Hyung Lim, Woon-Kyung Kim, Kyung-Rok Lee
Communication Signal Processing Laboratory
School of Electrical Engineering, Korea University
E-mail : jhlim@davinci.korea.ac.kr

Abstract

There are many methods of generating PN sequences. In this paper, we propose and examine a new class of composite shift register to generate PN sequences. The new composite generator, in comparison with the original LFSR which generates PN codes of period 2^n-1, when coupled with codes of period k, generates PN codes with (longer) period LCM(2^n-1,k).

I. 서론

PN 코드 및 Walsh 코드와 같은 직교 코드는 DS/CDMA Spread System에서 다중 접속과 채널 코딩 목적으로 사용된다. 그러나, 간섭 신호의 영향을 최소화하기 위해 완전한 직교 성질을 갖는 코드는 필요하다. 이런 목적으로 개선된 correlation 성질을 갖는 새로운 복합 코드로서 기존의 PN코드를 주기 4배로 확장한 코드를 제안한다. 그리고 코드 하나 하나가 통신 자원임을 생각할 때, 여기서 제시하는 간단한 방법으로써 지금까지 알려진 m-시퀀스 generator 마다 새로운 코드 generator가 하나씩 늘어난다고 생각할 수 있으므로 코드의 수가 2배 이상으로 늘어난다[1,2,3].

본 논문에서는 DS/CDMA 시스템에서 사용하는 PN 코드와 Walsh 코드의 역할 및 특성을 통해 본 논문에서 새로 제시하는 코드 generator의 출력 코드 시퀀스를 분석할 것이다. 즉, 새로 제시할 구조의 출력 코드는 정보 신호를 확산하는 코드로서 채널 구분과 멀티플 액세스를 가능케 하는 Walsh 코드 및 PN 코드와 같이 통신에 활용할 경우 기본 바탕이 되는 복합 코드의 특성을 수학적 분석을 통해 알아본다.

II. Ramdomness Properties of Composite Sequences

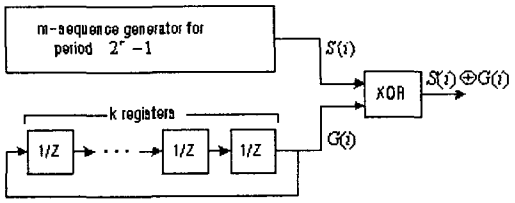

그림 1. 주기확장을 위한 복합코드 발생기
(1/Z: 지연 연산자(delay operator))

PN 시퀀스는 m-시퀀스라 해서 여러 가지 특성을 가지는데 특히 CDMA 시스템에서 이 시퀀스를 사용하는 근거가 되는 평형 특성(Balanced Property), 런 길이 특성(Run Length Property), 자기상관함수 특성(Corr

elation Property)의 세 가지 랜덤 특성들을 가진다. 여기서 제시되는 복합코드의 경우도 이 특성들이 만족하는지를 그림 1의 출력 단에서 본 확률적 관점을 통해 알아본다. [1,2]

일단, 본문에서는 복합코드가 $GCD(2^r-1, k)=1$일 때 주기가 $(2^r-1)k$이 경우를 대상으로 하고 전개했으며 다음처럼 자주 쓰이는 수학적 기호를 정의하였다.

$S(i)$: m-시퀀스 발생기의 출력 시퀀스로서 길이가 $(2^r-1)k$인 i번째 순환(cyclic) 시퀀스

$G(i)$: k-registers 발생기의 출력 시퀀스로서 길이가 $(2^r-1)k$인 i번째 순환(cyclic) 시퀀스 (단, $G(0)$: 00…01을 초기 값으로 갖는 시퀀스)

$\oplus$: 비트간의 EX-OR 연산자

2.1 평형 특성(Balanced Property)

그림 1의 출력 시퀀스는 0, 1로 구성된 일련의 시퀀스이다. 복합코드 발생기의 초기 값이 랜덤이라면 한 클락 시점에서 발생기의 출력 비트 0 또는 1의 확률은

$$\Pr(0) = \sum_{l=1}^{(2^r-1)k} \Pr(0|l)\Pr(l) = \frac{1}{2}\left\{1+\frac{2-k}{(2^r-1)\cdot k}\right\}$$

$$\Pr(1) = \sum_{l=1}^{(2^r-1)k} \Pr(1|l)\Pr(l) = \frac{1}{2}\left\{1-\frac{2-k}{(2^r-1)\cdot k}\right\}$$

이다. r=10, 30, 50이고 k=4일 경우, $\frac{2-k}{(2^r-1)\cdot k}$ 는 대략적으로 -4.9×10^{-4}, -4.7×10^{-10},-4.4×10^{-16} 값을 가진다.

2.2 런 길이 특성(Run Length Property)

복합 코드 발생기의 출력 시퀀스들은 총 $(2^r-1)k$의 개수를 가지고 이를 나열한 것이 그림 2이다. 가령 런 길이 1인 경우의 개수를 구할 때는 그림 2의 상자 안의 101 또는 010의 패턴을 갖는 것들의 수를 계산하면 된다. 이런 식으로 런 길이 $r-2$까지 할 수 있다. 그리고, 그 이후의 각 런 길이들은 LFSR의 구조, 즉 연결 변수들(connection variables)에 의해 결정된다[2].

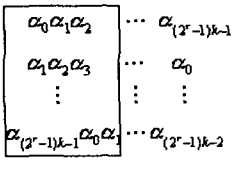

그림 2. 복합코드 발생기의 출력 시퀀스들

특정 런 길이의 상대적 빈도 수를 다음과 같이 정의 내리면,

$$\text{런 길이 n의 상대적 빈도 수} = \frac{\text{런 길이 n의 수}}{\text{전체 런 길이들의 총 수}}$$

이다. 그리고, 위 정의에 의해서 구해진 값들을 표 1에서 보여주고 있다. (M 은 여분의 런 길이들의 개수를 나타낸다.)

표 1. 런 길이 n의 상대적 빈도 수

($k>2$, $r>k+1$, $s=2,3,\cdots,r-k$)

런 길이 n	런 길이 n의 상대적 빈도 수	$r\to\infty$
1	$\frac{k\cdot 2^{r-2}-1}{k\cdot(1-(1/2)^{r-2})\cdot 2^{r-1}+M-2}$	$\frac{1}{2}$
2	$\frac{k\cdot 2^{r-3}}{k\cdot(1-(1/2)^{r-2})\cdot 2^{r-1}+M-2}$	$\frac{1}{2^2}$
⋮	⋮	⋮
$k-2$	$\frac{k\cdot 2^{r-(k-1)}}{k\cdot(1-(1/2)^{r-2})\cdot 2^{r-1}+M-2}$	$\frac{1}{2^{k-2}}$
$k-1$	$\frac{k\cdot 2^{r-k}-1}{k\cdot(1-(1/2)^{r-2})\cdot 2^{r-1}+M-2}$	$\frac{1}{2^{k-1}}$
k	$\frac{k\cdot 2^{r-(k+1)}}{k\cdot(1-(1/2)^{r-2})\cdot 2^{r-1}+M-2}$	$\frac{1}{2^k}$
$k+1$	$\frac{k\cdot 2^{r-(k+2)}}{k\cdot(1-(1/2)^{r-2})\cdot 2^{r-1}+M-2}$	$\frac{1}{2^{k+1}}$
⋮	⋮	⋮
$k+s-2$	$\frac{k\cdot 2^{r-(k+s-1)}-1}{k\cdot(1-(1/2)^{r-2})\cdot 2^{r-1}+M-2}$	$\frac{1}{2^{k+s-2}}$
⋮	⋮	⋮
$r-2$	$\frac{k\cdot 2^{r-(r-1)}-1}{k\cdot(1-(1/2)^{r-2})\cdot 2^{r-1}+M-2}$	0
여분의 런 길이들	$\frac{M}{k\cdot(1-(1/2)^{k+i-2})\cdot 2^{r-1}+M-2}$	0

표 1에서 보는 바와 같이 k가 고정되었을 때 $r\to\infty$ 함에 따라 m-시퀀스의 런 길이 특성과 같은 결과를 보여주고 있다. 반면, 반대로 r이 고정되어 있을 때에는 복합 코드 발생기의 동작이 m-시퀀스의 k 번째마다 비트의 보수를 취함 줌으로써 이루어지기 때문에, $k\to\infty$이라면 결국 생성되는 복합 코드는 자연스럽게 m-시퀀스의 런 길이 특성을 따라간다.

2.3 자기상관함수 특성(Correlation Property)

자기상관함수 값을 구하는 방법은 수신되는 시퀀스 $S(i)\oplus G(i)$을 $S(j)\oplus G(j)$과 비트마다 EX-OR을 해 준 다음 $0\to1$, $1\to-1$로 매핑(mapping)하고 이렇게 매핑된 $(2^r-1)k$개의 값들을 더해준 결과 값 $R(i-j)$으로써 구해진다.

먼저, $i=j$ 일 경우를 살펴보면, 같은 시퀀스의 EX-OR이므로 $R(0)$는 $(2^r-1)k$ 값을 갖는다.

$i\neq j$ 일 때는 두 가지로 나누어서 생각할 수 있다. 하나는 $|i-j|=k\cdot l$ (l은 정수)인 경우고 다른 하나는 $|i-j|\neq k\cdot l$ (l은 정수)인 경우이다. 전자의 경우는 $G(i)$와 $G(j)$이 서로 같기 때문에 결국 m-시퀀스 $S(i)$와 $S(j)$의 EX-OR가 되므로 $R(i-j)$은 $-k$ 값을 갖는다. 한편, 후자의 경우는 아래와 같이 분석된다.

$$[S(i)\oplus G(i)]\oplus[S(j)\oplus G(j)]=\{[S(i)\oplus S(j)]\oplus G(i)\}\oplus G(j)$$

$$S(i)\oplus S(j)\equiv \alpha_0\alpha_1\cdots\alpha_{2^r-1}\,\alpha_0\alpha_1\cdots\alpha_{2^r-1}\cdots\alpha_0\alpha_1\cdots\alpha_{2^r-1}$$

$$[S(i)\oplus S(j)]\oplus G(i)$$

$$=\alpha_{0\bmod 2^r-1}\alpha_{1\bmod 2^r-1}\cdots\overline{\alpha}_{|(k-1)-i|\bmod 2^r-1}\cdots\alpha_{(k-1)\bmod 2^r-1}$$

$$\alpha_{k\bmod 2^r-1}\alpha_{(k+1)\bmod 2^r-1}\cdots\overline{\alpha}_{|(2k-1)-i|\bmod 2^r-1}\cdots\alpha_{(2k-1)\bmod 2^r-1}$$

$$\vdots$$

$$\alpha_{(2^r-2)k\bmod 2^r-1}\alpha_{|(2^r-2)k+1|\bmod 2^r-1}\cdots\overline{\alpha}_{|(2^r-1)k-1-i|\bmod 2^r-1}\cdots\alpha_{|(2^r-1)k-1|\bmod 2^r-1}$$

이 때, 다음과 같은 명제의 참을 증명할 필요가 있다.

명제 1. $^{\exists}i\ (i=0,1,\cdots,k-1)$, $\left\{\overline{\alpha}_{|(mk-1)-i|\bmod 2^r-1}\right\}_{m=1}^{2^r-1}$ 의 각 원소는 오직 하나 밖에 없다.

증명) 정수 p,q에 대해서 $[(pk-1)-i]\bmod 2^r-1$과 $[(qk-1)-i]\bmod 2^r-1$을 같다고 가정하자.

이 때, $(pk-1)-i=a(2^r-1)+c$과 $(qk-1)-i=b(2^r-1)+c$의 방정식 차(a,b는 묶이고 c는 나머지)는 $(p-q)k=(a-b)(2^r-1)$이다. 여기서, $p-q<2^r-1$ 과 $GCD(2^r-1,k)=1$에 의해 가정은 모순이 된다.

위 명제는 $\left\{\overline{\alpha}_{|(mk-1)-i|\bmod 2^r-1}\right\}_{m=1}^{2^r-1}$과 $\{\overline{\alpha}_l\}_{l=0}^{2^r-2}$이 같다는 것을 암시하고 있다.

따라서, $\overline{\alpha}_{|(k-1)-i|\bmod 2^r-1}\overline{\alpha}_{|(2k-1)-i|\bmod 2^r-1}\cdots\overline{\alpha}_{|(2^r-1)k-1-i|\bmod 2^r-1}$을 재배열하면 $\overline{\alpha}_0\overline{\alpha}_1\cdots\overline{\alpha}_{2^r-1}$이 되기 때문에 다음과 같이 $[S(i)\oplus S(j)]\oplus G(i)$을 재배열하면 한 개의 $\overline{\alpha}_0\overline{\alpha}_1\cdots\overline{\alpha}_{2^r-1}$과 $(k-1)$개의$\alpha_0\alpha_1\cdots\alpha_{2^r-1}$으로 구성되어진다. 마찬가지로 $[S(i)\oplus S(j)]\oplus G(j)$일 경우도 똑같은 결과가 나온다. 이때, $G(i)$과 $G(j)$사이에 "1"의 위치가 일치하는 자리는 없으므로 결국, $[S(i)\oplus G(i)]\oplus[S(j)\oplus G(j)]$의 재배열은 두 개의 $\overline{\alpha}_0\overline{\alpha}_1\cdots\overline{\alpha}_{2^r-1}$과 $(k-2)$개의 $\alpha_0\alpha_1\cdots\alpha_{2^r-1}$으로 구성되어진다. 그러므로, 자기상관함수 $R(i-j)$ 값은 $-(k-4)$이 된다.

지금까지 구한 상관함수 값들을 그림 3에 도시하였다.

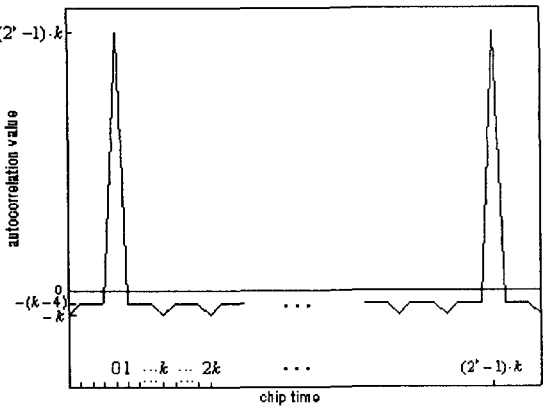

그림 3. 새로운 복합코드의 자기상관함수 $R(i-j)$

이 밖의 복합코드의 특성으로서 자기상관함수의 대칭적 특성이 있다. 예를 들어, $k=4$일 때 초기값 (0,0,0,1)의 주기 4인 $G(i)$시퀀스의 경우 복합코드의 자기상관함수는 초기값 (1,1,1,0)의 $\overline{G(i)}$ 시퀀스를 사용하는 복합코드의 자기상관함수와 같다. ($\overline{G(i)}$: $G(i)$의 보수)

III. 결론

지금까지 PN 코드의 랜덤 특성 세 가지가 이 새로운 복합코드에도 적용됨을 알았고 그 밖의 복합코드의 특성과 실제 통신 시스템에 적용시키는 연구가 필요할 것이라 사료된다.

Acknowledgement

본 논문은 한국학술진흥재단의 지원으로 수행된 연구과제 "디지털 위성 통신 변·복조, 부·복호화, 암호화 기반기술에 관한 연구"의 결과 중 일부입니다.

참고문헌(또는 Reference)

[1] J. S. Lee, "Theory of Linear Binary Sequences for CDMA Spread Applications", 한국전자통신연구소, 1993

[2] Andrew J. Viterbi, "CDMA Principle of Spread Spectrum Communication", Addison Wesley, 1995.

[3] 이경록, 김운경, 송문호, 김수원, "입력을 통한 PN

코드의 주기 확장". 대한 전자공학회 추계학술대회 논문집(A), 1996.

[4] Athanasions Papoulis, "Probability, Random Variables, and Stochastic Processes", McGraw-Hill, 1991.