세로운 주기 확장된 코드에 관한 연구

임지형, 김용경, 이경목
동음 신호처리 연구실
고려대학교 전기공학과, (주)현대전자
전화: 02-3290-3901 / 팩스: 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^k-1, when coupled with codes of period k generates PN codes with (longer) period LCM(2^k-1,k).

I. 서론

PN 코드 및 Walsh 코드와 같은 적약 코드는 DS/CDMA Spread System에서 다중 접속과 제필 코딩 목적으로 사용된다. 그러나, 간섭 신호의 영향을 최소화하기 위해 적절한 적약 코딩이 필요하다. 이런 목적으로 개선된 correlation 성질을 갖는 새로운 복합 코드로서 기존의 PN코드를 추가 4배로 확장할 코드를 제안한다. 그리고 코딩 하나가 동시에 사용할 때, 여기서 제시하는 간단한 방법으로써 지급까지 알려진 m-sequens generator에 새로운 코딩 generator가 하나씩 늘어나다 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 제안하는 코드 generator의 출력 코드 시퀀스를 분석한 것이다. 즉, 새로운 제시할 구조의 출력 코드는 정보 신호를 확산하는 코드로서 채널 구분과 인터 폴 액세스를 가능하게 하는 Walsh 코드 및 PN 코드와 같이 통신에 활용할 경우 기본 벡터가 되는 복합 코드의 특성을 수학적 분석을 통해 알아본다.

II. Randomness Properties of Composite Sequences

![Composite Sequence Diagram](attachment:composite_sequence.png)

그림 1. 주기확장된 복합 코드 생성기 (1/2: 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), 린 길이 특성(Run Length Property), 자기상관수 특성(Corr
2000年度 大韓電子工學會 秋季綜合學術大會 論文集 第23巻 第2호 2000/11

2.1 평형 특성(Balanced Property)

그림 1의 출력 시퀀스는 0, 1로 구성된 일련의 시퀀스이다. 복합 코드 발생기의 초기 값이 랜덤이라면 한 클럭 사이에서 발생기의 출력 비트 0 또는 1의 확률은

\[ P_r(0) = \frac{2-r}{2} \sum_{i=1}^{r} P_{r-i}(1) P_{i} \]

\[ P_r(1) = \frac{2-r}{2} \sum_{i=1}^{r} P_{r-i}(0) P_{i} \]

이므로, \( r=10, 30, 50 \)이고 \( k=4 \)일 경우, \( (2^{-1})^{k} \)는 대략적으로 \(-4.9 \times 10^{-4}, -4.7 \times 10^{-10}, -4.4 \times 10^{-16} \)을 가지게 된다.

2.2 힌 길이 특성(Run Length Property)

복합 코디 발생기의 출력 시퀀스들은 총 \( 2^{-1} \)의 개수들이 힌 길이를 彙로 이들 힌 길이가 그림 2이하다. 가령 힌 길이 1인 경우의 개수를 구할 때는 그림 2의 상자 안의 \( 101 \) 또는 \( 001 \)의 콘보를 갖는 것들의 수를 계산함으로써, \( \frac{1}{2} \times 2=1 \)가 된다. 이로써, 그 이후의 각 힌 길이들은 LFSR의 구조, 즉 연결 변수들에 의해 결정된다[2].

\[
\begin{array}{cccc}
\alpha_{0} \alpha_{1} \alpha_{2} & \cdots & \alpha_{r-1} \\
\alpha_{0} \alpha_{1} \alpha_{2} & \cdots & 0 \\
\alpha_{0} \alpha_{1} \alpha_{2} & \cdots & 0 \\
\end{array}
\]

그림 2 복합코드 발생기의 출력 시퀀스들

특정 힌 길이의 상대적 빈도 수를 다음과 같이 정의해보자.

\[
\text{단, } n\text{의 상대적 빈도 수 } = \frac{\text{전체 힌 길이들의 총 수}}{\text{단, } n\text{의 힌 길이들의 총 수}}
\]

이따라, 위 정의에 의해 구해진 결과들은 표 1에서 보여주고 있다. \( M \)은 여분의 힌 길이들의 개수를 나타낸다.

표 1. 힌 길이 n의 상대적 빈도 수

<table>
<thead>
<tr>
<th>n</th>
<th>힌 길이 n의 상대적 빈도 수</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( 2^{-1} )</td>
</tr>
<tr>
<td>2</td>
<td>( 2^{-1} )</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>k-1</td>
<td>( 2^{-1} )</td>
</tr>
<tr>
<td>k</td>
<td>( 2^{-1} )</td>
</tr>
<tr>
<td>k+1</td>
<td>( 2^{-1} )</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>r-2</td>
<td>( 2^{-1} )</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>\text{여분의 힌 길이들}</td>
<td>( k )</td>
</tr>
</tbody>
</table>

 표 1에서 보는 바와 같이 \( k \)가 고정되었을 때 \( r \rightarrow \infty \)함에 따라 m-시퀀스의 한 길이 특성이 같은 결과를 보여주고 있다. 반면, 반대로 \( r \)가 고정되어 있을 때에는 복합 코드 발생기의 동작이 m-시퀀스의 \( k \) 번째마디 비트의 보수를 취할 것으로 여겨져기 때문에, \( r \rightarrow \infty \)이라면 결과 생성되는 복합 코드는 자연스럽게 m-시퀀스의 한 길이 특성을 따르게 된다.

2.3 자기상관함수 특성(Correlation Property)

 자기상관함수를 구하는 방법은 수신되는 시퀀스 \( S(0) \otimes G(0) \)을 \( S(0) \otimes G(0) \)과 비트마다 EX-OR로 해 줄 다음 \( 0 \rightarrow 1, 1 \rightarrow 1 \)로 매핑(mapping)하고 이동계 매핑

\[
\text{단, } G(0) = (2^{-1})^{k} \]

\( \text{여분의 힌 길이들} \)의 결과를 다음과 같이 \( R(i-j) \)으로

\[ R(i-j) = \sum_{x=0}^{k-1} s(x) s(x+j) \]

과 매핑된다.
먼저, \( i = j \) 일 경우를 살펴보면, 같은 시퀀스의 EX-OR이므로 \( \mathcal{R}(0) \)는 \((2^r-1)k\) 값을 갖는다.

\( i \neq j \) 일 때는 두 가지로 나누어 생각할 수 있다. 하나는 \( |i-j| = k \cdot l \) (은 정수)인 경우이고, 다른 하나는 \( |i-j| \neq k \cdot l \) (은 정수)인 경우이다. 전자의 경우는 \( G(i) \)와 \( G(j) \)가 서로 같기 때문에 결국 \( m \)-시퀀스 \( S(\mathcal{G}) \)와 \( S(\mathcal{G}) \)의 EX-OR가 되므로 \( \mathcal{R}(i-j) \)은 \(-k\) 값을 갖는다.

한편, 후자의 경우는 아래와 같이 분석된다.

\[
\mathcal{R}(i-j) = \mathcal{S}(i) \oplus \mathcal{S}(j) \oplus \mathcal{G}(i) \oplus \mathcal{G}(j) = (\mathcal{S}(i) \oplus \mathcal{S}(j)) \oplus (\mathcal{G}(i) \oplus \mathcal{G}(j))
\]

\[
\mathcal{S}(i) \oplus \mathcal{S}(j) = a_1 a_2 \ldots a_{k-1} a_k a_1 \ldots a_{k-1}
\]

\[
\mathcal{G}(i) = a_{k+1} a_{k+2} \ldots a_{2r-1}
\]

\[
\mathcal{G}(j) = a_{k+1} a_{k+2} \ldots a_{2r-1}
\]

그림 3. 새로운 복합코드의 자기상관함수 \( \mathcal{R}(i-j) \)

이 방의 복합코드의 특성으로서 자기상관함수의 대칭적 특성이 있다. 예를 들어, \( k=4 \)일 때 초기값 \((0,0,1,1)\)의 위의 4인 \( G(i) \)시퀀스의 복합코드의 자기상관함수는 초기값 \((1,1,0,0)\)의 \( G(i) \)시퀀스를 사용하는 복합코드의 자기상관함수와 같다. (\( G(i) \)는 \( G(0) \)의 보수)

III. 결론

지금까지 PN 코드의 랜덤 특성 세 가지가 이 새로운 복합코드에서도 적용받을 것으로 예상하고 그 밖의 복합코드의 특성과 실제 통신 시스템에 적용시키는 연구가 필요할 것으로 사료된다.

Acknowledgement

본 논문은 한국과학기술연구원의 지원으로 수행된 연구와 "디지털 통신 통신 복호화, 붐호화, 암호화 기반기술에 관한 연구"의 결과 중 일부입니다.

참고문헌(또는 Reference)

[3] 이경목, 김은경, 송송호, 김수현, "입력은 동한 PN
코도의 추기 확장", 대한 전자공학회 추계학술대회
논문집(A), 1996.

Variables, and Stochastic Processes",