通信情報保護學會誌
第2卷, 第2號, 1992. 6

의사불규칙시퀀스들 사이의 관계

Relationship among pseudorandom sequences

노 종 선*

1. 개 요

지난 30여년 동안, 확산 스펙트럼의 개념은 다원접속(multiple access), 낮은 인터셉트 확률(low probability of intercept : LPI), 그리고 간섭과 전파방해에 대한 강한 면역성 등이 요구되는 통신 시스템에서 성공적으로 이용되어져 왔다[2,5,6,7]. 다원접속능력은 서명(signature) 시퀀스로써 의사불규칙시퀀스(pseudo random sequence)의 사용에 의해 가능해진다. 수 년에 걸쳐 m-시퀀스, GMW시퀀스, Kasami시퀀스, Gold시퀀스, bent시퀀스, 그리고 노(No)시퀀스와 같은 좋은 상관관계(correlation)의 성질을 갖는 몇몇 종류의 의사불규칙시퀀스들이 발견되었다. 본 논문에서는, 그러한 의사불규칙시퀀스들의 성질이 서술되었고, 그러한 시퀀스군 사이에 존재하는 상호관계를 규명하였다.

2. 의사불규칙시퀀스의 바람직한 성질들

주어진 크기의 의사불규칙시퀀스군에 대해 바람직한 몇가지 특성들이 있다.

- 낮은 out-of-phase 자기상관값(out-of-phase autocorrelation values)
- 낮은 상호상관값(crosscorrelation values)
- 큰 linear span
- 심볼의 균형(balance of symbols)
- 많은 서로 다른의 시퀀스군들의 존재
- 구현의 용이성
- 낮은 nontrivial partial-period(p-p) 상관값

낮은 nontrivial 자기상관값은 동기화(synchronization), ranging, 다중경로파에 대한 diversity를 위해서 중요하다. 주기 2^n-1인 이진 ± 1시퀀스에 대한 이상적인 자기상관함수는 nontrivial인 경우에 -1, trivial인 경우에 2^n-1값을 취하는 두개의 값을 가지는 함수이다. m-시퀀스[1]와 GMW시퀀스[12]는 이러한 이상적인 자기상관함수를 갖고 있다. 낮은 상호상관값은 동시에 여러개의 target들의 ranging뿐만이 아니라 코드분할 다원접속의 능력을 갖을 수 있기 위해 중요하다. Welch[17]에 의해서 유도된 최대 상관값에 대한 lower bound는 의사불규칙시퀀스군의 상관관계 성질을 평가하는데 자주 이용된다. Small set의 Kasami시퀀스군, 노시퀀스군[8], 그리고 bent시퀀스군[13,14,15] 등은 이러한 lower bound의 견지에서 최적인 상관값을 갖는 시퀀스군들이다.

시퀀스의 linear span은 최근에 많은 관심의 대상이 되고 있으며, 그것의 중요성은 큰 linear span을 갖고 있는 시퀀스들을 사용함에 의해서 얻게되는 intelligent jamming에 대한 증대되는 protection에 의해 기인된

* 건국대학교 전자공학과

다. 노, bent, GMW시퀀스의 linear span은 같은 주기를 갖고 있는 m-시퀀스, Gold와 Kasami시퀀스의 linear span과 비교했을 때 매우 크다. 전송된 신호의 스펙트럼 분석은 개략적으로 같은 수의 심볼을 가지는 의사불규칙시퀀스를 채택하는 것이 바람직하다는 것을 나타낸다. 사용가능한 시퀀스군의 갯수는 사용된 시퀀스군과 관련하여 도청자에 대한 불확실성의 척도로써 간주될 수 있으므로 서로 다른 시퀀스군의 갯수가 많다는 것은 바람직한 것이다. 또한, 구현하기 쉬운 시퀀스 사용의 중요성은 명백하다. 의사불규칙시퀀스의 주기가 너무 커서 전체 시퀀스에 대한 상관값을 계산하는 것이 실행가능하지 않다면 이때 p-p 상관값은 중요하다. 이것은 전체주기의 상관값에 대한 차선책이지만 p-p에 대한 상관값은 종종 사용되어진다. 의사불규칙시퀀스의 p-p상관 성질들은 분석하기가 어렵고 심지어는 경계의 결정조차 어려운 일이다[11,18].

이러한 잘 알려진 시퀀스군들의 성질들이 표 1에서 비교되어졌다. Gold시퀀스와 Kasami시퀀스의 linear span은 매우 작으나, bent시퀀스와 노시퀀스는 linear span이 대단히 커서 LPI가 요구되는 곳에서 유용한 시퀀스이다. 주어진 주기와 군의 크기에 대한 최대 상관값에 의하면, Kasami시퀀스군, bent시퀀스군, 그리고 노시퀀스군은 모두 Welch의 lower bound의 견지에서 최적이다. 주기가 2^n-1일때, bent시퀀스군은 n값이 4의 배수일때 존재하지만, 노시퀀스군은 n이 짝수일때 존재한다는 잇점을 가진다.

표 1. 여러가지 시퀀스군의 특성 비교

Family	Period	n	Size of Family	Maximum Correlation Value	Maximum Linear Span	Range of Sequence Imbalance
Gold	2^n-1	$2m+1$	2^n+1	$2^{(n+1)/2}+1$	$2n$	$[1,\ 2^{(n+1)/2}+1]$
Gold	2^n-1	$4m+2$	2^n+1	$2^{(n+2)/2}+1$	$2n$	$[1,\ 2^{(n+2)/2}+1]$
Kasami (Small Set)	2^n-1	$2m$	$2^{n/2}$	$2^{n/2}+1$	$3n/2$	$[1,\ 2^{n/2}+1]$
Kasami (Large Set)	2^n-1	$2m$	$2^{n/2}(2^n+1)$	$2^{(n+2)/2}+1$	$5n/2$	$[1,\ 2^{(n+2)/2}+1]$
Bent	2^n-1	$4m$	$2^{n/2}$	$2^{n/2}+1$	$\geq\binom{n/2}{n/4}\cdot 2^{n/4}$	1
No	2^n-1	$2m$	$2^{n/2}$	$2^{n/2}+1$	*	$[1,\ 2^{n/2}+1]$

* 시퀀스군내의 각 시퀀스의 linear span은 그 시퀀스군에 있는 GMW시퀀스의 linear span 보다 크다.

3. 여러가지 의사불규칙시퀀스의 정의

Trace 함수는 finite field로 부터 subfield로의 선형 매핑인데 이 함수는 의사불규칙시퀀스의 디자인과 분석을 위한 중요한 수학적 도구로써 널리 사용된다. Trace 함수에 대한 정의와 그것의 성질들을 보면, 대부분의 이진 의사불규칙시퀀스들은 trace 함수의 형태로 표현될 수 있다. 임의의 두 정수

$k,\ l>0,\ k|l$에 대해, trace 함수 $tr_k^l(\cdot)$는 다음과 같은 관계식에 의해 정의된다.

$$tr_k^l(x)=\sum_{i=0}^{\frac{l}{k}-1} x^{2^{i\cdot k}}, \qquad (1)$$

여기서 x는 $GF(2^l)$의 원소이다.

Trace 함수는 다음과 같은 유용한 성질들을 갖고

있으며 이 성질들은 쉽게 증명된다.

• $GF(2^l)$의 모든 α에 대해, $tr_k^l(\alpha)$는 $GF(2^k)$의 요소이다.

• 모든 i, $0\leq i\leq l/k-1$에 대해

$$tr_k^l(\alpha^{2^{k\cdot i}})=tr_k^l(\alpha). \tag{2}$$

• Trace함수는 선형이다. 즉, 모든 a, $b\in GF(2^k)$와 α, $\beta\in GF(2^l)$에 대해

$$tr_k^l(a\cdot\alpha+b\cdot\beta)=a\cdot tr_k^l(\alpha)+b\cdot tr_k^l(\beta). \tag{3}$$

• $GF(2^k)$의 요소인 a를 고정시켰을 경우, α가 $GF(2^l)$의 모든 요소로 변함에 따라 $tr_k^l(\alpha)=a$는 정확하게 2^{l-k}번 발생한다.

• $GF(2^l)$에서, 어떤 γ, $\gamma\neq 0$에 대해

$$\sum_{a\in GF(2^l)}(-1)^{tr_1^l(a\cdot\gamma)}=0. \tag{4}$$

• 만약 $GF(2^k)\subset GF(2^l)$ 이라면,

$$tr_k^m\{tr_m^l(\alpha)\}=tr_k^l(\alpha). \tag{5}$$

$m_a(x)$를 $GF(2^k)$의 요소를 계수로 갖는, $GF(2^l)$에 있는 한 원소 α의 d차 최소다항식이라 하자. 그러면 $m_a(x)$의 근들은 α, α^{2^k}, $\alpha^{2^{2k}}$, …, $\alpha^{2^{(d-1)\cdot k}}$이고 $m_a(x)$에서 x^{d-1}의 계수는 $-\sum_{i=0}^{d-1}\alpha^{2^{i\cdot k}}$이다. 그러므로, $-tr_k^l(\alpha)$는 $GF(2^k)$의 요소를 계수로 갖는 α의 최소다항식에서, x^{d-1}의 계수이며 $GF(2^k)$의 요소다. Trace 함수에 대한 위와같은 성질들은 이미 알려진 시퀀스들을 정의하고 이러한 시퀀스들의 많은 성질들을 증명하는데 사용될 것이다.

m-시퀀스, $m(t)$와 GMW시퀀스, $g(t)$는 각각 아래와 같이 주어진다.

$$m(t)=tr_1^n(\alpha^t), \tag{6}$$

$$g(t)=tr_1^m\{[tr_m^n(\alpha^t)]^r\}, \tag{7}$$

여기서 α는 $GF(2^n)$의 한 primitive 원소이고, m|n, $1\leq r<2^m-1$, $gcd(2^m-1,\ r)=1$이다. 그리고 Kasami시퀀스와 노시퀀스는 아래와 같이 주어진다.

n, $n>0$,은 짝수라 하고, $N=2^n-1$, $m=n/2$, 그리고 $T=\dfrac{2^n-1}{2^m-1}=2^m+1$이라 하자. 그러면 Kasami시퀀스는

$$k_i(t)=tr_1^n(\alpha^{2t})+tr_1^m(\gamma_i\cdot\alpha^{T\cdot t}), \tag{8}$$

로서 주어진다. 여기서 α는 $GF(2^n)$의 한 primitive 원소이고 γ_i는 $GF(2^m)$의 요소이다. 그리고 노시퀀스는

$$s_i(t)=tr_1^m\{[tr_m^n(\alpha^{2t})+\gamma_i\cdot\alpha^{T\cdot t}]^r\}, \tag{9}$$

로서 정의된다. 여기서 α는 $GF(2^n)$의 한 primitive 원소이고, 정수 r, $1\leq r<2^m-1$, 은 $gcd(2^m-1,\ r)=1$을 만족시키고, 원소 γ_i는 i가 1과 2^m 사이의 값을 가질때 각각의 i값에 대해 $GF(2^m)$의 요소를 정확하게 하나씩 취한다.

4. m-시퀀스와 GMW시퀀스와의 관계

이 절에서는, GMW시퀀스와 m-시퀀스사이의 관계에 대해서 설명한다. $s(t)$가 주기가 N인 의사불규칙시퀀스라 하고 q는 1과 $N-1$ 사이의 임의의 정수라 하자. 그러면 시퀀스 $s(q\cdot t)$ (곱셈은 modulo N으로 이행됨.)는 $s(t)$의 q에 의한 decimation시퀀스라고 한다. n을 합성수(composite integer)라 하자.

$$n=e\cdot m. \tag{10}$$

모든 m-시퀀스 $s(t)$의 시간이 천이된 시퀀스 $s(t+\tau)$, $0\leq\tau\leq N-1$ 중에서 다음의 성질을 만족시키는 경우는 한 경우만 존재한다.

$$s(2\cdot(t+\tau))=s(t+\tau),\quad 0\leq t\leq N-1. \tag{11}$$

위의 성질을 만족하는 m-시퀀스 $s(t+\tau)$는 *characteristic phase* m-시퀀스라고 불리어진다.

$m(t)$를 아래의 수식으로 주어지는 주기가 $N=2^n-1$의 m-시퀀스라 하자.

$$m(t)=tr_1^n(\alpha^t), \tag{12}$$

여기서 α는 $GF(2^n)$의 한 primitive 원소이다. 그러면 수식 (2)에 의해서 $m(t)$는 *characteristic phase* m-시퀀스가 된다. Trace 함수의 특성을 이용하여, $m(t)$는 아래의 형태로 쓸 수 있다.

$$m(t)=tr_1^m\{tr_m^n(\alpha^t)\}. \tag{13}$$

$T=\dfrac{2^n-1}{2^m-1}$ 라 하고, t_1, t_2는 t의 기수-T확장(base-T expansion)에서 생기는 10진수(digit)라 한다. 즉, $t=t_1\cdot T+t_2$, $0\leq t_1\leq 2^m-2$, $0\leq t_2\leq T-1$ 이다.

α^T의 차수는 2^m-1이기 때문에, α^T는 $GF(2^n)$의 subfield인 $GF(2^m)$의 primitive 원소이다. Trace 함수의 선형성을 사용하여, $m(t)$에 대하여 다음과 같이 변형된 표현을 얻는다.

$$m(t)=tr_1^m\{\alpha^{t_1\cdot T}\cdot tr_m^n(\alpha^{t_2})\}. \quad (14)$$

$\beta=\alpha^T$라 하면 β는 $GF(2^m)$의 primitive 원소이다. 그러면, m-시퀀스는 두개의 독립변수에 의해서 다음과 같이 표현될 수 있다.

$$m(t)=tr_1^m(\beta^{t_1}\cdot\beta^{f(\alpha,t_2)}). \quad (15)$$

$f(\alpha, t_2)\neq-\infty$인 t_2의 고정된 값에 대하여, $m(t)$를 t_1의 함수로 간주하여 얻어진 $m(t)$의 부분시퀀스(subsequence)는 주기가 2^m-1인 m-시퀀스이다. 여기서 위상은 $f(\alpha, t_2)$에 의해서 결정된다. 그러므로, 각각의 부분시퀀스는 $f(\alpha, t_2)$의 값에 따라 all-zero 시퀀스 또는 주기가 2^m-1 m-시퀀스가 된다. 수식 (7)로 부터, GMW시퀀스의 두개의 독립변수에 의한 표현은 아래와 같다.

$$g(t)=tr_1^m(\beta^{r\cdot t_1}\cdot\beta^{r\cdot f(\alpha,t_2)}). \quad (16)$$

여기서도 마찬가지로 $g(t)$는 $f(\alpha, t_2)\neq-\infty$인 t_2의 고정된 값에 대하여 2^m-1 주기의 m-시퀀스이므로, 각각의 부분시퀀스는 f(α, t_2)의 값에 따라 all-zero 시퀀스 또는 주기가 2^m-1인 이전 m-시퀀스의 decimation시퀀스이다.

[예제] $n=6$, $m=3$, $r=3$, 그리고 α의 primitive 다항식을 x^6+x+1라 하자. 그러면 주기 63의 m-시퀀스는 다음과 같이 표현될 수 있다.

$$m(t)=tr_1^6(\alpha^t) \quad (17)$$

$$g(t)=tr_1^3\{[tr_3^6(\alpha^t)]^3\}. \quad (18)$$

M-sequence

t_1 \ t_2	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	1	0	0	0
1	0	1	1	0	0	0	1	0	1
2	0	0	1	1	1	1	0	1	0
3	0	0	1	1	1	0	0	1	0
4	0	1	0	1	1	0	1	1	1
5	0	1	1	0	0	1	1	0	1
6	0	1	0	1	1	1	1	1	1

GMW-sequence

0	1	2	3	4	5	6	7	8
0	1	1	1	1	0	1	1	1
0	0	1	1	1	1	0	1	0
0	1	0	1	1	0	1	1	1
0	1	0	0	0	1	1	0	1
0	1	1	0	0	1	1	0	1
0	0	0	1	1	1	0	1	0
0	0	1	0	0	0	0	0	0

Each pair of column sequences
are related by decimation by 3.

$m(t)=$	000001000	011000101	001111010	001110010	010110111	011001101	010111111
$g(t)=$	011110111	001111010	010110111	010001101	011001101	000111010	001000000
$t_1=$	0	1	2	3	4	5	6

Characteristic phase subsequence of m-sequence : 1110100
Characteristic phase subsequence of GMW sequence : 1001011

그림 1. 주기가 63인 m-시퀀스와 GMW시퀀스의 관계

수식 (15)와 (16)을 이용하여 얻어진 이러한 시퀀스의 2차원 표현이 그림 1에 나타나 있다. 이전에 언급한 것처럼 각각의 부분시퀀스는 all-zero 시퀀스 또는 주기 7의 m-시퀀스임을 그림 1에서 볼 수 있다. 각 열에서 굵은 획의 글씨(boldface) 1은 각 부분(열) 시퀀스의 characteristic phase 시퀀스의 시작점을 나타낸다. 다시 사전에 언급했든 것처럼, m-시퀀스에서 각 부분시퀀스의 characteristic phase로 부터의 위상 천이는 GMW시퀀스에서 대응된 각 부분시퀀스의 위상천이와 같다. 그러나 GMW시퀀스에서 i번째 부분(열) 시퀀스는 m-시퀀스에서 i번째 부분(열) 시퀀스의 3에 의한 decimation을 통해 얻어진다.

5. 노시퀀스와 Kasami 시퀀스와의 관계

앞의 절에서 처럼, Kasami 시퀀스는 2차원 배열로 나타내기 위해 다음과 같은 t의 표현을 바꿀 수 있다. $t=t_1 \cdot T+t_2$, $0\le t_1\le 2^m-2$, $0\le t_2\le T-1$과 $T=2^m+1$이라 하자. 그러면,

$$\begin{aligned} k_i(t) &= tr_1^m\{tr_m^n(\alpha^{2t})+\gamma_i\cdot\alpha^{T\cdot t}\} \\ &= tr_1^m\{tr_m^n(\alpha^{2t_1\cdot T+2t_2})+\gamma_i\cdot\alpha^{T\cdot(t_1\cdot T+t_2)}\} \\ &= tr_1^m\{\alpha^{2t_1\cdot T}\cdot[tr_m^n(\alpha^{2\cdot t_2})+\gamma_i\cdot\alpha^{T\cdot t_2}]\}, \end{aligned} \tag{19}$$

여기서

$$\alpha^{T^2\cdot t_1}=\alpha^{T\cdot(2^m-1)\cdot t_1+2T\cdot t_1}=\alpha^{2T\cdot t_1}. \tag{20}$$

앞절에서 처럼 $\beta=\alpha^T$로 놓고 함수 $f(\alpha,\ \gamma_i,\ t_2)$가

$$\beta^{2f(\alpha,\gamma_i,t_2)}=tr_m^n(\alpha^{2\cdot t_2})+\gamma_i\cdot\alpha^{T\cdot t_2},\quad 0\le t_2\le 2^n-2. \tag{21}$$

로 정의 된다고 하자. 결과적으로 Kasami 시퀀스에 대한 두개의 독립변수에 의한 표현

$$k_i(t)=tr_1^m\{\beta^{t_1+f(\alpha,\gamma_i,t_2)}\} \tag{22}$$

는 $(2^m-1)\times T$ 행렬이 된다. $f(\alpha,\ \gamma_i,\ t_2)$의 값에 따라, t_1 변수에 의한 시퀀스로써 t_2번째 부분(열) 시퀀스는 all-zero 시퀀스 또는 주기가 2^m-1인 m-시퀀스이다. 함수 $f(\alpha,\ \gamma_i,\ t_2)$의 값은 t_2번째 부분(열) 시퀀스의 위상을 결정해 준다.

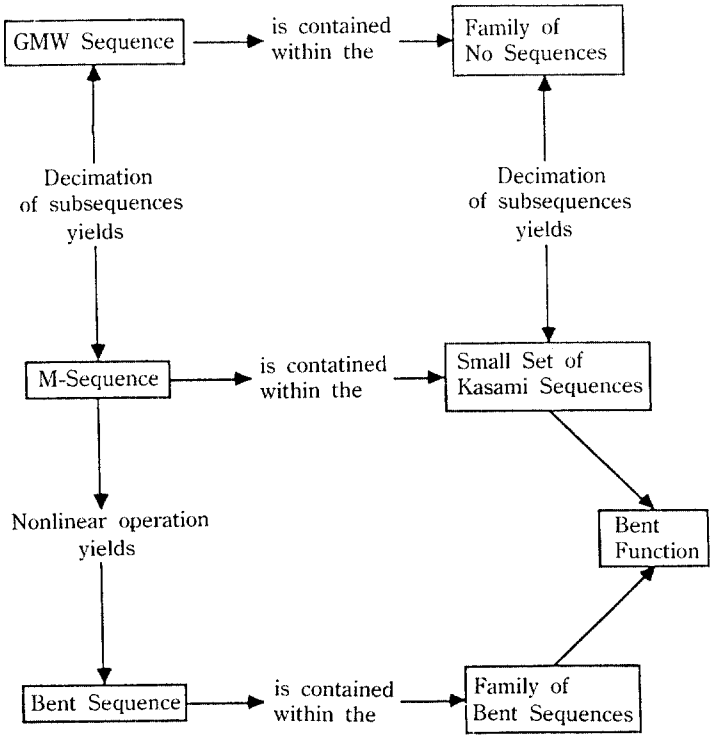


그림 2. 여러가지 의사불규칙시퀀스 사이의 관계

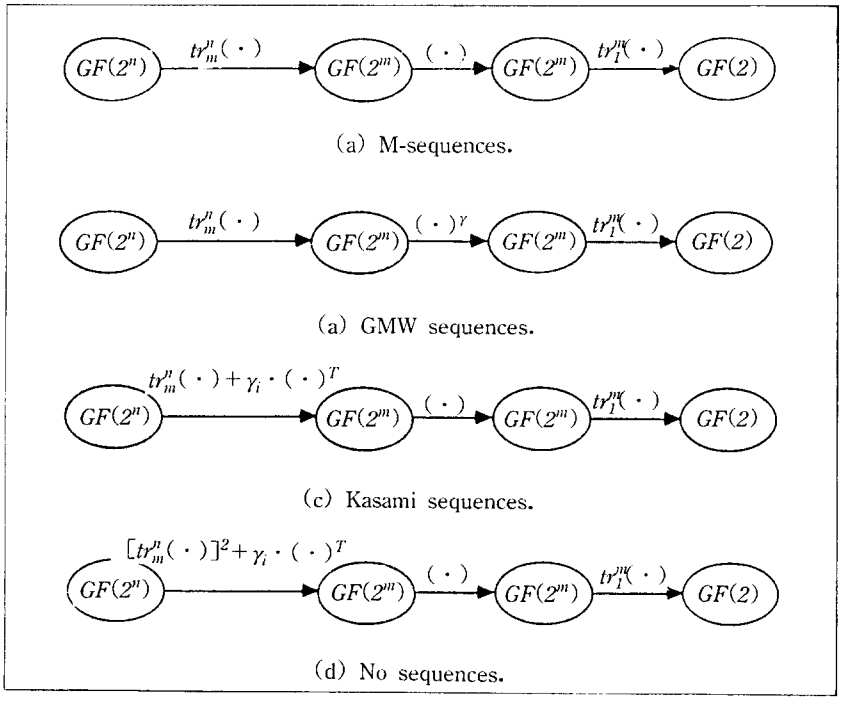


그림 3. 노시퀀스군과 Kasami 시퀀스군의 수학적인 관계

수식 (9), (16) 그리고 (19)로 부터, 같은 방법에 의해 노시퀀스의 두개의 독립변수에 의한 표현을 다음과 같이 나타낼 수 있다.

$$s_i(t)=tr_1^m\{\beta^{r\cdot[t_1+f(\alpha,\gamma_i,t_2)]}\}. \qquad (23)$$

만약 $f(\alpha,\ \gamma_i,\ t_2)=-\infty$이면, 변수 t_1에 의한 부분(열) 시퀀스는 all-zero 시퀀스가 됨을 주목해야 한다.

분명히 Kasami 시퀀스와 노시퀀스 모두에 대하여 위상함수 $f(\alpha,\ \gamma_i,\ t_2)$는 같다. 더구나, 다음장에서 볼 수 있듯이, 군의 크기, 상관관계(correlation), 그리고 균형 특성(balance property)들은 두 시퀀스군에 있어서 같다. 두 시퀀스군 사이의 차이점은 Kasami 시퀀스의 t_2번째 부분(열) 시퀀스를 r에 의한 decimation을 행하면 노시퀀스의 대응되는 열의 부분시퀀스가 된다는 것이다.

노시퀀스를 다른 이미 잘 알려진 시퀀스와의 관련을 설명하기 위하여 수식 (9)에서 $\gamma_i=0$라 하자. 그러면 (9)에서의 노시퀀스는 GMW시퀀스가 된다. 다른말로 하면 노시퀀스의 각 군은 정확히 하나의 GMW시퀀스를 포함한다. 만약 r을 1로 놓으면 노시퀀스군은 Kasami시퀀스군이 된다. 즉 Kasami시퀀스군은 노시퀀스군의 특별한 경우로 간주할 수 있다. 더구나, (9)에서 $r=1$, $\gamma_i=0$로 놓으면, 노시퀀스는 m-시퀀스가 된다. 이러한 관계는 그림 2에 요약되어 있다.

그림 3에서 여러가지 시퀀스사이에 존재하는 $GF(2^n)$로 부터 $GF(2)$로의 매핑을 도시하였다.

참 고 문 헌

[1] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA : Holden-Day, 1967 ; revised edition, Laguna Hills, CA : Aegean Park Press, 1982.

[2] M.K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications. Volume I*, Rockville, MD : Computer Science Press, 1985.

[3] E. R. Berlekamp, *Algebraic Coding Theory*. New York : McGraw-Hill, 1968.

[4] F. J. MacWilliams and N. J. A. Sloane, *The*

Theory of Error-Correcting Codes. Amsterdam, the Netherlands : North-Holland, 1977.

[5] R. A. Scholtz, "The origins of spread-spectrum communications", *IEEE Trans. Commun.*, Vol. COM-30, pp. 822-854, May, 1982.

[6] R. A. Scholtz, "The spread spectrum concept", *IEEE Trans. Commun.* Vol. COM-25, pp. 748-755, Aug, 1977.

[7] D. V. Sarwarte and M. B. Pursley, "Cross-correlation properties of pseudorandom and related sequences", *Proc. IEEE*, Vol. 68, pp. 593-620, May, 1980.

[8] J. S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span", *IEEE Trans. Inform. Theory*, Vol IT-35, no. 2, pp. 371-379, March, 1989.

[9] J. S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span", in *IEEE Int. Conf. Communication* (Philadelphia, PA), Conference Record, pp. 25. 4. 1-25. 4. 5., June 12-15, 1988.

[10] J. S. No and P. V. Kumar, "Exact linear span expressions for a family of recently discovered binary pseudorandom sequences", in *1988 IEEE International Symposium on Information Theory* (Kobe, Japan), Proceeding p. 10, June 19-24, 1988.

[11] J. S. No and P. V. Kumar, "On the partial-period correlation moments of GMW sequences", in *IEEE MILCOM' 87 Conf. Record* (Washington D. C.), pp. 33. 6. 1-33. 6. 4. Oct. 19-22, 1987.

[12] R. A. Scholtz and L. R. Welch, "GMW sequences", *IEEE Trans. Inform. Theory*, Vol. IT-30, pp. 548-553, May, 1984.

[13] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences", *IEEE Trans. Inform. Theory*, Vol. IT-28, pp. 858-864, Nov. 1982.

[14] P. V. Kumar and R. A. Scholtz, "Bounds on the linear span of bent sequences", *IEEE Trans. Inform. Theory*, Vol. IT-29, pp. 854-862, Nov. 1983.

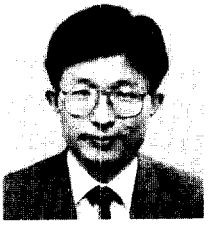
[15] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties", *Journal of Combinatorial Theory*, Series A, Vol. 40, pp. 90-107, Sep, 1985.

[16] R. Gold, "Optimal binary sequences for spread spectrum multiplexing", *IEEE Trans. Inform. Theory*, Vol. IT-13, pp. 619-621, Oct, 1967.

[17] L. R. Welch, "Lower bounds on the maximum cross correlation of signals", *IEEE Trans. Inform. Theory*, Vol. IT-20, pp. 397-399, May, 1974.

[18] P. V. Kumar, "The partial-period correlation moments of arbitrary binary sequences", in *IEEE Global Telecommunications Record*, pp. 499-503, December 2-5, New Orleans, 1985, *IEEE Trans. Inform. Theory*, Vol. IT-14, No. 4, pp. 569-576, July, 1968.

□ 著者紹介



盧 宗 善(終身會員)

서울대학교 공과대학 전자공학과(학사)
서울대학교 대학원 전자공학과(석사)
University of Southern California Dept. of Electrical Eng. (공학박사)
1988년 2월~1990년 7월 (미국) Hughes Network Systems 연구원
1990년 9월 1일~현재 : 건국대학교 공과대학 전자공학과 조교수
관심분야 : 위성통신, 이동통신, 암호학, Error Correcting Codes