



저작자표시-비영리-동일조건변경허락 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.
- 이차적 저작물을 작성할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



동일조건변경허락. 귀하가 이 저작물을 개작, 변형 또는 가공했을 경우에는, 이 저작물과 동일한 이용허락조건하에서만 배포할 수 있습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

이 학 석 사 학 위 논 문

낮은 상관관계 함수를 갖는 이진수열



2012년 2월

부 경 대 학 교 대 학 원

응 용 수 학 과

안 현 주

이 학 석 사 학 위 논 문

낮은 상관관계 함수를 갖는 이진수열

지도교수 조 성 진

이 논문을 이학석사 학위논문으로 제출함.



2012년 2월

부 경 대 학 교 대 학 원

응 용 수 학 과

안 현 주

안현주의 이학석사 학위논문을 인준함.

2011년 12 월



주 심 이학박사 표 용 수 (인)

위 원 이학박사 박 진 한 (인)

위 원 이학박사 조 성 진 (인)

< 목 차 >

그림 목차		ii
표 목차		ii
Abstract		iii
1. 서론		1
2. 배경지식		2
2.1 트레이스 함수		2
2.2 유한체위에서의 2차 방정식의 해 구하기		3
2.3 의사난수열의 기본성질 및 구조		7
2.4 부호분할다중접속(CDMA)		12
2.5 Welch의 lower bound		13
3. 기존 이진수열 분석		14
3.1 이상적인 상관관계 함수를 갖는 이진수열		14
3.2 3개의 상관관계 함수를 갖는 기존 이진수열		19
3.3 5개의 상관관계 함수를 갖는 기존 이진수열		24
4. 확장 Zeng 수열군의 생성 및 분석		26
5. 결론		34
참고문헌		35

< 그림 목차 >

<그림 3.1>	$x^2 + x + 1, x^3 + x + 1$ 의 window property	15
<그림 3.2>	m -수열과 GMW-수열 관계	18
<그림 3.3>	Kasami-수열과 No-수열 관계	21
<그림 3.4>	수열의 관계도	21

< 표 목차 >

<표 2.1>	Run 분포성질	10
<표 2.2>	$x^5 + x^2 + 1$ 분포성질	10
<표 3.1>	$\alpha^4 + \alpha + 1$ 생성된 수열	23
<표 3.2>	수열 $s_{63,2}$, 수열 $s_{43,7}$ 의 상관관계 함수	25
<표 3.3>	기존 이진수열의 특성	25
<표 4.1>	매개변수 변화에 따른 수열들의 모임	27
<표 4.2>	수열 s_{ij} , 수열 s_{pq} 의 상관관계 함수	32
<표 4.3>	수열 s_{ij} , 수열 s_{pq} 의 상관관계 함수	33

Binary Sequences with Low Correlation Functions

Hyun-Ju An

Department of Applied Mathematics, Graduate School,
Pukyong National University

Abstract

In Code Division Multiple Access system (CDMA), a family of binary sequences with low correlation needs to minimize multiple access interference (MAI). Sequences with low correlation play crucial roles in DS-CDMA(Direct sequence code division multiple access) systems and DS-UWB(DS Ultra wide band) systems.

Low correlation systems are used in many applications in digital spread spectrum communication systems. The correlation values can be computed using the relation between the degree of the polynomial and the number of the roots.

In thesis paper, we propose the extended Zeng-sequences with large family size and high linear span and analyze the correlation of the sequence. A new family of binary sequences include m -sequences, GMW-sequences, Kasami-sequences, No-sequences and Zeng-sequences.

1. 서 론

오늘날 다양한 매체를 통한 통신량은 지금까지도 꾸준히 증가해 오고 있다. 이러한 통신량의 증가는 전 세계 사용자들로 하여금 통신 채널들을 공유할 수 있도록 할당해 주는 다양한 방법들에 대한 필요성을 야기 했다. 또다른 상대방으로 부터의 불필요한 방해로 저항하는 그것의 능력 덕분에 전체 혹은 부분적인 공유를 위해 부호분할다중접속(CDMA: Code Division Multiple Access) 통신 시스템은 효율성 매우 높다. 예를 들면, 낮은 상호상관관계를 가지는 여러 수열들은 각 채널에 보내진 신호들을 결정짓기 위해 CDMA통신에서 중요하며, 효율적인 성능을 내기 위해서는 낮은 상관관계 함수를 갖는 수열군을 사용하는 것이 필수적이다. 쉽게 생성된 이진수열들의 큰 모임을 찾는 것 역시 필수적이며, 상관관계 함수값들이 작아지고 그 모임이 커질수록, 시스템의 용량은 더 높아진다[4,6,8].

시스템의 효율적인 성능을 내기 위해서는 낮은 상관관계 함수를 갖는 많은 서로 다른 수열군들의 존재가 필수적이다. 수열들의 모임이 이와 같은 응용분야에 대하여 가져야할 바람직한 사항들은 낮은 상관관계 함수이며, 또한 이러한 상관관계 함수는 방정식의 차수와 근의 개수 사이의 관계를 기반으로 하여 구할 수 있다.

Welch의 lower bound[16]에서 최적의 상관관계 함수를 갖는 수열들은 사용할 수 있는 수열군의 개수가 작고 선형 복잡도가 낮기 때문에 이를 개선하기 위해서는 확산수열의 상관관계를 높이는 것이 불가피하다. Zeng등은 상호상관관계 함수값이 5개인 이진수열군을 제안했다[17].

본 논문에서는 수열군의 크기가 크고 선형 복잡도가 높은 새로운 확장 Zeng 수열군을 제안하고 그 상관관계를 분석한다. 이 수열군은 m -수열, GMW-수열, Kasami-수열, No-수열, Zeng-수열을 모두 포함 한다[3,10,14,15,17].

2. 배경지식

2.1 트레이스 함수(Trace function)

<정의 2.1.1 [11,12]> 임의의 두 정수 $m, n (> 0, m | n)$ 에 대하여 $m | n$ 이므로 $GF(2^m)$ 은 $GF(2^n)$ 의 부분체(subfield)이다. 따라서 $GF(2^n)$ 을 정의역으로 하고 $GF(2^m)$ 을 공역으로 하는 트레이스 함수 $Tr_m^n(\cdot)$ 를 다음과 같이 정의한다.

$$Tr_m^n(\alpha) = \sum_{i=0}^{\frac{n}{m}-1} \alpha^{2^{m \cdot i}} \quad (2.1)$$

여기서 α 는 n 차 원시 다항식 $f(x)$ 의 원시근이다. 특별히 $m=1$ 이면 식 (2.1)은 $Tr_1^n(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + \alpha^{2^3} + \dots + \alpha^{2^{n-1}}$ 이다. 이와 같이 정의된 트레이스 함수는 다음과 같은 여러 가지 유용한 성질을 만족한다.

<정리 2.1.2 [11,12]> 임의의 두 자연수 $m, n (m | n)$ 에 대하여 트레이스 함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$ 는 다음 성질을 갖는다.

- (1) $\forall x, y \in GF(2^n), Tr_m^n(x+y) = Tr_m^n(x) + Tr_m^n(y)$
- (2) $\forall x \in GF(2^n), \forall c \in GF(2^m), Tr_m^n(cx) = c \cdot Tr_m^n(x)$
- (3) $GF(2^m)$ 의 모든 고정된 원소 c 에 대하여, $Tr_m^n(x) = c$ 를 만족하는 $GF(2^n)$ 상에서 x 는 정확히 2^{n-m} 개를 갖는다.
- (4) $\forall x, y \in GF(2^n), Tr_m^n(c) = nc$
- (5) $\forall x, y \in GF(2^n), Tr_m^n(x^{2^{m \cdot i}}) = Tr_m^n(x)$
- (6) $\forall x, y \in GF(2^n), Tr_1^n(x) = Tr_1^m(Tr_m^n(x))$

2.2 유한체 위에서의 2차 방정식의 해 구하기

무한체인 $\mathbb{R}$ 위에서의 2차방정식 $Ax^2 + Bx + C = 0$, $A, B, C \in \mathbb{F}_{2^n}$ 은 판별식 $B^2 - 4AC$ 에 의해서 결정된다[1,12]. 예를 들어 $x^2 + x + 1$ 은 $\mathbb{R}$ 위에서 해를 갖지 않으나 복소수체 $\mathbb{C}$ 위에서 해를 갖는다. 그 해를 α_1, α_2 라 하면

$$x^2 + x + 1 = (x - \alpha_1)(x - \alpha_2) = 0 \quad (2.2)$$

이다. $\alpha_1 \cdot \alpha_2 = 1$ 이다.

(1) $B=0$ 인 경우 : $Ax^2 = C$ 이다. $x^2 = CA^{-1}$ 이므로 반드시 해를 갖는다.

(2) $A=B=1$ 인 경우 : $x^2 + x = C$ 이다. 이러한 방정식은 $\mathbb{F}_{2^n}$ 에서 해를 가질 수도 있고 그렇지 않을 수도 있다. 또한 해를 갖는 경우와 해를 갖지 않는 경우에 대해 알아본다.

① $\mathbb{F}_{2^n}$ 에서 해를 갖는 경우 : 해가 $\alpha \in \mathbb{F}_{2^n}$ 이라 하자. 그러면 $\alpha^2 + \alpha = C$ 이다. $Tr_1^n(\alpha^2) = Tr_1^n(\alpha)$ 이므로 $Tr_1^n(C) = Tr_1^n(\alpha^2 + \alpha) = Tr_1^n(\alpha^2) + Tr_1^n(\alpha) = 0$ 이다.

② $\mathbb{F}_{2^n}$ 에서 해를 갖지 않는 경우 : $\mathbb{F}_{2^{2n}}$ 에서 해를 가지므로 그 해를 $\beta \in \mathbb{F}_{2^{2n}}$ 이라 하자. 그러면 $\beta^2 + \beta = C$ 이다. 따라서

$$\begin{aligned} Tr_1^n(C) &= C + C^2 + C^3 + \dots + C^{2^{n-1}} \\ &= (\beta^2 + \beta) + (\beta^2 + \beta)^2 + (\beta^2 + \beta)^3 + \dots + (\beta^2 + \beta)^{2^{n-1}} \\ &= (\beta + \beta^2) + (\beta^2 + \beta^2^2) + (\beta^3 + \beta^2^3) + \dots + (\beta^{2^{n-1}} + \beta^{2^n}) \\ &= \beta + \beta^{2^n} \end{aligned} \quad (2.3)$$

이다.

만일 $\beta \in \mathbb{F}_{2^n}$ 이면 $\beta^{2^n} = \beta$ 이므로 식 (2.4)에서 $Tr_1^n(C) = 0$ 이다. 그러므로 다음 정리를 얻는다.

2차방정식 $x^2 + x + C = 0$ 가 $\mathbb{F}_{2^n}$ 에서 해를 가질 필요충분조건은 $Tr_1^n(C) = 0$ 이다.

<보조정리 2.2.1> $\lambda, C \in \mathbb{F}_{2^n}$ 에 대하여 β 가

$$\beta := C\lambda^2 + (C+C^2)\lambda^{2^2} + \dots + (C+C^2+\dots+C^{2^{n-2}})\lambda^{2^{n-1}} \quad (2.4)$$

를 만족한다면

$$\beta - \beta^2 = C(Tr_1^n(\lambda) - \lambda) - \lambda(Tr_1^n(C) - C) \quad (2.5)$$

를 만족한다.

(증명) β 의 정의에 의하여

$$\beta^2 = C^2\lambda^{2^2} + (C^2+C^4)\lambda^{2^3} + \dots + (C^2+C^4+\dots+C^{2^{n-1}})\lambda^{2^n} \quad (2.6)$$

이다. 따라서

$$\beta - \beta^2 = C(\lambda^2 + \lambda^4 + \dots + \lambda^{2^{n-1}}) - (C^2 + C^4 + \dots + C^{2^{n-1}})\lambda^{2^n} \quad (2.7)$$

이다. $\lambda \in \mathbb{F}_{2^n}$ 이므로 $\lambda^{2^n} = \lambda$ 이다. 또한,

$$\lambda^2 + \dots + \lambda^{2^{n-1}} = Tr_1^n(\lambda) - \lambda \quad (2.8)$$

이고

$$C^2 + C^{2^2} + \dots + C^{2^{n-1}} = Tr_1^n(C) - C \quad (2.9)$$

이므로 식 (2.8)이 성립한다. □

(참조) (보조정리 2.2.1)에서 $Tr_1^n(\lambda) := 1$ 이고 $Tr_1^n(C) := 0$ 라면 식 (2.9)은 $\beta - \beta^2 = C$ 가 된다. 즉 2차방정식 $x^2 + x = C$ 에서 $Tr_1^n(C) = 0$ 이면 해 β 를 가지며 $Tr_1^n(\lambda) = 1$ 인 $\lambda \in \mathbb{F}_{2^n}$ 를 구하여 식 (2.4)에 대입하면 β 를 얻을 수 있다.

<예제 2.2.2> $x^2 + x = \alpha^{10}$, $\mathbb{F}_{2^4} = \mathbb{F}_2(\alpha)(\alpha^4 + \alpha + 1 = 0)$ 는 $Tr_1^4(\alpha^{10}) = 0$ 이므로 해를 갖는다.

$\lambda := \alpha^3$ 이라 하면 $Tr_1^4(\lambda) = 1$ 이다. $C = \alpha^{10}$ 이므로 식 (2.4)에 대입하면

$$\begin{aligned} x &= \alpha^{10}(\alpha^3)^2 + (\alpha^{10} + \alpha^{20})(\alpha^3)^4 + (\alpha^{10} + \alpha^{20} + \alpha^{40})(\alpha^3)^8 \\ &= \alpha^2 \end{aligned}$$

이 된다. 실제로 α^2 을 대입하면 $(\alpha^2)^2 + \alpha^2 = \alpha^4 + \alpha^2 = \alpha^{10}$ 이다.

<예제 2.2.3> α 를 $x^4 + x + 1$ 의 원시근일 때 $x^4 + x = \alpha^{10}$ 의 해를 구하면 $Tr_1^4(\alpha^3) = 1$ 이므로 해를 갖지 않는다.

2차방정식 $x^2 + x = C$ 가 $\mathbb{F}_{2^4}$ 에서 해를 갖지 않는 경우는 $Tr_1^4(C) = 1$ 임을 뜻한다. 그러나 $Tr_1^4(C) = Tr_1^4(C^2) = Tr_1^4(C^4)$ 이므로

$$Tr_1^8(C) = Tr_1^4(Tr_4^8(C)) = Tr_1^4(C+C^4) = Tr_1^4(C) + Tr_1^4(C^4) = 0$$

가 되어 $\mathbb{F}_{2^8}$ 에서 해를 갖는다.

또한 일반적인 경우 즉, $Ax^2+Bx+C=0$ 에서 $A \neq 0, B \neq 0$ 에 대하여 $y:=AB^{-1}x$, $\gamma:=ACB^{-2}$ 라 두면 $x=A^{-1}By$, $C=\gamma A^{-1}B^2$ 이므로 $y^2+y=\gamma$ 가 되어 방정식의 해를 구할 수 있다.



2.3 의사난수열(PN:Pseudo Noise sequences)의 기본성질 및 구조 [8,9,14]

2.3.1. 상관관계(Correlation)

상관관계 [5,9]란 두 수열 사이의 유사성, 즉 관련성에 대한 척도이다. 적절하게 표준화한 상관척도를 $R_a(\tau)$ 라 두면

$$-1 \leq R_a(\tau) \leq +1$$

을 갖는다.

상관관계 함숫값이 (+1)이면 두 수열은 같고, 반대로 (-1)이면 두 수열이 정반대이며, 상관관계 값이 0이면 두 수열의 상관관계가 없음을 뜻한다. 즉, 정확하게 반이 같고 반은 다르다는 것을 뜻한다.

(1) 자기상관관계(Auto-correlation)

주기가 $2^n - 1$ 이며, t 가 0에서 $2^n - 2$ 까지 변할 때 0 또는 1의 값을 가지는 이진수열 $s(t)$ 의 주기적 상관관계 함수 $R_a(\tau)$ 를 $\tau = 0, 1, 2, \dots, 2^n - 2$ 에 대하여 다음과 같이 정의 한다.

$$R_a(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s(t+\tau)+s(t)} \quad (2.10)$$

이때 이상적인 상관관계 함수를 갖는 PN수열의 주기적 상관관계 함수 $R_a(\tau)$ 는 다음을 만족한다.

$$R_a(\tau) = \begin{cases} 2^n - 1, & \text{if } \tau = 0 \bmod (2^n - 1) \\ -1, & \text{otherwise} \end{cases} \quad (2.11)$$

(2) 상호상관관계(Cross-correlation)

주기가 각각 $2^n - 1$ 인 이진수열의 $s_a(t)$ 와 $s_b(t)$ 의 주기적 상관관계 함수 $R_{ab}(\tau)$ 를 $\tau = 0, 1, 2, \dots, 2^n - 2$ 에 대해 다음과 같이 정의 한다.

$$R_{ab}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_b(t+\tau) + s_a(t)} \quad (2.12)$$

2.3.2. 선형복잡도(Linear span)

PN수열은 선형복잡도 성질을 가지며, 이러한 수열은 몇 개의 이전 값들의 선형결합에 의해 표현 된다.

$$s(t) = \sum_{a=1}^{2^n-1} \alpha_a \cdot s(t-1) \quad (2.13)$$

여기서 α_a 는 0 또는 1의 값을 갖는 계수이며, 식 (2.13)에서 $2^n - 1$ 을 PN수열의 선형복잡도라 정의하며, PN수열의 복잡성, 및 또다른 사용자에게 의한 복원가능성의 척도라 할 수 있다. 선형복잡도가 클수록 안전성 및 보안성이 우수한 PN수열이라 할 수 있다.

$2^n - 1$ 개의 이전 값에 의해서 정해진 값으로 식 (2.13)에서 계수 α_a 를 알면 수열을 발생시킬 수 있으며, $2^n - 1$ 의 값이 크면 클수록 또다른 사용자가 정상 경로가 아닌 불법적인 접근의 침입을 막을 수 있으므로 계수 α_a 를 찾는 것은 어렵다.

2.3.3. 균형성질(Balance property)

PN수열은 한 주기 내에서 1과 0의 개수 차로써 정의된다. 이러한 차가 1보다 작거나 같은 관계를 만족하면, 다음식과 같이 나타낼 수 있다.

$$\left| \sum_{t=0}^{2^n-2} (-1)^{s(t)} \right| \leq 1 \quad (2.14)$$

이때 수열 $s(t)$ 는 균형성질 [7]을 갖는다고 하며, m -수열의 경우 1의 개수가 0의 개수보다 하나 더 많다.

<예제 2.3.1> x^3+x+1 은 0010111일 때 1의 개수는 4, 0의 개수는 3이고 x^4+x+1 은 000100110101111일 때 1의 개수는 8, 0의 개수는 7이며, x^5+x^2+1 은 0000100101100111110001101110101일 때 1의 개수는 16, 0의 개수는 15이다. 그러므로 m -수열의 경우 1과 0의 개수 차이는 1이다.

2.3.4. Run 분포성질(Run property)

생성다항식 $f(x)=x^5+x^2+1$ 에 의해서 생성된 PN수열 0000100101100111110001101110101...에서 0가 연이어 4개인 run을 길이가 4인 0-run이라 하며, 중간에 11111과 같이 연이어 1이 5개인 run을 길이가 5인 1-run이라 한다. 길이가 2^m-1 인 m -수열의 run 분포는 다음과 같다.

<표 2.1 Run 분포성질>

길이	0-run	1-run
1	2^{m-3}	2^{m-3}
2	2^{m-4}	2^{m-4}
$\vdots$	$\vdots$	$\vdots$
r	2^{m-r-2}	2^{m-r-2}
$\vdots$	$\vdots$	$\vdots$
$m-2$	1	1
$m-1$	1	0
m	0	1
합계	2^{m-2}	2^{m-2}

주기가 $31 = 2^5 - 1$ 이며, 특성다항식 $x^5 + x^2 + 1$ 인 Run 분포도는 아래와 같다.

<표 2.2 $x^5 + x^2 + 1$ 분포성질>

길이	0-run	1-run
1	4	4
2	2	2
3	1	1
4	1	0
5	0	1
합계	2^3	2^3

m -수열 이러한 스펙성질과 Run 분포도 성질을 동시에 만족하며 PN수열 중에서 유일하다.

2.3.5. PN수열들의 데시메이션(Decimation)

생성다항식이 $f(x)$ 인 m -수열 $\mathbf{s}$ 에서 τ 칸씩 건너 뛴 것을 데시메이션이라 하며, 이렇게 만든 수열을 $\mathbf{s}[\tau]$ 라 쓰기로 한다. $\mathbf{s}[\tau] = (000000\cdots)$ 이 아닌 $\mathbf{s}[\tau]$ 의 주기는 $\frac{2^m - 1}{\gcd(2^m - 1, \tau)}$ 이며, $\mathbf{s}[\tau]$ 의 생성다항식은 $f(x^\tau)$ 이다.

<예제 2.3.2> $s=(000100110101111\cdots)$ 라 하면 생성다항식은

$$x^4+x+1=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(:=f(\alpha))(\alpha^4=\alpha+1)$$

이다.

$s[5]=(000000000000000\cdots)$, $s[2]=(000100110101111\cdots)$, $s[3]=(0111101111\cdots)$

$s[7]=(011110101100100\cdots)$ 이 된다. $s[7]$ 의 생성다항식은 $f(\alpha^7)=x^4+x^3+1$ 이다.

$s[3]$ 의 생성다항식은 $f(\alpha^3)=x^4+x^3+x^2+x+1$ 이다. $s[2]$ 의 생성다항식은 $f(\alpha^2)=x^4+x+1$ 이다.



2.4 부호분할 다중접속(CDMA:Code Division Multiple Access)

CDMA방식은 주파수를 많은 사용자가 사용할 수 있는 한 방법으로서 디지털 신호의 크기가 연속적인 값을 가지지 않고 '0'과 '1'만 가지는 신호이며, 이러한 디지털 신호는 '0'과 '1'만 구별하면 된다. 이러한 방식은 신호 전송시 잡음에 강한 특성을 보인다. 디지털 신호 여러 개를 동시에 전송하는 대표적인 방법이 CDMA 통신 방식이다.

여러 사용자가 동일한 주파수를 동시에 사용하는 CDMA 통신 시스템은 송신자의 통화에 대하여 특별한 확산코드를 더하여 주파수 대역폭을 넓혀서 송신한다. 이 때 수신측은 송신측에서 부여한 것과 동일한 코드에 의해 전송되는 많은 통신량 중에서 자기에게 전송되는 신호를 구별해 낸다. 사용하는 확산코드는 보내려는 정보와 독립적인 코드신호에 의해 이루어져야 하며, 수신측에서는 송신측에서 정보를 확산시킨 코드신호와 동기가 맞추어진 신호의 상관관계에 의해 확산되어진 정보를 복원하게 된다. 그러므로 확산코드 신호의 변조 및 복조에 관여하고 있는 상관관계는 통신에 아주 중요한 역할을 담당한다.

2.5 Welch의 lower bound

Welch[16]에 의해서 유도된 최대 상관관계 함숫값에 대한 lower bound는 의사난수열의 상관관계 성질을 평가하는데 이용되며, 주기가 $2^n - 1$ 인 A 개의 의사난수열군에 대해서 최대 자기상관관계 함숫값 K_a 와 최대 상호상관관계 함숫값 K_c 는 각각 다음과 같이 정의된다.

$$K_a = \max_i \max_{\tau=1}^{2^n-2} |C_i(\tau)| \quad (2.15)$$

$$K_c = \max_{i \neq j} \max_{\tau=1}^{2^n-2} |C_{i,j}(\tau)| \quad (2.16)$$

식 (2.15), (2.16)으로 부터 의사난수열의 최대 상관관계 값 $K_{\max}$ 는 다음과 같이 정의 된다.

$$K_{MAX} = MAX(K_a, K_c) \quad (2.17)$$

$K_{\max}$ 값은 Welch의 lower bound에 의해서 다음과 같이 lower bound된다.

$$K_{\max} \geq 2^n - 1 \cdot \sqrt{\frac{A-1}{A \cdot 2^n - 2}} \quad (2.18)$$

주기가 $2^n - 1$ 이고, 의사난수열에서 의사난수열의 개수가 $A \pm 1$ 이고 $n = 2m$ 인 경우, Welch의 bound는 다음과 같이 표현될 수 있다.

$$K_{\max} \geq 2^m + 1 \quad (2.19)$$

3. 기존 이진수열 분석

3.1 이상적인 상관관계 함수를 갖는 이진수열

3.1.1 m -수열

<정의 3.1.1> $n \in \mathbb{N}$, $0 \neq \omega \in GF(2^n)$ ($0 \leq t \leq 2^n - 2$), $\alpha \in GF(2^n)$ 의 원시원소라 할 때

$$S = Tr_1^n(\omega \alpha^t) \quad (3.1)$$

를 m -수열이라 한다.

이상적인 상관관계 함수를 가지며 선형 성질을 갖는 m -수열은 다음과 같은 여러 성질들을 가진다.

(1) The shift property : m -수열의 순환이동(cyclic shift)에 의해 발행한 수열 역시 m -수열이다.

<예제 3.1.2>

m -수열	왼쪽 한 칸 이동	m -수열
0010111...	$\rightarrow$	0101110...

이다.

(2) The Recurrence property [1,2] : m -수열은 식 (3.2)과 같은 선형 점화관계식을 만족한다.

$$s_{a+n} = f_{n-1}s_{a+n-1} + f_{n-2}s_{a+n-2} + \cdots + f_1s_{a+1} + s_a \pmod{2}, f_i \in \{0, 1\} \quad (3.2)$$

5차 m -수열 생성다항식 $x^5 + x^2 + 1$ 은 선형점화식 $s_{a+5} = s_{a+2} + s_a$ 를 만족한다.

(3) The window property : 차수 n 인 원시다항식에 의해 생성된 m -수열에서 m -비트씩 구분하면 $1, 2, \dots, 2^m - 1$ 가 모두 단 한 번씩 나타난다.

<예제 3.1.3> 0010111...를 3비트씩 구분해서 읽으면

001(=1), 010(=2), 101(=5), 011(=3), 111(=7), 110(=6), 100(=4)가 한 번씩 나온다.



<그림 3.1 x^2+x+1 , x^3+x+1 의 window property>

(4) The Addition property : 두 개의 m -수열의 배타적 논리합(XOR) 결과역시 m -수열이다.

<예제 3.1.4>

$$0010111\cdots \oplus 1110010\cdots = 1100101\cdots \text{ 는 } m\text{-수열이다.}$$

(5) The shift and add property : m -수열과 그것의 순환이동의 합은 또다른 m -수열이다. 즉, $(s_t)_{t=0}^n$ 을 길이가 $n = 2^m - 1$ 인 m -수열이라 하고 $\tau \not\equiv 0 \pmod{n}$ 라면, δ ($1 \leq \delta \leq n-1$)이 존재하여 다음 식을 만족한다.

$$s_t + s_{t+\tau} = s_{t+\delta} \quad (t \geq 0) \quad (3.3)$$

<예제 3.1.5> $s=0010111\cdots$ 라 하면

$$\begin{aligned} s_t &= 0010111\cdots \\ s_t + s_{t+\tau} &= 1110010\cdots \\ &= 1100101\cdots \end{aligned} \quad s_t + s_{t+4} = s_{t+5} \text{ 이다.}$$

(6) Thumb and Tack property : 자기상관관계 함숫값은 1 또는 $-\frac{1}{N}$ 이다.

$$\rho(a) := \frac{1}{N} \sum_{b=0}^{N-1} (-1)^{s_{a+b} \oplus s_b} \quad (3.4)$$

$(N = 2^m - 1)$

<예제 3.1.6> 원시다항식 $x^3 + x + 1$ 에 의해 생성된 m -수열 $0010111\cdots$ 대하여

$\begin{matrix} 00 \\ 00 \\ 11 \\ 00 \\ 11 \\ 11 \\ 11 \end{matrix}$	이므로 $\rho(0) = 1$ 이다. 또한	$\begin{matrix} 00 \\ 01 \\ 10 \\ 01 \\ 11 \\ 11 \\ 10 \end{matrix}$
--	--------------------------	--

인 경우는 $\rho(a) = -\frac{1}{7}$ 이다.

(7) Characteristic Phase : m -수열 $\mathbf{s}=(s_a)$ 에 대하여 $(s_{2a})=\mathbf{s}$ 인 m -수열은 단 하나 존재한다. 그러한 m -수열을 Characteristic m -수열이라 한다. 예를 들면 $\mathbf{s}=(10010111\cdots)$ 라 하면 $(s_{2a})=\mathbf{s}$ 이다.

주어진 m -수열을 적당히 이동한 또 다른 m -수열에 대하여 위의 성질이 성립한다. 위의 예제에서 처음 m -수열이 0010111 $\cdots$ 라면 이 수열을 왼쪽으로 2칸 이동한 수열에 대하여 2칸씩 건너뛰면서 수열을 만들면 같은 수열이 된다.

(8) m -수열의 상관관계 함숫값은 식 (2.12)으로 나타낼 수 있으며, 이상적인 자기상관관계 함수를 갖는 수열이다.

3.1.2 GMW-수열

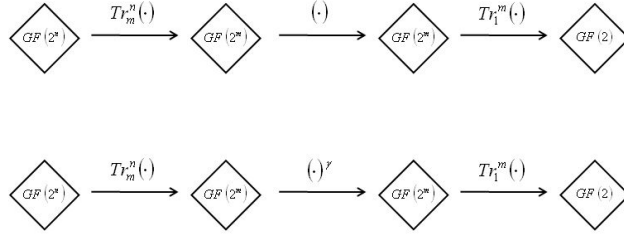
<정의 3.1.7> $m, n \in \mathbb{N}$, $n = km$, $\gcd(r, 2^m - 1) = 1$, $\alpha \in GF(2^n)$ 의 원소라 할 때

$$S := \{s_a(t) | 0 \leq t \leq 2^n - 2, 1 \leq a \leq 2^m\} \quad (3.5)$$

$$s_a(t) = Tr_1^m \{ [Tr_m^n(\alpha^t)]^r \}$$

GMW-수열이라 한다.

여기서 트레이스 함수 성질 (6)를 이용하면 매개변수 $r=1$ 일 때, m -수열이 된다. GMW-수열의 상관관계 함수는 식 (2.12)으로부터 이상적인 상호상관관계 함수를 갖는다.



<그림 3.2 m -수열과 GMW-수열 관계>

<예제 3.1.8> $n = 4, m = 2, \alpha \in GF(2^4), \alpha^4 = \alpha + 1$ 이고, $\gcd(r, 2^m - 1) = 1$ 이므로 $r = 2$ 일 때

$$\begin{aligned}
 [Tr_1^4(\alpha^t)]^2 &= Tr_1^4(\alpha^{2t}) = \alpha^{2t} + (\alpha^{2t})^2 + (\alpha^{2t})^4 + (\alpha^{2t})^8 \\
 &= \alpha^{2t} + \alpha^{4t} + \alpha^{8t} + \alpha^t \\
 &= \alpha^t + \alpha^{2t} + \alpha^{4t} + \alpha^{8t}
 \end{aligned}$$

그러므로 $[Tr_1^4(\alpha)]^2 = \alpha + \alpha^2 + \alpha^4 + \alpha^8 = 0$ 이다. 같은 방법으로

$$\begin{aligned}
 [Tr_1^4(\alpha^2)]^2 &= 0, & [Tr_1^4(\alpha^3)]^2 &= 1, & [Tr_1^4(\alpha^4)]^2 &= 0, & [Tr_1^4(\alpha^5)]^2 &= 0, & [Tr_1^4(\alpha^6)]^2 &= 1, \\
 [Tr_1^4(\alpha^7)]^2 &= 1, & [Tr_1^4(\alpha^8)]^2 &= 0, & [Tr_1^4(\alpha^9)]^2 &= 1, & [Tr_1^4(\alpha^{10})]^2 &= 0, & [Tr_1^4(\alpha^{11})]^2 &= 1, \\
 [Tr_1^4(\alpha^{12})]^2 &= 1, & [Tr_1^4(\alpha^{13})]^2 &= 1, & [Tr_1^4(\alpha^{14})]^2 &= 1, & [Tr_1^4(\alpha^{15})]^2 &= 0
 \end{aligned}$$

이렇게 하여 얻어진 수열은 000100110101111...이다.

3.2 3개의 상관관계 함수를 갖는 기존 이진수열

3.2.1 Kasami-수열

<정의 3.2.1> $m, n \in \mathbb{N}$, $n = 2m$, $\alpha \in GF(2^n)$, $\gamma_a \in GF(2^m)$ 이고, $\beta = \alpha^Q$,

$Q = 2^m + 1$ 일 때

$$S := \{s_a(t) | 0 \leq t \leq 2^n - 2, 1 \leq a \leq 2^m\} \quad (3.6)$$

$$s_a(t) = Tr_1^m \{ [Tr_m^n(\alpha^{2t}) + \gamma_a \beta^t] \}$$

Kasami-수열이라 한다.

Kasami-수열에는 다음과 같이 큰 · 작은 집합으로 분류한다.

(1) Kasami-수열들의 작은 집합

- Decimation 수열 $\mathbf{y} := \mathbf{x}[s(m)]$, $s(m) := 2^{m/2} + 1$
- $\mathbf{y}$: 주기가 $N = \frac{2^m - 1}{s(m)} = 2^{m/2} - 1$ 인 m 수열
- Kasami-수열들의 작은 집합은 다음과 같다.

$$S := \{\mathbf{x}, \mathbf{x} \oplus \mathbf{y}, \mathbf{x} \oplus T^{-1}\mathbf{y}, \mathbf{x} \oplus T^{-2}\mathbf{y}, \dots, \mathbf{x} \oplus T^{-(2^{m/2}-2)}\mathbf{y}\} \quad (3.7)$$

여기서 $T^{-1}\mathbf{y} = (y_1, y_2, \dots, y_{N-1}, y_0)$ 는 $\mathbf{y}$ 의 왼쪽으로 순환이동(cyclic shift)이다.

- 두 개의 Kasami-수열의 상관관계 함수 $R(\tau) \in \{-1, -s(m), s(m)-2\}$ 이다.
- 이 집합의 원소의 개수는 $2^{m/2}$ 이다.

<예제 3.2.2> $m = 4$ 에 대한 Kasami-수열의 원시다항식 $x^4 + x + 1$ 이며,

$\{x_a\} = 100010011010111\cdots$ $s(m) = 2^{m/2} + 1 = 5$ 이고, $\{y_a\} = \{x_{5a}\} = 101101101101101\cdots$ 를 얻는다. $\{y_i\}$ 의 주기가 $2^{m/2} - 1 = 3$ 인 m -수열이다.

다음과 같이 Kasami-수열들의 개수는 $2^{m/2} = 4$ 주기가 15인 Kasami-수열

100010011010111
001111111110011
111001000001100
010100101100001

이다.

(2) <Kasami-수열들의 큰 집합>

- 주기가 $2^m - 1$ 인 수열을 포함하고, Gold-수열 및 부분집합으로 Kasami-수열들의 작은 집합을 포함한다.
- m -수열 x 의 $2^{m/2} + 1$ 과 $2^{(m+2)/2} + 1$ 의 Decimation에 의해서 얻어진 수열들을 각각 y 와 z 라 하면 y 와 z 의 다른 이동차들에 의해서 얻어진 수열들을 x, y 그리고 z 에 더해서 얻어진 모든 수열들이 모임이다.

Kasami-수열의 상관관계 함수 $R(\tau) \in \{-2^m - 1, -1, 2^m - 1\}$ 이다.

3.2.2 No-수열

<정의 3.2.3> $m, n \in \mathbb{N}$, $n = 2m$, $\gcd(r, 2^m - 1) = 1$, $\alpha \in GF(2^n)$, $\gamma_a \in GF(2^m)$ 이고, $\beta = \alpha^Q$, $Q = 2^m + 1$ 일 때

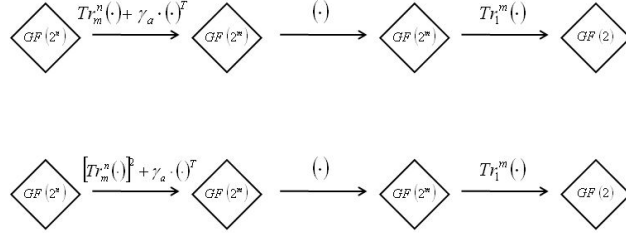
$$S := \{s_a(t) \mid 0 \leq t \leq 2^n - 2, 1 \leq a \leq 2^m\} \quad (3.8)$$

$$s_a(t) = Tr_1^m \{ [Tr_m^n(\alpha^{2t}) + \gamma_a \alpha^{T \cdot t}]^r \}$$

No-수열이라 한다.

No-수열의 상관관계 함수 $R(\tau) \in \{-2^m - 1, -1, 2^m - 1\}$ 이다. 식 (3.8)에서

매개변수 $r=1$ 일 때, Kasami-수열이 된다.



<그림 3.3 Kasami-수열과 No-수열 관계>

다음 그림 (3.4)은 m -수열, GMW-수열, Kasami-수열, No-수열의 관계도이다.



<그림 3.4 기존 이진수열의 관계도>

<예제 3.2.4> $n=4, m=2, Q=5, r=2, \gcd(r, 2^m-1)=1$ 일 때

$S = \{s_1(0), s_1(1), \dots, s_1(14), s_2(0), s_2(1), \dots, s_2(14), \dots, s_4(0), s_4(1), \dots, s_4(14)\}$ 이다.

$s_a(t) = Tr_1^2\{[Tr_2^4(\alpha^{2^t}) + \gamma_a \alpha^{Q \cdot t}]^2\}$ 이며, $\gamma_a \in GF(2^2) = \{0, 1, \beta, \beta^2\}$ 일 때 $\alpha^4 = \alpha + 1, \beta^2 = \beta + 1$ 라 둔다.

i) $\gamma_1 := 0$ 일 때

$$s_1(t) = Tr_1^2\{[Tr_2^4(\alpha^{2t})]^2\} = \alpha^t + \alpha^{2t} + \alpha^{4t} + \alpha^{8t} \text{ 이 된다.}$$

수열 001001101011110을 얻는다. 수열 $s_a(t)$ 의 최소다항식은 $x^4 + x + 1$ 이다.

ii) $\gamma_2 := 1$ 일 때

$$s_2(t) = Tr_1^2\{[Tr_2^4(\alpha^{2t}) + \alpha^{5 \cdot t}]^2\} = \alpha^t + \alpha^{2t} + \alpha^{4t} + \alpha^{8t} + \alpha^{5t} + \alpha^{10t} \text{ 이다.}$$

수열 111111011101000을 얻는다.

iii) $\gamma_3 := \beta(= \alpha^5)$ 일 때

$$s_3(t) = Tr_1^2\{[Tr_2^4(\alpha^{2t}) + \beta\alpha^{5 \cdot t}]^2\} = \alpha^t + \alpha^{2t} + \alpha^{4t} + \alpha^{8t} + \beta^2\alpha^{10t} + \beta\alpha^{5t} \text{ 이다.}$$

수열 010010110000101을 얻는다.

iv) $\gamma_4 := \beta^2$ 일 때

$$s_4(t) = Tr_1^2\{[Tr_2^4(\alpha^{2t}) + \beta^2\alpha^{5 \cdot t}]^2\} = \alpha^t + \alpha^{2t} + \alpha^{4t} + \alpha^{8t} + \beta\alpha^{10t} + \beta^2\alpha^{5t} \text{ 이다.}$$

수열 100100000110011을 얻는다.

<표 3.1 $\alpha^4 + \alpha + 1$ 생성된 수열>

a	$s_1(t)$	$s_2(t)$	$s_3(t)$	$s_4(t)$
0	0	0	1	1
1	0	1	1	0
2	0	1	0	1
3	1	1	0	0
4	0	1	1	0
5	0	1	0	1
6	1	1	0	0
7	1	0	0	1
8	0	1	0	1
9	1	1	0	0
10	0	1	1	0
11	1	0	1	0
12	1	1	0	0
13	1	0	0	1
14	1	0	1	0

$1 \leq a, b \leq 2^m$ 에 대하여 $R_{a,b}(\tau)$ 을 S 의 a 번째 수열과 b 번째 수열에 연관된 상관관계 함수는 임의의 $a, b, \tau (1 \leq a, b \leq 2^m, 0 \leq \tau \leq 2^n - 2)$ 에 대하여 $a \neq b$ 이거나 $\tau \neq 0$ 이면

$$R_{a,b}(\tau) \in \{-2^m - 1, -1, 2^m - 1\}$$

이다.

3.3 5개의 상관관계 함수를 갖는 기존 이진수열

<정의 3.3.1> $m, n \in \mathbb{N}$, $n = 2m$, $\gcd(r, 2^m - 1) = 1$, α 는 $GF(2^n)$ 의 원시원소이며, $\gamma_a \in GF(2^n)$, $\eta_a \in GF(2^m)$ 이고, $\beta = \alpha^Q$, $Q = 2^m + 1$ 이라 할 때

$$S := \{s_{a,b}(t) \mid 0 \leq t \leq 2^n - 2, 1 \leq a \leq 2^n, 1 \leq b \leq 2^m\} \quad (3.9)$$

$$s_{a,b}(t) = Tr_1^m \left\{ \left[Tr_m^n \left(\alpha^{2t} + \gamma_a \alpha^{(3 \cdot 2^m - 1)t} \right) + \gamma_b \alpha^{(2^m + 1)t} \right]^r \right\}$$

을 Zeng등이 제안한 5개의 상관관계 함수를 갖는 이진수열이라 한다.

Zeng등이 제안한 수열의 상관관계 함수 $R(\tau) \in \{-2^m - 1, -1, 2^m - 1, 2 \cdot 2^m - 1, 3 \cdot 2^m - 1\}$ 이다.

식 (3.9)에서 매개변수 $\gamma_a = 0$ 일 때, $s_{a,b}(t) = Tr_1^m \left\{ \left[Tr_m^n (\alpha^{2t}) + \gamma_b \alpha^{(2^m + 1)t} \right]^r \right\}$ 이므로 No-수열이 된다.

<예제 3.3.2> $n = 6$, $m = 3$, $Q = 9$, $\beta = \alpha^9$, $r := 3$ 일 때, $\gcd(r, 2^m - 1) = 1$ 이므로

$$s_{63,2} = (010111011 \cdots 111010111) \quad s_{43,7} = (010010001 \cdots 110001111)$$

$s_{63,2}$ 와 $s_{43,7}$ 의 7×9 배열을 다음과 같이 둔다.

$$A(s_{a,b}) = \begin{bmatrix} 010111011 \\ 010010001 \\ 101101100 \\ 000101010 \\ 111111101 \\ 101000110 \\ 111010111 \end{bmatrix} \quad A(s_{a,d}) = \begin{bmatrix} 010010001 \\ 010010111 \\ 100011110 \\ 000000110 \\ 110001001 \\ 100011000 \\ 110001111 \end{bmatrix}$$

따라서 두 수열의 상관관계 함수값은 $\{-9, -1, 7, 15, 23\}$ 이다.

$$R_{(63,2)(43,7)}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_{63,2}(t+\tau) + s_{43,7}(t)} \in \{-9, -1, 7, 15, 23\}$$

<표 3.2 수열 $s_{63,2}$, 수열 $s_{43,7}$ 의 상관관계 함수>

7	-9	-1	-1	-1	7	-1	-1	-9
7	-1	-9	7	-1	-9	7	-1	-1
-1	-9	15	-1	-1	-1	7	-1	15
-1	-1	-1	-9	-1	-9	-9	-9	-9
-1	7	-9	-1	-1	23	7	7	7
-9	7	-1	-9	-1	-9	-9	-1	-9
-9	-1	-1	7	-1	-9	-9	-1	-1

<표 3.3 기존 이진수열의 특성>

수열군	주기	n	수열군 크기
m	$2^n - 1$	m	$\cdot$
GMW	$2^n - 1$	km	$2^{(n+1)/2} + 1$
Kasami (small set)	$2^n - 1$	$2m$	$2^{n/2} + 1$
Kasami (large set)	$2^n - 1$	$2m$	$2^{(n+1)/2} + 1$
No	$2^n - 1$	$2m$	$2^{n/2} + 1$
Zeng	$2^n - 1$	$2m$	$\cdot$

4. 확장 Zeng 수열군의 생성 및 분석

이 장에서 Zeng[5]이 제안한 수열에 대한 수열군의 크기가 크고 선형복잡도가 높은 확장 Zeng 수열군을 제안하고, 그 상관관계 함수를 분석한다.

주기가 $2^n - 1$ 인 이진수열의 상관관계 함수 $R_{ij}(\tau)$ 는 이동량 τ 에 대하여 두 수열 $s_i(t + \tau)$ 와 $s_j(t)$ 에 대하여 식 (2.12)과 같다.

<정의 4.1> $n = 2m$ ($m \in \mathbb{N}$, $m > 1$)이고, $Q = 2^m + 1$, $u - v = 2$ ($u \geq 0$, $v \geq 0$)이다.

α 는 $GF(2^n)$ 의 원시원소이고, β 는 $GF(2^m)$ 의 원시원소이면 $\beta := \alpha^Q$ 이다.
 $\gcd(r, 2^m - 1) = 1$ 이고, $0 \leq t \leq 2^n - 2$ 이다. γ_i ($\gamma_1 = 0, \gamma_2 = 1, \gamma_a = \alpha^{a-2}$ ($a = 3, 4, \dots, 2^n - 2$))
 는 $GF(2^n)$ 원소이고, η_j ($\eta_1 = 0, \eta_2 = 1, \eta_b = \beta^{b-2}$ ($b = 3, 4, \dots, 2^m - 2$))는 $GF(2^m)$ 원소를 만족
 할때

$$S = \{s_{ij}(t) : 0 \leq i \leq 2^n - 2, 0 \leq j \leq 2^m - 2, 0 \leq t \leq 2^n - 2\} \quad (4.1)$$

$$s_{ij}(t) = Tr_1^m \left\{ \left[Tr_m^n \left(\alpha^{2t} + \gamma_i \alpha^{(2^m \cdot u - v)t} \right) + \eta_j \beta^t \right]^r \right\} \quad (4.2)$$

이다.

제안한 확장 이진수열군은 $\gamma_i = 0$ 이고 $\eta_j = 0$ 이며 $r = 1$ 이면 수열군 S 는 m -수열들의 모임이며, $\gamma_i = 0$ 이고 $\eta_j = 0$ 이면 수열군 S 는 GMW-수열들의 모임이다. $\gamma_i = 0$ 이고 $\eta_j \neq 0$ 이며 $r = 1$ 이면 수열군 S 는 Kasami-수열들의 모임이며, $\gamma_i = 0$ 이고 $\eta_j \neq 0$ 이면 수열군 S 는 No-수열들의 모임이다. 또한 $u = 3$, $v = 1$ 일 때 Zeng등이 정의한 수열들의 모임이다. 따라서 수열군 S 는 m -수열, GMW-수열, Kasami-수열, No-수열, Zeng-수열 등을 포함하는 수열군이다. 표 (4.1)은 매개변수들의 변화에 따른 수열들의 모임을 정리한 것이다.

<표 4.1 매개변수 변화에 따른 수열들의 모임>

새로운 이진수열모임	$s_{ij}(t) = Tr_1^m \left\{ \left[Tr_m^n (\alpha^{2t} + \gamma_i \alpha^{(2^m \cdot u - v)t}) + \eta_j \beta^t \right]^r \right\}$	
m -sequences	$r := 1, \gamma_i := 0, \eta_j := 0$	$m(t) = Tr_1^n (\alpha^{2t})$
GMW-sequences	$\gamma_i := 0, \eta_j := 0$	$g(t) = Tr_1^m \left\{ \left[Tr_m^n (\alpha^{2t}) \right]^r \right\}$
Kasami-sequences	$r := 1, \gamma_i := 0, \eta_j := \neq 0$	$k(t) = Tr_1^m \left\{ \left[Tr_m^n (\alpha^{2t}) + \eta_j \beta^t \right]^r \right\}$
No-sequences	$\gamma_i := 0, \eta_j := \neq 0$	$n(t) = Tr_1^m \left\{ \left[Tr_m^n (\alpha^{2t}) + \eta_j \beta^t \right]^r \right\}$
Zeng-sequences	$u := 3, v := 1$	$z(t) = Tr_1^m \left\{ \left[Tr_m^n (\alpha^{2t} + \gamma_i \alpha^{(3 \cdot 2^m - 1)t}) + \eta_j \beta^t \right]^r \right\}$

다음 정리는 주기가 $2^n - 1$ 인 수열 $s_{ij}(t)$ 의 상호상관관계를 주기가 $2^m - 1$ 인 수열 $2^m + 1$ 개로 나누어 수열 $s_{ij}(t)$ 를 $(2^m - 1) \times (2^m + 1)$ 배열로 나타낸 것이며, 매개변수 $t = Q \cdot t_1 + t_2$ ($0 \leq t_1 < 2^m - 1, 0 \leq t_2 < 2^m + 1$)로 둔다.

<보조정리 4.2 [13]> 임의의 $\delta x \in GF(2^n)$ 에 대하여

$$\sum_{x \in GF(2^n)} (-1)^{Tr(\delta x)} = \begin{cases} 0, & \delta \neq 0 \\ 2^n, & \delta = 0 \end{cases} \quad (4.3)$$

(증명)

(i) $\delta = 0$ 일 때 자명하다.

(ii) $\delta \neq 0$ 일 때 $\delta x \in GF(2^n)$ 이고 $GF(2^n)$ 에서 정확하게 한 번씩 나온다. 그러므로

$$\sum_{x \in GF(2^n)} (-1)^{Tr(\delta x)} = \sum_{x \in GF(2^n)} (-1)^{Tr(x)}$$

$x \in GF(2^n)$ 가 될 필요충분조건은 $x + x^{2^n} = 0$ 이고

$$x+x^{2^n}=(x+x^2+x^{2^2}+\cdots+x^{2^{n-1}})(1+x+x^2+x^{2^2}+\cdots+x^{2^{n-1}}) \quad (4.4)$$

$$=Tr(x)\{1+Tr(x)\}=0$$

식 (4.4)에서 $Tr(x)=0$ 또는 $Tr(x)=1$ 이며

$$x+x^2+x^{2^2}+\cdots+x^{2^{n-1}}=0, \quad x+x^2+x^{2^2}+\cdots+x^{2^{n-1}}=1$$

이며, 각각의 해의 최대 개수는 2^{n-1} 이다. $x^{2^n}+x$ 의 다항식의 차수가 2^n 차
이므로 해의 개수는 2^n 개 이다. 따라서 각각의 해의 개수는 2^{n-1} 이다.
그러므로

$$\sum_{x \in GF(2^n)} (-1)^{Tr(x)} = 0$$

이다. □

<보조정리 4.3> $\alpha \in GF(2^n), \beta \in GF(2^m)$ 각각의 원시원소이며, $\beta := \alpha^Q$,
 $Q = 2^m + 1$ 일 때 $\alpha^{Q^2} = \beta^Q = \beta^{2^m} \cdot \beta = \beta^2$ 이다.

(증명)

$$\alpha^{(2^m \cdot u - v)Q} = \beta^{2^m \cdot u - v} \quad (4.5)$$

$$= (\beta^{2^m})^u \cdot \beta^{-v}$$

$$= \beta^{u - v}$$

$$= \beta^2$$

□

다음 식은 (보조정리 4.4)을 이용하여 $s_{ij}(t)$ 를 나타내면 다음과 같다.

$$\begin{aligned}
 s_{ij}(t) &= Tr_m^n(\alpha^{2t} + \gamma_i \alpha^{(2^m \cdot u - v)t}) + \eta_j \beta^t \\
 &= Tr_m^n(\alpha^{2(t_1 Q + t_2)} + \gamma_i \alpha^{(2^m \cdot u - v)(t_1 \cdot Q + t_2)}) + \eta_j \beta^{(t_1 \cdot Q + t_2)} \\
 &= \beta^{2t_1} \{ Tr_m^n(\alpha^{2 \cdot t_2} + \gamma_i \alpha^{(2^m \cdot u - v)t_2}) + \eta_j \beta^{t_2} \}
 \end{aligned} \tag{4.6}$$

따라서 두 수열 $s_{ij}(t)$, $s_{pq}(t)$ 와 이동량 τ 에 대하여 상호상관관계 함수 $R_{ij,pq}(\tau)$ 는 (정리4.4)와 같다.

<정리 4.4> 임의의 두 이진수열 $s_{ij}(t)$, $s_{pq}(t) \in S$ 에 대하여

$$R_{ij,pq}(\tau) \in \{-2^m - 1, -1, 2^m - 1, \dots, (u + v - 1)2^m - 1\} \tag{4.7}$$

이다.

(증명) 임의의 τ ($0 \leq \tau \leq 2^n - 2$)에 대하여 두 수열 $s_{ij}(t)$ 와 $s_{pq}(t)$ 의 상관관계 함수

$$R_{ij,pq}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_{ij}(t+\tau) + s_{pq}(t)} \tag{4.8}$$

$$\begin{aligned}
 &s_{ij}(t + \tau) + s_{pq}(t) \\
 &= Tr_1^m \{ \beta^{2^r t_1} f(t_2, \tau) \}
 \end{aligned} \tag{4.9}$$

식 (4.9)에서 새로운 함수 $f(t_2, \tau)$ 를 도입하여 정리하면

$$\begin{aligned} f(t_2, \tau) &= \left[Tr_m^n \left(\alpha^{2(t_2 + \tau)} + \gamma_i \alpha^{(2^m \cdot u - v)(t_2 + \tau)} \right) + \eta_j \beta^{(t_2 + \tau)} \right]^r \\ &\quad - \left[Tr_m^n \left(\alpha^{2t_2} + \gamma_p \alpha^{(2^m \cdot u - v)t_2} \right) + \eta_q \beta^{t_2} \right]^r \end{aligned} \quad (4.10)$$

이다. 식 (4.8)은 다음과 같다.

$$\begin{aligned} R_{ij,pq}(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{s_{ij}(t+\tau) + s_{pq}(t)} \\ &= \sum_{t_2=0}^{Q-1} \sum_{t_1=0}^{2^m-2} (-1)^{Tr_1^m \{ \beta^{2^r t_1} f(t_2, \tau) \}} \\ &= \sum_{t_2=0}^{Q-1} \left(\sum_{x \in GF(2^m)} (-1)^{Tr_1^m \{ \beta^{2^r t_1} \cdot f(t_2, \tau) \}} - 1 \right) \\ &= -Q + 2^m \cdot N(\tau) \end{aligned} \quad (4.11)$$

식 (4.11)에서 수열 $s_{ij}(t)$ 와 $s_{pq}(t)$ 의 상관관계 함수 $R_{ij,pq}(\tau)$ 를 계산하기 방법은

$$N(\tau) := |\{t_2 \mid f(t_2, \tau) = 0, 0 \leq t_2 \leq Q-1\}| \quad (4.12)$$

이다.

$$A := \alpha^{2\tau} - 1, \quad B := \gamma_i \alpha^{(2^m \cdot u - v)\tau} - \gamma_p, \quad C := \eta_j \alpha^{(2^m + 1)\tau} - \eta_q \text{라 하고}$$

$$F(t_2, \tau) := Tr_m^n \left(A \alpha^{2t_2} + B \alpha^{(u2^m - v)t_2} \right) + C \alpha^{(2^m + 1)t_2} \quad (4.13)$$

라 하면 $(r, 2^m - 1) = 1$ 이므로

$$f(t_2, \tau) = 0 \Leftrightarrow F(t_2, \tau) = 0 \quad (4.14)$$

이다. 식 (4.13)에서 α^{t_2} 를 x 로 바꾼 식을 $g(x)$ 라 하면 $x^{(2^m \cdot u - v)2^m} = x^{u - 2^m \cdot v}$
이므로

$$\begin{aligned} g(x) &= T_m^n(Ax^2 + Bx^{(u2^m - v)}) + Cx^Q \\ &= Ax^2 + Bx^{(2^m \cdot u - v)} + A^{2^m}x^{2^{m+1}} + B^{2^m}x^{(2^m \cdot u - v)2^m} + Cx^Q \\ &= Ax^2 + Bx^{(2^m \cdot u - v)} + A^{2^m}x^{2^{m+1}} + B^{2^m}x^{u - 2^m \cdot v} + Cx^Q \\ &= 0 \end{aligned} \quad (4.15)$$

이다. 식 (4.15)에서 $x^{2^m - 1} := y$ 라 하고 양변을 x^2 로 나누어 정리하면

$$A + By^u + A^{2^m}y^2 + B^{2^m}y^{-v} + Cy = 0 \quad (4.16)$$

이다. 방정식 (4.16)의 양변에 y^v 을 곱하면

$$B^{2^m} + Ay^v + Cy^{v+1} + A^{2^m}y^{v+2} + By^{u+v} = 0 \quad (4.17)$$

식 (4.17)를 얻으며, 최대 $u + v$ 개의 근을 갖는 방정식이다. 그러므로 다음 정리를 얻는다. 임의의 $s_{ij}(t), s_{pq}(t) \in S$ 에 대하여

$$R_{ij,pq}(\tau) \in \{-2^m - 1, -1, 2^m - 1, \dots, (u + v - 1)2^m - 1\}$$

이다. □

<예제 4.5> $n=6, m=3$, 다항식 $f(x)=x^6+x+1$ 이라 하면 $Q=9$ 이다.

$u=3, v=1$ 이고, $\beta=\alpha^9$ 이면 $\beta^3=\beta^2+1$ 을 만족한다.

(a) $\gamma_i=\alpha, \eta_j=\beta, \gamma_p=\alpha^2, \eta_q=\beta^2$ 일 때 주기 63인 두 수열은 다음과 같다.

$$s_{ij}(t)=Tr_1^3\{[Tr_3^6(\alpha^{2t}+\alpha^2\cdot\alpha^{23t})+\beta\cdot\beta^t]^3\} \quad s_{pq}(t)=Tr_1^3\{[Tr_3^6(\alpha^{2t}+\alpha^2\cdot\alpha^{23t})+\beta^2\cdot\beta^t]^3\}$$

$s_{ij}(t)$ 와 $s_{pq}(t)$ 의 7×9 배열을 다음과 같이 둔다.

$$\begin{array}{c} s_{ij}(t) \\ \left(\begin{array}{ccccccccc} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{array} \right) \end{array} \quad \begin{array}{c} s_{pq}(t) \\ \left(\begin{array}{ccccccccc} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right) \end{array}$$

두 수열 $s_{ij}(t)$ 와 $s_{pq}(t)$ 상관관계 함수 $R_{ij,pq}(\tau) \in \{-9, -1, 7, 15, 23\}$ 이다.

$$R_{ij,pq}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_{ij}(t+\tau)+s_{pq}(t)} \in \{-9, -1, 7, 15, 23\}$$

<표 4.2 수열 $s_{i,j}(t)$, 수열 $s_{pq}(t)$ 의 상관관계 함수>

-9	-1	-1	15	-9	-1	-9	7	7
7	-9	-1	-1	-1	-1	1	-1	1
-1	1	11	1	-1	-1	-1	-9	-1
-1	-1	7	7	7	7	-1	-9	7
7	-9	-9	-1	15	-1	-1	-9	7
-9	-1	-1	-1	-1	7	-1	7	7
-1	-9	-9	-9	-1	-9	-1	15	23

(b) $\gamma_i = \alpha, \eta_j = \beta, \gamma_p = \alpha^2, \eta_q = \beta^3$ 일 때 주기 63인 두 수열은 다음과 같다.

$$s_{ij}(t) = \text{Tr}_1^3 \{ [\text{Tr}_3^6 (\alpha^{2t} + \alpha^2 \cdot \alpha^{23t}) + \beta \cdot \beta^t]^3 \} \quad s_{pq}(t) = \text{Tr}_1^3 \{ [\text{Tr}_3^6 (\alpha^{2t} + \alpha^2 \cdot \alpha^{23t}) + \beta^3 \cdot \beta^t]^3 \}$$

$s_{ij}(t)$ 와 $s_{pq}(t)$ 를 7×9 배열로 나타내면 다음과 같이 둔다.

$$\begin{array}{c} s_{ij}(t) \\ \left(\begin{array}{ccccccccc} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{array} \right) \end{array} \quad \begin{array}{c} s_{pq}(t) \\ \left(\begin{array}{ccccccccc} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right) \end{array}$$

두 수열 $s_{ij}(t)$ 와 $s_{pq}(t)$ 상관관계 함수 $R_{ij,pq}(\tau) \in \{-9, -1, 7, 15\}$ 이다.

$$R_{ij,pq}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_{ij}(t+\tau) + s_{pq}(t)} \in \{-9, -1, 7, 15\}$$

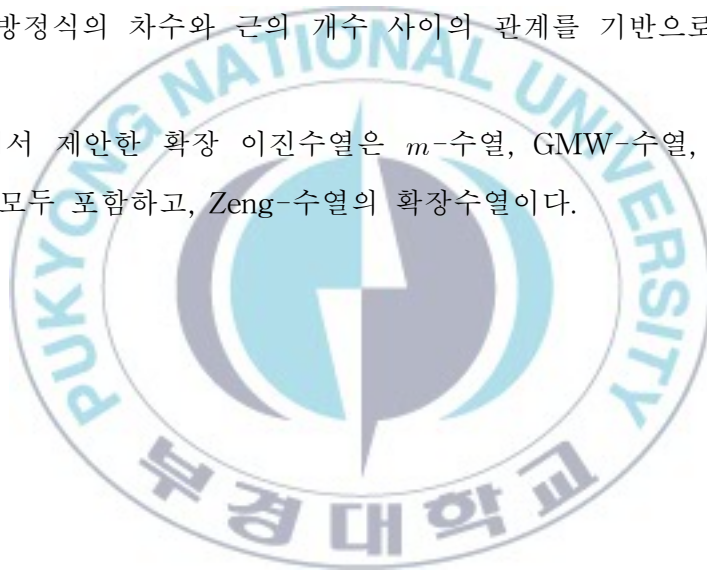
<표 4.3 수열 $s_{i,j}(t)$, 수열 $s_{pq}(t)$ 의 상관관계 함수>

-9	-1	15	7	7	15	7	-9	-1
-1	-1	-1	-9	-9	15	-1	-9	-9
7	-1	-9	-1	7	7	-1	15	7
-1	-1	-1	-1	7	7	-9	-1	-9
-9	7	-1	-9	-9	7	-1	-1	15
7	-1	-1	15	-1	7	-1	-1	-1
-1	-9	-9	-9	-9	-1	-1	-1	-9

5. 결 론

본 논문에서는 Welch의 lower bound 관점에서 적절한 상호상관관계 함수값을 갖는 확장 이진수열군을 제안하고 그 수열의 상호상관관계 함수를 분석했다. 이상적인 상관관계 함수를 갖는 m -수열, GMW-수열, 3개의 상관관계 함수를 갖는 Kasami-수열 및 No-수열에 관한 정의와 성질 그리고 5개의 상관관계 함수를 갖는 Zeng-수열을 소개했다. 또한 수열들의 모임이 응용분야에 대하여 가져야 할 바람직한 사항들은 낮은 상관관계 함수이며, 그러한 상관관계 함수는 방정식의 차수와 근의 개수 사이의 관계를 기반으로 하여 구하였다.

본 논문에서 제안한 확장 이진수열은 m -수열, GMW-수열, Kasami-수열, No-수열을 모두 포함하고, Zeng-수열의 확장수열이다.



참고문헌

- [1] 조성진, “유한체 및 그 응용”, 교우사, 2007.
- [2] 조성진, 김한두, “수론과 암호의 만남”, 교우사, 2009.
- [3] R.A. Games, “Cross correlation of m -sequences and GMW-sequences with the same primitive polynomial”, Discrete Appl. Math, Vol. 12, pp. 139-146, 1985.
- [4] R. Gold, “Optimal binary sequences for spread spectrum multiplexing”, IEEE Trans. Inform. Theory, Vol. IT-13, No. 5, pp. 619-621, 1967.
- [5] R. Gold, “Maximal recursive sequences with 3-valued recursive cross correlation functions”, IEEE Trans. Inform. Theory, Vol. IT-14, No. 1, pp. 154-156, 1968.
- [6] S.W. Golomb, “Shift Register Sequences”, Holden Day, 1967.
- [7] S.W. Golomb, “On the classification of balanced binary sequences of period $2^n - 1$ ”, IEEE trans. Inform. Theory, Vol. IT-26(6), pp. 730-732, 1980.
- [8] S.W. Golomb and G. Gong, “Signal design for good correlation for wireless communication, Cryptography, and Radar”, Cambridge University Press, 2005.
- [9] T. Helleseth and P.V. Kumar, “Sequences with low correlation”, in Handbook of Coding Theory, V.S. Pless and W.C. Huffman, Eds., Amsterdam, The Netherlands: North-Holland, Vol. II, pp. 1765-1853, 1998.
- [10] T. Kasami, “Weight distribution formula for some class of cyclic codes”, Coordinated Science Laboratory, University of Illinois, Urbana,

- Tech. Rep. R-285 (AD632574), 1966.
- [11] R. Lidl and H. Niederreiter, "Finite Fields", Cambridge University Press, 1997.
- [12] R.J. McEliece, "Finite fields for computer scientists and engineers", Kluwer Academic Publishers, 1987.
- [13] Y. Niho "multi-valued cross-correlation functions between two maximal linear recursive sequences", 1972.
- [14] 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. 35, No. 2, pp. 37-379, 1989.
- [15] R.A. Scholtz and L. Welch, "GMW sequences", IEEE Trans. Inform. Theory, Vol. IT-30, No. 3, pp. 548-553, 1984.
- [16] L.R. Welch, "Lower bounds on the maximum cross correlation of signals", IEEE Trans. Inf. Theory, Vol. IT-20, no. 3, pp. 397-399, 1974.
- [17] F. Zeng and Z. Zhang, "Binary sequences with large family size and high linear complexity for spread spectrum communication systems", 2010 2nd Inter. Conf. on Signal Processing Systems (ICSPS), pp. 48-51, 2010.