



## 저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

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

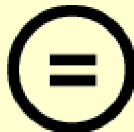
다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 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 박 사 학 위 논 문

낮은 상호상관관계를 갖는  
비선형 이진수열의 생성



2013년 8월

부 경 대 학 교 대 학 원

응 용 수 학 과

권 민 정

이 학 박 사 학 위 논 문

낮은 상호상관관계를 갖는  
비선형 이진수열의 생성

지도교수 조 성 진

이 논문을 이학박사 학위논문으로 제출함.



2013년 8월

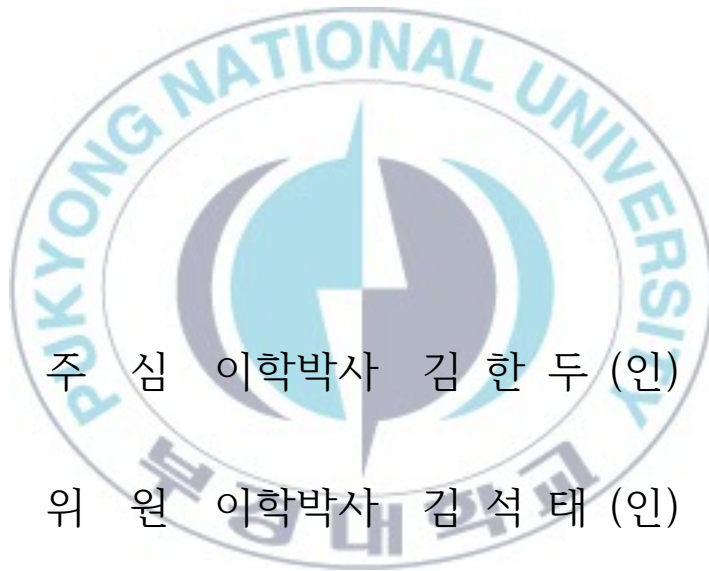
부 경 대 학 교 대 학 원

응 용 수 학 과

권 민 정

권민정의 이학박사 학위논문을 인준함.

2013년 8월 23일



주 심 이학박사 김 한 두 (인)

위 원 이학박사 김 석 태 (인)

위 원 이학박사 표 용 수 (인)

위 원 이학박사 박 진 한 (인)

위 원 이학박사 조 성 진 (인)

## 목 차

|                                                                                                            |     |
|------------------------------------------------------------------------------------------------------------|-----|
| Abstract                                                                                                   | iii |
| 1. 서론                                                                                                      | 1   |
| 2. 배경 지식                                                                                                   |     |
| 2.1. 트레이스 함수                                                                                               | 3   |
| 2.2. 상호상관함수                                                                                                | 4   |
| 2.3. 데시메이션                                                                                                 | 6   |
| 2.4. 선형다항식                                                                                                 | 8   |
| 2.5. 집합 $S$ 의 성질                                                                                           | 11  |
| 2.6. 기존연구                                                                                                  | 12  |
| 3. Niho 타입의 새로운 데시메이션                                                                                      |     |
| 3.1. $d = \frac{2^{m-st}-1}{2^s-1}(2^n + 2^{st+s+1} - 2^{m+st+1} - 1)$                                     | 16  |
| 3.2. $d = \frac{2^{m-1}}{2^s-1}(2^{m(i+1)} - 2^{mi} + 2^{s+1} - 2^m - 1)$                                  | 26  |
| 4. 새로운 수열의 상호상관 함수                                                                                         |     |
| 4.1. 새로운 비선형 이진수열의 생성                                                                                      | 32  |
| 4.2. $d = 2 \cdot 2^m - 1$ 일 때 새로운 수열의 상호상관 함숫값                                                            | 33  |
| 4.3. $d = 2^{m-1}(3 \cdot 2^m - 1)$ 일 때 새로운 수열의 상호상관 함숫값                                                   | 41  |
| 4.4. $\begin{cases} d \equiv 1 \pmod{2^m-1} \\ d \equiv 2^k \pmod{2^m+1} \end{cases}$ 일 때 새로운 수열의 상호상관 함숫값 | 48  |
| 5. 결론                                                                                                      | 67  |
| 참고문헌                                                                                                       | 68  |
| 감사의 글                                                                                                      | 71  |

## 그 립 목 차

|                                                                     |    |
|---------------------------------------------------------------------|----|
| 그림 1. 수열 $u(t) = Tr_1^4(\alpha^t)$ .....                            | 6  |
| 그림 2. 수열 $v(t) = u(17t)$ .....                                      | 6  |
| 그림 3. 수열 $u(t) = Tr_1^8(\alpha^t)$ 의 $15 \times 17$ 배열 .....        | 25 |
| 그림 4. 수열 $v(t) = u(31t)$ 의 $15 \times 17$ 배열 .....                  | 25 |
| 그림 5. 수열 $v(t) = u(227t)$ 의 $15 \times 17$ 배열 .....                 | 31 |
| 그림 6. 수열 $u(201+t)$ 의 $15 \times 17$ 배열 .....                       | 31 |
| 그림 7. $C_{0,\beta^2}(\tau)$ 값의 $15 \times 17$ 배열 .....              | 40 |
| 그림 8. $C_{0,\beta}(\tau)$ , $(0 \leq \tau \leq 2^n - 2)$ 의 배열 ..... | 47 |

## 표 목 차

|                                    |    |
|------------------------------------|----|
| 표 1. $C_{31}(\tau)$ 값의 발생횟수 .....  | 25 |
| 표 2. $C_{0,b}(\tau)$ 값의 발생횟수 ..... | 65 |

# **The Construction of Nonlinear Binary Sequences with Low Cross-correlation**

Min-Jeong Kwon

*Department of Applied Mathematics, The Graduate School,*

*Pukyong National University*

## **Abstract**

Spreading sequence is used for spreading spectrum in CDMA. For the purpose of minimizing multiple access interference and expanding the number of the users, it is desirable to use such sequences with low cross-correlation and high linear span. To make the family size larger and the linear span higher, it is inevitable to raise the cross-correlation function value. In the transmission performance and efficiency, an important problem is to find the spectrum and the number of the occurrences of the cross-correlation function values between two different maximal sequences. In this paper, we propose the new maximal sequences which are obtained by the new decimations  $d = \frac{2^{m-s}-1}{2^s-1}(2^n + 2^{st+s+1} - 2^{m+st+1} - 1)$ ,  $d = \frac{2^{m-1}}{2^s-1}(2^{n(i+1)} - 2^{mi} + 2^{s+1} - 2^m - 1)$  from some maximal sequences. We will also find the spectrum and the number of the occurrences of the cross-correlation function value from the proposed decimations. Also we propose the new family of the sequences using the decimation which satisfies the condition  $d \equiv 1 \pmod{2^m - 1}$ , calculate the cross-correlation spectrum for  $0 \leq t \leq 2^n - 2$  and count the number of the whole value occurring for  $0 \leq \tau \leq 2^n - 2$ . For the decimation  $d = 2 \cdot 2^m - 1$  we count the number of the cross-correlation function value  $C_d(\tau) = 2^m - 1$  occurring for  $0 \leq t \leq 2^n - 2$ , for  $d = 2^{m-1}(3 \cdot 2^m - 1)$  we resolve the number of the cross-correlation function value around  $\tau = Q\tau_1 (0 \leq \tau_1 \leq 2^m - 2)$ . Finally, for the decimation with the condition  $d \equiv 1 \pmod{2^m - 1}$ ,  $d \equiv 2^k \pmod{2^m + 1}$ , we analyze the cross-correlation spectrum and the number of the occurrences for  $0 \leq \tau \leq 2^n - 2$ . The work on this paper can make it easier to count the number of the occurrence of the cross-correlation function value.

## 1. 서론

디지털 이동통신 기술 중 하나인 CDMA(Code Division Multiple Access)는 대역확산 기술을 활용하여 각각의 정보를 특정 부호로 분할하여 보내고 동일한 부호로 확산된 정보만을 선택하여 원래 신호를 재생하는 방식의 통신망이다. 이 방식은 아날로그 형태인 음성을 디지털 신호로 전환한 후 여러 개의 디지털 코드로 변환하여 통신하는 것으로 통화자의 채널에 고유하게 부여된 부호만을 인식하기 때문에 통화 품질이 좋고 통신 비밀이 보장된다는 장점이 있다. 시간과 주파수를 공유하는 각 사용자에게 상호상관 함수값의 크기가 작은 부호를 할당하면 송신할 때는 각자에게 할당된 부호를 이용하여 송신할 신호를 대역확산하여 전송하고, 수신할 때는 송신할 때 사용한 것과 같은 부호를 발생시켜 동기를 맞추고 이를 이용하여 수신된 신호를 역확산시켜 원하는 신호로 복원함으로써 정보가 전달된다. 따라서 직접 시퀀스를 대역확산 기법으로 사용하려면 PN(Pseudo Noise) 수열처럼 상호상관 함수값의 크기가 작고 개체수가 많은 수열이 필요하다. 이러한 수열을 확산수열로 사용한 통신망은 서로 다른 사용자에게 의해 발생하는 간섭을 최소화하면서도 다중접속 능력을 갖게 된다. 즉, 대역확산 다중접속 통신 시스템에서 사용된 수열들의 상호상관 함수값의 크기가 작으면 여러 사용자가 동시에 시스템에 접속할 때 발생하는 다중접속 간섭을 최소화하며, 통신 및 정보 보안성을 향상시킬 수 있기 때문에 확산신호와 수신신호의 상호상관 함수값의 크기는 작고 자기상관 함수값의 크기는 큰 수열을 부호로 사용하는 것이 바람직하다 ([1], [7], [23], [28], [31]).

Welch's lower bound에서 최적의 상관을 갖는 수열들은 수열군의 크기가 작고 선형스팬이 낮기 때문에 이를 개선하기 위해서는 확산수열의



상관관계를 높이는 것이 불가피하다([14], [32]). 따라서 Zeng 등은 수열군의 크기를 늘리고 상호상관 함숫값이 5개인 이진수열군을 제안했다([33]).

최대 주기를 갖는 이진 수열에 대한 상호상관함수는 1967년 Golomb에 의해 처음 연구되기 시작했으며([7]) 1980년 Sarwate에 의해 상호상관 함숫값의 범위는 수열을 어디서부터 선택하느냐가 아니라 어떻게 선택하느냐를 결정하는 데시메이션의 값에 의해 달라진다는 것이 알려졌다([29]). 최적의 상관도를 갖는 수열군을 생성하기 위해  $m$ -수열과 수열의 데시메이션에 대한 연구가 다양하게 진행되면서([8], [13], [16], [27]) 생성된 수열이 통신 시스템에 적용되었을 때 얼마나 적합한지를 판단하기 위해 상호상관 함숫값의 범위와 발생빈도를 분석하는 것은 중요한 과정이 되었다([8], [23]). 그러나 다중접속 가능성과 보안성을 향상시키기 위해 생성된 수열의 상호상관 함숫값의 범위와 발생빈도를 계산하는 것이 점점 어려워지면서 결과를 이끌어내는 과정이 수학적으로도 큰 의미를 갖게 되었다([11], [16], [18]).

본 논문의 3장에서는  $d \equiv 1 \pmod{2^m - 1}$ 을 만족하는 Niho 타입의 새로운 데시메이션을 제안하고 그 수열의 상호상관 함숫값의 범위와 함숫값의 발생빈도를 분석한다. Welch's lower bound에 따르면 새로운 데시메이션에 의해 생성된 수열은 최적에 가까운 상관관계를 갖는 우수한 비선형 이진수열이다.

4장에서는 수열군의 크기가 크고 이상적인 상관관계를 갖는 새로운 수열군을 생성하고 그 수열의 상호상관 함숫값의 범위와 함숫값의 발생빈도를 분석한다.

## 2. 배경지식

### 2.1. 트레이스 함수

트레이스(trace) 함수는 유한체  $GF(2^n)$ 에서 부분체  $GF(2^m)$  위로 대응되는 선형함수이며 다음과 같이 정의된다([7]).

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

$a, b \in GF(2^m)$ ,  $x, y \in GF(2^n)$ 에 대하여 트레이스 함수는 다음과 같은 성질을 갖는다.

- (a)  $Tr_m^n(ax+by) = aTr_m^n(x) + bTr_m^n(y)$ ,
- (b)  $Tr_m^n(x^{2^m}) = Tr_m^n(x)$ ,
- (c)  $Tr_1^n(x) = Tr_1^m[Tr_m^n(x)]$ ,
- (d)  $Tr_m^n(x) = a$ 를 만족하는  $GF(2^n)$ 의 원소  $x$ 의 개수는  $2^{n-m}$ .

트레이스 함수의 성질 (d)에 의해

$$\sum_{x \in GF(2^n)} (-1)^{Tr_1^n(\delta x)} = \begin{cases} 0 & , \delta \neq 0 \\ 2^n & , \delta = 0 \end{cases} \quad (2.1.1)$$

임은 자명하다.

## 2.2. 상호상관함수

상호상관함수는 두 현상 사이의 유사성 또는 관계성을 측정하기 위해 사용되는 수학적 도구로써 상호상관 함숫값이 0에 가까울수록 관계가 적음을 나타낸다. 위상이동차  $\tau$ 에 대하여 주기가  $2^n - 1$ 인 두 수열  $u(t)$ 와  $v(t)$ 의 상호상관함수  $C(\tau)$ , ( $\tau = 0, 1, \dots, 2^n - 2$ )는

$$C(\tau) = \sum_{t=0}^{2^n-2} (-1)^{u(t)+v(t+\tau)}$$

으로 정의된다([8]). 이 때 두 수열  $u(t)$ 와  $v(t)$ 가 같으면 자기상관함수, 다르면 상호상관함수라 한다. 주기가  $2^n - 1$ 이면서 상호상관 함숫값의 범위가 이상적인 수열로는  $m$ -수열, GMW 수열, generalized GMW 수열이 있다([7], [26], [30]).

$GF(2^n)$ 의 원시원소  $\alpha$ 에 대하여 수열  $u(t)$ 는  $u(t) = Tr_1^n(\alpha^t)$ 이라 정의하고  $\gcd(d, 2^n - 1) = 1$ 을 만족하는  $d$ 에 대하여  $v(t) = u(dt)$ 라 하자. 그러면 두 수열  $u(t)$ 와  $v(t)$ 의 상호상관함수  $C_d(\tau)$ 는

$$C_d(\tau) = \sum_{t=0}^{2^n-2} (-1)^{u(t-\tau)+v(t)} = \sum_{t=0}^{2^n-2} (-1)^{u(t)+v(t+\tau)} \quad (2.2.1)$$

으로 정의한다.  $u(t-\tau) = Tr_1^n(\alpha^{-\tau}\alpha^t)$ 이고  $v(dt) = Tr_1^n(\alpha^{dt})$ 이므로  $\alpha^t = x$ 로 두면  $x \in GF(2^n)^*$ 이고  $\{\alpha^{-\tau} | 0 \leq \tau \leq 2^n - 2\} = GF(2^n)^*$ 이다. 그리고  $\alpha^{-\tau} = y$ 라 두면  $y \in GF(2^n)^*$ 이므로

$$\sum_{t=0}^{2^n-2} (-1)^{u(t-\tau)+v(t)} = \sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(\alpha^{-\tau}\alpha^t) + Tr_1^n(\alpha^{dt})} = \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(yx + x^d)} - 1$$

이다. 마찬가지로  $\gcd(d, 2^n - 1) = 1$ 이므로  $\{\alpha^{d\tau} | 0 \leq \tau \leq 2^n - 2\} = GF(2^n)^*$ 임을 이용하여  $\alpha^{d\tau} = y$ 라 두면  $y \in GF(2^n)^*$ 이고

$$\sum_{t=0}^{2^n-2} (-1)^{u(t)+v(t+\tau)} = \sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(\alpha^t) + Tr_1^n(\alpha^{d(t+\tau)})} = \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(x + yx^d)} - 1$$

이다. 따라서 식 (2.2.1)로부터

$$\sum_{x \in GF(2^n)} (-1)^{Tr_1^n(x + yx^d)} = \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(yx + x^d)} \quad (2.2.2)$$

이다.



### 2.3. 데시메이션

수열  $u(dt)$ 는 수열  $u(t)$ 의 임의의 항에서 시작하여  $d$  번째 항을 추출하여 만든 수열이다. 이와 같이 수열을 추출하는 과정에 적용되는  $d$ 의 값을 **데시메이션(decimation)**이라 한다([21]).

**<예제 2.3.1>**  $n = 4$ ,  $p = 3$ ,  $d = 17$ 이라 하자.  $GF(3^4)$ 에서  $f(x) = x^4 + x + 2$ 를 만족하는  $\alpha$ 에 대하여  $u(t) = Tr^4(\alpha^t)$ , ( $t = 0, 1, \dots, 3^4 - 2$ )를  $8 \times 10$  배열로 나타내면 그림 1과 같다. 또한  $\gcd(d, 3^n - 1) = 1$ ,  $d \equiv 1 \pmod{3^2 - 1}$ 이므로  $u(dt) = Tr_1^4(\alpha^{dt})$ 는 그림 2와 같다.

|                              |                              |
|------------------------------|------------------------------|
| 1, 0, 0, 0, 1, 0, 0, 2, 1, 0 | 1, 2, 2, 2, 2, 0, 2, 2, 1, 2 |
| 1, 1, 1, 2, 0, 0, 2, 2, 0, 1 | 1, 0, 2, 1, 1, 0, 2, 0, 2, 0 |
| 0, 2, 2, 1, 1, 0, 1, 0, 1, 2 | 0, 2, 0, 1, 1, 0, 0, 2, 2, 2 |
| 1, 2, 2, 1, 2, 0, 1, 2, 2, 2 | 1, 1, 2, 0, 0, 0, 2, 1, 0, 1 |
| 2, 0, 0, 0, 2, 0, 0, 1, 2, 0 | 2, 1, 1, 1, 1, 0, 1, 1, 2, 1 |
| 2, 2, 2, 1, 0, 0, 1, 1, 0, 2 | 2, 0, 1, 2, 2, 0, 1, 0, 1, 0 |
| 0, 1, 1, 2, 2, 0, 2, 0, 2, 1 | 0, 1, 0, 2, 2, 0, 0, 1, 1, 1 |
| 2, 1, 1, 2, 1, 0, 2, 1, 1, 1 | 2, 2, 1, 0, 0, 0, 1, 2, 0, 2 |

그림 1. 수열  $u(t) = Tr_1^4(\alpha^t)$

그림 2. 수열  $v(t) = u(17t)$

본 논문에서는  $n = 2m$ 을 만족하는  $m, n$ 에 대하여  $d \equiv 1 \pmod{2^m - 1}$ 을 만족하는  $d$ 에 의하여 생성된 수열의 상호상관 함숫값과 그 분포를 분석한다. 이와 같은 형태의 데시메이션은 1972년 Niho에 의하여 처음 연구되었고 그 이후  $m$ -수열과 암호 이론에서 가장 많이 인용되는 결과 중 하나이다([24]).

<정의 2.3.2> 두 데시메이션  $d$ 와  $e$ 에 대하여

$$e \equiv 2^i d \pmod{2^n - 1}$$

를 만족하는 양의 정수  $i$ 가 존재할 때  $d$ 와  $e$ 는 동치(equivalent)라고 한다([27]).

<보조정리 2.3.3> 임의의 자연수  $k$ 와 데시메이션  $d$ 에 대하여

$$C_d(\tau) = C_d(2^k \tau)$$

이 성립한다([24]).

$\gcd(d, 2^n - 1) = 1$ 이면  $\{\alpha^d \mid \alpha \in GF(2^n)^*\} = GF(2^n)^*$ 이므로 두 데시메이션  $d$ 와  $e$ 가 동치이면  $C_d(\tau)$ 와  $C_e(\tau)$ 가 같고 상호상관 함수값의 발생횟수도 같다.

<보조정리 2.3.4> 두 데시메이션  $d, e$ 가 동치이면  $\tau = 0, 1, 2, \dots$ 에 대하여

$$C_d(\tau) = C_e(-d\tau)$$

이 성립한다([24]).

## 2.4. 선형다항식

<정의 2.4.1> 계수가  $GF(2^m)$ 의 원소일 때 다음과 같은 형태의 다항식을  $GF(2^m)$ 위에서의 **선형다항식**(linearized polynomial)이라 한다.

$$L(x) = \sum_{i=0}^n a_i x^{2^i}$$

이 선형다항식의 해의 개수에 관하여 다음이 알려져 있다([20]).

<보조정리 2.4.2>  $GF(2^m)$  위에서의 선형다항식  $L(x)$ 에 대하여  $L(x)$ 의 모든 해가  $GF(2^m)$ 의 확장체인  $GF(2^s)$ 에 포함된다면  $L(x)$ 의 모든 근은 같은 중복도를 갖고, 그 중복도는 1 또는 2의 멍승이다.

또한  $GF(2^s)$ 을  $GF(2)$  위에서의 선형공간으로 보았을 때, 방정식  $L(x)=0$ 의 해집합  $\{x \in GF(2^s) | L(x)=0\}$ 는  $GF(2^s)$ 의 **선형부분공간**(linear subspace)이다.

**증명.**  $U = \{x \in GF(2^s) | L(x)=0\}$ 이라 하고  $x_1, x_2 \in U$ 이면

$$L(x_1 + x_2) = \sum_{i=0}^n a_i (x_1 + x_2)^{2^i} = \sum_{i=0}^n a_i x_1^{2^i} + \sum_{i=0}^n a_i x_2^{2^i} = L(x_1) + L(x_2) = 0$$

이므로  $x_1 + x_2 \in U$ 이다. 또한  $c \in GF(2)$ 에 대하여

$$L(cx_1) = \sum_{i=0}^n a_i (cx_1)^{2^i} = \sum_{i=0}^n a_i c x_1^{2^i} = c \sum_{i=0}^n a_i x_1^{2^i} = c L(x_1) = 0$$

이므로  $cx_1 \in U$ 이다. 따라서  $\{x \in GF(2^s) | L(x)=0\}$ 은  $GF(2^s)$ 의 부분공간을

이룬다. 그런데  $L(x) = \sum_{i=0}^n a_i x^{2^i}$ 에 대해  $L'(x) = a_0$ 이므로



- i)  $a_0 \neq 0$ 인 경우, 방정식  $L(x)=0$ 은 중복도가 1인 단순근만을 갖는다.  
 ii)  $a_0 = 0$ 인 경우,  $a_0 = a_1 = \dots = a_{k-1} = 0$ ,  $a_k \neq 0$ 를 만족하는 1보다 큰  $k$ 가 존재하므로

$$L(x) = \sum_{i=0}^n a_i x^{2^i} = \sum_{i=k}^n a_i^{2^{mk}} x^{2^i} = \left( \sum_{i=k}^n a_i^{2^{(m-1)k}} x^{2^{i-k}} \right)^{2^k} = 0 \quad (2.4.1)$$

이다. 식 (2.4.1)의  $\sum_{i=k}^n a_i^{2^{(m-1)k}} x^{2^{i-k}}$ 도  $GF(2^m)$  위에서의 선형다항식이므로 (i)에 의하여 단순근만을 갖는다. 따라서 식 (2.4.1)의 모든 근은 중복도가  $2^k$ 이다. ■

<정의 2.4.3> 선형다항식  $L(x)$ 에 대하여

$$A(x) = L(x) - \alpha$$

형태의 다항식을 **아핀선형다항식**(affine linearized polynomial)이라 한다.

$GF(2^m)$ 의 확장체  $GF(2^s)$ 에서  $x_1$ 이  $A(x)=0$ 의 근이 될 필요충분조건은  $L(x_1)=\alpha$ 이다. 다음 정리는 아핀선형방정식의 해를 구하기 위해 필요하다.

<보조정리 2.4.4> 선형다항식  $L(x)$ 에 대하여  $A(x)=L(x)-\alpha$ 라 할 때,  $A(x)$ 는  $GF(2^m)$  위에서의 아핀선형다항식이며  $A(x)=0$ 의 모든 근들이  $GF(2^m)$ 의 확장체인  $GF(2^s)$ 에 포함된다면  $A(x)=0$ 의 모든 근은 같은 중복도를 갖고, 그 중복도는 1 또는 2의 멍승이다.

또한  $GF(2^s)$ 을  $GF(2)$  위에서의 선형공간으로 보았을 때,  $\{x \in GF(2^s) | A(x)=0\}$ 는  $GF(2^s)$ 의 **아핀부분공간**(affine subspace)이다.



**증명.** 중복도에 대해서는 보조정리 2.4.2와 같은 방법으로 증명할 수 있다.

$U = \{x \in GF(2^s) \mid L(x) = 0\}$ ,  $V = \{x \in GF(2^s) \mid A(x) = 0\}$ 라 하고  $x_1 \in V$ 라 하면  $L(x_1) = \alpha$ 이다.

$x_2 \in V$ 가 될 필요충분조건은  $L(x_2) = \alpha$ 이므로  $L(x_1) = L(x_2)$ 로부터  $L(x_1 + x_2) = 0$ 이다. 따라서  $x_1 + x_2 \in U$ 이고  $x_2 \in x_1 + U$ 이다.  $U$ 는  $GF(2)$  위에서  $GF(2^s)$ 의 선형부분공간이므로  $V$ 는  $GF(2^s)$ 에서의 아핀부분공간이다. ■

다음 정리는 아핀선형다항식의 해의 개수를 구하는데 중요한 역할을 한다.

**<정리 2.4.5>**  $GF(2^n)$  위에서의 선형다항식  $L(x)$ 와  $\alpha \in GF(2^n)$ 에 대하여  $|\{x \in GF(2^n) \mid L(x) = \alpha\}| \neq 0$ 이면

$$|\{x \in GF(2^n) \mid L(x) = \alpha\}| = |\{x \in GF(2^n) \mid L(x) = 0\}|$$

이다([20]).

## 2.5. 집합 $S$ 의 성질

$n = 2m$ 일 때,  $x^{2^m} = \bar{x}$ 로 간단히 표기하고  $x^{2^m+1} = 1$ 을 만족하는  $GF(2^n)$ 의 원소들로 이루어진 집합을  $S$ 라 하자. 즉,  $S = \{x \in GF(2^n) | x\bar{x} = 1\}$ 이다.

<보조정리 2.5.1> 집합  $S$ 에 대해

$$GF(2^m) \cap S = \{1\}$$

이 성립한다([18]).

**증명.**  $S = \{x \in GF(2^n) | x^{2^m+1} = 1\}$ 이고  $\gcd(2^m+1, 2^m-1) = 1$ 이므로  $GF(2^m) \cap S = \{1\}$ 이다. ■

<보조정리 2.5.2>  $n = 2m$ 일 때,  $S \setminus \{1\}$ 의 원소  $w$ 에 대하여 집합  $S \setminus \{1\}$ 과  $S \setminus \{w\}$ 는 다음과 같이 나타낼 수 있다([10], [24]).

$$(i) \quad S \setminus \{1\} = \left\{ \frac{\bar{z}+u}{z+u} \mid u \in GF(2^m) \right\}, \quad z \in GF(2^n) \setminus GF(2^m)$$

$$(ii) \quad S \setminus \{w\} = \left\{ \frac{uw+1}{u+w} \mid u \in GF(2^m) \right\} \\ = \left\{ w \frac{\bar{w}+u}{w+u} \mid u \in GF(2^m) \right\}$$

$n = 2m$ 일 때  $GF(2^n)$ 의 원시원소  $\alpha$ 는  $\delta^{2^m} = \delta$ ,  $\gamma^{2^m} = \gamma^{-1}$ 을 만족하는  $\delta$ ,  $\gamma$ 를 이용하여 다음과 같이 나타낼 수 있다([24]).

$$\alpha = \delta \gamma \tag{2.5.1}$$

이때  $\delta \in GF(2^m)$ ,  $\gamma \in S$ 이다.

## 2.6. 기존연구

$m$ -수열은 특성다항식이 원시다항식인 선형점화식을 만족하는 0 수열이 아닌 이진 수열이다. 최대주기수열(maximal length sequence)이라고도 하며 1967년 Golomb은  $m$ -수열의 성질에 대한 연구 결과를 발표했다([7]).

트레이스 함수는 새로운 수열군을 정의하는데 중요한 역할을 한다. 특히 트레이스 함수의 성질 (c)를 이용하여 이상적인 상호상관 함수값을 갖는 여러 가지 수열을 정의할 수 있다.

$GF(2^n)$ 의 원시원소  $\alpha$ 에 대하여  $GF(2)$ 상의  $m$ -수열은 다음과 같이 정의한다([8]).

$$\begin{aligned} \mathbb{S} &= \{s(t) \mid t = 0, 1, 2, \dots, 2^n - 2\}, \\ s(t) &= \text{Tr}_1^n(\omega \alpha^t), \omega \in GF(2^n)^*. \end{aligned}$$

이 수열  $\mathbb{S}$ 는 주기가  $2^n - 1$ 이고 상호상관 함수값은 집합  $\{-1, 2^n - 1\}$ 의 원소이다.  $m$ -수열은 상호상관 함수값의 크기는 작으면서 자기상관 함수값은 크기 때문에 대역확산 통신 시스템에서 확산코드로 사용하면 다중접속 시스템의 성능이 좋아진다.

양의 정수  $m, n$ 은  $m|n$ 이고 정수  $r$ ,  $(1 \leq r \leq 2^m - 2)$ 은  $\gcd(r, 2^m - 1) = 1$ 일 때,  $GF(2^n)$ 의 원시원소  $\alpha$ 에 대하여 다음과 같이 정의된  $GF(2)$ 상의 수열  $\mathbb{S}$ 를 GMW 수열이라 한다([30]).

$$\begin{aligned} \mathbb{S} &= \{s(t) \mid t = 0, 1, 2, \dots, 2^n - 2\}, \\ s(t) &= \text{Tr}_1^m \{ [\text{Tr}_m^n(\alpha^{2t})]^r \}. \end{aligned}$$

GMW 수열의 상호상관 함숫값은 집합  $\{-1, 2^n - 1\}$ 의 원소이다.  $r=1$ 인 경우 트레이스 함수의 성질 (c)를 이용하면 GMW 수열은  $m$ -수열이 된다. GMW 수열은  $m$ -수열과 같은 상호상관 함숫값을 가지면서 비선형인 우수한 수열이다.

자연수  $m, n$ 이  $n=2m$ 를 만족하고  $Q=2^m+1$ 일 때,  $GF(2^n)$ 의 원시원소  $\alpha$ 에 대하여,  $GF(2)$  상에서 다음과 같이 정의된 수열군은 Kasami 수열이다([14]).

$$\mathbb{S} = \{s_i(t) \mid 0 \leq t \leq 2^n - 2, 1 \leq i \leq 2^m\},$$

$$s_i(t) = Tr_1^m \{ Tr_m^n(\alpha^{2t}) + \gamma_i \alpha^{Q^t} \}.$$

여기서  $i$ 의 값이 1부터  $2^m$ 까지 변함에 따라  $\gamma_i$ 는  $GF(2^m)$ 의 모든 원소가 되고  $(\alpha^Q)^{2^m-1} = 1$ 이므로  $\alpha^Q$ 은  $GF(2^m)$ 의 원시원소가 된다. 따라서 수열군  $\mathbb{S}$ 의 수열은 주기가  $2^n - 1$ 인  $m$ -수열과 주기가  $2^m - 1$ 인 부분체의  $m$ -수열을 더해서 만들어진 수열이므로 Kasami 수열 또한  $m$ -수열의 일반화된 형태임을 알 수 있다. 이와 같이 주기가 서로 다른  $m$ -수열을 이용하여 만든 Kasami 수열의 상호상관 함숫값은 집합  $\{-2^m - 1, -1, 2^m - 1\}$ 의 원소이다.

$m$ -수열의 확장된 형태이면서 상호상관 함숫값이 3개인 또다른 수열로 No 수열을 들 수 있다([25]). 이 수열은 1보다 큰 양의 정수  $m$ 에 대해서  $n=2m$ 을 만족하는  $n$ 과  $\gcd(r, 2^m - 1) = 1$ 을 만족하는  $r$ , ( $1 \leq r \leq 2^m - 2$ )을 이용하여

$$\mathbb{S} = \{s_i(t) \mid 0 \leq t \leq 2^n - 2, 1 \leq i \leq 2^m\},$$

$$s_i(t) = Tr_1^m \{ [ Tr_m^n(\alpha^{2t}) + \gamma_i \alpha^{Q^t} ]^r \} \quad (2.6.1)$$

으로 정의되고 상호상관 함숫값은 집합  $\{-2^m - 1, -1, 2^m - 1\}$ 의 원소이다. 여기서  $\alpha$ 는  $GF(2^n)$ 의 원시원소이고  $\gamma_i$ 는  $GF(2^m)$ 의 원소이다. GMW 수열은 No 수열에서  $\gamma_i = 0$ 인 특수한 경우이다. No 수열군은 상호상관 함숫값이 Kasami 수열과 같으나 선형 스패는 GMW 수열보다 더 크다는 것이 장점이다.

$n = 2m$ 을 만족하는 자연수  $m, n$ 과  $Q = 2^m + 1$ 에 대하여  $GF(2)$  상에서 다음과 같이 정의된 수열군은 Zeng 등이 제안한 수열이다([33]).

$$\begin{aligned} \mathbb{S} &= \{s_{i,j}(t) \mid 0 \leq t \leq 2^n - 2, 0 \leq i \leq 2^n - 1, 0 \leq j \leq 2^m - 1\}, \\ s_{i,j}(t) &= Tr_1^m \left\{ \left[ Tr_m^n \left( \alpha^{2t} + \gamma_i \alpha^{(3 \cdot 2^m - 1)t} \right) + \eta_j \alpha^{Q^t} \right]^r \right\}. \end{aligned} \quad (2.6.2)$$

여기서  $r$ ,  $(1 \leq r < 2^m - 1)$ 은  $\gcd(r, 2^m - 1) = 1$ 을 만족하는 정수이고  $0 \leq i \leq 2^n - 1$ ,  $0 \leq j \leq 2^m - 1$ 에 대하여  $\gamma_i \in GF(2^n)$ ,  $\eta_j \in GF(2^m)$ 이다.  $\gamma_i = 0$ 인 경우 식 (2.6.2)는 식 (2.6.1)의 형태가 되므로 Zeng 수열은 No 수열을 포함한다. Zeng이 제안한 수열군의 상호상관 함숫값의 집합은  $\{-2^m - 1, -1, 2 \cdot 2^m - 1, 3 \cdot 2^m - 1\}$ 으로 Kasami 수열이나 No 수열에 비해 상호상관 함숫값은 커졌으나 수열군의 크기와 선형스패인이 크기 때문에 활용도가 높다는 장점을 갖고 있다([33]).

최적의 상관관계를 갖는 수열들은 통신 시스템에서 중요한 역할을 하기 때문에 낮은 상관관계를 갖는 수열군을 생성하기 위해  $m$ -수열과 수열의 테시메이션에 대한 연구가 다양하게 진행되어 왔다. 상호상관 함숫값이 3개인 수열에 대한 지금까지의 연구 결과는 다음과 같다([2], [4], [6], [15], [24]).

$$(3a) \ d = 2^k + 1, \ \frac{n}{\gcd(n, k)} : \text{홀수},$$

$$(3b) \ d = 2^{2k} - 2^k + 1, \ \frac{n}{\gcd(n, k)} : \text{홀수},$$

$$(3c) \ d = 2^{n/2} + 2^{(n+2)/4} + 1, \ n \equiv 2 \pmod{4},$$

$$(3d) \ d = 2^{(n-1)/2} + 3, \ n : \text{홀수},$$

$$(3e) \ d = 2^{n/2+1} + 3, \ n \equiv 2 \pmod{4},$$

$$(3f) \ d = 2^{(n-1)/2} + 2^{(n-1)/4} - 1, \ n \equiv 1 \pmod{4},$$

$$(3g) \ d = 2^{(n-1)/2} + 2^{(3n-1)/4} - 1, \ n \equiv 3 \pmod{4}.$$

다음은 상호상관 함수값이 4개인 잘 알려진 데시메이션이다. 이와 같은 형태의 데시메이션은 Niho에 의해 처음 연구되었고([24]) Hellesteth 외 여러 연구자들에 의해 제안되었다([11]).

$$(4a) \ d = 2^{n/2+1} - 1, \ n \equiv 0 \pmod{4},$$

$$(4b) \ d = (2^{n/2} + 1)(2^{n/4} - 1) + 2, \ n \equiv 0 \pmod{4},$$

$$(4c) \ d = \sum_{i=0}^{n/2} 2^{im}, \ n \equiv 0 \pmod{4}, \ 0 < m < n, \ \gcd(m, n) = 1,$$

$$(4d) \ d = \frac{2^{k-1}}{2^{s-1}}(2^{2k} + 2^{s+1} - 2^{k+1} - 1), \ n = 2k, \ 2s|k,$$

$$(4e) \ d = \frac{1}{2^{s-1}}(2^{2m} + 2^{2s+1} - 2^{m+s+1} - 1), \ n = 2m, \ 2s|m.$$

Niho([24])는 (4a), (4b)의 데시메이션을 제안하였고 이 중 (4a)의 데시메이션은 Dobbertin([5])이 제시한 (4c)의 데시메이션에 포함된다. 또한 (4b)와 (4c)의 데시메이션은 Rosendahl과 Hellesteth가 제시한 (4d)의 특별한 형태이다([27]). (4e)는 2012년 Kim 등이 제안한 데시메이션이다([17]).

### 3. Niho 타입의 새로운 데시메이션

$$3.1. d = \frac{2^{m-st-1}}{2^s-1} (2^n + 2^{st+s+1} - 2^{m+st+1} - 1)$$

이 절에서는 주기가  $2^n-1$ 인  $m$ -수열로부터 새로운  $d$ 를 이용하여 수열을 생성하고 상호상관 함숫값과 발생빈도를 계산한다.

$n=2m$ 을 만족하는 정수  $m, n$ 과  $\gcd(s, n)=1$ 을 만족하는 정수  $s$ , 그리고  $2st < m$ ,  $2s|m$  ( $t$ 는 정수)일 때 새로운  $d$ 는 다음과 같다.

$$d = \frac{2^{m-st-1}}{2^s-1} (2^n + 2^{st+s+1} - 2^{m+st+1} - 1)$$

<정리 3.1.1>  $\gcd(d, 2^n-1)=1$ 을 만족하는  $d$ 에 대하여 다음이 성립한다.

$$(a) \sum_{\tau=0}^{2^n-2} (C_d(\tau) + 1) = 2^n,$$

$$(b) \sum_{\tau=0}^{2^n-2} (C_d(\tau) + 1)^2 = 2^{2n},$$

$$(c) \sum_{\tau=0}^{2^n-2} (C_d(\tau) + 1)^3 = 2^{2n} N, \quad N = |\{x \in GF(2^n) \mid (x+1)^d = x^d + 1\}|.$$

(a)와 (b)는 트레이스 함수의 성질을 이용하여 1972년 Niho가 증명하였고, (c)는 Helleseth에 의하여 1976년 증명되었다([9], [24]).

$$C_d(\tau) = \sum_{t=0}^{2^n-2} (-1)^{u(t+\tau)+u(dt)} = \sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(\alpha^\tau \alpha^t + \alpha^{dt})} \text{에서 } y = \alpha^\tau \text{으로 두고 식}$$

(2.5.1)와 같이  $\alpha = \delta\gamma$ 로 나타내면



$$Tr_1^n(y\alpha^t + \alpha^{dt}) = Tr_1^m[Tr_m^n(y\gamma^t\delta^t + \gamma^{dt}\delta^{dt})] = Tr_1^m[\delta^t(y\gamma^t + \gamma^{dt} + \bar{y}\gamma^{-t} + \gamma^{-dt})]$$

이다. 따라서

$$\sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(\alpha^t\alpha^t + \alpha^{dt})} = \sum_{t=0}^{2^n-2} (-1)^{Tr_1^m[\delta^t(y\gamma^t + \gamma^{dt} + \bar{y}\gamma^{-t} + \gamma^{-dt})]}$$

이고  $C_d(\tau)$ 의 함숫값은 식 (3.1.1)을 만족하는  $x \in S$ 의 개수에 의해 결정된다.

$$x^{2d} + yx^{d+1} + \bar{y}x^{d-1} + 1 = 0 \quad (3.1.1)$$

이와 같은 사실을 이용하여 Niho는 다음 정리를 증명하였다([24]).

**<정리 3.1.2>**  $d$ 는  $d \equiv 1 \pmod{2^m - 1}$ 를 만족할 때,  $GF(2^n)^*$ 의 임의의 원소  $y$ 와 위상이동차  $\tau = 0, 1, 2, \dots, 2^n - 2$ 에 대하여  $C_d(\tau)$ 의 함숫값은 다음과 같다.

$$C_d(\tau) = -1 + 2^m (N(y) - 1)$$

단,  $N(y) = |\{x \in S \mid x^{2d} + yx^{d+1} + \bar{y}x^{d-1} + 1 = 0\}|$ 이다.

Helleseth는 2005년 방정식  $x^{2^s+1} + yx^{2^s} + \bar{y}x + 1 = 0$ 의 해의 개수에 관한 다음 정리를 증명하였다([12]).

**<정리 3.1.3>**  $n = 2m$ 이고  $y \in GF(2^n)^*$ 에 대하여 방정식

$$x^{2^s+1} + yx^{2^s} + \bar{y}x + 1 = 0$$

의  $S$ 에 존재하는 해  $x$ 의 개수는  $0, 1, 2, 2^{\gcd(s, m)} + 1$  중 하나이다.

<보조정리 3.1.4[17]>  $n = 2m$  일 때,  $d \equiv 1 \pmod{2^m - 1}$ 에 대하여  $x \in GF(2^n) \setminus \{0, 1\}$  가  $(x+1)^d = x^d + 1$  의 해가 될 필요충분조건은  $x^{d-1} = (x+1)^{d-1} = 1$  또는  $x^{d-2^m} = (x+1)^{d-2^m}$  이다.

증명.  $(x+1)^d = x^d + 1$  (3.1.2)

이므로,  $(\bar{x}+1)^d = (x^{2^m}+1)^d = (x+1)^{2^m d} = \{(x+1)^d\}^{2^m} = \bar{x}^d + 1$  이다. 따라서

$$(x\bar{x} + x + \bar{x} + 1)^d = (x\bar{x})^d + x^d + \bar{x}^d + 1$$

이고  $x\bar{x} \in GF(2^m)$ ,  $x + \bar{x} \in GF(2^m)$ ,  $x\bar{x} + x + \bar{x} + 1 \in GF(2^m)$  이므로

$$(x\bar{x} + x + \bar{x} + 1)^d = x\bar{x} + x + \bar{x} + 1$$

이고

$$(x\bar{x})^d = x\bar{x}$$

이다. 따라서  $x\bar{x} + x + \bar{x} + 1 = x\bar{x} + x^d + \bar{x}^d + 1$  이므로

$$x + \bar{x} = x^d + \bar{x}^d$$

이다. 양변에  $x^{d-1-2^m}$  을 곱하면

$$x^{d-2^m} + x^{d-1} = x^{2d-2^m-1} + x^{2^m d + d - 2^m - 1}$$

이고  $d \equiv 1 \pmod{2^m - 1}$  이므로  $d-1 = (2^m - 1)s$  를 만족하는 자연수  $s$  가 존재한다. 따라서

$$x^{2^m d + d - 2^m - 1} = x^{(2^m + 1)(d-1)} = x^{(2^m + 1)(2^m - 1)s} = 1$$

이고

$$x^{2d-2^m-1} - x^{d-2^m} - x^{d-1} + 1 = (x^{d-1} - 1)(x^{d-2^m} - 1) = 0$$

이다. 따라서  $x^d = x$  또는  $x^d = x^{2^m} = \bar{x}$ 이다.

(i)  $x^d = x$ 이면  $(x+1)^d = x^d + 1 = x + 1$ 이므로  $(x+1)^{d-1} = 1$ 이다.

(ii)  $x^d = \bar{x}$ 이면  $(x+1)^d = \bar{x} + 1 = (x+1)^{2^m}$ 이므로  $(x+1)^{d-2^m} = 1$ 이다.

역으로,  $x^{d-1} = (x+1)^{d-1} = 1$ 이라 하면  $(x+1)^d = x+1$ 이고  $x^d = x$ 이다.

따라서

$$(x+1)^d = x+1 = x^d + 1$$

를 만족하므로  $x$ 는 방정식 (3.1.2)의 해다.  $x^{d-2^m} = (x+1)^{d-2^m} = 1$ 이라 하면

$$(x+1)^d = (x+1)^{2^m} = x^{2^m} + 1 = x^d + 1$$

따라서  $x$ 는 방정식 (3.1.2)의 해다. ■

보조정리 3.1.4를 사용하여 보조정리 3.1.5를 얻을 수 있다.

**<보조정리 3.1.5>**  $n = 2^m$  이고  $d \equiv 1 \pmod{2^m - 1}$  일 때,  $x \in GF(2^n)^*$ 가  $(x+1)^d = x^d + 1$ 의 해라고 하면  $\left(\frac{x+1}{x+1}\right)^{d-1} = 1$  또는  $\left(\frac{x+1}{x+1}\right)^{d+1} = 1$ 이다.

**증명.** 보조정리 3.1.4에 의해서  $x^d = x$  또는  $x^d = \bar{x}$ 이다.

(i)  $x^d = x$  일 때,  $\overline{x^d} = \bar{x}$  이므로  $\left(\frac{x+1}{x+1}\right)^d = \frac{x^d+1}{x^d+1} = \frac{x+1}{x+1}$  이고

$\left(\frac{x+1}{x+1}\right)^{d-1} = 1$ 이다.

(ii)  $x^d = \bar{x}$  일 때,  $\overline{x^d} = x$  이므로  $\left(\frac{x+1}{x+1}\right)^d = \frac{x^d+1}{x^d+1} = \frac{\bar{x}+1}{x+1}$  이고

$\left(\frac{x+1}{x+1}\right)^{d+1} = 1$ 이다. ■

보조정리 3.1.4와 보조정리 3.1.5로부터 다음을 얻을 수 있다.

**<정리 3.1.6>**  $d \equiv 1 \pmod{2^m - 1}$ 을 만족하는  $d$ 에 대하여  $\gcd(d \pm 1, 2^m + 1) = 1$  이면

$$|\{x \in GF(2^n) \mid (x+1)^d = x^d + 1\}| = 2^m$$

이다.

**증명.**  $d \equiv 1 \pmod{2^m - 1}$  이므로  $GF(2^m)$ 의 모든 원소는 방정식 (3.1.2)의 해이므로

$$2^m \leq |\{x \in GF(2^n) \mid (x+1)^d = x^d + 1\}|$$

이다. 따라서 방정식 (3.1.2)를 만족하는 또다른 해  $x (\neq 0, 1)$ 가 존재한다고 가정할 수 있다. 보조정리 3.1.4에 의해 방정식 (3.1.2)의 해  $x$ 는  $x^d = x$  또는  $x^d = \bar{x}$ 를 만족하므로  $x^d = x$ 이면  $\left(\frac{x+1}{x+1}\right)^{d-1} = 1$ 이고  $x^d = \bar{x}$ 이면  $\left(\frac{x+1}{\bar{x}+1}\right)^{d+1} = 1$ 이다. 가정에 의해  $\frac{x+1}{x+1} = 1$  이므로  $x \in GF(2^m)$ 이다. 즉,  $\{x \in GF(2^n) \mid (x+1)^d = x^d + 1\} \subset GF(2^m)$ 이므로  $|\{x \in GF(2^n) \mid (x+1)^d = x^d + 1\}| \leq 2^m$ 이다. 따라서

$$|\{x \in GF(2^n) \mid (x+1)^d = x^d + 1\}| = 2^m$$

이다. ■

<보조정리 3.1.7>  $n = 2m$  이고 정수  $s, t$  에 대해  $2st < m$  이고  $2s | m$  일 때

$$d = \frac{2^{m-st-1}}{2^s - 1} (2^n + 2^{st+s+1} - 2^{m+st+1} - 1) \quad (3.1.3)$$

라 하면 다음 성질을 만족한다.

$$(1) \ d \equiv 1 \pmod{2^m - 1}$$

$$(2) \ d \equiv \frac{2^m - 2^s}{2^s - 1} \pmod{2^m + 1}$$

$$(3) \ \gcd(d, 2^n - 1) = 1$$

증명. (1) 
$$\begin{aligned} d &= \frac{2^{m-st-1}}{2^s - 1} \{ (2^m - 1)^2 + 2(2^m - 1) - 2^{st+1}(2^m - 2^s) \} \\ &= \frac{2^{m-st-1}}{2^s - 1} \{ (2^m - 1)^2 - 2(2^{st} - 1)(2^m - 1) \} + 2^m \\ &\equiv 2^m \pmod{2^m - 1} \end{aligned}$$

이므로  $d \equiv 1 \pmod{2^m - 1}$  이다.

(2)

$$\begin{aligned} d &= \frac{2^{m-st-1}}{2^s - 1} \{ (2^m - 1)(2^m + 1) - 2^{st+1}(2^m - 2^s) \} \\ &= \frac{2^{m-st-1}}{2^s - 1} (2^m - 1)(2^m + 1) - \frac{2^m(2^m - 2^s)}{2^s - 1} \end{aligned}$$

이고  $2s | m$  이므로  $\frac{2^m - 2^s}{2^s - 1}$  은 정수이다. 따라서  $d \equiv \frac{2^m - 2^s}{2^s - 1} \pmod{2^m + 1}$  이다.

(3) (1)에 의해  $\gcd(d, 2^n - 1) = \gcd(d, 2^m + 1)$  이고, (2)에 의해  $\gcd(d, 2^m + 1)$   
 $= \gcd\left(\frac{2^m - 2^s}{2^s - 1}, 2^m + 1\right)$  이다. 그런데

$$2^m + 1 = \frac{2^m - 2^s}{2^s - 1}(2^s - 1) + 2^s + 1$$

이므로  $\gcd\left(\frac{2^m - 2^s}{2^s - 1}, 2^m + 1\right) = \gcd\left(\frac{2^m - 2^s}{2^s - 1}, 2^s + 1\right)$  이다. 여기서  $2^m + 1 =$

$\frac{2^m - 2^s}{2^s - 1}(2^s - 1) + 2^s + 1$  이고  $\gcd(2^s - 1, 2^s + 1) = 1$  이므로

$$\begin{aligned}\gcd\left(\frac{2^m - 2^s}{2^s - 1}, 2^m + 1\right) &= \gcd\left(\frac{2^m - 2^s}{2^s - 1}, 2^s + 1\right) \\ &= \gcd(2^m - 2^s, 2^s + 1) \\ &= \gcd(2^m + 1, 2^s + 1) \\ &= 1\end{aligned}$$

이다. 마지막 등식은  $2s \mid m$  이므로 성립한다. ■

식 (3.1.3)의  $d$  는  $t=0$  이면 Rosendahl([12])의  $d$ ,  $t=0$  이면서  $m=2s$  를 만족하면 Niho([24])의  $d$  이다.

<정리 3.1.8>  $n=2m$  을 만족하는  $m, n$  과 정수  $s, t$  에 대해  $2st < m$  이고  $2s \mid m$  일 때  $d$  를 다음과 같이 정의하자.

$$d = \frac{1}{2^s - 1}(2^n + 2^{st+s+1} - 2^{m+st+1} - 1)$$

그러면

$$|\{x \in GF(2^n) \mid (x+1)^d = x^d + 1\}| = 2^m$$

이다.

**증명.** 보조정리 3.1.7 (1)에 의해  $d \equiv 1 \pmod{2^m - 1}$  이므로  $GF(2^m)$ 의 모든 원소는 방정식 (3.1.2)의 해이다.

이제  $x (\neq 0, 1)$ 가 식 (3.1.2)를 만족한다고 가정하고 식 (3.1.2)의 양변을  $2^s$  제곱하면  $(x+1)^{d2^s} = x^{d2^s} + 1$ , 여기서 다시 양변을 식 (3.1.2)로 나누면  $(x+1)^{(2^s-1)d} = \frac{x^{d2^s} + 1}{x^d + 1}$  이다. 이를 정리하면

$$x^{2^{st+s+1}+d} + x^{2^{st+m+1}+d2^s} = x^{2^{st+s+1}} + x^d + x^{2^{st+m+1}} + x^{d2^s} \quad (3.1.4)$$

이다. 그런데

$$\begin{aligned} 2^{st+s+1} + d - 2^{st+m+1} - d2^s &= -(2^s - 1)d + 2^{st+s+1} - 2^{st+m+1} \\ &= -(2^n - 1) \\ &\equiv 0 \pmod{2^n - 1} \end{aligned}$$

이므로  $x^{2^{st+s+1}} + x^d + x^{2^{st+m+1}} + x^{d2^s} = (x^{2^{m+st+1}} + x^d)(x^{(2^s-1)d} + 1) = 0$  이다. 따라서  $x^{2^{m+st+1}} = x^d$  또는  $(x^d)^{2^s-1} = 1$  이다.

(i)  $x^{2^{m+st+1}} = x^d$  일 때, 식 (3.1.4)를 이용하면  $x^{2^{m+st+1}(2^s-1)} = (x^{2^{m+st+1}})^{2^s-1} = (x^d)^{2^s-1} = x^{2^{st+s+1}-2^{m+st+1}}$  이므로  $x^{2^{m+st+1}} = x^{2^{st+s+1}}$  이다. 즉,  $x^{2^{st+s+1}} = (x^{2^{st+s+1}})^{2^m}$  이므로  $x^{2^{st+s+1}} \in GF(2^m)$  이다. 따라서  $x^{2^m} = (x^{2^{st+s+1}})^{2^{m-st-s-1}} \in GF(2^m)$  이고  $x = x^{2^n} = (x^{2^m})^{2^m}$  이므로  $x$  는  $GF(2^m)$ 의 원소이다.

(ii)  $(x^d)^{2^s-1} = 1$  일 때,  $x^d \in GF(2^s)$  이고  $2s|m$  이므로  $x^d \in GF(2^m)$  이다. 보조정리 3.1.4에 의하여  $x (\neq 0, 1)$ 가 방정식 (3.1.2)를 만족하면  $x^d = x$  또는  $x^d = x^{2^m}$  이다.  $x^d = x$  이면 분명히  $x \in GF(2^m)$  이고,  $x^d = x^{2^m}$  이면  $x^{2^m} = x^d \in GF(2^m)$  이므로  $x = (x^{2^m})^{2^m} = (x^d)^{2^m}$  이다. 그러므로  $x \in GF(2^m)$  이다. 따라서 (i), (ii)에 의하여 방정식 (3.1.2)의 해는  $GF(2^m)$ 의 원소이고  $|\{x \in GF(2^m) \mid (x+1)^d = x^d + 1\}| = 2^m$  이다. ■



<정리 3.1.9>  $n = 2m$  이고 정수  $s, t$  에 대해  $2st < m$ ,  $2s \mid m$  을 만족하면

$$d = \frac{1}{2^s - 1} (2^n + 2^{st+s+1} - 2^{m+st+1} - 1)$$

에 대하여  $C_d(\tau)$  의 함숫값과 발생횟수는 다음과 같다.

$$-1 - 2^m \quad \text{occurs} \quad \frac{2^{n+s-1} - 2^{m+s-1}}{2^s + 1} \quad \text{times}$$

$$-1 \quad \text{occurs} \quad \frac{2^n - 2^m - 2^s}{2^s} \quad \text{times}$$

$$-1 + 2^m \quad \text{occurs} \quad \frac{2^{n+s-1} - 2^n + 2^{m+s-1}}{2^s - 1} \quad \text{times}$$

$$-1 + 2^{m+s} \quad \text{occurs} \quad \frac{2^n - 2^m}{2^{3s} - 2^s} \quad \text{times}$$

증명. 정리 3.1.3과 식 (3.1.1)에 의해 다음 식을 얻는다.

$$x^{\frac{2^m - 2^s}{2^s - 1}} + yx + yx^{-1} + x^{-\frac{2^m - 2^s}{2^s - 1}} = 0$$

정리 3.1.3에 의해  $C_d(\tau)$ 는 4개의 함숫값을 갖고 정리 3.1.2에 의하여  $C_d(\tau) \in \{-2^m - 1, -1, 2^m - 1, 2^{m+s} + 1\}$ 이다. 집합  $S$ 에서  $i$ , ( $i = 0, 1, 2, 2^s + 1$ ) 개의 해를 가지는 횟수를  $N_i$ 라 하면 정리 3.1.1과 정리 3.1.8에 의해 다음 식이 성립하고

$$\begin{aligned} N_0 + N_1 + N_2 + N_{2^s+1} &= 2^{n-1} \\ -2^m N_0 + 0 \cdot N_1 + 2^m N_2 + 2^{m+s} N_{2^s+1} &= 2^n \\ 2^n N_0 + 0 \cdot N_1 + 2^n N_2 + 2^{n+2s} N_{2^s+1} &= 2^{2n} \\ -2^{n+m} N_0 + 0 \cdot N_1 + 2^{n+m} N_2 + 2^{n+m+3s} N_{2^s+1} &= 2^{2n+m} \end{aligned}$$

이 연립방정식을 풀면 각  $N_i$ 의 값을 구할 수 있다. ■

<예제 3.1.10> 원시다항식  $f(x) = x^8 + x^4 + x^3 + x^2 + 1$ 의 원시근  $\alpha$ 에 대하여,  $n=8$ ,  $s=1$ ,  $t=2$ 로 두면  $d=31$ 이다.  $u(t) = \text{Tr}_1^8(\alpha^t)$ 와  $v(t) = u(31t)$ 를  $15 \times 17$  배열로 나타내면 각각 그림 3, 그림 4와 같다.

0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0  
0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1  
0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0  
0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0  
0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1  
0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1  
0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0  
0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1  
0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0  
0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1  
0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1  
0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1  
0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1  
0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0  
0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0

0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0  
0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0  
0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1  
0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0  
0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0  
0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1  
0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1  
0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0  
0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1  
0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0  
0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1  
0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1  
0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1  
0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1  
0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0

그림 3. 수열  $u(t) = \text{Tr}_1^8(\alpha^t)$ 의  $15 \times 17$  배열      그림 4. 수열  $v(t) = u(31t)$ 의  $15 \times 17$  배열

그림 3에 나타난 수열에 위상이동차를 0부터 254까지 적용시켜 그림 4에 나타난 수열과의 상호상관 함숫값  $C_{31}(\tau)$ 를 구하면  $C_{31}(\tau) \in \{-17, -1, 15, 31\}$ 이고 각 함숫값의 발생횟수는 표 1과 같다.

표 1.  $C_{31}(\tau)$  값의 발생횟수

| 상호상관 함숫값 | -17 | -1  | 15 | 31 |
|----------|-----|-----|----|----|
| 발생횟수     | 80  | 119 | 16 | 40 |

$$3.2. d = \frac{2^{m-1}}{2^s - 1} (2^{m(i+1)} - 2^{mi} + 2^{s+1} - 2^m - 1)$$

이 절에서는 상호상관 함숫값이 4개인 새로운  $d$ 를 제안하고  $m$ -수열과  $d$ 에 의해 생성된 수열의 상호상관 함숫값의 범위와 함숫값의 발생빈도를 분석한다.

짝수  $m$ 에 대하여  $n = 2m$ 이라 하고 홀수  $i$ 의 약수인  $s$ 는  $\gcd(s, n) = 1$ 를 만족하는 정수일 때 새로운  $d$ 를 다음과 같이 정의한다.

$$d = \frac{2^{m-1}}{2^s - 1} (2^{m(i+1)} - 2^{mi} + 2^{s+1} - 2^m - 1)$$

<보조정리 3.2.1> 짝수  $m$ 과  $\gcd(s, m) = 1$ 를 만족하는  $s$ 에 대하여 다음이 성립한다.

$$(a) \gcd(2^m + 1, 2^s - 1) = 1$$

$$(b) \gcd(2^m + 1, 2^s + 1) = 1$$

**증명.** (a) 짝수  $m$ 에 대하여  $\gcd(s, m) = 1$ 이므로  $s$ 는 홀수다. 따라서  $\frac{s}{\gcd(s, m)}$ 이 홀수이므로  $\gcd(2^m + 1, 2^s - 1) = 1$ 이다.

(b)  $2^m + 1 = 2^{m-s} (2^s + 1) - 2^{m-s} + 1$ 이므로  $\gcd(2^m + 1, 2^s + 1) = \gcd(2^s + 1, 2^{m-s} - 1)$ 이다. 그런데  $\frac{m-s}{\gcd(s, m-s)} = \frac{m-s}{\gcd(s, m)}$ 도 홀수이므로  $\gcd(2^s + 1, 2^{m-s} - 1) = 1$ 이고, 따라서  $\gcd(2^m + 1, 2^s + 1) = 1$ 이다. ■

<보조정리 3.2.2> 짝수  $m$ 에 대하여  $n = 2m$  이고  $s$  는  $\gcd(s, n) = 1$  을 만족하는 정수일 때

$$d = \frac{2^{m-1}}{2^s - 1} (2^{m(i+1)} - 2^{mi} + 2^{s+1} - 2^m - 1)$$

에 대하여  $s$  가 홀수  $i$  의 약수이면 다음 성질을 만족한다.

$$(1) \ d \equiv 1 \pmod{2^m - 1}$$

$$(2) \ d \equiv \frac{2^{mi} - 2^s}{2^s - 1} \pmod{2^m + 1}$$

$$(3) \ \gcd(d, 2^n - 1) = 1$$

증명. (1)은 분명하다.

$$(2) \ d = 2^{m-1} \left\{ \frac{2^{mi} - 2^s}{2^s - 1} (2^m - 1) + 2^m + 1 \right\} \equiv \frac{2^{mi} - 2^s}{2^s - 1} \pmod{2^m + 1}$$

(3) (1)과 (2)에 의해

$$\gcd(d, 2^n - 1) = \gcd(d, 2^m + 1) = \gcd\left(\frac{2^{mi} - 2^s}{2^s - 1}, 2^m + 1\right)$$

이다. 그리고  $\gcd(2^s - 1, 2^m + 1) = 1$  이므로

$$\gcd\left(\frac{2^{mi} - 2^s}{2^s - 1}, 2^m + 1\right) = \gcd(2^{mi} - 2^s, 2^m + 1)$$

이다. 또한  $2^{mi} - 2^s \equiv -1 - 2^s \pmod{2^m + 1}$  이므로  $\gcd(2^{mi} - 2^s, 2^m + 1) = \gcd(2^m + 1, 2^s + 1) = 1$  이다. 따라서  $\gcd(d, 2^n - 1) = 1$  이다. ■

<보조정리 3.2.3> 짝수  $m$ 에 대하여  $n = 2m$  이고  $s$  는  $\gcd(s, n) = 1$  인 정수이다. 홀수  $i$ 의 약수  $s$ 에 대하여

$$d = \frac{2^{m-1}}{2^s - 1} (2^{m(i+1)} - 2^{mi} + 2^{s+1} - 2^m - 1)$$

일 때, 다음이 성립한다.

(a)  $\gcd(d+1, 2^m+1) = 1,$

(b)  $\gcd(d-1, 2^m+1) = 1.$

**증명.** (a) 보조정리 3.2.1에 의하여  $\gcd(2^s-1, 2^m+1) = 1$  이다.

$$\begin{aligned} (2^s-1)(d+1) &= 2^{m-1}(2^{m(i+1)} - 2^{mi} + 2^{s+1} - 2^m - 1) + (2^s-1) \\ &\equiv -2 \pmod{2^m+1} \end{aligned}$$

이므로  $\gcd(d+1, 2^m+1) = \gcd((2^s-1)(d+1), 2^m+1) = \gcd(2^{s+1}, 2^m+1)$  이다.

따라서  $\gcd(d+1, 2^m+1) = 1$  이다.

(b)  $(2^s-1)(d-1) = 2^{m-1}(2^{m(i+1)} - 2^{mi} + 2^{s+1} - 2^m - 1) - (2^s-1)$  이고 보조정리 3.2.1 (a)에 의하여  $(2^s-1)(d-1) \equiv -2^{s+1} \pmod{2^m+1}$  이다. 따라서  $\gcd(d-1, 2^m+1) = \gcd((2^s-1)(d-1), 2^m+1) = \gcd(2^{s+1}, 2^m+1) = 1$  이다. ■

보조정리 3.2.2에 의하여  $d \equiv 1 \pmod{2^m - 1}$  이다. 정리 3.1.6과 보조정리 3.2.3에 의하여 다음 정리를 얻을 수 있다.

<정리 3.2.4>  $m$  이 짝수일 때  $n = 2m$  을 만족하는  $n$  과 홀수  $i$  의 약수 이면서  $\gcd(s, n) = 1$  을 만족하는 정수  $s$  에 대하여

$$d = \frac{2^{m-1}}{2^s - 1} (2^{m(i+1)} - 2^{mi} + 2^{s+1} - 2^m - 1)$$

이면 두  $m$ -수열 사이의  $C_d(\tau)$  값의 발생빈도는 다음과 같다.

|                |        |                           |       |
|----------------|--------|---------------------------|-------|
| $-1 - 2^m$     | occurs | $\frac{2^n - 2^m}{3}$     | times |
| $-1$           | occurs | $\frac{2^n - 2^m - 2}{2}$ | times |
| $-1 + 2^m$     | occurs | $2^m$                     | times |
| $-1 + 2^{m+1}$ | occurs | $\frac{2^n - 2^m}{6}$     | times |

증명. 보조정리 3.2.2에 의하여  $d \equiv \frac{2^{mi} - 2^s}{2^s - 1} \pmod{2^m + 1}$ ,

$d \equiv 1 \pmod{2^m - 1}$  이므로 정리 3.1.2에 의하여 아래의 식을 얻는다.

$$x^{\frac{2^{mi} - 2^s}{2^s - 1}} + yx + y^{2^m} x^{-1} + x^{-\frac{2^{mi} - 2^s}{2^s - 1}} = 0 \quad (3.2.1)$$

$$x^{2^{m+1}} = 1$$

보조정리 3.2.1에 의하여  $\gcd(2^m + 1, 2^s - 1) = 1$  이므로 방정식 (3.2.1)의 해의 개수는 식 (3.2.1)의  $x$  에  $x^{2^s - 1}$  을 대입하여 얻은 아래 방정식 (3.2.2)의 해의 개수와 같다.

$$yx^{2^s - 1} + x^{2^{mi} - 2^s} + \bar{y}x^{1 - 2^s} + x^{-2^{mi} + 2^s} = 0 \quad (3.2.2)$$

식 (3.2.2)의 양변에  $x^{2^{mi}-2^s}$  을 곱하면 식 (3.2.3)을 얻는다.

$$yx^{2^{mi}-1} + x^{2(2^{mi}-2^s)} + \bar{y}x^{2^{mi}-2^{s+1}+1} + 1 = 0 \quad (3.2.3)$$

$2^m \equiv -1 \pmod{2^m+1}$  이므로

$$x^{2(-1-2^s)} + yx^{-2} + \bar{y}x^{-2^{s+1}} + 1 = 0 \quad (3.2.4)$$

이고 방정식 (3.2.4)의 해의 개수는 방정식 (3.2.5)의 해의 개수와 같다.

$$x^{2^s+1} + yx^{2^s} + \bar{y}x + 1 = 0 \quad (3.2.5)$$

따라서 정리 3.1.2에 의해  $C_d(\tau)$  는 4개의 값을 가지고  $C_d(\tau) \in \{-2^m-1, -1, 2^m-1, 2 \cdot 2^m-1\}$  이다. 정리 3.1.1과 정리 3.1.6에 의하여

$$\sum_{\tau=0}^{2^n-2} (C_d(\tau)+1)^3 = 2^{2n}2^m$$

이다. 집합  $S$ 에 포함되는 해의 개수가  $i$ 인 횟수를  $N_i$ , ( $i=0, 1, 2, 3$ )라 하면 다음이 성립한다.

$$\begin{aligned} N_0 + N_1 + N_2 + N_3 &= 2^n - 1 \\ -2^m N_0 + 0 \cdot N_1 + 2^m N_2 + 2^{m+1} N_3 &= 2^n \\ -2^n N_0 + 0 \cdot N_1 + 2^n N_2 + 2^{n+2} N_3 &= 2^{2n} \\ -2^{n+m} N_0 + 0 \cdot N_1 + 2^{n+m} N_2 + 2^{n+m+3} N_3 &= 2^{2n+m} \end{aligned}$$

이 연립방정식을 풀면  $N_0 = \frac{2^{2k}-2^m}{3}$ ,  $N_1 = \frac{2^n-2^m-2}{2}$ ,  $N_2 = 2^m$ ,

$N_3 = \frac{2^n-2^m}{6}$  이다. ■





## 4. 새로운 수열의 상호상관 함숫값

### 4.1. 새로운 비선형 이진수열의 생성

$n = 2m$ ,  $m = 2k$  일 때,  $\gcd(r, 2^m - 1) = 1$  를 만족하는  $r$  과  $d$  에 대하여 새로운 수열군  $S^r$  을 다음과 같이 정의한다.

$$S^r = \{s_a^r(t) \mid a \in GF(2^m), 0 \leq t \leq 2^n - 2\},$$

$$s_a^r(t) = Tr_1^m([Tr_n^m(a\alpha^t + \alpha^{dt})]^r).$$

수열군  $S^r$  에서 주기가  $2^n - 1$  인 두 수열  $s_a^r(t)$ ,  $s_b^r(t)$  에 대한 상호상관함수  $C_{a,b}(\tau)$  는

$$C_{a,b}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_a^r(t+\tau) + s_b^r(t)}$$

이다.

## 4.2. $d=2 \cdot 2^m - 1$ 일 때 새로운 수열의 상호상관 함숫값

이 절에서는 수열군  $S^r$  에서  $d=2 \cdot 2^m - 1$  에 의해 생성된 수열의 상호상관 함숫값의 범위와 상호상관 함숫값  $2^m - 1$  의 발생빈도를 분석한다.

<보조정리 4.2.1> 짝수  $m$  에 대하여  $n=2m$  이고  $d=2 \cdot 2^m - 1$  일 때, 다음이 성립한다.

$$(a) \ d \equiv 1 \pmod{2^m - 1}$$

$$(b) \ d \equiv -3 \pmod{2^m + 1}$$

<보조정리 4.2.2>  $\gcd(r, 2^m - 1) = 1$  를 만족하는  $r$  과  $t$ , ( $0 \leq t \leq 2^m$ ) 에 대하여  $H(t, \tau, r) = [Tr_m^n(a \alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r + [Tr_m^n(b \alpha^t + \alpha^{dt})]^r$  일 때  $N(t, \tau, r) = |\{t \mid H(t, \tau, r) = 0, 0 \leq t \leq 2^m\}|$  이라 하면 다음이 성립한다.

$$N(t, \tau, r) = N(t, \tau, 1)$$

증명.  $N(t, \tau, r)$  의 값은  $H(t, \tau, r) = 0$  을 만족하는  $t$  의 개수이다. 정의에 의하여

$$H(t, \tau, r) = 0 \Leftrightarrow [Tr_m^n(a \alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r = [Tr_m^n(b \alpha^t + \alpha^{dt})]^r$$

이고  $\gcd(r, 2^m - 1) = 1$  이므로

$$\begin{aligned} & \{t \mid [Tr_m^n(a \alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r = [Tr_m^n(b \alpha^t + \alpha^{dt})]^r, 0 \leq t \leq 2^m\} \\ &= \{t \mid Tr_m^n(a \alpha^{t+\tau} + \alpha^{d(t+\tau)}) = Tr_m^n(b \alpha^t + \alpha^{dt}), 0 \leq t \leq 2^m\} \end{aligned}$$

이다. 즉,  $\{t \mid H(t, \tau, r) = 0, 0 \leq t \leq 2^m\} = \{t \mid H(t, \tau, 1) = 0, 0 \leq t \leq 2^m\}$  이므로  $N(t, \tau, r) = N(t, \tau, 1)$  이다. ■

<보조정리 4.2.3> 짝수  $m$  에 대하여  $n=2m$  이고  $r$  은  $\gcd(r, 2^m - 1)=1$  을 만족할 때,  $d=2 \cdot 2^m - 1$  이면  $C_{a,b}(\tau)$  는 4 값 함수이다. 즉,

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

이다.

**증명.** 수열군  $S^r$  의 두 수열  $s_a^r(t)$ ,  $s_b^r(t)$  에 대한  $C_{a,b}(\tau)$  를 계산하기 위해  $s_a^r(t+\tau) + s_b^r(t)$  를 먼저 구한다.

$$\begin{aligned} s_a^r(t+\tau) + s_b^r(t) &= Tr_1^m \left( [Tr_m^n(a \alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r \right) + Tr_1^m \left( [Tr_m^n(b \alpha^t + \alpha^{dt})]^r \right) \\ &= Tr_1^m \left( [Tr_m^n(a \alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r + [Tr_m^n(b \alpha^t + \alpha^{dt})]^r \right) \end{aligned}$$

$Q=2^m+1$  로 두고  $t=t_1Q+t_2$ , ( $0 \leq t_1 \leq 2^m-2$ ,  $0 \leq t_2 \leq 2^m$ ) 라 하자. 또  $GF(2^n)$  의 원시원소  $\alpha$  에 대하여  $\alpha^Q = \beta$  라 두면  $\beta \in GF(2^m)^*$  이다.  $d \equiv 1 \pmod{2^m-1}$  이므로  $\beta^d = \beta$  임을 이용하면

$$\begin{aligned} a \alpha^{t+\tau} + \alpha^{d(t+\tau)} &= a \alpha^{t_1Q+t_2+\tau} + \alpha^{d(t_1Q+t_2+\tau)} \\ &= a \beta^{t_1} \alpha^{t_2+\tau} + \beta^{dt_1} \alpha^{d(t_2+\tau)} \\ &= \beta^{t_1} (a \alpha^{t_2+\tau} + \alpha^{d(t_2+\tau)}) \end{aligned}$$

이고

$$b \alpha^t + \alpha^{dt} = b \alpha^{t_1Q+t_2} + \alpha^{d(t_1Q+t_2)} = \beta^{t_1} (b \alpha^{t_2} + \alpha^{dt_2})$$

이다. 따라서

$$\begin{aligned} &Tr_1^m \left( [Tr_m^n(a \alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r + [Tr_m^n(b \alpha^t + \alpha^{dt})]^r \right) \\ &= Tr_1^m \left( [\beta^{t_1} Tr_m^n(a \alpha^{t_2+\tau} + \alpha^{d(t_2+\tau)})]^r + [\beta^{t_1} Tr_m^n(b \alpha^{t_2} + \alpha^{dt_2})]^r \right) \end{aligned}$$

$$\begin{aligned}
&= Tr_1^m \left( \beta^{t_1 r} \left\{ \left[ Tr_m^n \left( a \alpha^{t_2 + \tau} + \alpha^{d(t_2 + \tau)} \right) \right]^r + \left[ Tr_m^n \left( b \alpha^{t_2} + \alpha^{dt_2} \right) \right]^r \right\} \right) \\
&= Tr_1^m \left( \beta^{t_1 r} H(t_2, \tau, r) \right)
\end{aligned}$$

이고, 여기서  $H(t_2, \tau, r) = \left[ Tr_m^n \left( a \alpha^{t_2 + \tau} + \alpha^{d(t_2 + \tau)} \right) \right]^r + \left[ Tr_m^n \left( b \alpha^{t_2} + \alpha^{dt_2} \right) \right]^r$  이다.

또  $\beta \in GF(2^m)^*$  에 대하여  $\gcd(r, 2^m - 1) = 1$  이므로  $\{\beta^{t_1 r} \mid 0 \leq t_1 \leq 2^m - 2\} = GF(2^m)^*$  이다. 따라서

$$\begin{aligned}
C_{a,b}(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{s_a^r(t+\tau) + s_b^r(t)} \\
&= \sum_{t_1=0}^{2^m-2} \sum_{t_2=0}^{2^m} (-1)^{Tr_1^m \{ \beta^{t_1 r} H(t_2, \tau, r) \}} \\
&= \sum_{\eta \in GF(2^m)^*} \sum_{t_2=0}^{2^m} (-1)^{Tr_1^m \{ \eta H(t_2, \tau, r) \}} \\
&= \sum_{\eta \in GF(2^m)} \sum_{t_2=0}^{2^m} (-1)^{Tr_1^m \{ \eta H(t_2, \tau, r) \}} - (2^m + 1)
\end{aligned}$$

이다. 여기서  $N(t_2, \tau, r) = |\{t_2 \mid H(t_2, \tau, r) = 0, 0 \leq t_2 \leq 2^m\}|$  이라 하면

$$\begin{aligned}
C_{a,b}(\tau) &= \sum_{\eta \in GF(2^m)} \sum_{t_2=0}^{2^m} (-1)^{Tr_1^m \{ \eta H(t_2, \tau, r) \}} - (2^m + 1) \\
&= N(t_2, \tau, r) 2^m - (2^m + 1) \\
&= \{N(t_2, \tau, r) - 1\} 2^m - 1
\end{aligned}$$

이다. 보조정리 4.2.2에 의하여  $N(t_2, \tau, r) = N(t_2, \tau, 1)$  이므로  $H(t_2, \tau, r) = 0$  을 만족하는  $t_2$  의 개수 대신  $H(t_2, \tau, 1) = 0$  을 만족하는  $t_2$  의 개수를 구하면

$$\begin{aligned}
& Tr_m^n(a \alpha^{t_2+\tau} + \alpha^{d(t_2+\tau)} + b \alpha^{t_2} + \alpha^{dt_2}) \\
&= Tr_m^n\{(a\alpha^\tau + b)\alpha^{t_2} + (\alpha^{d\tau} + 1)\alpha^{dt_2}\} \\
&= Tr_m^n\{A(\tau)\alpha^{t_2} + B(\tau)\alpha^{dt_2}\} \\
&= A(\tau)\alpha^{t_2} + B(\tau)\alpha^{dt_2} + \overline{A(\tau)}\alpha^{2^m t_2} + \overline{B(\tau)}\alpha^{2^m dt_2} \\
&= 0
\end{aligned} \tag{4.2.1}$$

여기서  $A(\tau) = a\alpha^\tau + b$ ,  $B(\tau) = \alpha^{d\tau} + 1$  이다.

$GF(2^n)$ 의 원시원소  $\alpha$ 는  $\delta^{2^m} = \delta$ ,  $\gamma^{2^m} = \gamma^{-1}$ 를 만족하는  $\delta, \gamma$ 를 이용하여  $\delta\gamma$ 로 나타낼 수 있다. 보조정리 4.2.1에 의하여  $\delta^d = \delta$ ,  $\gamma^d = \gamma^{-3}$ 이고  $\delta \in GF(2^m)$ ,  $\gamma \in S$ 임은 자명하다. 그러면

$$\begin{aligned}
& A(\tau)\alpha^{t_2} + B(\tau)\alpha^{dt_2} + \overline{A(\tau)}\alpha^{2^m t_2} + \overline{B(\tau)}\alpha^{2^m dt_2} \\
&= A(\tau)\delta^{t_2}\gamma^{t_2} + B(\tau)\delta^{dt_2}\gamma^{dt_2} + \overline{A(\tau)}\delta^{2^m t_2}\gamma^{2^m t_2} + \overline{B(\tau)}\delta^{2^m dt_2}\gamma^{2^m dt_2} \\
&= \delta^{t_2}(A(\tau)\gamma^{t_2} + B(\tau)\gamma^{-3t_2} + \overline{A(\tau)}\gamma^{-t_2} + \overline{B(\tau)}\gamma^{3t_2}) \\
&= 0
\end{aligned}$$

이고  $\delta^{t_2} \neq 0$ 이므로 식 (4.2.1)은

$$\overline{B(\tau)}\gamma^{6t_2} + A(\tau)\gamma^{4t_2} + \overline{A(\tau)}\gamma^{2t_2} + B(\tau) = 0 \tag{4.2.2}$$

와 동치이다.  $\gamma^{2t_2} = x$ 로 두면,  $\{\gamma^{2t_2} | 0 \leq t_2 \leq 2^m, \gamma^{2^{m+1}} = 1\} = S$ 이므로  $x \in S$ 이고

$$\overline{B(\tau)}x^3 + A(\tau)x^2 + \overline{A(\tau)}x + B(\tau) = 0 \tag{4.2.3}$$

이다. 식 (4.2.3)은 3차 방정식이므로  $N(t_2, \tau, r) = 0, 1, 2, 3$ 이다. 따라서  $C_{a,b}(\tau) \in \{-2^m - 1, -1, 2^m - 1, 2 \cdot 2^m - 1\}$ 이고 상호상관함수  $C_{a,b}(\tau)$ 는 4값 함수이다. ■

이제 4 값 함수인  $C_{a,b}(\tau)$ 에 대하여 특별히  $a=0, b \neq 0$  인 경우로 제한하여 상호상관 함수값의 범위와 발생빈도를 분석한다.

$C_{0,b}(\tau) = \{N(t_2, \tau, r) - 1\}2^m - 1, N(t_2, \tau, r) = |\{t_2 | H(t_2, \tau, r) = 0, 0 \leq t_2 \leq 2^m\}|$   
이므로  $N(t_2, \tau, r)$ 의 값을 구하기 위해 방정식

$$\overline{B(\tau)}x^3 + bx^2 + bx + B(\tau) = 0 \quad (4.2.4)$$

의 집합  $S$ 에 존재하는 해의 개수를 구한다. 보조정리 2.5.1에 의하여  $GF(2^m) \cap S = \{1\}$ 이므로  $x=1$ 이 방정식 (4.2.4)의 해가 되는지를 먼저 확인한다.  $x=1$ 이 해가 될 필요충분조건은  $\overline{B(\tau)} = B(\tau)$ 이므로  $B(\tau) \in GF(2^m)$ 인 경우와  $B(\tau) \notin GF(2^m)$ 인 경우로 나누어 생각한다.

(a)  $B(\tau) \in GF(2^m)$ 인 경우

$B(\tau) = 0$ 일 때는  $x=1$ 이 유일한 해가 되므로  $C_{0,b}(\tau) = -1$ 이다.

$B(\tau) \neq 0$ 이면 식 (4.2.4)에서 최고차 항의 계수를 1로 만들 수 있다.

$$\begin{aligned} \overline{B(\tau)}x^3 + bx^2 + bx + B(\tau) &= 0 \\ \Leftrightarrow 0 \leq k_1 \leq 2^m - 2 \text{에 대하여 } x^3 + \beta^{k_1}x^2 + \beta^{k_1}x + 1 &= 0 \\ \Leftrightarrow (x+1)\{x^2 + (\beta^{k_1} + 1)x + 1\} &= 0 \end{aligned} \quad (4.2.5)$$

이므로  $k_1 = 0$ 이면 방정식 (4.2.5)는  $x=1$ 을 유일한 근으로 갖고 이때  $C_{0,b}(\tau) = -1$ 이다.  $k_1 \neq 0$ 이면 방정식 (4.2.5)의 해의 개수는 방정식

$$x^2 + (\beta^{k_1} + 1)x + 1 = 0 \quad (4.2.6)$$

의 해의 개수에 따라 달라진다. 식 (4.2.6)에서  $Tr_1^4\left(\frac{1}{\beta^{2k_1} + 1}\right) = 0$ 이면, 방정식 (4.2.6)의 해는 모두  $GF(2^m)$ 에 존재하므로 방정식 (4.2.5)의 해는  $x=1$  뿐이고  $C_{0,b}(\tau) = -1$ 이다.  $Tr_1^4\left(\frac{1}{\beta^{2k_1} + 1}\right) = 1$ 이면 트레이스 함수의 성질



(c)에 의하여  $Tr_1^s\left(\frac{1}{\beta^{2k_i}+1}\right)=0$ 이다. 그러면 방정식 (4.2.6)은  $GF(2^n)$ 에서 인수분해되고 집합  $S$ 에서 2개의 해를 갖는다. 따라서 방정식 (4.2.5)는 모두 3개의 해를 갖고  $C_{0,b}(\tau)=2 \cdot 2^m - 1$ 이다. 즉,  $B(\tau) \in GF(2^m)$ 인 경우  $C_{a,b}(\tau) \in \{-1, 2 \cdot 2^m - 1\}$ 이다.

(b)  $B(\tau) \notin GF(2^m)$ 인 경우

우선 방정식 (4.2.4)의 해가 존재하지 않는다면  $C_{0,b}(\tau) = -2^m - 1$ 이다.

그런데 방정식 (4.2.4)의 해가 존재한다면 그 해를  $w$ 라 두고  $w$  이외의 다른 해를 찾는다.  $B(\tau) \notin GF(2^m)$ 이므로  $w \neq 1$ 이다. 보조정리 2.5.2 (ii)에 의해  $S \setminus \{w\} = \left\{ \frac{uw+1}{u+w} \mid u \in GF(2^m) \right\}$ 이므로  $S \setminus \{1, w\}$ 의 원소인 또다른 해를 찾기 위해 방정식 (4.2.4)의  $x$ 에  $\frac{uw+1}{u+w}$ 을 대입한다. 그러면

$$\begin{aligned} (\overline{B(\tau)}w^3 + bw^2 + bw + B(\tau))u^3 + (\overline{B(\tau)}w + bw^3 + b + B(\tau)w)u^2 \\ + (\overline{B(\tau)}w^2 + b + bw^3 + B(\tau)w^2)u = \overline{B(\tau)} + bw + bw^2 + B(\tau)w^3 \end{aligned} \quad (4.2.7)$$

이고,  $w$ 는 방정식 (4.2.4)의 해이므로 식 (4.2.7)에서  $u^3$ 의 계수는 0이다. 따라서 식 (4.2.7)은 다음과 같이  $u$ 에 관한 이차방정식이 된다.

$$\begin{aligned} (\overline{B(\tau)}w + bw^3 + b + B(\tau)w)u^2 + (\overline{B(\tau)}w^2 + b + bw^3 + B(\tau)w^2)u \\ = \overline{B(\tau)} + bw + bw^2 + B(\tau)w^3 \end{aligned} \quad (4.2.8)$$

방정식 (4.2.8)은 0, 1 또는 2개의 해를 가질 수 있으므로 방정식 (4.2.4)의 해의 개수는 1, 2 또는 3이다. 즉,  $C_{0,b}(\tau) \in \{-1, 2^m - 1, 2 \cdot 2^m - 1\}$ 이다. ■

<정리 4.2.4>  $b \in GF(2^m)^*$  일 때 다음이 성립한다.

$$|\{\tau \mid C_{0,b}(\tau) = 2^m - 1, 0 \leq \tau \leq 2^n - 2\}| = 2^m$$

**증명.**  $C_{a,b}(\tau) = 2^m - 1$  인 경우는 방정식 (4.2.4)가 서로 다른 2의 해를 가질 때이므로 두 개 중 하나는 중복도가 2인 근이다.

우선  $B(\tau) = 0$  이면 중근이 존재할 수 없으므로  $B(\tau) \neq 0$  이어야 한다. 다음으로 도함수를 이용하여 어떤 경우에 중근이 존재하는지 확인하면  $C_{a,b}(\tau) = 2^m - 1$  의 발생횟수를 알 수 있다. 식 (4.2.4)의 도함수를 구하면  $\overline{B(\tau)}x^2 + b = 0$  이므로  $x^2 = \frac{b}{\overline{B(\tau)}}$  일 때 중근을 갖는다. 식 (4.2.4)의  $x^2$ 에  $\frac{b}{\overline{B(\tau)}}$  를 대입하면 다음과 같다.

$$B(\tau)\overline{B(\tau)} = b^2 \quad (4.2.9)$$

여기서  $B(\tau) \in GF(2^n)^*$ ,  $b \in GF(2^m)^*$  이므로  $B(\tau)$ 는  $\alpha^{k_2}$ , ( $0 < k_2 \leq 2^n - 2$ ) 로,  $b$ 는  $\alpha^{Qk_3}$ , ( $0 \leq k_3 \leq 2^m - 2$ ) 으로 각각 바꿔 쓸 수 있다. 그러면 식 (4.2.9)는

$$\begin{aligned} \alpha^{Qk_2} &= \alpha^{2Qk_3}, \\ Qk_2 &\equiv 2Qk_3 \pmod{2^n - 1}, \\ k_2 &\equiv 2k_3 \pmod{2^m - 1} \end{aligned}$$

이므로  $0 \leq l \leq 2^m$  에 대해  $k_2 = (2^m - 1) \cdot l + 2k_3$  이다. 따라서 방정식 (4.2.4)가 중근을 갖는 경우는  $2^m + 1$  번 존재한다.

그런데  $b = \overline{B(\tau)}$  인 경우, 방정식 (4.2.4)는 삼중근  $x = 1$  하나만 갖기 때문에  $0 \leq l \leq 2^m$  범위에서  $l = k_3$  인 경우는 제외된다. 따라서 중근을 갖는 경우는 모두  $2^m$  번 존재한다. ■

**<예제 4.2.5>**  $n = 8, \quad m = 4, \quad d = 31, \quad r = 7$  일 때 수열군  $S^7 = \{s_a^7(t) | a \in GF(2^4), 0 \leq t \leq 2^n - 2\}$  의 두 수열  $s_0^7(t) = Tr_1^4([Tr_4^8(\alpha^{31t})]^7)$  과  $s_{\beta^2}^7(t) = Tr_1^4([Tr_4^8(\beta^2 \alpha^t + \alpha^{31t})]^7)$  의 상호상관함수  $C_{0,\beta^2}(\tau)$  의 함숫값은  $C_{0,\beta^2}(\tau) \in \{-17, -1, 15, 31\}$  이고  $\tau$  의 값이 22, 24, 60, 77, 86, 97, 101, 129, 143, 171, 175, 186, 195, 212, 248, 250 일 때  $C_{0,\beta^2}(\tau) = 15$  이다. 즉  $C_{0,\beta^2}(\tau) = 15$  인 경우는 모두 16 번 발생한다. 그림 7은  $0 \leq \tau \leq 254$  에 대한  $C_{0,\beta^2}(\tau)$  의 함숫값을  $15 \times 17$  배열로 나타낸 것이다.



그림 7.  $C_{0,\beta^2}(\tau)$  값의  $15 \times 17$  배열

### 4.3. $d=2^{m-1}(3 \cdot 2^m - 1)$ 일 때 새로운 수열의 상호상관 함숫값

이 절에서는 수열군  $S^r$ 에서  $d=2^{m-1}(3 \cdot 2^m - 1)$ 에 의해 생성된 수열의 상호상관 함숫값의 범위와 특별한 경우 상호상관 함숫값의 발생빈도를 분석한다. 제안된 수열군  $S^r$ 은 Choi 등의 연구 결과와 같은 범위의 상호상관 함숫값을 갖는다([3]).

<보조정리 4.3.1[21]>  $m|n$ 을 만족하는  $m, n$ 과  $\alpha \in GF(2^n)$ 에 대하여  $Tr_m^n(\alpha)=0$ 일 필요충분조건은  $\alpha = x^{2^m} + x$ 를 만족하는  $GF(2^n)$ 의 원소  $x$ 가 존재한다는 것이다.

<예제 4.3.2>  $n=4, m=1$ 일 때  $\alpha^4 = \alpha + 1$ 을 만족하는  $GF(2^4)$ 의 원시 원소  $\alpha$ 에 대하여  $Tr_1^4(\alpha^4)=0$ 이다. 이때  $x^2 + x = \alpha^4$ 의 해는  $x = \alpha^6$ 이다.

보조정리 4.3.1과 트레이스 함수의 성질을 이용하면 이차방정식

$$ax^2 + bx + c = 0, \quad a, b, c \in GF(2^n) \quad (4.3.1)$$

을 만족하는 해의 개수를 구할 수 있다.

(i)  $b \neq 0$  :  $y = ab^{-1}x, \kappa = acb^{-2}$ 이라 두면 식 (4.3.1)은  $y^2 + y = \kappa$ 가 된다. 보조정리 4.3.1에 의하여  $y^2 + y = \kappa$ 의 해가  $GF(2^n)$ 에 존재할 필요충분조건은  $Tr_1^n(\kappa)=0$ 이다. 이차방정식  $y^2 + y = \kappa$ 의 해가 존재할 경우 방정식 (4.3.1)의 해는  $x = ba^{-1}y, ba^{-1}(y+1)$ 이다.

(ii)  $b=0$  :  $\kappa = ca^{-1}$ 이라 두면 식 (4.3.1)은  $x^2 = \kappa$ 가 되고 방정식  $x^2 = \kappa$ 는  $x = \kappa^{2^{n-1}}$ 을 중근으로 갖는다.

<예제 4.3.3>  $\alpha^4 = \alpha + 1$  을 만족하는  $GF(2^4)$  의 원시원소  $\alpha$  에 대하여 이차방정식  $x^2 + \alpha^4 x + \alpha = 0$  의 해를 구해보자.

$y = \alpha^{-4} x = \alpha^{11} x$ ,  $\gamma = \alpha \cdot \alpha^{-8} = \alpha^8$  라 두면 이차방정식  $x^2 + \alpha^4 x + \alpha = 0$  는  $y^2 + y = \alpha^8$  이 된다.  $Tr_1^4(\alpha^8) = 0$  이므로 방정식  $y^2 + y = \alpha^8$  의 해는  $GF(2^4)$  에 존재한다.  $y = \alpha^{12}$  은  $y^2 + y = \alpha^8$  을 만족하므로 방정식  $y^2 + y = \alpha^8$  의 해는  $y = \alpha^{12}$  또는  $y = \alpha^{12} + 1 = \alpha^{11}$  이다.  $x = \alpha^4 y$  로부터 방정식  $x^2 + \alpha^4 x + \alpha = 0$  의 해는  $x = \alpha$  또는  $x = 1$  이다.

<정리 4.3.4>  $n = 2m$  일 때,  $k \in GF(2^m)^*$  에 대하여  $R = \{x \in S \mid x^2 + kx + 1 = 0\}$  으로 정의하면 다음이 성립한다.

$$|R| = 0 \text{ 또는 } |R| = 2$$

증명.  $k \in GF(2^m)^*$  일 때, 집합  $S$ 의 원소이면서 이차방정식

$$x^2 + kx + 1 = 0 \quad (4.3.2)$$

을 만족하는 서로 다른  $x$ 는 최대 2개까지 존재할 수 있다.  $|R| = 1$ 인 경우는 방정식 (4.3.2)가 중근을 가지면서 그것이 집합  $S$ 의 원소일 때이거나 방정식 (4.3.2)가 2개의 해를 갖지만 그 중 하나만 집합  $S$ 의 원소일 때이다.

(i) 방정식 (4.3.2)가 중근을 가지면서 그것이 집합  $S$ 의 원소인 경우 :  $k \in GF(2^m)^*$  이므로 식 (4.3.2)는 완전제곱식이 될 수 없다. 따라서 중근을 갖는 경우는 발생하지 않는다.

(ii) 방정식 (4.3.2)가 서로 다른 2개의 해를 갖지만 그 중 하나만 집합  $S$ 의 원소인 경우 :  $k \in GF(2^m)^*$  일 때,  $x = 1 \in S$ 는 방정식 (4.3.2)의 해가 아니다. 집합  $S$ 의 원소  $x_1$ 이 방정식 (4.3.2)의 해라면

$$\overline{x_1}^2 + k\overline{x_1} + 1 = \overline{x_1^2 + kx_1 + 1} = 0$$

이므로  $\overline{x_1} \in S$ 도 방정식 (4.3.2)의 해이다. 한편  $k \neq 0$ 이므로  $x_1 \neq \overline{x_1}$ 이다. 따라서 방정식 (4.3.2)가 서로 다른 2개의 해를 갖지만 그 중 하나만 집합  $S$ 의 원소인 경우는 발생하지 않는다.

(i), (ii)에 의하여  $|R|=1$ 인 경우는 발생하지 않으므로  $|R|=0$  또는  $|R|=2$ 이다. ■

<정리 4.3.5> 수열군  $S^r$ 에서  $C_{a,b}(\tau)$ 는 5값 함수이며

$$C_{a,b}(\tau) \in \{-2^m - 1, -1, 2^m - 1, 2 \cdot 2^m - 1, 3 \cdot 2^m - 1\}$$

이다.

증명. 수열군  $S^r$ 의 두 수열  $s_a^r(t)$ ,  $s_b^r(t)$ 에 대한 상호상관함수는

$$\begin{aligned} C_{a,b}(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{s_a^r(t+\tau) + s_b^r(t)} \\ &= \sum_{t=0}^{2^n-2} (-1)^{Tr_1^m([Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r + [Tr_m^n(b\alpha^t + \alpha^{dt})]^r)} \end{aligned}$$

이다. 여기서  $Q=2^m+1$ 로 두고  $t=t_1Q+t_2$ , ( $0 \leq t_1 \leq 2^m-2$ ,  $0 \leq t_2 \leq 2^m$ ),  $\alpha^Q = \beta$ 라 두면  $\beta \in GF(2^m)^*$ 이다. 그러면  $\gcd(r, 2^m-1)=1$ 이므로

$$\{\beta^{t_1r} \mid 0 \leq t_1 \leq 2^m-2\} = GF(2^m)^*$$

이다. 그러므로

$$\begin{aligned} s_a^r(t+\tau) + s_b^r(t) &= Tr_1^m(\beta^{t_1r} \{ [Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{d(t_2+\tau)})]^r + [Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})]^r \}) \\ &= Tr_1^m(\eta H(t_2, \tau, r)) \end{aligned}$$

여기서  $H(t, \tau, r) = [Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r + [Tr_m^n(b\alpha^t + \alpha^{dt})]^r$ 이고  $\eta \in GF(2^n)^*$ 이다. 따라서

$$\begin{aligned} C_{a,b}(\tau) &= \sum_{\eta \in GF(2^m)} \sum_{t_2=0}^{2^m-1} (-1)^{Tr_1^m(\eta H(t_2, \tau, r))} - (2^m + 1) \\ &= \{N(t_2, \tau, r) - 1\}2^m - 1 \end{aligned}$$

이다. 여기서  $N(t, \tau, r) = |\{t | H(t, \tau, r) = 0, 0 \leq t \leq 2^m-1\}|$ 이다.  $\gcd(r, 2^m - 1) = 1$ 이므로 보조정리 4.2.2에 의하여  $N(t_2, \tau, r)$ 의 값을 구하기 위해  $H(t_2, \tau, 1) = 0$ 을 만족하는  $t_2$ 의 개수를 구한다.

$$H(t_2, \tau, 1) = 0 \Leftrightarrow Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{d(t_2+\tau)}) = Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})$$

이므로

$$Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{d(t_2+\tau)} + b\alpha^{t_2} + \alpha^{dt_2}) = Tr_m^n((a\alpha^\tau + b)\alpha^{t_2} + (\alpha^{d\tau} + 1)\alpha^{dt_2}) = 0$$

이다. 여기서  $A(\tau) = a\alpha^\tau + b$ ,  $B(\tau) = \alpha^{d\tau} + 1$ 로 두고 식 (2.5.1)을 이용하여  $\alpha = \delta\gamma$ 로 표현하면  $d \equiv 1 \pmod{2^m-1}$ ,  $d \equiv 2 \pmod{2^m+1}$ 이므로

$$\begin{aligned} Tr_m^n(A(\tau)\alpha^{t_2} + B(\tau)\alpha^{dt_2}) &= B(\tau)\alpha^{dt_2} + A(\tau)\alpha^{t_2} + \overline{B(\tau)}\alpha^{2^m dt_2} + \overline{A(\tau)}\alpha^{2^m t_2} \\ &= B(\tau)\delta^{dt_2}\gamma^{dt_2} + A(\tau)\delta^{t_2}\gamma^{t_2} + \overline{B(\tau)}\delta^{2^m dt_2}\gamma^{2^m dt_2} + \overline{A(\tau)}\delta^{2^m t_2}\gamma^{2^m t_2} \\ &= B(\tau)\delta^{t_2}\gamma^{2t_2} + A(\tau)\delta^{t_2}\gamma^{t_2} + \overline{B(\tau)}\delta^{t_2}\gamma^{-2t_2} + \overline{A(\tau)}\delta^{t_2}\gamma^{-t_2} \\ &= 0 \end{aligned}$$

이다.  $\gamma^{t_2} = x$ 로 두면  $x \in S$ 이고  $\delta^{t_2} \neq 0$ 이므로

$$B(\tau)x^4 + A(\tau)x^3 + \overline{A(\tau)}x + \overline{B(\tau)} = 0 \quad (4.3.3)$$

이다. 방정식 (4.3.3)은  $x$ 에 관한 4차식이므로 최대 4개의 해가 존재할 수 있다. 즉,  $N(t_2, \tau, r) = 0, 1, 2, 3, 4$ 이므로  $C_{a,b}(\tau) \in \{-2^m - 1, -1, 2^m - 1, 2 \cdot 2^m - 1, 3 \cdot 2^m - 1\}$ 이다. ■



특별히  $a=0$ ,  $b \neq 0$  일 때, 위상이동차  $\tau = Q\tau_1$ , ( $0 \leq \tau_1 \leq 2^m - 2$ )에 대한  $C_{0,b}(\tau)$ 의 분포는 다음과 같다.

**<정리 4.3.6>** 수열군  $S^r$ 에서 위상이동차  $\tau = Q\tau_1$ , ( $0 \leq \tau_1 \leq 2^m - 2$ ),  $b \neq 0$  일 때  $C_{0,b}(\tau)$ 의 발생빈도는 다음과 같다.

$$Tr_1^m\left(\frac{1}{b}\right) = 1 : \begin{cases} C_{0,b}(\tau) = 2 \cdot 2^m - 1, & 2^{m-1} - 1 \text{ times} \\ C_{0,b}(\tau) = -1 & , 2^{m-1} \text{ times} \end{cases},$$

$$Tr_1^m\left(\frac{1}{b}\right) = 0 : \begin{cases} C_{0,b}(\tau) = 2 \cdot 2^m - 1, & 2^{m-1} \text{ times} \\ C_{0,b}(\tau) = -1 & , 2^{m-1} - 1 \text{ times} \end{cases}$$

**증명.** 첫 번째 단계로, 발생 가능한 상호상관 함숫값을 구한다.

$a=0$ ,  $b \neq 0$  일 때 식 (4.3.3)의  $A(\tau)=b$ 이고,  $\tau = Q\tau_1$ , ( $0 \leq \tau_1 \leq 2^m - 2$ )이므로  $\overline{B(\tau)}=B(\tau)$ 이다. 따라서 식 (4.3.3)은

$$B(\tau)x^4 + bx^3 + bx + B(\tau) = 0 \quad (4.3.4)$$

이다. 방정식 (4.3.4)는 최대 4개의 해를 가질 수 있고

$$B(\tau)x^4 + bx^3 + bx + B(\tau) = (x+1)^2(B(\tau)x^2 + bx + B(\tau)) = 0$$

이므로  $x=1$  이외의 다른 해의 개수는 방정식

$$B(\tau)x^2 + bx + B(\tau) = 0 \quad (4.3.5)$$

이 집합  $S$ 에서 몇 개의 해를 갖는지 확인하면 알 수 있다.  $B(\tau) \in GF(2^m)$ ,  $b \in GF(2^m)^*$ 이므로 정리 4.3.4에 의하여 방정식 (4.3.5)는  $GF(2^n)$ 에서 항상 2개의 해를 갖는다. 이제 2개의 해가 모두 집합  $S$ 의 원소인지 확인해야 한다.

(i)  $Tr_1^m\left(\frac{B(\tau)^2}{b^2}\right) = 0$ 이면 방정식 (4.3.5)의 해는 모두  $GF(2^m) \setminus \{1\}$ 에

존재한다. 그러나 보조정리 2.5.1에 의해  $GF(2^m) \cap S = \{1\}$  이므로 이 경우 방정식 (4.3.5)의 해는 모두 집합  $S$ 의 원소가 아니다. 따라서 방정식 (4.3.4)의 해는 중근  $x=1$  하나이므로  $C_{0,b}(\tau)=-1$ 이다.

(ii)  $Tr_1^m\left(\frac{B(\tau)^2}{b^2}\right)=1$ 이면 방정식 (4.3.5)의 두 해는 모두  $GF(2^n) \setminus GF(2^m)$ 에 존재하고, 근과 계수의 관계에 의해 두 해는 모두 집합  $S$ 의 원소이다. 따라서 중근  $x=1$ 을 포함하면 방정식 (4.3.4)의 해는 모두 3개, 즉  $N(t_2, \tau, r)=3$ 이므로  $C_{0,b}(\tau)=2 \cdot 2^m - 1$ 이다.

(i), (ii)에 의해  $\tau=Q\tau_1$ ,  $(0 \leq \tau_1 \leq 2^m-2)$ 일 때  $C_{0,b}(\tau)$ 의 값은  $-1$ ,  $2 \cdot 2^m - 1$ 만 가능하다.

두 번째 단계로,  $C_{0,b}(\tau)=-1$ ,  $C_{0,b}(\tau)=2 \cdot 2^m - 1$ 의 발생빈도를 분석한다.

$Tr_1^m\left(\frac{B(\tau)^2}{b^2}\right)$ 에서  $B(\tau) \neq 1$ 이므로  $\frac{B(\tau)}{b} \neq \frac{1}{b}$ 이다. 따라서  $Tr_1^m\left(\frac{B(\tau)^2}{b^2}\right)$ 의 값 중 0과 1의 개수는  $Tr_1^m\left(\frac{1}{b^2}\right)$ 의 값에 따라 달라지고  $Tr_1^m\left(\frac{1}{b^2}\right)=Tr_1^m\left(\frac{1}{b}\right)$ 이므로  $Tr_1^m\left(\frac{1}{b}\right)$ 의 값을 생각하면 된다.

(a)  $Tr_1^m\left(\frac{1}{b}\right)=0$  :  $Tr_1^m\left(\frac{B(\tau)}{b}\right)$ 의 값 중 0인 것이 하나 빠지기 때문에  $Tr_1^m\left(\frac{B(\tau)}{b}\right)=\begin{cases} 0, & 2^{m-1}-1 \text{ times} \\ 1, & 2^{m-1} \text{ times} \end{cases}$ 이다. 따라서  $\tau=Q\tau_1$ ,  $(0 \leq \tau_1 \leq 2^m-2)$ 일 때,  $C_{0,b}(\tau)=-1$ 은  $2^{m-1}-1$ 번,  $C_{0,b}(\tau)=2 \cdot 2^m - 1$ 은  $2^{m-1}$ 번 나타난다.

(b)  $Tr_1^m\left(\frac{1}{b}\right)=1$  :  $Tr_1^m\left(\frac{B(\tau)}{b}\right)$ 의 값 중 1인 것이 하나 빠지기 때문에  $Tr_1^m\left(\frac{B(\tau)}{b}\right)=\begin{cases} 0, & 2^{m-1} \text{ times} \\ 1, & 2^{m-1}-1 \text{ times} \end{cases}$ 이다. 따라서  $\tau=Q\tau_1$ ,  $(0 \leq \tau_1 \leq 2^m-2)$ 일 때  $C_{0,b}(\tau)=-1$ 은  $2^{m-1}$ 번,  $C_{0,b}(\tau)=2 \cdot 2^m - 1$ 은  $2^{m-1}-1$ 번 나타난다. ■

<예제 4.3.7>  $n=8$ ,  $m=4$  이고  $a=0$ ,  $b=\beta$  일 때,  $\tau=17\tau_1$ ,  $(0 \leq \tau_1 \leq 14)$ 에 대한  $C_{0,\beta}(\tau)$  값의 분포를 살펴보자.

$Tr_1^m\left(\frac{1}{b}\right) = Tr_1^m(\beta^{14}) = 1$  이어서  $Tr_1^m\left(\frac{B(\tau)}{b}\right)$ 의 값 중 1인 것이 하나 빠지므로  $Tr_1^m\left(\frac{B(\tau)}{b}\right) = 1$ 은 7번,  $Tr_1^m\left(\frac{B(\tau)}{b}\right) = 0$ 은 8번 발생한다. 따라서 해의 개수가 3개인 것은 7번, 해의 개수가 1개인 것은 8번 존재한다.

$\tau$  값에 따른  $C_{0,\beta}(\tau)$  값을  $(2^m - 1) \times (2^m + 1)$  배열로 나타내면  $\tau=17\tau_1$ ,  $(0 \leq \tau_1 \leq 14)$ 일 때  $C_{0,\beta}(\tau)$  값은 그림 8과 같이 첫 열에 분포하고  $C_{0,\beta}(\tau)=31$ 이 7개,  $C_{0,\beta}(\tau)=-1$ 이 8개 존재한다.



|    |     |     |     |     |     |    |     |     |     |     |    |     |     |     |     |     |
|----|-----|-----|-----|-----|-----|----|-----|-----|-----|-----|----|-----|-----|-----|-----|-----|
| 1  | -17 | -17 | 15  | -1  | -1  | 15 | -17 | 15  | -17 | -17 | -1 | -17 | -17 | -1  | 47  | -17 |
| 31 | -1  | -1  | -17 | -1  | -1  | 47 | -17 | -1  | 15  | -1  | -1 | -17 | -1  | 15  | -17 | -1  |
| 31 | 15  | -17 | -1  | -1  | -1  | 15 | -17 | -1  | -1  | -1  | 15 | -1  | -17 | 15  | -1  | 15  |
| 31 | -1  | -17 | -17 | -17 | 15  | -1 | -17 | -1  | -17 | -1  | 15 | 15  | -1  | -17 | -17 | -1  |
| -1 | -1  | -17 | -1  | 15  | 15  | 15 | -1  | -17 | 15  | -17 | 15 | -1  | -1  | -1  | -17 | -1  |
| 31 | -1  | -1  | -1  | -17 | 15  | 15 | 15  | -17 | -17 | 15  | 15 | -1  | -1  | -17 | -17 | -1  |
| 31 | -17 | -17 | -1  | 15  | -17 | 47 | -17 | 15  | -1  | -17 | 47 | -1  | -17 | -1  | -1  | -17 |
| -1 | -17 | -1  | 15  | -17 | -17 | -1 | 47  | -17 | 15  | -17 | 15 | 15  | -1  | -17 | -17 | -17 |
| -1 | 15  | -1  | -17 | 15  | -17 | 15 | -1  | -17 | -1  | -17 | -1 | 15  | -17 | -1  | -1  | 15  |
| 31 | 15  | -1  | -17 | -1  | -1  | -1 | -17 | 15  | -1  | -17 | 15 | 15  | 15  | 15  | -1  | 15  |
| -1 | -17 | 15  | -17 | -17 | -17 | -1 | -1  | -1  | -1  | -1  | 15 | -17 | -17 | -17 | -1  | -17 |
| 31 | -17 | -17 | -17 | 15  | -17 | -1 | -1  | -17 | -17 | 15  | 47 | -17 | 15  | -17 | 15  | -17 |
| -1 | -1  | -17 | 15  | -17 | -17 | 15 | -1  | 15  | -17 | -17 | -1 | -17 | -1  | -17 | -17 | -1  |
| -1 | 15  | 15  | -1  | -1  | -1  | 15 | -17 | -17 | 15  | 47  | 15 | -1  | -17 | -17 | -17 | 15  |
| -1 | -17 | 47  | 15  | -17 | 15  | 15 | 15  | -1  | -17 | -1  | -1 | -17 | 15  | 15  | 15  | -17 |

그림 8.  $C_{0,\beta}(\tau)$ ,  $(0 \leq \tau \leq 2^n - 2)$ 의 배열

<예제 4.3.9>  $n=8$ ,  $m=4$  일 때  $a=0$ 으로 두고  $b$ 를 변화시켰을 때  $\tau=Q\tau_1$ ,  $(0 \leq \tau_1 \leq 14)$ 에 대한  $C_{0,b}(\tau)$  값의 분포는 다음과 같다.

$C_{0,b}(\tau)=31$ 이 8개(또는  $C_{0,b}(\tau)=-1$ 이 7개)인 경우 :

$$b=1, \beta^5, \beta^7, \beta^{10}, \beta^{11}, \beta^{13}, \beta^{14} \quad (7 \text{ 번}),$$

$C_{0,b}(\tau)=31$ 이 7개(또는  $C_{0,b}(\tau)=-1$ 이 8개)인 경우 :

$$b=\beta, \beta^2, \beta^3, \beta^4, \beta^6, \beta^8, \beta^9, \beta^{12} \quad (8 \text{ 번}).$$

#### 4.4. $\begin{cases} d \equiv 1 \pmod{2^m-1} \\ d \equiv 2^k \pmod{2^m+1} \end{cases}$ 일 때 새로운 수열의 상호상관 함숫값

R. McEliece([22])에 의하면  $Tr_{\gcd(l,m)}^m(a)=0$  일 때

$$|\{x | x^{2^l} + x = a, a \in GF(2^m)\}| = 2^{\gcd(l,m)} \quad (4.4.1)$$

이다.

<보조정리 4.4.1>  $m=2k$ ,  $a \in GF(2^m)$  일 때 방정식  $u^{2^k} + au = 0$  에 대해

$$|\{u \in GF(2^m) | u^{2^k} + au = 0\}| = \begin{cases} 1 & , a \neq \beta^{(2^k-1)i} \\ 2^k & , a = \beta^{(2^k-1)i} \end{cases}, i = 0, 1, 2, \dots, 2^k$$

단  $\beta$  는  $GF(2^m)$  의 원시원소이다.

증명.  $n=2m$ ,  $m=2k$ ,  $a \in GF(2^m)$  일 때 방정식

$$u^{2^k} + au = 0 \quad (4.4.2)$$

의 해의 개수를 구한다.

( i )  $a = \beta^{(2^k-1)i}$ ,  $i = 0, 1, 2, \dots, 2^k$  꼴인 경우,  $u = a_1 u_1$  으로 두면

$$u^{2^k} + \beta^{(2^k-1)i} u = (a_1 u_1)^{2^k} + \beta^{(2^k-1)i} (a_1 u_1) = a_1^{2^k} u_1^{2^k} + \beta^{(2^k-1)i} a_1 u_1 = 0$$

이고  $a_1 \neq 0$  이므로  $a_1^{2^k}$  으로 양변을 나누면  $u_1^{2^k} + (\beta^i a_1^{-1})^{(2^k-1)} u_1 = 0$  이다.

여기서  $a_1 = \beta^i$  으로 두면 식 (4.4.2)는

$$u_1^{2^k} + u_1 = 0 \quad (4.4.3)$$

이 되고

$$|\{u \in GF(2^m) | u^{2^k} + au = 0\}| = |\{u_1 \in GF(2^m) | u_1^{2^k} + u_1 = 0\}|$$

이다. 식 (4.4.1)에 의해 방정식 (4.4.3)은  $2^{\gcd(k,m)} = 2^k$  개의 근을 갖는다. 따라서 방정식 (4.4.2)도  $2^k$  개의 근을 갖는다.

(ii)  $a \neq \beta^{(2^k-1)i}$ ,  $i = 0, 1, 2, \dots, 2^k$  꼴인 경우,  $u^{2^k} + au = u(u^{2^k-1} + a) = 0$  이므로  $u = 0$  이거나  $u^{2^k-1} = a$  이다. 그런데  $a \neq \beta^{(2^k-1)i}$  이므로  $u^{2^k-1} = a$  를 만족하는  $u$  는 존재하지 않는다. 따라서 방정식 (4.4.2)는 한 개의 해  $u = 0$  만 갖는다. ■

<정리 4.4.2>  $n = 2m$ ,  $m = 2k$  일 때,  $A(\tau) = a\alpha^\tau + b$ ,  $B(\tau) = \alpha^{d\tau} + 1$  에 대하여  $a \neq b$  이거나  $\tau \neq 0$  일 때, 집합  $S$ 의 원소이면서 다음 방정식

$$B(\tau)x^{2^k+1} + \overline{A(\tau)}x^{2^k} + A(\tau)x + \overline{B(\tau)} = 0 \quad (4.4.4)$$

을 만족하는 해의 개수는 0, 1, 2 또는  $2^k + 1$  이다.

**증명.**  $A(\tau) + B(\tau) \in GF(2^m)$  인 경우와  $A(\tau) + B(\tau) \in GF(2^n) \setminus GF(2^m)$  인 경우로 나누어 증명한다.

(i)  $A(\tau) + B(\tau) \in GF(2^m)$  일 때  
 $A(\tau) + B(\tau) \in GF(2^m)$  이면  $A(\tau) + B(\tau) = \overline{A(\tau) + B(\tau)}$  이므로

$$B(\tau) + \overline{A(\tau)} + A(\tau) + \overline{B(\tau)} = 0 \quad (4.4.5)$$

이다. 이것은 식 (4.4.4)에  $x = 1$  을 대입한 것과 같으므로  $x = 1$  은 방정식 (4.4.4)의 해이다.

이제  $S$ 의 원소 중 1이 아닌 또다른 해가 있는지 확인한다. 보조정리 2.5.2 (i)에 의하여  $z \in GF(2^n) \setminus GF(2^m)$  에 대하여 1이 아닌 집합  $S$ 의

원소는  $u \in GF(2^m)$  에 대하여  $\frac{\bar{z}+u}{z+u}$  로 유일하게 표현할 수 있다. 따라서

식 (4.4.4)의  $x$  에  $\frac{\bar{z}+u}{z+u}$  을 대입하면

$$B(\tau) \left( \frac{\bar{z}+u}{z+u} \right)^{2^k+1} + \overline{A(\tau)} \left( \frac{\bar{z}+u}{z+u} \right)^{2^k} + A(\tau) \left( \frac{\bar{z}+u}{z+u} \right) + \overline{B(\tau)} = 0$$

이다. 양변에  $(z+u)^{2^k+1}$  을 곱하고 정리하면

$$\begin{aligned} & (A(\tau) + B(\tau) + \overline{A(\tau)} + \overline{B(\tau)})u^{2^k+1} + (A(\tau) + B(\tau))(z + \bar{z})u^{2^k} \\ & + (\overline{A(\tau)} + \overline{B(\tau)})(z + \bar{z})^{2^k}u = z^{2^k}(A(\tau)\bar{z} + \overline{B(\tau)}z) + \bar{z}^{2^k}(\overline{A(\tau)}z + B(\tau)\bar{z}) \end{aligned} \quad (4.4.6)$$

이다. 그런데  $A(\tau) + B(\tau) \in GF(2^m)$  이므로 식 (4.4.6)은 식 (4.4.7)과 같다.

$$\begin{aligned} & (A(\tau) + B(\tau))(z + \bar{z})u^{2^k} + (\overline{A(\tau)} + \overline{B(\tau)})(z + \bar{z})^{2^k}u \\ & = z^{2^k}(A(\tau)\bar{z} + \overline{B(\tau)}z) + \bar{z}^{2^k}(\overline{A(\tau)}z + B(\tau)\bar{z}) \end{aligned} \quad (4.4.7)$$

$i_a)$   $A(\tau) + B(\tau) = 0$  이면 식 (4.4.7)은

$$(\overline{A(\tau)} + A(\tau))(z + \bar{z})^{2^k}u = z^{2^k}(A(\tau)\bar{z} + \overline{A(\tau)}z) + \bar{z}^{2^k}(\overline{A(\tau)}z + A(\tau)\bar{z}) \quad (4.4.8)$$

이고 이것은  $u$  에 대한 일차방정식이다. 이때  $A(\tau) = 0$  이면  $B(\tau) = 0$  이므로  $\tau = 0$ ,  $a = b$  가 되어 가정에 모순이다. 따라서 동시에  $A(\tau) = 0$ ,  $B(\tau) = 0$  이 될 수는 없다.

먼저  $A(\tau) \in GF(2^m)$  이면  $u$  의 계수가 0 이므로 식 (4.4.8)은 다음과 같다.

$$0 \cdot u = A(\tau)(z + \bar{z})^{2^k+1} \quad (4.4.9)$$

여기서  $A(\tau)(z + \bar{z})^{2^k+1} \neq 0$  이므로 식 (4.4.9)를 만족하는  $u$  는 존재하지 않는다. 따라서 이 경우 방정식 (4.4.4)의 해는 1개이다.



다음으로  $A(\tau) \notin GF(2^m)$  이면 방정식 (4.4.8)은 반드시 한 개의 해를 갖기 때문에 방정식 (4.4.4)는 2개의 해를 갖는다.

$i_b)$   $A(\tau) + B(\tau) \neq 0$ 이면 식 (4.4.7)은

$$u^{2^k} + C_1(\tau)u = C_2(\tau) \quad (4.4.10)$$

여기서  $C_1(\tau) = \frac{\overline{A(\tau)} + B(\tau)}{A(\tau) + B(\tau)}(z + \bar{z})^{2^k - 1}$ ,

$C_2(\tau) = \frac{z^{2^k}(A(\tau)\bar{z} + \overline{B(\tau)}z) + \bar{z}^{2^k}(\overline{A(\tau)}z + B(\tau)\bar{z})}{(A(\tau) + B(\tau))(z + \bar{z})}$  이다.  $C_1(\tau), C_2(\tau) \in GF(2^m)$  이

므로 방정식 (4.4.10)의 해가 존재하지 않는 경우 방정식 (4.4.4)는 해를 하나만 갖는다. 그러나 방정식 (4.4.10)의 해가 존재한다면 정리 2.4.5와 보조정리 4.4.1에 의해 해의 개수는 1개 또는  $2^k$ 개다. 따라서 방정식 (4.4.4)는 2개 또는  $2^k + 1$ 개의 해를 갖는다.

(ii)  $A(\tau) + B(\tau) \notin GF(2^m)$  일 때

$ii_a)$  방정식 (4.4.4)의 해가 없으면 해의 개수는 0이다.

$ii_b)$  방정식 (4.4.4)의 해가 존재한다면 그 해를  $w$ 라 두자. 이때  $A(\tau) + B(\tau) \notin GF(2^m)$  이므로  $w \neq 1$ 이다. 이제  $w$  이외의 다른 해가 존재한다면  $\{GF(2^n) \setminus GF(2^m)\} \cap (S \setminus \{w\})$ 의 원소이므로 보조정리 2.5.2 (ii)에 의해  $GF(2^m)$ 의 원소  $u$ 를 이용하여  $w \frac{\bar{w} + u}{w + u}$ 로 표현할 수 있다.

$A(\tau) + B(\tau) \notin GF(2^m)$  일 때  $x = 1$ 이 해가 될 수 없으므로  $u \neq 1$ 이다.

$w \frac{\bar{w} + u}{w + u}$ 를 식 (4.4.4)의  $x$ 에 대입하면 다음과 같다.

$$B(\tau) \left( w \frac{\bar{w} + u}{w + u} \right)^{2^k + 1} + \overline{A(\tau)} \left( w \frac{\bar{w} + u}{w + u} \right)^{2^k} + A(\tau) \left( w \frac{\bar{w} + u}{w + u} \right) + \overline{B(\tau)} = 0,$$

$$B(\tau) w^{2^k + 1} (\bar{w} + u)^{2^k + 1} + \overline{A(\tau)} w^{2^k} (\bar{w} + u)^{2^k} (w + u)$$



$$+ A(\tau)w(\bar{w}+u)(w+u)^{2^k} + \overline{B(\tau)}(w+u)^{2^k+1} = 0,$$

$$B(\tau)w^{2^k+1}(\bar{w}+u)^{2^k}(\bar{w}+u) + \overline{A(\tau)}w^{2^k}(\bar{w}+u)^{2^k}(w+u)$$

$$+ A(\tau)w(\bar{w}+u)(w+u)^{2^k} + \overline{B(\tau)}(w+u)^{2^k}(w+u) = 0,$$

$$(B(\tau)w^{2^k+1} + \overline{A(\tau)}w^{2^k} + A(\tau)w + \overline{B(\tau)})u^{2^k+1}$$

$$+ (B(\tau)w^{2^k+1}\bar{w} + \overline{A(\tau)}w^{2^k+1} + A(\tau)w\bar{w} + \overline{B(\tau)}w)u^{2^k}$$

$$+ (B(\tau)w^{2^k+1}\bar{w}^{2^k} + \overline{A(\tau)}w^{2^k}\bar{w}^{2^k} + A(\tau)w^{2^k+1} + \overline{B(\tau)}w^{2^k})u$$

$$= B(\tau)w^{2^k+1}\bar{w}^{2^k+1} + \overline{A(\tau)}w^{2^k+1}\bar{w}^{2^k} + A(\tau)w^{2^k+1}\bar{w} + \overline{B(\tau)}w^{2^k+1}.$$

$w$ 는 방정식 (4.4.4)의 해이므로  $u^{2^k+1}$ 의 계수가 0이고  $w\bar{w}=1$ 임을 이용하면

$$(\overline{A(\tau)}w^{2^k+1} + B(\tau)w^{2^k} + \overline{B(\tau)}w + A(\tau))u^{2^k}$$

$$+ (A(\tau)w^{2^k+1} + \overline{B(\tau)}w^{2^k} + B(\tau)w + \overline{A(\tau)})u$$

$$= \overline{B(\tau)}w^{2^k+1} + A(\tau)w^{2^k} + \overline{A(\tau)}w + B(\tau)$$

이다. 이를

$$Au^{2^k} + Bu = C \tag{4.4.11}$$

로 나타내자. 먼저 방정식 (4.4.4)의 해  $w$ 에 대하여  $A=B=C=0$ 이면

$$B(\tau)w^{2^k+1} + \overline{A(\tau)}w^{2^k} + A(\tau)w + \overline{B(\tau)} = 0,$$

$$\overline{A(\tau)}w^{2^k+1} + B(\tau)w^{2^k} + \overline{B(\tau)}w + A(\tau) = 0,$$

$$A(\tau)w^{2^k+1} + \overline{B(\tau)}w^{2^k} + B(\tau)w + \overline{A(\tau)} = 0,$$

$$\overline{B(\tau)}w^{2^k+1} + A(\tau)w^{2^k} + \overline{A(\tau)}w + B(\tau) = 0$$

이 성립하므로 이 식들을 모두 더하면

$$(A(\tau) + B(\tau) + \overline{A(\tau)} + \overline{B(\tau)})(w+1)^{2^k+1} = 0 \tag{4.4.12}$$

이다. 그런데  $w+1 \neq 0$ ,  $A(\tau)+B(\tau) \notin GF(2^m)$  이므로

$$(A(\tau)+B(\tau)+\overline{A(\tau)}+\overline{B(\tau)})(w+1)^{2^k+1} \neq 0$$

이다. 이것은 식 (4.4.12)에 모순이므로  $A, B, C$ 는 동시에 0이 될 수 없다.

우선  $A=0$ 일 때, 방정식 (4.4.11)의 해의 개수는 0 또는 1이다.

다음으로  $A \neq 0$ 일 때,

$$\begin{aligned}\overline{A} &= A(\tau)\overline{w^{2^k+1}} + \overline{B(\tau)}\overline{w^{2^k}} + B(\tau)\overline{w} + \overline{A(\tau)} \\ &= A(\tau)w^{-2^k-1} + \overline{B(\tau)}w^{-2^k} + B(\tau)w^{-1} + \overline{A(\tau)} \\ &= w^{-2^k-1}(\overline{A(\tau)}w^{2^k+1} + B(\tau)w^{2^k} + \overline{B(\tau)}w + A(\tau)) \\ &= w^{-2^k-1} \cdot A\end{aligned}$$

이고 같은 방법으로  $\overline{B} = w^{-2^k-1}B$ ,  $\overline{C} = w^{-2^k-1}C$ 이므로  $\frac{B}{A}, \frac{C}{A} \in GF(2^m)$  이

다. 따라서 식 (4.4.11)은

$$u^{2^k} + \frac{B}{A}u = \frac{C}{A} \quad (4.4.13)$$

이고 방정식 (4.4.13)의 해의 개수는 0이거나  $(i_b)$ 와 같이 1 또는  $2^{\gcd(k,m)} = 2^k$ 이다. 즉, 방정식 (4.4.4)의 해의 개수는 1, 2 또는  $2^k+1$ 이다. ■

<정리 4.4.3> 수열군  $S^r$ 에서 두 수열  $s_a^r(t)$ ,  $s_b^r(t)$ 에 대한 상호상관함수  $C_{a,b}(\tau)$ 는 4값 함수이며 함숫값은 다음과 같다.

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

증명. 
$$C_{a,b}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_a^r(t+\tau) + s_b^r(t)}$$

$$= \sum_{t=0}^{2^n-2} (-1)^{Tr_1^m([Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r + [Tr_m^n(b\alpha^t + \alpha^{dt})]^r)}$$

이다. 여기서  $Q = 2^m + 1$ 로 두고  $t = t_1Q + t_2$ , ( $0 \leq t_1 \leq 2^m - 2$ ,  $0 \leq t_2 \leq 2^m$ ),  $GF(2^n)$ 의 원시원소  $\alpha$ 에 대하여  $\alpha^Q = \beta$ 라 두면  $\beta$ 는  $GF(2^m)$ 의 원시원소이다.  $d \equiv 1 \pmod{2^m - 1}$ 이므로  $\beta^d = \beta$ 이다. 그러므로

$$\begin{aligned} & s_a^r(t+\tau) + s_b^r(t) \\ &= Tr_1^m([Tr_m^n(a\alpha^{t_1Q+t_2+\tau} + \alpha^{d(t_1Q+t_2+\tau)})]^r + [Tr_m^n(b\alpha^{t_1Q+t_2} + \alpha^{d(t_1Q+t_2)})]^r) \\ &= Tr_1^m([Tr_m^n(\beta^{t_1}a\alpha^{t_2+\tau} + \beta^{dt_1}\alpha^{d(t_2+\tau)})]^r + [Tr_m^n(\beta^{t_1}b\alpha^{t_2} + \beta^{dt_1}\alpha^{dt_2})]^r) \\ &= Tr_1^m(\beta^{t_1r} \{ [Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{d(t_2+\tau)})]^r + [Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})]^r \}) \end{aligned}$$

이다.

$$H(t, \tau, r) = [Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r + [Tr_m^n(b\alpha^t + \alpha^{dt})]^r$$

라 두면  $\{\beta^{t_1r} | 0 \leq t_1 \leq 2^m - 2, \gcd(r, 2^m - 1) = 1\} = GF(2^m)^*$  이므로

$$\begin{aligned} C_{a,b}(\tau) &= \sum_{t_1=0}^{2^m-2} \sum_{t_2=0}^{2^m} (-1)^{Tr_1^m(\beta^{t_1r} H(t_2, \tau, r))} \\ &= \sum_{\eta \in GF(2^m)} \sum_{t_2=0}^{2^m} (-1)^{Tr_1^m(\eta H(t_2, \tau, r))} - (2^m + 1) \end{aligned}$$

이다. 식 (2.1.1)에 의해  $N(t_2, r) = |\{t_2 \mid H(t_2, \tau, r) = 0, 0 \leq t_2 \leq 2^m\}|$  이라 두면

$$\begin{aligned} C_{a,b}(\tau) &= 2^m \cdot N(t_2, r) + 0 \cdot \{2^m + 1 - N(t_2, r)\} - (2^m - 1) \\ &= 2^m \{N(t_2, r) - 1\} - 1 \end{aligned}$$

이다.  $\gcd(r, 2^m - 1) = 1$  이므로 보조정리 4.2.2에 의해  $N(t_2, r) = N(t_2, 1)$  이고  $H(t_2, \tau, 1) = 0$  은

$$Tr_m^n((a\alpha^\tau + b)\alpha^{t_2} + (\alpha^{d\tau} + 1)\alpha^{dt_2}) = 0 \quad (4.4.14)$$

이다.  $A(\tau) = a\alpha^\tau + b$ ,  $B(\tau) = \alpha^{d\tau} + 1$  로 두면

$$Tr_m^n(A(\tau)\alpha^{t_2} + B(\tau)\alpha^{dt_2}) = A(\tau)\alpha^{t_2} + B(\tau)\alpha^{dt_2} + \overline{A(\tau)}\alpha^{2^m t_2} + \overline{B(\tau)}\alpha^{2^m dt_2}$$

이고 식 (2.5.1)를 이용하여  $\alpha = \delta\gamma$ 로 표현하면  $d \equiv 1 \pmod{2^m - 1}$ ,  $d \equiv 2^k \pmod{2^m + 1}$  이므로 식 (4.4.14)는

$$A(\tau)\delta^{t_2}\gamma^{t_2} + B(\tau)\delta^{t_2}\gamma^{2^k t_2} + \overline{A(\tau)}\delta^{t_2}\gamma^{-t_2} + \overline{B(\tau)}\delta^{t_2}\gamma^{-2^k t_2} = 0$$

이다. 양변에  $\gamma^{2^k t_2}$  을 곱하면

$$A(\tau)\delta^{t_2}\gamma^{(2^k+1)t_2} + B(\tau)\delta^{t_2}\gamma^{2 \cdot 2^k t_2} + \overline{A(\tau)}\delta^{t_2}\gamma^{(2^k-1)t_2} + \overline{B(\tau)}\delta^{t_2} = 0$$

이고,  $\gamma^{(2^k-1)t_2} = x$  라 두면  $x \in S$  이므로

$$B(\tau)x^{2^k+1} + \overline{A(\tau)}x^{2^k} + A(\tau)x + \overline{B(\tau)} = 0 \quad (4.4.15)$$

이다. 정리 4.4.2에 의해 방정식 (4.4.15)의 해는 0, 1, 2 또는  $2^k + 1$  개이므로  $N(t_2, \tau) = 0, 1, 2, 2^k + 1$  이고  $C_{a,b}(\tau) \in \{-2^m - 1, -1, 2^m - 1, 2^{m+k} - 1\}$  이다. ■

<보조정리 4.4.4>  $n = 2m$ ,  $m = 2k$  일 때,  $d \equiv 1 \pmod{2^m - 1}$ ,  
 $d \equiv 2^k \pmod{2^m + 1}$  을 만족하는  $d$  에 대하여

$$\sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + x^d)} = \begin{cases} 0 & , b \neq \beta^{(2^k-1)i} \\ 2^{m+k} & , b = \beta^{(2^k-1)i} \end{cases}$$

이다. 여기서  $i = 1, 2, \dots, 2^k$  이고  $\beta = \alpha^Q$  이다.

**증명.**  $GF(2^n)$  의 원시원소  $\alpha$  에 대하여

$$\sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + x^d)} = \sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(b\alpha^t + \alpha^{dt})} + 1 \quad (4.4.16)$$

이다.  $t = t_1Q + t_2$ ,  $(0 \leq t_1 \leq 2^m - 2, 0 \leq t_2 \leq 2^m)$ ,  $\beta = \alpha^Q$  이라 하면

$$\begin{aligned} Tr_1^n(b\alpha^t + \alpha^{dt}) &= Tr_1^m\{Tr_m^n(b\alpha^{t_1Q+t_2} + \alpha^{d(t_1Q+t_2)})\} \\ &= Tr_1^m\{\beta^{t_1} Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})\} \end{aligned}$$

이고 식 (4.4.16)은

$$\sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + x^d)} = \sum_{t_2=0}^{2^m-2} \sum_{t_1=0}^{2^m-2} (-1)^{Tr_1^m\{\beta^{t_1} Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})\}} + 1$$

이다. 식 (2.1.1)에 의하여

$$\sum_{t_1=0}^{2^m-2} (-1)^{Tr_1^m\{\beta^{t_1} Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})\}} = \begin{cases} -1 & , Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2}) \neq 0 \\ 2^m - 1 & , Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2}) = 0 \end{cases}$$

이므로

$$\begin{aligned} \sum_{t_2=0}^{2^m-2} \sum_{t_1=0}^{2^m-2} (-1)^{Tr_1^m\{\beta^{t_1} Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})\}} &= N(t_2) \cdot (2^m - 1) + \{2^m + 1 - N(t_2)\} \cdot (-1) \\ &= \{N(t_2) - 1\} 2^m - 1, \end{aligned}$$

단  $N(t_2) = \left| \{t_2 \mid Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2}) = 0, 0 \leq t_2 \leq 2^m\} \right|$  이다. 따라서

$$Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2}) = 0 \Leftrightarrow b\alpha^{t_2} + \alpha^{dt_2} + b\alpha^{2^m t_2} + \alpha^{2^m dt_2} = 0 \quad (4.4.17)$$

이고 식 (2.5.1)에 의하여  $\alpha = \delta\gamma$ 라 두면  $\alpha^d = \delta^{t_2}\gamma^{2^{k_2}}$ ,  $\alpha^{2^m} = \delta^{t_2}\gamma^{-t_2}$ ,  $\alpha^{2^m d} = \delta^{t_2}\gamma^{-2^{k_2}}$  이므로 식 (4.4.17)은

$$\delta^{t_2}(b\gamma^{t_2} + \gamma^{2^{k_2}} + b\gamma^{-t_2} + \gamma^{-2^{k_2}}) = 0 \quad (4.4.18)$$

이다. 양변에  $\gamma^{2^{k_2}}$ 를 곱하고  $\gamma^{(2^k+1)t_2} = y$ 로 두면  $\gamma^{(2^k-1)t_2} = \gamma^{(2^k+2^m)t_2} = y^{2^k}$ ,  $\gamma^{2 \cdot 2^{k_2}} = y^{2^{k+1}}$ ,  $y \in S$ 이고  $\delta^{t_2} \neq 0$ 이므로 식 (4.4.18)은

$$y^{2^{k+1}} + by^{2^k} + by + 1 = 0 \quad (4.4.19)$$

와 동치이다. 따라서  $N(t_2) = \left| \{y \in S \mid y^{2^{k+1}} + by^{2^k} + by + 1 = 0\} \right|$  이다.  $N(t_2)$ 의 값을 구하기 위해 방정식 (4.4.19)의 해의 개수를 구해야 한다.

식 (4.4.19)는 정리 4.4.2에서  $B(\tau) = 1$ ,  $A(\tau) = b$ 인 경우이므로 정리 4.4.2의  $(i_b)$ 를 만족한다. 따라서  $y = 1$ 이 해가 되고  $y = 1$  이외의 또다른 해를 구하기 위해  $y$ 에  $\frac{\bar{z}+u}{z+u}$ 를 대입하면 식 (4.4.19)는

$$(1+b)(z+\bar{z})u^{2^k} + (1+b)(z+\bar{z})^2 u = z^{2^{k+1}} + bz^{2^k}\bar{z} + bz\bar{z}^{2^k} + \bar{z}^{2^{k+1}} \quad (4.4.20)$$

이다.

먼저  $b = 1$ 인 경우, 방정식 (4.4.20)은  $0 \cdot u = (z+\bar{z})^{2^{k+1}}$ 이므로 해가 존재하지 않는다. 따라서 방정식 (4.4.19)의 해는 1개이다.

다음으로  $b \neq 1$ 인 경우, 식 (4.4.20)의 양변을 정리하면

$$u^{2^k} + (z+\bar{z})^{2^k-1}u = \frac{z^{2^{k+1}} + bz^{2^k}\bar{z} + bz\bar{z}^{2^k} + \bar{z}^{2^{k+1}}}{(1+b)(z+\bar{z})} \quad (4.4.21)$$

이고 방정식 (4.4.21)의 해가 없으면 방정식 (4.4.19)의 해는 1개다.

방정식 (4.4.21)의 해가 존재하면 정리 2.4.5에 의해

$$\left| \left\{ u \in GF(2^m) \mid u^{2^k} + (z + \bar{z})^{2^k-1} u = \frac{z^{2^k+1} + bz^{2^k}\bar{z} + bz\bar{z}^{2^k} + \bar{z}^{2^k+1}}{(1+b)(z+\bar{z})} \right\} \right| \\ = \left| \left\{ u \in GF(2^m) \mid u^{2^k} + (z + \bar{z})^{2^k-1} u = 0 \right\} \right|$$

이고 보조정리 4.4.1에 의해  $\left| \left\{ u \in GF(2^m) \mid u^{2^k} + (z + \bar{z})^{2^k-1} u = 0 \right\} \right| = 2^k$ 이다.

또한  $\left\{ u \in GF(2^m) \mid u^{2^k} + (z + \bar{z})^{2^k-1} u = 0 \right\}$ 는 원소가  $2^k$ 개인  $GF(2^m)$ 의 부분공간을 이루기 때문에

$$\left| \left\{ u \in GF(2^m) \mid u^{2^k} + (z + \bar{z})^{2^k-1} u = 0 \right\} \right| \\ = \left| \left\{ u \in GF(2^m) \mid u^{2^k} + (z + \bar{z})^{2^k-1} u = a \right\} \right|, \quad a \in GF(2^m)$$

를 만족하는  $GF(2^m)$ 의 부분공간은 모두  $2^k$ 개 존재할 수 있고 그때마다  $b$ 의 값은 유일하게 결정된다. 따라서

$$\left| \left\{ u \in GF(2^m) \mid u^{2^k} + (z + \bar{z})^{2^k-1} u = \frac{z^{2^k+1} + bz^{2^k}\bar{z} + bz\bar{z}^{2^k} + \bar{z}^{2^k+1}}{(1+b)(z+\bar{z})} \right\} \right| = 2^k$$

을 만족하는  $b$ 도  $2^k$ 개다.

이제 해의 개수가  $2^k$ 이기 위한  $b$ 의 조건이 필요하다.

우선 어떤 방정식이  $2^k$ 개의 해를 갖는지 확인하기 위해 식 (4.4.21)의  $u$ 에  $(z + \bar{z})u_1$ 을 대입하면  $u_1 \in GF(2^m)$ 이고 식 (4.4.21)은

$$(z + \bar{z})^{2^k} u_1^{2^k} + (z + \bar{z})^{2^k-1} (z + \bar{z}) u_1 = \frac{z^{2^k+1} + bz^{2^k}\bar{z} + bz\bar{z}^{2^k} + \bar{z}^{2^k+1}}{(1+b)(z+\bar{z})} \quad (4.4.22)$$

이다. 식 (4.4.22)의 양변을  $(z + \bar{z})^{2^k}$ 으로 나누면

$$u_1^{2^k} + u_1 = \frac{z^{2^k+1} + bz^{2^k}\bar{z} + bz\bar{z}^{2^k} + \bar{z}^{2^k+1}}{(1+b)(z+\bar{z})^{2^k+1}}$$



이고 McEliece의 식 (4.4.1)에 의하여

$$Tr_{\gcd(k,m)}^m \left( \frac{z^{2^k+1} + bz^{2^k} \bar{z} + b\bar{z} z^{2^k} + \bar{z}^{2^k+1}}{(1+b)(z+\bar{z})^{2^k+1}} \right) = 0 \quad (4.4.23)$$

일 때 해의 개수는  $2^k$  이다.

$$\begin{aligned} & Tr_k^m \left( \frac{z^{2^k+1} + bz^{2^k} \bar{z} + b\bar{z} z^{2^k} + \bar{z}^{2^k+1}}{(1+b)(z+\bar{z})} \right) \\ &= \frac{z^{2^k+1} + bz^{2^k} \bar{z} + b\bar{z} z^{2^k} + \bar{z}^{2^k+1}}{(1+b)(z+\bar{z})^{2^k+1}} + \left( \frac{z^{2^k+1} + bz^{2^k} \bar{z} + b\bar{z} z^{2^k} + \bar{z}^{2^k+1}}{(1+b)(z+\bar{z})^{2^k+1}} \right)^{2^k} \\ &= \frac{z^{2^k+1} + \bar{z}^{2^k+1} + b(z^{2^k} \bar{z} + \bar{z} z^{2^k})}{(1+b)(z+\bar{z})^{2^k+1}} + \frac{\bar{z} z^{2^k} + \bar{z} z^{2^k} + b^2(z^{2^k+1} + \bar{z}^{2^k+1})}{(1+b)^{2^k}(z+\bar{z})^{(2^k+1)2^k}} \end{aligned}$$

이므로 식 (4.4.23)은

$$\frac{z^{2^k+1} + \bar{z}^{2^k+1} + b(z^{2^k} \bar{z} + \bar{z} z^{2^k})}{(1+b)(z+\bar{z})^{2^k+1}} = \frac{\bar{z} z^{2^k} + \bar{z} z^{2^k} + b^2(z^{2^k+1} + \bar{z}^{2^k+1})}{(1+b)^{2^k}(z+\bar{z})^{(2^k+1)2^k}}$$

이다. 양변에  $(1+b)^{2^k+1}(z+\bar{z})^{2^k+1}$  을 곱하여 정리하면

$$b^{2^k+1}(z+\bar{z})^{2^k+1} = (z+\bar{z})^{2^k+1}$$

이고  $z+\bar{z} \neq 0$  이므로  $b^{2^k+1} = 1$  이다. 따라서  $b \in \{\beta^{(2^k-1)i} \mid i = 1, 2, 3, \dots, 2^k\}$

이므로  $b = \beta^{(2^k-1)i}$ , ( $i = 1, 2, \dots, 2^k$ ) 인 경우  $N = 2^k + 1$  이고,  $b \neq \beta^{(2^k-1)i}$ , ( $i = 1, 2, \dots, 2^k$ ) 인 경우  $N = 1$  이다. 즉,

$$\sum_{x \in GF(2^m)} (-1)^{Tr_1^n(bx+x^i)} = \begin{cases} 0 & , b \neq \beta^{(2^k-1)i} \\ 2^{m+k} & , b = \beta^{(2^k-1)i} \end{cases}, i = 1, 2, \dots, 2^k$$

이다. ■

<정리 4.4.5>  $a = 0$ ,  $b \in GF(2^m)^*$  일 때  $i = 1, 2, \dots, 2^k$  에 대하여 다음이 성립한다.

$$(a) \sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau) + 1\} = \begin{cases} 2^n, & b \neq \beta^{(2^k-1)i} \\ 2^{m+k}(2^k-1), & b = \beta^{(2^k-1)i}, \end{cases}$$

$$(b) \sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau) + 1\}^2 = \begin{cases} 2^{2n}, & b \neq \beta^{(2^k-1)i} \\ 2^{n+m}(2^m-1), & b = \beta^{(2^k-1)i}, \end{cases}$$

$$(c) \sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau) + 1\}^3 = \begin{cases} 2^{2n} \cdot 2^m, & b \neq \beta^{(2^k-1)i} \\ 2^{2n}(2^m-2^k), & b = \beta^{(2^k-1)i}. \end{cases}$$

증명. (a)

$$\sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau) + 1\} = \sum_{\tau=0}^{2^n-2} \left( \sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(b\alpha^t + (\alpha^{d\tau} + 1)\alpha^{dt})} + 1 \right) \quad (4.4.24)$$

이므로  $\alpha^t = x$  라 두면  $x \in GF(2^n)^*$  이고  $\{\alpha^{d\tau} | 0 \leq \tau \leq 2^n - 2\} = GF(2^n)^*$  이므로 식 (4.4.24)는

$$\begin{aligned} \sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau) + 1\} &= \sum_{u \in GF(2^n)^*} \sum_{x \in GF(2^n)} (-1)^{Tr_1^n\{bx + (u+1)x^d\}} \\ &= \sum_{u \in GF(2^n)} \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + (u+1)x^d)} - \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + x^d)} \end{aligned}$$

이다.  $\{u+1 | u \in GF(2^n)\} = GF(2^n)$  이므로 보조정리 4.4.4에 의해

$$\sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau) + 1\} = \begin{cases} \sum_{u \in GF(2^n)} \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + ux^d)}, & b \neq \beta^{(2^k-1)i} \\ \sum_{u \in GF(2^n)} \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + ux^d)} - 2^{m+k}, & b = \beta^{(2^k-1)i} \end{cases}$$

이다. 그런데

$$\begin{aligned}
\sum_{u \in GF(2^n)} \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + ux^d)} &= \sum_{u \in GF(2^n)} \sum_{x \in GF(2^n)} (-1)^{Tr_1^n\left(bx + \frac{u}{b^d}(bx)^d\right)} \\
&= \sum_{v \in GF(2^n)} \sum_{z \in GF(2^n)} (-1)^{Tr_1^n(z + vz^d)}
\end{aligned}$$

이고 식 (2.2.2)에 의하여

$$\sum_{v \in GF(2^n)} \sum_{z \in GF(2^n)} (-1)^{Tr_1^n(z + vz^d)} = \sum_{v \in GF(2^n)} \sum_{z \in GF(2^n)} (-1)^{Tr_1^n(vz + z^d)}$$

이므로

$$\sum_{u \in GF(2^n)} \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + ux^d)} = \sum_{u \in GF(2^n)} \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(ux + x^d)}$$

이다. 그러면

$$\begin{aligned}
\sum_{u \in GF(2^n)} \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(ux + x^d)} &= \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(x^d)} \sum_{u \in GF(2^n)} (-1)^{Tr_1^n(ux)} \\
&= \sum_{x \in GF(2^n)^*} (-1)^{Tr_1^n(x^d)} \sum_{u \in GF(2^n)} (-1)^{Tr_1^n(ux)} + 2^n \\
&= 2^n
\end{aligned}$$

이므로

$$\sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau) + 1\} = \begin{cases} 2^n & , b \neq \beta^{(2^k-1)i} \\ 2^n - 2^{m+k} & , b = \beta^{(2^k-1)i} \end{cases}$$

이다.

(b) 보조정리 4.4.4에 의하여

$$\left( \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + x^d)} \right)^2 = \begin{cases} 0 & , b \neq \beta^{(2^k-1)i} \\ 2^{n+m} & , b = \beta^{(2^k-1)i} \end{cases}$$

이므로  $i = 1, 2, \dots, 2^k$  에 대하여

$$\begin{aligned}
& \sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau)+1\}^2 \\
&= \sum_{\tau=0}^{2^n-2} \left( \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + (\alpha^{d\tau} + 1)x^d)} \sum_{y \in GF(2^n)} (-1)^{Tr_1^n(by + (\alpha^{d\tau} + 1)y^d)} \right) \\
&= \sum_{u \in GF(2^n)^*} \sum_{x, y \in GF(2^n)} (-1)^{Tr_1^n\{b(x+y) + (u+1)(x^d+y^d)\}} \\
&= \sum_{u \in GF(2^n)} \left( \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + (u+1)x^d)} \right)^2 - \left( \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + x^d)} \right)^2 \\
&= \begin{cases} \sum_{u \in GF(2^n)} (-1)^{Tr_1^n\{(u+1)(x^d+y^d)\}} \sum_{x, y \in GF(2^n)} (-1)^{Tr_1^n\{b(x+y)\}} & , b \neq \beta^{(2^k-1)i} \\ \sum_{u \in GF(2^n)} (-1)^{Tr_1^n\{(u+1)(x^d+y^d)\}} \sum_{x, y \in GF(2^n)} (-1)^{Tr_1^n\{b(x+y)\}} - 2^{n+m} & , b = \beta^{(2^k-1)i} \end{cases}
\end{aligned}$$

이다. 여기서

$$\begin{aligned}
& \sum_{u \in GF(2^n)} (-1)^{Tr_1^n\{(u+1)(x^d+y^d)\}} \sum_{x, y \in GF(2^n)} (-1)^{Tr_1^n\{b(x+y)\}} \\
&= \sum_{v \in GF(2^n)} \sum_{x, y \in GF(2^n)} (-1)^{Tr_1^n\{v b(x+y) + (x^d+y^d)\}} \\
&= \sum_{\substack{x=y \\ x, y \in GF(2^n)}} (-1)^{Tr_1^n(x^d+y^d)} \sum_{v \in GF(2^n)} (-1)^{Tr_1^n\{v b(x+y)\}} \\
& \quad + \sum_{\substack{x \neq y \\ x, y \in GF(2^n)}} (-1)^{Tr_1^n(x^d+y^d)} \sum_{v \in GF(2^n)} (-1)^{Tr_1^n\{v b(x+y)\}} \\
&= \left\{ \sum_{\substack{x=y \\ x, y \in GF(2^n)}} (-1)^{Tr_1^n(x^d+y^d)} \right\} \cdot 2^n + \left\{ \sum_{\substack{x \neq y \\ x, y \in GF(2^n)}} (-1)^{Tr_1^n(x^d+y^d)} \right\} \cdot 0 \\
&= 2^{2n}
\end{aligned}$$

이므로

$$\sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau)+1\}^2 = \begin{cases} 2^{2n} & , b \neq \beta^{(2^k-1)i} \\ 2^{2n} - 2^{n+m} & , b = \beta^{(2^k-1)i} \end{cases}$$

이다.

(c) 보조정리 4.4.4에 의하여

$$\left( \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + x^d)} \right)^3 = \begin{cases} 0 & , b \neq \beta^{(2^k-1)i} \\ 2^{2n+k} & , b = \beta^{(2^k-1)i} \end{cases}$$

이므로

$$\begin{aligned} & \sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau)+1\}^3 \\ &= \sum_{u \in GF(2^n)^*} \left( \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + (u+1)x^d)} \right)^3 \\ &= \sum_{u \in GF(2^n)} \left( \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + (u+1)x^d)} \right)^3 - \left( \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + x^d)} \right)^3 \end{aligned}$$

이다. 그런데

$$\begin{aligned} & \sum_{u \in GF(2^n)} \left( \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx + (u+1)x^d)} \right)^3 \\ &= \sum_{u \in GF(2^n)} \sum_{x,y,z \in GF(2^n)} (-1)^{Tr_1^n\{b(x+y+z) + (u+1)(x^d+y^d+z^d)\}} \\ &= \sum_{x,y,z \in GF(2^n)} (-1)^{Tr_1^n(x^d+y^d+z^d)} \sum_{v \in GF(2^n)} (-1)^{Tr_1^n\{vb(x+y+z)\}} \\ &= 2^n \sum_{x+y+z=0} (-1)^{Tr_1^n(x^d+y^d+z^d)} + \sum_{\substack{x+y+z \neq 0 \\ x,y,z \in GF(2^n)}} (-1)^{Tr_1^n(x^d+y^d+z^d)} \cdot 0 \quad (4.4.25) \\ &= 2^n \sum_{x,y} \sum_{z=x+y} (-1)^{Tr_1^n\{x^d+y^d+z^d\}} \\ &= 2^n \sum_{x,y} (-1)^{Tr_1^n\{x^d+y^d+(x+y)^d\}} \\ &= 2^n \left( 2^n + \sum_{\substack{x \in GF(2^n)^* \\ y \in GF(2^n)}} (-1)^{Tr_1^n\{x^d+y^d+(x+y)^d\}} \right) \end{aligned}$$

이므로  $c \in GF(2^n)$ 에 대하여  $y = cx$ 라 두면

$$\begin{aligned}
\sum_{\substack{x \in GF(2^n)^* \\ y \in GF(2^n)}} (-1)^{Tr_1^n\{x^d + y^d + (x+y)^d\}} &= \sum_{x \neq 0} \sum_{c \in GF(2^n)} (-1)^{Tr_1^n\{x^d + (cx)^d + (x+cx)^d\}} \\
&= \sum_{x \neq 0} \sum_{c \in GF(2^n)} (-1)^{Tr_1^n\{x^d(1+c^d+(1+c)^d)\}} \quad (4.4.26) \\
&= (2^n - 1) \cdot N + (-1)(2^n - N) \\
&= 2^n(N - 1)
\end{aligned}$$

이고, 이때  $N = |\{x \in GF(2^n) | (x+1)^d = x^d + 1\}|$  이다. 따라서 식 (4.4.26)을 식 (4.4.25)에 대입하면

$$\sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau) + 1\}^3 = \begin{cases} 2^{2n} \cdot N & , b \neq \beta^{(2^k-1)} \\ 2^{2n} \cdot N - 2^{2n+k} & , b = \beta^{(2^k-1)} \end{cases}$$

이고 정리 3.1.6에 의해  $N = 2^m$  을 대입하면 다음과 같다.

$$\sum_{\tau=0}^{2^n-2} \{C_{0,b}(\tau) + 1\}^3 = \begin{cases} 2^{2n+m} & , b \neq \beta^{(2^k-1)} \\ 2^{2n}(2^m - 2^k) & , b = \beta^{(2^k-1)} \end{cases}$$

■

<정리 4.4.6>  $n = 2m$ ,  $m = 2k$  일 때,  $d \equiv 1 \pmod{2^m - 1}$ ,  $d \equiv 2^k \pmod{2^m + 1}$  을 만족하는  $d$ 에 대하여  $C_{0,b}(\tau)$  값과 그 값의 발생빈도 수는 다음과 같다.

표 2.  $C_{0,b}(\tau)$  값의 발생횟수

| 발생빈도<br>상호상관 함수값 | $b \neq \beta^{(2^k-1)i}$ | $b = \beta^{(2^k-1)i}$ |
|------------------|---------------------------|------------------------|
| $-2^m - 1$       | $2^{n-1} - 2^{m+k-1}$     | $2^{n-1} - 2^{m+k-1}$  |
| $-1$             | $2^{m+k} - 2^k - 1$       | $2^{m+k} - 2^k$        |
| $2^m - 1$        | $2^{n-1} - 2^{m+k-1}$     | $2^{n-1} - 2^{m+k-1}$  |
| $2^{m+k} - 1$    | $2^k$                     | $2^k - 1$              |

**증명.**  $n = 2m$ ,  $m = 2k$  일 때,  $d \equiv 1 \pmod{2^m - 1}$ ,  $d \equiv 2^k \pmod{2^m + 1}$  이므로 정리 4.4.3에 의하여  $C_{a,b}(\tau) \in \{-2^m - 1, -1, 2^m - 1, 2^{m+k} - 1\}$  이다. 집합  $S$ 에 포함되는 해의 개수가  $i$ 인 경우가 발생하는 횟수를  $N_i$ , ( $i = -2^m - 1, -1, 2^m - 1, 2^{m+k} - 1$ )라 하면

( i )  $b \neq \beta^{(2^k-1)i}$ ,  $i = 0, 1, 2, \dots, 2^k$  일 때, 정리 4.4.5에 의하여

$$N_0 + N_1 + N_2 + N_{2^k+1} = 2^{n-1}$$

$$-2^m N_0 + 0 \cdot N_1 + 2^m N_2 + 2^{m+k} N_{2^k+1} = 2^n$$

$$2^n N_0 + 0 \cdot N_1 + 2^n N_2 + 2^{n+m} N_{2^k+1} = 2^{2n}$$

$$-2^{n+m} N_0 + 0 \cdot N_1 + 2^{n+m} N_2 + 2^{2n+k} N_{2^k+1} = 2^{2n+m}$$

이므로  $N_0, N_1, N_2, N_{2^k+1}$ 에 관한 방정식을 풀면,  $N_0 = 2^{n-1} - 2^{m+k-1}$ ,  $N_1 = 2^{m+k} - 2^k - 1$ ,  $N_2 = 2^{n-1} - 2^{m+k-1}$ ,  $N_{2^k+1} = 2^k$  이다.



(ii)  $b = \beta^{(2^k-1)i}$ ,  $i = 0, 1, 2, \dots, 2^k$  일 때, 정리 4.4.5에 의하여

$$N_0 + N_1 + N_2 + N_{2^{k+1}} = 2^{n-1}$$

$$-2^m N_0 + 0 \cdot N_1 + 2^m N_2 + 2^{m+k} N_{2^{k+1}} = 2^n - 2^{m+k}$$

$$2^n N_0 + 0 \cdot N_1 + 2^n N_2 + 2^{n+m} N_{2^{k+1}} = 2^{2n} - 2^{n+m}$$

$$-2^{n+m} N_0 + 0 \cdot N_1 + 2^{n+m} N_2 + 2^{2n+k} N_{2^{k+1}} = 2^{2n+m} - 2^{2n+k}$$

이므로  $N_0, N_1, N_2, N_{2^{k+1}}$ 에 관한 방정식을 풀면,  $N_0 = 2^{n-1} - 2^{m+k-1}$ ,  
 $N_1 = 2^{m+k} - 2^k$ ,  $N_2 = 2^{n-1} - 2^{m+k-1}$ ,  $N_{2^{k+1}} = 2^k - 1$ 이다. ■



## 5. 결론

본 논문에서는 의사난수열 생성기를 설계하고 연구하기 위해 중요한 수학적 도구인 트레이스 함수와 낮은 상관관계를 갖는 수열군을 생성하기 위한 강력한 도구인 데시메이션의 성질을 설명하였고 방정식의 해의 개수를 확인하기 위해 큰 역할을 하는 선형다항식과 그 선형다항식의 해집합의 성질에 대해 소개하였다.

기존 연구에서는 선형 수열인  $m$ -수열과  $m$ -수열에 비해 상호상관 함수값의 범위는 크지만 선형스팬이 크기 때문에 활용도가 높은 Kasami 수열, No 수열, GMW 수열, Zeng 수열을 소개하였고 상관관계를 결정하는 데시메이션에 대한 연구결과를 살펴보았다.

본론에서는 의사난수열인  $m$ -수열로부터 또다른  $m$ -수열을 생성하기 위해 Rosendahl과 Niho의  $d$ 를 포함하는 새로운  $d$ 의 값을 제안하였다.  $d \equiv 1 \pmod{2^m - 1}$ 을 만족하는 Niho 타입의 새로운 데시메이션에 의해 생성된 수열에서 상호상관 함수값의 범위를 확인하였고, 상호상관 함수값  $C_d(\tau) = 2^m - 1$ 인 경우, 위상이동차  $\tau = Q\tau_1$ ,  $(0 \leq \tau_1 \leq 2^m - 2)$ 인 경우로 제한하여 함수값의 발생빈도를 조사하였다.

마지막으로 본 논문에서는  $n = 2m$ ,  $m = 2k$ 일 때,  $\gcd(r, 2^m - 1) = 1$ 을 만족하는  $r$ 에 대하여 새롭게 정의된 수열군을 제시하였고 이 수열군의 상호상관 함수값의 범위를 확인하였다. 그리고 특별히  $a = 0$ ,  $b \in GF(2^m)^*$ 인 경우 위상이동차  $\tau$ ,  $(0 \leq \tau \leq 2^n - 2)$ 에 대한 모든  $C_{0,b}(\tau)$  값의 발생빈도에 대하여 살펴보았다. 이 연구를 바탕으로 모든  $a, b \in GF(2^n)$ 에 대한 상호상관 함수값의 분포에 관한 연구가 이루어질 수 있을 것이라 생각된다.

## 참 고 문 헌

- [1] L.D. Baumert, Cyclic Difference Sets(Lecture Notes in Mathematics), New York : Springer-Verlag, Vol. 182, 1971.
- [2] A. Canteaut, P. Charpin and H. Dobbertin, Binary  $m$ -sequences with three-valued cross-correlation: a proof of Welch's conjecture, IEEE Trans. Inf. Theory., Vol. 46, pp. 4-8. 2000.
- [3] U.S. Choi, S.J. Cho and H.D. Kim, Design and analysis of linear span of A new family of non-linear binary sequences with 5-valued cross-correlation functions, J. The Korea Institute of Electronic Communication Sciences, Vol. 17, No. 3, pp. 619-626, 2013.
- [4] T.W. Cusick and H. Dobbertin, Some new three-valued crosscorrelation functions for binary  $m$ -sequences, IEEE Trans. Inf. Theory, Vol. 42, pp. 1238-1240, 1996.
- [5] H. Dobbertin, One-to-one highly nonlinear power functions on  $GF(2^n)$ , AAECC Applicable Algebra in Engineering, Communication and Computing, Vol. 9, pp. 139-152, 1998.
- [6] R. Gold, Maximal recursive sequences with 3-valued cross-correlation functions, IEEE Trans. Inf. Theory, Vol. 14, pp. 154-156, 1967.
- [7] S.W. Golomb, Shift-Register Sequences, Holden Day, 1967.
- [8] S.W. Golomb and G. Gong, Signal Design for Good Correlation-For Wireless Communication, Cryptography and Radar. Cambridge, U.K. : Cambridge Univ. Press, 2005.
- [9] T. Helleseht, Some results about the cross-correlation function between two maximal linear sequences, Discrete Mathematics, Vol. 16, No. 3, pp.209-232, 1976.
- [10] T. Helleseht, J. Lahtonen and P. Rosendahl, On certain equations over finite fields and cross-correlations of  $m$ -sequences, Progress in Computer Science and Applied Logic, Vol. 23, pp. 169-176, 2004.

- [11] T. Helleseeth, J. Lahtonen and P. Rosendahl, On Niho type cross-correlation functions of  $m$ -sequences, *Finite Fields and Their Applications*, Vol. 13, pp. 305–317, 2007.
- [12] T. Helleseeth and P. Rosendahl, New pairs of  $m$ -sequences with 4-level cross-correlation, *Finite Fields and Their Applications*, Vol. 11, pp. 647–683, 2005.
- [13] T. Helleseeth and P. V. Kumar, Sequences with low correlation, in *Handbook in Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science B. V., ch. 21, pp. 1765–1853, 1998.
- [14] T. Kasami, Weight distribution formula for some class of cyclic codes, Coordinated Science Laboratory, University of Illinois, Urbana, Tech. Rep. R-285 (AD632574), 1966.
- [15] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, *Inform. Control*, Vol. 18, pp. 369–394, 1971.
- [16] H.D. Kim and S.J. Cho, A new proof about the decimations with Niho type five-valued cross-correlation functions, *J. Appl. Math. and Informatics*, Vol. 30, No. 5–6, pp. 903–911, 2012.
- [17] H.D. Kim, S.J. Cho, S.T. Kim and U.S. Choi, Four-valued cross-correlation function between two-maximal linear recursive sequences, submitted.
- [18] M.J. Kwon, S.J. Cho, Analysis of The Sequences with Optimal Cross-correlation Property, in press.
- [19] M.J. Kwon, S.J. Cho, S.H. Kwon, J.G. Kim, H.D. Kim and U.S. Choi, New decimations with 4-valued cross-correlations, *J. The Korea Institute of Electronic Communication Sciences*, Vol. 7, No. 4, pp. 827–832, 2012.
- [20] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, 1997.
- [21] R.J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Pub., pp. 103–110, 1987.

- [22] R. McEliece, D. Coding theory: Efficient solutions of equations for decoding, JPL SPS 37-40, Vol. 4, pp. 216-218, 1966.
- [23] W. Meier and O. Staffelbach, Fast Correlation Attacks on Certain Stream Ciphers, Journal of Cryptology, Vol. 1, No. 3, pp.159-176, 1989.
- [24] Y. Niho, Multi-valued cross-correlation functions between two maximal linear recursive sequences, Ph.D. thesis, University of Southern California, 1972.
- [25] J.S. No, A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span, Ph.D. thesis, Univ. Southern California, Los Angeles, CA, May 1988.
- [26] J.S. No, Generalization of GMW sequences and No sequences, IEEE Trans. Inf. Theory, Vol. 42, No. 1, pp. 260-262, 1996.
- [27] P. Rosendahl, Niho type cross-correlation functions and related equations, Ph.D. thesis, Turku center for computer science, 2004.
- [28] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, In Communications and Control Engineering Series, 1996.
- [29] D.V. Sarwate, M.B. Pursley, Crosscorrelation properties of pseudorandom and related sequences, Proc. IEEE. Vol. 68, No. 5, pp. 593-619, 1980.
- [30] R.A. Scholtz and L. Welch, GMW sequences, IEEE Trans. Inform. Theory, Vol. IT-30, No. 3, pp. 548-553, 1984.
- [31] M.K. Simon, J.K. Omura, R.A. Sholtz, and B. K. Levitt, Spread Spectrum Communications, Rockville, MD : Computer.
- [32] 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.
- [33] 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.

## 감사의 글

무엇보다 지금의 결실을 얻을 때까지 포기하지 않고 공부할 수 있도록 격려해 주시고 힘을 주신 부모님께 이 논문을 바칩니다.

어떻게 연구하고 공부해야 하는지 뿐만 아니라 교사란 어떤 마음가짐으로 학생들을 대해야 하는지에 대해서도 깊은 가르침을 주신 조성진 교수님과 늘 넓은 마음으로 보살피 주신 김한두 교수님, 무사히 수료할 수 있도록 큰 도움을 주신 박진한 교수님, 바쁘신 중에도 완성도 높은 논문을 작성할 수 있도록 조언해 주신 김석태 교수님, 표용수 교수님께도 머리 숙여 감사드립니다.

누구보다 바쁘지만 연구 방법이나 논문 작성법 등 여러 방면에서 도움을 주신 동명대 최연숙 교수님, 학회 발표와 관련하여 많은 조언을 해주신 김진경 박사님, 연구실에서 같이 연구하며 마음으로 큰 의지가 되었던 권숙희, 김나령 선생님 감사합니다.

마지막으로 고등학교 교사로 근무하면서 이와 같은 결실을 얻을 때까지 공부할 수 있도록 도와주신 남재구 부장님, 임철화 선생님께도 감사의 마음을 전합니다.