유한체위에서 방정식 $(x+1)^d = x^d + 1$에 대한 연구

조성진* · 김한두**· 최언숙***· 권숙희* · 권민정* · 김진경*

*부경대학교 · **인제대학교 · ***동명대학교

The Study of the Equation $(x+1)^d = x^d + 1$ over Finite Fields

Song-jin Cho* · Han-doo Kim** · Un-sooK Choi*** · Sook-hee Kwon*

· Min-jeong Kwon* · Jin-gyoung Kim*

*Pukyong National University · **Inje University · ***Tongmyong University

E-mail : sjcho@pknu.ac.kr

요 약

주기가 $N=2^n-1$인 이진수열은 공학과 과학의 많은 분야에서 폭넓게 사용된다. 코드분할 다중접속(CDMA) 통신시스템과 스트림암호시스템은 잘 알려진 응용분야이다. 본 논문에서는 유한체위에서 방정식$(x+1)^d = x^d+1$의 특성을 분석한다. 특히 이 방정식의 d는 이진수열의 상호상관관계를 분석하는데 사용된다.

ABSTRACT

Binary sequences of period $N=2^k-1$ are widely used in many areas of engineering and sciences. Some well-known applications include code-division multiple-access (CDMA) communications and stream cipher systems. In this paper, we analyze the equation $(x+1)^d = x^d+1$ over finite fields. The d of the equation is used to analyze cross-correlation of binary sequences.

키워드

이진수열, 유한체, 방정식, 데시메이션, 상호상관관계

Key word

binary sequences, finite fields, equation, decimation, cross-correlation

Ⅰ. 서 론

무선통신의 접속 방식 중에는 크게 시간 분할 다중접속(TDMA, Time Division Multiple Access) 방식과 코드 분할 다중접속(CDMA, Code Division Multiple Access) 방식으로 나눌 수 있는데 코드분할 다중접속 방식은 이미 널리 사용 중인 대역확산(Spread Spectrum) 기술에 근거를 둔 것으로 같은 지역, 같은 시간, 같은 공간, 같은 주파수를 사용하면서 혼돈 없이 통화할 수 있는 우수한 이동전화 시스템이다[1-3].

특히, 코드 분할 다중접속 방식은 여러 사용자가 주파수와 시간을 공유하면서 각 사용자에게 의사 불규칙 수열(Pseudo random sequence)을 할당하여 각 사용자는 송신 신호를 확산(Spreading)하여 전송하고 수신부에서는 송신측에서 사용한 것과 동일한 의사난수열(Pseudo noise sequence)을 발생시켜 동기를 맞추고 수신된 신호를 역확산(Despreading)하여 신호를 복원하는 방식이다. 하나의 위성과 여러 개의 지상 지구국으로 구성되어 있는 위성통신에 그 근원을 둔 다중접속은 일정의 주파수 대역을 가지는 공동의 통신 채널을 여러 사용자가 나누어 사용하는 것이다. 의사난수열은 이동통신 시스템의 다중접속 방식의 표준인 코드 분할 다중 접속 방식과 같은 확산대역 통신시스템에서 많이 응용되고 있고 중요한 역할을 한다. 이러한 통신 시스템 사이에서 의사난수열의 중요한 기능은 다중 접속 충돌을 최소화하고, 가능한 시스템의 보안수준을 높이는 것, 그리고 더 많은 사용자들이 사용할 수 있도록

사용자수를 확대하는 것 등이 있다. 특히 다중 접속 충돌은 여러 사용자가 동시에 접속할 때 생기는 충돌에 의해 발생 할 수 있는데, 의사난수열의 낮은 상관관계는 다중 접속 충돌을 최소화 할 수 있다[1-5]. 그러므로 수열의 바람직한 성질 중 낮은 상관관계는 코드 분할 다중 접속의 능력을 가지기 위해 중요하다.

본 논문에서는 주기가 $N=2^n-1$인 이진수열의 상호상관관계를 분석에서 중요한 역할을 하는 $d \equiv 1 (\mathrm{mod}\, q-1)$인 방정식 $(x+1)^d = x^d+1$을 만족하는 해 x에 대하여 분석한다.

II. 배경 지식 및 기존 연구

2.1 코드 분할 다중접속

코드 분할 다중접속에서 적합한 코드는 수신기가 입력신호의 동기화를 용이하게 하고 잡음이 신호를 왜곡시킬지라도 수신자가 원래의 데이터를 정확하게 재구성할 수 있도록 좋은 상관관계를 가지는 것이다[6-8].

그림 1은 확산 코드에 의한 통신의 예를 보여주고 있다. 먼저 송신 데이터에 확산코드 10110100101 을 곱해준다. 곱해진 원래의 송신 데이터는 훨씬 속도가 높은 확산코드와 같은 속도의 확산신호와 같이 된다. 이 확산신호를 전자파에 실어서 송신을 하고, 수신 쪽에서는 이 확산신호에 다시 송신 쪽에서 사용한 동일한 확산 코드를 곱해주면, 원래 송신하고자 했던 데이터와 동일한 수신 데이터를 얻을 수 있다.

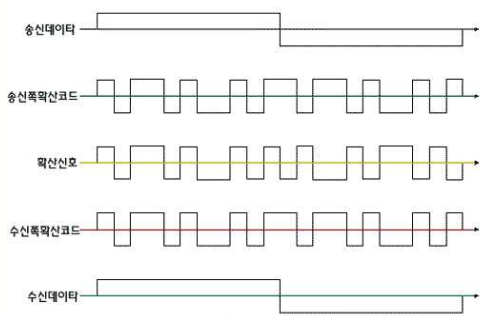


그림 1. 확산코드에 의한 통신 예

Fig. 1. Sample of communication by spreading code

그러나 수신된 확산신호에 다른 확산코드 01101001010 를 곱해 주면 수신 데이터가 그림 2와 같이 되어서, 원래의 데이터를 복구할 수 없다. 물론 이때 확산코드를 곱해주는 시간이 맞지 않으면 마치도 다른 확산코드를 곱해주는 것과 같으므로, 확산코드가 시작하는 시간까지 맞아야 한다. 따라서 사전에 미리 확산코드와 시작 시간을 모르는 사람은 데이터를 복구할 수 없고, 확산코드 신호와 시작 시간을 알고 있는 사람만 데이터를 복구할 수 있기 때문에 자연히 높은 비화 특성을 가지게 된다.

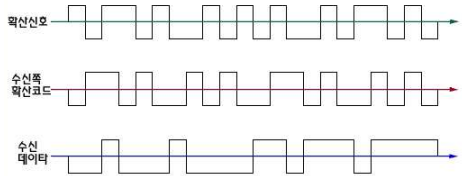


그림 2. 다른 확산코드를 곱한 경우

Fig. 2. Case of multiple different spreading code

확산코드는 송신 데이터와 아무런 관계도 없으며 확산코드를 추정하기 곤란하게 거의 잡음과 같은 의사난수열을 사용한다. (디지털 신호인 경우 랜덤 시퀀스(Random Sequence)) 이 수열은 거의 무한히 만들 수 있기 때문에 임의의 확산코드를 쉽게 재생할 수 없다. CDMA 방식에서는 코드 개수에 의해서 채널수가 결정되는 것이 아니라, 주변의 간섭량에 의해서 채널수가 결정된다.

그림 3은 송신 데이터 신호에 확산코드 신호를 곱해주면, 이론적으로 확산 신호의 비트 속도가 확산코드 속도와 같게 되므로 확산신호와 확산코드의 대역폭은 거의 비슷하다는 것을 알 수 있다. 이 과정을 확산이라 하고 이때 송신 데이터가 가지고 있는 에너지는 일정하므로 데이터에 해당하는 크기는 넓어진 대역폭만큼 반비례하여 작아진다. 이 확산신호에 다시 동일한 확산코드를 곱해주면, 그림 1에서 원래의 데이터를 복구할 수 있다는 것을 알 수 있다. 즉, 이를 주파수 영역에서 보면 확산신호의 대역폭이 다시 원래 데이터 신호의 대역폭으로 줄어든 것으로 이해할 수 있다. 이를 역확산이라 한다. 그리고 이 과정은 데이터가 가지고 있는 에너지가 일정하기 때문에 신호의 크기도 줄어든 대역폭만큼 다시 커져서, 다른 신호로부터 분리하여 데이터를 복구할 수 있다[5].

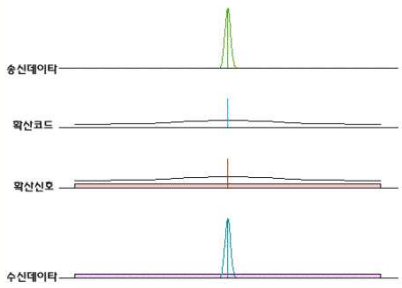


그림 3. 각 신호의 대역폭 비교

Fig. 3. Compared to the bandwidth of each signal

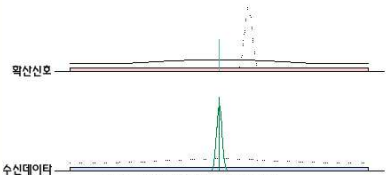


그림 4. 강한 간섭 신호가 있을 경우
Fig. 4. Case of strong interfering signals

그림 4에서 점선으로 된 간섭신호가 포함되어도 역확산 과정에서 확산이 되어 그 크기가 줄어들어 간섭신호의 크기는 줄이고, 자기 신호는 크기를 키워 외부의 간섭에 매우 강한 특성을 가지게 된다.

2.2 트레이스 함수

트레이스 함수(Trace function)는 유한체로부터 부분체로의 선형 매핑인데, 의사불규칙 수열의 설계와 분석을 위한 중요한 수학적 도구로 사용된다. 그리고 대부분의 이진 의사난수열들은 트레이스 함수의 형태로 표현될 수 있다.

본 논문에서 수열의 생성을 위해 사용되는 트레이스 함수는 x는 $GF(2^n)$의 원소일 때, $Tr_m^n : GF(2^n) \to GF(2^m)$ 는 $Tr_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{m \cdot i}}$ 같이 정의된다. $Tr_m^n : GF(2^n) \to GF(2^m)$ 는 선형함수이고 전사함수이며 임의의 고정된 $\omega \in GF(2^m)$에 대하여 방정식 $Tr_m^n(x) = \omega$를 만족하는 해 $x(\in GF(2^n))$가 2^{n-m}개 존재한다[9,10].

2.3 상호상관관계 함수

주기가 $2^n - 1$인 두 수열 $a_i = Tr(\alpha^i)$와 $b_i = Tr(\alpha^{ri})$에 대하여 상호상관관계 함수 $C_{ab}(\tau)$를 $C_{ab}(\tau) = \sum_{i=0}^{2^n-2} (-1)^{a_{i+\tau}} (-1)^{b_i}$ 이라 하고 $\{b_i\}$를 $\{a_i\}$의 r-데시메이션(decimation)한 수열이라 하면 $b_i = a_{ri}$이고 $\gcd(r, 2^n - 1) = 1$이다. 그러면, $C_{ab}(\tau)$는 다음과 같다.

$$\begin{aligned} C_{ab}(\tau) &= \sum_{i=0}^{2^n-2} (-1)^{a_{i+\tau}} (-1)^{a_{ri}} \\ &= \sum_{i=0}^{2^n-2} (-1)^{Tr(\alpha^{i+\tau} + \alpha^{ri})} \\ &= \sum_{\substack{x \in GF(2^n) \\ x \neq 0}} (-1)^{Tr(xy + x^r)} \\ &= -1 + \sum_{x \in GF(2^n)} (-1)^{Tr(xy + x^r)} \qquad (1) \end{aligned}$$

여기서 $x = \alpha^i$, $y = \alpha^\tau$ 이다.

$\Delta_r(y) = \sum_{x \in GF(2^n)} (-1)^{Tr(xy + x^r)} = C_{ab}(\tau) + 1$이고 임의의 k와 y에 대하여 $r' = r \cdot 2^j (0 \le j \le n-1)$이면 $\Delta_r(y) = \Delta_r(y^{2^k})$, $\Delta_r(y) = \Delta_{r'}(y)$을 만족하고 $\Delta_r(y) = \Delta_{r'}(y)$을 만족한다[11,12].

<정리 2.1[11]>

$$\sum_{y \in GF(2^n)} \{\Delta_r(y)\} = 2^n \qquad (2)$$

$$\sum_{y \in GF(2^n)} \{\Delta_r(y)\}^2 = 2^{2n} \qquad (3)$$

$$\sum_{y \in GF(2^n)} \{\Delta_r(y)\}^3 = 2^{2n} b \qquad (4)$$

여기서 b는 $(x+1)^d = x^d + 1$의 방정식의 해의 개수이다. 따라서 유한체 상에서 $(x+1)^d = x^d + 1$의 방정식에 대한 연구는 이진수열의 상관관계를 분석하는데 있어 매우 중요하다.

Ⅲ. 방정식 $(x+1)^d = x^d + 1$ 분석

$q := 2^k$, $d \equiv 1 \pmod{q-1}$이고 x가 $GF(q^2) - \{0,1\}$의 원소일 때, $\bar{x} = x^q$이라 하고 $S = \{x \in GF(q^2) : x\bar{x} = 1\}$이라 하자. S는 주기가 $q+1$인 순환군이다. $(x+1)^d = x^d + 1$이고 $(\bar{x}+1)^d = \bar{x}^d + 1$이며 $(x\bar{x} + x + \bar{x} + 1)^d = (x\bar{x})^d + x^d + \bar{x}^d + 1$이다. $x\bar{x}$가 $GF(q)$의 원소이고 $x + \bar{x}$가 $GF(q)$의 원소이면, $x\bar{x} + x + \bar{x} + 1$는 $GF(q)$의 원소이다. 또한 $(x\bar{x} + x + \bar{x} + 1)^d = x\bar{x} + x + \bar{x} + 1$ 이고 $(x\bar{x})^d = x\bar{x}$이므로 $x + \bar{x} = x^d + \bar{x}^d$이며 양변에 x^{d-q-1}를 곱하면, $x^{d-q} + x^{d-1} = x^{2d-q-1} + x^{qd+d-q-1}$이 된다.

$d \equiv 1 \pmod{q-1}$이고 $d - 1 = (q-1)s$인 자연수 s가 존재하면 $x^{qd+d-q-1} = x^{(q+1)(d-1)} = x^{(q+1)(q-1)s} = 1$이다. 식 $x^{2d-q-1} - x^{d-q} - x^{d-1} + 1 = 0$은 $(x^{d-1} - 1)(x^{d-q} - 1) = 0$이므로 $x^d = x$ 또는 $x^d = x^q = \bar{x}$을 만족한다.

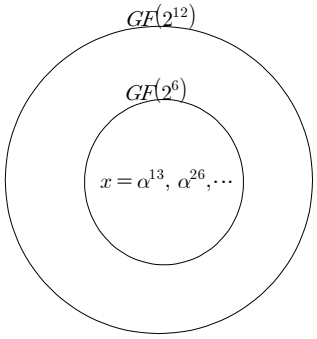
(i) $x^d = x$: $(x+1)^{d-1} = 1$, $\left(\frac{x+1}{\bar{x}+1}\right)^{d-1} = 1$

(ii) $x^d = \bar{x}$: $(x+1)^{d-q} = 1$, $\left(\frac{x+1}{\bar{x}+1}\right)^{d+1} = 1$

그러므로 x가 $(x+1)^d = x^d + 1$의 해가 될 필요충분조건은 $x^{d-1} = (x+1)^{d-1} = 1$ 또는 $x^{d-q} = (x+1)^{d-q} = 1$ 이다. 여기서 $\gcd(d-1, q+1) = \gcd(d+1, q+1) = 1$ 이고 $\frac{x+1}{\bar{x}+1} \in S$ 이고 $\{x \in GF(q^2) | (x+1)^d = x^d + 1\} = GF(q)$ 이므로 x는 $GF(q)$의 원소이다.

<정리 3.1> $q:=2^k$, $d\equiv 1 \pmod{q-1}$이고 모든 $x\in GF(q)$가 $(x+1)^d=x^d+1$의 해이면 $x^d=x$ $\left(\left(\frac{x+1}{\overline{x}+1}\right)^{d-1}=1\right)$ 또는 $x^d=\overline{x}\left(\left(\frac{x+1}{\overline{x}+1}\right)^{d+1}=1\right)$이고 $\gcd(d\pm 1,q+1)=1$이므로 $\frac{x+1}{\overline{x}+1}=1$이다. 이때 $\overline{x}=x$이고 이것은 $x\in GF(q)$을 의미하며 정확하게 $GF(2^n)$에서 $q(=2^k)$개의 해를 가진다.

<예제 3.2> $n=12$, $q=2^6$ 이고 $s=5$이면, $\gcd(s,q+1)=5$이다. $\alpha^{12}+\alpha^{10}+\alpha^2+\alpha+1=0$을 만족하는 $\beta:=\alpha^{65}(\beta^6+\beta+1=0)$이다. $S=\{1,\alpha^{63},\alpha^{126},\cdots,\alpha^{63\times 64}\}$이고 $d=316$이다. 여기서 $\omega:=\beta^{21}=\alpha^{1365}$이다.
만약 $x_0=\alpha^{13}$, $x_1=\alpha^{26}$이면 $x_0^{q-1}=\alpha^{819}$, $x_1^{q-1}=\alpha^{1638}$이고 $x_0^{d-1}=(\alpha^{13})^{315}=\alpha^{65\times 63}=1$, $x_1^{d-1}=(\alpha^{26})^{315}=(\alpha^{65\times 63})^2=1$이다. 그러므로 $x_0,x_1\in GF(2^6)$을 의미하며 정확하게 $GF(2^{12})$에서 2^6의 해를 가진다.



$$\alpha^{12}+\alpha^{10}+\alpha^2+\alpha+1=0$$
$$\beta:=\alpha^{65}\Rightarrow\beta^6+\beta+1=0$$

Ⅳ. 결 론

본 논문에서는 주기가 $N=2^n-1$인 이진수열의 상호상관관계를 분석에서 중요한 역할을 하는 방정식 $(x+1)^d=x^d+1$을 만족하는 해 x에 대하여 분석하였다. 이때 $d\equiv 1 \pmod{q-1}$이다. $(x+1)^d=x^d+1$을 만족하는 해 집합이 $x^d=x$ 또는 $x^d=\overline{x}$임을 보였고 $\gcd(d\pm 1,2^k+1)=1$ 이면 $\overline{x}=x$이고 이것은 $x\in GF(2^k)$을 의미하며 정확하게 $GF(2^n)$에서 2^k의 해를 가진다.

참고문헌

[1] S.W. Golomb, Shift Register Sequences, Holden Day, 1967.

[2] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, “Spread Spectrum Communications”, Vol. 1, Rockville, MD: Computer Science Press 1985.

[3] K. Fazel and S. Kaiser, Multi-carrier and Spread Spectrum Systems, John Wiley and Sons Ltd. 2003.

[4] N. Yee, J-P. Linnartz and G. Fettweis, “Multi-carrier CDMA in indoor wireless Radio Network”, Proc. of IEEE PIMRC 93, Yokohama, Japan, Sept. 1993, pp. 109-13.

[5] R. Prasad, “CDMA for Wireless Personal Communications”, Artech House Publishers, 1996.

[6] T. Helleseth and P.V. Kumar, “Sequences with low correlation”, in Handbook of Coding Theory, Vol. II, pp. 1765-1853, 1998.

[7] G. Gong, “New designs for signal sets with low cross correlation, balance property, and large linear span: GF(p) case”, IEEE trans. Inform. Theory, Vol. 4, pp. 2847-2867, 2002.

[8] R.A. Games, “Cross correlation of $m-$ sequences and GMW sequences with the same primitive polynomial”, Discrete Appl. Math. Vol. 12, pp. 139-146, 1985.

[9] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.

[10] S.J. Cho, Finite Fields with Their Applications, Kyowoosa, Press, 2007.

[11] Y. Niho, “Multi-valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences”, Ph.D. thsis, University of Southern California, 1972.

[12] P. Rosendahl, “Niho Type Cross – Correlation Functions and Rrlated Equations”, Ph.D. thsis, University of Turku, 2004.