Regular paper http://dx.doi.org/10.13067/JKIECS.2013.8.11.1749

$GF(2^n)$위에서 $x^5+bx^3+b^{2^m}x^2+1=0$의 서로 다른 해의 개수

최언숙* · 조성진**

Number of Different Solutions to $x^2+bx^3+b^{2^m}x^2+1=0$ over $GF(2^n)$

Un-Sook Choi* · Sung-Jin Cho**

요 약

주기가 2^n-1인 이진수열은 부호이론, CDMA와 같은 통신시스템과 암호체계 등 많은 분야에서 폭넓게응용되고 있다. 본 논문에서는 $n=2m$, $m=4k(k\geq 2)$이고 $d=3\cdot 2^m-2$일 때 생성되는 비선형 이진수열의 상호상관관계의 빈도를 분석하기 위해 $GF(2^n)$위에서 방정식 $x^5+bx^3+b^{2^m}x^2+1=0$의 해의 유형에 대하여 분석하고 서로 다른 해의 개수를 결정하는 알고리즘을 제안한다.

ABSTRACT

Binary sequences of period 2^n-1 are widely used in many areas of engineering and sciences. Some well-known applications include coding theory, code-division multiple-access (CDMA) communications, and stream cipher systems. In this paper we analyze different solutions to $x^5+bx^3+b^{2^m}x^2+1=0$ over $GF(2^n)$. The number of different solutions determines frequencies of cross-correlations of nonlinear binary sequences generated by $d=3\cdot 2^m-2$, $n=2m, m=4k(k\geq 2)$. Also we give an algorithm for determination of number of different solutions to the equation.

키워드

Number of Solutions, Finite Fields, Trace Function, Cross-Correlation, Equation
해의 개수, 유한체, 트레이스 함수, 상호상관관계, 방정식

Ⅰ. 서 론

의사난수열(pseudorandom sequence)은 디지털 통신 시스템에서 다양하게 사용되고 있다. 이러한 의사난수열을 설계하는데 있어서 낮은 상호상관관계 값, 큰 선형스팬, 큰 수열군, 구현의 용이성 등이 바람직한 성질이다[1-3]. 그 동안 많은 연구자들에 의해 다양한 방법으로 낮은 상호상관관계 값을 갖는 수열에 대한 설계와 분석이 이루어져 왔다. 그 중 트레이스 함수를 이용하여 설계된 대표적인 수열로는 m-수열, GMW 수열, Kasami 수열, No 수열, 한 개의 m-수열과 그 수열을 적당히 건너뛰어가면서 발생시킨 Gold 계열 수열이 있다[4-7]. 또한 Gold 계열 수열과 GMW 수열의 확장으로 낮은 상호상관관계와 비선형

* 동명대학교 자율전공학부(choies@tu.ac.kr)
** 교신저자(corresponding author) : 부경대학교 응용수학과(sjcho@pknu.ac.kr)
접수일자 : 2013. 09. 11 심사(수정)일자 : 2013. 10. 21 게재확정일자 : 2013. 11. 15

성을 높여 선형스팬이 큰 비선형 이진수열에 관한 연구가 활발히 진행되고 있다[8-13]. 이러한 수열이 트레이스 함수를 이용해 설계되는 것은 수열에 대한 여러 가지 특성을 분석하는 데 있어 수학적 분석이 용이하다는 것이다. 본 논문에서는 $n=2m$일 때 $GF(2^n)$ 위에서 수열의 상호상관관계에 대한 빈도분석을 위해 중요한 요소가 되는 방정식 $x^5+bx^3+b^{2^m}x^2+1=0$의 해의 유형과 서로 다른 해의 개수를 결정하는 알고리즘을 제안한다. 이 방정식의 해의 개수에 대한 연구는 Kloosterman 합이라는 함수를 이용하여 나타내고 있으나 그 방법은 매우 복잡하고 어느 정도의 오차를 가지고 있다[13]. 본 논문에서는 유한체에서 이차방정식이 해를 갖는 조건을 이용하여 해의 개수를 결정하는 알고리즘을 제안한다.

II. 배경지식 및 기존연구

$GF(2^n)$를 2^n개의 원소를 가진 유한체라 하고, $GF(2^n)^*=GF(2^n)\setminus\{0\}$ 라 하자. 차수가 n인 원시다항식 $f(x)$에 대하여 $f(x)=0$의 한 원시근을 $\alpha(\in GF(2^n))$라 하자. $n=km(k>1)$에 대하여 트레이스 함수 $Tr_m^n: GF(2^n)\rightarrow GF(2^m)$ 는 다음과 같다[13,14].

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

함수 $Tr_m^n: GF(2^n)\rightarrow GF(2^m)$는 다음과 같은 성질을 갖는다. $GF(2^n)$의 임의의 원소 x, y와 $GF(2^m)$의 임의의 원소 a, b에 대하여 다음이 성립한다.

(a) $Tr_m^n(ax+by)=aTr_m^n(x)+bTr_m^n(y)$.

(b) $Tr_1^n(x)=Tr_1^m\left[Tr_m^n(x)\right]$.

(c) $Tr_m^n\left(x^{2^m}\right)=Tr_m^n(x)$.

(d) Tr_m^n는 전사함수이다.

(e) $GF(2^m)$의 모든 원소 c에 대하여

$$\left|\left\{x|\, Tr_m^n(x)=c,\ \forall c\in GF(2^m)\right\}\right|=2^{n-m}\quad .$$

유한체 $GF(2^n)$위에서 이차방정식 $x^2+x=\alpha$ 에 대하여 $Tr_1^n(\alpha)=0$이면 해가 존재한다[13,14]. 이를 이용하여 A, B, C가 $GF(2^n)$의 원소일 때, 식

$$Ax^2+Bx+C=0\,(A\neq 0) \tag{2}$$

의 해를 $B\neq 0$인 경우와 $B=0$인 경우로 나누어 구한다.

ⅰ) $B\neq 0$인 경우 ; $y=AB^{-1}x$, $\gamma=ACB^{-2}$이라 두고 이를 식(2)에 대입하면
$A^{-1}B^2y^2+A^{-1}B^2y+A^{-1}B^2\gamma=0$이 되고 양변을 $A^{-1}B^2$으로 나누면

$$y^2+y=\gamma \tag{3}$$

가 된다. 따라서 식(2)가 해를 가질 필요충분조건은 $Tr(\gamma)=Tr(AC/B^2)=0$이 된다. 이 때 식(3)의 해를 y_1이라 하면 식(2)의 해는 $x=\frac{B}{A}y_1$, $\frac{B}{A}(y_1+1)$이 된다. 그러므로 $Tr(AC/B^2)=0$이면 두 개의 해, $Tr(AC/B^2)=1$이면 해가 존재하지 않는다.

ⅱ) $B=0$인 경우 ; $\gamma=\frac{C}{A}$라 두고 식(2)에 대입하면 $Ax^2+A\gamma=0$이 되고 이를 A로 나누면 $x^2=\gamma$ 이다. 그러므로 $GF(2^n)$위에서 해는 정확히 한 개로 $x=\gamma^{2^{n-1}}$이다.

예를 들어 $n=6, m=3$, $f(x)=x^6+x^5+1$일 때 $GF(2^6)$의 원시근 α에 대하여 $\beta=\alpha^{2^3+1}$라 두면 $\beta^3=\beta+1$이 된다. 이때 $x^2+\beta x+1=0$에 대하여 $GF(2^m)$상에서 해를 갖는지 판단해 보면 다음과 같다.

$$Tr_1^3(AC/B^2)=Tr_1^3(\beta^{-2})=Tr_1^3(\beta^5)=1$$

따라서 $GF(2^3)$위에서 해가 존재하지 않는다. 그런데 $GF(2^6)$에서 풀면 $\beta=\alpha^9$이므로

$$Tr_1^6(\alpha^{-18})=Tr_1^6(\alpha^{45})=Tr_1^6(\alpha^5+\alpha^2+\alpha)=0$$

이고 $GF(2^6)$에서 두 개의 해를 갖는다. $GF(2^6)$에서 실제 해를 구하기 위하여 $Tr_1^6(\theta)=1$인 θ가 필요하다. $Tr_1^6(\alpha)=1$이므로 $\theta=\alpha$라 두고 이를 이용하여 기저가 되는 행렬 T를 만들면 다음과 같다.

$$T=\begin{pmatrix}1&0&1&1&0&1\\0&0&0&1&1&0\\0&1&1&1&0&1\\0&0&0&0&1&1\\0&0&0&0&0&0\\1&1&1&0&0&1\end{pmatrix}$$

주어진 이차 방정식 $x^2+\alpha^9x+1=0$을 식(3)과 같은 표준형으로 고치기 위해 $y=\alpha^{-9}x,\ \gamma=\alpha^{45}$라 두면 $y^2+y=\alpha^{45}$이 된다. $\alpha^{45}=\alpha^5+\alpha^2+1(=100101)$이므로 방정식의 해는 $y_1=\gamma\cdot T=(010111)=\alpha^{26}$이고 $y_2=y_1+1=\alpha^{26}+1=\alpha^{19}$이다. 따라서 주어진 방정식의 해는 $x_1=\frac{B}{A}y_1=\alpha^{35}$과 $x_2=\alpha^{28}$이다.

$n=2m,\ m=4k\,(k\geq 2),\ d=3\cdot 2^m-2$일 때 비선형 이진수열을 $s_a^r(t)=Tr_1^m\left\{\left[Tr_m^n(a\alpha^t+\alpha^{dt})\right]^r\right\}$라 두면 두 수열 $s_a^r(t)$와 $s_b^r(t)$의 상호상관함수 $C_{a,b}(\tau)$는 다음과 같이 정의된다[12].

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

여기서 $Q=2^m+1$라 두고 t를 t_1Q+t_2 $(0\leq t_1\leq 2^m-2,\ 0\leq t_2\leq 2^m)$로 나타내면 $C_{a,b}(\tau)$는

$$C_{a,b}(\tau)=\sum_{t_1=0}^{2^m-2}\sum_{t_2=0}^{2^m}(-1)^{Tr_1^m\left\{\beta^r H(t_2,\tau,r)\right\}}$$

이다. 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. 그런데 $\gcd(r,2^m-1)$이므로 $H(t_2,\tau,r)=0$의 해의 개수와 $H(t_2,\tau,1)=0$의 해의 개수는 같다[12]. $H(t_2,\tau,1)=0$에서 $\alpha=\gamma\delta(\delta^{2^m-1}=1,\gamma^{2^m+1}=1)$라 두고, $x=\gamma^{2^{t_2}}$라 두면 다음과 같은 연립 방정식이 유도된다.

$$\begin{cases}x^5+bx^3+b^{2^m}x^2+1=0\ (b\in GF(2^m))\\x^{2^m+1}=1\end{cases}\tag{4}$$

본 논문에서는 주어진 연립방정식을 분석하고 5개의 해를 갖는 조건을 제시하며 그것을 판단하는 알고리즘을 제안한다.

III. 방정식의 서로 다른 해의 개수

$n=2m, m=4k$일 때 $x\in GF(2^n)$에 대하여 $\bar{x}=x^{2^m}$라 정의하자. 그러면 $GF(2^n)$의 원소 x,y에 대하여 다음이 성립한다.

(ⅰ) $\overline{x+y}=\bar{x}+\bar{y}$.

(ⅱ) $x+\bar{x}\in GF(2^m),\ x\bar{x}=x^{2^m+1}\in GF(2^m)$.

$GF(2^n)$의 단위원을

$$S=\{x\in GF(2^n)\,|\,x\bar{x}=1\}$$

라 정의하자. $\gcd(2^m-1,2^m+1)=1$이므로 $u,v\in\mathbb{N}$가 존재해서 $1=u(2^m-1)+v(2^m+1)$로 표현 할 수 있다. 따라서 $x=x^1=x^{u(2^m-1)+v(2^m+1)}=x^{u(2^m-1)}\cdot x^{v(2^m+1)}$이고, $x^{v(2^m+1)}=\delta,\ x^{u(2^m-1)}=\gamma$라 정의하면 $x=\delta\gamma$ 이다. 여기서 $\delta\neq 0$이고 $\delta^{2^m-1}=1$이므로 $\delta\in GF(2^m)^*$이다. $\gamma^{2^m+1}=1$이므로 $\gamma\in S$이다.

식(4)의 $x^{2^m+1}=1$을 만족하는 해의 개수는 많아야 2^m+1이다. 그런데 이 방정식의 해는 S의 원소가 된다. S의 각 원소는 $GF(2^n)$의 원시원소 α에 대하여 $\alpha^{u(2^m-1)}(0\leq u\leq 2^m)$ 로 나타낼 수 있으므로 S의 원소의 개수는 2^m+1이다.

따라서 $\{x\in GF(2^n)\,|\,x^{2^m+1}=1\}=S$이다.

식(4)의 해는 $\{x\in S\,|\,x^5+bx^3+\bar{b}x^2+1=0\}$와 같다. $x^5+bx^3+\bar{b}x^2+1=0$의 해를 구해 보자. $b\in GF(2^m)$이므로 $b^{2^m}=b$이다. 따라서

$$\begin{aligned}&x^5+bx^3+\bar{b}x^2+1=0\\&\Leftrightarrow(x+1)(x^4+x^3+(1+b)x^2+x+1)=0\end{aligned}\tag{5}$$

이다. $b=1$이면 식(5)는 $(x+1)^3(x^2+x+1)=0$이므로 방정식의 해는 1(삼중근)뿐이다.

<정리 1> 방정식 $x^4+x^3+(1+b)x^2+x+1=0$의 한 해가 η_1이면 $\overline{\eta_1}$도 해이다.

[증명] η_1이 방정식의 해이므로

$$\eta_1^4+\eta_1^3+(1+b)\eta_1^2+\eta_1+1=0$$

이고 양변을 2^m제곱하면 $1+b\in GF(2^m)$이므로 다음이 성립한다.

$$\overline{\eta_1}^4+\overline{\eta_1}^3+(1+b)\overline{\eta_1}^2+\overline{\eta_1}+1=0 \qquad \square$$

정리 1에 의해 방정식 $x^5+bx^3+\bar{b}x^2+1=0$의 해의 개수 N은 1 또는 3 또는 5이다. 방정식의 해의 개수가 5라고 하면 주어진 방정식은 다음과 같이 나타낼 수 있다.

$$\begin{aligned}&x^5+bx^3+bx^2+1\\&=(x+1)(x+\eta_1)(x+\overline{\eta_1})(x+\eta_2)(x+\overline{\eta_2})\\&=(x+1)(x^2+(\eta_1+\overline{\eta_1})x+1)(x^2+(\eta_2+\overline{\eta_2})x+1)\end{aligned}$$

여기서 $\eta_1,\eta_2\in S$이다. $\eta_1+\overline{\eta_1}=u$, $\eta_2+\overline{\eta_2}=v$라 하면 $u, v\in GF(2^m)$이고,

$$\begin{aligned}&x^4+x^3+(1+b)x^2+x+1\\&=(x^2+ux+1)(x^2+vx+1)\end{aligned} \tag{6}$$

이므로 $u+v=1$, $uv=1+b$이다. 또한 식(6) 각 이차방정식 $x^2+ux+1=0$, $x^2+vx+1=0$이 S에서 서로 다른 해를 갖기 위해서는 $Tr(1/u)=Tr(1/v)=1$이어야 한다. 만약 $Tr(1/u)=0$이면 방정식 $x^2+ux+1=0$은 $GF(2^m)$에서 해를 가지므로 S에서 해가 존재하지 않게 된다. 이제 주어진 b에 대하여 $u+v=1, uv=1+b$가 되는 u와 v는 $X^2+X+(1+b)=0$ 의 해이다. 따라서 $Tr_1^m(b+1)=0$이면 $GF(2^m)$의 원소인 u와 v가 존재한다. m이 짝수이므로 $Tr_1^m(1+b)+Tr_1^m(b)$이다. 그러므로 다음 정리 2가 성립한다.

<정리 2> $n=2m, m=4k$일 때, 방정식 $x^5+bx^3+\bar{b}x^2+1=0 (x\in S)$의 해의 개수가 5이면 $Tr(b)=0$, $Tr(1/u)=Tr(1/v)=1$이다. $\square$

다음은 설계된 수열의 상호상관관계의 효율적인 빈도분석을 할 수 있는 중요한 정리이다.

<정리 3> mod (2^m-1)에 관한 원분잉여류의 두 원소 $\beta_1,\beta_2\in GF(2^m)\setminus\{0,1\}$에 대하여 다음 두 방정식의 해의 개수는 같다.

$$x^5+\beta_1x^3+\overline{\beta_1}x^2+1=0 \tag{7}$$

$$x^5+\beta_2x^3+\overline{\beta_2}x^2+1=0 \tag{8}$$

[증명] β_1과 β_2가 같은 동치류의 원소이므로 $\beta_2=\beta_1^{2^i}$로 표현될 수 있다. 따라서 식(8)은

$$x^5+\beta_1^{2^i}x^3+\overline{\beta_1}^{2^i}x^2+1=0 \tag{9}$$

이다. $\gcd(2^i,2^m+1)=1$이므로 x대신에 x^{2^i}을 대입하여도 근의 개수는 변하지 않는다. 따라서 식(9)는

$$\begin{aligned}&x^{5\cdot 2^i}+\beta_1^{2^i}x^{3\cdot 2^i}+\overline{\beta_1}^{2^i}x^{2\cdot 2^i}+1=0\\&\Leftrightarrow\quad \left(x^5+\beta_1x^3+\overline{\beta_1}\,x^2+1\right)^{2^i}=0\end{aligned}$$

따라서 식(7)과 식(8)의 방정식의 근의 개수는 같고 식(7)의 해가 γ_1이라면 식(8)의해는 γ^{2^i}이다.$\square$

정리 3은 수열의 상호상관관계의 빈도분석을 하기 위해 $GF(2^m)$의 모든 원소 b에 대하여 방정식을 풀 필요가 없고 원분잉여류의 대표원에 대해서만 풀면 된다는 것을 뒷받침하고 있다. $I_2(d)$를 $GF(2)$위에서의 d차 기약다항식의 개수라고 할 때 $GF(2^m)$에서 생성되는 원분잉여류의 총 개수는 $-1+\sum_{d|m}I_2(d)$이다[14]. 그러므로 이 개수만큼의 대표원 $b(\neq 0,1)$에 대하여 조사하면 5개의 해를 갖는 경우를 모두 찾을 수 있다.

1	2	4	8	16	32	64	128
3	6	12	24	48	96	192	129
5	10	20	40	80	160	65	130
7	14	28	56	112	224	193	131
9	18	36	72	144	33	66	132
11	22	44	88	176	97	194	133
13	26	52	104	208	161	67	134
15	30	60	120	240	225	195	135
17	34	68	136				
19	38	76	152	49	98	196	137
21	42	84	168	81	162	69	138
23	46	92	184	113	226	197	139
25	50	100	200	145	35	70	140
27	54	108	216	177	99	198	141
29	58	116	232	209	163	71	142
31	62	124	248	241	227	199	143
37	74	148	41	82	164	73	146
39	78	156	57	114	228	201	147
43	86	172	89	178	101	202	149
45	90	180	105	210	165	75	150
47	94	188	121	242	229	203	151
51	102	204	153				
53	106	212	169	83	166	77	154
55	110	220	185	115	230	205	155
59	118	236	217	179	103	206	157
61	122	244	233	211	167	79	158
63	126	252	249	243	231	207	159
85	170						
87	174	93	186	117	234	213	171

그림 1. $GF(2^8)$의 원분잉여류
Fig. 1 $GF(2^8)$ cyclotomic cosets

[예제] $n=16, m=8, f(x)=x^{16}+x^{15}+x^{12}+x^{10}+1$이고, α를 $GF(2^{16})$의 한 원시근이라 하자. $\beta=\alpha^{2^8+1}$이라 두면 $\beta^8+\beta^6+\beta^5+\beta^4+1=0$을 만족하고, β를 한 원시근으로 하는 부분체 $GF(2^8)$가 생성된다.
$b=\beta^{17}$이라 할 때, $x^5+\beta^{17}x^3+\overline{\beta^{17}}x^2+1=0, x\in S$의 해의 개수를 구해보자.

$$x^5+\beta^{17}x^3+\overline{\beta^{17}}x^2+1$$
$$=(x+1)(x^4+x^3+(1+\beta^{17})x^2+x+1)$$

이므로 $x=1$이 아닌 다른 해를 갖는다면 $Tr(1+\beta^{17})=Tr(\beta^{204})=0$이어야 한다. 그런데 $Tr(\beta^{204})=0$이다. 그리고 기저행렬 T와 β^{204}의 이진표현은 다음과 같다.

$$T=\begin{pmatrix}1&1&1&0&1&0&0&1\\0&0&0&1&0&0&0&0\\0&1&0&1&0&1&0&1\\0&1&0&0&0&1&1&1\\1&1&0&0&1&0&0&0\\0&0&0&0&0&0&1&1\\0&0&0&1&1&1&0&1\\1&1&0&1&1&0&0&1\end{pmatrix},\ \beta^{204}=(10010110)$$

따라서 $u=(b+1)T=(10110000)=\beta^{158}$이고, $v=u+1=\beta^{65}$이다. 이제 각 u,v에 대해 $Tr(1/u)=Tr(\beta^{97})=1$, $Tr(1/v)=Tr(\beta^{190})=1$이다. 따라서 5개의 해를 갖는다.

표 1. b에 대한 방정식의 해의 개수
Table 1. Number of solutions to equation according to b

N	$i(b=\beta^i)$
3	1, 9, 19, 39, 47, 59, 127
5	17, 31, 45, 55, 63

그림 1은 $GF(2^8)$에서 0을 제외한 원분잉여류이며 첫 열은 각 원분잉여류의 대표원이다. 표 1은 $GF(2^8)$의 동치류 대표원에 대한 방정식 $x^5+bx^3+\bar{b}x^2+1=0(x\in S)$의 해의 개수 N이 3인 경우와 5인 경우를 나타낸다. 표 2는 n의 변화에 따른 원분잉여류의 개수이다. 이는 정리 3에 의해 모든 $GF(2^n)$의 원소 b를 풀지 않고 원분잉여류의 수만큼 풀면 되므로 계산량을 효율적으로 줄일 수 있음을 알 수 있다. 그림 2는 주어진 b에 대하여 5차 방정식 $x^5+bx^3+\bar{b}x^2+1=0(x\in S)$의 해의 개수를 결정짓는 알고리즘이다.

Input : n, b
Output : N(number of different solutions)
Step 1. Compute $Tr_1^m(b)$.
If $Tr_1^m(b)=0$, $N=1$.
Step 2. Find u, v such that $u+v=1, uv=b+1$.
Step 3. Compute $Tr_1^m(1/u)$, $Tr_1^m(1/v)$.
Step 4. Find N and solutions to equation such that $Tr(\cdot)=1$ in step 3.

그림 2. 방정식의 해의 개수 계산 알고리즘
Fig. 2 Counting algorithm for number of different solutions to equation

표 2. 원분잉여류의 개수
Table 2. Number of cyclotomic cosets

n	Number of $GF(2^n)^*$	Number of cyclotomic cosets
7	127	19
8	255	35
9	511	59
10	1023	107
11	2047	187
12	4095	351
13	8191	631
14	16383	1181
15	32767	2191
16	65535	4115

Ⅳ. 결 론

본 논문에서는 $n=2m$일 때 $GF(2^n)$ 위에서 수열의 상호상관관계에 대한 빈도분석을 위해 중요한 요소가 되는 방정식 $y^5+by^3+b^{2^m}y^2+1=0$의 해의 유형과 서로 다른 해의 개수를 결정하는 알고리즘을 제안하였다. 이 알고리즘은 수열 발생에서 사용하고 있는 트레이스 함수를 이용하여 해의 존재여부를 판단하였으며 실제 5차 방정식을 푸는 것이 아니라 2차 방정식을 풀어 5차 방정식의 해를 구하는 방법을 제안하였다. 이는 기존의 Kloosterman 합이라는 함수를 이용하여 계산하는 알고리즘에 비하여 매우 효율적이라

사료된다. 또한 동치류의 대표원에 대해서만 주어진 방정식을 풀어 $GF(2^m)$의 모든 원소 b에 대해 방정식의 해를 구할 수 있음을 보였다.

참고 문헌

[1] M. K. Simon, J. K. Omura, R.A. Sholtz and B. K. Levitt, “Spread Spectrum Commu- nications”, Rockville, MD : Computer Sci., Vol. Ⅰ, 1985.

[2] Y. Niho, "Multi-valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences", Ph.D. thesis, Univ. of Southern California, 1972.S.

[3] W. Golomb, “Shift-Register Sequences”, Laguna Hills, CA : Aegean Park, 1982.

[4] R. Gold, “Maximal recursive sequences with 3-valued recursive cross-correlation functions”, IEEE Trans. Inform. Theory, IT-14, pp. 154-156, 1968.

[5] 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.

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

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

[8] M.J. Kwon and S.J. Cho, “The distribution of the values of the cross-correlation function between the maximal period binary sequences,” The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 8, No. 6, pp. 891-898, 2013.

[9] M.J. Kwon, S.J. Cho, S.H. Kwon, J.G. Kim, H.D. Kim, U.S. Choi, “New Decimations with 4-Valued Cross- Correlations”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 7, No. 4, pp. 827-832, 2012.

[10] U.S. Choi and S.J. Cho, “Analysis of Cross-Correlation of m-sequences and Equation on Finite Fields”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 7, No. 4, pp. 821-826, 2012.

[11] S.J. Cho, J.M. Yim, J.G. Kim and S.T. Kim, “Extended sequences of sequences generated by GMW sequences and No sequences”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 7, No. 2, pp. 271-277, 2012.

[12] J.G. Kim, S.J. Cho, H.D. Kim and U.S. Choi, “New decimations with 5-level cross- correlation and large linear span”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 8, No. 2, pp. 263-269, 2013.

[13] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendalh, "Niho type cross-correlation function via Dickson polynomials and Kloosterman sums", IEEE Trans. Inf. Theory, Vol. 52, No. 2, pp. 613-627, 2006.

[13] S.J. Cho, Finite fields and its applications, Kyowoosa, 2007.

[14] R. McEliece, “Finite fields for computer scientists and engineers”, Kluwer Academic Publisher, Boston, 1987.

저자 소개

최언숙(Un-Sook Choi)

1992년 성균관대학교 산업공학과 공학사

2000년 부경대학교 응용수학과 이학석사

2004년 부경대학교 응용수학과 이학박사

2009년 부경대학교 정보보호학과 공학박사

2006년~현재 동명대학교 자율전공학부 조교수

※ 관심분야 : 셀룰라 오토마타론, 정보보호, 암호이론

조성진(Sung-Jin Cho)

1979년 강원대학교 수학교육학과 이학사

1981년 고려대학교 수학과 이학석사

1988년 고려대학교 수학과 이학박사

1988년~현재 부경대학교 응용수학과 교수

※ 관심분야 : 셀룰라 오토마타론, 정보보호