情報保護學會論文誌
第12券 第2號, 2002. 4

차균형성질을 갖는 d-동차함수로부터 생성된 새로운 순회상대차집합*

김 상 효**, 노 종 선***

New Cyclic Relative Difference Sets Constructed from d-Homogeneous Functions with Difference-balanced Property

Sang-Hyo Kim**, Jong-Seon No***

요 약

본 논문에서는 q는 소수 p의 멱승이고, F_{q^n}이 원소의 개수가 q^n개인 유한체라 할 때, $F_{q^n}\setminus\{0\}$으로부터 F_q로의 차균형 성질을 갖는 d-동차함수로부터 $\left(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2}\right)$ 순회상대차집합이 얻어질 수 있음을 보인다. 이에 따라 주기가 q^n-1이고, 이상적인 자기상관성질을 갖는 p진 시퀀스 Helleseth-Gong 시퀀스 및, d-형 시퀀스로부터 $\left(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2}\right)$의 파라미터를 갖는 새로운 순회상대차집합을 생성시킨다.

ABSTRACT

In this paper, for any prime power q, it is shown that new cyclic relative difference sets with parameters $\left(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2}\right)$ can be constructed by using d-homogeneous functions on $F_{q^n}\setminus\{0\}$ over F_q with difference-balanced property, where F_{q^n} is a finite field with q^nelements. Several new cyclic relative difference sets with parameters $\left(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2}\right)$ are constructed by using p-ary sequences of period q^n-1 with ideal autocorrelation property introduced by Helleseth and Gong and d-form sequences.

keyword : *Difference sets, Cyclic difference sets, Relative difference sets, d-homogeneous functions*

I. 서 론

Singer 파라미터 $\left(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1}\right)$를 갖는 순회차집합이 주기가 소수의 멱승인 q에 대하여 q^n-1이고, 이상적인 자기상관특성을 갖는 의사불규칙 시퀀스와 등가라는 것은 알려진 사실이다.[1,4,10] No는 차균형 성질을 갖는 d-동차함수로부터 Singer 파라미터를 갖는 새로운 순회차집합의 생성법을 제시하였다.[14] $p=3$일 때, Helleseth-Kumar-Martinsen (HKM) 시퀀스로부터 새로운 순회차집합이 생성되었다.[8,14] 근래에는 Chandler와 Xiang이 HKM 시퀀스로부터 $q=3^e$에 대해서 $\left(\frac{q^{3n}-1}{q-1}, q-1, q^{3n-1}, q^{3n-2}\right)$의 파라미터를 갖는 순회상대차집합을 생성하였다.

G는 위수(order)가 $u \cdot v$인 곱셈군이고, N은 위수가

---

* 본 연구는 BK21과 ITRC 지원 및 관리로 수행되었습니다.
** 서울대학교 전기·컴퓨터공학부(kimsh@ccl.snu.ac.kr) 박사과정
*** 서울대학교 전기·컴퓨터공학부(jsno@snu.ac.kr) 부교수

u인 정규부분군(normal subgroup)이라 한다. k개의 원소를 갖는 G의 부분집합 D가 있을 때, $k(k-1)$의 원소를 갖는 집합

$$\{d_1d_2^{-1} \mid d_1, d_2 \in D,\ d_1 \neq d_2\}$$

가 단위원(identity)을 제외한 $G\setminus N$의 모든 원소를 정확히 λ번씩 포함하고, N의 원소는 포함하지 않을 때, D는 G내의 N에 상대적인 (v, u, k, λ) 상대차집합이라 한다. 그러므로, 상대차집합의 파라미터는 다음과 같은 식을 만족시킨다.

$$k(k-1) = u(v-1)\lambda$$

만약 G가 순회군이면, D는 순회상대차집합이라 한다. 또한 $u=1$이면, D는 일반적인 (v, k, λ) 차집합이 된다. 두 순회상대차집합 D_1, D_2에 대해서 $D_1^h = \{d^h \mid d \in D_1\}$이고, $D_2g = \{dg \mid d \in D_2\}$라 할 때, $D_1^h = D_2g$를 만족시키는 $\gcd(h, uv) = 1$인 정수 h과 $g \in G$가 존재하면, D_1, D_2는 서로 등가이다.

본 논문에서는 q는 소수의 멱승이고, F_{q^n}이 원소의 개수가 q^n개인 유한체라 할 때, $F_{q^n}\setminus\{0\}$으로부터 F_q로의 차균형 성질을 갖는 d-동차함수로부터 $\left(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2}\right)$ 순회상대차집합이 얻어질 수 있음을 보인다. 이에 따라 주기가 q^n-1이고, 이상적인 자기상관성질을 갖는 p진 시퀀스인 Helleseth-Gong 시퀀스 및, d-형 시퀀스로부터 $\left(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2}\right)$의 파라미터를 갖는 새로운 순회상대차집합을 생성시킨다.

II. 주 정리

q는 소수의 멱승이고, 어떤 양의 정수 e, m에 대하여, $n = e \cdot m > 1$이라 한다. 그러면, 유한체 F_{q^n}으로부터 F_{q^m}으로의 트레이스 함수 $tr_{q^m}^{q^n}(\cdot)$는 다음과 같이 정의된다.[12]

$$tr_{q^m}^{q^n}(x) = \sum_{i=0}^{e-1} x^{q^{m \cdot i}}$$

단, $x \in F_{q^n}$.

트레이스 함수가 다음의 성질들을 만족시킨다.

(i) $tr_{q^m}^{q^n}(ax+by) = a \cdot tr_{q^m}^{q^n}(x) + b \cdot tr_{q^m}^{q^n}(y)$ for all $a, b \in F_{q^m}$, $x, y \in F_{q^n}$

(ii) $tr_{q^m}^{q^n}(x^{q^m}) = tr_{q^m}^{q^n}(x)$, for all $x \in F_{q^n}$

(iii) $tr_q^{q^n} = tr_q^{q^m}\left(tr_{q^m}^{q^n}(x)\right)$, for all $x \in F_{q^n}$.

q는 소수의 멱승이라 하고, α가 F_{q^n}의 원시원일 때, $f(\alpha^t)$는 $F_{q^n}^*$으로부터 F_q로의 함수라 한다. 이때, $f(\alpha^0), f(\alpha^1), f(\alpha^2), \cdots, f(\alpha^{q^n-2})$에서 F_q상의 원소 '0'이 다른 모든 원소들 보다 단 한번만 적게 나오는 경우에 함수 $f(x)$는 F_q상에서 "균형"이라 한다. 또한 함수 $f(\alpha^{t+\tau}) - f(\alpha^t)$가 있을 때, $1 \le \tau \le q^n-2$인 모든 τ에 대해서 위의 함수가 균형이면, $f(\alpha^t)$는 "차균형"(difference balanced)이라 부른다.

Klapper는 d-동차함수를 제시하였고 이를 이용하여, d-형 시퀀스를 구성하였다. 여기서는 다음과 같은 F_{q^n}에서 F_q로의 d-동차함수에 대해 논한다.

$$H(xy) = y^d H(x), \quad x \in F_{q^n}, y \in F_q$$

차균형(difference-balanced)성질을 가진 d-동차 함수는 균형이라는 것은 이미 증명되었으며 다음과 같다.

[보조정리 1]

q는 소수의 멱승이고, n은 양의 정수라 하자. α가 유한체 F_{q^n}의 원시원이고, $f(\alpha^t)$는 F_{q^n}으로부터 F_q로의 함수라 한다. $f(\alpha^t)$가 d-동차이고 차균형이면, $f(\alpha^t)$는 균형이다. □

Chandler와 Xiang은 이미 언급된 Helleseth-Kumar-Martinsen의 이상적인 자기상관특성을 갖는 3진 시퀀스로부터 상대차집합을 발견했다.[3] 여기서는 다음의 정리와 같이 차균형인 d-동차함수를 이용하여 더 일반적인 방법으로 상대차집합을 생성시킨다.

[정리 2 (주정리)]

q는 소수의 멱승이라 하고, n은 1 보다 큰 양의 정수라 하자. α가 유한체 F_{q^n}의 원시원이고, $f(\alpha^t)$는 F_{q^n}으로부터 F_q로의 함수라 한다. $f(\alpha^t)$가 d-동차 및 차균형이고, d가 $q-1$과 서로 소이면, 다음과 같이 정의되는 집합

$$D = \{\alpha^t \mid f(\alpha^t) = 1,\ \alpha^t \in F_{q^n}^*\} \tag{1}$$

는 곱셈군 $F^*_{q^n}$내에서 F^*_q에 상대적인 순회상대차집합이며 다음과 같은 파라미터를 갖는다.

$$\left(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2}\right)$$

[증명]

보조정리 1로부터 $f(\alpha^t)$는 균형이고, 그러므로, t가 0에서 q^n-2까지 변할 때, $f(\alpha^t)=1$은 q^{n-1}번 나온다. 그러므로, D의 크기는 $k=q^{n-1}$이 된다.

$T=\frac{q^n-1}{q-1}$이라 하자. 그리고, $\beta=\alpha^T$라 하면, F_q의 원시원이 된다. d-동차인 성질을 이용하면, 다음의 관계를 얻을 수 있다.

$$\begin{aligned} f(\alpha^{t+iT}) &= \alpha^{di\cdot T}\cdot f(\alpha^t) \\ &= \beta^{di}\cdot f(\alpha^t) \end{aligned}$$

$\beta^{di}\neq 0$이므로, $f(\alpha^{t+iT})$는 $f(\alpha^t)=0$인 것과 필요충분조건이다. 그러므로, $0\le t\le T-1$에 대해서 $f(\alpha^t)=0$은 $\frac{q^{n-1}-1}{q-1}$번 나온다.

d는 $q-1$과 서로소이므로, $d\cdot d^{-1}=1 \mod q-1$이 성립한다. $f(\alpha^t)$대신에 1-동차함수인 $f(\alpha^{d^{-1}t})$를 생각하는 것이 가능하다. 그러므로, $f(\alpha^t)$는 1-동차함수라 가정하여도 일반성을 잃지 않는다.

이제 $1\le\tau\le q^n-2$인 모든 τ에 대해, $d_1\cdot d_2^{-1}=\alpha^{t+\tau}\cdot(\alpha^t)^{-1}=\alpha^\tau$를 만족시키며 D에 속하는 쌍 $\alpha^{t+\tau}$와 α^t이, $\tau\neq 0 \mod T$일 때, $\lambda=q^{n-2}$번 나오고, $\tau=0 \mod T$일 때는, 하나도 나오지 않음을 증명해야 한다. $\tau=0 \mod T$이면, α^τ는 정규부분군에 속하기 때문에 나오지 않는 것을 주지하자. 위의 증명은 $1\le\tau\le q^n-2$인 τ에 대해서, t가 $0\le t\le q^n-2$에서 변할 때, $(f(\alpha^{t+\tau}), f(\alpha^t))=(1,1)$이 $\tau\neq 0 \mod T$인 τ에 대해서 $\lambda=q^{n-2}$번 발생하고, $\tau=0 \mod T$일 때는 한번도 발생하지 않음을 증명하는 것과 같다.

경우 1) $\tau=0 \mod T$이고, $\tau\neq 0 \mod q^n-1$;

$0\le i\le q-2$인 정수 i에 대해서 $\tau=i\cdot T$라 하자. 그러면, $f(\alpha^t)$는 1-동차함수이므로,

$$f(\alpha^{t+iT})=\beta^i\cdot f(\alpha^t)$$

가 만족된다. 가 t가 $1\le t\le q^n-2$에서 변할 때, $(f(\alpha^{t+iT}), f(\alpha^t))=(1,1)$가 일어나지 않는 것은 명백하다. 그러므로, 어떤 $d_1, d_2\in D$에 대하여, $d_1 d_2^{-1}\neq\alpha^{iT}$이다. 이는 $d_1 d_2^{-1}\notin F^*_q$를 의미한다.

경우 2) $\tau\neq 0 \mod T$;

$0\le i,j\le q-2$인 i,j에 대해서 $x_i=\beta^i$, $x_j=\beta^j$라 하고, $x_\infty=0$이라 한다. 그리고, $a_{i,j}$는 t가 $1\le t\le q^n-2$에서 변할 때, 고정된 $x_i, x_j\in F_q$에 대해서 $(f(\alpha^{t+\tau}), f(\alpha^t))=(x_i, x_j)$가 일어나는 경우의 수라 한다. $f(\alpha^t)$가 차균형인 함수이므로, t가 $1\le t\le q^n-2$에서 변할 때, $\tau\neq 0 \mod T$인 τ에 대해서 $f(\alpha^{t+\tau})-f(\alpha^t)=x_i-x_j=0$는 $q^{n-1}-1$번 일어난다. 그러므로, 다음의 관계가 성립한다.

$$\sum_{i=0}^{q-2} a_{i,i}+a_{\infty,\infty}=q^{n-1}-1 \qquad (2)$$

어떤 정수 k에 대해서 다음의 쌍을 얻을 수 있다.

$$\begin{aligned} (f(\alpha^{t+\tau}), f(\alpha^{t+kT})) &= (f(\alpha^{t+\tau}), \beta^k\cdot f(\alpha^t)) \\ &= (x_i, \beta^k\cdot x_j) \end{aligned}$$

t가 $1\le t\le q^n-2$에서 변함에 따라 위의 쌍 $(x_i, \beta^k\cdot x_j)$는 $a_{i,j}$번 발생하고, $f(\alpha^{t+\tau})$와 $f(\alpha^t)$의 차 함수

$$f(\alpha^{t+\tau})-f(\alpha^{t+kT})=x_i-\beta^k\cdot x_j$$

는 균형이다. x_i, x_j의 표기를 이용하면, 두 수의 차를 다음과 같이 다시 쓸 수 있다.

$$x_i-\beta^k\cdot x_j=\begin{cases} x_i-x_{j+k}, & \text{for } x_j\neq 0, \\ x_i, & \text{for } x_j=0 \end{cases}$$

단, x_{j+k}의 아래첨자는 법(modulo) $q-1$로 계산된다. t가 $1\le t\le q^n-2$에서 변함에 따라 어떤 쌍이 발생하는 수는 다음과 같다.

$x_j\neq 0$ 에 대하여, (x_j, x_{j+k})는 $a_{i,j}$번 발생

$x_j=0$ 에 대하여, (x_i, x_∞)는 $a_{i,\infty}$번 발생

$x_j\neq 0$에 대해서, $x_i-x_{j+k}=\beta^i-\beta^{j+k}=0$은

$$j+k=i \mod q-1$$

을 뜻한다. 그리고, 이것은 $a_{i,j}=a_{i,i-k}$번 발생한다. $x_j=0$에 대해서는 $x_i-x_j=0$이 $a_{\infty,\infty}$번 발생한다. 또한, 차균형 성질을 이용하면, t가 $1\le t\le q^n-2$에서 변함에 따라 $f(\alpha^{t+\tau})-f(\alpha^{t+kT})=0$이 발생하는 수는 $q^{n-1}-1$이다. 그러므로, $0\le k\le q-2$인 k에 대해서 다음이 성립한다.

$$\sum_{i=0}^{q-2} a_{i,i-k}+a_{\infty,\infty}=q^{n-1}-1 \tag{3}$$

단, 첨자들은 모두 법 $q-1$로 계산된다. 그러므로, 식 (3)은 다음과 같이 다시 쓰여질 수 있다.

$$\begin{aligned}
&k=0: a_{0,0}+a_{1,1}\cdots+a_{q-2,q-2}+a_{\infty,\infty}=q^{n-1}-1\\
&k=1: a_{0,q-2}+a_{1,0}\cdots+a_{q-2,q-3}+a_{\infty,\infty}=q^{n-1}-1\\
&k=2: a_{0,q-3}+a_{1,q-2}\cdots+a_{q-2,q-4}+a_{\infty,\infty}\\
&\qquad =q^{n-1}-1\\
&\qquad\qquad \cdots\cdots\\
&k=q-2: a_{0,1}+a_{1,2}\cdots+a_{q-2,0}+a_{\infty,\infty}=q^{n-1}-1\\
&k=\infty: a_{0,\infty}+a_{1,\infty}\cdots+a_{q-2,\infty}+a_{\infty,\infty}=q^{n-1}-1
\end{aligned} \tag{4}$$

마지막 등식은 $f(\alpha^t)$가 균형이어서 $0\le t\le q^n-2$에서 $f(\alpha^t)$가 변할 때, 0이 $q^{n-1}-1$번 나온다는 사실로부터 얻어진 것이다. 위 식 (4)의 모든 좌항을 더하면, 다음을 얻을 수 있다.

$$LHS=\sum_{i=0}^{q-2}\left\{\sum_{j=0}^{q-2} a_{i,j}+a_{i,\infty}\right\}+q\cdot a_{\infty,\infty} \tag{5}$$

단, 위 식의 괄호안의 합은 (4)의 등식의 같은 열끼리의 합이다. 또한, 우항들의 합은 다음과 같다.

$$RHS=q\cdot(q^{n-1}-1) \tag{6}$$

식 (5)의 괄호 안의 합은 t가 $0\le t\le q^n-2$에서 변함에 따라 어떤 정해진 i에 대해서 $f(\alpha^{t+\tau})=\beta^i(\ne 0)$가 되는 회수임은 쉽게 증명되며, 이 값은 q^{n-1}이다.

식 (5)와 (6)으로부터, 다음의 관계를 얻을 수 있다.

$$(q-1)\cdot q^{n-1}+q\cdot a_{\infty,\infty}=q\cdot(q^{n-1}-1)$$

그러므로, $a_{\infty,\infty}$의 값은 $q^{n-2}-1$이 된다.

이제 $a_{0,0}$의 값을 알아야 한다. $a_{0,0}$는 t가 $0\le t\le q^n-2$에서 변할 때, $f(\alpha^{t+\tau}, f(\alpha^t))=(1,1)$이 발생하는 수이다. 만약 어떤 $t=t_1$에 대해서 $(f(\alpha^{t_1+\tau}), f(\alpha^{t_1}))=(1,1)$이라면 다음이 성립한다.

$$\begin{aligned}
&(f(\alpha^{t_1+\tau+T}), f(\alpha^{t_1+T}))\\
&\quad=(\beta\cdot f(\alpha^{t_1+\tau}),\beta\cdot f(\alpha^{t_1})) \qquad =(\beta,\beta)\\
&(f(\alpha^{t_1+\tau+2T}), f(\alpha^{t_1+2T}))\\
&\quad=(\beta^2\cdot f(\alpha^{t_1+\tau}),\beta^2\cdot f(\alpha^{t_1})) \qquad =(\beta^2,\beta^2)\\
&\qquad\qquad\cdots\cdots\\
&(f(\alpha^{t_1+\tau+(q-2)T}), f(\alpha^{t_1+(q-2)T}))\\
&\quad=(\beta^{q-2}\cdot f(\alpha^{t_1+\tau}),\beta^{q-2}\cdot f(\alpha^{t_1}))=(\beta^{q-2},\beta^{q-2})
\end{aligned}$$

그리고, 이것은 모든 $i=0,1,2,\cdots q-2$에 대하여 $a_{i,i}$가 같은 값을 가짐을 의미한다. 식 (2)와 $a_{\infty,\infty}=q^{n-2}-1$로부터 모든 i에 대하여 $a_{i,i}$는 q^{n-2}가 됨을 알 수 있으며 이로써 증명이 완성된다. □

만약 차균형 성질을 갖는 d-동차함수가 존재한다면 그로부터 순회상대차집합을 생성할 수 있을 것이다. 이어지는 장에서 그 생성과정을 보일 것이다.

Ⅲ. q진 시퀀스로부터 생성된 순회상대차집합

$f(\alpha^t)$가 $F_{p^n}^*$으로부터 F_p로의 함수라 하면, 이는 주기가 p^n-1인 p진 시퀀스로 생각할 수 있다. 먼저 주기가 L인 p진 시퀀스에 대해 생각해 보면, 주기적 자기상관 함수는 다음과 같이 정의된다.

$$R(\tau)=\sum_{t=0}^{L-1} w^{f(\alpha^{t+\tau})-f(\alpha^t)}$$

단, 여기서 w는 단위원 '1'의 p제곱근이다. 만약 이 자기상관함수가 다음과 같은 분포를 가지면, 이것은 이상적인 자기상관성질을 갖는다고 한다.

$$R(\tau)=\begin{cases} L, & \text{for } \tau=0 \bmod L\\ -1, & \text{for } \tau\ne 0 \bmod L\end{cases}$$

만약 $f(\alpha^t)$가 차균형이라면, 이것인 이상적인 자기상관성질을 갖는 것은 쉽게 증명될 수 있고, 그 역도 성립한다. 그러므로, 이전 장에서 소개된 정리에 의하면, 새로운 이상적인 자기상관 성질을 갖는 시

퀀스를 존재는 새로운 상대차집합의 존재를 뜻함을 알 수 있다.

최근에 Helleseth와 Gong은 이상적인 자기상관성질을 갖는 새로운 p진 시퀀스를 발견하였다.[7] 그리고, 이 시퀀스는 3진 시퀀스인 HKM 시퀀스[8]를 포함하는 것이다. Helleseth-Gong 시퀀스는 다음의 정리와 같이 주어진다.

[정리 3]

〔Helleseth, Gong[7]〕: p가 소수이고, α는 F_{p^n}의 원시원이라 하자. $q=p^k$이며, $n=(2m+1)\cdot k$라 하자. 또한 s는 $1\le s\le 2m$이며, $\gcd(s,2m+1)=1$을 만족한다. $b_0=2u_0$ 이고, $i=1,2,\cdots,m$에 대해서 $u_i=b_{2i}=b_{2m+1-2i}$일 때, $g(x)$를 다음과 같이 정의한다.

$$g(x)=\sum_{i=0}^{k}u_i\cdot x^{\frac{q^{2i}+1}{2}} \tag{7}$$

$b_0=\pm 1$이고, $i=1,2,\cdots,m$에 대해서 $b_{is}=(-1)^i$이라 하면, F_p상에서의 시퀀스는 다음과 같이 정의된다.

$$f(\alpha^t)=tr_p^{p^n}(g(\alpha^t)) \tag{8}$$

그리고, 위 시퀀스 $f(\alpha^t)$는 이상적인 자기상관성질을 갖는다. □

위의 시퀀스는 다음과 같이 다시 쓸 수 있고,

$$f(\alpha^t)=\sum_{i=0}^{m}u_i\cdot tr_p^{p^n}\left(\alpha^{\frac{q^{2i}+1}{2}t}\right) \tag{9}$$

이 시퀀스가 차균형 성질을 갖는 1-동차함수임을 보일 수 있다.

[보조정리 4]

식 (9)에서 정의된 함수 $f(\alpha^t)$는 차균형이고, $F^*_{p^n}$에서 F_p로의 1-동차함수이다.

[증명]

$T=\frac{p^n-1}{p-1}$이라 한다. 그러면 α^T는 F_p의 원시원이 된다. $0\le i\le m$인 정수 i에 대하여 다음이 성립하는 것은 명백하다.

$$\frac{q^{2i}+1}{2}=\frac{q^i+1}{2}(q^i-1)+1=1 \bmod p-1$$

그러므로 F_p내의 0이 아닌 원소 α^{jT}에 대해서 다음 식이 성립하는 것도 명백하다.

$$\alpha^{jT\cdot\left(\frac{q^i+1}{2}(q^i-1)+1\right)}=\alpha^{jT}$$

그러므로,

$$f(\alpha^{jT}\cdot\alpha^t)=\alpha^{jT}\cdot f(\alpha^t)$$

이것은 $f(\alpha^t)$는 $F^*_{p^n}$에서 F_p로의 1-동차함수이다.

t는 다음과 같은 T기저 표현 $t=t_1\cdot T+t_2$로 표현 가능하다. 단, $0\le t_1\le p-2$, $0\le t_2\le T-1$이다. 식 (9)에서 정의된 $f(\alpha^t)$의 2차원적 표현은 다음과 같이 주어질 수 있다.

$$\begin{aligned}f(\alpha^t)&=f(\alpha^{t_1T+t_2})\\&=\alpha^{t_1T}\cdot f(\alpha^{t_2})\end{aligned}$$

위의 식에서 고정된 t_2, $0\le t_2\le T-1$에 대한 주기 $p-1$인 부분 시퀀스는 $f(\alpha^{t_2})=0$일 때는 항상 0인 시퀀스가 되고, 아닌 경우에는 주기 $p-1$인 시퀀스 α^{t_1T}의 순회적 천이가 된다. 함수 $f(\alpha^t)$의 차는 다음과 같이 쓸 수 있다.

$$\begin{aligned}f(\alpha^{t+\tau})-f(\alpha^t)&=\alpha^{t_1T}\cdot f(\alpha^{t_2+\tau})-\alpha^{t_1T}\cdot f(\alpha^{t_2})\\&=\alpha^{t_1T}\cdot[f(\alpha^{t_2+\tau})-f(\alpha^{t_2})]\end{aligned}$$

그러므로, 위의 차 시퀀스 $f(\alpha^{t+\tau})-f(\alpha^t)$를 생각하면, 고정된 t_2, $0\le t_2\le T-1$에 대한 주기 $p-1$인 부분 시퀀스는 $f(\alpha^{t_2+\tau})=f(\alpha^{t_2})$일 때는 항상 '0'인 시퀀스가 되고, 아닌 경우에는 주기 $p-1$인 시퀀스 α^{t_1T}의 순회적 천이가 된다. 전체가 0은 아닌 부분 시퀀스내에서는 F_p내의 모든 0이 아닌 원소가 단 한 번씩만 나타난다. 이것은 차 시퀀스 $f(\alpha^{t+\tau})-f(\alpha^t)$의 전 주기동안 F_p상의 모든 0이 아닌 원소가 같은 수로 나타난다는 것을 의미한다. 그리고, 0이 아닌 τ에 대해서 $R(\tau)=-1$라는 사실은 차 시퀀스에서 F_p상의 '0'아닌 모든 원소가 나타나는 수가 같을 때, 0이 나타나는 경우는 그보다 1작다는 것을 의미한다는

것은 명백하다. 그러므로, $f(\alpha^t)$는 차균형이라는 사실이 증명되었다. □

l은 $l \mid k$을 만족시키는 양의 정수라 하면, $u_i \in F_p$ 일 때, 식 (9)의 시퀀스는 다음과 같이 다시 쓸 수 있다.

$$f(\alpha^t) = tr_p^{p^l}\left\{ \sum_{i=0}^{m} u_i \cdot tr_{p^l}^{p^n}\left(\alpha^{\frac{q^{2i}+1}{2}t}\right)\right\} \tag{10}$$

이 때, 함수 $h(\alpha^t)$를 다음과 같이 정의한다.

$$h(\alpha^t) = \sum_{i=0}^{m} u_i \cdot tr_{p^l}^{p^n}\left(\alpha^{\frac{q^{2i}+1}{2}t}\right) \tag{11}$$

그러면, 함수 $h(\alpha^t)$는 다음과 같은 성질을 갖는다.

[정리 5]

식 (11)에서 정의된 $h(\alpha^t)$는 차균형이고, $F^*_{p^n}$상에서 F_{p^l}로의 1-동차함수이다.

[증명]

$T = \frac{p^n-1}{p^l-1}$이라 한다. 그러면, α^T는 F_{p^l}의 원시원이다. $0 \le i \le m$인 정수 i에 대하여 다음이 성립하는 것은 명백하다.

$$\frac{q^{2i}+1}{2} = \frac{q^i+1}{2}(q^i-1)+1 = 1 \mod p^l-1$$

단, $q=p^k$이고, $l \mid k$이다. 그러면, 어떤 0이 아닌 F_{p^l}의 원소 α^{jT}에 대하여, 다음은 명백하다.

$$\alpha^{jT\cdot\left(\frac{q^i+1}{2}(q^i-1)+1\right)} = \alpha^{jT}$$

그러므로,

$$h(\alpha^{jT}\cdot\alpha^t) = \alpha^{jT}\cdot h(\alpha^t)$$

이고, 이것은 $h(\alpha^t)$는 $F^*_{p^n}$에서 F_{p^l}로의 1-동차함수임을 의미한다. t는 다음과 같은 T기저 표현 $t = t_1 \cdot T + t_2$로 표현가능하다. 단, $0 \le t_1 \le p^l-2$, $0 \le t_2 \le T-1$이다. 식 (10)에서 정의된 $f(\alpha^t)$의 2차원적 표현은 다음과 같이 주어질 수 있다.

$$\begin{aligned} f(\alpha^t) &= tr_p^{p^l}(h(\alpha^{t_1T+t_2})) \\ &= tr_p^{p^l}(\alpha^{t_1T}\cdot h(\alpha^{t_2})) \end{aligned}$$

어떤 정해진 t_2에 대해서 주기가 p^l-1인 부분 시퀀스는 $h(\alpha^{t_2})=0$일 때는 항상 '0'인 시퀀스가 되며, $h(\alpha^{t_2}) \ne 0$일 때에는 주기가 p^l-1인 m-시퀀스 $tr_p^{p^l}(\alpha^{t_1T})$의 순회적 천이가 된다. $f(\alpha^t)$의 차 함수는 다음과 같이 다시 쓸 수 있다.

$$\begin{aligned} & f(\alpha^{t+\tau}) - f(\alpha^t) \\ &= tr_p^{p^l}(\alpha^{t_1T}\cdot h(\alpha^{t_2+\tau})) - tr_p^{p^l}(\alpha^{t_1T}\cdot h(\alpha^{t_2})) \\ &= tr_p^{p^l}(\alpha^{t_1T}[h(\alpha^{t_2+\tau}) - h(\alpha^{t_2})]) \end{aligned}$$

그러므로, 위의 차 시퀀스 $f(\alpha^{t+\tau}) - f(\alpha^t)$를 생각하면, 고정된 t_2, $0 \le t_2 \le T-1$에 대한 주기 p^l-1인 부분 시퀀스는 $h(\alpha^{t_2+\tau}) = h(\alpha^{t_2})$일 때는 항상 '0'인 시퀀스가 되고, 아닌 경우에는 주기 p^l-1인 m-시퀀스 $tr_p^{p^l}(\alpha^t)$의 순회적 천이가 된다.

부분 시퀀스 $tr_p^{p^l}(\alpha^t)$의 한 주기 동안 F_p에서 '0'이 $p^{l-1}-1$번 나오는 것은 명백하다. 그리고, '0'이 아닌 원소는 각각 p^{l-1}번씩 나타나는 것은 잘 알려져 있다. t_2가 $0 \le t_2 \le T-1$에서 변할 때, $h(\alpha^{t_2+\tau}) = h(\alpha^{t_2})$인 경우가 B번 발생하고, 갖지 않은 경우가 $T-B$번 발생한다고 가정한다. 그러므로, $f(\alpha^t)$의 한 주기동안의 차 시퀀스에서 '0'은

$$(p^l-1)\cdot B + (p^{l-1}-1)(T-B)$$

번 발생하고, 나머지의 F_p의 모든 '0'이 아닌 원소는 $p^{l-1}(T-B)$번 나타난다. 보조정리 4를 이용하여, $f(\alpha^t)$는 균형이고, 다음을 얻을 수 있다.

$$\begin{aligned} (p^l-1)\cdot B + (p^{l-1}-1)(T-B) &= p^{n-1}-1 \\ p^{l-1}\cdot(T-B) &= p^{n-1} \end{aligned}$$

위의 식으로부터 계산하면, B는 $\frac{p^{n-l}-1}{p^l-1}$이고, $T-B = p^{n-1}$이 된다. 그리고, 다음과 같은 관계를 얻는다.

$$\begin{aligned} & h(\alpha^{t_1T+t_2+\tau}) - h(\alpha^{t_1T+t_2}) \\ &= \alpha^{t_1T}\cdot\{h(\alpha^{t_2+\tau}) - h(\alpha^{t_2})\} \end{aligned}$$

고정된 정수 t_2가 $h(\alpha^{t_2+\tau})-h(\alpha^{t_2})\neq 0$를 만족시킨다면, $h(\alpha^{t_1T+t_2+\tau})-h(\alpha^{t_1T+t_2})$는 t_1이 $0\leq t_1\leq p^l-2$에서 변함에 따라 F_{p^l}상의 모든 '0'이 아닌 원소를 정확히 한 번씩만 취한다. 그러므로, 차 시퀀스 $h(\alpha^{t+\tau})-h(\alpha^t)$에서 t가 $0\leq t\leq p^n-2$에서 변하는 동안 원소 '0'는

$$(p^l-1)\cdot B=p^{n-l}-1$$

번 나타난다. 그리고, F_{p^l}의 모든 '0'이 아닌 원소는

$$T-B=p^{n-l}$$

번 나타난다. 이렇게 $h(\alpha^t)$의 차균형 성질이 증명되었다. □

차균형이면서 1-동차함수인 $h(\alpha^t)$와 II장의 주정리를 이용하면 다음의 정리에서와 같이 새로운 순회상대차집합이 생성될 수 있다.

[정리 6]

$n=(2m+1)k$ 이고, l은 $l\,|\,k$를 만족시키는 양의 정수라 하자. $h(\alpha^t)$는 식 (11)에서 정의된 함수라면, 다음의 집합

$$D=\{\alpha^t\mid h(\alpha^t)=1,\ \alpha^t\in F^*_{p^n}\}$$

는 곱셈군 $F^*_{p^n}$내의 $F^*_{p^l}$에 상대적인 순회상대차집합이 되며, $\left(\frac{p^n-1}{p^l-1}, p^l-1, p^{n-l}, p^{n-2l}\right)$의 파라미터를 갖는다. □

정리 6의 순회상대차집합이 Chandler와 Xiang의 순회상대차집합을 $p=3$이고, $m=1$인 특별한 경우로서 포함시킨다는 것은 쉽게 알 수 있다.

[예제 7]

α는 F_{5^6}의 원시원이다. 그리고, $h(\alpha^t)$는 $F^*_{5^6}$로부터 F_{5^2}으로의 함수라 하고 다음과 같이 주어진다 하자.

$$h(\alpha^t)=\sum_{i=0}^{1}u_i\cdot tr^{5^6}_{5^2}\left(\alpha^{\frac{5^{4i}+1}{2}t}\right)$$
$$=2\cdot tr^{5^6}_{5^2}(\alpha^t)+tr^{5^6}_{5^2}(\alpha^{313t})$$

그러면 다음의 집합

$$D=\{\alpha^t\mid h(\alpha^t)=1,\ \alpha^t\in F^*_{5^6}\} \qquad (12)$$

는 $F^*_{5^2}$내의 $F^*_{5^2}$에 상대적인 순회상대차집합이며, $\left(\frac{5^6-1}{5^2-1}, 5^2-1, 5^4, 5^2\right)$의 파라미터를 갖는다. □

지금까지 알려진 $\left(\frac{5^6-1}{5^2-1}, 5^2-1, 5^4, 5^2\right)$의 파라미터를 갖는 유일한 순회상대차집합은

$$D=\{\alpha^t\mid tr^{5^6}_{5^2}(\alpha^t)=1,\ \alpha^t\in F^*_{5^6}\} \qquad (13)$$

이다. 컴퓨터 모의실험으로 식 (12)와 (13)에서 정의된 두 상대차집합이 비등가라는 것을 확인하였으며, 그러므로, 식 (12)에서 주어진 순회상대차집합은 새로운 것이다.

[14]에서 주어진 순회차집합의 생성방법을 이용하면, 다음의 집합

$$D=\{\alpha^t\mid h(\alpha^t)=0,\ \alpha^t\in F^*_{p^n}\}$$

은 Singer 파라미터 $\left(\frac{p^n-1}{p^l-1}, \frac{p^{n-l}-1}{p^l-1}, \frac{p^{n-2l}-1}{p^l-1}\right)$를 갖는 순회차집합이 된다. 이는 $h(\alpha^t)$이 차균형이며, 1-동차함수이기 때문이다.

[13]의 p진 d-형 시퀀스의 생성방법을 이용하면, 이상적인 자기상관특성을 갖는 Helleseth-Gong 의 새로운 시퀀스[7]로부터 p진 d-형 시퀀스를 얻어낼 수 있다.

l_1, l_2는 $l_1\,|\,l_2\,|\,k$를 만족시키는 양의 정수들이라 한다. 그러면 (11)에서 정의된 시퀀스는 다음과 같이 다시 쓸 수 있다.

$$f(\alpha^t)=tr^{p^{l_2}}_{p}\left\{\sum_{i=0}^{m}u_i\cdot tr^{p^n}_{p^{l_2}}(\alpha^t)\right\}$$

r을 $p^{l_2}-1$과 서로 소인 정수이며, $1\leq r\leq p^{l_2}-1$이라 한다. 그러면, 다음과 같은 이상적인 자기상관특성을 갖는 p진 d-형 시퀀스를 얻을 수 있다.

$$f_d(\alpha^t)=tr^{p^{l_2}}_{p}\left\{\left[\sum_{i=0}^{m}u_i\cdot tr^{p^n}_{p^{l_2}}\left(\alpha^{\frac{q^{2i}+1}{2}t}\right)\right]^r\right\}$$

이를 다시 쓰면,

$$f_d(\alpha^t)=tr_p^{p^{l_1}}\left\{ tr_{p^{l_1}}^{p^{l_2}}\left\{\left[\sum_{i=0}^{m} u_i \cdot tr_{p^{l_2}}^{p^n}\left(\alpha^{\frac{q^{2i}+1}{2}t}\right)\right]^r\right\}\right\}$$

$h_d(\alpha^t)$를 다음과 같이 정의한다.

$$h_d(\alpha^t)=tr_{p^{l_1}}^{p^{l_2}}\left\{\left[\sum_{i=0}^{m} u_i \cdot tr_{p^{l_2}}^{p^n}\left(\alpha^{\frac{q^{2i}+1}{2}t}\right)\right]^r\right\} \tag{14}$$

$f_d(\alpha^t)$가 이상적인 자기상관특성을 시퀀스라는 사실과 정리 5의 증명을 이용하면, $h_d(\alpha^t)$가 $F^*_{p^n}$에서 $F_{p^{l_1}}$위로의 차균형이고, r'-동차함수임을 보이는 것은 쉽다. 단, $r=r' \bmod p^{l_1}-1$이다.

그리고 $\gcd(r, p^{l_2}-1)=1$이므로, $\gcd(r', p^{l_1}-1)$을 보이는 것도 쉽다. 그러므로, 새로운 순회상대차집합이 다음의 정리와 같이 생성될 수 있다.

[정리 8]

$n=(2m+1)k$라 하자. 그리고, l_1, l_2는 $l_1|l_2|k$를 만족시키는 양의 정수들이다. $h_d(\alpha^t)$를 (14)에서 정의된 함수라 하면 집합

$$D=\{\alpha^t \mid h_d(\alpha^t)=0,\ \alpha^t \in F^*_{p^n}\}$$

는 $F^*_{p^n}$내에서 $F^*_{p^{l_1}}$에 상대적인 순회상대차집합이며 파라미터

$$\left(\frac{p^n-1}{p^{l_1}-1}, p^{l_1}-1, p^{n-l_1}, p^{n-2l_1}\right)$$

를 갖는다. □

(14)의 생성방법을 이용하면, $h_d(\alpha^t)$는 차균형이고, r'-동차함수이므로, 다음의 집합

$$D=\{\alpha^t \mid h_d(\alpha^t)=0,\ \alpha^t \in F^*_{p^n}\}$$

는 Singer 파라미터 $\left(\frac{p^n-1}{p^{l_1}-1}, \frac{p^{n-l_1}-1}{p^{l_1}-1}, \frac{p^{n-2l_1}-1}{p^{l_1}-1}\right)$를 갖는 순회차집합이 된다.

〔13〕의 통합 시퀀스의 생성방법과, Helleseth-Gong의 p진 시퀀스를 이용하면, Singer 파라미터를 갖는 새로운 순회차집합 및 새로운 순회상대차집합을 생성시킬 수 있다.

순회상대차집합의 비등가임을 증명하기 위해서 그것들의 p-rank를 이용한다. $p=3$, $m=1$인 경우는 Chandler와 Xiang에 이들의 p-rank를 구함으로써 정리 6의 새로운 상대차집합이 기존의 상대차집합과 비등가임을 증명하였다. 또한, 예제 7에서는 파라미터 $\left(\frac{5^6-1}{5^2-1}, 5^2-1, 5^4, 5^2\right)$을 가지며 같은 파라미터를 갖는 기존의 상대차집합 비등가인 상대차집합의 예를 제시하였다. 그러나, 새로운 정리 6과 정리 8에서 주어진 상대차집합의 일반적인 p-rank를 구하는 것은 어렵다.

참 고 문 헌

〔1〕 L.D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Springer Verlag, 1971.

〔2〕 T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Vol. 1, Second edition, Cambridge University Press, Cambridge, 1999.

〔3〕 D. Chandler and Q. Xiang, "Cyclic relative difference sets and their p-ranks," preprint, 2001.

〔4〕 J.F. Dillon and H. Dobbertin, "Cyclic difference sets with Singer parameters," preprint, 1999.

〔5〕 R. Evans, H. Hollman, C. Krattenthaler and Q. Xiang, "Gauss sums, Jacobi sums and p-ranks of cyclic difference sets," preprint, 1999.

〔6〕 B. Gordon, W.H. Mills and L.R. Welch, "Some new difference sets," *Canad. J. Math.*, Vol. 14, pp. 614~625, 1962.

〔7〕 T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation function," preprint, 2001.

〔8〕 T. Helleseth, P.V. Kumar and H.M. Martinsen, "A new family of ternary sequences with ideal two-level autocorrelation," preprint, 2001.

〔9〕 D. Jungnickel, "Difference sets," in *Contemporary Design Theory: A Coll- ection for Surveys*, J. Dinitz and D.R. Stinson eds. John Wiley and Sons, 1992.

[10] D. Jungnickel and A. Pott, "Difference sets: an introduction," in *Difference Sets, Sequences and their Corr- elation Properties*, eds., A. Pott, P.V. Kumar, T. Helleseth and D. Jungnickel, pp. 259~295, Amsterdam: Kulwer, 1999.

[11] A. Klapper, "d-form sequence: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 423-431, Mar. 1995.

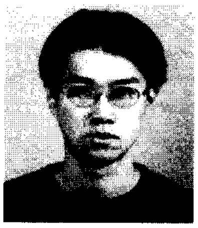
[12] R. Lidl and H. Niederreiter, *Finite Fields*, Vol. 20 of Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.

[13] J.S. No, "p-ary unified sequences: p-ary extended d-form sequences with ideal autocorrelation properties," preprint, 2001.

[14] J.S. No, "New cyclic difference sets with Singer parameters constructed from d-homogeneous function," preprint, 2001.

[15] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.* Vol. 43, pp. 377~385, 1938.

〈著者紹介〉



김 상 효 (Sang-Hyo Kim)
1998년 2월 : 서울대학교 전기공학부 공학사
2000년 2월 : 서울대학교 대학원 전기공학부 공학석사
2000년 3월~현재 : 서울대학교 대학원 전기컴퓨터공학부 박사과정
〈관심분야〉 시퀀스, 오류정정부호, 암호학, 이동통신

노 종 선 (Jong-Seon No) 종신회원
1981년 2월 : 서울대학교 전자공학과 공학사
1984년 2월 : 서울대학교 대학원 전자공학과 공학석사
1988년 5월 : University of Southern California, 전기공학과 공학박사
1988년 2월~1990년 7월 : Hughes Network Systems, Senior MTS
1990년 9월~1999년 7월 : 건국대학교 전자공학과 부교수
1999년 8월~현재 : 서울대학교 전기·컴퓨터공학부 부교수
〈관심분야〉 시퀀스, 오류정정부호, 암호학, 이동통신