情報保護學會論文誌
第12券 第1號, 2002. 2

d-동차함수로부터 생성된 Singer 파라미터를 갖는 새로운 순회차집합*

노 종 선**

New Cyclic Difference Sets with Singer Parameters Constructed from d-Homogeneous Functions

Jong-Seon No**

요 약

본 논문에서는 소수 p의 멱승인 q에 대해서 주기 q^n-1인 q진 시퀀스(d-동차함수)로부터 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 새로운 순회차집합을 생성하였다. q가 3의 멱승일 때, Helleseth, Kumar, Martinsen의 주기가 q^n-1이고, 이상적인 자기상관성질을 갖는 3진 시퀀스로부터 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 새로운 순회차집합을 생성시킨다.

ABSTRACT

In this paper, for any prime power q, new cyclic difference sets with Singer parameter $\left(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1}\right)$ are constructed by using the q-ary sequences (d-homogeneous functions) of period q^n-1. When q is a power of 3, new cyclic difference sets with Singer parameter $\left(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1}\right)$ are constructed from the ternary sequences of period q^n-1 with ideal autocorrealtion found by Helleseth, Kumar and Martinsen.

keyword : *d-homogeneous functions, Cyclic difference sets, Pseudo-noise sequences*

Ⅰ. 서 론

시퀀스들은 스트림암호의 키스트림 그리고 블록암호의 S-box 등에 활용될 수 있어 암호학의 연구분야에서 중요한 연구의 주제가 되어왔다. 순회차집합의 특성함수(characteristic function)은 이상적인 자기상관특성을 갖는 의사 불규칙 시퀀스가 된다는 것은 잘 알려진 사실이다.[1,6] 즉, Singer 파라미터 $(2^n-1, 2^{n-1}-1, 2^{n-2}-1)$[2,3]을 갖는 순회차집합은 주기가 2^n-1인 이상적 자기 상관 특성을 갖는 2진 시퀀스와 등가이며, 다음과 같이 정의된다.

$$D=\{t \mid s(\alpha^t)=0,\ 0\le t\le 2^n-2\}$$

단, 위 식에서 α는 F_{2^n}의 원시원이다. 최근에 No, Chung, Yun[16], No, Golomb, Gong, Lee, Gaal[17]과, Dillon, Dobbertin[5]와 Xiang[7]등에 의해서 주기 2^n-1을 갖는 새로운 이상적인 자기상관성질

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

을 갖는 시퀀스들이 소개되었다. Dillon은 덧셈군의 푸리에 분석을 이용하여, No, Chung, Yun[16]과 No, Golomb, Gong, Lee, Gall[17]의 추측정리(conjecture)를 증명하였다. 또한 Dillon은 주기가 2^n-1인 이상적인 자기상관성질을 갖는 이진 시퀀스를 이용하여 Singer 파라미 $(2^n-1, 2^{n-1}-1, 2^{n-2}-1)$를 갖는 새로운 순회차집합을 생성하였다.

현재까지, $\left(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1}\right)$의 파라미터를 갖는 순회차집합에 관한 대부분의 연구는 이진 시퀀스로부터 생성시킨 것, q진 m-시퀀스로부터 생성시킨 것(Singer 차집합)[2], q진 GMW 시퀀스, (GMW 차집합)[3]에 관한 것들이 있다. Klapper는 d-동차함수라는 동차함수를 이용하여 만든 d-형 시퀀스를 소개하였다[13]. Helleseth, Kumar, Martinsen은 이상적인 자기상관성질을 갖는 새로운 3진 시퀀스를 발견하였다.[14] 이것은 p진 m-시퀀스, p진 GMW 시퀀스, p진 직렬 GMW 시퀀스를 제외하면 이상적인 자기상관특성을 갖는 유일한 시퀀스이다.

본 논문에서는 소수 p의 멱승인 q에 대해서 주기 q^n-1인 q진 시퀀스 d-동차함수)로부터 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 새로운 순회차집합을 생성시킨다. q가 3의 멱승일 때, Helleseth, Kumar, Martinsen의 주기가 q^n-1이고, 이상적인 자기상관성질을 갖는 3진 시퀀스로부터 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 새로운 순회차집합을 생성시킨다.

q가 소수의 멱승일 때, $f(\alpha^t)$는 F_{q^n}으로부터 F_q로의 함수라 한다. 단, F_{q^n} F_q는 각각 원소의 개수가 q^n, q인 유한체이다. 그리고, α는 F_{q^n}의 원시원이라 한다. $f(\alpha^t)$에서 t가 0에서 q^n-2까지 변할 때, F_q의 덧셈의 항등원인 원소 '0'이 다음 모든 원소들보다 1만큼 적게 나오면 이 시퀀스 $f(\alpha^t)$는 '균형'이라 한다. 그리고, $1 \le \tau \le q^n-2$인 τ에 대해서 함 $f(\alpha^{t+\tau})-f(\alpha^t)$를 생각하자. t가 $0 \le t \le q^n-2$에서 변할 때, 함수 $f(\alpha^{t+\tau})-f(\alpha^t)$가 균형이면 이를 '차균형'이라 한다. 단, α멱수는 법(modulo) q^n-1로 계산된다.

D를 k개의 원소를 갖고 법 v의 나머지로 계산되는 (v, k, λ) 차집합이라 하고 다음과 같이 정의된다 하자.

$$D = \{c_1, c_2, c_3, \cdots, c_k\} \tag{1}$$

그러면, $k(k-1)$개의 차 $c_i - c_j, i \ne j$에서 법 v의 나머지로 0이 모든 값이 정확히 λ번 씩 나온다. 그러므로, 다음이 성립한다.

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

$1 \le a, b \le v-1$인 두 정수 a, b에 대하여 $aD+b$는 다음과 같이 정의된다.

$$aD+b = \{a \cdot c_1 + b, a \cdot c_2 + b, \cdots, a \cdot c_k + b\}$$

두 차집합 D_1, D_2에 대하여 $D_1 = aD_2 + b$인 정수 a, b가 존재하면, 이 두 차집합은 등가라 한다.

식 (1)에서 정의된 순회차집합 D의 특성 시퀀스는 다음과 같이 정의되며, 이진 시퀀스가 된다.

$$c(t) = \begin{cases} 1, & \text{if } t \in D \\ 0, & \text{if } t \notin D \end{cases}$$

순회차집합 D의 p-rank는 특성 시퀀스 $c(t)$의 Z_p상의 선형 회귀 방정식의 차수를 뜻한다.

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.[10]

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

단, $x \in F_{q^n}$.

트레이스 함수를 이용한 다음의 함수는 주기가 q^n-1인 q진 m-시퀀스가 된다.

$$m(\alpha^t) = tr_q^{q^n}(\alpha^t) \tag{2}$$

이 m-시퀀스가 균형 및 차균형이라는 것은 쉽게 증명이 가능하다.

II. 주 정리

Klapper는 d-동차함수 $H(x)$를 소개했으며, d-형 시퀀스를 생성시키는데 이용했다.[13] 그의 논문

에서는 F_{q^n}으로부터 F_q로의 d-동차함수 $H(x)$는 $x \in F_{q^n}$과 $y \in F_q$에 대하셔 는 다음과 같은 성질을 만족시킨다.

$$H(yx) = y^d H(x)$$

d-동차성질을 이용하면, 차균형성질을 가진 d-동차함수는 균형이라는 것은 다음과 같이 증명할 수 있다.

[보조정리 1]

q가 소수의 멱승이고, n이 양의 정수라 하자. 또한 α는 유한체 F_{q^n}의 원시원이라 하고 $f(\alpha^t)$가 F_{q^n}에서 F_q로의 함수라 하자. 이 때, $f(\alpha^t)$가 차균형인 d-동차함수라면 $f(\alpha^t)$는 균형이다.

[증명]

$q=2$에 대해서, 이것은 쉽게 증명이 된다. $q>2$에 대해서, $T=\frac{q^n-1}{q-1}$이라 하자. 그러면 $\beta=\alpha^T$는 F_q의 원시원이 된다. $f(\alpha^t)$가 F_{q^n}에서 F_q로의 d-동차함수이므로, 다음의 관계를 얻을 수 있다.

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

$f(\alpha^t)$의 차균형 성질을 이용하면, 어떤 0이 아닌 τ에 대해서도, 차 시퀀스 $f(\alpha^{t+\tau}) - f(\alpha^t)$는 균형이다. $\tau=T$에 대해서는 $f(\alpha^t)$의 차가 다음과 같이 주어진다.

$$\begin{aligned} f(\alpha^{t+\tau}) - f(\alpha^t) &= \beta^d \cdot f(\alpha^t) - f(\alpha^t) \\ &= (\beta^d - 1) \cdot f(\alpha^t) \end{aligned}$$

$\beta^d - 1 \neq 0$은 명백하고, 그러므로, $f(\alpha^t)$은 균형이다. □

현재까지의 모든 Singer 파라미터를 갖는 순회차집합은 이진 시퀀스, q진 m-시퀀스, q진 GMW 시퀀스, q진 직렬 GMW 시퀀스등으로부터 얻어진 것이다. 이 장에서는 소수의 멱승인 q에 대해서 차균형성질을 갖는 d-동차함수를 이용하여 Singer 파라미터를 갖는 새로운 순회차집합이 생성될 수 있음을 보인다.

[정리 2 (주정리)]

q가 소수의 멱승이고, n이 2보다 큰 정수라 하자. 또한 α는 유한체 F_{q^n}의 원시원이라 하고 $f(\alpha^t)$가 F_{q^n}에서 F_q로의 함수라 하자. 이 때, $q-1$과 서로소인 d에 대해 $f(\alpha^t)$가 차균형인 d-동차함수라면 다음과 같이 정의되는 정수의 집합은 Singer 파라미터

$$\left(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1} \right) \tag{3}$$

를 갖는 차집합이 된다.

$$D = \left\{ t \,\middle|\, f(\alpha^t) = 0,\ 0 \le t \le \frac{q^n-1}{q-1} \right\}$$

[증명]

보조정리 1에 따르면, $f(\alpha^t)$는 균형이다. 그러므로, t가 0에서 q^n-2까지 변할 때, $f(\alpha^t)=0$은 $q^{n-1}-1$번 나온다.

t는 다음과 같이 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. 함수 $f(\alpha^t)$의 2차원적 표현은 다음과 같이 주어질 수 있다.

$$\begin{aligned} f(\alpha^t) &= f(\alpha^{t_1 T + t_2}) \\ &= \alpha^{d t_1 T} \cdot f(\alpha^{t_2}) \\ &= \beta^{d t_1} \cdot f(\alpha^{t_2}) \end{aligned}$$

$\beta^{d t_1} \neq 0$이므로, $f(\alpha^t)$가 0가 된다는 것 $f(\alpha^{t_2})=0$와 서로 필요충분조건이다. 그러므로, $0 \le t \le T-1$에 대해서, $f(\alpha^t)=0$이 $\frac{q^{n-1}-1}{q-1}$번 나온다. 그러므로, D의 원소의 개수 k는 $\frac{q^{n-1}-1}{q-1}$이다.

이제 어떤 0이 아닌 τ에 대해서 t가 $0 \le t \le T-1$내에서 변할 때 $(f(\alpha^{t+\tau}), f(\alpha^t)) = (0,0)$이 $\frac{q^{n-2}-1}{q-1}$번 나온다는 것을 증명하면 된다.

d는 $q-1$과 서로 소이므로 $d \cdot d^{-1} = 1 \bmod q-1$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.

$0 \le i, j \le q-2$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 $0 \le t \le q^n-2$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. $f(\alpha^t)$는 차균형성질로부터, 0이 아닌 τ에 대해서 t가 $0 \le t \le q^n-2$에서 변할 때,

$$f(\alpha^{t+\tau})-f(\alpha^t)=x_i-x_j=0$$

가 $q^{n-1}-1$번 발생함을 알 수 있다. 그러므로 다음의 식을 얻을 수 있다. $\sum_{i=0}^{q-2} a_{i,i}+a_{\infty,\infty}=q^{n-1}-1$.

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 $0 = T \le q^n-2$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

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

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

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

단, x_{j+k}의 아래첨자는 법(modulo) $q-1$로 계산된다. t가 $0 \le t \le q^n-2$에서 변함에 따라 어떤 쌍이 발생하는 수는 다음과 같다.

$x_j \ne 0$ 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.

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

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

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 $0 \le t \le q^n-2$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.

$$\sum_{i=0}^{q-2} a_{i,i-k}+a_{\infty,\infty}=q^{n-1}-1 \tag{4}$$

단, 첨자들은 모두 법 $q-1$로 계산된다. 그러므로, 식 (4)는 다음과 같이 다시 쓰여질 수 있다.

$$\begin{aligned}
k=0 &: a_{0,0}+a_{1,1}\cdots+a_{q-2,q-2}+a_{\infty,\infty}=q^{n-1}-1 \\
k=1 &: a_{0,q-2}+a_{1,0}\cdots+a_{q-2,q-3}+a_{\infty,\infty}=q^{n-1}-1 \\
k=2 &: a_{0,q-3}+a_{1,q-2}\cdots+a_{q-2,q-4}+a_{\infty,\infty} \\
&=q^{n-1}-1 \qquad \cdots\cdots \\
k=q-2 &: a_{0,1}+a_{1,2}\cdots+a_{q-2,0}+a_{\infty,\infty}=q^{n-1}-1 \\
k=\infty &: a_{0,\infty}+a_{1,\infty}\cdots+a_{q-2,\infty}+a_{\infty,\infty}=q^{n-1}-1
\end{aligned} \tag{5}$$

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 (5)의 모든 좌항을 더하면, 다음을 얻을 수 있다.

$$LHS=\sum_{i=0}^{q-2}\left\{\sum_{j=0}^{q-2} a_{i,j}+a_{i,\infty}\right\}+q \cdot a_{\infty,\infty} \tag{6}$$

단, 위 식의 괄호안의 합은 (5)의 등식들의 같은 열끼리의 합이다. 또한, 우항들의 합은 다음과 같다.

$$RHS=q \cdot (q^{n-1}-1) \tag{7}$$

식 (6)와 (7)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. $a_{i,j}$의 정의에 따르면, 0이 아닌 τ에 대해서 t가 0에서 q^n-2까지 변함에 따 $a_{\infty,\infty}$는

$$(f(\alpha^{t+\tau}), f(\alpha^t))=(0,0)$$

이 일어나는 수이다. $0 \le k \le q-2$인 한 정수 k에 대해서 다음이 만족된다.

$$(f(\alpha^{t+\tau+k \cdot T}), f(\alpha^{t+k \cdot T}))=(\beta^k \cdot f(\alpha^{t+\tau}), \beta^k \cdot f(\alpha^t))$$

그러므로, $0 \le t \le T-1$에 대 $(f(\alpha^{t+\tau+kT}), f(\alpha^{t+kT}))$이 $(0,0)$이라는 것은 $(f(\alpha^{t+\tau}), f(\alpha^t))=(0,0)$과 필요충분조건이다. 그러므로, $0 \le t \le T-1$에 대해서

$(f(\alpha^{t+\tau}), f(\alpha^t))=(0,0)$은 $\frac{q^{n-2}-1}{q-1}$번 발생한다. 그러므로 정리가 증명되었다. □

소수의 멱승인 q에 대해 위와 같은 Singer 파라미터를 갖는 순회차집합들로는 q진 m-시퀀스, GMW 시퀀스, 직렬 GMW 시퀀스 등을 이용하여 얻어진 것이 이미 알려져 있다. 그리고, 그 시퀀스 들은 다음과 같이 정의된다.

$$c_m(t)=tr_q^{q^m}(\alpha^t)$$
$$c_g(t)=tr_q^{q^m}\{[tr_{q^m}^{q^n}(\alpha^t)]^r\}$$
$$c_{cg}(t)=tr_q^{q^k}\{[tr_{q^k}^{q^m}\{[tr_{q^m}^{q^n}(\alpha^t)]^r\}]^u\}$$

단, α는 F_{q^n}의 원시원이고, k, m, n은 $k|m|n$을 만족시키는 정수들이다. 또 $\gcd(q^k-1, u)=1$, $1\le u\le q^k-2$이고, $\gcd(q^m-1, r)=1$, $1\le r\le q^m-2$이다. 위의 함수들이 차균형이고, d-동차함수라는 사실을 증명하는 것은 쉽다. 그러므로, 정리 2 는 q진 m-시퀀스, GMW 시퀀스, 직렬 GMW 시퀀스를 이용한 생성을 모두 포함한다.

위의 주 정리를 이용해서 순회차집합을 생성시키기 위하여 트레이스 함수를 이용한 d-동차함수가 다음의 정리에서 주어진다.

[보조정리 3]

q가 소수의 멱승이고, m, n은 양의 정수, m은 n의 약수라 하자. 또한, α는 유한체 F_{q^n}의 원시원이고 $T=\frac{q^n-1}{q^m-1}$에 대해 $\beta=\alpha^T$이라 하자. 이제 주어진 집합 I의 모든 원소 s에 대해 $s=d \bmod (q^m-1)$이 성립하면 다음과 같이 주어지는 유한체 F_{q^n}에서 유한체 F_{q^m}으로의 함수는 F_{q^n}에서 F_{q^m}으로의 d-동차함수이다.

$$H(\alpha^t)=\sum_{s\in I} tr_{q^m}^{q^n}(\alpha^{st}) \tag{8}$$

[증명]

β는 F_{q^m}의 원시원이다. 다음이 만족된다.

$$\begin{aligned}H(\beta\alpha^t)&=\sum_{s\in I} tr_{q^m}^{q^n}((\beta\alpha^t)^s)\\&=\sum_{s\in I}\beta^s\cdot tr_{q^m}^{q^n}((\alpha^t)^s)\\&=\sum_{s\in I}\beta^d\cdot tr_{q^m}^{q^n}((\alpha^t)^s)\\&=\beta^d\cdot\sum_{s\in I}\cdot tr_{q^m}^{q^n}((\alpha^t)^s)\\&=\beta^d\cdot H(\alpha^t)\end{aligned}$$

단, 집합 I에 속한 모든 s에 대해서 $s=d \bmod q^m-1$이므로, $\beta^s=\beta^d$이 된다. □

유한체 F_{q^n}에서 F_q으로의 d-동차함수 $H(\cdot)$를 사용하여 다음 정리에 나오는 차균형인 F_{q^n}에서 F_{q^m}으로의 d-동차함수를 얻을 수 있다.

[정리 4]

q가 소수의 멱승이고, m, n은 양의 정수, m은 n의 약수라 하자. 또한, α는 F_{q^n}의 원시원이고, $T=\frac{q^n-1}{q^m-1}$에 대해 $\beta=\alpha^T$이라 하자. 이제 주어진 집합 I에 대해 다음과 같이 주어진 F_{q^n}에서 F_{q^m}으로의 함수 $H(\beta^{t_1})$가 차균형이고 d-동차함수라 하자.

$$H(\beta^{t_1})=\sum_{a\in I} tr_q^{q^m}(\beta^{at_1}) \tag{9}$$

이 때, $1\le r\le q-2$이고 $q-1$과 서로 소인 정수 r에 대해 다음과 같이 정의되는 F_{q^n}에서 F_q으로의 함수 역시 차균형인 d-동차함수이다.

$$f(\alpha^t)=\sum_{a\in I} tr_q^{q^m}\{[tr_{q^m}^{q^n}(\alpha^t)]^{ar}\} \tag{10}$$

[증명]

여기서 q진 시퀀스로 $H(\beta^{t_1})$과 $f(\alpha^t)$를 생각하자. $H(\beta^{t_1})$이 차균형이라는 것은 당연하다. 그리고, 이것의 주기는 $M=q^m-1$이다.

t는 다음과 같이 T기저 표현 $t=t_1\cdot T+t_2$로 표현가능하다. 단, $0\le t_1\le M-1$, $0\le t_2\le T-1$이다. 식 (10) 의 함수 $f(\alpha^t)$는 다음과 같이 이차원적 표현으로 나타낼 수 있다.

$$\begin{aligned}f(\alpha^t)&=\sum_{a\in I} tr_q^{q^m}\{[tr_{q^m}^{q^n}(\alpha^t)]^{ar}\}\\&=\sum_{a\in I} tr_q^{q^m}\{[tr_{q^m}^{q^n}(\alpha^{t_1\cdot T+t_2})]^{ar}\}\\&=\sum_{a\in I} tr_q^{q^m}\{\alpha^{arTt_1}[tr_{q^m}^{q^n}(\alpha^{t_2})]^{ar}\}\\&=\sum_{a\in I} tr_q^{q^m}\{\beta^{art_1}[tr_{q^m}^{q^n}(\alpha^{t_2})]^{ar}\}\end{aligned}$$

앞의 $f(\alpha^t)$에서 t_2를 고정시킨 부분 시퀀스를 생각하자. 그러면, $tr_{q^m}^{q^n}(\alpha^{t_2})=0$일 때는 항상 '0'인 시퀀스가 되고, $tr_{q^m}^{q^n}(\alpha^{t_2})\neq 0$이면, 식 (9)에서 정의된 q진 시퀀스의 r로 데시메이티드된 시퀀스인 아래의 시퀀스의 순회적 천이가 된다.

$$H(\beta^{rt_1})=\sum_{a\in I} tr_q^{q^m}(\beta^{art_1})$$

위의 시퀀스는 $\gcd(q^m-1,r)=1$이므로, 주기가 M이 된다. $H(\beta^{t_1})$이 차균형이라는 가정을 했으므로, 이것은 균형이다. 즉, 한 주기동안에 '0'가 $q^{m-1}-1$번 나오고 F_q상의 '0'이 아닌 다른 모든 원소는 q^{m-1}번 나온다. $f(\alpha^t)$의 차는 다음과 같이 표현된다.

$$\begin{aligned} f(\alpha^{t+\tau})-f(\alpha^t) &= \sum_{a\in i} tr_q^{q^m}\{\beta^{art_1}[tr_{q^m}^{q^n}(\alpha^{t_2+\tau})]^{ar}\} \\ &\quad -\sum_{a\in i} tr_q^{q^m}\{\beta^{art_1}[tr_{q^m}^{q^n}(\alpha^{t_2})]^{ar}\} \\ &= \sum_{a\in I} tr_q^{q^m}\{\beta^{art_1}[\beta^{g(t_2+\tau)}]^{ar}\} \\ &\quad -\sum_{a\in I} tr_q^{q^m}\{\beta^{art_1}[\beta^{g(t_2)}]^{ar}\} \\ &= \sum_{a\in I} tr_q^{q^m}\{\beta^{ar(t_1+g(t_2+\tau))}-\beta^{ar(t_1+g(t_2))}\} \end{aligned} \quad (11)$$

단, $g(t_2)$는 다음과 같이 정의된다. $tr_{q^m}^{q^n}(\alpha^{t_2})\neq 0$일 때는 $\beta^{g(t_2)}=tr_{q^m}^{q^n}(\alpha^{t_2})$이 되고, $tr_{q^m}^{q^n}(\alpha^{t_2})=0$인 경우에는 $g(t_2)=-\infty$이다. 식 (11)의 차 시퀀스에서 t_2를 고정시킨 부분 시퀀스가 있을 때, 만약 $g(t_2+\tau)=g(t_2)$라면, 그 부분 시퀀스는 항상 0인 시퀀스가 되고, 그렇지 않으면 식 (9)의 시퀀스를 r로 데시메이트한 시퀀스의 순회적 천이가 된다. q^m진 m-시퀀스 $tr_{q^m}^{q^n}(\alpha^t)$는 차균형 성질을 갖고 있으므로, t_2가 0에서 $T-1$까지 변할 때, $g(t_2+\tau)=g(t_2)$ 는 $\frac{q^{n-m}-1}{q-1}$번 발생하고, 서로 다른 경우는 $T-\frac{q^{n-m}-1}{q-1}=q^{n-m}$번 발생한다. 그러므로, 차 시퀀스의 한 주기에서 $f(\alpha^{t+\tau})-f(\alpha^t)=0$은

$$\begin{aligned} &(q^m-1)\frac{q^{n-m}-1}{q^m-1} \\ &\quad +(q^{m-1}-1)\left(\frac{q^n-1}{q^m-1}-\frac{q^{n-m}-1}{q^m-1}\right)=q^{n-1}-1 \end{aligned}$$

번 발생한다. 그리고 F_a상의 0이 아닌 모든 다른 원소들은 각각

$$q^{m-1}\cdot q^{n-m}=q^{n-1}$$

번 발생한다. 그러므로, $f(\alpha^t)$는 차균형이다.

$H(\beta^{rt_1})$ d-동차함수이면, $f(\alpha^t)$도 d-동차함수가 되는 것은 자명하다. 그러므로, 정리가 증명되었다. □

이미 언급된 정리들을 이용해서 다음의 정리와 같이 새로운 순회차집합을 생성시킬 수 있다. 그리고, 이것은 GMW 차집합에 대응된다.[3]

[정리 5]

q는 소수의 멱승, $f(\alpha^t)$는 식 (10)어서 정의된 차균형인 d-동차함수라 하자. 또한, α는 확장 유한체 F_{q^n}의 원시원이라 하자. 이 때, 다음과 같이 정의되는 정수의 집합은 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 된다.

$$D=\left\{t \,\middle|\, f(\alpha^t)=0, 0\le t< \frac{q^n-1}{q-1}\right\}$$

□

사실상, 함수 $f(\alpha^t)$는 주기가 q^n-1인 q진 시퀀스로 생각될 수 있다. 다음의 장에서는 이상적인 자기상관특성을 갖는 q진 시퀀스로부터 순회차집합을 생성시킨다.

Ⅲ. q진 시퀀스로부터 생성된 순회차집합

소수 p에 대하여, F_{p^n}으로부터 F_p로의 함수 $f(\alpha^t)$는 주기 p^n-1인 p진 시퀀스가 된다. ω는 단위원 '1'의 p제곱근일 때, 주기적 자기상관함수 $R(\tau)$는 다음과 같이 주어진다. $R(\tau)=\sum_{t=0}^{N-1}\omega^{f(\alpha^{t+\tau})\cdot f(\alpha^t)}$

시퀀스 $f(\alpha^t)$가 다음의 자기상관함수를 가지면 이상적인 자기상관특성을 갖는다고 한다.

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

만약 함수 $f(\alpha^t)$가 차균형성질을 갖는다면 이것은 이상적인 자기상관특성을 갖는다는 것은 쉽게 증명할 수 있다.

최근에 Helleseth, Kumar, Martinsen은 이상적인 자기상관특성을 갖는 새로운 3진 시퀀스를 발견하였다. 이것은 p진 m-시퀀스, p진 GMW 시퀀스, p진 직렬 GMW 시퀀스를 제외하고는 최초의 비이진 시퀀스이다. 이 시퀀스는 다음의 정리에 주어진다.

[정리 6 (Helleseth, Kumar, Martinsen[14])]

양의 정수 k에 대해서 $s=3^{2k}-3^{k}+1$이라 하자. 또한 α는 유한체 $F_{3^{3k}}$의 원시원이라 하자. 그러면 다음과 같이 주어지는 주기가 $3^{3k}-1$인 3진 시퀀스는 이상적인 자기상관특성을 갖는다.

$$f(\alpha^t)=tr_3^{3^{3k}}(\alpha^t)+tr_3^{3^{3k}}(\alpha^{st}) \tag{12}$$

□

주기가 3^n-1인 3진 시퀀스가 이상적인 자기상관특성을 가진다면 차 시퀀스 $f(\alpha^{t+\tau})-f(\alpha^t)$의 한주기동안 에서 1, 2가 각각 3^{n-1}번씩 나오는 것은 자명한 사실이다. 그러므로, 0는 $3^{n-1}-1$번 나오고 따라서 이상적인 자기상관특성을 갖는 3진 시퀀스는 차균형성을 갖는다.

주어진 식 (12)에서 정의된 $f(\alpha^t)$안의 s는 모두 1 mod 2이므로, 다음의 관계를 얻을 수 있다.

$$f(\beta\cdot\alpha^t)=\beta\cdot f(\alpha^t),\quad \beta\in F_3$$

그러므로, $f(\alpha^t)$는 차균형이고, 1-동차함수이며, $f(\alpha^t)$에 대해 다음의 정리를 얻어낼 수 있다.

[정리 7]

양의 정수 k에 대해서 $s=3^{2k}-3^k+1$이라 하자. 또한 α는 유한체 $F_{3^{3k}}$의 원시원이라 하자. 이 때, 다음과 같이 정의되는 정수들의 집합은 Singer 파라미터 $\left(\frac{3^{3k}-1}{2},\frac{3^{3k-1}-1}{2},\frac{3^{3k-2}-1}{2}\right)$을 갖는 순회차집합이 된다.

$$D=\left\{t\,\middle|\,tr_3^{3^{3k}}(\alpha^t)+tr_3^{3^{3k}}(\alpha^{st})=0,\ 0\le t\le\frac{3^{3k}-1}{2}\right\} \tag{13}$$

□

합성 n에 대해서 유한체 F_{q^n}에서 F_q로의 d-동차이고, 차균형인 함수를 이용하여, 다음의 정리와 같이 유한체 F_{q^n}에서 F_{q^m}로 d-동차이고 차균형인 함수를 만들 수 있다.

[보조정리 8]

q가 소수의 멱승이고, m,n은 양의 정수, m은 n의 약수라 하자. 또한, α는 F_{q^n}의 원시원이라 하자. 이제, 주어진 집합 I에 대해 다음과 같이 주어진 F_{q^n}에서 F_q로의 함수 $c(\alpha^t)$가 차균형이고, I의 모든 원소 s가 $1\le d\le q^m-2$이고 q^m-1과 서로소인 d에 대해 $s=d \bmod q^m-1$을 만족한다고 가정하자.

$$c(\alpha^t)=\sum_{s\in I}tr_q^{q^n}(\alpha^{st}) \tag{14}$$

그러면, 다음과 같이 주어지는 F_{q^n}에서 F_{q^m}으로의 함수 $f(\alpha^t)$는 차균형인 d-동차함수가 된다.

$$f(\alpha^t)=\sum_{s\in I}tr_{q^m}^{q^n}(\alpha^{st}) \tag{15}$$

[증명]

정리 3과 모든 $s\in I$에 대해서 $s=d \bmod q^m-1$인 사실을 이용하면, $f(\alpha^t)$가 d-동차함수라는 것은 자명하다. $T=\frac{q^n-1}{q^m-1}$이라 한다 t를 $t=t_1\cdot T+t_2$와 같이 T기저 표현으로 나타낼 수 있다. 단, $0\le t_1\le q^m-2$, $0\le t_2\le T-1$이다. 그러면 위의 $c(\alpha^t)$는 다음과 같이 2차원적으로 표현하는 것이 가능하다.

$$\begin{aligned}
c(\alpha^t)&=\sum_{s\in I}tr_q^{q^n}(\alpha^{s\cdot(t_1\cdot T+t_2)})\\
&=\sum_{s\in I}tr_q^{q^m}\{tr_{q^m}^{q^n}(\alpha^{s\cdot(t_1\cdot T+t_2)})\}\\
&=\sum_{s\in I}tr_q^{q^m}\{\alpha^{dt_1\cdot T}tr_{q^m}^{q^n}(\alpha^{s\cdot t_2})\}\\
&=tr_q^{q^m}\Big\{\beta^{dt_1}\cdot\sum_{s\in I}tr_{q^m}^{q^n}(\alpha^{s\cdot t_2})\Big\}\\
&=tr_q^{q^m}\{\beta^{dt_1}\cdot f(\alpha^{t_2})\}
\end{aligned}$$

위의 시퀀스에서 t_2를 고정시키면 주기가 q^m-1인 부분 시퀀스가 되고 이 부분 시퀀스는 $f(\alpha^{t_2})=0$일 때는 모두 0인 시퀀스이고, $f(\alpha^{t_2})\ne 0$일 때는 데시메이티드 m-시퀀스 $tr_q^{q^m}(\beta^{dt_1})$의 순회적 천이가 된다. 함수 $c(\alpha^t)$의 차 시퀀스는 다음과 같이 쓸 수 있다.

$$\begin{aligned}
&c(\alpha^{t+\tau})-c(\alpha^t)\\
&=tr_q^{q^m}(\beta^{dt_1}\cdot f(\alpha^{t_2+\tau}))-tr_q^{q^m}(\beta^{dt_1}\cdot f(\alpha^{t_2}))
\end{aligned}$$

부분 시퀀스 $tr_q^{q^m}(\beta^{dt_1})$의 한 주기동안에는 '0'가 $q^{m-1}-1$번 나오고, F_q의 '0'이외의 모든 원소가 q^{m-1}번 나온다. t_2가 $0\le t_2\le T-1$에서 변하는 동안, $f(\alpha^{t_2+\tau})=f(\alpha^{t_2})$가 B번 발생하고, $f(\alpha^{t_2+\tau})\neq f(\alpha^{t_2})$가 $T-B$번 발생을 한다고 가정한다. 그러면, $c(\alpha^t)$의 차 시퀀스 $c(\alpha^{t+\tau})-c(\alpha^t)$의 한 주기 동안에 '0'는 $(q^m-1)\cdot B+(q^{m-1}-1)(T-B)$번 발생할 것이고, '0' 이외의 원소는 $q^{m-1}\cdot(T-B)$번 발생할 것이다. $c(\alpha^t)$는 차균형이라는 가정을 이용하면, 다음을 얻을 수 있다.

$$(q^m-1)\cdot B+(q^{m-1}-1)(T-B)=q^{n-1}-1$$
$$q^{m-1}\cdot(T-B)=q^{n-1}$$

계산하면, $B=\frac{q^{n-m}-1}{q^m-1}$이 되고, $T-B=q^{n-m}$이 된다.

다음의 관계를 보자.

$$f(\alpha^{t_1\cdot T+t_2+\tau})-f(\alpha^{t_1\cdot T+t_2})=\beta^{dt_1}\{f(\alpha^{t_2+\tau})-f(\alpha^{t_2})\}$$

고정된 t_2에 대해서, $f(\alpha^{t_2+\tau})-f(\alpha^{t_2})\neq 0$일 때는, $f(\alpha^{t_1\cdot T+t_2+\tau})-f(\alpha^{t_1\cdot T+t_2})$에서 t_1이 $0\le t_1\le q^n-2$에서 변할 때, F_{q^m}상의 0이 아닌 모든 원소가 한번씩만 나온다. 그러므로, $f(\alpha^{t+\tau})-f(\alpha^t)$의 한 주기 동안에 '0'은 $(q^m-1)\cdot B=q^{n-m}-1$번 발생하고, F_{q^m}상의 '0'이 아닌 모든 다른 원소들은 각각 $T-B=q^{n-m}$번 발생한다. 그러므로, $f(\alpha^t)$이 차균형임이 증명되었다. □

정리 2와 정리 8로부터 다음의 정리와 같이 Singer 파라미터를 갖는 순회차집합이 생성될 수 있다.

[정리 9]

q가 소수의 멱승이고 α가 유한체 F_{q^n}의 원시원이라 하자. 또한 $f(\alpha^t)$가 식 (15)에서 정의된 차균형 성질을 갖는 F_{q^n}에서 F_{q^m}으로의 d-동차 함수라 하자. 그러면 다음과 같이 정의되는 정수의 집합은 Singer 파라미터

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

를 갖는 순회차집합이 된다.

$$D=\left\{t\,\middle|\,f(\alpha^t)=0,\ 0\le t<\frac{q^n-1}{q^m-1}\right\}$$ □

양의 정수 e,k가 있고, 정리 6의 $n=3ek$라 한다. 정리 8로부터 $F_{q^{3e}}$에서 F_q로의 함수

$$tr_{3^k}^{3^{3ek}}(\alpha^t)+tr_{3^k}^{3^{3ek}}(\alpha^{st})$$

는 d-동차함수이고, 차균형성질을 가짐을 알 수 있다. 정리 2와 정리 8로부터 다음과 같이 다른 순회차집합을 생성시킬 수 있다.

[따름정리 10]

e,k는 양의 정수, $s=3^{2ek}-3^{ek}+1$ 이라 하자. 또한 α는 $F_{3^{3ek}}$의 원시원이라 하자. 그러면 다음과 같이 정의되는 정수들의 집합은 Singer 파라미터

$$\left(\frac{3^{3ek}-1}{3^k-1},\ \frac{3^{(3e-1)k}-1}{3^k-1},\ \frac{3^{(3e-2)k}-1}{3^k-1}\right)$$

를 갖는 순회차집합이 된다.

$$D=\left\{t\,\middle|\,tr_{3^k}^{3^{3ek}}(\alpha^t)+tr_{3^k}^{3^{3ek}}(\alpha^{st})=0,\ 0\le t<\frac{3^{3ek}-1}{3^k-1}\right\}$$ □

따름정리 10에서 $e=1$이고, $q=3^k$인 경우를 생각하면, 정수의 집합

$$D=\left\{t\,\middle|\,tr_{3^k}^{3^{3k}}(\alpha^t)+tr_{3^k}^{3^{3k}}(\alpha^{st})=0,\ 0\le t<\frac{3^{3k}-1}{3^k-1}\right\} \tag{16}$$

는 $(q^2+q+1,q+1,1)$의 파라미터를 갖는 평면 차집합(planar difference set)이 된다. 수치 해석에 의해서 식 (16)에서 정의된 순회 평면 차집합이 같은 파라미터를 갖는 Singer 차집합과 일치한다는 것을 $k=1,2,3,4$의 경우에 대해서 확인하였다. 한 파라미터 쌍에 대해서 순회 평면 차집합은 단 하나만 존재한다고 알려져 있다. 그러므로, 다음의 추측을 제시한다.

[추측정리 11]

양의 정수 k에 대해 $q=3^k$이고, $s=q^2-q+1$이라 하자. 또한 α는 F_{q^3}의 원시원이라 한다. 이 때, 다음과

같이 정의되는 파라미터 $(q^2+q+1, q+1, 1)$를 갖는 평면 순회차집합

$$\left\{t \,\middle|\, tr_q^{q^3}(\alpha^t)+tr_q^{q^3}(\alpha^{st}),\ 0\le t\le \frac{q^3-1}{q-1}\right\}$$

는 다음과 같이 주어지는 Singer 파라미터 $(q^2+q+1, q+1, 1)$를 갖는 차집합과 일치한다.

$$\left\{t \,\middle|\, tr_q^{q^3}\left(\alpha^{\frac{q+1}{2}t}\right)=0,\ 0\le t< \frac{q^3-1}{q-1}\right\} \qquad \square$$

Klapper[13]가 유도한 것과 유사하게 차균형성을 갖는 F_{q^n}에서 F_q으로의 d-동차함수를 만들기 위해서 필요한 차균형이고 F_{q^n}에서 F_{q^m}로의 d-동차함수의 조건을 다음의 정리에서 볼 수 있다.

[보조정리 12]

q는 소수의 멱승이고, 양의 정수 m, n에 대해 $m|n$이고, $M=q^m-1$이라 하자. 또한 α는 F_{q^n}의 원시원이라 하고, $T=\frac{q^n-1}{q^m-1}$에 대해 $\beta=\alpha^T$이라 하자. 이제 $H(\alpha^t)$가 F_{q^n}에서 F_{q^m}으로의 d-동차함수이고, d는 $1\le d\le M-1$인 M과 서로 소인 정수라 하자. 이 때, $1\le r\le M-1$이고 M과 서로 소인 정수 r에 대해 다음과 같이 주어지는 F_{q^n}에서 F_q로의 함수가 있다.

$$f(\alpha^t)=tr_q^{q^m}([H(\alpha^t)]^r) \tag{17}$$

이 때, 위 함수 $f(\alpha^t)$가 $dr\equiv d' \mod q-1$에 대해 차균형이고 F_{q^n}에서 F_{q^m}으로의 d'-동차함수라는 것은 0이 아닌 모든 τ에 대해 집합

$$\{t|H(\alpha^t)=H(\alpha^{t+\tau}),\ 0\le t\le T-1\} \tag{18}$$

의 크기 $\frac{q^{n-m}-1}{q^m-1}$이라는 것과 필요충분조건이다.

[증명]

$H(\alpha^t)$는 d-동차함수이므로, 0이 아닌 모든 $\gamma\in F_q\subset F_{q^m}$에 대해서 다음이 성립한다.

$$H(\gamma\cdot\alpha^t)=\gamma^d\cdot H(\alpha^t)$$

그러므로,

$$\begin{aligned} f(\gamma\cdot\alpha^t) &= tr_q^{q^m}([H(\gamma\cdot\alpha^t)]^r) \\ &= tr_q^{q^m}(\gamma^{dr}\cdot[H(\alpha^t)]^r) \\ &= \gamma^{d'}\cdot tr_q^{q^m}([H(\alpha^t)]^r) \\ &= \gamma^{d'}\cdot f(\alpha^t) \end{aligned}$$

위의 식은 $f(\alpha^t)$가 d'-동차함수임을 의미한다. t를 $t=t_1\cdot T+t_2$와 같이 T기저 표현으로 나타낸다. 단, $0\le t_1\le M-1$, $0\le t_2\le T-1$이다. 그러면, $f(\alpha^t)$의 차 시퀀스를 다음과 같이 2차원적으로 표현하는 것이 가능하다.

$$\begin{aligned} & f(\alpha^{t+\tau})-f(\alpha^t) \\ &= tr_q^{q^m}\{[H(\alpha^{t+\tau})]^r\}-tr_q^{q^m}\{[H(\alpha^t)]^r\} \\ &= tr_q^{q^m}\{[H(\alpha^{t_1T+t_2+\tau})]^r\}-tr_q^{q^m}\{[H(\alpha^{t_1T+t_2})]^r\} \\ &= tr_q^{q^m}\{\alpha^{Tdrt_1}[H(\alpha^{t_2+\tau})]^r\}-tr_q^{q^m}\{\alpha^{Tdrt_1}[H(\alpha^{t_2})]^r\} \\ &= tr_q^{q^m}\{\beta^{drt_1}[H(\alpha^{t_2+\tau})]^r\}-tr_q^{q^m}\{\beta^{drt_1}[H(\alpha^{t_2})]^r\} \\ &= tr_q^{q^m}\{\beta^{drt_1}\{[H(\alpha^{t_2+\tau})]^r-[H(\alpha^{t_2})]^r\}\} \end{aligned}$$

위에서 dr은 M과 서로 소이다. 또한 차 함수는 고정된 t_2에 대해서 $H(\alpha^{t_2+\tau})=H(\alpha^{t_2})$이면, t_1이 변화할 때 모두 '0'이 되고, $H(\alpha^{t_2+\tau})\ne H(\alpha^{t_2})$이면 주기가 M인 데시메이티드된 q진 m-시퀀스의 순회적 천이가 된다. 0이 아닌 τ에 대해서, t_2가 0에서 $T-1$까지 변할 때, $H(\alpha^{t_2+\tau})=H(\alpha^{t_2})$인 경우는 $B=\frac{q^{n-m}-1}{q^m-1}$번 일어나고, $H(\alpha^{t_2+\tau})\ne H(\alpha^{t_2})$인 경우는 $T-B=q^{n-m}$번 발생한다고 가정한다. $H(\alpha^{t_2+\tau})\ne H(\alpha^{t_2})$인 t_2에 대해 부분 시퀀스에서 t_1이 변할 때, '0'은 $q^{m-1}-1$번 발생하고, F_q상의 다른 원소들은 q^{m-1}번 발생한다. 그러므로, $f(\alpha^t)$의 차 시퀀스에 대해서 t가 $0\le t\le q^n-2$ 사이에서 변할 때, 원소 '0'은 $B\cdot(q^m-1)+(T-B)(q^{m-1}-1)=q^{n-1}-1$번 발생한다. 그리고, F_q상의 '0'이 아닌 원소들은 $(T-B)\cdot q^{m-1}=q^{n-1}$번 발생한다. 그러므로, $f(\alpha^t)$는 차균형이다. 역으로 먼저 $f(\alpha^t)$가 차균형임을 가정할 때, $B=\frac{q^{n-m}-1}{q^m-1}$가 되는 것은 쉽게 증명된다. $\square$

어떤 계수들의 집합 J에 대해서 F_{q^n}에서 F_{q^m}으로의 함수 $H(\alpha^t)=\sum_{s\in J}tr_{q^m}^{q^n}(\alpha^{st})$는 d-동차함수이고, 차균형이라 한다. 앞에서 주어진 정리를 이용하면, 주

어진 차균형이고 F_{q^n}으로부터 F_{q^m}으로의 d-동차함수인 함수를 이용하면, 이것으로부터 F_{q^n}에서 F_q로의 d-동차함수를 만들 수 있으며, 이를 이어지는 정리에서 볼 수 있다.

[정리 13]

q는 소수의 멱승이고, m, n은 양의 정수이며, $m|n$이다. 그리고, α는 유한체 F_{q^n}의 원시원이라 한다. 계수의 집합 J에 대해서, F_{q^n}에서 F_{q^m}로의 함수 $H(\alpha^t)$는 다음과 같이 주어지고, d-동차함수이며, 차균형이라 하자.

$$H(\alpha^t) = \sum_{s\in J} tr_{q^m}^{q^n}(\alpha^{st})$$

$1 \le r \le q^m - 2$이고, $M = q^m - 1$과 서로 소인 한 정수 r에 대하여, 주어지는 함수

$$f(\alpha^t) = tr_q^{q^m}\left\{\left[\sum_{s\in J} tr_{q^m}^{q^n}(\alpha^{st})\right]^r\right\} \tag{19}$$

는 d-동차함수이고, 차균형성질을 갖는다. □

주어진 정리들로부터 다음 정리과 같이 Singer 파라미터를 갖는 새로운 차집합을 만들 수 있다.

[정리 14]

q는 소수의 멱승이고, α는 F_{q^n}의 원시원이라 하자. 또한 $f(\alpha^t)$는 식 (19)에서 정의된 F_{q^n}에서 F_q로의 함수라 하자. 이 때, 다음과 같이 정의되는 정수의 집합 $D = \left\{t \,\middle|\, f(\alpha^t) = 0,\ 0 \le t < \frac{q^n - 1}{q-1}\right\}$는 Singer 파라미터 $\left(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-2}\right)$를 갖는 순회차집합이 된다. □

q는 3의 멱승이고, 양의 정수 e, k가 있다. α는 $F_{q^{3ek}}$의 원시원이라 한다. 정수 집합 $J = \{1, q^{2ek} - q^{ek} + 1\}$가 있다. $q^{2ek} - q^{ek} + 1 = 1 \bmod (q^k - 1)$임은 명백하고, $d = 1$이 되므로, $F_{q^{3ek}}$에서 F_{q^k}로의 함수

$$H(\alpha^t) = \sum_{s\in J} tr_{q^k}^{q^{3ek}}(\alpha^{st}) \tag{20}$$

는 정리 8에 의하여 d-동차함수이고, 차균형이다. 정리 13와 식 (20)의 함수로부터, $1 \le r \le q^k - 2$이고, $q^k - 1$과 서로 소인 정수 r과 $s = q^{2ek} - q^{ek} + 1$에 대해서 다음과 같이 정의되는 함수

$$f(\alpha^t) = tr_q^{q^k}\left\{\left[tr_{q^k}^{q^{3ek}}(\alpha^t) + tr_{q^k}^{q^{3ek}}(\alpha^{st})\right]^r\right\} \tag{31}$$

는 $r = d \bmod q-1$일 때, d-동차함수이며, 차균형성질을 갖는다.

정리 14와 (21)에서 정의된 함수를 이용하면, Singer 파라미터를 갖는 순회차집합을 쉽게 구할 수 있다.

[따름정리 15]

q는 3의 멱승이고, α는 유한체 $F_{q^{3ek}}$의 원시원이라 하자. 또한 $f(\alpha^t)$는 식 (21)에서 정의된 함수이다. 이 때, 다음과 같이 정의되는 정수의 집합

$$D = \left\{t \,\middle|\, f(\alpha^t) = 0,\ 0 \le t < \frac{q^{3ek} - 1}{q-1}\right\}$$

은 파라미터가

$$\left(\frac{q^{3ek}-1}{q-1}, \frac{q^{3ek-1}-1}{q-1}, \frac{q^{3ek-2}-1}{q-1}\right)$$

인 순회차집합이 된다. □

만약 부분 시퀀스를 주기가 $q^k - 1$인 Helleseth, Kumar, Martinsen의 3진 시퀀스로 대체하면, 이것은 (21)에서 정의된 것과 같은 d-형 시퀀스가 될 것이다. 주기 8인 3진 m-시퀀스 $tr_3^{3^2}(\alpha^t)$와 이것의 5로 데시메이티드된 시퀀스의 '0'의 위치는 같다. 그러므로, $s = 3^{4k} - 3^{2k} + 1$일 때,

$$\left(\frac{3^{6k}-1}{3-1}, \frac{3^{6k-1}-1}{3-1}, \frac{3^{6k-2}-1}{3-1}\right)$$

의 파라미터를 갖는 순회차집합

$$\left\{t \,|\, tr_3^{3^2}\left(\left[tr_{3^2}^{3^{6k}}(\alpha^t) + tr_{3^2}^{3^{6k}}(\alpha^{st})\right]^5\right) = 0, 0 \le t < \frac{3^{6k}-1}{3-1}\right\}$$

는 같은 파라미터를 갖는 순회차집합

$$\left\{t \,|\, tr_3^{3^{6k}}(\alpha^t) + tr_3^{3^{6k}}(\alpha^{st}) = 0, 0 \le t < \frac{3^{6k}-1}{3-1}\right\}$$

과 일치한다.

그러나, 수치적인 해석에 따르면, 따름정리 15에 정의된 $q=3$ $e=1$ $k=3$, $r=1,5,7,17$의 경우에 해당하는 (9841,3280,1093)의 파라미터를 갖는 4개의 새로운 순회차집합이 존재한다. 이들은 서로 비등가이며, 같은 파라미터를 같은 Singer 차집합 및 GMW 차집합들과도 비등가이다.

Ⅳ. 결 론

의사불규칙시퀀스들은 스트림암호의 키스트림 그리고 블록암호의 S-box 등에 활용될 수 있어 많은 연구가 되어 왔다. 그런데 순회차집합의 특성함수(characteristic function)은 이상적인 자기상관 특성을 갖는 의사 불규칙 시퀀스가 된다는 것은 잘 알려진 사실이다. 본 논문에서는 새로운 순회차집합을 발견하였고 이러한 내용은 향후 시퀀스 및 암호학의 분야에서 활용될 수 있을 것이다.

참 고 문 헌

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

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

[3] B. Gordon, W.H. Mills and L.R. Welch, "some new difference sets," *Canad. J. Math.*, Vol. 14, pp. 614~625, 1962.

[4] J.F. Dillon, "Multiplicative difference sets via additive characters," *Designs, Codes and Cryptography*, Vol. 17, pp. 225~235, 1999.

[5] J.F. Dillon and H. Dobbertin, "Cyclic difference sets with Singer parameters," preprint, 1999.

[6] D. Jungnickel, "Difference sets," in *Contemporary Design Theory: A Collection fo Surveys*, J. Dinitz and D.R. Stinson eds. John Wiley and Sons, 1992.

[7] Q. Xiang, "Recent results on difference sets with classical parameters," in *Difference Sets, Sequence and their Correlation Properties*, eds., A. Pott, P.V. Kumar, T. Helleseth and D. Jungnickel, pp. 419~434, Amsterdam: Kluwer, 1999.

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

[9] A. Chang, S.W. Golomb, G. Gong and P.V. Kumar, "Trace expansion and linear span of ideal autocorrelation sequences associated to the Segre hyperoval," preprint, 1999.

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

[11] M.K. Simon, J.K. Omura, R.A. Sholtz and B.K. Levitt, *Spread Spectrum Communications*, Vol. 1, Computer Science Press, Rockvile, MD, 1985.

[12] M. Goresky, A.H. Chan and A. Klapper, "Cross-correlation of linearly and quadratically related geometric sequences and GMW sequences," *Discrete Appl. Math.*, Vol. 46, No. 1, pp. 1~20, 1993.

[13] A. Klapper, "d-form sequecne: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, Vol. 41, No. 2, pp. 423~431, Mar. 1995.

[14] T. Helleseth, P.V. Kumar and H.M. Martinsen, "A new family of ternary sequences with ideal two~level autocorrelation," preprint, 2001.

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

[16] J.S. No and H. Chung and M.S. Yun, "Binary pseudorandom sequences of period 2^m-1 with ideal autocorrelation generated

by the polynomial $z^d+(z+1)^d$," *IEEE Trans. Inform. Theory*, Vol. 44, pp. 1278 ~1282, 1998.

[17] J.S. No, S.W. Golomb, G. G. Gong, H.K. Lee and P. Gaal, "Binary pseudorandom sequences of period 2^n-1 with ideal autocorrelation," *IEEE Trans. Inform. Theory*, Vol. 44, pp. 814~817, 1998.

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

[19] H.A. Lin, "From cyclic Hadamard differece sets to perfectly balanced sequences," Ph.D. dissertation, University of Southern California, May 1998.

〈著者紹介〉

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