Journal of Combinatorial Theory, Series A 116 (2009) 109–119

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Optimal and perfect difference systems of sets

Cunsheng Ding

Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

ARTICLE INFO

Article history:
Received 17 January 2008
Available online 16 June 2008

Keywords:
Difference systems of sets
Codes for synchronization
Perfect nonlinear functions

ABSTRACT

Difference systems of sets (DSS) were introduced in 1971 by Levenstein for the construction of codes for synchronization, and are closely related to cyclic difference families. In this paper, algebraic constructions of difference systems of sets using functions with optimum nonlinearity are presented. All the difference systems of sets constructed in this paper are perfect and optimal. One conjecture on difference systems of sets is also presented.

1. Introduction

Let n be a positive integer, and let $\mathbf{Z}_n$ be the residue ring of integers modulo n. A *difference system of sets* (DSS) with parameters $(n, \{\tau_0, \tau_1, \ldots, \tau_{q-1}\}, \rho)$ is a collection of q disjoint sets $D_i \subset \mathbf{Z}_n$ such that $|D_i| = \tau_i$ for all i with $0 \leqslant i \leqslant q-1$ and the multiset

$$\{(a-b) \bmod n:\ a \in D_i,\ b \in D_j,\ i \neq j,\ 0 \leqslant i, j \leqslant q-1\} \tag{1}$$

contains every number i, $1 \leqslant i \leqslant n-1$, at least ρ times. A DSS is said *perfect* if every nonzero integer in $\mathbf{Z}_n$ is contained exactly ρ times in the multiset of (1). A DSS is called *regular* if all the subsets D_i are of the same size.

Levenstein [7] (see also [8]) introduced DSSs for the construction of codes that allow for synchronization in the presence of errors, where the number

$$r_q(n, \rho) := \sum_{i=0}^{q-1} |D_i| \tag{2}$$

is required to be as small as possible. Levenstein [7] proved the following lower bound on $r_q(n, \rho)$:

E-mail address: cding@cse.ust.hk.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2008.05.007

$$r_q(n,\rho) \geqslant \sqrt{\frac{q\rho(n-1)}{q-1}}, \tag{3}$$

with equality if and only if the DSS is perfect and regular. In the sequel, this bound is referred to as *Levenstein bound*.

The Levenstein bound of (3) cannot be achieved in many cases. Below we describe an improved bound. For any positive integer n, define SQUARE(n) to be the smallest square number that is no less than n. Then the following bound follows easily from the bound of (3) (see [14]):

$$r_q(n,\rho) \geqslant \sqrt{\mathrm{SQUARE}\left(\rho(n-1)+\left\lceil \frac{\rho(n-1)}{q-1}\right\rceil\right)}, \tag{4}$$

where $\lceil x\rceil$ denotes the ceiling function. It will be demonstrated later that this improved bound is better than the Levenstein bound in many cases.

Tonchev constructed difference systems of sets using cyclotomic classes, difference sets, and balanced generalized weighing matrices [10,11]. Fuji-Hara, Munemasa and Tonchev obtained difference systems of sets from hyperplane line spreads and hyperplanes [3]. Tonchev and Wang developed algorithms for constructing optimal difference systems of sets [12,13]. Wang improved the Levenstein bound of (3). In this paper, we present a number of algebraic constructions of optimal and perfect difference systems of sets. The key idea of our constructions is to use functions with optimum nonlinearity. The parameters of the DSSs are new in many cases.

2. Cyclotomic classes and group characters

Cyclotomy and group characters are powerful tools for constructing combinatorial designs. In this section, we introduce cyclotomy and group characters that will be needed in subsequent sections. Throughout this paper, let p be a prime, m and s be positive integers, $q = p^s$, and let $r = q^m$.

Let $\mathbb{F}_q$ be the finite field with q elements, and let $q-1 = ef$, where e and f are positive integers. Given a generator ω of $\mathbb{F}_q^*$, define $C_0^{(e,q)} = \langle \omega^e\rangle$, the multiplicative group generated by ω^e, and

$$C_i^{(e,q)} = \omega^i C_0^{(e,q)} \quad \text{for } i = 1,2,\ldots,e-1.$$

The $C_i^{(e,q)}$ are called *cyclotomic classes* of order e [9].

Let $\mathrm{Tr}_{q/p}$ be the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. An *additive character* of $\mathbb{F}_q$ is a nonzero function χ from $\mathbb{F}_q$ to the set of nonzero complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any pair $(x,y) \in \mathbb{F}_q^2$. For each $b \in \mathbb{F}_q$, the function

$$\chi_b(c) = e^{2\pi\sqrt{-1}\,\mathrm{Tr}_{q/p}(bc)/p} \quad \text{for all } c \in \mathbb{F}_q, \tag{5}$$

defines an additive character of $\mathbb{F}_q$. When $b = 0$, $\chi_0(c) = 1$ for all $c \in \mathbb{F}_q$, and is called the *trivial additive character* of $\mathbb{F}_q$. The character χ_1 in (5) is called the *canonical additive character* of $\mathbb{F}_q$.

A *multiplicative character* of $\mathbb{F}_q$ is a nonzero function ψ from $\mathbb{F}_q^*$ to the set of complex numbers such that $\psi(xy) = \psi(x)\psi(y)$ for all pairs $(x,y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. Let ω be a fixed generator of $\mathbb{F}_q^*$. For each $j = 0,1,\ldots,q-2$, the function ψ_j with

$$\psi_j(\omega^k) = e^{2\pi\sqrt{-1}\,jk/(q-1)} \quad \text{for } k = 0,1,\ldots,q-2, \tag{6}$$

defines a multiplicative character of $\mathbb{F}_q$. When $j = 0$, $\psi_0(c) = 1$ for all $c \in \mathbb{F}_q^*$, and is called the *trivial multiplicative character* of $\mathbb{F}_q$.

Let q be odd and $j = (q-1)/2$ in (6), we then get a multiplicative character η such that $\eta(c) = 1$ if c is the square of an element and $\eta(c) = -1$ otherwise. This η is called the *quadratic character* of $\mathbb{F}_q$.

In this paper, we denote the canonical additive characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ respectively by

$$\chi_1(x) = e^{2\pi\sqrt{-1}\,\mathrm{Tr}_{q/p}(x)/p}, \quad x \in \mathbb{F}_q,$$
$$\chi_2(x) = e^{2\pi\sqrt{-1}\,\mathrm{Tr}_{q^m/p}(x)/p}, \quad x \in \mathbb{F}_{q^m};$$

and the quadratic characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ respectively by η_1 and η_2.

Suppose ω is a generator of $\mathbb{F}_{q^m}^*$. Then $\omega' = \omega^{(q^m-1)/(q-1)}$ is a generator of $\mathbb{F}_{q^m}^*$. We note that when q is odd, $(q^m-1)/(q-1) = \sum_{i=0}^{m-1} q^i$ is even if and only if m is even. Hence we have

$$\eta_2(x) = \begin{cases} 1 & \text{if } m \text{ is even,} \\ \eta_1(x) & \text{if } m \text{ is odd,} \end{cases} \tag{7}$$

for all $x \in \mathbb{F}_q$.

Let ψ be a multiplicative and χ an additive character of $\mathbb{F}_q$. Then the *Gaussian sum* $G(\psi, \chi)$ is defined by

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c).$$

It is well known that [5]

$$G(\psi, \chi) = \begin{cases} q-1 & \text{for } \psi = \psi_0,\ \chi = \chi_0, \\ -1 & \text{for } \psi = \psi_0,\ \chi \neq \chi_0, \\ 0 & \text{for } \psi \neq \psi_0,\ \chi = \chi_0. \end{cases} \tag{8}$$

If $\psi \neq \psi_0$ and $\chi \neq \chi_0$, then $|G(\psi, \chi)| = q^{1/2}$. If p is an odd prime, then

$$G(\eta, \chi_1) = \begin{cases} (-1)^{s-1} q^{1/2} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{s-1} (\sqrt{-1})^s q^{1/2} & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{9}$$

Let χ be a nontrivial additive character of $\mathbb{F}_q$ and let the polynomial $f \in \mathbb{F}_q[x]$ be of positive degree. Sums of the form $\sum_{c \in \mathbb{F}_q} \chi(f(c))$ are called *Weil sums*.

The following is referred to as Weil's bound [5].

Lemma 1. *Let $f \in \mathbb{F}_q[x]$ be of degree $h \geqslant 1$ with $\gcd(h, q) = 1$ and let χ be a nontrivial additive character of $\mathbb{F}_q$. Then*

$$\left| \sum_{c \in \mathbb{F}_q} \chi\big(f(c)\big) \right| \leqslant (h-1)q^{1/2}.$$

3. A generic construction of optimal and perfect difference systems of sets

Let $(G, +)$ be a finite abelian group. A function f from $(\mathbf{Z}_n, +)$ to $(G, +)$ is called an (n, λ) *zero difference balanced*, in short *ZDB*, function if

$$\big|\{x \in \mathbf{Z}_n\colon\ f(x+a) - f(x) = 0\}\big| = \lambda$$

for every nonzero $a \in \mathbf{Z}_n$, where λ is a positive integer.

Theorem 2. *Let f be a function from $(\mathbf{Z}_n, +)$ to $(G, +)$. For each $g \in G$, put*

$$D_g = \{x \in \mathbf{Z}_n\colon\ f(x) = g\}. \tag{10}$$

Define

$$\mathcal{S} = \{D_g\colon\ g \in G\}. \tag{11}$$

If f is an (n, λ) ZDB function, the set $\mathcal{S}$ of (10) is an $(n, \{\tau_g\colon\ g \in G\}, n-\lambda)$ perfect DSS, where $\tau_g = |D_g|$.

Proof. Note that

$$\big|\{x \in \mathbf{Z}_n\colon\ f(x+a) - f(x) = 0\}\big| = \sum_{g \in G} \big|D_g \cap (D_g - a)\big|.$$

On the other hand, $\{D_g\colon\ g \in G\}$ is a partition of $\mathbf{Z}_n$, and we have the following multiset equality:

$$n\mathbf{Z}_n = \{x - y\colon\ x \in \mathbf{Z}_n,\ \ y \in \mathbf{Z}_n\} = \left[\bigcup_{g \neq h}(D_g - D_h)\right] \cup \left[\bigcup_{g \in G}(D_g - D_g)\right],$$

where $D_g - D_h$ denotes the multiset $\{x - y\colon\ x \in D_g,\ \ y \in D_h\}$. It follows that for each nonzero $a \in \mathbf{Z}_n$,

$$\begin{aligned}\sum_{g \neq h}\left|D_g \cap (D_h + a)\right| &= n - \sum_{g \in G}\left|D_g \cap (D_g - a)\right| \\ &= n - \left|\left\{x \in \mathbf{Z}_n\colon\ f(x + a) - f(x) = 0\right\}\right|.\end{aligned}$$

The conclusions of this theorem then follow from the definition of ZDB functions. □

4. Optimal difference systems of sets from perfect nonlinear functions

Let f be a function from a finite abelian group $(A, +)$ to another finite abelian group $(B, +)$. We say that f is *linear* if and only if $f(x + y) = f(x) + f(y)$ for all $x, y \in A$. A function g is *affine* if and only if $g = f + b$, where f is linear and b is a constant.

A robust measure of nonlinearity of f is defined by

$$P_f = \max_{0 \neq a \in A}\max_{b \in B}\frac{|\{x \in A\colon\ f(x + a) - f(x) = b\}|}{|A|},$$

where $|A|$ denotes the cardinality of the set A. The smaller the value of P_f, the higher the corresponding nonlinearity of f.

It is easily seen that $P_f \geqslant \frac{1}{|B|}$ [1]. A function $f : A \to B$ has *perfect nonlinearity* if $P_f = \frac{1}{|B|}$. The following lemma is proved in [1].

Lemma 3. *A function f from a finite abelian group $(A, +)$ to a finite abelian group $(B, +)$ is perfect nonlinear if and only if for each nonzero $a \in A$, $f(x + a) - f(x)$ takes on each element of b the same numbers of times when x ranges over all elements of A.*

As a corollary of Theorem 2 and Lemma 3, we have the following.

Corollary 4. *Let ℓ, k be positive integers, and $n = \ell k$. Let G be an abelian group of size ℓ. Suppose there is a perfect nonlinear function f from $\mathbf{Z}_n$ to G. Then the set $\mathcal{S}$ of (11) is an $(n, \{\tau_b\colon\ b \in G\}, n - k)$ perfect DSS.*

This construction is generic in the sense that it works for every perfect nonlinear function from $\mathbf{Z}_n$ to an abelian group B. As examples, we obtain difference systems of sets based on the following perfect nonlinear functions from $\mathbf{Z}_{p^2}$ to $\mathbf{Z}_p$.

Lemma 5. *(See [1].) Let p be an odd prime. Define $f : \mathbf{Z}_{p^2} \to \mathbf{Z}_p$ by $f(h + jp) = hj \bmod p$ for $0 \leqslant h, j \leqslant p - 1$. Then f has perfect nonlinearity with respect to $(\mathbf{Z}_{p^2}, +)$ and $(\mathbf{Z}_p, +)$.*

Corollary 6. *Let f be the perfect nonlinear function from $\mathbf{Z}_{p^2}$ to $\mathbf{Z}_p$ defined in Lemma 5. Then the set $\mathcal{S}$ of (11) is a $(p^2, \{2p - 1, p - 1, p - 1, \ldots, p - 1\}, p^2 - p)$ perfect DSS, and is optimal with respect to the lower bound of (4).*

Proof. It follows from Lemma 5 and Corollary 4 that the set $\mathcal{S}$ of (11) is a perfect DSS. We need to determine the parameters τ_b. It is easy to see that $\tau_0 = 2p - 1$ and $\tau_b = p - 1$ for all nonzero $b \in \mathbf{Z}_p$. It is straightforward to check that the bound of (4) is met. □

Lemma 7. *(See [1].) Let $f : \mathbf{Z}_{p^2} \to \mathbf{Z}_p$ be a mapping whose restriction to $\mathbf{Z}_{p^2}^*$ is a surjective homomorphism with respect to $(\mathbf{Z}_{p^2}^*, \cdot)$ and $(\mathbf{Z}_p, +)$ and is zero otherwise. Then f has perfect nonlinearity with respect to $(\mathbf{Z}_{p^2}, +)$ and $(\mathbf{Z}_p, +)$.*

A specific perfect nonlinear function of this type is the following [1]. Let p be an odd prime, and let α be a primitive root modulo p^2. Define f as

$$f(x) = \begin{cases} h \bmod p & \text{if } x = \alpha^h \text{ for some } h, \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

Then f satisfies the conditions of Lemma 7 and is thus a perfect nonlinear function.

Here we have in fact $p-1$ perfect nonlinear functions from $\mathbf{Z}_{p^2}$ to $\mathbf{Z}_p$ by selecting the primitive root α. Thus, we have obtained $p-1$ DSSs described in the following corollary.

Corollary 8. *Let f be the perfect nonlinear function from $\mathbf{Z}_{p^2}$ to $\mathbf{Z}_p$ defined in* (12)*. Then the set $\mathcal{S}$ of* (11) *is a $(p^2, \{2p-1, p-1, p-1, \ldots, p-1\}, p^2-p)$ perfect DSS, and is optimal with respect to the lower bound of* (4)*.*

Proof. It follows from Lemma 5 and Corollary 4 that the set $\mathcal{S}$ of (11) is a perfect DSS. We need to determine the parameters τ_b. It is easy to see that $\tau_0 = 2p-1$ and $\tau_b = p-1$ for all nonzero $b \in \mathbf{Z}_p$. It is straightforward to check that the bound of (4) is met. □

5. Optimal difference systems of sets from special power functions

Let N be a positive integer such that $q \equiv 1 \pmod N$. Let $(G, +) = (\mathbb{F}_q, +)$. Let ω be a generator of $\mathbb{F}_{q^m}^*$. Define $\alpha = \omega^N$, $n = (q^m-1)/N$, and a function f from $(\mathbf{Z}_n, +)$ to $(G, +)$ by

$$f(x) = \mathrm{Tr}_{q^m/q}\left(\alpha^x\right), \quad x \in \mathbf{Z}_n, \tag{13}$$

where $\mathrm{Tr}_{q^m/q}$ is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

Theorem 9. *If $\gcd(m, N) = 1$, the set $\mathcal{S}$ of* (11) *is an $(n, \{\tau_b\colon b \in \mathbb{F}_q\}, \frac{q^{m-1}(q-1)}{N})$ perfect DSS, where $\tau_b = |D_b|$ for each $b \in \mathbb{F}_q$. Furthermore, the DSS $\mathcal{S}$ is optimal with respect to the lower bound of* (4)*.*

Proof. Because $q \equiv 1 \pmod N$, we have

$$\frac{q^m-1}{q-1} \equiv m \pmod N.$$

It then follows from $\gcd(m, N) = 1$ that

$$\gcd\left(\frac{q^m-1}{q-1} \bmod N, N\right) = 1. \tag{14}$$

Let $r = q^m$, and let $Z(a, 0)$ denote the number of solutions $x \in \mathbb{F}_r$ of the equation $\mathrm{Tr}_{r/q}(ax^N) = 0$. Let $\epsilon_p = e^{2\pi\sqrt{-1}/p}$ and $\chi(x) = \epsilon_p^{\mathrm{Tr}_{r/p}(x)}$, where $\mathrm{Tr}_{r/p}$ is the trace function from $\mathbb{F}_r$ to $\mathbb{F}_p$. Then χ is an additive character of $\mathbb{F}_r$. We have then

$$\begin{aligned} Z(a, 0) &= \frac{1}{q} \sum_{y \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_r} \epsilon_p^{\mathrm{Tr}_{q/p}(y\,\mathrm{Tr}_{r/q}(ax^N))} \\ &= \frac{1}{q} \sum_{y \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_r} \chi\left(yax^N\right) \\ &= \frac{1}{q}\left[q + r - 1 + \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_r^*} \chi\left(yax^N\right)\right] \end{aligned}$$

$$= \frac{1}{q}\left[q + r - 1 + N \sum_{y \in \mathbb{F}_q^*} \sum_{x \in C_0^{(N,r)}} \chi(yax)\right]. \tag{15}$$

Let ω be the generator of $\mathbb{F}_r^*$. Note that $\gamma = \omega^{(r-1)/(q-1)}$ is a generator of $\mathbb{F}_q^*$. Since $\gcd((r-1)/(q-1) \bmod N, N) = 1$, each cyclotomic class $C_i^{(N,r)}$ contains exactly $(q-1)/N$ elements of $\mathbb{F}_q^*$. It then follows from (15) that

$$\begin{aligned} Z(a,0) &= \frac{1}{q}\left[q + r - 1 + (q-1) \sum_{x_3 \in \mathbb{F}_r^*} \chi(x_3)\right] \\ &= \frac{1}{q}\left[r + (q-1) \sum_{x_3 \in \mathbb{F}_r} \chi(x_3)\right] \\ &= q^{m-1}. \end{aligned}$$

For any nonzero $t \in \mathbf{Z}_n$, we have $\alpha^t - 1 \neq 0$ and

$$f(x+t) - f(x) = \mathrm{Tr}_{r/q}\left[\left(\alpha^t - 1\right)\alpha^x\right].$$

It then follows that

$$\left|\left\{x \in \mathbf{Z}_n\colon\ f(x+t) - f(x) = 0\right\}\right| = \frac{q^{m-1} - 1}{N}$$

for every nonzero $t \in \mathbf{Z}_n$. It then follows from Theorem 2 that the set $\mathcal{S}$ of (11) is a perfect DSS with parameters $(n, \{\tau_b\colon\ b \in \mathbb{F}_q\}, \frac{q^{m-1}(q-1)}{N})$.

Finally, we prove the optimality of the DSS with respect to the bound of (4). It suffices to prove that

$$\rho(n-1) + \left\lceil \frac{\rho(n-1)}{q-1} \right\rceil > (n-1)^2. \tag{16}$$

Note that

$$(n-1)^2 - \rho(n-1) = \frac{q^{m-1} - 1 - N}{N}(n-1) < \frac{q^{m-1}}{N}(n-1) \leqslant \left\lceil \frac{\rho(n-1)}{q-1} \right\rceil.$$

This completes the proof. □

Example 1. Let $q = 3$, $m = 3$ and $N = 2$. Then the set $\mathcal{S}$ of (11) is a $(13, \{4, 3, 6\}, 9)$ optimal and perfect DSS consisting of the following blocks:

$$D_0 = \{0, 7, 8, 11\}, \qquad D_1 = \{4, 10, 12\}, \qquad D_2 = \{1, 2, 3, 5, 6, 9\}.$$

For the difference systems of sets described in Theorem 9, the determination of the parameters τ_b is a hard problem in general. However, it can be done in certain special cases. In what follows in section, we will give a lower and upper bound on these τ_b and compute them in the special case $N = 2$.

The following theorem presents a lower and upper bound on τ_b.

Theorem 10. *Let $r = q^m$. Then*

$$\frac{q^{m-1} - Nq^{m/2} - 1}{N} \leqslant \tau_b \leqslant \frac{q^{m-1} + Nq^{m/2} - 1}{N}.$$

Proof. Note that $q \equiv 1 \pmod N$. We have that $\gcd(q, N) = 1$. Let $Z(a,b)$ denote the number of solutions $x \in \mathbb{F}_r$ of the equation $\mathrm{Tr}_{r/q}(ax^N) = b$. Let $\epsilon_p = e^{2\pi\sqrt{-1}/p}$ and $\chi(x) = \epsilon_p^{\mathrm{Tr}_{r/p}(x)}$, where $\mathrm{Tr}_{r/p}$ is the trace function from $\mathbb{F}_r$ to $\mathbb{F}_p$. Then χ is an additive character of $\mathbb{F}_r$. We have then

$$\begin{aligned} Z(a,b) &= \frac{1}{q}\sum_{y\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_r} \epsilon_p^{\mathrm{Tr}_{q/p}(y[\mathrm{Tr}_{r/q}(ax^N)-b])} \\ &= \frac{1}{q}\sum_{y\in\mathbb{F}_q} \chi_1(-by)\sum_{x\in\mathbb{F}_r}\chi_2\big(yax^N\big) \\ &= \frac{1}{q}\Bigg[r+\sum_{y\in\mathbb{F}_q^*} \chi_1(-by)\sum_{x\in\mathbb{F}_r}\chi_2\big(yax^N\big)\Bigg]. \end{aligned}$$

It then follows from Lemma 1 that

$$\big|Z(a,b)-q^{m-1}\big| \leqslant \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\Bigg|\sum_{x\in\mathbb{F}_r}\chi_2\big(yax^N\big)\Bigg| \leqslant Nq^{m/2}.$$

The conclusion of the theorem then follows.

The proof of the first part of the following lemma can be found in [2]. The second part of the following lemma is similarly proved. □

Lemma 11. *If $r\equiv 1 \pmod 4$, we have*

$$\sum_{x\in C_0^{(2,r)}}\chi_2(x)=\frac{-1\pm\sqrt{r}}{2}, \qquad \sum_{x\in C_1^{(2,r)}}\chi_2(x)=\frac{-1\mp\sqrt{r}}{2}.$$

If $r\equiv 3 \pmod 4$, we have

$$\sum_{x\in C_0^{(2,r)}}\chi_2(x)=\frac{-1\pm\sqrt{-r}}{2}, \qquad \sum_{x\in C_1^{(2,r)}}\chi_2(x)=\frac{-1\mp\sqrt{-r}}{2}.$$

The values τ_b in the case $N=2$ are given in the following theorem.

Theorem 12. *Let $N=2$. For the DSS of Theorem 9 we have*

$$\tau_b\in\big\{r\pm\sqrt{r}, r\pm(q-1)\sqrt{r}\big\}, \quad b\in\mathbb{F}_q,$$

if m is even; and

$$\tau_b\in\{r, r\pm\sqrt{qr}\}, \quad b\in\mathbb{F}_q,$$

if m is odd.

Proof. We have

$$\begin{aligned} Z(a,b) &= \frac{1}{q}\sum_{y\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_r} \epsilon_p^{\mathrm{Tr}_{q/p}(y[\mathrm{Tr}_{r/q}(ax^2)-b])} \\ &= \frac{1}{q}\sum_{y\in\mathbb{F}_q} \chi_1(-by)\sum_{x\in\mathbb{F}_r}\chi_2\big(yax^2\big) \\ &= \frac{1}{q}\Bigg[r+\sum_{y\in\mathbb{F}_q^*} \chi_1(-by)\sum_{x\in\mathbb{F}_r}\chi_2\big(yax^2\big)\Bigg] \\ &= \frac{1}{q}\Bigg[r+\sum_{y\in\mathbb{F}_q^*} \chi_1(-by)+\sum_{y\in\mathbb{F}_q^*} \chi_1(-by)\sum_{x\in\mathbb{F}_r^*}\chi_2\big(yax^2\big)\Bigg]. \end{aligned} \tag{17}$$

We continue with the proof by considering the following cases.

Case I. $r \equiv 1 \pmod 4$.

It follows from Lemma 11 and (17) that

$$q \cdot Z(a,b) = r \pm \sqrt{r} \sum_{y \in \mathbb{F}_q^*} \chi_1(-by)\eta_2(ay).$$

If $b = 0$, it then follows from (7) that

$$\begin{aligned} q \cdot Z(a,b) &= r \pm \sqrt{r} \sum_{y \in \mathbb{F}_q^*} \chi_1(-by)\eta_2(ay) \\ &= r \pm \sqrt{r} \sum_{y \in \mathbb{F}_q^*} \eta_2(ay) \\ &= \begin{cases} r \pm (q-1)\sqrt{r}, & \text{when } m \text{ is even}, \\ r, & \text{when } m \text{ is odd}. \end{cases} \end{aligned}$$

If $b \neq 0$, it then follows from (7) and (9) that

$$\begin{aligned} q \cdot Z(a,b) &= r \pm \sqrt{r} \sum_{y \in \mathbb{F}_q^*} \chi_1(-by)\eta_2(ay) \\ &= r \pm \sqrt{r}\eta_2\big(-ab^{-1}\big) \sum_{y \in \mathbb{F}_q^*} \chi_1(-by)\eta_2(-by) \\ &= \begin{cases} r \mp \sqrt{r}\eta_2(-ab^{-1}), & \text{when } m \text{ is even}, \\ r \pm \sqrt{r}\eta_2(-ab^{-1})G(\eta_1, \chi_1), & \text{when } m \text{ is odd}, \end{cases} \\ &= \begin{cases} r \pm \sqrt{r}, & \text{when } m \text{ is even}, \\ r \pm \sqrt{rq} & \text{when } m \text{ is odd}. \end{cases} \end{aligned}$$

Case II. $r \equiv 3 \pmod 4$.

Since $r \equiv 3 \pmod 4$, both s and m must be odd. Similar to that in Case I, we can prove that $q \cdot Z(a,0) = r$ and $q \cdot Z(a,b) = r \pm \sqrt{rq}$ if $b \neq 0$.

Combining the results in Cases I and II completes the proof of this theorem. □

6. Optimal difference systems of sets from ternary sequences

Let $(u(i))_{i=0}^{\infty}$ be a sequence of period n over $\mathbb{F}_r$. The autocorrelation function of the sequence is defined by

$$A_u(t) = \sum_{i=0}^{n-1} \chi_2\big(u(i+t) - u(i)\big), \tag{18}$$

where χ_2 is the group character on $\mathbb{F}_r$. The sequence is said to have *ideal autocorrelation* if $A_u(t) = -1$ for all $1 \leqslant t \leqslant n-1$. In this section, we propose an approach to the construction of perfect difference systems of sets using special ternary sequences.

In this section, let $s = 1$ and $p = 3$. So we have $q = p = 3$ and $r = q^m$. Let $h(x)$ be polynomial over $\mathbb{F}_r$. Define a ternary sequence $(u(i))_{i=0}^{\infty}$ of period $r-1$ by

$$u(i) = \mathrm{Tr}_{q^m/q}\big(h\big(\omega^i\big)\big) \tag{19}$$

for all $i \geqslant 0$.

Theorem 13. *Let $n = r - 1$. Define a function f from $\mathbf{Z}_n$ to $\mathbb{F}_3$ by $f(i) = u(i)$ for all i. If the polynomial h satisfies $h(-x) = -h(x)$ for all $x \in \mathbb{F}_r$ and the sequence $(u(i))_{i=0}^{\infty}$ in (19) has ideal autocorrelation, the $\mathcal{S}$ of (11) is a $(3^m - 1, \{\tau_b\colon\ b \in \mathbb{F}_q\}, 2 \cdot 3^{m-1})$ perfect DSS, where $\tau_b = |D_b|$ for each $b \in \mathbb{F}_q$. Furthermore, the DSS $\mathcal{S}$ is optimal with respect to the bound of (4).*

Proof. Note that $h(0) = 0$. For any $1 \leqslant t \leqslant n-1$, it follows from the definitions of the autocorrelation function and the sequence in (19) that

$$A_u(t) = -1 + \sum_{x \in \mathbb{F}_r} \chi_2\big(h\big(\omega^t x\big) - h(x)\big).$$

Because $(u(i))_{i=0}^{\infty}$ has ideal autocorrelation, we have

$$\sum_{x \in \mathbb{F}_r} \chi_2\big(h\big(\omega^t x\big) - h(x)\big) = 0 \tag{20}$$

for all $1 \leqslant t \leqslant n-1$.

It then follows from $h(-x) = -h(x)$ for all x that

$$\sum_{x \in \mathbb{F}_r} \chi_2\big(-\big[h\big(\omega^t x\big) - h(x)\big]\big) = 0 \tag{21}$$

for all $1 \leqslant t \leqslant n-1$.

We now prove that the function $f = u$ defined in the statement of this theorem is a ZDB function. For any $1 \leqslant t \leqslant n-1$, define

$$Z_f(t) = \big|\big\{x \in \mathbf{Z}_n\colon\ f(x+t) - f(x) = 0\big\}\big|.$$

We have then

$$\begin{aligned} q \cdot Z_f(t) &= -q + \sum_{x \in \mathbb{F}_r} \sum_{y \in \mathbb{F}_q} \chi_2\big(y\big[h\big(\omega^t x\big) - h(x)\big]\big) \\ &= -q + r + \sum_{x \in \mathbb{F}_r} \chi_2\big(h\big(\omega^t x\big) - h(x)\big) + \sum_{x \in \mathbb{F}_r} \chi_2\big(-\big[h\big(\omega^t x\big) - h(x)\big]\big) \\ &= -q + r \end{aligned}$$

for any $1 \leqslant t \leqslant n-1$. Hence $Z_f(t) = 3^{m-1} - 1$ for any $1 \leqslant t \leqslant n-1$. This proves that the function f is a ZDB function. The conclusion of the first part of this theorem then follows from Theorem 2.

It is straightforward to check that

$$(n-1)^2 - \rho(n-1) < \left\lceil \frac{\rho(n-1)}{q-1} \right\rceil.$$

So the lower bound of (4) is met. □

For the construction of difference systems of sets described above, we have the following comments.

- It works only for ternary and binary sequences with ideal autocorrelation. So there may not be any simple connection between perfect difference systems of sets and periodic sequences with ideal autocorrelation.
- The parameters τ_b cannot be determined in general, and have to be computed case by case.

In what follows in this section, we describe a few classes of optimal and perfect difference systems of sets using the generic construction above.

6.1. Difference systems of sets from the function $x^{3^{2t}-3^t+1}+x$ over $\mathbb{F}_{3^{3t}}$

In this section, let $p=3$, $s=1$, $m=3t$ for a positive integer t, $d=3^{2t}-3^t+1$, and let $n=r-1=3^m-1$. Let $(G,+)=(\mathbb{F}_q,+)$, where $q=3$. Let ω be a generator of $\mathbb{F}_{q^m}{}^*$. Define a function f from $(\mathbf{Z}_n,+)$ to $(G,+)$ by

$$f(x)=\mathrm{Tr}_{q^m/q}\left(\omega^x+\omega^{dx}\right),\quad x\in\mathbf{Z}_n, \tag{22}$$

where $\mathrm{Tr}_{q^m/q}$ is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

Theorem 14. *The $\mathcal{S}$ of* (11) *is a $(3^m-1,\{\tau_b\colon\ b\in\mathbb{F}_q\},2\cdot 3^{m-1})$ perfect DSS, where $\tau_0=3^{m-1}-1$ and $\tau_b=3^{m-1}$ for each nonzero $b\in\mathbb{F}_q$. Furthermore, the DSS $\mathcal{S}$ is optimal with respect to the bound of* (4).

Proof. Define the sequence $(u(i))_{i=0}^{\infty}$ by $u(i)=f(i \bmod n)$ for all $i\geqslant 0$, where f is defined in (22). Helleseth, Kumar and Martinsen proved that the sequence has ideal autocorrelation [4]. Define $h(x)=\omega^x+\omega^{dx}$ over $\mathbb{F}_r$. Clearly, $h(-x)=-h(x)$ for all $x\in\mathbb{F}_r$. It then follows from Theorem 13 that the set $\mathcal{S}$ of (11) is a $(3^m-1,\{\tau_b\colon\ b\in\mathbb{F}_q\},2\cdot 3^{m-1})$ perfect DSS.

We now determine the parameters τ_b. For any $1\leqslant t\leqslant n-1$, define $u=\omega^t-1$ and $v=\omega^{dt}-1$. It is proved in [4] that

$$\sum_{x\in\mathbb{F}_r}\epsilon_3^{\mathrm{Tr}_{q^m/q}(ux+vx^d)}=0 \tag{23}$$

for all $1\leqslant t\leqslant n-1$, where $\epsilon_3=e^{2\pi\sqrt{-1}/3}$. There must exist an integer $1\leqslant t\leqslant n-1$ such that $\omega^t=-1$. We have then $u=1$ and $u=1$ for this t as d is odd. It then follows from (23) that

$$\sum_{x\in\mathbb{F}_r}\epsilon_3^{\mathrm{Tr}_{q^m/q}(x+x^d)}=0. \tag{24}$$

Hence

$$\sum_{x\in\mathbb{F}_r}\epsilon_3^{\mathrm{Tr}_{q^m/q}(-(x+x^d))}=0. \tag{25}$$

If $b\neq 0$, then

$$\begin{aligned}\tau_b&=\frac{1}{q}\left[\sum_{x\in\mathbb{F}_r}\sum_{y\in\mathbb{F}_q}\epsilon_3^{y[\mathrm{Tr}_{q^m/q}(x+x^d)-b]}\right]\\&=\frac{1}{q}\left[r+\sum_{y\in\mathbb{F}_q^*}\epsilon_3^{-by}\sum_{x\in\mathbb{F}_r}\epsilon_3^{y[\mathrm{Tr}_{q^m/q}(x+x^d)]}\right]\\&=\frac{1}{q}\left[r+\epsilon_3^{-b}\sum_{x\in\mathbb{F}_r}\epsilon_3^{\mathrm{Tr}_{q^m/q}(x+x^d)}+\epsilon_3^{b}\sum_{x\in\mathbb{F}_r}\epsilon_3^{-[\mathrm{Tr}_{q^m/q}(x+x^d)]}\right]\\&=q^{m-1}.\end{aligned}$$

Similarly, we have

$$\tau_0=-1+\frac{1}{q}\left[\sum_{x\in\mathbb{F}_r}\sum_{y\in\mathbb{F}_q}\epsilon_3^{y[\mathrm{Tr}_{q^m/q}(x+x^d)]}\right]=q^{m-1}-1.$$

The optimality of the DSS follows from Theorem 13. □

Example 2. Let $q = 3$ and $m = 3$. Then the set $\mathcal{S}$ of (11) is a $(26, \{8, 9, 9\}, 18)$ optimal and perfect DSS consisting of the following blocks:

$$D_0 = \{0, 7, 8, 11, 13, 20, 21, 24\},$$
$$D_1 = \{4, 5, 10, 12, 14, 15, 16, 19, 22\},$$
$$D_2 = \{1, 2, 3, 6, 9, 17, 18, 23, 25\}.$$

6.2. Two classes of conjectured perfect difference systems of sets

In this subsection, we describe two classes of conjectured perfect difference systems of sets. Both are related to ternary sequences with ideal autocorrelation.

Conjecture 1. *Let $p = 3$, $s = 1$, $m = 2t + 1$ for a positive integer t, $d = 2 \cdot 3^t + 1$, and let $n = r - 1 = 3^m - 1$. Let $(G, +) = (\mathbb{F}_q, +)$, where $q = 3$. Let ω be a generator of $\mathbb{F}_{q^m}^*$. Define a function f from $(\mathbf{Z}_n, +)$ to $(G, +)$ by*

$$f(x) = \mathrm{Tr}_{q^m/q}\left(\omega^x + \omega^{dx}\right), \quad x \in \mathbf{Z}_n, \tag{26}$$

where $\mathrm{Tr}_{q^m/q}$ is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

With the function f of (26), the $\mathcal{S}$ of (11) is a $(3^m - 1, \{\tau_b\colon\ b \in \mathbb{F}_q\}, 2 \cdot 3^{m-1})$ perfect DSS, where $\tau_0 = 3^{m-1} - 1$ and $\tau_b = 3^{m-1}$ for each nonzero $b \in \mathbb{F}_q$. Furthermore, the DSS $\mathcal{S}$ is optimal with respect to the lower bound of (4).

Define the sequence $(u(i))_{i=0}^{\infty}$ by $u(i) = f(i \bmod n)$ for all $i \geqslant 0$, where f is given in (26). Lin [6] conjectured that this ternary sequence has ideal autocorrelation. If the Lin conjecture is true, this conjecture about perfect difference systems of sets above will be true. However, it is open whether the two conjectures are equivalent.

Acknowledgments

The author is grateful to the two referees for their careful reading of the original version of this paper, their detailed comments and suggestions that much improved the quality of this paper. The author's research is supported by the Research Grants Council of the Hong Kong Special Administrative Region, China, Proj. No. 612405.

References

[1] C. Carlet, C. Ding, Highly nonlinear mappings, J. Complexity 20 (2004) 205–244.
[2] C. Ding, Complex codebooks from combinatorial designs, IEEE Trans. Inform. Theory 52 (9) (2006) 4229–4235.
[3] R. Fuji-Hara, A. Munemasa, V.D. Tonchev, Hyperplane partitions and difference systems of sets, J. Combin. Theory Ser. A 113 (2006) 1689–1698.
[4] T. Helleseth, P.V. Kumar, H. Martinsen, A new family of ternary sequences with ideal two-level autocorrelation function, Des. Codes Cryptogr. 23 (2001) 157–166.
[5] R. Lidl, H. Niederreiter, Finite Fields, Cambridge Univ. Press, Cambridge, 1997.
[6] A. Lin, From cyclic difference sets to perfectly balanced sequences, PhD thesis, University of Southern California, Los Angeles, 1998.
[7] V.I. Levenstein, On method of constructing quasi codes providing synchronization in the presence of errors, Probl. Inf. Transm. 7 (3) (1971) 215–222.
[8] V.I. Levenstein, Combinatorial problems motivated by comma-free codes, J. Combin. Des. 12 (2004) 184–196.
[9] T. Storer, Cyclotomy and Difference Sets, Markham, Chicago, 1967.
[10] V.D. Tonchev, Difference systems of sets and code synchronization, Rend. Sem. Mat. Messina Ser. II 9 (2003) 217–226.
[11] V.D. Tonchev, Partitions of difference sets and code synchronization, Finite Fields Appl. 11 (2005) 601–621.
[12] V.D. Tonchev, H. Wang, Optimal Difference Systems of Sets with Multipliers, Lecture Notes in Comput. Sci., vol. 3967, 2006, pp. 612–618.
[13] V.D. Tonchev, H. Wang, An algorithm for optimal difference systems of sets, J. Comb. Optim. 14 (2007) 165–175.
[14] H. Wang, A new bound for difference systems of sets, J. Combin. Math. Combin. Comput. 58 (2006) 161–167.