Discrete Mathematics 309 (2009) 3954–3961

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Perfect difference systems of sets and Jacobi sums

Ryoh Fuji-Hara [a], Koji Momihara [b,*], Mieko Yamada [c]

[a] Graduate School of Systems and Information Engineering, University of Tsukuba, Tsukuba, 305-8573, Japan

[b] Graduate School of Information Science, Nagoya University, Furo-cho, Chikusa-ku, Nagoya, 464-8601, Japan

[c] Institute of Science and Engineering, Kanazawa University, Kakuma-cho, Kanazawa, 920-1192, Japan

ARTICLE INFO

Article history:
Received 21 April 2008
Received in revised form 3 November 2008
Accepted 7 November 2008
Available online 19 December 2008

Keywords:
Difference systems of sets
Codes for synchronization
Cyclotomic cosets
Jacobi sums

ABSTRACT

A perfect $(v, \{k_i \mid 1 \leq i \leq s\}, \rho)$ difference system of sets (DSS) is a collection of s disjoint k_i-subsets D_i, $1 \leq i \leq s$, of any finite abelian group G of order v such that every non-identity element of G appears exactly ρ times in the multiset $\{a-b \mid a \in D_i, b \in D_j, 1 \leq i \neq j \leq s\}$. In this paper, we give a necessary and sufficient condition in terms of Jacobi sums for a collection $\{D_i \mid 1 \leq i \leq s\}$ defined in a finite field $\mathbb{F}_q$ of order $q = ef + 1$ to be a perfect $(q, \{k_i \mid 1 \leq i \leq s\}, \rho)$-DSS, where each D_i is a union of cyclotomic cosets of index e (and the zero $0 \in \mathbb{F}_q$). Also, we give numerical results for the cases $e = 2, 3$, and 4.

1. Introduction

Definition 1.1. Let G be any abelian group of order v. A collection of s disjoint k_i-subsets D_i, $1 \leq i \leq s$, of G is called a $(v, \{k_i \mid 1 \leq i \leq s\}, \rho)$ difference system of sets, briefly DSS, if every non-identity element of G appears at least ρ times in the multiset

$$\{a - b \mid a \in D_i, b \in D_j, 1 \leq i \neq j \leq s\}. \tag{1}$$

A DSS is called perfect if every non-identity element of G appears exactly ρ times in the multiset (1). A DSS is said to be regular if $k_1 = k_2 = \cdots = k_s$.

If the group G is cyclic, we say that the DSS is cyclic.

The combinatorial problem for the existence of DSSs is motivated by applications for coding theory and cryptography. The concept of DSSs over a cyclic group was first introduced by Levenshtein [8,9] with an application to construct codes that allow for synchronization in the presence of errors. Let U_s^v be a subset of the set of all vectors of length v over $U_s = \{0, 1, \ldots, s-1\}$ of s elements. The ith overlap of $x = (x_0, x_1, \ldots, x_{v-1})$ and $y = (y_0, y_1, \ldots, y_{v-1})$ in U_s^v is defined as

$$T_i(x, y) = (x_{i+1}, \ldots, x_{v-1}, y_0, \ldots, y_i).$$

The comma-free code C of index $\rho(C)$ is a subset $C \subseteq U_s^v$ with $\rho = \min d(z, T_i(x, y))$, where the minimum is taken over all $x, y, z \in C$ and all i, $0 \leq i \leq v-1$, and d means the Hamming distance. The comma-free index $\rho = \rho(C)$ allows one to distinguish a codeword from an overlap of codewords provided that at most $\lfloor \rho/2 \rfloor$ errors have occurred in the given codeword [6]. When $s = q$ with q a prime power, we identify U_s with the finite field $\mathbb{F}_q$ of order q. Levenshtein [8]

[*] Corresponding author.
E-mail addresses: fujihara@sk.tsukuba.ac.jp (R. Fuji-Hara), momihara@math.cm.is.nagoya-u.ac.jp (K. Momihara), myamada@kenroku.kanazawa-u.ac.jp (M. Yamada).

0012-365X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.11.009

gave a construction of a comma-free code of index $\rho > 0$ obtained as cosets of linear codes $C \subseteq \mathbb{F}_q^v$ by utilizing a cyclic $(v, \{k_i \mid 1 \le i \le q\}, \rho)$-DSS, where q is a prime power. In this application of DSSs to codes for synchronization, one requires that $r_s(v, \rho)$ is as small as possible, where let $r_s(v, \rho)$ denote the minimum number of $\sum_{i=1}^{s} k_i$ of DSSs with parameters v, ρ, and s. Levenshtein [8] proved the lower bound

$$r_s(v, \rho) \ge \sqrt{\frac{s\rho(v-1)}{s-1}},$$

with equality if and only if the cyclic DSS is perfect and regular. In [16], Wang improved the bound as follows:

Proposition 1.2. *Let $\{D_i \mid 1 \le i \le s\}$ be a cyclic $(v, \{k_i \mid 1 \le i \le s\}, \rho)$-DSS. Then,*

$$r_s(v, \rho) \ge \begin{cases} \sqrt{\frac{s\rho(v-1)}{s-1}} + 1 & \text{if } \sqrt{\frac{s\rho(v-1)}{s-1}} \text{ is square free;} \\ \sqrt{\frac{s\rho(v-1)}{s-1}} & \text{otherwise.} \end{cases}$$

We define a DSS in any abelian group because it also has an application in the other area of informatics. In [11], Ogata et al. found an application of perfect and regular DSSs (not necessarily cyclic) for authentication codes and secret sharing, and used the term "external difference families" instead of perfect and regular DSSs. For details of this application and related researches, see [1,4,5,11] and the references therein.

In [13,14], Tonchev gave many constructions of cyclic DSSs from cyclic difference sets and balanced generalized weighing matrices. Mutoh and Tonchev [10] gave a method for constructions of cyclic DSSs from cyclotomic cosets of a finite field. Fuji-Hara, Munemasa, and Tonchev [3] presented constructions using hyperplanes of a projective geometry. Cummings [2] gave another construction method of cyclic DSSs and two easily expressed conditions for a systematic code to be comma free. In [15], Tonchev and Wang gave a general algorithm for finding cyclic DSSs attaining the bound of Proposition 1.2 for the given parameters v, s, and ρ. Chang and Ding investigated the existence of external difference families in relation to disjoint difference families. In this paper, we give a necessary and sufficient condition in terms of Jacobi sums for a collection $\{D_i \mid 1 \le i \le s\}$ defined in a finite field $\mathbb{F}_q$ of order $q = ef + 1$ to be a perfect $(q, \{k_i \mid 1 \le i \le s\}, \rho)$-DSS, where each D_i is a union of cyclotomic cosets of index e (and the zero $0 \in \mathbb{F}_q$). We also give numerical results for the cases $e = 2$, 3, and 4, and the resultant perfect DSSs are new in some cases. The method used in this paper was also used by Yamada [17] for supplementary difference sets.

2. Preliminaries

Let $\mathbb{F}_q$ be a finite field of order $q = ef + 1$ a prime power and α a primitive root of $\mathbb{F}_q$. Note that the additive group of $\mathbb{F}_p$ with p a prime is isomorphic to a cyclic group of order p. The cyclotomic cosets C_i, $0 \le i \le e-1$, of index e of $\mathbb{F}_q$ are defined as

$$C_i = \{\alpha^{ej+i} \mid 0 \le j \le f-1\}.$$

And we also define $C_\infty = \{0\}$ for the zero $0 \in \mathbb{F}_q$.

Let $\zeta = \exp(\frac{2\pi\sqrt{-1}}{e}) \in \mathbb{C}$ be a primitive eth root of unity, and denote the integer ring of the cyclotomic field $\mathbb{Q}(\zeta_e)$ by $\mathcal{O}$. We denote the zero $0 \in \mathcal{O}$ by ζ^∞. Let $\mathcal{O}\mathbb{F}_q$ denote the ring of formal polynomials $\mathcal{O}\mathbb{F}_q = \{\sum_{\alpha\in\mathbb{F}_q} c_\alpha X^\alpha \mid c_\alpha \in \mathcal{O}\}$, where X is an indeterminate, which is equipped with an addition and multiplication in the natural way. The zero and unit of $\mathcal{O}\mathbb{F}_q$ are $\sum_{\alpha\in\mathbb{F}_q} 0X^\alpha := 0$ and $X^0 := 1$, respectively. For the convenience of notations, we may identify each subset S defined on $\mathbb{F}_q$ with the group ring element $\sum_{\alpha\in S} X^\alpha \in \mathcal{O}\mathbb{F}_q$ and also regard the element $\sum_{\alpha\in S} X^\alpha$ as the characteristic function F_S from $\mathbb{F}_q$ to $\mathcal{O}$ defined by

$$F_S(\alpha) = \begin{cases} 1 & \text{when } \alpha \in S; \\ 0 & \text{when } \alpha \notin S. \end{cases}$$

Then we can define the addition $F_{S_1} + F_{S_2}$ as

$$(F_{S_1} + F_{S_2})(\alpha) = F_{S_1}(\alpha) + F_{S_2}(\alpha).$$

Furthermore, we define the convolution product $F_{S_1} * F_{S_2}$ as

$$(F_{S_1} * F_{S_2})(\alpha) = \sum_{\beta\in\mathbb{F}_q} F_{S_1}(\beta)F_{S_2}(\alpha - \beta).$$

The conjugate $\hat{F}_S$ of F_S is defined by $\hat{F}_S(\alpha) = F_S(-\alpha)$.

2.1. Jacobi sums over finite fields

A multiplicative character χ of $\mathbb{F}_q$ is a homomorphism of $\mathbb{F}_q^*$ into the multiplicative group of complex $(q-1)$th roots of unity. It is well known that the multiplicative characters of $\mathbb{F}_q$ form a cyclic group C of order $q-1$, called the character group of $\mathbb{F}_q$, that is isomorphic to $\mathbb{F}_q^*$. The identity element of C is the principal character χ_0 that maps each element of $\mathbb{F}_q^*$ to 1. In this paper, we extend the domain in the definition of a multiplicative character to all of $\mathbb{F}_q$ as $\chi(0) = \zeta^{\infty}$. The eth power residue characters are e elements of the unique subgroup of order e of C, i.e., $\chi(\alpha) = \zeta^m$ for a non-negative integer m. Let χ be the primitive eth power residue character, which is defined by $\chi(\alpha) = \zeta^{\ell}$ for $\alpha \in C_{\ell}$. Then, we redefine the eth power residue characters as a cyclic group of order e generated by the primitive character χ.

We define the Jacobi sum for two eth power residue characters χ_1 and χ_2 as follows:

$$\pi(\chi_1, \chi_2) = \sum_{\alpha \in \mathbb{F}_q} \chi_1(\alpha)\chi_2(1-\alpha).$$

The following proposition on Jacobi sums is well known [7].

Proposition 2.1. *The following relations on Jacobi sums hold:*

(i) $\pi(\chi_1, \chi_2) = \pi(\chi_2, \chi_1)$;
(ii) $\pi(\chi_1, \chi_2) = \chi_1(-1)\pi(\chi_1, \overline{\chi_1\chi_2})$;
(iii) $\pi(\chi_0, \chi_0) = q-2$;
(iv) $\pi(\chi, \chi_0) = -1$ *for* $\chi \neq \chi_0$;
(v) $\pi(\chi, \overline{\chi}) = -\chi(-1)$ *for* $\chi \neq \chi_0$;
(vi) *If* χ_1, χ_2, *and* $\chi_1\chi_2$ *are non-principal characters, then* $\pi(\chi_1, \chi_2)\overline{\pi(\chi_1, \chi_2)} = q$,

where $^{-}$ *means the complex conjugation.*

We define $\hat{\chi}$ by $\hat{\chi}(\alpha) = \chi(-\alpha)$.

2.2. Lemmas

The following two lemmas were given in [17].

Lemma 2.2. *For the primitive eth power residue character* χ *and any* $\ell \neq \infty$, *we have*

$$F_{C_\ell} = \frac{1}{e}\sum_{m=0}^{e-1} \zeta^{-\ell m}\chi^m.$$

Lemma 2.3. *For the primitive eth power residue character* χ, *we have*

$$\chi^{\ell} * \hat{\chi}^m = \pi(\chi^m, \chi^{-\ell-m})\chi^{\ell+m} + (q-1)\delta_{\ell+m}F_{C_\infty},$$

where

$$\delta_{\ell+m} = \begin{cases} 1 & \text{when } \ell+m \equiv 0 \pmod{e}; \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, we have the following lemma.

Lemma 2.4. *For the primitive eth power residue character* χ *and any* $\ell \neq \infty$, *we have*

$$F_{C_\ell} * \hat{F}_{C_\infty} + F_{C_\infty} * \hat{F}_{C_\ell} = \frac{1}{e}\sum_{m=0}^{e-1}(1+\chi^m(-1))\zeta^{-\ell m}\chi^m.$$

Proof. For any $\alpha \in \mathbb{F}_q$, we have

$$\begin{aligned}(F_{C_\ell} * \hat{F}_{C_\infty} + F_{C_\infty} * \hat{F}_{C_\ell})(\alpha) &= \left(\left(\frac{1}{e}\sum_{m=0}^{e-1}\zeta^{-\ell m}\chi^m\right) * \hat{F}_{C_\infty} + F_{C_\infty} * \left(\frac{1}{e}\sum_{m=0}^{e-1}\zeta^{-\ell m}\hat{\chi}^m\right)\right)(\alpha) \\ &= \frac{1}{e}\sum_{m=0}^{e-1}\sum_{\beta\in\mathbb{F}_q}\zeta^{-\ell m}(F_{C_\infty}(\beta)\chi^m(\beta-\alpha) + \chi^m(\beta)F_{C_\infty}(\beta-\alpha)) \\ &= \frac{1}{e}\sum_{m=0}^{e-1}\zeta^{-\ell m}(F_{C_\infty}(0)\chi^m(-\alpha) + \chi^m(\alpha)F_{C_\infty}(0)) \\ &= \frac{1}{e}\sum_{m=0}^{e-1}(1+\chi^m(-1))\zeta^{-\ell m}\chi^m(\alpha). \quad \square\end{aligned}$$

3. Main results

Lemma 3.1. *A collection $\{D_i \mid 1 \le i \le s\}$ of s subsets $D_i \subseteq \mathbb{F}_q$ becomes a perfect $(q, \{d_i \mid 1 \le i \le s\}, \rho)$-DSS if and only if*

$$\sum_{1\le i\ne j\le s} F_{D_i} * \hat{F}_{D_j} = \rho\chi_0, \tag{2}$$

where $d_i = |D_i|$, $1 \le i \le s$.

Proof. For any $\alpha \in \mathbb{F}_q^*$,

$$\left(\sum_{1\le i\ne j\le s} F_{D_i} * \hat{F}_{D_j}\right)(\alpha) = \sum_{1\le i\ne j\le s}\sum_{\beta\in\mathbb{F}_q} F_{D_i}(\beta)F_{D_j}(\beta-\alpha) = \rho$$

if and only if there are ρ triples (β, i, j) s.t. $\beta \in D_i$ and $\beta - \alpha \in D_j$, i.e., α is expressed as differences $\beta - (\beta - \alpha)$ exactly ρ ways. For $\alpha = 0 \in \mathbb{F}_q$,

$$\left(\sum_{1\le i\ne j\le s} F_{D_i} * \hat{F}_{D_j}\right)(0) = \sum_{1\le i\ne j\le s}\sum_{\beta\in\mathbb{F}_q} F_{D_i}(\beta)F_{D_j}(\beta) = 0$$

if and only if $\beta \notin D_i$ or $\beta \notin D_j$ for all triples (β, i, j), i.e., D_i and D_j are disjoint for all i and j with $i \ne j$. □

We now give our main theorem.

Theorem 3.2. *Let $q = ef + 1$ be a prime power and let $A_1, A_2, \ldots, A_s$ be mutually disjoint subsets of $\{\infty, 0, 1, \ldots, e-1\}$. We define*

$$D_i = \bigcup_{\ell\in A_i} C_\ell \quad \text{and} \quad k_i = |D_i|.$$

The collection $\{D_i \mid 1 \le i \le s\}$ becomes a perfect $(q, \{k_i \mid 1 \le i \le s\}, \rho)$-DSS if and only if the following are satisfied:

(i) $\sum_{1\le i\ne j\le s} k_ik_j = (q-1)\rho$*; and*
(ii) $\sum_{1\le i\ne j\le s}(\sum_{m=0}^{e-1}\omega_{i,m}\omega_{j,t-m}\pi(\chi^m, \chi^{-t}) + e\gamma_j\omega_{i,t}(1+\chi^t(-1))) = 0$ *for all t, $1 \le t \le e-1$,*

where $\omega_{i,m} = \sum_{\ell\in A_i}\zeta^{-\ell m}$ and $\gamma_j = 1$ if $\infty \in A_j$, otherwise 0. When q and f are odd, i.e., $-1 \in C_{e/2-1}$, it is enough to verify equation (ii) *for even $t > 0$.*

Proof. Put $B_i = A_i \setminus \{\infty\}$ and $u_i = |B_i|$ for each i, $1 \le i \le s$, where $A_i \setminus \{\infty\}$ means that ∞ is removed from A_i when $\gamma_i = 1$. We note that $\sum_{\ell\in B_i}\zeta^{-\ell m} = \omega_{i,m}$ for any m. Then, from Lemmas 2.2–2.4, we have

$$\begin{aligned}
\sum_{1\le i\ne j\le s} F_{D_i} * \hat{F}_{D_j} &= \sum_{1\le i\ne j\le s}\left(\left(\sum_{\ell\in B_i} F_{C_\ell} + \gamma_i F_{C_\infty}\right) * \left(\sum_{\ell\in B_j}\hat{F}_{C_\ell} + \gamma_j\hat{F}_{C_\infty}\right)\right)\\
&= \sum_{1\le i\ne j\le s}\left(\sum_{\ell\in B_i} F_{C_\ell}\right) * \left(\sum_{\ell\in B_j}\hat{F}_{C_\ell}\right) + \sum_{1\le i\ne j\le s}\left(\left(\sum_{\ell\in B_i} F_{C_\ell}\right) * \gamma_j\hat{F}_{C_\infty}\right)\\
&\quad + \sum_{1\le i\ne j\le s}\left(\gamma_i F_{C_\infty} * \left(\sum_{\ell\in B_j}\hat{F}_{C_\ell}\right)\right) + \sum_{1\le i\ne j\le s}\gamma_i\gamma_j(F_{C_\infty} * \hat{F}_{C_\infty})\\
&= \frac{1}{e^2}\sum_{1\le i\ne j\le s}\sum_{\ell=0}^{e-1}\sum_{m=0}^{e-1}\omega_{i,\ell}\omega_{j,m}\chi^\ell * \hat{\chi}^m\\
&\quad + \frac{1}{e}\sum_{1\le i\ne j\le s}\sum_{\ell\in B_i}\sum_{m=0}^{e-1}\gamma_j(1+\chi^m(-1))\zeta^{-\ell m}\chi^m\\
&= \frac{1}{e^2}\sum_{1\le i\ne j\le s}\sum_{\ell=0}^{e-1}\sum_{m=0}^{e-1}\omega_{i,\ell}\omega_{j,m}(\pi(\chi^m, \chi^{-\ell-m})\chi^{\ell+m} + (q-1)\delta_{\ell+m}F_{C_\infty})\\
&\quad + \frac{1}{e}\sum_{1\le i\ne j\le s}\sum_{\ell\in B_i}\sum_{m=1}^{e-1}\gamma_j(1+\chi^m(-1))\zeta^{-\ell m}\chi^m + \frac{2}{e}\sum_{1\le i\ne j\le s}u_i\gamma_j\chi_0
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{e^2}\sum_{1\le i\ne j\le s}\sum_{\ell=0}^{e-1}\sum_{m=0}^{e-1}\omega_{i,\ell}\omega_{j,m}\pi(\chi^m,\chi^{-\ell-m})\chi^{\ell+m} + \frac{q-1}{e^2}\sum_{1\le i\ne j\le s}\sum_{m=0}^{e-1}\omega_{i,m}\omega_{j,-m}F_{C_\infty}\\
&\quad + \frac{1}{e}\sum_{m=1}^{e-1}\sum_{1\le i\ne j\le s}\omega_{i,m}\gamma_j(1+\chi^m(-1))\chi^m + \frac{2}{e}\sum_{1\le i\ne j\le s}u_i\gamma_j\chi_0\\
&= \frac{1}{e^2}\sum_{t=0}^{e-1}\sum_{1\le i\ne j\le s}\sum_{m=0}^{e-1}\omega_{i,m}\omega_{j,t-m}\pi(\chi^m,\chi^{-t})\chi^t + \frac{f}{e}\sum_{1\le i\ne j\le s}\sum_{m=0}^{e-1}\omega_{i,m}\omega_{j,-m}F_{C_\infty}\\
&\quad + \frac{1}{e}\sum_{t=1}^{e-1}\sum_{1\le i\ne j\le s}\omega_{i,t}\gamma_j(1+\chi^t(-1))\chi^t + \frac{2}{e}\sum_{1\le i\ne j\le s}u_i\gamma_j\chi_0.
\end{aligned}$$

Furthermore, we have

$$\begin{aligned}
\sum_{1\le i\ne j\le s}\sum_{m=0}^{e-1}\omega_{i,m}\omega_{j,-m} &= \sum_{1\le i\ne j\le s}\sum_{m=0}^{e-1}\left(\sum_{\ell\in A_i}\zeta^{-\ell m}\right)\left(\sum_{h\in A_j}\zeta^{hm}\right)\\
&= \sum_{1\le i\ne j\le s}\sum_{\ell\in A_i}\sum_{h\in A_j}\sum_{m=0}^{e-1}\zeta^{(-\ell+h)m} = 0,
\end{aligned}$$

and

$$\begin{aligned}
\sum_{1\le i\ne j\le s}\sum_{m=0}^{e-1}\omega_{i,m}\omega_{j,-m}\pi(\chi^m,\chi_0) &= \sum_{1\le i\ne j\le s}\sum_{m=1}^{e-1}\omega_{i,m}\omega_{j,-m}(-1) + \sum_{1\le i\ne j\le s}\omega_{i,0}\omega_{j,0}(q-2)\\
&= -\sum_{1\le i\ne j\le s}\sum_{m=0}^{e-1}\omega_{i,m}\omega_{j,-m} + (q-1)\sum_{1\le i\ne j\le s}u_iu_j\\
&= (q-1)\sum_{1\le i\ne j\le s}u_iu_j.
\end{aligned}$$

Hence, we get

$$\begin{aligned}
\sum_{1\le i\ne j\le s}F_{D_i}*\hat{F}_{D_j} &= \frac{1}{e^2}\sum_{t=1}^{e-1}\sum_{1\le i\ne j\le s}\sum_{m=0}^{e-1}\omega_{i,m}\omega_{j,t-m}\pi(\chi^m,\chi^{-t})\chi^t + \frac{f}{e}\sum_{1\le i\ne j\le s}u_iu_j\chi_0\\
&\quad + \frac{1}{e}\sum_{t=1}^{e-1}\sum_{1\le i\ne j\le s}\omega_{i,t}\gamma_j(1+\chi^t(-1))\chi^t + \frac{2}{e}\sum_{1\le i\ne j\le s}u_i\gamma_j\chi_0.
\end{aligned}$$

In order to satisfy (2) of Lemma 3.1, by the independency of multiplicative characters, the coefficients of χ^t, $\chi^t\ne\chi_0$, must be equal to 0, i.e.,

$$\sum_{1\le i\ne j\le s}\left(\sum_{m=0}^{e-1}\omega_{i,m}\omega_{j,t-m}\pi(\chi^m,\chi^{-t}) + e\gamma_j\omega_{i,t}(1+\chi^t(-1))\right) = 0,$$

which follows equation (ii). Similarly, the coefficient of χ_0 must be equal to ρ, i.e., it must be satisfied

$$\sum_{1\le i\ne j\le s}u_i(fu_j+2\gamma_j) = e\rho,$$

which follows equation (i).

By replacing m of $\pi(\chi^m,\chi^{-t})$ by $t-m$, we have

$$\pi(\chi^{t-m},\chi^{-t}) = \chi^{-t}(-1)\pi(\chi^m,\chi^{-t}).$$

When q and f are odd, i.e., $-1\in C_{e/2-1}$, and t is odd, we get

$$\pi(\chi^{t-m},\chi^{-t}) = -\pi(\chi^m,\chi^{-t}) \quad\text{and}\quad 1+\chi^t(-1)=0.$$

Hence equation (ii) always holds in this case. □

Table 1
We put $\pi = \pi(\chi, \chi)$. In this table, the $(1, 1)$ entry means $\pi(\chi_0, \chi_0) = q - 2$, and the $(1, 2)$ entry means $\pi(\chi_0, \chi) = -1$ and so on.

	χ_0	χ	χ^2
χ_0	$q-2$	-1	-1
χ	-1	π	-1
χ^2	-1	-1	$\overline{\pi}$

Table 2
This table shows numerical results for $e = 3$.

s	A_i	q
2	$A_1 = \{\infty, 0\}, A_2 = \{1\}$	$q = 7, (a, b) = (2, 3)$
	$A_1 = \{0\}, A_2 = \{\infty, 1\}$	$q = 7, (a, b) = (-1, -3)$
	$A_1 = \{\infty, 0\}, A_2 = \{1, 2\}$	$q = 16, (a, b) = (-4, 0)$
	$A_1 = \{0\}, A_2 = \{\infty, 1, 2\}$	$q = 4, (a, b) = (2, 0)$
3	$A_1 = \{0\}, A_2 = \{1\}, A_3 = \{2\}$	q: any

4. Numerical results for small *e*

If the transformation $\sigma : C_i \to C_{i+j}$, where both of i and j are not ∞, acts on any DSS $\{D_i \mid 1 \le i \le s\}$, then the resultant $\{D_i^\sigma \mid 1 \le i \le s\}$ also becomes a DSS with the same parameter. In this sense, we treat only the representatives of equivalent classes of DSSs. Again, put $B_i = A_i \setminus \{\infty\}$ for each i, $1 \le i \le s$, in Theorem 3.2. From now on, we assume that $A_i \ne \{\infty\}$ for all i in view of our applications.

4.1. The quadratic case

For the quadratic character χ and the principal character χ_0, by Proposition 2.1, the values of Jacobi sums are

$$\pi(\chi_0, \chi_0) = q - 2, \qquad \pi(\chi, \chi) = -\chi(-1), \quad \text{and} \quad \pi(\chi_0, \chi) = \pi(\chi, \chi_0) = -1. \tag{3}$$

Now, put $(e, s) = (2, 2)$, $B_1 = \{0\}$, and $B_2 = \{1\}$ in Theorem 3.2. Then, the case $t = 1$ of condition (ii) in Theorem 3.2 is that

$$0 \cdot \pi(\chi_0, \chi) + 0 \cdot \pi(\chi, \chi) + 2\gamma_2(1 + \chi(-1)) - 2\gamma_1(1 + \chi(-1)) = 2(\gamma_2 - \gamma_1)(1 + \chi(-1)) = 0,$$

i.e., condition (ii) is satisfied iff $\gamma_1 = \gamma_2 = 0$ or f is odd. As immediate consequences, we get:

Corollary 4.1. *There exist a perfect and regular $(q = 2f + 1, \{f, f\}, f)$-DSS for any odd prime power q.*

Proof. Put $(e, s, \rho) = (2, 2, f)$, $A_1 = \{0\}$, and $A_2 = \{1\}$ in Theorem 3.2. □

Corollary 4.2. *There exist a perfect $(q = 2f + 1, \{f + 1, f\}, f + 1)$-DSS for any odd prime power $q \equiv 3 \pmod 4$.*

Proof. Put $(e, s, \rho) = (2, 2, f + 1)$, $A_1 = \{\infty, 0\}$, and $A_2 = \{1\}$ in Theorem 3.2. □

4.2. The cubic case

For the cubic character χ and the principal character χ_0, by Proposition 2.1, the values of Jacobi sums are in Table 1.

Lemma 4.3 (*Proposition 8.3.4 in [7]*). *Put $\pi = \pi(\chi, \chi) = a + b\omega$, where ω is a primitive cube root of unity. Then, $a \equiv -1 \pmod 3$ and $b \equiv 0 \pmod 3$.*

To apply Theorem 3.2 for $e \ge 3$, we may need to know the values of Jacobi sums by factorizing the prime power q with a unique representation in the integer ring $\mathcal{O}$. However, in the case of $e = 3$, we do not need it since there is no infinite series of DSSs, except for the trivial case $A_1 = \{0\}, A_2 = \{1\}, A_3 = \{2\}$, and one can calculate the values of Jacobi sums directly for individual cases. For complete numerical results, see Table 2.

Example 4.4. Put $e = 3$, $B_1 = \{0\}$, and $B_2 = \{1\}$ in Theorem 3.2. Then condition (i) implies that either of γ_1 or γ_2 is equal to 1. Next, the cases $t = 1$ and 2 of condition (ii) are that

$$\begin{aligned}(1 + \omega^2)\pi(\chi_0, \chi^2) &+ (1 + \omega^2)\pi(\chi, \chi^2) + 2\omega\pi(\chi^2, \chi^2) + 6(\gamma_2 + \omega^2\gamma_1) \\ &= 2\omega + 2\omega\overline{\pi} + 6(\gamma_2 + \omega^2\gamma_1) = 2(b - 3\gamma_1 + 3\gamma_2) + 2\omega(1 + a - 3\gamma_1) = 0,\end{aligned}$$

and

$$\begin{aligned}(1 + \omega)\pi(\chi_0, \chi) &+ 2\omega^2\pi(\chi, \chi) + (1 + \omega)\pi(\chi^2, \chi) + 6(\gamma_2 + \omega\gamma_1) \\ &= 2\omega^2 + 2\omega^2\pi + 6(\gamma_2 + \omega\gamma_1) = 2(b - 3\gamma_1 + 3\gamma_2) + 2\omega^2(1 + a - 3\gamma_1) = 0,\end{aligned}$$

Table 3
We put $\pi = \pi(\chi, \chi^2)$. The left and right are applied for the cases when $-1 \notin C_0$ and $-1 \in C_0$, respectively.

	χ_0	χ	χ^2	χ^3	χ_0	χ	χ^2	χ^3
χ_0	$q-2$	-1	-1	-1	$q-2$	-1	-1	-1
χ	-1	$-\pi$	π	1	-1	π	π	-1
χ^2	-1	π	-1	$\overline{\pi}$	-1	π	-1	$\overline{\pi}$
χ^3	-1	1	$\overline{\pi}$	$-\overline{\pi}$	-1	-1	$\overline{\pi}$	$\overline{\pi}$

Table 4
This table shows numerical results for $e = 4$. In the column f, the symbols e and o indicate that f is even or odd, respectively.

s	A_i	f	q
2	$A_1 = \{\infty, 0\}, A_2 = \{1\}$	o	$q = a^2 + 4, b = 2$
	$A_1 = \{0\}, A_2 = \{\infty, 1\}$	o	$q = a^2 + 4, b = -2$
	$A_1 = \{\infty, 0\}, A_2 = \{2\}$	o	$q = 1 + b^2, a = 1$
	$A_1 = \{0\}, A_2 = \{2\}$	e	$q = 1 + b^2, a = -1$
	$A_1 = \{0\}, A_2 = \{1, 3\}$	o	q: any
	$A_1 = \{0\}, A_2 = \{2, 3\}$	o	$q = 2a(a + 1) + 1, b = -1 - a$
	$A_1 = \{\infty, 0\}, A_2 = \{2, 3\}$	o	$q = 2a(a + 1) + 1, b = -1 - a$
	$A_1 = \{\infty, 0\}, A_2 = \{1, 2, 3\}$	o	$q = b^2 + 9, a = -3$
	$A_1 = \{0\}, A_2 = \{\infty, 1, 2, 3\}$	o	$q = b^2 + 1, a = 1$
	$A_1 = \{0, 1\}, A_2 = \{2, 3\}$	e	$q = a^2, b = 0$
	$A_1 = \{0, 2\}, A_2 = \{1, 3\}$	any	q: any
3	$A_1 = \{\infty, 0\}, A_2 = \{1\}, A_3 = \{2, 3\}$	o	$q = a^2 + 4, b = -2$
	$A_1 = \{0\}, A_2 = \{\infty, 1\}, A_3 = \{2, 3\}$	o	$q = a^2 + 4, b = 2$
	$A_1 = \{0\}, A_2 = \{1\}, A_3 = \{\infty, 2, 3\}$	e	$q = 9, (a, b) = (3, 0)$
	$A_1 = \{\infty, 0\}, A_2 = \{2\}, A_3 = \{1, 3\}$	o	$q = b^2 + 9, a = -3$
	$A_1 = \{0\}, A_2 = \{2\}, A_3 = \{\infty, 1, 3\}$	e	$q = b^2 + 9, a = 3$
	$A_1 = \{0\}, A_2 = \{2\}, A_3 = \{1, 3\}$	e	$q = b^2 + 1, a = -1$
4	$A_1 = \{0\}, A_2 = \{1\}, A_3 = \{2\}, A_4 = \{3\}$	any	q: any

respectively. Hence, the conditions of Theorem 3.2 are satisfied iff $\gamma_1 = 1$ and $(a, b) = (2, 3)$ or $\gamma_2 = 1$ and $(a, b) = (-1, -3)$. In this case, there exists a perfect $(7, \{2, 3\}, 2)$-DSS. In fact, when we take a primitive root of $q = 7$ as 5, then $\pi = 2 + 3\omega$ and $\{C_\infty \cup C_0 = \{0, 1, 6\}, C_1 = \{2, 5\}\}$ becomes a DSS with the parameter. On the other hand, when we take a primitive root as 3, then $\pi = -1 - 3\omega$ and $\{C_0 = \{1, 6\}, C_\infty \cup C_1 = \{0, 3, 4\}\}$ becomes a DSS with the same parameter.

4.3. The quartic case

For the quartic character χ and the principal character χ_0, by Proposition 2.1, the values of Jacobi sums are in Table 3.

Lemma 4.5. *([12,17]) Put $\pi = \pi(\chi, \chi^2) = a + bi$, where i is a primitive fourth root of unity. Then,*

(i) $a \equiv -1 \pmod 4$ *and* $b \equiv 0 \pmod 4$ *if* $q \equiv 1 \pmod 8$*;*
(ii) $a \equiv 1 \pmod 4$ *and* $b \equiv 2 \pmod 4$ *if* $q \equiv 5 \pmod 8$.

Conversely, for a prime power $q = p^\ell = a^2 + b^2$ with the form (i) *or* (ii) *such that* $\gcd(a, q) = 1$, *it holds* $\pi(\chi, \chi^2) = a + bi$, *where the sign of b is ambiguously determined. If* $p \equiv 3 \pmod 4$, *then ℓ is even, $b = 0$, and* $\pi(\chi, \chi^2) = a$.

Example 4.6. Put $e = 4, B_1 = \{0\}, B_2 = \{1\}, B_3 = \{2, 3\}$, and $q \equiv 5 \pmod 8$ in Theorem 3.2. Then condition (i) implies that either of γ_1 or γ_2 is equal to 1. For condition (ii), it is enough to check the case when $t = 2$, that is,

$$\begin{aligned}&0 \cdot \pi(\chi_0, \chi^2) + 2i\pi(\chi, \chi^2) + 0 \cdot \pi(\chi^2, \chi^2) - 2i\pi(\chi^3, \chi^2) + 8(\gamma_2 - \gamma_1)\\ &\quad = 2i\pi - 2i\bar{\pi} + 8(\gamma_2 - \gamma_1) = -4(b - 2(\gamma_2 - \gamma_1)) = 0.\end{aligned}$$

Hence, the conditions of Theorem 3.2 are satisfied iff $\gamma_1 = 1$ and $b = -2$ or $\gamma_2 = 1$ and $b = 2$. Therefore, by Lemma 4.5, there exists a perfect $(q = 4f + 1 = a^2 + 4, \{f, f + 1, 2f\}, (5f + 3)/2)$-DSS, where q is an odd prime power $\equiv 5 \pmod 8$.

The numerical results for the case when $e = 4$ are given in Table 4. One can easily verify the conditions of Theorem 3.2 and Lemma 4.5.

Remark 4.7. For the complete numerical results on the existence of perfect DSSs for the case when $e = 4$, we only refer to Table 4. However, in actual constructions of the perfect DSSs, one needs a suitable choice of a primitive root of q. For example, in the case of $q = 13, A_1 = \{\infty, 0\}, A_2 = \{1\}$, it must be $a = -3$ and $b = 2$ by Lemma 4.5 and Table 4. When we take a primitive root of $q = 13$ as -2, then $\pi = -3 - 2i$ and it is not suitable. On the other hand, when we take a primitive root of $q = 13$ as 2 (which is essentially equivalent to take the sets obtained by acting the transformation $\sigma : C_i \to C_{3i}$ with $i \neq \infty$ for the DSS, i.e., to take $A_1 = \{\infty, 0\}$ and $A_2 = \{3\}$), then $\pi = -3 + 2i$ and $\{C_\infty \cup C_0, C_1\}$ (or $\{C_\infty \cup C_0, C_3\}$, respectively) gives the desired perfect $(13, \{3, 4\}, 2)$-DSS. The same is applied for the other cases.

Acknowledgements

The authors would like to thank the anonymous referees for their helpful comments and valuable suggestions. The authors also thank Prof. Masakazu Jimbo, Nagoya University, for his constructive suggestions to improve the readability of this paper.

References

[1] Y. Chang, C. Ding, Constructions of external difference families and disjoint difference families, Des. Codes Cryptogr. 40 (2006) 167–185.
[2] L.J. Cummings, A family of circular systematic comma-free codes, J. Combin. Math. Combin. Comput. 58 (2006) 87–96.
[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] G. Ge, Y. Miao, L. Wang, Combinatorial constructions for optimal splitting authentication codes, SIAM J. Discrete. Math. 18 (2005) 663–678.
[5] E.N. Gilbert, F.J. MacWilliams, N.J.A. Sloane, Codes which detect deception, Bell Syst. Tech. J. 53 (1974) 405–424.
[6] S.W. Golomb, B. Gordon, L.R. Welch, Comma-free codes, Canad. J. Math. 10 (2) (1958) 202–209.
[7] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, 1980.
[8] V.I. Levenshtein, On method of constructing quasi codes providing synchronization in the presence of errors, Probl. Inform. Trans. 7 (3) (1971) 215–222.
[9] V.I. Levenshtein, Combinatorial problems motivated by comma-free codes, J. Combin. Des. 12 (2004) 184–196.
[10] Y. Mutoh, V.D. Tonchev, Difference systems of sets and cyclotomy, Discrete Math. 308 (14) (2008) 2959–2969.
[11] W. Ogata, K. Kurosawa, D.R. Stinson, H. Saido, New combinatorial designs and their applications to authentication codes and secret sharing schemes, Discrete Math. 279 (2004) 383–405.
[12] T. Storer, Cyclotomy and Difference Sets, in: Lectures in Advanced Mathematics, Markham Publishing Company, 1967.
[13] V.D. Tonchev, Difference systems of sets and code synchronization, Rend. Sem. Mat. Messina, Ser. II 9 (2003) 217–226.
[14] V.D. Tonchev, Partitions of difference sets and code synchronization, Finite Fields Appl. 11 (2005) 601–621.
[15] V.D. Tonchev, H. Wang, An algorithm for optimal difference systems of sets, J. Combin. Optim. 14 (2007) 165–175.
[16] H. Wang, A new bound for difference systems of sets, J. Combin. Math. Combin. Comput. 58 (2006) 161–168.
[17] M. Yamada, Supplementary difference sets and Jacobi sums, Discrete Math. 103 (1992) 75–90.