Acta Mathematica Sinica, English Series
Dec., 2013, Vol. 29, No. 12, pp. 2261–2272
Published online: November 15, 2013
DOI: 10.1007/s10114-013-2726-7
Http://www.ActaMath.com

Acta Mathematica Sinica, English Series
© Springer-Verlag Berlin Heidelberg &
The Editorial Office of AMS 2013

Difference Systems of Sets Based on Cosets Partitions

Geng Sheng ZHANG Hong Rui WANG
College of Mathematics and Information Science, Hebei Normal University,
Shijiazhuang 050024*, P. R. China*
and
Hebei Key Laboratory of Computational Mathematics and Applications,
Shijiazhuang 050024*, P. R. China*
E-mail: *gshzhang@hebtu.edu.cn zjfwdl@163.com*

Abstract Difference systems of sets (DSS) are combinatorial configurations that arise in connection with code synchronization. This paper proposes a new method to construct DSSs, which uses known DSSs to partition some of the cosets of Z_ν relative to subgroup of order k, where $\nu = km$ is a composite number. As applications, we obtain some new optimal DSSs.

Keywords Difference systems of sets, code synchronization, difference set, coset, optimal

MR(2010) Subject Classification 05B30, 94B50

1 Introduction

Let Z_ν denote the residue additive group of integers modulo ν, that is, $Z_\nu = \{0, 1, \dots, \nu - 1\}$. A difference system of set (DSS) with parameters $(\nu, \{\tau_0, \tau_1, \dots, \tau_{p-1}\}, p, \rho)$ is a collection $\mathcal{P}$ of p disjoint subsets $B_i \subset Z_\nu$, $|B_i| = \tau_i, 0 \le i < p - 1$, such that the multiset

$$\Delta\mathcal{P} := \{(a - b)(\mathrm{mod}\nu) : a \in B_i, b \in B_j, i \neq j,\ 0 \le i, j \le p - 1\} \tag{1.1}$$

contains every number k $(1 \le k \le \nu - 1)$, at least ρ times, and is denoted by DSS$(\nu, \{\tau_0, \tau_1, \dots, \tau_{p-1}\}, p, \rho)$. A DSS is called perfect if every non-zero element of Z_ν appears exactly ρ times in the multi-set (1.1). A DSS is said to be regular if all the subsets B_i are of the same size w and is denoted by (ν, w, p, ρ).

DSSs over a cyclic group were first introduced by Levenshtein [8] and were used for the construction of codes that allow for synchronization in the presence of errors in [7]. Let p be a prime power. Then a DSS$(\nu, \{\tau_0, \tau_1, \dots, \tau_{p-1}\}, p, \rho)$ generates a comma-free code over F_p^ν of index ρ with $\nu - r$ information bits (see [5]), where F_p^ν is a set of all vectors of length ν over a finite field F_p of p elements and $r = \sum_{i=0}^{p-1} |\tau_i|$. In this sense, the number r is called redundancy and p is called the base of the resulting comma-free code over F_p^ν. Clearly, if ν, p, ρ are fixed, then the redundancy r is required to be as small as possible for applying the DSS to code synchronization.

Received November 23, 2012, accepted March 22, 2013
Supported by Natural Science Foundation of Hebei Province (Grant No. A2013205073)

Let $r_p(\nu, \rho)$ denote the minimum redundancy r of a DSS for the given parameters ν, p and ρ. A DSS is called optimal if it has minimum redundancy $r_p(\nu, \rho)$ for the given parameters ν, p and ρ. Levenshtein [8] proved the following lower bound on $r_p(\nu, \rho)$:

$$r_p(\nu, \rho) \geq \sqrt{\frac{p\rho(\nu - 1)}{p - 1}}, \tag{1.2}$$

where the equality holds if and only if the DSS is perfect and regular. In the sequel, this bound is referred to as Levenshtein bound.

The Levenshtein bound of (1.2) cannot be achieved in many cases. If the right-hand side of the inequality (1.2) is not an integer, we get

$$r_p(\nu, \rho) \geq \left\lceil \sqrt{\frac{p\rho(\nu - 1)}{p - 1}} \right\rceil, \tag{1.3}$$

where $\lceil x \rceil$ denotes the ceiling function. It is easy to see that the inequality (1.3) is an equality if and only if

$$r_p(\nu, \rho) - 1 < \sqrt{\frac{p\rho(\nu - 1)}{p - 1}} \leq r_p(\nu, \rho). \tag{1.4}$$

In the following, we can give a sufficient condition that a DSS is optimal.

Lemma 1.1 ([3]) *If a* DSS(ν, $\{\tau_0, \tau_1, \ldots, \tau_{p-1}\}$, p, ρ) *satisfies*

$$\sqrt{\frac{p\rho(\nu - 1)}{p - 1}} > r - 1, \tag{1.5}$$

then it is optimal.

Based on cyclotomic classes, difference sets, and balanced generalized weighting matrices, Tonchev obtained several classes of DSSs (see [11, 12]). Later, Mutoha and Tonchev [9] extended the construction in [12]. Fuji-Hara et al. [4] constructed DSSs from hyperplane line spreads and hyperplanes. Algorithms for constructing optimal DSSs with given parameters n, q, ρ were developed in [13, 14]. Fan et al. [3] gave some constructions of DSSs from cyclic designs. Ding [2] constructed three classes of optimal DSSs. These three classes are based on perfect nonlinear functions, power functions, and ternary sequences with ideal autocorrelation, respectively. Zhou and Tang [16] constructed optimal and perfect difference systems of sets from q-ary sequences with a difference-balanced property. Very recently, [15] give a recursive construction for a DSS with smaller redundancy from a partition-type DSS and a difference set, and Lei, Fan [6] give some recursive constructions of DSSs by using the partition-type cyclic difference packing.

In this paper, using the partitions of cosets of Z_ν relative to subgroup H of order k, where $\nu = km$ is a composite number, we give a recursive constructions of DSSs from the known difference sets and DSSs. As an application, we obtain some new infinite classes of optimal DSSs.

2 A Recursive Construction of DSS

In this section, we will give a recursive construction of DSSs by using partition of cosets of Z_ν, difference sets and DSSs.

Let A, B be given multisets of Z_n and λ be a positive integer. We define some multisets as follows:

$Z_n^* = Z_n \backslash \{0\}$.

$\Delta A = \{x - y : x, y \in A, x \neq y\}$.

$\Delta(A, B) = \{x - y : x \in A, y \in B\}$.

λA means every element of A repeats exactly λ times.

$A \geq \lambda B$ means every element of B appears at least λ times in A.

$A + B = A \cup B$ means their union as a multiset.

Let Z_ν be the additive group of integers modulo ν, where ν is a composite number. Set $\nu = km$, where k and m are positive integers.

We take a subgroup A_0 of order k of Z_ν as follows

$$A_0 = \{0, m, 2m, \ldots, (k-1)m\}.$$

Let σ be the mapping of Z_ν: $\sigma : x \mapsto x + 1$. Then all the cosets of Z_ν modulo A_0 are given by $A_i = \sigma^i(A_0),\ i \in Z_m$. Let

$$\mathcal{A} = \{A_i : i \in Z_m\}.$$

Obviously, for any $A_i, A_j \in \mathcal{A}$, we have

$$\Delta A_i = \Delta A_j = kA_0^*.$$

Lemma 2.1 *For any $A_i, A_j \in \mathcal{A}\,(i \neq j)$, we have*

$$\Delta(A_i, A_j) = kA_{i-j}.$$

Proof For any $A_i, A_j \in \mathcal{A}\,(i \neq j)$,

$$\begin{aligned}\Delta(A_i, A_j) &= \{x - y + i - j : x, y \in A_0\}\\ &= \{x - y + i - j : x \neq y \in A_0\} + \{x - x + i - j : x \in A_0\}\\ &= \sigma^{i-j}(\Delta A_0) + |A_0|\{i - j\}\\ &= k\sigma^{i-j}(A_0^*) + k\{i - j\}\\ &= k(A_{i-j}\backslash\{i - j\}) + k\{i - j\}\\ &= kA_{i-j}.\end{aligned}$$

□

The following is our main theorem.

Theorem 2.2 *Let $\nu = km$ with k and m positive integers. Let $\mathcal{A} = \{A_i : i \in Z_m\}$ be as defined above. Assume that there exists a cyclic (m, h, λ)-difference set H over Z_m, and a* DSS$(k, \{s_1, \ldots, s_n\}, n, \rho')$ *over Z_k, which satisfies $\sum_{i=1}^n s_i = k$. Then there exists a* DSS $(\nu, \{\underbrace{s_1, \ldots, s_1}_{h_0}, \ldots, \underbrace{s_n, \ldots, s_n}_{h_0}, \underbrace{k, \ldots, k}_{h-h_0}\}, h + (n-1)h_0, \rho)$ *over Z_ν, where $1 \leq h_0 \leq h$, $\rho =$* $\min\{k\lambda, h_0\rho'\}$.

Proof Let H be a cyclic (m, h, λ)-difference set over Z_m. By the definition of a difference set, we have

$$\Delta H = \lambda Z_m^*.$$

Let $\mathcal{P}_0 = \{Q_1, \ldots, Q_n\}$ be a DSS$(k, \{s_1, \ldots, s_n\}, n, \rho')$ over Z_k, where $|Q_i| = s_i$, and $\sum_{i=1}^n s_i = k$. According to the definition of DSS, we have

$$\Delta\mathcal{P}_0 = \sum_{1 \le i \ne j \le n} \{x_1 - x_2 : x_1 \in Q_i, x_2 \in Q_j\} \ge \rho' Z_k^*.$$

Let $D_{0,1} = \{mx : x \in Q_1\}, D_{0,2} = \{mx : x \in Q_2\}, \ldots, D_{0,n} = \{mx : x \in Q_n\}$. Obviously, $\sum_{i=1}^n D_{0,i} = A_0$, and

$$\begin{aligned}&\sum_{1 \le i_1 \ne i_2 \le n} \Delta(D_{0,i_1}, D_{0,i_2})\\ &\quad= \sum_{1 \le i_1 \ne i_2 \le n} \{mx_1 - mx_2 : x_1 \in Q_{i_1}, x_2 \in Q_{i_2}\}\\ &\quad\ge \rho'\{mx : x \in Z_k^*\} = \rho' A_0^*.\end{aligned}$$

Let $D_{j,1} = \{mx + j : x \in Q_1\}, D_{j,2} = \{mx + j : x \in Q_2\}, \ldots, D_{j,n} = \{mx + j : x \in Q_n\}$. Similarly, for $j \in Z_m$, we have $\sum_{i=1}^n D_{j,i} = A_j$, and

$$\sum_{1 \le i_1 \ne i_2 \le n} \Delta(D_{j,i_1}, D_{j,i_2}) = \sum_{1 \le i_1 \ne i_2 \le n} \Delta(D_{0,i_1}, D_{0,i_2}) \ge \rho' A_0^*.$$

We take a subset H_0 of H, where $|H_0| = h_0$. Suppose

$$H_0 = \{j_0, j_1, j_2, \ldots, j_{h_0-1}\},$$

where $j_0 < j_1 < j_2 < \cdots < j_{h_0-1}$, and

$$H \backslash H_0 = \{l_1, l_2, \ldots, l_{h-h_0}\},$$

where $l_1 < l_2 < \cdots < l_{h-h_0}$. Now let us construct our DSS. Let

$$\begin{aligned}B_{t,1} &= D_{j_t,1} = \{mx + j_t : x \in Q_1\},\\ B_{t,2} &= D_{j_t,2} = \{mx + j_t : x \in Q_2\},\\ &\vdots\\ B_{t,n} &= D_{j_t,n} = \{mx + j_t : x \in Q_n\},\end{aligned}$$

where $0 \le t \le h_0 - 1,\ j_t \in H_0$ and

$$\mathcal{P} = \{B_{i,1}, B_{i,2}, \ldots, B_{i,n} : 0 \le i \le h_0 - 1\} \cup \{A_{l_i} : l_i \in H \backslash H_0\}.$$

Since

$$\begin{aligned}\Delta\mathcal{P} = &\sum_{t_1=0}^{h_0-1} \sum_{1 \le s_1 \ne s_2 \le n} \Delta(B_{t_1,s_1}, B_{t_1,s_2})\\ &+ \sum_{s_1=1}^{n} \sum_{0 \le t_1 \ne t_2 \le h_0-1} \Delta(B_{t_1,s_1}, B_{t_2,s_1}) + \sum_{\substack{1 \le t_1 \ne t_2 \le h_0-1\\ 1 \le s_1 \ne s_2 \le n}} \Delta(B_{t_1,s_1}, B_{t_2,s_2})\\ &+ \sum_{i=1}^{h-h_0} \sum_{t_1=0}^{h_0-1} \sum_{s_1=1}^{n} \Delta(B_{t_1,s_1}, A_{l_i}) + \sum_{i=1}^{h-h_0} \sum_{t_1=0}^{h_0-1} \sum_{s_1=1}^{n} \Delta(A_{l_i}, B_{t_1,s_1})\end{aligned}$$

$$
\begin{aligned}
&+\sum_{1\leq i\neq j\leq h-h_0}\Delta(A_{l_i},A_{l_j})\\
&=\sum_{t_1=0}^{h_0-1}\sum_{1\leq s_1\neq s_2\leq n}\Delta(B_{t_1,s_1},B_{t_1,s_2})\\
&\quad+\sum_{\substack{i,j\in H_0\\ i\neq j}}\Delta(A_i,A_j)+\sum_{\substack{i\in H_0\\ j\in H\setminus H_0}}\Delta(A_i,A_j)+\sum_{\substack{i\in H_0\\ j\in H\setminus H_0}}\Delta(A_j,A_i)+\sum_{\substack{i,j\in H\setminus H_0\\ i\neq j}}\Delta(A_i,A_j)\\
&=\sum_{t_1=0}^{h_0-1}\sum_{1\leq s_1\neq s_2\leq n}\Delta(B_{t_1,s_1},B_{t_1,s_2})+\sum_{i\neq j\in H}\Delta(A_i,A_j)\\
&\geq\sum_{i=1}^{h-h_0}\rho' A_0^*+\sum_{\substack{i,j\in H\\ i\neq j}}kA_{i-j}\\
&=h_0\rho' A_0^*+\lambda k(Z_\nu\setminus A_0),
\end{aligned}
$$

$\mathcal{P}$ is a DSS with parameters $(\nu,\{\underbrace{s_1,\ldots,s_1}_{h_0},\ldots,\underbrace{s_n,\ldots,s_n}_{h_0},\underbrace{k,\ldots,k}_{h-h_0}\},h+(n-1)h_0,\rho)$ over Z_ν. $\square$

The following example illustrates Theorem 2.2.

Example 2.3 Let $k=7, m=19$, and $\nu=133$. Then cosets A_i of Z_{133}, $0\leq i\leq 18$, are the following:

$$
\begin{aligned}
&A_0=\{0,19,38,57,76,95,114\},\ A_1=\{1,20,39,58,77,96,115\},\\
&A_2=\{2,21,40,59,78,97,116\},\ A_3=\{3,22,41,60,79,98,117\},\\
&A_4=\{4,23,42,61,80,99,118\},\ A_5=\{5,24,43,62,81,100,119\},\\
&A_6=\{6,25,44,63,82,101,120\},\ A_7=\{7,26,45,64,83,102,121\},\\
&A_8=\{8,27,46,65,84,103,122\},\ A_9=\{9,28,47,66,85,104,123\},\\
&A_{10}=\{10,29,48,67,86,105,124\},\ A_{11}=\{11,30,49,68,87,106,125\},\\
&A_{12}=\{12,31,50,69,88,107,126\},\ A_{13}=\{13,32,51,70,89,108,127\},\\
&A_{14}=\{14,33,52,71,90,109,128\},\ A_{15}=\{15,34,53,72,91,110,129\},\\
&A_{16}=\{16,35,54,73,92,111,130\},\ A_{17}=\{17,36,55,74,93,112,131\},\\
&A_{18}=\{18,37,56,75,94,113,132\}.
\end{aligned}
$$

Let H be a cyclic $(19,9,4)$-difference set over Z_{19} and $\{Q_1,Q_2\}$ be a perfect DSS$(7,\{3,4\},2,4)$ over Z_7,

$$H=\{1,4,5,6,7,9,11,16,17\},\quad Q_1=\{1,2,4\},\quad Q_2=\{0,3,5,6\}.$$

Case 1 We take

$$H_0=\{1,4,5,6,7,9,11\}$$

and $h_0=|H_0|=7$. From the above definition of $D_{j,i}$, we have

$$
\begin{aligned}
&B_{01}=\{20,39,77\},\ B_{02}=\{1,58,96,115\},\\
&B_{11}=\{23,42,80\},\ B_{12}=\{4,61,99,118\},
\end{aligned}
$$

$$\begin{aligned} B_{21} &= \{24, 43, 81\},\ \ B_{22} = \{5, 62, 100, 119\}, \\ B_{31} &= \{25, 44, 82\},\ \ B_{32} = \{6, 63, 101, 120\}, \\ B_{41} &= \{26, 45, 83\},\ \ B_{42} = \{7, 64, 102, 121\}, \\ B_{51} &= \{28, 47, 85\},\ \ B_{52} = \{9, 66, 104, 123\}, \\ B_{61} &= \{30, 49, 87\},\ \ B_{62} = \{11, 68, 106, 125\}. \end{aligned}$$

Let

$$\mathcal{P}_1 = \{B_{01}, \dots, B_{61}, B_{02}, \dots, B_{62}, A_{16}, A_{17}\}.$$

Since

$$\rho = k\lambda = h_0\rho' = 28,$$

by the proof of Theorem 2.2, we get a perfect DSS$(133, \{3, \dots,\ 3, 4, \dots, 4, 7, 7\},\ 16,\ 28)$ over Z_{133}. A direct calculation can also confirm it. According to the inequality (1.5) and

$$\sqrt{\frac{p\rho(\nu-1)}{p-1}} = \sqrt{\frac{16 \times 28 \times (133-1)}{16-1}} \approx \sqrt{3942} > r - 1 = 62,$$

the DSS is optimal.

Case 2 We take

$$H_0 = H = \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$$

with $h_0 = |H_0| = 9$. From the definition of $D_{j,i}$, we have

$$\begin{aligned} B_{71} &= \{35, 54, 92\},\ \ B_{72} = \{16, 73, 111, 130\}, \\ B_{81} &= \{36, 55, 93\},\ \ B_{82} = \{17, 74, 112, 131\}. \end{aligned}$$

Let

$$\mathcal{P}_2 = \{B_{01}, \dots, B_{81}, B_{02}, \dots, B_{82}\}.$$

Because $k\lambda = 28, h_0\rho' = 36$, it follows that $\rho = 28$. Thus we get a DSS$(133, \{3, \dots, 3, 4, \dots, 4\}, 18, 28)$ over Z_{133}. According to the inequality (1.5), since

$$\sqrt{\frac{p\rho(\nu-1)}{p-1}} = \sqrt{\frac{18 \times 28 \times (133-1)}{18-1}} \approx \sqrt{3913} > r - 1 = 62,$$

this DSS is optimal.

3 Some Results on Optimal DSSs

In this section, we apply Theorem 2.2 to some known DSSs and difference sets to obtain some new infinite classes of optimal DSSs. First, we give some known DSSs and cyclic difference sets, which are needed in our construction.

Lemma 3.1 ([3]) *Let* $k = \frac{q^{t+1}-1}{q-1}$ *be an odd integer, where* q *is a prime power and* t *is a positive integer. Then there exists a perfect* DSS$(k, \{1, 2, \dots, 2\}, \frac{k+1}{2}, k-1)$ *over* Z_k.

Lemma 3.2 ([3]) *Suppose* $k \equiv 3 \pmod 4$ *is a positive integer such that there exists a Hadamard-difference set. Then there exists a* DSS$(k, \{\frac{k-1}{2}, \frac{k+1}{2}\}, 2, \frac{k+1}{2})$ *over* Z_k.

Lemma 3.3 ([1]) *Let k be an odd prime. Then there exists a* DSS$(k,\ \frac{k-1}{2},\ 2,\ \frac{k-1}{2})$ *over* Z_k.

Corollary 3.4 ([1]) *Let k be an odd prime. Then there exists a* DSS$(k,\ \{1,\ \frac{k-1}{2},\ \frac{k-1}{2}\},\ 3,\ \frac{k+3}{2})$ *over* Z_k.

Lemma 3.5 ([10]) *Let $m = \frac{q^{t+1}-1}{q-1}$, where q is a prime power and t is a positive integer. Then there exists a cyclic $(m, m-1, m-2)$-difference set over Z_m.*

Lemma 3.6 ([10]) *Let $m = \frac{q^{t+1}-1}{q-1}$, where q is a prime power, t is an integer and $t \geq 2$. Then there exists a cyclic $(\frac{q^{t+1}-1}{q-1}, \frac{q^{t}-1}{q-1}, \frac{q^{t-1}-1}{q-1})$-difference set over Z_m.*

Lemma 3.7 ([10]) *Let q be a prime power. Then there exists a $(q^2+q+1, q+1, 1)$-difference set over Z_{q^2+q+1}.*

Lemma 3.8 ([10]) *Let $m = 4q-1$ be a prime. Then the quartic residues in Z_m form a $(4q-1, 2q-1, q-1)$-difference set over Z_m.*

Theorem 3.9 *Let $k = m = \frac{q^{t+1}-1}{q-1}$ be an odd integer and $\nu = km = (\frac{q^{t+1}-1}{q-1})^2$, where q is a prime power and t is a positive integer. Then there exists an optimal* DSS$(\nu,\ \{2,\ \ldots,\ 2, 1,\ \ldots,\ 1\},\ \frac{(q^{t+1}-q)(q^{t+1}+q-2)}{2(q-1)^2},\ \frac{(q^{t+1}-1)(q^{t+1}-2q+1)}{(q-1)^2})$ *over* Z_ν.

Proof Apply Lemmas 3.1 and 3.5 to Theorem 2.2. When $h_0 = m-1$, we obtain the DSS in Theorem 3.9. Regarding the optimality of the DSS, we need to discuss whether the following parameters satisfy the inequality (1.5).

$$\nu = \left(\frac{q^{t+1}-1}{q-1}\right)^2, \quad p = \frac{(q^{t+1}-q)(q^{t+1}+q-2)}{2(q-1)^2},$$
$$\rho = \frac{(q^{t+1}-1)(q^{t+1}-2q+1)}{(q-1)^2}, \quad r = \frac{(q^{t+1}-1)(q^{t+1}-q)}{(q-1)^2}.$$

That is, we need to discuss when the following inequality holds:

$$\sqrt{\frac{\frac{(q^{t+1}-q)(q^{t+1}+q-2)}{2(q-1)^2} \cdot \frac{(q^{t+1}-1)(q^{t+1}-2q+1)}{(q-1)^2} \cdot [(\frac{q^{t+1}-1}{q-1})^2 - 1]}{\frac{(q^{t+1}-q)(q^{t+1}+q-2)}{2(q-1)^2} - 1}} > \frac{(q^{t+1}-1)(q^{t+1}-q)}{(q-1)^2} - 1. \tag{3.1}$$

In fact, the inequality (3.1) can be simplified as follows:

$$-1 + \frac{2q\left(-1+q^t\right)\left(-1+q^{1+t}\right)\left(-2+q+q^{1+t}\right)\left(1+q\left(-2+q^t\right)\right)}{(-1+q)^2\left(-2+q\left(6-3q-2q^t+q^{1+2t}\right)\right)} > 0.$$

It is easy to see that

$$2q\left(-1+q^t\right)\left(-1+q^{1+t}\right)\left(-2+q+q^{1+t}\right)\left(1+q\left(-2+q^t\right)\right) > 0,$$
$$(-1+q)^2 > 0$$

always holds, while q is a prime power and t is a positive integer.

If $q = 2$ and $t > 0$,

$$-2+q\left(6-3q-2q^t+q^{1+2t}\right) = -2+2\left(2^{1+2t}-2^{t+1}\right) = -2+2^{t+2}(2^t-1) > 0.$$

If $q \geq 3$ and $t > 0$,

$$-2+q\left(6-3q-2q^t+q^{1+2t}\right)=-2+q\left(6+q(-3+q^{t-1}(-2+q^{t+1}))\right)>0.$$

To sum up, the inequality (3.1) always holds while q is a prime power and t is a positive integer. So the resultant DSS is optimal. □

Theorem 3.10 *Suppose $k \equiv 3 \pmod 4$ is a positive integer such that there exists a Hadamard-difference set. Let $m = \frac{q^{t+1}-1}{q-1}$, $\nu = km = \frac{k(q^{t+1}-1)}{q-1}$, where q is a prime power, $t \geq 2$ is an integer. Then we have the following:*

(a) *If $k \leq 2q+6$, there exists an optimal* DSS$(\nu$, $\{\frac{k-1}{2}, \ldots, \frac{k-1}{2}, \frac{k+1}{2}, \ldots, \frac{k+1}{2}, k, \ldots, k\}$, $\frac{(q^t+2q^{t-1}-3)}{q-1}$, $\frac{k(q^{t-1}-1)}{q-1})$ *over* Z_ν.

(b) *If $k \leq q+3$ and $q \geq 3$, there exists an optimal* DSS$(\nu$, $\{\frac{k-1}{2}, \ldots, \frac{k-1}{2}, \frac{k+1}{2}, \ldots, \frac{k+1}{2}, k, \ldots, k\}$, $\frac{(q^t+3q^{t-1}-4)}{q-1}$, $\frac{k(q^{t-1}-1)}{q-1})$ *over* Z_ν.

(c) *If $k \leq \frac{6q+20}{9}$ and $q \geq 5$, there exists an optimal* DSS$(\nu$, $\{\frac{k-1}{2}, \ldots, \frac{k-1}{2}, \frac{k+1}{2}, \ldots, \frac{k+1}{2}, k, \ldots, k\}$, $\frac{(q^t+4q^{t-1}-5)}{q-1}$, $\frac{k(q^{t-1}-1)}{q-1})$ *over* Z_ν.

Proof Apply Lemmas 3.2 and 3.6 to Theorem 2.2. When $h_0 = \frac{2(q^{t-1}-1)}{q-1}$, we obtain the DSS of (a). When $h_0 = \frac{3(q^{t-1}-1)}{q-1}$ and $q \geq 3$, we obtain the DSS of (b). When $h_0 = \frac{4(q^{t-1}-1)}{q-1}$ and $q \geq 5$, we obtain the DSS of (c). In the following, we discuss the optimality of these DSSs separately.

(i) Regarding the optimality of DSS of (a), we need to discuss whether the following parameters satisfy (1.5).

$$\nu = \frac{k(q^{t+1}-1)}{q-1}, \quad p = \frac{(q^t+2q^{t-1}-3)}{q-1}, \quad \rho = \frac{k(q^{t-1}-1)}{q-1}), \quad r = \frac{k(q^t-1)}{q-1}.$$

That is, we need to discuss when the following inequality holds:

$$\sqrt{\frac{\frac{q^t+2q^{t-1}-3}{q-1}\cdot\frac{k(q^{t-1}-1)}{q-1}\cdot\left[\frac{k(q^{t+1}-1)}{q-1}-1\right]}{\frac{q^t+2q^{t-1}-3}{q-1}-1}} > \frac{k(q^t-1)}{q-1}-1. \tag{3.2}$$

In fact, the inequality (3.2) can be simplified as follows:

$$(-q+2q^t-q^{1+t})k^2-(q+2q^2+2q^t-3q^{1+t}-2q^{2+t})k-q\left(-2+q+q^2\right)>0. \tag{3.3}$$

Let k_1, k_2, where $k_1 \leq k_2$, be the solution of the following equation:

$$(-q+2q^t-q^{1+t})k^2-(q+2q^2+2q^t-3q^{1+t}-2q^{2+t})k-q\left(-2+q+q^2\right)=0. \tag{3.4}$$

Note that

$$(-q+2q^t-q^{1+t})<0.$$

Clearly, when $k_1 < k < k_2$, (3.3) holds. When $k=1$, (3.3) holds, so we have $k_1 < 1$. Thus, we have

$$\begin{aligned} k_2 &= \frac{q+2q^2+2q^t-3q^{1+t}-2q^{2+t}}{-q+2q^t-q^{1+t}} - k_1 \\ &\geq \frac{q+2q^2+2q^t-3q^{1+t}-2q^{2+t}}{-q+2q^t-q^{1+t}} - 1 \end{aligned}$$

$$\geq 2q+6.$$

It is not hard to get that (3.2) always holds if $k \leq 2q+6$. So the resultant DSS is optimal when $k \leq 2q+6$.

(ii) Regarding the optimality of DSS of (b), we need to discuss when the following inequality holds:

$$\sqrt{\frac{\frac{q^t+3q^{t-1}-4}{q-1}\cdot\frac{k(q^{t-1}-1)}{q-1}\cdot[\frac{k(q^{t+1}-1)}{q-1}-1]}{\frac{q^t+3q^{t-1}-4}{q-1}-1}} > \frac{k(q^t-1)}{q-1}-1. \tag{3.5}$$

In fact, (3.5) can be simplified as follows:

$$-(2q^t-3q^{t-1}+1)k^2+(2q^{t+1}+5q^t-3q^{t-1}-2q-2)k-(q+3)(q-1)>0.$$

Similar to the discussion of (i), it is not hard to get that (3.5) always holds if $k \leq q+3$ and $q \geq 3$. So the resultant DSS is optimal when $k \leq q+3$ and $q \geq 3$.

(iii) Regarding the optimality of DSS of (c), we need to discuss when the following inequality holds:

$$\sqrt{\frac{\frac{q^t+4q^{t-1}-5}{q-1}\cdot\frac{k(q^{t-1}-1)}{q-1}\cdot[\frac{k(q^{t+1}-1)}{q-1}-1]}{\frac{q^t+4q^{t-1}-5}{q-1}-1}} > \frac{k(q^t-1)}{q-1}-1. \tag{3.6}$$

In fact, (3.6) can be simplified as follows:

$$-(3q^t-4q^{t-1}+1)k^2+(2q^{t+1}+7q^t-4q^{t-1}-2q-3)k+(q+4)(q-1)>0.$$

Similar to the discussion of (i), it is not hard to get that (3.6) always holds if $k \leq \frac{6q+20}{9}$ and $q \geq 5$. So the resultant DSS is optimal when $k \leq \frac{6q+20}{9}$ and $q \geq 5$. □

Theorem 3.11 *Suppose* $k \equiv 3 \pmod 4$ *is a positive integer such that there exists a Hadamard-difference set. Let* $m = q^2+q+1$, $\nu = km = k(q^2+q+1)$, *where* q *is a prime power. Then we have the following*:

(a) *If* $k \leq 2q+6$, *there exists an optimal* $\mathrm{DSS}(\nu, \{\frac{k-1}{2}, \ldots, \frac{k-1}{2}, \frac{k+1}{2}, \ldots, \frac{k+1}{2}, k, \ldots, k\}, q+3, k)$ *over* Z_ν.

(b) *If* $k \leq q+3$, *there exists an optimal* $\mathrm{DSS}(\nu, \{\frac{k-1}{2}, \ldots, \frac{k-1}{2}, \frac{k+1}{2}, \ldots, \frac{k+1}{2}, k, \ldots, k\}, q+4, k)$ *over* Z_ν.

Proof Apply Lemmas 3.2 and 3.7 to Theorem 2.2. When $h_0 = 2$, we obtain the DSS of (a). When $h_0 = 3$, we obtain the DSS of (b).

Regarding the optimality of DSS of (a) and (b), we need to discuss when the following inequality holds:

$$\sqrt{\frac{(q+1+h_0)\cdot\ k\cdot[k(q^2+q+1)-1]}{q+h_0}} > (q+1)k-1. \tag{3.7}$$

In fact, (3.7) can be simplified as follows:

$$[(1-h_0)q+1]k^2+[2q^2+2qh_0+q+h_0-1]k-q-h_0>0. \tag{3.8}$$

When $h_0 = 2$, (3.8) can be simplified as follows:

$$(1-q)k^2+(2q^2+5q+1)k-q-2>0.$$

Similar to the discussion of (i) in Theorem 3.10, it is not hard to get that (3.7) always holds if $k \le 2q+6$. So, the resultant DSS is optimal when $k \le 2q+6$.

When $h_0 = 3$, (3.8) can be simplified as follows:

$$(1-2q)k^2 + (2q^2+7q+2)k - q - 3 > 0.$$

Similar to the discussion of (i) in Theorem 3.10, it is not hard to get that (3.8) always holds if $k \le q+3$. So, the resultant DSS is optimal when $k \le q+3$. □

Theorem 3.12 *Suppose* $k \equiv 3 \pmod 4$ *is a positive integer such that there exists a Hadamard-difference set. Let* $m = 4q-1$ *be a prime,* $\nu = km = k(4q-1)$*. Then we have the following*:

(a) *If* $k \le 2q-3$*, there exists an optimal* DSS$(\nu, \{\frac{k-1}{2}, \ldots, \frac{k-1}{2}, \frac{k+1}{2}, \ldots, \frac{k+1}{2}, k, k\}, 4q-4, k(q-1))$ *over* Z_ν*. In particular, when* $k = 2q-3$*, the resultant* DSS *is perfect.*

(b) *If* $k \le 12q-6$*, there exists an optimal* DSS$(\nu, \{\frac{k-1}{2}, \ldots, \frac{k-1}{2}, \frac{k+1}{2}, \ldots, \frac{k+1}{2}, k\}, 4q-3, k(q-1))$ *over* Z_ν*.*

(c) *If* $k \le 6q-5$*, there exists an optimal* DSS$(\nu, \{\frac{k-1}{2}, \ldots, \frac{k-1}{2}, \frac{k+1}{2}, \ldots, \frac{k+1}{2}\}, 4q-2, k(q-1))$ *over* Z_ν*.*

Proof Apply Lemmas 3.2 and 3.8 to Theorem 2.2. When $h_0 = 2q-3$ and $k \le 2q-3$, we obtain the DSS of (a). When $h_0 = 2q-2$, we obtain the DSS of (b). When $h_0 = 2q-1$, we obtain the DSS of (c). In the following, we discuss the optimality of these DSSs separately.

(i) Regarding the optimality of DSS of (a), we need to discuss when the following inequality holds:

$$\sqrt{\frac{(4q-4)\cdot k(q-1)\cdot[k(4q-1)-1]}{4q-5}} > (2q-1)k-1. \tag{3.9}$$

In fact, (3.9) can be simplified as follows:

$$k^2 + (12q^2-20q+6)k - 4q + 5 > 0. \tag{3.10}$$

It is easy to see that (3.10) always holds for any give $q > 1$ and k. So the resultant DSS is optimal.

(ii) Regarding the optimality of DSS of (b), we need to discuss when the following inequality holds:

$$\sqrt{\frac{(4q-3)\cdot k(q-1)\cdot[k(4q-1)-1]}{4q-4}} > (2q-1)k-1. \tag{3.11}$$

In fact, (3.11) can be simplified as follows:

$$-(q-1)k^2 + (q-1)(12q-5)k - 4q + 4 > 0.$$

Similar to the discussion of (i) in Theorem 3.10, it is not hard to get that (3.11) always holds if $k \le 12q-6$. So the resultant DSS is optimal, when $k \le 12q-6$.

(iii) Regarding the optimality of DSS of (c), we need to discuss when the following inequality holds:

$$\sqrt{\frac{(4q-2)\cdot k(q-1)\cdot[k(4q-1)-1]}{4q-3}} > (2q-1)k-1. \tag{3.12}$$

In fact, (3.12) can be simplified as follows:

$$-(2q-1)k^2+(2q-1)(6q-4)k-4q+3>0.$$

Similar to the discussion of (i) in Theorem 3.10, it is not hard to get that (3.12) always holds if $k \le 6q-5$. So, the resultant DSS is optimal when $k \le 6q-5$. □

Theorem 3.13 *Let* $m=q^2+q+1, \nu=k(q^2+q+1)$*, where* k *is an odd prime,* q *is a prime power. Then there exists a* DSS$(\nu,\ \{1,1,\ \frac{k-1}{2},\ \ldots,\ \frac{k-1}{2},\ k,\ \ldots,\ k\},\ q+5,\ k)$ *over* Z_ν*. When* $k \le \frac{6q+20}{9}$*, the resultant* DSS *is optimal.*

Proof Apply Lemma 3.7 and Corollary 3.4 to Theorem 2.2. When $h_0=2$, we obtain the DSS of Theorem 3.13.

Regarding the optimality of the DSS, we need to discuss when the following inequality holds:

$$\sqrt{\frac{(q+5)\cdot k\cdot[k(q^2+q+1)-1]}{q+4}} > (q+1)k-1. \tag{3.13}$$

In fact, (3.13) can be simplified as follows:

$$(-3q+1)k^2+(2q^2+9q+3)k-q-4>0.$$

Similar to the discussion of (i) in Theorem 3.10, it is not hard to get that (3.13) always holds if $k \le \frac{6q+20}{9}$. So, the resultant DSS is optimal when $k \le \frac{6q+20}{9}$. □

Acknowledgements The authors express their gratitude to the referee for his helpful suggestions and comments.

References

[1] Chang, Y., Ding, C.: Constructions of external difference families and disjoint difference families. *Des. Codes Cryptogr.*, **40**, 167–185 (2006)

[2] Ding, C.: Optimal and perfect difference systems of sets. *J. Combin. Theory Ser. A*, **116**, 109–119 (2009)

[3] Fan, C., Lei, J., Chang, Y.: Constructions of difference systems of sets and disjoint difference families. *IEEE Trans. Inform. Theory*, **54**, 3195–3201 (2008)

[4] Fuji-Hara, R., Munemasa, A., Tonchev, V. D.: Hyperplane partitions and difference systems of sets. *J. Combin. Theory Ser. A*, **113**, 1689–1698 (2006)

[5] Golomb, S. W., Gordon, B., Welch, L. R.: Comma-free codes. *Canad. J. Math.*, **10**, 202–209 (1958)

[6] Lei, J., Fan, C.: Optimal difference systems of sets and partition-type cyclic difference packings. *Des. Codes Cryptogr.*, **58**, 135–153 (2011)

[7] Levenshtein, V. I.: Combinatorial problems motivated by comma-free codes. *J. Combin. Des.*, **12**, 184–196 (2004)

[8] Levenshtein, V. I.: One method of constructing quasi codes providing synchronization in the presence of errors. *Probl. Inf. Transm.*, **7**, 215–222 (1971)

[9] Mutoh, Y., Tonchev, V. D.: Difference systems of sets and cyclotomy. *Discrete Math.*, **308**, 2959–2969 (2008)

[10] Stinson, D. R.: Combinatorial Designs: Constructions and Analysis, Springer-Verlag, New York, 2004

[11] Tonchev, V. D.: Difference systems of sets and code synchronization. *Rend. Sem. Mat. Messina Ser. II*, **9**, 217–226 (2003)

[12] Tonchev, V. D.: Partitions of difference sets and code synchronization. *Finite Fields Appl.*, **11**, 601–621 (2005)

[13] Tonchev, V. D., Wang, H.: An algorithm for optimal difference systems of sets. *J. Comb. Optim.*, **14**, 165–175 (2007)

[14] Tonchev, V. D., Wang, H.: Optimal difference systems of sets with multipliers. *Lecture Notes in Comput. Sci.*, **3967**, 612–618 (2006)

[15] Wang, X., Wang, J.: Optimal difference systems of sets and difference sets. *Aequationes Math.*, **82**, 155–164 (2011)

[16] Zhou, Z., Tang, X.: Optimal and perfect difference systems of sets from q-ary sequences with difference-balanced property. *Des. Codes Cryptogr.*, **57**, 215–223 (2010)