

Hyperplane partitions and difference systems of sets [☆]

Ryoh Fuji-Hara ^a, Akihiro Munemasa ^b, Vladimir D. Tonchev ^c

^a Graduate School of System and Information Engineering, University of Tsukuba, Tsukuba, Ibaraki 305-8573, Japan

^b Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan

^c Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA

Received 29 July 2005

Available online 12 June 2006

Abstract

Difference Systems of Sets (DSS) are combinatorial configurations that arise in connection with code synchronization. This paper gives new constructions of DSS obtained from partitions of hyperplanes in a finite projective space, as well as DSS obtained from balanced generalized weighing matrices and partitions of the complement of a hyperplane in a finite projective space.

© 2006 Elsevier Inc. All rights reserved.

Keywords: Code synchronization; Difference set; Generalized balanced weighing matrix; Line spread; Projective space

1. Introduction

A *Difference System of Sets* (DSS) with parameters $(n, \tau_0, \dots, \tau_{q-1}, \rho)$ is a collection of q disjoint subsets $B_i \subseteq \{0, 1, \dots, n-1\}$, $|B_i| = \tau_i$, $0 \leq i \leq q-1$, such that the multiset

$$\{a - b \pmod{n} \mid a \in B_i, b \in B_j, i \neq j\} \quad (1)$$

contains every number i , $1 \leq i \leq n-1$ at least ρ times. A DSS is *perfect* if every number i , $1 \leq i \leq n-1$ is contained exactly ρ times in the multiset (1). A DSS is *regular* if all subsets B_i are of the same size: $\tau_0 = \tau_1 = \dots = \tau_{q-1} = m$.

Difference systems of sets were introduced by V. Levenshtein [8] (see also [9]) and were used for the construction of codes that allow for synchronization in the presence of errors.

[☆] Research supported by NSF Grant CCR-0310632.

E-mail address: tonchev@mtu.edu (V.D. Tonchev).

A q -ary code of length n is a subset of the set F_q^n of all vectors of length n over a set F_q of q elements. If q is a prime power, we often identify F_q with a finite field $\text{GF}(q)$ of order q . A linear q -ary code (q a prime power), is a linear subspace of the vector space $\text{GF}(q)^n$. If $x = x_1 \cdots x_n$, $y = y_1 \cdots y_n \in F_q^n$, and $0 \leq i \leq n-1$, the i th concatenation of x and y is defined as $T_i(x, y) = x_{i+1} \cdots x_n y_1 \cdots y_i$. The comma-free index $\rho = \rho(C)$ of a code $C \subseteq F_q^n$ is defined as

$$\rho = \min d(z, T_i(x, y)),$$

where the minimum is taken over all $x, y, z \in C$ and all $i = 1, \dots, n-1$, and d is the Hamming distance between vectors in F_q^n . The comma-free index $\rho(C)$ allows one to distinguish a codeword from any concatenation of two codewords (and hence provides for synchronization of codewords) provided that at most $\lfloor \rho(C)/2 \rfloor$ errors have occurred in the given codeword. Levenshtein [8] gave a construction of a q -ary comma-free code of index $\rho > 0$ obtained as a coset of a linear code of length n with redundancy $r = \sum_{j=0}^{q-1} |B_j|$ that utilizes a DSS with parameters $(n, \tau_0, \dots, \tau_{q-1}, \rho)$.

The singletons $B_0 = \{x_0\}$, $B_1 = \{x_1\}$, $\dots$, $B_{k-1} = \{x_{k-1}\}$ of any (n, k, λ) cyclic difference set yield a DSS with parameters $q = k$ and $\rho = \lambda$. The following lemma gives a simple generalization of this observation that can be used for the construction of DSS as partitions of cyclic difference sets (for undefined terms concerning designs see [1,2]).

Lemma 1.1. [10] *Let $D \subseteq \{0, 1, \dots, n-1\}$, $|D| = k$, be a cyclic (n, k, λ) difference set. Assume that D is partitioned into q disjoint subsets $B_0, \dots, B_{q-1}$ that are the base blocks of a cyclic design $\mathcal{D}$ with block sizes $\tau_i = |B_i|$, $i = 0, \dots, q-1$ such that every pair of points is contained in at most λ_1 blocks. Then the sets $B_0, \dots, B_{q-1}$ form a DSS with parameters $(n, \tau_0, \dots, \tau_{q-1}, \rho = \lambda - \lambda_1)$. The DSS $\{B_i\}_{i=0}^{q-1}$ is perfect if and only if $\mathcal{D}$ is a pairwise balanced design with every pair of points occurring in exactly λ_1 blocks.*

Applying this lemma to a difference set of Singer type, where the difference set D is a hyperplane in a projective geometry $\text{PG}(2s, p^e)$, (p prime), leads to the problem of finding a partition of a hyperplane in $\text{PG}(2s, p^e)$ into disjoint projective lines that belong to different orbits under the Singer cyclic group acting regularly on the points of $\text{PG}(2s, p^e)$ [10]. Any such partition is a special case of a more general type of partition of the hyperplanes of $\text{PG}(2s, p^e)$ into lines studied by Fuji-Hara, Jimbo and Vanstone [3] in connection with packings of lines in $\text{PG}(2s+1, p)$. Fuji-Hara, Jimbo and Vanstone [3] proved the existence of such partitions invariant under the Singer cyclic group in $\text{PG}(2s, 2)$ for $s \leq 5$, and in $\text{PG}(2s, 3)$ for $s \leq 3$, thus establishing the existence of perfect regular DSS obtainable from a Singer difference set in these particular projective spaces.

In this paper, we investigate further the problem of partitioning a hyperplane into a DSS.

In Section 2, we show that partitions of a hyperplane into regular and perfect (hence optimal) DSS, where the parts are projective lines, exist in $\text{PG}(4, 5)$, $\text{PG}(4, 8)$, and $\text{PG}(4, 9)$. We also show that the Singer $(341, 85, 21)$ difference set cannot be partitioned into a regular and perfect DSS with $q = 17$ and $\rho = 20$, or in geometric language, a hyperplane in $\text{PG}(4, 4)$ cannot be partitioned into disjoint lines that belong to different orbits under the Singer group of order 341. This is the first and only known example of a projective space $\text{PG}(2s, p^e)$ such that every line spread of a hyperplane contains a pair of lines belonging to the same Singer cycle of length $(p^{e(2s+1)} - 1)/(p^e - 1)$. This example shows that line spreads of hyperplanes in $\text{PG}(2s, p^e)$ that are perfect and regular DSS do not exist in every dimension and for every prime power p^e .

In Section 3, we describe a construction of irregular DSS obtained by partitioning a hyperplane of $\text{PG}(2t+1, p^e)$ into a projective $(t+1)$ -subspace and parallel affine subspaces. Such partitions exist for any $t \geq 2$.

The last Section 4 gives a construction of perfect DSS that uses balanced generalized weighing matrices. Applied to a special class of such matrices obtained from finite projective spaces, this construction yields perfect DSS obtained as partitions of the complement of a hyperplane in $\text{PG}(d, p^e)$ for any $d \geq 1$ and any prime power p^e such that $p^e - 1$ and $(p^{e(d+1)} - 1)/(p^e - 1)$ are relatively prime. The same construction yields perfect DSS obtained from balanced generalized weighing matrices related to difference sets of GMW type studied by Jungnickel and the third author in [4,7].

2. DSS from hyperplane line spreads

In this section, we show that a difference set of Singer type in $\text{PG}(4, p^e)$ admits a line spread whose members belong to different orbits under the Singer group, for $p^e = 5, 8$ and 9 . As a result, we obtain perfect regular DSSs with parameters

$$n = \frac{p^{5e} - 1}{p^e - 1}, \quad q = p^{2e} + 1, \quad \rho = p^e(p^e + 1)$$

for $p^e = 5, 8$ and 9 . For $p^e = 4$, we found by an exhaustive computer search that no such line spread exists. This is the first and only known example of a projective space $\text{PG}(2s, p^e)$ such that every line spread of a hyperplane contains a pair of lines belonging to the same Singer cycle of length $(p^{e(2s+1)} - 1)/(p^e - 1)$.

We now fix notation in order to describe our results. If we identify the underlying 5-dimensional vector space of $\text{PG}(4, p^e)$ with $\text{GF}(p^{5e})$, then the points of $\text{PG}(4, p^e)$ can be represented by $a^0, a^1, \dots, a^{n-1}$, where a is a primitive element of $\text{GF}(p^{5e})$, to be specified later. The Singer cycle σ is the multiplication by a , while the Frobenius automorphism f is defined by $a \mapsto a^p$. Note that f is in general a semilinear transformation, and f^e is a linear transformation.

Since the kernel H of the trace map of $\text{GF}(p^{5e})$ over $\text{GF}(p^e)$ is a hyperplane of $\text{GF}(p^{5e})$, regarded as a 5-dimensional vector space over $\text{GF}(p^e)$, we may restrict our attention to line spreads of H . An advantage of taking H is that H is fixed by the Frobenius automorphism f , so we can hope to find a spread invariant under f with the desired property, namely, that lines of the spread belong to distinct orbits under the Singer cycle. This approach turns out to be successful for $p^e = 5, 8$ and 9 .

For each of $p^e = 5, 8$ and 9 , we fix a primitive element a of $\text{GF}(p^{5e})$ as follows, in order to identify the points of $\text{PG}(4, p^e)$ with the integers $\{0, 1, \dots, n-1\}$. When $p^e = 5$, we let a be an element satisfying

$$a^5 + 4a + 3 = 0.$$

When $p^e = 8$, we let a be an element satisfying

$$a^{15} + a^5 + a^4 + a^2 + 1 = 0.$$

When $p^e = 9$, we let a be an element satisfying

$$a^{10} + 2a^6 + 2a^5 + 2a^4 + a + 2 = 0.$$

We now give the DSS found by computer search. In Table 1, we give a list of lines whose images under $\langle f \rangle$ form a spread of H and also a perfect DSS. The second column of Table 1

Table 1
PG(4, 5)

B	$ B^{\langle f \rangle} $	B	$ B^{\langle f \rangle} $
{0, 1, 5, 25, 125, 625}	1	{0, 1, 5, 25, 125, 625}	1
{3, 26, 113, 131, 458, 470}	5	{7, 387, 480, 539, 588, 650}	5
{11, 169, 197, 364, 417, 675}	5	{27, 41, 112, 329, 565, 701}	5
{51, 83, 112, 496, 539, 642}	5	{6, 151, 458, 509, 627, 724}	5
{6, 48, 266, 439, 616, 715}	5	{3, 143, 190, 197, 462, 775}	5
{2, 153, 155, 303, 567, 644}	5	{2, 48, 255, 448, 579, 585}	5

Table 2
PG(4, 8)

B	$ B^{\langle f \rangle} $
{417, 1037, 2567, 3020, 3035, 3500, 3982, 4228, 4337}	5
{27, 1159, 1907, 1932, 3099, 3163, 3751, 3949, 4003}	15
{81, 478, 863, 1845, 2307, 2908, 3103, 4208, 4626}	15
{245, 1338, 1670, 2126, 2602, 2804, 3153, 3437, 3885}	15
{17, 1857, 2297, 2377, 2791, 2976, 3154, 3791, 4079}	15

Table 3
PG(4, 9)

B	$ B^{\langle f \rangle} $
{59, 531, 2171, 3125, 3287, 4777, 4779, 5982, 6088, 6106}	2
{50, 248, 737, 1216, 1947, 2318, 4769, 4880, 6039, 6771}	5
{244, 1617, 1708, 1738, 2263, 2745, 3715, 4250, 4392, 6791}	5
{20, 148, 917, 1624, 2489, 3363, 3902, 5013, 6396, 6984}	10
{73, 979, 1088, 1181, 1270, 2348, 2862, 3984, 4017, 4642}	10
{23, 560, 731, 781, 1409, 2590, 2865, 5410, 6503, 7260}	10
{7, 109, 937, 3432, 3456, 3678, 4354, 4462, 4718, 7141}	10
{119, 705, 2879, 3912, 4059, 5180, 5737, 6781, 7085, 7289}	10
{164, 1725, 2423, 2856, 2974, 4449, 5220, 6360, 6598, 6674}	10
{83, 595, 748, 1324, 1979, 2105, 3897, 5631, 6572, 6618}	10

gives the length of the orbit under $\langle f \rangle$, hence we obtain a total of 26 lines. We note that, according to our exhaustive search, the two spreads in Table 1 are the only DSS formed by an $\langle f \rangle$ -invariant spread of H . Similarly, each of Tables 2, 3 gives the unique DSS formed by an $\langle f \rangle$ -invariant spread of H , for $p^e = 8, 9$, respectively.

We remark that, when $p^e = 4$, an exhaustive search found no DSS formed by a spread of H , even after we dropped the $\langle f \rangle$ -invariance assumption.

3. DSS from partitions into subspaces

Consider the projective space $\text{PG}(n, p^e)$, where $n = 2t + 1$ is odd. In this section, we describe two infinite classes of irregular DSS obtained from hyperplane partitions defined by t -flats in $\text{PG}(n, p^e)$. To avoid cumbersome formulas, we use q to denote an arbitrary prime power p^e throughout this section.

For subsets D, A, B of an additive group, let ΔD and $\Delta(A, B)$ be multisets defined by

$$\Delta D := \{x - y \mid x, y \in D, x \neq y\} \quad \text{and} \\ \Delta(A, B) := \{x - y \mid x \in A, y \in B\},$$

respectively. Note that $\Delta A = \lambda B$, where λ is an positive integer, means that every element of B appears λ times in ΔA . We also denote by $A + B$ their union as multisets, or more formally, the sum in the group algebra of the underlying additive group.

By taking a primitive element of $\text{GF}(q^{n+1})$, we may identify the points of $\text{PG}(n, q)$ with the additive group Z_v of integers modulo v , where $v = (q^{n+1} - 1)/(q - 1)$. The t -flat corresponding to the subfield $\text{GF}(q^{t+1})$ is then given by

$$S = \{0, m, 2m, \dots, (k-1)m\},$$

where $m = (q^{n+1} - 1)/(q^{t+1} - 1)$ and $k = (q^{t+1} - 1)/(q - 1)$. Let $S^* = S \setminus \{0\}$. The set of differences of S is

$$\Delta S = kS^*.$$

Let W be the set of all $(t+1)$ -flats that contain S , and pick $F_0 \in W$. There is an automorphism σ of $\text{PG}(n, q)$ such that $\sigma: x \mapsto x + m$. This automorphism fixes S . Therefore, the $(t+1)$ -flats

$$F_i = \sigma^i F_0 \quad (0 \leq i \leq k-1)$$

all contain S . Since $|W| = k$, we conclude $W = \{F_i \mid 0 \leq i \leq k-1\}$. It is easy to see that $\Delta F_i = \Delta F_j$ for any $F_i, F_j \in W$.

Lemma 3.1. *Let L_c be the set of lines of $\text{PG}(n, q)$ incident with a point c . Then we have*

$$\sum_{l \in L_c} \Delta l = (q+1)Z_v^*,$$

where $Z_v^* = Z_v \setminus \{0\}$.

Proof. First observe that the left-hand side is independent of the choice of a point c . Thus

$$\begin{aligned} \sum_{l \in L_c} \Delta l &= \frac{1}{v} \sum_{c: \text{point}} \sum_{l \in L_c} \Delta l \\ &= \frac{1}{v} \sum_{l: \text{line}} (q+1) \Delta l \\ &= (q+1)Z_v^*. \quad \square \end{aligned}$$

It is not difficult to generalize this lemma to any cyclic 2-design with v points and block size k , $\sum_{l \in L_c} \Delta l = kZ_v^*$ even if it has a short orbit.

Lemma 3.2. *Let A_i be the affine part of F_i , i.e., $A_i = F_i \setminus S$. Then we have*

$$\Delta A_i = (q-1)(Z_v^* \setminus S^*) \quad \text{for each } i = 0, 1, \dots, k-1.$$

Proof. For two distinct points $x, y \notin S$, there exists i such that $x, y \in A_i$ if and only if the line through x, y meets S . Thus,

$$\sum_{i=0}^{k-1} \Delta A_i = \sum_{c \in S} \sum_{\substack{l: \text{line} \\ l \cap S = \{c\}}} \Delta(l \setminus \{c\})$$

$$\begin{aligned}
&= \sum_{c \in S} \sum_{l \in L_c} \Delta l - \sum_{c \in S} (\Delta(Z_v \setminus S, \{c\}) + \Delta(\{c\}, Z_v \setminus S)) \\
&= \sum_{c \in S} \left(\sum_{l \in L_c} \Delta l - \sum_{l \in L_c \cap L(S)} \Delta l \right) - (\Delta(Z_v \setminus S, S) + \Delta(S, Z_v \setminus S)) \\
&= \sum_{c \in S} ((q+1)Z_v^* - (q+1)S^*) - 2|S|(Z_v^* \setminus S^*) \\
&= (q-1)|S|(Z_v^* \setminus S^*).
\end{aligned}$$

Since ΔA_i is independent of i , the result follows. $\square$

Lemma 3.3.

$$\Delta(S, A_i) = \Delta(A_i, S) = Z_v^* \setminus S^* \quad \text{for each } i = 0, 1, \dots, k-1.$$

Proof. Observe that $\Delta(S, A_i)$ is independent of i , and

$$\begin{aligned}
\sum_{i=0}^{k-1} \Delta(S, A_i) &= \Delta(S, Z_v \setminus S) \\
&= |S|(Z_v^* \setminus S^*).
\end{aligned}$$

Thus $\Delta(S, A_i) = Z_v^* \setminus S^*$, and similarly, we obtain $\Delta(A_i, S) = Z_v^* \setminus S^*$. $\square$

Lemmas 3.2 and 3.3 imply the following lemma.

Lemma 3.4.

$$\Delta F_i = (q+1)(Z_v^* \setminus S^*) + kS^*$$

for each $i = 0, 1, \dots, k-1$.

Theorem 3.5. Let H_0 be a hyperplane of $\text{PG}(2t+1, q)$ containing the t -flat S . Let $W' = \{F_0, F_1, \dots, F_{h-1}\}$ be the set of $(t+1)$ -flats of H_0 containing S , where $h = (q^t - 1)/(q - 1)$, and set $A_i = F_i \setminus S$, $v = (q^{2t+1} - 1)/(q - 1)$, $\rho = q^{2t-1} + q^{2t-2} + \dots + q^{t+1}$.

- (i) The partition $\{F_0, A_1, A_2, \dots, A_{h-1}\}$ of the hyperplane H_0 is a DSS with parameters $(v, \tau_0, \tau_1, \dots, \tau_{h-1}, \rho)$, where $\tau_0 = (q^{t+2} - 1)/(q - 1)$, $\tau_1 = \tau_2 = \dots = \tau_{h-1} = q^{t+1}$.
- (ii) The partition $\{A_0, A_1, A_2, \dots, A_{h-1}, S\}$ of the hyperplane H_0 is a DSS with parameters $(v, \tau_0, \tau_1, \dots, \tau_h, \rho)$, where $\tau_0 = \tau_1 = \dots = \tau_{h-1} = q^{t+1}$, $\tau_h = (q^{t+1} - 1)/(q - 1)$.

Proof. It is well known that H_0 is a difference set, that is, $\Delta H_0 = (q^{2t} - 1)/(q - 1)Z_v^*$. From the above lemmata,

$$\Delta F_0 + \Delta A_1 + \Delta A_2 + \dots + \Delta A_{h-1} = (q^t + 1)(Z_v^* \setminus S^*) + \frac{q^{t+1} - 1}{q - 1}S^*.$$

Since $(q^{t+1} - 1)/(q - 1) \geq q^t + 1$, the partition $\{F_0, A_1, A_2, \dots, A_{h-1}\}$ is a DSS with parameters $(v, \tau_0, \tau_1, \dots, \tau_{h-1}, \rho)$, where

$$\begin{aligned}\rho &= (q^{2t} - 1)/(q - 1) - (q^{t+1} - 1)/(q - 1) \\ &= q^{2t-1} + q^{2t-2} + \cdots + q^{t+1}.\end{aligned}$$

This proves the assertion (i). The proof of (ii) is similar. $\square$

Example 3.6. Here we give an example in $\text{PG}(5, 2)$. We take a primitive element a of $\text{GF}(2^6)$ with minimal polynomial $a^6 + a + 1 = 0$, so that the point set is represented by Z_{63} , and

$$S = \{0, 9, 18, 27, 36, 45, 54\}.$$

The following partition is a DSS with parameters $(63, 15, 8, 8, \rho = 8)$,

$$F_0 = \{0, 1, 6, 8, 9, 14, 18, 27, 36, 38, 45, 48, 49, 52, 54\},$$

$$A_1 = \{2, 12, 13, 16, 28, 33, 35, 41\},$$

$$A_2 = \{3, 4, 7, 19, 24, 26, 32, 56\},$$

while the following partition is a DSS with $(63, 8, 8, 8, 7, \rho = 8)$:

$$A_0 = \{1, 6, 8, 14, 38, 48, 49, 52\},$$

$$A_1 = \{2, 12, 13, 16, 28, 33, 35, 41\},$$

$$A_2 = \{3, 4, 7, 19, 24, 26, 32, 56\},$$

$$S = \{0, 9, 18, 27, 36, 45, 54\}.$$

4. Perfect DSS from the complement of a hyperplane

Let $B_0, B_1, \dots, B_{q-1}$ be disjoint subsets of $Z_n = \{0, 1, \dots, n-1\}$. We define a circulant $n \times n$ array A (see (2)), having all entries in its first row that are indexed by elements of B_i equal to i ($0 \leq i \leq q-1$), and entries that are not indexed by any $\alpha \in B_i$ for some i are left empty.

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_j & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{j-1} & \cdots & a_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n-i+1} & a_{n-i+2} & \cdots & a_{j-i+1} & \cdots & a_{n-i} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n-i'+1} & a_{n-i'+2} & \cdots & a_{j-i'+1} & \cdots & a_{n-i'} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_1 & a_2 & \cdots & a_{j+1} & \cdots & a_0 \end{pmatrix}. \quad (2)$$

Example 4.1. Let $n = 7$, $q = 4$, $B_0 = \{2\}$, $B_1 = \{4\}$, $B_2 = \{5\}$, $B_3 = \{6\}$. The corresponding circulant array is

$$A = \begin{pmatrix} & 0 & 1 & 2 & 3 \\ 3 & & 0 & 1 & 2 \\ 2 & 3 & & 0 & 1 \\ 1 & 2 & 3 & & 0 \\ & 1 & 2 & 3 & \\ 0 & 1 & 2 & 3 & \\ & 0 & 1 & 2 & 3 \end{pmatrix}.$$

Lemma 4.2. *The collection $\mathcal{B} = \{B_i\}_{i=0}^{q-1}$ is a DSS of index ρ if and only if for every pair of rows i, i' of A , ($i \neq i'$), there exist at least ρ columns that intersect rows i, i' in two nonempty entries that contain different symbols from $\{0, 1, \dots, q-1\}$. The DSS is perfect if and only if equality holds for all pairs i, i' ($i \neq i'$).*

Proof. The difference of the indices of two entries $a_{j-i+1}, a_{j-i'+1}$ ($0 \leq i < i' \leq n-1$) in the j th column ($0 \leq j \leq n-1$) and rows i and i' of A , is

$$(j-i+1) - (j-i'+1) = i' - i.$$

Assume that $\mathcal{B}$ is a DSS of index ρ . Then we have

$$i' - i = x_1 - y_1 = x_2 - y_2 = \dots = x_m - y_m, \quad (3)$$

where $m \geq \rho$ and x_s and y_s ($1 \leq s \leq m$) belong to different blocks from $\mathcal{B}$. It follows that there are m columns $j_1, j_2, \dots, j_m$ of A such that the entries $a_{j_s-i+1}, a_{j_s-i'+1}$ are two different numbers from the set $\{0, 1, \dots, q-1\}$.

Conversely, assume that the hypothesis of the lemma holds, and let s be an integer, $1 \leq s \leq n-1$. We can write s as a difference

$$s = i - i',$$

where i and i' ($0 \leq i < i' \leq n-1$) are indices of two different rows of A . Since there are at least ρ columns of A that intersect rows i and i' in entries that contain different symbols from $\{0, 1, \dots, q-1\}$, and since the difference of the indices of two entries of A located in the same column of rows i and i' is $i' - i$, it follows that the equation

$$s = i' - i = x_l - y_l$$

has at least ρ solutions $\{x_l, y_l\}$, where x_l and y_l belong to different blocks from $\mathcal{B}$. $\square$

Definition 4.3. Let G be a multiplicative group. A *balanced generalized weighing matrix* $BGW(n, k, \mu)$ with parameters n, k, μ over G is an $n \times n$ matrix $W = (g_{ij})$ with entries from $\bar{G} = G \cup \{0\}$ such that each row of W contains exactly k nonzero entries, and for every $a, b \in \{1, \dots, n\}$, $a \neq b$, the multiset $\{g_{ai}g_{bi}^{-1} : 1 \leq i \leq n, g_{ai}, g_{bi} \neq 0\}$ contains every element of G exactly $\mu/|G|$ times.

Note 4.4. Replacing the nonzero entries in a $BGW(n, k, \mu)$ with 1's yields a $(0, 1)$ -incidence matrix of a symmetric 2 -(n, k, μ) design.

An immediate corollary of Lemma 4.2 is the following.

Theorem 4.5. *The existence of a circulant balanced generalized weighing matrix $W = BGW(n, k, \mu)$ over a group G of order g implies the existence of a perfect DSS with parameters*

$$n, \quad q = g, \quad \rho = (g-1)\mu/g.$$

Proof. Consider the circulant array A obtained from W by deleting all zeros. By the property of W , every pair of rows of A differ in exactly

$$\mu - \frac{\mu}{g} = (g-1)\mu/g$$

columns that contain elements from G in both rows. $\square$

It is known that for every prime power p^e and every integer $d \geq 1$ there exists a $BGW(n, k, \mu)$ with parameters

$$n = \frac{p^{e(d+1)} - 1}{p^e - 1}, \quad k = p^{ed}, \quad \mu = p^{ed} - p^{e(d-1)} \quad (4)$$

over a group of order $p^e - 1$ being the multiplicative group of $\text{GF}(p^e)$, such that the related symmetric $2-(n, k, \mu)$ design is isomorphic to the design having as blocks the complements of hyperplanes in $\text{PG}(d, p^e)$ [6]. In addition, this $BGW(n, k, \mu)$ can be put in circulant form whenever $p^e - 1$ and $(p^{e(d+1)} - 1)/(p^e - 1)$ are relatively prime [5]. Thus, by Theorem 4.5, we obtain the following.

Theorem 4.6. *For every prime power p^e and every integer $d \geq 1$ such that $\gcd(p^e - 1, (p^{e(d+1)} - 1)/(p^e - 1)) = 1$, there exists a perfect DSS with parameters*

$$n = \frac{p^{e(d+1)} - 1}{p^e - 1}, \quad q = p^e - 1, \quad \rho = p^{e(d-1)}(p^e - 2).$$

Corollary 4.7. *The complement of a hyperplane in $\text{PG}(d, p^e)$ can be partitioned into blocks of a perfect DSS for every prime power p^e and $d \geq 1$ such that $\gcd(p^e - 1, (p^{e(d+1)} - 1)/(p^e - 1)) = 1$.*

Example 4.8. The 13×13 circulant with first row

1011122012100

is a balanced generalized weighing matrix $W = BGW(13, 9, 6)$ over the multiplicative group of $\text{GF}(3)$. The blocks

$$B_1 = \{0, 2, 3, 4, 8, 10\}, \quad B_2 = \{5, 6, 9\}$$

that correspond to the sets of indices of 1's and 2's in the first row of W yield a perfect DSS with $n = 13$, $q = 2$ and $\rho = 3$. The set of indices $\{1, 7, 11, 12\}$ not covered by B_1 and B_2 and its shifts modulo 13 are lines in $\text{PG}(2, 3)$.

Note 4.9. Balanced generalized weighing matrices with parameters (4) are obtainable also from difference sets of GMW type, as well as by some algebraic and combinatorial constructions described in [4,7].

Acknowledgment

The third author thanks the University of Tsukuba for the hospitality during his visit while this paper was initiated.

References

- [1] T. Beth, D. Jungnickel, H. Lenz, Design Theory, second ed., Cambridge Univ. Press, Cambridge, 1999.
- [2] P.J. Cameron, J.H. van Lint, Graph Theory, Coding Theory and Block Designs, Cambridge Univ. Press, Cambridge, 1975.
- [3] R. Fuji-Hara, M. Jimbo, S. Vanstone, Some results on the line partitioning problem in $\text{PG}(2k, q)$, Util. Math. 30 (1986) 235–241.

- [4] D. Jungnickel, V.D. Tonchev, Decompositions of difference sets, *J. Algebra* 217 (1999) 21–39.
- [5] D. Jungnickel, On automorphism groups of divisible designs, *Canad. J. Math.* 34 (1982) 257–297.
- [6] D. Jungnickel, V.D. Tonchev, Perfect codes and balanced generalized weighing matrices, *Finite Fields Appl.* 5 (1999) 294–300.
- [7] D. Jungnickel, V.D. Tonchev, Perfect codes and balanced generalized weighing matrices, II, *Finite Fields Appl.* 8 (2002) 155–165.
- [8] V.I. Levenshtein, One method of constructing quasi codes providing synchronization in the presence of errors, *Probl. Inf. Transm.* 7 (3) (1971) 215–222.
- [9] V.I. Levenshtein, Combinatorial problems motivated by comma-free codes, *J. Combin. Des.* 12 (2004) 184–196.
- [10] V.D. Tonchev, Difference systems of sets and code synchronization, *Rend. Sem. Mat. Messina, Ser. II* 9 (2003) 217–226.