Difference Systems of Sets and Cyclotomy

Yukiyasu Mutoh [a,1]

[a] *Graduate School of Information Science, Nagoya University, Nagoya, Aichi 464-8601, Japan, yukiyasu@jim.math.cm.is.nagoya-u.ac.jp*

Vladimir D. Tonchev [b,*,2]

[b] *Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan 49931, USA, tonchev@mtu.edu*

Abstract

Difference Systems of Sets (DSS) are combinatorial configurations that arise in connection with code synchronization. A method for the construction of DSS from partitions of cyclic difference sets was introduced in [6] and applied to cyclic difference sets $(n,(n-1)/2,(n-3)/4)$ of Paley type, where $n \equiv 3 \pmod 4$ is a prime number. This paper develops similar constructions for prime numbers $n \equiv 1 \pmod 4$ that use partitions of the set of quadratic residues, as well as more general cyclotomic classes.

Key words: difference set, cyclotomic class, code synchronization
1991 MSC: 05B, 94B

1 Introduction

A *Difference System of Sets* (DSS) with parameters $(n, \tau_0, \ldots, \tau_{q-1}, \rho)$ is a collection of q disjoint subsets $Q_i \subseteq \{1, 2, \ldots, n\}$, $|Q_i| = \tau_i$, $0 \le i \le q-1$, such that the multi-set

$$\{a - b \pmod n \mid a \in Q_i,\ b \in Q_j,\ 0 \le i, j < q,\ i \ne j\} \tag{1}$$

* Corresponding author
1 Research supported by JSPS Research Fellow 09978.
2 Research partially sponsored by NSF Grant CCR-0310832 and NSA Grant MDA904-03-1-0088.

contains every number $i,\ 1 \le i \le n-1$ at least ρ times. A DSS is *perfect* if every number $i,\ 1 \le i \le n-1$ is contained exactly ρ times in the multi-set (1). A DSS is *regular* if all subsets Q_i are of the same size: $\tau_0 = \tau_1 = \ldots = \tau_{q-1} = m$. We use the notation (n, m, q, ρ) for a regular DSS on n points with q subsets of size m.

Difference systems of sets were introduced by V. Levenshtein [4] (see also [5]) and were used for the construction of codes that allow for synchronization in the presence of errors. A q-ary code of length n is a subset of the set F_q^n of all vectors of length n over $F_q = \{0, 1, ..., q-1\}$. If q is a prime power, we often identify F_q with a finite field of order q, in which case i $(0 < i \le q-1)$ stands for the ith power of a primitive element. A *linear* q-ary code (q a prime power), is a linear subspace of F_q^n. If $x = x_1 \cdots x_n,\ y = y_1 \cdots y_n \in F_q^n$, and $0 \le i \le n-1$, the ith *joint* of x and y is defined as $T_i(x,y) = x_{i+1} \cdots x_n y_1 \cdots y_i$. In particular, $T_i(x,x)$ is a cyclic shift of x. 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 $i = 1, ..., n-1$, and d is the Hamming distance between vectors in F_q^n. The comma-free index $\rho(C)$ allows one to distinguish a code word from a joint of two code words (and hence provides for synchronization of code words) provided that at most $\lfloor \rho(C)/2 \rfloor$ errors have occurred in the given code word [3].

Since the zero vector belongs to any linear code, the comma-free index of a linear code is zero. Levenshtein [4] gave the following construction of comma-free codes of index $\rho > 0$ obtained as cosets of linear codes, that utilizes difference systems of sets. Given a DSS $\{Q_0, \ldots, Q_{q-1}\}$ with parameters $(n, \tau_0, \ldots, \tau_{q-1}, \rho)$, define a linear q-ary code $C \subseteq F_q^n$ of dimension $n - r$, where

$$r = \sum_{i=0}^{q-1} |Q_i|,$$

whose information positions are indexed by the numbers not contained in any of the sets $Q_0, \ldots, Q_{q-1}$, and having all redundancy symbols equal to zero. Replacing in each vector $x \in C$ the positions indexed by Q_i with the symbol i $(0 \le i \le q-1)$, yields a coset C' of C that has a comma-free index at least ρ.

This application of DSS to code synchronization requires that the number

$$r = r_q(n, \rho) = \sum_{j=0}^{q-1} |Q_i|$$

is as small as possible.

Levenshtein [4] proved the following lower bound on $r_q(n, \rho)$:

$$r_q(n, \rho) \geq \sqrt{\frac{q\rho(n-1)}{q-1}}, \tag{2}$$

with equality if and only if the DSS is perfect and regular.

In [6], Tonchev introduced a method for the construction of DSS from partitions of cyclic difference sets. This method was applied to the $(n, (n-1)/2, (n-3)/4)$ difference set of Paley (or quadratic residues) type, where n is any prime congruent to 3 modulo 4. In this paper, the method from [6] is extended to primes $n \equiv 1 \pmod 4$ by using partitions of the set of quadratic residues modulo n (Section 2), or partitions defined by more general cyclotomic classes (Section 3). Explicit constructions of infinite series of regular DSS are given for $2 \leq m \leq 6$ in Section 2. A general construction for arbitrary m based on cyclotomic classes is described in Section 3.

2 DSS and quadratic residues

Let $D = \{x_1, \ x_2, \ldots, x_k\}$ be a (v, k, λ) difference set (cf. [1], [2], [7]), that is, a subset of k residues modulo v such that every positive residue modulo v occurs exactly λ times in the multi-set of differences

$$\{x_i - x_j \pmod v \mid x_i, x_j \in D, \ x_i \neq x_j\}.$$

Then the collection of singletons $Q_0 = \{x_1\}, \ldots, Q_{k-1} = \{x_k\}$ is a perfect regular DSS with parameters $(n = v, m = 1, q = k, \rho = \lambda)$.

This simple construction was generalized in [6] by replacing the collection of singletons of a given cyclic difference set by any partition such that the parts are base blocks of a cyclic 2-design. More precisely, the following statement holds.

Lemma 1 *[6] Let $D \subseteq \{1, 2, \ldots, n\}$, $|D| = k$, be a cyclic (n, k, λ) difference set. Let D be partitioned into q disjoint subsets $Q_0, \ldots, Q_{q-1}$, and let Δ be the cyclic design having as a collection of blocks the union of orbits of the base blocks $Q_0, \ldots, Q_{q-1}$ under the cyclic group C_n. Assume that every two points are contained in at most λ_1 blocks of Δ. Then $\{Q_i\}_{i=0}^{q-1}$ is a DSS with parameters $(n, \tau_0, \ldots, \tau_{q-1}, \rho = \lambda - \lambda_1)$, where $\tau_i = |Q_i|$, $i = 0, \ldots, q-1$. The DSS $\{Q_i\}_{i=0}^{q-1}$ is perfect if and only if Δ is a pairwise balanced design with every two points occurring together in exactly λ_1 blocks.*

A class of new DSS were found in [6] from partitions of the $(n, (n-1)/2, (n-3)/4)$ cyclic difference set of quadratic-residue (QR) type, where $n = 4t + 3$ is prime. The partitions were defined by a subgroup of the multiplicative group Q of order $(n-1)/2$ consisting of all quadratic residues and its cosets in Q.

It is the aim of this section to present similar constructions for the case of prime numbers n of the form $n = 4t+1$. We use again partitions of the set Q of quadratic residues modulo n. The major difference between the cases $n = 4t+3$ or $n = 4t+1$ is that if $n \equiv 3 \pmod 4$ the set Q is a cyclic difference set (with $\lambda = (n-3)/4 = t$), while if $n \equiv 1 \pmod 4$ Q is a *relative* difference set: the multi-set of $2t(2t-1)$ differences

$$\{x - y \pmod n \mid x, y \in Q,\ x \neq y\}$$

contains every $z \in Q$ exactly $t-1$ times, and every $z \notin Q$ exactly t times. Equivalently, the cyclic 1-$(4t+1, 2t, 2t)$ design Q^* consisting of the cyclic shifts of Q modulo n is a partially balanced design such that any pair $x, y \in Z_n,\ x \neq y$ occurs in exactly $t-1$ blocks of Q^* whenever $x - y \in Q$, and in exactly t blocks if $x - y \notin Q$.

Assume that $|Q| = mq$ (thus, $n = 2mq+1$). We want to partition Q into q disjoint subsets of size m that will be the blocks of a regular DSS. Let α be a primitive element of the finite field of order n, $GF(n)$. Then

$$Q = \{\alpha^{2i} \mid 1 \leq i \leq (n-1)/2\}.$$

Let D_m be a subgroup of Q of order m,

$$D_m = \{\alpha^{2qi} \mid 1 \leq i \leq m\}.$$

Then Q is partitioned into q disjoint cosets of D_m:

$$Q = D_m \cup (D_m\alpha^2) \cup \ldots \cup (D_m\alpha^{2(q-1)}).$$

We consider the DSS having as blocks the following subsets of size m:

$$Q_0 = D_m, Q_1 = D_m\alpha^2, \ldots, Q_{q-1} = D_m\alpha^{2(q-1)}.$$

Let G be the group of transformations $\phi :\ GF(n) \longrightarrow GF(n)$, where

$$\phi(x) = a^2x + b \pmod n;\ a, b \in GF(n),\ a \neq 0.$$

The group G is of order $n(n-1)/2$ and contains the cyclic group Z_n and the multiplicative group Q as subgroups. The collection of (unordered) 2-subsets of Z_n is partitioned into two orbits under the action of G: one orbit consists of all pairs $\{x, y\}$ such that $x - y \in Q$, and the second orbit contains the pairs $\{x, y\}$ such that $x - y \notin Q$.

Note that D_m is a subgroup of Q of order m, Q acts regularly on itself, and n is prime. Thus, the stabilizer of D_m in G is of order m and the orbit D_m^G of

D_m under G consists of $|G|/m = nq$ subsets of size m. The collection $\Delta{=}D_m^G$ is a cyclic design with base blocks $Q_0, Q_1, \dots, Q_{q-1}$. Since the group G has two orbits on the 2-subsets of Z_n, Δ is a partially balanced design with two classes: each pair x, y such that $x - y \in Q$ occurs in λ_1 blocks of Δ (for some λ_1), while each pair x, y such that $x - y \notin Q$ occurs in λ_2 blocks (for some λ_2). It follows that the collection $\{Q_i\}_{i=0}^{q-1}$ is a DSS such that the multi-set of differences (1) contains every $z \in Q$ exactly $t - 1 - \lambda_1$ times, and every $z \notin Q$ exactly $t - \lambda_2$ times. Thus, we have the following.

Theorem 2 *The collection* $\{Q_i\}_{i=0}^{q-1}$ *is a DSS with parameters* (n, m, q, ρ), *where*

$$\rho = \min(t - 1 - \lambda_1, t - \lambda_2). \tag{3}$$

□

Let S_m be a subset of $GF(n)$ defined as follows:

$$S_m = \{\alpha^{2qi} - 1 \mid 1 \le i \le m - 1\},$$

where $m = (n - 1)/(2q)$. Then the multi-set of differences

$$\{x - y \pmod n \mid x, y \in D_m,\ x \neq y\}$$

coincides with the multi-set

$$\{s\alpha^{2qi} \pmod n \mid s \in S_m,\ 1 \le i \le m\}.$$

It follows that λ_1 is equal to the number of quadratic residues in S_m, while λ_2 is equal to the number of quadratic non-residues in S_m. Thus, the parameters λ_1 and λ_2 of Δ can be determined by counting the quadratic residues (resp. non-residues) in S_m. Therefore, we will often refer to λ_1, λ_2 as parameters of S_m.

Note that $\lambda_1 + \lambda_2 = m - 1$ and (3) imply the following lower bound on ρ in terms of m and q:

$$\rho \ge \frac{m(q-2)}{2}.$$

The next theorems utilize the construction of Theorem 2 for subgroups of relatively small order m. Applying this construction with a subgroup D_m of Q of order $m = 2$ yields the following result.

Theorem 3 *Let* $n = 4q+1$ *be a prime. The cosets of the subgroup* $Q_0 = \langle \alpha^{2q} \rangle$ *of order 2 in* Q

$$Q_0 = \{\alpha^{2q} = -1, \alpha^{4q} = 1\},\ Q_1 = \{\alpha^{2q+2}, \alpha^2\}, \dots,\ Q_{q-1} = \{\alpha^{4q-2}, \alpha^{2(q-1)}\} \tag{4}$$

form a regular DSS with parameters $(n, 2, q, \rho)$, where

$$\rho = \begin{cases} q-2 \text{ if } n \equiv 1 \pmod 8, \\ q-1 \text{ if } n \equiv 5 \pmod 8. \end{cases} \tag{5}$$

Proof. The difference of the two elements of $Q_0 = D_2 = \{\alpha^{2q} = -1, \alpha^{4q} = 1\}$ is ± 2 modulo n. Since $n \equiv 1 \pmod 4$, $-1 \in Q$. In addition, $2 \in Q$ by the QRL if $n \equiv \pm 1 \pmod 8$, and $2 \notin Q$ otherwise. Since $n = 4q+1$, then either $n \equiv 1 \pmod 8$ or $n \equiv 5 \pmod 8$. In the case when $n \equiv 1 \pmod 8$ the partially balanced cyclic design Δ with base blocks (4), i.e., D_2 and its cosets in Q, has parameters $\lambda_1 = 1,\ \lambda_2 = 0$, hence the corresponding DSS has parameter

$$\rho = \min\{(q-1)-1, q-0\} = q-2.$$

In the remaining case, $n \equiv 5 \pmod 8$, the parameters of Δ are $\lambda_1 = 0,\ \lambda_2 = 1$, and

$$\rho = \min\{(q-1)-0, q-1\} = q-1.$$

□

Note 1 The DSS of Theorem 3 in the case $n \equiv 5 \pmod 8$ is perfect, hence optimal with respect to the Levenshtein bound (2). If $n \equiv 1 \pmod 8$, we have a DSS with

$$r_q(n, \rho) = r_q(n, q-2) = (n-1)/2 = 2q,$$

and the right-hand side of the inequality (2) is

$$\sqrt{\frac{q(q-2)(4q)}{q-1}} = 2q\sqrt{\frac{q-2}{q-1}}.$$

Thus, this DSS is asymptotically optimal.

Example 4 (a) Let $n = 13$, $q = 3$. We use 2 as a primitive element of Z_{13}. The DSS with $\rho = 2$ from Theorem 3 is perfect and consists of the following three pairs Q_i:

$$\{1, 12\}, \{4, 9\}, \{3, 10\}.$$

(b) Let $n = 17$, $q = 4$. Now 3 is a primitive element of Z_{17}. The DSS from Theorem 3 has $\rho = 2$ and consists of the following four pairs Q_i:

$$\{1, 16\}, \{9, 8\}, \{13, 4\}, \{15, 2\}.$$

Next we apply this construction by using subgroups of Q of order $m = 3$, 4, 5 and 6.

Theorem 5 *Let $n = 6q+1$ be a prime, where q is an even integer. The cosets of the subgroup $Q_0 = \langle \alpha^{2q} \rangle$ of order 3 in Q*

$$Q_0 = \{\alpha^{2q}, \alpha^{4q}, \alpha^{6q} = 1\},\ Q_1 = \{\alpha^{2q+2}, \alpha^{4q+2}, \alpha^2\}, \ldots,\ Q_{q-1} = \{\alpha^{4q-2}, \alpha^{6q-2}, \alpha^{2q-2}\}$$

form a regular DSS with parameters $(n, 3, q, \rho)$, where

$$\rho = \begin{cases} 3q/2 - 3 \text{ if } (-3)^{(n-1)/4} \equiv 1 \pmod{n}, \\ 3q/2 - 2 \text{ if } (-3)^{(n-1)/4} \not\equiv 1 \pmod{n}. \end{cases} \tag{6}$$

Proof. Let $\varepsilon = \alpha^{(n-1)/3}$ be a primitive cubic root of unity in $GF(n)$. Then $(\varepsilon - 1)^2 = -3\varepsilon$. Since ε is a fourth power, -3 is a square, and $(-3)^{(n-1)/4} \equiv 1,$ or $-1 \pmod{n}$. In addition, $\varepsilon - 1$ belongs to Q if $(-3)^{(n-1)/4} \equiv 1 \pmod{n}$. Similarly, $\varepsilon^2 - 1$ belongs to Q if $\varepsilon - 1$ belongs to Q. It follows that $S_3 = \{\varepsilon - 1,\ \varepsilon^2 - 1\}$. In the case when $(-3)^{(n-1)/4} \equiv 1 \pmod{n}$, the parameters of the cyclic design Δ are $\lambda_1 = 2,\ \lambda_2 = 0$, hence by (3)

$$\rho = \min\{(3q/2 - 1) - 2, 3q/2 - 0\} = 3q/2 - 3.$$

In the remaining case, $(-3)^{(n-1)/4} \not\equiv 1 \pmod{n}$, the parameters of S_3 are $\lambda_1 = 0,\ \lambda_2 = 2$, and

$$\rho = \min\{(3q/2 - 1) - 0, 3q/2 - 2\} = 3q/2 - 2.$$

□

Example 6 (a) Let $n = 13,\ q = 2$. We use 2 as a primitive element of Z_{13}. Then $(-3)^3 \not\equiv 1 \pmod{13}$. Thus the DSS from Theorem 5 has $\rho = 1$, and the two blocks are the cyclic group $Q_0 = \{1, 3, 9\} = \langle 3 = 2^4 \rangle \simeq C_3$ and $Q_1 = 4Q_0 = \{4, 12, 10\}$.
(b) Let $n = 37,\ q = 6$. We use 2 as a primitive element of Z_{37}. Then $(-3)^9 \equiv 1 \pmod{37}$. Thus the DSS from Theorem 5 has $\rho = 6$, and the six blocks Q_i are

$$\{1, 26, 10\}, \{4, 30, 3\}, \{16, 9, 12\}, \{27, 36, 11\}, \{34, 33, 7\}, \{25, 21, 28\}.$$

Note that Q_0 is a cyclic subgroup of Q of order 3 and the remaining blocks are the cosets of Q_0 in Q.

Theorem 7 *Let $n = 8q+1$ be a prime. The cosets of the subgroup $Q_0 = \langle \alpha^{2q} \rangle$ of order 4 in Q*

$$\begin{aligned} Q_0 &= \{\alpha^{2q}, \alpha^{4q}, \alpha^{6q}, \alpha^{8q} = 1\}, \\ Q_1 &= \{\alpha^{2q+2}, \alpha^{4q+2}, \alpha^{6q+2}, \alpha^2\}, \\ &\vdots \\ Q_{q-1} &= \{\alpha^{4q-2}, \alpha^{6q-2}, \alpha^{8q-2}, \alpha^{2q-2}\} \end{aligned}$$

form a regular DSS with parameters $(n, 4, q, \rho)$*, where*

$$\rho = \begin{cases} 2q-4 \text{ if } q \text{ is even and 2 is a biquadratic of } n, \text{ or} \\ \qquad\qquad q \text{ is odd and 2 is a non-biquadratic of } n, \\ 2q-2 \text{ if } q \text{ is even and 2 is a non-biquadratic of } n, \text{ or} \\ \qquad\qquad q \text{ is odd and 2 is a biquadratic of } n. \end{cases} \tag{7}$$

Proof. Let $i = \alpha^{(n-1)/4}$ be a primitive quartic root of unity in $GF(n)$. Then $(i-1)^2 = -2i$ and $S_4 = \{i-1,\ -2,\ -i-1\}$ holds. Since $n-1 \equiv 0 \pmod 8$, -1 is a fourth power. Note that i is a fourth power if q is even. Otherwise, i is not a fourth power but a square. Thus, $i-1$ is a square if q is even and 2 is a biquadratic of n, or if q is odd and 2 is a non-biquadratic of n. In the first case, S_4 has parameters $\lambda_1 = 3,\ \lambda_2 = 0$, hence the corresponding DSS has parameter

$$\rho = \min\{(2q-1)-3, 2q-0\} = 2q-4.$$

In the remaining case, the parameters of S_4 are $\lambda_1 = 1,\ \lambda_2 = 2$, and

$$\rho = \min\{(2q-1)-1, 2q-2\} = 2q-2.$$

□

Note 2 The DSS of Theorem 7 is perfect in the case when q is even and 2 is a non-biquadratic of n, and when q is odd and 2 is a biquadratic of n.

Example 8 (a) Let $n = 17$, $q = 2$. We use 3 as a primitive element of Z_{17}. We have $2 \equiv 3^2 \pmod{17}$ and 2 is not a biquadratic of 17. Thus the DSS with $\rho = 2$ from Theorem 7 is perfect, and the two blocks Q_i are

$$\{1, 13, 16, 4\}, \{9, 15, 8, 2\}.$$

(b) Let $n = 73$, $q = 9$. Now 5 is a primitive element of Z_{73} and 2 is a biquadratic of 73. Thus the DSS with $\rho = 16$ from Theorem 7 is perfect, and the nine blocks Q_i are

$$\{1, 27, 72, 46\}, \{25, 18, 48, 55\}, \{41, 12, 32, 61\}, \{3, 8, 70, 65\}, \{2, 54, 71, 19\},$$
$$\{50, 36, 23, 37\}, \{9, 24, 64, 49\}, \{6, 16, 67, 57\}, \{4, 35, 69, 38\}.$$

(c) Let $n = 41$, $q = 5$. Now 6 is a primitive element of Z_{41}, and 2 is not a biquadratic of 41. Thus the DSS from Theorem 7 has $\rho = 6$, and the five blocks Q_i are

$$\{1, 32, 40, 9\}, \{36, 4, 5, 37\}, \{25, 21, 16, 20\}, \{39, 18, 2, 23\}, \{10, 33, 31, 8\}.$$

(d) Let $n = 113$, $q = 14$. Now 3 is a primitive element of Z_{13}, and 2 is a biquadratic of 113. Thus the DSS from Theorem 7 has $\rho = 24$, and the 14 blocks Q_i are

$$\{1, 98, 112, 15\}, \{9, 91, 104, 22\}, \{81, 28, 32, 85\}, \{51, 26, 62, 87\}, \{7, 8, 106, 105\},$$
$$\{63, 72, 50, 41\}, \{2, 83, 111, 30\}, \{18, 69, 95, 44\}, \{49, 56, 64, 57\}, \{102, 52, 11, 61\},$$
$$\{14, 16, 99, 97\}, \{13, 31, 100, 82\}, \{4, 53, 109, 60\}, \{36, 25, 77, 88\}.$$

Theorem 9 *Let $n = 10q + 1$ be a prime, where q is an even integer. The cosets of the subgroup $Q_0 = \langle \alpha^{2q} \rangle$ of order 5 in Q*

$$\begin{aligned}
Q_0 &= \{\alpha^{2q}, \alpha^{4q}, \alpha^{6q}, \alpha^{8q}, \alpha^{10q} = 1\},\\
Q_1 &= \{\alpha^{2q+2}, \alpha^{4q+2}, \alpha^{6q+2}, \alpha^{8q+2}, \alpha^{2}\},\\
&\vdots\\
Q_{q-1} &= \{\alpha^{4q-2}, \alpha^{6q-2}, \alpha^{8q-2}, \alpha^{10q-2}, \alpha^{2q-2}\}
\end{aligned}$$

form a regular DSS with parameters $(n, 5, q, \rho)$, where

$$\rho = 5q/2 - 3 \quad \text{if } 5^{(n-1)/4} \not\equiv 1 \pmod{n}. \tag{8}$$

Proof. Let $\varepsilon = \alpha^{(n-1)/5}$ be a primitive fifth root of unity in $GF(n)$. For $x \in GF(n)$, we have

$$x^4 + x^3 + x^2 + x + 1 = (x - \varepsilon)(x - \varepsilon^2)(x - \varepsilon^3)(x - \varepsilon^4) :$$

hence for $x = 1$

$$5 = (1 - \varepsilon)(1 - \varepsilon^2)(1 - \varepsilon^3)(1 - \varepsilon^4) = \varepsilon^2(\varepsilon - 1)^2(\varepsilon^2 - 1)^2. \tag{9}$$

Thus 5 is a square, and $5^{(n-1)/4} \equiv 1$, or $-1 \pmod{n}$. By (9) we see that 5 is a fourth power if $\varepsilon + 1$ is a square, since ε is a square. By (8) 5 is not a fourth power, that is, $\varepsilon + 1$ does not belong to Q. Thus either $\varepsilon - 1$ or $\varepsilon^2 - 1$ is a square, and $S_5 = \{\varepsilon - 1,\ \varepsilon^2 - 1,\ \varepsilon^3 - 1,\ \varepsilon^4 - 1\}$ holds. In the case when $5^{(n-1)/4} \not\equiv 1 \pmod{n}$, S_5 has parameters $\lambda_1 = 2,\ \lambda_2 = 2$, hence the corresponding DSS has parameter

$$\rho = \min\{(5q/2 - 1) - 2, 5q/2 - 2\} = 5q/2 - 3.$$

□

Example 10 Let $n = 41$, $q = 4$. We use 6 as a primitive element of Z_{41}. Then $5^{10} \not\equiv 1 \pmod{41}$. Thus the DSS from Theorem 9 has $\rho = 7$, and the four blocks Q_i are

$$\{1, 10, 18, 16, 37\}, \{36, 32, 33, 2, 20\}, \{25, 4, 40, 31, 23\}, \{39, 21, 5, 9, 8\}.$$

Note 3 If $n \equiv 1 \pmod{20}$ (resp. (mod12)) is a prime, then there is exactly one pair $(x, y) \in N \times N$ such that $n = x^2 + 4y^2$. Then 5(resp. -3) is a square in $GF(n)$, by the quadratic reciprocity law. In addition, 5 is a fourth power if and only if $y \equiv 0 \pmod 5$ and -3 is a fourth power if $y \equiv 0 \pmod 3$. Hence the value of ρ depends on whether the diophantine equation $x^2 + 36y^2 = n$ has solution in integers and (8) holds if the diophantine equation $x^2 + 100y^2 = n$ has no solution in integers. Similarly, it is known that 2 is a biquadratic of n if the diophantine equation $x^2 + 64y^2 = n$ has solution in integers.

Note 4 In the case $m = 5$, either $S_5 \subset Q$ or $S_5 \cap Q = \emptyset$ if $5^{(n-1)/4} \equiv 1 \pmod n$. In the case when $S_5 \subset Q$, i.e., $\varepsilon - 1$ is a quadratic of n, S_5 has parameters $\lambda_1 = 4$, $\lambda_2 = 0$, hence the corresponding DSS has parameter $\rho = 5q/2 - 5$. In the remaining case, i.e., $\varepsilon - 1$ is a non-quadratic of n, $S_5 \cap Q = \emptyset$, the parameters of S_5 are $\lambda_1 = 0$, $\lambda_2 = 4$, and $\rho = 5q/2 - 4$.

Example 11 Let $n = 101$, $q = 10$. We use 2 as a primitive element of Z_{101}. Then $5^{25} \equiv 1 \pmod{101}$ and $\varepsilon - 1 = 94 \equiv 2^{59} \pmod{101}$, where $\varepsilon = 95$ is a primitive fifth root of unity of Z_{101}. Thus the DSS from Note 4 has $\rho = 21$, and the ten blocks Q_i are

$$\{1, 95, 36, 87, 84\}, \{4, 77, 43, 45, 33\}, \{16, 5, 71, 79, 31\}, \{64, 20, 82, 13, 23\}, \{54, 80, 25, 52, 92\},$$
$$\{14, 17, 100, 6, 65\}, \{56, 68, 97, 24, 58\}, \{22, 70, 85, 96, 30\}, \{88, 78, 37, 81, 19\}, \{49, 9, 47, 21, 76\}.$$

Let $n = 461$, $q = 46$. We use 2 as a primitive element of Z_{461}. Then $5^{115} \equiv 1 \pmod{461}$ and $\varepsilon - 1 = 87 \equiv 2^{218} \pmod{461}$, where $\varepsilon = 88$ is a primitive fifth root of unity of Z_{461}. Thus the DSS from Note 4 has $\rho = 110$.

Theorem 12 *Let $n = 12q + 1$ be a prime. The cosets of the subgroup $Q_0 = \langle \alpha^{2q} \rangle$ of order 6 in Q*

$$\begin{aligned}
Q_0 &= \{\alpha^{2q}, \alpha^{4q}, \ldots, \alpha^{12q} = 1\}, \\
Q_1 &= \{\alpha^{2q+2}, \alpha^{4q+2}, \ldots, \alpha^{2}\}, \\
&\vdots \\
Q_{q-1} &= \{\alpha^{4q-2}, \alpha^{6q-2}, \ldots, \alpha^{2q-2}\}
\end{aligned}$$

form a regular DSS with parameters $(n, 6, q, \rho)$, *where*

$$\rho = \begin{cases} 3q-6 \text{ if } q \text{ is even and } (-3)^{(n-1)/4} \equiv 1 \pmod{n}, \\ 3q-5 \text{ if } q \text{ is odd and } (-3)^{(n-1)/4} \equiv 1 \pmod{n}, \\ 3q-4 \text{ if } q \text{ is even and } (-3)^{(n-1)/4} \not\equiv 1 \pmod{n}, \\ 3q-3 \text{ if } q \text{ is odd and } (-3)^{(n-1)/4} \not\equiv 1 \pmod{n}. \end{cases} \tag{10}$$

Proof. Let $\varepsilon = \alpha^{(n-1)/6}$ be a primitive 6th root of unity in $GF(n)$. Then $(\varepsilon-1)^2(\varepsilon^2-1)^2 = (\varepsilon-1)^4(\varepsilon+1)^2 = -3$ since $\varepsilon^2-\varepsilon+1 = 0$. Thus -3 is a square by the QRL, and $(-3)^{(n-1)/4} \equiv 1, \text{ or } -1 \pmod{n}$. In addition, $\varepsilon+1$ belongs to Q if $(-3)^{(n-1)/4} \equiv 1 \pmod{n}$. Thus if $(-3)^{(n-1)/4} \not\equiv 1 \pmod{n}$ then either $\varepsilon-1$ or ε^2-1 is a square. In the other case, if $(-3)^{(n-1)/4} \equiv 1 \pmod{n}$ then $\varepsilon-1$ and ε^2-1 are both squares since $(\varepsilon-1)^2 = -\varepsilon = \alpha^{8q}$. Thus $S_6 = \{\varepsilon-1,\ \varepsilon^2-1,\ \varepsilon^3-1,\ \varepsilon^4-1, \varepsilon^5-1\}$ holds and $\varepsilon^3-1 = -2$.

Since $n \equiv 1 \pmod{4}$, $-1 \in Q$. In addition, $2 \in Q$ if $n \equiv \pm 1 \pmod{8}$, and $2 \notin Q$ otherwise. Since $n = 4q+1$, then either $n \equiv 1 \pmod{8}$ or $n \equiv 5 \pmod{8}$. In the case when q is even and $(-3)^{(n-1)/4} \equiv 1 \pmod{n}$. Thus, S_6 has parameters $\lambda_1 = 5,\ \lambda_2 = 0$, and the corresponding DSS has parameter

$$\rho = \min\{(3q-1)-5, 3q-0\} = 3q-6.$$

In the second case when q is odd and $(-3)^{(n-1)/4} \equiv 1 \pmod{n}$, S_6 has parameters $\lambda_1 = 4,\ \lambda_2 = 1$, hence the corresponding DSS has parameter

$$\rho = \min\{(3q-1)-4, 3q-1\} = 3q-5.$$

In the third case when q is even and $(-3)^{(n-1)/4} \not\equiv 1 \pmod{n}$, S_6 has parameters $\lambda_1 = 3,\ \lambda_2 = 2$, hence the corresponding DSS has parameter

$$\rho = \min\{(3q-1)-3, 3q-2\} = 3q-4.$$

In the fourth case when q is odd and $(-3)^{(n-1)/4} \not\equiv 1 \pmod{n}$, S_6 has parameters $\lambda_1 = 2,\ \lambda_2 = 3$, hence the corresponding DSS has parameter

$$\rho = \min\{(3q-1)-2, 3q-3\} = 3q-3,$$

which is perfect. $\square$

Example 13 (a) Let $n = 37,\ q = 3$. Now 2 is a primitive element of Z_{37}, and $(-3)^9 = 1 \pmod{37}$. Thus the DSS from Theorem 12 has $\rho = 4$, and the three blocks Q_i are

$$\{1, 27, 26, 36, 10, 11\}, \{4, 34, 30, 33, 3, 7\}, \{16, 25, 9, 21, 12, 28\}.$$

(b) Let $n = 73$, $q = 6$. Now 5 is a primitive element of Z_{73}, and $(-3)^{18} = -1 \pmod{73}$. Thus the DSS from Theorem 12 has $\rho = 14$, and the three blocks Q_i are

$$\{1, 9, 8, 72, 64, 65\}, \{25, 6, 54, 48, 67, 19\}, \{41, 4, 36, 32, 69, 37\},$$
$$\{3, 27, 24, 70, 46, 49\}, \{2, 18, 16, 71, 55, 57\}, \{50, 12, 35, 23, 61, 38\}.$$

(c) Let $n = 109$, $q = 9$. 6 is a primitive element of Z_{109}. Then $(-3)^{27} = -1 \pmod{109}$. Thus the DSS with $\rho = 24$ from Theorem 12 is perfect, and the nine sets Q_i are

$$\{1, 64, 63, 108, 45, 46\}, \{36, 15, 88, 73, 94, 21\}, \{97, 104, 7, 12, 5, 102\},$$
$$\{4, 38, 34, 105, 71, 75\}, \{35, 60, 25, 74, 49, 84\}, \{61, 89, 28, 48, 20, 81\},$$
$$\{16, 43, 27, 93, 66, 82\}, \{31, 22, 100, 78, 87, 9\}, \{26, 29, 3, 83, 80, 106\}.$$

(d) Let $n = 193$, $q = 16$. Now 5 is a primitive element of Z_{193}, and $(-3)^{48} = 1 \pmod{193}$. Thus the DSS from Theorem 12 has $\rho = 42$.

3 DSS and cyclotomic numbers

For an integer e, let n be an odd prime such that $e|(n-1)$, and let α be a primitive element in $GF(n)$. Then the eth *cyclotomic classes* C_0^e, C_1^e, …, C_{e-1}^e are defined by

$$C_i^e = \{\alpha^t \,|\, t \equiv i \pmod{e}\} \quad \text{for} \quad 0 \leq i \leq e-1.$$

In other words, C_i^e are cosets of the subgroup C_0^e of eth powers in $GF(n)^*$. We calculate the subscripts of C_i^e modulo e, so that if $x \in C_i^e$ and $y \in C_j^e$, then $xy \in C_{i+j}^e$. We note that $-1 \in C_0^e$ if and only if $2e|(n-1)$, since $-1 = \alpha^{(n-1)/2}$ is an eth power if and only if $(n-1)/2 \equiv 0 \pmod{e}$. For a given n and e, the *cyclotomic numbers* (of order e) are defined as follows:

$$(i, j)_e = |\{(x, y) \mid x \in C_i^e,\ y \in C_j^e,\ x = y - 1\}|.$$

These numbers are important for the construction of difference sets in the additive group G of $GF(n)$ by taking suitable unions of cyclotomic classes. Details are given in [1]. We pick up the most important special case to construct DSS later on, where one uses just the cyclotomic class C_0^e.

Lemma 14 *[1]. For positive integers e and f, let $n = ef+1$ be a prime power. Then $D = C_0^e$ is a difference set in G (with parameters $(n, f, (f-1)/e)$) if and only if e is even, f is odd and $(i, 0)_e = (f-1)/e$ for $0 \leq i \leq e-1$.*

In this section we generalize some of the constructions from Section 2 by using more general cyclotomic cosets instead of the set of quadratic residues Q. For this purpose, we will use partitions of the set $D = C_0^e$. (Note that $D = Q$ for $e = 2$). Throughout this section, we assume that n is a prime. Note that for any prime $n = ef + 1$ D is a relative difference set: the multi-set of $f(f-1)$ differences

$$\{x - y \pmod{n} \mid x, y \in D,\ x \neq y\} = \{c(\alpha^t - 1) \mid c \in C_0^e,\ 1 \leq t < f\}$$

contains every $z \in C_i^e$ exactly $(i, 0)_e$ times for each i. Equivalently, the cyclic 1-(n, f, f) design D^* consisting of the cyclic shifts of D modulo n is a partially balanced design such that any pair $x, y \in Z_n,\ x \neq y$ occurs in exactly $(i, 0)_e$ blocks of D^* whenever $x - y \in C_i^e$. We note that if e is even and f is odd then -1 does not belong to C_0^e but C_ℓ^e, where $\ell = (n-1)/2$. Then $(i, j)_e = (j + \ell, i + \ell)_e$. Thus $(i, 0)_e = (i + \ell, 0)_e$ since $(i, j)_e = (-i, j - i)_e$.

Assume that $|D| = mq$ (thus, $n = emq + 1$). We want to partition D into q disjoint subsets of size m that will be the blocks of a regular DSS. Let D_m be a subgroup of C_0^e of order m,

$$D_m = C_0^{eq} = \{\alpha^{eqt} \mid 0 \leq t < e\}.$$

Then D is partitioned into q disjoint cosets of D_m:

$$D = D_m \cup (D_m \alpha^e) \cup \ldots \cup (D_m \alpha^{e(q-1)}) = C_0^{eq} \cup C_e^{eq} \cup \ldots \cup C_{e(q-1)}^{eq}.$$

We consider the DSS with q blocks of size m

$$Q_0 = D_m, Q_1 = D_m \alpha^e, \ldots, Q_{q-1} = D_m \alpha^{(q-1)e}.$$

Let G be the group of transformations $\phi :\ GF(n) \longrightarrow GF(n)$ of the form

$$\phi(x) = cx + b \pmod{n};\ c \in C_0^e,\ b \in GF(n).$$

The group G is of order $n(n-1)/e$ and contains the cyclic group Z_n and the multiplicative group D as subgroups. The group G partitions the 2-subsets of Z_n into e orbits: each orbit consists of all pairs $\{x, y\}$ such that $x - y \in C_i^e$ for $0 \leq i < e$.

The orbit D_m^G of D_m under G consists of $|G|/m = nq$ subsets of size m. The collection $\Delta = D_m^G$ is a cyclic design with base blocks $Q_0, Q_1, \ldots, Q_{q-1}$. Since the group G has q orbits on the 2-subsets of Z_n, Δ is a partially balanced design with q classes: each pair x, y such that $x - y \in C_i^e$ occurs in λ_i blocks of Δ (for some λ_i) for $0 \leq i < e$.

Let S_m be the subset of $GF(n)$ defined as follows.

$$S_m = \{\alpha^{eqi} - 1 \mid 1 \leq i \leq m - 1\}.$$

Then the multi-set of differences

$$\{x - y \pmod n \mid x, y \in D_m,\ x \neq y\}$$

equals

$$\{s\alpha^{eqi} \pmod n \mid s \in S_m,\ 0 \leq i < m\}.$$

Thus each λ_i depends on S_m and $(h,0)_{eq}$ is the number of s such that $s \in C_h^{eq}$. In addition, we have

$$C_i^e = C^e q_i \cup C^e q_{i+e} \cup C^e q_{i+2e} \cup \ldots \cup C^e q_{i+(q-1)e},$$

thus

$$\lambda_i = \sum_{j=0}^{q-1} (i + je, 0)_{eq}.$$

It follows that the collection $\{Q_i\}_{i=0}^{q-1}$ is a DSS such that the multi-set of differences (1) contains every $z \in C_i^e$ exactly $(i,0)_e - \sum_{j=0}^{q-1}(i+je,0)_{eq}$ times for $0 \leq i < e$.

Thus, we have the following theorem.

Theorem 15 *For positive integers e, m and q, let $n = emq + 1$ be a prime. The sets*

$$Q_0 = C_0^{eq},\ Q_1 = C_e^{eq},\ Q_2 = C_{2e}^{eq}, \ldots,\ Q_{q-1} = C_{(q-1)e}^{eq}$$

form a regular DSS with parameters (n, m, q, ρ), where

$$\rho = \min\{(i,0)_e - \sum_{j=0}^{q-1} (i + je, 0)_{eq} \mid 0 \leq i < e\}.$$

In particular, if $(i,0)_e - \sum_{j=0}^{q-1}(i+je,0)_{eq}$ is constant for each i, then the DSS is perfect, where $\rho = m(q-1)/e$.

Example 16 (a) Let $n = 73$, $e = 3$, $q = 2$, $m = 12$. We use 5 as a primitive element of Z_{73}. Then

$$(0,0)_3 = 8,\ (1,0)_3 = 6,\ (2,0)_3 = 9,$$
$$(0,0)_6 = 2,\ (1,0)_6 = 2,\ (2,0)_6 = 3,$$
$$(3,0)_6 = 2,\ (4,0)_6 = 2,\ (5,0)_6 = 0.$$

Thus the DSS from Theorem 15 has $\rho = 2$, and the blocks Q_i of size 12 are

$$\{1, 3, 9, 27, 8, 24, 72, 70, 64, 46, 65, 49\}, \{52, 10, 30, 17, 51, 7, 21, 63, 43, 56, 22, 66\}.$$

(b) Let $n = 109$, $e = 3$, $q = 2$, $m = 18$. We use 6 as a primitive element. Then the DSS with $\rho = 6$ is perfect since

$$(0,0)_3 = 11,\ (1,0)_3 = 10,\ (2,0)_3 = 14,$$
$$(0,0)_6 = 2,\quad (1,0)_6 = 0,\quad (2,0)_6 = 2,$$
$$(3,0)_6 = 3,\quad (4,0)_6 = 4,\quad (5,0)_6 = 6.$$

Example 17 (a) Let $n = 73$, $e = 4$, $q = 3$, $m = 6$. We use 5 as a primitive element of Z_{73}. Then

$$\begin{array}{llll} (0,0)_4 = 5, & (1,0)_4 = 6, & (2,0)_4 = 4, & (3,0)_4 = 2 \\ (0,0)_{12} = 2, & (1,0)_{12} = 0, & (2,0)_{12} = 0, & (3,0)_{12} = 0 \\ (4,0)_{12} = 0, & (5,0)_{12} = 0, & (6,0)_{12} = 0, & (7,0)_{12} = 0 \\ (8,0)_{12} = 1, & (9,0)_{12} = 2, & (10,0)_{12} = 0, & (11,0)_{12} = 0. \end{array}$$

Thus the DSS from Theorem 15 has $\rho = 2$, and its blocks Q_i of size 6 are

$$\{1, 9, 8, 72, 64, 65\}, \{41, 4, 36, 32, 69, 37\}, \{2, 18, 16, 71, 55, 57\}.$$

(b) Let $n = 769$, $e = 4$, $q = 3$, $m = 64$. We use 11 as a primitive element. Then the DSS with $\rho = 32$ is perfect since

$$\begin{array}{llll} (0,0)_4 = 38, & (1,0)_4 = 48, & (2,0)_4 = 51, & (3,0)_4 = 54 \\ (0,0)_{12} = 0, & (1,0)_{12} = 6, & (2,0)_{12} = 9, & (3,0)_{12} = 6 \\ (4,0)_{12} = 4, & (5,0)_{12} = 4, & (6,0)_{12} = 6, & (7,0)_{12} = 10 \\ (8,0)_{12} = 2, & (9,0)_{12} = 6, & (10,0)_{12} = 4, & (11,0)_{12} = 6. \end{array}$$

Acknowledgment. The first author would like to thank Michigan Technological University for the hospitality during his visit in June and July 2004 while this paper was being written.

References

[1] T. Beth, D. Jungnickel, H. Lenz, "Design Theory", Second Edition, Cambridge University Press, Cambridge 1999.

[2] C. J. Colbourn and J. F. Dinitz, eds., "The CRC Handbook of Combinatorial Designs", CRC Press, Boca Raton, 1996.

[3] S.W. Golomb, B. Gordon, L.R. Welch, “Comma-free codes”, *Canad. J. Math.*, vol. 10, no. 2, pp. 202–209, 1958.

[4] V. I. Levenshtein, One method of constructing quasi codes providing synchronization in the presence of errors, Problems of Information Transmission, vol. 7, No. 3 (1971), 215-222.

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

[6] V. D. Tonchev, Difference systems of sets and code synchronization, *Rendiconti del Seminario Matematico di Messina*, to appear.

[7] V. D. Tonchev, “Combinatorial Configurations”, Wiley, New York 1988.