Partitions of difference sets and code synchronization

Vladimir D. Tonchev
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931
USA
www.math.mtu.edu/∼tonchev

***Abstract*— Difference systems of sets can be used to transform an arbitrary linear code to a coset of a linear code with a given comma-free index by means of a minimal increase of its length. The paper discusses some constructions of difference systems of sets obtained from cyclic difference sets and finite geometry.**

Key Words: code synchronization, difference set, difference system of sets.

I. 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

$$\{a - b \pmod n \mid a \in Q_i,\ b \in Q_j,\ i \neq j\} \qquad (1)$$

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 of differences (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 [6] 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 [5].

Since the zero vector belongs to any linear code, the comma-free index of a linear code is zero. Levenshtein [6] 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 redundancy

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

is as small as possible.

Levenshtein [6] proved the following lower bound on $r_q(n, \rho)$:

Theorem 1.1:

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

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

In [6], Levenshtein found optimal DSS for $q = 2$ and $\rho = 1$ or $\rho = 2$, and proved that for all $n \ge 2$

$$r_2(n, 1) = \rceil \sqrt{2(n-1)} \lceil,\ r_2(n, 2) = \rceil 2\sqrt{n-1} \lceil.$$

Similar results are not known for $q \ge 3$.

In a recent paper Levenshtein [7] introduced some constructions of imperfect regular DSS obtained as products of cyclic difference sets. In particular, he proved that the existence of a cyclic (v, q, ρ) difference set with $2 \le q < v$ implies the existence of an DSS with parameters $(n = v^h, m, q, \rho)$ for every $h \ge 2$. A corollary of this result is that for any prime power t and any integer h there exists a regular DSS with $n=(t^2+t+1)^h$, $m=\frac{(t+1)^h-1}{t}$, $q=t+1$, and $\rho=1$.

In this paper we describe some direct constructions of perfect and regular, hence optimal difference systems of sets obtained as partitions of cyclic difference sets.

II. DSS AS PARTITIONS OF DIFFERENCE SETS

Let $D=\{x_1,\ x_2,\ldots,x_k\}$ be a (v,k,λ) difference set (cf. [1], [2], [9]), 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 $(n=v, m=1, q=k, \rho=\lambda)$. Thus, DSS are a generalization of cyclic difference sets. The next lemma generalizes this simple construction by using more general partitions of difference sets.

Lemma 2.1: Let $D\subseteq\{1,2,\ldots,n\}$, $|D|=k$, be a cyclic (n,k,λ) difference set. Assume that D is partitioned into q disjoint subsets $Q_0,\ldots,Q_{q-1}$ that are the base blocks of a cyclic design $\mathcal{D}$ with block sizes $\tau_i=|Q_i|$, $i=0,\ldots,q-1$ such that every two points are contained in at most λ_1 blocks. Then the sets $Q_0,\ldots,Q_{q-1}$ form a DSS with parameters $(n,\tau_0,\ldots,\tau_{q-1},\rho=\lambda-\lambda_1)$. The DSS $\{Q_i\}_{i=0}^{q-1}$ is perfect if and only if $\mathcal{D}$ is a pairwise balanced design with every two points occurring together in exactly λ_1 blocks.

The following theorem gives infinitely many perfect and regular DSS obtained by partitioning the trivial cyclic $(n,n-1,n-2)$ difference set $D=\{1,2,\ldots,n-1\}$, where n is an arbitrary prime number.

Theorem 2.2: Let $n=mq+1$ be a prime, and let α be a primitive element of the finite field of order n, $GF(n)$. The collection of sets

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

is a perfect regular $(n,m,q,\rho=n-m-1)$ DSS.

The DSS described in Theorem 2.2 has redundancy $r_q(n,\rho)=n-1$. However, the following example suggests that it is sometimes possible to obtain a DSS with a smaller value of $r_q(n,\rho)$ being a sub-collection of the DSS described in Theorem 2.2.

Example 2.3: Let $n=19,\ q=6, m=3$. The DSS from Theorem 2.2 has $\rho=15$, and the six sets Q_i of size 3 are

$$\{1,7,11\},\{2,14,3\},\{4,9,6\},\{5,16,17\},\{8,18,12\},\{10,13,15\}.$$

The two sets $\{1,7,11\},\ \{2,14,3\}$ form a perfect DSS with $q=2$, $\rho=1$, and $r=6$.

It is an interesting open problem to find an infinite class of such examples.

The following theorem gives perfect regular DSS's obtained as partitions of difference sets of quadratic-residue (QR) type.

Theorem 2.4: For every prime $n=2mq+1\equiv 3 \pmod 4$ there exists a perfect regular DSS with parameters $(n,m,q,\rho=(n-2m-1)/4)$.

Example 2.5: Let $n=31=2\cdot 5\cdot 3+1$. We take $m=5$, $q=3$, and $\alpha=3$ as a primitive element modulo 31. The set D_5 defined as in Theorem 2.4 for $m=5$ consists of the elements

$$3^6\equiv 16,\ 3^{12}\equiv 8,\ 3^{18}\equiv 4,\ 3^{24}\equiv 2,\ 3^{30}\equiv 1.$$

The sets

$$Q_0=D_5=\{16,8,4,2,1\}, Q_1=D_5 3^2=\{20,10,5,18,9\}, Q_2=D_5 3^4 =$$

are base blocks of a cyclic 2-$(31,5,2)$ design, and their union $Q_0\cup Q_1\cup Q_2$ is the set of all nonzero quadratic residues modulo 31. Consequently, the collection $Q_0,\ Q_1,\ Q_2$ is a perfect regular DSS with parameters $n=31,\ m=5,\ q=3,\ \rho=5$.

III. DIFFERENCE SYSTEMS OF SETS FROM FINITE GEOMETRY

Perfect DSS with reasonably small redundancy $r_q(n,\rho)$ can be obtained from difference sets related to finite geometry.

Let H be a hyperplane in the $2s$-dimensional projective space $PG(2s,p)$ over $GF(p)$. The $(p^{2s}-1)/(p-1)$ points of H form a cyclic difference set with parameters

$$v=\frac{p^{2s+1}-1}{p-1},\ k=\frac{p^{2s}-1}{p-1},\ \lambda=\frac{p^{2s-1}-1}{p-1}$$

in a cyclic group acting regularly on the points of $PG(2s,p)$, known in design theory and geometry as the Singer difference set. It is known [4] that the points of H can be partitioned into disjoint lines $Q_0,\ Q_1,\ldots,\ Q_{q-1}$, where

$$q=\frac{p^{2s}-1}{p^2-1}=p^{2s-2}+\ldots+p^2+1.$$

On the other hand, the collection of all lines in $PG(2s,p)$ is a cyclic 2-$(\frac{p^{2s+1}-1}{p-1},p+1,1)$ design $\mathcal{D}$. If the partition

$$H=Q_0\cup Q_1\cup\ldots\cup Q_{q-1}$$

is chosen so that $Q_0,\ \ldots,\ Q_{q-1}$ are base blocks of $\mathcal{D}$, then by Lemma 2.1 the collection $Q_0,\ Q_1,\ldots,\ Q_{q-1}$ is a perfect regular DSS with parameters

$$n=\frac{p^{2s+1}-1}{p-1},\ m=p+1,\ q=\frac{p^{2s}-1}{p^2-1},\ \rho=\frac{p^{2s-1}-p}{p-1}.$$

Hyperplane partitions with the above property were studied by Fuji-Hara, Jimbo and Vanstone in a different context in [3], who showed that such partitions exist in $PG(2s,2)$ for $s\leq 5$, and in $PG(2s,3)$ for $s\leq 3$.

Example 3.1: Let $p=2,\ s=2$. We consider $1,\alpha,\alpha^2,\ldots,\alpha^{30}$ as points of $PG(4,2)$, where α is a primitive element of $GF(2^5)$ defined by the polynomial x^5+x^3+1. The following set of 15 points

$$H=\{\alpha,\alpha^2,\alpha^4,\alpha^8,\alpha^{16},\alpha^3,\alpha^6,\alpha^{12},\alpha^{24},\alpha^{17},\alpha^{29},\alpha^{27},\alpha^{23},\alpha^{15},\alpha^{30}\}$$

is a hyperplane in $PG(4,2)$, and hence a $(31,15,7)$ difference set in the multiplicative group of $GF(2^5)$. The following partition of H,

$$H=\{\alpha,\alpha^3,\alpha^{29}\}\cup\{\alpha^2,\alpha^6,\alpha^{27}\}\cup\{\alpha^4,\alpha^{12},\alpha^{23}\}\cup\{\alpha^8,\alpha^{24},\alpha^{15}\}\cup\{\alpha^{16},$$

has the property that each of the five 3-subsets is a projective line, and these five lines are the base blocks of a cyclic 2-$(31, 3, 1)$ design under the multiplicative group of $GF(2^5)$. Thus, these five 3-subsets define a perfect DSS with parameters $(n = 31, m = 3, q = 5, \rho = 6)$.

IV. Acknowledgment

Research supported by NSF grant CCR-0310632.

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] R. Fuji-Hara, M. Jimbo, and S. Vanstone, Some results on the line partitioning problem in $PG(2k, q)$, *Utilitas Math.* **30** (1986), 235-241.
[4] J.W.P. Hirschfeld, "Projective Geometries over Finite Fields", Oxford University Press, Oxford, 1979.
[5] S.W. Golomb, B. Gordon, L.R. Welch, "Comma-free codes", *Canad. J. Math.*, vol. 10, no. 2, pp. 202–209, 1958.
[6] V. I. Levenshtein, One method of constructing quasilinear codes providing synchronization in the presence of errors, Problems of Information Transmission, vol. 7, No. 3 (1971), 215-222.
[7] V. I. Levenshtein, Combinatorial problems motivated by comma-free codes, *J. Combin. Designs*, **12** (2004), 184-196.
[8] V. I. Levenshtein and V.D. Tonchev, Constructions of difference systems of sets, in: "Algebraic and and Combinatorial Coding Theory", Eight International Workshop Proc., St. Petersburg, Russia, Sept. 2002, pp. 194-197.
[9] V. D. Tonchev, "Combinatorial Configurations", Wiley, New York 1988.