A PRINCIPAL DIFFERENCE SYSTEM AND ARITHMETIC PROGRESSIONS

Larry Cummings
University of Waterloo, Canada
ljcummings@math.uwaterloo.ca

Abstract

A difference systems of sets (DSS) is a collection of subsets of Z_n, the integers mod n, with the property that each non-zero element of Z_n appears at least once as the difference of elements from different sets. If there is just one set it is called a principal DSS. DSS arise naturally in the study of systematic synchronizable codes and are studied mostly over finite fields when n is a prime power. Using only triangular numbers mod n we constructed a DSS over Z_n for each positive integer $n > 3$. Necessary and sufficient conditions are given for the existence of a principal DSS using only triangular numbers in terms of coverings of $\{1, \ldots, n-1\}$ by finite arithmetic progressions.

1 Introduction

Finite difference systems of sets (DSS) have applications in synchronizable coding. The general case was introduced by Levenshtein in 1971 to construct systematic comma-free codes as cosets of linear codes with minimal redundancy in the presence of errors [10]. D. J. Clague [1] had previously studied the case for two sets in 1967.

Definition 1 *A* difference systems of sets (DSS) *is a collection of $q < n$ disjoint subsets $Q_i \subset Z_n$ such that the equation*

$$m \equiv a - b \pmod{n} \tag{1}$$

has at least one solution in integers a, b from Z_n for each $m = 1, \ldots n-1$ where $a \in Q_i, b \in Q_j, i \neq j$.

A DSS is *perfect* with index ρ if every m appears as a difference of elements from different sets exactly ρ times. A DSS is *regular* if all sets are the same size. The *redundancy*, r, of a DSS is the number of elements used; i.e., $|\cup_{i=0}^{q-1} Q_i|$. A single subset Q_0 with the property that all non-zero elements of Z_n can be written as differences of elements from Q_0 is called a *principal DSS*, or if no confusion is possible,

Any DSS, $\cup_{i=0}^{q-1} Q_i$ is itself a principal difference set in Z_n. A (v, k, λ) cyclic difference set, D, is a subset of k elements of Z_n such that every non-zero element of Z_n can be written in exactly λ different ways as a difference $a - b$ of elements in D. If $Q_0, \dots, Q_{q-1}$ is a DSS then $\cup Q_i$ is a difference set, but not necessarily a (v, k, λ) difference set as examples show [2]. As well the same reference gives an example of a DSS that is neither regular or perfect but $\cup Q_i - \{0\}$ is a $(11, 5, 2)$ perfect difference set. DSS are often constructed by clever partitioning of known (v, k, λ) difference sets where the set elements are from finite fields. Accordingly, one can view the study of DSS as a special case of the more general study of difference sets, but the properties of regularity and perfection which are usually assumed in the study of (v, k, λ) difference sets are not necessarily assumed when we consider difference sets generally. The case when the underlying difference set is a (v, k, λ) difference set has been studied extensively by a number of authors [5, 6, 4, 12, 13].

2 Using Triangular Numbers

The well-known triangular numbers are positive integers that may be defined in several different ways. Perhaps the most common is:

$$T_n = 1 + 2 + \cdots + n = \binom{n+1}{2},$$

where $n > 0$. For notational convenience we take zero as a triangular number and define $T_0 = 0$. An equivalent recursive definition which is useful for our purposes is

$$T_i = T_{i-1} + i, \qquad i > 0.$$

We illustrate the use of triangular numbers by constructing a principal DSS in the following theorem.

Theorem 1 *If* $n > 3$ *Then there exists a principal DSS in* Z_n *with redundancy* $\lfloor \frac{n}{2} \rfloor$.

Proof: If n is odd let $n = 2k + 1, n > 0$. We claim the following differences of triangular numbers and their negatives

$$1 = T_1 - T_0, \ldots, \quad k = T_k - T_{k-1}, -1 = T_0 - T_1, \ldots, -k = T_{k-1} - T_k$$

taken mod n lists all integers $1, \ldots, n-1$ mod n. Clearly, $1, \ldots, k$ are distinct mod n and therefore so are $-1 \equiv n-1, \ldots, -k \equiv n-k$. If i from the first of the list represents the same class as $-j$ in the second half of the list then $i + j \equiv 0$ mod n. Z_n is an additive Abelian group and the inverse mapping is injective. Therefore, there are $2k$ non-zero integers in the list as required since $n = 2k+1$. Further note that $n - k = k + 1$ since $n = 2k + 1$.

If n is even let $n = 2k, k > 0$. Then the above list of differences still yields all integers $1, \ldots, n-1$ mod n but in this case $n-1$ is odd and there is one duplication: $k = T_k - T_{k-1}$ and $-k = T_{k-1} - T_k$ are representatives of the same class since $n = 2k$.

The following difference matrix of consisting of the first three triangular numbers is a perfect principal DSS with index 2 that covers $\{1, 2, 3\}$ over Z_4:

$$\begin{matrix} 0 & 3 & 1 \\ 1 & 0 & 2 \\ 3 & 2 & 0 \end{matrix}$$

and illustrates the even case of Theorem 1. The matrix repeats each non-zero class exactly twice and therefore has index 2 over Z_4.

3 Coverings by Arithmetic Progressions

An arithmetic progression (AP) is a sequence of integers in which the difference of successive terms is constant. Studying the difference matrix determined by a collection of disjoint sets $Q_0, \ldots, Q_{q-1}$ of Z_n can help determine whether they form a DSS.

It what follows we say that an integer a in Z *covers* a class mod n represented by an integer b if $b \equiv a$ mod n. Further, a set of integers $A \subset Z$ cover a set of classes B in Z_n if for each b in some class of B there exists $a \in A$ such that $a \equiv b$ mod n.

Theorem 2 *Let $n > 3$ and $r = \lfloor \frac{n}{2} \rfloor$. The set of the first $r+1$ triangular numbers $\{T_0, \cdots, T_r\}$ determine a principal DDS in Z_n if and only if the $2(r-1)$ integers (not necessarily distinct) appearing in the arithmetical progressions determined by $\pm(T_i + ki)$, $0 \leq k \leq r - i$, cover $\{1, \ldots n-1\}$ in Z_n.*

Proof: Let $D = D(r)$ denote the $(r+1) \times (r+1)$ integer difference matrix determined by the ordered set of the first $r+1$ triangular numbers starting with $T_0 = 0$:

$$\begin{array}{c|cccccc}
- & T_0 & T_1 & \cdots & T_j & \cdots & T_r \\
\hline
T_0 & 0 & \cdots & \cdots & -\frac{j(j+1)}{2} & \cdots & -\frac{r(r+1)}{2} \\
T_1 & 1 & 0 & \cdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
T_i & \frac{i(i+1)}{2} & \vdots & \vdots & \frac{(i-j)(i+j+1)}{2} & \vdots & \vdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
T_r & \frac{r(r+1)}{2} & \cdots & \frac{(r-1)(2r-i+1)}{2} & \vdots & \vdots & 0
\end{array}$$

where it is assumed for notational convenience that $i < j$. The general term follows easily from the definition of triangular numbers and is easily adjusted if $i > j$. D is a skew-symmetric integer matrix with a main diagonal of all 0's.

If $0 < i \leq r$ let D_i denote the set of $r - i + 1$ subdiagonal entries:

$$T_i, T_{i+1} - T_1, \ldots, T_r - T_{r-i}.$$

Referring to the above difference matrix, D_i is illustrated and is seen to be the integer sequence

$$\frac{i(i+1)}{2}, \ldots, \frac{(r-1)(2r-i+1)}{2}.$$

Clearly D_1 is the sequence $1, 2, \ldots, r$ and D_r is the single number T_r. If these integers are taken as representatives of classes in Z_n then, by an abuse of notation, we can write $D_{-i} = -D_i = \{n-1, \ldots, n-r\}$.

We claim that D_i is an AP because the difference of any two successive terms in D_i is constant:

$$(T_{i+k} - T_k) - (T_{i+k-1}) = (i + k) - k = i, \qquad 0 \leq k \leq r - i + 1.$$

It follows immediately that D_{-i} is also an AP. Therefore, each non-zero difference in D must appear in at least one of the $\pm D_i$. Thus, if the set of the first $r + 1$ triangular numbers $\{T_0, \cdots, T_r\}$ is a principal DDS in Z_n then, by definition, the integers $\{1, \ldots n - 1\}$ are covered by the integer sets $D_i \cup -D_i$, $0 < i \leq r$.

Conversely, if the $r(r-1)$ non-zero integers in $\bigcup_1^r (D_i \cup -D_i)$ cover $\{1, \ldots n - 1\}$ then each distinct non-zero class in Z_n is a difference of elements of the set of the first $r + 1$ triangular numbers $\{T_0, \cdots, T_r\}$.

In 1990 Heath [7] proved that covering a finite set in Z with AP's is NP-complete but that doesn't preclude exact solutions in particular cases. Any extension of Theorem 2 to more than one set must take account of the structure of the partitions determined by the sets of triangular numbers. An open question is determining whether any DSS using triangular numbers with more than one set can have minimal redundancy.

References

[1] D. J. Clague, *New classes of synchronous codes*, IEEE Trans. on Electronic Computers **EC-16**(1967), 290–298.

[2] Larry Cummings, *Triangular numbers and difference systems of sets*, Congr. Numer. 196 (2009), 215–220.

[3] L.J. Cummings, *A family of systematic circular comma-free codes*, Journal of Combinatorial Mathematics and Combinatorial Computing, **58**(2006), 87–96.

[4] Cunsheng Ding, *Optimal and perfect difference systems of sets*, J. Combin. Theory Ser. A , **116**(2009), no. 1, 109–119.

[5] R. Fuji-Hara, K. Momihara, and M. Yamada, *Perfect difference systems of sets and Jacobi sums*, Discrete Mathematics (in press).

[6] R. Fuji-Hara, A. Munemasa, and V. D. Tonchev, *Hyperplane partitions and difference systems of sets*, J. Combin. Theory Ser. A, **113**(2006), no. 8, 1689–1698.

[7] Lenwood S. Heath, *Covering a set with arithmetic progression is NP-complete*, Information Processing Letters, **34**(1990), 293–298.

[8] V. I. Levenshtein, *Combinatorial problems motivated by comma-free codes*, Journal of Combinatorial Designs, **12**(2004), 184–196.

[9] V. I. Levenshtein, *Bounds for codes ensuring error correction and synchroniation*, Translation from: Problemy Peredachi Informatsii, **5**(1969), 3–13.

[10] V. I. Levenshtein, *One method of constructing quasilinear codes providing synchronization in the presence of errors*, Translation from: Problemy Peredachi Informatsii, **7**(1971), 30–40.

[11] V.I. Levenshtein and V.D. Tonchev, Constructions of difference systems of sets, in "Algebraic and Combinatorial Coding Theory", Eight International Workship Proc., St. Petersburg, Russia, Sept. 2002, pp. 194–197.

[12] V. D. Tonchev, *Difference systems of sets and code synchronization*, Rendiconti del Seminario Mathematico di Messina, Series II, **9**(2003), 217–226.

[13] V. D. Tonchev, *Partitions of difference systems of sets and code synchronization*, Finite Fields and their Applications, **11**(2005), 601–621.

[14] V.D. Tonchev and Y.Mutoh, *Difference systems of sets and cyclotomy* Discrete Math. 308 (2008), no. 14, 2959–2969.

[15] Hao Wang, *A new bound for difference systems of sets*, Journal of Combinatorial Mathematics and Combinatorial Computing, 58(2006), 161–168.