On the Existence of Triangular Difference Systems of Sets

Larry Cummings

Abstract

A difference system of sets (DSS) is any collection of subsets of Z_n with the property that the differences from distinct sets cover Z_n. That is, every non-zero class in Z_n can be written as a difference of classes in at least one way. DSS were introduced by Levenstein in 1971 only for finite fields but the case for just 2 subsets had been previously considered by Clauge. Their work emphasized an application to synchronizable codes. A DSS is triangular if its sets contain only triangular numbers mod n. We show that a triangular DSS cannot exist in Z_{2^k} for $k > 3$.

1 Introduction

The integers mod n will be denoted by Z_n. A difference systems of sets (DSS) is a collection of q subsets of Z_n with the property that each non-zero element of Z_n appears at least once as the difference of elements from different sets. More formally,

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

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

has at least one integer solution pair a, b for each $m = 1, \ldots n-1$ where $[a]_n \in Q_i, [b]_n \in Q_j, i \neq j,$ and $i, j = 0, \ldots q-1$.

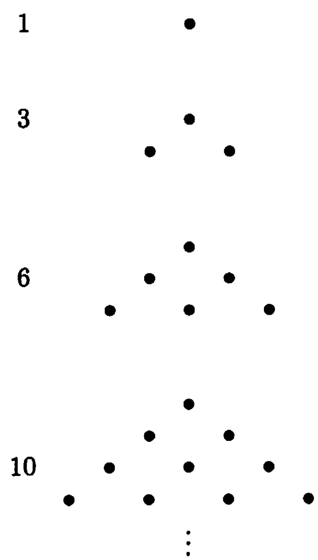
A DSS is said to be principal *if $q = 1$. The* trivial *DSS are the set of singletons $[0]_n, \ldots, [n-1]_n$ and the single set $\{[0]_n, \ldots, [n-1]_n\}$ in Z_n.*

JCMCC **90** (2014), pp. 139-143

This general definition was introduced by Levenstein over finite fields in a study of synchronizable and error-correcting codes published in 1971 [7]. The case for two sets was considered earlier by Clague in 1967 [1]. Difference systems of sets have been extensively studied over finite fields in design theory but with the added conditions of regularity and pefection that are not assumed here. Most constructions of general DSS have proceeded by partitioning known (v, k, λ) difference sets over finite fields; e.g., [4, 9]. Hao Wang [10] has compiled a list of smaller cases over finite fields. Motivation for studying general DSS came from research in synchronizable coding where a set Q_i contains the indices of positions of the ith 'check digit' in codewords of length n. The problem of constructing general DSS has been shown to be equivalent with that of covering $\{1, \ldots n-1\}$ with certain arithmetical progressions [2].

2 Triangular Numbers

In this paper we continue to explore the existence of DSS in for arbitrary $n > 1$ and chose elements of Z_n by considering the well-known triangular numbers, mod n. The triangular numbers are beloved by recreational mathematicians because of the many identities they satisfy. The first four are illustrated geometrically below:



In this paper we include 0 for notational convenence so the ordered list $\{T_0, T_1, \dots, T_i \dots\}$ of triangular numbers begins:

$$0, 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, \cdots.$$

We use the following equivalent formal definitions of the triangular numbers:

$$\textbf{Definition 1}: \quad \mathrm{T}_i = T_{i-1} + i \qquad\qquad i > 0.$$

$$\textbf{Definition 2}: \quad \mathrm{T}_i = 1 + 2 + \cdots + i = \binom{i+1}{2}.$$

Note that if $j < i$, $T_i - T_j = (j+1) + \cdots + i$ is a sum of consecutive positive integers. From Definition 2 the triangular numbers are seen to be a 'diagonal' of Pascal's triangle. Gauss first proved that every positive integer can be written as the sum of at most 3 triangular numbers [5]. For more background and generalizations we recommend the recent book [3].

3 Principal DSS

Since a principal DSS has only one set, the formal differences are not limited by any partition because of the condition $a \in Q_i, b \in Q_j, i \neq j$ in Definition 1, increasing the likelihood of representing all non-zero classes. This is seen immediately by simply observing there are always fewer entries available in the corresponding partitioned difference matrix.

The following theorem gives a sufficient condition for the existence of a non-trivial principal DSS.

Theorem 1 *If $n > 3$ is odd (even) and $T_{\frac{n-1}{2}} < n$ $\ (T_{\frac{n}{2}} < n)$ then there exists a principal triangular DSS in Z_n.*

Theorem 1 is stated and proved in [2] with a slightly stronger hypothesis. The weaker hypothesis here does not affect the proof. The proof of theorem is constructive and exhibits the required differences by using the subdiagonals immediately above and below the all zero main diagonal of the formal difference matrix of the ordered set of triangular numbers, since these contain the successive differences, $\pm(T_{i+1} - T_i)$. As mentioned above, it is shown in [2] that the existence of principal DSS is equivalent to the problem of covering $\{[0]_n, \dots, [n-1]_n\} \subset Z_n$ by classes of certain finite arithmetic progressions given in Theorem 2 below.

Theorem 2 *For every $n > 3$, if $r = \lfloor \frac{n}{2} \rfloor$ then the set $\{T_0, \cdots, T_r\}$ determines a principal DDS in Z_n if and only if the $2(r-1)$ classes of integers appearing in the arithmetic progressions*

$$\pm(T_i + ki),\ 0 \leq k \leq r - i$$

cover

$$\{[0]_n, \ldots, [n-1]_n\} \subset Z_n.$$

It is known that the general problem of covering sets with arithmetic progressions is NP-complete [6].

4 Powers of 2

The following lemma has been rediscovered many times and there are a number of elementary proofs in the literature. In 1912 Mason [8], writing in the American Mathematical Monthly, attributes the first proof to Lucas.

Lemma 1 *All positive integers except powers of 2 are sums of at least two consecutive integers.*

The following theorem asserts that for any choice of $Q_0, \ldots Q_{q-1}$ there cannot exist a triangular DSS when the modulus n is a power of 2 greater than 3.

Theorem 3 *If $k > 3$ there do not exist triangular DSS in Z_{2^k}, for $k > 3$.*

Proof By contradiction. Assume a triangular DSS $Q_0, \ldots, Q_{q-1}$ exists in Z_n where $n = 2^k$ and $k > 3$. Set $r = max\{i \mid T_i < n\}$ and, if necessary, permute the rows and columns of the integer difference matrix of the DSS to D_r, the integer difference table of the ordered set $T_0, \ldots, T_r$. $[D_r]_n$ denotes the latter difference table mod n.

Claim: $[2^{k-1}]_n$ does not appear in $[D_r]_n$.

Proof of Claim: If it did then by definition some non-zero integer $a \in [2^{k-1}]_n$ appears in D_r. Therefore, $a = 2^k t + 2^{k-1}$, for some integer t by the Euclidean algorithm. It follows that $2^{k-1} | a$. Write $a = 2^{k-1}s$ for some integer s. But $|a| < n = 2^k$ since a is a difference of triangular numbers all less than n (see the definition of r). Therefore $2^{k-1}|s| < 2^k$, or $|s| < 2$, So $s = 0$ or ± 1. In the first case, $s = 0$ implies $a = 0$, a contradiction, since $a \in [2^{k-1}]_n$ which contains only non-zero integers. If $s = 1$ then $a = 2^{k-1}$ must be a positive difference of triangular numbers $T_i - T_j, i > j$, contradicting lemma 1 . If If $s = -1$ then $a = -2^{k-1}$ must be a difference of triangular numbers $T_i - T_j$ with $i < j$. But then $-a = 2^{k-1} = T_j - T_i$ where $j > i$, again contradicting the lemma. Since $[2^{k-1}]_n$ does not appear in $[D_r]_n$, it cannot appear in the difference matrix of any DSS with the same parameters using the same set of triangular numbers because one matrix is similar to the other by a permutation matrix.

References

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

[2] L. J. Cummings, *A principal difference system and arithmetic progressions*, The Journal of Combinatorial Mathematics and Combinatorial Computing, **80**(2012), 193–198.

[3] E. Deza and M. M. Deza, *Figurate Numbers* World Scientific, Singapore, 2012.

[4] 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.

[5] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801.

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

[7] 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.

[8] T. E. Mason, *On the representation of an integer as the sum of consecutive integers*, American Mathematical Monthly **19**(1912),

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

[10] H. Wang, *A new bound for difference systems of sets*, The Journal of Combinatorial Mathematics and Combinatorial Computing, **58**(2006), 161-168.