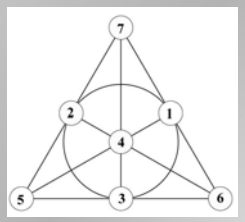
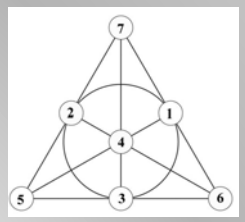


New LS[3][2, 3, 2^8] Geometric Large Sets

Michael Hurley, Balkumar Khadka, Spyros Magliveras

For more information, contact:

Department of Mathematics, Florida Atlantic University



Background

Let V be an n-dimensional vector space over the field of q elements. Given parameters t and k where $t < k \leq n$, W is called a **t-subspace** of V if W is a subspace of V of dimension t. A simple **geometric $t-[q^n, k, \lambda]$ design** is a pair (V,H), where H is a collection of k-subspaces of V, called blocks, such that any t-subspace of V is contained in exactly λ blocks.

If H is the collection of all k-subspaces in V, then (V,H) is a **trivial geometric design**, but partitioning this trivial design into disjoint $t-[q^n, k, \lambda]$ designs creates a resolution known as a **large set**. A large set of V, denoted by $LS[N][t, k, q^n]$, is a collection of N geometric $t-[q^n, k, \lambda]$ designs whose union is the collection of all k-subspaces of V.

Braun, Kohnert, Östergård, and Wassermann discovered the first large set of geometric 2-designs using $2-[2^8, 3, 21]$ designs over the finite field F_2. Earlier large sets of geometric designs existed for $t=1$, called **spreads** in finite geometry. Using the same procedures as the authors above, we found a number of new large sets over F_2 with the same parameters.

Group Actions

A **group action** is a function from $X \times G$ to X for a set X and a group G such that the identity element of the group G fixes every element of the set X, and products of group elements act on X by composition. The **G-orbit** of an element $x \in X$ is the set of elements in X that x can be mapped to by the group action and any of the $g \in G$. A group action is **transitive** if X consists of a single G-orbit, and is **t-homogeneous** if the induced action of G on the set of t-subsets of X is transitive.

Here, by an **t-orbit** we mean an orbit of G in its induced action on the t-subspaces of V. A group G is said to be an **automorphism group** of a large set $LS[N][t, k, q^n]$ L, if the elements of G preserve L as a whole, that is, if they permute the designs of L. If G is an automorphism group of a large set L we also say that L is **G-invariant**. If every $g \in G$ fixes each design of L, the large set is called **$[G]$-invariant**.

The Kramer-Mesner Matrices

Using a group action on the sets of t-subspaces and k-subspaces allows us to create a matrix $A_{t,k}$, known as the **Kramer-Mesner** matrix, that is the result of fusing the incidences between the t-subspaces and k-subspaces of V, creating an **incidence matrix** between the t-orbits and k-orbits of G acting on V. In principle, from $A_{t,k}$ one can find t-designs and large sets of designs, although the problem is in general **computationally intractable**.

Kramer and Mesner proved in 1976 that given parameters t, v, k, λ, there exists a $t-(v, k, \lambda)$ design invariant under G if and only if there is a collection of columns of $A_{t,k}$ that add up to the column vector λJ, where J is the all 1's column vector. Their theorem extends to geometric designs. There is also an extension theorem by S.M. and Charles Cusack that provides conditions for the existence of a large set of $t-[q^n, k, \lambda]$ designs.

Constructing the Orbits

Since the elements of our vector space V are 8-dimensional binary vectors, we can represent them by positive integers $\{0,1,\ldots,255\}$, with respect to base 2. The 10795 2-subspaces and 97155 3-subspaces are represented and indexed in lexicographic order by their minimal bases as 2-subsets, or 3-subsets of integers, respectively. The group G that was used to construct the orbits over these subspaces is a cyclic subgroup of **$GL(8,2)$**, the general linear group of dimension 8 over F_2. That is, $G = < X >$, where X is a matrix with columns (64,32,16,8,4,2,1,184) respectively. As a matrix over F_2, X is the following:

$$\begin{bmatrix} 0&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&1 \\ 0&0&1&0&0&0&0&1 \\ 0&0&0&1&0&0&0&1 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

This matrix has order 255. By allowing our group action of G on V to be left multiplication, we see that there are 43 orbits of 2-subspaces, 42 of orbit length 255, and a single orbit of length 85. On the other hand, there are 381 orbits of 3-subspaces all of length 255, and because a 3-subspace is an elementary abelian group of order 8, by removing 0 a 3-subspace can be identified with a **Fano-plane**. We call the 381 orbits **Fano-plane orbits**. Our resulting incidence matrix was over these orbits, though a single subspace can represent an entire orbit.

The Basis Matrix

Finding a large set now becomes a matter of finding a partition of the columns of the Kramer-Mesner matrix with 3 parts such that each part has row sum of 21. Determining the existence of a partition, and possibly finding more than one solution is a multidimensional knapsack problem and is considered computationally intractable, particularly in such high dimensions. There is a procedure for solving this problem called **Lattice Basis Reduction** which we employ here. Adjoining the Kramer-Mesner matrix (A) below an identity matrix, as well as a column of 0's and the negative of the intended row sums creates M, a **Basis Matrix:**

$$M = \begin{bmatrix} I & 0 \\ A & -21J \end{bmatrix}$$

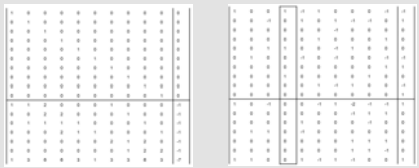
This basis matrix of 424 rows and 382 columns is a basis for an integral lattice Λ.

Weight Reduction

Restructuring M through column reduction can determine a linear combination of columns of M that have a required row sum. Reducing the weight of the columns is done by means of an algorithm known as L^3 which involves repeated applications integral Gram-Schmidt orthogonalization process and column permutations.

Basis Matrix Reduction Example:

Before **After**



Finding a Partition

After basis reduction, the matrix is then scanned to see if any column consists of 0's and 1's (or 0's and -1's) and this indicates the existence of design corresponding to non-zero entries of the column. If a design is found it is removed from the columns of $A_{t,k}$ and we proceed to look for another design in the remaining columns. The basis matrix is scanned for columns with two properties:

1. Row 1 to 381 consists of 0's and 1's (or -1's). This indicates that no column was combined with another column more than once.

2. Row 382 to 424 consists of 0's only. This indicates that there exists a linear combination of columns that adds up to a multiple of 21.

The **indices of the 1's** indicate the columns of the incidence matrix that have a row sum of a multiple of 21. The columns indicate the Fano-plane orbits to use as blocks in our designs of the large set, and after repeating the process on the remaining columns, we get a large set. There is not a guarantee that a column meeting the two above conditions will exist after basis reduction. If no column meets the two conditions, the process is repeated.

Before repeating, we reorder the columns of the basis matrix in one of three ways:

1. Smallest weight to largest weight

2. Alternating from first column to last column from left to right

3. Alternating from smallest weight to largest weight from left to right.

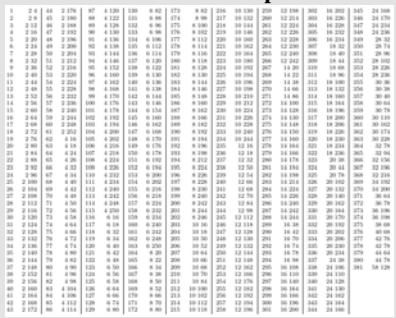
Each procedure required a different algorithm, each yielded a design from the basis matrix given. Using a branching pattern and switch algorithms after finding the first design resulted in 9 different large sets. Large sets shared designs between them, but were not necessarily equivalent or even isomorphic.

Results

Recreating the 43 by 381 $A_{t,k}$ matrix here is not possible. Instead we list the means to recreate the Fano-plane orbits and the solutions indicating which designs the orbits belong to in each large set solution.

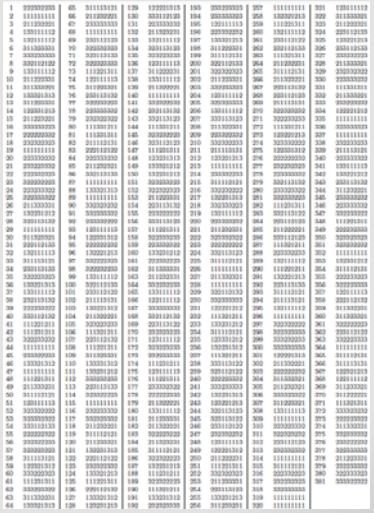
The designated Fano Plane orbit representatives all contain the vector 1, thus they are listed in lexicographic order in terms of the remaining two other vectors in the Fano Plane linearly independent to 1.

The Fano Plane Orbit Representatives



The solutions are denoted by assigning the 381 Fano-plane orbits a length 9 vector that indicates which of the three designs of equal parameter that orbit belonged to for the 9 different large sets. Certain Fano-plane orbits always appear together in the same designs regardless of the large set. The deterministic nature of the basis reduction algorithm is conjectured to be the reason for this.

The Large Sets



Observations

Different Fano-plane orbits had different incidence structure with respect to the 43 orbits on 2-subspaces. Some were incident with 2-subspace orbits no more than once, some were incident with certain 2-subspace orbits 3 times. Automorphisms that would map the Fano-plane orbits to each other would preserve the incidence structure of these orbits on 2-subspaces. Thus, an automorphism that maps one large set to another can only exist if both large sets have equivalent incidence structure. Only two pairs of large sets found in this study had equivalent incidence structure: #2 and #9, and #6 and #8. These large sets can potentially be isomorphic to each other, but the remaining large sets cannot be isomorphic.

Further Study

Large sets that are isomorphic to the large sets found in this study can be created using known automorphisms in $GL(8,2)$, one of which is the **Frobenius Automorphsim**, which permutes the vectors by the binary basis mapping (216, 54, 181, 113, 64, 16, 4, 1). Under matrix multiplication this mapping can be expressed by the binary matrix seen here.

$$\begin{bmatrix} 1&0&1&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0 \\ 0&1&1&1&0&0&0&0 \\ 1&1&1&1&0&1&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&1&1&0&0&0&1&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&1&0&0&0&1 \end{bmatrix}$$

This order 8 automorphism maps each of our large sets to 8 other isomorphic large sets. Finding other automorphisms that can preserve the incidence structures of the large sets can lead to other large sets and broaden the understanding of the automorphism group of $GL(8,2)$.

Finding large sets in higher dimensions over different finite fields is being done using basis reduction and other computational means. This procedure has found $2-[2^8, 4, 105]$ designs, and is trying to determine the existence of large sets of $2-[2^8, 4, \lambda]$ designs.

Further study in t-designs and large sets can be applied to means of creating **error-correction** in networks.

Each large set found in this study was found anywhere within a span of 8 hours and 5 days. The geometric $2-[2^8, 4, 105]$ designs were each found after a month of basis reduction.

Linear programming and more efficient APL programming that can find large sets and designs within a manageable error can improve the efficiency of finding large sets.

References

- Marshall Hall Jr., *Combinatorial Theory*, 2nd Ed., Wiley-Interscience, 1986
- Reinhard Laue, Spyros Magliveras, Alfred Wassermann, *New Large Sets of t-Designs*, John Wiley and Sons Inc., 2000
- Michael Kiermaier, Reinhard Laue, *Dervied and Residual Subspace Designs*, Mathematics Subject Classification, 2010
- Michael Braun, Axel Kohnert, Patric Östergård, and Alfred Wassermann, *Large Sets of t-Designs over Finite Fields*, math.CO, 2013
- D.L. Kreher and S.P. Radziszowski. *Finding Simple t-Designs by Using Basis Reduction*, Congressus Numerantium 55, 1986
- D.L. Kreher and S.P. Radziszowski. *Solving Subset-Sum Problems with the L^3 Algorithm*. Journal of Combinatorial Mathematics and Combinatorial Computing, 3, 1988
- R. Koetter and F. Kschischang. *Coding for Errors and Erasures in Random Network Coding*. IEEE Transactions on Information Theory, 54, 3579-3591, 2008