New Large Sets of Geometric Designs

Michael Robert Hurley
SUNY Oswego, michael.hurley@oswego.edu

June 4th, 2025

Introduction: Definitions

- A simple geometric $t - [q^n, k, \lambda]$ design is a collection $\mathcal{B}$ of k-dimensional subspaces of vector space $V = \mathbb{F}_q^n$, called blocks, over the finite field of order q, such that any t-dimensional subspace of V appears in exactly λ blocks.

Introduction: Definitions

- A simple geometric $t - [q^n, k, \lambda]$ design is a collection $\mathcal{B}$ of k-dimensional subspaces of vector space $V = \mathbb{F}_q^n$, called blocks, over the finite field of order q, such that any t-dimensional subspace of V appears in exactly λ blocks.
- A geometric $LS[N][t, k, q^n]$ large set is a partitioning of all k-subspaces of $V = \mathbb{F}_q^n$ into N disjoint collections of blocks, such that each collection is a $t - [q^n, k, \lambda]$ design.

Introduction: Problems

- Can we design efficient algorithms to find nontrivial $LS[N][t, k, q^n]$ large sets?

Introduction: Problems

- Can we design efficient algorithms to find nontrivial $LS[N][t, k, q^n]$ large sets?
- To create our large sets, we use group actions to fuse subspaces together into orbits, and collect blocks by collecting orbits in one of two ways.

Introduction: Problems

- Can we design efficient algorithms to find nontrivial $LS[N][t,k,q^n]$ large sets?
- To create our large sets, we use group actions to fuse subspaces together into orbits, and collect blocks by collecting orbits in one of two ways.
- Our first method, Lattice Basis Reduction, creates a lattice basis B from these orbits and constructs a very short basis B', which may yield a solution.

Introduction: Problems

- Can we design efficient algorithms to find nontrivial $LS[N][t, k, q^n]$ large sets?
- To create our large sets, we use group actions to fuse subspaces together into orbits, and collect blocks by collecting orbits in one of two ways.
- Our first method, Lattice Basis Reduction, creates a lattice basis B from these orbits and constructs a very short basis B', which may yield a solution.
- Our second method, Integer Linear Programming, creates a series of constraint equations out of these orbits and tries to optimize an objective function while satisfying all constraints simultaneously.

Preliminaries: The Gaussian Coefficient

Given a natural number n and a prime power q, define:

$$[0]_q = [0]_q! = 1$$

$$[n]_q = (1 + q + q^2 + \ldots + q^{n-1})$$

$$[n]_q! = [1]_q[2]_q \ldots [n]_q$$

Definition

The Gaussian Coefficient for a vector space $V = \mathbb{F}_q$ is defined as:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]_q!}{[k]_q![n-k]_q!},$$

which counts the number of k subspaces in an n-space over $\mathbb{F}_q$.

- If $V = \mathbb{F}_q^n$, then $\begin{bmatrix} V \\ k \end{bmatrix}_q$ is the collection of all k-subspaces in V.

Preliminaries: Necessary Conditions for a Geometric Design

- If $V = \mathbb{F}_q^n$, then $\begin{bmatrix} V \\ k \end{bmatrix}_q$ is the collection of all k-subspaces in V.

- Any t-$[q^n, k, \lambda]$ design is also an s-$[q^n, k, \lambda_s]$ design, where, for every $0 \leq s \leq t$:

$$\lambda_s = \lambda \cdot \begin{bmatrix} n-s \\ t-s \end{bmatrix} / \begin{bmatrix} k-s \\ t-s \end{bmatrix}$$

Preliminaries: Necessary Conditions for a Geometric Design

- If $V = \mathbb{F}_q^n$, then $\begin{bmatrix} V \\ k \end{bmatrix}_q$ is the collection of all k-subspaces in V.
- Any t-$[q^n, k, \lambda]$ design is also an s-$[q^n, k, \lambda_s]$ design, where, for every $0 \leq s \leq t$:

$$\lambda_s = \lambda \cdot \begin{bmatrix} n-s \\ t-s \end{bmatrix} \Big/ \begin{bmatrix} k-s \\ t-s \end{bmatrix}$$

- The parameters of an $LS[N][t, k, q^n]$ large set $\mathcal{L}$ imply that the constituent designs are t-$[q^n, k, \begin{bmatrix} n-t \\ k-t \end{bmatrix} / N]$ geometric designs.

Incidence and Fusion: Kramer-Mesner Matrix

- The action of G on V^* induces actions on $\begin{bmatrix} V \\ t \end{bmatrix}$ and $\begin{bmatrix} V \\ k \end{bmatrix}$ and partitions these sets into $\rho(t), \rho(k)$ orbits respectively:

$$\begin{bmatrix} V \\ t \end{bmatrix} = \Delta_1 + \Delta_2 + \ldots + \Delta_{\rho(t)}$$

$$\begin{bmatrix} V \\ k \end{bmatrix} = \Gamma_1 + \Gamma_2 + \ldots + \Gamma_{\rho(k)}$$

- The action of G on V^* induces actions on $\begin{bmatrix} V \\ t \end{bmatrix}$ and $\begin{bmatrix} V \\ k \end{bmatrix}$ and partitions these sets into $\rho(t), \rho(k)$ orbits respectively:

$$\begin{bmatrix} V \\ t \end{bmatrix} = \Delta_1 + \Delta_2 + \ldots + \Delta_{\rho(t)}$$

$$\begin{bmatrix} V \\ k \end{bmatrix} = \Gamma_1 + \Gamma_2 + \ldots + \Gamma_{\rho(k)}$$

- The $\rho(t) \times \rho(k)$ Kramer-Mesner matrix $A_{t,k} = (a_{t,k}(i,j))$ is defined by:

$$a_{t,k}(i,j) = |\{w \in \Gamma_j : u \leq w \ , \ \text{for a fixed } u \in \Delta_i\}|$$

Incidence and Fusion: Theorems

Theorem

Let V be a vector space of dimension n over the field $\mathbb{F}_q$, and let $G \leq \Gamma L_n(q)$ act on V^*, then there is a G-invariant, simple t-$[q^n, k, \lambda]$ design if and only if there is a $\rho(k) \times 1$ $\{0,1\}$-vector u which is a solution to the matrix equation:

$$A_{t,k} u = \lambda J \tag{3.1}$$

where J is the $\rho(t) \times 1$ vector of all 1's.

Theorem

(Cusack, Magliveras, 1999) There is a large set $LS[N][t, k, q^n]$ of G-invariant geometric designs if and only if there exists N distinct $\{0,1\}$ vector solutions $u_1, u_2, \ldots, u_N$, to (3.1), whose sum is the $\rho(k) \times 1$ all 1's vector.

Finding a solution X to the matrix equation $AX = B$, where B is a column vector, is equivalent to finding an X that satisfies the following matrix equation:

$$\begin{bmatrix} I_n & \vec{0}_n \\ A & -B \end{bmatrix} \begin{bmatrix} X \\ 1 \end{bmatrix} = \begin{bmatrix} X \\ \vec{0}_m \end{bmatrix} \tag{4.1}$$

where I_n is the identity matrix of order n, and $\vec{0}_s$ is the zero column vector of length s.

Finding New Large Sets: The Lattice Matrix

- We form this lattice matrix of rank $\rho(k) + 1$:

$$M = \begin{bmatrix} I_{\rho(k)} & \vec{0}_{\rho(k)} \\ A_{t,k} & -\lambda J \end{bmatrix}$$

Finding New Large Sets: The Lattice Matrix

- We form this lattice matrix of rank $\rho(k)+1$:

$$M = \begin{bmatrix} I_{\rho(k)} & \vec{0}_{\rho(k)} \\ A_{t,k} & -\lambda J \end{bmatrix}$$

- The set of all integer linear combinations of the columns of M forms a lattice $\mathcal{L}$ in $\mathbb{R}^{\rho(k)+\rho(t)}$.

Finding New Large Sets: The Lattice Matrix

- We form this lattice matrix of rank $\rho(k)+1$:

$$M = \begin{bmatrix} I_{\rho(k)} & \vec{0}_{\rho(k)} \\ A_{t,k} & -\lambda J \end{bmatrix}$$

- The set of all integer linear combinations of the columns of M forms a lattice $\mathcal{L}$ in $\mathbb{R}^{\rho(k)+\rho(t)}$.

- If $x = (x_1, x_2, \ldots, x_{\rho(k)+1}) \in \mathbb{Z}^{\rho(k)+1}$ with $x_i \in \{0,1\}$ for $1 \le i \le \rho(k)$, and $x_{\rho(k)+1} = 1$ such that:

$$Mx^T = (u_1, \ldots, u_{\rho(k)+\rho(t)})^T$$

where $u_i \in \{0,1\}$ for $1 \le i \le \rho(k)$ and $u_i = 0$ for $i > \rho(k)$, then u is a short vector in $\mathcal{L}$ spanned by the columns of M.

Finding New Large Sets: *LLL*

- The program we use to execute lattice basis reduction on M is a variation on *LLL* reduction, which turns the lattice basis M into a short basis M^*.

Finding New Large Sets: *LLL*

- The program we use to execute lattice basis reduction on M is a variation on *LLL* reduction, which turns the lattice basis M into a short basis M^*.

- If a short vector u appears as a column in M^*, then the indices of the 1's in u can form a t-$[q^n, k, \lambda]$ design D_1.

Finding New Large Sets: *LLL*

- The program we use to execute lattice basis reduction on M is a variation on *LLL* reduction, which turns the lattice basis M into a short basis M^*.

- If a short vector u appears as a column in M^*, then the indices of the 1's in u can form a t-$[q^n, k, \lambda]$ design D_1.

- The process is repeated on a new M, formed from $Q_{t,k}$, the columns of $A_{t,k}$ not chosen by our short vector u, with a new short vector u corresponding to another t-$[q^n, k, \lambda]$ design D_2, disjoint from D_1.

Finding New Large Sets: *LLL*

- The program we use to execute lattice basis reduction on M is a variation on *LLL* reduction, which turns the lattice basis M into a short basis M^*.

- If a short vector u appears as a column in M^*, then the indices of the 1's in u can form a t-$[q^n, k, \lambda]$ design D_1.

- The process is repeated on a new M, formed from $Q_{t,k}$, the columns of $A_{t,k}$ not chosen by our short vector u, with a new short vector u corresponding to another t-$[q^n, k, \lambda]$ design D_2, disjoint from D_1.

- The process repeats until we find the resulting collection $\{D_1, D_2, \ldots, D_N\}$ a geometric large set.

Our $\{0,1\}$ Integer Linear Programming problem (ILP) is the search for a vector $x \in \{0,1\}^{\rho(k)}$ that maximizes a function $f(x)$ while satisfying a series of linear restraints expressed below as a matrix equation:

$$\begin{aligned}
&\text{(i)} && \text{maximize :} && f(x) = c^T \cdot x \\
&\text{(ii)} && \text{subject to :} && Ax^T + s = B, \\
&\text{(iii)} && \text{where :} && s \geq 0, \\
&\text{(iv)} && \text{and :} && x \in \{0,1\}^n
\end{aligned} \tag{4.2}$$

Kramer-Mesner Matrices: The Singer Cycle

Both solution methods generate G-invariant designs, and require an $A_{t,k}$, so we construct our $A_{2,3}$ matrix from a Singer subgroup $G = \langle \alpha \rangle$, generated by a Singer cycle $\alpha \in GL_8(2)$ that acts regularly on the non-zero vectors of $V = \mathbb{F}_2^8$.

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

The New Large Sets: Lattice-Basis Reduction

- Our Singer subgroup is the same one used by Braun et al. to find the first $LS[3][2, 3, 2^8]$.

The New Large Sets: Lattice-Basis Reduction

- Our Singer subgroup is the same one used by Braun et al. to find the first $LS[3][2, 3, 2^8]$.

- With $A_{2,3}$ constructed, we create our lattice basis matrix M with $\lambda = 21$.

The New Large Sets: Lattice-Basis Reduction

- Our Singer subgroup is the same one used by Braun et al. to find the first $LS[3][2, 3, 2^8]$.
- With $A_{2,3}$ constructed, we create our lattice basis matrix M with $\lambda = 21$.
- We have 3 different ways of permuting the columns of M after each LLL lattice-basis reduction, and each returns a solution to (3.1) from M.

The New Large Sets: Lattice-Basis Reduction

- Our Singer subgroup is the same one used by Braun et al. to find the first $LS[3][2,3,2^8]$.

- With $A_{2,3}$ constructed, we create our lattice basis matrix M with $\lambda = 21$.

- We have 3 different ways of permuting the columns of M after each LLL lattice-basis reduction, and each returns a solution to (3.1) from M.

- 1) By increasing weight
  2) By alternating between the chronologically first and chronologically last columns of M^*
  3) By alternating between small weight and large weight columns.

The New Large Sets: Lattice-Basis Reduction

- Our Singer subgroup is the same one used by Braun et al. to find the first $LS[3][2, 3, 2^8]$.

- With $A_{2,3}$ constructed, we create our lattice basis matrix M with $\lambda = 21$.

- We have 3 different ways of permuting the columns of M after each LLL lattice-basis reduction, and each returns a solution to (3.1) from M.

- 1) By increasing weight
  2) By alternating between the chronologically first and chronologically last columns of M^*
  3) By alternating between small weight and large weight columns.

- This results in 9 large sets found with lattice basis reduction.

- To find large sets using linear programming, we create the following version of (4.2):

$$\begin{array}{lll} \text{(i)} & \text{maximize} & f(x) = J^{\mathsf{T}} \cdot x \\ \text{(ii)} & \text{subject to} & A_{2,3}x^T + s = 21J, \\ \text{(iii)} & \text{where} & s = 0, \\ \text{(iv)} & \text{and} & x \in \{0,1\}^n \end{array} \tag{5.1}$$

- To find large sets using linear programming, we create the following version of (4.2):

$$
\begin{array}{lll}
\text{(i)} & \text{maximize} & f(x) = J^{\mathsf{T}} \cdot x \\
\text{(ii)} & \text{subject to} & A_{2,3}x^{T} + s = 21J, \\
\text{(iii)} & \text{where} & s = 0, \\
\text{(iv)} & \text{and} & x \in \{0,1\}^{n}
\end{array}
\tag{5.1}
$$

- We found two solutions to (3.1) using the above *ILP*, one using $A_{2,3}$, another by permuting the columns of $A_{2,3}$ first.

Proving Non-Isomorphism: The Normalizer of G in $GL_8(2)$

- The normalizer of a Singer subgroup in $GL_n(q)$ has order $n(q^n - 1)$ and is the extension of $\langle \alpha \rangle$ by ζ, the Frobenius automorphism of $GL_8(2)$.

Proving Non-Isomorphism: The Normalizer of G in $GL_8(2)$

- The normalizer of a Singer subgroup in $GL_n(q)$ has order $n(q^n - 1)$ and is the extension of $\langle \alpha \rangle$ by ζ, the Frobenius automorphism of $GL_8(2)$.
- Let $\Lambda = \{\mathcal{L}_0, \mathcal{L}_1, \ldots, \mathcal{L}_{11}\}$ be our large sets found, with $\mathcal{L}_0$ the large set found by Braun et al.

Proving Non-Isomorphism: The Normalizer of G in $GL_8(2)$

- The normalizer of a Singer subgroup in $GL_n(q)$ has order $n(q^n - 1)$ and is the extension of $\langle\alpha\rangle$ by ζ, the Frobenius automorphism of $GL_8(2)$.
- Let $\Lambda = \{\mathcal{L}_0, \mathcal{L}_1, \ldots, \mathcal{L}_{11}\}$ be our large sets found, with $\mathcal{L}_0$ the large set found by Braun et al.
- $G = \langle\alpha\rangle$ is in the automorphism group of every one of these large sets and designs, while exhaustive search showed that ζ is not.

Proving Non-Isomorphism: The Stabilizers of the Large Set Designs

- Let $M \leq GL_8(2)$ be the only maximal subgroup up to conjugacy that contains G, and by extension the automorphism groups of these designs.

Proving Non-Isomorphism: The Stabilizers of the Large Set Designs

- Let $M \leq GL_8(2)$ be the only maximal subgroup up to conjugacy that contains G, and by extension the automorphism groups of these designs.
- If M_1 is the stabilizer in M of vector 1, M_1 is a complete collection of left coset representatives of G in M

Proving Non-Isomorphism: The Stabilizers of the Large Set Designs

- Let $M \leq GL_8(2)$ be the only maximal subgroup up to conjugacy that contains G, and by extension the automorphism groups of these designs.
- If M_1 is the stabilizer in M of vector 1, M_1 is a complete collection of left coset representatives of G in M
- Exhaustive search reveals that no non-identity coset representative is an automorphism of any design in any of these large sets.

Proving Non-Isomorphism: Design Permutation

- Let $\mathcal{L} = \{\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3\}$ be one of our large sets and Q be the subgroup of A=Aut($\mathcal{L}$) that fixes each design.

Proving Non-Isomorphism: Design Permutation

- Let $\mathcal{L} = \{\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3\}$ be one of our large sets and Q be the subgroup of A=Aut($\mathcal{L}$) that fixes each design.
- $G = Q$ is a normal subgroup of A, and A/Q is a subgroup $T \leq \mathcal{S}_3$.

Proving Non-Isomorphism: Design Permutation

- Let $\mathcal{L} = \{\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3\}$ be one of our large sets and Q be the subgroup of A=Aut($\mathcal{L}$) that fixes each design.
- $G = Q$ is a normal subgroup of A, and A/Q is a subgroup $T \leq \mathcal{S}_3$.
- Since $Q \cap T = \{1\} \in \mathcal{S}_3$, A is a split extension of Q by T.

Proving Non-Isomorphism: Design Permutation

- Let $\mathcal{L} = \{\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3\}$ be one of our large sets and Q be the subgroup of A=Aut($\mathcal{L}$) that fixes each design.
- $G = Q$ is a normal subgroup of A, and A/Q is a subgroup $T \leq \mathcal{S}_3$.
- Since $Q \cap T = \{1\} \in \mathcal{S}_3$, A is a split extension of Q by T.
- However, an element of order 2 in T would have to fix one of the three designs, but the only automorphisms that fix any of these designs are in G, which has odd order.

Proving Non-Isomorphism: Design Permutation

- Let $\mathcal{L} = \{\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3\}$ be one of our large sets and Q be the subgroup of A=Aut($\mathcal{L}$) that fixes each design.
- $G = Q$ is a normal subgroup of A, and A/Q is a subgroup $T \leq \mathcal{S}_3$.
- Since $Q \cap T = \{1\} \in \mathcal{S}_3$, A is a split extension of Q by T.
- However, an element of order 2 in T would have to fix one of the three designs, but the only automorphisms that fix any of these designs are in G, which has odd order.
- Also, an element of order 3 in T cannot normalize Q as the only elements of order 3 in $N_{GL_8(2)}(Q)$ are in $Q = \langle \alpha \rangle$, which fixes the designs instead of permuting them.

Proving Non-Isomorphism: Design Permutation

- Let $\mathcal{L} = \{\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3\}$ be one of our large sets and Q be the subgroup of A=Aut($\mathcal{L}$) that fixes each design.
- $G = Q$ is a normal subgroup of A, and A/Q is a subgroup $T \leq \mathcal{S}_3$.
- Since $Q \cap T = \{1\} \in \mathcal{S}_3$, A is a split extension of Q by T.
- However, an element of order 2 in T would have to fix one of the three designs, but the only automorphisms that fix any of these designs are in G, which has odd order.
- Also, an element of order 3 in T cannot normalize Q as the only elements of order 3 in $N_{GL_8(2)}(Q)$ are in $Q = \langle \alpha \rangle$, which fixes the designs instead of permuting them.
- Therefore, the automorphism groups of these large sets are all G.

Proving Non-Isomorphism: An Important Theorem

Theorem

(Betten, Laue, and Wasserman, 2015) *Let G be a finite group acting on a set X. Suppose that $x_1, x_2 \in X$ and $g \in G$ such that $x_1^g = x_2$. Moreover, suppose that a Sylow p-subgroup $P \in G$ is contained in both stabilizers G_{x_1} and G_{x_2}. Then $x_1^n = x_2$ for some $n \in N_G(P)$.*

Proving Non-Isomorphism: The Result

Theorem

All 12 of the large sets found are non-isomorphic.

Proving Non-Isomorphism: The Result

Theorem

All 12 of the large sets found are non-isomorphic.

- Let X be the collection of all large sets of type $LS[3][2, 3, 2^8]$. $GL_8(2)$ acts on X and the stabilizer of any $\lambda \in X$ is the full automorphism group of λ.

Proving Non-Isomorphism: The Result

Theorem

All 12 of the large sets found are non-isomorphic.

- Let X be the collection of all large sets of type $LS[3][2,3,2^8]$. $GL_8(2)$ acts on X and the stabilizer of any $\lambda \in X$ is the full automorphism group of λ.

- We have $\langle \alpha^{15} \rangle = P$, a Sylow 17-subgroup in the stabilizer of every one of our large sets in Λ, so if $\lambda, \mu \in \Lambda$ are isomorphic, there is $n \in N_{GL_8(2)}(P) = N_{GL_8(2)}(G)$ where $\lambda^n = \mu$.

Proving Non-Isomorphism: The Result

Theorem

All 12 of the large sets found are non-isomorphic.

- Let X be the collection of all large sets of type $LS[3][2, 3, 2^8]$. $GL_8(2)$ acts on X and the stabilizer of any $\lambda \in X$ is the full automorphism group of λ.
- We have $\langle \alpha^{15} \rangle = P$, a Sylow 17-subgroup in the stabilizer of every one of our large sets in Λ, so if $\lambda, \mu \in \Lambda$ are isomorphic, there is $n \in N_{GL_8(2)}(P) = N_{GL_8(2)}(G)$ where $\lambda^n = \mu$.
- $N_{GL_8(2)}(G)$ contains no element that sends any large set in Λ to another. Thus, all 12 of these large sets are non-isomorphic.

Future Problems: Constructing More Large Sets

- Kiermaier and Laue's work on recursive constructions of geometric large sets can confirm the admissibility of the parameters of different $LS[N][t, k, q^n]$.

Future Problems: Constructing More Large Sets

- Kiermaier and Laue's work on recursive constructions of geometric large sets can confirm the admissibility of the parameters of different $LS[N][t, k, q^n]$.

- Braun, Kiermaier, and Kohnert devised a recursive construction method for proving the existence of geometric halvings, large sets where $N = 2$. Constructing these infinite families of geometric large sets is still being worked on.

Thank You

Thanks to all of you for listening!