B. Tech. Project

Set Systems with Restricted Intersections

Submitted in partial fulfillment of the requirements
for the degree of
Bachelor of Technology

by

Subhash Ajit Khot
95005008

under the guidance of

Dr. Sundar Vishwanathan

Department of Computer Science and Engineering
Indian Institute of Technology, Bombay
April 5, 1998

Acknowledgment

April 5, 1999

I would like to thank **Dr. Sundar Vishwanathan** for the constant guidance, help and encouragement he provided during the course of the project.

Subhash A. Khot

Abstract

The aim of the project is to find necessary and sufficient conditions on a fixed set L of nonnegative integers and a fixed positive integer k so that for every large n, there exists an L-intersecting, k-uniform family of subsets of $[n]$ with size $\Omega(n^3)$. We have obtained a fairly general construction of $\Omega(n^3)$ size families. Explicit examples of (L, k) with $|L| = 3$ and $|L| = 4$ are presented. We also obtain a necessary condition in terms of 2-$(k, l, 1)$ designs when $L = \{0, 1, l\}$. We show that the problem is related to several interesting topics in design theory.

Contents

Chapter 1

Introduction

Let k be a fixed positive integer. Consider the following problem : *What is the maximum size of a family $\mathcal{F}$ of subsets of $\{1, 2, \ldots, n\}$ such that every subset in this family has cardinality k and the cardinality of intersection of any two distinct subsets in this family is even.*

If k is odd, it can be shown that $|\mathcal{F}| \leq n$ using linear algebra techniques. However if k is even, we can construct a family of size $\binom{\lfloor n/2 \rfloor}{k/2}$. Indeed, we can pair off the elements and consider the family of all subsets obtained by choosing any $k/2$ of these pairs. Thus the order of magnitude of maximum size of $\mathcal{F}$ is $\Omega(n^{k/2})$ when k is even.

Let $[n]$ denote the set $\{1, 2, \ldots, n\}$.

Definition 1.1 *A family $\mathcal{F}$ of subsets of $[n]$ is said to be k-uniform if each member of the family has cardinality k.*

Definition 1.2 *Let $L = \{l_1, l_2, \ldots\}$ be a set of nonnegative integers. A family $\mathcal{F}$ of subsets of $[n]$ is said to be L-intersecting if $|F_1 \bigcap F_2| \in L$ for any two distinct members F_1 and F_2 of the family $\mathcal{F}$.*

Given a set L and integer k, let $m(n, k, L)$ denote the maximum size of an L-intersecting, k-uniform family of subsets of $[n]$. In the example given, L is the set of all even numbers. When k is odd, $m(n, k, L) \leq n$ and when k is even, $m(n, k, L) \geq \binom{\lfloor n/2 \rfloor}{k/2}$. Thus the number $m(n, k, L)$, even its order of magnitude, depends heavily on L and k.

Babai and Frankl proved the following theorem [4].

Theorem 1.1 *(Linear Threshold Theorem)*
Assume that L is finite and $0 \in L$, i.e., $l_1 = 0$.
(a) Suppose that $gcd(l_2, l_3, \ldots)$ does not divide k. Then $m(n, k, L) \leq n$.

(b) Assume $gcd(l_2, l_3, \dots)$ *divides* k *and* $k \geq |L| l_{max}^2$ *where* l_{max} *is the largest number in* L*. Then for any* $n \geq 2k^2$, $m(n,k,L) \geq (n/2k)^2$.

The linear threshold theorem gives a necessary and sufficient condition for $m(n,k,L) = \Omega(n^2)$ for large enough k. The aim of this project is to extend this theorem by one level of magnitude. If possible, we want to give necessary and sufficient conditions on L and k so that $m(n,k,L) = \Omega(n^3)$. The situation becomes much more complicated than just looking at the *gcd* of numbers in L.

The report is organized as follows.

- Chapter 2 gives an overview of the previous work.
- Chapter 3 gives a few necessary conditions.
- Chapter 4 gives a few constructions i.e., sufficient conditions.
- Chapter 5 considers embedding of designs in projective planes.

Chapter 2

Previous Work

This chapter states the important theorems in the area of set systems with restricted intersections.

Theorem 2.1 (*Frankl* [6])

$$m(n, k, \{l_1, \ldots, l_s\}) \;=\; \theta(m(n, k - l_1, \{0, l_2 - l_1, \ldots, l_s - l_1\})).$$

Thus we can always assume that $l_1 = 0$ since we are concerned only with the order of magnitude of $m(n, k, L)$.

The following is a slight restatement of the linear threshold theorem mentioned in the introduction.

Theorem 2.2 (*Babai, Frankl* [4])
Let $|L| = s$ and assume $0 \in L$ i.e., $l_1 = 0$.
(a) If $gcd(l_2, \ldots, l_s)$ does not divide k, then $m(n, k, L) \leq n$.
(b) If there exist nonnegative integers $d_2, \ldots, d_s$ such that $k = d_2 l_2 + \ldots + d_s l_s$, then $m(n, k, L) \geq (n/2k)^2$ for $n \geq 2k^2$. If $gcd(l_2, \ldots, l_s)$ divides k and $k \geq |L| l_{max}^2$, then such integers do exist.

Theorem 2.3 (*Ray-Chaudhuri, Wilson* [1, *page* 143])
Let L be a set of s integers and $s \leq k$. Then $m(n, k, L) \leq \binom{n}{s}$.

Theorem 2.4 (*Frankl, Wilson* [1, *page* 143])
Let f be a polynomial of degree s with integer coefficients. Suppose there exists a prime power p^α such that $f(l) \equiv 0 \pmod{p^\alpha}$ for every $l \in L$ and $f(k) \not\equiv 0 \pmod{p^\alpha}$. Then $m(n, k, L) \leq \binom{n}{s}$.

In particular, if $m(n,k,L) = \Omega(n^3)$, it is necessary that there must not exist a quadratic polynomial which has every $l \in L$ as its root modulo p^α and does not have k as its root modulo p^α.

Theorem 2.5 [1, *Exercise* 5.9.3]
Consider the polynomial $f(x) = \sum_{i=0}^{d} \alpha_i \binom{x}{i}$ where the α_i are nonnegative integers. For a set L of nonnegative integers, let $f(L) = \{f(l) \mid l \in L\}$. Then given a k-uniform L-intersecting family $\mathcal{F}$ on n elements, there exists an $f(k)$-uniform $f(L)$-intersecting family $\mathcal{G}$ on $f(n)$ elements with $|\mathcal{F}| = |\mathcal{G}|$.

Theorem 2.6 (*Frankl* [9])
For every rational number $r \geq 1$, there exists a positive integer k and a set L of non-negative integers such that $m(n,k,L) = \theta(n^r)$.

When $L = \{0, a, b\}$, we have a necessary condition.

Theorem 2.7 (*Deza, Erdös, Frankl* [5])
Let $L = \{0, a, b\}$. Then unless $a|b$ and $(b-a)|(k-a)$, we have $m(n,k,L) = O(n^2)$.

Finally, there is an open conjecture which gives a necessary condition. Let us denote by $(L \ mod \ r)$, the set of distinct modulo r classes of integers in L. For example, $(\{0,2,3,6,8\} \ mod \ 3) = \{0,2\}$. We say that $k \in L \ (mod \ r)$ if there exists $l \in L$ such that r divides $k - l$.

Conjecture 2.1 [1, *page* 145]
Suppose there exists an integer $r \geq 3$ such that $|(L \ mod \ r)| \leq 2$ and $k \notin L(mod \ r)$. Then $m(n,k,L) \leq \binom{n}{2}$.

This conjecture is true when r is a prime power.

Chapter 3

Necessary Conditions for $m(n,k,L) = \Omega(n^3)$

In this chapter, we give some necessary conditions on L and k so that $\Omega(n^3)$ size L-intersecting, k-uniform families do exist. We mainly concentrate on $L = \{0,a,b\}$. Theorem 2.7 implies that b and k must be divisible by a. It is proved in [3] that $m(n,k_1,\{0,a,b\}) = \Omega(n^3)$ iff $m(n,k,\{0,1,l\}) = \Omega(n^3)$ where $k = k_1/a$, $l = b/a$. So it is sufficient to consider the case $L = \{0,1,l\}$, $l \geq 2$.

We first introduce block designs and related terms.

3.1 Designs

Definition 3.1 *A t-(k,l,λ) design $\mathcal{D}$ is a pair $(\mathcal{P},\mathcal{B})$ where $\mathcal{P}$ is a set with cardinality k, $\mathcal{B}$ is a family of distinct l-subsets of $\mathcal{P}$ and every t-subset of $\mathcal{P}$ is contained is exactly λ members of the family $\mathcal{B}$. The sets in $\mathcal{B}$ are called blocks or lines of the design $\mathcal{D}$.*

In this report we consider only 2-$(k,l,1)$ designs and we use the term (k,l) *design* to mean a 2-$(k,l,1)$ design.

The most familiar designs arise from projective and affine spaces over finite fields. Let $PG(n,q)$ denote the design of points and lines in the projective space of dimension n over $\mathbb{F}_q$. This is a $(\frac{q^{n+1}-1}{q-1}, q+1)$ design. The points and blocks of this design correspond to 1-dimensional and 2-dimensional subspaces of $\mathbb{F}_q^{n+1}$ respectively. Let $AG(n,q)$ denote the design of points and lines in the affine space of dimension n over $\mathbb{F}_q$. This is a (q^n, q) design.

Definition 3.2 *A design $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1)$ is said to be embedded in a design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ if there exist injective maps $f\ : \mathcal{P}_1 \to \mathcal{P}$ and $g\ : \mathcal{B}_1 \to \mathcal{B}$ such that for any $p_1 \in \mathcal{P}_1,\ B_1 \in \mathcal{B}_1$, we have $p_1 \in B_1$ iff $f(p_1) \in g(B_1)$.*

Definition 3.3 *A design $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1)$ is said to be isomorphic to a design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ if there exist bijective maps $f\ : \mathcal{P}_1 \to \mathcal{P}$ and $g\ : \mathcal{B}_1 \to \mathcal{B}$ such that for any $p_1 \in \mathcal{P}_1,\ B_1 \in \mathcal{B}_1$, we have $p_1 \in B_1$ iff $f(p_1) \in g(B_1)$.*

An automorphism of a design is an isomorphism onto itself.

3.2 Necessary Condition in terms of Designs

We need the following results from extremal set theory.

Theorem 3.1 (*Erdös, Rado* [7])
Suppose $\mathcal{A}$ is a k-uniform set system, $k, d \geq 2$. If $|\mathcal{A}| > d^k k!$ then $\mathcal{A}$ contains a Δ-system of size $d+1$, i.e., sets $A_1, A_2, \ldots, A_{d+1}$ such that for some set K, called the kernel, $A_i \bigcap A_j = K$ for every $1 \leq i < j \leq d+1$.

Lemma 3.1.1 [5]
Suppose both K_1 and K_2 are kernels of Δ-systems, consisting of $k+1$ members of an $(n, k, \{l_1, \ldots, l_s\})$ system $\mathcal{F}$. Then $|K_1 \bigcap K_2| \in \{l_1, \ldots, l_s\}$.

Let $\mathcal{F}$ be a k-uniform $\{0,1,l\}$-intersecting family of subsets of $[n]$. If $|\mathcal{F}| > \binom{n}{2}$, from Theorem 2.5, it follows that there exists a $\binom{k}{2}$-uniform $\{0, \binom{l}{2}\}$-intersecting family of subsets of $[\binom{n}{2}]$ with size $> \binom{n}{2}$. From linear threshold theorem, we conclude that $\binom{l}{2}$ divides $\binom{k}{2}$.

Suppose $|\mathcal{F}| \geq n^2/k$. We count $\{(i, F) |\ i \in [n],\ F \in \mathcal{F}\}$ in two ways to conclude that $\exists\ x \in [n]$ such that x is contained in at least n members of $\mathcal{F}$. Let $\mathcal{F}_1 = \{F \setminus \{x\} \mid F \in \mathcal{F}, x \in F\}$. Thus $\mathcal{F}_1$ is a $(k-1)$-uniform, $\{0, l-1\}$ intersecting family of subsets of $[n-1]$ and $|\mathcal{F}_1| > n-1$. By linear threshold theorem, it follows that $(l-1)|(k-1)$.

Thus $(l-1)|(k-1)$ and $\binom{l}{2}|\binom{k}{2}$ are necessary conditions for $m(n,k,L) = \Omega(n^3)$. Now we prove a stronger condition. The proof is just a slight modification of a similar proof in [3].

Theorem 3.2 *Let $L = \{0, 1, l\}$, k be given. If there exists an L-intersecting k-uniform family $\mathcal{F}$ of subsets of $[n]$ and $|\mathcal{F}| > k!k^k\binom{n}{2}$ then, there exists a (k, l) design i.e., there exists a family of l-subsets of $[k]$ such that every 2-subset is contained in precisely one member of this family.*

Proof: Let $\mathcal{B}$ be the family of those l-subsets which are kernels of Δ-systems of size $k+1$ consisting of members of $\mathcal{F}$, i.e., if $B \in \mathcal{B}$ then there exist $F_1, \ldots, F_{k+1} \in \mathcal{F}$ such that $F_i \bigcap F_j = B$ for $1 \le i < j \le k+1$.

A set $F \in \mathcal{F}$ is said to be 2-covered by $\mathcal{B}$ if for every 2-subset C of F, there exists $B \in \mathcal{B}$ such that $C \subseteq B \subseteq F$. Let $\mathcal{F}_0$ be the sub-collection of $\mathcal{F}$ consisting of those sets which are not 2-covered by $\mathcal{B}$. We prove that $|\mathcal{F}_0| \le k!k^k\binom{n}{2}$. To every $F \in \mathcal{F}_0$, there is a corresponding 2-set C_F such that $C_F \subseteq F$ and there is no $B \in \mathcal{B}$ such that $C_F \subseteq B \subseteq F$. It is sufficient to prove that any 2-subset D corresponds to at most $k!k^k$ members of $\mathcal{F}_0$. If this is not true, by Theorem 3.1, $\exists$ a Δ-system $F_1, \ldots, F_{k+1} \in \mathcal{F}_0$ with kernel K. We have $F_i \bigcap F_j = K \; \forall\, i \neq j$. Since D is contained in every F_i, $D \subseteq K \;\Rightarrow |K| \ge 2$. Since the family $\mathcal{F}$ is $\{0, 1, l\}$-intersecting, $|K| = l$. This implies $K \in \mathcal{B}$. But this contradicts the choice of D because now $D \subseteq K \subseteq F_1$. Hence $|\mathcal{F}_0| \le k!k^k\binom{n}{2}$.

Now $|\mathcal{F}| > |\mathcal{F}_0|$, so $\exists\, G \in \mathcal{F}$ which is 2-covered by $\mathcal{B}$. Let $B_1, \ldots, B_t$ be the distinct members of $\mathcal{B}$ contained in G. By Lemma 3.1.1, $|B_i \bigcap B_j| \in \{0, 1\}$ for $1 \le i < j \le t$. Thus the sets $B_1, \ldots, B_t$ do form a (k, l) design with the point set G. □

It is known that there is no $(43, 7)$ design. [2, page 264]. Thus the theorem implies that the maximum size of 43-uniform $\{0, 1, 7\}$-intersecting family is $O(n^2)$.

An interesting question is whether the bound $k!k^k\binom{n}{2}$ in Theorem 3.2 can be replaced by $\binom{n}{2}$.

Theorem 3.2 gives rise to the question of determining values of k for which a (k, l) design exists. One condition that follows by simple counting arguments is $(l-1)|(k-1)$ and $l(l-1)|k(k-1)$. Wilson [12] proved that this condition is sufficient for existence of a (k, l) design for every large k.

Existence of a (k, l) design may not be sufficient for existence of $\Omega(n^3)$ size k-uniform $\{0, 1, l\}$-intersecting families. By Wilson's theorem, there exists a $(k, 6)$ design for some $k \equiv 16 (mod\ 30)$. However for such k, Conjecture 2.1 implies that $m(n, k, \{0, 1, 6\}) = O(n^2)$.

3.3 Existence of Designs

A $(k, 3)$ design is also known as Steiner Triple System (STS). It is known [8] that a STS exists iff $k \equiv 1$ *or* 3 $(mod\ 6)$. It is known that for $k = 7$ and $k = 9$, there exists only one STS, viz. the designs $PG(2, 2)$ and $AG(2, 3)$ respectively. For higher values of k, there are more than one non-isomorphic STS. We give a construction of a STS in a special case.

Theorem 3.3 *Let $gcd(n, 6) = 1$. Assume that if a prime $p|n$ then the order of -2 modulo p is even. Then a STS exists for $n + 2$.*

Proof: Let us work in the ring R of integers modulo n.
Let S_0 be the set system $\{\ \{x, y, -x-y\} | 2x + y \neq 0,\ 2y + x \neq 0,\ x \neq y\}$. The conditions imposed guarantee that every member of S_0 has cardinality 3. The operation $-x-y$ is symmetric in the sense that $-x-(-x-y) = y$. So every pair $\{x, y\}$ is contained in at most one triple in S_0. It is not contained in any triple iff $x = -2y$ *or* $y = -2x$. Since $gcd(-2, n) = 1$, the operation of multiplication by -2 partitions R into orbits. Orbit is a subset of R with elements acting as vertices of a directed cycle such that if (x, y) is an edge of the directed cycle, then $y = -2x$. Assume these orbits to be $O_0, O_1, \ldots, O_h$ where $O_0 = \{0\}$. Let $O_i = \{x_{i1}, x_{i2}, \ldots, x_{i\alpha_i}\}$ for $1 \leq i \leq h$. Orbit means $\forall, 1 \leq i \leq h, 1 \leq j \leq \alpha_i$, we have $x_{ij+1} = -2x_{ij}$ with the convention that $x_{i(\alpha_i+1)} = x_{i1}$. Thus a pair $\{x, y\}$ is not contained in any triple in S_0 iff x and y are adjacent in one of the orbits. Since $gcd(6, n) = 1$, size of each orbit $O_i,\ i \geq 1$ is at least 3. We prove that every orbit $O_i,\ i \geq 1$ has even size, i.e., the α_i's are all even.

For orbit O_i, $x_{i1}\dot{(}-2)^{\alpha_i} \equiv x_{i1}\ (mod\ n) \Rightarrow x_{i1}\dot{(}(-2)^{\alpha_i} - 1) \equiv 0\ (mod\ n)$. Since $x_{i1} \neq 0$ in the ring R, there exists a prime $p|n$ and p does not divide $x_{i1} \Rightarrow p|(-2)^{\alpha_i} - 1$. The hypothesis says that the order of -2 modulo p is even, hence α_i is even.

Now let us introduce two more elements a and b. Let

$$S_i = \{\ \{a, x_{i1}, x_{i2}\}, \{b, x_{i2}, x_{i3}\}, \{a, x_{i3}, x_{i4}\}, \ldots, \{b, x_{i\alpha_i}, x_{i1}\}\ \},\ \ |S_i| = \alpha_i$$
$$Define\ S\ =\ \{\ \{0, a, b\}\ \} \bigcup S_0 \bigcup S_1 \bigcup \ldots \bigcup S_h$$

It can be verified that this is a STS over the set of elements $\{x | x \in R\} \bigcup \{a, b\}$. Thus a STS exists for $n + 2$. □

Definition 3.4 *A finite affine plane consists of a finite set P of points and a family of nonempty subsets of P called lines such that :*

1. *every pair of points is contained in a unique line.*
2. *every point p not contained in a line L is contained in a unique line L' such that $L \bigcap L' = \emptyset$.*
3. *there exist four points such that no three of them are contained in a single line.*

It is known that [2, page 254] for every finite affine plane, there exists a positive integer $m \geq 2$, called the order of the affine plane, such that every line has cardinality m and the total number of points is m^2. Thus an affine plane of order m is same as a (m^2, m) design. It is also known that affine plane exists if m is a prime power and it does not exist for $m = 6, 10$. Following theorem gives a construction of (m^r, m) designs provided an affine plane of order m exists.

Theorem 3.4 *If there exists an affine plane of order m then a (m^r, m) design exists for every $r \geq 1$.*

Proof: Affine plane of order m has $m^2 + m$ lines. Out of these, we can find m horizontal lines $F_1, \ldots, F_m$ and m vertical lines $G_1, \ldots, G_m$, i.e., $F_i \bigcap F_j = \emptyset$, $G_i \bigcap G_j = \emptyset$ for $i \neq j$ and $|F_i \bigcap G_j| = 1$ for all i, j. We can arrange these $2m$ lines as rows and columns of $m \times m$ array. The rest of the $m^2 - m$ lines contain exactly one element from each row and each column. So each such line corresponds to a permutation of $[m]$. Any two lines intersect at 0 or 1 points. Thus we obtain a set $\prod$ of $m^2 - m$ permutations with the property that if $\sigma, \tau \in \prod$, $\sigma \neq \tau$, then $|\{\ i \mid \sigma(i) = \tau(i)\ \}| = 0$ or 1. This set $\prod$ also has the property that for any $i \neq j$ and $i' \neq j'$, there is a unique permutation $\sigma \in \prod$ such that $\sigma(i) = i'$, $\sigma(j) = j'$.

Now we prove the claim by induction on r. For $r = 1$, this is trivial. The single set $\{1, 2, \ldots, m\}$ forms a (m, m) design. Assume that the claim holds for some $r \geq 1$. Let $A_1, \ldots, A_q$ be the blocks of a (m^r, m) design with $q = \binom{m^r}{2} / \binom{m}{2}$. We identify $[m^{r+1}]$ with the set

$$X = \{(i, j) \mid 1 \leq i \leq m^r,\ \ 1 \leq j \leq m\}.$$

Now we define the sets $B_{\alpha\beta}$, C_γ as follows:

$$B_{\alpha\beta} = \{(i, \beta) \mid i \in A_\alpha\} \ \ for\ 1 \leq \alpha \leq q,\ 1 \leq \beta \leq m.$$
$$C_\gamma = \{(\gamma, j) \mid 1 \leq j \leq m\} \ \ for\ 1 \leq \gamma \leq m^r.$$

Next we define sets $D_{\alpha\sigma}$ for every choice of A_α and $\sigma \in \prod$.
Let $A_\alpha = \{i_1, i_2, \ldots, i_m\}$. Define

$$D_{\alpha\sigma} = \{(i_t, \sigma(t)) \mid 1 \leq t \leq m\}$$

Now let us prove that every 2-subset of X is contained in at least one of the sets $B_{\alpha\beta}, C_\gamma, D_{\alpha\sigma}$. Let $\{(a,b),(c,d)\}$ be a 2-set. If $b = d$, this set is contained in $B_{\alpha b}$ where $\{a,c\}$ is contained in A_α. If $a = c$, this set is contained in C_a. Otherwise, let A_α be the set containing $\{a,c\}$. Let $A_\alpha = \{i_1, i_2, \ldots, i_m\}$ and $a = i_{t_1},\ c = i_{t_2}$. Let σ be the permutation in $\prod$ such that $\sigma(t_1) = b$ and $\sigma(t_2) = d$. This implies that the 2-set is contained in $D_{\alpha\sigma}$.

The number of sets $B_{\alpha\beta}, C_\gamma, D_{\alpha\sigma}$ is $mq + m^r + q(m^2 - m) = \binom{m^{r+1}}{2} / \binom{m}{2}$. Thus these sets do form a (m^{r+1}, m) design. □

3.4 Second Necessary Condition

In Chapter 2, we mentioned some necessary conditions for $m(n,k,L) = \Omega(n^3)$. We restate these conditions in two more equivalent forms.

Theorem 3.5 *Let $L = \{l_1, l_2, \ldots, l_s\}$. Assume that $0 \in L$. The following are equivalent conditions for $m(n,k,L) = \Omega(n^3)$.*

1. *There must not exist a polynomial $f(x) = bx + cx^2$ and a prime power p^α such that $f(l) \equiv 0 \pmod{p^\alpha}\ \forall, l \in L$ and $f(k) \not\equiv 0 \pmod{p^\alpha}$.*
2. *If for some prime power p^α, $|(L \bmod p^\alpha)| \leq 2$, then $k \in L \pmod{p^\alpha}$.*
3. *For any integers α, β, $\quad gcd_i(\ \alpha l_i + \beta l_i^2)$ divides $\alpha k + \beta k^2$.*
4. *There exist integers $d_1, \ldots, d_s$ such that $k = d_1 l_1 + \ldots + d_s l_s$ and $k^2 = d_1 l_1^2 + \ldots + d_s l_s^2$.*

We omit the proof of the equivalence of these conditions since it is long and not very interesting. The only point to state this theorem is to contrast condition 3 and condition 4 with the conditions $gcd(l_i) | k$ and $k = d_1 l_1 + \ldots + d_s l_s$ respectively in the linear threshold theorem.

Chapter 4

Constructions of $\Omega(n^3)$ Size Families

Let us denote an arbitrary prime power by q. Let $\mathbb{F}_q$ be the finite field with q elements.

4.1 The Main Construction

In this section, we give a fairly general construction of $\Omega(n^3)$ size L-intersecting k-uniform families of subsets of $[n]$. We obtain several concrete examples as corollaries in the next section.

Let $L = \{l_1, l_2, \dots\}$ and k be given, $k \notin L$.

Theorem 4.1 *Suppose there exists a set S of k points in space $\mathbb{F}_q^r$, $r \geq 3$, such that any subspace V of dimension at most 2 satisfies $|V \bigcap S| \in L$. Then for every large n, $\exists$ a family $\mathcal{F}$ of size at least $(n/kq)^3$ which is k-uniform and L-intersecting.*

Proof: We choose n_1 such that $n_1 = kq^t$, $t \geq r$ and $n/q < n_1 \leq n$. Let $U = \mathbb{F}_{q^t} = \mathbb{F}_q^t$ i.e., U can be regarded as the field $\mathbb{F}_{q^t}$ as well as a vector space of dimension t over $\mathbb{F}_q$. Let W be a subspace of U of dimension r. By hypothesis, $\exists$ $S \subseteq W$, $|S| = k$ such that every subspace V of W of dimension at most 2 satisfies $|V \bigcap S| \in L$. Therefore, every subspace V_1 of U of dimension at most 2 also satisfies $|V_1 \bigcap S| \in L$. Now we identify $[n_1]$ with the set

$$A = \{(s, x) \mid s \in S,\ x \in \mathbb{F}_{q^t}\}.$$

Our family $\mathcal{F}$ consists of sets F which are in one-to-one correspondence with the triples $(a, b, c) \in \mathbb{F}_{q^t}^3$. The set F corresponding to the triple (a, b, c) is defined as

$$F = \{(s,\ as^{q^2} + bs^q + cs) \mid s \in S\}$$

We have $|F| = |S| = k$. $|\mathcal{F}|$ =number of triples $= (q^t)^3 > (n/kq)^3$. Let F_1, F_2 be any two distinct members of $\mathcal{F}$ corresponding to the triples (a_1, b_1, c_1) and (a_2, b_2, c_2) respectively. We have,

$$|F_1 \bigcap F_2| = |\{s \in S \mid (a_1 - a_2)s^{q^2} + (b_1 - b_2)s^q + (c_1 - c_2)s = 0\}|.$$

We note that the set of solutions of $ay^{q^2} + by^q + cy = 0$ in $\mathbb{F}_{q^t}$ is a vector space of dimension at most 2 over $\mathbb{F}_q$. The reason is, $(x + y)^{q^i} = x^{q^i} + y^{q^i}$, $\lambda^{q^i} = \lambda$ if $x, y \in \mathbb{F}_{q^t}$, $\lambda \in \mathbb{F}_q$, $i \geq 0$. Let V_1 be the space of solutions of $(a_1 - a_2)s^{q^2} + (b_1 - b_2)s^q + (c_1 - c_2)s = 0$ in $\mathbb{F}_{q^t}$ with $dim(V_1) \leq 2$. Then $|F_1 \bigcap F_2| = |V_1 \bigcap S| \in L$ as seen earlier. Hence the family $\mathcal{F}$ is L-intersecting. $\square$

Remark : This theorem can be generalized to obtain a construction of $\Omega(n^s)$ size families. The statement will be
Suppose there exists a set S of k points in space $\mathbb{F}_q^r$, $r \geq s$, such that any subspace V of dimension at most $s-1$ satisfies $|V \bigcap S| \in L$. Then for every large n, $\exists$ a family $\mathcal{F}$ of size at least $(n/kq)^s$ that is k-uniform and L-intersecting.
The proof is the same except that we use the polynomial $d_{s-1}y^{q^{s-1}} + d_{s-2}y^{q^{s-2}} + \ldots + d_0 y$. The set of solutions of this polynomial in any extension field of $\mathbb{F}_q$ is a vector space of dimension at most $s-1$ over $\mathbb{F}_q$.

Theorem 4.2 *If a (k, l) design is embedded in $PG(r, q)$, $r \geq 2$ then, $m(n, k, \{0, 1, l\}) = \Omega(n^3)$.*

Proof: The statement that a (k, l) design is embedded in $PG(r, q)$ is equivalent to saying that there exists a set S of k points in $\mathbb{F}_q^{r+1}$ such that every subspace of dimension at most 2 intersects S at $0, 1$ or l points. Now we apply Theorem 4.1. $\square$

Definition 4.1 *A straight line in space $\mathbb{F}_q^r$ is a subset* $\{\mathbf{v_1} + \alpha\mathbf{v_2} | \mathbf{v_1}, \mathbf{v_2} \in \mathbb{F}_q^r$ are fixed, $\mathbf{v_2} \neq 0,\ \alpha \in \mathbb{F}_q\}$.

Theorem 4.3 *Let $L = \{0, 1, l_3, l_4, \dots\}$ and k be given. Suppose there exists a set S of k points in the affine space $A = \mathbb{F}_q^r$, $r \geq 2$ such that every straight line $\mathcal{L}$ in A satisfies $|\mathcal{L} \bigcap S| \in L$. Then $\exists$ $\Omega(n^3)$ size L-intersecting k-uniform families.*

Proof: We regard A as an affine subspace of $\mathbb{F}_q^{r+1}$ which does not contain the origin. S is a subset of A. By Theorem 4.1, it is sufficient to prove that if V is a subspace of $\mathbb{F}_q^{r+1}$ of dimension at most 2 then $|V \bigcap S| \in L$. If $dim(V)$ is 0, then $V \bigcap S = \emptyset$ since the origin does not belong to S. If $dim(V)$ is 1, then $|V \bigcap S| = 0$ *or* 1 since a straight line passing through the origin can contain at most one point of the affine subspace A. Now let $dim(V)$ be 2. Then V will intersect A at $0, 1$ or q points. If it intersects A at q points, the intersection is a straight line $\mathcal{L}$ in A. This implies $|V \bigcap S| = |(V \bigcap A) \bigcap S| = |\mathcal{L} \bigcap S| \in L$ by hypothesis. □

4.2 Corollaries to the Main Construction

Corollary 4.3.1 *Let $L = \{0, 1, 2\}$, $k > 2$. Then $m(n, k, L) = \Omega(n^3)$.*

Proof: Note that there exist q points in general position in $\mathbb{F}_q^3$, i.e., any 3 of them are linearly independent. Choose $q \geq k$. So $\exists$ a set S of k points in $\mathbb{F}_q^3$ in general position. Any subspace of dimension at most 2 contains at most 2 points from S. Now we apply Theorem 4.1. □

Corollary 4.3.2 *Let $L = \{0, 1, q\}$, $k = q^\alpha$, $\alpha \geq 2$. Then $m(n, k, L) = \Omega(n^3)$.*

Proof: Let $A = \mathbb{F}_q^\alpha$ and S = A. Any straight line in A has exactly q points common with S. Now we apply Theorem 4.3. □

The special case $k = q^2$ of this corollary is mentioned in [1, page 90].

Corollary 4.3.3 *Let $L = \{0, 1, q+1\}$, $k = q^\alpha + q^{\alpha-1} + \dots + q + 1$, $\alpha \geq 2$. Then $m(n, k, L) = \Omega(n^3)$.*

Proof: The design $PG(\alpha, q)$ is a $(q^\alpha + \dots + 1, q + 1)$ design. We apply Theorem 4.2. □

The special case $k = q^2 + q + 1$ of this corollary is mentioned in [1, page 90].

Corollary 4.3.4 *Let $L = \{0, 1, q\}$, $k = 2q^2 - q$ where q is a power of 2. Then $m(n, k, L) = \Omega(n^3)$.*

Proof: When q is a power of 2, there exists a class of $(2q^2-q,q)$ designs embedded in $PG(2,2q)$ known as *Oval Designs.* We apply Theorem 4.2. For a discussion on Oval Designs, please refer to [10, page 90]. $\square$

Corollary 4.3.5 *Let* $L=\{0,1,q+1\}$, $k=q^3+1$. *Then* $m(n,k,L)=\Omega(n^3)$.

Proof: There exists a class of $(q^3+1,q+1)$ designs embedded in $PG(2,q^2)$ known as *Unital Designs.* We apply Theorem 4.2. For a discussion on Unital Designs, please refer to [11, page 177-180]. $\square$

Corollary 4.3.6 *Let* $L=\{0,1,q^2-q,q^2\}$, $k=q^2(q^2-q+1)$. *Then* $m(n,k,L)=\Omega(n^3)$.

Proof: Let S_1 be a set of q^3+1 points in $PG(2,q^2)$ forming the Unital Design. This design has the property that every line in $PG(2,q^2)$ intersects S_1 at 1 or $q+1$ points. Noting that a line in $PG(2,q^2)$ has q^2+1 points, it follows that every line intersects $S=PG(2,q^2)\setminus S_1$ at q^2 or q^2-q points and $|S|=q^2(q^2-q+1)$. Now we apply theorem 4.1. $\square$

Corollary 4.3.7 *Let* $L=\{0,1,l,q\}$, $3\leq l<q$, $k=lq^{\alpha}$, $\alpha\geq 1$. *Then* $m(n,k,L)=\Omega(n^3)$.

Proof: Let $A=\mathbb{F}_{\mathrm{q}}^{\alpha+1}$. A can be partitioned into exactly q disjoint (parallel) affine subspaces of dimension α. Let these be $A_1,\ldots,A_q$. Let $S=A_1\bigcup A_2\bigcup\ldots\bigcup A_l$. Now any straight line in A either lies entirely in one of the A_i's or it contains exactly one point from each of the A_i's. So the line has $0,l$ or q points in common with S. We apply Theorem 4.3. $\square$

Corollary 4.3.8 *Let* $L=\{0,1,q-2,q-1\}$, $k=q^{\alpha}(q-1)^2$, $\alpha\geq 0$. *Then* $m(n,k,L)=\Omega(n^3)$.

Proof: Let $A=\mathbb{F}_{\mathrm{q}}^{\alpha+2}$. Let H_1,H_2 be two distinct hyperplanes in A. Let $S=A\setminus H_1\setminus H_2$. Then any line in A meets S at $0,q-2$ or $q-1$ points and $|S|=q^{\alpha}(q-1)^2$. We apply theorem 4.3. $\square$

Corollary 4.3.9 *Let* $L=\{0,1,q,q+1\}$, $k=q^{\alpha}+q^{\alpha-1}+\ldots+q^{\beta}$, $\alpha>\beta$. *Then* $m(n,k,L)=\Omega(n^3)$.

Proof: Let $U=\mathbb{F}_{\mathrm{q}}^{\alpha+1}$. Let V be a subspace of U of dimension β. Let $S_1=\{\mathcal{L}\mid\mathcal{L}$ is a line passing through origin, $\mathcal{L}\nsubseteq V\}$. It is clear that $|S_1|=q^{\alpha}+q^{\alpha-1}+\ldots+q^{\beta}$. Let S contain exactly one nonzero point on every line in S_1. This implies that every subspace of dimension 2 of U has $0,q$ or $q+1$ points common with S. Now we apply Theorem 4.1. $\square$

4.3 The Second Construction

We get one more construction of k-uniform L-intersecting families using Theorem 2.5. For a set L of integers and a polynomial f, let $f(L) = \{f(l) \mid l \in L\}$.

Theorem 4.4 *Let $f(x) = \sum_{i=0}^{d} \alpha_i \binom{x}{i}$ be a polynomial of degree d where α_i are nonnegative integers. Suppose that for some (L, k), $m(n, k, L) = \Omega(n^s)$. Let $L_1 = f(L)$, $k_1 = f(k)$. Then $m(n, k_1, L_1) = \Omega(n^{s/d})$.*

For example, let $d = 2$, $f(x) = \binom{x}{2}$. We know that $m(n, k, \{0, 1, 2, 3, 4, 5\}) = \Omega(n^6)$ for $k \geq 6$. From Theorem 4.4, we get $m(n, \binom{k}{2}, \{0, 1, 3, 6, 10\}) = \Omega(n^3)$.

Similarly $m(n, \binom{k}{2}, \{0, 1, 3, 6\}) = \Omega(n^{2.5})$. It is an interesting question to determine the correct bound in this case.

4.4 The Third Construction

Let $\mathcal{D}$ be a STS on k points. We use the notation $u \in \mathcal{D}$ and $\{u, v, w\} \in \mathcal{D}$ to denote that u is a point of the STS and $\{u, v, w\}$ is a triple(block) of the STS.

A subsystem of a STS $\mathcal{D}$ is a set $A \subseteq \mathcal{D}$ such that whenever $\{u, v\} \subseteq A$, the unique block in $\mathcal{D}$ containing u and v is contained in A. The empty set, singleton set, a single block and the whole set $\mathcal{D}$ are trivial subsystems. A STS is called reduced if it contains no non-trivial subsystem.

Our construction of $\Omega(n^{2+\epsilon})$ size families is motivated by proof of Theorem 3.2 and a well known construction for a STS on $k_1 k_2$ points given STS on k_1 and k_2 points.

Looking at the proof of Theorem 3.2, (l=3), we see that $\mathcal{B}$ is a $\{0, 1\}$-intersecting family of 3-subsets and members in $\mathcal{F} \setminus \mathcal{F}_0$ are 2-covered by $\mathcal{B}$. So we may attempt to first define $\mathcal{B}$ and then declare $\mathcal{F}$ to be the family of all k-sets which are 2-covered by $\mathcal{B}$. So every $F \in \mathcal{F}$ is a STS. If $F_1, F_2 \in \mathcal{F}$, $F_1 \bigcap F_2$ is a subsystem of F_1. If the STS on F_1 is reduced, it follows that $|F_1 \bigcap F_2| \in \{0, 1, 3\}$. Thus the family $\mathcal{F}$ will be $\{0, 1, 3\}$-intersecting provided the STS on every $F \in \mathcal{F}$ is reduced. In fact, we will require that STS on all $F \in \mathcal{F}$ are isomorphic and reduced.

Now let us present a method of constructing a STS.

Theorem 4.5 *If $\mathcal{D}_1$, $\mathcal{D}_2$ are STS on k_1, k_2 points respectively, there exists a STS $\mathcal{D}$ on k_1k_2 points.*

Proof: Let $\mathcal{D} = \mathcal{D}_1 \times \mathcal{D}_2$ as a set of points. Define blocks of $\mathcal{D}$ as follows.

$$\begin{aligned}\mathcal{D} \quad = \quad & \{\ \{(u,\alpha),(u,\beta),(u,\gamma)\} \mid u \in \mathcal{D}_1, \{\alpha,\beta,\gamma\} \in \mathcal{D}_2\} \ \bigcup \\ & \{\ \{(u,\alpha),(v,\alpha),(w,\alpha)\} \mid \{u,v,w\} \in \mathcal{D}_1, \alpha \in \mathcal{D}_2\} \ \bigcup \\ & \{\ \{(u,\alpha),(v,\beta),(w,\gamma)\} \mid \{u,v,w\} \in \mathcal{D}_1, \{\alpha,\beta,\gamma\} \in \mathcal{D}_2\}.\end{aligned}$$

Note that for $\{u,v,w\} \in \mathcal{D}_1$ and $\{\alpha,\beta,\gamma\} \in \mathcal{D}_2$, there are 6 blocks in $\mathcal{D}$ of the form $\{(u,\alpha),(v,\beta),(w,\gamma)\}$ corresponding to all 6 combinations. It can be verified that these blocks do form a STS. □

Now we give our construction based on reduced STS with large automorphism group.

Theorem 4.6 *Let $\mathcal{D}$ be a reduced STS on k points with automorphism group $\mathcal{A}$. Suppose $|\mathcal{A}| > k^2 - k$. Let $\log_k(|\mathcal{A}| + k) = 2 + \epsilon$ with $\epsilon > 0$. Then $m(n,k,\{0,1,3\}) = \Omega(n^{2+\epsilon})$.*

Proof: We prove by induction on n that for every $[k^n]$, there exists a $\{0,1\}$-intersecting family $\mathcal{B}$ of 3-sets and a family $\mathcal{F}$ of k-sets such that every $F \in \mathcal{F}$ is 2-covered by $\mathcal{B}$ and the STS on F so obtained is isomorphic to $\mathcal{D}$ and $|\mathcal{F}| \geq k^{-(2+\epsilon)}k^{(2+\epsilon)n}$. For any $F_1, F_2 \in \mathcal{F}$, $F_1 \bigcap F_2$ is a subsystem of F_1. Since $\mathcal{D}$ is reduced STS, it follows that $|F_1 \bigcap F_2| \in \{0,1,3\}$.

For $n = 1$, the STS $\mathcal{D}$ itself forms a singleton family $\mathcal{F}$. The family $\mathcal{B}$ is just the set of all blocks of the STS. Assuming the claim for n, we prove it for $n+1$. Let $\mathcal{B}, \mathcal{F}$ be families corresponding to $[k^n]$ with properties described above. We identify $[k^{n+1}]$ with $\mathcal{D} \times [k^n]$. We define $\mathcal{B}_1, \mathcal{F}_1$ corresponding to $[k^{n+1}]$ as follows.

$\mathcal{B}_1$ is defined in a similar manner as in Theorem 4.5.

$$\begin{aligned}\mathcal{B}_1 \quad = \quad & \{\ \{(u,\alpha),(u,\beta),(u,\gamma)\} \mid u \in \mathcal{D},\ \{\alpha,\beta,\gamma\} \in \mathcal{B}\} \ \bigcup \\ & \{\ \{(u,\alpha),(v,\beta),(w,\gamma)\} \mid \{u,v,w\} \in \mathcal{D}, \{\alpha,\beta,\gamma\} \in \mathcal{B}\}\end{aligned}$$

Since $\mathcal{D}, \mathcal{B}$ are $\{0,1\}$-intersecting families of 3-sets, so is $\mathcal{B}_1$. Now we define families of k-sets as follows.

$\mathcal{F}_1^a = \{\ \bigcup_{f \in F}(u,f) \mid u \in \mathcal{D},\ F \in \mathcal{F}\}$

$\mathcal{F}_1^b = \{\ \bigcup_{u \in \mathcal{D}}(u,\sigma(u)) \mid \sigma \in \mathcal{A},\ F \in \mathcal{F},\ \sigma : \mathcal{D} \to F\}$

Note that σ is automorphism of $\mathcal{D}$, and STS on $F \in \mathcal{F}$ is isomorphic to $\mathcal{D}$. So σ can be considered as an isomorphism from $\mathcal{D}$ to F. It can be easily verified that sets in $\mathcal{F}_1^a, F_1^b$ are 2-covered by $\mathcal{B}_1$ and every set in these families has a STS structure isomorphic to $\mathcal{D}$. Let $\mathcal{F} = \mathcal{F}_1^a \bigcup \mathcal{F}_1^b$. Clearly, $|\mathcal{F}_1^a| = k|\mathcal{F}|$, $|\mathcal{F}_1^b| = |\mathcal{A}||\mathcal{F}|$. So $|\mathcal{F}_1| = (|\mathcal{A}|+k)|\mathcal{F}| \geq k^{2+\epsilon}k^{-(2+\epsilon)}k^{(2+\epsilon)n} = k^{-(2+\epsilon)}k^{(2+\epsilon)(n+1)}$. □

Unfortunately, we don't know any good application of Theorem 4.7. For $k = 7$, the STS on 7 points is the design $PG(2,2)$. The group of automorphisms of this STS is the group of projective linear transformations of $PG(2,2)$. Its order is 168. So Theorem 4.7 implies that $m(n, 7, \{0,1,3\}) = \Omega(n^{\log_7 175})$. For $k = 9$, the STS on 9 points is the design $AG(2,3)$. The group of automorphisms of this STS is the group of all invertible affine transformations of $AG(2,3)$. The order of this group is 432. Theorem 4.7 implies that $m(n, 9, \{0,1,3\}) = \Omega(n^{log_9 441})$. But we already know that $m(n, 7, \{0,1,3\})$ and $m(n, 9, \{0,1,3\})$ are both $\Omega(n^3)$.

However, this theorem seems to suggest that in order to have $m(n, k, \{0,1,3\}) = \Omega(n^3)$, it is necessary not only to have a STS on k points, but a STS with a large automorphism group. Future work could be directed in this direction.

Theorem 4.7 can be generalized by removing the restriction that the STS $\mathcal{D}$ be reduced as follows :

Theorem 4.7 *Let $\mathcal{D}$ be a STS on k points with automorphism group $\mathcal{A}$. Suppose $|\mathcal{A}| > k^2 - k$. Let $\log_k(|\mathcal{A}| + k) = 2 + \epsilon$ with $\epsilon > 0$. Let*

$L = \{|A| \mid A \text{ is a subsystem of } \mathcal{D},\ A \neq \mathcal{D}\}$

Then $m(n, k, L) = \Omega(n^{2+\epsilon})$. Note that $\{0,1,3\} \subseteq L$.

The proof of this theorem is essentially the same. □

Chapter 5

Embedding Designs in Projective Plane

The work in this chapter was done independently by us. But the work is not new. The same results with possibly different proofs can be found in the paper [13].

5.1 Embedding Projective Space in Projective Plane

We prove that the design $PG(n,q)$ is embedded in the design $PG(2,q^{n^2})$. We prove this in three steps.

Theorem 5.1 *The design $PG(n,q)$ is embedded in design $AG(n,q^n)$.*

Proof: $PG(n,q)$ can be identified with a set S of non-zero points in $\mathbb{F}_q^{n+1}$ such that every 1-dim subspace of $\mathbb{F}_q^{n+1}$ contains exactly one point of S. For every $t \geq 1$, we have a natural embedding of $\mathbb{F}_q^{n+1}$ in $\mathbb{F}_{q^t}^{n+1}$ and consequently embedding of S in $\mathbb{F}_{q^t}^{n+1}$. We claim that for large enough t, there exists a hyperplane of $\mathbb{F}_{q^t}^{n+1}$ which does not contain any point of S. If on the contrary, every hyperplane contains a point of S, then by counting $\{\ (s,H)\ | s \in S,\ H\ is\ a\ hyperplane\ of\ \mathbb{F}_{q^t}^{n+1}$ containing s$\}$ in two ways, we get,

$$|S| \geq \frac{\#\ hyperplanes\ in\ \mathbb{F}_{q^t}^{n+1}}{\#\ hyperplanes\ containg\ a\ fixed\ non-zero\ point}$$

$$= \frac{(q^{t(n+1)} - 1)/(q^t - 1)}{(q^{tn} - 1)/(q^t - 1)} > q^t$$

So if $t = n$, $|S| = \frac{q^{n+1}-1}{q-1} > q^n$, a contradiction. Thus we can assume that $t = n$ and there is a hyperplane H of $\mathbb{F}_{q^t}^{n+1}$ not containing any point of S. Let H_1 be a hyperplane parallel to H not containing the origin. So for every point of S, the line joining this point to the origin intersects H_1 at a point. Let S_1 be the set of these intersection points. Clearly the design formed by points of S in $\mathbb{F}_{q^t}^{n+1}$ is same as the design formed by points of S_1 in H_1 where H_1 is considered as the affine space $\mathbb{F}_{q^t}^{n}$. □

Theorem 5.2 *The design $AG(n,q)$ is embedded in design $AG(2,q^n)$.*

Proof: We identify $AG(n,q)$ with points in $\mathbb{F}_q^n$. These points can be also identified with elements of $\mathbb{F}_{q^n}$.

Define an injective map $\phi : AG(n,q) = \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}^2$ as $\phi(x) = (x, x^q)$. Note that for any three points $x, y, z \in AG(n,q)$, x, y, z are collinear in $AG(n,q)$ iff $\phi(x), \phi(y), \phi(z)$ are collinear in the affine plane $\mathbb{F}_{q^n}^2$. Thus ϕ defines an embedding of $AG(n,q)$ into $AG(2,q^n)$. □

Theorem 5.3 *The design $AG(2,q)$ is embedded in design $PG(2,q)$.*

Proof: This is usual embedding of affine plane into projective plane which maps the point $(x,y) \in AG(2,q)$ to the point $[1,x,y] \in PG(2,q)$. □

Combining the above three theorems, we see that :

Theorem 5.4 *The design $PG(n,q)$ is embedded in the design $PG(2,q^{n^2})$.*

□

Suppose we want to construct $\Omega(n^3)$ size k-uniform $\{0,1,l\}$-intersecting family of subsets of $[n]$. In order to apply Theorem 4.2, we must try to embed a (k,l) design in some projective space. But Theorem 5.4 implies that an embedding in a projective space is possible iff an embedding in a projective plane is possible. The following theorem gives a necessary and sufficient condition for a design to be embedable in projective plane $PG(2,q)$.

Theorem 5.5 *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a (k, l) design. Let $p_1, \ldots, p_k$ be points of the design and $B_1, \ldots, B_t$ be blocks of the design. Note that $t = \binom{k}{2}/\binom{l}{2}$. This design is embedable in $PG(2, q)$ iff there exists a matrix $M_{k \times t}$ with entries in $\mathbb{F}_q$ with rank 3 over $\mathbb{F}_q$ and $m_{ij} = 0$ iff $p_i \in B_j$.*

Proof: Assume that the design is embedable in $PG(2, q)$.

Let $\{p_i = [x_i, y_i, z_i] | 1 \le i \le k\}$ be the set $\mathcal{P}$ of points. Let $H_1, \ldots, H_t$ be the lines in $PG(2, q)$ such that $|H_j \bigcap \mathcal{P}| = l$. The sets $B_j = H_j \bigcap \mathcal{P}$ form the given design. Let the equation of the line H_j be $a_j x + b_j y + c_j z = 0$. Consider the matrix $M = (m_{ij})$ where $m_{ij} = a_j x_i + b_j y_i + c_j z_i$. So $m_{ij} = 0$ iff the point $p_i = [x_i, y_i, z_i] \in B_j$. The matrix M can be written as a product $M = AB$ where A is a matrix with rows (x_i, y_i, z_i) and B is a matrix with columns $(a_j, b_j, c_j)^t$. It follows that $rank(M) = 3$.

The converse can be proved similarly. □

There are 2 non-isomorphic $(13, 3)$ designs. We proved (by brute force) that the rank of the matrix associated with any of these designs cannot be 3 over any finite field. So none of these designs is embedable in any projective plane. A much simpler proof of this fact is given in [13]. This paper also says that no $(k, 3)$ design is known to be embedable in projective plane except the designs $AG(n, 3)$ and $PG(n, 2)$.

5.2 Embedding the STS on 9 Points

Theorem 5.6 *Let $char(\mathbb{F}_q) \neq 2, 3$. Suppose there exists an elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$ with 9 points on it satisfying $3P = 0$. Then we can select a set S of 9 points in space $\mathbb{F}_q^3$ such that every subspace of dimension at most 2 has $0, 1$ or 3 points in common with S.*

Proof: Let $(x_1, y_1), \ldots, (x_8, y_8)$ be the nonzero points on the curve that satisfy $3P = 0$. Note that these points along with the zero, form a subgroup. Let $S \subseteq \mathbb{F}_q^3$ be defined as

$$S = \{(x_1, y_1, 1), \ldots, (x_8, y_8, 1), (0, 1, 0)\}.$$

The set S has one point on y-axis and 8 points in the plane $z = 1$. The curve lies in the plane $z = 1$. Let us call the points $(x_i, y_i, 1)$ to be the nonzero points in S. Let V be a subspace of dimension at most 2. If $dim(V)$ is 0, $V \bigcap S = \emptyset$. If $dim(V)$ is 1, $|V \bigcap S| = 0$ *or* 1 since no two points in S are collinear with the origin. So we assume $dim(V)$ to be 2. Let $\mathcal{L}$ be the line of intersection of V with the plane $z = 1$.

Suppose V does not contain the y-axis. Then $\mathcal{L}$ is not parallel to the y-axis. We need to prove that $\mathcal{L}$ can't intersect the curve at exactly two nonzero points in S. If $P, Q,\ P \neq Q$ are two nonzero points in S at which $\mathcal{L}$ intersects the curve, the point $R = -(P+Q) \in S$ is also a point of intersection. Since $\mathcal{L}$ is not parallel to $y-$axis, $P + Q \neq 0$ and R is nonzero. Also R is distinct from P and Q because $P = R$ would imply that $P = -(P+Q)\ \Rightarrow 2P + Q = 0\ \Rightarrow P = Q$ since $3P = 0$. This contradicts the assumption that $P \neq Q$.

The case that remains is when V contains the $y-$axis. V contains the point $(0,1,0)$ of S. The line $\mathcal{L}$ is now parallel to the y-axis. We need to prove that this line meets the curve at 0 or 2 nonzero points in S. This is true because if it meets the curve at one point $P \in S$, then $-P$ is also on this line, $3P = 0, P \neq 0$ and hence $P \neq -P$. □

The points on elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{F}$ which satisfy $3P = 0$, are called 3-torsion points. There are exactly 9 of them provided $\mathbb{F}$ is algebraically closed. However we can take a curve over $\mathbb{F}_{\mathrm{q}}$, get all the 3-torsion points in its algebraic closure and then take a suitable extension of $\mathbb{F}_{\mathrm{q}}$ to include all these 3-torsion points. Thus the STS on 9 points is embedded in the projective plane of every characteristic $\neq 2, 3$.

Chapter 6

Conclusion

There are many open problems and most of them appear very difficult. Some of them are listed below.

1. For which values of k, do we have $m(n, k, \{0, 1, 3\}) = \Omega(n^3)$? The first open case is k=13. In spite of our hard efforts, this case is still unanswered.
2. Is the Conjecture 2.1 true ?
3. Are there any more designs embedable in projective plane apart from $PG(n, q)$, $AG(n, q)$, Oval designs and Unitals.
4. If $m(n, k, \{0, 1, a, b\}) = \Omega(n^3)$, is it necessary that there exists a 2-$(k, \{a, b\}, 1)$ design ? That is, a 2-design where the block size can be either a or b.

As suggested by Theorem 4.7, it might help to study existence of Steiner Triple Systems with large automorphism groups.

References

[1] L. Babai, P. Frankl. *Linear Algebra Methods in Combinatorics with Applications to Geometry and Computer Science.* Preliminary Version 2 (Sept. 1992), Dept. of Computer Science, The University of Chicago.

[2] R. Lidl, H. Niederreiter. *Introduction to Finite Fields and their Applications.* Cambridge University Press, 1986.

[3] P. Frankl. *Families of Finite Sets with Three Intersection Sizes.* Combinatorica 4 (1984), 141-148.

[4] L. Babai, P. Frankl. *On Set Intersections.* Journal of Combinatorial Theory A, 28 (1980), 103-105.

[5] M. Deza, P. Erdös, P. Frankl. *Intersection Properties of Systems of Finite Sets.* Proc. London Math. Soc. 36 (1978), 369-384.

[6] P. Frankl. *Families of Finite Sets with Prescribed Cardinalities for Pairwise Intersections.* Math. Acad. Hung. 35 (1980), 351-360.

[7] P. Erdos, R. Rado. *Intersection Theorems for Systems of Sets.* Journal of London Math. Soc. 35 (1960), 85-90.

[8] T. Kirkman. *On a Problem in Combinatorics.* Cambridge Dublin Math. Journal, 2 (1847), 191-204.

[9] P. Frankl. *All rationals occur as exponents.* Journal of Combinatorial Theory A, 42 (1986), 200-206.

[10] W. D. Wallis. *Combinatorial Designs.*

[11] D.R. Hughes and F.C. Piper. *Design Theory.* Cambridge Univ. Press.

[12] R.M. Wilson. *An existence theory for pairwise balanced designs, III : Proof of the existence conjecture.* Journal of Combinatorial Theory A, 18 (1975), 71-79.

[13] M. Limbos. *Projective Embedding of Small Steiner Triple Systems.* Topics on Steiner Systems, Annals of Discrete Mathematics, 7 (1980) 151-173.