Intern Report

Yu-Han Wu

1 Introduction

It was such an honor to be able to have an intern with Dr. Conlon at Caltceh. The research of dr. Conlon mainly focused on extremal combinatorics, graph theory, etc.. Here are some of the things I've learnt during the intern.

2 Research

Being able to attend different courses, such as *Extremal Combinatorics* and *Ramsey Theory* at Caltech provided me a great opputunity to different topics in combinatorics, and there are several interesting things that caught my eyes that I looked into them carefully.

3 Erdös Matching Conjecture(EMC)

First thing that I've learnt about is the Erdös matching conjecture, which I've given a talk to the other students attending the same course. To state the conjecture, we will need some notation:

Notation 3.1. *Given n, k, s three natural numbers. We denote*

$$[n] = \{1, \dots, n\}, \binom{[n]}{k} = \{A \subseteq [n] : |A| = k\}$$

$$\mathcal{A}(k, s) = \binom{[k(s+1)-1]}{k}$$

$$\mathcal{B}(n, k, s) = \left\{ B \in \binom{[n]}{k} : B \cap [s] \neq \phi \right\}$$

Now we can state the actual conjecture:

Conjecture 3.1 (Erdös Matching Conjecture)**.** *Let $n \geq (s+1)k$ and $\mathcal{F} \subseteq \binom{[n]}{k}$. Then $\nu(\mathcal{F}) \leq s$ then*

$$|\mathcal{F}| \leq \max \mathcal{A}(k, s), \mathcal{B}(n, k, s)$$

where $\nu(\mathcal{F})$ is the maximal matching number of $\mathcal{F}$.

From the historical viewpoint, Erdös stated this conjecture after proving the Intersecting Family theorem, which is just a special case where $s = 1$ of this conjecture. And in the same paper, Erdös managed to prove that the conjecture is correct when n is large enough. Then some improvements have been made so that the conjecture is ture when $n \geq 3k^2 s$. After that a groundbreaking result by Frankl makes the conjecture almost always true:

Theorem 3.1 (Frankl)**.** *Given $n \geq (2s+1)k - s$ and $\mathcal{F} \subseteq \binom{[n]}{k}$. If $\nu(\mathcal{F}) \leq s$ then $|\mathcal{F} \leq |\mathcal{B}(n,k,s)|$*

After this theorem has been proved, by exploiting the same method of Frankl, Han proved a result on an universal bound of EMC.

Theorem 3.2 (Han)**.** *Suppose n, k, s are non-negative integers and $\alpha \in (1, 2 - 1/k]$ is a real number such that $n \geq \alpha k(s+1) + k - 1$. Let $\mathcal{F} \subseteq \binom{[n]}{k}$ and $\nu(\mathcal{F}) = s$ then*

$$|\mathcal{F}| \leq \binom{n}{k} - \binom{n-s}{k} + \frac{(2-\alpha)k-1}{\alpha k - 1} s \binom{n-s-1}{k-1}$$

We will need some extra notation for the proof of these theorems.

Notation 3.2. *For a family $\mathcal{F} \subset \binom{[n]}{k}$, its shadow is defined as*

$$\partial\mathcal{F} := \{G \in \binom{[n]}{k-1} : \exists F \in \mathcal{F}, G \subset F\}$$

And for a given s and a set $A \subseteq [s+1]$, we define

$$\mathcal{F}(A) := \{F \in \mathcal{F} : F \cap [s+1] = A\}$$

Given $1 \leq i < j \leq n$, then for a subset $F \subseteq [n]$ and a family of subsets $\mathcal{F} \subseteq \binom{[n]}{k}$ we define the shifting as

$$\sigma_{ij}(F) := \begin{cases} F \setminus \{j\} \cup \{i\} & \text{if } i \notin F, j \in F \\ F & \text{otherwise} \end{cases}$$

$$\sigma_{ij}(\mathcal{F}) := \mathcal{F} \cup \{\sigma_{ij}(F) : F \in \mathcal{F}\}$$

We then say that the family $\mathcal{F}$ is shifted if $\sigma_{ij}(\mathcal{F}) = \mathcal{F}$ for all possible pair of i, j.

The proof of both theorems use the following couple key lemmas

Lemma 3.1. *If $\mathcal{F} \subseteq \binom{[n]}{k}$ and $\nu(\mathcal{F}) = s$, then*

$$s|\partial\mathcal{F}| \geq |\mathcal{F}|$$

We say that the families$\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_{s+1}$ are nested if $\mathcal{F}_{s+1} \subseteq \mathcal{F}_s \subseteq \cdots \subseteq \mathcal{F}_1$ holds and are cross-dependent if there is no choice of $F_i \in \mathcal{F}_i$ such that $F_1, \ldots, F_{s+1}$ are pairwise disjoint.

Lemma 3.2. *Let $\beta \in (0,1)$ and let $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_{s+1} \subseteq \binom{Y}{l}$, be nested, cross-dependent families, $|Y| \geq tl$. Suppose further that $t \geq \beta(2s+1)$, then*

$$|\mathcal{F}_1| + |\mathcal{F}_1| + \cdots + |\mathcal{F}_{s+1}| \leq \frac{s}{\beta}\binom{Y}{l}$$

The proof then follows by the following facts:
First observe that the shifting opertion σ_{ij} does not increase the maximal matching number, i.e. $\nu(\sigma_{ij}(\mathcal{F})) \leq \nu(\mathcal{F})$, hence we may assume that the family $\mathcal{F}$ is shifted.
Second that for any family $\mathcal{F} \subseteq \binom{[n]}{k}$, we have

$$\sum_{S \subseteq [s+1]} |\mathcal{F}(S)| = |\mathcal{F}|$$

and if $S \neq \phi, \{s+1\}$ then we have $|B(n,k,s)(S)| = \binom{n-s-1}{k-|S|}$.
Then by denoting $\mathcal{F}_0 = \mathcal{F}(\phi), \mathcal{F}_1 = \mathcal{F}(\{1\}), \ldots, \mathcal{F}_{s+1} = \mathcal{F}(\{s+1\})$, the question reduces to proving

$$|\mathcal{F}_0| \leq s|\mathcal{F}_{s+1}|$$

$$\sum_{i=1}^{s} |\mathcal{F}_i| + (s+1)|\mathcal{F}_{s+1}| \leq s\binom{n-s-1}{k-1}$$

First follows easily by lemma 2.1 and the fact that $\partial(\mathcal{F}_0) \subset \mathcal{F}_{s+1}$. And to see the second we observe see that $\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_{s+1}$ are nested and cross-dependent since $\mathcal{F}$ is shifted. Hence the second inequality follows by lemma 2.2. And we then have proved the theorem

Surprisingly, we can actually again exploit this same simple idea to prove a tighter bound on n which is done again by Frankl and Kupavskii.

Notation 3.3. *Given n, k, s, we define*

$$m(n,k,s) := \max\left\{|\mathcal{F}| : \mathcal{F} \subset \binom{[n]}{k},\ \nu(\mathcal{F}) \leq s\right\}$$

Theorem 3.3. *There exists an absolute constant s_0, such that*

$$m(n,k,s) = \binom{n}{k} - \binom{n-s}{k}$$

holds if $n \geq \frac{5}{3}sk - \frac{2}{3}s$ and $s \geq s_0$.

Theorem 3.4. *Fix some $1\gamma \leq \frac{5}{3}$. Then there exists s_0, such that the following holds for any $s \geq s_0$. If $n \geq \gamma sk - (\gamma - 1)s$ then*

$$m(n,k,s) \leq \binom{n}{k} - \frac{(\gamma-1)(5k-2)}{2(\gamma k - (\gamma-1))}\binom{n-s}{k}$$

The proof of these theorems are much more difficult and uses some other surprising result proved earlier by Frankl.

Theorem 3.5 (Frankl, 2012)**.** *The EMC is true when $k = 3$.*

4 Sidon Sets

The second subject I've been doing research on is the Sidon sets.

Definition 4.1. *Given a subset $A \subset [n]$, we say that A is Sidon if there is no choice of $a, b, c, d \in A$ such that $a + b = c + d$.*

Given a Sidon set A in $[n]$. Since we know that for every pair of elements of A a, b the sum of them are all distinct, we then get an inequality $\binom{|A|}{2} \leq n$, which gives $|A| = O(\sqrt{n})$. Some rather fundamental results have been established over the years, here are some of the results. First is the upper bound of the largest Sidon sets:

Theorem 4.1 (Upper Bound)**.** *A Sidon set $A \subset [n]$ has size at most $n^{1/2} + n^{1/4} + 1$.*

Proof. *Let $a_1 < a_2 < \cdots < a_r$ be a Sidon set and consider the differences*

$$a_2 - a_1, a_3 - a_2, \ldots, a_r - a_{r-1}$$

$$a_3 - a_1, a_4 - a_2, \ldots, a_r - a_{r-2}$$

$$\vdots$$

$$a_{u+1} - a_1, a_{u+2} - a_2, \ldots, a_r - a_{r-u},$$

where $u = \lfloor n^{1/4} \rfloor$. The kth row contains $r - k$ differences and, since A is a Sidon set, these

$$\sum_{k=1}^{u}(r-k) = ru - \binom{u+1}{2}$$

differences are all distinct. The sum of all these differences is at least

$$\sum_{i=1}^{ru-\binom{u+1}{2}} = \frac{1}{2}\left(ru - \binom{u+1}{2}\right)\left(ru - \binom{u+1}{2} + 1\right).$$

On the other hand, by telescoping, the sum of the differences in the kth row is

$$\sum_{i=r-k+1}^{r} a_i - \sum_{i=1}^{k} a_i < kn,$$

so the sum of all the differences is less than

$$\sum_{k=1}^{u} kn = \binom{u+1}{2} n.$$

That is,

$$\frac{1}{2}\left(ru - \binom{u+1}{2}\right)\left(ru - \binom{u+1}{2} + 1\right) < \binom{u+1}{2} n.$$

Simplifying yields that $r < n^{1/2} + n1/4 + 1$, as required.

We now give some constructions to show the lower bound of Sidon sets.

Example 4.1 (Ruzsa's sets)**.** *We begin with a construction due to Ruzsa. Let theta be a primitive root modulo p and consider the set $A = \{a_t : 1 \leq t \leq p-1\}$ defined by*

$$1 \leq a_t < p^2 - p, a_t \equiv t(mod\ (p-1)), a_t \equiv \theta^t (mod\ p).$$

Note that such an a_t exists by the Chinese remainder theorem. Suppose now that $a_i + a_j = k$, where a_i, a_j are in A and $k \in \mathbb{N}$. Then

$$a_i a_j \equiv \theta^{i+j} \equiv \theta^{a_i + a_j} \equiv \theta^k (mod\ p).$$

But that means that both $a_i + a_j$ and $a_i a_j$ are determined mod p by k. In turn, this easily implies that $\{a_i, a_j\}$ is determined mod p by k.
Suppose now that $a_i \equiv a_{i'} (mod\ p)$. Then

$$\theta^i \equiv a_i \equiv a_{i'} \equiv \theta^{i'} (mod\ p).$$

But since θ has multiplicative order $p-1$, this implies that $i \equiv i' (mod\ (p-1))$ or, by choice of a_i, $a_i \equiv a_{i'} (mod\ (p-1))$. But together with $a_i \equiv a_{i'} (mod\ p)$, this implies that $a_i = a_{i'}$.

Remarque 1. *This construction of Ruzsa gives a lower bound of $(1 - o(1))\sqrt{n}$.*

Example 4.2 (Bose)**.** *We now look at a construction of Bose. Let q be a prime power and θ a multiplicative generator of $\mathbb{F}_{q^2}^*$. We then consider the set*

$$\{a \in [q^2 - 1] : \theta^a - \theta \in \mathbb{F}_q\}.$$

If $a+b=c+d$, then $\theta^a=\theta+a'$, etc., so

$$(\theta+a')(\theta+b')=\theta^{a+b}=\theta^{c+d}=(\theta+c')(\theta+d')$$

or

$$(a'+b'-c'-d')\theta+(a'b'-c'd')=0.$$

Since $\{1,\theta\}$ form a basis for $\mathbb{F}_q^2$ over $\mathbb{F}_q$, we must have $a'+b'=c'+d'$ and $a'b'=c'd'$ in $\mathbb{F}_q$. But then $\{a',b'\}=\{c',d'\}$, which in turn means that $\{a,b\}=\{c,d\}$.

Example 4.3 (Ruzsa)**.** *We now give another construction due to Ruzsa, not nearly as sharp as above, but very different in flavour. Observe first that if p,q,r and s are primes, then the only solutions oto $pq=rs$ are when $\{p,q\}=\{r,s\}$. If we take logs, we get that these are again the only solutions to $\log p+\log q=\log r+\log s$. Unfortunately, these are not integers, so we must round them out somehow. Note first that if $|pq-rs|\geq 1$, then $|\log pq-\log rs|\geq 1/2pq$ (since the derivative of $\log x$ is $1/x$). Consider now all of the $cm/\log m$ primes up to m. Consider now th e set $\{6m^2\log p : p\leq m\}$. Then all the differences between sums of elements from this set are at least 3, since $|\log pq-\log rs|\geq 1/2m^2$ and we have multiplied them by $6m^2$. In particular, if we move each elements $6m^2\log p$ to the nearest integer, the sum $6m^2\log p+6m^2\log q$ changes by at most 1, so $6m^2\log p+6m^2\log q$ and $6m^2\log r+6m^2\log s$ remain at least one apart. That is, we have a Sidon set. Is is a subset of $6m^2\log m$ of size at least $m/2\log m$, so we have a Sidon set of order roughly $n^{1/2}/(\log n)^{3/2}$ in $[n]$.*

We may also consider a generalization of the Sidon set.

Definition 4.2. *A set $A\subseteq[n]$ is said to be a B_k-set if it contains no nontrivial solution to the equation*

$$a_1+\cdots+a_k=b_1+\cdots+b_k,$$

where the trivial solutions are those for which $\{a_1,\ldots,a_k\}=\{b_1,\ldots,b_k\}$.

Remarque 2. *An upper bound is again easy, since we must have that the sum of any k distinct elements of A be different, so $\binom{A}{k}\leq kn$. That is $|A|\leq c_k n^{1/k}$.*

We also give a construction of the lower bound of B_h-sets.

Example 4.4 (Bose-Chowla)**.** *Let t be an element of $\mathbb{F}_{q^h}$ whose minimum polynomial over $\mathbb{F}_q$ has degree h and let θ be a multiplicative generator of $\mathbb{F}_{q^h}^*$. We now consider the set*

$$\{a : \theta^a-t\in\mathbb{F}_q\}.$$

Suppose that $a_1+\cdots+a_h = b_1+\cdots+b_h$. *As before, let* $a_i' = \theta^{a_i}-t, b_j' = \theta^{b_j}-t$. *Then*

$$(t+a_1')\dots(t+a_h') = \theta^{a_1+\cdots+a_h} = \theta^{b_1+\cdots+b_h} = (t+b_1')\dots(t+b_h')$$

Is these two polynomials are distinct, we can subtract them to get a ploynomial of degree at most $h-1$ *for which* t *is a solution, contradicting the choice of* t. *It must therefore be that* $\{a_1', \dots, a_h'\} = \{b_1', \dots, b_h'\}$ *and, consequently,* $\{a_1, \dots, a_h\} = \{b_1, \dots, b_h\}$

4.1 Main Problem

The main question considered during the intern is a slightly modified version of the Sidon set.

Definition 4.3 (Sidon sets on a general group)**.** *Given a (not necessarily abelian) group* G, *a non-abelian* B_h*-set in* G *is a subset* A *of* G *which avoids trivial solution to*

$$a_1 \dots a_h = b_1 \dots b_h$$

where the trivial solutions are those for which $(a_1, \dots, a_h) = (b_1, \dots, b_h)$.

Remarque 3. *By a similar argument as the previous section, we have that for any non-abelian* B_h*-set* $S \subseteq G$, *we have that* $|S| \leq |G|^{1/h}$.

We begin by a theorem due to Odlyzko and Smith.

Theorem 4.2 (Odlyzko, Smith)**.** *For every integer* $h \geq 2$ *and every prime* p *with* $h|(p-1)$, *there is a non-abelian group* G *of order* $|G| = (p^h-1)h$ *and a non-abelian* B_h*-subset* $S \subset G$ *of order* $(p-1)/h$.

The proof of the theorem uses the following lemma.

Lemma 4.1. *For integer* $h \geq 2$ *and every prime* p *with* $h|(p-1)$, *there is a* B_h*-set* A *of order* p *inside the group* $\mathbb{Z}_m$, *where* $m = p^h - 1$, *such that* $pA = A$.

Proof. *Let theta be a primitive element in* $\mathbb{F}_{p^h}$ *and* t *be an element of* $\mathbb{F}_{p^h}$ *whose minimum polynomial has degree* h. *For a fixed* $b \in \mathbb{Z}_m$, *we let*

$$A_b = \{a+b : \theta^a - t \in \mathbb{F}_p\}.$$

The construction of B_h*-sets given in the last section (which remains valid over* $\mathbb{Z}_m$*) is just* A_0. *The sets* A_b *are just translates of this basic set, so they are also* B_h*-sets.*
We now show that if we choose t *and* b *appropriately, we can guarantee that* $pA_b = A_b$. *Note that the requirement is that for every* $a_1 + b \in A_b$ *such that*

$$p(a_1+b) = a_2 + b.$$

But this is equivalent to

$$\theta^{p(a_1+b)} = \theta^{p(a_2+b)}$$

or, writing $\theta^{a_i} = t + a_i'$,

$$\theta^{pb}(t + a_1')^p = \theta^b(t + a_2').$$

But, using $(x + y)^p = x^p + y^p$ *over a field of characteristic* p*, this is just*

$$t^p = \theta^{-(p-1)b}t + \theta^{-(p-1)b}a_2' - a_1',$$

where we used that $(a_1')^p = a_1'$ *since* $a_1' \in \mathbb{F}_p$*. If there are fixed* θ, t *and* b*, such that as* a_1' *varies over* $\mathbb{F}_p$*, then* a_2'*, as given by this equation, also remains in* $\mathbb{F}_p$*, then it must be that* $\alpha = \theta^{-(p-1)b}$ *is also in* $\mathbb{F}_p$*. With this, the equation becomes*

$$t^p = \alpha t + \alpha a_2' - a_1'$$

If this equation holds for even a single pair (a_1', a_2')*, then, for any* a_1'*, there will be an* a_2' *satisfying the equation and the associated set* A_b *will satisfy* $pA_b = A$*.*
We will now show that a suitable choice of t *and* α *exists such that* $a_2' = (a_1' + 1)/\alpha$ *for all* a_1'*. We let*

$$\alpha = \theta^{(p^h-1)/h}.$$

First note that this is in $\mathbb{F}_p$*, since the elements of* $\mathbb{F}_p^*$ *are exactly those elements of the form* $\theta^{(p^h-1)i/(p-1)}$ *and* $h|(p-1)$*. Moreover,* α *is of the form* $\theta^{-b(p-1)}$*, since* $p - 1$ *divided* $(p^h - 1)/h$*. To see this, note that*

$$\frac{p^h - 1}{p - 1} = p^{h-1} + \cdots + p + 1,$$

We claim that over $\mathbb{F}_p$*, this has one linear factor and* $(p - 1)/h$ *irreducible factors of degree* h*. If* $x \in \mathbb{F}_p$ *is a root, then* $x^p = x$ *by Fermat's little theorem, so* $x = -1/(\alpha - 1)$*. Since it is easy to verify that this is not a root of the derivative, it is a simple root and there is one linear factor, as claimed.*
Suppoed now that $x \notin \mathbb{F}_p$ *is a root. Then for its minimal polynomial, all of the elements* $x^p, x^{p^2}, \ldots$ *are also roots. Bute note that*

$$x^{p^2} = (\alpha x + 1)^p = \alpha x^p + 1 = \alpha^2 x + \alpha + 1.$$

By induction,

$$x^{p^r} = \alpha^r x + \frac{\alpha^r - 1}{\alpha - 1}.$$

Since α *is a primitive* h*th root of unity, we see that* $x^{p^r} = x$ *when* $r = h$ *but for no smaller* r*. Hence,* x *is of degree* h *ovver* $\mathbb{F}_q$*, as required.*

We are now done, since we can choose an element t, satisfying the equation $x^p - \alpha x - 1 = 0$ with minimum polynomial over $\mathbb{F}_q$ of degree t. But then, to find a'_2 given a'_1, we just need that

$$1 = t^p - \alpha t = \alpha a'_2 - a'_1$$

or $a'_2 = (a'_1 + 1)/\alpha$, where α is as chosen above.

Now we can give the proof of the theorem.

Proof (Theorem 4.2)**.** *We let G be the permutation group on $m = p^h - 1$ elements generated by rotations of the form*

$$x \to x + a (mod\ m)\ for\ a = 0, 1, \ldots, m-1$$

and scramblings of the form

$$a \to px + a (mod\ m)\ for\ a = 0, 1, \ldots, m-1$$

More explicitly, the set of permutations is

$$x \to p^e x + a (mod\ m)\ for\ e = 0, 1, \ldots, h-1\ and\ a = 0, 1, \ldots, m-1$$

Note that the group has order hm and the hth power of any scramblings is a rotation. More generally, the composition of h scramblings with a-values $a_1, a_2, \ldots, a_h$ is

$$x \to p^h x + (p^{h-1} a_1 + p^{h-2} a_2 + \cdots + a_h)$$

which is actually a rotation, since $p^h = 1 (mod\ m)$.
Now let A be the symmetric B_h-set of order p in $\mathbb{Z}_m$ which was constructed in the lemma. We divide the elements of A into $(p-1)/h$ equivalence classes under this symmetry plus a singleton. We then let S be the collection of scramblings with a's consisting of one element from each equivalence class. And we're done.

Inspired by the theorem above, we started to looking at the maximum size of Sidon sets in a general non-abelian group. The main goal is to prove the following conjecture.

Conjecture 4.1. *Given a group G such that every non-trivial presentation of G has a dimension, then the maximum size of Sidon set in G is rather small,* i.e. *of size at most $|G|^{1/2-\epsilon}$.*

4.2 First attempt

We first looked at an intriguing idea using the methods in the paper *Quasirandom Group* of Gowers [2], which is the following theorem

Theorem 4.3. *Let G be a finite group. Then the following are polynomially equivalent.*

- *For every subset $A \subset G$, the directed Cayley graph with generators in A is c_1-quasirandom.*
- *For every subset $A \subset G$ and every function $f : G \to \mathbb{C}$ that sums to 0, $||A * f|| \leq c_2 n^{1/2} |A|^{1/2}$*
- *Every function f from G to the closed unit disc in $\mathbb{C}$ such that $\sum_g f(g) = 0$ is c_3-quasirandom.*

We will omit the proof here but instead give some key idea behind the proof.
The proof uses the idea of the Cayley graph, which means given a subset $X \subset G$ a bipartite graph $A \cup B$ where $A = G = B$ and $x \in A$ is adjacent to $y \in B$ if there are some $z \in X$ such that $zx = y$. We can then use the double counting technique to count the number of edges in this graph.
Using this idea, we can then again double count the graph, which improves the the upper bound by a constant $\sqrt{2}$.
The reason for this idea is not working is that every Sidon set of G has at most $|G|^{1/2}$ elements, which is no where near the case considered in the original paper of Gowers, in which a subset of size $|G|^{8/9}$ is taken.

4.3 Second attempt

We then tried to look at some more specific groups such as $GL_n(q), SL_n(q),$.
Looking at $GL_n(q)$ and $SL_n(q)$, it is interesting to construct a corresponding function from a Sidon set of $GL_n(q)$ to a Sidon set of $SL_n(q)$. If we are able to do this, then we can focus only on one of them and try to prove the problem.
It is not so easy due to the fact that if we have any $A \in GL_n(q)$ selected as an element of the Sidon set, then any multiplication by a constant of A cannot then not be included, which means that we will need several Sidon sets in $SL_n(q)$ to be able to construct one in $GL_n(q)$.
Lastly, if we consider the ... group W, *i.e.* a subgroup of the revertible upper triangular matrices of dimension 3 with diagonal 1, which are the matrices of the form

$$W = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}$$

We can denote every element X of W by a triplet (a, b, c) corresponding to the unit $(1, 2), (1, 3)$ and $(2, 3)$.
Hence if B is a Sidon set of W, then every pair X, Y of elements of B has a distinct product, which means that if $X = (a, b, c)$ and $Y = (a', b', c')$ we have to have distinct triplet $(a + a', c + c', b + b' + ac')$.
It is then natural to take a two additive Sidon sets S, T of $\mathbb{Z}_p$ and consider

$$B = \begin{pmatrix} 1 & S & D \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}$$

where D is a set to be decided. So now if we take two pair of elements $X = (a, b, c), Y = (x, y, z)$ and $X' = (a', b', c'), Y' = (x', y', z')$ of W, we then have distinct products if $\{a, x\} \neq \{a', x'\}$ or $\{c, z\} \neq \{c', z'\}$. The only case left to consider is when these are equal, but then this is again not so easy, since we will need to have ST to be somewhat regular and this leads to an interest to consider both multiplicative and additive Sidon sets of $\mathbb{Z}_p$. Since this seems to be approaching a rather classic conjecture by Erdös and Szemerédi:

Conjecture 4.2 (Sum-product Conjecture)**.** *For any set $A \subset \mathbb{R}$. One has* $\max(|A + A|, |AA|) \geq |A|^{2-o(1)}$.

We did not try further down this road, since many partial results have been established but it is still nowhere near proving the actual conjecture. We will instead end this section by giving some recent development in this area and hope this will help for further researches.

Theorem 4.4 ([1])**.** *Let h be a natural number, let $A \subset \mathbb{Z}$ be a finite set, and let B and C be the largest additive and multiplicative B_h-sets of A respectively. Then*

$$\max(|B|, |C|) \gg |A|^{\frac{\eta_h}{h}}$$

where $\eta_h \gg (\log \log h)^{1/2-o(1)}$.

Theorem 4.5 ([1])**.** *Let $A \subset \mathbb{Z}$ be a finite set and let $h \geq 3$. Then there exists $g \leq 30h$ and $\delta_h \gg h^{-3}$ such that A contains either a additive B_h-set B or a multiplicative B_h-set C satisfying*

$$\max(|B|, |C|) \gg |A|^{1/2+\delta}$$

5 Euclidean Ramsey Theory

The main subject we've been working on during the intern is the Euclidean Ramsey Theory. Let's start with some definitions,

Definition 5.1. *A finite set $X \subset \mathbb{R}^n$ is said to be* Ramsey *if for every natural number r, there exists $N := N(X, r)$ such that any r-colouring of the points of $\mathbb{R}^N$ contains a monochromatic subset congruent to X.*

This concept is first introduced by Erdos, Graham, Montgomery, Rothschild, Spencer and Straus in a series of seminal papers in the early 1970s [3], [4]. Here are some results established in these two papers.

Lemma 5.1 ([3])**.** *All equilateral triangles are Ramsey.*

Proof. *Consider the collection of $2r+1$ points in dimension $2r+1$ of the form $(0, \ldots, 0, \frac{1}{\sqrt{2}}, 0, \ldots, 0)$. Since any two points are of unit distant, and by the pigeonhole principle, at least 3 points are of the same color. We have a monochromatic equilateral triangle.*

One of the important results found in [3] is that any cartesian product of two Ramsey sets is also Ramsey. More formally, given sets $X \subset \mathbb{R}^m$ and $Y \subset \mathbb{R}^n$, we define their cartesian product $X \times Y$ by

$$X \times Y = \{(x, y) \in \mathbb{R}^{m+n} : x \in X, y \in Y\}$$

Lemma 5.2. *If X and Y are Ramsey, then $X \times Y$ is Ramsey.*

Proof. *Suppose $X \subset \mathbb{R}^m$ and $Y \subset \mathbb{R}^n$. Since X is Ramsey, there exists $M := M(X, r)$ such that any r-colouring of the points of $\mathbb{R}^M$ contains a monochromatic subset congruent to X. By compactness, there exits a finitet subset U of $\mathbb{R}^M$ such that any r-colouring of U contains a monochromatic subset congruent to X. Let $u = |U|$ and let $U = \{x_1, \ldots, x_u\}$. Now choose N such that any r^u-colouring of $\mathbb{R}^N$ contains a monochromatic subset congruent to Y. This is possible since Y is Ramsey. We claim that any colouring of $\mathbb{R}^{M+N}$ contains a monochromatic subset congruent to $X \times Y$.*
To prove the claim, suppose that χ is an r-colouring of $\mathbb{R}^{M+N}$. Define an auxiliary r^u-colouring χ' of $\mathbb{R}^N$ by

$$\chi'(y) = (\chi(x1, y), \ldots, \chi(x_u, y))$$

By the choice of N, there i a monochromatic copy of Y in this colouring . Now define an r-colouring χ'' of U by setting $\chi''(x_i) = \chi(x_i, y)$ for any y in our monochromatic copy of Y (note taht the particular choice is irrelevant). By the choice of U, there is a monochromatic copy of X in this colouring. But this easily lifts to give a monochromatic copy of $X \times Y$.

This theorem in fact proves the following.

Theorem 5.1. *Every triangle is Ramsey.*

The following is the strongest result we can get thus far,

Theorem 5.2 ([3])**.** *All Ramsey sets are spherical.*

The key component of the proof is the following lemma.

Lemma 5.3. *A set $X = \{x_0, \ldots, x_t\}$ is not spherical if and only if there exist c_i for $1 \leq i \leq t$, not all 0, such that*

1. $\sum_{i=1}^{t} c_i(x_i - x_0) = 0$
2. $\sum_{i=1}^{t} c_i(x_i \cdot x_i - x_0 \cdot x_0) = b \neq 0$

As we can see, most of the results are due to the original paper. And hence this leads to an interesting conjecture.

Conjecture 5.1. *All spherical sets are Ramsey.*

5.1 Main Problem

Instead of proving the actual conjecture, we look at a different direction due to the paper [5]. We need the following definition to state the theorem.

Definition 5.2. *Given a positive integer n. Denote the n-dimensional Euclidean space by $\mathbb{E}^n$. Let A, B be two finite sets of points. Then if every red-blue colouring of $\mathbb{E}^n$ contains either a red congruent copy of A or a blue congruent copy of B, then we say $\mathbb{E}^n \to (A, B)$.*
Also, we denote k points on a straight line separated by distance 1 by l_k.

Theorem 5.3 ([5])**.** *There exists a positive constant c' such that $\mathbb{R}^n \to (l_2, K)$, for any $K \subset \mathbb{E}^n$ of size at most $2^{c'n}$.*

This then gives us an intuition to prove the following theorem.

Theorem 5.4. *There exits a positive integer m such that for every positive integer n, $\mathbb{E}^n \nrightarrow (l_3, l_m)$.*

The idea is actually quite simple which uses the method of spherical colouring.

Proof. *Suppose that $a_1, a_2, a_3 \in \mathbb{R}^n$ form a copy of l_3 with $|a_1 - a_2| = |a_2 - a_3| = 1$. If the points are at distances x_1, x_2 and x_3, respectively, from the origin O and the angle xyO is θ, then we have*

$$x_1^2 = x_2^2 + 1 - 2x_2 \cos\theta$$

and

$$x_3^2 = x_2^2 + 1 - 2x_2 \cos\theta$$

Hence we get

$$x_3^2 + x_1^2 = 2x_2^2 + 2$$

Similarly, if $a_1, a_2, \ldots, a_m \in \mathbb{R}^n$ form a copy of l_m with $|a_i - a_{i+1}| = 1$ for all $i = 1, 2, \ldots, m-1$, then

$$x_{i-1}^2 + x_{i+1}^2 = 2x_i^2 + 2$$

for all $i = 2, 3, \ldots, m-1$. Given these observations, our aim will be to colour $\mathbb{R}_{\geq 0}$ so that there is no red solution to $y_1 + y_2 = 2y_3 + 2$ and no blue solution to the system $y_{i-1} + y_{i+1} = 2y_i + 2$ with $i = 2, 3, \ldots, m-1$. Assuming that we have such a colouring χ, we can simply colour a point $a \in \mathbb{R}^n$ by $\chi(|a|^2)$ and it is easy to check that there is no red copy of l_3 and no blue copy of l_m. We have therefor moved our problem to one of finding a colouring χ of $\mathbb{R}_{\geq 0}$ with no red solution to $y_1 + y_2 = 2y_3 + 2$ and no blue solution to the system $y_{i-1} + y_{i+1} = 2y_i + 2$ with $i = 2, \ldots, m-1$. We will define χ by choosing an appropriate colouring χ' of $\mathbb{Z}_q$ for $q = (1 + o(1))m^{1/4}$ a prime number and then setting $\chi(y) = \chi'(\lfloor y \rfloor \bmod q)$ for all $y \in \mathbb{R}_{\geq 0}$. Our aim now is to show that there is a choice for χ' with the required properties. For this, we consider a random red/blue-colouring χ' of $\mathbb{Z}_q$ and show that, for q sufficiently large, the probability that the resulting colouring χ contains either of the banned configurations is small.
Concretely, suppose that $\mathbb{Z}_q$ is coloured randomly in red and blue with each element of $\mathbb{Z}_q$ coloured red with probability $p = q^{-3/4}$ and blue with probability $1 - p$. With this choice, the expected number of solutions in red to any of the equations $y_1 + y_2 = 2y_3 + c$ with $c \in \{1, 2, 3\}$ is at most

$$p^3 q^2 + 9p^2 q < 10q^{-1/4} \leq \frac{1}{2}$$

where we used that there are at most 3 solutions to any of our 3 equations with two of the variables $\{y_1, y_2, y_3\}$ being equal and that q is sufficiently large. Note that if there are indeed no red solutions to these three equations over $\mathbb{Z}_q$, then there is no red solution to $y_1 + y_2 = 2y_3 + 2$ in the colouring χ of $\mathbb{R}$. Indeed, if $y_i = n_i + \epsilon_i$ with $0 \leq \epsilon < 1$, then n_1 is also coloured red and

$$n_{i-1} + n_{i+1} = 2n_i + 2 + 2\epsilon_1 - \epsilon_{i-1} - \epsilon i + 1$$

But $|2\epsilon_i - \epsilon_{i-1} - \epsilon_{i+1}| < 2$, so we must have

$$n_{i-1} + n_{i+1} = 2n_i + c$$

for $c \in \{1, 2, 3\}$. However, we know that there are no red solutions to this equation in our colouring, so there is no red solution to $y_1 + y_2 = 2y_3 + 2$ in the colouring χ.
For the blue configurations, we first observe that if the y_i satisfy the equations $y_{i-1} + y_{i+1} = 2y_i + 2$ with $i = 2, \ldots, m-1$ with $y_1 = a$ and $y_2 = a + d$, then $y_i = a + id + (i^i - i)$. We claim that taken mod q (extended in the natural way to real numbers), at least $q/6$ elements of the sequence $y_1, \ldots, y_m$ lie in

different intervals $[i, i+1)$ *with* $i \in \{0, 1, \ldots, q-1\}$. *This can be done by a delicate approximation which we will omit the proof here.*
Now as in [5], we apply the Milnor-Thom theorem, which we recall.

Theorem 5.5. *For* $M \geq N \geq 2$, *the number of sign patterns of* M *polynomials in* N *variables, each of degree at most* D, *is at most* $\left(\frac{50DM}{N}\right)^N$

We apply this theorem to count the number of ways in which a set of solutions $(y_1, y_2, \ldots, y_m)$ *of our system of equations can overlap the collection of intervals* $[i, i+1)$ *with* $0 \leq i \leq q-1$ *considered mod* q. *Since, over* $\mathbb{R}$, *any solution set spans a length of at most* $2m^2$, *it will suffice to count the number of feasible overlaps with the intervals* $[i, i+1)$ *with* $0 \leq i \leq 2m^2 - 1$. *But the placement of the points are determined by a collection of linear inequalities in* y_1 *and* y_2. *That is, we can take* $N = 2$ *and* $M = 2 \cdot m \cdot 2m^2 = 4m^3$, *since we need to check at most 2 inequalities to check whether each of the* m *points are placed in each of the* $2m^2$ *intervals. Hence, by Milnor-Thom, there are at most* $(8m^3)^2 = 64m^6$. *But now, since at least* $q/6$ *of the* y_i *must be in distinct intervals, the probability that we have a blue solution to our system is at most*

$$64m^6(1 - q^{-3/4})^{q/6} < 1/2$$

for m *sufficiently large. Combined with our earlier estimates for the probability of a red solution to* $y_1 + y_2 = 2y_3 + 2$, *we see that for* m *sufficiently large there exists a colouring with no red* l_3 *and no blue* l_m, *as required.*

In fact, using this idea and the following lemma

Lemma 5.4. *Given two sets of points* X *and* Y, *a positive number* c, *then*

$$\mathbb{E}^n \to (X, Y) \Leftrightarrow \mathbb{E}^n \to (cX, cY)$$

.

We can prove that

Theorem 5.6. *Given a set* $X = \{x_0, x_1, \ldots, x_k\}$ *and* $b \in \mathbb{R}$, $c_i \in \mathbb{Z}$ *for* $1 \leq i \leq k$ *such that*

$$\sum_{i=1}^{k} c_i(|x_i|^2 - |x_0|^2) = b \neq 0$$

then there is a positive integer m *such that*

$$\mathbb{E}^n \nrightarrow (X, l_m)$$

for every positive integer n.

We are then stuck to prove the following problem

Problem 5.1. *Given a non-spherical point set* X, *does there always exist a positive integer* m *such that for every positive integer* n, $\mathbb{E}^n \nrightarrow (X, l_m)$*?*

We thought that the lemma 5.3 might come into use, but if the c_i's are not all rational numbers, we cannot apply the same proof as above.

5.2 Further Development

The consideration so far has been focused on the Euclidean space, which uses the l^2 norm by default. But if we change the norm to l^q with a positive q or to l^∞, we get some interesting results. For example in [6], they proved that every finite set is Ramsey with l^∞-norm.
If we instead consider the l^q-norm with a given positive q, it is already interesting to see if every Ramsey set is spherical.

Problem 5.2. *Is every l^q-Ramsey set l^q-spherical?*

This is true if $q = 2$ (Euclidean) and $q = \infty$ (maximum norm). In fact, if we can prove this is wrong for some q, it might give us some confidence that the conjecture 5.1 might be wrong.
Although we can not yet prove the previous problem, there are some generalization that can be made.

Theorem 5.7. *Every equilateral triangle is l^q-Ramsey.*

Theorem 5.8. *If X and Y are l^q-Ramsey, then $X \times Y$ is also l^q-Ramsey.*

Theorem 5.9. *Every triangle is l^q-Ramsey.*

These all follow from the proof of the original theorem on Euclidean space.

6 Conclusion

It has been an interesting intern in California at Caltech with Dr. Conlon. Being able to do some research with him is such a delightful experience, and this really widens my view. Also meeting some of the students at Caltech is really fun to be able to share our experience to each other. Above all, Euclidean Ramsey theory has become one of my favorite subject once I've learnt it. On top of that, proving a new result in Euclidean Ramsey theory is just a cherry on top of the cake, which is something that I didn't even think of before the intern. Hope that our result might be useful in further development in this area.

References

[1] Yifan Jing and Akshat Mudgal, 2022, *'Finding large additive and multiplicative sidon sets in sets of integers'*, arxiv:2203.13174v1.

[2] W. T. Gowers, 2007, *'Quasirandom groups'*, arXiv:0710.3877v1

[3] Erdos, Graham, Montgomery, Rothschild, Spencer and Straus, 1973, *'Euclidean Ramset Theorem I'*, Journal of Combinatorial Theory (A), vol. 14, pp. 341-363

[4] Erdos, Graham, Montgomery, Rothschild, Spencer and Straus, 1973, *'Euclidean Ramset Theorem II'*, Colloquia mathematica Societatis Janos Bolyai

[5] David Conlon and Jacob Fox, *Lines in Euclidean Ramsey Theory*, Discrete Comput. Geom. 61, pp. 218-225

[6] Andrey Kupavskii and Arsenii Sagdeev, *All finite sets are Ramsey in the maximum norm*, Forum of Mathematics, Sigma (2021), Vol. 9:e55 112