# Polymath Report

Arpon Basu

March 7, 2023

## Contents

# 1 Introduction

Recently, in an exciting new development by Mubayi and Verstraete [3], it was established that the existence of optimally pseudo-random graphs would also determine the asymptotic behavior of the off-diagonal Ramsey numbers upto a poly-log factor, which would be a breakthrough in the field of Ramsey Theory, where otherwise progress has been slow. Stated a bit more precisely, consider a $(n, d, \lambda)$ regular graph, ie:- a $d$-regular graph on $n$ vertices, the second largest eigenvalue of which has magnitude $\lambda$. By the Alon-Bopanna bound [4], we know that $\lambda = \Omega(\sqrt{d})$.
Now, a $(n, d, \lambda)$ regular graph is called *optimally pseudo-random* if $\lambda = \mathcal{O}(\sqrt{d})$. Using the expander mixing lemma, it is possible to show that if an optimally pseudo-random graph is $K_s$-free, ie:- doesn't have any graph isomorphic to $K_s$ as its subgraph, then it must satisfy $d/n = \mathcal{O}(n^{1/(2s-3)})$. It is here that Mubayi and Verstraete came in and showed that if one can construct pseudo-random graphs with $d/n = \Theta(n^{1/(2s-3)})$, then that would imply that the Ramsey number $R(s,t)$, with $s$ being a constant and $t \to \infty$, would be $\mathcal{O}(t^{s-1}/\log^{k(s)} t)$, with $k(s) \in [s-2, 2s-4]$. This would be due to the inequality, that if we have a $K_s$-free optimally pseudo-random graph with $d/n = \Omega(n^{-1/f(s)})$, then

$$\Omega\left(\frac{t^{\frac{f(s)+1}{2}}}{\log^{f(s)-1} t}\right) \leq R(s,t) \leq \mathcal{O}\left(\frac{t^{s-1}}{\log^{s-2} t}\right)$$

Thus constructing optimally pseudo-random graphs has direct ramifications on bounds in Ramsey theory. Moreover, even if the exact bound of $2s-3$ is not achieved, improving the density of our pseudo-random graph directly improves lower bounds of $R(s,t)$, and thus is a valuable gain in itself.
Thus, constructing families of optimally pseudo-random graphs with high densities was the larger backdrop under which this project was conducted. Now, all existing constructions of such graphs came from the context of *finite geometry*: The graphs that arise in these situations are "nice" in the way we want them to be.
Thus, we will first study these constructions and some of their properties. Then, for specific graphs in these families, we will try and locate some small Ramsey graphs inside them, so that we can build a corpus of specific cases to give us intuition into what might be happening in the general case. So off we go!

# 2 Notation and Convention

Unless specified otherwise, in the subsequent report, $p$ will denote a prime and $q$ denotes a prime power. Also, in all of the constructions below, let $\mathbb{F}_q$ be the finite field containing $q$ elements.
The complete graph with $\ell$ vertices is denoted as $K_\ell$.
Coming to Ramsey numbers, we usually define, for $s, t \in \mathbb{N}$, the Ramsey number $R(s,t)$ to be the minimum number $n$ such that the graph $K_n$, whose edges are

colored arbitrarily with two colors (say red and blue), either has a red $K_s$ or a blue $K_t$ as its subgraph. For this report, we change our perspective slightly to avoid a reference to colorings: We say $R(s,t) = n$ if *any* graph of $n$ vertices either has a clique of $s$ vertices, or an independent set of $t$ vertices. Consequently, $R(s,t) = n$ implies that there exists a $K_s$-free graph on $n-1$ vertices which doesn't have an independent set of size $t$.
For any graph $G$, we also define $\omega(G)$ to be the size of the largest clique contained in it, and $\alpha(G)$ to be the size of the largest independent set contained in it.

# 3 Acknowledgements

This project was done under the aegis of the Polymath Jr. REU of 2022, under the guidance of Prof. Anurag Bishnoi. Not all of the ideas presented here are my original contributions, as this report is intended to be the work done as a whole during the project, including work done by other attendees.
I would in particular like to mention Declan Stacy, who came up with many abstract algebraic insights.
I apologize in advance if I failed to (specifically) mention the contribution of any other person: In any case, I reiterate that not all of the results here are my contributions.

# 4 Constructions

Our main reference for this section is [1].

## 4.1 Conlon-Ferber

For this family of graphs, let $n = 2k$ be an even integer. Our vertex set $V$ is then defined as

$$V := \{v \in \mathbb{F}_2^n \setminus \{\mathbf{0}\} : v \cdot v = 0\}$$

ie:- the set of all non-zero self-orthogonal $n$-dimensional vectors over $\mathbb{F}_2$. Note that a vector $v \in \mathbb{F}_2^n$ belongs to $V$ only if it has an even number of ones among its entries.
Two vertices $v_1, v_2$ in $V$ are connected if $v_1 \cdot v_2 = 1$. Then

**Proposition 1.** *The graph defined above contains no cliques of size $n$.*

*Proof.* Note that $V' := V \cup \{\mathbf{0}\}$ is a subspace of $\mathbb{F}_2^n$ of dimension $n-1$ (we choose the first $n-1$ coordinates arbitrarily, the last coordinate is then fixed by parity considerations. Also, it's easy to see that if $u \cdot u = v \cdot v = 0$, then $(u+v)\cdot(u+v) = u \cdot u + v \cdot v + 2u \cdot v = 0 + 0 + 0 = 0$).
Now, assume for the sake of contradiction that $\mathcal{B} := \{v_1, v_2, ..., v_n\} \subseteq V$ form a $K_n$ among themselves. Since they reside in a subspace of dimension $n-1$, we

get that the vectors in $\mathcal{B}$ are linearly dependent. Thus, say, $v_n$ is expressible as the sum of $\ell$ other $v$'s in $\mathcal{B}$. Then

$$v_n := \sum_{i=1}^{\ell} v_{k_i} \implies v_n \cdot v_n := \sum_{i=1}^{\ell} v_{k_i} \cdot v_n \implies 0 = \ell \bmod 2$$

Thus $\ell$ is even, and thus $\mathcal{C} := \{v_n, v_{k_1}, ..., v_{k_\ell}\}$ is a set of odd cardinality. But since $n$ is even, we have that $\mathcal{B} \setminus \mathcal{C}$ is non-empty. Let $v \in \mathcal{B} \setminus \mathcal{C}$. Then

$$v_n \cdot v := \sum_{i=1}^{\ell} v_{k_i} \cdot v \implies 1 = \ell \bmod 2$$

which implies that $\ell$ is odd, leading to a contradiction. □

However, the plain dot product gives rise to some degeneracies: Indeed, consider the vector $w := \mathbf{1} \in V$, ie:- the vector all of whose entries are 1. Then $w$ isn't connected to any other vector in $V$, since all of them have an even number of ones in them, and thus their dot product with $w$ is 0.

To resolve this issue, we introduce a new **bilinear form** $\beta$ (which we also call a "symplectic form"), which is defined as

$$\beta : \mathbb{F}_2^{2k-2} \times \mathbb{F}_2^{2k-2} \mapsto \mathbb{F}_2$$

$$\beta(x, y) := \sum_{i=1}^{k-1} (x_{2i-1}y_{2i} - x_{2i}y_{2i-1})$$

Thus, the vertex set of our graph $G$ remains the same, but two vertices $v_1, v_2 \in V$ are now adjacent if $\beta(v_1, v_2) = 1$.

A key point to be noted about $\beta$ is that the entire linear-algebraic proof of the even-town theorem, for which our "bilinear function" was the ordinary dot product, carries over verbatim for $\beta$. Thus, the eventown theorem holds for $\beta$ too, ie:- let $\mathcal{W}$ be a set of vectors in $\mathbb{F}_2^{2k-2}$ such that $\beta(w_1, w_2) = 0$ for any $w_1, w_2 \in \mathcal{W}$. Then $|\mathcal{W}| \leq 2^{k-1}$. If we only allow non-zero vectors in $\mathcal{W}$, then $|\mathcal{W}| \leq 2^{k-1} - 1$.

But in the context of our graph $G$, an "even-town" corresponds to an independent set, and thus $\alpha(G) = 2^{(n-2)/2} - 1$ [1], where $\alpha(G)$ denotes the size of the largest independent set in $G$.

Finally, to top it up, we prove that $G$ is regular too.

**Proposition 2.** *$G$ is regular.*

*Proof.* For any $v = [x_1\ x_2\ \ldots x_{2k-3}\ x_{2k-2}] \in \mathbb{F}_2^{2k-2}$, define $v_\# := [x_2\ x_1\ \ldots x_{2k-2}\ x_{2k-3}]$, such that $\beta(u, v) = u \cdot v_\# = u_\# \cdot v$.

For any non-zero vector $v$, $v_\#$ has atleast one 1 as its, say $i^{\text{th}}$ coordinate. Then for any vector $w$ such that $v_\# \cdot w = 1$, we can arbitrarily choose all but the $i^{\text{th}}$ coordinates of $w$, and once we do that, the $i^{\text{th}}$ coordinate of $w$ is automatically

[1] its easy to verify that equality is achieved

fixed.
Thus, the graph is regular, and the degree of regularity is $d = 2^{n-3}$, and by the Delsarte-Hoffman bound,

$$\lambda \geq 2^{(n-4)/2} \implies \lambda = \Omega(\sqrt{N})$$

$\square$

Thus, the Conlon-Ferber graph is an optimally pseudo-random graph, with $(N, d, \lambda) = (2^{n-2} - 1, 2^{n-3}, \Omega(\sqrt{N}))$.

## 4.2 Kopparty

Apart from [1], we also refer to [2] for this section.
For $s = 3$, a construction by Kopparty achieves the best possible bound posited by Mubayi and Verstraete, ie:- it is a triangle-free optimally pseudo-random graph, and consequently, it gives a lower bound of $\Omega(t^2/(\log t)^2)$ for $R(3,t)$, which differs only logarithmically from the actual value, $\Theta(t^2/\log t)$.
So without ado, let's see what it is. However, before presenting the Kopparty graph, we first build its "skeleton".

**Definition 1.** *Consider the field $\mathbb{F}_q$ for any prime power $q$. Define $D := \{(1, u, u^2) : u \in \mathbb{F}_q\}$. Define the undirected graph $G$ with vertex set $\mathbb{F}_q^3$, and the edge set*

$$E := \{\{x, y\}, x, y \in \mathbb{F}_q^3 : x - y = \alpha \cdot d, \alpha \in \mathbb{F}_q, d \in D\}$$

*We call this graph the "pre-Kopparty" graph for easy reference.*

The graph satisfies an interesting property: Triangles in $G$ correspond to lines in $\mathbb{F}_q^3$. Indeed,

**Lemma 4.1.** *Let $(u, v, w)$ form a triangle in $G$. Then there exists $d \in D$ such that $u - v = \alpha_1 \cdot d, v - w = \alpha_2 \cdot d, w - u = \alpha_3 \cdot d$, for some $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q$.*

*Proof.* Since $u, v, w$ are connected to each other in $G$, there exist $d_1, d_2, d_3 \in D$ such that $u - v = \alpha_1 d_1, v - w = \alpha_2 d_2, w - u = \alpha_3 d_3$. Then, since $(u - v) + (v - w) + (w - u) = 0$, we get that $\alpha_1 d_1 + \alpha_2 d_2 + \alpha_3 d_3 = 0$, implying

$$\begin{bmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \tag{1}$$

where $d_i = (1, x_i, x_i^2)$. But if $x_1, x_2, x_3$ are all distinct, then the $3 \times 3$ matrix in the above equation is invertible, and thus can't send a non-zero vector like $[\alpha_1 \ \alpha_2 \ \alpha_3]^T$ to 0. Thus, atleast two of $x_1, x_2, x_3$, say $x_1$ and $x_2$, must be equal, ie:- $x_1 = x_2 = x$. But then if $(u - v) = \alpha_1 d$ and $(v - w) = \alpha_2 d$, then $(u - w) = (\alpha_1 + \alpha_2)d = -\alpha_3 d_3$, thus showing that all the vectors are separated by multiples of some same vector $d$. $\square$

Thus, every triangle in $G$ corresponds to a line in $\mathbb{F}_q^3$. Consequently, we get that **every clique in $G$ must correspond to a line in $\mathbb{F}_q^3$, whose direction is in $D$**. Since any two distinct lines in $\mathbb{F}_q^3$ can share at most one point among themselves, we also get that any two cliques $C_1, C_2$ such that $C_1 \not\subset C_2, C_2 \not\subset C_1$ **don't share an edge**, as sharing an edge amounts to their corresponding lines sharing two points. Consequently, all maximal cliques in $G$ correspond to non-intersecting lines in $\mathbb{F}_q^3$.
Having set up the skeleton, we now move on to construct the actual Kopparty graph. But before that, some definitions.

**Definition 2** (Absolute Trace)**.** *For any finite field $\mathbb{F}_q$, where $q = p^n$, one can define the trace map*

$$\mathrm{tr} : \mathbb{F}_q \mapsto \mathbb{F}_p : x \mapsto \sum_{k=0}^{n-1} x^{p^k}$$

**Definition 3** (Cayley Graphs)**.** *Let $H$ be a group, and let $S \subset H$ be a symmetric subset of this group, ie:- if $s \in S$, then $-s$ also belongs to $S$ [2]. Then the Cayley graph $\mathrm{Cay}(H, S)$ is an undirected graph whose vertex set is $H$, and whose edges are given by*

$$E := \{\{x, y\} : x - y \in S\}$$

*Note that a Cayley graph is a $|S|$-regular graph.*

**Definition 4** (The Kopparty Graph)**.** *Let $q = 2^h$, and consider the set*

$$S := \{a(1, u, u^2), a, u \in \mathbb{F}_q^\times : \mathrm{tr}(au^{-1}) = 1\}$$

*The Kopparty graph $G'$ is then the Cayley graph $\mathrm{Cay}(\mathbb{F}_q^3, S)$, ie:- an undirected graph defined with vertex set $\mathbb{F}_q^3$, and the edge set*

$$E := \{\{x, y\}, x, y \in \mathbb{F}_q^3 : x - y \in S\}$$

*Note that $G'$ is a subgraph of $G$.*

We prove that the Kopparty graph is an optimally pseudo-random triangle-free graph.

**Lemma 4.2.** *$G'$ is triangle-free.*

*Proof.* Let $x, y, z$ form a triangle in $G'$. Then, since $G'$ is a subgraph of $G$, $x, y, z$ are collinear in $\mathbb{F}_q^3$. Consequently, $x - y = a(1, u, u^2), y - z = b(1, u, u^2)$ and $z - x = c(1, u, u^2)$ for some $u \in \mathbb{F}_q^\times$. Moreover, we also have $\mathrm{tr}(au^{-1}) = \mathrm{tr}(bu^{-1}) = \mathrm{tr}(cu^{-1}) = 1$, implying that $\mathrm{tr}((a + b + c)u^{-1}) = 1 + 1 + 1 = 1$. On the other hand, $0 = (x - y) + (y - z) + (z - x) = (a + b + c)(1, u, u^2)$ implies that $a + b + c = 0$, leading to a contradiction. $\square$

To establish the pseudo-randomness of $G'$, we need to calculate its eigenvalues. The proof of this lemma, however, requires the knowledge of Cayley graphs and representation theory, and thus we shall not present it here.

**Theorem 4.3.** *$G'$ is a $(n, d, \lambda)$ graph with $n = q^3, d = (q - 1)^2, \lambda = 3q$.*

[2] we are presenting the group in additive notation

# 5 Some Small Cases

Now that we have seen many constructions, we arrive at the main goal of the program, which was to hunt small Ramsey graphs inside the above constructions. Even this wasn't easy, but various techniques were developed, and some intuition was built to aid the search.
Before that, we present a small bit of notation: Suppose we are given two numbers $s, t$ such that $R(s,t) > k$ for some $k$. Then we define

$$R(s,t,k) := \{\mathcal{G}, |\mathcal{G}| = k : \mathcal{G} \text{ is a } K_s\text{−free graph with no independent set of size } t\}$$

In other words, $R(s,t,k)$ is a (possibly singleton) set of graphs which *demonstrate* that $R(s,t) > k$. In case $R(s,t,k)$ is a singleton, we use abuse notation slightly and use the term $R(s,t,k)$ to refer to the (unique) graph it contains.
For example, $R(4,4,17)$ is the famous *Paley graph* on 17 vertices whose clique-number is 3, and whose independence number is 3 as well. Moreover, the Paley graph is the *unique* graph on 17 vertices which is Ramsey-demonstrating, ie:- $|R(4,4,17)| = 1$. The graph is constructed with $\mathbb{F}_{17}$ as its vertex set, and the edge set is given by [3]

$$E := \{\{x,y\} : x - y \text{ is a non} - \text{zero quadratic residue in } \mathbb{F}_{17}\}$$

The above graph has other very nice properties: For starters, it is *self-complementary* (ie:- isomorphic to its complement [4]) and *strongly regular* (ie:- every vertex has the same degree, and every pair of non-adjacent vertices have the same number of mutual neighbors). Due to its high symmetry and other properties, it shows up in many variants of the Conlon-Ferber constructions.
We now describe some methods used to hunt Ramsey-graphs down.

## 5.1 Brute-Force Search

Although specialized techniques aid one a lot when graphs become large, in many small cases it is directly possible to search for the desired graphs. Indeed,

1. Take the usual Conlon-Ferber construction (defined with the symplectic form $\beta$) on $\mathbb{F}_2^8$. Then one can locate $R(4,4,17)$ in this by a direct **brute force search**. One may further note that $R(4,4,17)$ is an *induced subgraph* of the Conlon-Ferber construction.

2. Consider the pre-Kopparty graph on $\mathbb{F}_9$, ie:- with the vertex set $\mathbb{F}_9^3$. Then $R(3,5,13)$ is an induced subgraph of this graph [5].

[3] Since $17 \equiv 1 \bmod 4$, $x - y$ is a quadratic residue if and only if $y - x$ is, since $-1$ is a square in $\mathbb{F}_{17}$, and thus the definition is symmetric. Moreover, this definition can be extended for any prime power $q \equiv 1 \bmod 4$

[4] here by the complement of a graph $G = (V,E)$ we mean $(V, \mathcal{V} \setminus E)$, where $\mathcal{V} = \{\{v_1, v_2\} : v_1, v_2 \in V, v_1 \neq v_2\}$

[5] $R(3,5,13)$ is a singleton set

3. Consider the following construction: Let $G_q$ be the graph whose vertex set is the set of all one-dimensional subspaces of $\mathbb{F}_q^4$, with two vertices $\langle u\rangle, \langle v\rangle$ being adjacent if $\beta(u,v)=0$, where $\beta$ is our usual symplectic form.
Then $R(3,5,13)$ is a subgraph of $G_8$ (defined on $\mathbb{F}_8^4$).

## 5.2 Random Hill Climbing

Even though $R(4,4,17)$ is discoverable through a direct brute force search, it is worthwhile to describe another search technique, which we call **Random Hill Climbing**: The basic crux of the technique is to randomly sample 17 vertices (let the induced subgraph generated thus be $G'$), and calculate the clique and independence numbers of $G'$. If they're both less than 4, then we have found our graph and we can stop. Otherwise, let $C$ be the largest clique in our graph. Randomly delete a vertex $v$ from $C$. Then, iterating over all vertices in our graph, find the vertex $u$ which minimizes $\max\{\omega(G'-v+u), \alpha(G'-v+u)\}$. If there are multiple such $u$'s, then break the tie by calculating which vertex induces the minimum number of maximum-sized cliques/independent sets [6], and if there is a tie after this stage too, break that tie arbitrarily. Finally, the algorithm is executed until our desired subgraph is found.
Heuristically, it is not too difficult to see why the above algorithm works: It makes a greedy choice at every step, and it is designed in a way that it doesn't get "trapped" in local minima [7].

## 5.3 Via Insights from Abstract Algebra

Sometimes brute force search may be aided by insights from abstract algebra, as happened for the cases mentioned below:

1. We identify $\mathbb{F}_2^8$ with $\mathbb{F}_{256}$, and consequently, construct a graph with the vertex set as $\mathbb{F}_{256}^\times$, and edge set given by [8]

$$E := \{\{x,y\} : \mathrm{tr}(xy^{16}) = 1\}$$

   Now note that the elements of $\mathbb{F}_{256}^\times$ form a multiplicative group $G$ of order 255, and this group is cyclic [9]. Consequently, let $H$ be the subgroup of $G$ of order 17. Then it turns out that the subgraph induced by $H$ on $G$ is $R(4,4,17)$!

2. Similar to the above, consider the multiplicative group formed by elements of $\mathbb{F}_{2^{12}}^\times$ and consider the subgroup $H$ having 13 elements. Then, build a

[6] ie:- if $G'-v+u_1$ has 5 maximum cliques, while $G'-v+u_2$ has 4 maximum independent sets, then we choose $u_2$ over $u_1$

[7] some other heuristic algorithms which were experimented with suffered this issue: For example, one of them got stuck with a clique number of 3 and an independence number of 4, and was not able to improve in subsequent iterations of the algorithm

[8] this construction is symmetric too

[9] Since 255 is co-prime to its Euler totient function, it is a cyclicity forcing number, ie:- any group of order 255 is cyclic

graph on it, with the edge indicator function being given by $\beta(x, y) := \mathrm{tr}(cxy^{2^6})$, where $c \in \mathbb{F}_{2^6}^{\times}$. It turns out that for a specific value of $c$, the graph generated by these 13 vertices is $R(3, 5, 13)$! Thus a larger brute force over $\mathbb{F}_{2^{12}}^{\times}$ is reduced to a search on $\mathbb{F}_{2^6}^{\times}$.

## 6 Conclusion

As stated in the report, one of the main objectives of the project wa to build a corpus of small Ramsey graphs in geometric constructions for gaining insight. In that respect, the project was a success, as many small Ramsey graphs were indeed located in the Conlon-Ferber, pre-Kopparty and other constructions. Some neat abstract algebraic explanations were also found for some of these things.
However, from a larger point of view, much remains to be done, in that these small observations need to be placed in a general context, and explained as part of a larger pattern. The final goal of all this is to eventually achieve the Mubayi-Verstraete goal of finding dense pseudo-random graphs.

## References


[1] Anurag Bishnoi. *Finite Geometry and Ramsey Theory*. URL: https://anuragbishnoi.files.wordpress.com/2021/01/minicourse.pdf.

[2] Swastik Kopparty. *Cayley Graphs*. URL: https://sites.math.rutgers.edu/~sk1233/courses/graphtheory-F11/cayley.pdf.

[3] Dhruv Mubayi and Jacques Verstraete. "A note on pseudorandom Ramsey graphs". In: (2019). URL: https://arxiv.org/pdf/1909.01461.pdf.

[4] A. Nilli. "On the second eigenvalue of a graph". In: (1991). URL: https://doi.org/10.1016%2F0012-365X%2891%2990112-F.