The Polynomial Method in Combinatorics

Alexander Milner

April 2024

Abstract

The polynomial method aims to solve combinatorial problems by encoding their structure in carefully-constructed polynomials and then analysing the sets on which said polynomials vanish. The method has only begun to be formalised in the last 25 years and has garnered attention by providing relatively short and simple solutions to long-standing problems.

In this report, we first aim to give a well-rounded representation of the polynomial method by exploring a range of problems from extremal combinatorics. We include arguably the most well-known results which use the polynomial method; Dvir's proof of the Finite Field Kakeya Conjecture and Ellenberg and Gijswijt's cap set bound, where, in doing so, we also explore Tao's symmetric reformulation of the Croot-Lev-Pach Lemma. We then explore some of the many applications of the Combinatorial Nullstellensatz, where we extend a result from Alon's original paper [Alo99] about k-colourings of hypergraphs.

Finally, letting S_{n^2} act on the elements of an $n \times n$ matrix by permutation, we investigate when a matrix can be permuted by elements in certain subsets of S_{n^2} such that it is invertible. To do this, we generalise and extend a result, based on the Combinatorial Nullstellensatz, by Brauch, Kézdy and Snevily and we use this, in particular, to give an exact condition on when n^2 elements of a field can be rearranged to form an invertible matrix.

Plagiarism Declaration

This piece of work is a result of my own work except where it forms an assessment based on group project work. In the case of a group project, the work has been prepared in collaboration with other members of the group. Material from the work of others not involved in the project has been acknowledged and quotations and paraphrases suitably indicated.

Acknowledgements

I would like, particularly, to thank my supervisor Dr. Dan Evans for his constant guidance, enthusiasm and support during my time working on this report. Working and researching under his supervision has fueled my interest in a myriad of topics in and around the polynomial method which I will cherish greatly as I continue my academic career with the start of a PhD in Edinburgh this coming autumn.

Contents

Introduction

Combinatorics is the branch of mathematics traditionally associated with counting. It shows up in almost every other area of mathematics and, as a result, has only been considered an area of mathematics in its own right since the late 20th century, much more recently than other more traditional staples of the mathematical curriculum. Due to its incredibly broad reach into other areas of mathematics and applications to computer science, combinatorics is now a flourishing area of mathematical research.

In a similar vein, methods incorporating the vanishing properties of polynomials had been in use decades before the term *the polynomial method* was coined in the 1990s by Alon, referring to applications of his theorem, the Combinatorial Nullstellensatz from [Alo99]. This was the case particularly in the area of number theory where Baker's theorem and Stepanov's method used key insights about the zero sets of well-constructed polynomials in the 1960s, as covered in Chapter 4 of [Tao14]. Arguably, however, it was Dvir's 2-page proof of the Finite Field Kakeya Conjecture in 2008, [Dvi08], using a relatively basic argument that brought the polynomial method to the attention of many. In a comment from 2010 on `mathoverflow.net`, [Tao10], Tao remarks that Dvir's short proof of the Finite Field Kakeya Conjecture came as shock to those who had been working on the problem, him included, as it had been thought to be a fairly intractable problem.

Since 2008, a number of texts covering different aspects of the polynomial method have appeared and many textbooks and lecture series in combinatorics now contain a chapter dedicated to the polynomial method. However, as Tao notes in his survey article from 2014, [Tao14], the capabilities of the polynomial method are still fairly unknown, making great leaps in some directions and very little progress in others.

The two key areas in which the polynomial method has been developed furthest are extremal combinatorics, where we focus on bounding the size of finite sets with given properties, and combinatorial geometry, where we study discrete geometric objects. Although we will not cover polynomial methods in combinatorial geometry in this report, they are an incredibly rich area of research. Notable successes include Guth and Katz's proof of the 3D joint conjecture in [GK10] and also their tight bound on the Erdős distinct distances problem in [GK15]. This and much more is covered in Guth's [Gut16] and Sheffer's [She22] textbooks which are both devoted to the subject of polynomial methods in geometry.

In this report, we aim to give a general overview of the polynomial method as it is used in extremal combinatorics. In Chapter 1 we study vector spaces of polynomials, as well as proving general results about how the degree of a polynomial affects the size of its zero set such as the Schwartz-Zippel Lemma. These results allow us to conclude the chapter by stating Dvir's proof of the Finite Field Kakeya Conjecture, a result giving a lower bound on the size of so-called Kakeya sets. In Chapter 2, we turn our attention to the Croot-Lev-Pach Lemma, which we use in Tao's symmetrised form to prove upper bounds on the size of sunflower free sets and cap sets. In Chapter 3, we focus almost entirely on Alon's Cominatorial Nullstellensatz, a seemingly magical result, which we use to give lower bounds on the size of sum sets in the Cauchy-Davenport Inequality and the Erdős-Heilbronn conjecture.

From this point forwards, we take a more research-based stance and start using the Combinatorial Nullstellensatz to give results about the existence of objects instead of extremal statements. In this way, we end Chapter 3 by proving two original existence statements: the first, showing we can always construct an invertible matrix using every element from a given set at least once, and the second, an exact condition on when a hypergraph is k-colourable in terms of a polynomial ideal. These ideas lead us into Chapter 4 where we define the notion of a matrix being able to be unlocked and extend some theory, developed by Brauch, Kézdy and Snevily in [BKS14], to prove a set of original theorems giving exact conditions on when a matrix can be unlocked by various subsets of S_{n^2}. In particular, we give exact conditions on when n^2 elements of a field can be arranged into an $n \times n$ matrix such that the matrix is invertible. We conclude Chapter 4 by discussing a broader result by Kézdy and Snevily, the main result in [KS04], and indicate some further directions that research could be taken before concluding the project.

Notation

For $n \in \mathbb{N}$, S a set, R a commutative ring and $\mathbb{F}$ a field, then

- $\mathbb{N}_0 \coloneqq \{0\} \cup \mathbb{N}$,
- $[n] \coloneqq \{1, 2, ..., n\}$,
- $\mathbb{Z}_n \coloneqq \mathbb{Z}/n\mathbb{Z}$,
- S_n denotes the set of permutations of $[n]$,
- $\overline{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$,
- $x \coloneqq (x_1, ..., x_n)$ and for $a \in \mathbb{F}^n$, then $x + a \coloneqq (x_1 + a_1, ..., x_n + a_n)$,
- for $\alpha \in \mathbb{N}_0^n$, then $|\alpha| = \sum_{i\in[n]} \alpha_i$ and $x^\alpha \coloneqq \prod_{i\in[n]} x_i^{\alpha_i}$,
- μ_n denotes the set of the nth roots of unity, generated by a primitive nth root of unity ω,
- the standard dot product of vectors $x, y \in \mathbb{F}^n$ is given by $x \cdot y = \sum_{i\in[n]} x_i y_i$,
- $M_n(\mathbb{F})$ denotes the set of $n \times n$ matrices with coefficients in $\mathbb{F}$ where $M = (M_{i\,j})_{i,j\in[n]}$,
- Id_n denotes the identity $n \times n$ matrix,
- for a function $f : S \to \mathbb{F}$, $Z(f) \coloneqq \{x \in S : f(x) = 0\}$ is the set of roots of f,
- $R[x] = R[x_1, ..., x_n] \coloneqq \{\sum_{\alpha\in\mathbb{N}_0^n} c_\alpha x^\alpha : c_\alpha \in R, c_\alpha \neq 0 \text{ for only finitely-many } \alpha \in \mathbb{N}_0^n\}$ is the vector space/ring of polynomials in n variables with $0 \in R[x]$ denoting the zero polynomial,
- $P, Q \in R[x]$ are identical, denoted $P(x) \equiv Q(x)$, if they have exactly the same coefficients.
- for polynomials $p_i \in R[x]$, $\langle p_i(x)\rangle$ denotes the ideal in $R[x]$ generated by the p_i,
- for $P \in R[x]$, we naturally let $Z(P) \coloneqq \{x \in R^n : P(x) = 0\}$ however for a subset $A \subseteq R^n$ then $Z(P)[A] \coloneqq \{x \in A : P(x) = 0\}$,
- the indicator function on S is defined to be $\mathbb{I}_S : S \to R$ where

$$\mathbb{I}_S(x) \coloneqq \begin{cases} 1 & \text{if } x \in S, \\ 0 & \text{if } x \notin S, \end{cases}$$

- we denote a graph $G = (V(G), E(G))$ (sometimes just $G = (V, E)$) where $V(G)$ is the set of vertices and $E(G)$ is the set of edges and for a subset of the vertices $W \subseteq V(G)$, $N_G(W)$ denotes the set of neighbours of elements in W,
- if G is a bipartite graph, the vertices of G can be divided into two disjoint sets A and B, denoted $V(G) = (A, B)$, and we denote edges of G by (a, b) where $a \in A$ and $b \in B$.

Chapter 1

Vector Spaces and Polynomials

In this Chapter, we will study vector spaces of polynomials in many variables using methods from linear algebra to leverage results. We will also look at the interaction between polynomials, their degrees and their roots. Combining these two viewpoints we will finish the chapter by proving the Finite Field Kakeya Conjecture following Dvir's elegant approach in [Dvi08].

1.1 Linear Algebra Method

Before we look at vector spaces of polynomials, we first motivate their use with two classic problems from combinatorics, which can be solved using the linear algebra method. In the same way that the polynomial method uses properties of sets where polynomials vanish to give insight into the problem, the linear algebra method traditionally uses properties about the rank of a carefully-constructed matrix. To introduce the linear algebra method, we first travel to Oddtown and Eventown, following [BF22].

Oddtown and Eventown

Suppose there are two neighbouring towns, Oddtown and Eventown, each with n residents, who are intent on forming as many clubs as possible where any two clubs must share an even number of people. However, while Oddtown has the tradition that every club must have an odd number of residents in it, Eventown insists that its clubs contain an even number. The two towns have had violent disagreements about whose rule allows the most distinct clubs to be created. So who is correct?

Theorem 1.1. *Try as they might, the residents of Oddtown will never be able to form more than n distinct clubs, whereas the Eventowners will be able to create up to $2^{\lfloor \frac{n}{2} \rfloor}$ distinct clubs.*

Definition 1.2. *The characteristic vector of a subset $S \subseteq [n]$, denoted by $x_S \in \mathbb{F}^n$, is defined to be*

$$(x_S)_i \coloneqq \begin{cases} 1 & \text{if } i \in T, \\ 0 & \text{if } i \notin T. \end{cases}$$

Proof. Since we are considering the number of distinct clubs, we can think of the residents of the 2 towns as the members of the set $[n]$ and the clubs in the 2 towns as collections of subsets of $[n]$. To simplify things, we let our characteristic vectors sit in $\mathbb{F}_2^n$. Then, we see that for clubs $A, B \subseteq [n]$, then $x_A \cdot x_B = |A \cap B|$, in particular, $\|x_A\|^2 = x_A \cdot x_A = |A|$.

We first prove the bound for Oddtown. So, assume that $\mathcal{F}$ is a set of clubs satisfying Oddtown's rules. Then, for $A, B \in \mathcal{F}$,

$$x_A \cdot x_B = \begin{cases} 1 & \text{if } A = B, \\ 0 & \text{if } A \neq B. \end{cases}$$

Notice that the matrix $M = (x_C)_{C \in \mathcal{F}}$ with columns given by the characteristic vectors for the clubs in $\mathcal{F}$ is orthogonal since $M^T M = \mathrm{Id}_{|\mathcal{F}|}$. Using the fact from linear algebra that for matrices $A, B \in M_n(\mathbb{F})$ then $\mathrm{rank}(AB) \leq \min(\mathrm{rank}(A), \mathrm{rank}(B))$ then $\mathrm{rank}(M) \geq \mathrm{rank}(M^T M) = \mathrm{rank}(\mathrm{Id}_{|\mathcal{F}|}) = |\mathcal{F}|$. Now, since M is of size $|\mathcal{F}| \times n$, we get the bound $|\mathcal{F}| \leq \mathrm{rank}(M) \leq \min(|\mathcal{F}|, n) \leq n$.

On the other hand, assume $\mathcal{G}$ is a set of clubs satisfying Eventown's rules and consider the subspace $S = \mathrm{span}_{\mathbb{F}_2}\{x_C : C \in \mathcal{G}\}$. We can note that $x_A \cdot x_B = 0,\ \forall A, B \in \mathcal{G}$ and this implies that $S \subseteq S^\perp = \{v \in \mathbb{F}_2^n : x \cdot v = 0, \forall x \in S\}$, in particular, $\dim(S) \leq \dim(S^\perp)$. Using the rank-nullity theorem for the matrix with rows given by vectors x_C for all $C \in \mathcal{G}$, we have $2\dim(S) \leq \dim(S) + \dim(S^\perp) = \dim(\mathbb{F}_2^n) = n$ and thus $\dim(S) \leq \lfloor \frac{n}{2} \rfloor$. So, we have our desired bound $|\mathcal{G}| \leq |S| = 2^{\lfloor \frac{n}{2} \rfloor}$. □

Corollary 1.3. *Both of these bounds are saturated. Thus, Eventown can form an exponential number of clubs as opposed to Oddtown's linear bound on the number of clubs and so they win the argument.*

Proof. We can create n clubs in Oddtown by assigning each person to their own club and we can create $2^{\lfloor \frac{n}{2} \rfloor}$ clubs in Eventown by creating $\lfloor \frac{n}{2} \rfloor$ pairs of residents and taking every possible combination of those pairs. □

Remark 1.4. *Since $2^{\lfloor \frac{n}{2} \rfloor} \leq n$ for $n \leq 5$, Eventown only wins as long as Oddtown doesn't find a way to drastically reduce the number of people in Eventown!*

We note that the key step in proving the Oddtown bound was showing that each characteristic vector representing a club was linearly independent, thus, we were able use the dimension of the whole space as a bound. Fisher's inequality is a generalisation of the Oddtown bound which can also be proved using a simple rank argument. It states that, given a collection $\mathcal{F}$ of non-empty subsets of $[n]$, then if, for some fixed k, $|A \cap B| = k$ for all distinct $A, B \in \mathcal{F}$, then $|\mathcal{F}| \leq n$. Frankl and Wilson gave an even greater generalisation of this in [FW81].

Maximal Equidistant Sets

Let's ask a seemingly unrelated question, but one where rank will again play a key role: what is the maximum number of points you can draw on a piece of paper such that the distance between every 2 points is the same?

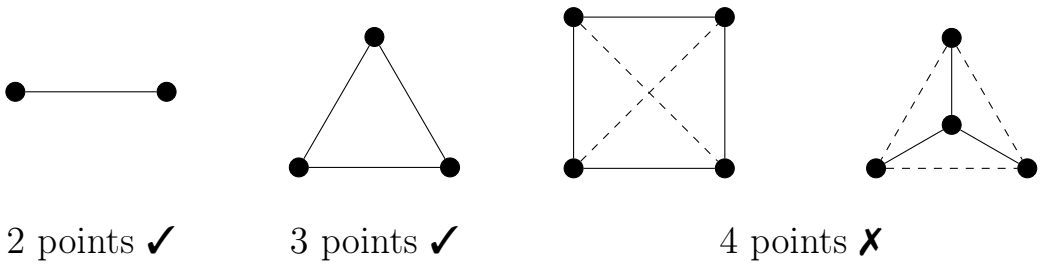


Figure 1.1: Subsets of $\mathbb{R}^2$ marked as to whether they are equidistant sets or not.

Example 1.5. *Figure 1.1 seems to suggest that we will never be able to draw* 4 *points in* $\mathbb{R}^2$ *which are all the same distance apart unless we allow ourselves* 2 *different distances. Indeed,* 3 *distinct circles in the plane have maximum* 3 *points where all* 3 *intersect. However, if we allow ourselves an extra dimension, a tetrahedron in* $\mathbb{R}^3$ *has* 4 *equidistant points.*

Moving down a dimension instead, if we try to draw 3 *equidistant points* $a < b < c$ *in* $\mathbb{R}$*, then* $c-b = c-a = b-a$ *then* $a = b = c$ *so we get a contradiction, thus we can draw maximum* 2 *equidistant points on a line.*

With this in mind, we might conjecture that the maximum number of equidistant points in $\mathbb{R}^d$ is $d+1$ which we will prove now in a very similar way to the Oddtown and Eventown problem.

Theorem 1.6. *Let* $d \in \mathbb{N}$ *and let* $N(d)$ *denote the maximum number of equidistant points in* $\mathbb{R}^d$ *with respect to the standard Euclidean metric. Then* $N(d) \leq d+1$.

Proof. Without loss of generality, let $\{0, p_1, ..., p_n\} \subseteq \mathbb{R}^d$ be our equidistant set where $\|p_i\|^2 = 1$ and $\|p_i - p_j\|^2 = 1, \forall i, j \in [n]$. Using the standard dot product on $\mathbb{R}^d$, we thus have $\|p_i - p_j\|^2 = \|p_i\|^2 + \|p_j\|^2 - 2p_i \cdot p_j = 2(1 - p_i \cdot p_j)$ and thus

$$p_i \cdot p_j = \begin{cases} 1 & \text{if } i = j, \\ \frac{1}{2} & \text{if } i \neq j. \end{cases}$$

Now we define the matrix $M = (p_1^T, ..., p_n^T)$ of dimension $n \times d$ with columns given by the points in our equidistant set. Notice that the $n \times n$ matrix $M^T M$ is simply the Gram matrix of our equidistant set and we can rewrite it as $M^T M = \frac{1}{2}(\mathrm{Id} + \mathbb{J})$ where $\mathbb{J}$ is the $n \times n$ matrix filled with 1s. The eigenvectors of $\mathbb{J}$ are $e_1 - e_i$ for $2 \leq i \leq n$ which all have eigenvalue 0 and $e_1 + ... + e_n$ which has eigenvalue n. Thus, $\det(t\,\mathrm{Id} - \mathbb{I}) = (t-n)t^{n-1}$ and substituting in $t = -1$ and multiplying both sides $(-\frac{1}{2})^n$, we have

$$\det(M^T M) = \det(\frac{1}{2}(\mathrm{Id} + \mathbb{I})) = \left(-\frac{1}{2}\right)^n \det(-\mathrm{Id} - \mathbb{I}) = (-1)^n \frac{1}{2^n}(-1-n)(-1)^{n-1} = \frac{n+1}{2^n} \neq 0$$

and thus $n = \mathrm{rank}(M^T M) \leq \mathrm{rank}(M) \leq d$. So we have $N(d) \leq d+1$. □

Just as in the proof of the bound on Oddtown, the key step in proving $N(d) \leq d+1$ was proving that, ignoring 0, each equidistant point p_i is linearly independent in $\mathbb{R}^d$. We can also saturate this bound since a regular d-simplex in $\mathbb{R}^d$ is an equidistant set with $d+1$ points. The regular d-simplex can be explicitly constructed by considering the d-dimensional hyperplane $x_1 + x_2 + ... + x_{d+1} = 1$ in $\mathbb{R}^{d+1}$. Now the points $e_1, ..., e_{d+1}$ form the vertices of a regular d-simplex and are thus also an equidistant set in a space isomorphic to $\mathbb{R}^d$. This construction will give us insight as well when we want to construct examples of 2-distance set later on.

1.2 Polynomials over Vector Spaces

Now we have had a look at some linear algebra techniques, we can start looking at the interaction between vector spaces of polynomials and the degree and zeroes of said polynomials, following the proof of the Finite Field Kakeya Conjecture by Sheffer in [She22]. This will give us results which we will need to prove the Finite field Kakeya Conjecture and Theorem 2.3 later on.

Lemma 1.7 (Factor Theorem)**.** *For a commutative ring* R *and polynomial* $f \in R[t]$*, then* $\forall a \in R$*,* $f(a) = 0 \Leftrightarrow (t-a) | f(t)$.

Corollary 1.8. *For a polynomial $f \in R[t]$, if $\deg(f) < |Z(f)|$ then f is the zero polynomial.*

Thus, for a non-zero polynomial in 1 variable, its degree gives us a bound on the size of its zero set and the zero sets of low-degree polynomials carry 'less' combinatorial information in some sense, which will hold as we introduce more variables.

Definition 1.9. *For a commutative ring R and a non-zero polynomial $P \in R[x_1, ..., x_n]$ where $P(x) = \sum_{\alpha \in \mathbb{N}_0^n} c_\alpha x^\alpha$ for $c_\alpha \in R$, the degree of P, denoted $\deg(P) \coloneqq \max\{\sum_{i \in [n]} \alpha_i : \alpha \in \mathbb{N}_0^n, c_\alpha \neq 0\}$ ie. the sum of the powers in the "largest" monomial with non-zero coefficient. For convenience, we set $\deg(0) \coloneqq -\infty$.*

It is well-known that both functions and polynomials form vector spaces and we examine the sizes of these spaces.

Lemma 1.10. *For a finite set E and field $\mathbb{F}$, the vector space of functions on E, denoted $\mathbb{F}^E \coloneqq \{f : E \to \mathbb{F}\}$, has dimension $|E|$.*

Proof. A basis for $\mathbb{F}^E$ is given by $\{\mathbb{I}_{\{e\}}\}_{e \in E}$. □

Lemma 1.11. *The vector space of polynomials in n variables with degree at most d, denoted $\mathrm{Poly}_d(\mathbb{F}) \subseteq \mathbb{F}[x_1, ...x_n]$ has dimension $\binom{n+d}{n}$.*

Proof. There is a bijection between the number of monic monomials with degree at most d ie. x^i for $i \in \mathbb{N}_0^n$ where $|i| \leq d$ and integer partitions of d with $n+1$ partitions, given by $x^i \leftrightarrow (d-|i|, i_1, i_2, ..., i_n)d$. Counting the number of ways we can decompose d elements into $n+1$ groups is equivalent to choosing n places for the partitions to go out of $n+d$ spaces. □

Definition 1.12. *For $E \subset \mathbb{F}^n$, the natural evaluation map, denoted $\phi_E : \mathrm{Poly}_d(\mathbb{F}) \to \mathbb{F}^E$, maps polynomials with degree at most d to functions on E given by $\phi_E(P) : E \to \mathbb{F}, e \mapsto P(e)$. Since $(P+Q)(e) = P(e) + Q(e)$, then ϕ_E is a linear map.*

While Definition 1.12 may seem trivial, it is important to take care when using properties of polynomials and the functions they induce in vector spaces.

We can now prove a relation on the size of sets that can be captured as the zero set of a low-degree polynomial using the evaluation map.

Lemma 1.13. *For $d \in \mathbb{N}_0$ and field $\mathbb{F}$, if $E \subseteq \mathbb{F}^n$ is a set such that $|E| < \binom{n+d}{n}$, then there exists a non-zero polynomial $P \in \mathrm{Poly}_d(\mathbb{F})$ such that $E \subseteq Z(P)$.*

Proof. Consider the evaluation map ϕ_E from Definition 1.12. By the rank-nullity theorem, $\dim(\ker \phi_E) = \dim(\mathrm{Poly}_d(\mathbb{F})) - \dim(\mathrm{Im}\, \phi_E) \geq \dim(\mathrm{Poly}_d(\mathbb{F})) - \dim(\mathbb{F}^E) = \binom{n+d}{n} - |E| > 0$ using Lemma 1.10 and Lemma 1.11. Thus, there is a non-trivial element in $\ker \phi_E$ which is what we wanted. □

1.3 The Schwartz-Zippel Lemma

We briefly pause our study of vector spaces of polynomials in order to prove the Schwartz-Zippel Lemma. The Schwartz-Zippel Lemma effectively shows that, when working in a finite field, the degree of a non-zero polynomial controls the number of roots of the polynomial. Thus, at least when working over finite fields, zero sets of low-degree polynomials are combinatorially simpler which is in parallel with the 1 variable case. Before we prove the Schwartz-Zippel Lemma, we first need one more crucial Lemma, Lemma 1.14, which, in some sense, says that as long as the degree of a non-zero polynomial over a finite field is not too large, it is not zero everywhere.

Lemma 1.14. *For a finite field $\mathbb{F}$ and a non-zero polynomial $P \in \mathbb{F}[x_1, ..., x_n]$ such that $\deg(P) < |\mathbb{F}|$, there exists $a \in \mathbb{F}^n$ such that $P(a) \neq 0$.*

Proof. We will prove this by induction on k. For $k = 1$, using Lemma 1.7, suppose $P(a) = 0$ for all $a \in \mathbb{F}$, then $x_1(x_1 - 1)...(x_1 - |\mathbb{F}| + 1)$ divides $P(x_1)$ meaning $\deg(P) \geq |\mathbb{F}|$. For our induction step, assume the statement holds for $n = k$ and suppose we have non-zero $P \in \mathbb{F}[x_1, ..., x_k, x_{k+1}]$ with degree at most $\mathbb{F} - 1$. If $P(x_1, ..., x_k, r) \neq 0$ for some $r \in \mathbb{F}$, since $P(x_1, ..., x_k, r)$ is simply a non-zero polynomial in k variables with degree at most $\mathbb{F} - 1$, there is a $(b_1, ..., b_k) \in \mathbb{F}^n$ such that $P(b_1, ..., b_k, r) \neq 0$ so now just set $a = (b_1, ..., b_k, r)$. Else, setting $R = \mathbb{F}[x_1, ..., x_k]$ we can treat P as a polynomial in x_{k+1} in $R[x_{k+1}]$. Thus, applying Lemma 1.7, $x_{k+1}(x_{k+1} - 1)...(x_{k+1} - |\mathbb{F}| + 1)$ divides P meaning $\deg(P) \geq |\mathbb{F}|$ which is a contradiction since we assumed P had degree at most $\mathbb{F} - 1$. □

Although we will not need it for the Finite Field Kakeya Conjecture, the Schwartz-Zippel Lemma, which we state in its commonly used form below, can be seen as the generalisation of Lemma 1.14. Indeed we will use Lemma 1.14 as a key building block in our proof of the Schwartz-Zippel Lemma with Lemma 1.14 also following as a corollary.

Lemma 1.15 (Schwartz-Zippel Lemma)**.** *For a finite field $\mathbb{F}$ and a non-zero polynomial $P \in \mathbb{F}[x_1, ..., x_n]$, $|Z(P)| \leq \deg(P)|\mathbb{F}|^{n-1}$.*

We provide a relatively short proof of the Schwartz-Zippel Lemma by Moshkovitz in [Mos10].

Proof. Let $d = \deg(P)$, then we can write $P = P_d + P_{<d}$ where P_d is the sum of all the degree d monomials in P. We can assume $d < |\mathbb{F}|$ otherwise the result follows trivially. Given a line in $\mathbb{F}^n$, say $\{w + tx | t \in \mathbb{F}\}$ for some $w, x \in \mathbb{F}^n$, we have that the coefficient in front of the t^d term in $P(w + tx)$ is $P_d(x)$. However, by Lemma 1.14, since $P_d \not\equiv 0$ and $\deg(P_d) = d < |\mathbb{F}|$, there exists an $a \in \mathbb{F}^n$ such that $P_d(a) \neq 0$. In addition, we can choose a to be non-zero since if $d > 0$, $P_d(0) = 0$ and if $d = 0$, then $P_d \equiv P$ is non-zero and constant.

For a non-zero vector $v \in \mathbb{F}^n$, the points of $\mathbb{F}^n$ can be partitioned into the set of parallel lines with direction v, denoted $\mathcal{L}_v \coloneqq \{l(v, c) : c \in \mathbb{F}^n\}$ where $l(v, c) = \{vt + c : t \in \mathbb{F}\}$, thus $|\mathcal{L}_v| = |\mathbb{F}|^{n-1}$ since each line has $\mathbb{F}$ points on it. We claim that none of the lines in $\mathcal{L}_a$ intersect $Z(P)$ in more than d places. Indeed, for some $w \in \mathbb{F}^n$, if $P(w + ta) = 0$ for more than d different values of $t \in \mathbb{F}$, then $P(w + ta)$ is the zero polynomial by Corollary 1.8. Furthermore, the coefficient of t^d in $P(w + ta)$ is $P_d(a)$, implying $P_d(a) = 0$ which is a contradiction. Thus, we have a bound on $Z(P)$ which is precisely that $Z(P) \leq d|\mathbb{F}|^{n-1}$. □

The Schwartz-Zippel Lemma was originally a result from the theory of probabilistic polynomial identity testing, given as the following Corollary.

Corollary 1.16. *For a finite field $\mathbb{F}$ and non-zero $f \in \mathbb{F}[x_1, ..., x_n]$, then $\mathbb{P}[f(r_1, ..., r_n) = 0] \leq \frac{\deg(f)}{|\mathbb{F}|}$ where $r_1, ..., r_n$ are random elements of $\mathbb{F}$ selected uniformly and independently.*

Following Williams' notes from [Wil21], the key problem that identity testing deals with is this: given two polynomials p_1, p_2 where we don't know the coefficients of either polynomial but can evaluate them at any point we'd like, what is the best way of testing if $p_1 \equiv p_2$ ie. the two polynomials have the same coefficients?

Clearly this is equivalent to asking when a polynomial $p \coloneqq p_1 - p_2$ is the zero polynomial, and here we can use Corollary 1.16. Plug a random element of $\mathbb{F}^n$ into p. If the output is non-zero, then $p \not\equiv 0$ and we are done. Otherwise, if the output is zero then by Corollary 1.16, the probability that $p \equiv 0$

is $1 - \frac{\deg(p)}{|\mathbb{F}|}$. Either by plugging in more random elements of $\mathbb{F}^n$ or evaluating the polynomials over a larger finite field, we can make the probability of the output being 0 when $p \not\equiv 0$ as small as we'd like.

Perfect Matchings of Graphs

We demonstrate the value of the Schwartz-Zippel Lemma and Corollary 1.16 by showing its relevance to perfect matchings of graph. Determining whether a graph has a perfect matching will hold particular importance in Chapter 4 so it is well worth the detour to mention perfect matchings here.

Definition 1.17. *A perfect matching of a graph $G = (V(G), E(G))$ is a subset of the edge set $E(G)$ such that every vertex in $V(G)$ is connected to exactly one edge in the subset.*

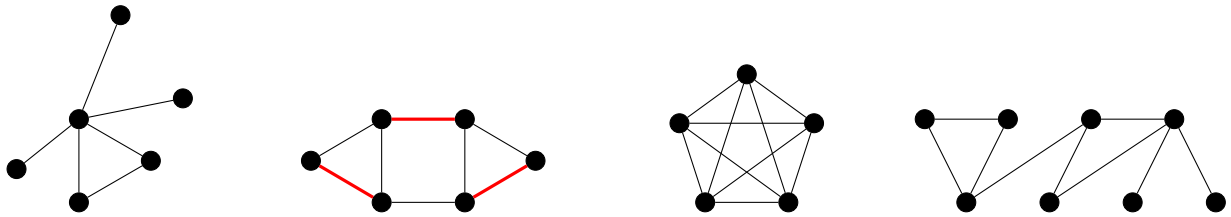


Figure 1.2: Graph (b) is the only graph which has a perfect matching, indicated by red edges.

Note that any graph with an odd number of vertices will not have a perfect matching. But, given a graph G with an even number of vertices, how can we tell when there is a perfect matching? The answer lies in the polynomial given by the determinant of the Tutte matrix.

Definition 1.18. *Given a graph G, where we enumerate the vertices $V = \{v_i\}_{i\in[n]}$, we define the Tutte matrix of the graph G to be $A \in M_n(\mathbb{C}[x_{ij}])$ for $i, j \in [n]$ where*

$$A_{i\,j} = \begin{cases} x_{ij} & \text{if } (v_i, v_j) \in E \text{ and } i < j, \\ -x_{ji} & \text{if } (v_i, v_j) \in E \text{ and } i > j, \\ 0 & \text{otherwise.} \end{cases}$$

The following Theorem was first proved by Tutte in 1947 in [Tut47]. We note that the determinant of the Tutte matrix will be a polynomial and the determinant of the Tutte matrix being non-zero means the polynomial is not identically zero.

Theorem 1.19. *A graph G contains a perfect matching if and only if the Tutte matrix of G has non-zero determinant.*

So, given a graph G, we can check if G has a perfect matching by computing the determinant of its corresponding Tutte matrix A and checking if it vanishes. However, by implementing Corollary 1.16 and using our observations from before, we can get a probabilistic estimate much more quickly. Since $det(A)$ has degree at most $2n$, if we evaluate $\det(A)$ at a random point in $\mathbb{F}^{2n}$ and the output is zero, the probability that $\det(A) = 0$ is at least $1 - \frac{2n}{|\mathbb{F}|}$ giving us an efficient but probabilistic method of checking if G has a perfect matching. By increasing $|\mathbb{F}|$ we can make the above probability as small as we'd like, however, this will likely be a trade-off with the time needed to evaluate the random point due to doing calculations in a larger field.

A proof of Theorem 1.19 is given in Appendix A along with a further exploration of perfect matchings and disjoint cycle covers of directed and undirected graphs.

1.4 Finite Kakeya Sets

We now set the scene for Dvir's proof of the Finite Field Kakeya Conjecture, which many argue was the result that kicked off the acknowledgement of the so-called polynomial method, starting with a question from geometry. The question was first asked by Japanese mathematician Soichi Kakeya in 1917: what is the smallest set in the plane in which one can rotate a needle around completely?[1] These sets have become known as Kakeya sets which in turn prompted the notion of the Besicovitch set, which boils down the essence of the Kakeya set.

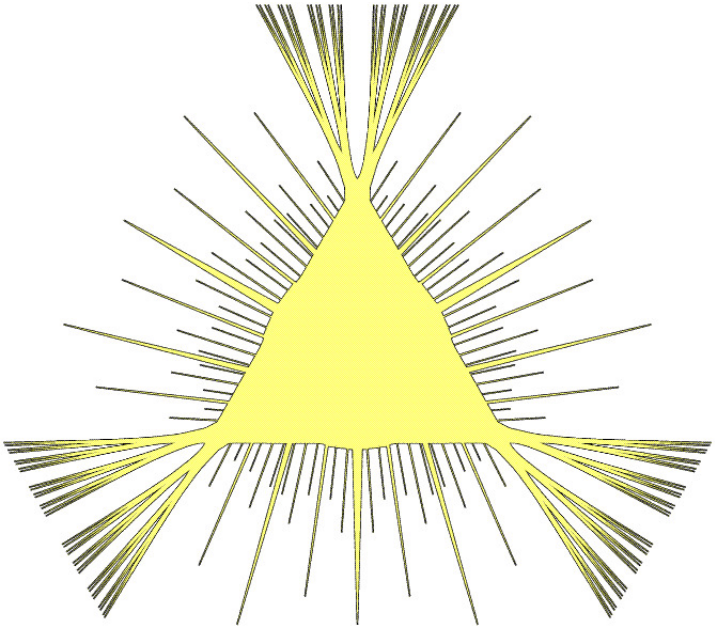


Figure 1.3: An example by [Gtg09] of a Kakeya set, constructed from "Perron trees". These were described by Perron in [Per28] as a method of constructing arbitrarily 'small' Kakeya sets.

Definition 1.20 (Besicovitch set)**.** *A Besicovitch set is a set of points in Euclidean space $\mathbb{R}^n$ (ie. n is a positive integer) such that given any direction, there is a unit vector pointing in that direction starting and ending at two points from our set.*

For $n = 2$, the circle with radius equal to $\frac{1}{2}$ is a Kakeya set and thus also a Besicovitch set. However, we can do much better than this. It was shown in 1919 by Besicovitch in [Bes19] that there are Besicovitch sets with arbitrarily small measure. However, there is still one conjecture from Elder's lecture notes, [Eld12], about the 'size' of these sets where the notion of size we use is that of Hausdorff dimension.

Conjecture 1.21 (Kakeya Set Conjecture)**.** *Besicovitch sets in $\mathbb{R}^n$ have Hausdorff dimension greater than $n - \epsilon$ for any $\epsilon > 0$.*

This, as it turns out is a very difficult problem, and so far we have only been able to prove it completely for $n = 1$ or $n = 2$. When faced with a tough problem, it is often productive to attempt a simpler version. In the case of Kakeya Set Conjecture, Wolff reposed the Kakeya set conjecture over finite fields in [Wol99], thus avoiding the technicalities of dealing with the Hausdorff dimension and moving the problem into a more combinatorial setting.

[1] According to [Juk11], Kakeya likened this to a samurai turning a lance round in a small toilet.

Finite Field Kakeya Conjecture

Definition 1.22 (Finite Kakeya set)**.** *For $n \in \mathbb{N}$ and $\mathbb{F}$ a finite field, a finite Kakeya set is a set of points in $\mathbb{F}^n$ such that the set contains a line in every direction.*

We can now state and prove the Finite Field Kakeya conjecture which gives a lower bound on the size of finite Kakeya sets. It was originally proved in 2008 by Dvir in [Dvi08] in a surprisingly short proof using only basic techniques from the polynomial method, all of which we have covered already. In the following proof, we incorporate lines of argument from [Tao08] and [She22].

Theorem 1.23 (Finite Field Kakeya Conjecture)**.** *If E is a finite Kakeya set in $\mathbb{F}^n$,*

$$|E| \geq \binom{|\mathbb{F}| - 1 + n}{n}.$$

Proof. Suppose E is a finite Kakeya set where $|E| < \binom{|\mathbb{F}|-1+n}{n}$, seeking a contradiction. Then, by Lemma 1.13, there exists a non-zero polynomial $P \in \text{Poly}_{|\mathbb{F}|-1}(\mathbb{F})$ such that P vanishes on E. Then we can write $P = P_d + P_{<d}$ where $0 < d < |\mathbb{F}|$ is the degree of P, noting $d \neq 0$ since P vanishes on a non-empty set, and P_d is the sum of all the degree d monomials in P.

Given any direction $v \in \mathbb{F}^n \backslash \{0\}$, there is a $u \in \mathbb{F}^n$ such that $\{u + tv : t \in \mathbb{F}\} \subseteq E$ and thus we can define $Q(t) \coloneqq P(u + tv) = 0$ for all $t \in \mathbb{F}$. Since $\deg(Q) < |\mathbb{F}|$ and Q vanishes at $|\mathbb{F}|$ different points, then using Corollary 1.8, Q is the zero polynomial. In particular, the coefficient in front of t^d, which is $P_d(v)$, is zero for all non-zero vectors $v \in \mathbb{F}^n$. Finally, noting $P_d(\mathbf{0}) = 0$ since $d \neq 0$ then $P_d(v) = 0 \, \forall v \in \mathbb{F}^n$ and $\deg(P_d) = d < \mathbb{F}$ so, using Lemma 1.14, P_d is also the zero polynomial. However, this contradicts the fact that P had degree d. □

Corollary 1.24. *Every finite Kakeya set in $\mathbb{F}^n$ has at least $\frac{1}{n!}|\mathbb{F}|^n$ elements. So, for any vector space of dimension n over a finite field, a finite Kakeya set takes up at least a fixed proportion of the available space.*

Proof. We have $\binom{k+n}{n} = \frac{(k+n)!}{n!k!} = \frac{1}{n!}(k+n)(k+n-1)...(k+1) \geq \frac{1}{n!}(k+1)^n$. For a Kakeya set E, then $|E| \geq \binom{|\mathbb{F}|-1+n}{n} \geq \frac{1}{n!}|\mathbb{F}|^n$. □

This bound was improved in 2013 in [Dvi+13] using the method of multiplicities, another facet of the polynomial method, covered in [Tao14], which we will not go into here.

Finite Kakeya Sets in 2 Dimensions

Using Theorem 1.23, we know that the size of any finite Kakeya set over $\mathbb{F}^2$ is at least $\binom{|\mathbb{F}|+1}{2} = \frac{1}{2}(|\mathbb{F}| + 1)|\mathbb{F}|$ so let us now try to find finite Kakeya sets which are minimal in size.

Notation 1.25. *For $m, c \in \mathbb{F}$ let $l(m, c)$ and $l(\infty, a)$ denote the set of points on the line $y = mx + c$ and the line $x = a$ in $\mathbb{F}^2$ respectively.*

Since we are trying to find minimal finite Kakeya sets and we know that a finite Kakeya set E contains a line in every direction, for some $c_m \in \mathbb{F}$, we can always write

$$E = \bigcup_{m \in \mathbb{F} \cup \{\infty\}} l(m, c_m).$$

Finally, for $P \in \mathbb{F}^2$, we let $m_P \coloneqq |\{m \in \mathbb{F} \cup \{\infty\} : P \in l(m, c_m)\}|$.

We now present a formula, called the Incidence formula by Faber in [Fab07], which can be shown by inclusion-exclusion, however, we don't prove it here.

Theorem 1.26 (Incidence formula)**.** *For E a finite Kakeya set with m_P defined as above,*

$$|E| = \frac{(|\mathbb{F}|+1)|\mathbb{F}|}{2} + \sum_{P\in\mathbb{F}^2} \frac{(m_P-1)(m_P-2)}{2}$$

Guided by this formula and by [Fab07], let us now construct a Kakeya set which minimizes $\sum_{P\in\mathbb{F}^2} \frac{(m_P-1)(m_P-2)}{2}$. We claim that the finite Kakeya set

$$E = l(\infty, 0) \cup \bigcup_{m\in\mathbb{F}} l(m, -m^2). \tag{1.1}$$

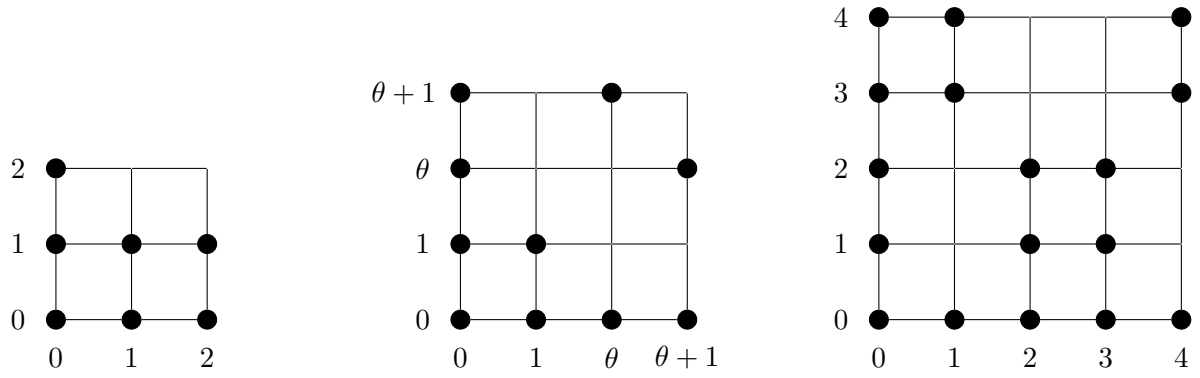
does so. Indeed, since $l(i,-i^2)\cap l(j,-j^2) = \{(i+j, ij)\}$ for distinct $i, j \in \mathbb{F}$ then $l(i,-i^2)\cap l(j,-j^2)\cap l(k,-k^2) = \emptyset$ for distinct $i, j, k \in \mathbb{F}$. So, if $P \notin l(\infty, 0)$, then $m_P \leq 2$ and clearly $m_P \leq 3$ for all $P \in \mathbb{F}^2$.

Now assume $|\mathbb{F}|$ is even ie. $\mathbb{F} = \mathbb{F}_2[\theta]$ for some algebraic integer θ. Thus, for any $i \in \mathbb{F}$, $i = -i$, and so, for distinct $i, j \in \mathbb{F}$, $l(i,-i^2)\cap l(j,-j^2)\cap l(\infty, 0) = \emptyset$. So $m_P \leq 2$ for all $P \in \mathbb{F}^2$ and thus E hits the lower bound we found in Theorem 1.23 using the Incidence Formula, Theorem 1.26.

On the other hand if $|\mathbb{F}|$ is odd, then, for $i \in \mathbb{F}^\times$, $i \neq -i$ and thus we have $l(i,-i^2)\cap l(-i,-i^2)\cap l(\infty, 0) = \{(0,-i^2)\}$. Thus, we have $m_P = 3$ if and only if $P = (0,-i^2)$. In $\mathbb{F}$, there are precisely $\frac{|\mathbb{F}|-1}{2}$ squares and thus, using the Incidence Formula, Theorem 1.26, we have

$$|E| = \frac{(|\mathbb{F}|+1)|\mathbb{F}|}{2} + \frac{|\mathbb{F}|-1}{2}.$$

Faber conjectured, but was not able to prove, that this was the smallest a finite Kakeya set could be in $\mathbb{F}^2$ for $|\mathbb{F}|$ odd. However, a year later in [BM08], it was shown that this is, in fact, the lower bound for the size of a Kakeya set in $\mathbb{F}^2$ for $|\mathbb{F}|$ odd.



$\mathbb{F} = \mathbb{Z}/3\mathbb{Z} \cong \mathbb{F}_3$ $|E| = 7$

$\mathbb{F} = \mathbb{F}_2[\theta] \cong \mathbb{F}_4$ $|E| = 10$

$\mathbb{F} = \mathbb{Z}/5\mathbb{Z} \cong \mathbb{F}_5$ $|E| = 17$

Figure 1.4: Examples of minimal finite Kakeya sets using the explicit construction in Equation 1.1 over the fields: $\mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z}$, $\mathbb{F}_4 \cong \mathbb{F}_2[\theta]$ where $\theta^2 + \theta + 1 = 0$ and $\mathbb{F}_5 \cong \mathbb{Z}/5\mathbb{Z}$.

Chapter 2

The Croot-Lev-Pach Lemma

We now move from one version of the modern polynomial method, Dvir's proof of the Finite Field Kakeya Conjecture, to another, namely the proof of the cap set bound. Although this bound was proved independently by Ellenberg and Gijswijt who co-authored [EG16], both proofs were along the same lines, relying on what has become known as the Croot-Lev-Pach Lemma. This Lemma was first demonstrated in Croot, Lev and Pach's paper, [CLP17], where they gave a new upper bound for the size sets with no 3-term progressions in $\mathbb{Z}_4^n$ and has been the main ingredient in a range results from the s-distance sets in [PP19] to results about the bounds on matrix multiplication speed as demonstrated in [Bla+17]. In 2016, Terence Tao made the amazing connection between the Croot-Lev-Pach Lemma and the slice rank of k-tensors which allowed him to symmetrise Ellenberg and Gijswijt's arguments in [Tao16]. Before we introduce k-tensors and slice rank which we use to prove results about sunflowers and cap sets, we prove an upper bound on the size of s-distance sets, the proof of which uses results about vector spaces of polynomials which we proved in Chapter 1 as well as cutting directly to the heart of the Croot-Lev-Pach Lemma.

2.1 s-distance Sets

In Section 1.1, we studied maximal equidistant sets and noted in Example 1.5 that in the plane we could draw 4 points with only 2 distinct distances between pairs of points. But could we have drawn more? We now generalise the notion of equidistant sets to that of s-distance sets where we allow s distinct distances between pairs of points.

Definition 2.1. *For $s \in \mathbb{N}$, an s-distance set in a metric space M is a subset $A \subseteq M$ where, letting $\Delta \coloneqq \{\|a-b\| : a, b \in A, a \neq b\}$, $|\Delta| = s$.*

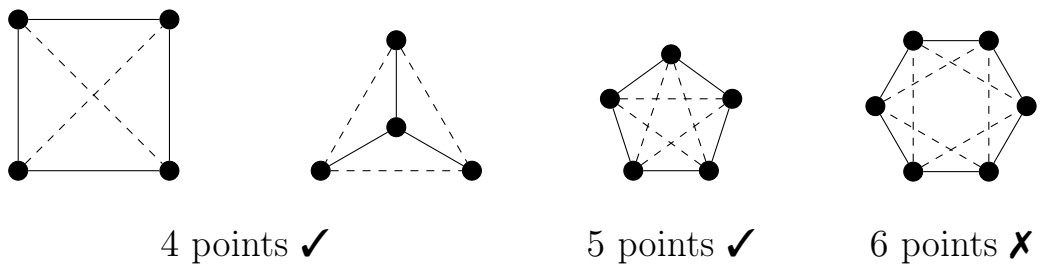


Figure 2.1: Sets of points in $\mathbb{R}^2$ marked as to whether they are 2-distance sets or not.

We begin by examining the case of 2-distance sets with some examples shown in Figure 2.1. In order to warm up for the proof of the bound for general s, we first prove an upper bound on the size of 2-distance sets, first shown by Blokhuis in [Blo84] which uses techniques about polynomials in vector spaces reminiscent of Chapter 1.

Theorem 2.2. *Every 2-distance set in $\mathbb{R}^d$ with the Euclidean metric has at most $\binom{d+2}{2}$ elements.*

Proof. Let $A \subseteq \mathbb{R}^d$ be a 2-distance set with pairwise distances $\Delta = \{d_1, d_2\}$. It is natural to associate with each point $a \in A$ a polynomial f_a given by

$$f_a(x) = \left(\frac{1}{d_1^2}\|x-a\|^2 - 1\right)\left(\frac{1}{d_2^2}\|x-a\|^2 - 1\right) \text{ where for } a, b \in A, \ f_a(b) = \begin{cases} 1 & \text{if } a = b, \\ 0 & \text{if } a \neq b. \end{cases}$$

Working over the vector space of functions, $V \coloneqq \{f : \mathbb{R}^d \to \mathbb{R}\}$, we notice that for all $a \in A$, $\|x-a\|^2 \in \langle \|x\|^2, x_i, 1 : i \in [d]\rangle$ ie. $\|x-a\|^2$ can be written as a linear combination of $\|x\|^2$, x_i for $i \in [d]$ and 1. Thus, $\langle f_a(x), x_i, 1 : a \in A, i \in [d]\rangle \subseteq \langle \|x\|^4, \|x\|^2 x_j, x_j x_k, x_j, 1 : j, k \in [d]\rangle$ which is a subspace of V of dimension at most $1 + d + (\binom{d}{2} + d) + d + 1 = \binom{d+2}{2} + d + 1$. We further claim that $\{f_a(x), x_i, 1 : a \in A, i \in [d]\}$ is a linearly independent set in V which would imply $|A| + d + 1 \leq \binom{d+2}{2} + d + 1$ so we are done. Indeed, suppose that for all $x \in \mathbb{R}^d$

$$\sum_{a \in A} c_a f_a(x) + \sum_{i \in [d]} c_i x_i + c = 0 \text{ for some } c_a, c_i, c \in \mathbb{R}.$$

Plugging in $b \in A$, we have the identity $c_b + \sum_{i \in [d]} c_i b_i + c = 0$ for all $b \in A$. Furthermore, plugging in te_i for $t \in \mathbb{R}$ and $i \in [d]$, we have for all $t \in \mathbb{R}$

$$\begin{aligned} 0 &= \sum_{a \in A} c_a f_a(te_i) + c_i t + c = \sum_{a \in A} c_a \left(\frac{1}{d_1^2}\|te_i - a\|^2 - 1\right)\left(\frac{1}{d_2^2}\|te_i - a\|^2 - 1\right) + c_i t + c \\ &= \sum_{a \in A} c_a \left(\frac{1}{d_1^2}t^2 - \frac{2a_i}{d_1^2}t + \frac{1}{d_1^2}\|a\|^2 - 1\right)\left(\frac{1}{d_2^2}t^2 - \frac{2a_i}{d_2^2}t + \frac{1}{d_2^2}\|a\|^2 - 1\right) + c_i t + c \\ &= \frac{1}{d_1^2 d_2^2}\left(\sum_{a \in A} c_a\right) t^4 - \frac{2}{d_1^2 d_2^2}\left(\sum_{a \in A} c_a a_i\right) t^3 + \text{ lower order terms} \end{aligned}$$

Treating this as a polynomial in $\mathbb{R}[t]$ which vanishes on all of $\mathbb{R}$, by Corollary 1.8, it is the zero polynomial and thus $\sum_{a \in A} c_a = 0$ and $\sum_{a \in A} c_a a_i = 0$ for all $i \in [d]$ since d_1 and d_2 are both non-zero. Now, multiplying $\sum_{a \in A} c_a a_i = 0$ by $-c_i$ and summing over $i \in [d]$, we have

$$0 = \sum_{i \in [d]} -c_i \left(\sum_{a \in A} c_a a_i\right) = \sum_{a \in A} -c_a \left(\sum_{i \in [d]} c_i a_i\right) = \sum_{a \in A} -c_a(-c_a - c) = \sum_{a \in A} c_a^2 + c\sum_{a \in A} c_a = \sum_{a \in A} c_a^2$$

using the fact that $c_b + \sum_{i \in [d]} c_i b_i + c = 0$ for all $b \in A$ and $\sum_{a \in A} c_a = 0$. Since $c_a \in \mathbb{R}$, then $c_a = 0$ for all $a \in A$ and thus we have $c_i t + c = 0$ for all $i \in [d]$. Again, treating these as polynomials in $\mathbb{R}[t]$ which vanish on $\mathbb{R}$, by Corollary 1.8, they are all the zero polynomial so $c = 0$ and $c_i = 0$ for all $i \in [d]$ along with $c_a = 0$ for all $a \in A$. □

Along similar lines to when we constructed equidistant sets, we can construct large explicit 2-distance sets in the d-dimensional hyperplane $x_1 + x_2 + ... + x_{d+1} = 2$ in $\mathbb{R}^{d+1}$ which is isomorphic to $\mathbb{R}^d$. We let our 2-distance set be given by $A = \{e_i + e_j : i, j \in [d+1], i \neq j\}$ where $\Delta = \{\sqrt{2}, 2\}$. Indeed, for $i, j, k, l \in [d+1]$ all distinct, $\|e_i + e_j - (e_i + e_k)\| = \|e_j - e_k\| = \sqrt{2}$ and $\|e_i + e_j - (e_k + e_l)\| = \sqrt{4} = 2$. So, $|A| = \binom{d+1}{2}$ which gives us a lower bound for the maximal size of 2-distance sets.

Table 2.1: This table contains the sizes of maximal 2-distance sets in up to 8 dimensions along with the number of such sets up to similarity ie. up to isometry and scaling.

Dimension d	1	2	3	4	5	6	7	8
$\binom{d+2}{2}$	3	6	10	15	21	28	36	45
Size of maximal 2-distance set in $\mathbb{R}^d$	3	5	6	10	16	27	29	45
$\binom{d+1}{2}$	1	3	6	10	15	21	28	36
# maximal 2-distance sets up to similarity	1	1	6	1	1	1	1	≥ 1

Table 2.1 demonstrates how the size of a maximal 2-distance set in $\mathbb{R}^d$ fluctuates between $\binom{d+1}{2}$ and $\binom{d+1}{2}$ meaning the 2-distance sets we just constructed give us a good lower bound, and in dimensions 3 and 4 they actually turn out to be maximal! It was Kelly, in [Kel47], who first proved that 5 points is the best we can do in $\mathbb{R}^2$ and Erdős and Fishburn proved it was unique in [EF96] up to similarity. In fact, all 2-distance sets in $\mathbb{R}^2$ and $\mathbb{R}^3$ had already been classified by Einhorn and Schoenberg in [ES66] in 1966. For dimensions $4, 5$ and 6, it was Seidel in [Sei95], who first conjectured the values given in the table above but it was Lisoněk in [Lis97] who, in 1997, proved the sizes of maximal 2-distance sets in $\mathbb{R}^d$ for $4 \leq d \leq 8$ and proved uniqueness of these sets for $4 \leq d \leq 7$, finding a set in $\mathbb{R}^8$ which hits the upper bound of $\binom{8+2}{2} = 45$. In fact the construction in 8 dimensions just takes our explicit 2-distance set embedded in the hyperplane $x_1 + x_2 + ... + x_9 = 2$ in $\mathbb{R}^9$ with 36 elements from before and adds 9 more points to get the 2-distance set with 45 points given by

$$A = \{e_i + e_j : i, j \in [9], i \neq j\} \cup \{-e_i + \frac{1}{3}\sum_{k\in[9]} e_k : i \in [9]\}$$

There are many avenues of research into 2-distance sets. One such avenue asks questions such as: which 2-distance sets maximise the ratio between the pairwise distances? It is shown in [HP93] that the 2-distance set which forms a pentagon, as shown in Figure 2.1, maximises this for all 2-distance sets with 5 points with the golden ratio. It is also interesting to note that any simple graph can be represented as a 2-distance set and Einhorn and Schoenberg sparked the use of this correspondence in [ES66], which has branched into many other areas of research such as: what is the minimum number of dimensions needed to construct a 2-distance set representing a given graph? Finally, spherical 2-distance sets, as seen in [Mus09], are sets where the inner product of two different elements take precisely 2 values. Let's now generalise to s-distance sets.

Theorem 2.3. *The size of an s-distance set in $\mathbb{R}^d$ is at most $\binom{d+s}{s}$.*

Theorem 2.3 demonstrates our current upper bound on s-distance sets which was given in [BBS83] in a fairly technical paper. However, in [PP19], a much quicker and easier proof is given by introducing a second variable which symmetrises the polynomial from the proof of Theorem 2.2 and gives us the more general result which we state now. Attentive readers will notice the similarity between this bound and the bound in Lemma 1.11, and this is no accident.

Proof. Let A be our s-distance set and let $\Delta = \{\|a - b\| : a, b \in A, a \neq b\}$ so $|\Delta| = s$. Define the polynomial $P(x, y) \coloneqq \prod_{d\in\Delta}\left(1 - \frac{1}{d^2}\|x - y\|^2\right)$ where $\deg(P) \leq 2s$. Then, we can write $P(x, y)$ as a sum of monomials of the form $c_{\alpha,\beta}x^\alpha y^\beta$ for $\alpha, \beta \in \mathbb{N}_0^d$ where, since $|\alpha| + |\beta| \leq \deg(P) = 2s$, then by

the pigeonhole principle, $\min\{|\alpha|, |\beta|\} \leq s$. In addition, notice that for $a, b \in A$

$$P(a,b) = \begin{cases} 1 & \text{if } a = b, \\ 0 & \text{if } a \neq b. \end{cases}$$

Now recall that the vector space of functions $\mathbb{R}^A = \{f : A \to \mathbb{R}\}$ has an inner product given by $(f,g) \coloneqq \sum_{a\in A} f(a)g(a)$. Using the evaluation map $\phi_A : \text{Poly}_s(\mathbb{R}) \to \mathbb{R}^A$ where $\phi_A(P) : A \to \mathbb{R}, a \mapsto P(a)$ from Definition 1.12, then for $f \in \text{Im}(\phi_A)^\perp$

$$\begin{aligned}(f,f) = \sum_{a\in A} f(a)f(a) = \sum_{a,b\in A} f(a)P(a,b)f(b) = \sum_{a,b\in A}\sum_{\alpha,\beta\in\mathbb{N}_0^d} c_{\alpha,\beta}\, a^\alpha b^\beta f(a)f(b) \\ = \sum_{\alpha,\beta\in\mathbb{N}_0^d} c_{\alpha,\beta}\left(\sum_{a\in A} a^\alpha f(a)\right)\left(\sum_{b\in A} b^\beta f(b)\right) = 0\end{aligned}$$

since $\min\{|\alpha|, |\beta|\} \leq s$, implying that $f = 0$. Thus, $\text{Im}(\phi_A) = \mathbb{R}^A$ and so,

$$|A| = \dim \mathbb{R}^A = \dim \text{Im}(\phi_A) \leq \dim \text{Poly}_s(\mathbb{R}) = \binom{d+s}{s}$$

using Lemma 1.11 and the fact that ϕ_A is a linear map, □

This proof really is quite incredible, as there is almost nothing to it. It is even shorter than our proof of the upper bound on the size of both equidistant sets and 2-distance sets, even though these results follow as immediate corollaries to Theorem 2.3. The proof boils down to the pulling apart of the inner product (f,f) into two parts, one of which must be zero meaning the inner product is zero. This is, in some sense, the essence of the Croot-Lev-Pach Lemma which will show up in a similar fashion in Tao's slice rank Lemma. Thus, we will now introduce the machinery of k-tensors and slice rank and then use those results to prove bounds, first conjectured by Erdős, on the size of sunflower free sets and also on the size of maximal cap sets.

2.2 The Slice Rank Method

If we view square matrices as being '2-dimensional', we can view k-tensors as being the k-dimensional analogues.

Definition 2.4. *Let $\mathbb{F}$ be a field, $k \in \mathbb{N}$ and X a finite set. Then a k-tensor is a function $T : X^k \to \mathbb{F}$. Furthermore, a k-tensor is diagonal if T is only non-zero when evaluated at k of the same element in X ie. $T(x_1, ..., x_k) \neq 0$ implies $x_1 = ... = x_k$.*

It is important to note that there are no restrictions on the function defining a k-tensor in the same way that matrices have no restrictions on their elements.

Example 2.5. *As implied, a square matrix is simply a 2-tensor. For a matrix $M \in M_n(\mathbb{F})$, then $T_M : [n]^2 \to \mathbb{F}, (i,j) \mapsto M_{ij}$ is the corresponding 2-tensor. In addition, M is diagonal if and only if T_M is diagonal since $T_M(i,j) = M_{ij} \neq 0$ implies $i = j$.*

It is important to note that the product of two k-tensors does not align with the standard notion of matrix multiplication, instead aligning with the element-wise product of 2 matrices.

Definition 2.6. *For $k, l \in \mathbb{N}$, the product of a k-tensor T and an l-tensor S is a $(k+l)$-tensor TS given by $(TS)(x_1, ...x_{k+l}) = T(x_1, ..., x_k)S(x_{k+1}, ..., x_{k+l})$.*

Now we have the basic notion of a k-tensor extending the notion of square matrices, we can now generalise the notion of rank. However, there is not one agreed-upon definition for the rank of k-tensors and we will need different notions of rank for k-tensors to solve different types of problems. Perhaps the most intuitive type of k-tensor rank is that of slice rank.

Notation 2.7. *For brevity, we denote* $x^{\{i\}} \coloneqq (x_1, ..., x_{i-1}, x_{i+1}, ..., x_k)$.

Definition 2.8. *A* k*-tensor* S *is a slice if there exists a* 1*-tensor* S_1 *and a* $(k-1)$*-tensor* S_{k-1} *such that for some* $i \in [k]$*,*

$$S(x) = S_1(x_i)S_{k-1}(x^{\{i\}}).$$

Let T *be a* k*-tensor. Then the slice rank of* T*, denoted* $\operatorname{srk}(T)$*, is the smallest integer* r *such that* T *can be written as the sum of* r *slices.*

Example 2.9. *Given a finite set* $X \subseteq \mathbb{R}$*, take the* 4*-tensor* $S : X^4 \to \mathbb{R}$ *given by* $S(x_1, x_2, x_3, x_4) = x_1x_2 - x_2x_3 + x_2x_4^3$*.* S *is a slice since, if we define* 1*-tensor* $S_1 : X \to \mathbb{R}$*,* $x_2 \mapsto x_2$ *and* 3*-tensor* $S_3 : X^2 \to \mathbb{R}$*,* $(x_1, x_3, x_4) \mapsto x_1 - x_3 + x_4^3$*, then* $S(x_1, x_2, x_3) = x_2(x_1 - x_3 + x_4^3) = S_1(x_2)S_3(x_1, x_3, x_4)$*. Thus,* $\operatorname{srk}(S) = 1$ *since any slice has slice rank* 1*.*

Now, take the 3*-tensor* $T : X^3 \to \mathbb{R}$ *given by* $T(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_3^2$*. It is easy to check that* T *is not a slice by trying to factor out a linear polynomial of each variable and coming to a contradiction. However, we can write* $T(x_1, x_2, x_3) = x_1(x_2 + x_3) + x_3^2$ *as the sum of two slices and thus* $\operatorname{srk}(T) = 2$*.*

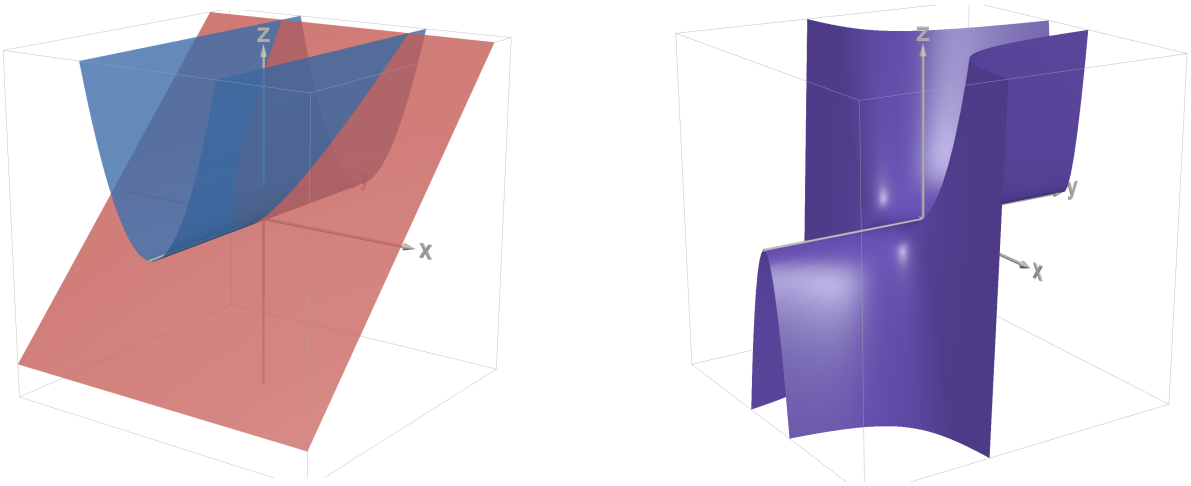


Figure 2.2: A visulisation of the 1-tensors $R(y) = y + 1$ in red and $B(x) = x^2$ in blue (left) and their product, the 2-tensor $P(x, y) = R(y)B(x) = yx^2 + y$ (right). Thus $P(x, y)$ is a slice so $\operatorname{srk}(P) = 1$.

Remark 2.10. *Let's now compare the notion of the slice rank of a* 2*-tensor and the rank of the corresponding matrix. Recalling some linear algebra, the rank of a matrix is the number of linearly independent rows. Thus, a rank* 1 *matrix has rows which are all multiples of each other. Thus, we can rewrite a rank* r *matrix as a sum of* r *rank* 1 *matrices, where all the rows in each of the rank* 1 *matrices are multiples of one of the* r *linearly independent rows in our rank* r *matrix. In the other direction, using that for two matrices* A *and* B*,* $\operatorname{rank}(A + B) \leq \operatorname{rank}(A) + \operatorname{rank}(B)$*, then the rank of* $r - 1$ *rank* 1 *matrices is at most* $r - 1$*, so we need to sum at least* r *rank* 1 *matrices to get back to our rank* r *matrix. Thus the rank of a matrix is the smallest integer* r *such that the matrix can be written as a sum of* r *rank* 1 *matrices. Finally, we notice that a rank* 1 *matrix* $M \in M_n(\mathbb{F})$ *can be written in the form* $M = uv^T$ *for some* $u, v \in \mathbb{F}^n$ *and thus, the corresponding* 2*-tensor is a product of two* 1*-tensors*

given by $T_M(i,j) = T_u(i)T_v(j)$ where $T_u, T_v : [n] \to \mathbb{F}$ given by $T_u(i) = u_i$ and $T_v(j) = v_j$. Now it is clear that the notions of slice rank for 2-tensors and rank of the corresponding matrix are identical so slice rank is indeed a generalisation of the notion of rank for square matrices.

Now, we will prove two results which will provide the machinery for our later proofs.

Lemma 2.11. *For a k-tensor $T : X^k \to \mathbb{F}$, $\mathrm{srk}(T) \leq |X|$.*

Proof. We can rewrite $T(x_1, ..., x_k) = \sum_{a \in X} \mathbb{I}_{\{a\}}(x_1)\, T(a, x_2, ...x_k)$. □

It is a standard result in linear algebra that the rank of a diagonal matrix is equal to the number of non-zero diagonal entries. In [Tao16], Tao proved that this result extends to diagonal k-tensors, commonly referred to as the slice rank lemma which we now prove.

Lemma 2.12. *[Slice rank lemma] For $k \geq 2$, the slice rank of a diagonal k-tensor is equal to the number of non-zero diagonal elements.*

Proof. We induct on k, with base case $k = 2$. In Remark 2.10, we showed that, for 2-tensors, their slice rank was equivalent to the rank of the corresponding matrix. Thus, since the rank of a diagonal matrix is equal to the number of non-zero diagonal entries, it follows that the slice rank of a diagonal 2-tensor is just equal to the number of non-zero diagonal elements.

For the induction step, assume the $k-1$ case. Let $T : X^k \to \mathbb{F}$ be our diagonal k-tensor and thus, we can write $T(x) = \sum_{a \in X} c_a \prod_{i \in [k]} \mathbb{I}_{\{a\}}(x_i)$ for some $c_a \in \mathbb{F}$. Letting $A \coloneqq \{a \in X : c_a \neq 0\}$,we then have $T(x) = \sum_{a \in A} c_a \prod_{i \in [k]} \mathbb{I}_{\{a\}}(x_i)$. It is now clear that $\mathrm{srk}(T) \leq |A|$ since $\prod_{i \in [k]} \mathbb{I}_{\{a\}}(x_i)$ are all slices. Seeking a contradiction, assume $\mathrm{srk}(T) < |A|$, then, we can write $T(x) = \sum_{i \in [k]} \sum_{\alpha \in I_i} f_{i,\alpha}(x_i) g_{i,\alpha}(x^{\{i\}})$ for some indexing sets $I_1, ..., I_k$ where $\sum_{i \in [k]} |I_k| < |A|$ and 1-tensors $f_{i,\alpha} : A \to \mathbb{F}$ and $(k-1)$-tensors $g_{i,\alpha} : A^{k-1} \to \mathbb{F}$. For 1-tensors $f, g : A \to \mathbb{F}$, we consider the subspace V orthogonal to all $f_{k,\alpha}$ for all $\alpha \in I_k$, with respect to our bilinear form (f, g),

$$V \coloneqq \langle f_{k,\alpha} : \alpha \in I_k \rangle^{\perp} = \left\{ h : A \to \mathbb{F} : \sum_{a \in A} h(a) f_{k,\alpha}(a) = 0 \, \forall \alpha \in I_k \right\}.$$

Since the space of 1-tensors has a basis $\{\mathbb{I}_{\{a\}}(x) : a \in A\}$, it has dimension $|A|$, and since $\dim\langle f_{k,\alpha} : \alpha \in I_k \rangle \leq |I_k|$ then $\dim V \geq |A| - |I_k|$. Construct the $\dim V \times |A|$ matrix with columns given by basis vectors for V in the basis $\{\mathbb{I}_{\{a\}}(x) : a \in A\}$. This matrix has rank $\dim V$ so we can find $|A| - \dim V$ linearly dependent rows and remove them leaving us with a full rank $\dim V \times \dim V$ matrix, with rows indexed by elements $a \in A'$ for some subset $A' \subseteq A$. Thus $\langle \mathbb{I}_{\{a\}}(x) : a \in A' \rangle$ is contained in the image of our original $\dim V \times |A|$ matrix and thus there exists a 1-tensor $h \in V$ which is non-zero on A' where $|A'| = \dim V \geq |A| - |I_k|$. Multiplying T by $h(x_k)$ and summing over $x_k \in A$,

$$\begin{aligned}
\sum_{x_k \in A} T(x) h(x_k) &= \sum_{x_k \in A} \sum_{i \in [k]} \sum_{\alpha \in I_i} f_{i,\alpha}(x_i) h(x_k) g_{i,\alpha}(x^{\{i\}}) \\
&= \sum_{i \in [k-1]} \sum_{\alpha \in I_i} \sum_{x_k \in A} f_{i,\alpha}(x_i) h(x_k) g_{i,\alpha}(x^{\{i\}}) + \sum_{\alpha \in I_k} \left(\sum_{x_k \in A} f_{k,\alpha}(x_k) h(x_k) \right) g_{k,\alpha}(x^{\{k\}}) \qquad (2.1) \\
&= \sum_{i \in [k-1]} \sum_{\alpha \in I_i} \sum_{x_k \in A} f_{i,\alpha}(x_i) h(x_k) g_{i,\alpha}(x^{\{i\}}) = \sum_{i \in [k-1]} \sum_{\alpha \in I_i} f_{i,\alpha}(x_i) \widehat{g}_{i,\alpha}(x^{\{i\}})
\end{aligned}$$

where $\widehat{g}_{i,\alpha}(x_1, ..., x_{i-1}, x_{i+1}, ..., x_{k-1}) = \sum_{x_k \in A} g_{i,\alpha}(x^{\{i\}}) h(x_k)$. This is a double sum of slices and thus has slice rank at most $\sum_{i \in [k-1]} |I_k| < |A| - |I_k|$. However, we can also write

$$\sum_{x_k \in A} T(x) h(x_k) = \sum_{a \in A} c_a \left(\sum_{x_k \in A} h(x_k) \mathbb{I}_{\{a\}}(x_k) \right) \prod_{i \in [k-1]} \mathbb{I}_{\{a\}}(x_i) = \sum_{a \in A} c_a h(a) \prod_{i \in [k-1]} \mathbb{I}_{\{a\}}(x_i)$$

which is a diagonal $(k-1)$-tensor where $c_a h(a)$ is non-zero for all $a \in A'$. Thus, by our induction hypothesis, we know that it has slice rank at least $|A'| \geq |A| - |I_k|$ and thus we have a contradiction. $\square$

Although we have now reformulated things in terms of k-tensors and slice rank, the essence of the slice rank lemma, Lemma 2.12, is the same technique from the Croot-Lev-Pach Lemma which we saw when we were dealing with s-distance sets in Section 2.1. In the proof of the slice rank lemma, it occurred in Equation 2.1 when we started pulling apart our big $(k-1)$-tensor and then using our orthogonality condition to set it equal to zero. The slice rank lemma will act as the crux of the proofs in the following two sections when we want to give bounds on the size of sets using the properties of elements of those sets. The utility of the slice rank lemma comes from defining a well-picked k-tensor T say on the set X, the size of which we want to bound ie. $T : X \to \mathbb{F}$ for some field $\mathbb{F}$. We then show that T is diagonal and is non-zero along its diagonal so we can invoke the slice rank lemma to show $|X| = \text{srk}(T)$. Now, we can simply split T into a sum of slices and give a bound on $\text{srk}(T)$ and thus $|X|$.

In addition to the standard rank and slice rank, there is also the concept of partition rank. In fact, identically to slice rank, the partition rank of a diagonal k-tensor is equal to the number of non-zero diagonal elements. As we will see in the case of slice rank in Sections 2.3 and Section 2.4, this is the key fact that allows us to leverage combinatorial results and this is also used in the case of partition rank by Naslund in [Nas20] where it is used to give an upper bound on the size of sets in $\mathbb{F}_q^n$ not containing corners.

2.3 Sunflowers

It is finally time to implement the theory we have been cooking up in Section 2.2, in order to prove an upper bound on the size of sunflower free sets, first shown in 2017 in Naslund and Sawin's paper [NS17].

Definition 2.13. *A collection of k sets, $\{S_i \subseteq [n] : i \in [k]\}$, is a k-sunflower if the intersection of any two distinct sets from the collection is the same set ie. $S_i \cap S_j = S \ \forall i, j \in [k]$ for some set $S \subseteq [n]$. Furthermore, a collection of sets $\mathcal{F}$ is called k-sunflower free if $\mathcal{F}$ doesn't contain any k-sunflowers and if $\mathcal{F}$ doesn't contain any 3-sunflowers then $\mathcal{F}$ is just called sunflower free.*

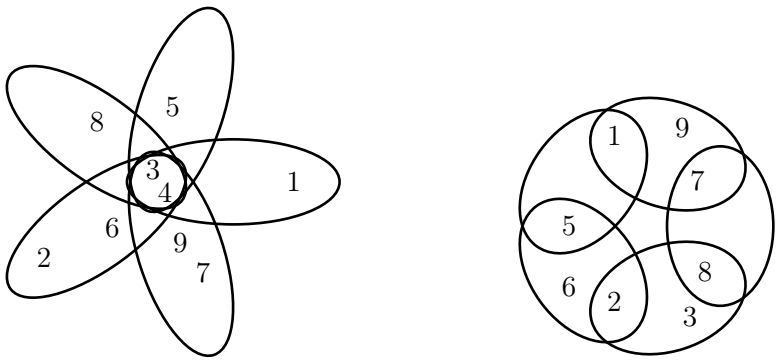


Figure 2.3: A visualisation of a k-sunflower and a sunflower free collection where $n = 9, k = 5$.

The concept of a k-sunflower goes back to Erdős who proposed the following two conjectures alongside Rado in [ER60] and Szemerédi in [ES78].

Conjecture 2.14 (Erdős-Rado sunflower conjecture)**.** *For $k \geq 3$ and $\mathcal{F}$ a k-sunflower free collection of sets all of size n, then $|\mathcal{F}| \leq C_k^n$ for some $C_k > 0$ depending only on k.*

Conjecture 2.15 (Erdős-Szemerédi sunflower conjecture)**.** *For $k \geq 3$ and $\mathcal{F}$ a k-sunflower free collection of subsets of $[n]$, then $|\mathcal{F}| \leq c_k^n$ for some $c_k < 2$ depending only on k.*

Both conjectures are still unsolved as of today however progress on the Erdős-Rado sunflower conjecture has recently been made in [Alw+20]. In addition, Theorem 2.16, which we prove now, following Naslund and Sawin's proof in [NS17], is the $k = 3$ case of the Erdős-Szemerédi Sunflower Conjecture.

Theorem 2.16. *If $\mathcal{F}$ is a sunflower free collection of subsets of $[n]$, then $|\mathcal{F}| \leq 3(n+1)\left(\frac{3}{\sqrt[3]{4}}\right)^n$ so $|\mathcal{F}| = O(1.89^n)$.*

Proof. Define $\mathcal{S}_j \coloneqq \{x_S \in \mathbb{R}^n : S \in \mathcal{F}, |S| = j\} \subseteq \mathbb{R}^n$ using characteristic vector notation as in Definition 1.2. Then define the 3-tensor $T : \mathcal{S}_j^3 \to \mathbb{R}$, where

$$T(x,y,z) = \prod_{i=1}^{n}(2 - (x+y+z)_i)$$

and we claim that T is a diagonal 3-tensor. Indeed, since $\mathcal{F}$ is a sunflower free set, then for any 3 distinct sets $A, B, C \in \mathcal{F}$, $\exists\, i \in [n]$ such that $(x_A + x_B + x_C)_i = 2$. Thus, for distinct $x_A, x_B, x_C \in \mathcal{S}_j \subseteq \mathcal{F}$, $\exists\, i \in [n]$ such that $2 - (x_A + x_B + x_C)_i = 0$ so $T(x_A, x_B, x_C) = 0$. In addition, for distinct $A, B \in \mathcal{S}_j$, since $|A| = |B|$, then $A \not\subseteq B$ so $\exists\, i \in [n]$ such that $(x_A + x_A + x_B)_i = 2$ and as before, $T(x_A, x_A, x_B) = 0$.

We can now apply Lemma 2.12 to T and since, for any $x_A \in \mathcal{S}_j$, $T(x_A, x_A, x_A) = (-1)^j 2^{n-j} \neq 0$, then $|\mathcal{S}_j| = \operatorname{srk}(T)$. All we need to do now is find an upper bound on $\operatorname{srk}(T)$ by decomposing $T(x,y,z)$ into slices.

Denoting $x^I \coloneqq \prod_{i \in I} x_i$ for some $I \subseteq [n]$, we can expand T as

$$T(x,y,z) = \sum_{I \sqcup J \sqcup K \sqcup L = [n]} (-1)^{|I|+|J|+|K|} 2^{|L|} x^I y^J z^K$$

which, as a polynomial, clearly has degree at most n. By the pigeonhole principle, given any monomial $x^I y^J z^K$ in T as above, one of I, J, K has size at most $\frac{n}{3}$. Thus, there are constants $c_{IJKL}, d_{IJKL}, e_{IJKL} \in \mathbb{R}$, such that we can further decompose

$$\begin{aligned} T(x,y,z) &= \sum_{\substack{I \sqcup J \sqcup K \sqcup L = [n] \\ |I| \leq \frac{n}{3}}} c_{IJKL} x^I y^J z^K + \sum_{\substack{I \sqcup J \sqcup K \sqcup L = [n] \\ |J| \leq \frac{n}{3}}} d_{IJKL} x^I y^J z^K + \sum_{\substack{I \sqcup J \sqcup K \sqcup L = [n] \\ |K| \leq \frac{n}{3}}} e_{IJKL} x^I y^J z^K \\ &= \sum_{\substack{I \subseteq [n] \\ |I| \leq \frac{n}{3}}} x^I f(y,z) + \sum_{\substack{J \subseteq [n] \\ |J| \leq \frac{n}{3}}} y^J g(x,z) + \sum_{\substack{K \subseteq [n] \\ |K| \leq \frac{n}{3}}} z^K h(x,y) \end{aligned}$$

for some 2-tensors $f, g, h : \mathcal{S}_j^2 \to \mathbb{R}$. However, we now see that each term in each sum is a slice since, for $I \subseteq [n]$ then $x^I = \prod_{i \in I} x_i$ is still a 1-tensor and thus

$$\operatorname{srk}(T) \leq 3 \sum_{\substack{I \subseteq [n] \\ |I| \leq \frac{n}{3}}} 1 = 3 \sum_{i=0}^{\frac{n}{3}} \binom{n}{i} \quad \text{so} \quad |\mathcal{F}| = \sum_{j=0}^{n} |\mathcal{S}_j| \leq 3(n+1) \sum_{i=0}^{\frac{n}{3}} \binom{n}{i}$$

To find an explicit constant, let $m(t) = \frac{1+t}{\sqrt[3]{t}}$ defined for $t \in (0,1)$. Then, $\forall t \in (0,1)$,

$$(m(t))^n = t^{-\frac{n}{3}}(1+t)^n = t^{-\frac{n}{3}} \sum_{i=0}^{n} \binom{n}{i} t^i = \sum_{i=0}^{n} \binom{n}{i} t^{i-\frac{n}{3}} > \sum_{i=0}^{\frac{n}{3}} \binom{n}{i} t^{i-\frac{n}{3}} \geq \sum_{i=0}^{\frac{n}{3}} \binom{n}{i}$$

since $t^{i-\frac{n}{3}} \geq 1$ when $t \in (0,1)$ and $i \leq \frac{n}{3}$. $m(\frac{1}{2}) = \frac{3}{\sqrt[3]{4}}$, so $|\mathcal{F}| \leq 3(n+1)\left(\frac{3}{\sqrt[3]{4}}\right)^n$ and $\frac{3}{\sqrt[3]{4}} < 1.89$. $\square$

2.4 SET®

The game of SET is an easy-to-learn card game where players study a selection of cards and have to try and form 'sets' of 3 cards. Each card has 1 out of 3 possibilities for each of the 4 properties; colour, number, shape and shading. Since each card is unique, the deck consists of $3^4 = 81$ cards. 3 cards are said to form a 'set' if, for all 4 properties separately, the cards either all share the same feature or all have distinct features. Equivalently, for any property, a 'set' can **not** have two cards with the same feature and the third, a different feature from the other two.

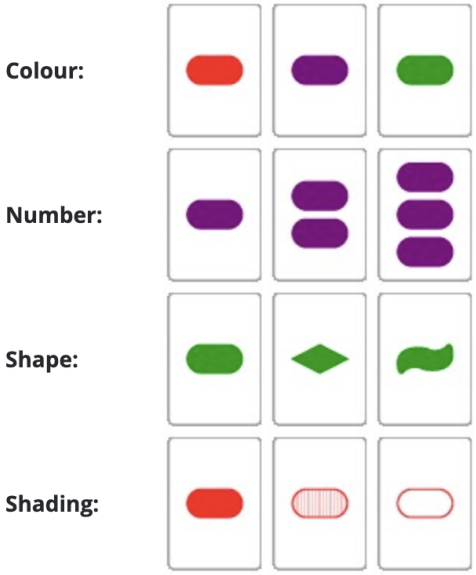


Figure 2.4: The 4 properties of cards in SET with examples, taken from [Aus16].

A game of SET begins with the dealer dealing out 12 cards, at which point the players have to start frantically trying to make 'sets', each of which earns them a point. This begs the question: can we guarantee that there will always be a 'set' having dealt any 12 cards from the deck? The rules of the game luckily cover for this by stating that if there are no 'sets' the dealer keeps dealing until one appears. So, in theory, how many cards would the dealer have to deal to guarantee a 'set' exists?

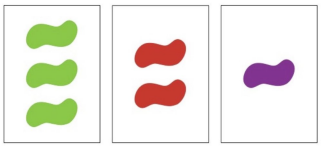


Figure 2.5: A 'set' in the game SET, from [Mar21].

As is often the case in maths, this question had already been answered in 1970 by Pellegrino in [Pel70] before the game of SET had even been invented by geneticist Marsha Falco in 1974. Pellegrino proved that, as long as the dealer deals 21 cards, there is guaranteed to be a 'set'. Using a program from his repository, [Knu], Knuth calculated there are 682344 'set'-less hands of 20 cards (a minute percentage of the possible number of hands of 20 cards). However, what if we added another property to the cards with 3 distinct choices ie. each card now has a background from a choice of 3 backgrounds? We could then create a deck with $3^5 = 243$ cards, but now would not know how many cards the dealer would need to deal to guarantee a 'set' where we extend the definition of a 'set' to include this extra property?

We can restate the game and its infinitely-many extensions in mathematical terms by treating each card as an element of the vector space $\mathbb{F}_3^n$ for $n \in \mathbb{N}$ with each dimension corresponding to a property of the cards. Note that for $x, y, z \in \mathbb{F}_3$ then $x + y + z = 0 \Leftrightarrow x = y = z$ or x, y, z are all distinct. Thus $a, b, c \in \mathbb{F}_3^n$ form a 'set' $\Leftrightarrow a_i + b_i + c_i = 0, \forall\, i \in [n] \Leftrightarrow a + b + c = 0$.

Definition 2.17. *A cap set is a subset $A \subseteq \mathbb{F}_3^n$ such that, for any distinct $a, b, c \in A$, $a + b + c \neq 0$.*

Maximal cap sets have been verified manually up to $n = 5$, constructed in [Ede+02]. Upper bounds are given for $6 \leq n \leq 10$ in [DM03] and a 6-cap of size 112 is constructed in [CF94], seen in Table 2.2.

n	1	2	3	4	5	6	7	8	9	10
size of maximal cap set	2	4	9	20	45	$112 \leq \quad \leq 114$	≤ 291	≤ 771	≤ 2070	≤ 5619

Table 2.2: A table showing the known sizes of maximal cap sets in dimensions 1 through 10.

The result that brought cap sets, and, indeed, the polynomial method, to the attention of many, and which we state and prove now, was the bound on maximal cap sets proved in [EG16], coauthored by Ellenberg and Gijswijt. The crux of their argument relies on the Croot-Lev-Pach Lemma, and it was only after [EG16] was published that Tao formulated the slice rank lemma and rewrote the proof of the bound in terms of k-tensors in [Tao16]. Similar to our proof of the bound on the size of sunflower free sets, having put in the groundwork by proving the slice rank lemma, the result falls out defining a 3-tensor on our cap set and then finding an upper bound on its slice rank by decomposing it into slices.

Theorem 2.18. *If $A \subseteq \mathbb{F}_3^n$ is a cap set, then $|A| \leq 3(2.76)^n$ ie. $|A| = O(2.76^n)$.*

Proof. We start by defining a 3-tensor $T : A^3 \to \mathbb{F}_3$ with a very similar form to the one we constructed in the sunflower case, where

$$T(x, y, z) = \prod_{i \in [n]} (1 - (x_i + y_i + z_i)^2)$$

and we claim that T is diagonal. Indeed, since A is a cap set, then for distinct $a, b, c \in A$, $\exists\, i$ such that $a_i + b_i + c_i \neq 0$. Using that for non-zero $x \in \mathbb{F}_3$ then $1 - x^2 = 0$, we have $T(a, b, c) = 0$ for distinct $a, b, c \in A$. In addition, similar logic holds assuming $a = b \neq c$, since then $2b + c \neq 0$ so $a + b + c \neq 0$. Finally $T(a, a, a) = 1$ and so it turns out that T is the 'identity' 3-tensor on A in some sense. However, it is enough that it is non-zero along its diagonal since it follows by Lemma 2.12 that $|A| = \mathrm{srk}(T)$. We now find an upper bound on the slice rank of T in a similar way to before.

As a polynomial, T clearly has degree at most $2n$. For some $c_{\alpha\beta\gamma} \in \mathbb{F}_3$, we can expand T as

$$T(x, y, z) = \sum_{\alpha,\beta,\gamma \in \{0,1,2\}^n} c_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma$$

so by the pigeonhole principle, given any monomial $x^\alpha y^\beta z^\gamma$ in T as above, one of $|\alpha|, |\beta|, |\gamma|$ has size at most $\frac{2n}{3}$. Thus $\exists\, c_{\alpha\beta\gamma}, d_{\alpha\beta\gamma}, e_{\alpha\beta\gamma} \in \mathbb{F}_3$, such that we can further decompose

$$\begin{aligned} T(x, y, z) &= \sum_{\substack{\alpha,\beta,\gamma \in \{0,1,2\}^n \\ |\alpha| \leq \frac{2n}{3}}} c_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma + \sum_{\substack{\alpha,\beta,\gamma \in \{0,1,2\}^n \\ |\beta| \leq \frac{2n}{3}}} d_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma + \sum_{\substack{\alpha,\beta,\gamma \in \{0,1,2\}^n \\ |\gamma| \leq \frac{2n}{3}}} e_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma \\ &= \sum_{\substack{\alpha \in \{0,1,2\}^n \\ |\alpha| \leq \frac{2n}{3}}} x^\alpha f(y, z) + \sum_{\substack{\beta \in \{0,1,2\}^n \\ |\beta| \leq \frac{2n}{3}}} y^\beta g(x, z) + \sum_{\substack{\gamma \in \{0,1,2\}^n \\ |\gamma| \leq \frac{2n}{3}}} z^\gamma h(x, y) \end{aligned}$$

for some 2-tensors $f, g, h : A^2 \to \mathbb{F}_3$. However, we now see that each term in each sum is a slice since for $\alpha \in \{0, 1, 2\}^n$, then $x^\alpha = \prod_{i \in [n]} x_i^{\alpha_i}$ is still a 1-tensor and thus

$$\mathrm{srk}(T) \leq 3 \sum_{\substack{\alpha \in \{0,1,2\}^n \\ |\alpha| \leq \frac{2n}{3}}} 1 = 3 \sum_{\substack{i,j,k \in \mathbb{N}_0 \\ i+j+k=n \\ j+2k \leq \frac{2n}{3}}} \frac{n!}{i!j!k!}$$

by treating i, j, k as the number of 0's, 1's, 2's respectively that α has as coordinates.

To find an explicit constant, let $m(t) = \frac{1+t+t^2}{\sqrt[3]{t^2}}$ defined for $t \in (0, 1)$. Then, $\forall t \in (0, 1)$,

$$\begin{aligned} (m(t))^n = t^{-\frac{2n}{3}}(1 + t + t^2)^n = t^{-\frac{2n}{3}} \sum_{\substack{i,j,k \in \mathbb{N}_0 \\ i+j+k=n}} \frac{n!}{i!j!k!} t^{j+2k} = \sum_{\substack{i,j,k \in \mathbb{N}_0 \\ i+j+k=n}} \frac{n!}{i!j!k!} t^{j+2k-\frac{2n}{3}} \\ \geq \sum_{\substack{i,j,k \in \mathbb{N}_0 \\ i+j+k=n \\ j+2k \leq \frac{2n}{3}}} \frac{n!}{i!j!k!} t^{j+2k-\frac{2n}{3}} \geq \sum_{\substack{i,j,k \in \mathbb{N}_0 \\ i+j+k=n \\ j+2k \leq \frac{2n}{3}}} \frac{n!}{i!j!k!} \end{aligned}$$

since $t^{j+2k-\frac{2n}{3}} \geq 1$ when $t \in (0, 1)$ and $j + 2k \leq \frac{2n}{3}$. $m(\frac{\sqrt{33}-1}{8}) < 2.76$, so $|A| = \mathrm{srk}(T) \leq 3(2.76)^n$. $\square$

Chapter 3

Combinatorial Nullstellensatz

The Combinatorial Nullstellensatz, closely related to Hilbert's famous Nullstellensatz, is one of the most powerful and versatile tools in the polynomial method's arsenal (Nullstellensatz is German for "theorem about zero points") and is widely used in both extremal and existence problems. It is unique from the polynomial methods we have been studying so far in Chapters 1 and 2, as it does not require theory about vector spaces or rank, just the algebraic information contained in the polynomial. The Combinatorial Nullstellenstaz was first formulated by Alon and Tarsi in 1989 in [AT89] and later developed by Alon, Nathanson and Rusza in 1996 in [ANR96]. Then, in 1999, it was reformulated a final time by Alon in [Alo99], where he used it to provide deceptively short proofs for a range of results from combinatorics, number theory and graph theory, some of which we explore now.

3.1 Chevalley-Warning Theorem

Before we prove the Chevalley-Warning Theorem, we need the following Lemma from Section 9.4 of [TV06], which incorporates a useful technique from the polynomial method. This technique relies on the simple observation that, for a finite field $\mathbb{F}$, a polynomial $P \in \mathbb{F}[t]$ and a bijection $\phi : \mathbb{F} \to \mathbb{F}$, then $\sum_{a\in\mathbb{F}} P(a) = \sum_{a\in\mathbb{F}} P(\phi(a))$. Usually we will take ϕ to be the map $t \mapsto st$ for some $s \in \mathbb{F}^\times$.

Lemma 3.1. *Let $\mathbb{F}$ be a finite field and $n \in \mathbb{N}$. For some $t = (t_1, ..., t_n) \in \mathbb{N}_0^n$ such that $\exists\, i \in [n]$ where $t_i < |F| - 1$, then $\sum_{x\in\mathbb{F}^n} x^t = 0$.*

Proof. Clearly $\sum_{x\in\mathbb{F}^n} x^t = \left(\sum_{x\in\mathbb{F}^{n-1}} x_1^{t_1}...x_{i-1}^{t_{i-1}}x_{i+1}^{t_{i+1}}...x_n^{t_n}\right)\left(\sum_{x_i\in\mathbb{F}} x_i^{t_i}\right)$ where $0 \le t_i < |F| - 1$. If $t_i = 0$, then $\sum_{x_i\in\mathbb{F}} x_i^{t_i} = |F| = 0$ and we are done. Now, let $t_i > 0$ and ω be a primitive $(|\mathbb{F}| - 1)$th root of unity ie. $\langle\omega\rangle = \mathbb{F}^\times$ and consider the map $\phi : \mathbb{F} \to \mathbb{F}$, $a \mapsto \omega a$. Since ϕ is a bijection, then $0 = \sum_{x_i\in\mathbb{F}} \phi(x_i)^{t_i} - \sum_{x_i\in\mathbb{F}} x_i^{t_i} = \sum_{x_i\in\mathbb{F}} \omega^{t_i} x_i^{t_i} - \sum_{x_i\in\mathbb{F}} x_i^{t_i} = (\omega^{t_i} - 1)\sum_{x_i\in\mathbb{F}} x_i^{t_i}$. Since $0 < t_i < |F| - 1$, $\omega^{t_i} \neq 1$ and thus $\sum_{x_i\in\mathbb{F}} x_i^{t_i} = 0$. □

We will now state and prove the Chevalley-Warning Theorem, which can be seen as a predecessor to the Combinatorial Nullstellensatz, also following as a Corollary. According to Chapter 14 from Clark's lecture notes, [Cla09], Artin originally conjectured Corollary 3.4 as a problem for his student, Ewald Warning, to solve. However, on a visit to Göttingen in 1935, Chevalley managed to get wind of the problem and was the first to prove it. Warning went on to prove what is now known as the Chevalley-Warning Theorem which is, in fact, the stronger statement.

Theorem 3.2 (Chevalley-Warning Theorem)**.** *Let $\mathbb{F}$ be a finite field and let $h_i \in \mathbb{F}[x_1, ..., x_n]$ for $i \in [n]$ such that $\sum_{i\in[n]} \deg(h_i) < n$. Then the number of solutions $x = (x_1, ..., x_n) \in \mathbb{F}^n$ satisfying $h_i(x) = 0$ for all $i \in [n]$ is a multiple of* $\mathrm{char}(\mathbb{F})$.

Proof. Since we are working in a finite field, we have $\mathbb{I}_{\{0\}}(t) = 1 - t^{|\mathbb{F}|-1}, \forall\, t \in \mathbb{F}$. Thus, an indicator function for when an h_i evaluates to zero can be written simply as $\mathbb{I}_{Z(h_i)}(x) = 1 - (h_i(x))^{|\mathbb{F}|-1}$. Defining $Z(h) \coloneqq \{x \in \mathbb{F}^n : h_i(x) = 0\ \forall i \in [n]\}$,

$$\mathbb{I}_{Z(h)}(x) = \prod_{i\in[n]} \mathbb{I}_{Z(h_i)} = \prod_{i\in[m]} (1 - h_i(x)^{|\mathbb{F}|-1}) = \sum_{t\in\mathbb{N}_0^n} c_t x^t$$

for some $c_t \in \mathbb{F}$. It is clear that the degree of every monomial $\deg(x^t) = \sum_{i\in[n]} t_i \leq (\mathbb{F}-1)\sum_{i\in[n]} \deg(h_i) < n(\mathbb{F}-1)$ since $\sum_{i\in[n]} \deg(h_i) < n$ by assumption. Thus by the pigeonhole principle, for every monomial x^t, $\exists\, i \in [n]$ such that $t_i < |\mathbb{F}| - 1$ so, using Lemma 3.1 and working modulo $\mathrm{char}(\mathbb{F})$,

$$\begin{aligned} |\{x \in \mathbb{F}^n : h_i(x) = 0\, \forall\, i \in [m]\}| &\equiv \sum_{x\in\mathbb{F}^n} \mathbb{I}_{Z(h)}(x) = \sum_{x\in\mathbb{F}^n}\sum_{t\in\mathbb{N}_0^n} c_t x^t \\ &= \sum_{t\in\mathbb{N}_0^n} c_t \sum_{x\in\mathbb{F}^n} x^t = 0 \end{aligned}$$

□

The following Corollary follows since $\mathrm{char}(\mathbb{F})$ is prime and is thus at least 2.

Corollary 3.3. *If there is one solution, $x = (x_1, ..., x_n) \in \mathbb{F}^n$ satisfying $h_i(x) = 0$ for all $i \in [n]$, then there must exist at least one other solution.*

Corollary 3.4. *If the h_i are homogeneous polynomials ie. $h_i(0) = 0\ \forall i \in [n]$ then there exists $v \neq 0$ satisfying $h_i(v) = 0\ \forall i$.*

There is still research into various generalisations of the Chevalley-Warning Theorem, including [Bri11], which uses the Combinatorial Nullstellensatz to prove an extension of the Chevalley-Warning where we allow variables to be restricted to arbitrary subsets.

We now reuse the observation we introduced at the start of this section to prove a beautiful result about how the size of the output of a polynomial of 1 variable depends on its degree. It was first proved by Wan in [Wan87] using p-adic liftings, after which Turnwald gave a much simpler argument in [Tur88] which we present here.

Theorem 3.5. *Let $\mathbb{F}$ be a finite field and let $P \in \mathbb{F}[t]$ be a polynomial of degree n. Then $P(\mathbb{F}) = \{a \in \mathbb{F} : \exists\, t \in \mathbb{F}, P(t) = a\}$ is either equal to $\mathbb{F}$ or has size at most $|\mathbb{F}| - \frac{|\mathbb{F}|-1}{n}$.*

Taking $P(t) = t$, then $P(\mathbb{F}) = \mathbb{F}$ and it is shown in [CM96] that the latter bound is sharp, in particular, if we take the polynomial $P(t) = (t-1)t^{p-1}$ where $p = \mathrm{char}(\mathbb{F})$.

Proof. Subtracting a constant from P does not change $|P(\mathbb{F})|$ so we assume $P(0) = 0$. Now define $Q \in \mathbb{F}[t]$ where

$$Q(t) = \prod_{a\in\mathbb{F}} (t - P(a)) = t^{|\mathbb{F}|} + \sum_{i=0}^{|\mathbb{F}|-1} c_i t^i \tag{3.1}$$

for some $c_i \in \mathbb{F}$ and $Z(Q) = P(\mathbb{F})$. Since $\mathbb{F}$ is a field, for $s \in \mathbb{F}^\times$ then $t \mapsto st$ for $t \in \mathbb{F}$ is a bijection and thus we also have

$$Q(t) = \prod_{a\in\mathbb{F}} (t - P(a)) = \prod_{a\in\mathbb{F}} (t - P(sa)) = t^{|\mathbb{F}|} + \sum_{i=0}^{|\mathbb{F}|-1} p_i(s) t^i \tag{3.2}$$

for some polynomials p_i which have degree at most $n(|\mathbb{F}| - i)$. Equating coefficients of Q in the RHS of Equation 3.1 and Equation 3.2, we have $p_i(s) = c_i$ for all $s \in \mathbb{F}^\times$ and thus defining polynomials

$q_i(s) \coloneqq p_i(s) - c_i$ then $Z(q_i) \subseteq \mathbb{F}^\times$ and $\deg(q_i) \leq n(|\mathbb{F}| - i)$. Now by the Factor Theorem, Lemma 1.7, if $n(|\mathbb{F}| - i) < |\mathbb{F}| - 1$ then $q_i(s) \equiv 0$ and thus $p_i(s) \equiv c_i$. However, since $\prod_{a\in\mathbb{F}}(t - P(sa)) = \sum_{i=0}^{|\mathbb{F}|} p_i(s)t^i$ holds $\forall\, s \in \mathbb{F}$ and $P(0) = 0$ then plugging in $s = 0$ gives us that $p_i(s) = 0$ and thus $c_i = 0, \forall\, i > |\mathbb{F}| - \frac{|\mathbb{F}|-1}{n}$. Finally, define $\hat{Q} \in \mathbb{F}[t]$ where

$$\hat{Q}(t) \coloneqq Q(t) - (t^{|\mathbb{F}|} - t) = t^{|\mathbb{F}|} + \left(\sum_{i=0}^{|\mathbb{F}|-1} c_i t^i\right) - (t^{|\mathbb{F}|} - t) = \left(\sum_{i=0}^{|\mathbb{F}|-\frac{|\mathbb{F}|-1}{n}} c_i t^i\right) - t$$

so $\deg(\hat{Q}) \leq |\mathbb{F}| - \frac{|\mathbb{F}|-1}{n}$. Since $t^{|\mathbb{F}|} - t = 0, \forall\, t \in \mathbb{F}$, then $Z(\hat{Q}) = Z(Q) = P(\mathbb{F})$ and if $\hat{Q}$ is a non-zero polynomial then we use the Factor Theorem, Lemma 1.7, once more to conclude that $|P(\mathbb{F})| = |Z(\hat{Q})| \leq |\mathbb{F}| - \frac{|\mathbb{F}|-1}{n}$. If $\hat{Q}(t) \equiv 0$ then $Q(t) \equiv t^{|\mathbb{F}|} - t \equiv \prod_{a\in\mathbb{F}}(t - a) \equiv \prod_{a\in\mathbb{F}}(t - P(a))$ and thus $P(\mathbb{F}) = \mathbb{F}$. □

3.2 Combinatorial Nullstellensatz

We now state and prove the Combinatorial Nullstellensatz, Theorem 1.2 in Alon's paper, [Alo99].

Theorem 3.6 (Combinatorial Nullstellensatz)**.** *Given an arbitrary field $\mathbb{F}$, let $P \in \mathbb{F}[x_1, ..., x_n]$ be a polynomial of degree $d_1 + ... + d_n$ where the coefficient of $x_1^{d_1}...x_n^{d_n}$ in P is non-zero. Then P does not vanish on any set of the form $E_1 \times ... \times E_n$ where $E_1, ..., E_n \subseteq \mathbb{F}$ and $|E_1| > d_1, ..., |E_n| > d_n$.*

In [Alo99], Theorem 3.6 in fact follows as a corollary from a result that we state in Section 3.7, but which has a technical proof. Instead, we prove Theorem 3.6 from scratch in a short proof by Michałek from [Mic10].

Proof. We prove this by induction on the degree of P. Clearly, if $\deg(P) = 0$, the results follows immediately. If $\deg(P) = 1$, exactly one d_j is non-zero, so, taking any values in E_k for $k \neq j$, and plugging them into the polynomial, we have a linear polynomial in one variable since $\deg(P) = 1$. Thus, since $|E_j| > 1$, there is an element in E_j at which the polynomial is non-zero.

Now, for the induction step, suppose $\deg(P) > 1$ and the claim is true when $\deg(P) = n - 1$. Looking for a contradiction, assume $P(x) = 0$ for all $x \in E_1 \times ... \times E_n$, and, without loss of generality, assume $d_1 > 0$. Fixing some $a \in E_1$, write $P = (x_1 - a)Q + R$ using the long division algorithm where we treat P as a polynomial in x_1 over the ring $\mathbb{F}[x_2, ..., x_n]$. Since, $\deg(R) < \deg(x_1 - a) = 1$, R is a constant in the ring $\mathbb{F}[x_2, ..., x_n]$ and thus doesn't contain the variable x_1. Using the original conditions on P , Q must have a non-vanishing monomial of the form $x_1^{d_1-1}x_2^{d_2}...x_n^{d_n}$ and also $\deg(Q) = \deg(P) - 1$. Now for any $x \in \{a\} \times E_2 \times ... \times E_n$, $P(x) = 0$ which implies $R(x) = 0$ also. However, R doesn't contain x_1 so R also vanishes on $E_1\backslash\{a\} \times E_2 \times ... \times E_n$. Thus, for any $x \in E_1\backslash\{a\} \times E_2 \times ... \times E_n$, since $P(x) = R(x) = 0$ and $x_1 - a \neq 0$, then $Q(x) = 0$. However this contradicts our induction step assumption. □

Harnessing the power of the Combinatorial Nullstellensatz to prove extremal results usually works by contradiction, as we will demonstrate in Section 3.3. We assume that we have a set which fulfils the conditions of the problem but is outside the bounds we want to prove and construct a polynomial which vanishes on this set. We then find a non-zero monomial in that polynomial with the required properties and apply the Combinatorial Nullstellensatz to find a non-zero point on said polynomial in our set which gives us our contradiction. In practice, it is often finding the non-zero monomial that tends to provide resistance. However, there are many theorems available to help this process, such as Dyson's conjecture, which we state later, and results found in Chapter 9 of [TV06].

3.3 Sum Sets

Sum sets are the archetypal objects that the area of additive combinatorics, a relatively modern area of maths which Tao and Vu unified in [TV06], aims to study. Before we use the Combinatorial Nullstellensatz to tackle the Cauchy-Davenport Inequality and the Erdős-Heilbronn conjecture, both of which give a lower bounds on the size of sum sets over finite fields, we introduce sum sets over $\mathbb{R}$ and look at the inverse problem: given a sum set of minimal size, what is its structure?

Definition 3.7. *For a field $\mathbb{F}$, let $A, B \subseteq \mathbb{F}$ where A and B are non-empty sets. Then the sum set of A and B is the set $A + B = \{a + b : a \in A, b \in B\}$.*

As in Wheeler's notes, [Whe09], many famous solved and unsolved problems can be restated in simple terms using sum set notation.

Theorem 3.8 (Lagrange's four-square theorem)**.** *Let $\square = \{x^2 : x \in \mathbb{Z}\}$, then*

$$\mathbb{N}_0 = \square + \square + \square + \square$$

Conjecture 3.9 (Goldbach conjecture)**.** *For $\mathbb{E} = \{2x : x \in \mathbb{Z}_{\geq 3}\}$ and $\mathbb{P} = \{p : p \text{ is an odd prime}\}$*

$$\mathbb{E} = \mathbb{P} + \mathbb{P}$$

Using the total order on $\mathbb{R}$ makes bounding the size of sum sets very easy.

Lemma 3.10. *For sets A, $B \in \mathbb{R}$, $|A + B| \geq |A| + |B| - 1$.*

Proof. Let $A = \{a_1, ..., a_k\}$ and $B = \{b_1, ..., b_l\}$ where $a_1 < a_2 < ... < a_k$ and $b_1 < b_2 < ... < b_l$. Then, $a_1 + b_1 < a_1 + b_2 < ... < a_1 + b_l < a_2 + b_l < ... < a_k + b_l$ are $k + l - 1$ distinct elements. □

Taking A and B to be arithmetic progressions with the same common difference, we note that this is a tight bound. Even better, this is an if and only if statement for which we provide our own proof.

Lemma 3.11. *For sets A, $B \in \mathbb{R}$, $|A + B| = |A| + |B| - 1$ if and only if A and B are arithmetic progressions with the same common difference.*

Proof. For the $\Leftarrow$ direction, let $A = \{a_0, ..., a_k\}$ and $B = \{b_0, ..., b_l\}$ be arithmetic progressions, both with common difference $d \neq 0$ ie. $a_m = a_0 + dm$ for $m \in [k]$ and $b_n = b_0 + dn$ for $j \in [l]$. Then $a_m + b_n = a_0 + b_0 + d(m+n)$ and thus $|A+B| = |\{m+n : 0 \leq m \leq k, 0 \leq n \leq l\}| = k+l+1 = |A|+|B|-1$.

For the $\Rightarrow$ direction, let $A, B, A + B$ be the ordered sets $\{a_0, ..., a_k\}, \{b_0, ..., b_l\}, \{c_0, ..., c_{k+l}\}$ respectively. For an arbitrary element $a_m + b_n \in A + B$, then $a_0 + b_0 < a_0 + b_1 < ... < a_0 + b_n < a_1 + b_n < ... < a_m + b_n < ... < a_k + b_n < a_k + b_{n+1} < ... < a_k + b_l$ and thus, by the pigeonhole principle, $c_{m+n} = a_m + b_n$. Now for all $0 \leq m \leq k, 0 \leq n \leq l$, we have $a_{m+1} + b_n = a_m + b_{n+1}$ and so we can define $d \coloneqq a_{m+1} - a_m = b_{n+1} - b_n$ and thus A and B are both arithmetic progressions with common difference d. □

To bound the size of sum sets over fields without a total order such as finite fields requires more complex techniques, as we will see when we tackle the Cauchy-Davenport inequality. There are also many results about sum sets over the complex numbers, including the following interesting relation between sum and product sets by Chang in [Cha05].

Theorem 3.12. *Given a finite set $A \subset \mathbb{C}$, denote the product set $A \cdot A = \{a_1 a_2 : a_1, a_2 \in A\}$. Then*

$$\max(A + A, A \cdot A) \geq |A|^{1 + \frac{1}{54}}$$

Cauchy-Davenport Inequality

While we might expect that, if we switch $\mathbb{R}$ to a finite field of order p, we will get smaller sum sets, the Cauchy-Davenport inequality says otherwise. First proved by Cauchy in [Cau13] in 1813, it was later reproved independently by Davenport in [Dav35] in 1935. However, perhaps the quickest method, and the one which we use now, was found by Alon, Nathanson and Ruzsa in Chapter 3 of [ANR95] and uses the Combinatorial Nullstellensatz.

Theorem 3.13 (Cauchy-Davenport inequality)**.** *Let $A, B \subseteq \mathbb{F}_p$ where A, B are non-empty sets. Then $|A+B| \geq \min(|A|+|B|-1, p)$.*

Example 3.14. *Let $p = 7$. To minimise $|A+B|$, as was the case in $\mathbb{R}$, we might try to make A and B contain arithmetic progressions with the same difference. For example, taking $A = \{0,2,4\}$, $B = \{1,3,5\}$, then $A+B = \{0,1,2,3,5\}$. However, we still haven't done better than if we had just worked over $\mathbb{R}$ since $\{0,2,4\}+\{1,3,5\} = \{1,3,5,7,9\}$.*

Proof. If $|A|+|B| > p$, then for any $x \in \mathbb{F}$ let $x - B \coloneqq \{x-b : b \in B\}$, then $|A| + |x-B| \geq p+1$ since $|B| = |x-B|$. By the pigeonhole principle and the fact that $|\mathbb{F}| = p$, then $|A \cap (x-B)| \geq 1$ and thus $\exists\, a \in A, b \in B$ such that $a = x - b \Leftrightarrow a + b = x$. Since x was arbitrary then $A + B = \mathbb{F}$.

Now assume $|A|+|B| \leq p$, and, seeking a contradiction, assume that $A + B \subseteq C$ for some set C with $|C| = |A|+|B|-2$. Now define the polynomial $P \in \mathbb{F}[x,y]$,

$$P(x,y) \coloneqq \prod_{c \in C} (x+y-c)$$

which has degree $|C|$ and has $A \times B \subseteq Z(P)$. Now notice that the coefficient of $x^{|A|-1}y^{|B|-1}$ in P is $\binom{|A|+|B|-2}{|B|-1} \bmod p$ which is non-zero since $|A|+|B|-2 < p$. Thus by the Combinatorial Nullstellensatz, Theorem 3.6, $A \times B \nsubseteq Z(P)$ and thus we have our contradiction. □

There are many other proofs of the Cauchy-Davenport inequality using Fourier analysis or the e-transform amongst other techniques. We do not go into these here but they are covered in depth in [TV06].

Erdős-Heilbronn Conjecture

An interesting variant of the sum set is the restricted sum set. According to [Whe09], a similar bound to the Cauchy-Davenport inequality but this time for restricted sum sets, was first conjectured by Erdős and Heilbronn in the 1960s. This result resisted any sort of progress until it was proven by Alon, Nathanson and Ruzsa in 1995 in [ANR95]. Their proof of the Erdős-Heilbronn conjecture follows almost exactly the same structure, using the Combinatorial Nullstellensatz, as their proof the Cauchy-Davenport inequality.

Definition 3.15. *For a field $\mathbb{F}$, let $A, B \subseteq \mathbb{F}$ where A and B are non-empty sets. Then the restricted sum-set of A and B is the set $A \hat{+} B = \{a+b : a \in A, b \in B, a \neq b\}$.*

Theorem 3.16 (Erdős-Heilbronn conjecture)**.** *Let $A, B \subseteq \mathbb{F}_p$ where A, B are non-empty sets, then $|A \mathbin{\widehat{+}} B| \geq \min(|A|+|B|-3, p)$. Furthermore, if $|A| \neq |B|$, then $|A \mathbin{\widehat{+}} B| \geq \min(|A|+|B|-2, p)$.*

Example 3.17. *Let $p = 7$. We again try to minimise $|A \mathbin{\widehat{+}} B|$ by letting $A = B = \{1,3,5\}$ be the same set and also an arithmetic progression. Thus $|A \mathbin{\widehat{+}} B| = |\{1,4,6\}| = 3 = |A|+|B|-3$.*

We fill in the gaps of the proof of the Erdős-Heilbronn conjecture in Section 9.2 of [TV06].

Proof. It is enough to prove the latter result since if $|A| = |B| > 1$, then, for any $a \in A$, $|A \widehat{+} B| \geq |A\backslash\{a\} \widehat{+} B| \geq \min(|A| + |B| - 3, p)$ so assume $|A| \neq |B|$. In addition, if either $|A| = 1$ or $|B| = 1$, then wlog, letting $|A| = \{a\}$, $|A \widehat{+} B| = |B\backslash\{a\} + a| = |B\backslash\{a\}| \geq |B| - 1 = |A| + |B| - 2$. Finally, if $|A| + |B| - 2 \geq p$, then for any $x \in \mathbb{F}$, $|A| + |x - B| \geq p + 2$ since $|B| = |x - B|$. By the pigeonhole principle and the fact that $|\mathbb{F}| = p$, then $|A \cap (x - B)| \geq 2$ and thus $\exists\, a \in A, b \in B$ such that $a \neq b$ and $a = x - b \Leftrightarrow a + b = x$. Since x was arbitrary then $A + B = \mathbb{F}$ and $|A + B| = p$.

Assume $|A| + |B| - 2 < p$, and, seeking a contradiction, assume that $A + B \subseteq C$ for some set C with $|C| = |A| + |B| - 3$. Define the polynomial $P \in \mathbb{F}[x, y]$,

$$Q(x, y) \coloneqq (x - y) \prod_{c \in C} (x + y - c)$$

where $Q(a, b) = 0, \forall a \in A, b \in B$ and $\deg(Q) = |C| + 1$. The coefficient of $x^{|A|-1}y^{|B|-1}$ in Q can be computed as $\binom{|A|+|B|-3}{|A|-2} - \binom{|A|+|B|-3}{|B|-2} \equiv \frac{(|A|+|B|-3)!}{(|A|-2)!(|B|-2)!}(|A| - |B|) \bmod p$ which is non-zero since $|A|+|B|-3 < p$ and $|A| \neq |B|$. Thus by the Combinatorial Nullstellensatz, Theorem 3.6, $A \times B \nsubseteq Z(Q)$ and thus we have our contradiction. □

Corollary 3.18. *For a non-empty subset $A \subseteq \mathbb{F}_p$, then $|A \widehat{+} A| \geq \min(2|A| - 3, p)$.*

The year before Alon, Nathanson and Ruzsa proved the Erdős-Heilbronn conjecture in 1995, Da Silva, Dias and Hamidoune in [DH94] had used a variant of the polynomial method and a general result about Grassmann derivatives to prove the following theorem, Theorem 3.19, from which Corollary 3.18 follows by setting $k = 2$.

Theorem 3.19. *For p prime, $A \subseteq \mathbb{F}_p$ and $1 \leq k \leq |A|$, then*

$$\left| \left\{ \sum_{i=1}^{k} a_k : a_i \in A, a_1 \neq ... \neq a_k \right\} \right| \geq \min(k|A| - k^2 + 1, p).$$

Generalisation to Finite Groups

Following Wheeler's lecture notes [Whe09] again, we can extend the Cauchy-Davenport Inequality and the Erdős-Heilbronn Conjecture to results for any finite group G. In the process, we need to define the minimal torsion element of a group, however, with that in hand, both theorems are effectively the same as they were when we were just looking over finite fields of order p.

Definition 3.20. *We define the minimal torsion element $p(G)$ of a group G to be the smallest positive integer p for which there exists a $g \in G\backslash\{e\}$, such that $g^p = e$. If no such g exists then $p(G) = \infty$.*

Theorem 3.21 (Cauchy-Davenport Inequality for Finite Groups)**.** *Let G be a finite group with non-empty subsets A, $B \subseteq G$ then*

$$|\{a \cdot b : a \in A, b \in B\}| \geq \min(p(G), |A| + |B| - 1)$$

Theorem 3.22 (Erdős-Heilbronn Conjecture for Finite Groups)**.** *Let G be a finite group with non-empty subsets A, $B \subseteq G$ then*

$$|\{a \cdot b : a \in A, b \in B, a \neq b\}| \geq \min(p(G), |A| + |B| - 3)$$

3.4 Latin Squares and Latin Transversals

As discussed earlier, the challenging part of applying the Combinatorial Nullstellensatz is often finding the relevant non-zero monomial. To prove Theorem 3.26, a result about Latin squares below, we will need Dyson's conjecture, an incredibly useful piece of machinery, however, one which we will not prove here but has a short proof given by Good in [Goo70].

Theorem 3.23 (Dyson's conjecture)**.** *Let $a_1, ..., a_n \in \mathbb{N}$. Then the coefficient of*

$$\prod_{i\in[n]} x_i^{(n-1)a_i} \quad \text{in} \quad \prod_{\substack{i,j\in[n]\\ i\neq j}} (x_j - x_i)^{a_j} \quad \text{is} \quad \frac{(a_1 + ... + a_n)!}{a_1!...a_n!}.$$

We can now introduce Latin squares, an example of which are sudoku grids and another key object of study in additive combinatorics.

Definition 3.24. *A Latin square $\mathcal{S}$ is an $n \times n$ array of n symbols in which each symbol appears exactly once in each row and column. A Latin transversal of $\mathcal{S}$ is a set of cells containing every symbol such that no two cells share a row or column.*

Remark 3.25. *It is easy to see that for subsets $A, B \subseteq R$ for ring R, the addition table given by $(a + b)_{a\in A, b\in B}$ is a Latin square. An example is given in Figure 3.1.*

Figure 3.1: An arbitrary 4×4 Latin square (left) and the addition table of $\mathbb{F}_5$ (right).

4×4 Latin square

AA	BB	CC	DD
BB	CC	DD	AA
CC	DD	AA	BB
DD	AA	BB	CC

No Latin transversals possible.

$\mathbb{F}_5$ addition table

$+$	0	1	2	3	4
0	0	1	2	**3**	4
1	1	**2**	3	4	0
2	2	3	4	0	**1**
3	3	4	**0**	1	2
4	**4**	0	1	2	3

Latin transversal coloured.

The following theorem was proved by Alon in a follow-up paper to [Alo99], where he proved the Combinatorial Nullstellensatz and demonstrates the strength of the Combinatorial Nullstellensatz in an existence problem. We follow Section 9.3 of [TV06] which proves effectively the same statement.

Theorem 3.26. *For subsets $A, B \subseteq \mathbb{F}_p$ for odd prime p where we enumerate $A = \{a_1, ..., a_n\}$ and $B = \{b_1, ..., b_n\}$ for $n \in \mathbb{N}$, then the addition table $(a_i + b_j)_{i,j\in[n]}$ has a Latin transversal.*

Proof. If $n = p$ then the main diagonal is a Latin transversal since 2 generates $\mathbb{F}_p$ so assume $n < p$. Now define $T \in \mathbb{F}_p[x_1, ..., x_n]$ by

$$T(x_1, ..., x_n) \coloneqq \prod_{1\leq i<j\leq n} (x_j - x_i)(x_i - x_j + a_i - a_j).$$

By Dyson's conjecture, Theorem 3.23, taking $a_i = 1, \forall\, i \in [n]$, the coefficient of $x_1^{n-1} ... x_n^{n-1}$ in T is $n!$ which is non-zero in $\mathbb{F}_p$ since $n < p$. So, by the Combinatorial Nullstellensatz with $E_i = B$, there exist $b_i \in B$ for $i \in [n]$ such that $b_i \neq b_j$ and $a_i + b_i \neq a_j + b_j$ for $i \neq j$ where $i, j \in [n]$. □

Shortly after Alon published his proof, Dasgupta, Károlyi, Serra and Szegedy generalised the proof to work for subsets of cyclic groups of any order in [Das+01]. The generalisation of Theorem 3.26 to any abelian group of odd order is known as Snevily's Conjecture, which was proved in 2011 by Arsovski using the theory of characters in [Ars11]. We state Snevily's Conjecture in its original form, which is equivalent to our formulation in terms of Latin squares.

Theorem 3.27 (Snevily's Conjecture)**.** *For G, an abelian group with odd order and subsets $A = \{a_1, ..., a_k\}$ and $B = \{b_1, ..., b_k\}$, then there exists a permutation $\sigma \in S_k$ such that sums $a_i + b_{\sigma(i)}$ for $i \in [k]$ are distinct.*

The theory of Latin transversals is, perhaps surprisingly, difficult. In fact, the following, conjectured by Ryser in 1976, is still unsolved.

Conjecture 3.28. *For n odd, every Latin square has a Latin transversal.*

3.5 Vandermonde's Matrix

The Vandermonde matrix and the ensuing Vandermonde's identity, a formula for the determinant of the Vandermonde matrix, will prove incredibly useful for the remainder of this report. As covered in Section 9.2 of [TV06], the determinant, and even permanent, of the Vandermonde matrix can be used in the proof of Dyson's conjecture, Theorem 3.23, and Snevily's Conjecture, Theorem 3.27.

Definition 3.29 (Vandermonde matrix)**.** *For each $n \in \mathbb{N}$, let $V_n \in M_n(\mathbb{F}[x_1, ..., x_n])$ be the Vandermonde matrix, with elements $(V_n)_{i\,j} = x_i^{j-1}$ for all $i, j \in [n]$.*

Example 3.30. $V_3 = \begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix} \in M_3(\mathbb{C}[x_1, x_2, x_3])$ *is the 3×3 Vandermonde matrix where we notice that the determinant is* $\det V_3 = x_2x_3^2 - x_3x_2^2 + x_3x_1^2 - x_1x_3^2 + x_1x_2^2 - x_2x_1^2 = (x_3 - x_2)(x_3 - x_1)(x_2 - x_1)$*. The reason for this interesting factorisation becomes clearer when we notice that if $x_1 = x_2$, the first two rows are the same and thus the determinant will be 0. Similarly for $x_1 = x_3$ or $x_2 = x_3$. This pattern continues to hold for V_n for any $n \in \mathbb{N}$ and is known as Vandermonde's identity.*

Lemma 3.31 (Vandermonde's identity)**.** *If $V_n \in M_n(\mathbb{F}[x_1, ..., x_n])$ is the Vandermonde matrix, then*

$$\det V_n(x) = \prod_{1\leq i<j\leq n} (x_j - x_i)$$

Just before we present our own version of the proof of Vandermonde's identity, Lemma 3.31, we need to state the Leibniz determinant formula, a nice form for the determinant as sums of permutations.

Lemma 3.32 (Leibniz determinant formula)**.** *Given an $n \times n$ matrix A with entries A_{ij}, we have*

$$det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i \in [n]} A_{i\,\sigma(i)}$$

where $\operatorname{sgn}(\sigma) = (-1)^{N_\sigma}$, where N_σ is the number of transpositions in the decomposition of σ.

Proof of Vandermonde's identity. We will prove this by induction on k. The $k = 1$ case holds since, on the LHS, the 1×1 Vandermonde matrix is simply the number 1. On the RHS, there are no terms in the product so it is automatically 1. Now assume the $k \times k$ Vandermonde matrix has determinant $\det V_k(x) = \prod_{1 \le i < j \le k}(x_j - x_i)$. Take the $(k+1) \times (k+1)$ Vandermonde matrix V_{k+1} and consider its determinant $\det V_{k+1}$ as a polynomial in x_{k+1} over the ring $R \coloneqq \mathbb{F}[x_1, x_1, ..., x_k]$ ie. $\det V_{k+1} \in R[x_{k+1}]$. As in Example 3.30, we notice that plugging x_i for any $i \in [k]$ into $\det V_{k+1}(x_i) = 0$, since then the matrix has two identical rows so the determinant will be 0. Letting $Q \coloneqq \prod_{i \in [k]}(x_{k+1} - x_i) \in R[x_{k+1}]$, by the Factor Theorem, Theorem 1.7, $\det V_{k+1} = QP$ for some polynomial $P \in R[x_{k+1}]$. We now notice that $\deg(\det V_{k+1}) = k$, since the Leibniz determinant formula, Lemma 3.32, insists that in each monomial of $\det V_{n+1}$, we must pick one element from each row. Now consider the coefficient in front of x_{k+1}^k on both sides of $\det V_{k+1} = QP$. On the LHS, since we have to pick one element from each row and column, the coefficient in front of x_{k+1}^k is simply the determinant of the $k \times k$ Vandermonde matrix V_k. On the RHS, $\deg(Q) = k$ and thus $\deg(P) = 0$ so $P \in R$ and we in fact have that P is also the coefficient of x_{k+1}^k. Matching these coefficients and using our induction hypothesis,

$$\det V_{k+1} = QP = \prod_{1 \le i \le k}(x_{k+1} - x_i) \det V_k = \prod_{1 \le i \le k}(x_{k+1} - x_i) \prod_{1 \le i < j \le k}(x_j - x_i) = \prod_{1 \le i < j \le k+1}(x_j - x_i)$$

so the claim also holds for the $(k+1) \times (k+1)$ Vandermonde matrix. □

We demonstrate a use case of Vandermonde's identity in the proof of the next result, first shown by Schur in [Sch08], and reformulated by Tao and Vu in [TV06]. The proof also incorporates a variant of the observation made at the start of Section 3.1, where this time we only sum over a subset of $\mathbb{F}$, not necessarily the whole field.

Theorem 3.33. *Let $\mathbb{F}$ be a finite field with non-empty $U \subseteq \mathbb{F}^\times$ and let $P \in \mathbb{F}[t]$ be a polynomial of degree n such that $P(t+U) = \{P(t+u) : u \in U\} = \{P(t) + u : u \in U\} = P(t) + U$ for all $t \in \mathbb{F}$. Then, if $n > 1$, then $|U| > |\mathbb{F}| - n$.*

We provide Müller's proof from [Mül05] in which he uses this result to prove a theorem by Burnside.

Proof. If $n \le |\mathbb{F}|$ then the statement is trivial so assume $n < |\mathbb{F}|$. Let m be the largest integer such that $mn < |\mathbb{F}|$. Then define $Q \in \mathbb{F}[t]$ where

$$Q(t) = \sum_{u \in U} (P(t+u))^m - (P(t) + u))^m$$

which has degree at most mn and $Q(t) = 0, \forall\, t \in \mathbb{F}$. In addition, since $mn < |\mathbb{F}|$ then by the Factor Theorem, Lemma 1.7, then $Q(t) \equiv 0$ and thus

$$\sum_{u \in U} (P(t+u))^m \equiv \sum_{u \in U} (P(t) + u)^m. \tag{3.3}$$

Let us enumerate $U = \{u_1, ..., u_{|U|}\}$ then consider the matrix $M_{i\,j} = u_i^j$ for $i, j \in [|U|]$. It is clear to see that

$$\det(M) = \left(\prod_{i=1}^{|U|} u_i\right) \det V_{|U|}(u_1, ..., u_{|U|}) = \left(\prod_{i=1}^{|U|} u_i\right) \left(\prod_{1 \le i < j \le |U|} (u_j - u_i)\right) \neq 0.$$

For $k \in \mathbb{N}$, set $S(k) \coloneqq \sum_{u \in U} u^k$ and assume $S(k) = 0$ for all $1 \le k \le |U|$. Thus, each column of M adds up to 0, implying that adding up the rows of M as vectors gives the zero vector, which means the rows are not linearly dependent contradicting the fact that $\det(M) \neq 0$. Thus, we can let $1 \le r \le |U|$ be the minimal positive integer such that $S(r) \neq 0$. We now notice that, using Equation 3.3, we can write

$$\begin{aligned}\sum_{u \in U} (P(t+u))^m - P(t)^m &= \sum_{u \in U} (P(t)+u)^m - P(t)^m = \sum_{u \in U} \sum_{i=1}^{m} \binom{m}{i} u^i P(t)^{m-i} \\ &= \sum_{i=1}^{m} \binom{m}{i} S(i) P(t)^{m-i} = \sum_{i=r}^{m} \binom{m}{i} S(i) P(t)^{m-i}.\end{aligned}$$

We note that $\deg(P(t)^m) = mn$ so t^{mn} is an $\mathbb{F}$-linear combination of the formal derivatives of $P(t)^m$ so we can write $t^{mn} = \sum_{j=0}^{mn} c_j \frac{d^j}{dt^j}(P(t)^m)$. Thus we obtain

$$\begin{aligned}\sum_{u \in U} (t+u)^{mn} - t^{mn} &= \sum_{u \in U} \left(\sum_{j=0}^{mn} c_j \frac{d^j}{dt^j}(P(t+u)^m)\right) - \sum_{j=0}^{mn} c_j \frac{d^j}{dt^j}(P(t)^m) \\ &= \sum_{j=0}^{mn} c_j \frac{d^j}{dt^j}\left(\sum_{u \in U} (P(t+u))^m - P(t)^m\right) = \sum_{j=0}^{mn} c_j \frac{d^j}{dt^j}\left(\sum_{i=r}^{m} \binom{m}{i} S(i) P(t)^{m-i}\right) \\ &= \sum_{j=0}^{mn} \sum_{i=r}^{m} c_j \binom{m}{i} S(i) \frac{d^j}{dt^j} P(t)^{m-i}\end{aligned}$$

which has degree at most $n(m-r)$ since $\deg(\frac{d^j}{dt^j} P(t)^{m-i}) \le n(m-r)$ for $0 \le j \le mn, r \le i \le m$. Now, suppose that $r \le nm$, then we also have

$$\sum_{u \in U} (t+u)^{mn} - t^{mn} = \sum_{u \in U} \sum_{i=1}^{mn} \binom{m}{i} u^i t^{mn-i} = \sum_{i=1}^{mn} \binom{mn}{i} S(i) t^{mn-i}$$

and thus the coefficient of x^{nm-r} in the expansion is $\binom{mn}{r} S(r) \neq 0$ contradicting the degree being at most $n(m-r)$ since $n > 1$. Thus we conclude that $r > nm$ and hence $mn < r \le |U| < |\mathbb{F}| \le (m+1)n$. Thus, $|\mathbb{F}| - |U| < n$ since m is an integer and $|U| > |\mathbb{F}| - n$. □

3.6 Invertible Matrices Constructed from Sets

We will now use the Combinatorial Nullstellensatz along with properties of the Vandermonde matrix to prove another existence statement, now about invertible matrices, first described to me by my supervisor, Dr. Dan Evans.

Theorem 3.34. *Given a field $\mathbb{F}$, an integer $n > 1$ and a set $S \subseteq \mathbb{F}$, where $1 < |S| \le n^2 \le |\mathbb{F}|$, we can construct an invertible $n \times n$ matrix using all elements in S at least once each.*

Our proof of this Theorem is split into two cases: $|S| > n+1$ and $|S| \le n+1$. We will prove the $|S| > n+1$ case using the Combinatorial Nullstellensatz and the properties of the Vandermonde matrix, $V_{|S|}$, whereas we prove the $|S| \le n+1$ by manually constructing a matrix with $|S|$ variables and

computing the determinant which we show is non-zero. It would be hard to apply the Combinatorial Nullstellensatz for smaller $|S|$ due to the condition that each variable in our chosen monomial has to have degree less than $|S|$. Likewise, if $|S|$ is larger, computing the determinant of a matrix with $|S|$ variables would become unruly very quickly.

Proof. We first consider the case $|S| > n+1$ and construct two matrices with entries in $\mathbb{F}[x_1, ..., x_{|S|}]$. We define $M \in M_n(\mathbb{F})$ to be the $n \times n$ matrix where we put $x_{|S|}$ in the bottom left corner, $x_{|S|-n}$ up to $x_{|S|-1}$ along the main diagonal and arrange $x_1, ..., x_{|S|-n-1}$ in the other entries of the matrix in any way but including each at least once. We also let $V_{|S|}$ be the $|S| \times |S|$ Vandermonde matrix from Definition 3.29. For example, taking $|S| = n+2$, we would have

$$M = \begin{pmatrix} x_2 & x_1 & x_1 & \dots & x_1 & x_1 & x_1 \\ x_1 & x_3 & x_1 & \dots & x_1 & x_1 & x_1 \\ x_1 & x_1 & x_4 & \dots & x_1 & x_1 & x_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ x_1 & x_1 & x_1 & \dots & x_{n-1} & x_1 & x_1 \\ x_1 & x_1 & x_1 & \dots & x_1 & x_n & x_1 \\ x_{n+2} & x_1 & x_1 & \dots & x_1 & x_1 & x_{n+1} \end{pmatrix} \quad V_{n+2} = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n+1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n+1} & x_{n+1}^2 & \dots & x_{n+1}^{n+1} \\ 1 & x_{n+2} & x_{n+2}^2 & \dots & x_{n+2}^{n+1} \end{pmatrix}.$$

Now, we can construct the polynomial $P \in \mathbb{F}[x_1, ..., x_{|S|}]$, using Lemma 3.31, given by

$$P = \det M \det V_{|S|} = \det M \prod_{1 \le i < j \le |S|} (x_j - x_i) \text{ where } \deg(P) \le n + \binom{|S|}{2} = n + \sum_{k=1}^{|S|-1} k$$

Note that the existence of a non-zero solution of P in $S^{|S|}$ is equivalent to Theorem 3.34 so, if we can apply the Combinatorial Nullstellensatz to P with sets $E_k = S$ for $k \in [|S|]$, we are done. Using the Leibniz formula for the determinant, Lemma 3.32, and the definition of the Vandermonde matrix $V_{|S|}$, we can write

$$\det V_{|S|} = \sum_{\tau \in S_{|S|}} \operatorname{sgn}(\tau) \prod_{k=1}^{|S|} (V_{|S|})_{k\,\tau(k)} = \sum_{\tau \in S_{|S|}} \operatorname{sgn}(\tau) \prod_{k=1}^{|S|} x_k^{\tau(k)-1}$$

Clearly, each term in the sum over $\tau \in S_{|S|}$ gives a unique monomial in $\det V_{|S|}$ which has coefficient $\operatorname{sgn}(\tau)$. In addition, since x_i for $i \in \{|S|-n, ..., |S|-1\}$ appear only once each in M along the diagonal, then the monomial $\prod_{i=|S|-n}^{|S|-1} x_i$ appears once in the Leibniz formula for $\det(M) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} M_{i\,\sigma(i)}$ corresponding to $\sigma \in S_n$ where $\sigma(i) = i, \forall\, i \in [n]$.

We now claim that given any monomial $\prod_{i=1}^{n} M_{i\,\sigma(i)}$ for some $\sigma \in S_n$ with non-zero coefficient in $\det M$ and any monomial $\prod_{k=1}^{|S|} x_k^{\tau(k)-1}$ for some $\tau \in S_{|S|}$ with non-zero coefficient in $\det V_{|S|}$, such that

$$m \coloneqq \prod_{k=1}^{|S|} x_k^{k-1} \prod_{i=|S|-n}^{|S|-1} x_k = \prod_{k=1}^{|S|} x_k^{\tau(k)-1} \prod_{i=1}^{n} M_{i\,\sigma(i)} \tag{3.4}$$

then we get unique forms of σ and τ, given by $\sigma(i) = i$ for $i \in [n]$ and $\tau(k) = k$ for $k \in [|S|]$. This then implies that m has coefficient $\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) \neq 0$ in P. In addition, $\deg(m) = n + \sum_{k=1}^{|S|}(k-1) = n + \sum_{k=1}^{|S|-1} k = n + \binom{|S|}{2}$ and $x_k^{|S|} \nmid m$ for $k \in [|S|]$. Thus, as in Theorem 3.6, taking sets $E_k = S$ for $k \in [|S|]$ and applying the Combinatorial Nullstellensatz, the claim follows for $|S| > n+1$.

We first prove that Equation 3.4 implies that $\tau(k) = k$ for $1 \le k < |S| - n$. We first work by induction on k. The base case $k = 1$ follows since $x_1 \nmid m$ since $|S| - n > 1$, but thus on the RHS

of Equation 3.4, $\tau(1) = 1$. Now assume $\tau(j) = j$ for all $1 \leq j < k < |S| - n$. Since τ is a bijection, $\tau(k) \geq k$, but looking at the LHS of Equation 3.4, clearly $x_k^k \nmid m$, so $\tau(k) \leq k$ and thus $\tau(k) = k$.

We will now show that this implies $\sigma(i) = i$ for $i \in [n]$. This follows by noticing that if, for some $i \in [n]$, $M_{i\,\sigma(i)} = x_k$ for some $1 \leq k < |S| - n$ then since $\tau(k) = k$ and using the RHS of Equation 3.4, $x_k^k | m$ which gives us a contradiction since $x_k^k \nmid m$ on the LHS. This implies that $\forall\, i \in [n]$, $M_{i\,\sigma(i)} = x_j$ for some $|S| - n \leq j \leq |S|$. However, these x_j are precisely the elements along the main diagonal together with the bottom left corner of the matrix M by its construction. Thus, we must have that $M_{i\,\sigma(i)} = M_{i\,i}$ for all $1 \leq i < n$ and since σ is a bijection, then we find $\sigma(i) = i$ for $i \in [n]$.

Finally, we can now continue our induction on k. So assume $\tau(j) = j$ for all $0 \leq j < k$ where $|S| - n \leq k \leq |S| - 1$. Since τ is a bijection, $\tau(k) \geq k$, but looking at the LHS of Equation 3.4, clearly $x_k^{k+1} \nmid m$ and $M_{k-(|S|-n-1)\,k-(|S|-n-1)} = x_k$, so $\tau(k) \leq k$ and thus $\tau(k) = k$. Using that τ is a bijection a final time, $\tau(|S|) = |S|$ and thus $\tau(k) = k$ for all $k \in [|S|]$.

We now tackle the case $|S| \leq n + 1$. Again, we construct a matrix M with entries in $\mathbb{F}[x_1, ..., x_{|S|}]$, given by putting x_1 in all entries below the main diagonal and filling the rest of the ith column with $x_{\min(i+1,|S|-1)}$. We demonstrate with the matrix for $|S| = n + 1$ below.

$$M = \begin{pmatrix} x_2 & x_3 & x_4 & \dots & x_n & x_{n+1} \\ x_1 & x_3 & x_4 & \dots & x_n & x_{n+1} \\ x_1 & x_1 & x_4 & \dots & x_n & x_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ x_1 & x_1 & x_1 & \dots & x_n & x_{n+1} \\ x_1 & x_1 & x_1 & \dots & x_1 & x_{n+1} \end{pmatrix}$$

By taking the nth row away from every other row, due to the standard linear algebra fact that adding a multiple of one column to another column doesn't change the determinant, we get a matrix $\tilde{M}$, where $\det M = \det \tilde{M}$. For $|S| = n + 1$, this is given by

$$\tilde{M} = \begin{pmatrix} x_2 - x_1 & x_3 - x_1 & x_4 - x_1 & \dots & x_n - x_1 & 0 \\ 0 & x_3 - x_1 & x_4 - x_1 & \dots & x_n - x_1 & 0 \\ 0 & 0 & x_4 - x_1 & \dots & x_n - x_1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \dots & x_n - x_1 & 0 \\ x_0 & x_0 & x_0 & \dots & x_0 & x_{n+1} \end{pmatrix}$$

Taking the determinant is now much simpler so

$$\det \tilde{M} = x_{n+1}(x_{|S|} - x_1)^{n-|S|+1} \prod_{k=2}^{|S|-1} (x_k - x_1) = \det M$$

and thus, by choosing $x_1 \notin \{x_2, ..., x_{|S|}\}$ and $x_{n+1} \neq 0$ which is always possible since $|S| \geq 2$, M has non-zero determinant. □

In Chapter 4, we will generalise this result and give an exact condition on when a set of elements S can be turned into an invertible matrix. However, to get to this point, we will need more specialised theory about the interaction of Vandermonde's identity and the determinants of matrices, all building on the Combinatorial Nullstellensatz.

3.7 Polynomial Ideals

In Chapter 3 thus far, we have focused almost exclusively on the Combinatorial Nullstellensatz, Theorem 3.6, and its applications. However, it is slightly ungenuine to talk about this result as *the* Combinatorial Nullstellensatz. As we noted in Section 3.2, in Alon's original paper, [Alo99], what we have called the Combinatorial Nullstellensatz so far, Theorem 3.6, is proved as a consequence of the following theorem, Theorem 1.1 in [Alo99], which we will not prove, due to its technical proof.

Theorem 3.35. *Given an arbitrary field $\mathbb{F}$, let $f \in \mathbb{F}[x_1, ..., x_n]$. Let $S_1, ..., S_n$ be non-empty subsets of $\mathbb{F}$ and, for $i \in [n]$, define $g_i(x_i) \coloneqq \prod_{a \in S_i}(x_i - a) \in \mathbb{F}[x_i]$. If $f(s) = 0$ for all $s \in S_1 \times ... \times S_n$, then there exist polynomials $h_1, h_2, ..., h_n \in \mathbb{F}[x_1, ..., x_n]$, where, for all $i \in [n]$, $\deg(h_i) \leq \deg(f) - |S_i|$ such that $f = \sum_{i \in [n]} h_i g_i$.*

Later on we will need the following almost identical result to Theorem 3.35, which follows easily as a Corollary from it. However, we will prove it fully using the Combinatorial Nullstellensatz we have been using so far, Theorem 3.6, (the other way round to the way Alon did) for continuity.

Theorem 3.36. *Given an arbitrary field $\mathbb{F}$, let $f \in \mathbb{F}[x_1, ..., x_n]$. Let $S_1, ..., S_n$ be non-empty subsets of $\mathbb{F}$ and, for $i \in [n]$, define $g_i(x_i) \coloneqq \prod_{a \in S_i}(x_i - a) \in \mathbb{F}[x_i]$. Then, $f(s) = 0$ for all $s \in S_1 \times ... \times S_n$ if and only if $f \in \langle g_i(x_i) : i \in [n] \rangle$.*

Proof. The $\Leftarrow$ direction follows since $f \in \langle g_i(x_i) : i \in [n] \rangle$ implies that, for some $f_i \in \mathbb{F}[x]$, we can write $f(x) = \sum_{i \in [n]} f_i(x) g_i(x_i)$. Since, $g_i(s_i) = 0$ for all $s_i \in S_i, i \in [n]$ then clearly $f(s) = 0$ for all $s \in S_1 \times ... \times S_n$.

For the $\Rightarrow$ direction, let $\overline{f}$ be the reduced polynomial obtained by writing f as a sum of monomials and repeatedly substituting each instance of $x_i^{e_i}$ with $e_i \geq \deg(g_i)$ with a linear combination of smaller powers of x_i using $g_i(x_i)$. Then we can guarantee that, for all $i \in [n]$, the degree of $\overline{f}$ in just the variable x_i is less than $\deg(g_i)$ ie. treating $\overline{f} \in R[x_i]$ where $R = \mathbb{F}[x_1, ..., x_{i-1}, x_{i+1}, ..., x_n]$ then $\deg(\overline{f}) < \deg(g_i)$. We can then write $f = \overline{f} + \sum_{i \in [n]} h_i g_i$ for some $h_i \in \mathbb{F}[x]$ implying that $\overline{f}(s) = 0, \forall\, s \in S_1 \times ... \times S_n$. Assume $\overline{f} \not\equiv 0$ and take a monomial x^α such that $|\alpha| = \deg(\overline{f})$. This then contradicts the Combinatorial Nullstellensatz, Theorem 3.6, by taking sets $E_i = S_i, \forall\, i \in [n]$ since $\overline{f}(s) = 0, \forall\, s \in S_1 \times ... \times S_n$. Thus $\overline{f} \equiv 0$ and so $f = \sum_{i \in [n]} h_i g_i$ and $f \in \langle g_i(x_i) : i \in [n] \rangle$. □

Using Theorem 3.36, instead of talking about polynomials vanishing at all points in a set as we did in Theorem 3.6, we can wrap up this information by talking about polynomials being members of ideals, which will prove more useful in Chapter 4. The ideal we will almost always use is $\langle x_i^k - 1 : i \in [n] \rangle$ for some $k, n \in \mathbb{N}$. Then, by Theorem 3.36, for polynomial $f \in \mathbb{F}[x_1, ..., x_n]$ then $f \in \langle x_i^k - 1 : i \in [n] \rangle$ if and only if $f(s) = 0$ for all $s \in \mu_k^n$. The choice of ideal is almost completely arbitrary but the main reason we use this ideal is that we get nice properties from the fact that $f(x) \bmod \langle x_i^n - 1 : i \in [n] \rangle$ is just f where the exponent of each monomial is taken modulo k ie. if $f(x) = \sum_{\alpha \in \mathbb{N}_0^n} c_\alpha x^\alpha$ then $\bmod \langle x_i^k - 1 : i \in [n] \rangle$, we have $f \equiv \sum_{\beta \in \mathbb{Z}_k^n} c'_\beta x^\beta$ where $c'_\beta = \sum_{\alpha \equiv \beta \,(\mathrm{mod}\ k)} c_\alpha$. We have to be careful that $\mathrm{char}(\mathbb{F}) \nmid k$ otherwise, $g_i(x_i) = x_i^k - 1 = (x_i - 1)^k$ and then the condition of Theorem 3.36 is no longer satisfied. Indeed, in Section 4.1, we will have to consider the cases $\mathrm{char}(\mathbb{F}) | k$ and $\mathrm{char}(\mathbb{F}) \nmid k$ separately for this reason. Furthermore, in Section 3.8, when working over $\mathbb{C}$, the fact that all kth roots of unity point in different directions and have the same absolute value will be important.

3.8 (Hyper)graph k-colourings

We now apply Theorem 3.36 to the colouring of graphs and hypergraphs and give an original result, inspired by Section 7 of [Alo99] and Section 4.2 of [Ale19].

Definition 3.37. *A proper vertex colouring of a graph G is a labelling of the graph's vertices with colours such that no two vertices joined by an edge are labelled the same colour. A proper vertex colouring of G containing at most k colours is called a k-colouring and if such a colouring exists, G is k-colourable.. Equivalently, a k-colouring of $G = (V, E)$ is a function $c : V \to \mathbb{Z}_k$ where for any $v, w \in V$ then $(v, w) \in E \Rightarrow c(v) \neq c(w)$.*

The following result, first proved by Alon and Tarsi in [AT93], gives an exact condition on when a graph is k-colourable using the concept of the graph polynomial. This polynomial has been studied since as early as 1891 by Peterson in [Pet91].

Definition 3.38. *The graph polynomial $f_G \in \mathbb{C}[x_1, ..., x_n]$ of a graph $G = (V, E)$ where we enumerate $V = \{v_i\}_{i\in[n]}$ is given by*

$$f_G(x) \coloneqq \prod_{\substack{(v_i,v_j)\in E \\ i<j}} (x_j - x_i).$$

Theorem 3.39. *Let $G = (V, E)$ be a graph where we enumerate $V = \{v_i\}_{i\in[n]}$. Then G is not k-colourable if and only if the graph polynomial $f_G \in \langle x_i^k - 1 : i \in [n]\rangle$.*

We will provide a condensed proof by Alon from his paper where he introduced the Combinatorial Nullstellensatz, [Alo99].

Proof. Let ω be a primitive kth root of unity in $\mathbb{C}$. Then the following are equivalent:

- G is k-colourable,
- $\exists\, c : V \to \mathbb{Z}_k$, letting $\alpha_i = c(v_i)$, where $(v_i, v_j) \in E$ implies $\alpha_i \neq \alpha_j$,
- $\forall\, (v_i, v_j) \in E$ we have $\alpha_i - \alpha_j \neq 0$,
- $\forall\, (v_i, v_j) \in E$ we have $\omega^{\alpha_i} - \omega^{\alpha_j} \neq 0$,
- $\exists\, \alpha \in \mathbb{Z}_k^n$ such that $f_G(\omega^{\alpha_1}, ..., \omega^{\alpha_n}) \neq 0$,
- $f_G \notin \langle x_i^k - 1 : i \in [n]\rangle$,

where the last equality follows from Theorem 3.36 with $g_i(x_i) \coloneqq x_i^k - 1$. □

However, we don't have to stop at graphs, we can extend this type of result to hypergraphs.

Definition 3.40. *A hypergraph $H = (V, E)$ where V is a finite set of vertices and E is a collection of sets of vertices or hyperedges ie. a hyperedge is a set 'connecting' any number of vertices. For $m \in \mathbb{N}$, a hypergraph is m-uniform if each hyperedge contains precisely m vertices.*

A proper vertex colouring of a hypergraph H is a labelling of its vertices such that no edge is monochromatic. A proper vertex colouring containing at most k colours is called a k-colouring and if such a colouring exists, H is k-colourable. Equivalently, k-colouring of H is a function $c : V \to \mathbb{Z}_k$ such that for all hyperedges $e \in E$, for all possible 'colours' $A \in \mathbb{Z}_k$, then $\{c(v) : v \in e\} \neq \{A\}$.

It is now possible to give a similar result to Theorem 3.39, where we can give an exact condition on when an m-uniform hypergraph is k-colourable. This result is given in Alon's paper, [Alo99], for the case $k = 2, m = 3$, however, the proof has been generalised in Alexandr's thesis, [Ale19], to all $k, m \in \mathbb{N}$ using a similar argument. We now generalise this further to any hypergraph, not just m-uniform ones, by tightening Alexandr's argument to give the following original result.

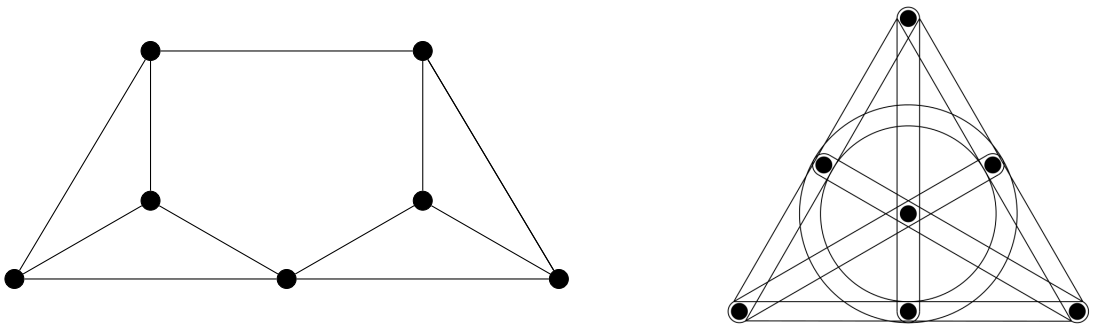


Figure 3.2: The Moser spindle from [Mos61] (left) and the hypergraph of the Fano plane (right) are shown. It is easy to check that the Moser spindle is not 3-colourable and the Fano plane is not 2-colourable.

Theorem 3.41. *For $k, n \in \mathbb{N}$, let ω be a primitive kth root of unity in $\mathbb{C}$ and let $H = (V, E)$ be a hypergraph where we enumerate the vertices $V = \{v_i\}_{i\in[n]}$. Now define a polynomial $g_H \in \mathbb{C}[x_1, ..., x_n]$ where*

$$g_H(x) = \prod_{e\in E}\prod_{\tau\in\mu_k}\left(\left(\sum_{v_i\in e} x_i\right) - |e|\tau\right)$$

Then $H = (V, E)$ is not k-colourable if and only if $g_H \in \langle x_i^k - 1 : i \in [n]\rangle$.

Before we prove Theorem 3.41, we must first prove a technical Lemma in which we use facts specific to roots of unity in $\mathbb{C}$, which explains why we defined our polynomials over $\mathbb{C}$.

Lemma 3.42. *Let $\alpha \in \mathbb{Z}_k^n$, $A \in \mathbb{Z}_k$ and $I \subseteq [n]$. Then $\sum_{i\in I}\omega^{\alpha_i} = |I|\omega^A \Leftrightarrow \alpha_i = A$ for all $i \in I$.*

Proof. Let $|I| = m$. The $\Leftarrow$ direction follows trivially. For the $\Rightarrow$ direction, notice that if $|\omega^{\alpha_j} + \omega^{\alpha_k}| < 2$ for some distinct $j, k \in I$ then

$$m = |m\omega^A| = |\sum_{i\in I}\omega^{\alpha_i}| \le |\omega^{\alpha_j} + \omega^{\alpha_k}| + \sum_{i\in I\setminus\{i,j\}}|\omega^{\alpha_i}| = |\omega^{\alpha_j} + \omega^{\alpha_k}| + m - 2 < m$$

and thus $|\omega^{\alpha_j} + \omega^{\alpha_k}| = 2$. In addition, this means equality holds in the Cauchy-Schwarz Inequality since $2 = |\omega^{\alpha_j} + \omega^{\alpha_k}| = |\omega^{\alpha_j}| + |\omega^{\alpha_k}| = 2$ and thus $\omega^{\alpha_j} = \omega^{\alpha_k}$, meaning $\alpha_j = \alpha_k$. Since j and k were arbitrary, all α_i are equal and $m\omega^A = \sum_{i\in V_e}\omega^{\alpha_i} = m\omega^{\alpha_1}$ so $\alpha_i = A$ for all $i \in I$. □

Proof of Theorem 3.41. Let $\alpha \in \mathbb{Z}_k^n$, $e \in E$ and $\tau = \omega^A \in \mu_k$ for some $A \in \mathbb{Z}_k$ then we can apply Lemma 3.42 to get $\left(\sum_{v_i\in e}\omega^{\alpha_i}\right) - |e|\tau = \left(\sum_{v_i\in e}\omega^{\alpha_i}\right) - |e|\omega^A \neq 0 \Leftrightarrow \exists v_i \in e$ such that $\alpha_i \neq A$. Then the following are equivalent:

- H is k-colourable,
- $\exists\, c : V \to \mathbb{Z}_k$, letting $\alpha_i = c(v_i)$, where $\forall\, e \in E, \forall\, A \in \mathbb{Z}_k$, $\{c(v_i) : v_i \in e\} = \{\alpha_i : v_i \in e\} \neq \{A\}$,
- $\forall\, e \in E, \forall\, A \in \mathbb{Z}_k$, $\exists v_i \in e$ such that $\alpha_i \neq A$,
- $\exists\, \alpha \in \mathbb{Z}_k^n$ such that $g_H(\omega^{\alpha_1}, ..., \omega^{\alpha_n}) \neq 0$,
- $g_H \notin \langle x_i^k - 1 : i \in [n]\rangle$,

where the last equality follows from Theorem 3.36 with $g_i(x_i) \coloneqq x_i^k - 1$. □

Even with these results under our belt, it is still no easier to tell whether a given (hyper)graph is k-colourable or not. As Alon notes in his concluding remarks of [Alo99], deciding whether a hypergraph is not k-colourable is coNP-complete and there is (currently, at least) not an efficient way to check if a polynomial is a member of an ideal, even if the ideal has a nice form. That being said, in Chapter 4, although we will find a similar correspondence, we will instead be able to prove that there is an algorithm such that we can find a polynomial that does not lie in the ideal but still has the desired coefficients, giving us tangible results.

Chapter 4

When can a matrix be unlocked...

Definition 4.1. *Let the symmetric group S_{n^2} act on the n^2 elements of a matrix $M \in M_n(\mathbb{F})$ by permutation. Then, M is unlocked by a set $S \subseteq S_{n^2}$ if we can apply a sequence of group elements from S to M after which M is invertible ie. M is unlocked by S if $\exists\, \sigma \in \langle S \rangle \subseteq S_{n^2}$ such that $\det(\sigma(M)) \neq 0$.*

The motivation for this chapter comes from Chapters 1 and 2 of Brauch, Kézdy and Snevily's paper, [BKS14], where they first present the connection between bipartite graphs and the unlocking of matrices over the complex numbers by rotating its rows. They present this idea as an algorithm for determining whether a bipartite graph has a perfect matching by turning the problem into a question about whether a matrix can be unlocked, which, in turn, can be solved in polynomial time using matroids and Edmond's Matroid Intersection Algorithm. By defining the bipartite graph first, they only consider a small selection of matrices with coefficients in $\mathbb{C}$. In the following chapter, we extend these ideas to work for any matrix and over any field, and also introduce a new criterion on when a matrix is unlocked by rotating is rows in the case that the character of the field we're working over divides the width of the matrix. We then introduce the original notions of cluster, minimal clusters and cluster density derived from the notion of the deficiency of a bipartite graph and use these to give an exact condition on when n^2 elements can form an invertible $n \times n$ matrix, equivalently when a matrix can be unlocked by all permutations in S_{n^2}. We are unsure whether a proof of this condition currently exists. Finally, we prove that the same conditions hold for a matrix being unlocked by permutations of both its rows and columns, and finish by looking at the theorem by Kézdy and Snevily in [KS04] which puts the ideas in [BKS14] in context and provides many more avenues that could be explored in the future.

4.1 ...by rotations of its rows?

We will first study what happens when we restrict ourselves to cyclically permuting (or rotating) the rows of a matrix $M \in M_n(\mathbb{F})$.

Notation 4.2. *For $\alpha \in \mathbb{Z}_n^n$, we denote $M[\alpha] \coloneqq (M_{i\, j+\alpha_i \,(\mathrm{mod}\, n)})$ ie. the matrix where we rotate the ith row by α_i positions. Letting e_i denote the standard ith basis vector, if we let $r_i(M) \coloneqq M[e_i]$ then $r_i \in S_{n^2}$ and for $R \coloneqq \{r_i : i \in [n]\} \subseteq S_{n^2}$, then $\langle R \rangle = \{\prod_{i\in[n]} r_i^{\alpha_i} : \alpha \in \mathbb{Z}_n^n\} \subseteq S_{n^2}$ since all r_i commute.*

In the language of Definition 4.1, we say M is unlocked by R or just M can be unlocked by rotations of its rows if and only if $\exists\, \sigma \in \langle R \rangle$ such that $\det(\sigma(M)) \neq 0$. This is equivalent to the existence of $\alpha \in \mathbb{Z}_n^n$ such that $\det(M[\alpha]) \neq 0$.

Example 4.3. *The matrix* $\pi = \begin{pmatrix} 3 & -1 & -4 \\ 1 & 5 & -9 \\ 2 & -6 & 5 \end{pmatrix} \in M_3(\mathbb{Q})$ *can be unlocked by row rotations as even though* $\det(\pi) = 0$, $r_3(\pi) = \pi[e_3] = \begin{pmatrix} 3 & -1 & -4 \\ 1 & 5 & -9 \\ -6 & 5 & 2 \end{pmatrix}$ *has determinant* -27. $\gamma = \begin{pmatrix} 2 & -7 & 5 \\ -3 & -8 & 11 \\ 2 & 0 & -2 \end{pmatrix} \in M_3(\mathbb{Q})$, *however, can not be unlocked by row rotations ie.* $\det(\sigma(\gamma)) = 0$ *for all* $\sigma \in \langle R \rangle$. *This is simply due to the fact that the digits in each row of* γ *add up to* 0. *An easy way to see that this is the case is that* $(1, 1, 1)$ *is an eigenvector of* $\sigma(\gamma)$ *with eigenvalue* 0 *for all* $\sigma \in \langle R \rangle$. *Since the determinant of a matrix is equal to the product of its eigenvalues then* $\det(\sigma(\gamma)) = 0$ *for all* $\sigma \in \langle R \rangle$. *But, as we will see, the rows of a matrix all adding up to* 0 *is not a necessary condition for a matrix not to be able to be unlocked by row rotations.*

Definition 4.4. *Given a matrix* $M \in M_n(\mathbb{F})$, *for* $i \in [n]$, *define* $g_i \in \mathbb{F}[x_i]$ *by*

$$g_i(x_i) \coloneqq \sum_{j=1}^{n} M_{i\,j} x_i^{j-1}.$$

Letting V_n *be the* $n \times n$ *Vandermonde matrix as in Definition 3.29, define* $f_M \in \mathbb{F}[x_1, ..., x_n]$ *as*

$$f_M(x) \coloneqq (\det V_n)(x) \prod_{k=1}^{n} g_k(x_k) = \prod_{1 \le i < j \le n} (x_j - x_i) \prod_{k=1}^{n} g_k(x_k)$$

While the definition of our key polynomial f_M may look fairly arbitrary, its key features are that it contains all the information about our matrix M, both its elements and their positions, and also that it vanishes on any input $x = (x_1, ..., x_n)$ where $x_i = x_j$ for some $i \neq j$.

We now prove a technical lemma.

Lemma 4.5. *For permutations* $\sigma, \beta \in S_n$, *if* $\sigma(i) + \beta(i) \equiv k \pmod{n}$ *for all* $i \in [n]$, *then* $\operatorname{sgn}(\sigma) = (-1)^{(n-1)k + \lfloor \frac{n-1}{2} \rfloor} \operatorname{sgn}(\beta)$.

Proof. For permutations $\tau, \beta \in S_n$, we can restate the condition that $\tau(i) + \beta(i) \equiv 0 \pmod{n}$ for all $i \in [n]$ in terms of permutations by adding in transpositions as such

$$\tau = (1, n-1)(2, n-2)...(\lfloor \frac{n-1}{2} \rfloor, n - \lfloor \frac{n-1}{2} \rfloor)\beta = \left(\prod_{j=1}^{\lfloor \frac{n-1}{2} \rfloor} (j, n-j) \right) \beta$$

We need $\lfloor \frac{n-1}{2} \rfloor$ transpositions since for n odd, every element except n gets swapped ie. $\frac{n-1}{2} = \lfloor \frac{n-1}{2} \rfloor$ swaps whereas for n even, every element except n and $\frac{n}{2}$ gets swapped ie. $\frac{n-2}{2} = \lfloor \frac{n-1}{2} \rfloor$ swaps.

Finally, setting $\sigma = (1, ..., n)^k \tau$ implies $\sigma(i) \equiv \tau(i) + k \pmod{n}$ so $\sigma(i) + \beta(i) \equiv k \pmod{n}$ for all $i \in [n]$. Thus,

$$\begin{aligned} \operatorname{sgn}(\sigma) &= \operatorname{sgn}\left((1, ..., n)^k \prod_{j=1}^{\lfloor \frac{n-1}{2} \rfloor} (j, n-j)\beta \right) = \operatorname{sgn}(1, ..., n)^k \prod_{j=1}^{\lfloor \frac{n-1}{2} \rfloor} \operatorname{sgn}(j, n-j) \operatorname{sgn}(\beta) \\ &= (-1)^{(n-1)k + \lfloor \frac{n-1}{2} \rfloor} \operatorname{sgn}(\beta) \end{aligned}$$

since $\operatorname{sgn}((1, ..., n)) = (-1)^{n-1}$. □

The following Lemma is an extension of part of Theorem 2 from [BKS14], however, the factor of $(-1)^{\lfloor \frac{n-1}{2} \rfloor}$ is missed in the original paper which we amend here.

Lemma 4.6. *Given a matrix $M \in M_n(\mathbb{F})$, then*

$$f_M(x) \equiv (-1)^{\lfloor \frac{n-1}{2} \rfloor} \sum_{\alpha \in \mathbb{Z}_n^n} \det(M[\alpha]) x^\alpha \mod \langle x_i^n - 1 : i \in [n] \rangle$$

Proof. Working modulo the ideal $\langle x_i^n - 1 : i \in [n] \rangle$, we notice that

$$\begin{aligned} x^{-\alpha} \prod_{i=1}^n g_i(x_i) &= \prod_{i=1}^n x_i^{-\alpha_i} g_i(x_i) = \prod_{i=1}^n \sum_{j=1}^n M_{i\,j} x_i^{j-1-\alpha_i} = \prod_{i=1}^n \sum_{j=1-\alpha_i}^{n-\alpha_i} (M)_{i\,j+\alpha_i} x_i^{j-1} \\ &= \prod_{i=1}^n \sum_{j=1-\alpha_i}^{n-\alpha_i} (M[\alpha])_{i\,j\,(\mathrm{mod}\, n)} x_i^{j-1} \equiv \prod_{i=1}^n \sum_{j=1}^n (M[\alpha])_{i\,j} x_i^{j-1} = \sum_{\beta \in \mathbb{Z}_n^n} \prod_{i=1}^n x_i^{\beta_i - 1} (M[\alpha])_{i\,\beta_i} \end{aligned}$$

and using the Leibniz determinant formula, Lemma 3.32,

$$(\det V_n)(x) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{k=1}^n (V_n)_{k\,\sigma(k)} = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{k=1}^n x_k^{\sigma(k)-1}$$

so

$$x^{-\alpha} f_M(x) \equiv \left(\sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{k=1}^n x_k^{\sigma(k)-1} \right) \left(\sum_{\beta \in \mathbb{Z}_n^n} \prod_{i=1}^n x_i^{\beta_i - 1} (M[\alpha])_{i\,\beta_i} \right) \tag{4.1}$$

By comparing coefficients, we can see it is enough to show that, for any $\alpha \in \mathbb{Z}_n^n$, the constant term of $x^{-\alpha} f_M(x)$ modulo the ideal $\langle x_i^n - 1 : i \in [n] \rangle$ is equivalent to $(-1)^{\lfloor \frac{n-1}{2} \rfloor} \det(M[\alpha])$. Looking at Equation 4.1, the constant term of $x^{-\alpha} f_M(x)$ is given by the sum of $\mathrm{sgn}(\sigma) \prod_{i \in [n]} (M[\alpha])_{i\,\beta_i}$ for $\sigma \in S_n, \beta \in \mathbb{Z}_n^n$ where $\sigma(k) - 1 \equiv -\beta_k - 1 \,(\mathrm{mod}\, n)$, equivalently $\sigma(k) \equiv -\beta_k \,(\mathrm{mod}\, n)$ for all $k \in [n]$. The only $\beta \in \mathbb{Z}_n^n$ that fulfil this are permutations of S_n since $\beta_k \equiv -\sigma(k) \,(\mathrm{mod}\, n)$ are distinct for all $k \in [n]$ since $\sigma \in S_n$. Using Lemma 4.5 with $k = 0$, the constant term of $x^{-\alpha} f_M(x)$ is thus

$$\begin{aligned} \sum_{\substack{\sigma \in S_n \\ \beta \in \mathbb{Z}_n^n \\ \sigma(k) \equiv -\beta_k}} sgn(\sigma) \prod_{i=1}^n (M[\alpha])_{i\,\beta_i} &= \sum_{\substack{\sigma, \beta \in S_n \\ \sigma(i) + \beta(i) \equiv 0}} sgn(\sigma) \prod_{i=1}^n (M[\alpha])_{i\,\beta(i)} \\ &= (-1)^{\lfloor \frac{n-1}{2} \rfloor} \sum_{\beta \in S_n} \mathrm{sgn}(\beta) \prod_{i=1}^n (M[\alpha])_{i\,\beta(i)} = (-1)^{\lfloor \frac{n-1}{2} \rfloor} \det(M[\alpha]). \end{aligned}$$

□

Corollary 4.7. *Given a matrix $M \in M_n(\mathbb{F})$, then M is not unlocked by row rotations if and only if $f_M(x) \in \langle x_i^n - 1 : i \in [n] \rangle$.*

Remark 4.8. *Given a matrix M which can be unlocked by row rotations, Theorem 4.6 actually implies that calculating the polynomial expansion of $f_M(x) \bmod \langle x_i^n - 1 : i \in [n] \rangle$ automatically tells us which group elements in $\langle R \rangle \subseteq S_{n^2}$ it is possible to unlock the matrix for. Simply find those $\alpha \in \mathbb{Z}_n^n$ with non-zero coefficients in $f_M(x) \bmod \langle x_i^n - 1 : i \in [n] \rangle$ and then $\prod_{i \in [n]} r_i^{\alpha_i}$ unlocks the matrix.*

As mentioned in Section 3.7, we now have to consider two cases which depend on whether the character of our field $\mathbb{F}$ divides the size of our matrix due to the number of roots of unity in each case.

Case 1: We now study matrices $M \in M_n(\mathbb{F})$ where $\mathrm{char}(\mathbb{F}) | n$.

When $\mathrm{char}(\mathbb{F}) | n$, we have $\mu_n = \{1\}$ as $(x-1)^n = \sum_{i=0}^n \binom{n}{i} (-1)^i x^{n-i} = x^n - 1$ since $n | \binom{n}{i}$ for $1 \leq i \leq n-1$ and $\mathrm{char}(\mathbb{F}) | n$. Following Bruen in [Bru92], we define the multiplicity of an element in a polynomial over any field.

Definition 4.9. *For non-zero polynomial $g \in \mathbb{F}[x_1, ..., x_n]$, then $g(x)$ has multiplicity t at $a \in \mathbb{F}^n$ if*

$$t = \min\{\sum_{i=1}^{n} \alpha_i : \alpha \in \mathbb{N}_0^n, c_\alpha \neq 0\} \quad \text{where} \quad g(x+a) = \sum_{\alpha \in \mathbb{N}_0^n} c_\alpha x^\alpha$$

For convenience, if $g(x) = 0$, we say $g(x)$ has multiplicity ∞ for all $a \in \mathbb{F}^n$.

Example 4.10. *Let $n = 1$ and $g \in \mathbb{F}[t]$. Then g has multiplicity k at $a \in \mathbb{F}$ if $g(t+a) = \sum_{i=0}^{\deg(g)} c_i t^i$ and $k = \min\{i : c_i \neq 0\}$. It is clear that this aligns with the usual notion of multiplicity since if $(t-a)^k | g(t)$, then $t^k | g(t+a)$.*

With Bruen's notion of multiplicity for multi-variable polynomials in hand, using Corollary 4.7, we can now prove an exact condition on when a matrix is unlocked by row rotations in the case that $\text{char}(\mathbb{F}) | n$.

Theorem 4.11. *Let $M \in M_n(\mathbb{F})$ be a matrix where $\text{char}(\mathbb{F}) | n$ with corresponding polynomials $g_i(x_i)$ for $i \in [n]$. Define the sequence $(n_i)_{i \in [n]}$, where $g_i(x_i)$ has multiplicity n_i at 1. Then, M is unlocked by row rotations if and only if there is a permutation $\sigma \in S_n$ such that $n_i < \sigma(i)$ for all $i \in [n]$.*

Proof. We start by proving $\forall\, \sigma \in S_n$, $\exists\, i \in [n]$ such that $n_i \geq \sigma(i) \Leftrightarrow f_M(x + 1_n) \in \langle x_i^n : i \in [n] \rangle$ where $1_n \coloneqq (1, ..., 1)$. For the $\Rightarrow$ direction, using the properties of the determinant of the Vandermonde matrix V_n from Lemma 3.31, we have

$$(\det V_n)(x + 1_n) = \prod_{1 \leq i < j \leq n} (x_j + 1 - x_i - 1) = \prod_{1 \leq i < j \leq n} (x_j - x_i) = (\det V_n)(x)$$

Also, from the definition of the n_i as multiplicities of the g_i, we have $g_i(x_i + 1) = h_i(x_i) x_i^{n_i}$ for some $h_i \in \mathbb{F}[x_i]$ where the h_i have a non-zero constant term. Thus, using the Leibniz formula for the determinant, Lemma 3.32, we have

$$\begin{aligned} f_M(x + 1_n) &= (\det V_n)(x + 1_n) \prod_{i=1}^{n} g_i(x_i + 1) = (\det V_n)(x) \prod_{i=1}^{n} h_i(x_i) x_i^{n_i} \\ &= \left(\sum_{\tau \in S_n} \text{sgn}(\tau) \prod_{i=1}^{n} x_i^{\tau(i)-1} \right) \prod_{i=1}^{n} h_i(x_i) x_i^{n_i} = \sum_{\tau \in S_n} \text{sgn}(\tau) \prod_{i=1}^{n} x_i^{n_i - 1 + \tau(i)} h_i(x_i) \\ &= (-1)^{n-1+\lfloor \frac{n-1}{2} \rfloor} \prod_{i=1}^{n} h_i(x_i) \left(\sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} x_i^{n + n_i - \sigma(i)} \right) \end{aligned}$$

where $\sigma \in S_n$ is defined by $\sigma(i) = (n+1) - \tau(i)$ for all $i \in [n]$ and where we use Lemma 4.5 with $k = 1$ for the $(-1)^{n-1+\lfloor \frac{n-1}{2} \rfloor}$. It is now clear that if $\forall\, \sigma \in S_n$, $\exists\, i \in [n]$ such that $n_i \geq \sigma(i)$ then $f_M(x + 1_n) \in \langle x_i^n : i \in [n] \rangle$.

To prove the $\Leftarrow$ direction, we define a process. For some $Q \subseteq S_n$, define

$$f^{(Q)}(x) = (-1)^{n-1+\lfloor \frac{n-1}{2} \rfloor} \prod_{i=1}^{n} h_i(x_i) \left(\sum_{\sigma \in S_n \backslash Q} \text{sgn}(\sigma) \prod_{i=1}^{n} x_i^{n + n_i - \sigma(i)} \right)$$

and assume $f^{(Q)}(x) \in \langle x_i^n : i \in [n] \rangle$. Now let $d = \min\{\sum_{i \in [n]} n + n_i - \sigma(i) : \sigma \in S_n \backslash Q\}$ and $Q' = \{\sigma \in S_n \backslash Q : \sum_{i \in [n]} n + n_i - \sigma(i) = d\}$. Then since the h_i all have a non-zero constant term, the sum of monomials of $f^{(Q)}(x)$ with degree d is given by a multiple of $\sum_{\sigma \in Q'} \text{sgn}(\sigma) \prod_{i \in [n]} x_i^{n + n_i - \sigma(i)}$. Since Q' is non-empty this sum is non-zero and thus $f^{(Q)}(x) \in \langle x_i^n : i \in [n] \rangle$ implies $\forall\, \sigma \in Q'$, $\exists\, i \in [n]$

such that $n_i \geq \sigma(i)$. In addition, $f^{(Q)}(x) \in \langle x_i^n : i \in [n] \rangle \Rightarrow f^{(Q \cup Q')}(x) \in \langle x_i^n : i \in [n] \rangle$ where $|Q \cup Q'| > |Q|$ and thus we can set $Q = Q \cup Q'$ and repeat the process.

We kick off the first iteration of this process by setting $Q = \emptyset$. Then since the size of Q strictly increases with each iteration, S_n is finite and $f_M(x + 1_n) = f^{(\emptyset)}(x) \in \langle x_i^n : i \in [n] \rangle$, we prove $\forall\, \sigma \in S_n$, $\exists\, i \in [n]$ such that $n_i \geq \sigma(i)$.

Forming a chain of equalities, $\forall\, \sigma \in S_n$, $\exists\, i \in [n]$ such that $n_i \geq \sigma(i) \Leftrightarrow f_M(x + 1_n) \in \langle x_i^n : i \in [n] \rangle$ $\Leftrightarrow f_M(x) \in \langle (x_i - 1)^n : i \in [n] \rangle = \langle x_i^n - 1 : i \in [n] \rangle \Leftrightarrow M$ is not unlocked by row rotations by Corollary 4.7. □

Example 4.12. $\begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{pmatrix} \in M_3(\mathbb{F}_3)$ *can not be unlocked by row rotations, since each row adds up to* 0 *and thus any polynomial with coefficients given by elements in a row will have* 1 *as a root so* $n_i \geq 1$ *for all* $i \in [n]$*. Then, for any* $\sigma \in S_n$*, taking* $\sigma(i) = 1$ *then* $n_i \not< \sigma(i) = 1$ *so by Theorem 4.11, the matrix can not be unlocked. Thus, it is easy to see that, in general, the rows adding up to* 0 *is a sufficient condition for a matrix to not be unlocked by row rotations. However, it is not a necessary condition. Take* $\begin{pmatrix} 1 & 2 & 0 & -1 & 0 \\ 1 & -1 & 2 & 0 & -2 \\ 2 & 1 & -1 & -2 & -2 \\ 2 & -1 & 0 & 1 & -2 \\ 1 & 0 & -1 & -2 & 2 \end{pmatrix} \in M_5(\mathbb{F}_5)$*, which cannot be unlocked by row rotations since the multiplicities at* 1 *are* $(0, 3, 0, 3, 3)$ *but rows* 1 *and* 3 *don't add up to* 0*.*

Case 2: We now study matrices $M \in M_n(\mathbb{F})$ where $\text{char}(\mathbb{F}) \nmid n$.

Lemma 4.13. *For* $n \in \mathbb{N}$*, let* $\mathbb{F}$ *be a field where* $\text{char}(\mathbb{F}) \nmid n$*. Then,* $t^n - 1 = \prod_{\tau \in \mu_n} (t - \tau)$*.*

Proof. Consider the roots of $x^n - 1$ in $\mathbb{F}$. Seeking a contradiction, assume $|\mu_n| < n$. Then $\exists\, \alpha \in \mu_n$ such that $x^n - 1 = (x - \alpha)^2 g(x)$. Taking the formal derivative on both sides, $D((x - \alpha)^2 g(x)) = (x - \alpha)^2 D(g(x)) + 2(x - \alpha) g(x) = D(x^n - 1) = nx^{n-1} =$ and plugging in α, we get $0 = n\alpha^{n-1} = \frac{n}{\alpha} \neq 0$ which is a contradiction. □

Lemma 4.14. *For* $n \in \mathbb{N}$*, let* $\mathbb{F}$ *be a field where* $\text{char}(\mathbb{F}) \nmid n$*. Then, given* $f \in \mathbb{F}[x_1, ..., x_n]$*,* $f \in \langle x_i^n - 1 : i \in [n] \rangle$ *if and only if* $\mu_n^n \subseteq Z(f)[\overline{\mathbb{F}}]$ *ie.* $f(x) = 0$ *for all* $x \in \mu_n^n$*.*

Proof. This follows by Theorem 3.36 using $g_i(x_i) = x_i^n - 1$ which factorises as $g_i(x_i) = \prod_{\omega \in \mu_n} (x_i - \omega)$ by Lemma 4.13. □

Definition 4.15. *Given a matrix* $M \in M_n(\mathbb{F})$*, where* $\text{char}(\mathbb{F}) \nmid n$*, with corresponding polynomials* $g_i(x_i)$*, define the bipartite graph* G_M *with vertices* $V(G_M) = ([n], \mu_n)$ *and edges given by* $(i, \omega^j) \in E(G_M)$ *if and only if* $\omega^j \notin Z(g_i)[\overline{\mathbb{F}}]$ *for all* $i, j \in [n]$*, where* ω *is a generator of* μ_n*.*

The following lemma is a generalisation of part of Theorem 2 from [BKS14] to any matrix over any field where $\text{char}(\mathbb{F}) \nmid n$. We recall the notion of a perfect matching from Definition 1.17.

Lemma 4.16. *Given a matrix* $M \in M_n(\mathbb{F})$ *with corresponding polynomial* $f_M(x)$ *and graph* G_M*, there exists a perfect matching on* G_M *if and only if* $\mu_n^n \not\subseteq Z(f_M)[\overline{\mathbb{F}}]$ *ie.* $f_M(x) \neq 0$ *for some* $x \in \mu_n^n$*.*

Proof. Let ω be a generator of μ_n. For the $\Rightarrow$ direction, let the perfect matching be given by $(i, \omega^{\sigma(i)}) \in E(G_M)$ for some $\sigma \in S_n$. Then by the definition of G_M, Definition 4.15, $\omega^{\sigma(i)} \notin Z(g_i)[\overline{\mathbb{F}}]$ for all

$i \in [n]$. Thus since σ is a permutation and using Lemma 3.31, then $\det V_n(\omega^{\sigma(1)}, ..., \omega^{\sigma(n)}) \neq 0$, thus $f_M(\omega^{\sigma(1)}, ..., \omega^{\sigma(n)}) \neq 0$. For the $\Leftarrow$ direction, assume $f_M(x) \neq 0$ for some $x \in \mu_n^n$, then since $(\det V_n)(x) \neq 0$, again using Lemma 3.31, then $x = (\omega^{\sigma(1)}, ..., \omega^{\sigma(n)})$ for some $\sigma \in S_n$ a permutation. Thus, for all $i \in [n]$, $\omega^{\sigma(i)} \notin Z(g_i)[\overline{\mathbb{F}}] \Leftrightarrow (i, \omega^{\sigma(i)}) \in E(G_M)$ and since σ is a permutation, this is a perfect matching on G_M. □

The equivalent of Theorem 4.17 for the case $\text{char}(\mathbb{F}) \nmid n$ now falls out.

Theorem 4.17. *Given a matrix $M \in M_n(\mathbb{F})$ where $\text{char}(\mathbb{F}) \nmid n$ with corresponding graph G_M, then M is unlocked by row rotations $\Leftrightarrow$ there exists a perfect matching on G_M.*

Proof. By Corollary 4.7, Lemma 4.14 and Lemma 4.16, M is unlocked by row rotations $\Leftrightarrow f_M \notin \langle x_i^n - 1 : i \in [n] \rangle \Leftrightarrow \mu_n^n \not\subseteq Z(f_M)[\overline{\mathbb{F}}] \Leftrightarrow$ there exists a perfect matching on G_M. □

Example 4.18. *We can now see another reason why the matrix* $\gamma = \begin{pmatrix} 2 & -7 & 5 \\ -3 & -8 & 11 \\ 2 & 0 & -2 \end{pmatrix} \in M_3(\mathbb{R})$ *from Example 4.3, or indeed any matrix where the rows add up to 0 can not be unlocked by row rotations. We can construct a polynomial with coefficients given by a row of the matrix; if the coefficients add up to 0, then the polynomial has a root at 1. If this is the case for every row, then when we construct our bipartite graph G_M, $(i, 1) \notin E(G)$ for any $i \in [n]$. Thus, by the pigeonhole principle, it is impossible for G_M to have a perfect matching, otherwise there would have to be an edge connected to $1 \in \mu_n$.*

For a slightly more complicated example, let $\mathbb{F} = \mathbb{F}_3$, and take $\mu = \begin{pmatrix} 0 & 1 & 0 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & 1 & 0 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \in M_4(\mathbb{F}_3)$. *You would have to calculate at most $4! = 24$ determinants to find out if μ can be unlocked by rotations, however, luckily for us we have some theorems we can use.*

Instead of taking the full closure of $\mathbb{F}_3$, it is enough to let $\theta^2 + 1 = 0$ and work in $\mathbb{F}_9 = \mathbb{F}_3[\theta]$ since $\mathbb{F}_9$ contains Ω_4 as $\mathbb{F}_9^\times \cong \mathbb{Z}_8$. Then notice that polynomials $g_1(x_1) = x_1^3 + x_1$, $g_2(x_2) = -x_2^3 - x_2^2 - x_2 - 1$, $g_3(x_3) = -x_3^3 + x_3 - 1$ and $g_4(x_4) = -x_4^3 + x_4^2 - x_4 + 1$ all have θ and $-\theta$ as roots. Thus G_μ, as depicted in Figure 4.1, does not have a perfect matching since only 3 is connected to θ and $-\theta$ and thus by Theorem 4.17, μ can not be unlocked by row rotations.

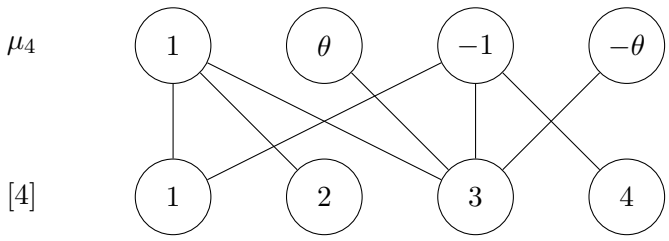


Figure 4.1: The bipartite graph G_μ corresponding to matrix μ from Example 4.18.

Remark 4.19. *It seems that whether* $\text{char}(\mathbb{F})$ *divides n or not gives rather different conditions on when the matrix can be unlocked by row rotations. However, these two cases are not so dissimilar if we reformulate the case* $\text{char}(\mathbb{F})|n$. *The constraint given in Theorem 4.11 was that $M \in M_n(\mathbb{F})$ was unlocked by row rotations if and only if there was a permutation $\sigma \in S_n$ such that $n_i < \sigma(i)$ for $i \in [n]$ where $(n_i)_{i \in [n]}$ was given by $g_i(x_i)$ having multiplicity n_i at 1. Similarly to Definition 4.15,*

where we defined G_M, we can define a graph H_M with vertices given by $V(H_M) = ([n], [n])$ and edges $(i, j) \in E(H_M)$ if and only if $n_i < j$ for all $i, j \in [n]$. Clearly $\exists\, \sigma \in S_n$ such that $n_i < \sigma(i)$ for all $i \in [n]$ $\Leftrightarrow (i, \sigma(i)) \in E(H_M) \Leftrightarrow H_M$ has a perfect matching since σ is a permutation. In some sense, we see that Theorem 4.11 (the $\mathrm{char}(\mathbb{F})|n$ case) is not as strong a statement as Theorem 4.17 (the $\mathrm{char}(\mathbb{F}) \nmid n$ case), since we can construct matrices M such that G_M is any bipartite graph whereas this is not true for H_M, since for any edge $(i, j) \in E(H_M)$, we automatically have $(i, j') \in E(H_M)$ for all $j' \geq j$. This will result in a more difficult proof of the more general versions of Theorem 4.11 and Theorem 4.17, where we want to prove the forms of matrices which are unlocked by the set of all permutations.

4.2 ...by all permutations?

We now have an exact condition on when a matrix is unlocked by row rotations. But what happens if we allow ourselves to rotate both the rows and columns as we please in any order? What if we allow any permutation of the elements of the matrix? It turns out that the latter question will help us answer the former, so we tackle that first.

We will first give an exact condition on when a matrix is unlocked by all permutations for the easier $\mathrm{char}(\mathbb{F})|n$ case, as a warm-up for the trickier $\mathrm{char}(\mathbb{F}) \nmid n$ case.

Theorem 4.20. *For $n \geq 2$, given n^2 elements in a field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F})|n$, where there are at most $n^2 - n + 1$ of the same element or at most $n^2 - n$ zeroes, we can always construct an invertible $n \times n$ matrix out of those elements.*

Before we prove Theorem 4.20, we must first prove some technical lemmas.

Lemma 4.21. *For $n \geq 1$, given a polynomial $p \in \mathbb{F}[t]$ with degree at most $n - 1$, $Z(p)[\overline{\mathbb{F}}] \cap \mu_n$ is invariant under cyclic permutations (rotations) of the coefficients of $p(t)$.*

Proof. The statement of this Lemma is equivalent to $\omega \in Z(p(t))[\overline{\mathbb{F}}] \Leftrightarrow \omega \in Z(t^k p(t) \bmod \langle t^n - 1\rangle)[\overline{\mathbb{F}}]$ for all $k \in [n]$, $\omega \in \mu_n$. Writing, $t^k p(t) \bmod \langle t^n - 1\rangle$as $t^k p(t) + (t^n - 1)q(t)$ for some $q \in \mathbb{F}[t]$, and evaluating at ω, we get $\omega^k p(\omega) + (\omega^n - 1)q(\omega) = \omega^k p(\omega)$ and the result follows since $\omega^k \neq 0, \forall\, k \in [n]$. □

Lemma 4.22. *For $n \geq 2$, given a polynomial $p \in \mathbb{F}[t]$, let $p(t) = \sum_{i=0}^{n-1} a_i t^i$. For some $b_0 \in \mathbb{F}$ where $b_0 \neq a_0$, let $\hat{p}(t) = \sum_{i=1}^{n-1} a_i t^i + b_0$. Then $p(t)$ and $\hat{p}(t)$ share no roots in $\overline{\mathbb{F}}$ ie. $Z(p)[\overline{\mathbb{F}}] \cap Z(\hat{p})[\overline{\mathbb{F}}] = \emptyset$.*

Proof. We have $p(t) - \hat{p}(t) = a_0 - b_0 \neq 0$, thus $p(t)$ and $\hat{p}(t)$ share no common values, in particular share no roots. □

Corollary 4.23. *Given a matrix M with corresponding sequence of multiplicities $(n_i)_{i\in[n]}$, if for $i, j \in [n]$, $0 < n_i, n_j \leq n - 1$, after swapping distinct elements of M, one from row i and one from row j, the new matrix will have multiplicities $n_i = n_j = 0$.*

Proof. Let α_i, α_j be the elements to be swapped in rows i, j respectively. Since $n_i, n_j > 0$, then $1 \in Z(g_i), Z(g_j)$. We start by rotating rows i, j, thus cyclically permuting the coefficients of g_i, g_j until α_i, α_j are the constant coefficients in g_i, g_j respectively ie. α_i, α_j are in the first column of M. By Lemma 4.21, 1 is still a root of g_i and g_j. Using Lemma 4.22 on both polynomials g_i, g_j separately, when we swap α_i, α_j, $1 \notin Z(g_i), Z(g_j)$. Finally, we can rotate rows i, j until α_i is in the old position of α_j and α_j is in the old position of α_i and, using 4.21, even after these rotations, $1 \notin Z(g_i), Z(g_j)$. The new matrix is just M with α_i and α_j swapped but since $1 \notin Z(g_i), Z(g_j)$ in the new matrix, $n_i = n_j = 0$. □

We will now prove Theorem 4.20. We start by arranging the n^2 elements in a matrix M (we can't guarantee M is invertible). We then swap a series of elements between rows until we can guarantee that the matrix is able to be unlocked by row rotations using our exact statement on when a matrix can be unlocked, Theorem 4.11. Finally, we can perform the relevant row rotations, leaving us with an invertible matrix made from the n^2 elements. Even though we are performing changes to the matrix M we will not keep track of these and will continually denote our matrix M.

Proof of Theorem 4.20. Since we have at most $n^2 - n + 1$ of the same element, we can always arrange the n^2 elements in a matrix M such that at most 1 row contains n copies of the same element and no row contains all zeroes. The condition that at most 1 row contains n copies of the same non-zero element implies that there is at most $i \in [n]$ such that $n_i = n-1$. This is because the polynomial with all entries the same and non-zero is equal to a multiple of $x^{n-1} + x^{n-2} + ... + x + 1 = \frac{x^n-1}{x-1} = \frac{(x-1)^n}{x-1} = (x-1)^{n-1}$. The condition that no row contains all zeroes implies that every n_i is finite and since $\deg(g_i(x_i)) \leq n-1$, $n_i \leq n-1$ for all $i \in [n]$.

We will now swap distinct elements from distinct rows, until all but one $n_i = 0$ for $i \in [n]$. Given two rows $i, j \in [n]$ with multiplicities $0 < n_i, n_j \leq n-1$, we can always find two distinct elements, one from each row, since at most one row contains n copies of the same element. By Corollary 4.23, after swapping these elements, $n_i = n_j = 0$. It is important to note that, in doing this, we never create a row which contains n copies of the same element and thus we can always guarantee that at most one row of the matrix M has n copies of the same element.

We repeat this process until there is at most one row $i \in [n]$ with $n_i \neq 0$. It is clear no elements have been swapped in row i since otherwise $n_i = 0$. However, since $n_i \leq n-1$ to start off with, we can choose any $\sigma \in S_n$ with $\sigma(i) = n$ and since all other $n_j = 0$, $n_j < \sigma(j)$ for all $j \in [n]$. Thus, by Theorem 4.11, M is unlocked by row rotations. Thus, by applying the necessary swaps and row rotations to our starting matrix we constructed an invertible matrix out of our original n^2 elements. □

Unfortunately, due to the more complex condition involving perfect matchings on bipartite graphs for the case when $\text{char}(\mathbb{F}) \nmid n$, we will not be able to prove the same statement as in Theorem 4.20 straight away. Instead, we must state Hall's marriage, an exact condition on when bipartite graphs have perfect matchings, and introduce the key concepts of clusters, minimal clusters and cluster density.

Hall's Marriage Theorem

First proved by Hall in [Hal86], Hall's marriage theorem gives an exact condition on when a bipartite graph has a perfect matching. According to [Hir07], it supposedly got its name from one of the many ways the theorem can be posed: suppose we have a group of boys and girls, where we need to find all the boys a partner from the group of girls. We can start by asking the girls to write a list of the boys they find acceptable and we assume the boys will not turn down a date with a girl. Given this information, can we match the boys and girls up in happy couples?

Definition 4.24. *We recall from Definition 1.17, that a perfect matching on a graph G is a subset of the edge set $S \subseteq E(G)$ such that every vertex in $V(G)$ is contained in some edge in S. Now let G be a bipartite graph with vertices $V(G) = (A, B)$. Then, we define an $A-$perfect matching on G to be a subset of the edge set $S \subseteq E(G)$, such that every vertex of A is contained in some edge in S.*

Remark 4.25. *For a bipartite graph G with vertices $V(G) = (A, B)$, if $|A| = |B|$, G has an $A-$perfect matching $\Leftrightarrow$ G has a $B-$perfect matching $\Leftrightarrow$ G has a perfect matching.*

We now state but do not prove Hall's Theorem. A good proof is found in [DeV] using the theory of M-alternating and M-augmenting paths.

Theorem 4.26 (Hall's marriage theorem)**.** *Given a bipartite graph G with vertices $V(G) = (A, B)$, there exists an $A-$perfect matching on $G \Leftrightarrow |W| \leq |N_G(W)|$ for all $W \subseteq A$.*

Definition 4.27. *Given a family of sets $\mathcal{F}$, let $\mathcal{F}_X = \bigcup_{S\in\mathcal{F}} S$. Then, a transversal of $\mathcal{F}$ is a subset of $\mathcal{F}_X$ which contains exactly one distinct element from every set $S \in \mathcal{F}$.*

Corollary 4.28. *A family of sets $\mathcal{F}$ has a transversal $\Leftrightarrow$ for all $\mathcal{G} \subseteq \mathcal{F}$, $|\mathcal{G}| \leq |\mathcal{G}_X|$.*

Proof. Given a family of sets $\mathcal{F}$, construct a bipartite graph $G_\mathcal{F}$ with vertices $V(G_\mathcal{F}) = (\mathcal{F}_X, \mathcal{F})$. Then for all elements $s \in S$, for all sets $S \in \mathcal{F}$, let $(s, S) \in E(G_\mathcal{F})$. It is now clear that $\mathcal{F}$ has a transversal $\Leftrightarrow$ $G_\mathcal{F}$ has an $\mathcal{F}-$perfect matching $\Leftrightarrow |W| \leq |N_{G_\mathcal{F}}(W)|$ for all $W \subseteq \mathcal{F} \Leftrightarrow |\mathcal{G}| \leq |\mathcal{G}_X|$ for all $\mathcal{G} \subseteq \mathcal{F}$. □

Example 4.29. *[Hir07] Given a standard deck of 52 cards, split the cards into 13 piles of 4 cards. Can we always pick one card from every pile such that we pick exactly one card of each rank[1] ?*

Let $\mathcal{F}$ be the family of sets where each set contains all the ranks of cards in a corresponding pile. Since there are only 4 cards of every rank and all piles contain 4 cards, by the pigeonhole principle, we must have that for any selection of k piles, there are at least k different cards contained in those piles. Then Corollary 4.28 tells us that $\mathcal{F}$ has a transversal ie. there is a way to pick exactly one card from each pile such that no two cards are the same rank, and since there are 13 piles and 13 ranks this implies every card we choose has a distinct rank.

We now introduce some notions that tie in closely with Hall's Marriage Theorem and perfect matchings, the first being the deficiency of a bipartite graph, originally defined by Ore in [Ore55].

Definition 4.30. *Given a bipartite graph G with vertices $V(G) = (A, B)$, the deficiency of a set $U \subseteq V(G)$, is defined to be $\mathrm{def}_G(U) \coloneqq |U| - |N_G(U)|$. Furthermore, the deficiency of G with respect to A is defined to be $\mathrm{def}(G; A) \coloneqq \max_{U\subseteq A} \mathrm{def}_G(U)$. Note that $\mathrm{def}_G(\emptyset) = 0$ so we have that $\mathrm{def}(G; A) \geq 0$. Finally, if $|A| = |B|$, the deficiency of G is defined to be $\mathrm{def}(G) \coloneqq \mathrm{def}(G; A) = \mathrm{def}(G; B)$.*

Lemma 4.31. *For a bipartite graph G where $|A| = |B|$, then $\mathrm{def}(G; A) = \mathrm{def}(G; B)$.*

Proof. For a set $U \subseteq A$, by Definition 4.30, we have

$$\begin{aligned}\mathrm{def}_G(U) &= |U| - |N_G(U)| = |A| - |A\backslash U| - |B| + |B\backslash N_G(U)| \\ &\leq -|N_G(B\backslash N_G(U))| + |B\backslash N_G(U)| = \mathrm{def}_G(B\backslash N_G(U)).\end{aligned}$$

Thus $\mathrm{def}(G; A) \leq \mathrm{def}(G; B)$, so by symmetry of swapping A and B, $\mathrm{def}(G; A) = \mathrm{def}(G; B)$. □

We now define the original notions of clusters, minimal clusters and cluster density.

Definition 4.32. *Let G be a bipartite graph with vertices $V(G) = (A, B)$. We define a cluster in G to be a set $W \subseteq A$ where $\mathrm{def}_G(W) > 0$ ie. $|W| > |N_G(W)|$. Furthermore we say that a cluster $W \subseteq A$ is minimal if there does not exist a set $U \subset W \subseteq A$ which is again a cluster. Let $\mathrm{clust}(G; A) = \{W \subseteq A : \mathrm{def}_G(W) > 0\}$ ie. the set of clusters in G and define the cluster density to be $\mathrm{cd}(G; A) \coloneqq \sum_{W\in\mathrm{clust}(G;A)} \mathrm{def}_G(W)$.*

[1] Every playing card contains precisely one symbol from the set $\{A, 2, ..., 10, J, Q, K\}$ which is its rank.

Remark 4.33. *It is easy to see, using Hall's Marriage Theorem, Theorem 4.26, and Definition 4.30 and Definition 4.32, for a bipartite graph G with vertices $V(G) = (A, B)$, the following are equivalent:*

- *G has an $A-$perfect matching,*
- *$|W| \leq |N_G(W)|$ for all $W \subseteq A$,*
- *$\mathrm{def}_G(W) \leq 0$ for all $W \subseteq A$,*
- *$\mathrm{def}(G; A) = 0$,*
- *$\mathrm{cd}(G; A) = 0$.*

We can finally return to our study of matrices and state the equivalent of Theorem 4.20 but now for the case $\mathrm{char}(\mathbb{F}) \nmid n$, which has a similar but substantially harder proof. We will then be able combine it with Theorem 4.20 to give an exact statement on when all matrices are unlocked by all permutations.

Theorem 4.34. *For $n \geq 3$, given n^2 elements in a field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \nmid n$, where there are at most $n^2 - n + 1$ of the same element or at most $n^2 - n$ zeroes, we can always construct an invertible $n \times n$ matrix out of those elements.*

Before we prove Theorem 4.34, we will need some technical lemmas. These aim to show that, by swapping elements of a matrix M, we can strictly reduce the cluster density of the corresponding bipartite graph G_M and, in some sense, remove clusters until we are guaranteed to be left with a bipartite graph which has a perfect matching, meaning M can be unlocked by row rotations.

Definition 4.35. *Let G be a bipartite graph with vertices $V(G) = (A, B)$. We will now define a set of graphs, depending on some point $p \in A$ and denoted $T_p(G)$ which we refer to as transformed graphs. A graph $G' \in T_p(G)$ if:*

- *$V(G') = (A, B)$ ie. G' has the same vertices as G,*
- *$(p, b) \notin G \Rightarrow (p, b) \in G'$ for all $b \in B$,*
- *$(q, b) \in G \Leftrightarrow (q, b) \in G'$ for all $q \in A \backslash \{p\}$.*

For a set of bipartite graphs S, let $T_p(S) \coloneqq \cup_{G \in S} T_p(G)$.

Lemma 4.36. *Let G be a bipartite graph with vertices $V(G) = (A, B)$ where $|A| = |B|$. Let W be a minimal cluster in G, then for any $p \in W$, for all $G' \in T_p(G)$, $\mathrm{cd}(G'; A) < \mathrm{cd}(G; A)$.*

Proof. Let $p \in W$ and $G' \in T_p(G)$. Then we aim to show that any set $W' \subseteq A$ where $p \in W'$ is not a cluster in G'.

- Letting $Q = (W \cap W') \backslash \{p\}$, then Q is not a cluster in G since otherwise W would not be minimal as $Q \subseteq W$. Thus $|N_G(Q)| \geq |Q|$.
- We now claim $N_G(Q) \sqcup (\mu_n \backslash N_G(W)) \subseteq N_{G'}(W')$. Since $(q, b) \in G \Leftrightarrow (q, b) \in G'$ for all $q \in A \backslash \{p\}$ and $p \notin Q$, then $N_G(Q) = N_{G'}(Q) \subseteq N_{G'}(W')$ as $Q \subseteq W'$. Furthermore, since $(p, b) \notin G \Rightarrow (p, b) \in G'$ for all $b \in B$ and $p \in W, W'$, we also have that $\mu_n = N_G(\{p\}) \cup N_{G'}(\{p\}) \subseteq N_G(W) \cup N_{G'}(W')$, and thus $(\mu_n \backslash N_G(W)) \subseteq N_{G'}(W')$ showing $N_G(Q) \cup (\mu_n \backslash N_G(W)) \subseteq N_{G'}(W')$. Finally, $N_G(Q) \cap (\mu_n \backslash N_G(W)) \subseteq N_G(W) \cap (\mu_n \backslash N_G(W)) = \emptyset$ and thus $|N_{G'}(W')| \geq |N_G(Q)| + |\mu_n \backslash N_G(W)|$.
- Since W is a cluster, we know $|W| > |N_G(W)|$, so as $W \subseteq [n]$ and $N_G(W) \subseteq \mu_n$, $|\mu_n \backslash N_G(W)| = n - |N_G(W)| > n - |W| = |[n] \backslash W| \geq |W' \backslash W|$. Thus $|\mu_n \backslash N_G(W)| \geq |W' \backslash W| + 1$.

Since $|N_{G'}(W')| \geq |N_G(Q)| + |\mu_n \backslash N_G(W)| \geq |Q| + |W' \backslash W| + 1 = |W \cap W'| - 1 + |W' \backslash W| + 1 = |W' \backslash W| + |W' \cap W| = |W'|$ then W' is not a cluster. Finally, let $U \in \mathrm{clust}(G'; A)$. By the above, $p \notin U$, so since $(q, b) \in G \Leftrightarrow (q, b) \in G'$ for all $q \in A \backslash \{p\}$ then $\mathrm{def}_{G'}(U) = |U| - |N_{G'}(U)| = |U| - |N_G(U)| = \mathrm{def}_G(U)$. Also, since $p \in W$, $W \notin \mathrm{clust}(G'; A)$ but $W \in \mathrm{clust}(G; A)$ and thus $\mathrm{cd}(G'; A) = \sum_{U \in \mathrm{clust}(G'; A)} \mathrm{def}_{G'}(U) < \sum_{U \in \mathrm{clust}(G; A)} \mathrm{def}_G(U) = \mathrm{cd}(G'; A)$. □

Remark 4.37. *It is interesting to note that Lemma 4.36 would not necessarily hold if we just required the point p to be in a cluster and not a minimal cluster.*

We now need to build up some results about how swapping elements in our matrix M affects the corresponding bipartite graph G_M

Lemma 4.38. *For $n \geq 2$, given a polynomial $p \in \overline{\mathbb{F}}[t]$, let $p(t) = \sum_{i=0}^{n-1} a_i t^i$. Consider the polynomial where we swap the first two entries ie. $\hat{p}(t) = \sum_{i=2}^{n-1} a_i t^i + a_0 t + a_1$. Then, if $a_0 \neq a_1$, $p(t)$ and $\hat{p}(t)$ share no roots except for $t = 1$ ie. $Z(p)[\overline{\mathbb{F}}] \cap Z(\hat{p})[\overline{\mathbb{F}}] \in \{\emptyset, \{1\}\}$.*

Proof. The result follows by considering $p(t) - \hat{p}(t) = (a_1 - a_0)(t-1)$ and using $a_0 \neq a_1$. Thus, $p(t)$ and $\hat{p}(t)$ share no common values, in particular no common roots, unless $t = 1$. □

Lemma 4.39. *Given a matrix M and bipartite graph G_M, if M' is the matrix where we replace any element in row $i \in [n]$ with a different element, then $G_{M'} \in T_i(G_M)$.*

Proof. Let M have corresponding polynomials $g_i(x_i) = \sum_{i \in [n]} M_{i\,j} x_i^{j-1}$ for all $i \in [n]$ and let α be the element we want to replace which is in position (i, j). Let $\hat{M} \coloneqq r_i^{j-1}(M)$ ie. the matrix where we can rotate the elements in the ith row so that α is now in position $(i, 1)$ and thus acts as the constant of $g_i(x_i)$. By Lemma 4.21, this does not change $Z(g_i)[\overline{\mathbb{F}}] \cap \mu_n$, thus $G_{\hat{M}} = G_M$. Now, let $\overline{M}$ be the matrix where we replace α with α'. By Lemma 4.22, if $\overline{g}_i(x_i) = \sum_{i \in [n]} \overline{M}_{i\,j} x_i^j$, since $\alpha \neq \alpha'$ then $Z(g_i)[\overline{\mathbb{F}}] \cap Z(\overline{g}_i)[\overline{\mathbb{F}}] \cap \mu_n = \emptyset$, thus in $G_{\overline{M}}$ the vertex $i \in [n]$ is connected to all the vertices in μ_n that it wasn't connected to in G_M and all other vertices in $[n]$ and their edges are identical, thus $G_{\overline{M}} \in T_i(G_M)$. Finally, let M' be the matrix where we undo the rotation we did at the beginning so M' is simply M with one element in row i changed. By Lemma 4.21 again, $G_{\overline{M}} = G_{M'}$ which implies $G_{M'} \in T_i(G_M)$. □

Notation 4.40. *For a graph G, for $S \subseteq V(G)$, the induced subgraph $G[S]$ is the graph whose vertex set is S and whose edge set are those edges in G where both endpoints are in S ie. $V(G[S]) = S$ and $(i, j) \in E(G[S]) \Leftrightarrow (i, j) \in E(G)$ and $i, j \in S$. Furthermore, if G is bipartite with vertices $V(G) = (A, B)$, then for $S_A \subseteq A$ and $S_B \subseteq B$, the induced subgraph is denoted $G[(S_A, S_B)]$.*

Corollary 4.41. *For $A \subseteq [n]$, if $\tilde{M}$ is the matrix where we swap two different adjacent elements in row i of M, then $G_{\tilde{M}}[(A, \mu_n \backslash \{1\})] \in T_i(G_M[(A, \mu_n \backslash \{1\})])$.*

Proof. By Lemma 4.21, we can move the two adjacent elements to be the first two row entries so that they are the constant and linear term in $g_i(x_i)$, leaving G_M unchanged. By Lemma 4.38, when we swap them, all the previous roots of $g_i(x_i)$ are no longer roots except for $x_i = 1$. Thus, the corresponding graph of the new matrix lies in $T_i(G_M[(A, \mu_n \backslash \{1\})])$. Finally, we use Lemma 4.21 to move the elements back to their starting positions implying $G_{\tilde{M}}[(A, \mu_n \backslash \{1\})] \in T_i(G_M[(A, \mu_n \backslash \{1\})])$. □

We are now in a position to prove Theorem 4.34, which will follow the same process we used for the $\text{char}(\mathbb{F})|n$, Theorem 4.20. We arrange our n^2 elements in a matrix M and perform a series of swaps of elements, thus reducing the cluster density of the corresponding bipartite graph G_M, until we can guarantee the matrix can be unlocked by row rotation using our exact condition on when matrices can be unlocked, Theorem 4.17. Applying the relevant row rotations, the matrix made out of the n^2 elements is now invertible.

Proof of Theorem 4.34. To start, since we have at most $n^2 - n + 1$ of the same element, we can always arrange the n^2 elements in the matrix M such that at most 1 row contains n copies of the same element and no row contains all zeroes. The condition that at most 1 row contains n copies of the same non-zero element implies that there is at most 1 vertex in $[n]$ which has only 1 edge and that edge is connected to $1 \in \mu_n$. This is because the polynomial with all entries the same and non-zero is equal to a multiple of $x^{n-1} + x^{n-2} + ... + x + 1 = \frac{x^n-1}{x-1}$ and thus has roots $\mu_n \backslash \{1\}$. The condition that no row contains all zeroes implies that every vertex in $[n]$ has at least 1 edge connected to it, since everything, including μ_n, is a root of the zero polynomial.

We need to resolve a few technicalities before we perform the majority of the switches. In particular, we need $1 \in \mu_n$ to be connected to at least 1 vertex in $[n]$ but still keep the condition that there is at most 1 vertex in $[n]$ which has only 1 edge and that edge is connected to $1 \in \mu_n$. If $1 \in \mu_n$ has no edges, we will swap two elements of M to rectify this. Since at most 1 row contains all the same elements, we can always find two different elements α and β in two different rows i and j respectively to swap, leaving us with a new matrix $\hat{M}$. By Lemma 4.39, since $(i,1),(j,1)$ are not edges of G_M, then $(i,1),(j,1)$ are edges in all the graphs in $T_i(T_j(G_M))$ and $G_{\hat{M}} \in T_i(T_j(G_M))$. There is now the unwanted case that in $G_{\hat{M}}$, i, $j \in [n]$ are both now only connected to $1 \in \mu_n$. If this happens, we know that rows i and j of $\hat{M}$ are both filled with n copies of β and α respectively. So swap α and β back so our matrix returns to M and now swap an extra β and α between rows i and j giving us a new matrix $\overline{M}$ with $G_{\overline{M}} \in T_i(T_j(G_M))$. This time, however, since $n \geq 3$, rows i, $j \in [n]$ in $\overline{M}$ both contain at least two distinct elements and thus in $G_{\overline{M}}$, i, $j \in [n]$ are connected to $1 \in \mu_n$ as well as another vertex in μ_n. We reset our notation so M is the matrix with the necessary switches such that G_M has our desired properties.

Since G_M satisfies these properties, if there is a vertex in $[n]$ which is only connected to $1 \in \mu_n$, denote it v, otherwise let v be any vertex connected to $1 \in \mu_n$. We now define the graph $G'_M \coloneqq G_M[([n]\backslash\{v\}, \mu_n\backslash\{1\})]$. The reason we performed all these tedious switches is so we can guarantee that every vertex in $[n]\backslash\{v\} \subset V(G'_M)$ has at least one edge, implying none of the rows are made up of only one distinct element.

If there is a cluster in G'_M, there is a minimal cluster in G'_M from which we pick a vertex i. We know that none of the rows of M are made up of only one distinct element, including row i, so by Corollary 4.41, we can swap two distinct adjacent elements, giving us a new matrix $\tilde{M}$ where $G'_{\tilde{M}} \coloneqq G_{\tilde{M}}[([n]\backslash\{v\}, \mu_n\backslash\{1\})] \in T_i(G'_M)$. Also, by Lemma 4.36, $\mathrm{cd}(G'_{\tilde{M}}; [n]\backslash\{v\}) < \mathrm{cd}(G'_M; [n]\backslash\{v\})$. Repeating the above process, resetting our notation back to M every time, we slowly untangle clusters in the graph G'_M thus reducing $\mathrm{cd}(G'_M; [n]\backslash\{v\})$ until $\mathrm{cd}(G'_M; [n]\backslash\{v\}) = 0$ and thus by Remark 4.33, we have a perfect matching on G'_M. At this point, we will see that we now have a perfect matching on G_M, since $(v,1) \in E(G_M)$. Now, by Theorem 4.17, since $\mathrm{char}(\mathbb{F}) \nmid n$, M can be unlocked by row rotations and after applying these rotations, our n^2 elements make up an invertible matrix. □

Remark 4.42. *It is very easy to apply the proof of the above Theorem, Theorem 4.34, to the $n = 2$ case since we only use the condition that $n \geq 3$ once. If we rewrite the third paragraph of the proof in the $n = 2$ case, it is easy to see that the only case we need to reconsider is when we have matrix $M = \begin{pmatrix} a & -a \\ -a & a \end{pmatrix}$ for any $a \in \mathbb{F}$ and thus $E(G_M) = \{(1,-1),(2,-1)\}$. In this case, when we swap two different elements, we get $\hat{M} = \begin{pmatrix} a & -a \\ a & -a \end{pmatrix}$. Now $E(G_{\hat{M}}) = \{(1,1),(2,1)\}$ so $G_{\hat{M}}$ now has two vertices connected to $1 \in \mu_2$ and by the proof, we should switch a and $-a$ back. However, when we switch the*

other a and $-a$, we're back to the matrix M and thus caught in an infinite loop. In fact, it is no wonder the proof doesn't work for this matrix, since we can never construct an invertible matrix if we're given the elements $\{a, a, -a, -a\}$! So, by considering this case separately, we can actually give the following statement.

For $n \in \mathbb{N}$, given n^2 elements in a field $\mathbb{F}$, then, unless there are more than $n^2 - n + 1$ of the same element, more than $n^2 - n$ zeroes or the elements are $\{a, a, -a, -a\}$ for some $a \in \mathbb{F}$, we can always construct an invertible $n \times n$ matrix out of those elements.

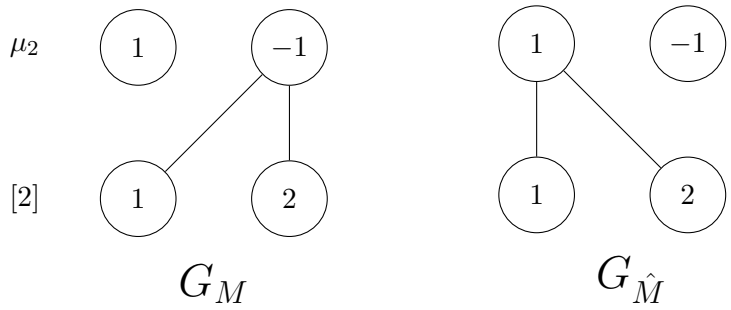


Figure 4.2: The bipartite graphs G_M and $G_{\hat{M}}$ corresponding to M and $\hat{M}$ respectively from Remark 4.42.

Corollary 4.43. *For $n \in \mathbb{N}$, given n^2 elements in a field $\mathbb{F}$, we can always construct an invertible $n \times n$ matrix out of those elements if and only if there are at most $n^2 - n + 1$ of the same element, at most $n^2 - n$ zeroes and the elements are not $\{a, a, -a, -a\}$ for some $a \in \mathbb{F}$.*

Proof. Then $n = 1$ case is trivial. For $n \geq 2$, the $\Leftarrow$ follows from Theorem 4.34, Theorem 4.20 and Remark 4.42. For the $\Rightarrow$ direction, if there are more than $n^2 - n + 1$ of the same element, by the pigeonhole principle, there are always going to be two rows filled with only one distinct element no matter how we rearrange the matrix. Thus, since those two rows are not linearly independent, the determinant of the matrix will always vanish. Similarly, if there are more than $n^2 - n$ zeroes, again by the pigeonhole principle, there will be at least one row made up of just zeroes and thus the determinant will always be zero. Finally, for $a \in \mathbb{F}$, the determinants of $\begin{pmatrix} a & a \\ -a & -a \end{pmatrix}$, $\begin{pmatrix} a & -a \\ -a & a \end{pmatrix}$ and $\begin{pmatrix} a & -a \\ a & -a \end{pmatrix}$ are all zero so if the elements are $\{a, a, -a, -a\}$, we cannot rearrange the elements such that the matrix is invertible. □

Remark 4.44. *Although we are talking about being able to construct invertible $n \times n$ matrices from n^2 elements in Theorem 4.20, Theorem 4.34 and Corollary 4.43, this is equivalent to saying matrices made up of those n^2 elements can be unlocked by all permutations.*

Remark 4.45. *Given n^2 elements in a field $\mathbb{F}$ which can be arranged into an invertible $n \times n$ matrix as in Corollary 4.43, the proofs of Theorem 4.34 and Theorem 4.20 in fact both give algorithms to find an invertible $n \times n$ matrix constructed from those elements when combined with Remark 4.8.*

Remark 4.46. *It is also nice to notice that Corollary 4.43 is a generalisation of Theorem 3.34 which we proved simply by using the Combinatorial Nullstellensatz.*

4.3 ...by rotations of its rows and columns?

We now consider rotations of both rows and columns of our matrix. Letting e_i denote the standard ith basis vector as before, let $c_i(M) \coloneqq (r_i(M^T))^T$ ie. a rotation of the ith column by 1 element. Then $c_i \in S_{n^2}$ and for $C \coloneqq \{c_i : i \in [n]\} \subseteq S_{n^2}$, then $\langle R, C\rangle \subseteq S_{n^2}$ is the set of all row and column rotations. We say M is unlocked by row and column rotations if $\exists\, \sigma \in \langle R, C\rangle$ such that $\det(\sigma(M)) \neq 0$.

Example 4.47. *Let's consider the matrix* $\gamma = \begin{pmatrix} 2 & -7 & 5 \\ -3 & -8 & 11 \\ 2 & 0 & -2 \end{pmatrix} \in M_3(\mathbb{C})$ *again. From Example 4.3 we know we won't get a non-zero determinant by rotating the rows, however, by rotating the first column, we get* $c_1(\gamma) = \begin{pmatrix} -3 & -7 & 5 \\ 2 & -8 & 11 \\ 2 & 0 & -2 \end{pmatrix}$ *which* $\det(c_1(\gamma)) = -150$. *Now consider* $\nu = \begin{pmatrix} -8 & 1 & 7 \\ 6 & 4 & 9 \\ 2 & -5 & 3 \end{pmatrix} \in M_3(\mathbb{F}_{19})$. *It is easy to see that* ν *is not unlocked by just rows or just columns ie.* $\det(\sigma(\nu)) = 0$ *for all* $\sigma \in \langle R\rangle \cup \langle C\rangle$ *since both the rows and columns add up to* 0. *However, if we rotate the first column down by one we have* $c_1^2(\nu) = \begin{pmatrix} 2 & 1 & 7 \\ -8 & 4 & 9 \\ 6 & -5 & 3 \end{pmatrix}$ *and then if we rotate the top row by one we get* $r_1^2 c_1^2(\nu) = \begin{pmatrix} 7 & 2 & 1 \\ -8 & 4 & 9 \\ 6 & -5 & 3 \end{pmatrix}$ *which has determinant* $1 \neq 0$.

We present a final original theorem, building on our work to which matrices are unlocked by all permutations.

Theorem 4.48. *For* $n \geq 3$, *given a matrix* $M \in M_n(\mathbb{F})$, *then* M *is unlocked by row and column rotations if and only if there are at most* $n^2 - n + 1$ *of the same element or at most* $n^2 - n$ *zeroes.*

As we can see, by comparing with Theorem 4.34, allowing rotations of both row and columns allows us as much freedom as rearranging the elements in any way we like. To see why, we need to briefly revisit some group theory of the symmetric groups S_n.

Lemma 4.49. *By rotating the rows and columns of a matrix* $M \in M_n(\mathbb{F})$, *we can cyclically permute any* n *elements of the matrix in any order leaving all other entries unchanged.*

Proof. Choose n elements in the matrix that we want to cyclically permute. We now want to manoeuvre all of these elements into the first row in the specified order just by using rotations of rows and columns. In the specified order that we want our elements to be cyclically permuted, we move one element at a time, making sure not to alter any of the elements already correctly placed in the first row. Say we have an element currently at (i, j) which we want to move to position $(1, k)$. If $i = 1$, then rotate the jth column by one position and let the element be at (i, j) where $i \neq 1$. Now rotate the ith row until the element is in column k and rotate the kth column until the element is in $(1, k)$. In this process, we do not alter the position of any element already placed correctly in the first row. By repeating this for all n elements we want to cyclically permute, we have a sequence of rotations which get us from our starting matrix M to the matrix with the elements we want to cyclically permute in the first row in the specified order. Now, we rotate the top row to cyclically permute the elements as specified and then perform the inverse of each rotation in our sequence in reverse order to get back to the starting matrix M now with those n elements cyclically permuted. Clearly this was done only using rotation of rows and columns since the inverse of a rotation is again a rotation. □

We will now need a standard result from group theory which we will not prove here, however, a proof can be found in Cook's lecture notes, [Coo10].

Lemma 4.50. *For $n \geq 5$, the only normal subgroups of S_n are $\{e\}, A_n$ and S_n.*

We now prove another group theory result utilising Lemma 4.50.

Lemma 4.51. *For $n \geq 3$,*

$$n\text{-cycles in } S_{n^2} \text{ generate } \begin{cases} A_{n^2} & \text{if } n \text{ is odd,} \\ S_{n^2} & \text{if } n \text{ is even.} \end{cases}$$

Proof. Since conjugacy classes in S_{n^2} are given by elements with the same cycle shape, the set of $n-$cycles form a full conjugacy class. Letting the subgroup generated by the $n-$cycles be denoted N, then N is normal in S_{n^2}. To see this, notice that for all $g \in S_{n^2}$,

$$g^{-1}Ng = g^{-1}\left\{\prod a : a \text{ is an } n-\text{cycle}\right\} g = \left\{\prod g^{-1}ag : a \text{ is an } n-\text{cycle}\right\} \subseteq N$$

since the $n-$cycles form a conjugacy class and thus $g^{-1}ag$ is again an $n-$cycle for any $g \in S_{n^2}$.

Now we use Lemma 4.50 and notice that for n odd, an $n-$cycle is an even permutation ie. has $\operatorname{sgn}(\sigma) = 1$, and since sgn is multiplicative, N will only contain elements $\sigma \in S_{n^2}$ with $\operatorname{sgn}(\sigma) = 1$ ie. even permutations. Thus, for n odd, $N \neq S_{n^2}$ as S_{n^2} contains odd permutations and N is clearly not the trivial subgroup then $N = A_{n^2}$. Similarly, for n even, $N \not\subseteq A_{n^2}$ since, for n even, an $n-$cycle is an odd permutation thus $N = S_{n^2}$. □

We will now prove Theorem 4.48 by using the fact that the n-cycles generate either A_{n^2} or S_{n^2} and then using Corollary 4.43.

Proof of Theorem 4.48. By Lemma 4.49, if we think of S_{n^2} acting on each of the elements in M, then the $n-$cycles given by rotations of the rows and columns generate all $n-$cycles in S_{n^2}. Now, combining this with Lemma 4.51, we have that for n even, we can apply any permutation to the elements of M just by rotating the rows and columns and for n odd, we can apply any even permutation to the elements of M just by rotating the rows and columns.

Now, the result follows for n even using Corollary 4.43, and we only have to work slightly harder for n odd. In this case, if we recall that, in the process of proving both Theorem 4.34 and Theorem 4.20, we proved that by swapping elements, we could rearrange M into a matrix with non-zero determinant. If this permutation is even, we are done since this permutation can be realised by rotating rows and columns. If this permutation is odd, we choose two rows and swap all pairs of elements in the same column between the rows. Since n is odd we are adding an odd number of transpositions to the odd permutation thus leaving us with an even permutation. Swapping two rows of a matrix multiplies the determinant by -1, thus, it stays non-zero, and since we applied an even permutation to get matrix into this form, we could also have got to this point by rotating rows and columns. □

Corollary 4.52. *For $n \in \mathbb{N}$, given a matrix $M \in M_n(\mathbb{F})$, then M is unlocked by row and column rotations if and only if there are at most $n^2 - n + 1$ of the same element, at most $n^2 - n$ zeroes and the elements are not $\{a, a, -a, -a\}$ for some $a \in \mathbb{F}$.*

Proof. Again, the $n = 1$ case is trivial and $n \geq 3$ is given by Theorem 4.48. Extending to the case $n = 2$, the normal subgroups of S_4 are given by $\{e\}, V_4, A_4, S_4$ where $V_4 \subseteq A_4$ so since a $2-$cycle is an odd permutation and using the fact that the rotations of rows and columns generates a normal subgroup, then any permutation of the elements of a 2×2 matrix can be generated by rotations of the rows and columns. The result now follows using Corollary 4.43. □

4.4 Polynomials that Vanish on Distinct Roots of Unity

The polynomial ideal $\mathcal{J}(n)$, defined in Definition 4.53, is the subject of Kézdy and Snevily's paper titled *Polynomials that Vanish on Distinct Roots of Unity*, [KS04], where amongst other things, they give a Gröbner basis for the ideal and use Gröbner basis methods to give a characterisation of the ideal based on the Combinatorial Nullstellensatz. In Section 4, titled 'Further Examples', they even state the connection between bipartite graphs and determinants of rotations of matrices (albeit in different terms which we show are equivalent below). Since Kézdy was Brauch's PhD advisor, it is likely [KS04] was the inspiration for the paper [BKS14], which itself was the inspiration for this Chapter.

Definition 4.53. *Let $\mathcal{J}(n)$ be an ideal in $\mathbb{C}[x_1, ..., x_n]$, where $g \in \mathcal{J}(n) \Leftrightarrow g(x) = 0$ for all $x \in \mu_n^n$ with distinct components ie. $x_i \neq x_j$ for $i \neq j$.*

Remark 4.54. *It is easy to see that for $g \in \mathbb{C}[x_1, ..., x_n]$, let $f(x) \coloneqq g(x)(\det V_n)(x)$, then, $g \in \mathcal{J}(n)$ $\Leftrightarrow \mu_n^n \subseteq Z(f)$ ie. $f(x) = 0$ for all $x \in \mu_n^n$. Combining the above with Lemma 4.14 we get $g \in \mathcal{J}(n)$ $\Leftrightarrow (\det V_n)g \in \langle x_i^n - 1 : i \in [n] \rangle$. This is given as a Remark on p.54 of [KS04] and should make the definition of $f_M(x)$ in Definition 4.4 slightly less arbitrary.*

The main result of [KS04], given in Theorem 4.56, gives an exact condition on the coefficients of polynomials in $\mathcal{J}(n)$. Note that the notation in the following definition and Theorem has been slightly altered from the original in [KS04].

Definition 4.55. *To each $\alpha \in \mathbb{N}_0^n$, associate a function $\pi_\alpha : [n] \to [n], i \mapsto \alpha_i + 1 \pmod n$. Then define the following set of n-tuples,*

$$\Lambda \coloneqq \{\alpha \in \mathbb{N}_0^n : \pi_\alpha \in S_n\}.$$

Theorem 4.56. *For $f \in \mathbb{C}[x_1, ..., x_n]$ where $f(x) = \sum_{\alpha \in \mathbb{N}_0^n} c_\alpha x^\alpha$, then $f \notin \mathcal{J}(n)$ if and only if there exists some $\beta \in \mathbb{N}_0^n$ satisfying $\beta_i \leq n - i$ for all $i \in [n]$ such that*

$$\sum_{\alpha+\beta \in \Lambda} c_\alpha \operatorname{sgn}(\pi_{\alpha+\beta}) \neq 0$$

The proof of Theorem 4.56 given in [KS04] is very long and we will not prove it here. However, while Theorem 4.56 has a fairly complicated condition on the membership of $f \in \mathcal{J}(n)$, when f is separable with coefficients that can be displayed in an $n \times n$ matrix, it reduces to a much more manageable condition and one which we have seen before.

Corollary 4.57. *For $g \in \mathbb{C}[x_1, ..., x_n]$ separable, assume $g(x) = \sum_{\alpha \in \mathbb{N}_0^n} c_\alpha x^\alpha = \prod_{i \in [n]} g_i(x_i)$ where $g_i \in \mathbb{C}[x_i]$ and $\deg(g_i) \leq n - 1$ for all $i \in [n]$. Furthermore, we can define a matrix $M \in M_n(\mathbb{C})$, by letting $g_i(x_i) = \sum_{j \in [n]} M_{i\,j} x_i^{j-1}$ for $j \in [n]$. Then $g \notin \mathcal{J}(n)$ if and only if M can be unlocked by row rotations.*

The key realisation here is that, by definition of M, for $\alpha \in \{0, ..., n-1\}^n$, then $c_\alpha = \prod_{i \in [n]} M_{i\,(\alpha_i+1)}$ otherwise $c_\alpha = 0$. Thus, using the substitution $\sigma = \pi_{\alpha+\beta}$ implying $\sigma(i) = \alpha_i + \beta_i + 1$, then

$$\sum_{\alpha+\beta \in \Lambda} c_\alpha \operatorname{sgn}(\pi_{\alpha+\beta}) = \sum_{\substack{\alpha \in \{0,...,n-1\}^n \\ \pi_{\alpha+\beta} \in S_n}} \operatorname{sgn}(\pi_{\alpha+\beta}) \prod_{i=1}^n M_{i\,(\alpha_i+1)} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n M_{i\,(\sigma(i)-\beta_i)}$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n M[-\beta]_{i\,\sigma(i)} = \det(M[-\beta]).$$

Combining Corollary 4.57 with Remark 4.54 and Definition 4.4, we have proved Corollary 4.7 again, but only for the special case $\mathbb{F} = \mathbb{C}$! In some sense then, taking $\beta = 0$, we can view $\sum_{\alpha\in\Lambda} c_\alpha \operatorname{sgn}(\pi_\alpha)$ as the generalisation of the determinant of a matrix to the 'determinant' of a polynomial. Then, the existence of a $\beta \in \mathbb{N}_0^n$ such that $\sum_{\alpha+\beta\in\Lambda} c_\alpha \operatorname{sgn}(\pi_{\alpha+\beta}) \neq 0$ would generalise the notion of a matrix being able to be unlocked by row rotations.

[KS04] applies Theorem 4.56 to give equivalent statements for the existence of a number of mathematical objects, including permutation polynomials, Latin transversals and Hamiltonian cycles in graphs as well as bipartite graphs. However, we will not cover these applications here.

4.5 Further Directions for Research

We conclude this chapter by discussing 3 further directions that research could be taken in, based off of the original material in this report.

- In Chapter 4, we gave exact conditions on when matrices could be unlocked by $\langle R\rangle$ (row rotations), $\langle R, C\rangle$ (row and column rotations) and S_{n^2} (all permutations) where we circumvented the proof for row and column rotations by proving that $\langle R, C\rangle$ was equal to either A_{n^2} or S_{n^2} depending on the parity of n and then appropriating our proof for all permutations. An obvious route for further research would be to give conditions on when matrices can be unlocked by other subsets of S_{n^2}. We assume that taking subsets such as $\langle R\rangle$ with nice properties will give nicer results.

- In [BKS14], for matrices M, constructed directly from bipartite graphs, a formula is given for the number of row rotations that unlock the matrix, given by $\operatorname{supp}(\hat{f}_M)$ where $\hat{f}_M$ is the discrete Fourier transform of f_M. An investigation into whether a similar formula could be given for any matrix M would likely be successful. However, trying to find formulae for the number of elements of other subsets of S_{n^2} that the matrix is unlocked by seems fruitless based on the slightly arduous proof of even one of these elements existing.

- It is interesting to note that, denoting K_n the complete graph on n nodes and V_n the Vandermonde matrix, $\det V_n = f_{K_n}$ where f_G is the graph polynomial for graph G, from Definition 3.38. Thus, for a graph $G = ([n], E(G))$, we could define the ideal $\mathcal{J}_G(n)$ where $g \in \mathcal{J}(n) \Leftrightarrow f_G g \in \langle x_i^n - 1 : i \in [n]\rangle$. Then, by Remark 4.54, $\mathcal{J}_{K_n}(n) = \mathcal{J}(n)$. $\mathcal{J}_G(n)$ would then have the property that $g \in \mathcal{J}(n) \Leftrightarrow g(x) = 0$ for all $x \in \mu_n^n$ where $x_i \neq x_j$ if $(i, j) \in E(G)$.
  Taking this idea a step further, for a hypergraph $H = ([n], E(H))$, using the definition of a hypergraph polynomial g_H from Definition 3.41, we could define ideals $\mathcal{J}_H(n)$ where $h \in \mathcal{J}(n) \Leftrightarrow g_H h \in \langle x_i^n - 1 : i \in [n]\rangle \Leftrightarrow h(x) = 0$ for all $x \in \mu_n^n$ where $|\{x_i : i \in e\}| \neq 1, \forall\, e \in E(H)$.
  Gröbner bases for these ideals could likely be found by hand and could certainly be computed. Perhaps even exact conditions on membership of these ideals such as in Theorem 4.56 could be constructed. One application, similar to those of [KS04], that could be established is the following. Let $G = (V, E)$ be the bipartite graph where $V = ([n], \mu_n)$, and ω is a primitive nth root of unity. Then define a polynomial $g \in \mathbb{C}[x_1, ..., x_n]$ where $\prod_{(i,\omega^j)\notin E(G)}(x_i - \omega^j)$. By Remark 4.54 and Lemma 4.16, we have that G has a perfect matching $\Leftrightarrow g \notin \mathcal{J}(n)$. Now let $H_{(n,3)}$ denote the hypergraph on n nodes where $E(H_{(n,3)})$ contains every possible hyperedge of size 3 and no others. Then G contains a matching where we allow at most two nodes in $[n]$ to connect to the same node in $\mu_n \Leftrightarrow g \notin \mathcal{J}_{H_{(n,3)}}(n)$.

Conclusion

In the first half of this report, we covered some of the main results that the polynomial method has to offer in the area of extremal combinatorics, including the Finite Field Kakeya Conjecture, one case of the Erdős-Szemerédi sunflower conjecture, the cap set bound, the Cauchy-Davenport inequality and the Erdős-Heilbronn conjecture. However, upon seeing these results pop out after defining just a single key polynomial (or 3-tensor), it is often easy to overlook the strength of the results being proved. To this end, studying alternate proofs of results, where these exist, such as in the case of the bound on the size of s-distance sets or the Cauchy-Davenport inequality, gives us a sense of just how intractable these problems seem before we apply a polynomial method and the answer falls out.

In this way, we can see the polynomial method as a double-edged sword; it can provide almost instantaneous results for some hard problems, however, it is difficult to ever guarantee that the polynomial method will work on a given problem. For example, in the concluding remarks of Alon's groundbreaking paper, [Alo99], he raises the possibility that the polynomial method may be the key in the study of the Four Colour Theorem. With the recent non-constructive proof of the Four Colour Theorem by Jackson and Richmond in [JR23], perhaps Alon's proposal might not be as far away from reality as we thought. However, until the right polynomial method is unearthed, it is hard to know.

On the other hand, in Tao's comment from 2010 on `mathoverflow.net`, [Tao10], he rightly predicts that the polynomial method may be useful in resolving the cap set problem, a task which Ellenberg and Gijswijt were able to accomplish in 2016 in [EG16]. In the preface to [Tao14], Tao conjectures that there might be opportunities to use deeper results from algebraic geometry and algebraic topology alongside polynomial methods and, based on Tao's expert intuition in the subject, this seems likely. However, we can only hope for an approach for deciding if a given problem is susceptible to the polynomial method.

In the latter half of the report, we proved a number of original existence statements using the Combinatorial Nullstellensatz, and demonstrated how we can wrap up information about the sets on which polynomials vanish into statements about polynomial ideals. We then applied these ideas in Chapter 4, inspired by a result from [BKS14], to questions about determinants of matrices. To prove our main result, the exact conditions on when a matrix can be unlocked by all permutations, we required the new notions of clusters, minimal clusters and cluster density, as well as a number of technical lemmas and fair amount of setup in the final proof. It is not unimaginable that there is a polynomial method from which this result falls out. However, the single counter example given by the set $\{a, a, -a, -a\}$ not included in the other conditions for a matrix not to be unlockable seems to imply that there will always be some degree of complexity and setup required for the proof, to allow for this case.

Finally, to put our methods in context, we briefly covered Kézdy and Snevily's paper [KS04] and discussed taking combinatorial problems and providing equivalent statements in terms of polynomial ideals. This notion is generalised in [De +11], where they define a problem as feasible if it has an equivalent statement in terms of zeroes of polynomials, although their main focus is computational rather than theoretical.

Appendix A

Perfect Matchings and Disjoint Cycle Covers

In this section, we state and prove Theorem 1.19, now given as Theorem A.2, which gives a condition on when a graph has a perfect matching. We then introduce the closely-related notion of a directed graph having a disjoint cycle cover and prove an analogue of Theorem A.2 in this case by introducing the Edmonds matrix.

Before we discuss Theorem A.2, we state the Leibniz formula which will be needed in the proof.

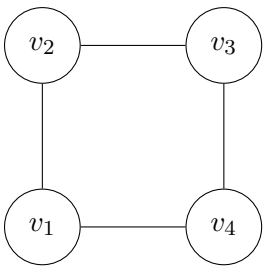
Lemma A.1 (Leibniz determinant formula)**.** *Given an $n \times n$ matrix A with entries $A_{i\,j}$, we have*

$$det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} A_{i\,\sigma(i)}$$

where S_n is the set of permutations of $[n]$ and for $\sigma \in S_n$, $\operatorname{sgn}(\sigma) = (-1)^{N_\sigma}$, where N_σ is the number of transpositions in the decomposition of σ.

We now restate the Theorem by Tutte from [Tut47] and provide an example before giving a proof from Williams' lecture notes, [Wil21].

Theorem A.2 (Theorem 1.19)**.** *A graph G contains a perfect matching if and only if the Tutte matrix of G has non-zero determinant.*



$$A = \begin{pmatrix} 0 & x_{12} & 0 & x_{14} \\ -x_{12} & 0 & x_{23} & 0 \\ 0 & -x_{23} & 0 & x_{34} \\ -x_{14} & 0 & -x_{34} & 0 \end{pmatrix}$$

Figure A.1: The graph S and the corresponding Tutte matrix A as in Example A.3.

Example A.3. *Let S be the graph with vertices $V(S) = \{v_1, v_2, v_3, v_4\}$ on the perimeter of a square and edges between adjacent vertices as shown, along with the corresponding Tutte matrix A, in Figure*

A.1. We have $\det(A) = x_{12}^2x_{34}^2 + x_{14}^2x_{23}^2 + 2x_{12}x_{23}x_{34}x_{14}$ *which is clearly not the zero polynomial and indeed there are two perfect matchings on* S *given by* $\{(v_1, v_2), (v_3, v_4)\}$ *and* $\{(v_1, v_4), (v_2, v_3)\}$.

It is interesting to note that rewriting this determinant as $\det(A) = x_{12}x_{21}x_{34}x_{43} + x_{14}x_{41}x_{23}x_{32} - 2x_{12}x_{23}x_{34}x_{41}$ *gives combinations of groupings of paths of even length starting and ending at the same vertex. It becomes clear in the proof of Theorem 1.19 that this is true in general for the determinant of any Tutte matrix as the non-zero terms in the Leibniz determinant formula come from permutations with only even cycles.*

Proof. For the $\Rightarrow$ statement of the theorem, it suffices to show $\det(A)$ is not the zero polynomial. So, given a perfect matching of a graph G, plug in $x_{ij} = 1$ if v_i and v_j are matched in the perfect matching and $x_{ij} = 0$ otherwise. Then, there will be only one non-zero entry in every row and column of A, since every vertex connects to exactly one edge. Thus $\det(A)$ is non-zero.

For $\Leftarrow$, we let P be the set of permutations in S_n containing at least one odd cycle. Then we can construct a map $\phi : P \to P$ where, for $\sigma \in P$ written in terms of disjoint cycles, ϕ reverses the odd cycle in σ which contains the minimum element of any odd cycle ie. for $\sigma = \tau\sigma'$ where τ is the odd cycle containing the minimum element of any odd cycle, $\phi(\sigma) = \tau^{-1}\sigma'$. Clearly $\phi^2 = \mathrm{Id}_P$, so ϕ is a bijection. Now, we consider the terms in the Leibniz determinant formula, Lemma A.1, corresponding to σ and $\phi(\sigma)$ for some $\sigma \in P$, letting $\sigma = \tau\sigma'$ as before.

$$\begin{aligned}
&\operatorname{sgn}(\sigma)\prod_{i=1}^{n} A_{i\,\sigma(i)} + \operatorname{sgn}(\phi(\sigma))\prod_{i=1}^{n} A_{i\,\phi(\sigma(i))} = \operatorname{sgn}(\sigma)\prod_{i=1}^{n} A_{i\,\tau\sigma'(i)} + \operatorname{sgn}(\sigma)\prod_{i=1}^{n} A_{i\,\tau^{-1}\sigma'(i)} \\
&= \operatorname{sgn}(\sigma)\prod_{i\in\sigma'} A_{i\,\sigma'(i)}\left(\prod_{i\in\tau} A_{i\,\tau(i)} + \prod_{i\in\tau} A_{i\,\tau^{-1}(i)}\right) = \operatorname{sgn}(\sigma)\prod_{i\in\sigma'} A_{i\,\sigma'(i)}\left(\prod_{i\in\tau} A_{i\,\tau(i)} + \prod_{i\in\tau} A_{\tau(i)\,i}\right) \\
&= \operatorname{sgn}(\sigma)\prod_{i\in\sigma'} A_{i\,\sigma'(i)}\left(\prod_{i\in\tau} A_{i\,\tau(i)} + (-1)^{|\tau|}\prod_{i\in\tau} A_{i\,\tau(i)}\right) = 0
\end{aligned}$$

using the fact that $|\tau|$ is odd, $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\phi(\sigma))$ and A is skew-symmetric so $A_{ij} = -A_{ji}$. In doing so, we have shown that every permutation $\sigma \in S_n$ containing an odd cycle will cancel out with the corresponding σ' in the determinant formula. Now we use the fact that $\det(A)$ is non-zero which implies that there exists at least one $\sigma \in S_n$ with only even cycles such that the coefficient of $\prod_{i=1}^{2n} A_{i\,\sigma(i)}$ is non-zero in $\det(A)$. Writing this σ as a product of disjoint even cycles, we can match consecutive elements from the same cycle in pairs ie. $(v_i, v_{\sigma(i)})$, giving a perfect matching of the graph G. This is indeed a perfect matching as, if any pairs of vertices $(v_i, v_{\sigma(i)})$ didn't share an edge in our matching, then $x_{i\sigma(i)} = 0$ and thus the coefficient of $\prod_{i=1}^{n} A_{i\,\sigma(i)}$ is zero in $\det(A)$ which is a contradiction. □

We will now extend the notion of a perfect matching to a disjoint cycle cover as well as generalising the notion of a graph to a directed graph.

Definition A.4. *A directed graph* $G = (V(G), E(G))$ *is a set of vertices where edges between vertices are ordered pairs ie. for vertices* $v, w \in V(G)$, (v, w) *may be an edge but* (w, v) *may not be. We draw directed graphs with arrows going from the first vertex in the ordered pair to the second.*

A cyclic sub-graph of a directed graph is a subset of the vertices that can be written in a permutation σ *such that* $(v, \sigma(v)) \in V(G)$.

Example A.5. *Graph* C *does not have a cyclic sub-graph, whereas graph* D *has* 4 *cyclic sub-graphs with vertices* $\{1, 2, 3\}, \{1, 3, 4\}, \{1, 2, 3, 4\}$ *and* $\{1, 3\}$. *Both graphs are visualised in Figure A.2.*

Figure A.2: We visualise graphs C and D from Example A.5.

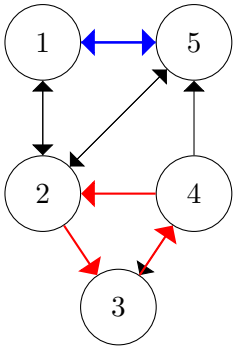
Definition A.6. *A disjoint cycle cover of a directed graph G is a set of cyclic sub-graphs of G which cover all vertices of G whilst having no vertices in common.*

From [MR95], we introduce the notion of the Edmonds matrix.

Definition A.7. *Given a directed graph G with vertices $V(G) = \{v_i\}_{i\in\{1,\dots,n\}}$, we define a very similar matrix to the Tutte matrix called the Edmonds matrix, $\hat{A} \in M_n(\mathbb{Z}[x_{ij}])$ for $i, j \in [n]$ given by:*

$$\hat{G}_{i\,j} = \begin{cases} x_{ij} & \text{if } (v_i, v_j) \in E(G), \\ 0 & \text{otherwise.} \end{cases}$$

Example A.8. *Let H be the the graph shown in Figure A.3, then H has two disjoint cycle covers. The determinant of the corresponding Edmonds matrix is $\det(\hat{G}) = x_{12}x_{23}x_{34}x_{45}x_{51} - x_{15}x_{52}x_{21}x_{34}x_{43} - x_{15}x_{51}x_{23}x_{34}x_{42} - x_{12}x_{25}x_{51}x_{34}x_{43}$. Whereas the determinant of the Tutte polynomial had terms with non-zero coefficients that didn't correspond to perfect matchings, we now see that terms in the determinant of our new matrix $\hat{A}$ with non-zero coefficients mark out precisely the disjoint cycle covers.*



$$\begin{pmatrix} 0 & x_{12} & 0 & x_{14} & x_{15} \\ x_{21} & 0 & x_{23} & 0 & x_{25} \\ 0 & 0 & 0 & x_{34} & 0 \\ 0 & x_{42} & x_{43} & 0 & x_{45} \\ x_{51} & x_{52} & 0 & 0 & 0 \end{pmatrix}$$

Figure A.3: We visualise a graph H and its corresponding Edmonds matrix. The two components of a disjoint cycle cover of H are highlighted in red and blue.

Definition A.9. *For a directed graph G, define the corresponding bipartite graph B_G where we define B_G to have vertices $V(B_G) = (V(G), V(G))$ and edges $(v, w) \in E(B_G) \Leftrightarrow (v, w) \in E(G)$ for all vertices $v, w \in V(G)$*

Lemma A.10. *There is a bijection between directed graphs and bipartite graphs. In addition, for a directed graph G and corresponding bipartite graph B_G, G has a disjoint cycle cover $\Leftrightarrow$ B_G has a perfect matching.*

Proof. The bijection can be given by $G \leftrightarrow B_G$ for G a directed graph and B_G defined in Definition A.9. Furthermore, G having a disjoint cycle cover is equivalent to having a permutation σ of the elements of G such that $(v, \sigma(v)) \in E(G)$ for all vertices $v \in V(G)$. By the definition of B_G and the fact σ is a permutation, this is equivalent to having a perfect matching on B_H made up of edges $(v, \sigma(v)) \in E(B_G)$. □

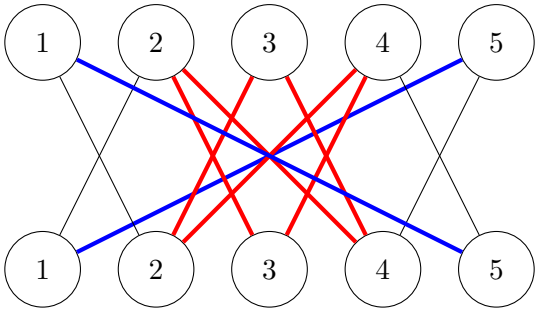


Figure A.4: We construct the corresponding bipartite graph B_H for graph H from Example A.8. Corresponding components to those of the disjoint cycle cover depicted in Figure A.3 are coloured.

Now we can give the analogue to Theorem A.2, this time on when directed graphs have disjoint cycle covers.

Theorem A.11. *A directed graph G has a disjoint cycle cover* $\Leftrightarrow \det(\hat{G}) \neq 0$.

Proof. Given the corresponding bipartite graph B_G of G, we can write the Tutte matrix of B_G as $A = \begin{pmatrix} 0_n & \hat{G} \\ -\hat{G}^T & 0_n \end{pmatrix}$ where 0_n is the $n \times n$ matrix of zeroes. Now using properties of determinants, $\det(A) = (\det(\hat{G}))^2$, thus by Theorem 1.19, $\det(\hat{G}) \neq 0 \Leftrightarrow B_G$ has a perfect matching. Finally, using Lemma A.10, the result follows. □

Definition A.12. *For matrix $M \in M_n(\mathbb{F})$, the permanent of M is defined as*

$$\operatorname{perm}(M) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} M_{i\,\sigma(i)}$$

It is worth remarking that that the permanent of the matrix is just the determinant without the multiplication by $sgn(\sigma)$ of each term.

Remark A.13. *Given a directed graph G,* $\operatorname{perm}(G)$ *evaluated at* 1 *on all variables x_{ij} for $i, j \in [n]$ gives the number of disjoint cycle covers of G.*

This result is used in [BH93] to prove the fact that computing the permanent of a matrix is #P-complete.

Bibliography

[Ale19] Yulia Alexandr. *Combinatorial Nullstellensatz: Various Proofs, Extensions and Applications.* 2019. DOI: 10.13140/RG.2.2.33259.57129.

[AT89] N. Alon and M. Tarsi. "A nowhere-zero point in linear mappings". In: *Combinatorica* 9 (4 1989), pp. 393–395. DOI: 10.1007/BF02125351.

[AT93] N. Alon and M. Tarsi. "Colorings and orientations of graphs". In: *Combinatorica* 12.2 (1993), pp. 125–134. DOI: 10.1007/BF01204715.

[Alo99] Noga Alon. "Combinatorial Nullstellensatz". In: *Combinatorics, Probability and Computing* 8.1-2 (1999), pp. 7–29. DOI: 10.1017/S0963548398003411.

[ANR95] Noga Alon, Melvyn B. Nathanson, and Imre Ruzsa. "Adding Distinct Congruence Classes Modulo a Prime". In: *The American Mathematical Monthly* 102.3 (1995), pp. 250–255. DOI: 10.2307/2975012.

[ANR96] Noga Alon, Melvyn B. Nathanson, and Imre Ruzsa. "The Polynomial Method and Restricted Sums of Congruence Classes". In: *Journal of Number Theory* 56.2 (1996), pp. 404–417. DOI: 10.1006/jnth.1996.0029.

[Alw+20] Ryan Alweiss et al. "Improved bounds for the sunflower lemma". In: *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*. Association for Computing Machinery, 2020, pp. 624–630. ISBN: 9781450369794. DOI: 10.1145/3357713.3384234.

[Ars11] Bodan Arsovski. "A proof of Snevily's Conjecture". In: *Israel Journal of Mathematics* 182.1 (2011), pp. 505–508. DOI: 10.1007/s11856-011-0040-6.

[Aus16] David Austin. *Game. SET. Polynomial.* 2016. URL: https://www.ams.org/publicoutreach/feature-column/fc-2016-08.

[BF22] László Babai and Péter Frankl. *Linear algebra methods in combinatorics.* 2022. URL: https://people.cs.uchicago.edu/~laci/babai-frankl-book2022.pdf.

[BBS83] Eiichi Bannai, Etsuko Bannai, and Dennis Stanton. "An upper bound for the cardinality of an s-distance subset in real euclidean space, II". In: *Combinatorica* 3 (1983), pp. 147–152. DOI: 10.1007/BF02579288.

[BH93] Amir Ben-Dor and Shai Halevi. "Zero-one permanent is #P-complete, a simpler proof". In: *Proceedings of the 2nd Israel Symposium on the Theory and Computing Systems* (1993), pp. 108–117. DOI: 10.1109/ISTCS.1993.253457.

[Bes19] Abram Besicovitch. "Sur deux questions d'integrabilite des fonctions". In: *J. Soc. Phys. Math.* 2 (1919), pp. 105–123.

[Bla+17] Jonah Blasiak et al. "On cap sets and the group-theoretic approach to matrix multiplication". In: *Discrete Analysis* (2017). DOI: 10.19086/da.1245.

[Blo84] A. Blokhuis. "A New Upper Bound for The Cardinality of 2-Distance Sets in Euclidean Space". In: *Annals of Discrete Mathematics (20): Convexity and Graph Theory*. Vol. 87. North-Holland Mathematics Studies. 1984, pp. 65–66. DOI: doi.org/10.1016/S0304-0208(08)72809-3.

[BM08] Aart Blokhuis and Francesco Mazzocca. "The Finite Field Kakeya Problem". In: *Building Bridges: Between Mathematics and Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 205–218. DOI: 10.1007/978-3-540-85221-6_6.

[BKS14] Timothy Brauch, André Kézdy, and Hunter Snevily. "The Combinatorial Nullstellensatz and DFT on Perfect Matchings in Bipartite Graphs". In: *Ars Combinatoria* 114 (2014), pp. 461–475.

[Bri11] David Brink. "Chevalley's theorem with restricted variables". In: *Combinatorica* 31 (1 2011), pp. 127–130. DOI: 10.1007/s00493-011-2504-z.

[Bru92] A. A. Bruen. "Polynomial multiplicities over finite fields and intersection sets". In: *Journal of Combinatorial Theory, Series A* 60.1 (1992), pp. 19–33. DOI: 10.1016/0097-3165(92)90035-S.

[CF94] A. R. Calderbank and P. C. Fishburn. "Maximal three-independent subsets of $0, 1, 2^n$". In: *Designs, Codes and Cryptography* 4.4 (1994), pp. 203–211. DOI: 10.1007/BF01388452.

[Cau13] A. L. Cauchy. "Recherches sur les nombres". In: *J. École Polytech* 9 (1813), pp. 99–116.

[Cha05] Mei-Chu Chang. "A sum-product estimate in algebraic division algebras". In: *Israel Journal of Mathematics* 150 (2005), pp. 369–380. DOI: 10.1007/BF02762388.

[Cla09] Pete L. Clark. *Number Theory: A Contemporary Introduction*. 2009. URL: http://www.math.uga.edu/~pete/4400FULL.pdf.

[Coo10] Bill Cook. *A_n is simple*. 2010. URL: https://www.billcookmath.com/courses/math4720-fall2010/math4720-fall2010-An_is_simple.pdf.

[CLP17] Ernie Croot, Vsevolod Lev, and Péter Pach. "Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small". In: *Annals of Mathematics* 185.1 (2017), pp. 331–337. DOI: 10.4007/annals.2017.185.1.7.

[CM96] Thomas W Cusick and Peter Müller. "Wan's bound for value sets of polynomials". In: *Finite Fields and Applications*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1996, pp. 69–72.

[DH94] J. A. Dias Da Silva and Y. O. Hamidoune. "Cyclic Spaces for Grassmann Derivatives and Additive Theory". In: *Bulletin of the London Mathematical Society* 26.2 (1994), pp. 140–146. DOI: 10.1112/blms/26.2.140.

[Das+01] Samit Dasgupta et al. "Transversals of additive Latin squares". In: *Israel Journal of Mathematics* 126 (Dec. 2001), pp. 17–28. DOI: 10.1007/BF02784149.

[Dav35] H. Davenport. "On the Addition of Residue Classes". In: *Journal of the London Mathematical Society* s1-10.1 (1935), pp. 30–32. DOI: 10.1112/jlms/s1-10.37.30.

[DM03] B. L. Davis and D. Maclagan. "The card game SET". In: *The Mathematical Intelligencer* 25.3 (2003), pp. 33–40. DOI: 10.1007/BF02984846.

[De +11] Jesús A. De Loera et al. “Computing infeasibility certificates for combinatorial problems through Hilbert’s Nullstellensatz”. In: *Journal of Symbolic Computation* 46.11 (2011), pp. 1260–1283. DOI: 10.1016/j.jsc.2011.08.007.

[DeV] M. DeVos. *Graph Theory*. URL: https://www.sfu.ca/~mdevos/notes/graph/345_matchings.pdf.

[Dvi08] Zeev Dvir. “On the size of Kakeya sets in finite fields”. In: *Journal of the American Mathematical Society* 22.4 (2008), pp. 1093–1097. DOI: 10.1090/s0894-0347-08-00607-3.

[Dvi+13] Zeev Dvir et al. “Extensions to the Method of Multiplicities, with Applications to Kakeya Sets and Mergers”. In: *SIAM Journal on Computing* 42.6 (2013), pp. 2305–2328. DOI: 10.1137/100783704.

[Ede+02] Y. Edel et al. “The Classification of the Largest Caps in AG(5, 3)”. In: *Journal of Combinatorial Theory, Series A* 99.1 (2002), pp. 95–110. DOI: 10.1006/jcta.2002.3261.

[ES66] Sheldon J Einhorn and IJ Schoenberg. “On Euclidean sets having only two distances between points II”. In: *Nederl. Akad. Wetensch. Proc. Ser. A*. Vol. 69. 1966, pp. 479–488.

[Eld12] Sam Elder. *The Kakeya Problem*. 2012. URL: https://math.mit.edu/~lguth/PolyMethod/lect33.pdf.

[EG16] Jordan Ellenberg and Dion Gijswijt. “On large subsets of F_q^n with no three-term arithmetic progression”. In: *Annals of Mathematics* 185 (2016). DOI: 10.4007/annals.2017.185.1.8.

[ES78] P Erdös and E Szemerédi. “Combinatorial properties of systems of sets”. In: *Journal of Combinatorial Theory, Series A* 24.3 (1978), pp. 308–313. DOI: 10.1016/0097-3165(78)90060-2.

[ER60] P. Erdős and R. Rado. “Intersection Theorems for Systems of Sets”. In: *Journal of the London Mathematical Society* s1-35.1 (1960), pp. 85–90. DOI: 10.1112/jlms/s1-35.1.85.

[EF96] Paul Erdős and Peter Fishburn. “Maximum planar sets that determine k distances”. In: *Discrete Math.* 160.1–3 (1996), pp. 115–125. DOI: 10.1016/0012-365X(95)00153-N.

[Fab07] XWC Faber. “On the finite field Kakeya problem in two dimensions”. In: *Journal of Number Theory* 124.1 (2007), pp. 248–257. DOI: 10.48550/arXiv.math/0510356.

[FW81] P. Frankl and R. M. Wilson. “Intersection theorems with geometric consequences”. In: *Combinatorica* 1.4 (1981), pp. 357–368. DOI: 10.1007/BF02579457.

[Goo70] I. J. Good. “Short Proof of a Conjecture by Dyson”. In: *Journal of Mathematical Physics* 11.6 (1970), pp. 1884–1884. DOI: 10.1063/1.1665339.

[Gtg09] Gtgith. *A Kakeya needle set constructed from Perron trees*. 2009. URL: https://en.wikipedia.org/wiki/Kakeya_set#/media/File:KakeyaNeedleSet3.GIF.

[Gut16] Larry Guth. *Polynomial Methods in Combinatorics*. Vol. 64. University Lecture Series. American Mathematical Society, 2016. ISBN: 978-1-4704-2890-7.

[GK10] Larry Guth and Nets Hawk Katz. “Algebraic methods in discrete analogs of the Kakeya problem”. In: *Advances in Mathematics* 225.5 (2010), pp. 2828–2839. DOI: 10.1016/j.aim.2010.05.015.

[GK15] Larry Guth and Nets Hawk Katz. “On the Erdős distinct distances problem in the plane”. In: *Annals of Mathematics* 181.1 (2015), pp. 155–190. DOI: 10.4007/annals.2015.181.1.2.

[Hal86] Marshall Jr. Hall. "Combinatorial Theory". In: *New York: John Wiley and Sons* (1986).

[HP93] Heiko Harborth and Lothar Piepmeyer. "Two-Distance Sets and the Golden Ratio". In: *Applications of Fibonacci Numbers*. Springer Netherlands, 1993, pp. 279–288. DOI: 10.1007/978-94-011-2058-6_27.

[Hir07] Jonathan Hirata. *Notes on Matching*. 2007. URL: https://math.mit.edu/~djk/18.310/Lecture-Notes/MatchingProblem.pdf.

[JR23] D. M. Jackson and L. B. Richmond. "A non-constructive proof of the Four Colour Theorem". In: *arXiv e-prints* (2023). DOI: 10.48550/arXiv.2212.09835.

[Juk11] S. Jukna. *Extremal Combinatorics - With Applications in Computer Science*. 2011. ISBN: 978-3-642-17364-6. DOI: 10.1007/978-3-642-17364-6.

[Kel47] L. Kelly. "Elementary problems and solutions. isosceles n-points". In: *Amer. Math. Monthly* 54 (1947), pp. 227–229.

[KS04] André Kézdy and Hunter Snevily. "Polynomials that Vanish on Distinct nth Roots of Unity." In: *Combinatorics, Probability and Computing* 13 (2004), pp. 37–59. DOI: 10.1017/S0963548303005923.

[Knu] Donald Knuth. *The programs setset, setset-all, and setset-random*. URL: https://www-cs-faculty.stanford.edu/~knuth/programs.html.

[Lis97] Petr Lisoněk. "New maximal two-distance sets". In: *journal of combinatorial theory, Series A* 77.2 (1997), pp. 318–338.

[Mar21] Thomas C. Martinez. *The Slice Rank Polynomial Method*. 2021. URL: https://scholarship.claremont.edu/hmc_theses/245.

[Mic10] Mateusz Michałek. "A short proof of Combinatorial Nullstellensatz". In: *The American Mathematical Monthly* 117.9 (2010), pp. 821–823. DOI: 10.4169/amermathmont.117.9.0821.

[Mos61] W. Moser. "Solution to problem 10". In: *Can. Math. Bull.* 4 (1961), pp. 187–189. DOI: 10.1017/S0008439500025753.

[Mos10] Dana Moshkovitz. "An Alternative Proof of The Schwartz-Zippel Lemma". In: *Electron. Colloquium Comput. Complex.* TR10 (2010). URL: https://api.semanticscholar.org/CorpusID:36035668.

[MR95] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge International Series on Parallel Computation. Cambridge University Press, 1995. ISBN: 9780521474658. URL: https://books.google.co.uk/books?id=QKVY4mDivBEC.

[Mül05] Peter Müller. "Permutation groups of prime degree, a quick proof of Burnside's theorem". In: *Archiv der Mathematik* 85.1 (2005), pp. 15–17. DOI: 10.1007/s00013-005-1421-z.

[Mus09] Oleg R. Musin. "Spherical two-distance sets". In: *Journal of Combinatorial Theory, Series A* 116.4 (2009), pp. 988–995. DOI: https://doi.org/10.1016/j.jcta.2008.09.003.

[Nas20] Eric Naslund. "The partition rank of a tensor and k-right corners in Fqn". In: *Journal of Combinatorial Theory, Series A* 174 (2020). DOI: 10.1016/j.jcta.2019.105190.

[NS17] Eric Naslund and Will Sawin. "Upper Bounds for Sunflower-free Sets". In: *Forum of Mathematics, Sigma* 5 (2017). DOI: 10.1017/fms.2017.12.

[Ore55] Oystein Ore. "Graphs and matching theorems". In: *Duke Mathematical Journal* 22.4 (1955), pp. 625–639. DOI: 10.1215/S0012-7094-55-02268-7.

[Pel70] Giuseppe Pellegrino. "Sul massimo ordine delle calotte in $S_{4,3}$". In: *Matematiche (Catania)* 25.10 (1970), pp. 149–157.

[Per28] O. Perron. "Über einen Satz von Besicovitch". In: *Mathematische Zeitschrift* 28 (1928), pp. 383–386. DOI: 10.1007/BF01181172.

[Pet91] Julius Petersen. "Die Theorie der regulären graphs". In: *Acta Mathematica* 15 (1891), pp. 193–220. DOI: 10.1007/BF02392606.

[PP19] Fedor Petrov and Cosmin Pohoata. "A remark on sets with few distances in $\mathbb{R}^d$". In: *arXiv e-prints* (2019). DOI: 10.48550/arXiv.1912.08181.

[Sch08] I. Schur. "Neuer Beweis eines Satzes von W. Burnside". In: *Jahresbericht der Deutsch. Math.-Ver.* 17 (1908), pp. 171–176.

[Sei95] JJ Seidel. "Discrete non-Euclidean geometry". In: *Handbook of incidence geometry*. Elsevier, 1995, pp. 843–920.

[She22] Adam Sheffer. *Polynomial Methods and Incidence Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2022. DOI: 10.1017/9781108959988.

[Tao16] Terence Tao. *A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound*. 2016. URL: https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the-croot-lev-pach-ellenberg-gijswijt-capset-bound/.

[Tao14] Terence Tao. *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*. 2014. DOI: 10.48550/arXiv.1310.6482.

[Tao08] Terence Tao. *Dvir's proof of the finite field Kakeya conjecture*. 2008. URL: https://terrytao.wordpress.com/2008/03/24/dvirs-proof-of-the-finite-field-kakeya-conjecture/.

[Tao10] Terence Tao. *How to recognise that the polynomial method might work*. MathOverflow. 2010. URL: https://mathoverflow.net/q/43549.

[TV06] Terence Tao and Van H. Vu. *Additive Combinatorics*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006. DOI: 10.1017/CBO9780511755149.

[Tur88] G. Turnwald. "Permutation polynomials of binomial type". In: *Contributions to General Algebra* 6 (1988), pp. 281–286.

[Tut47] W. T. Tutte. "The Factorization of Linear Graphs". In: *Journal of the London Mathematical Society* s1-22.2 (1947), pp. 107–111. DOI: 10.1112/jlms/s1-22.2.107.

[Wan87] Daqing Wan. "Permutation Polynomials over Finite Fields". In: *Acta Mathematica Sinica* 3.1 (1987), pp. 1–5. DOI: 10.1007/BF02564938.

[Whe09] Jeffrey Wheeler. *The Erdos-Heilbronn Conjecture*. 2009. URL: https://www.math.cmu.edu/users/af1p/Teaching/AdditiveCombinatorics/PolynomialMethodClassNotes.pdf.

[Wil21] Virginia Vassilevska Williams. *Matrix Multiplication and Graph Algorithms: Matchings in graphs*. 2021. URL: https://people.csail.mit.edu/virgi/6.890/lecture16.pdf.

[Wol99] Thomas Wolff. "On some variants of the Kakeya problem". In: *Pacific Journal of Mathematics* 190 (1999), pp. 111–154. DOI: 10.2140/pjm.1999.190.111.