University of Wisconsin Milwaukee

UWM Digital Commons

August 2020

Asymptotic Probability of Incidence Relations Over Finite Fields

Adam Buck
University of Wisconsin-Milwaukee

ASYMPTOTIC PROBABILITY OF INCIDENCE RELATIONS OVER FINITE FIELDS

by

Adam Buck

A Dissertation Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

in Mathematics

at

The University of Wisconsin-Milwaukee

August 2020

ABSTRACT

ASYMPTOTIC PROBABILITY OF INCIDENCE RELATIONS OVER FINITE FIELDS

by

Adam Buck

The University of Wisconsin-Milwaukee, 2020
Under the Supervision of Professor Jeb Willenbring

Given four generic lines in $\mathbb{FP}^3$, we ask, "How many lines meet the four?" The answer depends on the field. When $\mathbb{F} = \mathbb{C}$, the answer is two. When $\mathbb{F} = \mathbb{R}$, the answer is either zero or two.

If we work over a finite field $\mathbb{F}_q$, there are only finitely many projective lines. We compute the probability four lines are met by two. The main result is that as q approaches infinity, this probability approaches $1/2$. Asymptotically, the other half of the time zero lines will meet the four.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1   Introduction

Schubert calculus is a branch of enumerative geometry. Roughly speaking, a Schubert problem seeks to count the number of subspaces satisfying a collection of *Schubert conditions*. A Schubert condition specifies a set of subspaces of a fixed dimension which meet a flag in a particular way. These terms are rigorously and neatly defined using the language of Grassmannians. Before providing such definitions, we look at a specific Schubert problem in geometric terms. We call this the Four Lines Problem. Examining the Four Lines Problem over finite fields is the main topic of this dissertation.

Schubert calculus is named after its pioneer Herman Schubert (1848 - 1911). Schubert was a German school teacher who never held a professorship, although he was offered multiple positions. Schubert impressively answered many problems in enumerative geometry. Making Schubert calculus rigorous is Hilbert's 15th Problem [Hil02]. The problem remains only partially resolved.

1.1   The Four Lines Problem

A basic Schubert problem is

How many lines in $\mathbb{FP}^3$ meet four generic lines in $\mathbb{FP}^3$?

We call this the *Four Lines Problem over* $\mathbb{F}$. An *instance* of the Four Lines Problem refers to answering this question for a specific set of four lines. The figure below shows an instance of the Four Lines Problem over $\mathbb{R}$ where the answer is two.
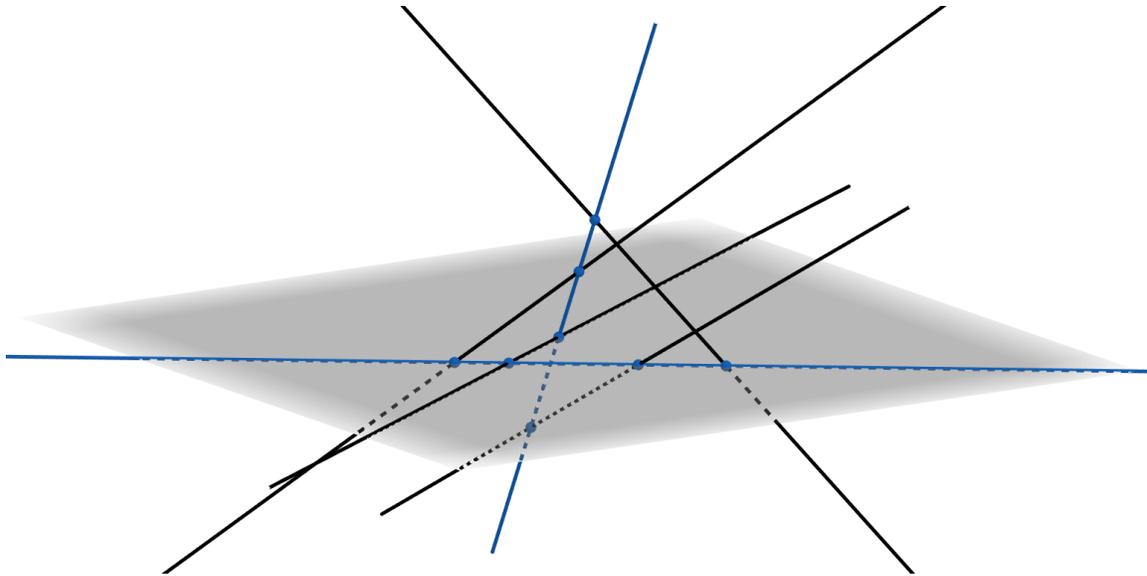
Figure 1.1: *Four black lines are met by two blue lines. Image created using GeoGebra.*

We shall rigorously define generic later, for now we provide an imprecise, and slightly inaccurate, intuitive definition. A collection of lines is generic if no special relations exist among them. An example of a special relation would be if any of the two lines intersected. This is special in the sense that we typically do not expect two lines in $\mathbb{FP}^3$ to intersect.

1.1.1   The Complex Case

When $\mathbb{F} = \mathbb{C}$ the answer two the Four Lines Problem is two. Historically, this was first answered non-rigorously by Schubert. He looked at a specialized instance of the problem where the answer is easily seen to be two. His *principle of conservation of number* then states that if the answer is finite in a specific case, the answer will be the same finite number in the generic case.

The particular specialized instance considered by Schubert is when the first two lines intersect at a point P and the last two lines intersect at another point Q. In this case the two lines meeting the four are easily found. The first is the line containing P and Q. The second is the line of intersection between the plane containing first two lines and the plane

containing the last two lines.
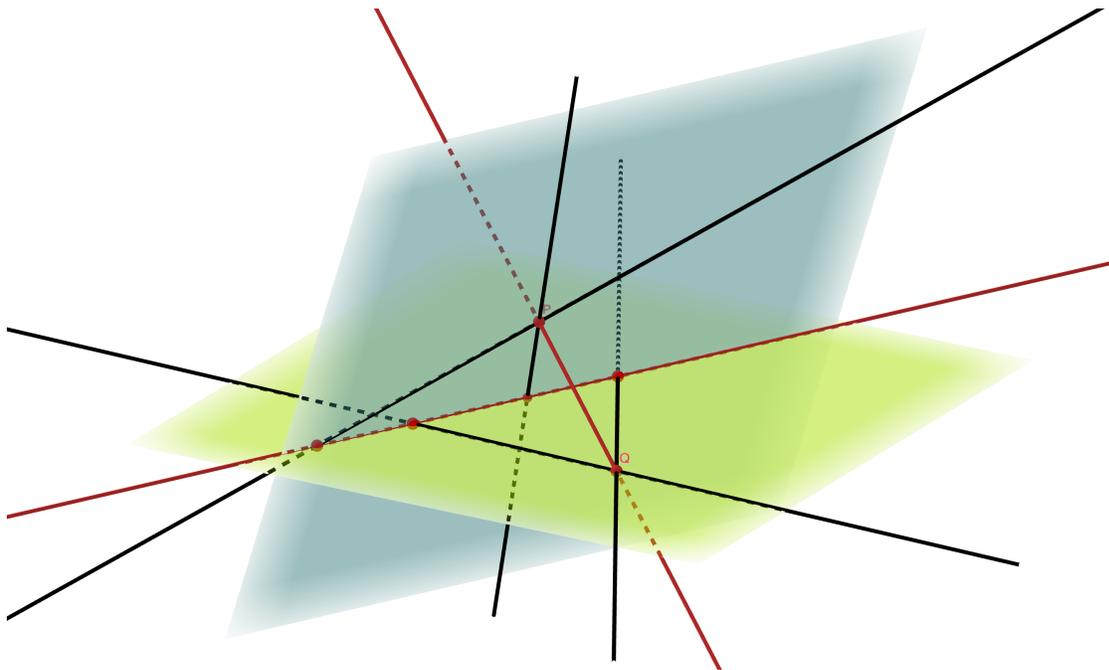
Figure 1.2: *Two black lines meeting at the point P contained in the blue plane. Two more black lines meeting at the point Q contained in the green plane. The two red lines meet the four black lines. One red line contains P and Q. The other is the line of intersection of the blue and green planes. Image created using GeoGebra.*

Of course, it could also have been the case these two lines coincide. As is the case with many enumerative problems, we would count this line with multiplicity two and thus the principle of conservation of number is not violated.

We could consider an even more specialized instance of the Four Lines Problem where all four lines are contained in the same plane. In this case, any line contained in this plane meets the four, so there are infinitely many lines meeting the four. This does not violate the principle of conservation of number since the principle only applies when the number of solutions is finite.

We make a few remarks about the principle of conservation of number, although it is not pertinent to the main result. The first rigorous treatment of Schubert's principle was done

by means of the cohomology theory of manifolds. The principle may be generalized to say that cohomology classes are conserved. In the case of a specific instance having finitely many solutions, counted with multiplicity, we happen to be conserving the cohomolgy class of a point. However, even in the case where there are infinitely solutions, such as the instance described in the preceding paragraph, a cohomology class is conserved. Details may be found in [KL72] and are also described in generality Section 1.2 below.

1.1.2 The Real Case

The Four Lines Problem over $\mathbb{R}$ is more interesting. Here the answer is generically zero or two. This non-unique answer to the Four Lines Problem leads to many interesting questions referred to as *reality problems*. The answer to the Four Lines Problem over the finite fields is also zero or two so we may ask analogous questions in these cases.

First we provide an intuitive argument to see why we have two answers in the real case. Consider a generic instance of the Four Lines Problem over $\mathbb{R}$. Considering these four real lines as complex lines, we know there are two complex lines meeting the four. These two complex lines are either real, in which case the answer to the problem over $\mathbb{R}$ is two, or the two complex lines are not real, in which case the answer is zero. We will see when the answer in the finite fields case is zero, we can find two lines in a degree two field extension which meet the four.

A first interesting follow-up question to the Four Lines Problem over $\mathbb{R}$ is

Under what conditions is the answer two?

The Shapiro conjecture for Grassmannians gives a large set of instances of the Four Lines Problem over $\mathbb{R}$ whose answer is two. The particular case of the Four Lines Problem is resolved in [Sot00] using Grassmannians and Gröbner bases. The conjecture for Grassmannians is fully proved in [MTV09]. The conjecture may be stated more generally, where it is not entirely true. This is discussed in [Sot10].

4

Another question we may ask is

What is the "probability" four "random" lines are met by two?

We use quotes since there is ambiguity as to how to define probability. A careful formulation is laid out in more generality in [BL20] and [BLLP19] and many asymptotic results are stated and proved. Answering the above question for the case of finite fields is the main result of this paper and is discussed in the next section.

1.1.3   The Case of Finite Fields

We shall see for any finite field the answer to the Four Lines Problem is generically zero or two. Let $\mathbb{F}_q$ be the field with q elements. We may ask the question

Given four random lines in $\mathbb{F}_q\mathbb{P}^3$, what is the probability two lines in $\mathbb{F}_q\mathbb{P}^3$ meet the four?

As there are finitely many points and lines in $\mathbb{F}_q\mathbb{P}^3$, we may simply count the number of instances of the Four Lines Problem whose answer is two. This is done in chapter 4. These counts are verified via Mathematica for finite fields of prime cardinality less than or equal to 19 in chapter 5.

The main result of this paper concerns the asymptotics of these probabilities.

Theorem 1. *The probability four random lines in $\mathbb{F}_q\mathbb{P}^3$ are met by two lines in $\mathbb{F}_q$ is a rational function in q approaching 1/2 as q approaches infinity. Further, the probability four random lines are not met by any is also a rational function in q also approaching 1/2.*

While the exact counts given in chapter 4 are sufficient to prove this result, we provide another proof of the result in chapter 3. We relate a large subset of 4-tuples of lines in $\mathbb{F}_q$ to monic quadratic polynomials over $\mathbb{F}_q$. Under this correspondence the number of lines meeting a 4-tuple is the number of solutions to this polynomial over $\mathbb{F}_q$. The proof applies in the real and complex cases as well.

1.2 Schubert Problems

The Four Lines Problem is an example of a *Schubert Problem*. While the Four Lines Problem is easy to phrase in terms of projective lines in $\mathbb{FP}^3$. Generalizations are much easier to phrase in terms of Grassmannians. In this section, we briefly describe these generalizations. In the case of $\mathbb{F} = \mathbb{C}$, solving Schubert problems is directly related to computing the cup product in the cohomology ring of Grassmannians. This is not directly related to our main result and details may be found in [Ful97].

Projective lines in $\mathbb{FP}^3$ are naturally in bijection with the Grassmannian of 2-planes in 4-space $\mathrm{Gr}_2(\mathbb{F}^4)$. This correspondence is described in section 3.3. We may rephrase the Four Lines Problem as

How many elements in $\mathrm{Gr}_2(\mathbb{F}^4)$ meet four generic elements of $\mathrm{Gr}_2(\mathbb{F}^4)$?

As we discuss Schubert Problems in generality, we turn back to the Four Lines Problem as a motivating example.

First, let E be a vector space of finite dimension m and let $r \leq m$ be an integer. Fix a (full) flag

$$F_\bullet : 0 = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m = E \tag{1.1}$$

For each Young diagram $\lambda = (\lambda_1, \lambda_2, ...)$ with at most r rows and $m - r$ columns, we have a *Schubert variety*

$$\Omega(F_\bullet) = \{X \in \mathrm{Gr}_r(E) : \dim(X \cap F_{m-r+i-\lambda_i}) \geq i \text{ for } 1 \leq i \leq r\} \tag{1.2}$$

and the collection of requirements that $dim(X \cap F_{m-r+i-\lambda_i}) \geq i$ is called a *Schubert condition*. $\mathrm{Gr}_r(E)$ may be given the structure of a projective variety via the Plücker embedding. The Schubert varieties are irreducible subvarieties of $\mathrm{Gr}_r(E)$ and the codimension of $\Omega_\lambda(F_\bullet)$ is $|\lambda|$. A *Schubert problem* is determined by a collection of Schubert conditions. To be a Schubert problem, the sum of the codimensions of these Schubert conditions should be the dimension

6

of $\mathrm{Gr}_r(E)$ which is $r(m-r)$. If we choose the flags for each Schubert condition generically, we expect finitely many points in $\mathrm{Gr}_r(E)$ to be contained in the intersection of these Schubert varieties.

For $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, we use these variety structures to define generic. Consider a k-tuple of Grassmannians $(X_1, X_2, ..., X_k) \in \mathrm{Gr}_{r_1} \times \mathrm{Gr}_{r_2} \times \cdots \mathrm{Gr}_{r_k}$. For each Zariski open set of this variety, we may look at the possible answers to specific instances of a Schubert problem. We call an answer to a Schubert problem generic if it is seen as an answer on every Zariski open set. Once we have the generic answers, then we call the instances of a Schubert problem generic if the instance has a generic answer.

In the case of $\mathbb{F}_q$ being a finite field, defining generic is more challenging. Since the Grassmannian contains finitely many elements, every set is Zariski open. We may find the probability a given number is an answer to a particular Schubert problem as a function of q. We say an answer is a generic answer for all $\mathbb{F}_q$ simultaneously if the limit of this probability is greater than 0 as q approaches infinity. After we have our generic answers, we may simply declare any instance of a Schubert problem to be generic if it has a generic answer.

When $\lambda = (k)$, we call $\Omega_\lambda(F_\bullet)$ a *special Schubert variety*. It consists of those r-planes which intersect $F_{m-r+1-k}$ non-trivially. We shall use the term *meet* to mean intersect non-trivially through this dissertation.

Let $E = \mathbb{F}^4$. Let $r = 2$ and fix four flags $F_\bullet^1, F_\bullet^2, F_\bullet^3, F_\bullet^4$ Let $\lambda = (1)$. Then $\Omega_\lambda(F_\bullet^i)$ consists of those elements of $\mathrm{Gr}_2(E)$ which meet F_2^i non-trivially. Notice F_2^i is a 2-plane, so each special Schubert variety $\Omega_{(1)}(F_\bullet^i)$ consists of those 2-planes which meet a given 2-plane. Translating this to the geometric formulation of lines in $\mathbb{FP}^3$, this corresponds to all lines which meet a fixed line. We see that answering this instance of the Four Lines Problem amounts to finding $|\cap \Omega_{(1)}(F_\bullet^i)|$.

2 Preliminaries

In this chapter we recall basic definitions and properties of finite fields. We also look at how polynomials over finite fields may factor. We also recall group actions, orbits, and stabilizers. We describe these notions generally then look specifically at group actions of the general linear groups on vector spaces and related objects. One such action is right multiplication of a matrix by an element of GL_r. We see the orbits of this action are in one-to-one correspondence with row reduced echelon form matrices. Another important example is the rational canonical form of a square matrix which serve as representatives of the orbits under the action of conjugation.

2.1 Finite Fields

In this section we recall basic properties of finite fields and the factorization of polynomials over finite fields. See [DF04]14.3 for details.

2.1.1 Realizing Finite Fields

First, every finite field has a prime characteristic. For each prime p and positive integer s, there is, up to isomorphism, exactly one finite field with $q = p^s$ elements; we denote the field with q elements by $\mathbb{F}_q$. When $s = 1$, the field $\mathbb{F}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. When $s > 1$, $\mathbb{F}_q$ may be realized as the splitting field of $x^q - x$ over $\mathbb{F}_p$. Elsewhere the notation $\mathrm{GF}(q)$ is also used to denote the field with q elements.

The field extensions of $\mathbb{F}_q$ are precisely $\mathbb{F}_{q^n}$ where n is a positive integer. Thus $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q'}$ if and only if $q = p^s$ and $q' = p^{s'}$ and s' divides s. The Galois Group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{q^n})$ is cyclic of order n and is generated by the Frobenius endomorphism, which sends each element of $\mathbb{F}_{q^n}$ to its p-th power.

$\mathbb{F}_q$ may also be realized as $\mathbb{F}_p[x]/\langle f(x) \rangle$. Where $f(x) \in \mathbb{F}_p[x]$ is a monic irreducible

polynomial of degree s. As finite fields are unique, choosing different monic irreducible polynomials to define $\mathbb{F}_q$ results in an isomorphic field.

2.1.2   Polynomials over Finite Fields

We shall be concerned with the factorization of polynomials over $\mathbb{F}_q$, we have the following

Proposition 2. *Every irreducible polynomial over a finite field $\mathbb{F}_q$ is separable. A polynomial in $\mathbb{F}_q[x]$ is separable if and only if it is the product of distinct irreducible polynomials.*

Thus factorization of polynomials over finite fields is similar to the familiar fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. See [DF04, 13.5] for an example of an inseparable irreducible polynomial over an infinite field with finite characteristic.

There are q^d monic polynomials of degree d in $\mathbb{F}_q[x]$. We shall be interested in counting the monic irreducible polynomials.

Proposition 3. *There are*

$$\psi_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$$

monic irreducible polynomials of degree d.

Where $\mu : \mathbb{N}_{\geq 0} \to \{-1, 0, 1\}$ is the *Möbius function*. Recall $\mu(k) = 0$ if k is not square free, otherwise $\mu(k) = (-1)^n$ where n is the number of distinct prime factors of k. To prove Proposition 3, we use the Möbius inverseion formula. If $f(n)$ is a function defined on the nonnegative integers and $F(n) = \sum_{d|n} f(d)$, then

$$f(n) = \sum_{d|n} \mu(d) F(n/d). \tag{2.1}$$

See [DF04]14.3 for more information on the Möbius inversion formula.

Proof. Let $\psi_q(n)$ be the number of irreducible polynomials of degree n over $\mathbb{F}_q$. Consider the field $\mathbb{F}_{q^n}$. Every element of $\mathbb{F}_{q^n}$ is a root of exactly one monic irreducible polynomial of

9

some degree d which divides n. We therefore have

$$q^n = |\mathbb{F}_{q^n}| = \sum_{d|n} d\psi_q(d)$$

Using the Möbius inversion formula with $f(n) = n\psi(n)$ shows $n\psi(n) = \sum \mu(d)q^{n/d}$. $\qquad\square$

Definition 1. Define $\mathcal{I}_q$, $\mathcal{F}_q$, and $\mathcal{S}_q$ by

$\mathcal{I}_q = \{f \in \mathbb{F}_q[x] : f \text{ is monic irreducible quadratic over } \mathbb{F}_q[x]\}$

$\mathcal{F}_q = \{f \in \mathbb{F}_q[x] : f \text{ is monic quadratic with distinct linear factors over } \mathbb{F}_q[x] \text{ and } f(0) \neq 0\}$

$\mathcal{S}_q = \{f \in \mathbb{F}_q[x] : f \text{ is monic quadratic and factors as a perfect square over } \mathbb{F}_q[x] \text{ and } f(0) \neq 0\}$

(2.2)

Example 2.

$$|\mathcal{I}_q| = \tfrac{1}{2}\sum_{k\in\{1,2\}} \mu(\tfrac{2}{k})q^k = \tfrac{1}{2}(-q + q^2) = \binom{q}{2}$$
$$|\mathcal{F}_q| = \binom{q-1}{2} \qquad\qquad (2.3)$$
$$|\mathcal{S}_q| = q - 1$$

We may see $|\mathcal{I}_q|$ independent of Proposition 3 when $q \neq 2$. There is a two-to-one map $\mathbb{F}_{q^2} - \mathbb{F}_q \to \mathcal{I}_q$ which sends an element to its minimal polynomial over $\mathbb{F}_q$. The cardinalities of $\mathcal{F}_q$ respectively $\mathcal{S}_q$ follow from choosing two distinct roots respectively one distinct root from $\mathbb{F}_q^\times$.

2.2   Group Actions

In this section, we record basic definitions and properties of group actions. The orbits and stabilizers of group actions will provide a convenient framework for proving the main result. See [DF04, 1.7, 4.1] for details.

Definition 3. A *left action* of a group G on a set S is a map from $G \times S$ to S written $g \cdot s$ satisfying

1. $g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s$ for all $g_1, g_2 \in G$ and $s \in S$; and

2. $1 \cdot a = a$ for all $s \in S$.

The notion of a *right action* is defined similarly.

2.2.1   Orbits and Stabilizers

Definition 4. Given an action of a group G on a set S, the *orbit* and *stabilizer* of an element $s \in S$, denoted $\mathrm{Orb}(s)$ and $\mathrm{Stab}_G(s)$ respectively are given by

$$\mathrm{Orb}(s) := \{g \cdot s : \ g \in G\} \tag{2.4}$$

and

$$\mathrm{Stab}_G(s) := \{g \in G : \ g \cdot s = s\}. \tag{2.5}$$

The orbits of a group action partition S and $\mathrm{Stab}_G(s)$ is a subgroup of G. The Orbit-Stabilizer Theorem relates these notions.

Theorem 4 (Orbit-Stabilizer Theorem)**.** *Let G be a group acting on a set S and $s \in S$. Then $|G| = |Orb(s)||Stab_G(s)|$.*

We say an element $g \in G$ *acts trivially* if $g \cdot s = s$ for all $s \in S$. We call a group action *trivial* if every element of G acts trivially. We call a group action *faithful* if only the identity element acts trivially.

2.2.2   k-transitivity

We say that a group action is *transitive* if for every $s, t \in S$, there exists $g \in G$ such that $g \cdot s = t$. In other words, a group action is transitive if there is only one orbit.

Given a group action of G on a set S and a positive integer k, G also naturally acts on S^k by

$$g \cdot (s_1, ..., s_k) = (g \cdot s_1, ..., g \cdot s_k). \tag{2.6}$$

The orbits of the action on the k-tuples are more complicated. First, if S contains more than 1 element and $k \geq 2$, the action is not transitive. To see this, let $s \neq t \in S$ then $(s, s, ..., s)$ and $(t, s, ..., s)$ are necessarily contained in separate orbits. If we restrict this action to the set D of those tuples containing distinct elements,

$$D := \{(s_1, ..., s_k) : s_i \neq s_j \; \forall i \neq j\}.$$

the action may be transitive. If this action is transitive, we say the original action of G on S is k-transitive. In other words an action is k-transitive if any k-tuple of distinct elements may be sent to any other k-tuple of distinct elements under the action of some group element.

2.3 Linear Algebra

In this section we recall the definition of the general linear group. The actions of the general linear groups play important roles in the proving the main result. We also recall the row-reduced echelon form, which provides a distinguished element of the orbits of the left action of a general linear group. We also examine the action of conjugation on a general linear group.

E will always denote a finite dimensional vector space of dimension m over a field $\mathbb{F}$. All vector spaces of a dimension m over $\mathbb{F}$ are isomorphic, thus $E \cong \mathbb{F}^m$. Let $(e_1, ..., e_m)$ denote the standard basis for $\mathbb{F}^m$.

2.3.1 The General Linear Group

The *general linear group*, denoted $\mathrm{GL}(E)$, is the set of invertible linear transformations $E \to E$ whose group operation is given by function composition. Fixing a basis for E, we have an isomorphism from $\mathrm{GL}(E)$ to the invertible $m \times m$ matrices over $\mathbb{F}$. We denote this group by $\mathrm{GL}_m(\mathbb{F})$ or simply GL_m when underlying field $\mathbb{F}$ is clear from context.

GL_m is in one-to-one correspondence with (ordered) bases for E. If we fix a standard basis

$(e_1, ..., e_m)$ for E, then $g \in \mathrm{GL}_m$ corresponds to the basis $(g(e_1), ..., g(e_m))$. This perspective will prove useful in many proofs.

Proposition 5.

$$|GL_m(\mathbb{F}_q)| = \prod_{i=0}^{m-1} (q^m - q^i) \tag{2.7}$$

Proof. We count the number of bases $(x_1, ..., x_m)$ for $\mathbb{F}_q^m$. First, choose $x_1 \in \mathbb{F}_q^m - \{0\}$ to be the first basis vector. The second basis vector x_2 must be chosen from $\mathbb{F}_q^m - \langle x_1 \rangle$. Proceeding in this way the ith basis vector x_i must be chosen from $\mathbb{F}_q^m - \langle x_1, ..., x_{i-1} \rangle$. $\qquad\square$

2.3.2 Row-Reduced Echelon Form

Let r, m be positive integers and let $M_{r,m}$ denote the set of $r \times m$ matrices with entries in $\mathbb{F}$. We write M_n in place of $M_{n,n}$. Let $M \in M_{r,n}$, the *row space* of M is the span of the rows of M viewed as vectors. The *rank* of M is the dimension of its row space. We say M is *full rank* if the rank of M is equal to $\min(r, m)$. We denote the set of full rank matrices by $M_{r,m}^\circ$.

Consider the action of GL_r on $M_{r,m}$ by left multiplication. Two matrices in $M_{r,m}$ are said to be *row equivalent*, if they are contained in the same orbit; equivalently, if they have the same row space. The *row-reduced echelon form (RREF)* of a matrix provides a distinguished representative of each orbit. The RREF of a matrix is the unique matrix in each orbit satisfying the following properties:

1. Each nonzero row has a 1 (called a *leading 1*) as its fist nonzero entry;

2. All other entries in the column of a leading 1 are 0;

3. All zero rows occur below every nonzero row; and

4. If two leading 1's occur in the (i, j) and (k, l) entries and $i < k$, then $j < l$.

The number of leading 1's is the rank of the matrix, which is also the dimension of the row space of M.

Example 5. Let $r = 2$ and $m = 4$. The full rank reduced row echelon form matrices are of the forms

$$\begin{bmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{bmatrix}, \begin{bmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{bmatrix}, \begin{bmatrix} 1 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{bmatrix}, \begin{bmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$
(2.8)

where $*$ denotes an arbitrary element of the field. If $\mathbb{F} = \mathbb{F}_q$, there are q choices for each starred entry and we see there are $q^4 + q^3 + 2q^2 + q + 1$ full rank RREF 2×4 matrices.

2.3.3 Similarity Classes of the General Linear Group

Any group G acts on itself by *conjugation*:

$$g \cdot s = gsg^{-1}$$
(2.9)

for all $g, s \in G$. Note that G is acting on itself, thus $S = G$, so s is an element of G as a set. We compute the action of g on s, by computing gsg^{-1} in G as a group.

The orbits of this action are called the *conjugacy classes* of G. Note that an element $g \in G$ will be alone its conjugacy class if and only if g is contained in the center $Z(G)$ of G. We call such a conjugacy class *central*. When G is a finite group, we may write the order of G as the sum of the cardinality of its center and of its non-central conjugacy classes. This is the *class equation* of G:

$$|G| = |Z(G)| + \sum_{i=1}^{k} |\mathrm{Orb}(g_i)|.$$
(2.10)

where there are k non-central conjugacy classes and each g_k is a representative of a distinct conjugacy class.

Of particular interest is the case $G = \mathrm{GL}_n$. In this case, we call the orbits *similarity classes* instead of conjugacy classes. Note that the term *similarity class* more accurately

refers to the orbits of GL_n acting on M_n, but we shall, by abuse of notation, use the term in both contexts. Two matrices in the same orbit are said to be *similar*. The center of GL_n respectively M_n are the *scalar matrices*, those matrices of the form cI for $c \in \mathbb{F}^\times$ respectively $c \in \mathbb{F}$.

The rational canonical form provides a distinguished representative of each similarity class. It is discussed in the proceeding paragraphs. We prefer this form over the Jordan canonical form. The rational canonical form only uses entries from the field $\mathbb{F}$, while the Jordan canonical form may require use of entries from a field extension of $\mathbb{F}$. Further, the invariant factors, used in the rational canonical form, play an important role in the proofs that follow.

We may view a finite dimensional vector space E over $\mathbb{F}$ as a module over $\mathbb{F}[t]$ by fixing $T \in \mathrm{GL}(E)$ and letting t act as T. Since $\mathbb{F}[t]$ is a principal ideal domain, the invariant factor form gives an isomorphism of $\mathbb{F}[t]$-modules:

$$E \cong \mathbb{F}[t]/(f_1(t)) \oplus \mathbb{F}[t]/(f_2(t)) \oplus \cdots \oplus \mathbb{F}[t]/(f_k(t)) \tag{2.11}$$

where $f_1(t), f_2(t), ..., f_k(t)$ are monic polynomials of degree at least one satisfying the divisibility requirements $f_1(t)|f_2(t)|\cdots|f_k(t)$. The polynomials $f_i(t)$ are called the *invariant factors* and play an important role in determining the Rational Canonical Form of a matrix, which in turn plays a major role in proving the main theorem.

For each term $\mathbb{F}[t]/(f(t))$ on the right side of 2.11, let $f(t) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + a_0$. We may choose $1, \bar{t}, \bar{t}^2, ..., \bar{t}^{d-1}$ as a basis for $\mathbb{F}[t]/(g(t))$. In this case the matrix of T has a particularly nice form

$$C_f = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{d-1} \end{bmatrix}$$

15

called the *companion matrix* of $f(t)$. Note that the characteristic polynomial of C_t is $f(t)$.

Combining such bases for each term on the right side of 2.11, yields a basis with respect to which the matrix of T is block diagonal with blocks $C_{f_1}, C_{f_2}, ..., C_{f_k}$. This is the *rational canonical form* of T or any matrix representing T.

We have two important facts about the invariant factors. The largest invariant factor $f_k(t)$ is the *minimal polynomial* m_T of T. The product of the invariant factors is the *characteristic polynomial* c_T of T. Thus the minimal polynomial divides the characteristic polynomial. These facts are particularly useful in classifying linear transformations over low-dimensional vector spaces since this heavily restricts the possibilities of the invariant factor decomposition of a given linear transformation.

Example 6. Given $M \in M_2$, then M has either one quadratic invariant factor or two linear invariant factors. If M has only one quadratic invariant factor f_1, then $f_1 = c_M = m_M$ and $M = C_{f_1}$. If M has two invariant linear factors f_1, f_2, then $f_1 | f_2$ so $f_1 = f_2$. Since f_1 and f_2 are linear, their companion matrices are 1×1 so M is a scalar matrix.

The above example plays an important role in finding the class equation of $\mathrm{GL}_2(\mathbb{F}_q)$.

Theorem 6 (The Class Equation of $\mathrm{GL}_2(\mathbb{F}_q)$)**.** *The class equation of $GL_2(\mathbb{F}_q)$ is*

$$|GL_2(\mathbb{F}_q)| = (q-1) + \underbrace{(q+1)(q-1) + \cdots (q+1)(q-1)}_{(q-1) \ times} + \underbrace{q(q+1) + \cdots + q(q+1)}_{\binom{q-1}{2} \ times}$$

$$+ \underbrace{q(q-1) + \cdots q(q-1)}_{\binom{q}{2} \ times}.$$

$$(2.12)$$

Further, the non-central similarity classes have size $(q+1)(q-1)$ when $c_M \in \mathcal{S}_q$; $q(q+1)$ when $c_M \in \mathcal{F}_q$; and $q(q-1)$ when $c_M \in \mathcal{I}_q$.

Proof. First, $|Z(\mathrm{GL}_n(\mathbb{F}_q))| = q - 1$ since the center consists of the non-zero scalar matrices.

In light of Example 6, the remaining non-central similarity classes may each be represented by the 2×2 companion matrix of their characteristic polynomial. We shall count

16

how many elements of GL_2 have a given characteristic polynomial. Consider the polynomial $c(t) = t^2 - Tt - D$ for $T, D \in \mathbb{F}_q$. To find the number of matrices with this characteristic polynomial is to count the solutions $(a, b, c, d) \in \mathbb{F}_q^4$ to

$$a + d = T$$
$$ad - bc = D \tag{2.13}$$

since the characteristic polynomial of $M \in \mathrm{GL}_2$ is $t^2 - (a + d)t - (ad - bc)$. We see T is the trace and D is the determinant of M. As we are considering GL_2, we have that $D \neq 0$.

First suppose, $c(t) \in \mathcal{F}_q$ factors into distinct linear factors so $c(t) = (t - \alpha)(t - \beta)$ for some $\alpha \neq \beta \in \mathbb{F}_q^\times$. First consider the 2 solutions (a, d) to $a + d = T$ and $ad = D$, namely (α, β) and (β, α). For each of these solutions, there are $2q - 1$ solutions (b, c) to the second equation in 2.13 since this amounts to finding solutions $cd = ad - D = 0$. Now consider the $q - 2$ solutions (a, d) to $a + d = T$ and $ad \neq D$. For each of these $q - 2$ solutions, there are $q - 1$ solutions (c, d) to the second equation in 2.13 since $cd = ad - D \neq 0$. Thus in the case of $c(t) \in \mathcal{I}_q$, there are $2(2q - 1) + (q - 2)(q - 1) = q(q + 1)$ solutions to 2.13 as claimed.

Next suppose, $c(t) \in \mathcal{I}_q$. In this case there are no solutions (a, d) to $a + d = T$ and $ad = D$, otherwise $c(t)$ would factor as $(t - a)(t - d)$ over $\mathbb{F}_q$. In this case there are q solutions to $a + d = T$ and $ad \neq D$. And, by the same argument above, for each of these q solutions (a, d), there are $q - 1$ solutions (c, d), to the second equation of 2.13. Thus in the case of $c(t) \in \mathcal{I}_q$, there are $q(q - 1)$ solutions to 2.13.

Finally, suppose $c(t) \in \mathcal{S}_q$, so $c(t) = (c - \alpha)^2$ for some $\alpha \in \mathbb{F}_q^\times$. The argument is similar to the first case, however, in this case there is only one solution (a, d) to $a + d = T$ and $ad = D$, namely (α, α). For this solution there are $2q - 1$ solutions (b, c) to the second equation in 2.13. The remaining $q - 1$ solutions to $a + d = T$ are such that $ad \neq D$. For each of these solutions (a, d), there are as above, $q - 1$ solutions (c, d) to the second equation of 2.13. We have that $(2q - 1) + (q - 1)^2 = q^2$ matrices have $c(t)$ as their characteristic polynomial, however, one of these matrices is scalar so there are $q^2 - 1 = (q + 1)(q - 1)$ matrices in the

17

non-central similarity class of a matrix with a perfect square characteristic polynomial.

It remains to count the number of similarity classes of each case. This was done in Example 2. □

An alternative proof of the class equation above, using the Orbit-Stabilizer Theorem, may be found in [Mat12]. The proof presented above provides technique and detail used in the main result. The above theorem may easily be altered to find the number and size of the similarity classes of $M_n(\mathbb{F}_q)$ by simply allowing 0 as a root of the characteristic polynomials considered.

Corollary 7. *Let $f \in \mathbb{F}_q[x]$ be a monic degree 2 polynomial with nonzero constant term. Then $|Stab(C_f)|$ is $q(q-1)$ when $f \in \mathcal{S}_q$, $(q-1)^2$ when $f \in \mathcal{F}_q$, and $(q+1)(q-1)$ when $f \in \mathcal{I}_q$.*

Proof. This follows directly from the Orbit-Stabilizer Theorem, Theorem 6, and Proposition 5. □

3   The Grassmannian

As mentioned in chapter 1, we prefer to frame the Four Lines Problem in terms of the Grassmannian of 2-spaces in $\mathbb{F}^4$. In this chapter we define the Grassmannians of r-spaces in $\mathbb{F}^m$. We also describe the natural bijection $\mathbb{FP}^{m-1} \leftrightarrow \mathrm{Gr}_1(\mathbb{F}^m)$. This correspondence extends so that we have a bijection

$$\{(r-1)\text{-planes in } \mathbb{FP}^{m-1}\} \leftrightarrow \mathrm{Gr}_r(\mathbb{F}^m) \tag{3.1}$$

for $r = 1, ..., m$. Realizing the Grassmannian as the row span of a (row-reduced Echelon form) matrix provides a unique representative for each element of Gr_r. These matrices are used in the computations of chapter 5.

First we define the Grassmannian.

Definition 7. Given a positive integer r, the *Grassmannian of r-planes in E* is

$$\mathrm{Gr}_r(E) := \{V \subseteq E : \dim V = r\} \tag{3.2}$$

We will often write Gr_r and omit the underlying vector space E. We also define the *Grassmannian of E* to be the set of all subspaces of E and denote it by Gr.

Let $x_1, ..., x_k \in E$. We denote the span of $x_1, ..., x_k$ by $\langle x_1, ..., x_k \rangle$. Thus if $x_1, ..., x_k$ are linearly independent, $\langle x_1, ..., x_k \rangle \in \mathrm{Gr}_k$.

To explicitly realize the Grassmannian of r-planes in E, fix a basis for E. An r-space $X \in \mathrm{Gr}_r$ is realized as the row span of $M \in M^\circ_{r,m}$. Two such matrices $M, M' \in M^\circ_{r,m}$ represent the same r-space if and only if there exists $g \in \mathrm{GL}_r$ such that $gM = M'$. We therefore have a bijection.

$$\mathrm{Gr}_r(E) \longleftrightarrow \mathrm{GL}(r)\backslash M^\circ_{r,m} \tag{3.3}$$

We will often use the distinguished RREF matrix to represent these orbits. We also write

$[X] \in M_{r,m}^{\circ}$ to represent the matrix corresponding to $X \in \mathrm{Gr}_r(E)$; the basis used to represent $[X]$ will be obvious from context.

3.1 The Cardinality of the Grassmannian

The goal of this section is to show $|\mathrm{Gr}_r(\mathbb{F}_q^m)|$ is the q-binomial coefficient $\binom{m}{r}_q$. To do so, we look at the possible 'shapes' of the free entries of the RRREF for full rank $r \times m$ matrices. Each 'shape' is a Young diagram. The matrices with a given shape are the Schubert cells with respect to the standard flag.

3.1.1 Partitions and Young Diagrams

Given an integer n, a *partition* λ of n, is a decreasing sequence $\lambda = (\lambda_1, \lambda_2, ...)$ of non-negative integers such that $\sum \lambda_i = n$. The size of a partition λ is denoted $|\lambda|$ and is equal to n. Such a sequence converges to 0, and we often write a partition as a finite tuple of the positive integers $\lambda = (\lambda_1, \lambda_2, ..., \lambda_k)$, omitting the zeros. The number k is called the length of the partition.

To each partition $\lambda = (\lambda_1, \lambda_2, ..., \lambda_k)$ of n, there is an associated *Young diagram* consisting of k left-justified rows of boxes; the ith rows containing λ_i boxes. We do not distinguish between λ as a partition and λ as the associated Young diagram. Given two Young diagrams λ and μ, we say μ is contained in λ, and write $\mu \subset \lambda$, if $\mu_i \leq \lambda_i$ for all i. Thus $\mu \subset \lambda$ if the diagram μ fits inside the diagram λ. The figure below shows the complete containment lattice of $\lambda = (2, 2)$. We let $\{\}$ represent the empty diagram.
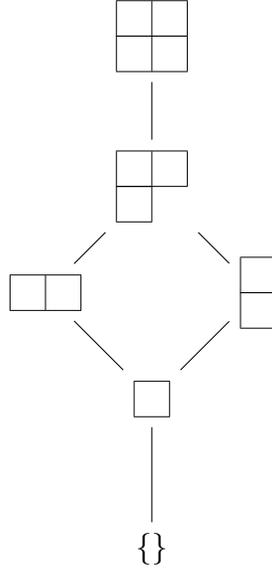
Figure 3.1: *Containment lattice of $\lambda = (2,2)$.*

There is an obvious correspondence between these diagrams and the possible types of RREF matrices in $M^\circ_{2,4}$ from Example 5. This correspondence generalizes, so that the types of RREF matrices in $M^\circ_{r,m}$ are in one-to-one correspondence with the Young diagrams contained in the $r \times (m-r)$ diagram.

Given λ contained in the $r \times (m-r)$ diagram, we have the *complimentary* diagram λ^C formed by removing λ from the $r \times (m-r)$ diagram and rotating the remainder $180\,\deg$. That is $\lambda^C = (m - r - \lambda_r, m - r - \lambda_{r-1}, ...)$. For our purposes, in what follows, we prefer the one-to-one correspondence between types of RREF matrices in $M^\circ_{r,m}$ and the diagrams contained in the $r \times (m-r)$ diagram be given by taking the complimentary diagram to the one described in the previous paragraph.

3.1.2   Schubert Cells

In this section, we describe a cellular decomposition of Gr_r. First, we fix a (full) flag $F_\bullet$

$$F_\bullet : 0 = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m = E \tag{3.4}$$

21

so $\dim F_i = i$. For each Young diagram $\lambda = (\lambda_1, \lambda_2, ... \lambda_k)$ with at most r rows and $m - r$ columns we define a *Schubert cell*

$$\Omega_\lambda^\circ = \Omega_\lambda^\circ(F_\bullet) = \{V \in \mathrm{Gr}_r : \dim V \cap F_k = i, m - r + i - \lambda_i \le k \le m - r + i - \lambda_{i+1}\}. \quad (3.5)$$

If we fix a basis $(x_1, x_2, ..., x_m)$ for E, thus associating $\mathrm{Gr}_r(E)$ with the RREF matrices in $M_{r,m}^\circ$, such that $F_i = \langle x_1, ..., x_i \rangle$, then Ω_λ° consists of those RREF matrices whose shape is given by λ^C.

Note, when $\mathbb{F} = \mathbb{C}$ or $\mathbb{R}$, $\mathrm{Gr}_r(E)$ has the structure of a manifold and the Schubert cells provide a cellular decomposition of $\mathrm{Gr}_r(E)$. The closure of the Schubert cell Ω_λ° is the *Schubert variety* $\Omega_\lambda = \cup_{\mu \subset \lambda} \Omega_\mu^\circ$.

3.1.3 The q-Binomial Coefficients

The cardinality of $\mathrm{Gr}_2(\mathbb{F}_q^m)$ is given by the q-binomial coefficients, which we describe in this section. The q-analog of an object, generalizes the object in such a way that the (limiting) case $q = 1$ produces the original object. In this section only, we consider q as an indeterminate. However, conveniently, the results will be used by letting q be a power of a prime.

We define the q-analogue of a positive integer n by

$$[n]_q = 1 + q + \cdots q^{n-1}. \quad (3.6)$$

Notice the case $q = 1$, we have $[n]_1 = n$. So this definition is a suitable q-analogue of an integer. We then define the q-analogue of the factorial by

$$[n]_q! = [1]_q [2]_q \cdots [n]_q. \quad (3.7)$$

Since $[n]_1 = n$, we also have $[n]_1! = n!$. Further, we have the q-analogue of the binomial

coefficients, which we refer to as the q-binomial coefficients.

$$\binom{n}{k}_q = \frac{[n]_q!}{[n-k]_q![k]_q!} \tag{3.8}$$

Each q-binomial coefficient is obviously a rational function in q. Many of the familiar relations among the binomial coefficients have q-analogues.

Proposition 8 (q-analogue of Pascal's Triangle).

$$\binom{n+1}{k+1}_q = \binom{n}{k}_q + q^{k+1}\binom{n}{k+1}_q \tag{3.9}$$

Proof.

$$\binom{n}{k}_q + q^{k+1}\binom{n}{k+1}_q$$

$$= \frac{[n]_q!}{[n-k]_q![k]_q!} + \frac{[n]_q!q^{k+1}}{[n-k-1]_q![k+1]_q!}$$

$$= \frac{[n]_q!([k+1]_q + q^{k+1}[n-k]_q!)}{[n-k]_q![k+1]_q!}$$

$$= \frac{[n]_q!((1+q+\cdots q^k)+q^{k+1}(1+q+\cdots q^{n-k}))}{[n-k]_q![k+1]_q!}$$

$$= \frac{[n+1]_q!}{[n-k]_q![k+1]_q!}$$

$$= \binom{n+1}{k+1}_q$$

$\square$

Corollary 9. *The q-binomial coefficients are polynomials in q.*

Proof. From the definitions, the q analogue of an integer and of the factorial are polynomials in q and the q-binomial coefficients are rational functions in q. Notice $\binom{n}{0}_q = \binom{n}{n}_q = 1$ and by Proposition 8 all q-binomial coefficients are products and sums of polynomials in q. $\square$

Proposition 10. *Let $k \leq n$ be non-negative integers and λ be the $(n-k) \times k$ Young diagram. Then*

$$\binom{n}{k}_q = \sum_{\mu \subset \lambda} q^{|\mu|}. \tag{3.10}$$

Proof. Let $P(n, k, i)$ denote the set of Young diagrams contained in the $(n-k) \times k$ diagram

23

with exactly i boxes. We wish to show

$$\binom{n}{k}_q = \sum_{i=0}^{n(n-k)} |P(n,k,i)|q^i. \tag{3.11}$$

This will prove the proposition. We define $\phi : P(n+1, k+1, i) \to P(n,k,i) \cup P(n, k+1, i-k-1)$. By

$$\phi(\mu_1, \mu_2, ..., \mu_{n-k}) = \begin{cases} (\mu_1, ..., \mu_{n-k}) \text{ if } \mu_1 \leq k \\ \\ (\mu_2, ..., \mu_{n-k}) \text{ if } \mu_1 = k+1 \end{cases} \tag{3.12}$$

This function is bijective and we have

$$\sum_{i=0}^{k(n-k)} |P(n+1, k+1, i)|q^i = \sum_{i=0}^{(k+1)(n-k)} |P(n,k,i)|q^i + q^{k+1} \sum_{i=0}^{(k+1)(n-k-1)} |(P, n, k+1, i)|q^i.$$

This is the same recurrence relation for the q-binomial coefficients in Proposition 8. It remains to see the trivial base cases

$$\binom{n}{0}_q = 1 = \sum_{i=0}^{0} |P(n,0,i)|q^i \tag{3.13}$$
$$\binom{n}{n}_q = 1 = \sum_{i=0}^{0} |P(n,n,i)|q^i.$$

$\square$

Corollary 11.

$$|Gr_2(\mathbb{F}_q^4)| = q^4 + q^3 + 2q^2 + q + 1 = (q^2 + 1)(q^2 + q + 1) \tag{3.14}$$

3.2   A Right Action on the Grassmannian

The left action of GL_r on Gr_r is trivial since the elements of Gr_r are the orbits of the action on $M_{r,m}^\circ$. However, letting $g \in \mathrm{GL}_m$ act by right multiplication

$$[M] \cdot g = [Mg]$$

gives a transitive right action of GL_m on Gr_r. We may also speak of the right action of GL_m on the general Grassmannian. In this case the orbits are Gr_i for $i = 0, 1, ..., m$.

We say two elements $X_1, X_2 \in \mathrm{Gr}$ *meet* if $X_1 \cap X_2 \neq \{0\}$. Representing X_1 and X_2 as row spaces of matrices $[X_1]$ and $[X_2]$, we have the following.

Proposition 12. $X_1, X_2 \in Gr$ *meet if and only if* $rank[X_1] + rank[X_2] > rank \begin{bmatrix} X_1 \\ X_2 \end{bmatrix}$.

The right action of GL_m on Gr_m is not k-transitive for any $k > 1$ and $1 < r < m - 1$. To see this, note that the action of GL_m on Gr commutes with intersections and direct sums.

$$(X_1 \cap X_2) \cdot g = (X_1 \cdot g) \cap (X_2 \cdot g) \text{ and } (X_1 \oplus X_2) \cdot g = (X_1 \cdot g) \oplus (X_2 \cdot g) \tag{3.15}$$

Letting $X_1 = \langle e_1, ..., e_r \rangle$, $X_2 = \langle e_2, e_3, ..., e_{r+1} \rangle$, and $X_2' = \langle e_3, e_4, ..., e_{r+2} \rangle$. We see $\dim X_1 \cap X_2 = r - 1$ and $\dim X_1 \cap X_2' = r - 2$ so $(X_1, X_2), (X_1, X_2') \in \mathrm{Gr}_2^2$ are necessarily elements of distinct orbits.

3.2.1 Orbits of Tuples of the Grassmannian

Many of the results in this section generalize, but we focus on the case $E = \mathbb{F}^4$ as this is fundamental to the main result.

As mentioned, the right action of GL_4 on Gr_2 is not 2-transitive. The action of GL_4 on $\mathrm{Gr}_2 \times \mathrm{Gr}_2$ has three orbits which are determined by the dimensions of the intersections.

Proposition 13. *There are three orbits of the right action of GL_4 on $Gr_2 \times Gr_2$. They have representatives* $(\langle e_1, e_2 \rangle, \langle e_3, e_4 \rangle)$, $(\langle e_1, e_2 \rangle, \langle e_1, e_3 \rangle)$, *and* $(\langle e_1, e_2 \rangle, \langle e_1, e_2 \rangle)$. *Further, if* $\mathbb{F} = \mathbb{F}_q$ *is a finite field, then*

$$\begin{aligned} |Orb((\langle e_1, e_2 \rangle, \langle e_3, e_4 \rangle))| &= q^4(q^2 + 1)(q^2 + q + 1) \\ |Orb((\langle e_1, e_2 \rangle, \langle e_1, e_3 \rangle))| &= q(q + 1)^2(q^2 + 1)(q^2 + q + 1) \\ |Orb((\langle e_1, e_2 \rangle, \langle e_1, e_2 \rangle))| &= (q^2 + 1)(q^2 + q + 1) \end{aligned} \tag{3.16}$$

25

Proof. Let $(X_1, X_2) \in \mathrm{Gr}_2 \times \mathrm{Gr}_2$. Then $\dim(X_1 \cap X_2) = 0, 1, 2$.

Suppose first $\dim(X_1 \cap X_2) = 0$. There exists $x_1, x_2 \in X_1$ and $x_3, x_4 \in X_2$ such that $X_1 = \langle x_1, x_2 \rangle$ and $X_2 = \langle x_3, x_4 \rangle$. Further, (x_1, x_2, x_3, x_4) is a basis for E since $E = X_1 \oplus X_2$. The linear transformation defined by $x_i \mapsto e_i$, shows this pair is in the orbit of $(\langle e_1, e_2 \rangle, \langle e_3, e_4 \rangle)$.

Next, suppose $\dim(X_1 \cap X_2) = 1$. There exists, $x_1 \in X_1 \cap X_2$, $x_2 \in X_1$ and $x_3 \in X_2$ such that $\langle x_1 \rangle = X_1 \cap X_2$, $\langle x_1, x_2 \rangle = X_1$, and $\langle x_1, x_3 \rangle = X_2$. Let $x_4 \in E - (X_1 \oplus X_2)$. The linear transformation defined by $x_i \mapsto e_i$ shows this pair is the orbit of $(\langle e_1, e_2 \rangle, \langle e_1, e_3 \rangle)$.

Finally, suppose $\dim(X_1 \cap X_2) = 2$. Then $X_1 = X_2$ and since the action on Gr is transitive, there is only one orbit for this pair. $\qquad\square$

Remark 3.2.1. We may also consider the action of GL_4 on unordered pairs $\{Y, Y'\}$ for $Y, Y' \in \mathrm{Gr}_2$. In this case, there are still only three orbits, the pairs where $Y = Y'$; the pairs where $Y \neq Y'$ but Y and Y' meet; and the pairs where Y and Y' do not meet.

Proposition 14. *Let* $U = \{(X_1, X_2, X_3) \in (\mathrm{Gr}_2)^3 : X_i$ *does not meet* X_j *for* $i \neq j\}$. *The action of* GL_4 *on* U *is transitive. The stabilizer of an element of* U *is isomorphic to* GL_2.

Proof. We show there exists a basis (x_1, x_2, x_3, x_4) for E such that $X_1 = \langle x_1, x_2 \rangle$, $X_2 = \langle x_3, x_4 \rangle$, and $X_3 = \langle x_1 + x_3, x_2 + x_4 \rangle$.

First, since X_1 does not meet X_2 and each are 2-dimensional, $E = X_1 \oplus X_2$. Since $X_3 \subset E$, there are vectors $x_1, x_2 \in X_1$ and $x_3, x_4 \in X_2$, such that $X_3 = \langle x_1 + x_3, x_2 + x_4 \rangle$. It remains to show that no $x_i = 0$. However, if any were 0, then X_3 necessarily meets either X_1 or X_2. This shows the action on U is transitive.

As there is only one orbit, we compute the stabilizer of the representative element

$$(X_1, X_2, X_3) = (\langle e_1, e_2 \rangle, \langle e_3, e_4 \rangle, \langle e_1 + e_3, e_2 + e_4 \rangle) \tag{3.17}$$

Representing these X_i as the row span of 2×2 matrices we have

$$[X_1] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \; ; \; [X_2] = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \; ; \; [X_3] = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \tag{3.18}$$

We represent an element of $g \in \mathrm{GL}_4$ in 2×2 blocks A, B, C, D

$$g = \begin{bmatrix} A & B \\ C & D \end{bmatrix}. \tag{3.19}$$

First we find $g \in \mathrm{GL}_4$ which fix the first component. Since

$$[X_1] \cdot g = \begin{bmatrix} I & 0 \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} A & B \end{bmatrix}, \tag{3.20}$$

the matrix A must be invertible, To row reduce $\begin{bmatrix} A & B \end{bmatrix}$, we multiply on the right by A^{-1} and see that $\begin{bmatrix} I & A^{-1}B \end{bmatrix}$ must equal $\begin{bmatrix} I & 0 \end{bmatrix}$ so B is the zero matrix.

By a similar computation and argument for the second component, we conclude C is the zero matrix and D is invertible. Putting both of these conditions together, we see that $g \in \mathrm{Stab}_{\mathrm{GL}_4}(X_1, X_2, X_3)$ must have the form

$$g = \begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix}. \tag{3.21}$$

Such an element must also fix the third component.

$$[X_3] \cdot g = \begin{bmatrix} I & I \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix} = \begin{bmatrix} A & D \end{bmatrix} \tag{3.22}$$

which is row equivalent to $\begin{bmatrix} I & I \end{bmatrix}$ if and only if $A = D$. $\qquad\qquad\square$

Notice $|\mathrm{Gr}_2^3| = (q^4 + q^3 + 2q^2 + q + 1)^3$ has leading term q^{12} and $|U| = \frac{|\mathrm{GL}_4|}{|\mathrm{GL}_2|} = q^{12} - q^9 - q^8 + q^5$. Thus as $q \to \infty$, the probability a random element of Gr_2^3 belongs to U approaches 1.

Proposition 15. *Let $U \subset (Gr_2)^4$ consist of the quadruples (X_1, X_2, X_3, X_4) such that X_1, X_2, X_3 pairwise do not meet and X_1, X_2, X_4 pairwise do not meet. The orbits of the GL_4 on U are in one-to-one correspondence with the similarity classes of GL_2.*

Proof. We have at least one representative of any orbit of U of the form

$$\left(\begin{bmatrix} I & 0 \end{bmatrix}, \begin{bmatrix} 0 & I \end{bmatrix}, \begin{bmatrix} I & I \end{bmatrix}, \begin{bmatrix} I & M \end{bmatrix} \right) \tag{3.23}$$

where $M \in \mathrm{GL}_2$. The first three components of 3.2.1 follow from Proposition 14. The fourth component must be the row span of some full rank RREF 2×4 matrix. If the leading ones did not occur in the first two columns, then the fourth component would necessarily intersect the second.

To see $M \in \mathrm{GL}_2$, suppose otherwise. Then M would row reduce to a matrix M' of the form $\begin{bmatrix} 1 & * \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, or $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Let $g \in \mathrm{GL}_2$, be a matrix which puts M into one of these forms. Then M is row equivalent to

$$g \cdot \begin{bmatrix} I & M \end{bmatrix} = \begin{bmatrix} g & M' \end{bmatrix} \tag{3.24}$$

since the bottom row of M' consists of zeros, the bottom row of the overall matrix is seen to meet X_1. Thus M must be invertible.

We let the stabilizer of the first three components act on the fourth component and we

remain in the same orbit. Thus $X_4 = \begin{bmatrix} I & M \end{bmatrix}$ is in the same orbit as

$$g^{-1} \begin{bmatrix} I & M \end{bmatrix} \begin{bmatrix} g & 0 \\ 0 & g \end{bmatrix} = \begin{bmatrix} I & g^{-1}Mg \end{bmatrix} \tag{3.25}$$

for any $g \in \mathrm{GL}_2$. Thus we see the orbits are in one-to-one correspondence with the similarity classes of GL_2 as claimed. $\qquad\square$

Given $(X_1, X_2, X_3, X_4) \in U$, we may choose a distinguished representative of the form (3.2.1) where M is in rational canonical form. The stabilizer of (X_1, X_2, X_3, X_4) has the same size as the stabilizer of M with respect to the action of conjugation.

The next proposition describes all orbits of Gr_2^3. The sizes of these orbits allow for an efficient computation of the exact counts of the number of ways exactly two lines meet four.

Proposition 16. *Let GL_4 act on $(Gr_2(\mathbb{F}^4))^3$. There are 17 orbits of this action. The tables below provides a representative of each orbit, as well as the stabilizer of the representative.*

O_i	X_3	Stabilizer		$|\text{Stab}_{\text{GL}_4}|$	$|O_i|$
O_1	$\langle e_1 + e_3, e_2 + e_4 \rangle$	$\begin{bmatrix} a_1 & a_2 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ 0 & 0 & a_1 & a_2 \\ 0 & 0 & b_1 & b_2 \end{bmatrix}$		$(q^2-1)(q^2-q)$	$q^5(q+1)(q-1)^2|\text{Gr}_2|$
O_2	$\langle e_1, e_2 + e_3 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ 0 & 0 & b_2 & 0 \\ 0 & 0 & d_3 & d_4 \end{bmatrix}$		$q^2(q-1)^3$	$q^4(q+1)^2(q-1)|\text{Gr}_2|$
O_3	$\langle e_3, e_1 + e_4 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & a_1 \end{bmatrix}$		$q^2(q-1)^3$	$q^4(q+1)^2(q-1)|\text{Gr}_2|$
O_4	$\langle e_1, e_3 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & d_4 \end{bmatrix}$		$q^2(q-1)^4$	$q^4(q+1)^2|\text{Gr}_2|$
O_5	$\langle e_1, e_2 \rangle$	$\begin{bmatrix} a_1 & a_2 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ 0 & 0 & c_3 & c_4 \\ 0 & 0 & d_3 & d_4 \end{bmatrix}$		$(q^2-1)^2(q^2-q)^2$	$q^4|\text{Gr}_2|$
O_6	$\langle e_3, e_4 \rangle$	$\begin{bmatrix} a_1 & a_2 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ 0 & 0 & c_3 & c_4 \\ 0 & 0 & d_3 & d_4 \end{bmatrix}$		$(q^2-1)^2(q^2-q)^2$	$q^4|\text{Gr}_2|$

Table 3.1: *Orbit size and stabelizer of* (X_1, X_2, X_3) *where* $X_1 = \langle e_1, e_2 \rangle$ *and* $X_2 = \langle e_3, e_4 \rangle$

O_i	X_3	Stabilizer	$|\text{Stab}_{\text{GL}_4}|$	$|O_i|$
O_7	$\langle e_2 + e_3, e_4 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ -b_1 & 0 & b_2 & 0 \\ 0 & d_2 & d_2 & d_4 \end{bmatrix}$	$q^2(q-1)^3$	$q^4(q+1)^2(q-1)|\text{Gr}_2|$
O_8	$\langle e_3, e_4 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & d_4 \end{bmatrix}$	$q^2(q-1)^4$	$q^4(q+1)^2|\text{Gr}_2|$
O_9	$\langle e_2, e_4 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ 0 & b_2 & 0 & 0 \\ c_1 & 0 & c_3 & 0 \\ 0 & d_2 & 0 & d_4 \end{bmatrix}$	$q^2(q-1)^4$	$q^4(q+1)^2|\text{Gr}_2|$
O_{10}	$\langle e_1, e_4 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ c_1 & 0 & c_3 & 0 \\ d_1 & 0 & 0 & d_4 \end{bmatrix}$	$q^3(q-1)^4$	$q^3(q+1)^2|\text{Gr}_2|$
O_{11}	$\langle e_2, e_3 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ 0 & b_2 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ d_1 & d_2 & d_3 & d_4 \end{bmatrix}$	$q^3(q-1)^4$	$q^3(q+1)^2|\text{Gr}_2|$
O_{12}	$\langle e_1, e_2 + e_3 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ c_1 & 0 & b_2 & 0 \\ d_1 & d_2 & d_3 & d_4 \end{bmatrix}$	$q^5(q-1)^3$	$q(q+1)^2(q-1)|\text{Gr}_2|$
O_{13}	$\langle e_1, e_3 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ c_1 & 0 & c_3 & 0 \\ d_1 & d_2 & d_3 & d_4 \end{bmatrix}$	$q^5(q-1)^4$	$q(q+1)^2|\text{Gr}_2|$
O_{14}	$\langle e_1, e_2 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ c_1 & 0 & c_3 & 0 \\ d_1 & d_2 & d_3 & d_4 \end{bmatrix}$	$q^5(q-1)^4$	$q(q+1)^2|\text{Gr}_2|$

Table 3.2: *Orbit size and stabelizer of* (X_1, X_2, X_3) *where* $X_1 = \langle e_1, e_2 \rangle$ *and* $X_2 = \langle e_1, e_3 \rangle$

O_i	X_3	Stabilizer	$|\text{Stab}_{\text{GL}_4}|$	$|O_i|$
O_{15}	$\langle e_3, e_4 \rangle$	$\begin{bmatrix} a_1 & a_2 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ 0 & 0 & c_3 & c_4 \\ 0 & 0 & d_3 & d_4 \end{bmatrix}$	$(q^2-1)^2(q^2-q)^2$	$q^4|\text{Gr}_2|$
O_{16}	$\langle e_1, e_3 \rangle$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ c_1 & 0 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{bmatrix}$	$(q-1)^4 q^5$	$q(q+1)^2|\text{Gr}_2|$
O_{17}	$\langle e_1, e_2 \rangle$	$\begin{bmatrix} a_1 & a_2 & 0 & 0 \\ b_1 & b_2 & 0 & 0 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{bmatrix}$	$q^4(q^2-1)^2(q^2-q)^2$	$|\text{Gr}_2|$

Table 3.3: *Orbit size and stabelizer of* (X_1, X_2, X_3) *where* $X_1 = X_2 = \langle e_1, e_2 \rangle$

Proof. The verification of the stated stabilizers is a simple. We have $\sum |O_i| = |\text{Gr}_2|^3$. It remains to show the listed orbits are distinct. For $i \neq j$, we may distinguish O_i from O_j by noticing $|O_i| \neq |O_j|$ for most pairs (i, j). We analyze the cases where $|O_i| = |O_j|$ below.

To distinguish O_{13}, O_{14}, and O_{16}, notice that the second and third components of O_{13} are equal, while the first and third components of O_{14} are equal, and the first and second components of O_{16} are equal. Similar reasoning distinguishes O_5, O_6, O_{15}. To distinguish O_2, O_3, O_7, notice the first and third components of O_2 meet, while the second and third components of O_3 meet, while the first and second components of O_7 meet. Similar reasoning distinguishes O_4, O_8, O_9. The triples of orbits just distinguished form a single orbit if we allow $S_3 \times \text{GL}_4$ to act on Gr_2^3. This allows a shortcut in computational methods.

Finally, to distinguish O_{10} from O_{11}, notice the components of O_{10} span $\mathbb{F}^4$ while the components of O_{11} span a 3-dimensional subspace. $\square$

3.3   Projective Spaces and Projective Geometry

Projective space $\mathbb{P}(E)$ is the set of equivalences classes of $E - \{0\}$ under the equivalence relation $\sim$, where $v \sim w$ if there exists $c \in \mathbb{F}^\times$ such that $v = cw$. As E is m-dimensional and isomorphic to all other vector spaces of dimension m over $\mathbb{F}$, we speak of *projective*

$(m-1)$-*space* and denote it $\mathbb{FP}^{m-1}$. Projective space is the Grassmannian of 1-planes, i.e. $\mathbb{FP}^{m-1} = \mathrm{Gr}_1$.

The projective points of $\mathbb{FP}^3$ are lines through the origin in $\mathbb{F}^4$. If we fix the hyperplane $H_1 = \{(1, x_2, x_3, x_4) \in \mathbb{F}^4\}$, most projective points intersect H_1. Those projective points which do not intersect H_1 are contained in the hyperplane $K_1 = \{(0, x_2, x_3, x_4)\})$, and most of these projective points intersect the plane $H_2 = \{(0, 1, x_3, x_4)\}$ a "projective plane a infinity". The projective points that do not intersect H_1 or H_2, intersect either $H_3 = \{(0, 0, 1, x_4) \in \mathbb{F}^4\}$ a "projective line at infinity" or $H_4 = \{(0, 0, 0, 1)\}$ a "projective point at infinity".

The figure below shows the analogous picture for $\mathbb{FP}^2$. We have two red lines through the origin (points in the Grassmannian). One of the red lines meets the blue plane at a point labelled $[1 : y : z]$. The other red line meets the 'line at infinity' at a point labelled $[0, 1, z]$. The z-axis is the line represented by the point at infinity labelled $[0, 0, 1]$. We note there is distinguished about these 'points at infinity.' If we chose a different reference plane, some or all of the points at infinity could meet the new reference frame.
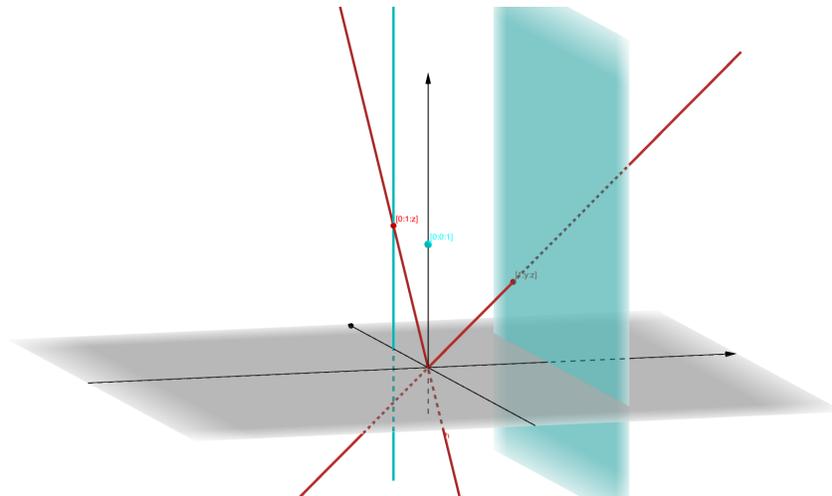

Figure 3.2: *Elements of Gr_2 (red lines through origin) meeting the affine plane $x = 1$ or the affine line $x = 0$ and $y = 1$ (line at infinity). The z axis is a line through the origin meeting the point at infinity.*

33

We use projective coordinates to describe the points in $\mathbb{FP}^{m-1}$. Since $\mathbb{FP}^3 = (E-\{0\})/\sim$, the points $(x_1, x_2, ..., x_m), (cx_1, cx_2, ..., cx_m) \in \mathbb{F}^m$ are equivalent for all $c \in \mathbb{F} - \{0\}$. We denote this equivalence class by $[x_1 : x_2 : \cdots : x_m]$ and sometimes omit the colons. Since not all x_i are 0, we made divide the projective coordinates by the leftmost x_n which is non-zero. Thus there is a unique representative of the equivalence class of the form

$$[0 : \cdots : 0 : 1 : \frac{x_{n+1}}{x_n} : \cdots : \frac{x_m}{x_n}] \tag{3.26}$$

which is simply the RREF of a $1 \times m$ matrix.

Given two distinct projective points $p_1, p_2 \in \mathbb{FP}^3$, there is a unique *projective line* containing p_1 and p_2. The projective line through p_1 and p_2 is the plane through the origin containing p_1 and p_2. If we view p_1 and p_2 as matrices, then the projective plane is described as the row span of p_1 and p_2. Thus projective planes are in one-to-one correspondance with Gr_2. In general, *projective $(r-1)$-planes in $\mathbb{FP}^{m-1}$* are in one-to-one correspondence with $Gr_r(\mathbb{F}^m)$.

3.4   The Four Lines Problem

In this subsection, let E be a vector space of dimension 4 over $\mathbb{F}_q$. Let $\mathcal{M}_q : (Gr_2)^4 \to \mathcal{P}(Gr_2)$ be given by

$$(X_1, X_2, X_3, X_4) \mapsto \{Y \in Gr_2 : X_i \text{ meets } Y \text{ for all } i\} \tag{3.27}$$

We call such a 4-tuple $(X_1, X_2, X_3, X_4) \in (Gr_2)^4$ *perfect* if $|\mathcal{M}_q(X_1, X_2, X_3, X_4)| = 2$. We call a 4-tuple *horrible* if $|\mathcal{M}_q(X_1, X_2, X_3, X_4)| = 0$. Let P_q denote the set of perfect 4-tuples and H_q denote the set of horrible 4-tuples.

Theorem 17. *Let E be a vector space of dimension 4 over $\mathbb{F}_q$, then*

$$\lim_{q \to \infty} \frac{|P_q|}{|Gr_2^4|} = \lim_{q \to \infty} \frac{|H_q|}{|Gr_2^4|} = \frac{1}{2}. \tag{3.28}$$

That is to say, the probabilities of random element of $(Gr_2)^4$ is perfect or horrible each asymptotically approach $\frac{1}{2}$.

Proof. Let $\mathcal{M}_q$ be as defined above. We shall restrict $\mathcal{M}_q$ to the subset $U \subset (Gr_2)^4$ of Proposition 15 and show that

$$\lim_{q \to \infty} \frac{|P_q \cap U|}{|Gr_2^4|} = \lim_{q \to \infty} \frac{|H_q \cap U|}{|Gr_2^4|} = \frac{1}{2}. \tag{3.29}$$

Since the limits in (3.29) are a lower bound for the limits (3.28) and the limits sum to 1; this will prove the theorem.

First, note that $|\mathcal{M}(X)|$ is constant on each orbit of U, since

$$\mathcal{M}(X_1, X_2, X_3, X_4) \cdot g = \mathcal{M}(X_1 \cdot g, X_2 \cdot g, X_3 \cdot g, X_4 \cdot g). \tag{3.30}$$

We compute $|\mathcal{M}(X)|$ on the distinguished representative of each orbit.

The 2-planes in Gr_2 which meet X_1, X_2, X_3 are

$$Y_t = \begin{bmatrix} 1 & t & 0 & 0 \\ 0 & 0 & 1 & t \end{bmatrix}; \quad Y_\infty = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.31}$$

for $t \in \mathbb{F}_q$. We may test which of these subspaces meets X_4 by stacking the matrices Y_t and X_4. If the determinant of the matrix is 0, the spaces X_4 and Y_t meet. First, if M is the identity matrix, then $X_3 = X_4$ and X_4 meets Y_t for all $t \in \mathbb{F}_q \cup \{\infty\}$. Now suppose M is not the identity matrix. If $t \in \mathbb{F}_q$, then the determinant of $\begin{bmatrix} X_4 \\ Y_t \end{bmatrix}$ is $-c_M(t)$, the negative of the characteristic polynomial of M. When $t = \infty$, the determinant is -1. Thus the number of lines meeting the four is the number of solutions to $c_M(t) = 0$ over the field $\mathbb{F}_q$.

We have

$$P_q \cap U = \bigcup_{f \in \mathcal{F}_q} \mathrm{Orb}(C_f)$$

$$H_q \cap U = \bigcup_{f \in \mathcal{I}_q} \mathrm{Orb}(C_f)$$

(3.32)

As $|\mathrm{Orb}(()C_f)| = |\mathrm{Orb}(()C_g)|$ if $f, g \in \mathcal{F}_q$ or if $f, g \in \mathcal{I}_q$. Since GL_4 is acting and has order $(q^4 - 1)(q^4 - q)(q^4 - q^2)(q^4 - q^3)$ we have

$$\mathrm{Orb}(C_f) = \frac{|\mathrm{GL}_4|}{|\mathrm{Stab}C_f|} = \begin{cases} \frac{(q^4-1)(q^4-q)(q^4-q^2)(q^4-q^3)}{(q-1)^2} & \text{if } f \in \mathcal{F}_q \\[2ex] \frac{(q^4-1)(q^4-q)(q^4-q^2)(q^4-q^3)}{(q+1)(q-1)} & \text{if } f \in \mathcal{I}_q \end{cases}$$

(3.33)

Multiplying the above quantities by the number of each type of orbit we have

$$|P_q \cap U| = \frac{(q-1)(q-2)(q^4-1)(q^4-q)(q^4-q^2)(q^4-q^3)}{2(q-1)^2}$$

$$|H_q \cap U| = \frac{q(q-1)(q^4-1)(q^4-q)(q^4-q^2)(q^4-q^3)}{2(q+1)(q-1)}$$

(3.34)

The leading term of each is $\frac{1}{2}q^{16}$, while the leading term of $|(\mathrm{Gr}_2(\mathbb{F}_q^4))^4|$ is q^{16}. This shows the limits in (3.29) are as claimed. $\qquad\square$

4 Exact Counts

In this chapter, we find and prove an exact count of P_q.

$$|\mathcal{P}_q| = \tfrac{1}{2}q^7(q+1)^2(q^2+1)(q^2+q+1)(q^3+5q^2-q+1)$$
$$= \tfrac{1}{2}q^7(q^9+8q^8+19q^7+29q^6+33q^5+27q^4+17q^3+7q^2+2q+1)$$

(4.1)

The approach is different from the previous chapters. We define a function from 'bipartite labelings' of bipartite graphs with four edges and no isolated nodes to (unordered) instances of the four lines problems where the answer is at least two. We call those 'bipartite labelings' where the answer is two, perfect. We show the perfect bipartite labelings covers all elements of $\mathcal{P}$ and that the number of 'bipartite labelings' which map to the same element of $\mathcal{P}$ is the cardinality of the corresponding 'bipartite automorphism group'.

4.1 Bipartite Graphs

A *bipartite graph* consists of disjoints sets of nodes $\mathcal{A}$ and $\mathcal{B}$ along with a set of edges $\mathcal{E} \subset \mathcal{P}(\mathcal{A} \sqcup \mathcal{B})$ which are two element sets $\{v_1, v_2\}$ such that $|\{v_1, v_2\} \cap \mathcal{A}| = 1$ and $|\{v_1, v_2\} \cap \mathcal{B}| = 1$. A graph is called bipartite if there exists a bipartition of the nodes into sets $\mathcal{A}$ and $\mathcal{B}$ as above. Note that this bipartition is not unique unless the graphs is connected.

Given a bipartite graph $(\mathcal{A}, \mathcal{B}, \mathcal{E})$, define $\text{Bip}(\mathcal{A}, \mathcal{B}, \mathcal{E})$, the *bipartite automorphism group* of $\mathcal{G}$ to be the set of graph auotomorphisms ϕ such that $\phi(\mathcal{A}) = \mathcal{A}$ or $\phi(\mathcal{A}) = \mathcal{B}$. The next example highlights the difference between graph automorphisms and bipartite graph automorphisms.

Example 8. Consider the graph $\mathcal{G}$ below
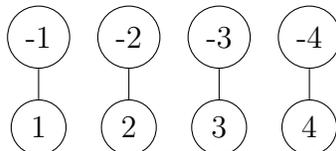
We have

$$\mathcal{G} = (\{-4, -3, -2, -1, 1, 2, 3, 4\}, \{\{-1, 1\}, \{-2, 2\}, \{-3, 3\}, \{-4, 4\}\}).$$

The set of graph automorphisms are the signed permutations of $1, 2, 3, 4$, which contains $2^4 \cdot 4! = 384$ elements. Notice $\mathcal{G}$ is bipartite with bipartition $\mathcal{A} = \{-1, -2, -3, -4\}$ and $\mathcal{B} = \{1, 2, 3, 4\}$. Then $\mathrm{Bip}(\mathcal{A}, \mathcal{B}, \mathcal{E}) \cong S_2 \times S_4$ has $2 \cdot 4! = 48$ elements. Thus not all graph automorphisms are bipartite graph automorphisms.

Notice also that the bipartite automorphism group depends on the chosen bipartition of the nodes, as the next example illustrates.

Example 9. Let $\mathcal{G} = (\{1, ..., 9\}, \{\{1, 7\}, \{2, 7\}, \{3, 8\}, \{4, 8\}, \{5, 9\}, \{6, 9\}\})$. Consider the bipartitions $A \sqcup B$ and $\mathcal{A}' \sqcup \mathcal{B}'$ of the nodes given by

$$\mathcal{A} = \{1, 2, 3, 4, 5, 6\}$$
$$\mathcal{B} = \{7, 8, 9\}$$
$$\mathcal{A}' = \{1, 2, 3, 4, 9\}$$
$$\mathcal{B}' = \{5, 6, 7, 8\}$$

each of which show $\mathcal{G}$ is a bipartite graph. If we draw the $\mathcal{G}$ with the nodes belonging to $\mathcal{A}$ above the nodes belonging to $\mathcal{B}$ we represent $\mathcal{G}$ as
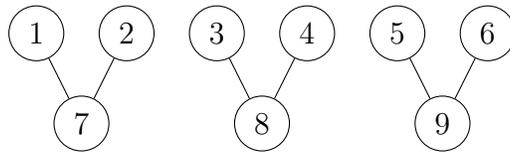
Note that $\mathrm{Bip}(\mathcal{A}, \mathcal{B}, \mathcal{E}) \cong S_3 \times S_2 \times S_2 \times S_2$, since permuting $\{7, 8, 9\}$ induces a permutation on $\{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$ and we may then permute the elements in each set.

However, if we draw the graph placing the nodes of $\mathcal{A}'$ above the nodes of $\mathcal{B}'$ we have
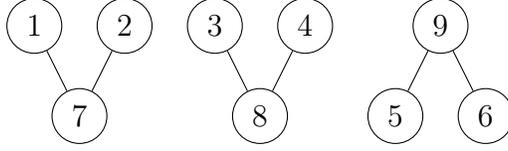
And we see $\mathrm{Bip}(\mathcal{A}', \mathcal{B}', \mathcal{E}) \cong S_2 \times S_2 \times S_2 \times S_2$ since permuting 7 and 8 induces a permutation on $\{\{1,2\}, \{3,4\}\}$ and 9 must remain fixed. Thus $\mathrm{Bip}(\mathcal{A}, \mathcal{B}, \mathcal{E}) \not\cong \mathrm{Bip}(\mathcal{A}', \mathcal{B}', \mathcal{E})$, though $(\mat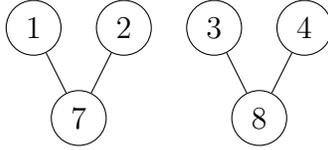hcal{A} \sqcup \mathcal{B}, \mathcal{E})$ and $(\mathcal{A}' \sqcup \mathcal{B}', \mathcal{E})$ represent the same graph.

As it will be important later, if we delete the nodes 5, 6, and 9 to form a new graph $\mathcal{G}'$.

the associated bipartitions $\mathcal{A} \sqcup \mathcal{B}$ and $\mathcal{A}' \sqcup \mathcal{B}'$ are identical and the bipartite automorphism group with respect to these bipartitions is $S_2 \times S_2 \times S_2$.

Further, if instead we delete the nodes 3, 4, and 8 to form a bipartite graph $\mathcal{G}''$, the associated bipartitions $\mathcal{A} \sqcup \mathcal{B}$ and $\mathcal{A}' \sqcup \mathcal{B}'$ are different. We demonstrate this by putting the nodes of $\mathcal{A}$ respectively of $\mathcal{A}'$ above and the nodes of $\mathcal{B}$ respectively $\mathcal{B}'$ below.

In both cases the bipartite automorphism groups are $S_2 \times S_2 \times S_2$. However, for every $\phi \in \mathrm{Bip}(\mathcal{A}, \mathcal{B}, \mathcal{G}'')$ we have $\phi(\mathcal{A}) = \mathcal{A}$. Whereas there exist bipartite automorphisms $\phi' \in \mathrm{Bip}(\mathcal{A}', \mathcal{B}', \mathcal{G}'')$ such that $\phi'(\mathcal{A}') = \mathcal{B}'$.

In what follows we will need to consider all bipartite graphs $(\mathcal{A}, \mathcal{B}, \mathcal{E})$ with four edges and no isolated nodes, as well as $\mathrm{Bip}(\mathcal{A}, \mathcal{B}, \mathcal{E})$. The table below provides an exhaustive list of such bipartite graphs, where the bipartition is given by taking $\mathcal{A}$ to be the set of nodes placed above and the nodes of $\mathcal{B}$ placed below. The table also provides a set of generators for their bipartite automorphism groups. The graphs $\mathcal{G}_3$ and $\mathcal{G}_9$ were analyzed in the last example.
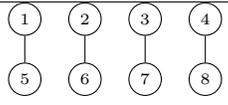
i	$\mathcal{G}_i$	$\mathrm{Bip}(\mathcal{G}_i)$	$|\mathrm{Bip}(\mathcal{G}_i)|$
1		$\langle(12)(56),(13)(57),(14)(58),(15)(26)(37)(48)\rangle$	48
2		$\langle(32),(14)(57)\rangle$	4
3		$\langle(14),(13)(24)(56)\rangle$	8
4		$\langle(12)(56)\rangle$	2
5		$\langle(15)(27)(36)\rangle$	2
6		$\langle(12),(15)(26)\rangle$	8
7		$\langle(23)\rangle$	2
8		$\langle(12),(13),(14)\rangle$	24
9		$\langle(23),(16)(25)(37)\rangle$	8
10		$\langle(23),(24)\rangle$	6
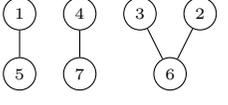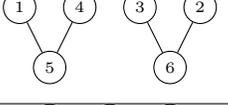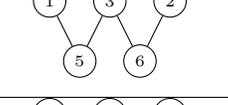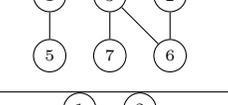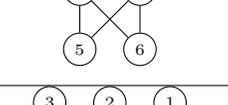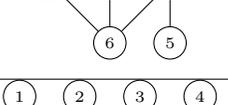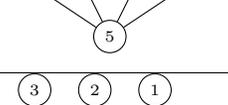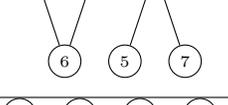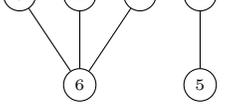
Table 4.1: *Each graph $\mathcal{G}_i$ has bipartition $\mathcal{A}_i \subseteq \{1,2,3,4\}$ and $\mathcal{B}_i \subseteq \{5,6,7,8\}$. $\mathrm{Bip}(\mathcal{G}_i)$ is given by a set of generators of S_8 using cycle notation.*

To end this section we provide a definition of a bipartite labelling of a bipartite graph. We shall use certain bipartite labelings by elements of Gr_2 to find the exact counts. Let $(\mathcal{A},\mathcal{B},\mathcal{E})$ be a bipartite graph and $(\mathcal{C},\mathcal{D})$ be a pair of sets. Let $\alpha : \mathcal{A} \to \mathcal{C}$ and $\beta : \mathcal{B} \to \mathcal{D}$ be injections, then we call (α,β) a *bipartite labelling* of $(\mathcal{A},\mathcal{B},\mathcal{E})$ by $(\mathcal{C},\mathcal{D})$. That is, we label

the nodes of $\mathcal{A}$ by elements of $\mathcal{C}$ and the nodes of $\mathcal{B}$ by elements of $\mathcal{D}$.

4.2 The Correspondence

Recall $\mathcal{M} : \mathrm{Gr}_2^4 \to \mathcal{P}(\mathrm{Gr}_2)$ sends (X_1, X_2, X_3, X_4) to those set of 2-planes which meet each X_i. Notice, that $\mathcal{M}$ is invariant under any permutation of the components (X_1, X_2, X_3, X_4). To simplify matters, let $\mathcal{IS}$ be the function from the 4-elements subsets $\{X_1, X_2, X_3, X_4\}$ to the elements of Gr_2 which meet each X_i.

We shall compute the preimage of $\{Y, Y'\}$ under $\mathcal{IS}$. First we show that if Y and Y' meet, then $\mathcal{IS}^{-1}(\{Y, Y'\}) = \{\}$. Thus if $\{Y, Y'\} \in \mathrm{Im}(\mathcal{IS})$ then Y and Y' do not meet.

Proposition 18. $\mathcal{IS}^{-1}(\{Y, Y'\}) = \{\}$ *if* Y *and* Y' *meet.*

Proof. Let $Y, Y' \in \mathrm{Gr}_2$ meet. Then there exists $y_1, \in Y - Y'$, $y_2 \in Y' - Y$, and $y_3 \in Y \cap Y'$, such that $Y = \langle y_1, y_3 \rangle$ and $Y' = \langle y_2, y_3 \rangle$. Let $X_1, X_2, X_3, X_4 \in \mathrm{Gr}_2$ all met Y and Y'. Then for each X_i, either $y_3 \in X_i$ or $X_i = \langle y_1 + a_i y_3, y_2 + b_i y_3 \rangle$ for some $a_i, b_i \in \mathbb{F}$. Consider $Y'' = \langle y_1 + y_2, y_3 \rangle$. Notice Y'' is distinct from Y and Y'', but meets all X_i. Thus $\{Y_1, Y', Y''\} \subset \mathcal{M}(\{X_1, X_2, X_3, X_4\}) \neq \{Y, Y'\}$. $\qquad\square$

Thus if $\{Y, Y'\}$ is in the image of $\mathcal{IS}$, Y and Y' do not meet. Let $X_1, X_2, X_3, X_4 \in \mathrm{Gr}_2$ be distinct and each meet Y and Y', then

$$\begin{aligned} X_i \cap Y &= \langle y_i \rangle \\ X_i \cap Y' &= \langle y_i' \rangle \end{aligned} \tag{4.2}$$

for some nonzero $y_i \in Y$ and $y_i' \in Y'$. Note that neither $\langle y_1 \rangle, ..., \langle y_4 \rangle$ nor $\langle y_1' \rangle, ..., \langle y_4' \rangle$ are necessarily distinct. Each $\{X_1, X_2, X_3, X_4\}$ meeting Y and Y' correspond to a bipartite labelling by $(\mathrm{Gr}_1(Y), \mathrm{Gr}_1(Y'))$ of exactly one of the graphs $\mathcal{G}_i$. Each X_i is represented by an edge of the graph as the direct sum of the labels of the nodes it connects. For example, if all $\langle y_i \rangle$ and all $\langle y_i' \rangle$ are distinct, this corresponds to the graph $\mathcal{G}_1$. We necessarily have $\{Y, Y'\} \subseteq \mathcal{IS}(\{X_1, X_2, X_3, X_4\})$, it remains to consider whether any other $Y'' \in \mathrm{Gr}_2$ meets

all X_i. If no such Y'' exists, we call the bipartite labelling *perfect* and (X_1, X_2, X_3, X_4) is a perfect 4-tuple. The next lemma will help us to determine which bipartite labelings of the graphs $\mathcal{G}_i$ are perfect.

Proposition 19. *Let $Y \in Gr_2$. And (Y_1, Y_2, Y_3, Y_4) be a 4-tuple of distinct elements of $Gr_1(Y)$, then there exists a non-unique basis (v, w) for Y and a unique $t \in \mathbb{F} - \{0, 1\}$ such that*

$$
\begin{aligned}
Y_1 &= \langle v \rangle \\
Y_2 &= \langle w \rangle \\
Y_3 &= \langle v + w \rangle \\
Y_4 &= \langle v + tw \rangle.
\end{aligned}
$$

(4.3)

Proof. Let Y_1, Y_2, Y_3, Y_4 be distinct elements of $Gr_1(Y)$. Since $Y = Y_1 \oplus Y_2$, we have $Y_1 = \langle v' \rangle$ and $Y_2 = \langle w' \rangle$ for some $v' \in Y_1$ and $w' \in Y_2$. Since Y_3 is a subspace of Y, there exists non-zero $a, b, c, d \in \mathbb{F}$ such that $Y_3 = \langle av' + bw' \rangle$ and $Y_4 = \langle cv' + dw' \rangle$. Further, since $Y_3 \neq Y_4$, $ad - bc \neq 0$.

Notice $Y_3 = \langle v' + \frac{b}{a}w' \rangle$ and $Y_4 = \langle v' + \frac{d}{c}w' \rangle$. Letting $v = v'$ and $w = \frac{b}{a}w'$, we have desired basis with $t = \frac{ad}{bc}$. Since a, b, c, d are non-zero and $ad \neq bc$, t cannot equal 0 or 1. $\square$

Suppose we are given a bipartite labelling (α, β) by $(Gr_1(Y), Gr_1(Y'))$ of a graph. Then we may choose a basis (v, v', w, w') such that $Y = \langle v, w \rangle$ and $Y' = \langle v', w' \rangle$ and

$$
\begin{aligned}
\alpha(1) &= \langle v \rangle & \beta(5) &= \langle v' \rangle \\
\alpha(2) &= \langle w \rangle & \beta(6) &= \langle w' \rangle \\
\alpha(3) &= \langle v + w \rangle & \beta(7) &= \langle v' + w' \rangle \\
\alpha(4) &= \langle v + tw \rangle & \beta(8) &= \langle v' + t'w' \rangle
\end{aligned}
$$

(4.4)

for some $t, t' \in \mathbb{F}_q - \{0, 1\}$. If $\mathcal{G}$ has fewer than 8 nodes, we ignore the extraneous outputs of the functions. With respect to such a basis, the matrices representing $X_1, X_2, X_3, X_4, Y, Y'$ are particularly simple.

Suppose we have a bipartite graph $\mathcal{G} = (\mathcal{A}, \mathcal{B}, \mathcal{E})$ and a bipartite labelling (α, β) by a pair $(\mathrm{Gr}_1(Y), \mathrm{Gr}_1(Y'))$ where $Y, Y' \in \mathrm{Gr}_2$ do not meet. To this data we may associate a four element subset of $\{X_1, X_2, X_3, X_4\} \subset \mathrm{Gr}_2$ by taking each edge $\{Y_i, Y_i'\} \in \mathcal{E}$ to $X_i = Y_i \oplus Y_i'$ for $i = 1, 2, 3, 4$. By construction we have

$$\{Y, Y'\} \subseteq \mathcal{M}(\{X_1, X_2, X_3, X_4\})$$

with equality if and only if there does not exist $Y'' \in \mathrm{Gr}_2$ distinct from Y and Y' which meets all X_i. We call this bipartite labelling *perfect*. In this case all $4! = 24$ permutations of (X_1, X_2, X_3, X_4) are perfect. However, any bipartite automorphism of $\mathcal{G}$ gives rise to the same set $\{X_1, X_2, X_3, X_4\}$.

Proposition 20. *If $i = 7, 8, 9, 10$, then all bipartite labelings of $\mathcal{G}_i$ by $(Gr_1(Y), Gr_1(Y')$ are not perfect.*

Proof. For $i = 7, 9, 10$, notice $Y'' = \alpha(1) \oplus \beta(6)$ meets all X_i. For $i = 8$, notice each X_i meets all X_j. $\square$

With one technical exception for $\mathcal{G}_1$, we shall show all other bipartite labelings of $\mathcal{G}_i$ by $(\mathrm{Gr}_1(Y), \mathrm{Gr}_1(Y'))$ are perfect for $i = 1, 2, 3, 4, 5, 6$.

First, with respect to the basis (v, v', w, w'), the RREF matrices representing Y and Y' are

$$[Y] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \text{ and } [Y'] = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.5}$$

The graphs $\mathcal{G}_i$ were carefully labelled so that all graphs contain the edges $\{1, 5\}$ and $\{2, 6\}$. Thus with respect to the basis (v, w, v', w') we may assume the matrices representing X_1 and X_2 are

$$[X_1] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \text{ and } [X_2] = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{4.6}$$

Any $Y'' \in \text{Gr}_2$ meeting X_1 and X_2 is non-uniquely represented by a matrix of the form

$$[Y''] = \begin{bmatrix} a & a' & 0 & 0 \\ 0 & 0 & b & b' \end{bmatrix} \tag{4.7}$$

for some $a, b, a', b' \in \mathbb{F}_q$. First note if $a = a' = 0$ or $b = b' = 0$, then $[Y'']$ is not full rank and does not represent an element of Gr_2. If $a = b = 0$, then $[Y'']$ is row equivalent to $[Y']$. Likewise if $a' = b' = 0$, then Y'' is row equivalent to $[Y]$. We call any of these cases *trivial*.

Proposition 21. *The bipartite labelings of $\mathcal{G}_1$ are perfect if and only if $t \neq t'$.*

Proof. The matrices of X_3 and X_4 are

$$[X_3] = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \text{ and } [X_4] = \begin{bmatrix} 1 & 0 & t & 0 \\ 0 & 1 & 0 & t' \end{bmatrix} \tag{4.8}$$

We stack the matrices $[X_3]$ and $[X_4]$ on $[Y'']$. If the determinant of both of these matrices is 0, then Y'' meets all X_i. In this case we have

$$\det \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ a & a' & 0 & 0 \\ 0 & 0 & b & b' \end{bmatrix} = a'b - ab' \tag{4.9}$$

and

$$\det \begin{bmatrix} 1 & 0 & t & 0 \\ 0 & 1 & 0 & t' \\ a & a' & 0 & 0 \\ 0 & 0 & b & b' \end{bmatrix} = a'bt' - ab't \tag{4.10}$$

Thus Y'' meets all X_i when $a'b - ab' = 0$ and $a'bt' - ab't = 0$. The first equation says $a'b = ab'$. If $a'b \neq 0$, this implies $t = t'$. If $a'b = ab' = 0$, then we must have a trivial solution. This

means there exists $Y'' \in \text{Gr}_2$ distinct from Y, Y' if and only if $t = t'$. $\qquad\square$

Proposition 22. *All bipartite labelings of $\mathcal{G}_i$ by $(Gr_1(Y), Gr_1(Y'))$ are perfect for $i =$*
2, 3, 4, 5, 6.

Proof. For $i = 2, 3, 4, 5$, all $\mathcal{G}_i$ contain the edge $\{3, 6\}$ so we have

$$[X_3] = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.11}$$

For Y'' to meet X_3 we must have

$$\det \begin{bmatrix} X_3 \\ Y'' \end{bmatrix} = a'b = 0 \tag{4.12}$$

For $i = 6$, we let X_3 correspond to the edge $\{1, 6\}$. In which case

$$[X_3] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.13}$$

Conveniently, this results in the same determinant as (4.12).

To conclude the proof, we form X_4 from the remaining edge of $\mathcal{G}_i$. The table below shows the matrix representing X_4 as well the $\det \begin{bmatrix} X_4 \\ Y'' \end{bmatrix}$.

i	$[X_4]$	det
2	$\begin{bmatrix} 1 & 0 & t & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$	$a'b - ab't$
3	$\begin{bmatrix} 1 & 0 & t & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$	$-ab't$
4	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$	$-ab'$
5	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$	$a'b - ab'$
6	$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$	$-ab'$

45

For each of the above determinants to simultaneously be 0 along with the determinant ab' from X_3, the solutions (a, a', b, b') are necessarily trivial so no $Y'' \in \mathrm{Gr}_2 - \{Y, Y'\}$ meets all X_i. All bipartite labelings of these graphs are perfect. $\qquad \square$

Theorem 23. *If $Y, Y' \in Gr_2$ do not meet, then*

$$|\mathcal{IS}^{-1}(\{Y, Y'\})| = \frac{1}{48}q^3(q+1)^2(q^3 + 5q^2 - q + 1) \qquad (4.14)$$

Proof. The number of bipartite labelings of $\mathcal{G}_1$ by $(\mathrm{Gr}_1(Y), \mathrm{Gr}_1(Y')$ is

$$\frac{(q+1)!}{(q+1-4)!} \frac{(q+1)!}{(q+1-4)!}. \qquad (4.15)$$

To each bipartite labelling we may find a unique $(t, t') \in \mathbb{F}_q - \{0, 1\}$ as in Proposition 19, and the biparite labelling is perfect if and only if $t \neq t'$. Thus $(q-3)/(q-2)$ of these labelings are perfect. As stated earlier, two bipartite labelings correspond to the same $\{X_1, X_2, X_3, X_4\}$ if and only if there is a bipartite automorphism between them. We divide the number of perfect bipartite labelings of $\mathcal{G}_1$ by $\mathrm{Bip}(\mathcal{G}_1) = 48$ to obtain the number of elements in $\mathcal{M}^{-1}(\{Y, Y'\})$ whose associated bipartite graph is isomorphic to $\mathcal{G}_1$

$$\frac{(q-3)(q+1)!(q+1)!}{48(q-2)(q-3)!(q-3)!} \qquad (4.16)$$

For $i = 2, 3, 4, 5, 6$, since every bipartite labelling of $\mathcal{G}_i$ is perfect, the number of elements in $\mathcal{M}^{-1}(\{Y, Y'\})$ whose associated bipartite graph is isomorphic to $\mathcal{G}_i$ is given by

$$\frac{1}{|\mathrm{Bip}(\mathcal{G}_i)|} \frac{(q+1)!}{(q+1-|\mathcal{A}_i|)!} \frac{(q+1)!}{(q+1-|\mathcal{B}_i|)!} \qquad (4.17)$$

Summing these expressions for $i = 2, 3, 4, 5, 6$ along with (4.16). Gives the desired result. $\quad \square$

Corollary 24. $|\mathcal{P}_q| = \frac{1}{2}q^3(q+1)^2(q^2 + 1)(q^2 + q + 1)(q^3 + 5q^2 - q + 1)$

Proof. We multiply (4.14) by $24q^4(q^2 + q + 1)(q^2 + 1)$ since there are 24 ordered 4-tuples of

a 4 element set and there are $q^4(q^2 + q + 1)(q^2 + 1)$ choices for $\{Y, Y'\} \subset \text{Gr}_2$ such that Y and Y' do not meet. $\qquad \square$

5   Appendix

5.1   Mathematica code

In this section, we verify the exact counts in the previous section using Mathematica. We first present a brute force approach to verify the counts for the cases $q = 2, 3$. We then take advantage of the action of GL_4 on Gr_2^3 to greatly improve efficiency to check the cases for all primes less than 19.

We provide wall clock run times for all computations using Wolfram Mathematica 12.0 Student Edition with an Intel Core i5-3470 3.2GHz Quad-Core processor.

First, we create a user-defined function $\mathcal{IS}[X, S]$ which accepts as inputs $X \in \mathrm{Gr}_2$ and $S \subseteq \mathrm{Gr}_2$ and returns those elements of S which meet X.

```
1  IS[X_, S_] :=
2   Module[{T = {}, i},
3     If[Length[S] > 0,
4       For[i = 1, i <= Length[S], i++,
5         If[MatrixRank[Join[X, S[[i]]], Modulus -> q] < 4,
6          AppendTo[T, S[[i]]]
7          ]
8         ]
9       ];
10     T
11    ]
```

Listing 5.1: The Intersection Set Function

After assigning a prime value to q, the following code generates $\mathrm{Gr}_2(\mathbb{F}_q^4)$, by creating all full rank RREF matrices.

```
1  Gr = {{{0, 0, 1, 0}, {0, 0, 0, 1}}};
2  For[i = 0, i < q, i++,
3      AppendTo[Gr, {{0, 1, i, 0}, {0, 0, 0, 1}}];
4      For[j = 0, j < q, j++,
5        AppendTo[Gr, {{1, i, j, 0}, {0, 0, 0, 1}}];
6        AppendTo[Gr, {{0, 1, 0, i}, {0, 0, 1, j}}];
7        For[k = 0, k < q, k++,
8          AppendTo[Gr, {{1, i, 0, j}, {0, 0, 1, k}}];
9          For[l = 0, l < q, l++,
10           AppendTo[Gr, {{1, 0, i, j}, {0, 1, k, l}}];
11          ]
12        ]
13      ]
14    ];
```

Listing 5.2: Generating the Grassmannian

5.2   Naive Approach

Since GL_4 acts transitively on Gr_2, we do not need to check all 4-tuples $(X_1, X_2, X_3, X_4) \in \text{Gr}_2^4$. We fix $X_1 = \langle e_1, e_2 \rangle$ and let X_2, X_3, X_4 range over all elements of Gr_2. We then multiply these counts by $|\text{Gr}_2|$.

```
1  counts = {};
2   For[i = 1, i <= Length[Gr], i++,
3      IS2 = IS[Gr[[i]], IS1];
4      For[j = 1, j <= Length[Gr], j++,
5        IS3 = IS[Gr[[j]], IS2];
6        For[k = 1, k <= Length[Gr], k++,
```

49

```
7      AppendTo[counts, Length[IS[Gr[[k]], IS3]]];
8      ]]];
9  Sort[Tally[counts]]]
```

<div align="center">Listing 5.3: Naive Approach</div>

The data from $q = 2$ and $q = 3$ is provided below. The the code above is too inefficient to compute the values for $q > 3$. We introduce the nine orbit approach in the next section, to compute the values for prime q less than or equal to 19.

	Answer	Number of instances		Answer	Number of Instances
	0	192		0	69984
	1	2880		1	279936
	2	15552		2	1224720
	3	14976		4	478244
q = 2	5	7344	q = 3	7	127008
6.4sec	7	1584	10600sec	13	15552
	9	112		16	567
	11	234		22	1008
	19	1		49	1

Table 5.1: *Number of instances of the Four Lines Problem with a given answer, where first line is fixed.*

5.3   Nine Orbit Approach

In Proposition 16, we established the action of GL_4 on Gr_2^4 has 17 orbits. If we also we let S_3 by permuting the components, the action of $S_3 \times \mathrm{GL}_4$ on Gr_3 has 9 orbits, and the orbits of this action are unions of the orbits of the original GL_4 action. The table below classifies these orbits.

Θ_i	Union of O_i	Orbit size
Θ_1	O_1	$q^5(q+1)(q-1)^2|\mathrm{Gr}_2|$
Θ_2	$O_2 \cup O_3 \cup O_7$	$3q^4(q+1)^2(q-1)|\mathrm{Gr}_2|$
Θ_3	$O_4 \cup O_8 \cup O_9$	$3q^4(q+1)^2|\mathrm{Gr}_2|$
Θ_4	O_{11}	$q^3(q+1)^2|\mathrm{Gr}_2|$
Θ_5	O_{10}	$q^3(q+1)^2|\mathrm{Gr}_2|$
Θ_6	O_{12}	$q(q+1)^2(q-1)|\mathrm{Gr}_2|$
Θ_7	$O_5 \cup O_6 \cup O_{15}$	$3q^4|\mathrm{Gr}_2|$
Θ_8	$O_{13} \cup O_{14} \cup O_{16}$	$3q(q+1)^2|\mathrm{Gr}_2|$
Θ_9	O_{17}	$|\mathrm{Gr}_2|$

Table 5.2: *Orbits of action of $S_3 \times GL_4$ on Gr_2^3 expressed as unions of orbits of GL_4 action.*

The code below chooses a representative $(X_1, X_2, X_3) \in \mathrm{Gr}_2^4$ of each orbit. For each representative, we solve the Four Lines Problem for (X_1, X_2, X_3, X_4) for each $X_4 \in \mathrm{Gr}_2$.

```
1
2 For[ii = 1, ii <= 8, ii++,
3   Print[Timing[
4     q = Prime[ii];
5     IS1 = {{{1, 0, 0, 0}, {0, 1, 0, 0}}};
6     For[i = 0, i < q, i++,
7       AppendTo[IS1, {{0, i, 1, 0}, {1, 0, 0, 0}}];
8       For[j = 0, j < q, j++,
9         AppendTo[IS1, {{i, 0, 1, 0}, {j, 1, 0, 0}}];
10        AppendTo[IS1, {{0, i, j, 1}, {1, 0, 0, 0}}];
11        For[k = 0, k < q, k++,
12          AppendTo[IS1, {{i, 0, j, 1}, {k, 1, 0, 0}}];
```

```
13        ]]];

14

15    IS2A = IS[{{0, 0, 1, 0}, {0, 0, 0, 1}}, IS1];

16    IS2B = IS[{{1, 0, 0, 0}, {0, 0, 1, 0}}, IS1];

17    IS2C = IS1;

18

19    IS3 = {

20      IS[{{1, 0, 1, 0}, {0, 1, 0, 1}}, IS2A],

21      IS[{{1, 0, 0, 0}, {0, 1, 1, 0}}, IS2A],

22      IS[{{1, 0, 0, 0}, {0, 0, 1, 0}}, IS2A],

23      IS[{{0, 1, 0, 0}, {0, 0, 1, 0}}, IS2B],

24      IS[{{1, 0, 0, 0}, {0, 0, 0, 1}}, IS2B],

25      IS[{{1, 0, 0, 0}, {0, 1, 1, 0}}, IS2B],

26      IS2A,

27      IS2B,

28      IS2C

29      };

30    counts = Table[{}, {i, 1, 9}];

31

32    For[n = 1, n <= 9, n++,

33     AppendTo[counts[[n]],

34      Length[IS[{{0, 0, 1, 0}, {0, 0, 0, 1}}, IS3[[n]]]]];

35     For[i = 0, i < q, i++,

36      AppendTo[counts[[n]],

37       Length[IS[{{0, 1, i, 0}, {0, 0, 0, 1}}, IS3[[n]]]]];

38      For[j = 0, j < q, j++,

39        AppendTo[counts[[n]],
```

```
40        Length[IS[{{0, 1, 0, i}, {0, 0, 1, j}}, IS3[[n]]]]];
41       AppendTo[counts[[n]],
42        Length[IS[{{1, i, j, 0}, {0, 0, 0, 1}}, IS3[[n]]]]];
43      For[k = 0, k < q, k++,
44        AppendTo[counts[[n]],
45         Length[IS[{{1, i, 0, j}, {0, 0, 1, k}}, IS3[[n]]]]];
46        For[l = 0, l < q, l++,
47         AppendTo[counts[[n]],
48          Length[IS[{{1, 0, i, j}, {0, 1, k, l}}, IS3[[n]]]]];
49        ]]]]];
50     {q, Table[Sort[Tally[counts[[i]]]], {i, 1, 9}]}]
51    ]]
```

Listing 5.4: Nine Orbit Approach

The table below summarizes all the data generative by the above code for prime q less than or equal to 19. We notice the number of lines meeting four lines is either $0, 1, 2, q + 1, 2q + 1, q^2 + q + 1, (q + 1)^2, 2q^2 + q + 1$ or $q^3 + 2q^2 + q + 1$.

Θ_i	Answer	$q = 2$	$q = 3$	$q = 5$	$q = 7$	$q = 11$	$q = 13$	$q = 17$	$q = 19$
	Runtime(sec)	0.03	0.17 sec	2.6 sec	18	300	860	5000	11000
Θ_1	0	2	18	200	882	6050	12168	36992	58482
	1	12	36	150	392	1452	2366	5205	7220
	2	18	72	450	1568	8712	16562	46818	72200
	$q + 1$	3	4	6	8	12	14	18	20
Θ_2	1	2	12	80	252	1100	1872	4352	6156
	2	16	81	625	2401	14641	28561	83521	130321
	$q + 1$	12	30	90	182	462	650	1122	1406
	$2q + 1$	5	7	11	15	23	27	35	39
Θ_3	1	2	12	80	252	1100	1872	4352	6156
	2	16	81	625	2401	14641	28561	83521	130321
	$q + 1$	12	30	90	182	462	650	1122	1406
	$2q + 1$	5	7	11	15	23	27	35	39
Θ_4	$q + 1$	28	117	775	2793	16093	30927	88723	137541
	$q^2 + q + 1$	7	13	31	57	133	183	307	381
Θ_5	$q + 1$	28	117	775	2793	16093	30927	88723	137541
	$q^2 + q + 1$	7	13	31	57	133	183	307	381
Θ_6	$2q + 1$	24	108	750	2744	15972	30758	88434	137180
	$q^2 + q + 1$	8	18	50	98	242	338	578	722
	$2q^2 + q + 1$	3	4	6	8	12	14	18	20
Θ_7	$q + 1$	6	48	480	2016	13200	26208	78336	123120
	$2q + 1$	27	80	324	832	3024	4900	10692	14800
	$(q + 1)^2$	2	2	2	2	2	2	2	2
Θ_8	$2q + 1$	24	108	750	2744	15972	30758	88434	137180
	$q^2 + q + 1$	8	18	50	98	242	338	578	722
	$2q^2 + q + 1$	3	4	6	8	12	14	18	20
Θ_9	$(q + 1)^2$	16	81	625	2401	14641	28561	83521	130321
	$2q^2 + q + 1$	18	48	180	448	1584	2548	5508	7600
	$q^3 + 2q^2 + q + 1$	1	1	1	1	1	1	1	1

Table 5.3: *Data from Nine Orbit Approach for prime $q \leq 19$*

If we assume the number of instances of the Four Lines Problem with a given answer is a polynomial in q on each orbit, we may use the data from Table 5.3 to find an exact count of $\mathcal{A}_d = \{(X_1, X_2, X_3, X_4) \in \mathrm{Gr}_2 : |\mathcal{M}(X_1, X_2, X_3, X_4)| = d\}$.

Proposition 25. *If we assume the counts in Table 5.3 are polynomials in q, we have the following.*

Θ_i	Answer	q
Θ_1	0	$\frac{1}{2}q^2(q-1)^2$
	1	$q^2(q+1)$
	2	$\frac{1}{2}q^2(q+1)^2$
	$q+1$	$q+1$
Θ_2	1	$q(q-1)^2$
	2	q^4
	$q+1$	$2q(2q-1)$
	$2q+1$	$2q+1$
Θ_3	1	$q(q-1)^2$
	2	q^4
	$q+1$	$2q(2q-1)$
	$2q+1$	$2q+1$
Θ_4	$q+1$	$q^4+q^3+q^2$
	q^2+q+1	q^2+q+1
Θ_5	$q+1$	$q^4+q^3+q^2$
	q^2+q+1	q^2+q+1
Θ_6	$2q+1$	q^4+q^3
	q^2+q+1	$2q^2$
	$2q^2+q+1$	$q+1$
Θ_7	$q+1$	$q(q-1)^2(q+1)$
	$2q+1$	$(q+1)^2(2q-1)$
	$(q+1)^2$	2
Θ_8	$2q+1$	q^4+q^3
	q^2+q+1	$2q^2$
	$2q^2+q+1$	$q+1$
Θ_9	$(q+1)^2$	q^4
	$2q^2+q+1$	q^3+2q^2+q
	q^3+2q^2+q+1	1

Table 5.4: *Number of instances of the Four Lines Problem with a given answer on a repre-sentative of each orbit*

Proof. The counts in Table 5.3, take a representative $(X_1, X_2, X_3) \in \mathrm{Gr}_2^2$ and solve all instances of the Four Lines Problem (X_1, X_2, X_3, X_4) for all $X_4 \in \mathrm{Gr}_2$. Thus if these counts are polynomials in q, their degree is at most 4. We have 8 data points in Table 5.3. $\square$

If we multiply these counts by the corresponding orbit sizes and combine terms with the same number of solutions, we achieve complete counts of the number of instances of the Four Line with a given answer.

$\lvert\mathcal{M}(X_1, X_2, X_3, X_4)\rvert$	Number of Instances
0	$\frac{1}{2}q^7(q+1)(q-1)^4\lvert\mathrm{Gr}_2\rvert$
1	$q^6(q+1)^2(q-1)^2(q+3)\lvert\mathrm{Gr}_2\rvert$
2	$\frac{1}{2}q^7(q+1)^2(q^3+5q^2-q+1)\lvert\mathrm{Gr}_2\rvert$
$q+1$	$3q^5(5q^4+9q^3+q^2-q+2)\lvert\mathrm{Gr}_2\rvert$
$2q+1$	$q^4(q+1)^2(7q^2+12q-1)\lvert\mathrm{Gr}_2\rvert$
q^2+q+1	$2q^3(q+1)^2(q^2+2q+3)\lvert\mathrm{Gr}_2\rvert$
$(q+1)^2$	$7q^4\lvert\mathrm{Gr}_2\rvert$
$2q^2+q+1$	$q(q+1)^2(q^2+3q+3)\lvert\mathrm{Gr}_2\rvert$
q^3+2q^2+q+1	$\lvert\mathrm{Gr}_2\rvert$

Table 5.5: *Number of instances of Four Lines Problem over $\mathbb{F}_q$ with given answer, assuming the counts are polynomial in q*

6 REFERENCES

[GP72] I. M. Gel′fand and V. A. Ponomarev, *Problems of linear algebra and classification of quadruples of subspaces in a finite-dimensional vector space*, Hilbert space operators and operator algebras (Proc. Internat. Conf., Tihany, 1970), North-Holland, Amsterdam, 1972, pp. 163–237. Colloq. Math. Soc. János Bolyai, 5. MR0357428 ↑

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236 ↑8, 9, 10

[Ful97] William Fulton, *Young tableaux*, London Mathematical Society Student Texts, vol. 35, Cambridge University Press, Cambridge, 1997. With applications to representation theory and geometry. MR1464693 ↑6

[Man01] Laurent Manivel, *Symmetric functions, Schubert polynomials and degeneracy loci*, SMF/AMS Texts and Monographs, vol. 6, American Mathematical Society, Providence, RI; Société Mathématique de France, Paris, 2001. Translated from the 1998 French original by John R. Swallow; Cours Spécialisés [Specialized Courses], 3. MR1852463 ↑

[HJ85] Roger A. Horn and Charles R. Johnson, *Matrix analysis*, Cambridge University Press, Cambridge, 1985. MR832183 ↑

[Mat12] Lindsey Mathewson, *The class equation of GL2(Fq)*, 2012. ↑18

[KL72] S. L. Kleiman and Dan Laksov, *Schubert calculus*, Amer. Math. Monthly **79** (1972), 1061–1082, DOI 10.2307/2317421. MR323796 ↑4

[Vak06] Ravi Vakil, *Schubert induction*, Ann. of Math. (2) **164** (2006), no. 2, 489–512, DOI 10.4007/annals.2006.164.489. MR2247966 ↑

[BL20] Peter Bürgisser and Antonio Lerario, *Probabilistic Schubert calculus*, J. Reine Angew. Math. **760** (2020), 1–58, DOI 10.1515/crelle-2018-0009. MR4069883 ↑5

[BLLP19] Saugata Basu, Antonio Lerario, Erik Lundberg, and Chris Peterson, *Random fields and the enumerative geometry of lines on real and complex hypersurfaces*, Math. Ann. **374** (2019), no. 3-4, 1773–1810, DOI 10.1007/s00208-019-01837-0. MR3985123 ↑5

[Sot10] Frank Sottile, *Frontiers of reality in Schubert calculus*, Bull. Amer. Math. Soc. (N.S.) **47** (2010), no. 1, 31–71, DOI 10.1090/S0273-0979-09-01276-2. MR2566445 ↑4

[Sot00] _____ , *Real Schubert calculus: polynomial systems and a conjecture of Shapiro and Shapiro*, Experiment. Math. **9** (2000), no. 2, 161–182. MR1780204 ↑4

[Sot99] _____ , *The special Schubert calculus is real*, Electron. Res. Announc. Amer. Math. Soc. **5** (1999), 35–39, DOI 10.1090/S1079-6762-99-00058-X. MR1679451 ↑

[Sot97] _____ , *Enumerative geometry for the real Grassmannian of lines in projective space*, Duke Math. J. **87** (1997), no. 1, 59–85, DOI 10.1215/S0012-7094-97-08703-2. MR1440063 ↑

[MTV09] Evgeny Mukhin, Vitaly Tarasov, and Alexander Varchenko, *The B. and M. Shapiro conjecture in real algebraic geometry and the Bethe ansatz*, Ann. of Math. (2) **170** (2009), no. 2, 863–881, DOI 10.4007/annals.2009.170.863. MR2552110 ↑

[Hil02] David Hilbert, *Mathematical problems*, Bull. Amer. Math. Soc. **8** (1902), no. 10, 437–479, DOI 10.1090/S0002-9904-1902-00923-3. MR1557926 ↑1

[MTV09] Evgeny Mukhin, Vitaly Tarasov, and Alexander Varchenko, *The B. and M. Shapiro conjecture in real algebraic geometry and the Bethe ansatz*, Ann. of Math. (2) **170** (2009), no. 2, 863–881, DOI 10.4007/annals.2009.170.863. MR2552110 ↑4

7   Curriculum Vitae

Adam Buck

Education

UW - Milwaukee, Milwaukee, WI

Ph.D., Department of Mathematics, anticipated May 2020

Advisor: Professor Jeb Willenbring

Topic: Asymptotic Probability of Incidence Relations over Finite Fields

Masters of Science, Mathematics, May 2014

UW - Stevens Point, Stevens Point, WI

Bachelor of Science, Mathematics and Physics, May 2012

Teaching Experience

UW - Milwaukee

Teaching Assistant - Instructor of Record for the following courses:

Math 098 Algebraic Literacy 1- Summer 15

Math 103 Contemporary Applications of Mathematics - Spring 18

Math 105 Intermediate Algebra - Fall 14, Spring 15, Fall 16

Math 115 Precalculus - Spring 17 Math 116 College Algebra - Fall 15, Spring 16

Math 211 Survey in Calculus and Analytic Geometry - Fall 17 online

Math 231 Calculus and Analytic Geometry I - Fall 18

Math 232 Calculus and Analytic Geometry II - Spring 19

Other Duties

Online Homework Lab - Assisted students for drop-in tutoring.

Gateway Testing Center - Test proctor for Calculus 1 quizzes.

Presentations

2019 Joint Mathematics Meetings, January 19, 2019

"The Probability Four Lines in $\mathbb{F}_q\mathbb{P}^3$ Meet Two Lines"

UW-Milwaukee Graduate Student Colloquium

"A Recursion Incursion Excursion" October 31, 2017

"Understanding the 17-gon" February 13, 2017

"The Game of NIM and Dots and Boxes" May 1, 2018

Service

Math Circle, Brown Street Academy, July 2018 - December 2020

Math enrichment activities for 3rd-6th graders through NEU-Life program.

Affiliations

AMS Student Member since Fall 2012

Pi Mu Epsilon since Spring 2010

Sigma Pi Sigma since Spring 2010