Commutativity of Generic Solutions to Polynomials in Matrices over Finite Fields

Sam Heil
Advisor: Dr. John Shareshian

26 March 2020

Introduction and Problem Motivation

This problem was inspired by the following theorem of Agler and McCarthy, proving commutativity of solutions to free polynomials in matrices over $\mathbb{C}$ satisfying certain genericity conditions.

Introduction and Problem Motivation

Theorem (Agler and McCarthy, 2014)

Let $d \in \mathbb{N}$, and let $\mathbb{P}^d$ be the set of free polynomials in d non-commuting variables. Let $k = d - 1$, and let $p_1, \ldots, p_k$ be free polynomials in $\mathbb{P}^d$ with the property that, when evaluated on d-tuples of complex numbers, they are not constant in the last k variables. Let $p = (p_1, \ldots, p_k)^T$, and let $V = \{(X, Y^1, \ldots, Y^k) : p(X, Y^1, \ldots, Y^k) = 0\}$. Let B be the finite set $B = \bigcup_{j=1}^k \{x \in \mathbb{C} : \forall y \in \mathbb{C}^k, p_j(x, y^1, \ldots, y^k) \neq 0\}$. If X_0 in $\mathbb{M}^n$ has n linearly independent eigenvectors and $\sigma(X_0) \cap B = \emptyset$ (where $\sigma(X_0)$ is the set of eigenvalues of X_0), there exists Y_0 in $\mathbb{M}_n^k$ satisfying $(X_0, Y_0) \in V$ so that every element Y_0^j commutes with X_0.
If (X_0, Y_0) is in V and X_0 and Y_0 do not commute, then we must have that

$$(X_0, Y_0) \in V \cap \{(X, Y) : Dp(X, Y) \text{ is not full rank on } 0 \times \mathbb{M}_n^k\}.$$

Introduction and Problem Motivation

Theorem (Agler and McCarthy, 2014: two-variable case, paraphrased)

For a free polynomial $f(X,Y)$ in two non-commuting variables, let $X \in \mathbb{C}^{n\times n}$ be any matrix satisfying the following genericity conditions:

1. *X has n linearly independent eigenvectors.*
2. *No eigenvalue λ of X satisfies $f(\lambda, y) \neq 0$ for all $y \in \mathbb{C}$.*
3. *The derivative map $Y' \mapsto Df(X,Y)[Y'] = \lim_{t\to 0} \frac{1}{t}[f(X, Y+tY') - f(X,Y)]$ is of full rank for each solution Y to $f(X,Y) = 0$.*

Then, for each $Y \in \mathbb{C}^{n\times n}$ with $f(X,Y) = 0$, we have $XY = YX$.

Introduction and Problem Motivation

We will consider an extension of the two-variable version of this problem to a discrete context, for a restricted special case. We make the following modifications and restrictions to the setup:

1. X and Y will be matrices over a finite field $\mathbb{F}_q$, instead of $\mathbb{C}$.
2. We add a restriction on the form of the polynomial f: instead of allowing any free polynomial in two non-commuting variable, our result will only consider polynomials of the form $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, for $a_i \in \mathbb{F}_q$.
3. Instead of fully determining the set of matrices for which non-commuting solutions exist, we will only bound its size asymptotically, as $q \to \infty$.

Finite Fields: Basic Terminology and Definitions

Definition

For a prime power $q = p^k$, the **finite field** $\mathbb{F}_q$ is the unique field with q elements. The elements of $\mathbb{F}_q$ can be represented by degree-k polynomials $\sum_{i=0}^{k-1} a_i t^i$, where the coefficients $a_i \in \mathbb{Z}/p\mathbb{Z}$ are residues modulo p. Addition is polynomial addition modulo p, and multiplication is taken modulo an irreducible degree-k polynomial with coefficients modulo p.

Definition

The **algebraic closure** of a field F, written $\overline{F}$, is the smallest field with $F \subseteq \overline{F}$ for which all polynomials with coefficients in $\overline{F}$ factor completely into linear factors over $\overline{F}$. For a finite field $\mathbb{F}_q$, we have

$$\overline{\mathbb{F}_q} \cong \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}.$$

Reducing Matrices to Polynomials: Sufficient Criterion

Definition

The **ratio set** of a polynomial $f \in \mathbb{F}_q[x]$, denoted $R(f)$, is the set of all ratios of *distinct* roots of f over the algebraic closure $\overline{\mathbb{F}_q}$.

Proposition 2.4

Let q be a prime power and let $n, d \in \mathbb{N}$. Let $X \in \mathbb{F}_q^{d \times d}$ be a regular, semisimple, invertible matrix with characteristic polynomial p_X, and let $f \in \mathbb{F}_q[x, y]$ be of the form $f(x, y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$. Let $g(t) = f(1, t)$. Then, if $R(g) \cap R(p_X) = \emptyset$, then any solution $Y \in \mathbb{F}_q^{d \times d}$ to $f(X, Y) = 0$ must commute with X.

Reducing Matrices to Polynomials: Sufficient Criterion

Proposition 2.4 (condensed)

If $f(x, y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1, t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X, Y) = 0 \implies XY = YX$.

Reducing Matrices to Polynomials: Sufficient Criterion

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

- X is regular and semisimple $\implies X = SDS^{-1}$, $S, D \in \overline{\mathbb{F}_q}^{d \times d}$

Reducing Matrices to Polynomials: Sufficient Criterion

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

- X is regular and semisimple $\implies X = SDS^{-1}$, $S, D \in \overline{\mathbb{F}_q}^{d\times d}$
- Write $Y = SAS^{-1}$ (A is not necessarily diagonal)
- Since

$$f(X,Y) = \sum_{j=0}^{n} a_j Y^j X^{n-j} = \sum_{j=0}^{n} a_j S A^j D^{n-j} S^{-1} = Sf(D,A)S^{-1},$$

$$f(X,Y) = 0 \implies f(D,A) = 0.$$

Reducing Matrices to Polynomials: Sufficient Criterion

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

- X is regular and semisimple $\implies X = SDS^{-1}$, $S, D \in \overline{\mathbb{F}_q}^{d \times d}$
- Write $Y = SAS^{-1}$ (A is not necessarily diagonal)
- Since

$$f(X,Y) = \sum_{j=0}^{n} a_j Y^j X^{n-j} = \sum_{j=0}^{n} a_j S A^j D^{n-j} S^{-1} = Sf(D,A)S^{-1},$$

$$f(X,Y) = 0 \implies f(D,A) = 0.$$

- $\overline{\mathbb{F}_q}$ is algebraically closed, so A^T has some eigenvector $\mathbf{v}$

Reducing Matrices to Polynomials: Sufficient Criterion

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

We prove the contrapositive: If there exists a solution Y to $f(X,Y) = 0$ with $XY \neq YX$, then $R(g) \cap R(p_X) \neq \emptyset$.

Reducing Matrices to Polynomials: Sufficient Criterion

Proposition 2.4 (condensed)

If $f(x, y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1, t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X, Y) = 0 \implies XY = YX$.

We prove the contrapositive: If there exists a solution Y to $f(X, Y) = 0$ with $XY \neq YX$, then $R(g) \cap R(p_X) \neq \emptyset$.
$X = SDS^{-1}, Y = SAS^{-1}, f(D, A) = 0$; $\mathbf{v}^T A = \lambda A$.
Two cases:

1. There is an eigenvector $\mathbf{v}$ of A^T with multiple nonzero components.
2. Every eigenvector is of the form $\mathbf{v} = c\mathbf{e}_i$ for some i.

Proof of Sufficient Criterion: Case 1

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

Suppose that $\mathbf{v}$ has multiple nonzero entries.

$$\mathbf{0} = \mathbf{v}^T \cdot 0 = \mathbf{v}^T \cdot f(D,A) = \sum_{j=0}^{n} a_j \mathbf{v}^T A^j D^{n-j}$$

$$= \mathbf{v}^T \sum_{j=0}^{n} a_j \lambda^j \begin{bmatrix} \alpha_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \alpha_d \end{bmatrix}^{n-j}$$

Proof of Sufficient Criterion: Case 1

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

Suppose that $\mathbf{v}$ has multiple nonzero entries.

$$\begin{aligned}
\mathbf{0} = \mathbf{v}^T \cdot 0 = \mathbf{v}^T \cdot f(D,A) &= \sum_{j=0}^{n} a_j \mathbf{v}^T A^j D^{n-j} \\
&= \mathbf{v}^T \sum_{j=0}^{n} a_j \lambda^j \begin{bmatrix} \alpha_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \alpha_d \end{bmatrix}^{n-j} \\
&= \mathbf{v}^T \begin{bmatrix} f(\alpha_1,\lambda) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & f(\alpha_d,\lambda) \end{bmatrix}
\end{aligned}$$

Proof of Sufficient Criterion: Case 1

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

Suppose that $\mathbf{v}$ has multiple nonzero entries: $v_i \neq 0$ and $v_j \neq 0$.

$$\mathbf{0} = \mathbf{v}^T \begin{bmatrix} f(\alpha_1,\lambda) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & f(\alpha_d,\lambda) \end{bmatrix} = \begin{bmatrix} v_1 f(\alpha_1,\lambda) & \dots & v_d f(\alpha_d,\lambda) \end{bmatrix}$$

This implies that $f(\alpha_i,\lambda) = f(\alpha_j,\lambda) = 0$.

Proof of Sufficient Criterion: Case 1

Proposition 2.4 (condensed)

If $f(x, y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1, t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X, Y) = 0 \implies XY = YX$.

Suppose that $\mathbf{v}$ has multiple nonzero entries: $v_i \neq 0$ and $v_j \neq 0$.

$$\mathbf{0} = \mathbf{v}^T \begin{bmatrix} f(\alpha_1, \lambda) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & f(\alpha_d, \lambda) \end{bmatrix} = \begin{bmatrix} v_1 f(\alpha_1, \lambda) & \dots & v_d f(\alpha_d, \lambda) \end{bmatrix}$$

This implies that $f(\alpha_i, \lambda) = f(\alpha_j, \lambda) = 0$.
$f(x, y) = x^n \sum_{i=0}^{n} a_i (\frac{y}{x})^i \implies f(\alpha, \lambda) = f(1, \alpha^{-1}\lambda) = g(\alpha^{-1}\lambda)$.

Proof of Sufficient Criterion: Case 1

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

Suppose that $\mathbf{v}$ has multiple nonzero entries: $v_i \neq 0$ and $v_j \neq 0$.

$$\mathbf{0} = \mathbf{v}^T \begin{bmatrix} f(\alpha_1,\lambda) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & f(\alpha_d,\lambda) \end{bmatrix} = \begin{bmatrix} v_1 f(\alpha_1,\lambda) & \dots & v_d f(\alpha_d,\lambda) \end{bmatrix}$$

This implies that $f(\alpha_i,\lambda) = f(\alpha_j,\lambda) = 0$.
$f(x,y) = x^n \sum_{i=0}^{n} a_i (\frac{y}{x})^i \implies f(\alpha,\lambda) = f(1,\alpha^{-1}\lambda) = g(\alpha^{-1}\lambda)$.
Thus, $\alpha_i^{-1}\lambda = \beta_1$, $\alpha_j^{-1}\lambda = \beta_2$ for roots β_1, β_2 of g, so $\alpha_j/\alpha_i = \beta_1/\beta_2$ and $R(p_X) \cap R(g) \neq \emptyset$.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

- Each eigenvector has only one nonzero entry; scale so that $\mathbf{v} = \mathbf{e}_i$ for some i.
- We claim that if $XY \neq YX$, then A is not diagonalizable over $\overline{\mathbb{F}_q}$.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

- Each eigenvector has only one nonzero entry; scale so that $\mathbf{v} = \mathbf{e}_i$ for some i.
- We claim that if $XY \neq YX$, then A is not diagonalizable over $\overline{\mathbb{F}_q}$.
  - A diagonalizable implies that A^T is diagonalizable, so there is a basis of eigenvectors of A^T.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

- Each eigenvector has only one nonzero entry; scale so that $\mathbf{v} = \mathbf{e}_i$ for some i.
- We claim that if $XY \neq YX$, then A is not diagonalizable over $\overline{\mathbb{F}_q}$.
    - A diagonalizable implies that A^T is diagonalizable, so there is a basis of eigenvectors of A^T.
    - Since every eigenvector is $\mathbf{e}_i$ for some i, this would imply that **every** $\mathbf{e}_i$ is an eigenvector, so A^T must be diagonal.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x, y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1, t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X, Y) = 0 \implies XY = YX$.

- Each eigenvector has only one nonzero entry; scale so that $\mathbf{v} = \mathbf{e}_i$ for some i.
- We claim that if $XY \neq YX$, then A is not diagonalizable over $\overline{\mathbb{F}_q}$.
  - A diagonalizable implies that A^T is diagonalizable, so there is a basis of eigenvectors of A^T.
  - Since every eigenvector is $\mathbf{e}_i$ for some i, this would imply that **every** $\mathbf{e}_i$ is an eigenvector, so A^T must be diagonal.
  - A and D both diagonal $\implies AD = DA$, so $X = SDS^{-1}$ and $Y = SAS^{-1}$ must commute, contradiction.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

- Consider the Jordan decomposition $A^T = TJT^{-1}$ over $\overline{\mathbb{F}_q}$.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x, y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1, t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X, Y) = 0 \implies XY = YX$.

- Consider the Jordan decomposition $A^T = TJT^{-1}$ over $\overline{\mathbb{F}_q}$.
- J must have a block of size $k \geq 2$. Apply a change of basis so the new basis vectors $v^{(1)}, \ldots, v^{(k)}$ form the k-dimensional cyclic subspace corresponding to this block.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

- Consider the Jordan decomposition $A^T = TJT^{-1}$ over $\overline{\mathbb{F}_q}$.
- J must have a block of size $k \geq 2$. Apply a change of basis so the new basis vectors $v^{(1)}, \ldots, v^{(k)}$ form the k-dimensional cyclic subspace corresponding to this block.
- Then, $A^T \mathbf{v}^{(1)} = \lambda \mathbf{v}^{(1)}$ and $A^T \mathbf{v}^{(j)} = \lambda \mathbf{v}^{(j)} + \mathbf{v}^{(j-1)}$ for $j \geq 2$.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

- Consider the Jordan decomposition $A^T = TJT^{-1}$ over $\overline{\mathbb{F}_q}$.
- J must have a block of size $k \geq 2$. Apply a change of basis so the new basis vectors $v^{(1)}, \ldots, v^{(k)}$ form the k-dimensional cyclic subspace corresponding to this block.
- Then, $A^T \mathbf{v}^{(1)} = \lambda \mathbf{v}^{(1)}$ and $A^T \mathbf{v}^{(j)} = \lambda \mathbf{v}^{(j)} + \mathbf{v}^{(j-1)}$ for $j \geq 2$.
- By induction on m, we have $(A^T)^m \mathbf{v}^{(2)} = \lambda^m \mathbf{v}^{(2)} + m\lambda^{m-1} \mathbf{v}^{(1)}$ and $(A^T)^m \mathbf{v}^{(1)} = \lambda^m \mathbf{v}^{(1)}$.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x, y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1, t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X, Y) = 0 \implies XY = YX$.

- $\mathbf{v}^{(1)}$ is an eigenvector of A^T, so

$$\mathbf{0} = (\mathbf{v}^{(1)})^T \begin{bmatrix} f(\alpha_1, \lambda) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & f(\alpha_d, \lambda) \end{bmatrix}$$

and since $\mathbf{v}^{(1)} = \mathbf{e}_i$, $f(\alpha_i, \lambda) = 0$.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

Choose $j \neq i$ for which $(\mathbf{v}^{(2)})_j \neq 0$. Using $f(A,D) = 0$, we have

$$\begin{aligned} 0 = (\mathbf{v}^{(2)})^T f(A,D)\mathbf{e}_j &= (\mathbf{v}^{(2)})^T f(A,D)\mathbf{e}_j \\ &= \sum_{\ell=0}^{n} a_\ell (\mathbf{v}^{(2)})^T A^\ell D^{n-\ell} \mathbf{e}_j \\ &= \sum_{\ell=0}^{n} a_\ell \alpha_j^{n-\ell} (\lambda^\ell (\mathbf{v}^{(2)})^T + \ell \lambda^{\ell-1} \mathbf{e}_i^T) \mathbf{e}_j \end{aligned}$$

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x,y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1,t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X,Y) = 0 \implies XY = YX$.

Simplifying and canceling, we have

$$0 = \sum_{\ell=0}^{n} a_\ell \alpha_j^{n-\ell} (\lambda^\ell (\mathbf{v}^{(2)})^T + \ell \lambda^{\ell-1} \mathbf{e}_i^T) \mathbf{e}_j = \sum_{\ell=0}^{n} a_\ell \alpha_j^{n-\ell} \lambda^\ell (\mathbf{v}^{(2)})^T \mathbf{e}_j$$
$$= (\mathbf{v}^{(2)})_j f(\alpha_j, \lambda),$$

so $f(\alpha_j, \lambda) = 0$.

Proof of Sufficient Criterion: Case 2

Proposition 2.4 (condensed)

If $f(x, y) = \sum_{i=0}^{n} a_i y^i x^{n-i}$, $g(t) = f(1, t)$, and $R(g) \cap R(p_X) = \emptyset$, then $f(X, Y) = 0 \implies XY = YX$.

- Now $f(\alpha_i, \lambda) = f(\alpha_j, \lambda) = 0$ for distinct i, j.
- As before, this implies that $g(\alpha_i^{-1}\lambda) = g(\alpha_j^{-1}\lambda) = 0$, so $\alpha_j/\alpha_i = \beta_1/\beta_2$ for distinct roots β_1, β_2 of g.
- Thus, $R(p_X) \cap R(g) \neq \emptyset$, proving the claim.

Applying the Commuting Criterion

Using Proposition 2.4, we prove our asymptotic commutativity result via the following argument:

1. Show that all but $O(1/q)$ pairs of polynomials (f, g) satisfy $R(f) \cap R(g) = \emptyset$ as $q \to \infty$.
2. Show that asymptotically equivalent numbers of matrices produce each characteristic polynomial for large q.

We will focus on (1) in this talk, since (2) is fairly well-known.

Counting Polynomial Pairs: Motivation and Example

- Consider pairs (f, g) in $\mathbb{F}_q[x]$ with $\deg f = \deg g = 2$.

Counting Polynomial Pairs: Motivation and Example

- Consider pairs (f, g) in $\mathbb{F}_q[x]$ with $\deg f = \deg g = 2$.
- If $f(x) = x^2 - ax + b$ has roots $r, s \in \mathbb{F}_{q^2}^*$ $(b \neq 0)$, then by Vieta $r + s = a$ and $rs = b$, so $r/s + s/r = \frac{a^2-2b}{b} \in \mathbb{F}_q$.

Counting Polynomial Pairs: Motivation and Example

- Consider pairs (f, g) in $\mathbb{F}_q[x]$ with $\deg f = \deg g = 2$.
- If $f(x) = x^2 - ax + b$ has roots $r, s \in \mathbb{F}_{q^2}^*$ $(b \neq 0)$, then by Vieta $r + s = a$ and $rs = b$, so $r/s + s/r = \frac{a^2-2b}{b} \in \mathbb{F}_q$.
- Since r/s and s/r are the roots of the quadratic $x^2 - cx + 1$ for $c = \frac{a^2-2b}{b}$, they are uniquely determined by $\frac{a^2-2b}{b}$.

Counting Polynomial Pairs: Motivation and Example

- Consider pairs (f, g) in $\mathbb{F}_q[x]$ with $\deg f = \deg g = 2$.
- If $f(x) = x^2 - ax + b$ has roots $r, s \in \mathbb{F}_{q^2}^*$ $(b \neq 0)$, then by Vieta $r + s = a$ and $rs = b$, so $r/s + s/r = \frac{a^2-2b}{b} \in \mathbb{F}_q$.
- Since r/s and s/r are the roots of the quadratic $x^2 - cx + 1$ for $c = \frac{a^2-2b}{b}$, they are uniquely determined by $\frac{a^2-2b}{b}$.
- Thus, for any $t \in \mathbb{F}_q^*$, $x^2 - ax + b$ and $x^2 - atx + bt^2$ have the same root ratios, so each ratio is produced by at least $q - 1$ of the $q(q-1)$ quadratics with nonzero constant term.

Counting Polynomial Pairs: Motivation and Example

- Consider pairs (f, g) in $\mathbb{F}_q[x]$ with $\deg f = \deg g = 2$.
- If $f(x) = x^2 - ax + b$ has roots $r, s \in \mathbb{F}_{q^2}^*$ $(b \neq 0)$, then by Vieta $r + s = a$ and $rs = b$, so $r/s + s/r = \frac{a^2-2b}{b} \in \mathbb{F}_q$.
- Since r/s and s/r are the roots of the quadratic $x^2 - cx + 1$ for $c = \frac{a^2-2b}{b}$, they are uniquely determined by $\frac{a^2-2b}{b}$.
- Thus, for any $t \in \mathbb{F}_q^*$, $x^2 - ax + b$ and $x^2 - atx + bt^2$ have the same root ratios, so each ratio is produced by at least $q - 1$ of the $q(q-1)$ quadratics with nonzero constant term.
- There are at least $q/2$ distinct values for $\frac{a^2-2b}{b}$, so the probability that $R(f) \cap R(g) \neq \emptyset$ for randomly chosen f, g is at least

$$\frac{q}{2} \cdot \left(\frac{q-1}{q(q-1)}\right)^2 = \frac{1}{2q}.$$

Counting Polynomial Pairs: Motivation and Example

- For polynomials of arbitrary degree, consider the set of pairs of the form $(f, g) = (f_1 f_2, g_1 g_2)$, with f_1 and g_1 quadratics. $R(f_1) \cap R(g_1) \neq \emptyset \implies R(f) \cap R(g) \neq \emptyset$ for any f_2, g_2, and this occurs with probability over $\frac{1}{2q}$ for randomly chosen f_1, g_1.

Counting Polynomial Pairs: Motivation and Example

- For polynomials of arbitrary degree, consider the set of pairs of the form $(f, g) = (f_1 f_2, g_1 g_2)$, with f_1 and g_1 quadratics. $R(f_1) \cap R(g_1) \neq \emptyset \implies R(f) \cap R(g) \neq \emptyset$ for any f_2, g_2, and this occurs with probability over $\frac{1}{2q}$ for randomly chosen f_1, g_1.
- However, there is also an *upper* bound of $O(1/q)$ on the proportion of pairs violating the criterion!

Counting Polynomial Pairs: Statement and Argument

Lemma 5.3

Let m and n be positive integers, and let q be a power of a prime p with $p > m$. Then, for any degree-n polynomial f over $\mathbb{F}_q$ with $f(0) \neq 0$, the number of monic, separable, degree-n polynomials $g \in \mathbb{F}_q[x]$ with nonzero constant term and $R(g) \cap R(f) \neq \emptyset$ is at most $\left(1 + \frac{C(m+1)}{3}\right) n(n-1)m(m-1)q^{m-1}$ for a constant C.

1. Strategy: show that for any $\alpha \in \overline{\mathbb{F}_q}^*$, at most $O(1/q)$ polynomials g (of any degree m) have $\alpha \in R(g)$.

Counting Polynomial Pairs: Statement and Argument

Lemma 5.3

Let m and n be positive integers, and let q be a power of a prime p with $p > m$. Then, for any degree-n polynomial f over $\mathbb{F}_q$ with $f(0) \neq 0$, the number of monic, separable, degree-n polynomials $g \in \mathbb{F}_q[x]$ with nonzero constant term and $R(g) \cap R(f) \neq \emptyset$ is at most $\left(1 + \frac{C(m+1)}{3}\right) n(n-1)m(m-1)q^{m-1}$ for a constant C.

1. Strategy: show that for any $\alpha \in \overline{\mathbb{F}_q}^*$, at most $O(1/q)$ polynomials g (of any degree m) have $\alpha \in R(g)$.
2. Factor g as a product of irreducibles: $g = g_1 g_2 \ldots g_k$.

Counting Polynomial Pairs: Statement and Argument

Lemma 5.3

Let m and n be positive integers, and let q be a power of a prime p with $p > m$. Then, for any degree-n polynomial f over $\mathbb{F}_q$ with $f(0) \neq 0$, the number of monic, separable, degree-n polynomials $g \in \mathbb{F}_q[x]$ with nonzero constant term and $R(g) \cap R(f) \neq \emptyset$ is at most $\left(1 + \frac{C(m+1)}{3}\right) n(n-1)m(m-1)q^{m-1}$ for a constant C.

1. Strategy: show that for any $\alpha \in \overline{\mathbb{F}_q}^*$, at most $O(1/q)$ polynomials g (of any degree m) have $\alpha \in R(g)$.
2. Factor g as a product of irreducibles: $g = g_1 g_2 \ldots g_k$.
3. Bound the number of polynomials with α as a ratio of roots of *distinct* irreducible factors g_i, g_j.
4. Bound the number of polynomials with α as a ratio of roots of the *same* irreducible factor g_i.

Bounding in the Distinct Factor Case

- We count triples (f, α_1, α_2), where f is a valid degree-n polynomial with α_1, α_2 as roots of distinct irreducible factors.

Bounding in the Distinct Factor Case

- We count triples (f, α_1, α_2), where f is a valid degree-n polynomial with α_1, α_2 as roots of distinct irreducible factors.
- To do this, we will partition $\overline{\mathbb{F}_q}^*$ into $q-1$ classes, and show that the number of triples (f, α_1, α_2) with the ratio $\alpha = \alpha_1\alpha_2^{-1}$ in class c is the same for all c.

Bounding in the Distinct Factor Case

- We count triples (f, α_1, α_2), where f is a valid degree-n polynomial with α_1, α_2 as roots of distinct irreducible factors.
- To do this, we will partition $\overline{\mathbb{F}_q}^*$ into $q-1$ classes, and show that the number of triples (f, α_1, α_2) with the ratio $\alpha = \alpha_1 \alpha_2^{-1}$ in class c is the same for all c.
- Then $|\{f : \alpha \in R(f)\}| \leq \frac{q^n \cdot n(n-1)}{q-1} = O(q^{n-1})$ since $n \ll q$.

Bounding in the Distinct Factor Case

We construct the $q-1$ classes so that given $\alpha \in \overline{\mathbb{F}_q}^*$, $r\alpha$ is in a different class for each $r \in \mathbb{F}_q^*$.
(Each class contains one element from each coset of $\mathbb{F}_q^*$ in $\overline{\mathbb{F}_q}^*$.)

Bounding in the Distinct Factor Case

We construct the $q-1$ classes so that given $\alpha \in \overline{\mathbb{F}_q}^*$, $r\alpha$ is in a different class for each $r \in \mathbb{F}_q^*$.
(Each class contains one element from each coset of $\mathbb{F}_q^*$ in $\overline{\mathbb{F}_q}^*$.)

- Given a polynomial f with α_1, α_2 as roots of different irreducible factors and $\alpha_1 \alpha_2^{-1} = \alpha$, we have $f = f_{\alpha_1} f_{\alpha_2} g$ for some polynomial g, where f_{α_1} and f_{α_2} are the minimal polynomials with α_1, α_2 as roots.
- For $r \in \mathbb{F}_q^*$, the minimal polynomial $f_{r\alpha_1}$ satisfies $\deg f_{r\alpha_1} = \deg f_{\alpha_1}$, so map f to $f_{r\alpha_1} f_{\alpha_2} g$.

Bounding in the Distinct Factor Case

We construct the $q-1$ classes so that given $\alpha \in \overline{\mathbb{F}_q}^*$, $r\alpha$ is in a different class for each $r \in \mathbb{F}_q^*$.

(Each class contains one element from each coset of $\mathbb{F}_q^*$ in $\overline{\mathbb{F}_q}^*$.)

- Given a polynomial f with α_1, α_2 as roots of different irreducible factors and $\alpha_1\alpha_2^{-1} = \alpha$, we have $f = f_{\alpha_1} f_{\alpha_2} g$ for some polynomial g, where f_{α_1} and f_{α_2} are the minimal polynomials with α_1, α_2 as roots.
- For $r \in \mathbb{F}_q^*$, the minimal polynomial $f_{r\alpha_1}$ satisfies $\deg f_{r\alpha_1} = \deg f_{\alpha_1}$, so map f to $f_{r\alpha_1} f_{\alpha_2} g$.
- More technical counting/PIE argument needed to handle special cases like $r\alpha_1 = \alpha_2$ while preserving separability; see Lemma 3.5

Bounding in the Single Factor Case

This reduces to the case where f is itself irreducible (reduction adds an extra factor of m from summing over individual factors). Let $n = \deg f$.

Bounding in the Single Factor Case

This reduces to the case where f is itself irreducible (reduction adds an extra factor of m from summing over individual factors). Let $n = \deg f$.

Let $\mathrm{ord}(\alpha)$ denote the multiplicative order of the ratio α in $\mathbb{F}_{q^n}^*$ (minimal d with $\alpha^d = 1$).

Two subcases:

1. Large order elements: $\mathrm{ord}(\alpha) \geq q^{1+\epsilon}$
2. Small order elements: $\mathrm{ord}(\alpha) < q^{1+\epsilon}$

Bounding in the Single Factor Case

Lemma 4.1

Let $n \in \mathbb{N}$, let $p > n$ be prime, and let $q = p^r$ for some $r \geq 1$. Then, if $\alpha, \beta \in \mathbb{F}_{q^n}^*$ and $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$, then the number of irreducible degree-n polynomials $f \in \mathbb{F}_q[x]$ with $\alpha \in R(f)$ is equal to the number of such polynomials with $\beta \in R(f)$.

Bounding in the Single Factor Case

Lemma 4.1

Let $n \in \mathbb{N}$, let $p > n$ be prime, and let $q = p^r$ for some $r \geq 1$. Then, if $\alpha, \beta \in \mathbb{F}_{q^n}^*$ and $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$, then the number of irreducible degree-n polynomials $f \in \mathbb{F}_q[x]$ with $\alpha \in R(f)$ is equal to the number of such polynomials with $\beta \in R(f)$.

- Let g be a generator of $\mathbb{F}_{q^n}^*$. Then, f splits over $\mathbb{F}_{q^n}^*$ as

$$f(x) = \prod_{j=1}^{n} (x - g^{r_j})$$

  for $0 \leq r_1 < r_2 < \cdots < r_n < q^n - 1$.
- α is a ratio of roots, so $\alpha = g^{r_i}/g^{r_j} = g^{r_i - r_j}$. Let $\beta = g^b$.

Bounding in the Single Factor Case

Lemma 4.1

Let $n \in \mathbb{N}$, let $p > n$ be prime, and let $q = p^r$ for some $r \geq 1$. Then, if $\alpha, \beta \in \mathbb{F}_{q^n}^*$ and $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$, then the number of irreducible degree-n polynomials $f \in \mathbb{F}_q[x]$ with $\alpha \in R(f)$ is equal to the number of such polynomials with $\beta \in R(f)$.

- Let g be a generator of $\mathbb{F}_{q^n}^*$. Then, f splits over $\mathbb{F}_{q^n}^*$ as

$$f(x) = \prod_{j=1}^{n}(x - g^{r_j})$$

  for $0 \leq r_1 < r_2 < \cdots < r_n < q^n - 1$.
- α is a ratio of roots, so $\alpha = g^{r_i}/g^{r_j} = g^{r_i - r_j}$. Let $\beta = g^b$.
- Then, $\gcd(r_i - r_j, q^n - 1) = \frac{q^n-1}{\mathrm{ord}(\alpha)} = \frac{q^n-1}{\mathrm{ord}(\beta)} = \gcd(b, q^n - 1)$, so $\exists t \in (\mathbb{Z}/(q^n-1)\mathbb{Z})^*$ with $t(r_i - r_j) \equiv b \pmod{q^n - 1}$.

Bounding in the Single Factor Case

Lemma 4.1

Let $n \in \mathbb{N}$, let $p > n$ be prime, and let $q = p^r$ for some $r \geq 1$. Then, if $\alpha, \beta \in \mathbb{F}_{q^n}^*$ and $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$, then the number of irreducible degree-n polynomials $f \in \mathbb{F}_q[x]$ with $\alpha \in R(f)$ is equal to the number of such polynomials with $\beta \in R(f)$.

- Now, apply the map

$$f(x) = \prod_{j=1}^{n}(x - g^{r_j}) \mapsto \tilde{f}(x) = \prod_{j=1}^{n}(x - g^{tr_j}).$$

Bounding in the Single Factor Case

Lemma 4.1

Let $n \in \mathbb{N}$, let $p > n$ be prime, and let $q = p^r$ for some $r \geq 1$. Then, if $\alpha, \beta \in \mathbb{F}_{q^n}^*$ and $\text{ord}(\alpha) = \text{ord}(\beta)$, then the number of irreducible degree-n polynomials $f \in \mathbb{F}_q[x]$ with $\alpha \in R(f)$ is equal to the number of such polynomials with $\beta \in R(f)$.

- Now, apply the map

$$f(x) = \prod_{j=1}^{n}(x - g^{r_j}) \mapsto \tilde{f}(x) = \prod_{j=1}^{n}(x - g^{tr_j}).$$

- We then have $\beta = g^b = g^{t(r_i - r_j)} = g^{tr_i}/g^{tr_j} \in R(\tilde{f})$!

Bounding in the Single Factor Case

Lemma 4.1

Let $n \in \mathbb{N}$, let $p > n$ be prime, and let $q = p^r$ for some $r \geq 1$. Then, if $\alpha, \beta \in \mathbb{F}_{q^n}^*$ and $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$, then the number of irreducible degree-n polynomials $f \in \mathbb{F}_q[x]$ with $\alpha \in R(f)$ is equal to the number of such polynomials with $\beta \in R(f)$.

- Now, apply the map

$$f(x) = \prod_{j=1}^{n}(x - g^{r_j}) \mapsto \tilde{f}(x) = \prod_{j=1}^{n}(x - g^{tr_j}).$$

- We then have $\beta = g^b = g^{t(r_i - r_j)} = g^{tr_i}/g^{tr_j} \in R(\tilde{f})$!
- Since t is an *invertible* residue, this is a bijection, and using Newton sum formulas we can show that $\tilde{f} \in \mathbb{F}_q[x]$.

Bounding in the Single Factor Case

Lemma 4.3

Let $f \in \mathbb{F}_q[x]$ be irreducible of degree n with $\alpha \in R(f)$. Then, all roots of f have the same multiplicative order in $\mathbb{F}_{q^n}^*$, and for any root r of f, $\mathrm{ord}(r) \leq q^{n/2} \cdot \mathrm{ord}(\alpha)$.

(Thanks to Nathan Smith for helping me prove this!)

Bounding in the Single Factor Case

Lemma 4.3

Let $f \in \mathbb{F}_q[x]$ be irreducible of degree n with $\alpha \in R(f)$. Then, all roots of f have the same multiplicative order in $\mathbb{F}_{q^n}^*$, and for any root r of f, $\mathrm{ord}(r) \leq q^{n/2} \cdot \mathrm{ord}(\alpha)$.

(Thanks to Nathan Smith for helping me prove this!)

- Galois theory implies that for any roots r_1, r_2 of f, there is an automorphism of $\mathbb{F}_{q^n}$ fixing $\mathbb{F}_q$ and mapping r_1 to r_2.

Bounding in the Single Factor Case

Lemma 4.3

Let $f \in \mathbb{F}_q[x]$ be irreducible of degree n with $\alpha \in R(f)$. Then, all roots of f have the same multiplicative order in $\mathbb{F}_{q^n}^*$, and for any root r of f, $\mathrm{ord}(r) \leq q^{n/2} \cdot \mathrm{ord}(\alpha)$.

(Thanks to Nathan Smith for helping me prove this!)

- Galois theory implies that for any roots r_1, r_2 of f, there is an automorphism of $\mathbb{F}_{q^n}$ fixing $\mathbb{F}_q$ and mapping r_1 to r_2.
- The only automorphisms of $\mathbb{F}_{q^n}$ fixing $\mathbb{F}_q$ are of the form $g \mapsto g^{q^j}$, for some $0 \leq j < n$.

Bounding in the Single Factor Case

Lemma 4.3

Let $f \in \mathbb{F}_q[x]$ be irreducible of degree n with $\alpha \in R(f)$. Then, all roots of f have the same multiplicative order in $\mathbb{F}_{q^n}^*$, and for any root r of f, $\operatorname{ord}(r) \leq q^{n/2} \cdot \operatorname{ord}(\alpha)$.

(Thanks to Nathan Smith for helping me prove this!)

- Galois theory implies that for any roots r_1, r_2 of f, there is an automorphism of $\mathbb{F}_{q^n}$ fixing $\mathbb{F}_q$ and mapping r_1 to r_2.
- The only automorphisms of $\mathbb{F}_{q^n}$ fixing $\mathbb{F}_q$ are of the form $g \mapsto g^{q^j}$, for some $0 \leq j < n$.
- Thus, $r_2 = r_1^{q^j}$. For $\alpha = \frac{r_2}{r_1}$ and $r_1 = g^a$, $\alpha = g^{a(q^j-1)}$.

Bounding in the Single Factor Case

Lemma 4.3

Let $f \in \mathbb{F}_q[x]$ be irreducible of degree n with $\alpha \in R(f)$. Then, all roots of f have the same multiplicative order in $\mathbb{F}_{q^n}^*$, and for any root r of f, $\text{ord}(r) \leq q^{n/2} \cdot \text{ord}(\alpha)$.

(Thanks to Nathan Smith for helping me prove this!)

- Galois theory implies that for any roots r_1, r_2 of f, there is an automorphism of $\mathbb{F}_{q^n}$ fixing $\mathbb{F}_q$ and mapping r_1 to r_2.
- The only automorphisms of $\mathbb{F}_{q^n}$ fixing $\mathbb{F}_q$ are of the form $g \mapsto g^{q^j}$, for some $0 \leq j < n$.
- Thus, $r_2 = r_1^{q^j}$. For $\alpha = \frac{r_2}{r_1}$ and $r_1 = g^a$, $\alpha = g^{a(q^j-1)}$.

$$\frac{q^n-1}{\text{ord}(\alpha)} = \gcd(q^n-1, a(q^j-1)) \leq \gcd(q^n-1, a) \cdot \gcd(q^n-1, q^j-1)$$
$$\leq \frac{q^n-1}{\text{ord}(r_1)} \cdot (q^{n/2}-1).$$

Bounding in the Single Factor Case

1. Large order elements: $\mathrm{ord}(\alpha) \geq q^{1+\epsilon}$

Bounding in the Single Factor Case

1. Large order elements: $\mathrm{ord}(\alpha) \geq q^{1+\epsilon}$
   Apply Lemma 4.1 directly: There are $\varphi(\mathrm{ord}(\alpha)) > q$ elements β with order $\mathrm{ord}(\alpha)$ and $q \gg n^2$, so only $O(1/q)$ of the polynomials f have $\alpha \in R(f)$.

Bounding in the Single Factor Case

1. Large order elements: $\mathrm{ord}(\alpha) \geq q^{1+\epsilon}$
   Apply Lemma 4.1 directly: There are $\varphi(\mathrm{ord}(\alpha)) > q$ elements β with order $\mathrm{ord}(\alpha)$ and $q \gg n^2$, so only $O(1/q)$ of the polynomials f have $\alpha \in R(f)$.
2. Small order elements: $\mathrm{ord}(\alpha) < q^{1+\epsilon}$

Bounding in the Single Factor Case

1. Large order elements: $\mathrm{ord}(\alpha) \geq q^{1+\epsilon}$
   Apply Lemma 4.1 directly: There are $\varphi(\mathrm{ord}(\alpha)) > q$ elements β with order $\mathrm{ord}(\alpha)$ and $q \gg n^2$, so only $O(1/q)$ of the polynomials f have $\alpha \in R(f)$.
2. Small order elements: $\mathrm{ord}(\alpha) < q^{1+\epsilon}$
   Combine Lemmas 4.1 and 4.3: The number of polynomials is at most $n\tau(q^n - 1)\frac{q^{n/2}\mathrm{ord}(\alpha)}{\varphi(\mathrm{ord}(\alpha))}$, where $\tau(n)$ denotes the number of divisors of n. Using asymptotic bounds on τ and φ, we have that this is at most $O(q^{n-1})$ for all $n \geq 3$, corresponding to $O(1/q)$ of the degree-n polynomials over $\mathbb{F}_q$.

Counting Matrices by Characteristic Polynomial: Sketch

1. Split $\mathbb{F}_q^{d\times d}$ into rational canonical form classes: each class corresponds to one characteristic polynomial.
2. Regular, semisimple, invertible matrices produce characteristic polynomials that are separable without zero as a root.
3. Under these conditions, show that all matrices commuting with an RCF matrix R can be written as polynomials in R.
4. Consider the action of $GL_d(\mathbb{F}_q)$ on $\mathbb{F}_q^{d\times d}$ by conjugation, and use the Orbit-Stabilizer Theorem. Bound the size of the stabilizer of each RCF class R by counting the number of degree-d polynomials in R that produce invertible matrices.

Final Results

Notation in statements of results:

- $SP_n(q)$: the set of separable monic degree-n polynomials over $\mathbb{F}_q$ without zero as a root
- $IRSS_d(q)$: the set of invertible, regular, semisimple $d \times d$ matrices over $\mathbb{F}_q$.

Final Results: Fixed Polynomial f

Proposition 7.1

Let p be prime, let $q = p^r$ be a prime power, and let d be a positive integer with $d < p$. Let $n \in \mathbb{N}$, and let $f \in \mathbb{F}_q[x]$ be a polynomial in two non-commuting variables of the form $f(X, Y) = \sum_{k=0}^{n} a_k Y^k X^{n-k}$ with $a_0 \neq 0$, $a_n \neq 0$. Let $N_{mat}(q)$ be the number of invertible, regular, semisimple matrices $X \in IRSS_d(q)$ for which there exists a solution $Y \in \mathbb{F}_q^{d\times d}$ to $f(X, Y) = 0$ with $XY \neq YX$. Then, for an absolute constant C,

$$N_{mat}(q) \leq \frac{q^d}{|SP_d(q)|} \cdot C(d+1)n(n-1)d(d-1) \cdot \frac{|IRSS_d(q)|}{q-d}.$$

In particular, in the asymptotic case as $q \to \infty$,

$$\frac{N_{mat}(q)}{|IRSS_d(q)|} \lesssim \frac{C(d+1)n(n-1)d(d-1)}{q} = O\left(\frac{n^2 d^3}{q}\right).$$

Final Results: Fixed Matrix X

Proposition 7.2

Let p be prime, let $q = p^r$ be a prime power, and let n be a positive integer with $n < p$. Let d be a positive integer, and let $X \in IRSS_d(q)$ be an invertible, regular, semisimple matrix over $\mathbb{F}_q$. Let $N_{poly}(q)$ be the number of polynomials $f \in SP_n(q)$ of the form $f(X,Y) = \sum_{k=0}^{n} a_k Y^k X^{n-k}$ for which there exists a solution $Y \in \mathbb{F}_q^{d \times d}$ to $f(X,Y) = 0$ with $XY \neq YX$. Then, for an absolute constant C we have that

$$N_{poly}(q) \leq C(n+1)n(n-1)d(d-1)q^{n-1},$$

and so the asymptotic upper bound $\frac{N_{poly}(q)}{|SP_n(q)|} = O\left(\frac{n^3 d^2}{q}\right)$ holds.

References

- J. Agler and J.E. McCarthy. *The Implicit Function Theorem and Free Algebraic Sets*. Trans. Amer. Math. Soc, 368 (5), 3157-3175 (2016).
- G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*, 6th ed. Oxford UP, 2008.
- J.M. Howie. *Fields and Galois Theory*. Springer, 2006.
- D.S. Kaliuzhnyi-Verbovetskyi and V. Vinnikov. *Foundations of Noncommutative Function Theory*. arXiv:1212.6345
- S. Lang. *Undergraduate Algebra*, 3rd ed. Springer, 2005.