# The Smith Normal Form of the Incidence Matrix of Skew Lines in $\mathrm{PG}(3, q)$

Peter Sin, University of Florida

JGT80 Cambridge, September 11, 2013 .

# Outline

# Skew lines graph

- Joint work with Andries Brouwer and Josh Ducey.
- We consider *skewness* of pairs of lines in $PG(3,q)$, $q = p^t$.
- Get strongly regular graph with parameters

  $$v = q^4+q^3+2q^2+q+1, k = q^4, \lambda = q^4-q^3-q^2+q, \mu = q^4-q^3.$$

- Under the Klein Correpondence, two lines are skew iff the corresponding points of the Klein quadric in $PG(5,q)$ are not orthogonal, i.e, not joined by a line in the quadric.
- Adjacency matrix $A$, Laplacian $L = D - A$, $D$ diagonal matrix of degrees. In our case $D = q^4 I$.

# Skew lines graph

- Joint work with Andries Brouwer and Josh Ducey.
- We consider *skewness* of pairs of lines in $PG(3, q)$, $q = p^t$.
- Get strongly regular graph with parameters

$$v = q^4+q^3+2q^2+q+1, k = q^4, \lambda = q^4-q^3-q^2+q, \mu = q^4-q^3.$$

- Under the Klein Correpondence, two lines are skew iff the corresponding points of the Klein quadric in $PG(5, q)$ are not orthogonal, i.e, not joined by a line in the quadric.
- Adjacency matrix $A$, Laplacian $L = D - A$, $D$ diagonal matrix of degrees. In our case $D = q^4 I$.

# Skew lines graph

- Joint work with Andries Brouwer and Josh Ducey.
- We consider *skewness* of pairs of lines in $PG(3,q)$, $q = p^t$.
- Get strongly regular graph with parameters

$$v = q^4+q^3+2q^2+q+1, k = q^4, \lambda = q^4-q^3-q^2+q, \mu = q^4-q^3.$$

- Under the Klein Correpondence, two lines are skew iff the corresponding points of the Klein quadric in $PG(5,q)$ are not orthogonal, i.e, not joined by a line in the quadric.
- Adjacency matrix $A$, Laplacian $L = D - A$, $D$ diagonal matrix of degrees. In our case $D = q^4 I$.

# Skew lines graph

- Joint work with Andries Brouwer and Josh Ducey.
- We consider *skewness* of pairs of lines in $PG(3, q)$, $q = p^t$.
- Get strongly regular graph with parameters

  $$v = q^4+q^3+2q^2+q+1, k = q^4, \lambda = q^4-q^3-q^2+q, \mu = q^4-q^3.$$

- Under the Klein Correpondence, two lines are skew iff the corresponding points of the Klein quadric in $PG(5, q)$ are not orthogonal, i.e, not joined by a line in the quadric.
- Adjacency matrix $A$, Laplacian $L = D - A$, $D$ diagonal matrix of degrees. In our case $D = q^4 I$.

# Skew lines graph

- Joint work with Andries Brouwer and Josh Ducey.
- We consider *skewness* of pairs of lines in $PG(3, q)$, $q = p^t$.
- Get strongly regular graph with parameters

$$v = q^4+q^3+2q^2+q+1, k = q^4, \lambda = q^4-q^3-q^2+q, \mu = q^4-q^3.$$

- Under the Klein Correpondence, two lines are skew iff the corresponding points of the Klein quadric in $PG(5, q)$ are not orthogonal, i.e, not joined by a line in the quadric.
- Adjacency matrix $A$, Laplacian $L = D - A$, $D$ diagonal matrix of degrees. In our case $D = q^4 I$.

# Smith normal forms

$A$, $L$ define endomorphisms of the free $\mathbb{Z}$-module on lines.

Cokernel of $A$ is called the *Smith group* and the torsion subgroup of the cokernel of $L$ is known as the *critical group* or *sandpile group*.

The order of the critical group is the number of spanning trees in the graph.

In our case $A$ and $L$ are closely related, and it suffices to consider the Smith group.

We compute it by using its structure as a module for $\mathrm{GL}(4, q)$.

# Smith normal forms

$A$, $L$ define endomorphisms of the free $\mathbb{Z}$-module on lines.

Cokernel of $A$ is called the *Smith group* and the torsion subgroup of the cokernel of $L$ is known as the *critical group* or *sandpile group*.

The order of the critical group is the number of spanning trees in the graph.

In our case $A$ and $L$ are closely related, and it suffices to consider the Smith group.

We compute it by using its structure as a module for $\mathrm{GL}(4, q)$.

# Smith normal forms

$A$, $L$ define endomorphisms of the free $\mathbb{Z}$-module on lines.

Cokernel of $A$ is called the *Smith group* and the torsion subgroup of the cokernel of $L$ is known as the *critical group* or *sandpile group*.

The order of the critical group is the number of spanning trees in the graph.

In our case $A$ and $L$ are closely related, and it suffices to consider the Smith group.

We compute it by using its structure as a module for $\mathrm{GL}(4, q)$.

# Smith normal forms

$A$, $L$ define endomorphisms of the free $\mathbb{Z}$-module on lines.

Cokernel of $A$ is called the *Smith group* and the torsion subgroup of the cokernel of $L$ is known as the *critical group* or *sandpile group*.

The order of the critical group is the number of spanning trees in the graph.

In our case $A$ and $L$ are closely related, and it suffices to consider the Smith group.

We compute it by using its structure as a module for $\mathrm{GL}(4, q)$.

# Smith normal forms

$A$, $L$ define endomorphisms of the free $\mathbb{Z}$-module on lines.

Cokernel of $A$ is called the *Smith group* and the torsion subgroup of the cokernel of $L$ is known as the *critical group* or *sandpile group*.

The order of the critical group is the number of spanning trees in the graph.

In our case $A$ and $L$ are closely related, and it suffices to consider the Smith group.

We compute it by using its structure as a module for $\mathrm{GL}(4, q)$.

# Outline

# All invariants are powers of $p$

The adjacency matrix of any $SRG(v, k, \lambda, \mu)$ satisfies

$$A^2 + (\mu - \lambda)A + (\mu - k)I = \mu J$$

($J$ is the all-one matrix)

$A^2 = q^4 I + (q^4 - q^3 - q^2 + q)A + (q^4 - q^3)(J - A - I)$

Eigenvalues of $A$ are $q$, $-q^2$, and $q^4$ with respective multiplicities $q^4 + q^2$, $q^3 + q^2 + q$, and 1.

Replace **Z** by a suitable $p$-adic ring $R = \mathbb{Z}_p[\xi]$, with $\xi$ a primitive $(q^4 - 1)$-th root of unity.

# All invariants are powers of $p$

The adjacency matrix of any $SRG(v, k, \lambda, \mu)$ satisfies

$$A^2 + (\mu - \lambda)A + (\mu - k)I = \mu J$$

($J$ is the all-one matrix)

$A^2 = q^4 I + (q^4 - q^3 - q^2 + q)A + (q^4 - q^3)(J - A - I)$

Eigenvalues of $A$ are $q$, $-q^2$, and $q^4$ with respective multiplicities $q^4 + q^2$, $q^3 + q^2 + q$, and 1.

Replace **Z** by a suitable $p$-adic ring $R = \mathbb{Z}_p[\xi]$, with $\xi$ a primitive $(q^4 - 1)$-th root of unity.

# All invariants are powers of $p$

The adjacency matrix of any $SRG(v, k, \lambda, \mu)$ satisfies

$$A^2 + (\mu - \lambda)A + (\mu - k)I = \mu J$$

($J$ is the all-one matrix)

$A^2 = q^4 I + (q^4 - q^3 - q^2 + q)A + (q^4 - q^3)(J - A - I)$

Eigenvalues of $A$ are $q$, $-q^2$, and $q^4$ with respective multiplicities $q^4 + q^2$, $q^3 + q^2 + q$, and 1.

Replace $\mathbf{Z}$ by a suitable $p$-adic ring $R = \mathbb{Z}_p[\xi]$, with $\xi$ a primitive $(q^4 - 1)$-th root of unity.

# All invariants are powers of $p$

The adjacency matrix of any $SRG(v, k, \lambda, \mu)$ satisfies

$$A^2 + (\mu - \lambda)A + (\mu - k)I = \mu J$$

($J$ is the all-one matrix)

$A^2 = q^4 I + (q^4 - q^3 - q^2 + q)A + (q^4 - q^3)(J - A - I)$

Eigenvalues of $A$ are $q$, $-q^2$, and $q^4$ with respective multiplicities $q^4 + q^2$, $q^3 + q^2 + q$, and 1.

Replace **Z** by a suitable $p$-adic ring $R = \mathbb{Z}_p[\xi]$, with $\xi$ a primitive $(q^4 - 1)$-th root of unity.

## Theorem 1

*Let $e_i = e_i(A)$ = number of invariant factors in the Smith Normal Form of $A$ which are exactly divisible by $p^i$.*

1. $e_{4t} = 1$.
2. $e_i = 0$ for $i > 4t$ and for $t < i < 2t$, $3t < i < 4t$.
3. $e_i = e_{3t-i}$ for $0 \leq i < t$.
4. $\sum_{i=0}^{t} e_i = q^4 + q^2$.
5. $\sum_{i=2t}^{3t} e_i = q^3 + q^2 + q$.

Thus we are reduced to finding $t$ of the numbers $e_0, \ldots, e_t$ (or the numbers $e_{2t}, \ldots, e_{3t}$).

## Theorem 1

*Let $e_i = e_i(A) =$ number of invariant factors in the Smith Normal Form of $A$ which are exactly divisible by $p^i$.*

1. $e_{4t} = 1$.
2. $e_i = 0$ for $i > 4t$ and for $t < i < 2t, 3t < i < 4t$.
3. $e_i = e_{3t-i}$ for $0 \leq i < t$.
4. $\sum_{i=0}^{t} e_i = q^4 + q^2$.
5. $\sum_{i=2t}^{3t} e_i = q^3 + q^2 + q$.

Thus we are reduced to finding $t$ of the numbers $e_0, \ldots, e_t$ (or the numbers $e_{2t}, \ldots, e_{3t}$).

## Theorem 1

*Let $e_i = e_i(A)$ = number of invariant factors in the Smith Normal Form of $A$ which are exactly divisible by $p^i$.*

1. $e_{4t} = 1$.
2. $e_i = 0$ for $i > 4t$ and for $t < i < 2t$, $3t < i < 4t$.
3. $e_i = e_{3t-i}$ for $0 \leq i < t$.
4. $\sum_{i=0}^{t} e_i = q^4 + q^2$.
5. $\sum_{i=2t}^{3t} e_i = q^3 + q^2 + q$.

Thus we are reduced to finding $t$ of the numbers $e_0, \ldots, e_t$ (or the numbers $e_{2t}, \ldots, e_{3t}$).

## Theorem 1

*Let $e_i = e_i(A)$ = number of invariant factors in the Smith Normal Form of $A$ which are exactly divisible by $p^i$.*

1. $e_{4t} = 1$.
2. $e_i = 0$ for $i > 4t$ and for $t < i < 2t$, $3t < i < 4t$.
3. $e_i = e_{3t-i}$ for $0 \leq i < t$.
4. $\sum_{i=0}^{t} e_i = q^4 + q^2$.
5. $\sum_{i=2t}^{3t} e_i = q^3 + q^2 + q$.

Thus we are reduced to finding $t$ of the numbers $e_0, \ldots, e_t$ (or the numbers $e_{2t}, \ldots, e_{3t}$).

## Theorem 1

*Let $e_i = e_i(A) =$ number of invariant factors in the Smith Normal Form of $A$ which are exactly divisible by $p^i$.*

1. $e_{4t} = 1$.
2. $e_i = 0$ for $i > 4t$ and for $t < i < 2t$, $3t < i < 4t$.
3. $e_i = e_{3t-i}$ for $0 \le i < t$.
4. $\sum_{i=0}^{t} e_i = q^4 + q^2$.
5. $\sum_{i=2t}^{3t} e_i = q^3 + q^2 + q$.

Thus we are reduced to finding $t$ of the numbers $e_0, \ldots, e_t$ (or the numbers $e_{2t}, \ldots, e_{3t}$).

## Theorem 1

*Let $e_i = e_i(A) =$ number of invariant factors in the Smith Normal Form of $A$ which are exactly divisible by $p^i$.*

1. $e_{4t} = 1$.
2. $e_i = 0$ *for* $i > 4t$ *and for* $t < i < 2t, 3t < i < 4t$.
3. $e_i = e_{3t-i}$ *for* $0 \leq i < t$.
4. $\sum_{i=0}^{t} e_i = q^4 + q^2$.
5. $\sum_{i=2t}^{3t} e_i = q^3 + q^2 + q$.

Thus we are reduced to finding $t$ of the numbers $e_0, \ldots, e_t$ (or the numbers $e_{2t}, \ldots, e_{3t}$).

## Theorem 1

*Let $e_i = e_i(A) =$ number of invariant factors in the Smith Normal Form of $A$ which are exactly divisible by $p^i$.*

1. $e_{4t} = 1$.
2. $e_i = 0$ *for* $i > 4t$ *and for* $t < i < 2t, 3t < i < 4t$.
3. $e_i = e_{3t-i}$ *for* $0 \le i < t$.
4. $\sum_{i=0}^{t} e_i = q^4 + q^2$.
5. $\sum_{i=2t}^{3t} e_i = q^3 + q^2 + q$.

Thus we are reduced to finding $t$ of the numbers $e_0, \ldots, e_t$ (or the numbers $e_{2t}, \ldots, e_{3t}$).

## Theorem 1

*Let $e_i = e_i(A) =$ number of invariant factors in the Smith Normal Form of $A$ which are exactly divisible by $p^i$.*

1. $e_{4t} = 1$.
2. $e_i = 0$ *for* $i > 4t$ *and for* $t < i < 2t$, $3t < i < 4t$.
3. $e_i = e_{3t-i}$ *for* $0 \le i < t$.
4. $\sum_{i=0}^{t} e_i = q^4 + q^2$.
5. $\sum_{i=2t}^{3t} e_i = q^3 + q^2 + q$.

Thus we are reduced to finding $t$ of the numbers $e_0, \ldots, e_t$ (or the numbers $e_{2t}, \ldots, e_{3t}$).

# Outline

Skew lines in $PG(3, q)$

Eigenvalues and invariants

$p$-filtrations

Proof of Theorem 1

The missing invariants

Reduction to Point-Line Incidence

SNF of a product

# $p$-filtrations

Let $\mathrm{F} = R/(p)$.

For $L \leq R^{\ell}$, set $\overline{L} = (L + pR^{\ell})/pR^{\ell}$.

$\eta\colon R^m \to R^n$, $R$-module homomorphism

$M_i(\eta) = \{x \in R^m \mid \eta(x) \in p^i R^n\}$

$N_i(\eta) = \{p^{-i}\eta(x) \mid x \in M_i(\eta)\}$ (and $N_{-1}(\eta) = \{0\}$)

$R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$

$N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$

$\mathrm{F}^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$

$\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

# $p$-filtrations

Let $\mathrm{F} = R/(p)$.

For $L \leq R^\ell$, set $\overline{L} = (L + pR^\ell)/pR^\ell$.

$\eta\colon R^m \to R^n$, $R$-module homomorphism

$M_i(\eta) = \{x \in R^m \mid \eta(x) \in p^i R^n\}$

$N_i(\eta) = \{p^{-i}\eta(x) \mid x \in M_i(\eta)\}$ (and $N_{-1}(\eta) = \{0\}$)

$R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$

$N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$

$\mathrm{F}^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$

$\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

# $p$-filtrations

Let $\mathrm{F} = R/(p)$.

For $L \leq R^\ell$, set $\overline{L} = (L + pR^\ell)/pR^\ell$.

$\eta\colon R^m \to R^n$, $R$-module homomorphism

$M_i(\eta) = \{x \in R^m \mid \eta(x) \in p^i R^n\}$

$N_i(\eta) = \{p^{-i}\eta(x) \mid x \in M_i(\eta)\}$ (and $N_{-1}(\eta) = \{0\}$)

$R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$

$N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$

$\mathrm{F}^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$

$\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

# $p$-filtrations

Let $\mathrm{F} = R/(p)$.

For $L \leq R^\ell$, set $\overline{L} = (L + pR^\ell)/pR^\ell$.

$\eta\colon R^m \to R^n$, $R$-module homomorphism

$M_i(\eta) = \{x \in R^m \mid \eta(x) \in p^i R^n\}$

$N_i(\eta) = \{p^{-i}\eta(x) \mid x \in M_i(\eta)\}$ (and $N_{-1}(\eta) = \{0\}$)

$R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$

$N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$

$\mathrm{F}^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$

$\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

# $p$-filtrations

Let $\mathrm{F} = R/(p)$.

For $L \leq R^\ell$, set $\overline{L} = (L + pR^\ell)/pR^\ell$.

$\eta\colon R^m \to R^n$, $R$-module homomorphism

$M_i(\eta) = \{x \in R^m \mid \eta(x) \in p^i R^n\}$

$N_i(\eta) = \{p^{-i}\eta(x) \mid x \in M_i(\eta)\}$ (and $N_{-1}(\eta) = \{0\}$)

$R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$

$N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$

$\mathrm{F}^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$

$\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

# $p$-filtrations

Let $\mathrm{F} = R/(p)$.

For $L \leq R^\ell$, set $\overline{L} = (L + pR^\ell)/pR^\ell$.

$\eta\colon R^m \to R^n$, $R$-module homomorphism

$M_i(\eta) = \{x \in R^m \mid \eta(x) \in p^i R^n\}$

$N_i(\eta) = \{p^{-i}\eta(x) \mid x \in M_i(\eta)\}$ (and $N_{-1}(\eta) = \{0\}$)

$R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$

$N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$

$\mathrm{F}^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$

$\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

# $p$-filtrations

Let $\mathrm{F} = R/(p)$.

For $L \leq R^\ell$, set $\overline{L} = (L + pR^\ell)/pR^\ell$.

$\eta \colon R^m \to R^n$, $R$-module homomorphism

$M_i(\eta) = \{x \in R^m \mid \eta(x) \in p^i R^n\}$

$N_i(\eta) = \{p^{-i}\eta(x) \mid x \in M_i(\eta)\}$ (and $N_{-1}(\eta) = \{0\}$)

$R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$

$N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$

$\mathrm{F}^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$

$\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

# $p$-filtrations

Let $\mathrm{F} = R/(p)$.

For $L \leq R^\ell$, set $\overline{L} = (L + pR^\ell)/pR^\ell$.

$\eta\colon R^m \to R^n$, $R$-module homomorphism

$M_i(\eta) = \{x \in R^m \mid \eta(x) \in p^i R^n\}$

$N_i(\eta) = \{p^{-i}\eta(x) \mid x \in M_i(\eta)\}$ (and $N_{-1}(\eta) = \{0\}$)

$R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$

$N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$

$\mathrm{F}^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$

$\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

## Lemma

*Let $\eta\colon R^m \to R^n$ be a homomorphism of free $R$-modules of finite rank. Then, for $i \geq 0$,*

$$e_i(\eta) = \dim_{\mathrm{F}}\left(\overline{M_i(\eta)}/\overline{M_{i+1}(\eta)}\right) = \dim_{\mathrm{F}}\left(\overline{N_i(\eta)}/\overline{N_{i-1}(\eta)}\right).$$

# Outline

- Skew lines in $PG(3, q)$
- Eigenvalues and invariants
- $p$-filtrations
- Proof of Theorem 1
- The missing invariants
- Reduction to Point-Line Incidence
- SNF of a product

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$

$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.

$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$

$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$

$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$

$(\mathbf{1})A = q^4 \mathbf{1}$

Let $A' = A|_{Y_2}$ (or its matrix in some basis).

$e_{4t}(A) = e_{4t}(A') + 1$

$e_i(A) = e_i(A')$ for $i \neq 4t$.

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$
$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.
$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
$(\mathbf{1})A = q^4 \mathbf{1}$
Let $A' = A|_{Y_2}$ (or its matrix in some basis).
$e_{4t}(A) = e_{4t}(A') + 1$
$e_i(A) = e_i(A')$ for $i \neq 4t$.

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$
$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.
$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
$(\mathbf{1})A = q^4 \mathbf{1}$
Let $A' = A|_{Y_2}$ (or its matrix in some basis).
$e_{4t}(A) = e_{4t}(A') + 1$
$e_i(A) = e_i(A')$ for $i \neq 4t$.

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$

$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.

$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$

$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \;\middle|\; \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$

$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$

$(\mathbf{1})A = q^4 \mathbf{1}$

Let $A' = A|_{Y_2}$ (or its matrix in some basis).

$e_{4t}(A) = e_{4t}(A') + 1$

$e_i(A) = e_i(A')$ for $i \neq 4t$.

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$

$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.

$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$

$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$

$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$

$(\mathbf{1})A = q^4 \mathbf{1}$

Let $A' = A|_{Y_2}$ (or its matrix in some basis).

$e_{4t}(A) = e_{4t}(A') + 1$

$e_i(A) = e_i(A')$ for $i \neq 4t$.

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$

$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.

$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$

$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$

$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$

$(\mathbf{1})A = q^4 \mathbf{1}$

Let $A' = A|_{Y_2}$ (or its matrix in some basis).

$e_{4t}(A) = e_{4t}(A') + 1$

$e_i(A) = e_i(A')$ for $i \neq 4t$.

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$
$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.
$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \;\middle|\; \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
$(\mathbf{1})A = q^4 \mathbf{1}$
Let $A' = A|_{Y_2}$ (or its matrix in some basis).
$e_{4t}(A) = e_{4t}(A') + 1$
$e_i(A) = e_i(A')$ for $i \neq 4t$.

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$

$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.

$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$

$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$

$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$

$(\mathbf{1})A = q^4 \mathbf{1}$

Let $A' = A|_{Y_2}$ (or its matrix in some basis).

$e_{4t}(A) = e_{4t}(A') + 1$

$e_i(A) = e_i(A')$ for $i \neq 4t$.

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$

$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.

$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$

$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \;\middle|\; \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$

$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$

$(\mathbf{1})A = q^4 \mathbf{1}$

Let $A' = A|_{Y_2}$ (or its matrix in some basis).

$e_{4t}(A) = e_{4t}(A') + 1$

$e_i(A) = e_i(A')$ for $i \neq 4t$.

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$
$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.
$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
$(\mathbf{1})A = q^4 \mathbf{1}$
Let $A' = A|_{Y_2}$ (or its matrix in some basis).
$e_{4t}(A) = e_{4t}(A') + 1$
$e_i(A) = e_i(A')$ for $i \neq 4t$.

# Split off the all-one vector

$V$, a 4-dimensional vector space over $\mathbb{F}_q$
$\mathcal{L}_r =$ set of subspaces of dimension $r$ in $V$

View $A$ as an $R$-module map $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$.
$\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
$Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
$R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
$(\mathbf{1})A = q^4 \mathbf{1}$
Let $A' = A|_{Y_2}$ (or its matrix in some basis).
$e_{4t}(A) = e_{4t}(A') + 1$
$e_i(A) = e_i(A')$ for $i \neq 4t$.

# SRG equation

$$A(A+(q^2-q)I) = q^3 I + (q^4-q^3)J$$

On $Y_2$, $A'(A'+(q^2-q)I) = q^3 I$.

Let $P$ and $Q$ be unimodular, with $D = PA'Q^{-1}$ diagonal. Then

$$Q(A'+(q^2-q)I)P^{-1} = q^3 D^{-1},$$

# SRG equation

$A(A+(q^2-q)I) = q^3 I + (q^4-q^3)J$

On $Y_2$, $A'(A'+(q^2-q)I) = q^3 I$.

Let $P$ and $Q$ be unimodular, with $D = PA'Q^{-1}$ diagonal. Then

$$Q(A'+(q^2-q)I)P^{-1} = q^3 D^{-1},$$

# SRG equation

$A(A+(q^2-q)I) = q^3 I + (q^4-q^3)J$

On $Y_2$, $A'(A'+(q^2-q)I) = q^3 I$.

Let $P$ and $Q$ be unimodular, with $D = PA'Q^{-1}$ diagonal. Then

$$Q(A'+(q^2-q)I)P^{-1} = q^3 D^{-1},$$

$$Q(A' + (q^2 - q)I)P^{-1} = q^3 D^{-1}$$

$e_i(A') = 0$ for $i > 3t$.

$e_{4t}(A) = 1$

$e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$for $0 \leq i \leq 3t$.

$Q(A' + (q^2 - q)I)P^{-1} = q^3 D^{-1}$

$e_i(A') = 0$ for $i > 3t$.

$e_{4t}(A) = 1$

$e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$for $0 \leq i \leq 3t$.

$Q(A' + (q^2 - q)I)P^{-1} = q^3 D^{-1}$

$e_i(A') = 0$ for $i > 3t$.

$e_{4t}(A) = 1$

$e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$for $0 \leq i \leq 3t$.

$$Q(A' + (q^2 - q)I)P^{-1} = q^3 D^{-1}$$
$e_i(A') = 0$ for $i > 3t$.
$$e_{4t}(A) = 1$$
$e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$for $0 \leq i \leq 3t$.

# Proof of Theorem 1

$A' \equiv A' + (q^2 - q)I \pmod{p^t}$

$e_i(A') = e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$, for $0 \le i < t$

Set $E := \mathrm{Frac}(R) \otimes_R R^{\mathcal{L}_2}$

$E_\lambda := \lambda$-eigenspace for $A$ in $E$.

$E_q \cap R^{\mathcal{L}_2}$ and $E_{-q^2} \cap R^{\mathcal{L}_2}$ are pure $R$-submodules of $Y_2$.

$E_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $E_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.

$$q^4 + q^2 = \dim_{\mathbb{F}}(\overline{E_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathbb{F}} \overline{N_t(A')} = \sum_{i=0}^{t} e_i(A')$$

and

$$q^3+q^2+q = \dim_{\mathbb{F}}(\overline{E_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathbb{F}} \overline{M_{2t}(A')} = \sum_{i=2t}^{3t} e_i(A').$$

Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_{\mathbb{F}} \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other $i$.

# Proof of Theorem 1

$A' \equiv A' + (q^2 - q)I \pmod{p^t}$

$e_i(A') = e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$, for $0 \le i < t$

Set $E := \mathrm{Frac}(R) \otimes_R R^{\mathcal{L}_2}$

$E_\lambda := \lambda$-eigenspace for $A$ in $E$.

$E_q \cap R^{\mathcal{L}_2}$ and $E_{-q^2} \cap R^{\mathcal{L}_2}$ are pure $R$-submodules of $Y_2$.

$E_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $E_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.

$$q^4 + q^2 = \dim_{\mathbb{F}}(\overline{E_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathbb{F}} \overline{N_t(A')} = \sum_{i=0}^{t} e_i(A')$$

and

$$q^3 + q^2 + q = \dim_{\mathbb{F}}(\overline{E_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathbb{F}} \overline{M_{2t}(A')} = \sum_{i=2t}^{3t} e_i(A').$$

Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_{\mathbb{F}} \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other $i$.

# Proof of Theorem 1

$A' \equiv A' + (q^2 - q)I \pmod{p^t}$
$e_i(A') = e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$, for $0 \le i < t$
Set $E := \mathrm{Frac}(R) \otimes_R R^{\mathcal{L}_2}$
$E_\lambda := \lambda$-eigenspace for $A$ in $E$.
$E_q \cap R^{\mathcal{L}_2}$ and $E_{-q^2} \cap R^{\mathcal{L}_2}$ are pure $R$-submodules of $Y_2$.
$E_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $E_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.

$$q^4 + q^2 = \dim_{\mathrm{F}}(\overline{E_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathrm{F}} \overline{N_t(A')} = \sum_{i=0}^{t} e_i(A')$$

and

$$q^3 + q^2 + q = \dim_{\mathrm{F}}(\overline{E_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathrm{F}} \overline{M_{2t}(A')} = \sum_{i=2t}^{3t} e_i(A').$$

Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_{\mathrm{F}} \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other $i$.

# Proof of Theorem 1

$A' \equiv A' + (q^2 - q)I \pmod{p^t}$
$e_i(A') = e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$, for $0 \le i < t$
Set $E := \mathrm{Frac}(R) \otimes_R R^{\mathcal{L}_2}$
$E_\lambda := \lambda$-eigenspace for $A$ in $E$.
$E_q \cap R^{\mathcal{L}_2}$ and $E_{-q^2} \cap R^{\mathcal{L}_2}$ are pure $R$-submodules of $Y_2$.
$E_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $E_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.

$$q^4 + q^2 = \dim_{\mathrm{F}}(\overline{E_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathrm{F}} \overline{N_t(A')} = \sum_{i=0}^{t} e_i(A')$$

and

$$q^3 + q^2 + q = \dim_{\mathrm{F}}(\overline{E_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathrm{F}} \overline{M_{2t}(A')} = \sum_{i=2t}^{3t} e_i(A').$$

Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_{\mathrm{F}} \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other $i$.

# Proof of Theorem 1

$A' \equiv A' + (q^2 - q)I \pmod{p^t}$
$e_i(A') = e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$, for $0 \le i < t$
Set $E := \mathrm{Frac}(R) \otimes_R R^{\mathcal{L}_2}$
$E_\lambda := \lambda$-eigenspace for $A$ in $E$.
$E_q \cap R^{\mathcal{L}_2}$ and $E_{-q^2} \cap R^{\mathcal{L}_2}$ are pure $R$-submodules of $Y_2$.
$E_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $E_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.

$$q^4 + q^2 = \dim_{\mathbb{F}}(\overline{E_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathbb{F}} \overline{N_t(A')} = \sum_{i=0}^{t} e_i(A')$$

and

$$q^3 + q^2 + q = \dim_{\mathbb{F}}(\overline{E_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathbb{F}} \overline{M_{2t}(A')} = \sum_{i=2t}^{3t} e_i(A').$$

Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_{\mathbb{F}} \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other $i$.

# Proof of Theorem 1

$A' \equiv A' + (q^2 - q)I \pmod{p^t}$

$e_i(A') = e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$, for $0 \leq i < t$

Set $E := \mathrm{Frac}(R) \otimes_R R^{\mathcal{L}_2}$

$E_\lambda := \lambda$-eigenspace for $A$ in $E$.

$E_q \cap R^{\mathcal{L}_2}$ and $E_{-q^2} \cap R^{\mathcal{L}_2}$ are pure $R$-submodules of $Y_2$.

$E_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $E_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.

$$q^4 + q^2 = \dim_{\mathbb{F}}(\overline{E_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_{\mathbb{F}} \overline{N_t(A')} = \sum_{i=0}^{t} e_i(A')$$

and

$$q^3 + q^2 + q = \dim_{\mathbb{F}}(\overline{E_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_{\mathbb{F}} \overline{M_{2t}(A')} = \sum_{i=2t}^{3t} e_i(A').$$

Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_{\mathbb{F}} \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other $i$.

# Proof of Theorem 1

$A' \equiv A' + (q^2 - q)I \pmod{p^t}$
$e_i(A') = e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$, for $0 \le i < t$
Set $E := \mathrm{Frac}(R) \otimes_R R^{\mathcal{L}_2}$
$E_\lambda := \lambda$-eigenspace for $A$ in $E$.
$E_q \cap R^{\mathcal{L}_2}$ and $E_{-q^2} \cap R^{\mathcal{L}_2}$ are pure $R$-submodules of $Y_2$.
$E_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $E_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.

$$q^4 + q^2 = \dim_{\mathrm{F}}(\overline{E_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathrm{F}} \overline{N_t(A')} = \sum_{i=0}^{t} e_i(A')$$

and

$$q^3 + q^2 + q = \dim_{\mathrm{F}}(\overline{E_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_{\mathrm{F}} \overline{M_{2t}(A')} = \sum_{i=2t}^{3t} e_i(A').$$

Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_{\mathrm{F}} \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other $i$.

# Proof of Theorem 1

$A' \equiv A' + (q^2 - q)I \pmod{p^t}$
$e_i(A') = e_i(A' + (q^2 - q)I) = e_{3t-i}(A')$, for $0 \le i < t$
Set $E := \mathrm{Frac}(R) \otimes_R R^{\mathcal{L}_2}$
$E_\lambda :=$ $\lambda$-eigenspace for $A$ in $E$.
$E_q \cap R^{\mathcal{L}_2}$ and $E_{-q^2} \cap R^{\mathcal{L}_2}$ are pure $R$-submodules of $Y_2$.
$E_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $E_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.

$$q^4 + q^2 = \dim_{\mathrm{F}} \overline{(E_q \cap \mathbb{Z}_p^{\mathcal{L}_2})} \le \dim_{\mathrm{F}} \overline{N_t(A')} = \sum_{i=0}^{t} e_i(A')$$

and

$$q^3 + q^2 + q = \dim_{\mathrm{F}} \overline{(E_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2})} \le \dim_{\mathrm{F}} \overline{M_{2t}(A')} = \sum_{i=2t}^{3t} e_i(A').$$

Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_{\mathrm{F}} \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other $i$.

## Remark

- Proof uses only the SRG equation, so Theorem 1 is valid for all SRGs with the same parameters. For $q = 2$, there are 3854 such SRGs (Spence).
- When $q = p$, the Smith group is determined once we know $e_0 = \mathrm{rank}_p A$. When $q = 2$, our $A$ is the unique one with $\mathrm{rank}_2 A = 6$.

## Remark

- Proof uses only the SRG equation, so Theorem 1 is valid for all SRGs with the same parameters. For $q = 2$, there are 3854 such SRGs (Spence).
- When $q = p$, the Smith group is determined once we know $e_0 = \mathrm{rank}_p A$. When $q = 2$, our $A$ is the unique one with $\mathrm{rank}_2 A = 6$.

# Outline

# Statement of Theorem 2

$[3]^t = \{(s_0, \dots, s_{t-1}) \,|\, s_i \in \{1, 2, 3\} \text{ for all } i\}$
For $\mathbf{s} = (s_0, \dots, s_{t-1}) \in [3]^t$

$$\lambda_i = ps_{i+1} - s_i,$$

(subscripts mod $t$) and

$$\lambda = (\lambda_0, \dots, \lambda_{t-1})$$

For an integer $k$, set $d_k$ to be the coefficient of $x^k$ in the expansion of $(1 + x + \cdots + x^{p-1})^4$. Set $d(\mathbf{s}) = \prod_{i=0}^{t-1} d_{\lambda_i}$.

## Theorem 2

*Let $e_i = e_i(A)$ denote the multiplicity of $p^i$ as an elementary divisor of $A$.*
*Then, for $0 \leq i \leq t$,*

$$e_{2t+i} = \sum_{\mathbf{s} \in \mathcal{H}(i)} d(\mathbf{s}),$$

*where*

$$\mathcal{H}(i) = \left\{(s_0, \ldots, s_{t-1}) \in [3]^t \,\middle|\, d(\mathbf{s}) \neq 0 \text{ and } \#\{j | s_j = 2\} = i\right\}.$$

# Example, $q = 9$

$$(1 + x + x^2)^4 =$$
$$1 + 4x + 10x^2 + 16x^3 + 19x^4 + 16x^5 + 10x^6 + 4x^7 + x^8$$

$$\mathcal{H}(0) = \{(11), (13), (31), (33)\},$$
$$\mathcal{H}(1) = \{(21), (23), (12), (32)\}, \mathcal{H}(2) = \{(22)\}.$$

$$e_4 = d(11) + d(13) + d(31) + d(33) = 202$$

$$e_5 = d(21) + d(23) + d(12) + d(32) = 256$$

$$e_6 = d(22) = 361$$

Table: The elementary divisors of the incidence matrix of lines vs. lines in $\mathrm{PG}(3,9)$, where two lines are incident when skew.

| Elem. Div. | 1 | 3 | $3^2$ | $3^4$ | $3^5$ | $3^6$ | $3^8$ |
|---|---|---|---|---|---|---|---|
| Multiplicity | 361 | 256 | 6025 | 202 | 256 | 361 | 1 |

**Theorem (Bardoe-S, 2000)**

(a) *The* $\mathrm{F}\,\mathrm{GL}(4, q)$*-permutation module* $\mathrm{F}^{\mathcal{L}_1} = \mathrm{F}\mathbf{1} \oplus \overline{Y}_1$ *is multiplicity-free and the composition factors of* $\overline{Y}_1$ *correspond to*

$$\mathcal{H} = \{\mathbf{s} \in [3]^t \mid d(\mathbf{s}) \neq 0\}.$$

*and* $d(\mathbf{s})$ *gives the dimension.*

(b) *If we define the partial order* $\mathbf{s} \leq \mathbf{s}'$ *iff* $s_i \leq s'_i$ *for all* $i$*, then the lattice of order ideals is isomorphic to the* $\mathrm{F}\,\mathrm{GL}(4, q)$*-submodule lattice of* $\overline{Y}_1$*.*

**Remark**

Each subquotient of the $\mathrm{F}\,\mathrm{GL}(4, q)$-module $\overline{Y}_1$ determines a subset of $\mathcal{H}$ correponding to its composition factors.

# Outline

$B :=$ the incidence matrix with rows indexed by $\mathcal{L}_1$ and columns indexed by $\mathcal{L}_2$, where incidence again means zero intersection.

$$B^tB = (q^3+q^2)I + (q^3+q^2-q-1)A + (q^3+q^2-q)(J-A-I).$$

$(\mathbf{1})B^tB = q^4(q^2+q+1)(q+1)\mathbf{1}$,
$e_i(B^tB) = e_i(B^tB|_{Y_2})$ for $i \neq 4t$.
$B^tB = -[A+(q^2-q)I] + q^2I + (q^3+q^2-q)J$
On $Y_2$, $B^tB = -[A+(q^2-q)I] + q^2I$.
$e_i((B^tB)|_{Y_2}) = e_i(A' + (q^2-q)I) = e_{3t-i}(A)$, for $0 \leq i \leq t$.

$B :=$ the incidence matrix with rows indexed by $\mathcal{L}_1$ and columns indexed by $\mathcal{L}_2$, where incidence again means zero intersection.

$$B^t B = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I).$$

$(\mathbf{1})B^t B = q^4(q^2+q+1)(q+1)\mathbf{1}$,

$e_i(B^t B) = e_i(B^t B|_{Y_2})$ for $i \neq 4t$.

$B^t B = -[A+(q^2-q)I]+q^2 I+(q^3+q^2-q)J$

On $Y_2$, $B^t B = -[A+(q^2-q)I]+q^2 I$.

$e_i((B^t B)|_{Y_2}) = e_i(A'+(q^2-q)I) = e_{3t-i}(A)$, for $0 \leq i \leq t$.

$B :=$ the incidence matrix with rows indexed by $\mathcal{L}_1$ and columns indexed by $\mathcal{L}_2$, where incidence again means zero intersection.

$B^t B = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I).$

$(\mathbf{1})B^t B = q^4(q^2+q+1)(q+1)\mathbf{1},$

$e_i(B^t B) = e_i(B^t B|_{Y_2})$ for $i \neq 4t$.

$B^t B = -[A+(q^2-q)I] + q^2 I + (q^3+q^2-q)J$

On $Y_2$, $B^t B = -[A+(q^2-q)I] + q^2 I$.

$e_i((B^t B)|_{Y_2}) = e_i(A' + (q^2-q)I) = e_{3t-i}(A)$, for $0 \leq i \leq t$.

$B :=$ the incidence matrix with rows indexed by $\mathcal{L}_1$ and columns indexed by $\mathcal{L}_2$, where incidence again means zero intersection.

$$B^t B = (q^3+q^2)I + (q^3+q^2-q-1)A + (q^3+q^2-q)(J-A-I).$$

$(\mathbf{1})B^t B = q^4(q^2+q+1)(q+1)\mathbf{1}$,
$e_i(B^t B) = e_i(B^t B|_{Y_2})$ for $i \neq 4t$.
$B^t B = -[A+(q^2-q)I] + q^2 I + (q^3+q^2-q)J$
On $Y_2$, $B^t B = -[A+(q^2-q)I] + q^2 I$.
$e_i((B^t B)|_{Y_2}) = e_i(A' + (q^2-q)I) = e_{3t-i}(A)$, for $0 \leq i \leq t$.

$B :=$ the incidence matrix with rows indexed by $\mathcal{L}_1$ and columns indexed by $\mathcal{L}_2$, where incidence again means zero intersection.

$$B^t B = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I).$$

$(\mathbf{1})B^t B = q^4(q^2+q+1)(q+1)\mathbf{1}$,

$e_i(B^t B) = e_i(B^t B|_{Y_2})$ for $i \neq 4t$.

$B^t B = -[A+(q^2-q)I] + q^2 I + (q^3+q^2-q)J$

On $Y_2$, $B^t B = -[A+(q^2-q)I] + q^2 I$.

$e_i((B^t B)|_{Y_2}) = e_i(A' + (q^2-q)I) = e_{3t-i}(A)$, for $0 \leq i \leq t$.

$B :=$ the incidence matrix with rows indexed by $\mathcal{L}_1$ and columns indexed by $\mathcal{L}_2$, where incidence again means zero intersection.

$$B^t B = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I).$$

$(\mathbf{1})B^t B = q^4(q^2+q+1)(q+1)\mathbf{1}$,

$e_i(B^t B) = e_i(B^t B|_{Y_2})$ for $i \neq 4t$.

$B^t B = -[A+(q^2-q)I] + q^2 I + (q^3+q^2-q)J$

On $Y_2$, $B^t B = -[A+(q^2-q)I] + q^2 I$.

$e_i((B^t B)|_{Y_2}) = e_i(A' + (q^2-q)I) = e_{3t-i}(A)$, for $0 \leq i \leq t$.

$B :=$ the incidence matrix with rows indexed by $\mathcal{L}_1$ and columns indexed by $\mathcal{L}_2$, where incidence again means zero intersection.

$$B^t B = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I).$$

$(\mathbf{1})B^t B = q^4(q^2+q+1)(q+1)\mathbf{1}$,

$e_i(B^t B) = e_i(B^t B|_{Y_2})$ for $i \neq 4t$.

$B^t B = -[A+(q^2-q)I] + q^2 I + (q^3+q^2-q)J$

On $Y_2$, $B^t B = -[A+(q^2-q)I] + q^2 I$.

$e_i((B^t B)|_{Y_2}) = e_i(A' + (q^2-q)I) = e_{3t-i}(A)$, for $0 \leq i \leq t$.

# Invariants of $B$

The $e_i(B)$ were previously calculated.

**Theorem (Chandler-S-Xiang, 2006)**

*Set* $B' := B|_{Y_1} : Y_1 \to Y_2$.

(a) *The composition factors of* $\overline{M}_k(B')/\overline{M}_{k+1}(B')$ *correspond to the set*

$$\mathcal{H}_k(2) = \{\mathbf{s} \in \mathcal{H} | \textit{exactly } k \textit{ of the } s_j \textit{ are equal to } 1\}.$$

(b) *The composition factors of* $\overline{N}_\ell({B'}^t)/\overline{N}_{\ell-1}({B'}^t)$ *correspond to*

$${}_\ell\mathcal{H}(2) = \{\mathbf{s} \in \mathcal{H} | \textit{exactly } \ell \textit{ of the } s_j \textit{ are equal to } 3\}.$$

# Outline

- Skew lines in $PG(3, q)$
- Eigenvalues and invariants
- $p$-filtrations
- Proof of Theorem 1
- The missing invariants
- Reduction to Point-Line Incidence
- SNF of a product

# Idea of proof for Theorem 2

Problem is to relate invariants of $B^t B$ to those of $B$.

Suppose that we can diagonalize $B^t$ and $B$ by:

$$PB^t E^{-1} = D_{2,1}$$

and

$$EBQ^{-1} = D_{1,2}$$

*with the same $E$ in both equations*.

Then we can diagonalize the product:

$$PB^t BQ^{-1} = D_{r,1} D_{1,s},$$

In general is not possible to find such a matrix $E$.

# Idea of proof for Theorem 2

Problem is to relate invariants of $B^t B$ to those of $B$.

Suppose that we can diagonalize $B^t$ and $B$ by:

$$PB^t E^{-1} = D_{2,1}$$

and

$$EBQ^{-1} = D_{1,2}$$

*with the same E in both equations*.

Then we can diagonalize the product:

$$PB^t BQ^{-1} = D_{r,1} D_{1,s},$$

In general is not possible to find such a matrix $E$.

# Idea of proof for Theorem 2

Problem is to relate invariants of $B^t B$ to those of $B$.

Suppose that we can diagonalize $B^t$ and $B$ by:

$$PB^t E^{-1} = D_{2,1}$$

and

$$EBQ^{-1} = D_{1,2}$$

*with the same $E$ in both equations*.

Then we can diagonalize the product:

$$PB^t BQ^{-1} = D_{r,1} D_{1,s},$$

In general is not possible to find such a matrix $E$.

# Idea of proof for Theorem 2

Problem is to relate invariants of $B^t B$ to those of $B$.

Suppose that we can diagonalize $B^t$ and $B$ by:

$$PB^t E^{-1} = D_{2,1}$$

and

$$EBQ^{-1} = D_{1,2}$$

*with the same $E$ in both equations*.

Then we can diagonalize the product:

$$PB^t BQ^{-1} = D_{r,1} D_{1,s},$$

In general is not possible to find such a matrix $E$.

# Left and right SNF Bases

For a homomorphism $\eta \colon R^m \to R^n$, consider bases $\mathcal{B} \subseteq R^m$ and $\mathcal{C} \subseteq R^n$ for which the matrix of $\eta$ is in diagonal form.

Call $\mathcal{B}$ a *left* SNF basis for $\eta$ and $\mathcal{C}$ a *right* SNF basis.

Lifting bases from the *M*-filtration

$$\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$$

gives a left SNF basis. The *N*-filtration gives right SNF basis.

# Left and right SNF Bases

For a homomorphism $\eta\colon R^m \to R^n$, consider bases $\mathcal{B} \subseteq R^m$ and $\mathcal{C} \subseteq R^n$ for which the matrix of $\eta$ is in diagonal form.

Call $\mathcal{B}$ a *left* SNF basis for $\eta$ and $\mathcal{C}$ a *right* SNF basis.

Lifting bases from the $M$-filtration

$$\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$$

gives a left SNF basis. The $N$-filtration gives right SNF basis.

# Left and right SNF Bases

For a homomorphism $\eta\colon R^m \to R^n$, consider bases $\mathcal{B} \subseteq R^m$ and $\mathcal{C} \subseteq R^n$ for which the matrix of $\eta$ is in diagonal form.

Call $\mathcal{B}$ a *left* SNF basis for $\eta$ and $\mathcal{C}$ a *right* SNF basis.

Lifting bases from the $M$-filtration

$$\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$$

gives a left SNF basis. The $N$-filtration gives right SNF basis.

## Lemma

*There exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ that is simultaneously a left SNF basis for $B$ and a right SNF basis for $B^t$.*

- $\mathrm{GL}(4, q)$ has a cyclic subgroup $S$ acting transitively on $\mathcal{L}_1$, hence all $S$-isotypic components of $R^{\mathcal{L}_1}$ have rank 1.
- Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$ compatible with both the $M$-filtration for $B$ and the $N$-filtration for $B^t$.
- $\mathcal{I}$ is both a left SNF basis for $B$ and a right SNF basis for $B^t$.

## Theorem 2

*Let $e_i = e_i(A)$ denote the multiplicity of $p^i$ as an elementary divisor of $A$. Then, for $0 \le i \le t$,*

$$e_{2t+i} = e_{t-i}(B^t B) = \sum_{\mathbf{s} \in \mathcal{H}(i)} d(\mathbf{s}).$$

Note $\mathcal{H}(i) = \bigcup_{k+\ell=t-i} \mathcal{H}_k(2) \cap {}_\ell\mathcal{H}(2)$.

## Lemma

*There exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ that is simultaneously a left SNF basis for $B$ and a right SNF basis for $B^t$.*

- $\mathrm{GL}(4, q)$ has a cyclic subgroup $S$ acting transitively on $\mathcal{L}_1$, hence all $S$-isotypic components of $R^{\mathcal{L}_1}$ have rank 1.
- Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$ compatible with both the $M$-filtration for $B$ and the $N$-filtration for $B^t$.
- $\mathcal{I}$ is both a left SNF basis for $B$ and a right SNF basis for $B^t$.

## Theorem 2

*Let $e_i = e_i(A)$ denote the multiplicity of $p^i$ as an elementary divisor of $A$. Then, for $0 \le i \le t$,*

$$e_{2t+i} = e_{t-i}(B^t B) = \sum_{\mathbf{s} \in \mathcal{H}(i)} d(\mathbf{s}).$$

Note $\mathcal{H}(i) = \bigcup_{k+\ell=t-i} \mathcal{H}_k(2) \cap {}_{\ell}\mathcal{H}(2)$.

## Lemma

*There exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ that is simultaneously a left SNF basis for $B$ and a right SNF basis for $B^t$.*

- $\mathrm{GL}(4, q)$ has a cyclic subgroup $S$ acting transitively on $\mathcal{L}_1$, hence all $S$-isotypic components of $R^{\mathcal{L}_1}$ have rank 1.
- Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$ compatible with both the $M$-filtration for $B$ and the $N$-filtration for $B^t$.
- $\mathcal{I}$ is both a left SNF basis for $B$ and a right SNF basis for $B^t$.

## Theorem 2

*Let $e_i = e_i(A)$ denote the multiplicity of $p^i$ as an elementary divisor of $A$. Then, for $0 \leq i \leq t$,*

$$e_{2t+i} = e_{t-i}(B^t B) = \sum_{\mathbf{s} \in \mathcal{H}(i)} d(\mathbf{s}).$$

Note $\mathcal{H}(i) = \bigcup_{k+\ell=t-i} \mathcal{H}_k(2) \cap {}_\ell\mathcal{H}(2)$.

## Lemma

*There exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ that is simultaneously a left SNF basis for $B$ and a right SNF basis for $B^t$.*

- $\mathrm{GL}(4, q)$ has a cyclic subgroup $S$ acting transitively on $\mathcal{L}_1$, hence all $S$-isotypic components of $R^{\mathcal{L}_1}$ have rank 1.
- Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$ compatible with both the $M$-filtration for $B$ and the $N$-filtration for $B^t$.
- $\mathcal{I}$ is both a left SNF basis for $B$ and a right SNF basis for $B^t$.

## Theorem 2

*Let $e_i = e_i(A)$ denote the multiplicity of $p^i$ as an elementary divisor of $A$. Then, for $0 \le i \le t$,*

$$e_{2t+i} = e_{t-i}(B^tB) = \sum_{\mathbf{s}\in\mathcal{H}(i)} d(\mathbf{s}).$$

Note $\mathcal{H}(i) = \bigcup_{k+\ell=t-i} \mathcal{H}_k(2) \cap {}_\ell\mathcal{H}(2)$.

## Lemma

*There exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ that is simultaneously a left SNF basis for $B$ and a right SNF basis for $B^t$.*

- $\mathrm{GL}(4, q)$ has a cyclic subgroup $S$ acting transitively on $\mathcal{L}_1$, hence all $S$-isotypic components of $R^{\mathcal{L}_1}$ have rank 1.
- Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$ compatible with both the $M$-filtration for $B$ and the $N$-filtration for $B^t$.
- $\mathcal{I}$ is both a left SNF basis for $B$ and a right SNF basis for $B^t$.

## Theorem 2

*Let $e_i = e_i(A)$ denote the multiplicity of $p^i$ as an elementary divisor of $A$. Then, for $0 \leq i \leq t$,*

$$e_{2t+i} = e_{t-i}(B^t B) = \sum_{\mathbf{s} \in \mathcal{H}(i)} d(\mathbf{s}).$$

Note $\mathcal{H}(i) = \bigcup_{k+\ell=t-i} \mathcal{H}_k(2) \cap {}_{\ell}\mathcal{H}(2)$.

## Lemma

*There exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ that is simultaneously a left SNF basis for $B$ and a right SNF basis for $B^t$.*

- $\mathrm{GL}(4, q)$ has a cyclic subgroup $S$ acting transitively on $\mathcal{L}_1$, hence all $S$-isotypic components of $R^{\mathcal{L}_1}$ have rank 1.
- Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$ compatible with both the $M$-filtration for $B$ and the $N$-filtration for $B^t$.
- $\mathcal{I}$ is both a left SNF basis for $B$ and a right SNF basis for $B^t$.

## Theorem 2

*Let $e_i = e_i(A)$ denote the multiplicity of $p^i$ as an elementary divisor of $A$. Then, for $0 \leq i \leq t$,*

$$e_{2t+i} = e_{t-i}(B^t B) = \sum_{\mathbf{s} \in \mathcal{H}(i)} d(\mathbf{s}).$$

Note $\mathcal{H}(i) = \bigcup_{k+\ell=t-i} \mathcal{H}_k(2) \cap {}_\ell\mathcal{H}(2)$.

## Lemma

*There exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ that is simultaneously a left SNF basis for $B$ and a right SNF basis for $B^t$.*

- $\mathrm{GL}(4, q)$ has a cyclic subgroup $S$ acting transitively on $\mathcal{L}_1$, hence all $S$-isotypic components of $R^{\mathcal{L}_1}$ have rank 1.
- Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$ compatible with both the $M$-filtration for $B$ and the $N$-filtration for $B^t$.
- $\mathcal{I}$ is both a left SNF basis for $B$ and a right SNF basis for $B^t$.

## Theorem 2

*Let $e_i = e_i(A)$ denote the multiplicity of $p^i$ as an elementary divisor of $A$. Then, for $0 \leq i \leq t$,*

$$e_{2t+i} = e_{t-i}(B^t B) = \sum_{\mathbf{s} \in \mathcal{H}(i)} d(\mathbf{s}).$$

Note $\mathcal{H}(i) = \bigcup_{k+\ell=t-i} \mathcal{H}_k(2) \cap {}_\ell\mathcal{H}(2)$.

## Lemma

*There exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ that is simultaneously a left SNF basis for $B$ and a right SNF basis for $B^t$.*

- $\mathrm{GL}(4, q)$ has a cyclic subgroup $S$ acting transitively on $\mathcal{L}_1$, hence all $S$-isotypic components of $R^{\mathcal{L}_1}$ have rank 1.
- Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$ compatible with both the $M$-filtration for $B$ and the $N$-filtration for $B^t$.
- $\mathcal{I}$ is both a left SNF basis for $B$ and a right SNF basis for $B^t$.

## Theorem 2

*Let $e_i = e_i(A)$ denote the multiplicity of $p^i$ as an elementary divisor of $A$. Then, for $0 \leq i \leq t$,*

$$e_{2t+i} = e_{t-i}(B^t B) = \sum_{\mathbf{s} \in \mathcal{H}(i)} d(\mathbf{s}).$$

Note $\mathcal{H}(i) = \bigcup_{k+\ell=t-i} \mathcal{H}_k(2) \cap {}_\ell\mathcal{H}(2)$.

Thank you for your attention!

# References


Matthew Bardoe and Peter Sin, *The permutation modules for* $\mathrm{GL}(n+1, \mathbf{F}_q)$ *acting on* $\mathbf{P}^n(\mathbf{F}_q)$ *and* $\mathbf{F}_q^{n-1}$, J. London Math. Soc. (2) **61** (2000), no. 1, 58–80.

David B. Chandler, Peter Sin, and Qing Xiang, *The invariant factors of the incidence matrices of points and subspaces in* $\mathrm{PG}(n, q)$ *and* $\mathrm{AG}(n, q)$, Trans. Amer. Math. Soc. **358** (2006), no. 11, 4935–4957 (electronic).

Noboru Hamada, *On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes*, Hiroshima Math. J. **3** (1973), 153–226.

Eric S. Lander, *Symmetric designs: An algebraic approach*, Cambridge University Press, 1983, London Math. Soc. Lecture Notes 74.

Joseph John Rushanan, *TOPICS IN INTEGRAL MATRICES AND ABELIAN GROUP CODES (SMITH NORMAL FORM (SNF), QUADRATIC, DUADIC, Q-CODES)*, ProQuest LLC, Ann Arbor, MI, 1986, Thesis (Ph.D.)–California Institute of Technology.

Peter Sin, *The elementary divisors of the incidence matrices of points and linear subspaces in* $\mathbf{P}^n(\mathbf{F}_p)$, J. Algebra **232** (2000), no. 1, 76–85.

Peter Sin, *The p-rank of the incidence matrix of intersecting linear subspaces*, Des. Codes Cryptogr. **31** (2004), no. 3, 213–220.

Qing Xiang, *Recent progress in algebraic design theory*, Finite Fields Appl. **11** (2005), no. 3, 622–653.

Qing Xiang, *Recent results on p-ranks and Smith normal forms of some* $2\text{-}(v,k,\lambda)$ *designs*, Coding theory and quantum computing, Contemp. Math., vol. 381, Amer. Math. Soc., Providence, RI, 2005, pp. 53–67.