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

Andries Brouwer, T. U. Eindhoven
Josh Ducey, University of Florida
Peter Sin, University of Florida

Discrete Mathematics Seminar, U. Delaware, April 27th, 2011.

Outline

Introduction

All invariants are powers of p

p-filtrations and SNF bases

Invariants of the Strongly Regular Graph

Relation with Point-Line Incidence

Simultaneous SNF Bases

Skew lines

- We consider the relation of *skewness* between lines in $PG(3,q)$, $q = p^t$.
- 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 of the quadric. Thus the graph of skew lines is the same as the non-collinearity graph of points in the hyperbolic polar space $O^+(5,q)$.
- This is a strongly regular graph.

Skew lines

- We consider the relation of *skewness* between lines in $PG(3,q)$, $q = p^t$.
- 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 of the quadric. Thus the graph of skew lines is the same as the non-collinearity graph of points in the hyperbolic polar space $O^+(5,q)$.
- This is a strongly regular graph.

Skew lines

- We consider the relation of *skewness* between lines in $PG(3, q)$, $q = p^t$.
- 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 of the quadric. Thus the graph of skew lines is the same as the non-collinearity graph of points in the hyperbolic polar space $O^+(5, q)$.
- This is a strongly regular graph.

Notation

- V, a 4-dimensional vector space over $\mathbf{F}_q$
- $\mathcal{L}_r =$ set of subspaces of dimension r in V
- A incidence matrix of skewness between lines in $\mathbb{P}(V)$
- A is square of size $(q^2 + q + 1)(q^2 + 1)$.
- For any matrix M, let $e_i(M) =$ number of invariant factors in the Smith Normal Form of M which are exactly divisible by p^i.

Outline

Introduction

All invariants are powers of p

p-filtrations and SNF bases

Invariants of the Strongly Regular Graph

Relation with Point-Line Incidence

Simultaneous SNF Bases

- $A^2 = q^4 I + (q^4 - q^3 - q^2 + q)A + (q^4 - q^3)(J - A - I)$
- Eigenvalues of A are q, $-q^2$, and q^4 with respective multiplicities $q^4 + q^2$, $q^3 + q^2 + q$, and 1.
- Special case of *oppositeness* relation
- We can replace $\mathbf{Z}$ by a suitable p-adic ring; We will use an unramified extension R of $\mathbb{Z}_p$ containing a $(q^4 - 1)$-th root of unity.

- $A^2 = q^4 I + (q^4 - q^3 - q^2 + q)A + (q^4 - q^3)(J - A - I)$
- Eigenvalues of A are q, $-q^2$, and q^4 with respective multiplicities $q^4 + q^2$, $q^3 + q^2 + q$, and 1.
- Special case of *oppositeness* relation
- We can replace $\mathbf{Z}$ by a suitable p-adic ring; We will use an unramified extension R of $\mathbb{Z}_p$ containing a $(q^4 - 1)$-th root of unity.

- $A^2 = q^4 I + (q^4 - q^3 - q^2 + q)A + (q^4 - q^3)(J - A - I)$
- Eigenvalues of A are q, $-q^2$, and q^4 with respective multiplicities $q^4 + q^2$, $q^3 + q^2 + q$, and 1.
- Special case of *oppositeness* relation
- We can replace **Z** by a suitable p-adic ring; We will use an unramified extension R of $\mathbb{Z}_p$ containing a $(q^4 - 1)$-th root of unity.

- $A^2 = q^4 I + (q^4 - q^3 - q^2 + q)A + (q^4 - q^3)(J - A - I)$
- Eigenvalues of A are q, $-q^2$, and q^4 with respective multiplicities $q^4 + q^2$, $q^3 + q^2 + q$, and 1.
- Special case of *oppositeness* relation
- We can replace **Z** by a suitable p-adic ring; We will use an unramified extension R of $\mathbb{Z}_p$ containing a $(q^4 - 1)$-th root of unity.

Theorem

Let $e_i = e_i(A)$.

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

Thus we get all the elementary divisor multiplicities once we know t of the numbers $e_0, \ldots, e_t$ (or the numbers $e_{2t}, \ldots, e_{3t}$).

More notation

- $[3]^t = \{(s_0, \dots, s_{t-1}) \mid s_i \in \{1, 2, 3\} \text{ for all } i\}$
- $\mathcal{H}(i) = \left\{(s_0, \dots, s_{t-1}) \in [3]^t \,\middle|\, \#\{j | s_j = 2\} = i\right\}$
- For $\vec{s} = (s_0, \dots, s_{t-1}) \in [3]^t$

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

  (subscripts mod t) and

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

- 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 $d(\vec{s}) = \prod_{i=0}^{t-1} d_{\lambda_i}$.

- Theorem

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

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

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

Outline

Introduction

All invariants are powers of p

p-filtrations and SNF bases

Invariants of the Strongly Regular Graph

Relation with Point-Line Incidence

Simultaneous SNF Bases

p-filtrations

- R, local principal ideal domain, max ideal pR, $F = R/pR$.
- 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 $N_{-1}(\eta) = \{0\}$)
- $R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$
- $N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$
- $F^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$
- $\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

p-filtrations

- R, local principal ideal domain, max ideal pR, $F = R/pR$.
- 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 $N_{-1}(\eta) = \{0\}$)
- $R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$
- $N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$
- $F^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$
- $\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

p-filtrations

- R, local principal ideal domain, max ideal pR, $F = R/pR$.
- For $L \leq R^\ell$, set $\overline{L} = (L + pR^\ell)/pR^\ell$.
- $\eta\colon R^m \to R^n$, R-module homomorphism
- $M_i(\eta) = \{x \in R^m \,|\, \eta(x) \in p^i R^n\}$
- $N_i(\eta) = \{p^{-i}\eta(x) \,|\, x \in M_i(\eta)\}$ (and $N_{-1}(\eta) = \{0\}$)
- $R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$
- $N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$
- $F^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$
- $\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

p-filtrations

- R, local principal ideal domain, max ideal pR, $F = R/pR$.
- 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 $N_{-1}(\eta) = \{0\}$)
- $R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$
- $N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$
- $F^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$
- $\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

p-filtrations

- R, local principal ideal domain, max ideal pR, $F = R/pR$.
- 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 $N_{-1}(\eta) = \{0\}$)
- $R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$
- $N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$
- $F^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$
- $\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

p-filtrations

- R, local principal ideal domain, max ideal pR, $F = R/pR$.
- 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 $N_{-1}(\eta) = \{0\}$)
- $R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$
- $N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$
- $F^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$
- $\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

p-filtrations

- R, local principal ideal domain, max ideal pR, $F = R/pR$.
- 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 $N_{-1}(\eta) = \{0\}$)
- $R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$
- $N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$
- $F^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$
- $\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

p-filtrations

- R, local principal ideal domain, max ideal pR, $F = R/pR$.
- 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 $N_{-1}(\eta) = \{0\}$)
- $R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$
- $N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$
- $F^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$
- $\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

p-filtrations

- R, local principal ideal domain, max ideal pR, $F = R/pR$.
- For $L \leq R^\ell$, set $\overline{L} = (L + pR^\ell)/pR^\ell$.
- $\eta\colon R^m \to R^n$, R-module homomorphism
- $M_i(\eta) = \{x \in R^m \,|\, \eta(x) \in p^i R^n\}$
- $N_i(\eta) = \{p^{-i}\eta(x) \,|\, x \in M_i(\eta)\}$ (and $N_{-1}(\eta) = \{0\}$)
- $R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots$
- $N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots$
- $F^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots$
- $\overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots$.

- Lemma

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

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

Left SNF Bases

- For a given homomorphism $\eta\colon R^m \to R^n$, we will be interested in pairs of bases $(\mathcal{B}, \mathcal{C})$ with respect to which the matrix of η is in Smith normal form.
- We define a *left* SNF basis for η to be any basis of R^m that belongs to such a pair. Similarly, a *right* SNF basis for η is any basis of R^n belonging to such a pair. We now describe how to construct such bases.
- $\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$
- $\overline{\mathcal{B}_{\ell+1}}$ basis of $\overline{\ker(\eta)}$
- Extend to a basis $\overline{\mathcal{B}_\ell} \cup \overline{\mathcal{B}_{\ell+1}}$ of $\overline{M_\ell(\eta)}$.
- Continue, to get a basis $\cup_{i=0}^{\ell+1}\overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$.
- Lift the elements of $\overline{\mathcal{B}_{\ell+1}}$ to a set $\mathcal{B}_{\ell+1}$ of preimages in $\ker(\eta)$.
- Continuing, enlarge each $\mathcal{B}_{i+1}$ by adjoining a set $\mathcal{B}_i$ of preimages in $M_i(\eta)$ of $\overline{\mathcal{B}_i}$.
- The set $\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i$ is an R-basis of R^m.

Left SNF Bases

- For a given homomorphism $\eta\colon R^m \to R^n$, we will be interested in pairs of bases $(\mathcal{B}, \mathcal{C})$ with respect to which the matrix of η is in Smith normal form.
- We define a *left* SNF basis for η to be any basis of R^m that belongs to such a pair. Similarly, a *right* SNF basis for η is any basis of R^n belonging to such a pair. We now describe how to construct such bases.
- $\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$
- $\overline{\mathcal{B}_{\ell+1}}$ basis of $\overline{\ker(\eta)}$
- Extend to a basis $\overline{\mathcal{B}_\ell} \cup \overline{\mathcal{B}_{\ell+1}}$ of $\overline{M_\ell(\eta)}$.
- Continue, to get a basis $\cup_{i=0}^{\ell+1} \overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$.
- Lift the elements of $\overline{\mathcal{B}_{\ell+1}}$ to a set $\mathcal{B}_{\ell+1}$ of preimages in $\ker(\eta)$.
- Continuing, enlarge each $\mathcal{B}_{i+1}$ by adjoining a set $\mathcal{B}_i$ of preimages in $M_i(\eta)$ of $\overline{\mathcal{B}_i}$.
- The set $\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i$ is an R-basis of R^m.

Left SNF Bases

- For a given homomorphism $\eta\colon R^m \to R^n$, we will be interested in pairs of bases $(\mathcal{B}, \mathcal{C})$ with respect to which the matrix of η is in Smith normal form.
- We define a *left* SNF basis for η to be any basis of R^m that belongs to such a pair. Similarly, a *right* SNF basis for η is any basis of R^n belonging to such a pair. We now describe how to construct such bases.
- $\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$
- $\overline{\mathcal{B}_{\ell+1}}$ basis of $\overline{\ker(\eta)}$
- Extend to a basis $\overline{\mathcal{B}_\ell} \cup \overline{\mathcal{B}_{\ell+1}}$ of $\overline{M_\ell(\eta)}$.
- Continue, to get a basis $\cup_{i=0}^{\ell+1} \overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$.
- Lift the elements of $\overline{\mathcal{B}_{\ell+1}}$ to a set $\mathcal{B}_{\ell+1}$ of preimages in $\ker(\eta)$.
- Continuing, enlarge each $\mathcal{B}_{i+1}$ by adjoining a set $\mathcal{B}_i$ of preimages in $M_i(\eta)$ of $\overline{\mathcal{B}_i}$.
- The set $\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i$ is an R-basis of R^m.

Left SNF Bases

- For a given homomorphism $\eta\colon R^m \to R^n$, we will be interested in pairs of bases $(\mathcal{B}, \mathcal{C})$ with respect to which the matrix of η is in Smith normal form.
- We define a *left* SNF basis for η to be any basis of R^m that belongs to such a pair. Similarly, a *right* SNF basis for η is any basis of R^n belonging to such a pair. We now describe how to construct such bases.
- $\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$
- $\overline{\mathcal{B}_{\ell+1}}$ basis of $\overline{\ker(\eta)}$
- Extend to a basis $\overline{\mathcal{B}_\ell} \cup \overline{\mathcal{B}_{\ell+1}}$ of $\overline{M_\ell(\eta)}$.
- Continue, to get a basis $\cup_{i=0}^{\ell+1} \overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$.
- Lift the elements of $\overline{\mathcal{B}_{\ell+1}}$ to a set $\mathcal{B}_{\ell+1}$ of preimages in $\ker(\eta)$.
- Continuing, enlarge each $\mathcal{B}_{i+1}$ by adjoining a set $\mathcal{B}_i$ of preimages in $M_i(\eta)$ of $\overline{\mathcal{B}_i}$.
- The set $\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i$ is an R-basis of R^m.

Left SNF Bases

- For a given homomorphism $\eta\colon R^m \to R^n$, we will be interested in pairs of bases $(\mathcal{B}, \mathcal{C})$ with respect to which the matrix of η is in Smith normal form.
- We define a *left* SNF basis for η to be any basis of R^m that belongs to such a pair. Similarly, a *right* SNF basis for η is any basis of R^n belonging to such a pair. We now describe how to construct such bases.
- $\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$
- $\overline{\mathcal{B}_{\ell+1}}$ basis of $\overline{\ker(\eta)}$
- Extend to a basis $\overline{\mathcal{B}_\ell} \cup \overline{\mathcal{B}_{\ell+1}}$ of $\overline{M_\ell(\eta)}$.
- Continue, to get a basis $\cup_{i=0}^{\ell+1} \overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$.
- Lift the elements of $\overline{\mathcal{B}_{\ell+1}}$ to a set $\mathcal{B}_{\ell+1}$ of preimages in $\ker(\eta)$.
- Continuing, enlarge each $\mathcal{B}_{i+1}$ by adjoining a set $\mathcal{B}_i$ of preimages in $M_i(\eta)$ of $\overline{\mathcal{B}_i}$.
- The set $\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i$ is an R-basis of R^m.

Left SNF Bases

- For a given homomorphism $\eta\colon R^m \to R^n$, we will be interested in pairs of bases $(\mathcal{B}, \mathcal{C})$ with respect to which the matrix of η is in Smith normal form.
- We define a *left* SNF basis for η to be any basis of R^m that belongs to such a pair. Similarly, a *right* SNF basis for η is any basis of R^n belonging to such a pair. We now describe how to construct such bases.
- $\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$
- $\overline{\mathcal{B}_{\ell+1}}$ basis of $\overline{\ker(\eta)}$
- Extend to a basis $\overline{\mathcal{B}_\ell} \cup \overline{\mathcal{B}_{\ell+1}}$ of $\overline{M_\ell(\eta)}$.
- Continue, to get a basis $\cup_{i=0}^{\ell+1}\overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$.
- Lift the elements of $\overline{\mathcal{B}_{\ell+1}}$ to a set $\mathcal{B}_{\ell+1}$ of preimages in $\ker(\eta)$.
- Continuing, enlarge each $\mathcal{B}_{i+1}$ by adjoining a set $\mathcal{B}_i$ of preimages in $M_i(\eta)$ of $\overline{\mathcal{B}_i}$.
- The set $\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i$ is an R-basis of R^m.

Left SNF Bases

- For a given homomorphism $\eta\colon R^m \to R^n$, we will be interested in pairs of bases $(\mathcal{B}, \mathcal{C})$ with respect to which the matrix of η is in Smith normal form.
- We define a *left* SNF basis for η to be any basis of R^m that belongs to such a pair. Similarly, a *right* SNF basis for η is any basis of R^n belonging to such a pair. We now describe how to construct such bases.
- $\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$
- $\overline{\mathcal{B}_{\ell+1}}$ basis of $\overline{\ker(\eta)}$
- Extend to a basis $\overline{\mathcal{B}_\ell} \cup \overline{\mathcal{B}_{\ell+1}}$ of $\overline{M_\ell(\eta)}$.
- Continue, to get a basis $\cup_{i=0}^{\ell+1}\overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$.
- Lift the elements of $\overline{\mathcal{B}_{\ell+1}}$ to a set $\mathcal{B}_{\ell+1}$ of preimages in $\ker(\eta)$.
- Continuing, enlarge each $\mathcal{B}_{i+1}$ by adjoining a set $\mathcal{B}_i$ of preimages in $M_i(\eta)$ of $\overline{\mathcal{B}_i}$.
- The set $\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i$ is an R-basis of R^m.

Left SNF Bases

- For a given homomorphism $\eta \colon R^m \to R^n$, we will be interested in pairs of bases $(\mathcal{B}, \mathcal{C})$ with respect to which the matrix of η is in Smith normal form.
- We define a *left* SNF basis for η to be any basis of R^m that belongs to such a pair. Similarly, a *right* SNF basis for η is any basis of R^n belonging to such a pair. We now describe how to construct such bases.
- $\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$
- $\overline{\mathcal{B}_{\ell+1}}$ basis of $\overline{\ker(\eta)}$
- Extend to a basis $\overline{\mathcal{B}_\ell} \cup \overline{\mathcal{B}_{\ell+1}}$ of $\overline{M_\ell(\eta)}$.
- Continue, to get a basis $\cup_{i=0}^{\ell+1} \overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$.
- Lift the elements of $\overline{\mathcal{B}_{\ell+1}}$ to a set $\mathcal{B}_{\ell+1}$ of preimages in $\ker(\eta)$.
- Continuing, enlarge each $\mathcal{B}_{i+1}$ by adjoining a set $\mathcal{B}_i$ of preimages in $M_i(\eta)$ of $\overline{\mathcal{B}_i}$.
- The set $\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i$ is an R-basis of R^m.

Left SNF Bases

- For a given homomorphism $\eta\colon R^m \to R^n$, we will be interested in pairs of bases $(\mathcal{B}, \mathcal{C})$ with respect to which the matrix of η is in Smith normal form.
- We define a *left* SNF basis for η to be any basis of R^m that belongs to such a pair. Similarly, a *right* SNF basis for η is any basis of R^n belonging to such a pair. We now describe how to construct such bases.
- $\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_\ell(\eta)} \supsetneq \overline{\ker(\eta)}$
- $\overline{\mathcal{B}_{\ell+1}}$ basis of $\overline{\ker(\eta)}$
- Extend to a basis $\overline{\mathcal{B}_\ell} \cup \overline{\mathcal{B}_{\ell+1}}$ of $\overline{M_\ell(\eta)}$.
- Continue, to get a basis $\cup_{i=0}^{\ell+1}\overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$.
- Lift the elements of $\overline{\mathcal{B}_{\ell+1}}$ to a set $\mathcal{B}_{\ell+1}$ of preimages in $\ker(\eta)$.
- Continuing, enlarge each $\mathcal{B}_{i+1}$ by adjoining a set $\mathcal{B}_i$ of preimages in $M_i(\eta)$ of $\overline{\mathcal{B}_i}$.
- The set $\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i$ is an R-basis of R^m.

Right SNF Bases

- $N_\ell(\eta) = N_{\ell+1}(\eta) = \cdots$, call this module N'
- N' the *purification* of $\operatorname{Im}\eta$
- The elementary divisors of η remain the same if we change its codomain N'.
- Basis $\overline{\mathcal{C}_0}$ of $\overline{N_0(\eta)}$,
- Extend to basis $\overline{\mathcal{C}_0} \cup \overline{\mathcal{C}_1}$ of $\overline{N_1(\eta)}$.
- Continue, ending with basis $\cup_{i=0}^{\ell}\overline{\mathcal{C}_i}$ of $\overline{N'}$.
- Now we lift $\overline{\mathcal{C}_0}$ to a set $\mathcal{C}_0$ of preimages in $N_0(\eta)$.
- Continuing, enlarge each $\mathcal{C}_i$ by adjoining a set $\mathcal{C}_{i+1}$ of preimages in $N_{i+1}(\eta)$ of $\overline{\mathcal{C}_{i+1}}$.
- $\mathcal{C}' = \bigcup_{i=0}^{\ell}\mathcal{C}_i$ is an R-basis of N'.
- Extend arbitrarily to a basis $\mathcal{C} = \bigcup_{i=0}^{\ell+1}\mathcal{C}_i$ of R^n.

Outline

Introduction

All invariants are powers of *p*

p-filtrations and SNF bases

Invariants of the Strongly Regular Graph

Relation with Point-Line Incidence

Simultaneous SNF Bases

Eliminating the all-one vector

- View A as an R-module map.
- $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$ sends a 2-subspace to the (formal) sum of the 2-subspaces incident with it.
- $\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
- $Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
- $R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
- $(\mathbf{1})A = q^4 \mathbf{1}$
- $e_{4t}(A) = e_{4t}(A|_{Y_2}) + 1$
- $e_i(A) = e_i(A|_{Y_2})$ for $i \neq 4t$.

Eliminating the all-one vector

- View A as an R-module map.
- $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$ sends a 2-subspace to the (formal) sum of the 2-subspaces incident with it.
- $\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
- $Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
- $R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
- $(\mathbf{1})A = q^4 \mathbf{1}$
- $e_{4t}(A) = e_{4t}(A|_{Y_2}) + 1$
- $e_i(A) = e_i(A|_{Y_2})$ for $i \neq 4t$.

Eliminating the all-one vector

- View A as an R-module map.
- $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$ sends a 2-subspace to the (formal) sum of the 2-subspaces incident with it.
- $\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
- $Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
- $R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
- $(\mathbf{1})A = q^4 \mathbf{1}$
- $e_{4t}(A) = e_{4t}(A|_{Y_2}) + 1$
- $e_i(A) = e_i(A|_{Y_2})$ for $i \neq 4t$.

Eliminating the all-one vector

- View A as an R-module map.
- $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$ sends a 2-subspace to the (formal) sum of the 2-subspaces incident with it.
- $\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
- $Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \,\middle|\, \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
- $R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
- $(\mathbf{1})A = q^4 \mathbf{1}$
- $e_{4t}(A) = e_{4t}(A|_{Y_2}) + 1$
- $e_i(A) = e_i(A|_{Y_2})$ for $i \neq 4t$.

Eliminating the all-one vector

- View A as an R-module map.
- $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$ sends a 2-subspace to the (formal) sum of the 2-subspaces incident with it.
- $\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
- $Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \;\middle|\; \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
- $R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
- $(\mathbf{1})A = q^4 \mathbf{1}$
- $e_{4t}(A) = e_{4t}(A|_{Y_2}) + 1$
- $e_i(A) = e_i(A|_{Y_2})$ for $i \neq 4t$.

Eliminating the all-one vector

- View A as an R-module map.
- $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$ sends a 2-subspace to the (formal) sum of the 2-subspaces incident with it.
- $\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
- $Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \;\middle|\; \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
- $R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
- $(\mathbf{1})A = q^4 \mathbf{1}$
- $e_{4t}(A) = e_{4t}(A|_{Y_2}) + 1$
- $e_i(A) = e_i(A|_{Y_2})$ for $i \neq 4t$.

Eliminating the all-one vector

- View A as an R-module map.
- $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$ sends a 2-subspace to the (formal) sum of the 2-subspaces incident with it.
- $\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
- $Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \;\middle|\; \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
- $R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
- $(\mathbf{1})A = q^4 \mathbf{1}$
- $e_{4t}(A) = e_{4t}(A|_{Y_2}) + 1$
- $e_i(A) = e_i(A|_{Y_2})$ for $i \neq 4t$.

Eliminating the all-one vector

- View A as an R-module map.
- $A : R^{\mathcal{L}_2} \to R^{\mathcal{L}_2}$ sends a 2-subspace to the (formal) sum of the 2-subspaces incident with it.
- $\mathbf{1} = \sum_{x \in \mathcal{L}_2} x$
- $Y_2 = \left\{ \sum_{x \in \mathcal{L}_2} a_x x \in R^{\mathcal{L}_2} \;\middle|\; \sum_{x \in \mathcal{L}_2} a_x = 0 \right\}$
- $R^{\mathcal{L}_2} = R\mathbf{1} \oplus Y_2$
- $(\mathbf{1})A = q^4 \mathbf{1}$
- $e_{4t}(A) = e_{4t}(A|_{Y_2}) + 1$
- $e_i(A) = e_i(A|_{Y_2})$ for $i \neq 4t$.

SRG equation

- $A(A+(q^2-q)I)=q^3I+(q^4-q^3)J$
- On Y_2, $A(A+(q^2-q)I)=q^3I$.
- Let P and Q be unimodular, with $D=PAQ^{-1}$ diagonal. Then we get the relation

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

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 $D = PAQ^{-1}$ diagonal. Then we get the relation

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

SRG equation

- $A(A+(q^2-q)I) = q^3I + (q^4-q^3)J$
- On Y_2, $A(A+(q^2-q)I) = q^3I$.
- Let P and Q be unimodular, with $D = PAQ^{-1}$ diagonal. Then we get the relation

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

SRG equation (continued)

- $Q(A + (q^2 - q)I)P^{-1} = q^3 D^{-1}$
- $e_i(A|_{Y_2}) = 0$ for $i > 3t$.
- $e_{4t}(A) = 1$
- $e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2})$for $0 \leq i \leq 3t$.

SRG equation (continued)

- $Q(A+(q^2-q)I)P^{-1} = q^3D^{-1}$
- $e_i(A|_{Y_2}) = 0$ for $i > 3t$.
- $e_{4t}(A) = 1$
- $e_i(A|_{Y_2} + (q^2-q)I) = e_{3t-i}(A|_{Y_2})$for $0 \leq i \leq 3t$.

SRG equation (continued)

- $Q(A + (q^2 - q)I)P^{-1} = q^3 D^{-1}$
- $e_i(A|_{Y_2}) = 0$ for $i > 3t$.
- $e_{4t}(A) = 1$
- $e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2})$for $0 \leq i \leq 3t$.

SRG equation (continued)

- $Q(A + (q^2 - q)I)P^{-1} = q^3 D^{-1}$
- $e_i(A|_{Y_2}) = 0$ for $i > 3t$.
- $e_{4t}(A) = 1$
- $e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2})$for $0 \leq i \leq 3t$.

Proof of First Theorem

- $A|_{Y_2} \equiv A|_{Y_2} + (q^2 - q)I \pmod{p^t}$
- $e_i(A|_{Y_2}) = e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2})$, for $0 \leq i < t$
- $V_\lambda := \lambda$-eigenspace for A (as a matrix over the field of fractions of R).
- $V_q \cap R^{\mathcal{L}_2}$ and $V_{-q^2} \cap R^{\mathcal{L}_2}$ are pure R-submodules of Y_2.
- $V_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $V_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.
- $$q^4 + q^2 = \dim_F(\overline{V_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_F \overline{N_t(A|_{Y_2})} = \sum_{i=0}^{t} e_i(A|_{Y_2})$$

  and

  $$q^3 + q^2 + q = \dim_F(\overline{V_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_F \overline{M_{2t}(A|_{Y_2})} = \sum_{i=2t}^{3t} e_i(A|_{Y_2}).$$
- Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_F \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other i.

Proof of First Theorem

- $A|_{Y_2} \equiv A|_{Y_2} + (q^2 - q)I \pmod{p^t}$
- $e_i(A|_{Y_2}) = e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2})$, for $0 \leq i < t$
- $V_\lambda :=$ λ-eigenspace for A (as a matrix over the field of fractions of R).
- $V_q \cap R^{\mathcal{L}_2}$ and $V_{-q^2} \cap R^{\mathcal{L}_2}$ are pure R-submodules of Y_2.
- $V_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $V_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.
- $$q^4 + q^2 = \dim_F(\overline{V_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_F \overline{N_t(A|_{Y_2})} = \sum_{i=0}^{t} e_i(A|_{Y_2})$$

  and

  $$q^3 + q^2 + q = \dim_F(\overline{V_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_F \overline{M_{2t}(A|_{Y_2})} = \sum_{i=2t}^{3t} e_i(A|_{Y_2}).$$
- Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_F \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other i.

Proof of First Theorem

- $A|_{Y_2} \equiv A|_{Y_2} + (q^2 - q)I \pmod{p^t}$
- $e_i(A|_{Y_2}) = e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2})$, for $0 \le i < t$
- $V_\lambda := \lambda$-eigenspace for A (as a matrix over the field of fractions of R).
- $V_q \cap R^{\mathcal{L}_2}$ and $V_{-q^2} \cap R^{\mathcal{L}_2}$ are pure R-submodules of Y_2.
- $V_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $V_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.
- $$q^4 + q^2 = \dim_F(\overline{V_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_F \overline{N_t(A|_{Y_2})} = \sum_{i=0}^{t} e_i(A|_{Y_2})$$

  and

  $$q^3 + q^2 + q = \dim_F(\overline{V_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \le \dim_F \overline{M_{2t}(A|_{Y_2})} = \sum_{i=2t}^{3t} e_i(A|_{Y_2}).$$
- Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_F \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other i.

Proof of First Theorem

- $A|_{Y_2} \equiv A|_{Y_2} + (q^2 - q)I \pmod{p^t}$
- $e_i(A|_{Y_2}) = e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2})$, for $0 \leq i < t$
- $V_\lambda := \lambda$-eigenspace for A (as a matrix over the field of fractions of R).
- $V_q \cap R^{\mathcal{L}_2}$ and $V_{-q^2} \cap R^{\mathcal{L}_2}$ are pure R-submodules of Y_2.
- $V_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $V_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.
-

$$q^4 + q^2 = \dim_F \overline{(V_q \cap \mathbb{Z}_p^{\mathcal{L}_2})} \leq \dim_F \overline{N_t(A|_{Y_2})} = \sum_{i=0}^{t} e_i(A|_{Y_2})$$

and

$$q^3 + q^2 + q = \dim_F \overline{(V_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2})} \leq \dim_F \overline{M_{2t}(A|_{Y_2})} = \sum_{i=2t}^{3t} e_i(A|_{Y_2}).$$

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

Proof of First Theorem

- $A|_{Y_2} \equiv A|_{Y_2} + (q^2 - q)I \pmod{p^t}$
- $e_i(A|_{Y_2}) = e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2})$, for $0 \leq i < t$
- $V_\lambda := \lambda$-eigenspace for A (as a matrix over the field of fractions of R).
- $V_q \cap R^{\mathcal{L}_2}$ and $V_{-q^2} \cap R^{\mathcal{L}_2}$ are pure R-submodules of Y_2.
- $V_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $V_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.
- $$q^4 + q^2 = \dim_F(\overline{V_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_F \overline{N_t(A|_{Y_2})} = \sum_{i=0}^{t} e_i(A|_{Y_2})$$

  and

  $$q^3+q^2+q = \dim_F(\overline{V_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_F \overline{M_{2t}(A|_{Y_2})} = \sum_{i=2t}^{3t} e_i(A|_{Y_2}).$$
- Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_F \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other i.

Proof of First Theorem

- $A|_{Y_2} \equiv A|_{Y_2} + (q^2 - q)I \pmod{p^t}$
- $e_i(A|_{Y_2}) = e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2})$, for $0 \leq i < t$
- $V_\lambda :=$ λ-eigenspace for A (as a matrix over the field of fractions of R).
- $V_q \cap R^{\mathcal{L}_2}$ and $V_{-q^2} \cap R^{\mathcal{L}_2}$ are pure R-submodules of Y_2.
- $V_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $V_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.
- $$q^4 + q^2 = \dim_F(\overline{V_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_F \overline{N_t(A|_{Y_2})} = \sum_{i=0}^{t} e_i(A|_{Y_2})$$

  and

  $$q^3 + q^2 + q = \dim_F(\overline{V_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_F \overline{M_{2t}(A|_{Y_2})} = \sum_{i=2t}^{3t} e_i(A|_{Y_2}).$$
- Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_F \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other i.

Proof of First Theorem

- $A|_{Y_2} \equiv A|_{Y_2} + (q^2 - q)I \pmod{p^t}$
- $e_i(A|_{Y_2}) = e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2})$, for $0 \leq i < t$
- $V_\lambda := \lambda$-eigenspace for A (as a matrix over the field of fractions of R).
- $V_q \cap R^{\mathcal{L}_2}$ and $V_{-q^2} \cap R^{\mathcal{L}_2}$ are pure R-submodules of Y_2.
- $V_q \cap R^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $V_{-q^2} \cap R^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$.
-
  $$q^4 + q^2 = \dim_F(\overline{V_q \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_F \overline{N_t(A|_{Y_2})} = \sum_{i=0}^{t} e_i(A|_{Y_2})$$

  and

  $$q^3+q^2+q = \dim_F(\overline{V_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}}) \leq \dim_F \overline{M_{2t}(A|_{Y_2})} = \sum_{i=2t}^{3t} e_i(A|_{Y_2}).$$
- Since $(q^4 + q^2) + (q^3 + q^2 + q) = \dim_F \overline{Y_2}$, we must have *equalities* throughout, so $e_i(A) = 0$ for all other i.

Remark

The above proof simply exploits the SRG equation, and makes no use of the geometry of $\mathrm{PG}(3, q)$. Therefore the first theorem is also true for the adjacency matrix A of any strongly regular graph with the same parameters.

Outline

Introduction

All invariants are powers of *p*

p-filtrations and SNF bases

Invariants of the Strongly Regular Graph

Relation with Point-Line Incidence

Simultaneous SNF Bases

- B denote 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 denotes the transpose of B, and is just the incidence matrix of lines vs. points.
- $$B^tB = (q^3+q^2)I + (q^3+q^2-q-1)A + (q^3+q^2-q)(J-A-I). \tag{2}$$
- $(\mathbf{1})B^tB = q^4(q^2+q+1)(q+1)\mathbf{1}$,
- $e_i(B^tB) = e_i(B^tB|_{Y_2})$ for $i \neq 4t$.
- $B^tB = -[A+(q^2-q)I] + q^2I + (q^3+q^2-q)J$
- On Y_2, $B^tB = -[A+(q^2-q)I] + q^2I$.
- $e_i(B^tB|_{Y_2}) = e_i(A|_{Y_2} + (q^2-q)I)$
- $e_{2t+i}(A) = e_{t-i}(B^tB)$, for $0 \leq i \leq t$.

- B denote 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 denotes the transpose of B, and is just the incidence matrix of lines vs. points.
- $$B^tB = (q^3+q^2)I + (q^3+q^2-q-1)A + (q^3+q^2-q)(J-A-I). \tag{2}$$
- $(\mathbf{1})B^tB = q^4(q^2+q+1)(q+1)\mathbf{1}$,
- $e_i(B^tB) = e_i(B^tB|_{Y_2})$ for $i \neq 4t$.
- $B^tB = -[A+(q^2-q)I] + q^2I + (q^3+q^2-q)J$
- On Y_2, $B^tB = -[A+(q^2-q)I] + q^2I$.
- $e_i(B^tB|_{Y_2}) = e_i(A|_{Y_2} + (q^2-q)I)$
- $e_{2t+i}(A) = e_{t-i}(B^tB)$, for $0 \leq i \leq t$.

- B denote 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 denotes the transpose of B, and is just the incidence matrix of lines vs. points.
- $$B^tB = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I). \tag{2}$$
- $(\mathbf{1})B^tB = q^4(q^2+q+1)(q+1)\mathbf{1}$,
- $e_i(B^tB) = e_i(B^tB|_{Y_2})$ for $i \neq 4t$.
- $B^tB = -[A+(q^2-q)I] + q^2I + (q^3+q^2-q)J$
- On Y_2, $B^tB = -[A+(q^2-q)I] + q^2I$.
- $e_i(B^tB|_{Y_2}) = e_i(A|_{Y_2} + (q^2-q)I)$
- $e_{2t+i}(A) = e_{t-i}(B^tB)$, for $0 \leq i \leq t$.

- B denote 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 denotes the transpose of B, and is just the incidence matrix of lines vs. points.
- $$B^tB = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I). \tag{2}$$
- $(\mathbf{1})B^tB = q^4(q^2+q+1)(q+1)\mathbf{1}$,
- $e_i(B^tB) = e_i(B^tB|_{Y_2})$ for $i \neq 4t$.
- $B^tB = -[A+(q^2-q)I] + q^2I + (q^3+q^2-q)J$
- On Y_2, $B^tB = -[A+(q^2-q)I] + q^2I$.
- $e_i(B^tB|_{Y_2}) = e_i(A|_{Y_2} + (q^2-q)I)$
- $e_{2t+i}(A) = e_{t-i}(B^tB)$, for $0 \leq i \leq t$.

- B denote 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 denotes the transpose of B, and is just the incidence matrix of lines vs. points.
- $$B^tB = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I). \tag{2}$$
- $(\mathbf{1})B^tB = q^4(q^2+q+1)(q+1)\mathbf{1}$,
- $e_i(B^tB) = e_i(B^tB|_{Y_2})$ for $i \neq 4t$.
- $B^tB = -[A+(q^2-q)I] + q^2I + (q^3+q^2-q)J$
- On Y_2, $B^tB = -[A+(q^2-q)I] + q^2I$.
- $e_i(B^tB|_{Y_2}) = e_i(A|_{Y_2} + (q^2-q)I)$
- $e_{2t+i}(A) = e_{t-i}(B^tB)$, for $0 \leq i \leq t$.

- B denote 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 denotes the transpose of B, and is just the incidence matrix of lines vs. points.
- $$B^tB = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I). \tag{2}$$
- $(\mathbf{1})B^tB = q^4(q^2+q+1)(q+1)\mathbf{1}$,
- $e_i(B^tB) = e_i(B^tB|_{Y_2})$ for $i \neq 4t$.
- $B^tB = -[A+(q^2-q)I]+q^2I+(q^3+q^2-q)J$
- On Y_2, $B^tB = -[A+(q^2-q)I]+q^2I$.
- $e_i(B^tB|_{Y_2}) = e_i(A|_{Y_2}+(q^2-q)I)$
- $e_{2t+i}(A) = e_{t-i}(B^tB)$, for $0 \leq i \leq t$.

- B denote 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 denotes the transpose of B, and is just the incidence matrix of lines vs. points.
- $$B^tB = (q^3+q^2)I + (q^3+q^2-q-1)A + (q^3+q^2-q)(J-A-I). \tag{2}$$
- $(\mathbf{1})B^tB = q^4(q^2+q+1)(q+1)\mathbf{1}$,
- $e_i(B^tB) = e_i(B^tB|_{Y_2})$ for $i \neq 4t$.
- $B^tB = -[A+(q^2-q)I] + q^2I + (q^3+q^2-q)J$
- On Y_2, $B^tB = -[A+(q^2-q)I] + q^2I$.
- $e_i(B^tB|_{Y_2}) = e_i(A|_{Y_2} + (q^2-q)I)$
- $e_{2t+i}(A) = e_{t-i}(B^tB)$, for $0 \leq i \leq t$.

- B denote 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 denotes the transpose of B, and is just the incidence matrix of lines vs. points.
- $$B^tB = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I). \tag{2}$$
- $(\mathbf{1})B^tB = q^4(q^2+q+1)(q+1)\mathbf{1}$,
- $e_i(B^tB) = e_i(B^tB|_{Y_2})$ for $i \neq 4t$.
- $B^tB = -[A+(q^2-q)I] + q^2I + (q^3+q^2-q)J$
- On Y_2, $B^tB = -[A+(q^2-q)I] + q^2I$.
- $e_i(B^tB|_{Y_2}) = e_i(A|_{Y_2} + (q^2-q)I)$
- $e_{2t+i}(A) = e_{t-i}(B^tB)$, for $0 \leq i \leq t$.

- B denote 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 denotes the transpose of B, and is just the incidence matrix of lines vs. points.
- $$B^tB=(q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I). \tag{2}$$
- $(\mathbf{1})B^tB=q^4(q^2+q+1)(q+1)\mathbf{1}$,
- $e_i(B^tB)=e_i(B^tB|_{Y_2})$ for $i\neq 4t$.
- $B^tB=-[A+(q^2-q)I]+q^2I+(q^3+q^2-q)J$
- On Y_2, $B^tB=-[A+(q^2-q)I]+q^2I$.
- $e_i(B^tB|_{Y_2})=e_i(A|_{Y_2}+(q^2-q)I)$
- $e_{2t+i}(A)=e_{t-i}(B^tB)$, for $0\leq i\leq t$.

Outline

Introduction

All invariants are powers of p

p-filtrations and SNF bases

Invariants of the Strongly Regular Graph

Relation with Point-Line Incidence

Simultaneous SNF Bases

Proof of Second Theorem

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

  $$PB^tE^{-1} = D_{2,1}$$

  and

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

  where E is the same matrix in both equations

- Then we can diagonalize the product:

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

- In general is not possible to find such a matrix E ([5] is a source of information on this topic).
- Yet that is exactly what we will do.

Proof of Second Theorem

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

  $$PB^tE^{-1} = D_{2,1}$$

  and

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

  where E is the same matrix in both equations
- Then we can diagonalize the product:

  $$PB^tBQ^{-1} = D_{r,1}D_{1,s},$$
- In general is not possible to find such a matrix E ([5] is a source of information on this topic).
- Yet that is exactly what we will do.

Proof of Second Theorem

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

  $$PB^tE^{-1} = D_{2,1}$$

  and

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

  where E is the same matrix in both equations
- Then we can diagonalize the product:

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

- In general is not possible to find such a matrix E ([5] is a source of information on this topic).
- Yet that is exactly what we will do.

Proof of Second Theorem

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

  $$PB^tE^{-1} = D_{2,1}$$

  and

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

  where E is the same matrix in both equations
- Then we can diagonalize the product:

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

- In general is not possible to find such a matrix E ([5] is a source of information on this topic).
- Yet that is exactly what we will do.

- 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.

  - The group G has a cyclic subgroup S which is isomorphic to $F^\times$, acting on $R^{\mathcal{L}_1}$ with all isotypic components of rank 1.
  - Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$.
  - By using idempotents in RG, we can show that $\mathcal{I}$ is simultaneously a left SNF basis for B and a right SNF basis for B^t.
  - Finally, the elementary divisors of B^t and B can be found in work of Chandler, Sin and Xiang.
  - This lemma generalizes. Let $A_{1,\ell}$ be the incidence matrix between 1-subspaces and ℓ-subspaces in any finite vector space. Using the generalization and the C-S-X formula, we can obtain the elementary divisors of the matrix $A_{1,r}^t A_{1,s}$.

- **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.

  - The group G has a cyclic subgroup S which is isomorphic to $F^{\times}$, acting on $R^{\mathcal{L}_1}$ with all isotypic components of rank 1.
  - Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$.
  - By using idempotents in RG, we can show that $\mathcal{I}$ is simultaneously a left SNF basis for B and a right SNF basis for B^t.
  - Finally, the elementary divisors of B^t and B can be found in work of Chandler, Sin and Xiang.
  - This lemma generalizes. Let $A_{1,\ell}$ be the incidence matrix between 1-subspaces and ℓ-subspaces in any finite vector space. Using the generalization and the C-S-X formula, we can obtain the elementary divisors of the matrix $A^t_{1,r}A_{1,s}$.

- 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.

  - The group G has a cyclic subgroup S which is isomorphic to $F^\times$, acting on $R^{\mathcal{L}_1}$ with all isotypic components of rank 1.
  - Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$.
  - By using idempotents in RG, we can show that $\mathcal{I}$ is simultaneously a left SNF basis for B and a right SNF basis for B^t.
  - Finally, the elementary divisors of B^t and B can be found in work of Chandler, Sin and Xiang.
  - This lemma generalizes. Let $A_{1,\ell}$ be the incidence matrix between 1-subspaces and ℓ-subspaces in any finite vector space. Using the generalization and the C-S-X formula, we can obtain the elementary divisors of the matrix $A^t_{1,r}A_{1,s}$.

- 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.

  - The group G has a cyclic subgroup S which is isomorphic to $F^\times$, acting on $R^{\mathcal{L}_1}$ with all isotypic components of rank 1.
  - Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$.
  - By using idempotents in RG, we can show that $\mathcal{I}$ is simultaneously a left SNF basis for B and a right SNF basis for B^t.
  - Finally, the elementary divisors of B^t and B can be found in work of Chandler, Sin and Xiang.
  - This lemma generalizes. Let $A_{1,\ell}$ be the incidence matrix between 1-subspaces and ℓ-subspaces in any finite vector space. Using the generalization and the C-S-X formula, we can obtain the elementary divisors of the matrix $A_{1,r}^t A_{1,s}$.

- 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.

  - The group G has a cyclic subgroup S which is isomorphic to $F^\times$, acting on $R^{\mathcal{L}_1}$ with all isotypic components of rank 1.
  - Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$.
  - By using idempotents in RG, we can show that $\mathcal{I}$ is simultaneously a left SNF basis for B and a right SNF basis for B^t.
  - Finally, the elementary divisors of B^t and B can be found in work of Chandler, Sin and Xiang.
  - This lemma generalizes. Let $A_{1,\ell}$ be the incidence matrix between 1-subspaces and ℓ-subspaces in any finite vector space. Using the generalization and the C-S-X formula, we can obtain the elementary divisors of the matrix $A^t_{1,r}A_{1,s}$.

- 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.

  - The group G has a cyclic subgroup S which is isomorphic to $F^\times$, acting on $R^{\mathcal{L}_1}$ with all isotypic components of rank 1.
  - Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$.
  - By using idempotents in RG, we can show that $\mathcal{I}$ is simultaneously a left SNF basis for B and a right SNF basis for B^t.
  - Finally, the elementary divisors of B^t and B can be found in work of Chandler, Sin and Xiang.
  - This lemma generalizes. Let $A_{1,\ell}$ be the incidence matrix between 1-subspaces and ℓ-subspaces in any finite vector space. Using the generalization and the C-S-X formula, we can obtain the elementary divisors of the matrix $A_{1,r}^t A_{1,s}$.

- 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.

  - The group G has a cyclic subgroup S which is isomorphic to $F^\times$, acting on $R^{\mathcal{L}_1}$ with all isotypic components of rank 1.
  - Taking a generator of each component, we get a basis $\mathcal{I}$ of $R^{\mathcal{L}_1}$.
  - By using idempotents in RG, we can show that $\mathcal{I}$ is simultaneously a left SNF basis for B and a right SNF basis for B^t.
  - Finally, the elementary divisors of B^t and B can be found in work of Chandler, Sin and Xiang.
  - This lemma generalizes. Let $A_{1,\ell}$ be the incidence matrix between 1-subspaces and ℓ-subspaces in any finite vector space. Using the generalization and the C-S-X formula, we can obtain the elementary divisors of the matrix $A_{1,r}^t A_{1,s}$.

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.