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

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

November 4–6, 2011
In memory of Bob Liebler

Outline

Smith normal form

- Recall that the Smith normal form of a (possibly nonsquare) integer matrix is a diagonal matrix of the same size, with the diagonal entries subject to certain divisibility conditions.

Smith normal form

- Recall that the Smith normal form of a (possibly nonsquare) integer matrix is a diagonal matrix of the same size, with the diagonal entries subject to certain divisibility conditions.
- More precisely, if A is an $m \times n$ integer matrix, then there exist unimodular (invertible over the integers) matrices P and Q such that the matrix $PAQ = (d_{i,j})$ satisfies

$$d_{i,j} = 0, \text{ for } i \neq j$$

and

$$d_{i,i} \text{ divides } d_{i+1,i+1}, \text{ for } 1 \leq i < \min\{m, n\}.$$

Smith normal form

- Recall that the Smith normal form of a (possibly nonsquare) integer matrix is a diagonal matrix of the same size, with the diagonal entries subject to certain divisibility conditions.
- More precisely, if A is an $m \times n$ integer matrix, then there exist unimodular (invertible over the integers) matrices P and Q such that the matrix $PAQ = (d_{i,j})$ satisfies

$$d_{i,j} = 0, \text{ for } i \neq j$$

  and

$$d_{i,i} \text{ divides } d_{i+1,i+1}, \text{ for } 1 \leq i < \min\{m, n\}.$$

- The diagonal entries of the Smith normal form of A are unique up to sign, and are called the invariant factors of the matrix A. The largest prime powers dividing the invariant factors are called the elementary divisors of A.

Outline

Incidence of Subspaces

- V an n-dimensional vector space over a finite field $\mathbb{F}_q$ of $q = p^t$ elements.

Incidence of Subspaces

- V an n-dimensional vector space over a finite field $\mathbb{F}_q$ of $q = p^t$ elements.
- $\mathcal{L}_r$ denotes the collection of r-dimensional subspaces.

Incidence of Subspaces

- V an n-dimensional vector space over a finite field $\mathbb{F}_q$ of $q = p^t$ elements.
- $\mathcal{L}_r$ denotes the collection of r-dimensional subspaces.
- $\mathcal{L}_r$ vs. $\mathcal{L}_s$; various possible notions of incidence.

Incidence of Subspaces

- V an n-dimensional vector space over a finite field $\mathbb{F}_q$ of $q = p^t$ elements.
- $\mathcal{L}_r$ denotes the collection of r-dimensional subspaces.
- $\mathcal{L}_r$ vs. $\mathcal{L}_s$; various possible notions of incidence.
- Consider the incidence relation of *zero-intersection*, and let $A_{r,s}$ denote the $\left[{n \atop r}\right]_q \times \left[{n \atop s}\right]_q$ incidence matrix.

Some History (zero-intersection)

- (1968) Hamada gives formula for p-rank of $A_{r,s}$ when $r = 1$.
- (1980) Lander gives SNF of points vs. lines in $PG(2, q)$.
- (1990) Black and List compute SNF of points vs. hyperplanes when $q = p$.
- (2000) Sin gives SNF of points vs. s-subspaces when $q = p$.
- (2002) Liebler and Sin work out SNF of points vs. hyperplanes for arbitrary q.
- (2004) Sin computes p-ranks for r-subspaces vs. s-subspaces.
- (2006) Chandler, Sin, Xiang give SNF of points vs. s-subspaces for arbitrary q.
- Natural to consider when V is 4-dimensional over $\mathbb{F}_q$, incidence of $\mathcal{L}_2$ vs. $\mathcal{L}_2$; i.e. skew lines in $\mathrm{PG}(3, q)$.

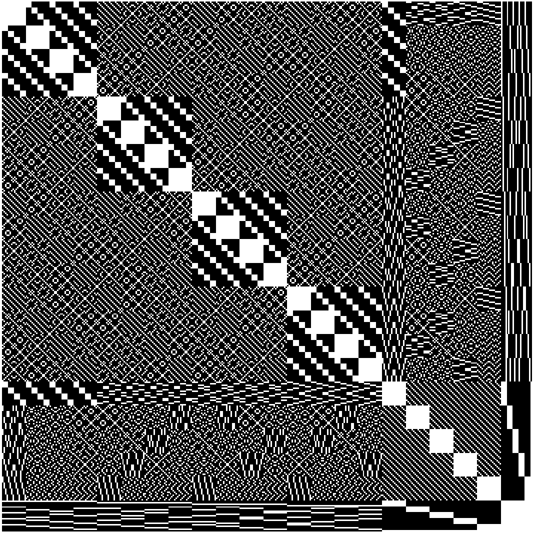
SRG equation

- $A = A_{2,2}$ satisfies

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

- A has eigenvalues q, $-q^2$, q^4 with respective multiplicities $q^4 + q^2, \quad q^3 + q^2 + q, \quad$ and 1
- $|\det(A)| = q^{q^4+2q^3+3q^2+2q+4}$
- In particular, all the invariant factors of A are powers of p

Example: skew lines in $\mathrm{PG}(3,4)$



Example: skew lines in $\mathrm{PG}(3,4)$

Table: The elementary divisors of the incidence matrix of lines vs. lines in $\mathrm{PG}(3,4)$, where two lines are incident when skew.

Elem. Div.	1	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8
Multiplicity	36	16	220	0	32	16	36	0	1

Table: LinBox computations for some small values of $q = p^t$.

	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	$\cdots$
$q = 2$	6	14	8	6	1									
$q = 3$	19	71	20	19	1									
$q = 5$	85	565	70	85	1									
$q = 7$	231	2219	168	231	1									
$q = 2^2$	36	16	220		32	16	36		1					
$q = 3^2$	361	256	6025		202	256	361		1					
$q = 2^3$	216	144	96	3704			128	96	144	216			1	

Here e_i denotes the multiplicity of p^i as an elementary divisor of A. An empty entry in the table denotes a 0.

Theorem (Brouwer–D–Sin, 2011)

Let e_i denote the number of times p^i occurs in the Smith normal form of A. Then, for $0 \leq i \leq t$,

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

Notation key:

- $\mathcal{H}(i) = \left\{(s_0, \ldots, s_{t-1}) \in [3]^t \;\middle|\; \#\{j | s_j = 2\} = i\right\}$.

Theorem (Brouwer–D–Sin, 2011)

Let e_i denote the number of times p^i occurs in the Smith normal form of A. Then, for $0 \leq i \leq t$,

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

Notation key:

- $\mathcal{H}(i) = \left\{ (s_0, \ldots, s_{t-1}) \in [3]^t \;\middle|\; \#\{j | s_j = 2\} = i \right\}$.
- For $\vec{s} = (s_0, \ldots, s_{t-1}) \in [3]^t$ define the integer tuple $\vec{\lambda} = (\lambda_0, \ldots, \lambda_{t-1})$ by $\lambda_i = ps_{i+1} - s_i$, with the subscripts read mod t.

Theorem (Brouwer–D–Sin, 2011)

Let e_i denote the number of times p^i occurs in the Smith normal form of A. Then, for $0 \le i \le t$,

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

Notation key:

- $\mathcal{H}(i) = \left\{ (s_0, \ldots, s_{t-1}) \in [3]^t \;\middle|\; \#\{j | s_j = 2\} = i \right\}$.
- For $\vec{s} = (s_0, \ldots, s_{t-1}) \in [3]^t$ define the integer tuple $\vec{\lambda} = (\lambda_0, \ldots, \lambda_{t-1})$ by $\lambda_i = ps_{i+1} - s_i$, with the subscripts read mod t.
- d_k is the coefficient of x^k in the expansion of $(1 + x + \cdots + x^{p-1})^4$.

Theorem (Brouwer–D–Sin, 2011)

Let e_i denote the number of times p^i occurs in the Smith normal form of A. Then, for $0 \le i \le t$,

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

Notation key:

- $\mathcal{H}(i) = \left\{ (s_0, \ldots, s_{t-1}) \in [3]^t \,\middle|\, \#\{j | s_j = 2\} = i \right\}$.
- For $\vec{s} = (s_0, \ldots, s_{t-1}) \in [3]^t$ define the integer tuple $\vec{\lambda} = (\lambda_0, \ldots, \lambda_{t-1})$ by $\lambda_i = ps_{i+1} - s_i$, with the subscripts read mod t.
- d_k is the coefficient of x^k in the expansion of $(1 + x + \cdots + x^{p-1})^4$.
- $d(\vec{s}) = \prod_{i=0}^{t-1} d_{\lambda_i}$.

Outline

1. Smith normal form
2. Incidence of Subspaces
3. Incidence maps and SNF bases

- R is a discrete valuation ring, maximal ideal generated by p.
- $\eta\colon R^m \to R^n$
- $M_i = \{x \in R^m \,|\, \eta(x) \in p^i R^n\}$
- $N_i = \{p^{-i}\eta(x) \,|\, x \in M_i\}$
- Set $F = R/pR$. $\overline{L} = (L + pR^\ell)/pR^\ell$ is an F-vector space.
- $e_i = \dim_F \left(\overline{M_i}/\overline{M_{i+1}}\right) = \dim_F \left(\overline{N_i}/\overline{N_{i-1}}\right)$

Some equations

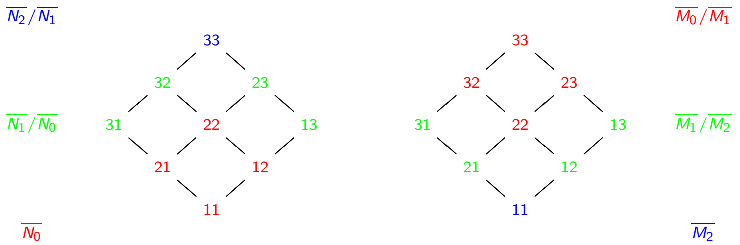
- $A(A+(q^2-q)I) = q^3 I + (q^4-q^3)J$

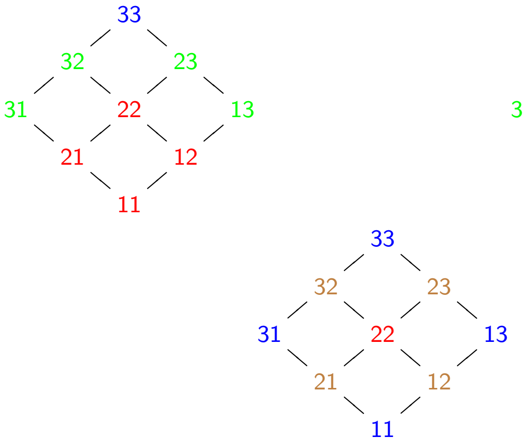
Some equations

- $A(A+(q^2-q)I) = q^3 I + (q^4-q^3)J$
- $A_{2,1}A_{1,2} = (q^3+q^2)I+(q^3+q^2-q-1)A+(q^3+q^2-q)(J-A-I)$

Some equations

- $A(A+(q^2-q)I) = q^3 I + (q^4-q^3)J$
- $A_{2,1}A_{1,2} = (q^3+q^2)I + (q^3+q^2-q-1)A + (q^3+q^2-q)(J-A-I)$
- $A_{2,1}A_{1,2} = -[A+(q^2-q)I] + q^2 I + (q^3+q^2-q)J$


$\overline{N_2}/\overline{N_1}$
$\overline{N_1}/\overline{N_0}$
$\overline{N_0}$
33
32 23
31 22 13
21 12
11
33
32 23
31 22 13
21 12
11
$\overline{M_0}/\overline{M_1}$
$\overline{M_1}/\overline{M_2}$
$\overline{M_2}$


33
32 23
31 22 13
21 12
11
33
32 23
31 22 13
21 12
11
33
32 23
31 22 13
21 12
11

Thank you for your attention!