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

Josh Ducey

University of Florida

March 14, 2011

Outline

Smith Normal Form

- Let M and N be matrices with integer entries.
- We call M and N "equivalent," and write $M \sim N$, if

$$PMQ = N$$

  where P and Q are invertible integer matrices with determinants ± 1.
- If M is an integer matrix, then M is equivalent to a diagonal matrix

$$S(M) = \mathrm{diag}(s_1, s_2, \ldots, s_k)$$

  with the property that s_i divides s_{i+1}, for $1 \leq i \leq k-1$. This matrix $S(M)$ is uniquely determined, up to the sign of the diagonal entries, and is called the Smith normal form of M.

An Example

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}, \; P = \begin{pmatrix} 1 & 0 \\ 4 & -1 \end{pmatrix}, \; Q = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}.$$

$$S(M) = PMQ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}.$$

Row/Column Operations

$S(M)$ can be computed from M using row and column operations. These are:

- Swap any two rows (columns) of M.
- Multiply any row (column) by -1.
- Add to any row (column) an integer multiple of another row (column).

That is, P and Q can be formed from products of elementary matrices.

GCDs of Minors

It follows from the Cauchy–Binet formula that $s_1 \cdot s_2 \cdots s_j$ is equal to the greatest common divisor of all determinants of $j \times j$ submatrices of M.

Some Uses

- Determinant, rank.
- Linear Diophantine problems.
- Structure of abelian groups.

Changing Perspective

- Can view the $m \times n$ matrix M as a linear map $\mathbb{R}^n \to \mathbb{R}^m$.
- P, Q arise from a change of basis.
- Correct way to view matrix is as a homomorphism of free abelian groups.

Outline

Incidence Matrices

- These arise when one attempts to find invariants of a relation between two finite sets.
- Studied by researchers in design theory, coding theory, algebraic graph theory, representation theory, finite geometry.
- The incidence structure is encoded in a zero-one matrix; various numerical invariants of the matrix now become invariants of the incidence structure.
- The zero-one matrix can be read over any commutative ring. Viewed over a field, we get rank, p-rank. Over the integers, we get SNF.

Incidence of Subsets

- X a finite set, $|X| = n$.
- X_r denotes the collection of subsets of size r.
- X_r vs. X_s; there are various possible incidence relations.

Application: Existence of Designs

- A $t-(v,k,\lambda)$ design is a set of v points together with a collection of subsets of size k, called blocks, satisfying the following property: each subset of size t is contained in exactly λ blocks.
- Let $|X| = v$. Consider the incidence structure X_t vs. X_k, where incidence means *inclusion*.
- $W_{t,k}$ the $\binom{v}{t} \times \binom{v}{k}$ incidence matrix.
- There exists a $t-(v,k,\lambda)$ design on X if and only if there exists a vector $\vec{x}$ with nonnegative integer entries such that

$$W_{t,k}\vec{x} = \lambda\mathbf{j}.$$

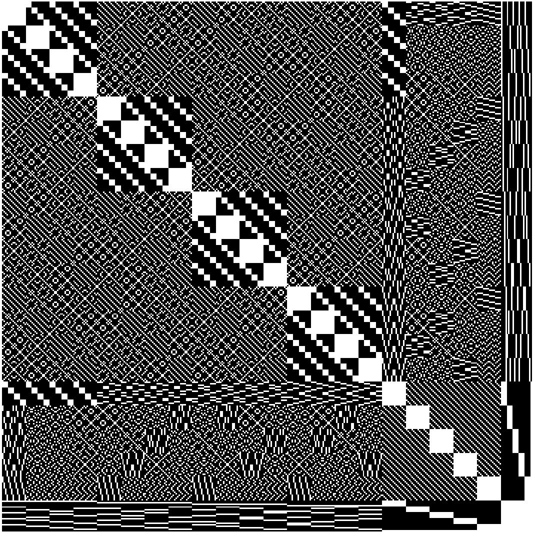
Incidence of Subspaces

- 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 $\mathrm{PG}(3, q)$.

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 Here $q = p^t$ and e_i denotes the multiplicity of p^i as an elementary divisor of $A_{2,2}$.

	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}
$q = 2$	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	0	32	16	36	0	1				
$q = 3^2$	361	256	6025	0	202	256	361	0	1				
$q = 2^3$	216	144	96	3704	0	0	128	96	144	216	0	0	1

Theorem (Brouwer, Ducey, Sin, 2011)

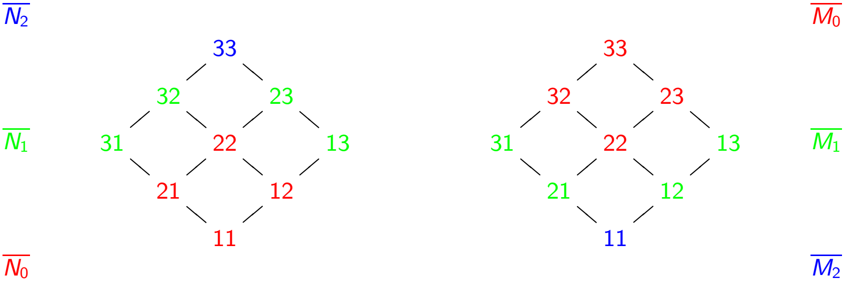
Let e_i denote the number of times p^i occurs in the Smith normal form of $A_{2,2}$. Then, for $0 \leq i \leq t$,

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

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.
- d_k is the coefficient of x^k in the expansion of $(1 + x + \cdots + x^{p-1})^4$.
- $d(\vec{s}) = \prod_{i=0}^{t-1} d_{\lambda_i}$.

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


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

Outline

Work to be done:

- zero-intersection of subspaces, subspace-inclusion, distinguished subspaces
- further applications of SNF
- further applications of representation theory

To undergraduates interested in research:

- learn linear algebra
- get SAGE

```
x = walltime()
p = 2
t = 1
q = p^t
F.<t> = GF(q)
V = VectorSpace(F, 6)
S = tuple(V.subspaces(3))
l = len(S)

print "now forming incidence matrix A"
A = matrix(ZZ, l)
for i in range(l-1):
    for j in range(i+1, l):
        if dim(S[i].intersection(S[j])) == 0:
            A[i,j] = 1

A = A + A.transpose()

y = walltime(x)
print "took", y, "seconds"

save(A, './programs/Results-6dim/incmat2')
```

Thank you for your attention!