Integer Invariants of Skew Lines in $PG(3,q)$

Joshua Ducey
University of Florida

Joint work with Peter Sin

The Problem

- V a 4-dimensional vector space over $\mathbb{F}_q$
- Form incidence matrix A, a zero-one matrix with rows and columns indexed by the 2-subspaces of V
- The entry of A corresponding to a pair of 2-subspaces is 1 if and only if their intersection is trivial
- Goal is to compute the Smith Normal Form of A as an integer matrix

Some Motivation (and some notation)

- More generally, let V be an $(n+1)$-dimensional vector space over $\mathbb{F}_q$
- $\mathcal{L}_i$ denotes the set of i-subspaces of V
- $A_{r,s}$ denotes incidence matrix of r-subspaces vs. s-subspaces where incidence means zero-intersection

Some Motivation

- (1968) Hamada gives formula for p-rank of $A_{r,s}$ when $r = 1$
- (2004) Sin computes p-ranks for r-subspaces vs. s-subspaces
- (1980) Lander gives SNF for points vs. lines in $PG(2, q)$
- (1990) Black and List compute SNF for points vs. hyperplanes when $q = p$
- (2000) Sin gives SNF for points vs. s-subspaces when $q = p$
- (2002) Liebler and Sin work out SNF for points vs. hyperplanes for arbitrary q. Conjecture a formula for points vs. s-subspaces
- (2006) Conjecture is proved by Chandler, Sin, Xiang

Back to Our Specific Example

- V is 4-dimensional over $\mathbb{F}_q$
- $A = A_{2,2}$, incidence matrix of lines vs. lines in $PG(3, q)$
- Two lines are incident when they are skew

- Can view this situation from the point-of-view of strongly regular graphs
- A has eigenvalues q, $-q^2$, q^4 with respective multiplicities $q^4 + q^2$, $q^3 + q^2 + q$, 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
- Let e_i denote the multiplicity of p^i as an invariant factor of A

The Prime Case: $q = p$

Some computations:

	$q=2$	$q=3$	$q=5$	$q=7$
e_0	6	19	85	231
e_1	14	71	565	2219
e_2	9	20	70	168
e_3	6	19	85	231
e_4	1	1	1	1

$q = p$

Theorem: The invariant factors of the incidence matrix A are all p-powers, and are as given in the table below.

Invariant Factor	Multiplicity
1	$p(2p^2+1)/3$
p	$p(3p^3-2p^2+3p-1)/3$
p^2	$p(p+1)(p+2)/3$
p^3	$p(2p^2+1)/3$
p^4	1

What about arbitrary q?

The General Case: $q = p^t$

	$q=2$	$q=3$	$q=5$	$q=7$	$q=2^2$	$q=3^2$	$q=2^3$
e_0	6	19	85	231	36	361	216
e_1	14	71	565	2219	16	256	144
e_2	8	20	70	168	220	6025	96
e_3	6	19	85	231	0	0	3704
e_4	1	1	1	1	32	202	0
e_5					16	256	0
e_6					36	361	128
e_7					0	0	96
e_8					1	1	144
e_9							216
e_{10}							0
e_{11}							0
e_{12}							1

A. E. Brouwer (private communication) deduced that

$$e_0 + \cdots + e_t = q^4 + q^2,$$

$$e_{2t} + \cdots + e_{3t} = q^3 + q^2 + q,$$

and

$$e_{4t} = 1.$$

All other multiplicities are then forced to be zero. Furthermore, $e_i = e_{3i-1}$ for $0 \leq i < t$. Brouwer did not make use of the geometry, so these facts hold for any strongly regular graph with the same parameters.

- Thus the problem has been reduced to calculating the numbers $e_0, e_1, \cdots, e_{t-1}$.
- I would now like to try and explain where these numbers come from.
- To do so, we recast the problem in terms of permutation-modules for $G = GL(4, q)$

The Modules M_i

- Can view the incidence matrix A as defining a homomorphism of free abelian groups

$$\eta : \mathbb{Z}^{\mathcal{L}_2} \to \mathbb{Z}^{\mathcal{L}_2}$$

  that sends an 2-subspace to the (formal) sum of all 2-subspaces incident with it.

- G acts transitively on the sets $\mathcal{L}_i$, and η a homomorphism of $\mathbb{Z}G$-permutation modules
- Define a sequence of $\mathbb{Z}G$-submodules $\{M_i\}_{i\geq 0}$ of $\mathbb{Z}^{\mathcal{L}_2}$ as follows. Put $M_0 = \mathbb{Z}^{\mathcal{L}_2}$, and for $i \geq 1$ put

$$M_i = \{m \in \mathbb{Z}^{\mathcal{L}_2} \mid \eta(m) \in p^i \mathbb{Z}^{\mathcal{L}_2}\}.$$

- $\mathbb{Z}^{\mathcal{L}_2} = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$

- We have an induced p-filtration

$$\mathbb{F}_p^{\mathcal{L}_2} = \overline{M_0} \supseteq \overline{M_1} \supseteq \overline{M_2} \supseteq \cdots$$

  of $\mathbb{F}_p G$-submodules.
- With a little thought, one sees that for each $i \geq 0$ the multiplicity of p^i as an elementary divisor of A is precisely $\dim_{\mathbb{F}_p}(\overline{M_i}/\overline{M_{i+1}})$.

Furthermore, if we define for $r = 1, 2, 3$

$$Y_r = \left\{ \sum_{x \in \mathcal{L}_r} a_x x \in \mathbb{F}_p^{\mathcal{L}_r} \;\middle|\; \sum_{x \in \mathcal{L}_r} a_x = 0 \right\}.$$

then we have the decompositions

$$\mathbb{F}_p^{\mathcal{L}_1} = \mathbb{F}_p \mathbf{1} \oplus Y_1.$$

$$\mathbb{F}_p^{\mathcal{L}_2} = \mathbb{F}_p \mathbf{1} \oplus Y_2.$$

$$\mathbb{F}_p^{\mathcal{L}_3} = \mathbb{F}_p \mathbf{1} \oplus Y_3.$$

The set $\mathcal{H}$

The module Y_1 is well understood from work of Bardoe and Sin (2000). Let $\mathcal{H}$ denote the set of t-tuples $(s_0, s_1, \cdots, s_{t-1})$ of integers satisfying (for $0 \le j \le t-1$):

1. $1 \le s_j \le 3$,
2. $0 \le ps_{j+1} - s_j \le 4(p-1)$,

with subscripts read modulo t.

Thanks for your attention!