PROBLEMS IN ALGEBRAIC COMBINATORICS

By

JOSHUA E. DUCEY

A DISSERTATION PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA

2011

I dedicate this work:

To my family, especially:

Lawrence and Ruth Ducey; Melissa and Michael Poteat; Mallory, Alex, Julie, and Nick

Your unconditional love and support have surely made me stronger than I can know.

To Matt Branco, my oldest friend

To my pug, Aro

Finally, to my future wife, Minah Oh

You have made the last few years of my life feel like a great adventure, and I cannot wait to begin a new adventure with you.

ACKNOWLEDGMENTS

I must begin by thanking my advisor, Dr. Peter Sin. You have taught me much about mathematics, and also about being a mathematician. Thank you for our many discussions, and for showing me things that I can think about for the rest of my life. I consider it a great honor to have been your student.

To the other members of my committee: Dr. Richard Crew, Dr. Pierre Ramond, Dr. Paul Robinson, and Dr. Alex Turull; I thank you all for the comments made, questions asked, and advice given during the completion of this work. You have each made me a better mathematician in some way.

I wish to thank Dr. Miklós Bóna for teaching me how to count, and to thank Dr. Yuli Rudyak for teaching me topology. To Jim Davis, I thank you for instilling confidence in me as my teacher, and for the support you have given me as my colleague. If not for you, I would not be here.

Many numerical experiments were performed during the completion of this work. I would like to thank the creators and developers of Sage (www.sagemath.org) for making available such powerful mathematical software. Thanks also to the team behind the exact linear algebra software LinBox (www.linalg.org), which I made much use of.

I am grateful to the University of Florida Mathematics Department for being a stimulating research environment, and also for giving me the opportunity to discover that I love to teach. I thank the University of Florida College of Liberal Arts and Sciences for awarding me with the Keene Dissertation Fellowship, which helped to make my final semester here a very productive one. For the generous support I received through the Chat Yin Ho Memorial Scholarship, I sincerely thank the family and friends of Professor Ho.

The most important results of this work make up a paper co–authored by Dr. Andries E. Brouwer, Dr. Peter Sin, and myself, that is currently being refereed. I am thankful for the unique perspectives and talents of these two, and I am convinced that

the rather different ways in which we each approached the problem were critical to our success. Finally, I thank the Banff International Research Station, where discussion of this work began at a workshop in March of 2009.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure page

Abstract of Dissertation Presented to the Graduate School
of the University of Florida in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy

PROBLEMS IN ALGEBRAIC COMBINATORICS

By

Joshua E. Ducey

May 2011

Chair: Peter Sin
Major: Mathematics

The main result of this work is the determination of the Smith normal form of the incidence matrix of lines vs. lines in $\mathrm{PG}(3, q)$, where $q = p^t$ is a prime power and two lines are defined to be incident if and only if they are skew. This principal result is essentially a corollary of a more general theorem. In order to prove the general theorem, we develop some new ideas in the basic theory of elementary divisors, and also employ some representation theory. As another corollary to the general theorem, we obtain some specific knowledge of the p-adic elementary divisors of the incidence matrix of r-dimensional subspaces vs. s-dimensional subspaces in $\mathrm{PG}(n, q)$, where incidence again means zero–intersection.

CHAPTER 1
INTRODUCTION

1.1 Incidence Matrices

One of the most ubiquitous concepts in mathematics is that of an incidence structure. This is just a triple $(X, Y, \mathcal{I})$ consisting of two sets of objects together with a relation $\mathcal{I} \subseteq X \times Y$ between them. If an object in the first set is related to an object in the second set, we say that these two are "incident." Often the sets are required to be disjoint, but that is not important to us. We will however deal exclusively with finite sets.

Given a finite incidence structure, it can be encoded into a rectangular array as follows. Let the rows of the array correspond to the first set of objects; the columns correspond to the second set of objects. Then we place a one in the (i, j)-position of the array if the object corresponding to row i is incident with the object corresponding to column j, otherwise that position gets a zero. Such an array is called an *incidence matrix*.

Since the incidence matrix carries all of the information, it is a good thing to study. Various numerical invariants of the matrix now become invariants of the incidence structure. Very often these matrices arise from geometric or combinatorial considerations, so in a sense these invariants are analogous to the homology or Euler characteristic of a topological space.

Consider, for example, the situation when the matrix is square (so both sets have the same size). If furthermore the two sets are equal and the relation is symmetric, then the incidence structure is just a graph, and the matrix is usually called an adjacency matrix (see Section 2.4). Natural invariants to consider are the eigenvalues, and certain properties of the graph are reflected in the spectrum of the matrix.

For non–square matrices, the rank of the incidence matrix is a good choice of invariant. By changing the field that you view the matrix entries to be coming from, the rank may change. The rank over a field of characteristic p is usually called the p-rank

of the matrix. An incidence matrix is in particular an integer matrix, so we can also consider its Smith normal form. This is just some uniquely determined diagonal matrix, see Sections 2.1 and 2.2 for details. The Smith normal form is a rather strong invariant, in the sense that from it one can immediately deduce the rank and p-rank of the matrix, for any prime p. For information about the relationship between the Smith normal form of an integer matrix and its spectrum, see [10, 11].

1.2 Statement of the Problem

Let V be a 4-dimensional vector space over the finite field $\mathbb{F}_q$ of $q = p^t$ elements, where p is a prime. We declare two 2-dimensional subspaces U and W to be incident if and only if $U \cap W = \{0\}$. Ordering the 2-dimensional subspaces in some arbitrary but fixed manner, we can form the incidence matrix A of this relation. The goal is to compute the Smith normal form of A as an integer matrix.

1.3 Some Motivation

It is useful to view this problem in a more general context. Suppose now that V is an $(n+1)$-dimensional vector space over the finite field $\mathbb{F}_q$ of $q = p^t$ elements. Denote by $\mathcal{L}_r$ the set of r-dimensional subspaces of V. So $\mathcal{L}_1$ denotes the points, $\mathcal{L}_2$ denotes the lines, etc. of the projective geometry $\mathbb{P}(V)$. Define an r-dimensional subspace U and an s-dimensional subspace W to be incident if and only if $U \cap W = \{0\}$, and denote by $A_{r,s}$ the $|\mathcal{L}_r| \times |\mathcal{L}_s|$ incidence matrix.

These matrices $A_{r,s}$ are naturally interesting, and mathematicians have been studying them since at least the 1960s. The reader is referred to the surveys [16, 17] (see also [4, Introduction]). By setting $n = 3$, $r = s = 2$, and $A = A_{2,2}$, we recover the situation described in the above problem. By the well–known Klein correspondence [7, Chapter 15] (identifying the lines in $\mathrm{PG}(3, q)$ with the points of a hyberbolic quadric in $\mathrm{PG}(5, q)$), A may also be regarded as the adjacency matrix of the non–collinearity graph on the points of the Klein quadric. In general, when $r = s$ these matrices can be viewed as adjacency matrices of q-analogues of the Kneser graphs.

When $r = 1$, the incidence structure is that of a 2-design with "classical parameters," and these incidence matrices are the generator matrices of codes closely related to the Reed–Muller codes [1]. This is what initially motivated their study, and in this case their Smith normal forms have been found [4, 9, 12]. The p-rank of $A_{r,s}$ has been found in general [13], but when neither r nor s is one its Smith normal form is not known. It is thus natural to consider when both r and s are greater than one, and the problem described above is just the first nontrivial case.

One can choose to consider notions of incidence other than zero–intersection. A basic example is the subspace–inclusion relation; that is, two subspaces would be called incident if the smaller one were contained in the larger. These incidence structures are obvious q-generalizations of corresponding relations between subsets of a finite set. Observe, however, that a subset T is contained in another subset K if and only if T is disjoint from the complement of K. Thus when dealing with *sets* the inclusion and empty–intersection relations are really the same thing, and in this case the integer invariants have been found [15]. This does not carry over to spaces. The subspace–inclusion relation is much more difficult to understand than zero–intersection: it is still an open problem to calculate the p-ranks of the inclusion matrices.

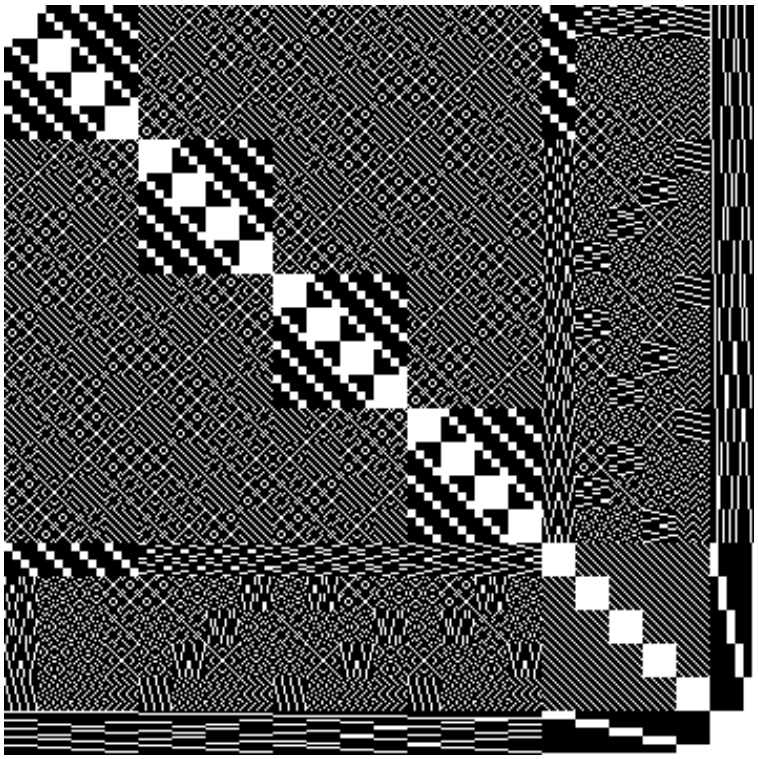

Figure 1-1. The incidence matrix of lines vs. lines in $\mathrm{PG}(3,4)$, where two lines are incident when skew. A black pixel is a 1, a white pixel is a 0.

CHAPTER 2
PRELIMINARIES AND DEFINITIONS

2.1 The Smith Normal Form

A square matrix with integer entries is called *unimodular* if its determinant is ± 1. If M and N are $m \times n$ matrices with integer entries, then we say M and N are *equivalent* if there exist unimodular integer matrices P and Q with

$$PMQ^{-1} = N.$$

This is an equivalence relation on the set of $m \times n$ integer matrices. The *Smith normal form* of an integer matrix M is just a particular diagonal matrix that represents the class of M. Precisely, if M is an $m \times n$ integer matrix, then there exist unimodular integer matrices P and Q such that the matrix $S(M) = PMQ^{-1} = (d_{i,j})$ satisfies

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

and

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

This divisibility condition determines $S(M)$ up to the sign of the diagonal entries, and it is always with this understanding that we refer to $S(M)$ as "the" Smith normal form of M. The nonzero diagonal entries of $S(M)$, counted with multiplicity, are called the *invariant factors* of the matrix M. Breaking apart the invariant factors into powers of distinct primes, we get the *elementary divisors* of M. These are also determined up to sign, and counted with multiplicity. A couple examples should make all of this clear.

Example 2.1. Let $M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$. Choosing

$$P = \begin{pmatrix} 1 & 0 \\ 4 & -1 \end{pmatrix}, \quad Q^{-1} = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix},$$

we have

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

The invariant factors are 1 and 3, each occurring with multiplicity one. The elementary divisors are also 1 and 3, each occurring with multiplicity one.

Example 2.2. Let

$$M = \begin{pmatrix} -31672 & 522 & -2632 & 12138 \\ -5824 & 96 & -484 & 2232 \\ 34224 & -564 & 2844 & -13116 \end{pmatrix}.$$

Setting

$$P = \begin{pmatrix} 3 & 13 & 5 \\ 2 & 1 & 2 \\ -2 & 5 & -1 \end{pmatrix}, \quad Q^{-1} = \begin{pmatrix} 3 & 2 & 3 & 2 \\ -6 & 4 & -4 & -5 \\ -5 & -5 & 0 & -2 \\ 7 & 4 & 8 & 5 \end{pmatrix},$$

we have

$$S(M) = PMQ^{-1} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The invariant factors are 2 and 12, each occurring with multiplicity one. The elementary divisors are 2, 4, and 3, each occurring with multiplicity one.

Many very interesting examples can be found in [11]. Since knowledge of the invariant factors is equivalent to knowledge of the elementary divisors, we will be focusing our attention on the latter. Our terminology is reasonably standard, although in the literature one finds an apparent dispute over what the exact meaning of these terms should be. The Smith normal form is named after Henry John Stephen Smith (1826–1883). Aside from being a very talented scholar and administrator, all accounts of his life seem to describe him as a charming and modest man who never made an enemy or lost a friend [5].

2.2 Localization

Since incidence matrices are zero–one matrices, we can view their entries as coming from any commutative ring R. When R is a principal ideal domain, there is a completely analogous notion of Smith normal form "over R." See for example [10]. Indeed, the statement that an integer matrix has a Smith normal form is really just a matrix–theoretic description of the structure theorem for finitely generated abelian groups, and this theorem generalizes to finitely generated modules over principal ideal domains [8, Chapters 4, 7]. In this context of matrices over R, the statement that P and Q are unimodular means that they have entries coming from R and their determinants are units in this ring (the purpose of this condition is to guarantee that P^{-1} and Q^{-1} also have entries in R). The diagonal entries of the Smith normal form over R are unique up to multiplication by a unit in R, and when speaking of invariant factors or elementary divisors over this ring we do not distinguish between associates. Thus when we speak of the multiplicity of a particular invariant factor or elementary divisor, we are really counting the number of occurrences of its associates.

An important special case is when R is an extension ring of the ring of integers $\mathbb{Z}$. Notice that if P and Q are unimodular as integer matrices then they are still unimodular as matrices over R. Thus if M is an integer matrix and $S(M)$ is its Smith normal form over $\mathbb{Z}$, then $S(M)$ is the Smith normal form of M over R. However, if there are non–unit elements of $\mathbb{Z}$ that become units in the ring R, then the elementary divisor multiplicities over each ring need not be the same. More generally, similar statements hold true when R contains a homomorphic image of $\mathbb{Z}$.

Example 2.3. Take $R = \mathbb{Q}$ to be the rational numbers and M to be the matrix from Example 2.2. Then the nonzero diagonal entries of $S(M)$ are all units in $\mathbb{Q}$, so that (as a rational matrix) M has 1 as its only elementary divisor, occurring with multiplicity two. Observe that the rank of an integer matrix is just the number of nonzero diagonal entries of its Smith normal form over $\mathbb{Z}$.

Example 2.4. Take $R = \mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ to be the finite field of 3 elements, and again let M be the matrix from Example 2.2. Let $\overline{M}$ be the matrix obtained by reducing all entries of $M \pmod 3$. Then 1 is the only elementary divisor of $\overline{M}$, occurring with multiplicity one. In general, the p-rank of an integer matrix is just the number of diagonal entries of its Smith normal form over $\mathbb{Z}$ that are not divisible by p.

Example 2.5. Take $R = \mathbb{Z}_p$ to be the ring of p-adic integers, M the matrix from Example 2.2. The elements of $\mathbb{Z}$ that become units in the ring $\mathbb{Z}_p$ are precisely the integers not divisible by p. Thus as a matrix over $\mathbb{Z}_2$, the elementary divisors of M are 2 and 4 both with multiplicity one. Over $\mathbb{Z}_3$, the elementary divisors of M are 1 and 3 both with multiplicity one. For any other (rational) prime p, M as a matrix over $\mathbb{Z}_p$ has 1 as its only elementary divisor, occurring with multiplicity two.

All of these examples show that the Smith normal form of an integer matrix carries a great deal of information. The last example in particular shows that if we are interested only in the p-elementary divisors of an integer matrix (that is, those elementary divisors that are positive powers of a particular prime p), then we may choose to view the matrix entries as coming from $\mathbb{Z}_p$ rather than $\mathbb{Z}$. We will always be clear about which ring we consider our matrix entries to be coming from.

2.3 Incidence Maps and Representation Theory

Representation theory can be a very powerful tool in the study of incidence matrices. This is because the incidence structures that are most interesting usually have some group acting on them. To be clear, consider an incidence structure $(X, Y, \mathcal{I})$, where X and Y are finite sets and $\mathcal{I}$ is the incidence relation

$$\mathcal{I} \subseteq X \times Y.$$

Ordering the sets X and Y, we form the incidence matrix M of this relation. When we view the matrix entries as coming from some commutative ring R, the $|X| \times |Y|$ matrix M

represents a homomorphism of free R-modules

$$\eta\colon R^X \to R^Y,$$

where R^Z consists of all R-valued functions on the set Z. Since we will not be needing this "function notation," we identify each element of Z with its characteristic function, and view R^Z as consisting of formal R-linear combinations of the elements of Z. With these identifications, the above mapping η sends each element of $x \in X$ to the sum of the elements of Y that are incident with x, and by linearity this property completely defines the map. If the ring R is a field, then the rank of M is just the dimension of the image of η. For R a principal ideal domain, there is module–theoretic description of the Smith normal form of M (see Chapter 4).

Now if G is a finite group acting transitively on the sets X and Y, then R^X and R^Y are permutation modules for the group ring RG. Furthermore, if the action of G preserves the incidence relation, i.e.

$$(x, y) \in \mathcal{I} \text{ implies } (gx, gy) \in \mathcal{I}, \quad \text{for all } g \in G,$$

then η becomes a homomorphism of RG-modules. Thus the image, kernel, etc. of η are RG-submodules, and in general this places extremely severe limitations on what their structure can be. In turn, this information becomes relevant and useful to our study of the incidence structure's invariants. As can be expected, various difficulties arise and techniques are used depending on the ring R. Most of what we need can be found nicely summarized in [9, Appendices D, E, F].

2.4 Graph Theory and Matrix Identities

A *graph* $(\mathcal{V}, \mathcal{E})$ is a set $\mathcal{V}$ of *vertices* and a collection $\mathcal{E}$ of 2-element subsets of $\mathcal{V}$ called *edges*. If $\{x, y\} \in \mathcal{E}$, then the vertices x and y are said to be adjacent. Graph theory terminology can vary considerably, and what we are calling a graph some authors would call a "simple" or "loopless" graph.

Alternatively, for us a graph is just an incidence structure $(\mathcal{V}, \mathcal{V}, \mathcal{I})$ where $\mathcal{I}$ is a symmetric relation and no element of $\mathcal{V}$ is incident with itself. Ordering the set $\mathcal{V}$, we can form the incidence matrix of this relation. This symmetric matrix is usually called the *adjacency matrix* of the graph.

A graph is called *regular* with valency k if each vertex is adjacent to exactly k other vertices. A graph $(\mathcal{V}, \mathcal{E})$ is *strongly regular* with parameters v, k, λ, μ if

1. $|\mathcal{V}| = v$,
2. the graph is regular of valency k,
3. if x and y are adjacent vertices, then there are exactly λ vertices adjacent to both x and y,
4. if x and y are (distinct) non–adjacent vertices, then there are exactly μ vertices adjacent to both x and y.

If M is the adjacency matrix of a strongly regular graph with parameters v, k, λ, μ, then M satisfies the equation

$$M^2 = kI + \lambda M + \mu(J - M - I), \tag{2–1}$$

where I and J respectively denote the identity matrix and all–one matrix of the same size as M. The reason that this equation holds follows from a more general fact explained below. From this equation it is not difficult to deduce both the eigenvalues of M and their multiplicities, we refer the reader to [3].

To see why Equation (2–1) holds, consider more generally the following situation. Let $(X, Y, \mathcal{I})$ and $(Y, Z, \mathcal{J})$ be two finite incidence structures, and fix an ordering of X, Y, and Z. With respect to these orderings, form the $|X| \times |Y|$ incidence matrix M of the first relation, and the $|Y| \times |Z|$ incidence matrix N of the second relation. Notice that the matrix product MN has rows indexed by X and columns indexed by Z. Let $x \in X$ and $z \in Z$. With a little thought one sees that the (x, z)-entry of the matrix product MN is

precisely the number of $y \in Y$ that are incident with both x and z. In symbols,

$$(MN)_{x,z} = |\{y \in Y \mid (x, y) \in \mathcal{I} \text{ and } (y, z) \in \mathcal{J}\}|.$$

We will frequently make use of this fact. Thus we see that Equation (2–1) is just expressing properties 2, 3, and 4 in the definition of a strongly regular graph.

CHAPTER 3
THE MAIN RESULT

3.1 Statements of Theorems

We return now to the problem described in the introduction (Section 1.2). Thus V is a 4-dimensional vector space over the finite field $\mathbb{F}_q$ of $q = p^t$ elements, $A = A_{2,2}$ is the incidence matrix with rows and columns indexed by the 2-dimensional subspaces of V, and incidence is defined to mean zero–intersection. We will compute the Smith normal form of A as an integer matrix.

It turns out that the elementary divisors of A are all powers of the prime p. A quick way to see this is to regard A as the adjacency matrix of the graph with vertex set $\mathcal{L}_2$, where two lines are adjacent when skew. This is a strongly regular graph (see Section 2.4), with parameters

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

Thus A satisfies the equation

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

where I and J denote the identity matrix and all–one matrix, respectively, of the appropriate sizes. From this equation one deduces that the eigenvalues of A are q, $-q^2$, and q^4 with respective multiplicities $q^4 + q^2$, $q^3 + q^2 + q$, and 1. Since (up to sign, of course) $\det(A)$ is the product of the elementary divisors, we see that the elementary divisors of A are all powers of the prime p.

Therefore describing the Smith normal form of A amounts to specifying the number of times each prime power p^i, $i \geq 0$, occurs as an elementary divisor of A. This number we denote by e_i (or $e_i(A)$, when we wish to emphasize the matrix under discussion). Since the problem is parametrized by our choice of $q = p^t$, it is to be expected that the elementary divisor multiplicities e_i will depend in some way on the exponent t.

The elementary divisor multiplicities are listed in Table 3-1, for some small values of $q = p^t$. It is worthwhile to examine this table briefly before moving on. The next theorem describes some relations that hold among the multiplicities in general, and studying the table for a moment should make the statement of the theorem much clearer.

For example, look at the row of Table 3-1 corresponding to when $q = 8 = 2^3$. Pay special attention to the fact that here $t = 3$. In this row one sees $4\,(= t + 1)$ nonzero entries, followed by $2\,(= t - 1)$ zeros, followed by $4\,(= t + 1)$ nonzero entries, followed by $2\,(= t - 1)$ zeros. The next entry is 1, corresponding to the multiplicity $e_{12}\,(= e_{4t})$, and all remaining multiplicities are zero. Observe the partial "reverse symmetry" in the two chunks of nonzero entries:

$$e_0 = e_9\,(= e_{3t}), \quad e_1 = e_8\,(= e_{3t-1}), \quad e_2 = e_7\,(= e_{3t-2}). \tag{3–2}$$

Adding the multiplicities in these nonzero chunks, we get

$$e_0 + e_1 + e_2 + e_3 = 4160\,(= q^4 + q^2) \tag{3–3}$$

and

$$e_6 + e_7 + e_8 + e_9 = 584\,(= q^3 + q^2 + q). \tag{3–4}$$

Theorem 3.1. *Let $e_i = e_i(A)$ denote the multiplicity of p^i as an elementary divisor of A.*

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

From the identities stated in the above theorem, we can deduce all of the elementary divisor multiplicities once we know t of the numbers $e_0, \ldots, e_t$ (or t of the numbers $e_{2t}, \ldots, e_{3t}$). For example, consider again the row of Table 3-1 corresponding to

$q = 8 = 2^3$ (so $t = 3$). Suppose we know only that $e_6 = 128$, $e_8 = 144$, and $e_9 = 216$. Then part (5) of the theorem is just Equation (3–4), and from this we calculate $e_7 = 96$. In this case part (3) becomes the equations (3–2), and we compute $e_0 = 216$, $e_1 = 144$, and $e_2 = 96$. From Equation (3–3) (part (4) of the theorem) we then get $e_3 = 3704$. Finally, $e_{12} = 1$ and all other multiplicities are zero by parts (1) and (2), respectively.

The next theorem shows how to directly compute each of the multiplicities $e_{2t}, \dots, e_{3t}$. By the discussion above, this data is more than sufficient to determine the Smith normal form of A. To state the theorem, we need some notation.

Set

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

and

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

In other words, $\mathcal{H}(i)$ consists of the tuples in $[3]^t$ with exactly i twos. To each tuple $\vec{s} \in [3]^t$ we associate a number $d(\vec{s})$ as follows. For $\vec{s} = (s_0, \dots, s_{t-1}) \in [3]^t$ define the integer tuple $\vec{\lambda} = (\lambda_0, \dots, \lambda_{t-1})$ by

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

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

Theorem 3.2. *Let $e_i = e_i(A)$ denote the multiplicity of p^i as an elementary divisor of A. Then, for $0 \le i \le t$,*

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

Remark. When $p = 2$, notice that $d(\vec{s}) = 0$ for any tuple $\vec{s}$ containing an adjacent 1 and 3 (coordinates read circularly). Thus the sum in Theorem 3.2 is significantly easier to compute in this case.

3.2 Examples and Calculations

To illustrate how to use these two theorems, let's consider an example.

Example 3.1. Suppose $q = 9 = 3^2$ (that is, $p = 3$ and $t = 2$). Then we have

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

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

Using Theorem 3.2 we compute

$$\begin{aligned}
e_4 &= d(11) + d(13) + d(31) + d(33)\\
&= d_2 \cdot d_2 + d_8 \cdot d_0 + d_0 \cdot d_8 + d_6 \cdot d_6\\
&= 10 \cdot 10 + 1 \cdot 1 + 1 \cdot 1 + 10 \cdot 10\\
&= 202,
\end{aligned}$$

$$\begin{aligned}
e_5 &= d(21) + d(23) + d(12) + d(32)\\
&= d_1 \cdot d_5 + d_7 \cdot d_3 + d_5 \cdot d_1 + d_3 \cdot d_7\\
&= 4 \cdot 16 + 4 \cdot 16 + 16 \cdot 4 + 16 \cdot 4\\
&= 256,
\end{aligned}$$

$$e_6 = d(22) = d_4 \cdot d_4 = 19 \cdot 19 = 361.$$

The remaining nonzero multiplicities are now given by Theorem 3.1. Observe that our calculation agrees with Table 3-1.

We only need a few of the coefficients of $(1 + x + \cdots + x^{p-1})^4$ when computing $d(\vec{s})$. In fact, it is not difficult to compute the coefficients that we need explicitly. These are listed in Table 3-2. Using these, we can in certain cases write closed–form expressions

for the elementary divisor multiplicities. For example, the case when $q = p$ (that is, $t = 1$) is shown in Table 3-3.

Table 3-1. 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.

Table 3-2. The coefficients d_{λ_i} that arise when calculating $d(\vec{s})$ in Theorem 3.2.

$(\dots, s_i, s_{i+1}, \dots)$	λ_i	d_{λ_i}
$(\dots, 1, 1, \dots)$	$p-1$	$p(p+1)(p+2)/6 = \binom{p+2}{3}$
$(\dots, 1, 2, \dots)$	$2p-1$	$2(p-1)p(p+1)/3 = 4\binom{p+1}{3}$
$(\dots, 2, 1, \dots)$	$p-2$	$(p-1)p(p+1)/6 = \binom{p+1}{3}$
$(\dots, 2, 2, \dots)$	$2p-2$	$p(2p^2+1)/3 = 4\binom{p+1}{3} + p$
$(\dots, 1, 3, \dots)$	$3p-1$	$(p-2)(p-1)p/6 = \binom{p}{3}$
$(\dots, 3, 1, \dots)$	$p-3$	$(p-2)(p-1)p/6 = \binom{p}{3}$
$(\dots, 2, 3, \dots)$	$3p-2$	$(p-1)p(p+1)/6 = \binom{p+1}{3}$
$(\dots, 3, 2, \dots)$	$2p-3$	$2(p-1)p(p+1)/3 = 4\binom{p+1}{3}$
$(\dots, 3, 3, \dots)$	$3p-3$	$p(p+1)(p+2)/6 = \binom{p+2}{3}$

Table 3-3. The Smith normal form of the incidence matrix of skew lines in $\mathrm{PG}(3, p)$.

Elementary Divisor	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

CHAPTER 4
ELEMENTARY DIVISORS

4.1 The Modules M_i and N_j

In this section we collect a few useful results regarding elementary divisors. Throughout this chapter we will be working over a discrete valuation ring R. In other words, R is a principal ideal domain with exactly one nonzero prime ideal. Let $p \in R$ be a prime generating this ideal. This is not such a special situation.

Example 4.1. Let M be an integer matrix, and $p \in \mathbb{Z}$ a prime integer. The ring of integers $\mathbb{Z}$ is not a discrete valuation ring. However, both $\mathbb{Z}_P$ (the localization of $\mathbb{Z}$ at the prime ideal P generated by p) and the p-adic integers $\mathbb{Z}_p$ are discrete valuation rings that contain a copy of $\mathbb{Z}$. Moreover, for $i > 0$ the multiplicity of p^i as an elementary divisor of M is the same whether we view the entries of M as coming from $\mathbb{Z}$, $\mathbb{Z}_P$, or $\mathbb{Z}_p$ (the multiplicity of p^0, i.e. the number of elementary divisors that are units, will in general be different over different rings).

An $m \times n$ matrix with entries in R can be viewed as a homomorphism of free R-modules of finite rank:

$$\eta\colon R^m \to R^n.$$

The elementary divisors of η are by definition just the elementary divisors of the matrix, and for the fixed prime p we always let $e_i(\eta)$ denote the multiplicity of p^i as an elementary divisor of η.

Set $F = R/pR$. If L is an R-submodule of a free R-module R^ℓ, then $\overline{L} = (L + pR^\ell)/pR^\ell$ is an F-vector space. For $i \geq 0$, define

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

and

$$N_i(\eta) = \{p^{-i}\eta(x) \,|\, x \in M_i(\eta)\}.$$

For convenience we also define $N_{-1}(\eta) = \{0\}$. Then we have chains of R-modules

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

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

and chains of F-vector spaces

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

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

Lemma 4.1. *Let $\eta\colon R^m \to R^n$ be a homomorphism of free R-modules of finite rank, and let $e_i(\eta)$ denote the multiplicity of p^i as an elementary divisor of η. Then, for $i \geq 0$,*

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

Proof. The lemma is certainly true if $\eta = 0$, so assume that η is nonzero. Then there is a unique largest nonnegative integer ℓ with $e_\ell(\eta) \neq 0$; in other words, ℓ is the largest exponent occurring among the powers of p in the Smith normal form of η. From the theory of modules over principal ideal domains, there exists a basis $\mathcal{B}$ of R^m and a basis $\mathcal{C}$ of R^n with respect to which the matrix of η is in Smith normal form. By considering this matrix we are lead to a partition of $\mathcal{B}$ and $\mathcal{C}$ as follows. For $0 \leq i \leq \ell$, let $\mathcal{B}_i$ be the elements of $\mathcal{B}$ whose image is exactly divisible by p^i. If we let $\mathcal{B}_{\ell+1}$ denote the elements of $\mathcal{B}$ that are mapped to zero, then we have the disjoint union

$$\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i.$$

For $0 \leq i \leq \ell$, set $\mathcal{C}_i = p^{-i}\eta(\mathcal{B}_i)$ (if $\mathcal{B}_i$ is empty, just set $\mathcal{C}_i$ to be the empty set also). Then we have the disjoint union

$$\mathcal{C} = \bigcup_{i=0}^{\ell+1} \mathcal{C}_i,$$

where $\mathcal{C}_{\ell+1}$ is defined to be $\mathcal{C} \setminus \cup_{i=0}^{\ell} \mathcal{C}_i$. It is easy to see that each of the R-submodules $M_i(\eta)$ (resp. $N_j(\eta)$) have a basis consisting of p-power multiples of elements of $\mathcal{B}$ (resp. $\mathcal{C}$). This is described in Table 4-1 and Table 4-2. When we represent the modules in this way, the lemma becomes clear. □

Table 4-1 and Table 4-2 provide a very useful way to visualize the R-modules $M_i(\eta)$ and $N_j(\eta)$, and really make clear their connection with the Smith normal form of η. The advantages of the module–theoretic approach to the Smith normal form will become increasingly apparent. This next result is very easy, but very useful.

Lemma 4.2. *Let $\gamma\colon R^m \to R^n$ be another R-module homomorphism, and suppose that for some $k \geq 1$ we have*

$$\eta(x) \equiv \gamma(x) \pmod{p^k}, \quad \textit{for all } x \in R^m.$$

Then

$$e_i(\eta) = e_i(\gamma), \quad \textit{for } 0 \leq i \leq k-1.$$

Proof. Verify that $M_i(\eta) = M_i(\gamma)$, for $0 \leq i \leq k$. The conclusion is now immediate from Lemma 4.1. □

4.2 Smith Normal Form 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 diagonal. We define a *left SNF basis* for η to be any basis $\mathcal{B}$ of R^m that belongs to such a pair. Similarly, a *right SNF basis* for η is any basis $\mathcal{C}$ of R^n belonging to such a pair. We now describe how to construct such bases.

Suppose $\eta\colon R^m \to R^n$ is nonzero. Then there is a unique largest nonnegative integer ℓ with $e_\ell(\eta) \neq 0$. We have

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

Table 4-1. Visualizing the R-submodules $M_i(\eta)$.

Submodule			Basis								
$(R^m =)$	M_0	$=\langle$	$\mathcal{B}_0$,	$\mathcal{B}_1$,	$\mathcal{B}_2$,	$\mathcal{B}_3$,	$\cdots$,	$\mathcal{B}_{\ell-1}$,	$\mathcal{B}_\ell$,	$\mathcal{B}_{\ell+1}$	$\rangle$
	M_1	$=\langle$	$p\mathcal{B}_0$,	$\mathcal{B}_1$,	$\mathcal{B}_2$,	$\mathcal{B}_3$,	$\cdots$,	$\mathcal{B}_{\ell-1}$,	$\mathcal{B}_\ell$,	$\mathcal{B}_{\ell+1}$	$\rangle$
	M_2	$=\langle$	$p^2\mathcal{B}_0$,	$p\mathcal{B}_1$,	$\mathcal{B}_2$,	$\mathcal{B}_3$,	$\cdots$,	$\mathcal{B}_{\ell-1}$,	$\mathcal{B}_\ell$,	$\mathcal{B}_{\ell+1}$	$\rangle$
	M_3	$=\langle$	$p^3\mathcal{B}_0$,	$p^2\mathcal{B}_1$,	$p\mathcal{B}_2$,	$\mathcal{B}_3$,	$\cdots$,	$\mathcal{B}_{\ell-1}$,	$\mathcal{B}_\ell$,	$\mathcal{B}_{\ell+1}$	$\rangle$
	$\vdots$										
	$M_{\ell-1}$	$=\langle$	$p^{\ell-1}\mathcal{B}_0$,	$p^{\ell-2}\mathcal{B}_1$,	$p^{\ell-3}\mathcal{B}_2$,	$p^{\ell-4}\mathcal{B}_3$,	$\cdots$,	$\mathcal{B}_{\ell-1}$,	$\mathcal{B}_\ell$,	$\mathcal{B}_{\ell+1}$	$\rangle$
	M_ℓ	$=\langle$	$p^\ell\mathcal{B}_0$,	$p^{\ell-1}\mathcal{B}_1$,	$p^{\ell-2}\mathcal{B}_2$,	$p^{\ell-3}\mathcal{B}_3$,	$\cdots$,	$p\mathcal{B}_{\ell-1}$,	$\mathcal{B}_\ell$,	$\mathcal{B}_{\ell+1}$	$\rangle$
	$M_{\ell+1}$	$=\langle$	$p^{\ell+1}\mathcal{B}_0$,	$p^\ell\mathcal{B}_1$,	$p^{\ell-1}\mathcal{B}_2$,	$p^{\ell-2}\mathcal{B}_3$,	$\cdots$,	$p^2\mathcal{B}_{\ell-1}$,	$p\mathcal{B}_\ell$,	$\mathcal{B}_{\ell+1}$	$\rangle$
	$\vdots$										
	$M_{\ell+k}$	$=\langle$	$p^{\ell+k}\mathcal{B}_0$,	$p^{\ell+k-1}\mathcal{B}_1$,	$p^{\ell+k-2}\mathcal{B}_2$,	$p^{\ell+k-3}\mathcal{B}_3$,	$\cdots$,	$p^{k+1}\mathcal{B}_{\ell-1}$,	$p^k\mathcal{B}_\ell$,	$\mathcal{B}_{\ell+1}$	$\rangle$
	$\vdots$										

Table 4-2. Visualizing the R-submodules $N_j(\eta)$.

Submodule			Basis								
$(\cdots = N_{\ell+1} =)$	N_ℓ	$=$	$\langle$ $\mathcal{C}_0$,	$\mathcal{C}_1$,	$\mathcal{C}_2$,	$\mathcal{C}_3$,	$\cdots$,	$\mathcal{C}_{\ell-1}$,	$\mathcal{C}_\ell$	$\rangle$
	$N_{\ell-1}$	$=$	$\langle$ $\mathcal{C}_0$,	$\mathcal{C}_1$,	$\mathcal{C}_2$,	$\mathcal{C}_3$,	$\cdots$,	$\mathcal{C}_{\ell-1}$,	$p\mathcal{C}_\ell$	$\rangle$
	$N_{\ell-2}$	$=$	$\langle$ $\mathcal{C}_0$,	$\mathcal{C}_1$,	$\mathcal{C}_2$,	$\mathcal{C}_3$,	$\cdots$,	$p\mathcal{C}_{\ell-1}$,	$p^2\mathcal{C}_\ell$	$\rangle$
	$\vdots$									
	N_3	$=$	$\langle$ $\mathcal{C}_0$,	$\mathcal{C}_1$,	$\mathcal{C}_2$,	$\mathcal{C}_3$,	$\cdots$,	$p^{\ell-4}\mathcal{C}_{\ell-1}$,	$p^{\ell-3}\mathcal{C}_\ell$	$\rangle$
	N_2	$=$	$\langle$ $\mathcal{C}_0$,	$\mathcal{C}_1$,	$\mathcal{C}_2$,	$p\mathcal{C}_3$,	$\cdots$,	$p^{\ell-3}\mathcal{C}_{\ell-1}$,	$p^{\ell-2}\mathcal{C}_\ell$	$\rangle$
	N_1	$=$	$\langle$ $\mathcal{C}_0$,	$\mathcal{C}_1$,	$p\mathcal{C}_2$,	$p^2\mathcal{C}_3$,	$\cdots$,	$p^{\ell-2}\mathcal{C}_{\ell-1}$,	$p^{\ell-1}\mathcal{C}_\ell$	$\rangle$
	N_0	$=$	$\langle$ $\mathcal{C}_0$,	$p\mathcal{C}_1$,	$p^2\mathcal{C}_2$,	$p^3\mathcal{C}_3$,	$\cdots$,	$p^{\ell-1}\mathcal{C}_{\ell-1}$,	$p^\ell\mathcal{C}_\ell$	$\rangle$

where only the last inclusion is necessarily strict. Choose a basis $\overline{\mathcal{B}_{\ell+1}}$ of $\overline{\ker(\eta)}$ and extend it to a basis $\overline{\mathcal{B}_\ell} \cup \overline{\mathcal{B}_{\ell+1}}$ of $\overline{M_\ell(\eta)}$. Continue in this fashion to get a basis $\cup_{i=0}^{\ell+1}\overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$. Now lift the elements of $\overline{\mathcal{B}_{\ell+1}}$ to a set $\mathcal{B}_{\ell+1}$ of preimages in $\ker(\eta)$. Continuing, at each stage we enlarge $\mathcal{B}_{i+1}$ by adjoining a set $\mathcal{B}_i$ of preimages in $M_i(\eta)$ of $\overline{\mathcal{B}_i}$. By Nakayama's Lemma, the set

$$\mathcal{B} = \bigcup_{i=0}^{\ell+1} \mathcal{B}_i$$

is an R-basis of R^m.

Notice that $N_\ell(\eta) = N_{\ell+1}(\eta) = \cdots$. Set $N' = N_\ell(\eta)$. Then N' is called the *purification* of $\operatorname{Im}\eta$, and is the smallest R-module direct summand of R^n containing $\operatorname{Im}\eta$. The elementary divisors of η remain the same if we change the codomain of η to N'. Choose a basis $\overline{\mathcal{C}_0}$ of $\overline{N_0(\eta)}$ and extend it to a basis $\overline{\mathcal{C}_0} \cup \overline{\mathcal{C}_1}$ of $\overline{N_1(\eta)}$. Continue in this fashion to get a basis $\cup_{i=0}^{\ell}\overline{\mathcal{C}_i}$ of $\overline{N_\ell(\eta)}$. Now we lift the elements of $\overline{\mathcal{C}_0}$ to a set $\mathcal{C}_0$ of preimages in $N_0(\eta)$. Continuing, at each stage we enlarge $\mathcal{C}_i$ by adjoining a set $\mathcal{C}_{i+1}$ of preimages in $N_{i+1}(\eta)$ of $\overline{\mathcal{C}_{i+1}}$. By Nakayama's Lemma, the set

$$\mathcal{C}' = \bigcup_{i=0}^{\ell} \mathcal{C}_i$$

is an R-basis of N'. We then set

$$\mathcal{C} = \bigcup_{i=0}^{\ell+1} \mathcal{C}_i$$

to be any R-basis of R^n obtained by adjoining to $\mathcal{C}'$ some set $\mathcal{C}_{\ell+1}$.

Lemma 4.3.

1. *The basis $\mathcal{B}$ constructed above is a left SNF basis for η.*
2. *The basis $\mathcal{C}$ constructed above is a right SNF basis for η.*

Proof. For $x \in \mathcal{B}_i$, $0 \leq i \leq \ell$, consider the element $y = p^{-i}\eta(x) \in N'$. The collection of all such elements form a linearly independent set, since the basis $\mathcal{B}$ extends the basis $\mathcal{B}_{\ell+1}$ of $\ker(\eta)$. Let Y denote the R-submodule generated by these elements. From Lemma 4.1 we see that the index of $\operatorname{Im}\eta$ in Y is the same as the index of $\operatorname{Im}\eta$ in N'. Hence $Y = N'$, and so these elements form a basis of N'. The matrix of η with respect to $\mathcal{B}$ and any basis of R^n obtained by extending this basis of N' will then be in diagonal form. This proves part (1).

Now, for each $y \in \mathcal{C}_i$, $0 \leq i \leq \ell$, choose an element $x \in M_i(\eta)$ such that $\eta(x) = p^i y$. Let X denote the R-submodule of R^m generated by these elements. The images of these elements are certainly linearly independent, hence $X \cap \ker(\eta) = \{0\}$. By Lemma 4.1 we see that $\operatorname{Im}\eta$ and $\eta(X + \ker(\eta))$ have the same index in N'. Therefore $R^m = X \oplus \ker(\eta)$, and adjoining any basis of $\ker(\eta)$ to these generators of X gives a basis of R^m. With respect to this basis and $\mathcal{C}$, the matrix of η is in diagonal form. □

CHAPTER 5
PROOFS OF THEOREMS

5.1 Proof of Theorem 3.1

For brevity, an r-dimensional subspace of V will usually just be called an r-subspace in what follows. Since all of the elementary divisors of A are powers of p, we might as well view A as a matrix over the p-adic integers $\mathbb{Z}_p$. None of the elementary divisor multiplicities are affected if we do this, and we may appeal to our results in Chapter 4. A represents a homomorphism of free $\mathbb{Z}_p$-modules

$$\mathbb{Z}_p^{\mathcal{L}_2} \to \mathbb{Z}_p^{\mathcal{L}_2}$$

that sends a 2-subspace to the (formal) sum of the 2-subspaces incident with it. We abuse notation by using the same symbol for both the matrix and the map. We also apply our matrices and maps on the right (so AB means "do A first, then B").

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

$$Y_2 = \Big\{ \sum_{x \in \mathcal{L}_2} a_x x \in \mathbb{Z}_p^{\mathcal{L}_2} \;\Big|\; \sum_{x \in \mathcal{L}_2} a_x = 0 \Big\}.$$

Since $|\mathcal{L}_2|$ is a unit in $\mathbb{Z}_p$, we have the decomposition

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

We now prove Theorem 3.1. The map A respects the above decomposition of $\mathbb{Z}_p^{\mathcal{L}_2}$, and thus we get all of the elementary divisors of A by computing those of the restriction of A to each summand. Since $(\mathbf{1})A = q^4\mathbf{1}$, we see that $e_{4t}(A) = e_{4t}(A|_{Y_2}) + 1$ and $e_i(A) = e_i(A|_{Y_2})$ for $i \neq 4t$.

Rewriting equation (3–1) we get

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

and if we now restrict A to Y_2, the above equation reads

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

Let P and Q be unimodular transformations so that $D = PAQ^{-1}$ acts diagonally on Y_2. Then we get the relation

$$Q(A + (q^2 - q)I)P^{-1} = q^3 D^{-1}, \tag{5–1}$$

which gives the Smith normal form of $A + (q^2 - q)I$ on Y_2. It follows from this equation that $e_i(A|_{Y_2}) = 0$ for $i > 3t$, and so $e_{4t}(A) = 1$, establishing part (1) of the theorem (and most of part (2)).

It also follows immediately from equation (5–1) that

$$e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2}) \tag{5–2}$$

for $0 \le i \le 3t$. Since $A|_{Y_2} \equiv A|_{Y_2} + (q^2 - q)I \pmod{p^t}$, we have from Lemma 4.2 that

$$e_i(A|_{Y_2}) = e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2}) \tag{5–3}$$

for $0 \le i < t$, which is part (3) of the theorem.

It remains to prove parts (4) and (5) of the theorem, and also the statement from part (2) that $e_i(A) = 0$ for $t < i < 2t$. Denote by V_λ the λ-eigenspace for A (as a matrix over $\mathbb{Q}_p$, the p-adic numbers). Then $V_q \cap \mathbb{Z}_p^{\mathcal{L}_2}$ and $V_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}$ are pure $\mathbb{Z}_p$-submodules of Y_2. Notice that $V_q \cap \mathbb{Z}_p^{\mathcal{L}_2} \subseteq N_t(A|_{Y_2})$ and $V_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2} \subseteq M_{2t}(A|_{Y_2})$. Therefore,

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

and

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

Since $(q^4+q^2)+(q^3+q^2+q) = \dim_{\mathbb{F}_p} \overline{Y_2}$, the above inequalities are actually *equalities*, and the remaining elementary divisor multiplicities must be zero. This completes the proof of Theorem 3.1. □

Remark. The above proof simply exploits equation (3–1), and makes no use of the geometry of $\mathrm{PG}(3,q)$. Therefore Theorem 3.1 is also true for the adjacency matrix A of any strongly regular graph with the same parameters.

Theorem 3.2 will follow from a more general result which we prove below. Here we explain the connection between these theorems. Let 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. It is easy to check that

$$B^tB = (q^3+q^2)I + (q^3+q^2-q-1)A + (q^3+q^2-q)(J-A-I). \tag{5–4}$$

Just like with A, we denote also by B and B^t the incidence maps these matrices represent over $\mathbb{Z}_p$. Notice that $(\mathbf{1})B^tB = q^4(q^2+q+1)(q+1)\mathbf{1}$, and so for $i \neq 4t$ we have $e_i(B^tB) = e_i(B^tB|_{Y_2})$. Thus again we concentrate on the summand Y_2.

We can rewrite the equation (5–4) as

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

and upon restriction of maps to Y_2 it reads

$$B^tB = -[A+(q^2-q)I] + q^2I.$$

Applying Lemma 4.2 we have, for $0 \leq i < 2t$,

$$e_i(B^tB|_{Y_2}) = e_i(A|_{Y_2} + (q^2-q)I). \tag{5–5}$$

Using equation (5–2), and considering only nonzero multiplicities, we then get

$$e_{2t+i}(A) = e_{t-i}(B^tB), \quad \text{for } 0 \leq i \leq t. \tag{5–6}$$

Therefore to prove Theorem 3.2 it is sufficient to compute the (p-adic) elementary divisors of the matrix B^tB. The final theorem below describes these. We can actually do this at the level of generality mentioned in the introduction.

5.2 The General Result

For the remainder of the work, V is an $(n+1)$-dimensional vector space over $\mathbb{F}_q$, where $q = p^t$ is a prime power. $A_{r,s}$ is the $|\mathcal{L}_r| \times |\mathcal{L}_s|$ incidence matrix with rows indexed by the r-subspaces of V and columns indexed by the s-subspaces of V, and two subspaces are incident if and only if their intersection is trivial. We will compute the elementary divisors of $A_{r,1}A_{1,s}$ as a matrix over $\mathbb{Z}_p$.

Let $\mathcal{H}$ denote the set of t-tuples of integers $\vec{s} = (s_0, \dots, s_{t-1})$ that satisfy, for $0 \le i \le t-1$,

1. $1 \le s_i \le n$,
2. $0 \le ps_{i+1} - s_i \le (p-1)(n+1)$,

with subscripts read modulo t. First introduced in [6], the set $\mathcal{H}$ was later used in [2] to describe the module structure of $\mathbb{F}_q^{\mathcal{L}_1}$ under the action of $\mathrm{GL}(n+1,q)$. For nonnegative integers α, β, define the subsets of $\mathcal{H}$

$$\mathcal{H}_\alpha(s) = \left\{ (s_0, \dots, s_{t-1}) \in \mathcal{H} \,\middle|\, \sum_{i=0}^{t-1} \max\{0, s - s_i\} = \alpha \right\}$$

and

$$\begin{aligned} {}_\beta\mathcal{H}(r) &= \{(n+1-s_0, \dots, n+1-s_{t-1}) \,|\, (s_0, \dots, s_{t-1}) \in \mathcal{H}_\beta(r)\} \\ &= \left\{ (s_0, \dots, s_{t-1}) \in \mathcal{H} \,\middle|\, \sum_{i=0}^{t-1} \max\{0, s_i - (n+1-r)\} = \beta \right\}. \end{aligned}$$

To each tuple $\vec{s} \in \mathcal{H}$ we associate a number $d(\vec{s})$ as follows. For $\vec{s} = (s_0, \dots, s_{t-1}) \in \mathcal{H}$ define the integer tuple $\vec{\lambda} = (\lambda_0, \dots, \lambda_{t-1})$ by

$$\lambda_i = ps_{i+1} - s_i \quad \text{(subscripts mod } t\text{)}.$$

For an integer k, set d_k to be the coefficient of x^k in the expansion of $(1 + x + \cdots + x^{p-1})^{n+1}$. Explicitly,

$$d_k = \sum_{j=0}^{\lfloor k/p \rfloor} (-1)^j \binom{n+1}{j} \binom{n+k-jp}{n}.$$

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

Theorem 5.1. *Let $e_i(A_{r,1}A_{1,s})$ denote the multiplicity of p^i as a p-adic elementary divisor of $A_{r,1}A_{1,s}$.*

1. $e_{t(r+s)}(A_{r,1}A_{1,s}) = 1$.
2. *For $i \neq t(r+s)$,*

$$e_i(A_{r,1}A_{1,s}) = \sum_{\vec{s} \in \Gamma(i)} d(\vec{s}),$$

where

$$\Gamma(i) = \bigcup_{\substack{\alpha+\beta=i \\ 0 \leq \alpha \leq t(s-1) \\ 0 \leq \beta \leq t(r-1)}} {}_\beta\mathcal{H}(r) \cap \mathcal{H}_\alpha(s).$$

Summation over an empty set is interpreted to result in 0.

It will be technically convenient to actually work over a larger ring than $\mathbb{Z}_p$. Let $K = \mathbb{Q}_p(\xi)$ be the unique unramified extension of degree $t(n+1)$ over $\mathbb{Q}_p$, where ξ is a primitive $(q^{n+1} - 1)^{\text{th}}$ root of unity in K. We set $R = \mathbb{Z}_p[\xi]$ to be the ring of integers in K. Then R is a discrete valuation ring, $p \in R$ generates the maximal ideal, and $F = R/pR \cong \mathbb{F}_{q^{n+1}}$. For the remainder of this work we view all matrix entries as coming from R.

Set $G = \mathrm{GL}(n+1, q)$. Upon fixing a basis of V there is a natural action of G on the sets $\mathcal{L}_i$, and in this way $R^{\mathcal{L}_i}$ becomes an RG-permutation module. As before, $A_{r,s}$ will denote both the matrix and the incidence map

$$R^{\mathcal{L}_r} \to R^{\mathcal{L}_s}$$

that sends an r-subspace to the (formal) sum of s-subspaces incident with it. Since the action of G preserves incidence, the $A_{r,s}$ are RG-module homomorphisms. Clearly the

$M_i(A_{r,s})$ and $N_j(A_{r,s})$ are RG-modules. We have the RG-decompositions

$$R^{\mathcal{L}_k} = R\mathbf{1} \oplus Y_k,$$

where $\mathbf{1} = \sum_{x \in \mathcal{L}_k} x$ and Y_k is the kernel of the splitting map

$$\sum_{x \in \mathcal{L}_k} a_x x \mapsto \Big(\frac{1}{|\mathcal{L}_k|} \sum_{x \in \mathcal{L}_k} a_x\Big)\mathbf{1},$$

and all the $A_{r,s}$ respect these decompositions. Reduction $(\mathrm{mod}\ p)$ induces a homomorphism of FG-permutation modules

$$F^{\mathcal{L}_r} \to F^{\mathcal{L}_s},$$

which we denote by $\overline{A_{r,s}}$.

Let us indicate how we will prove Theorem 5.1. Suppose that we are able to find unimodular matrices P, Q, and E such that

$$PA_{r,1}E^{-1} = D_{r,1}$$

and

$$EA_{1,s}Q^{-1} = D_{1,s}$$

where the matrices on the right are diagonal. Then these diagonal entries are the elementary divisors of the respective matrices $A_{r,1}$ and $A_{1,s}$. Since then

$$PA_{r,1}A_{1,s}Q^{-1} = D_{r,1}D_{1,s},$$

we will then have obtained the elementary divisors of the product matrix (provided that we have detailed enough knowledge of the elementary divisors of the factor matrices).

Example 5.1. Consider the matrix product

$$\begin{pmatrix} p & 1 \\ 0 & -p \end{pmatrix} \begin{pmatrix} 1 & p \\ 0 & -p^2 \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & p^3 \end{pmatrix}.$$

This product matrix is already in Smith normal form. Note that both of the factor matrices are equivalent to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p^2 \end{smallmatrix}\right)$. Even allowing permutation of the diagonal entries, it is not possible for two such diagonal matrices to multiply to $\left(\begin{smallmatrix} p & 0 \\ 0 & p^3 \end{smallmatrix}\right)$.

In general it is not possible to find such a matrix E, as the above example shows. Thus when trying to find the elementary divisors of a matrix product, knowledge of the elementary divisors of the factor matrices is in general not sufficient (for more information on this interesting topic, see [11] and [14]). Therefore we should not expect such an intermediate matrix E to exist in our situation. Yet it does! To see what is so special here, pass from matrices back to modules. The key ingredient is the structure of $R^{\mathcal{L}_1}$ as an RG-module, as the matrix E arises from choosing a basis of $R^{\mathcal{L}_1}$ that is "compatible" with both factor maps. We already have the correct terminology for this.

Lemma 5.1. *There exists a basis $\mathscr{B}$ of $R^{\mathcal{L}_1}$ that is simultaneously a left SNF basis for $A_{1,s}$ and a right SNF basis for $A_{r,1}$.*

Proof. The group G has a cyclic subgroup S which is isomorphic to $F^\times$. Since R contains a primitive $|S|^{\text{th}}$ root of unity, it follows that K is a splitting field for S and that the irreducible K-characters of S take their values in R. Let $\overline{S}$ denote the quotient of S by the subgroup of scalar matrices. Then $\overline{S}$ acts regularly on $\mathcal{L}_1$, and $|\overline{S}| = |\mathcal{L}_1|$ is a unit in R. Therefore, for each character χ of $\overline{S}$, the group ring $R\overline{S}$ contains an idempotent element h_χ that projects onto the (rank one) χ-isotypic component of $R^{\mathcal{L}_1}$. We thus obtain an R-basis $\mathscr{B} = \{v_\chi \,|\, \chi \in \mathrm{Hom}(\overline{S}, R^\times)\}$ of $R^{\mathcal{L}_1}$, where $v_\chi \in h_\chi \cdot R^{\mathcal{L}_1}$ such that $p \nmid v_\chi$.

Now let us construct a left SNF basis for $A_{1,s}$, in the manner and notation described in Section 4.2. Since each $F\overline{S}$-submodule of $F^{\mathcal{L}_1}$ is a direct sum of the isotypic components that it contains, we see that we can take each of the sets $\overline{\mathcal{B}_i}$ to be a subset of $\overline{\mathscr{B}}$. Suppose we lift $\overline{v_\chi} \in \overline{\mathcal{B}_i}$ to an element $f \in M_i(A_{1,s})$. Writing

$$f = \sum_{\theta \in \mathrm{Hom}(\overline{S}, R^\times)} c_\theta v_\theta,$$

we see that $\overline{f} = \overline{c_\chi v_\chi}$ and so c_χ must be a unit in R. Since $M_i(A_{1,s})$ is an $R\overline{S}$-submodule, we have that $h_\chi \cdot f = c_\chi v_\chi$ is also in $M_i(A_{1,s})$. This proves that we may choose to lift $\overline{v_\chi}$ to v_χ in the construction, and that $\mathscr{B}$ is a left SNF basis for $A_{1,s}$.

An identical argument (lifting each $\overline{v_\chi}$ into some $N_j(A_{r,1})$) shows that $\mathscr{B}$ is a right SNF basis for $A_{r,1}$. □

It remains to show that the elementary divisor multiplicities are as stated in the theorem. First we need a more precise description of the FG-submodule lattice of $F^{\mathcal{L}_1}$. The facts that we need are as follows (see [2, Theorem A]). $F^{\mathcal{L}_1} = F\mathbf{1} \oplus \overline{Y_1}$ is a multiplicity–free FG-module, and the FG-composition factors of $\overline{Y_1}$ are in bijection with the set $\mathcal{H}$. The dimension over F of the composition factor corresponding to the tuple $\vec{s}$ is $d(\vec{s})$. Moreover, if we give $\mathcal{H}$ the partial order

$$(s_0, \ldots, s_{t-1}) \leq (s'_0, \ldots, s'_{t-1}) \iff s_i \leq s'_i \text{ for all i}$$

then the FG-submodule lattice of $\overline{Y_1}$ is isomorphic to the lattice of order ideals of $\mathcal{H}$, and the tuples contained in an order ideal correspond to the composition factors of the respective submodule. Thus it is clear what is meant by the statement that a subquotient of $\overline{Y_1}$ *determines* a subset of $\mathcal{H}$.

Remarks.

1. The field k in [2] is actually an algebraic closure of $\mathbb{F}_q$, but (as observed in [4]) it follows from [2, Theorem A] that all kG-submodules of $k^{\mathcal{L}_1}$ are simply scalar extensions of $\mathbb{F}_q G$-modules, and therefore [2, Theorem A] is also true over our field $F \cong \mathbb{F}_{q^{n+1}}$. This observation also permits us to make use of certain results from [4], where the field is $\mathbb{F}_q$.

2. The detailed information that we need about the elementary divisors of $A_{r,1}$ and $A_{1,s}$ we obtain from [4]. It should also be noted that the incidence relation considered in [2, 4, 13] is *nonzero* intersection (i.e., the complementary relation where two subspaces are incident if and only if their intersection is nontrivial). If $A'_{r,s}$ is the corresponding incidence matrix for nonzero intersection, then we have

$$A_{r,s} = J - A'_{r,s}.$$

In particular,

$$A_{r,s}|_{Y_r} = -A'_{r,s}|_{Y_r}.$$

Therefore the (p-adic) Smith normal forms of $A_{r,s}$ and $A'_{r,s}$ can differ only with respect to where they map $\mathbf{1}$. This accounts for the extra term appearing in the calculation of p-ranks in [2, 4, 13].

Lemma 5.2.

1. *The FG-module $\overline{M_\alpha(A_{1,s}|_{Y_1})}/\overline{M_{\alpha+1}(A_{1,s}|_{Y_1})}$ determines the subset $\mathcal{H}_\alpha(s)$.*
2. *The FG-module $\overline{N_\beta(A_{r,1}|_{Y_r})}/\overline{N_{\beta-1}(A_{r,1}|_{Y_r})}$ determines the subset ${}_\beta\mathcal{H}(r)$.*

Proof. Part (1) is the content of [4, Theorem 3.3] (see Remarks above). In order to prove (2), first observe that for each k, $\mathcal{L}_k$ is an orthonormal basis for a nondegenerate G-invariant symmetric bilinear form $\langle\cdot\,,\cdot\rangle_k$ on $R^{\mathcal{L}_k}$. Use the induced form on $F^{\mathcal{L}_k}$ to identify each permutation module with its dual (contragredient) module, and observe that $\overline{A_{s,r}}$ is the dual map induced by $\overline{A_{r,s}}$. Since the tuples $(s_0, \dots, s_{t-1})$ and $(n+1-s_0, \dots, n+1-s_{t-1})$ are determined by dual composition factors [2, Lemma 2.5(c)], part (2) will follow immediately if we can show the FG-module isomorphism

$$\left(\overline{N_\beta(A_{r,s}|_{Y_r})}/\overline{N_{\beta-1}(A_{r,s}|_{Y_r})}\right)^* \cong \overline{M_\beta(A_{s,r}|_{Y_s})}/\overline{M_{\beta+1}(A_{s,r}|_{Y_s})}.$$

It is sufficient to show that

$$\overline{N_\beta(A_{r,s}|_{Y_r})}^\perp = \overline{M_{\beta+1}(A_{s,r}|_{Y_s})}.$$

We proceed by induction on β. When $\beta = 0$, we have

$$\begin{aligned}
\overline{N_0(A_{r,s}|_{Y_r})}^\perp &= \{\overline{y} \mid y \in Y_s,\ \langle (x)A_{r,s}, y\rangle_s \equiv 0 \pmod p \text{ for all } x \in Y_r\} \\
&= \{\overline{y} \mid y \in Y_s,\ \langle x, (y)A_{s,r}\rangle_r \equiv 0 \pmod p \text{ for all } x \in Y_r\} \\
&= \overline{M_1(A_{s,r}|_{Y_s})}.
\end{aligned}$$

where the last equality follows from the nondegeneracy of the induced form on $\overline{Y_r}$. Now assume $\beta > 0$. It is easy to check that $\overline{M_{\beta+1}(A_{s,r}|_{Y_s})} \subseteq \overline{N_\beta(A_{r,s}|_{Y_r})}^\perp$. We then have

$$\overline{M_{\beta+1}(A_{s,r}|_{Y_s})} \subseteq \overline{N_\beta(A_{r,s}|_{Y_r})}^\perp \subseteq \overline{N_{\beta-1}(A_{r,s}|_{Y_r})}^\perp = \overline{M_\beta(A_{s,r}|_{Y_s})},$$

with the equality by our induction hypothesis. Since clearly $e_\beta(A_{s,r}|_{Y_s}) = e_\beta(A_{r,s}|_{Y_r})$, it now follows from Lemma 4.1 and the above inclusions that $\overline{M_{\beta+1}(A_{s,r}|_{Y_s})} = \overline{N_\beta(A_{r,s}|_{Y_r})}^\perp$.

□

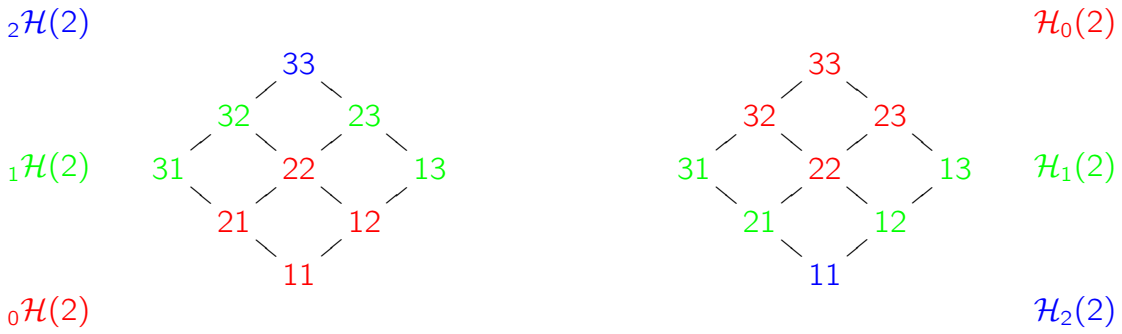

Figure 5-1. Illustrating Lemma 5.2 when $n = 3$ and $r = s = t = 2$.

Proof of Theorem 5.1. Fix an FG-composition series

$$\{0\} \subseteq F\mathbf{1} = U_0 \subseteq U_1 \subseteq \cdots \subseteq F^{\mathcal{L}_1}.$$

Starting with the F-basis $\{\overline{v_{1_{\overline{S}}}}\}$ of U_0, we can extend this using elements of $\overline{\mathscr{B}}$ to a basis of U_1. Continuing in this fashion, we thus get the disjoint union

$$\mathscr{B} = \{v_{1_{\overline{S}}}\} \cup \mathcal{D}_1 \cup \cdots$$

where $\overline{\mathcal{D}_i}$ are the elements of $\overline{\mathscr{B}}$ extending U_{i-1} to U_i. It is clear that each quotient U_i/U_{i-1} ($i \geq 1$) is isomorphic as an $F\overline{S}$-module to the $F\overline{S}$-submodule of $\overline{Y_1}$ spanned by $\overline{\mathcal{D}_i}$. If the simple FG-module U_i/U_{i-1} determines the tuple $\vec{s} \in \mathcal{H}$, then we say will say that each element of $\mathcal{D}_i$ *determines* the tuple $\vec{s}$. This assignment of elements of $\mathscr{B}$ to tuples in $\mathcal{H}$ is well–defined independent of the above composition series, as follows from

the fact that the isomorphism type of an $F\overline{S}$-submodule of $\overline{Y_1}$ is completely determined by the characters it affords.

By Lemma 5.2, the tuple determined by v_χ belongs to $\mathcal{H}_\alpha(s) \cap {}_\beta\mathcal{H}(r)$ precisely when the following two conditions hold:

1. $\overline{v_\chi} \in \overline{M_\alpha(A_{1,s}|_{Y_1})}$ but $\overline{v_\chi} \notin \overline{M_{\alpha+1}(A_{1,s}|_{Y_1})}$,
2. $\overline{v_\chi} \in \overline{N_\beta(A_{r,1}|_{Y_r})}$ but $\overline{v_\chi} \notin \overline{N_{\beta-1}(A_{r,1}|_{Y_r})}$.

It immediately follows that

$$e_i(A_{r,1}A_{1,s}|_{Y_r}) = \sum_{\alpha+\beta=i} \sum_{\vec{s}\in\mathcal{H}_\alpha(s)\cap{}_\beta\mathcal{H}(r)} d(\vec{s}), \quad \text{for } i \geq 0.$$

Since $\mathcal{H}_\alpha(s) = \emptyset$ for $\alpha > t(s-1)$ and ${}_\beta\mathcal{H}(r) = \emptyset$ for $\beta > t(r-1)$, we have

$$e_i(A_{r,1}A_{1,s}|_{Y_r}) = 0, \quad \text{for } i > t(r+s-2).$$

We will use the q-binomial coefficients

$$\begin{bmatrix} m \\ \ell \end{bmatrix}_q = \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-\ell+1}-1)}{(q-1)(q^2-1)\cdots(q^\ell-1)}$$

for non-negative integers m and ℓ with $m \geq \ell$. Then

$$(\mathbf{1})A_{r,1}A_{1,s} = q^{r+s}\begin{bmatrix} n \\ r \end{bmatrix}_q \begin{bmatrix} n+1-s \\ 1 \end{bmatrix}_q \mathbf{1},$$

and we have $e_{t(r+s)}(A_{r,1}A_{1,s}) = 1$, completing the proof of Theorem 5.1. □

Remark. Since $d(\vec{s}) = 0$ for $\vec{s} \in [n]^t \setminus \mathcal{H}$, there is no effect on the numerical result of Theorem 5.1 if we replace $\mathcal{H}$ with $[n]^t$ in the notation preceding the statement of the theorem.

Proof of Theorem 3.2. We recover our original situation by setting $n = 3$ and $r = s = 2$ (so $A_{2,2} = A$ and $A_{1,2} = B$). Replace $\mathcal{H}$ with $[3]^t$ in the notation preceding Theorem 5.1.

Then it is easy to see that

$$\mathcal{H}_\alpha(2) = \{\vec{s} \in [3]^t \mid \vec{s} \text{ contains exactly } \alpha \text{ ones}\}$$

and

$$_\beta\mathcal{H}(2) = \{\vec{s} \in [3]^t \mid \vec{s} \text{ contains exactly } \beta \text{ threes}\}.$$

Hence

$$\begin{aligned}\Gamma(i) &= \bigcup_{\alpha+\beta=i} \left(\mathcal{H}_\alpha(2) \cap {}_\beta\mathcal{H}(2)\right) \\ &= \{\vec{s} \in [3]^t \mid \vec{s} \text{ contains exactly } t-i \text{ twos}\} \\ &= \mathcal{H}(t-i).\end{aligned}$$

Therefore, for $0 \le i \le t$,

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

and in view of equation (5–6) we see that Theorem 3.2 follows from Theorem 5.1. □

As mentioned in the introduction, the problem of computing the integer invariants of $A_{r,s}$ in general is still very much unsolved. The p-ranks of the incidence matrices $A_{r,s}$ were computed in [13], and observe that the p-rank of an integer matrix is just the multiplicity of p^0 as a p-adic elementary divisor. We conclude with the following easy corollary of Theorem 5.1.

Corollary 5.2. *Notation is that of Theorem 5.1. Let $e_i(A_{r,s})$ denote the multiplicity of p^i as a p-adic elementary divisor of $A_{r,s}$. Then, for $0 \le i < t$,*

$$e_i(A_{r,s}) = \sum_{\vec{s}\in\Gamma(i)} d(\vec{s}).$$

Proof. Let $x \in \mathcal{L}_r$. Then

$$(x)A_{r,s} = \sum_{y\in\mathcal{L}_s} a_{x,y}y,$$

where

$$a_{x,y} = |\{z \in \mathcal{L}_1 \,|\, z \cap x = \{0\} \text{ and } z \cap y = \{0\}\}|$$
$$= \begin{cases} \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} r \\ 1 \end{bmatrix}_q - \begin{bmatrix} s \\ 1 \end{bmatrix}_q, & \text{if } x \cap y \neq \{0\} \\ \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} r \\ 1 \end{bmatrix}_q - \begin{bmatrix} s \\ 1 \end{bmatrix}_q + \begin{bmatrix} k \\ 1 \end{bmatrix}_q, & \text{if } \dim(x \cap y) = k \geq 1. \end{cases}$$

Then $a_{x,y} \equiv -1 \pmod{q}$ when $x \cap y = \{0\}$ and q divides $a_{x,y}$ otherwise. Hence

$$A_{r,1}A_{1,s} \equiv -A_{r,s} \pmod{p^t}$$

and the corollary now follows from Lemma 4.2. □

APPENDIX: SAMPLE SAGE PROGRAM

```
x = walltime()

p = 2

t = 2

q = p^t

F.<a> = GF(q)

V = VectorSpace(F, 4)

S = tuple(V.subspaces(2))

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-4dim/incmat2^2')
```

REFERENCES

[1] E. F. Assmus, Jr. and J. D. Key. *Designs and their codes*, volume 103 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1992.

[2] 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(1):58–80, 2000.

[3] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 1989.

[4] 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(11):4935–4957 (electronic), 2006.

[5] J.W.L. Glaisher. Henry John Stephen Smith. *MNRAS*, 44(6):138–149, 1884.

[6] 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.*, 3:153–226, 1973.

[7] J. W. P. Hirschfeld. *Finite projective spaces of three dimensions*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1985. Oxford Science Publications.

[8] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[9] Eric S. Lander. *Symmetric Designs: An Algebraic Approach*. Cambridge University Press, 1983. London Math. Soc. Lecture Notes 74.

[10] Morris Newman. *Integral matrices*. Academic Press, New York, 1972. Pure and Applied Mathematics, Vol. 45.

[11] Joseph John Rushanan. *Topics in integral matrices and abelian group codes*. ProQuest LLC, Ann Arbor, MI, 1986. Thesis (Ph.D.)–California Institute of Technology.

[12] Peter Sin. The elementary divisors of the incidence matrices of points and linear subspaces in $\mathbf{P}^n(\mathbf{F}_p)$. *J. Algebra*, 232(1):76–85, 2000.

[13] Peter Sin. The p-rank of the incidence matrix of intersecting linear subspaces. *Des. Codes Cryptogr.*, 31(3):213–220, 2004.

[14] Kyle D. Wallace. Extension of mappings in finite abelian groups. *Amer. Math. Monthly*, 79:622–624, 1972.

[15] Richard M. Wilson. A diagonal form for the incidence matrices of t-subsets vs. k-subsets. *European J. Combin.*, 11(6):609–615, 1990.

[16] Qing Xiang. Recent progress in algebraic design theory. *Finite Fields Appl.*, 11(3):622–653, 2005.

[17] Qing Xiang. Recent results on p-ranks and Smith normal forms of some 2-(v, k, λ) designs. In *Coding theory and quantum computing*, volume 381 of *Contemp. Math.*, pages 53–67. Amer. Math. Soc., Providence, RI, 2005.

BIOGRAPHICAL SKETCH

Joshua Evans Ducey was born in 1983 in Honolulu, Hawaii. He grew up in Hanover, Maryland, just a few miles from the National Security Agency. After graduating from Meade Senior High School in 2001, Josh attended college in Virginia at the University of Richmond. There, he studied mathematics and philosophy, earning his bachelor's degree in the former in 2005. It was in the middle of his senior year at Richmond that he decided that he wanted to be a mathematician. After building boat docks for a summer in St. Petersburg, Florida, Josh enrolled in graduate school at the University of Florida. It was here that he met his fiancée, Minah Oh. In 2011, Josh earned his doctorate in mathematics under the guidance of Dr. Peter Sin.