PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 8, August 2012, Pages 2561–2573
S 0002-9939(2011)11462-X
Article electronically published on December 21, 2011

THE ELEMENTARY DIVISORS OF THE INCIDENCE MATRIX OF SKEW LINES IN PG$(3, q)$

ANDRIES E. BROUWER, JOSHUA E. DUCEY, AND PETER SIN

(Communicated by Pham Huu Tiep)

Abstract. The elementary divisors of the incidence matrix of lines in PG$(3, q)$ are computed, where two lines are incident if and only if they are skew.

1. Introduction

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. By the well-known Klein correspondence, A is also the adjacency matrix of the noncollinearity graph on the points of the Klein quadric. The entries of this zero-one matrix may be read over any commutative ring. In this paper we compute the Smith normal form of A as an integer matrix.

In order to introduce some useful notation, we will view this setup as a special case of a more general situation. For brevity, an r-dimensional subspace will be called an r-subspace in what follows.

More generally, let V be an $(n+1)$-dimensional vector space over the finite field $\mathbb{F}_q$, where $q = p^t$ is a prime power. Let $\mathcal{L}_r$ denote the set of r-subspaces of V. Thus $\mathcal{L}_1$ denotes the points, $\mathcal{L}_2$ denotes the lines, etc. in $\mathbb{P}(V)$. An r-subspace $U \in \mathcal{L}_r$ and an s-subspace $W \in \mathcal{L}_s$ are incident if and only if $U \cap W = \{0\}$. The incidence matrix with rows indexed by the r-subspaces and columns indexed by the s-subspaces is denoted $A_{r,s}$.

These matrices $A_{r,s}$ and other closely related ones have been studied by a number of mathematicians. The reader is referred to the surveys [9, 8] (see also [2, Introduction]). Their p-ranks are determined in [7], but their elementary divisors have been computed only in the case that either r or s is equal to one [4, 6, 2].

We return now to the situation where V is 4-dimensional over $\mathbb{F}_q$ and $A = A_{2,2}$.

2. The main results

It turns out that the elementary divisors of A are all powers of 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, with parameters $v = q^4 + q^3 + 2q^2 + q + 1$, $k = q^4$, $\lambda = q^4 - q^3 - q^2 + q$, $\mu = q^4 - q^3$.

Received by the editors February 28, 2011.
2010 *Mathematics Subject Classification.* Primary 05B20; Secondary 20C33, 51E20.

Thus A satisfies the equation

$$A^2 = q^4 I + (q^4 - q^3 - q^2 + q)A + (q^4 - q^3)(J - A - I), \tag{2.1}$$

where I and J denote the identity matrix and the matrix of all ones, 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 $|\det(A)|$ is the product of the elementary divisors, we see that the elementary divisors of A are all powers of p.

The following two theorems give the Smith normal form of A.

Theorem 2.1. *Let $e_i = e_i(A)$ denote the multiplicity of p^i as an elementary divisor of A.*

(1) $e_i = e_{3t-i}$ *for* $0 \le i < t$.
(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 $e_0, \dots, e_t$ (or the numbers $e_{2t}, \dots, e_{3t}$). The next theorem describes these. 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

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

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

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

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 2.2. *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. Also, $d(\vec{s}) = 0$ for tuples $\vec{s}$ beginning with a 1 and ending with a 3 (and vice versa). Thus the sum in Theorem 2.2 is significantly easier to compute in this case.

As an example of how to use the above theorems, consider the case when $p = 3$, $t = 2$. 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 2.2 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 2.1. We collect this information in Table 2.1.

TABLE 2.1. The elementary divisors of the incidence matrix of lines vs. lines in 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

3. Elementary divisors and Smith normal form bases

In this section we collect a few useful results regarding elementary divisors. Let R be a discrete valuation ring, with $p \in R$ a prime generating the maximal ideal. 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 a 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 $\overline{L} = (L + pR^l)/pR^l$ is an F-vector space. For $i \geq 0$, define

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

and

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

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

$$\begin{gathered} R^m = M_0(\eta) \supseteq M_1(\eta) \supseteq \cdots, \\ N_0(\eta) \subseteq N_1(\eta) \subseteq \cdots \end{gathered}$$

and chains of F-vector spaces

$$\begin{gathered} F^m = \overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots, \\ \overline{N_0(\eta)} \subseteq \overline{N_1(\eta)} \subseteq \cdots. \end{gathered}$$

Lemma 3.1. *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. 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. Each of the above R-submodules $M_i(\eta)$ (resp. $N_j(\eta)$) are seen to have a basis consisting of p-power multiples of elements of $\mathcal{B}$ (resp. $\mathcal{C}$). When we represent the modules in this way, the lemma is clear. □

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 diagonal 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.

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

$$\overline{M_0(\eta)} \supseteq \overline{M_1(\eta)} \supseteq \cdots \supseteq \overline{M_l(\eta)} \supsetneq \overline{\ker(\eta)},$$

where only the last inclusion is necessarily strict. Choose a basis $\overline{\mathcal{B}_{l+1}}$ of $\overline{\ker(\eta)}$ and extend it to a basis $\overline{\mathcal{B}_l} \cup \overline{\mathcal{B}_{l+1}}$ of $\overline{M_l(\eta)}$. Continue in this fashion to get a basis $\bigcup_{i=0}^{l+1} \overline{\mathcal{B}_i}$ of $\overline{M_0(\eta)}$. Now lift the elements of $\overline{\mathcal{B}_{l+1}}$ to a set $\mathcal{B}_{l+1}$ 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

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

is an R-basis of R^m.

Notice that $N_l(\eta) = N_{l+1}(\eta) = \cdots$. Set $N' = N_l(\eta)$. 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 $\bigcup_{i=0}^{l} \overline{\mathcal{C}_i}$ of $\overline{N_l(\eta)}$. 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

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

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

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

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

Lemma 3.2.

(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 $x \in \mathcal{B}_i$, $0 \le i \le l$, consider the element $y = p^{-i}\eta(x) \in N'$. The collection of all such elements forms a linearly independent set, since the basis $\mathcal{B}$ extends the basis $\mathcal{B}_{l+1}$ of $\ker(\eta)$. Let Y denote the R-submodule generated by these elements. From Lemma 3.1 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 $y \in \mathcal{C}_i$, $0 \le i \le l$, 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 3.1 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. □

We end this section with an easy but very useful result.

Lemma 3.3. *Let $\gamma\colon R^m \to R^n$ be another R-module homomorphism, and suppose that for some $k \ge 1$ we have*

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

Then

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

Proof. Verify that $M_i(\eta) = M_i(\gamma)$, for $0 \le i \le k$. The conclusion is now immediate from Lemma 3.1. □

4. Proof of Theorem 2.1

Since all of the elementary divisors of A are powers of p, we lose nothing by viewing A as a matrix over $\mathbb{Z}_p$, the ring of p-adic integers. The matrix 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 2.1. 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 (2.1) 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

$$A|_{Y_2}(A|_{Y_2} + (q^2 - q)I) = q^3 I. \tag{4.1}$$

Looking carefully at this equation one sees that a left (resp. right) SNF basis for $A|_{Y_2}$ is a right (resp. left) SNF basis for $A|_{Y_2} + (q^2 - q)I$. It follows from equation (4.1) that $e_i(A|_{Y_2}) = 0$ for $i > 3t$, and so $e_{4t}(A) = 1$. Thus we have established part (5) of the theorem (and most of part (2)).

It also follows immediately from equation (4.1) that

$$e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2}) \tag{4.2}$$

for $0 \leq i \leq 3t$. Since $A|_{Y_2} \equiv A|_{Y_2} + (q^2 - q)I \pmod{p^t}$, we have from Lemma 3.3 that

$$e_i(A|_{Y_2}) = e_i(A|_{Y_2} + (q^2 - q)I) = e_{3t-i}(A|_{Y_2}) \tag{4.3}$$

for $0 \leq i < t$, which is part (1) of the theorem.

It remains to prove parts (3) and (4) 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). Since V_q is a $\mathbb{Q}_p$-subspace of ${\mathbb{Q}_p}^{\mathcal{L}_2}$, the intersection $V_q \cap \mathbb{Z}_p^{\mathcal{L}_2}$ is a pure sublattice of $\mathbb{Z}_p^{\mathcal{L}_2}$ and the same is true for $V_{-q^2} \cap \mathbb{Z}_p^{\mathcal{L}_2}$. 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,

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

and

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

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 2.1. □

Remark. The above proof simply exploits equation (2.1) and makes no use of the geometry of $\mathrm{PG}(3, q)$. Therefore Theorem 2.1 is also true for the adjacency matrix A of any strongly regular graph with the same parameters.

Theorem 2.2 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

$$B^t B = (q^3 + q^2)I + (q^3 + q^2 - q - 1)A + (q^3 + q^2 - q)(J - A - I). \tag{4.4}$$

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

We can rewrite equation (4.4) 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

$$B^tB|_{Y_2} = -[A|_{Y_2} + (q^2 - q)I] + q^2I.$$

Applying Lemma 3.3 we have, for $0 \le i < 2t$,

$$e_i(B^tB|_{Y_2}) = e_i(A|_{Y_2} + (q^2 - q)I). \tag{4.5}$$

Using equation (4.2), and considering only nonzero multiplicities, we then get the relations

$$e_{2t+i}(A) = e_{t-i}(B^tB), \quad \text{for } 0 \le i \le t. \tag{4.6}$$

Therefore to prove Theorem 2.2 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. The general result

For the remainder of the paper, 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 [3], the set $\mathcal{H}$ was later used in [1] 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 following 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

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

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

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

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

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

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

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 actually to 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 $F = R/pR \cong \mathbb{F}_{q^{n+1}}$.

Set $G = \mathrm{GL}(n+1, q)$. If one fixes a basis of V, then 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-submodules. We again have the RG-decomposition

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

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 this decomposition. Reduction modulo 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 have obtained the elementary divisors of the product matrix (provided that we have enough knowledge of the elementary divisors of the factor matrices).

In general it 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. The information that we need about the elementary divisors of $A_{r,1}$ and $A_{1,s}$ we obtain from [2].

Lemma 5.2. *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 transformations. 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 $\mathscr{B} = \{v_\chi \mid \chi \in \mathrm{Hom}(\overline{S}, R^\times)\}$ 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 following the proof of Lemma 3.1. 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 [1, 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 [1] is actually an algebraic closure of $\mathbb{F}_q$, but (as observed in [2]) it follows from [1, Theorem A] that all kG-submodules of $k^{\mathcal{L}_1}$ are simply scalar extensions of $\mathbb{F}_qG$-modules, and therefore [1, 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 [2], where the field is $\mathbb{F}_q$.

(2) It should also be noted that the incidence relation considered in [1, 7, 2] 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 [1, 7, 2].

Lemma 5.3.

(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 [2, 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 [1, 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

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

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 3.1 and the above inclusions that $\overline{M_{\beta+1}(A_{s,r}|_{Y_s})} = \overline{N_\beta(A_{r,s}|_{Y_r})}^\perp$. □

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 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 5.3, 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 nonnegative integers m and ℓ with $m \geq \ell$. Then

$$(\mathbf{1})A_{r,1}A_{1,s} = q^{r+s}\left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_q \left[\begin{smallmatrix} n+1-s \\ 1 \end{smallmatrix}\right]_q \mathbf{1},$$

and we have $e_{t(r+s)}(A_{r,1}A_{1,s}) = 1$. This completes 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 2.2. Consider the situation when $n+1 = 4$ 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

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

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

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

and in view of equation (4.6) we see that Theorem 2.2 follows from Theorem 5.1. □

As mentioned in the introduction, the problem of computing the elementary divisors of $A_{r,s}$ in general is still very much unsolved. The p-ranks of the incidence matrices $A_{r,s}$ were computed in [7]. Observe that the p-rank of an integer matrix is just the multiplicity of p^0 as a p-adic elementary divisor. We end the paper with the following easy corollary of Theorem 5.1.

Corollary 5.4. *The 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

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

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 3.3. □

Acknowledgements

The second author received generous support through the Chat Yin Ho Memorial Scholarship, for which he wishes to thank the family and friends of Professor Ho. The authors also thank the Banff International Research Station, where discussion of this work began at a workshop in March 2009.

References

1. 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. MR1745400 (2001f:20103)
2. 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). MR2231879 (2007c:05041)
3. 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. MR0332515 (48:10842)
4. Eric S. Lander, *Symmetric designs: An algebraic approach*, London Math. Soc. Lecture Notes 74. Cambridge University Press, 1983. MR697566 (85d:05041)
5. Joseph John Rushanan, *Topics in integral matrices and abelian group codes*, Thesis (Ph.D.)–California Institute of Technology, 1986, ProQuest LLC, Ann Arbor, MI. MR2635072
6. 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. MR1783914 (2001g:20060)
7. ———, *The p-rank of the incidence matrix of intersecting linear subspaces*, Des. Codes Cryptogr. **31** (2004), no. 3, 213–220. MR2047880 (2004m:05050)

8. Qing Xiang, *Recent progress in algebraic design theory*, Finite Fields Appl. **11** (2005), no. 3, 622–653. MR2158779 (2006j:05001)
9. ———, *Recent results on p-ranks and Smith normal forms of some* 2-(v, k, λ) *designs*, Coding theory and quantum computing, Contemp. Math., vol. 381, Amer. Math. Soc., Providence, RI, 2005, pp. 53–67. MR2170799 (2006h:05035)

Department of Mathematics, Technische Universiteit Eindhoven, 5600MB Eindhoven, The Netherlands
E-mail address: aeb@cwi.nl

Department of Mathematics, University of Florida, Gainesville, Florida 32611–8105
E-mail address: jducey21@ufl.edu
Current address: Department of Mathematics and Statistics, James Madison University, Harrisonburg, Virginia 22807
E-mail address: duceyje@jmu.edu

Department of Mathematics, University of Florida, Gainesville, Florida 32611–8105
E-mail address: sin@ufl.edu