Advanced Studies in Pure Mathematics 24, 1996
Progress in Algebraic Combinatorics
pp. 265–283

Incidence Matrix Diagonal Forms and Integral Hecke Algebras

Robert A. Liebler

§1. Introduction

Let $\mathcal{P}_k$ denote the set of flats in the projective geometry $PG_{n-1}(q)$ arising from the k-dimensional subspaces of an n-dimensional vector space over the Galois field $GF(q)$, q a power of the prime p. Let $\mathcal{M}_k(q)$ be incidence matrix of points $\mathcal{P}_1$ versus k-flats $\mathcal{P}_k$.

The study of $\mathbb{Z}$-span of the columns of $\mathcal{M}_k(q)$ as a submodule of $\mathbb{Z}\mathcal{P}_1$ is of interest in its own right, as a source of easily implemented codes and because it may provide a means for representing, and ultimately characterizing, associated combinatorial structures like the q-analog Johnson schemes. I also find this study particularly attractive because it provides an explicit setting to further develop the application of integral representation theory and number theory to combinatorics along the lines that have been so successful with non-abelian difference sets.

It is easy to see that the Smith normal form of $\mathcal{M}_k(q)$ has all but one of its diagonal entries a divisor of the difference : $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q - \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_q$ of the q-binomial coefficients. Even for $n = 3$, every conceivable p-elementary divisor arises. Indeed, the set of lines of an affine net of degree p^k is in the kernel of the incidence map mod p^k but not mod p^{k+1}.

The first formulas for the p-rank of $\mathcal{M}_k(q)$ are due to Hamada [6] and to Smith [12] for $k = n-1$. More recently Black and List [1] gave a generating function for the entries in a diagonal form of $\mathcal{M}_{n-1}(p)$ over $\mathbb{Z}$. Also, Lander [10, p 77] has apparently given information equivalent to a diagonal form of $\mathcal{M}_{n-1}(q)$ over $\mathbb{Z}$ in his (unpublished) Ph.D. thesis.

We show how diagonal forms for these incidence matrices arise naturally in the study of integral Hecke algebras and their geometrically significant eigenpotents. Within the $\mathbb{Z}$-module based on the chambers

Received February 7, 1995.
Revised January 15, 1996.
This research was partially supported by NSA grant 904-91-H-0048.

of the associated building we construct a certain lattice $\mathcal{L}$ that is invariant under the integral Hecke algebra $\mathcal{H}$. Theorem 3.7 asserts that $\mathcal{L}$ has a $\mathcal{H}$-completely reducible sublattice $\mathcal{N}$ of finite volume. It follows from Proposition 3.8 that the essential part of these incidence maps can be simultaneously diagonalized within $\mathcal{N}$ and that their Smith normal forms are computable from the multiplicites of the constituent irreducible $\mathcal{H}$-modules appearing in $\mathcal{N}$.

Unfortunately, I have no effective way of directly computing the constituent multiplicites of the $\mathbb{Z}$-forms appearing in $\mathcal{N}$. But, it turns out there is only one $\mathbb{Z}[1/p]$-form arising in $\mathcal{L} \otimes \mathbb{Z}[1/p]$. This allows the easy computation of the elementary divisors of $\mathcal{M}_k(q)$ that are not powers of p in Theorem 3.10.

We also give an independently obtained formula for a diagonal form for $\mathcal{M}_k(q)$ whenever k and n are relatively prime, Corollary 4.5. The proof of this formula involves and adaptation of an argument of Brouwer [2] to finite local rings. Some data from a Maple implementation of the formula is also given.

§2. Pure preliminaries

Let K be the quotient field of a Dedekind domain R. An *R-lattice* is a finitely generated R-torsionfree R-module. Each R-lattice M is naturally embedded in a finite dimensional K-vector space $KM := K \otimes_R M$. An R-sublattice $L \leq M$ is *pure* if M/L is R-torsionfree, or equivalently if L is a direct summand of M. Any submodule L of M has as its *pure closure* the inverse image of the torsion part of M/L. The importance of purity arises from:

Theorem 2.1 ([4, 4.12]). *Let M be an R-lattice. There is a bijective inclusion preserving correspondence between the R-pure sublattice of M and the K-subspaces of KM given by $L \to KL$ and $W \to W \cap M$.*

The theory of pure submodules is more subtle than that of vector spaces in part because a sum of two pure submodules that intersect trivially need not be pure. For example, $\mathcal{L}_\varepsilon = \{(a, \varepsilon a) |\ a \in \mathbb{Z}\}$ is a pure submodule of $\mathbb{Z}^2$ for any $\varepsilon \in \mathbb{Z}$. But $(2,0) \in \mathcal{L}_1 + \mathcal{L}_{-1}$ and $(1,0) \notin \mathcal{L}_1 + \mathcal{L}_{-1}$, so $\mathcal{L}_1 + \mathcal{L}_{-1}$ is not pure.

An *R-order* is a ring Λ whose center contains R, is finitely generated as an R-module and such that $A := K\Lambda$ is a K-algebra. Two Λ-modules M_1, M_2 that are R-lattices and with the property that KM_1 is equivalent (over K) to KM_2 are said to be *R-forms* for the associated A-module.

It is tempting to look for a Krull-Schmidt-Azumaya Theorem [4, Theorem 6.12] or even a Jordan-Hölder Theorem [4, Theorem 3.11] for

R-forms, but in Section 3.2 we see that the central object of our study $\mathcal{L}$ has a more subtle structure, not being completely reducible and failing the conclusion of the Jordan-Hölder Theorem. Indeed, (in the language of that Section) $\mathcal{L}$ contains two proper submodules $\mathcal{N}$ and $\mathcal{N}'$ each of which is a direct sum of irreducible $\mathbb{Z}$-forms for the natural representation but $\mathcal{L}/\mathcal{N}$ affords a finite version of the index representation while $\mathcal{L}/\mathcal{N}'$ affords a finite version of the Steinberg representation. Fortunately, Proposition 3.8 observes that this anomaly does not impact our incidence map study.

§3. Integral Hecke Algebras

Because this section is written in somewhat greater generality than the rest of this paper, examples are included to provide more explicit information about the most important case namely $PG_{n-1}(q)$.

Let $\mathcal{C}h$ be the set of chambers of a finite building $\mathcal{B}$ of type I and Weyl group $W = W(I) = \langle r_i | i \in I \rangle$. The *Standard module* $\mathbb{Z}\mathcal{C}h$ of $\mathcal{B}$ is the free $\mathbb{Z}$-module with $\mathcal{C}h$ as an orthonormal basis. The *integral Hecke algebra* $\mathcal{H}$ is the $\mathbb{Z}$-algebra generated by $\{\sigma_i | i \in I\} \subseteq \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}\mathcal{C}h)$ where σ_i is (the adjacency matrix of) the relation "differ only in type i" on $\mathcal{C}h$. Because each such relation determines an equivalence relation with equipotent classes, each σ_i satisfies

$$(\sigma_i + 1)(\sigma_i - q_i) = 0, \tag{1}$$

for some integer q_i called the *index parameter* of σ_i.

A fundamental result of Iwahori [9],[4, Section 67] implies that the rational Hecke algebra $\mathcal{H} \otimes \mathbb{Q}$ has a $\mathbb{Q}$-basis

$$\mathcal{F} := \{\sigma_w := \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_n} \mid \begin{array}{c} w \in W \text{ can be expressed} \\ \text{in reduced form } r_{i_1} r_{i_2} \ldots r_{i_n} \end{array} \}.$$

Notice that, elements of $\mathcal{F}$ are well defined and depend only the the associated element $w \in W$, not on the reduced form used to present w, because any two reduced forms for w can be transformed into each other using only rules of the form $r_i r_j r_i ... = r_j r_i r_j ...$, without any use of the relation $r_i^2 = 1$.

Because $\mathcal{F}$ is contained in $\mathcal{H}$, $\mathcal{H}$ is a $\mathbb{Z}$-order in the rational Hecke algebra. More than this, the result of Iwahori asserts that the rational Hecke algebra has a presentation (as an algebra) with generators $\{\sigma_i\}$ and relations: Equation (1) together with a relation equivalent to:

$$\begin{array}{c} \text{If } \sigma_w \in \mathcal{F} \text{ but } \sigma_w \sigma_j \notin \mathcal{F}, \text{ then } \sigma_w \\ \text{can be written in the form } \sigma_w = \cdots \sigma_j. \end{array} \tag{2}$$

Theorem 2.1 [4, 23.7] implies that any pure $\mathcal{H}$-submodule L of $\mathbb{Z}Ch$ is a $\mathbb{Z}$-form for a $\mathbb{Q}\mathcal{H}$-module.

3.1. Geometrically significant eigenpotents

For each $J \subseteq I$ and $c \in Ch$, define $c_J \in S$ to be the sum of all chambers having the same J residue as c. Explicitly the map $c \to c_J$ is realized by the *eigenpotent* $P_J \in \mathcal{H}$ where

$$P_J = \sum_{w \in W_J} \sigma_w$$

and W_J is the set of reduced words in the Weyl group W that involve only elements of $I \setminus J$. The elements P_J appear in [8] and [11]. The *Poincaré polynomial* [4, sec 67], p_J, of type J is obtained from P_J by replacing each σ_i with its index parameter.

In practice, one never really computes a geometrically significant eigenpotent as such a large sum. Instead, there are factored forms obtainable from chains of subgroups of the Weyl group.

Example 3.1. The building of type A_{n-1} with index parameters $q_i = q$ arises from the projective geometry $PG_{n-1}(q)$. It has as chambers the set of maximal chains (ordered by inclusion) of subspaces of the underlying vector space $GF(q)^n$. The relation giving rise to σ_i associates such a chain $0 < V_1 < \cdots < GF(q)^n$ to all other chains $0 < W_1 < \cdots < GF(q)^n$, where $W_j = V_j$ if and only if $i \neq j$. The associated Weyl group $W(A_{n-1})$ is the symmetric group S_n with the distinguished generators the transpositions $r_i = (i, i+1)$. The Iwahori relations for this Hecke algebra are Equation (1) and

$$\sigma_i\sigma_{i-1}\sigma_i = \sigma_{i-1}\sigma_i\sigma_{i-1} \text{ and } \sigma_i\sigma_j = \sigma_j\sigma_i \text{ whenever } |i-j| > 1.$$

Because S_n is doubly transitive and r_{n-1} commutes with S_{n-2}, S_n/S_{n-1} can be written $S_n = S_{n-1} \cup (S_{n-1}/S_{n-2})r_{n-1}S_{n-1}$. It follows that

$$\sum_{w \in W(A_{n-1})} w = \lambda_{n-1} \cdots \lambda_2\lambda_1, \text{ where } \lambda_k = (1 + \lambda_{k-1}r_k), \lambda_0 = 1.$$

Notice that the left most factor on the right hand side is the sum of left-coset representatives of S_n/S_{n-1} and, when multiplied out, each of the expressions is already in reduced form! It follows that the eigenpotent element associated with the empty set for a building of type A_{n-1} is $P_\phi(A_{n-1}) = L_{n-1}P_\phi(A_{n-2})$, where

$$L_{n-1} := 1 + L_{n-2}\sigma_{n-1} \qquad \text{and} \qquad L_0 = 1.$$

If instead we worked with right-cosets, we would obtain:

$$\sum_{w\in W(A_{n-1})} w = \rho_1 \cdots \rho_{n-1}, \text{ where } \rho_k = (1 + r_k\rho_{k-1}), \rho_0 = 1$$

and a different factorization: $P_\phi(A_{n-1}) = P_\phi(A_{n-2})R_{n-1}$, where

$$R_{n-1} := 1 + \sigma_{n-1}R_{n-2} \qquad \text{and} \qquad R_0 = 1.$$

The Weyl group $W(B_3) = \langle r_1, r_2, r_3 | (r_i r_j)^{m_{ij}} = 1\rangle$; where $m_{ij} = m_{ji}$ and $m_{ii} = 1, m_{12} = 3, m_{13} = 2, m_{23} = 4$. The (formal) sum $T = [(1+r_1+r_2r_1)+(1+r_2+r_1r_2)r_3r_2r_1] \in \mathbb{Z}W$ of left-coset representatives for $W/\langle r_2, r_3\rangle$ satisfies

$$\sum_{w\in W} w = T \sum_{h\in\langle r_2,r_3\rangle} h = T(1 + r_3)(1 + r_2r_3)(1 + r_2).$$

Again, each factor is the sum of left-coset representatives and, when multiplied out, each expression is already in reduced form. For this reason the eigenpotent P_ϕ associated with the empty set in a building of type B_3 can be factored:

$$P_\phi = [(1+\sigma_1+\sigma_2\sigma_1)+(1+\sigma_2+\sigma_1\sigma_2)\sigma_3\sigma_2\sigma_1](1+\sigma_3)(1+\sigma_2\sigma_3)(1+\sigma_2).$$

The reader may check that a different sequence of subgroups leads to the more pleasant factorization:

$$P_\phi = (1 + \sigma_3)(1 + \sigma_2\sigma_3)(1 + \sigma_1\sigma_2\sigma_3)(1 + \sigma_2 + \sigma_1\sigma_2)(1 + \sigma_1).$$

The name given P_J is perhaps motivated by the fact that P_J is almost idempotent.

Lemma 3.2. $P_J^2 = p_J P_J$

Proof. It is sufficient to show that $P_J\sigma_i = P_J q_i$ for each $i \in I \setminus J$. This follows from the Iwahori relations Equations (1) and (2). This last computation can be vastly simplified by using a factored form for $P_J = \cdots (1 + \sigma_i)$ developed from a sequence of subgroups of the associated Weyl group starting from $\langle r_i\rangle$ as described in Example 3.1. Q.E.D.

Let $\mathbb{Z}\,\mathrm{typ}^{-1}(J)$ denote the image of $P_J \in \mathrm{End}(\mathbb{Z}\mathcal{C}h)$. Since no chamber is incident with two different elements of type J, $\mathbb{Z}\,\mathrm{typ}^{-1}(J)$ is a pure $\mathbb{Z}$-submodule of $\mathbb{Z}\mathcal{C}h$ having a distinguished basis $\{P_J(x) : \mathrm{typ}(x) = J\}$. It is therefore natural to identify an element x_J of type J in $\mathcal{B}$ with its image in $\mathbb{Z}\,\mathrm{typ}^{-1}(J)$.

The importance of the geometrically significant eigenpotent elements for our purposes is made clear by the following:

Lemma 3.3 ([11]). *Identify an element x_J of type J in $\mathcal{B}$ with its image in $\mathbb{Z}\,\mathrm{typ}^{-1}(J)$ as above. Then the natural incidence map from* $\mathrm{typ}^{-1}(J)$ *to* $\mathrm{typ}^{-1}(K)$ *is afforded by:*

$$P_K/p_{J\cap K} : \mathbb{Z}\,\mathrm{typ}^{-1}(J) \to \mathbb{Z}\,\mathrm{typ}^{-1}(K),$$

where $p_{J\cap K}$ is the Poincaré polynomial defined above.

Proof. The (a, c) entry of $P_K P_J$ counts the number of $b \in Ch$ where a and b share a face of type J and where b and c share a face of type K. There is no such b unless a and c share a face of type $J \cap K$ and then the number of choices for b is $p_{J\cap K}$. Q.E.D.

In the notation of the introduction, it is well known that the composition of the incidence maps $\mathcal{P}_{i-1} \to \mathcal{P}_i \to \mathcal{P}_{i+1}$ is $(q+1)$ times the incidence map $\mathcal{P}_{i-1} \to \mathcal{P}_{i+1}$. We illustrate the present language by recording this familiar fact. There follows a related factorization of the point hyperplane (non)-incidence map: $\mathcal{P}_1 \to \mathcal{P}_{n-1}$ that plays a key role in the proof of Theorem 3.7.

Corollary 3.4. *Suppose $\mathcal{B}$ is of type A_{n-1} with index parameter q. Then* $\mathrm{typ}^{-1}(\{i\}) = \mathcal{P}_i$ *— the set of $i-1$-flats in $PG_{n-1}(q)$ (the set of i-dimensional subspaces of the underlying vector space). Abuse notation by writing i for $\{i\}$.*

1. *The Poincaré polynomial of incident $i-1$- and i-flats is*

$$p_{i\,i+1} = \prod_{j=1}^{i-1} \frac{(q^j-1)}{(q-1)} \prod_{j=1}^{n-i-2} \frac{(q^j-1)}{(q-1)}.$$

2. *For any chamber $c \in Ch$, $P_{i-1}(c)$ is (under the above identification) the $i-2$-flat of c and $P_{i+1}P_i(P_{i-1}(c))) = p_i P_{i+1}(P_{i-1}(c))$.*
3. *For $c \in Ch$, $P_{n-1}\sigma_{n-1}\cdots\sigma_1(c)$ is the sum of all hyperplanes off the point of c.*
4. *For $c \in Ch$,*

$$(\sigma_{n-1}-q)\cdots(\sigma_1-q)(P_1(c)) = -(\sigma_{n-1}-q)P_{n-1}\sigma_{n-1}\cdots\sigma_1(c).$$

Proof. The first two parts follow from Lemma 3.3. The chambers d in (the support of) $\sigma_{n-1}\cdots\sigma_1(c)$ are obtained from c by first changing the point (to another one on the line of c), then changing the line, etc. The result is chambers d having no i-flat in common with c but for whom each i-flat meets the i-flat of c in the $i-1$-flat of d. If two such chambers shared a k-flat, then the $k-1$-flat of each must be the intersection of their common k-flat with the k-flat of c. Consequently, no two distinct such chambers share a hyperplane. For any such chamber d, $P_{n-1}(d)$ is just the hyperplane of d, by Part 1, so the indicated expresssion counts each hyperplane off the point of c exactly once. This proves Part 3.

In order to prove Part 4, we embellish the notation introduced in Example 3.1 and begin with a sublemma. Suppose $a_1, a_2, \ldots, a_k$ is a monotonic sequence of consective integers between 1 and $n-1$. Define $R_i(a_1 \ldots a_k)$ recursively by $R_i(a_1 \ldots a_k) = 1 + \sigma_{a_i} R_{i-1}(a_1 \ldots a_k)$ and $R_0(a_1 \ldots a_k) = 1$. Note that $R_i(a_1 \ldots a_k)$ depends only on $a_1, \ldots, a_i$ and so $R_{k-1}(a_1 \ldots a_k) = R_{k-1}(a_1 \ldots a_{k-1})$. Argue inductively that:

$$(3) \qquad \sigma_{a_1} \ldots \sigma_{a_k} R_{k-1}(a_1 \ldots a_{k-1}) = R_{k-1}(a_2 \ldots a_k) \sigma_{a_1} \ldots \sigma_{a_k}.$$

By the recursive nature of R's and the Iwahori relations, we have:

$$\begin{aligned}
&\sigma_{a_1} \ldots \sigma_{a_k} (R_{k-1}(a_1 \ldots a_{k-1}) - 1) \\
&\quad = \sigma_{a_1} \ldots \sigma_{a_{k-2}} (\sigma_{a_{k-1}} \sigma_{a_k} \sigma_{a_{k-1}}) R_{k-2}(a_1 \ldots a_k) \\
&\quad = \sigma_{a_1} \ldots \sigma_{a_{k-2}} (\sigma_{a_k} \sigma_{a_{k-1}} \sigma_{a_k}) R_{k-2}(a_1 \ldots a_{k-1}) \\
&\quad = \sigma_{a_k} [\sigma_{a_1} \ldots \sigma_{a_{k-2}} \sigma_{a_{k-1}} R_{k-2}(a_1 \ldots a_{k-1})] \sigma_{a_k} \\
&\quad = \sigma_{a_k} [R_{k-2}(a_2 \ldots a_k) \sigma_{a_1} \ldots \sigma_{a_{k-2}} \sigma_{a_{k-1}}] \sigma_{a_k},
\end{aligned}$$

by the induction hypothesis. Therefore,

$$\sigma_{a_1} \ldots \sigma_{a_k} R_{k-1}(a_1 \ldots a_{k-1}) = (1 + \sigma_{a_k} R_{k-2}(a_2 \ldots a_k)) \sigma_{a_1} \ldots \sigma_{a_{k-1}} \sigma_{a_k}$$

as desired.

Now argue Part 4 by induction on n. In case $n = 2$:

$$\begin{aligned}
(\sigma_2 - q)(\sigma_1 - q)(\sigma_2 + 1) \quad &= \quad (\sigma_2 - q)\sigma_1(\sigma_2 + 1) - q(\sigma_2 - q)(\sigma_2 + 1) \\
= \quad (\sigma_2 - q)(-\sigma_2)\sigma_1(\sigma_2 + 1) - 0 &= -(\sigma_2 - q)(\sigma_2\sigma_1\sigma_2 + \sigma_2\sigma_1) \\
= \quad -(\sigma_2 - q)(\sigma_1\sigma_2\sigma_1 + \sigma_2\sigma_1) \quad &= -(\sigma_2 - q)(\sigma_1 + 1)\sigma_2\sigma_1
\end{aligned}$$

by the distributive law and two applications of Equation (1) for σ_2 followed by the relation $\sigma_2\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1$.

For the general case, begin with P_1 in the factored form with *reverse* lexicographical order and right cosets: $P_1 = R_1(n-1 \ldots 2) \cdots R_{n-2}(n-1 \ldots 2)$, and note that σ_2 appears in only the last factor. Since σ_1 commutes with each σ_i, $i \neq 2$, we have by induction:

$$\begin{aligned}
&(\sigma_{n-1} - q) \cdots (\sigma_1 - q) P_1 \\
&\quad = [(\sigma_{n-1} - q) \cdots (\sigma_2 - q) R_1(n-1 \ldots 2) \cdots R_{n-3}(n-1 \ldots 2)] \\
&\qquad \times (\sigma_1 - q) R_{n-2}(n-1 \ldots 2) \\
&\quad = -[(\sigma_{n-1} - q) R_1(n-2 \ldots 2) \cdots R_{n-3}(n-2 \ldots 2) \sigma_{n-1} \cdots \sigma_2] \\
&\qquad \times (\sigma_1 - q) R_{n-2}(n-1 \ldots 2).
\end{aligned}$$

Next distribute with respect to the $(\sigma_1 - q)$ term and apply Equation (3) repeatedly to the expression:

$$\begin{aligned}
&q(\sigma_{n-1} - q)[R_1(n-2\dots 2)\cdots R_{n-3}(n-2\dots 2)\sigma_{n-1}\cdots\sigma_2]\\
&\qquad \times R_{n-2}(n-1\dots 2)\\
&\quad = q(\sigma_{n-1} - q)[\cdots R_{n-4}(n-2\dots 2)\sigma_{n-1}\cdots\sigma_2]\\
&\qquad \times R_{n-3}(n-1\dots 2)R_{n-2}(n-1\dots 2)\\
&\quad \cdots = q(\sigma_{n-1} - q)\sigma_{n-1}\cdots\sigma_2[R_1(n-1\dots 2)\cdots R_{n-2}(n-1\dots 2)].
\end{aligned}$$

But the last expression P within brackets [ ] is a factored form of the trivial eigenpotent on $\{2\dots n-1\}$ and so can be rewritten in a factored form begining with $(\sigma_i + 1)$ for any $i = 2, \dots, n-1$. It follows that this term equals $q^{n-1}(\sigma_{n-1} - q)P = 0$. This shows that only the other expression survives and by one more application of Equation (3) it can be rewritten:

$$\begin{aligned}
&-(\sigma_{n-1} - q)R_1(n-2\dots 2)\cdots R_{n-3}(n-2\dots 2)\\
&\qquad \times[\sigma_{n-1}\cdots\sigma_2\sigma_1 R_{n-2}(n-1\dots 2)]\\
&\quad = -(\sigma_{n-1} - q)R_1(n-2\dots 1)\cdots R_{n-2}(n-2\dots 1)\sigma_{n-1}\cdots\sigma_2\sigma_1\\
&\quad = -(\sigma_{n-1} - q)P_{n-1}\sigma_{n-1}\cdots\sigma_2\sigma_1.
\end{aligned}$$

Q.E.D.

There is also a representation theoretic proof of Corollary 3.4.4 that amounts to verification of the indicated equation in all relevant $\mathcal{H}\otimes_{\mathbb{Z}}\mathbb{Q}$ representations. Because P_1 and P_{n-1} are trivial in all $\mathcal{H}\otimes_{\mathbb{Z}}\mathbb{Q}$ representations other than the index and natural representations, one need only verify Corollary 3.4.4 for the index representation, where it is immediate, and for the matrices appearing in Section 3.2.

In fact Corollary 3.4.4 is a combinatorial identity that was first obtained by a representation theoretic method. I leave it to the reader's taste which argument is more elementary.

3.2. The natural $\mathcal{H}$ representation and its irreducible $\mathbb{Z}$-forms

The representations of $\mathcal{H}\otimes\mathbb{C}$ are deformations of the irreducible representations of the associated Weyl group by a celebrated theorem of Tits. Hoefsmit [7] gives explicit formulas in case the building arises from a classical group. Because we are concerned with incidence maps involving the points $\mathcal{P}_1$ of $PG_{n-1}(q)$, we must deal explicitly with the $\mathcal{H}(A_{n-1})$-representations arising from $\mathbb{Z}\,\mathrm{typ}^{-1}(\{1\})$. These correspond to the S_n representations labelled by partitions $\{n\}$ and $\{n-1, 1\}$ [3, Theorem 2.1].

The *index* representation *Ind* corresponds to the trivial representation $\{n\}$ of S_n. *Ind* is the homomorphism $\mathcal{H} \to \mathbb{Z}$ that maps each generator σ_i to its index paramater q_i. Thus the Poincaré polynomial is just $Ind(P_\phi)$. The *Steinberg* representation *St* is the homomorphism $\mathcal{H} \to \mathbb{Z}$ that maps each generator σ_i to -1.

The *natural* representation corresponds to the natural representation $\{n-1, 1\}$ of S_n and is a homomorphism $\mathcal{H} \to \mathrm{Mat}_{n-1}(\mathbb{C})$. Hoefsmit's version of this representation is a natural generalization of Young's "semi-normal" form for the symmetric group representation and is:

$$(\sigma_1) = \left(\begin{array}{c|c} qI_{n-2} & \\ \hline & -1 \end{array}\right); \quad (\sigma_i) = \left(\begin{array}{c|cc|c} qI_{n-i-1} & & & \\ \hline & \frac{q-1}{1-q^i} & \frac{1-q^{i+1}}{1-q^i} & \\ & \frac{q-q^i}{1-q^i} & \frac{q^i-q^{i+1}}{1-q^i} & \\ \hline & & & qI_{i-2} \end{array}\right)$$

for $i = 2, \dots, n-1$. We record a few easy consequences of this explicit representation.

Lemma 3.5. *Under the natural representation of $\mathcal{H}$ we have:*

1. $(\sigma_k - q)(\sigma_i - q) = 0$ *whenever* $|i-k| > 1$,
2. *For all* $j \notin J \subseteq I$, $\mathrm{Im}(P_J) \cap \ker(\sigma_j + 1) = 0$.

Proof. In each case this follows from a simple matrix computation. The result is a little more transparent if a general $\mathbb{Z}$-form presented below is used. Q.E.D.

The restriction of the centralizer in $\mathcal{H}$ of P_J to the image of P_J is called the J-th *parabolic* subalgebra of $\mathcal{H}$. The adjacency algebras of many distance transitive graphs arise as parabolic subalgebras for $|J| = 1$. One can in principle compute the eigenvalues of these graphs [11] from the explicit $\mathbb{C}$-representations of $\mathcal{H}$.

Say a $\mathbb{Z}$-form for an irreducible representation of $\mathcal{H} \otimes \mathbb{C}$ is of *type* $\mathcal{N}$ (respectively of *type* $\mathcal{N}'$) if the associated $\mathcal{H}$-module is generated by the -1-eigenspaces (respectively q_i-eigenspaces) of $\{\sigma_i\}$.

Of particular interest to us are the irreducible $\mathbb{Z}$-forms for the natural representation of $\mathcal{H}(A_n)$. One can show that the irreducible $\mathbb{Z}$-forms of the natural representation of type $\mathcal{N}$ are parameterized by integers $a_1, \dots, a_{n-1}$, all divisors of q and the block diagonal matrices:

$$(\sigma_1) = \left(\begin{array}{cc|c} -1 & q/a_1 & \\ 0 & q & \\ \hline & & qI_{n-2} \end{array}\right); (\sigma_n) = \left(\begin{array}{c|cc} qI_{n-2} & & \\ \hline & q & 0 \\ & a_{n-1} & -1 \end{array}\right)$$

$$(\sigma_i) = \left(\begin{array}{c|ccc|c} qI_{i-1} & & & & \\ \hline & q & 0 & 0 & \\ & a_{i-1} & -1 & q/a_i & \\ & 0 & 0 & q & \\ \hline & & & & qI_{n-i-2} \end{array}\right) ; \text{ for } i = 2, \dots, n-1.$$

In particular, distinct $a_1, \dots, a_{n-1}$ give $\mathbb{Z}$-inequivalent forms. Denote the $\mathbb{Z}$-form with parameters $a_1, \dots, a_{n-1}$ by $\mathcal{N}(a_1, \dots, a_{n-1})$. The same computation shows that there is but one $\mathbb{Z}[1/p]$-form of type $\mathcal{N}$ for the natural representation when q is a power of the prime p.

Example 3.6. The reader must be warned that there do exist indecomposable $\mathbb{Z}$-forms having all natural $\mathcal{H}$-composition factors that are reducible. Indeed, the matrices

$$\sigma_1 = \begin{pmatrix} -1 & q/a & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & -1 & q/b \\ 0 & 0 & 0 & q \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} q & 0 & bq & -(q+1)q \\ a & -1 & ab(q+1) & -aq \\ 0 & 0 & q & 0 \\ 0 & 0 & b & -1 \end{pmatrix}$$

satisfy the relations defining $\mathcal{H}(A_2)$. Moreover any transition matrix $P \in SL(4, \mathbb{Z})$, taking these matrices to a sum of the above forms, must leave invariant the -1-eigenspace of σ_1 and take the -1-eigenspace of σ_2 to $\langle e_2, e_4 \rangle$. Computation of $P^{-1}\sigma_i P$ shows that P is forced to have the form

$$P = \begin{pmatrix} g(vb - uab(q+1)) & uq & h(fb - wab(q+1)) & wq \\ 0 & v & 0 & x \\ uag & 0 & wah & 0 \\ 0 & u & 0 & w \end{pmatrix},$$

for integers g, h, u, v, w, x. But $\det(P) = abgh(xu - vw)^2$, so this representation does not split over $\mathbb{Z}$ whenever $|ab| \neq 1$.

The reader must also be warned that not every irreducible natural $\mathcal{H}$-module is of type $\mathcal{N}$. For example, the transposes of the above displayed $\mathbb{Z}$-form of $\mathcal{H}(A_n)$ is again a $\mathbb{Z}$-form of $\mathcal{H}(A_n)$, but of type $\mathcal{N}'$.

When one attempts to transform such a represenation to one of type $\mathcal{N}$, exploitation of eigenspaces as above leads to an essentially unique transition matrix and to the form $\mathcal{N}(q/a_1, \dots, q/a_{n-1})$. When $n = 4$ the transition matrix is

$$\begin{pmatrix} (1+q)(1+q^2) & (1+q+q^2)a_1 & a_1a_2(1+q) & a_1a_2a_3 \\ (1+q+q^2)q/a_1 & (1+q)(1+q+q^2) & (1+q)^2a_2 & (1+q)a_2a_3 \\ (1+q)q^2/(a_1a_2) & (1+q)^2q/a_2 & (1+q)(1+q+q^2) & (1+q+q^2)a_3 \\ q^3/(a_1a_2a_3) & (1+q)q^2/(a_2a_3) & (1+q+q^2)q/a_3 & (1+q)(1+q^2) \end{pmatrix}$$

and has determinant $(1+q+q^2+q^3+q^4)^3$. Therefore these forms are not $\mathbb{Z}$-equivalent. Thanks to L. Solomon for sharing this observation.

Let $\mathcal{L}$ be the pure closure in $\mathbb{Z}\mathcal{C}h$ of $\mathcal{H}(\sigma_1 - q)P_{\{1\}}\mathcal{C}h$. The module $\mathcal{L}$ is fundamental to our study of the incidence maps $\mathcal{M}_k(q)$. It will turn out that $\mathcal{L}$ is the largest $\mathcal{H}$-submodule of the standard module affording only the natural representation of $\mathcal{H}$. It seems unlikely, however, that $\mathcal{L} \otimes_{\mathbb{Z}} R$ is a summand of $R\mathcal{C}h$ unless the Poincaré polynomial $p_{\{1\}}$ is a unit in the domain R.

Theorem 3.7. *The sum of the components of $\mathbb{Q}\mathcal{C}h$ affording the natural representations of $\mathcal{H} \otimes \mathbb{Q}$ is $\mathcal{L} \otimes \mathbb{Q}$.*

Let $\mathcal{L}_i \leq \mathcal{L}$ be the -1-eigenspace of σ_i. Then

1. *$\sum \mathcal{L}_i$ is a direct sum of irreducible $\mathcal{H}$-modules of type $\mathcal{N}$,*
2. *$\mathcal{L}/\sum \mathcal{L}_i$ is torsion of exponent dividing $1+q+\cdots+q^n$ and affords (a modular version of) the index representation of $\mathcal{H}$.*

Proof. As already mentioned, $\mathcal{H}P_{\{1\}}\mathbb{Z}\mathcal{C}h \otimes \mathbb{Q}$ is the sum of the components of $\mathbb{Q}\mathcal{C}h$ associated with the index and the natural representations of $\mathcal{H} \otimes \mathbb{Q}$. By Equation (1) $\sigma_1 v = -v$, for all $v \in (\sigma_1 - q)\mathbb{Z}\mathcal{C}h$ so $\mathcal{L} \otimes \mathbb{Q}$ affords only the natural representation of $\mathcal{H} \otimes \mathbb{Q}$ and to full multiplicity.

Define $m_i : \mathcal{L}_1 \to \mathcal{L}_i$ by $m_i(v) = (\sigma_i - q)m_{i-1}(v)$. When m_{n-1} is regarded as an homomorphism of rational vector spaces, it is invertible. Therefore m_{n-1} is of maximal rank. Pick bases $\{\ell_{11}, \dots, \ell_{1m}\}$, of $\mathcal{L}_1$ and $\{\ell_{n-1\,1}, \dots, \ell_{n-1\,m}\}$ of $\mathcal{L}_{n-1}$ so that m_{n-1} is in Smith normal form. Let ℓ_{ij} span the pure $\mathbb{Z}$-submodule generated by $m_i(\ell_{1j})$ and define $a_{ij} \in \mathbb{Z}$ by $(\sigma_i - q)(\ell_{i-1\,j}) = a_{ij}\ell_{ij}$. Finally set $N_j := \mathbb{Z}\{\ell_{ij} | i = 1, \dots, n-1\}$.

Notice that m_{n-1} appears in Corollary 3.4.4. This result implies that the pure closure of $\operatorname{Im}(\sigma_{n-1} - q)$ within $\mathcal{H}\operatorname{Im}(P_{\{n\}})$ is exactly $\mathcal{L}_{n-1}$, the pure closure of $\operatorname{Im}(m_{n-1})$. Thus, we could as well have started with hyperplanes rather than points, the same module $\mathcal{L}$ would arise. Moreover, m_{n-1} is in Smith normal form with respect to the bases $\{\ell_{11}, \dots, \ell_{1m}\}$, of $\mathcal{L}_1$ and $\{\ell_{n-1\,1}, \dots, \ell_{n-1\,m}\}$ of $\mathcal{L}_{n-1}$ if and only if its transpose is in Smith normal form with respect to the bases $\{\ell_{n-1\;1}, \dots, \ell_{n-1\;m}\}$ of $\mathcal{L}_{n-1}$ and $\{\ell_{11}, \dots, \ell_{1m}\}$, of $\mathcal{L}_1$. Therefore, this point - hyperplane symmetry leaves invariant the set $\{\ell_{ij}\}$ as well.

In order to show that N_j is $\mathcal{H}$-invariant it is sufficient to show $(\sigma_k - q)\ell_{ij} \in N_j$ for $|k-i| = 1$, by Lemma 3.5.1. But this follows from the above noted symmetry and the definition $\ell_{kj} = (\sigma_k - q)(\ell_{k-1j})$. This completes the proof that N_j is $\mathcal{H}$-invariant.

To see that N_j affords the $\mathbb{Z}$-form with parameters a_{ij} relative to $\{\ell_{ij}\}$, note that $(\sigma_i - q)(\sigma_k - q) = 0$ in $\mathcal{L} \otimes \mathbb{Q}$, whenever $|i-k| > 1$, by Lemma 3.5.1. Since $\ell_{jk} \in \mathrm{Im}(\sigma_k - q)$, this and the definition of a_{ij} forces each of the columns of the matrix of σ_i to be as specified except perhaps the $i+1$-st column. This column is forced by the others and the Iwahori relations. Since $\mathcal{N} := \sum N_j = \sum \mathcal{L}_i$, this establishes Part 1.

Suppose $\ell \in \mathcal{L} \setminus \mathcal{N}$ and set $n_i = (\sigma_i(\ell) - q)(\ell)$. Then $\sigma_i(n_i) = \sigma_i(\sigma_i - q)(\ell) = -(\sigma_i - q)(\ell) = -n_i$, so $n_i \in \mathcal{N}$. Now $\mathcal{L}/\mathcal{N}$ affords the index representation because $\sigma_i(\ell) \equiv q\ell \pmod{\mathcal{N}}$.

Clearly $\mathcal{L} \leq \mathcal{N} \otimes \mathbb{Q}$ and it suffices to show that $\mathcal{L}/(\sum_{j\neq k} N_j)$ has the indicated exponent. But this finite abelian group has order dividing the volume of $N_k \leq N_k \otimes \mathbb{Q}$, which in turn equals the absolute value of the determinant, say k_n, of

$$\sum(\sigma_i - q) = \begin{pmatrix} -q-1 & q/a_{1k} & & & \\ a_{1k} & -q-1 & q/a_{2k} & & \\ & a_{2k} & \ddots & \ddots & \\ & & \ddots & -q-1 & q/a_{n-1k} \\ & & & a_{n-1k} & -q-1 \end{pmatrix}.$$

The result follows from the recurrence $k_n = -(1+q)k_{n-1} - qk_{n-2}$. Q.E.D.

If we use the common q-eigenspaces of all but one of the σ_i's (as in the last part of Example 3.6) instead of -1-eigenspaces, the ideas of this proof lead to $\mathbb{Z}$-forms of the natural $\mathcal{H}$-representation of type $\mathcal{N}'$ and a submodule $\mathcal{N}'$ of $\mathcal{L}$ of finite volume such that $\mathcal{L}/\mathcal{N}'$ affords a finite version of the Steinberg representation.

Proposition 3.8. *The Smith normal form of an integral incidence map π coincides with that computed using any submodule of finite volume v in* domain(π).

Proof. Because any free $\mathbb{Z}$-module M is $\mathbb{Z}$-isomorphic to its submodule vM, the incidence map has the same algebraic invariants as their restriction to $v \cdot \mathrm{domain}(\pi)$. Q.E.D.

Example 3.9. For $\mathcal{H}$-modules of type $\mathcal{N}'$, $\mathrm{Im}(P_{\{i\}})$ is contained in the span of the i-th natural basis vector. In case $n = 4$, the i,j entry of the matrix $(P_1 + P_2 + P_3 + P_4)$ gives the diagonal entry of the i-space versus j-space incidence matrix of $PG(4,q)$ arising from the $\mathbb{Z}$-form of transposes of $\mathcal{N}(a_1, a_2, a_3)$ and is, amazingly enough, the matrix appearing in Example 3.6 left multiplied by $\mathrm{diag}\{(q^2+q+1)(q+1), q+1, q+1, (q^2+q+1)(q+1)\}$.

In case $q = p$ is prime one can use the known p-rank formulae for incidence maps to compute the multiplicites of each of the $\mathbb{Z}$-forms. All multiplicities are zero except: $m_{1,1,1} = m_{p,p,p} = (p+3)(p+2)(p+1)p/24$; $m_{1,1,p} = m_{1,p,p} = p(p+1)(11p^2 - 5p + 6)/24$.

The fact that Propositon 3.8 can be applied to either $\mathcal{N} \leq \mathcal{L}$ or to $\mathcal{N}' \leq \mathcal{L}$ seems to imply a well known symmetry in the multiplicities of the p-power elementary divisors of $\mathcal{M}_{n-1}(q)$, $p|q$.

Also, as noted just before Example 3.6, any two irreducible $\mathbb{Z}$-forms for the natural $\mathcal{H}$-module are equivalent if coefficients are extended to $\mathbb{Z}[1/p]$ so that p is a unit. Some results of Frumkin and Yakir [5] about certain incidence maps' modular rank therefore extend to statements about elementary divisors.

Theorem 3.10. *Let $\mathcal{V}$ be the sublattice of $\mathbb{Z}\mathcal{P}_1$ whose elements have coordinate sum equal to zero. Then the p'-part of the finite abelian group $\mathcal{V}/(\mathcal{V} \cap$ column space$\mathcal{M}_k(q))$ is homocyclic of exponent e where e is the $(1,k)$ entry of the $\mathcal{H}(A_{n-1})$-form $\mathcal{N}(q,\ldots,q_{n-1})$.*

It is natural to extend the above arguments to more general incidence maps from, say from i-flats to j-flats, or to other buildings. For example, one may consider the algebra generated by $\{P_{\{i\}} | i \in I\}$ acting on the $\mathbb{Z}$-span $\mathcal{T}$ of $\{\operatorname{Im} P_{\{i\}} | i \in I\}$. This is almost the incidence algebra of the associated uniform poset in the sense of Terwilliger [13], so the spectral nature of these incidence algebras may also be studied using the $\mathbb{C}$-representations of $\mathcal{H}$. If the coefficient ring is only localized at a prime dividing an index parameter, then $\mathcal{T}$ a summand of standard module. In general, $\mathcal{T}$ is a pure submodule of $\mathbb{Z}\mathcal{C}h$ and therefore its direct sum decomposition as $\mathbb{Z}$-forms exhibits each of the geometrically significant eigenpotents $P_{\{i\}}$ in a block diagonal form over $\mathbb{Z}$. Because $P_{\{i\}}$ is rank one in each relevant representation, each of the level schemes is what Terwilliger calls "thin" and no blocks are bigger than 1 by 1. This means that all incidence maps are simultaneously in a diagonal form over $\mathbb{Z}$ and all important information conveyed by their Smith normal form is visible from the direct sum decomposition of $\mathbb{Z}\mathcal{T}$ as $\mathbb{Z}$-forms. One serious difficulty in this enterprise seems to be finding the relevant $\mathbb{Z}$-forms.

From the nature of the $\mathbb{Z}$-forms on other pure submodules of $\mathbb{Z}\mathcal{C}h$ and their multiplicities (whatever that means), one can compute a variety of additional arithmetic invariants of the building beyond incidence map invariant factors. Moreover much of the above machinery also applies to finite Tits geometries of "type M". So there is some hope that these additional arithmetic invariants might help resolve the celebrated question of existence of non-building Tits geometries of type B_3.

§4. Incidence matrices and finite local rings

This section is concerned with the multiplicities of powers of p as elementary divisors of the incidence matrices $\mathcal{M}_{n-k}(p^d)$. The main tools are finite local rings and the discrete Fourier transform.

Here is one (not particularly standard) way of constructing the finite field $GF(p^m)$. Let ζ be primitive a complex $p^m - 1$-th root of unity. The integral domain $\mathbb{Z}[\zeta] \leq \mathbb{C}$ of $\mathbb{Z}$-linear combinations of powers of ζ is called a ring of *Cyclotomic Integers* and is a basic construct of algebraic number theory. Although $\mathbb{Z}[\zeta]$ is not a principal ideal domain, its ideal structure is well understood. Any prime ideal π of $\mathbb{Z}[\zeta]$ that contains (p) has the form $(p, f(\zeta))$, where $f(x) \in \mathbb{Z}[x]$ is congruent modulo p to an irreducible polynomial of degree m in $GF(p)[x]$. Since the quotient ring $\mathbb{Z}[\zeta]/\pi$ is an integral domain of order p^m, it must be $GF(p^m)$.

The finite local rings are most naturally constructed by considering $\mathbb{Z}[\zeta]/(\pi)^s$ instead. We record the basic facts about these rings.

Theorem 4.1. *Let $p \in \mathbb{N}$ be a prime, ζ a primitive complex $(p^m - 1)$-th root of unity. Let $f(x) \in \mathbb{Z}[x]$ be an integral polynomial whose reduction modulo (p) is irreducible of degree m. (For $m = 0$, set $\zeta = 1$ and $f = 0$.)*

1. *Then $\pi := (p, f(\zeta))$ is a prime ideal of $\mathbb{Z}[\zeta]$ over (p).*
2. *Then the ring $R_s := \mathbb{Z}[\zeta]/\pi^s$ has order p^{ms} and characteristic p^s.*
3. *The multiplicative group $R_s^\star$ of R_s contains $\langle\zeta\rangle$ and $1 + r\pi$ for all $r \in R$.*
4. *$R_s^\star$ consists of all elements of R_s not in π and is of exponent $p^s(p^m - 1)$.*
5. *The ring R_s is a local ring.*

The basic idea of the method of Brouwer is to present the incidence matrix to be studied as the table of values of a function in two variables. Then one uses a finite Fourier transform to substitute the coefficient matrix for the incidence matrix.

Lemma 4.2 (cf. [2]). *Let U be a cyclic multiplicative group of order u in the commutative ring $\mathcal{R}$. For $X \subseteq U$, let V_X denote a Vandermonde matrix with rows indexed by $x \in X$ with x-th row consists of the successive powers $1, x, x^2, \ldots, x^{u-1}$ of x. Suppose $p(x, y) = \sum\sum c_{ij} x^i y^j$, is a polynomial function with coefficients in $\mathcal{R}$ of x-degree* *and y-degree less than u and C the u by u matrix of coefficients of $p(x,y)$. Then for $A, B \subset U$, the matrix of values of*

$$M := (p(a,b))_{a\in A\ b\in B} \text{ is given by } M = V_A C V_B^t.$$

In particular M and C are equivalent whenever V_A and V_B possess right-inverses having coefficients in $\mathcal{R}$,

Proof. Just multiply out the right hand side. Q.E.D.

Adopt the notation of Theorem 4.1, so ζ is a primitive complex $(p^m - 1)$-th root of unity, π is a prime ideal of $\mathbb{Z}[\zeta]$ over (p) and $R_s := \mathbb{Z}[\zeta]/\pi^s$ is a finite local ring of order p^{ms} and characteristic p^s.

We intend to apply Lemma 4.2 with $\mathcal{R} = R_s$, and M one of the incidence matrices $\mathcal{M}_k(p^e)$. In view of Theorem 4.1, the most natural choice for U is perhaps a maximal cyclic subgroup of $R_s^\star$, but then V_U does not have a right inverse defined over R_s. If one chooses $U \le R_s^\star$ small enough for V_A and V_B to have right inverses over R_s, then one is forced to deal with polynomial function $p(x,y)$ of uncomfortably small degree. Either way, one is led to the same results. We choose to present the later line of argument because it avoids explicit computation of the Smith normal form of the character table of a cyclic p-group as appears in [1].

Suppose $m = ef$, and $r = p^e$, define the function:

$$\mathrm{tr}_r(z) := z + z^r + \cdots + z^{r^{f-1}}; \quad z \in U := \langle\zeta\rangle.$$

Observe $\mathrm{tr}_r(z) \in \pi$ if and only if z is in the kernel of the trace map from the field R_s/π to $E := GF(r)$. This trace map gives rise to the nondegenerate symmetric bilinear form on the E-vector space R_s/π given by $(x,y) = \mathrm{tr}_r(xy)$.

Organize the elements of U into cosets of the subgroup $E^\star$ of order $(r-1)$ and consider the matrix M whose rows and columns are labelled by the elements of U in this order and whose x, y entry is $\mathrm{tr}_r(xy)$. Then the blocks of this matrix can be labelled with the points and hyperplanes of $PG_{f-1}(r)$ in such a way that the point labelled by $\bar{x}$ is incident with the hyperplane $\bar{y}$ if and only if some entry of the $(\bar{x},\bar{y})$ block of M is in π. This occurs if and only if all entries of the $(\bar{x},\bar{y})$ block of M are in π. Since $\mathrm{Im}(\mathrm{tr}_r)/\pi \le E$, $M^{\circ(r-1)} \pmod{\pi}$ is a zero one matrix (here $\circ$ denotes the Schur, or termwise, product). And, in fact,

$$M^{\circ(r-1)} \equiv J_{p^m-1} - \mathcal{M}_{f-1}(r) \otimes J_{r-1} \pmod{\pi},$$

where J denotes the appropriate matrix of all ones, $\otimes$ denotes Kronecker product of matrices, and $\mathcal{M}_{f-1}(r)$ a point-hyperplane incidence matrix of $PG_{f-1}(r)$ as above.

By Theorem 4.1.5 R_s is a local ring and all of its elements not in π are units, so this also implies:

$$M^{\circ(r-1)p^s} \equiv J_{p^n-1} - \mathcal{M}_{f-1}(r) \otimes J_{r-1} \pmod{\pi^s}.$$

This equation is sufficient to study the point-hyperplane matrix $\mathcal{M}_{f-1}(r)$ because left hand side is the table of values of the polynomial function $(\mathrm{tr}_r(xy))^{(r-1)p^s}$.

But in order to deal with the matrices $\mathcal{M}_{k-1}(q)$, we need to take R_s/π to be much larger than the underlying vector space and replace the field E with two fields.

Let $d = \gcd(e, f)$, and let $e = dk, f = nd$ define k and n. Set $q = p^d$, so $r = p^e = q^k$. Let $F^\star \leq L^\star$ be the subgroups of U having order $q^n - 1$, $r^n - 1$, respectively. Then, modulo π, the groups $L^\star$, $F^\star$, $E^\star$ and $F^\star \cap E^\star$ are the multiplicative groups of fields having like names (without the *) and isomorphic to $GF(r^n) \geq GF(q^n)$, $GF(r) \geq GF(q)$, respectively. We collect some required geometric facts in a lemma.

Lemma 4.3.

1. *Any $E \cap F$-subspace $W \leq F$ generates an E-subspace EW and $EW \cap F = W$. Moreover $\dim_{E\cap F} W = \dim_E EW$.*
2. *Suppose V is an E-hyperplane in R_s/π. Then $L \cap V$ is an $E \cap F$-subspace containing E and of codimension less than or equal to k in F.*
3. *Conversely, if $W \leq F$, has $E \cap F$-codimension less than or equal to k then $W = F \cap V$ for some E-hyperplane V in R_s/π.*

Proof. Part 1 follows from the fact that k and n are relatively prime. Of course an E-hyperplane has $E \cap F$-codimension $k = [E : E \cap F]$ in R_s/π, so Part 2 is also clear. Finally, Part 1 implies that EW is and E-subspace of L having like codimension, from which Part 3 follows. Q.E.D.

Recall that the matrix M has blocks of size $r - 1$ and the blocks of this matrix can be labelled with the points and hyperplanes of $PG_{f-1}(r)$ in such a way that the point labelled by $\bar{x}$ is incident with the hyperplane $\bar{y}$ if and only if all entries of the $(\bar{x}, \bar{y})$ block of M are in π. Let M_F be the submatrix of M with rows labelled by elements of $F^\star$. Then

$$M_F^{\circ(r-1)} \equiv J - A_F \otimes J_r \pmod{\pi},$$

where A_F is a zero-one matrix whose columns are the characteristic functions of $F \cap V$ where V is an E-hyperplane in R_s/π. By Lemma 4.3, the column space of A_F is the R_s-span of (the characteristic vectors of) the $E \cap F$-subspaces of codimension less than or equal to k in F. By Lemma 3.4.2, the R_s-incidence map from $\mathcal{P}_1$ to $\mathcal{P}_{n-j}$ factors through the incidence map from $\mathcal{P}_1$ to $\mathcal{P}_{n-k}$, whenever $k \geq j$. Therefore the R_s-column space of A_F is the R_s-module spanned by the columns of $\mathcal{M}_{n-k}(q) \otimes J_r$.

Again, since R_s is a local ring, this also implies:

$$M_F^{\circ(r-1)p^s} \equiv J - A_L \otimes J_r \pmod{\pi^s}. \tag{4}$$

Now M_F is just the table of values of the function $(\mathrm{tr}_{q^k}(xy))^{(q^k-1)p^s}$ for $x \in F^\star$, $y \in U$. Unfortunately the degree of this polynomial is too high to apply Lemma 4.2 directly.

Proposition 4.4. *Suppose n and k are relatively prime and $q = p^d$. Let C be the coefficient matrix of $1 - f(x,y)$ where*

$$f(x,y) \equiv (\mathrm{tr}_{q^k}(xy))^{(q^k-1)p^s} \quad \mathrm{mod}\ (x^{q^n-1}-1, y^{q^{nkd}-1}-1)$$

has x-degree $\leq q^n - 2$ and y degree $\leq q^{nkd} - 2$. Then $\mathcal{M}_{n-k}(q)$ has the same non-zero R_s-elementary divisors as C.

Proof. By definition of $F^\star$ and U, the two polynomials take exactly the same values for $x \in F^\star$, $y \in U$. Lemma 4.2, Equation 4 and the fact that the Vandermonde matrix V_U is the character table of the group U having order not divisible by p, imply that $\mathcal{M}_{n-k}(q) \otimes J_{q^k-1}$ and C are R_s-equivalent. The result follows from the fact that J_{q^k-1} has rank 1 and that $q^k - 1$ is a unit in R_s. Q.E.D.

Corollary 4.5. *Suppose n and k are relatively prime and $q = p^d$. Set $p_0 = 1$ and for $0 \leq i \leq q^n - 2$, define $d_i = \gcd\{p_j | j \equiv i \pmod{q^n-1}\}$, where p_j is the multinomial coefficient sum:*

$$p_j := \sum_{\sum r_\alpha q^{k\alpha} \equiv j \pmod{q^{nkd}-1}} \binom{(q^k-1)p^s}{r_0, r_1, \ldots}.$$

Then $\mathcal{M}_{n-k}(q)$ has an R_s-diagonal form $D := \mathrm{diag}\{1, d_i\}$. In particular, p^d , $d < s$ occurs as an elementary divisor over $\mathbb{Z}$ to like multiplicity in $\mathcal{M}_{n-k}(q)$ and in D.

Proof. The coefficient matrix C of $(\mathrm{tr}_{q^k}(xy))^{(q^k-1)p^s}$ is diagonal since each term in the expansion of this expression has like degree in x

and y. Moreover $c_{jj} \equiv p_j \pmod{(xy)^{q^{nkd}-1} - 1}$. Since $q^n - 1$ divides $q^{nkd} - 1$, the coefficient matrix of $f(x, y) - 1$ appearing in Proposition 4.4 is

$$\left(\begin{array}{cccc|ccc|ccc} -1 & & & & p_{q^n-1} & & & p_{q^{nkd}-q^n-1} & & \\ & p_1 & & & & \ddots & & & \ddots & \\ & & \ddots & & & & \ddots & & & \ddots \\ & & & p_{q^n-2} & & & & & & p_{q^{nkd}-2} \end{array}\right).$$

Since each column has only one nonzero entry, the result follows from permuting the columns so those having nonzero in a given row are adjacent. Q.E.D.

The actual multiplicities of p^k as an elementary divisor of $\mathcal{M}_{n-1}$ arising from this formula seem to be difficult to compute. Thanks to Maple, here are some numerical results with new values in **boldface**:

	1	p	p^2	p^3	p^4	p^5	p^6
$PG_2(4)$	9	2	9				
$PG_3(4)$	16	**8**	**36**	**8**	16		
$PG_4(4)$	25	**20**	**100**	**50**	**100**	**20**	25
$PG_5(4)$	36	**40**	**225**	**180**	**402**	**180**	**225**
$PG_6(4)$	49	**70**	**441**	**490**	**1239**	**882**	**1239**
$PG_2(8)$	27	9	9	27			
$PG_3(8)$	64	**48**	**72**	**216**	**72**	**48**	64
$PG_4(8)$	125	**150**	**400**	**1015**	**750**	**750**	**1015**
$PG_2(9)$	36	8	36				
$PG_3(9)$	100	**128**	**363**	**128**	100		
$PG_4(9)$	225	**510**	**2055**	**1800**	**2055**	**510**	225

References

[1] S. C. Black and R. J. List, On certain Abelian groups associated with finite projective geometries, Geom. Dedicata, **33** (1990), 13–19.

[2] A. E. Brouwer and H. Wilbrink, Block designs, in "The Handbook of Incidence Geometries", (F. Buekenhout, ed.), North-Holland, 1994.

[3] C. W. Curtis, N. Iwahori and R. Kilmoyer, Hecke algebras and characters of parabolic type of finite groups with (B,N)-pairs, Inst. Hautes Études Sci. Publ. Math., **40** (1972), 81–116.

[4] C. W. Curtis and I. Reiner, Methods of Representation Theory, J. Wiley, New York, 1987.

[5] A. Frumkin and A. Yakir, Rank of inclusion matrices and modular representaion theory, Israel J. Math., **71** (1990), 309–320.

[6] N. Hamada, The rank of the incidence matrix of points and d-flats in finite geometries, J. Sci. Hiroshima Univ. Ser A-1, **32** (1968), 381–396.

[7] P. N. Hoefsmit, Representations of Hecke algebras of finite groups with BN-pairs of classical type, Ph. D. Thesis, Univ. British Columbia, 1974.

[8] R. Howlet and G. Lehrer, Representations of generic algebras of finite groups of Lie type, Trans. Amer. Math. Soc., **280** (1983), 753–777.

[9] N. Iwahori, On the structure of the Hecke ring of a Chevalley group over a finite field, J. Fac. Sci. Univ. Tokyo, **10** (1964), 215–236.

[10] E. S. Lander, "Symmetric Designs: an Algebraic Approach", London Math. Soc. Lecture Notes **74**, Cambridge Univ Press, 1983.

[11] R. A. Liebler, A representation theoretic appoach to finite geometries of spherical type, (1985), unpublished.

[12] K. J. C. Smith, On the p-rank of the incidence matrix of points and hyperplanes in a finite geometry, J. Combin. Theory, **7** (1969), 122–129.

[13] P. Terwilliger, The incidence algebra of a uniform poset, in "Coding Theory and Design Theory part I: Coding Theory", IMA volumes in Mathematics and its applications, Vol. 20, Springer, New York, 1990, pp. 193–212.

Department of Mathematics
Colorado State University
Fort Collins, Colorado 80523
U.S.A.