THE UNIVERSITY OF CHICAGO

FACTORING CARTAN MATRICES OF GROUP ALGEBRAS

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY
BRIAN W. JOHNSON

CHICAGO, ILLINOIS
AUGUST 2003

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The Cartan matrix of a group algebra generally contains incomplete information about the decomposition numbers. For the groups $\mathrm{SL}(2, q)$, we show that the information in the Cartan matrix, along with knowledge that every decomposition number is either zero or one, is sufficient to recover the complete decomposition matrix. In the process of proving this, we obtain a new combinatorial description of the decomposition numbers.

ACKNOWLEDGEMENTS

I would like to thank Shahriar Shahriari for getting me interested in group theory as an undergraduate, Jon Alperin for proposing this problem and for much advice and encouragement, and Bhama Srinivasan for several helpful conversations.

CHAPTER 1
INTRODUCTION

1.1 Motivation

There are two main directions to go in determining the representation theory of a finite group G. First, we can examine the group algebra $\mathbb{C}G$ over the complex numbers. Since this algebra is semisimple, its structure is not very hard to determine. In fact, we can consult the Atlas [5] to find character tables of some impressively large groups. If we wish to construct the irreducible representations ourselves, we have a wide array of techniques at our disposal; for instance, we can lift representations from quotients, induce from subgroups, take tensor products of representations with each other, compute symmetric or alternating powers, and look for permutation characters of natural actions of G. Once the irreducible characters are constructed, we have a complete description of the algebra $\mathbb{C}G$.[1]

Now let k be an algebraically closed field of prime characteristic p. We can also ask for the representation theory of the algebra kG, which is not semisimple. This presents considerable difficulties: not only are the "modular" irreducibles usually harder to construct (owing to the lack of a natural inner product on the ring of Brauer characters), but there is also much additional structure in the algebra kG. We might wish to construct the projective indecomposable modules (PIMs), decompose the algebra into blocks, find the dimensions of various Ext groups, calculate the Cartan matrix of the algebra, determine the full submodule lattices of the PIMs, find projective resolutions for the irreducibles, and so on. Since the algebra $\mathbb{C}G$ is much easier to analyze, it seems natural to use our knowledge of $\mathbb{C}G$ as a guide to

[1] $\mathbb{C}G$ is always a direct sum of complete matrix algebras over $\mathbb{C}$, where the sizes of the matrices correspond to the character degrees. Knowing the character values is roughly equivalent to knowing how the *group* acts.

determining the (possibly very complicated) structure of kG. Indeed, we can often determine a substantial amount of information about the p-blocks of G from the character table.

In this exposition, we are going to do the exact opposite. We will assume we can determine some information about the algebra kG, and ask how we can pin down the structure of $\mathbb{C}G$. In particular, we will assume we have a good description of the irreducibles, p-blocks, and Cartan invariants of kG, and our goal will be to construct the decomposition matrix D. We will primarily be interested in the groups $G = \mathrm{SL}(2, p^n)$, but we begin with a few motivating examples. Let $G = \mathrm{Alt}(4)$ and $p = 2$. The Cartan matrix of kG is:

$$C = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

Since $D^{\top} D = C$, we can attempt to "reverse engineer" D using our knowledge of C. We know that the entries of D are nonnegative integers, and if we ignore arbitrary permutations of the rows of D, and disallow a row of all zeros, we easily see that there are a priori two possibilities for the decomposition matrix:

$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \text{or} \qquad D = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

The second possibility is quickly eliminated; for instance, the number of ordinary irreducibles must be greater than the number of modular irreducibles whenever p divides $|G|$, which means the decomposition matrix can't be square. (There also must be a row corresponding to the trivial module.) Now that the decomposition matrix is known, one could multiply it by the table of irreducible Brauer characters to obtain the character table of G on p'-elements. Since there is a unique class of elements of even order in $\mathrm{Alt}(4)$, we could fill in the remainder of the character table using row orthogonality. So, for this group and prime, the structure of kG very tightly constrains the structure of $\mathbb{C}G$.

For a more complicated example, let $G = M_{11}$ and $p = 3$. From the Cartan matrix, one can again try to deduce the decomposition matrix using the equation $D^{\mathsf{T}}D = C$. In this case, we obtain a *unique* result for D, despite the apparent complexity of C:

$$C = \begin{bmatrix} 5 & 3 & 3 & 0 & 2 & 2 & 1 & 0 \\ 3 & 4 & 3 & 1 & 1 & 2 & 2 & 0 \\ 3 & 3 & 4 & 1 & 2 & 1 & 2 & 0 \\ 0 & 1 & 1 & 2 & 0 & 0 & 1 & 0 \\ 2 & 1 & 2 & 0 & 3 & 1 & 1 & 0 \\ 2 & 2 & 1 & 0 & 1 & 3 & 1 & 0 \\ 1 & 2 & 2 & 1 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \qquad D = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

In fact, for many simple or almost simple groups of small order, it seems to be the case that C uniquely determines D in this way. An interesting exception is $\mathrm{Alt}(5) \cong \mathrm{SL}(2,4)$ for the prime 2, which we remark on in the following chapter.

Now let G be a p-group. kG has one irreducible module and one p-block (which is indecomposable as a module over itself), and the Cartan matrix of kG is the one by one matrix $[\,|G|\,]$. Since the decomposition matrix is a list of the character degrees, it is clear that we cannot determine much about D from the Cartan matrix. We could allow more information about kG – for instance, knowing the submodule lattice of kG is equivalent, by work of Jennings, to knowing the order of certain structural subgroups of G. But even this isn't enough to determine the decomposition matrix of G, since these subgroups sometimes have the same orders for groups with quite different character tables – for instance, $C_4 \times C_2$ and D_8. So, in some cases, rather detailed knowledge of the structure of kG tells us very little about $\mathbb{C}G$.

For a final example, suppose B is a cyclic block of kG with Cartan matrix C. The following result shows that the decomposition matrix of the block can often be determined using only the matrix equation $D^\top D = C$:

Proposition 1. Suppose the Brauer tree of B has no exceptional vertex, and is not a star with three edges. Then there is a unique nonnegative integer matrix D, up to a permutation of rows, such that D has no zero row and $D^\top D = C$.

Proof. See the Appendix. □

Our main result is that the decomposition matrix D can be recovered from the Cartan matrix C when $G = \mathrm{SL}(2, p^n)$. In this case, we will show that the matrix equation $D^\top D = C$, together with the knowledge that every decomposition number is zero or one, suffices to determine D. In the course of proving this result, we will obtain new combinatorial descriptions of the decomposition matrix of G, and a new description of the Cartan matrix of G for odd p. These descriptions of D and C have geometric interpretations as collections of unit n-cubes in $\mathbb{R}^n$.

1.2 Notation

Let p be a prime and n a positive integer; for convenience, let $q = p^n$. Let $G = \mathrm{SL}(2, q)$. In most of what follows, we will not deal with the case $n = 1$; so we may as well streamline the exposition and require now that $n \geq 2$. Let k an algebraically closed field of characteristic p. Let σ be the Frobenius automorphism of k over its prime field, so $\sigma(x) = x^p$. Note that $\mathbb{F}_q$ is the fixed field of σ^n.

Brauer and Nesbitt first described the simple kG-modules in [2]. Let V_i be the i-dimensional module obtained by letting G act on homogeneous polynomials of degree $i - 1$ in $k[x, y]$.[2] V_i is a simple module iff $1 \leq i \leq p$. For any kG-module M, let M^σ be the module obtained by precomposing the action of G on M with σ; that is, M^σ

[2] In some expositions, including [1] and [4], it is more convenient to let V_i be the $(i+1)$-dimensional module obtained by letting G act on homogeneous polynomials of degree i. Our choice of convention will lead to simpler formulas in chapter 3.

is the “Frobenius twist” of M. Since σ induces an automorphism of G, the modules $V_i^{\sigma^j}$ are simple for $1 \leq i \leq p$. Furthermore, σ has order n on G, so we may take $0 \leq j \leq n-1$ with no loss of generality.

Let $J \in \{1, \ldots, p\}^n$, and let J_i be the i-th component of this vector. Brauer and Nesbitt's result is that the modules

$$V_J = \bigotimes_{i=1}^{n} (V_{J_i})^{\sigma^{i-1}}$$

form a complete set of irreducible kG-modules. (This also follows from the Steinberg tensor product theorem.) Note that the dimension of V_J is $\prod_{i=1}^n J_i$. The module obtained for $J = (p, \ldots, p)$ is called the Steinberg module. It is projective, and its character (plus the trivial character) is the doubly transitive permutation character of the action of G on one dimensional subspaces of k^n. When q is even, all other simple kG-modules fall into the principal block. If q is odd, then there are two other blocks, and which block V_J belongs to is determined by the parity of $\sum_{i=1}^n J_i$. In this case, we will sometimes refer to the principal and nonprincipal blocks of kG, even though the Steinberg module is technically another nonprincipal block.

If M is a simple kG-module, let P_M be its projective cover. For any set A, we let $\mathcal{P}(A)$ denote the power set of A, and A^m the Cartesian product of m copies of A. For $B \subseteq A$, $A \setminus B$ is the difference of the two sets. If X is a matrix, then $X^\top$ is the transpose of X. Finally, C_n, D_{2n}, $\mathrm{Sym}(n)$, and $\mathrm{Alt}(n)$ are the cyclic group of order n, the dihedral group of order $2n$, and the symmetric and alternating groups on n symbols, respectively.

Finally, unless otherwise indicated, the letters D and C denote the decomposition and Cartan matrices, respectively, of G in defining characteristic. We caution those not familiar with modular representation theory that C is *not* a Cartan matrix in the sense of Lie algebras. Its rows and columns are indexed by the irreducible kG-modules, and its M, N entry is $c_{MN} = \dim \mathrm{Hom}(P_M, P_N)$, which is the number of times M occurs as a composition factor of P_N.

CHAPTER 2
EVEN CHARACTERISTIC

If k has characteristic 2, then the simple kG-modules are parametrized by elements of $\{1,2\}^n$. We will identify an element of this set with a subset of $N = \{1, \ldots, n\}$, where the subset corresponding to $\mathbf{x} = (x_1, \ldots, x_n) \in \{1,2\}^n$ is $\{i \in N \mid x_i = 2\}$. Thus, we have 2^n simples $\{V_I \mid I \subseteq N\}$, where $V_\varnothing$ is the trivial module, V_N is the Steinberg module, and $\dim V_I = 2^{|I|}$. We will always think of arithmetic on elements of N as happening in $\mathbb{Z}/n\mathbb{Z}$, so that we have (for instance) ${V_I}^\sigma = V_{I+1}$.

2.1 The Cartan Matrix

In [1], Alperin gives a concise combinatorial description of the Cartan invariants c_{IJ} of kG. In stating that result, it is convenient to introduce a symmetric relation on subsets of N.

Definition 2. Subsets $I, J \subseteq N$ are *compatible* iff, whenever $i \in I \cap J$, then either $i+1 \in I \cap J$ or $i+1 \notin I \cup J$. As an exception, we require that $\varnothing$ and N are *not* compatible. We will write $I \sim J$ when I and J are compatible, and $I \nsim J$ otherwise.

Thus, I and J are compatible iff, whenever maximal sequences of consecutive elements of I and J have a nonempty intersection, those sequences end at the same element of N. For instance, if $n = 6$, we have $\{1,2,3,4\} \nsim \{3,4,5\}$, and $\{2,4\} \sim \{1,2,4,6\}$.[1]

With this notation, Alperin's result is:

$$c_{IJ} = \begin{cases} 2^{n-|I \cup J|} & \text{if } I \sim J \\ 0 & \text{if } I \nsim J. \end{cases}$$

[1] Since we are thinking of arithmetic in N as happening in $\mathbb{Z}/n\mathbb{Z}$, $\{6,1,2\}$ is a maximal sequence of consecutive elements in $\{1,2,4,6\}$.

C	$\varnothing$	1	2	3	12	13	23	123
$\varnothing$	8	4	4	4	2	2	2	0
1	4	4	2	2	0	2	1	0
2	4	2	4	2	2	1	0	0
3	4	2	2	4	1	0	2	0
12	2	0	2	1	2	0	0	0
13	2	2	1	0	0	2	0	0
23	2	1	0	2	0	0	2	0
123	0	0	0	0	0	0	0	1

Figure 2.1: The matrix C for $n = 3$

2.2 Factoring C: Statement of Results

It would also be desirable to have a concise combinatorial description of D, the decomposition matrix. Previous attempts to do so have relied on some knowledge of the $\mathbb{C}G$-modules; this is reasonable, since the decomposition matrix describes relationships between $\mathbb{C}G$-modules and kG-modules. In particular, this is the route taken by Srinivasan (for q odd) [12], Burkhardt [3], and van Ham, Springer, and van der Wel [6], all of whom obtain varying amounts of information about D. The results obtained in [6], which also include a description of the Cartan matrix (for all q), are particularly noteworthy for being extremely complicated.

In contrast, we will follow the route indicated in the introduction, using the matrix equation $D^{\top}D = C$ to "work backwards" from the combinatorial description of C above. We will show that this matrix equation basically determines a unique matrix D. Furthermore, once D is determined, it would be possible to write down the character table of G without ever having constructed a $\mathbb{C}G$-module. Our main result is:

Main Theorem. There is a unique nonnegative integer matrix M, up to a permutation of rows, such that:

1. Every entry is a zero or one,

2. Every row contains a nonzero entry, and

3. $M^{\mathsf{T}}M = C$.

At the end of this chapter, we will indicate how the hypothesis that the entries are zero or one can be lifted from this theorem. However, we need the result in the form stated above for use in the following chapter, because we will be able to weaken the hypothesis that $M^{\mathsf{T}}M = C$. Moreover, it is not difficult to show that the actual decomposition matrix D has the required properties:

Proposition 3. D satisfies conditions 1–3 of the theorem.

Proof. Properties 2 and 3 are obvious, so we must show that every decomposition number is a zero or one. Suppose for the moment that every decomposition number in column $\varnothing$ is a zero or one. If I is any proper subset of N, then $\varnothing \sim I$, so:

$$2^{n-|I|} = c_{\varnothing I} = \sum_{\chi \in \mathrm{Irr}(G)} d_{\chi\varnothing} d_{\chi I} \leq \sum_{\chi \in \mathrm{Irr}(G)} d_{\chi I} \leq \sum_{\chi \in \mathrm{Irr}(G)} d_{\chi I}^2 = c_{II} = 2^{n-|I|}.$$

Therefore we have equality throughout. In particular, $\sum d_{\chi I} = \sum d_{\chi I}^2$, which implies that every decomposition number in column I is a zero or one. Finally, since $c_{NN} = 1$, it is clear that the decomposition numbers in column N are all zero or one. Therefore, it suffices to show that every decomposition number in column $\varnothing$ is a zero or one, i.e., that the complex character of $P_\varnothing$ is a sum of ordinary irreducible characters, each with multiplicity one.

By Schur's Lemma, $\mathrm{End}_{\mathbb{C}G}(P_\varnothing)$ is a direct sum of complete matrix algebras over $\mathbb{C}$, each with dimension equal to the multiplicity of an irreducible character as a constituent of $P_\varnothing$. Consequently, this endomorphism algebra is commutative if and only if the irreducibles all appear with multiplicity zero or one in $P_\varnothing$. We will now show that $\mathrm{End}_{\mathbb{C}G}(P_\varnothing)$ is commutative, using an elementary Hecke algebra argument.[2]

Let H be a cyclic subgroup of order 2^n+1 in G. We claim that $P_\varnothing \cong 1_H{\uparrow}^G$ as $\mathbb{C}G$-modules. Since H is a $2'$-subgroup of G, 1_H is projective as a kH-module. Induction preserves projectives, so $1_H{\uparrow}^G$ is a projective kG-module. By Frobenius reciprocity,

[2] I thank Prof. Alperin for pointing out this well-known argument.

$\mathrm{Hom}_{kG}(1_H{\uparrow}^G, 1_G) \cong \mathrm{Hom}_{kG}(1_H, 1_G{\downarrow}_H) \cong k$; so $1_H{\uparrow}^G$ has $P_\varnothing$ as a direct summand. To show that there are no other summands, we check that $\dim 1_H{\uparrow}^G = \dim P_\varnothing$.

Clearly, we have $\dim 1_H{\uparrow}^G = |G : H| = 2^n(2^n - 1)$. We can compute $\dim P_\varnothing$ using Alperin's description of the Cartan invariants. Since each composition factor V_I of $P_\varnothing$ has dimension $2^{|I|}$ and appears with multiplicity $c_{\varnothing I}$, we calculate:

$$\dim P_\varnothing = \sum_{I \subseteq N} 2^{|I|} c_{\varnothing I} = \sum_{I \subsetneq N} 2^{|I|} 2^{n-|I|} = 2^n(2^n - 1).$$

Therefore $\dim 1_H{\uparrow}^G = \dim P_\varnothing$, and we have $P_\varnothing \cong 1_H{\uparrow}^G$ as kG-modules. Since the modules are projective, $P_\varnothing \cong 1_H{\uparrow}^G$ as $\mathbb{C}G$-modules as well.

To establish the proposition, we must show that $\mathrm{End}_{\mathbb{C}G}(1_H{\uparrow}^G)$ is commutative. This endomorphism algebra is isomorphic to the subalgebra of $\mathbb{C}G$ spanned by the double coset sums $\sum_{g \in HxH} g$. We claim that each double coset HxH contains either the identity or an involution. Clearly, H itself contains the identity, and no involutions. H has index 2 in its normalizer, which is dihedral; so there are 2^n+1 involutions in $N(H) \setminus H$. Now, suppose a left coset $xH \nsubseteq N(H)$ contains two involutions, y and z. Then $yh = z$ for some $h \in H$, and $1 = z^2 = (yh)^2 = h^y h^{-1}$, so $h^y = h$. But $y \notin N(H)$, a contradiction. Therefore, each left coset xH not in $N(H)$ contains at most one involution.

But $G \setminus N(H)$ consists of $|G : H| - 2 = 2^n(2^n - 1) - 2 = 2^{2n} - 2^n - 2$ left cosets, and G has a total of $(2^n - 1)(2^n + 1) = 2^{2n} - 1$ involutions, of which $2^n + 1$ have already been accounted for in $N(H)$. This leaves $2^{2n} - 2^n - 2$ involutions, which means each remaining left coset must have exactly one involution. Thus, each double coset HxH contains the identity or an involution. Now, the linear extension of the function $\alpha(g) = g^{-1}$ to $\mathbb{C}G$ is an anti-automorphism of $\mathbb{C}G$, and its restriction to the algebra spanned by the double coset sums gives an anti-automorphism of that algebra. But if every double coset contains a group element which is its own inverse, then α must be the identity function on double coset sums. Since the identity is an anti-automorphism, the algebra is commutative, which establishes the proposition. □

2.3 A Description of D

We now give a combinatorial description of a matrix E that satisfies the conditions of the theorem. Of course, once the theorem is proved, we will immediately conclude that E is the decomposition matrix of G. By describing E now, we will know one matrix that satisfies conditions 1–3 of the theorem. This will streamline the proof of the theorem, because any other such matrix will necessarily share certain properties with E. Our definition of E involves another binary relation on subsets of N:

Definition 4. Let $R, I \subseteq N$. R *respects* I if, whenever $i \in I$, then either $i+1 \in I$ or $i \in R$, but not both. As an exception, we require that $\varnothing$ does not respect N. We write $R \prec I$ if R respects I, and $R \not\prec I$ otherwise.

Whenever $I \subsetneq N$, define $\operatorname{Final}(I) = \{i \in I \mid i+1 \notin I\}$. Then, for $I \neq N$, an equivalent definition is that R respects I iff $R \cap I = \operatorname{Final}(I)$. For example, if $n = 6$ again, then $\operatorname{Final}(\{1,2,4,6\}) = \{2,4\}$. Therefore, exactly four sets R respect $\{1,2,4,6\}$, namely $\{2,4\}$, $\{2,3,4\}$, $\{2,4,5\}$, and $\{2,3,4,5\}$.

Definition 5. Let E be the $2^n + 1$ by 2^n matrix with columns labeled by $\mathcal{P}(N)$, and rows labeled by $\mathcal{P}(N) \cup \{\mathrm{St}\}$. If R is a row label and I is a column label, then let the R, I entry of E be:

$$e_{RI} = \begin{cases} 1 & \text{if } R \subseteq N \text{ and } R \prec I \\ 0 & \text{if } R \subseteq N \text{ and } R \not\prec I \\ 1 & \text{if } R = \mathrm{St} \text{ and } I = N \\ 0 & \text{if } R = \mathrm{St} \text{ and } I \neq N. \end{cases}$$

Proposition 6. The matrix E satisfies conditions 1–3 of the theorem.

Proof. Clearly, E is a zero-one matrix. It's also clear that $R \prec \varnothing$ for any $R \subseteq N$, so every row has at least one nonzero entry. We must check that $E^{\top} E = C$.

E	$\varnothing$	1	2	3	12	13	23	123
$\varnothing$	1	0	0	0	0	0	0	0
1	1	1	0	0	0	1	0	0
2	1	0	1	0	1	0	0	0
3	1	0	0	1	0	0	1	0
12	1	1	1	0	0	1	0	0
13	1	1	0	1	0	0	1	0
23	1	0	1	1	1	0	0	0
123	1	1	1	1	0	0	0	0
St	0	0	0	0	0	0	0	1

Figure 2.2: The matrix E for $n = 3$

Let $I, J \subseteq N$; we will check that the I, J entry of C equals the I, J entry of $E^{\mathsf{T}}E$. For convenience, suppose $|I| \geq |J|$.[3] If $I = J = N$, then $I \sim J$ and $c_{IJ} = 1$. From the definition of $\prec$, we see that no subset $R \subseteq N$ respects N. So column N of E has a single one in row St, and thus the I, J entry of $E^{\mathsf{T}}E$ is also one.

Now suppose $I = N$ and $J \subsetneq N$. Then $I \nsim J$, so $c_{IJ} = 0$. Since no row $R \subseteq N$ respects I, columns I and J of E have no ones in common, and thus the I, J entry of $E^{\mathsf{T}}E$ is also zero.

Finally, suppose I and J are both proper in N. Then the I, J entry of $E^{\mathsf{T}}E$ is simply the number of sets $R \subseteq N$ which respect both I and J. If $I \nsim J$, then there is some $i \in N$ such that $i \in I \cap J$, but $i + 1$ is in exactly one of I and J. Without loss of generality, say $i + 1 \in I$ and $i + 1 \notin J$. Then, if R respects both I and J, we have $i \notin R$ and $i \in R$, a contradiction. So no R respects both sets, which agrees with $c_{IJ} = 0$.

Conversely, if $I \sim J$, then there is no $i \in N$ such that $i \in I \cap J$ and $i + 1$ is in exactly one of I or J. In other words, it never happens that $i \in \mathrm{Final}(I)$ but $i \in J \setminus \mathrm{Final}(J)$, or vice-versa. This implies that the set conditions $R \cap I = \mathrm{Final}(I)$ and $R \cap J = \mathrm{Final}(J)$ are not inconsistent, and so there are sets R which respect both I and J. If R is such a set, then R has uniquely determined intersections with I and

[3] Both C and $E^{\mathsf{T}}E$ are symmetric matrices, so we need only check one of the I, J and J, I entries.

J, and there are no restrictions on the other elements of R. So the number of such sets is $2^{n-|I \cup J|}$, which is c_{IJ}. This proves the proposition. $\square$

2.4 Proof of the Main Theorem

Let M be a zero-one matrix with no all-zero row, satisfying $M^{\top} M = C$. The rows and columns of C are labeled by subsets of N, so this induces a labeling of the 2^n columns of M. We will incrementally determine the structure of M, eventually concluding that it is uniquely determined by these conditions, up to a permutation of its rows.

First, $c_{\varnothing\varnothing} = 2^n$, so the column of M labeled by $\varnothing$ must consist of 2^n ones and some number of zeros. Moreover, if $I \neq N$, then $c_{\varnothing I} = c_{II} = 2^{n-|I|}$; from this, we conclude that column I shares a one with column $\varnothing$ in exactly as many rows as column I has ones. That is, every one in column I occurs in a row in which column $\varnothing$ also has a one. Therefore, only column N can have a one in a row that has a zero in column $\varnothing$. Since $c_{NN} = 1$ and $c_{\varnothing N} = 0$, we conclude that there is exactly one such row, and this row contains a one in column N and no other ones. This accounts for the unique one in column N. Since there is no zero row, the matrix M has exactly $2^n + 1$ rows; we label the 2^n rows which have a one in column $\varnothing$ with the 2^n subsets of N, and the one row with a one in column N with the symbol St. At this point, we have shown that M has the structure depicted in figure 2.3.

$$\begin{array}{c|ccccc} M & \varnothing & \varnothing \subsetneq & I & \subsetneq N & N \\ \hline \varnothing & 1 & * & \cdots & * & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ N & 1 & * & \cdots & * & 0 \\ \mathrm{St} & 0 & 0 & \cdots & 0 & 1 \end{array}$$

Figure 2.3: The matrix M after examining $c_{\varnothing I}$ and c_{NN}.

Henceforth, we will ignore row St and column N, and concentrate on the principal block of M. We inductively determine the columns of M according to the following linear order on subsets of N:

Definition 7. Let I and J be subsets of N. Then $I < J$ iff there exists a $k \in N$ such that $I \cap \{k+1, \ldots, n\} = J \cap \{k+1, \ldots, n\}$, $k \notin I$, and $k \in J$.

Thus, we have $\varnothing < \{1\} < \{2\} < \{1,2\} < \{3\} < \ldots$, and we can think of $<$ as a "binary enumerative" order on $\mathcal{P}(N)$.

We have already determined column $\varnothing$ of M, so we now let I be a proper, nontrivial subset of N, and assume by induction that any column J of M with $J < I$ has entries matching the corresponding entries of the matrix E described above. We have two cases, depending on whether $|I| > 1$ or $|I| = 1$.

Case $|I| > 1$: In this case, we will determine the entries in column I using columns $\{k\}$ and the Cartan invariants $c_{\{k\}I}$, for $k \in I$. First, observe that if $k \in I$, then $\{k\} < I$, so column $\{k\}$ of M has been uniquely determined.

For each $k \in I$, either $k+1 \in I$ or $k+1 \notin I$. If $k+1 \in I$, then columns $\{k\}$ and I are not compatible, so $c_{\{k\}I} = 0$. This implies that column I has a zero in whichever rows column $\{k\}$ has a one. Since these are exactly the rows R with $k \in R$, column I must have zeros in all rows R with $k \in R$.

Conversely, if $k+1 \notin I$, then columns $\{k\}$ and I are compatible, and $c_{\{k\}I} = 2^{n-|I|} = c_{II}$. This implies that the ones in column I are restricted to those rows where column $\{k\}$ also has a one. Thus, if column $\{k\}$ has a zero in row R, column I also has a zero on row R. Since the rows with zeros in column $\{k\}$ are exactly those rows with $k \notin R$, column I must have zeros in all rows R with $k \notin R$.

Repeating this argument for each $k \in I$, we find that column I has zeros in all rows R except those for which $R \cap I = \{k \in I \mid k+1 \notin I\}$. The number of rows satisfying this condition is $2^{n-|I|}$, which is equal to c_{II}; therefore, column I must have ones in all of the remaining $2^{n-|I|}$ rows.

This uniquely determines column I of M, and the formula in the preceding paragraph shows that this column is equal to the corresponding column of the matrix E described previously. See figure 2.4 for an example when $n = 4$.

Case $I = \{k\}$: In this case, we partition the rows R of M into sets, according to the value of the set $R \cap \{1, \ldots, k-1\}$. We will show that, within each group of rows, the column I has ones in exactly half of the rows. Since the rows of M within

	1	2	4	124
$\varnothing$	0	0	0	$\cdot$
3	0	0	0	$\cdot$
1	1	0	0	0
13	1	0	0	0
2	0	1	0	$\cdot$
23	0	1	0	$\cdot$
12	1	1	0	0
123	1	1	0	0
4	0	0	1	$\cdot$
34	0	0	1	$\cdot$
14	1	0	1	0
134	1	0	1	0
24	0	1	1	$\cdot$
234	0	1	1	$\cdot$
124	1	1	1	0
1234	1	1	1	0

$c_{\{1\},\{1,2,4\}} = 0$

	1	2	4	124
$\varnothing$	0	0	0	0
3	0	0	0	0
1	1	0	0	0
13	1	0	0	0
2	0	1	0	$\cdot$
23	0	1	0	$\cdot$
12	1	1	0	0
123	1	1	0	0
4	0	0	1	0
34	0	0	1	0
14	1	0	1	0
134	1	0	1	0
24	0	1	1	$\cdot$
234	0	1	1	$\cdot$
124	1	1	1	0
1234	1	1	1	0

$c_{\{2\},\{1,2,4\}} = 2$

	1	2	4	124
$\varnothing$	0	0	0	0
3	0	0	0	0
1	1	0	0	0
13	1	0	0	0
2	0	1	0	$\cdot$
23	0	1	0	$\cdot$
12	1	1	0	0
123	1	1	0	0
4	0	0	1	0
34	0	0	1	0
14	1	0	1	0
134	1	0	1	0
24	0	1	1	0
234	0	1	1	0
124	1	1	1	0
1234	1	1	1	0

$c_{\{4\},\{1,2,4\}} = 0$

Figure 2.4: Determining column $\{1, 2, 4\}$ of the decomposition matrix of $\mathrm{SL}(2, 2^4)$. The Cartan invariants shown force zeros in all but two rows.

each partition are equal for the columns that have been determined so far, we will make an arbitrary choice for which rows have zeros and which have ones within each group. The key observation for this strategy is:

Lemma 8. Let $k \in N$. If $J < \{k\}$, then there is a unique $R \subseteq \{1, \ldots, k-1\}$ such that $R \prec J$, but $R \not\prec K$ for any $J < K < \{k\}$.

Proof. Consider the set $R = \mathrm{Final}(J) \cup \{i \notin J \mid i < k \text{ and } i + 1 \in J\}$. Clearly, $R \cap J = \mathrm{Final}(J)$, so $R \prec J$. If $J < K < \{k\}$, then there is a unique largest element s in the symmetric difference of J and K. Since $J < K$, we must have $s \notin J$ and $s \in K$. If $s + 1 \in J$, then $s \in R$; but then we also have $s + 1 \in K$, so we conclude that $R \not\prec K$. On the other hand, if $s + 1 \notin J$, then $s \notin R$; but now $s + 1 \notin K$, and we again conclude that $R \not\prec K$. This shows that there exists an R with the given properties.

To show uniqueness, let $R \neq R' \subseteq \{1, \dots, k-1\}$. If $R' \prec J$, then $R' \cap J = \text{Final}(J)$. Let s be the largest element of the symmetric difference of R and R', so $s \notin J$. Let $K = (J \cap \{s+1, \dots, k-1\}) \cup \{s\}$. Since $s \notin J$, we have $J < K < \{k\}$. Furthermore, $s+1 \in K$ iff $s+1 \in J$ iff (by definition of R) $s \in R$ iff $s \notin R'$, which implies that $R' \prec K$. Therefore R' cannot also satisfy the conditions of the lemma, which shows that R is unique. □

It follows from the lemma that the columns J of the matrix M with $J < I = \{k\}$ have a triangular structure. Within these columns, the previously determined entries in row R depend only on $R \cap \{1, \dots, k-1\}$. As we move backwards through the ordering on columns from $\{1, \dots, k-1\}$ to $\varnothing$, each new column has ones in exactly one additional group of rows. (Figure 2.5 depicts this structure for the case $n = 4$, $k = 4$.) This triangular structure allows us to reason as follows: for each group of rows, there is an integer linear combination of various columns $J < \{k\}$ which has ones only in that group of rows. If we calculate the corresponding linear combination of Cartan invariants $c_{J\{k\}}$, we obtain the number of ones in column $\{k\}$ which are in the given group of rows. But we already know one matrix, E, which satisfies the conditions of the theorem; so instead of actually calculating this linear combination of Cartan invariants, we can simply look at column $\{k\}$ of E to see what the number of ones in this group of rows must be. Each group of rows contains an equal number of rows containing k and not containing k, so examination of E tells us that column $\{k\}$ of M must have half ones and half zeros in each group of rows.

Since the rows within each group are identical so far, the choice of which rows have zeros in column $\{k\}$ and which have ones is arbitrary, and the resulting (partially determined) matrices will be equal under a permutation of rows. Since each group consists of an equal number of rows containing k and rows not containing k, we choose to place ones in rows containing k and zeros elsewhere. Note that this choice agrees with the matrix E previously described.

This completes the proof of the main theorem. □

M	$\varnothing$	1	2	12	3	13	23	123	4
3	1	·	·	·	1	·	1	1	·
34	1	·	·	·	1	·	1	1	1
13	1	1	·	·	1	1	1	·	·
134	1	1	·	·	1	1	1	·	1
123	1	1	1	·	1	1	·	·	·
1234	1	1	1	·	1	1	·	·	1
23	1	·	1	1	1	·	·	·	·
234	1	·	1	1	1	·	·	·	1
2	1	·	1	1	·	·	·	·	·
24	1	·	1	1	·	·	·	·	1
12	1	1	1	·	·	·	·	·	·
124	1	1	1	·	·	·	·	·	1
1	1	1	·	·	·	·	·	·	·
14	1	1	·	·	·	·	·	·	1
$\varnothing$	1	·	·	·	·	·	·	·	·
4	1	·	·	·	·	·	·	·	1

Figure 2.5: Determining column $\{4\}$ of the decomposition matrix of $\mathrm{SL}(2, 2^4)$.

2.5 Observations

2.5.1 Labeling the Characters of G

As a consequence of the main theorem, the rows of the decomposition matrix, and hence the simple $\mathbb{C}G$-modules, can be labeled with subsets of N in a combinatorially meaningful way. However, we caution the reader that these labels are not defined in a unique way, because the Brauer character table of G is not uniquely defined. Even so, some of the information about these labels is still available in the character table of G. Let χ_I denote the character labeled by the subset I. If subsets I and J are cyclic permutations of each other, then it is clear that the characters χ_I and χ_J are algebraically conjugate via a lift of the Frobenius automorphism from roots of unity in $k^\times$ to roots of unity in $\mathbb{C}^\times$. Also, the parity of I is easily recovered from χ_I:

Proposition 9.

$$\chi_I(1) = \begin{cases} 2^n + (-1)^{|I|} & \text{if } I \subseteq N \text{ and } I \neq \varnothing, \\ 1 & \text{if } I = \varnothing, \text{ and} \\ 2^n & \text{if } I = \mathrm{St}. \end{cases}$$

Proof. Clearly, $\chi_\varnothing$ is the trivial character and χ_{St} is the Steinberg character, so their degrees are as indicated. If I is a nonempty subset of N, then we calculate the degree of χ_I modulo four as:

$$\chi_I(1) = \sum_{\substack{J \\ I \prec J}} 2^{|J|} = 1 + \sum_{j \in I} 2 = 1 + 2|I|.$$

Since every nontrivial character of G has degree $2^n - 1$, 2^n, or $2^n + 1$, we conclude that the degree must be $2^n + 1$ if $|I|$ is even, and $2^n - 1$ if $|I|$ is odd. □

Finally, we note that the only subsets $I \subseteq N$ which are fixed under cyclic permutations of N are $\varnothing$ and N; thus, G has at most three rational integer valued characters: $\chi_\varnothing = 1_G$, χ_N, and, of course, the Steinberg character χ_{St}.

2.5.2 Lifting the Zero-One Hypothesis

We briefly indicate an alternative proof of the main theorem which eliminates the zero-one hypothesis. However, in removing this hypothesis, we must use more data from the Cartan matrix to obtain our result. In the next chapter, we will make use of the fact that we were able to prove the main theorem only using the Cartan entries c_{IJ} with $\min(|I|, |J|) \leq 1$, so this alternative proof is somewhat less desirable.

Since the combinatorics is conceptually easy but notationally difficult to describe, we indicate the idea of the proof for the case $n = 3$; as we will see, the general case is completely analogous. We begin by writing the matrix E with rows and columns in the same order as in figure 2.5, ignoring the block corresponding to the Steinberg representation:

E	$\varnothing$	1	2	12	3	13	23
2	1	·	1	1	·	·	·
23	1	·	1	1	1	·	·
12	1	1	1	·	·	1	·
123	1	1	1	·	1	·	·
1	1	1	·	·	·	1	·
13	1	1	·	·	1	·	1
$\varnothing$	1	·	·	·	·	·	·
3	1	·	·	·	1	·	1

We will deduce the entries of E, using only Cartan invariants. In light of the discussion earlier in this chapter, it suffices to show that column $\varnothing$ consists entirely of ones, because this implies that the entire matrix has no entry greater than one. At that point, we can invoke the prior proof of the main theorem.

We work backwards through the columns, starting at column 12. Whenever we have an arbitrary choice for which entries of E have zeros or ones, we will always choose so that our partially completed matrix agrees with E. Since $c_{12,12} = 2$, column 12 has two ones, which we place in rows 2 and 23. $c_{2,12} = 2$, so the entries in column 2 in those rows must either be two ones, or a two and a zero. However, $c_{2,13} = 1$ and $c_{12,13} = 0$, so column 2 must have a nonzero entry (in fact, a one) in some row other than rows 2 and 23. Since $c_{2,2} = 4$, we conclude that column 2 must not have a two. Thus, column 2 has ones in rows 2 and 23, and in two more new rows, i.e. rows 12 and 123.

Next, we deal with column 1. $c_{1,12} = 0$ and $c_{1,2} = 2$, so column 1 has zeros in rows 2 and 23, and either two ones or a zero and a two in rows 12 and 123. But $c_{1,23} = 1$, and column 23 has no ones in common with any column that has already been determined; so column 1 must have at least one additional one in some new row. Since $c_{1,1} = 4$, we conclude that column 1 must not have a two, and we can fill it in as indicated.

Finally, we show that column $\varnothing$ has no entry larger than one. $c_{\varnothing,12} = 2$, so column $\varnothing$ has either two ones or a two and a zero in rows 2 and 23. $c_{\varnothing,2} = 4$, so, having accounted for rows 2 and 23, we see that rows 12 and 123 must also have either two ones or a two and a zero. Similarly, examining $c_{\varnothing,1}$ shows that there are either two ones or a two and a zero in rows 1 and 13. If there is a two in any of these rows, then column $\varnothing$ must have zeros in rows $\varnothing$ and 3, because $c_{\varnothing,\varnothing} = 8$. But $c_{\varnothing,23} = 2$ (in general, $c_{\varnothing,\{2,3,\ldots,n\}} = 2$), and this column is easily seen to have zeros in every row except possibly rows 1, 13, $\varnothing$, and 3 (generally, rows 1, $1n$, $\varnothing$, and n) by calculating Cartan invariants with columns that have already been determined. Therefore, if column $\varnothing$ has zeros in rows $\varnothing$ and 3, then there must be a two in either row 1 or row 13. This must be the only two in column $\varnothing$, because $c_{\varnothing,\varnothing} = 8$, and any additional two would force this Cartan invariant to exceed 8.

Now we examine column 13 (generally, column $\{1, 3, 4, \ldots, n\}$). This column has two ones, and by examining Cartan invariants with already determined columns, these ones must be distributed as follows: one between rows 12 and 123 (generally, 12 and $12n$), and one between rows 1 and 13 (generally, rows 1 and $1n$). In rows 12 and 123, column $\varnothing$ has ones; in rows 1 and 13, column $\varnothing$ has a zero and a two. Therefore, we must have $c_{\varnothing,13} = 1$ or 3; but $c_{\varnothing,13} = 2$, a contradiction. Therefore column $\varnothing$ consists entirely of ones, and we proceed as indicated with the previous proof.

Finally, note that this proof is possible only if $n \geq 3$; for instance, we made use of column $\{1, 3, 4, \ldots, n\}$ (which is different from column 1). In fact, the result is false if $n = 2$, in which case there is another nonnegative integer matrix F with $F^{\mathsf{T}}F = C$, namely

$$F = \begin{bmatrix} 2 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Of course, this matrix can't be the decomposition matrix, since it is square.

2.5.3 Submatrices of D

In this section, we explain how certain submatrices of D are (almost) equal to decomposition matrices of $\mathrm{SL}(2, 2^k)$ for $k \leq n/2$. Since we will be dealing with decomposition matrices of G for different n, we will write $D(n)$ for the decomposition matrix of $G_n = \mathrm{SL}(2, 2^n)$.

Definition 10. A subset $I \subsetneq N$ is *dense* if $i \notin I$ implies $i + 1 \in I$.

Clearly, if I is dense, then $|I| \geq n/2$, and $c_{II} \leq 2^{n/2}$. For each I which is dense, we will identify a subset of the rows and columns of $D(n)$ such that the submatrix of $D(n)$ corresponding to these rows and columns is (almost) equal to $D(k)$, where $k = n - |I|$. Choosing the columns involves a little effort:

Definition 11. If I is dense, and $S \subseteq N \setminus I$, then define the subset $A(I, S)$ as follows:

$$A(I, S) = S \cup \{j \in N \mid \text{For some } k, \{j, j + 1, \ldots, k\} \subseteq I, k + 1 \notin I, \text{ and } k + 1 \notin S\}.$$

We note that since S can be any subset of the complement of I, there are $2^{n-|I|}$ sets $A(I, S)$. These are the columns of the submatrix of $D(n)$ corresponding to I; the rows are simply the $2^{n-|I|}$ rows which respect I. For example, if $n = 7$ and $I = \{1, 2, 3, 5, 6\}$, then we have $A(I, \varnothing) = I$, $A(I, \{4\}) = \{4, 5, 6\}$, $A(I, \{7\}) = \{1, 2, 3, 7\}$, and $A(I, \{4, 7\}) = \{4, 7\}$. The sets respecting I are $\{3, 6\}$, $\{3, 4, 6\}$, $\{3, 6, 7\}$, and $\{3, 4, 6, 7\}$; the corresponding submatrix is:

$D(7)$	12356	456	1237	47
36	1	1	1	0
346	1	0	1	0
367	1	1	0	0
3467	1	0	0	1

which is *almost* $D(2)$. In order to make this matrix equal $D(2)$ exactly, we would have to move the one in column 47 into a row of its own. With this one minor change, all matrices obtained in this way are equal to $D(k)$, where $k = n - |I|$.

To see that this always happens, let $N \setminus I = \{g_1, g_2, \ldots, g_k\}$, and let $S \subseteq N \setminus I$. Suppose we examine the column of $D(n)$ labeled $A(I, S)$. Among those rows R which respect I (i.e., the rows satisfying $R \cap I = \mathrm{Final}(I)$), the rows which also respect

D	∅	234	1	134	2	124	3	123	4	14	23	13	24	12	34	1234
∅	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
4	1	1	0	·	·	·	·	·	1	·	·	·	·	·	1	·
14	1	1	1	·	·	·	·	·	1	·	·	·	·	·	1	·
1	1	·	1	1	0	·	·	·	·	1	·	·	·	·	·	·
12	1	·	1	1	1	·	·	·	·	1	·	·	·	·	·	·
2	1	·	·	·	1	1	0	·	·	·	·	·	·	1	·	·
23	1	·	·	·	1	1	1	·	·	·	·	·	·	1	·	·
3	1	·	·	·	·	·	1	1	0	·	1	·	·	·	·	·
34	1	·	·	·	·	·	1	1	1	·	1	·	·	·	·	·
13	1	·	1	·	·	·	1	·	·	1	1	1	0	·	·	·
123	1	·	1	·	1	·	1	·	·	1	0	1	0	·	·	·
134	1	·	1	·	·	·	1	·	1	0	1	1	0	·	·	·
1234	1	·	1	·	1	·	1	·	1	0	0	1	1	0	0	·
234	1	·	·	·	1	·	1	·	1	·	·	0	1	1	0	·
124	1	·	1	·	1	·	·	·	1	·	·	0	1	0	1	·
24	1	·	·	·	1	·	·	·	1	·	·	0	1	1	1	·
St	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1

Figure 2.6: The decomposition matrix of $\mathrm{SL}(2, 2^4)$ with each submatrix indicated. Dots are zero entries.

$A(I, S)$ are those for which (1) whenever $g_j \in S$ and $g_{j+1} \notin S$, $g_j \notin R$, and (2) whenever $g_j \in S$ and $g_{j+1} \in S$, $g_j \in R$. From this, we can conclude that the binary relation which determines whether an entry in this submatrix of $D(n)$ is a zero or a one is essentially identical to the relation $\prec$, but with each row replaced by its complement.

It is unclear if these submatrices simply appear because of the elementary combinatorial nature of the relation $\prec$, or if this structure is somehow also reflected in the algebra kG. Figure 2.6 shows all such submatrices when $n = 4$. Note that, in general, the rows and columns spanned by these submatrices are almost disjoint. The overlapping submatrices in the figure only occur when n is even, and only for the submatrices corresponding to the two dense subsets of minimal weight.

2.5.4 A Geometric Interpretation of C and D

We finish this discussion by noting that the results of this chapter have a geometric interpretation. In particular, there is an arrangement $\mathcal{A}_n$ of n-dimensional unit cubes in $\mathbb{R}^n$ with the following properties:

- Each cube corresponds to a unique proper subset $I \subsetneq N$,
- Each Cartan invariant can be calculated by counting the number of certain vertices that the two corresponding cubes share, and
- The decomposition matrix is the incidence matrix of those certain vertices with the set of cubes.

This geometric interpretation is a preview of the viewpoint we will take in the following chapter.

Specifically, to $I \subsetneq N$, we associate the unit cube centered at the integer lattice point $\mathbf{x} = (x_1, \ldots, x_n)$, where:

$$x_i = \begin{cases} 0 & \text{if } i \notin I \\ 1 & \text{if } i \in I \text{ and } i+1 \notin I \\ -1 & \text{if } i \in I \text{ and } i+1 \in I. \end{cases}$$

Vertices of the cubes are all at half-integer lattice points. We call a half-integer lattice point $\mathbf{y}$ *relevant* if $y_i = \pm 1/2$ for all i. Thus, the relevant vertices are exactly the vertices of the cube corresponding to $\varnothing$. We will call this arrangement of labeled cubes and relevant vertices $\mathcal{A}_n$.

Proposition 12. The Cartan invariant c_{IJ} is equal to the number of relevant vertices that the cubes associated to I and J share.

Proof. For $I \subsetneq N$, the relevant vertices of the cube labeled I are simply the relevant vertices satisfying the equations $\{x_i = 1 \mid i \in I, i+1 \notin I\} \cup \{x_i = -1 \mid i \in I, i+1 \in I\}$. So, clearly, the number of relevant vertices of the cube labeled I is $2^{n-|I|}$. Taking the union of the corresponding sets of equations for the cubes labeled I and J, we see that there are two possibilities: first, that an equation for I (resp. J) requires that $x_i = 1$, and an equation for J (resp. I) requires that $x_i = -1$. In this case, the cubes share no relevant vertices. Moreover, it must be the case that the i-th coordinate of one cube's center is 1, and the other is -1. This can only happen if $i \in I \cap J$, but $i + 1 \in I$ or J, but not both; in other words, only if $I \nsim J$.

The second possibility is that there is no such inconsistency in the sets of equations defining the relevant vertices for the cubes I and J. In this case, the number of relevant vertices shared by cubes I and J is $2^{n-|I \cup J|}$, since we clearly must take the union of the two sets of equations. Moreover, this implies that whenever the i-th coordinate of the center of cube I is 1 (resp. -1), the corresponding coordinate of the center of cube J is not -1 (resp. 1). Checking the formula for the centers of cubes, we see that this is equivalent to $I \sim J$. □

Proposition 13. The incidence matrix with rows indexed by relevant vertices and columns indexed by cubes is equal to the decomposition matrix of G in the principal block.

Proof. Clearly, the inner product of columns I and J of the incidence matrix gives the number of relevant vertices shared by cubes I and J. Since this incidence matrix is a zero-one matrix with no zero row, the conclusion follows from the main theorem of the chapter. □

CHAPTER 3
ODD CHARACTERISTIC

When p is odd, there is no simplification of the set $\{1, \ldots, p\}^n$ which parametrizes the simple kG-modules. Even so, some of the results in this chapter can be thought of as a generalization of the combinatorics of subsets of N which played a key role in the previous chapter. We continue with the convention that arithmetic in $N = \{1, \ldots, n\}$ is thought of as happening in $\mathbb{Z}/n\mathbb{Z}$. However, when we do arithmetic on elements of $\{1, \ldots, p\}$, we will think of the operations as taking place in $\mathbb{Z}$.[1]

3.1 The Cartan Matrix

In [4], Cheng describes the Cartan invariants of $G = \mathrm{SL}(2, q)$ in defining characteristic. This result is surprisingly concise, given the previous descriptions in [6] and [13], which, as Cheng notes, are "so complicated that there is little hope of generalizing them to other groups of Lie type." Cheng's result is phrased in terms of products of certain matrices, but we will find it more convenient to restate the result in combinatorial terms.

We begin with a definition that extends the notion of compatibility to odd primes.

Definition 14. Let $J, K \in \{1, \ldots, p\}^n$. Then J is *associated to* K via $A \subseteq N$ if

$$K_i = \begin{cases} J_i & \text{if } i \notin A \text{ and } i+1 \notin A \\ J_i \pm 1 & \text{if } i \in A \text{ and } i+1 \notin A \\ p - J_i & \text{if } i \notin A \text{ and } i+1 \in A \\ p - J_i \pm 1 & \text{if } i \in A \text{ and } i+1 \in A. \end{cases}$$

[1] Technically, this is an ambiguous convention, since 1 (say) is an element of both sets, and (worse) we may very well have $n = p$. We trust the reader to make the proper distinction from context.

We will write $J \underset{A}{\to} K$ when J is associated to K via A. [2]

Note that it is possible for a given J to be associated to more than one K via the same set A. For instance, if $q = 7^4$, then $(1,1,1,1)$ is associated to both $(1,6,5,2)$ and $(1,6,7,2)$ via $A = \{3,4\}$. In addition, J might be associated to K via more than one subset A; for instance, $(3,4,3,4)$ is associated to $(3,3,4,4)$ via $A = \{3\}$, and via $A = \{1,2,4\}$. Fortunately, we can put strong restrictions on the latter occurance:

Proposition 15. *J is associated to K via at most two different subsets A. If there are two, then $J, K \in \{\frac{p-1}{2}, \frac{p+1}{2}\}^n$, and the two subsets are complements of each other.*

Proof. Suppose that J is associated to K via two distinct sets A_1 and A_2. Since the definition is invariant under a cyclic permutation of N, we may assume without loss of generality that $1 \in A_1$ and $1 \notin A_2$. Therefore, when J is associated to K via A_1, we have $K_1 = J_1 \pm 1$ or $K_1 = p - J_1 \pm 1$, and when J is associated to K via A_2, $K_1 = J_1$ or $K_1 = p - J_1$. Since the equalities $J_1 \pm 1 = J_1$ and $p - J_1 \pm 1 = p - J_1$ are clearly impossible, we must have $K_1 = J_1 \pm 1 = p - J_1$ or $K_1 = p - J_1 \pm 1 = J_1$. In the first case, we have $2 \notin A_1$ and $2 \in A_2$, and in the second, $2 \in A_1$ and $2 \notin A_2$. Repeating this argument n times, we see that A_1 and A_2 are complements of each other.

Furthermore, induction shows that for all $i \in N$, $J_i \pm 1 = p - J_i$, which implies that $J_i = \frac{p\pm1}{2}$. We also have that $K_i = p - J_i$ or $K_i = J_i$ for each i, which shows that $K_i = \frac{p\pm1}{2}$ as well. Finally, inspection of the above argument shows that the sets J and K uniquely determine A_1 and A_2, which precludes the possibility of a third subset A_3 via which J is associated to K. This proves the proposition. □

Note that not all $J, K \in \{\frac{p\pm1}{2}\}^n$ are associated to each other. For instance, if $n = 2$, then $(\frac{p-1}{2}, \frac{p-1}{2})$ is not associated to $(\frac{p-1}{2}, \frac{p+1}{2})$. Indeed, the simple modules corresponding to these two labels are in different blocks.

[2] It is perhaps worth noting that $J \underset{A}{\to} K$ if and only if $K \underset{A}{\to} J$; however, we will make no use of this fact, and therefore leave it as an exercise to the reader.

Now we are ready to state a modified version of Cheng's result on the Cartan invariants of G, which we will prove equivalent to Cheng's original result momentarily. If either J or K is $(p, \ldots, p)$, then one of the corresponding modules is the Steinberg module, and we require that $c_{JK} = \delta_{JK}$. Otherwise,

$$c_{JK} = \sum_{J \underset{A}{\to} K} 2^{n - \#\{\, i \in N \,|\, i \in A \text{ or } J_i = p \,\}}.$$

For instance, if $q = 7^6$, $J = (1, 5, 7, 2, 6, 7)$, and $K = (6, 1, 6, 5, 7, 7)$, then there is exactly one A for which $J \underset{A}{\to} K$, namely $A = \{2, 3, 5\}$. Since $J_3 = 7$ and $J_6 = 7$, the cardinality of $\{i \in N \mid i \in A \text{ or } J_i = p\}$ is four, and we have that $c_{JK} = 2^{6-4} = 4$.

Corollary 16. Every Cartan invariant of G is either zero, 2^k, or $2^k + 2^{n-k}$ for some $1 \leq k \leq n$.

Proof. This is an easy consequence of the above proposition. We have $J \underset{A}{\to} K$ for exactly zero, one, or two sets A. If zero, then $c_{JK} = 0$; if one, then c_{JK} is a power of two; and if there are two such A, then $J, K \in \{\frac{p \pm 1}{2}\}$. This implies that no $J_i = p$, so we have $c_{JK} = 2^{n-|A_1|} + 2^{n-|A_2|}$. Since A_1 and A_2 are complements of each other, the corollary follows. □

Finally, we must prove that this description of the Cartan invariants is equivalent to Cheng's original result in [4]. Let ρ_i be the Brauer character of V_i, with the convention that $\rho_i = 0$ if $i < 1$ or $i > p$.[3] Note that Cheng numbers the simple modules differently; the results quoted here take this difference into account. Define the following matrices over $\mathbb{Z}[\mathrm{IBr}(G)]$:

$$A_j = \begin{pmatrix} 2\rho_j & \rho_{p-j} \\ 2\rho_{j-1} + 2\rho_{j+1} & \rho_{p-j-1} + \rho_{p-j+1} \end{pmatrix} \qquad \text{if } 1 \leq j < p,$$

$$A_p = \begin{pmatrix} \rho_p & 0 \\ \rho_{p-1} & \rho_1 \end{pmatrix}.$$

[3] Recall that V_i is the simple module of dimension i obtained by letting G act on homogeneous bivariate polynomials of degree $i - 1$.

Theorem 3.1 of [4] gives a formula for the projective character η_J of P_J. As long as $J \neq (p, \ldots, p)$, the theorem states:

$$\eta_J = \operatorname{tr} \prod_{i=1}^{n} (A_{J_i})^{\sigma^{i-1}}.$$

We begin by rephrasing the definition of the matrices A_j. Define functions X and Y on $\mathbb{Z}[\mathrm{IBr}(G)]$ by letting $X(\rho_j) = \rho_{p-j}$ and $Y(\rho_j) = \rho_{j-1} + \rho_{j+1}$, and by requiring that X and Y are linear and commute with the Frobenius automorphism σ. We will also need to use the composite map of X and Y. Note that X and Y almost commute; $X \circ Y$ and $Y \circ X$ agree on ρ_j when $2 \leq j \leq p-1$, but we have:

$$\begin{aligned} X \circ Y(\rho_1) &= \rho_{p-2} & \qquad X \circ Y(\rho_p) &= \rho_1 \\ Y \circ X(\rho_1) &= \rho_{p-2} + \rho_p & \qquad Y \circ X(\rho_p) &= 0. \end{aligned}$$

Both of these irregularities result from the convention that $\rho_0 = 0$. Rather than fixing this by using some unusual convention with the symbol ρ_0, we will simply define a third map XY. Let $XY = X \circ Y = Y \circ X$ on ρ_j, $2 \leq j \leq p-1$, and define $XY(\rho_1) = \rho_{p-2} + \rho_p$ and $XY(\rho_p) = \rho_1$.

Next, let X_i, Y_i, and XY_i be the functions which equal X, Y, and XY, respectively, on $\rho_j^{\sigma^i}$, and are the identity on all other Frobenius twists of the ρ_j. Thus, $X = X_0 \circ \cdots \circ X_{n-1}$. For consistency, we will require that $X_i^{\sigma} = X_{i+1}$, and similarly for the Y_i and XY_i. Also let $\psi(j) = 2$ if $1 \leq j \leq p-1$, and $\psi(p) = 1$. With these definitions, we can rewrite the matrices A_j as:

$$A_j = \begin{pmatrix} \psi(j) \cdot \rho_j & X_0(\rho_j) \\ \psi(j) \cdot Y_0(\rho_j) & XY_0(\rho_j) \end{pmatrix}.$$

We require one more family of functions on $\mathbb{Z}[\mathrm{IBr}(G)]$. Define Z_i as:

$$Z_i(\rho_{J_1} \rho_{J_2}^{\sigma} \cdots \rho_{J_n}^{\sigma^{n-1}}) = \sum_{A \subseteq \{1, \ldots, i\}} \left[2^{i - \#\{1 \leq k \leq i \,|\, k \in A \text{ or } J_k = p\}} \left(\bigodot_{k \in A} X_{k-1} \circ Y_k \right) \right]$$

where $\odot$ behaves like function composition, except for the requirement that $X_k \odot Y_k = XY_k$. Note that $Z_0 = 1$.

As an example, suppose $n \geq 3$. As long as no $J_k = p$, we have $Z_2 = 4 + 2X_0 \circ Y_1 + 2X_1 \circ Y_2 + X_0 \circ XY_1 \circ Y_2$, and if $p = 7$ (switching back from Cheng's notation to ours), $Z_2(\rho_1 \cdot \rho_2^{\sigma} \cdot \rho_3^{\sigma^2}) = Z_2(1, 2, 3) = 4 \cdot (1, 2, 3) + 2 \cdot (6, 1, 3) + 2 \cdot (6, 3, 3) + 2 \cdot (1, 5, 2) + 2 \cdot (1, 5, 4) + (6, 4, 3) + (6, 4, 5) + (6, 6, 3) + (6, 6, 5)$.

Note that our description of the Cartan invariants is equivalent to saying that $Z_n(J)$ is the character of the projective cover of V_J; this is simply a matter of verifying that the compositions $X_{k-1} \circ Y_k$ above correspond to the formulas in definition 14. Thus, to show the equivalence of Cheng's description of the Cartan invariants with ours, we must show that $Z_n(J) = \eta_J$.

To this end, we prove by induction on i that:

$$\prod_{k=1}^{i} (A_{J_k})^{\sigma^{k-1}} = \begin{pmatrix} \psi(J_i) \cdot Z_{i-1}(J) & X_{i-1} \odot Z_{i-1}(J) \\ \psi(J_i) \cdot Y_0 \odot Z_{i-1}(J) & X_{i-1} \odot Y_0 \odot Z_{i-1}(J) \end{pmatrix}$$

where, for convenience, $J = (J_1, \ldots, J_k) = \rho_{J_1} \rho_{J_2}^{\sigma} \ldots \rho_{J_k}^{\sigma^{k-1}}$.

If $i = 1$, this simply states that

$$A_{J_1} = \begin{pmatrix} \psi(J_1) \cdot \rho_{J_1} & X_0(\rho_{J_1}) \\ \psi(J_1) \cdot Y_0(\rho_{J_1}) & XY_0(\rho_{J_1}) \end{pmatrix},$$

which is true. Now, we calculate:

$$\prod_{k=1}^{i+1} (A_{J_k})^{\sigma^{k-1}} = \left(\prod_{k=1}^{i} (A_{J_k})^{\sigma^{k-1}} \right) (A_{J_{i+1}})^{\sigma^i}$$

$$= \begin{pmatrix} \psi(J_i) Z_{i-1}(J) & X_{i-1} \odot Z_{i-1}(J) \\ \psi(J_i) Y_0 \odot Z_{i-1}(J) & X_{i-1} \odot Y_0 \odot Z_{i-1}(J) \end{pmatrix} \begin{pmatrix} \psi(J_{i+1}) \rho_{J_{i+1}} & X_0(\rho_{J_{i+1}}) \\ \psi(J_{i+1}) Y_0(\rho_{J_{i+1}}) & XY_0(\rho_{J_{i+1}}) \end{pmatrix}^{\sigma^i}$$

$$= \begin{pmatrix} \psi(J_i) Z_{i-1}(J) & X_{i-1} \odot Z_{i-1}(J) \\ \psi(J_i) Y_0 \odot Z_{i-1}(J) & X_{i-1} \odot Y_0 \odot Z_{i-1}(J) \end{pmatrix} \begin{pmatrix} \psi(J_{i+1}) \rho_{J_{i+1}}^{\sigma^i} & X_i(\rho_{J_{i+1}}^{\sigma^i}) \\ \psi(J_{i+1}) Y_i(\rho_{J_{i+1}}^{\sigma^i}) & XY_i(\rho_{J_{i+1}}^{\sigma^i}) \end{pmatrix}$$

$$= \begin{pmatrix} \psi(J_i)\psi(J_{i+1})Z_{i-1}(J)\cdot\rho + \psi(J_{i+1})X_{i-1}\odot Z_{i-1}(J)\cdot Y_i(\rho) \\ \psi(J_i)\psi(J_{i+1})Y_0\odot Z_{i-1}(J)\cdot\rho + \psi(J_{i+1})X_{i-1}\odot Y_0\odot Z_{i-1}(J)\cdot Y_i(\rho) \end{pmatrix.$$

$$\begin{matrix} \psi(J_i)Z_{i-1}(J)\cdot X_i(\rho) + X_{i-1}\odot Z_{i-1}(J)\cdot XY_i(\rho) \\ \psi(J_i)Y_0\odot Z_{i-1}(J)\cdot X_i(\rho) + X_{i-1}\odot Y_0\odot Z_{i-1}(J)\cdot XY_i(\rho) \end{pmatrix},$$

where $\rho = \rho_{J_{i+1}}^{\sigma^i}$. Now observe that $\psi(J_i)Z_{i-1}(J)\cdot\rho + X_{i-1}\odot Z_{i-1}(J)\cdot Y_0(\rho) = Z_i(J,\rho)$, so

$$\cdots = \begin{pmatrix} \psi(J_{i+1})Z_i(J,\rho) & X_i\odot Z_i(J,\rho) \\ \psi(J_{i+1})Y_0\odot Z_i(J,\rho) & X_i\odot Y_0\odot Z_i(J,\rho) \end{pmatrix},$$

completing the induction.

Therefore,

$$\eta_J = \operatorname{tr}\prod_{i=1}^{n}(A_{J_i})^{\sigma^{i-1}} = \operatorname{tr}\begin{pmatrix} \psi(J_n)\cdot Z_{n-1}(J) & X_{n-1}\odot Z_{n-1}(J) \\ \psi(J_n)\cdot Y_0\odot Z_{n-1}(J) & X_{n-1}\odot Y_0\odot Z_{n-1}(J) \end{pmatrix}$$

$$= \psi(J_n)\cdot Z_{n-1}(J) + X_{n-1}\odot Y_0\odot Z_{n-1}(J) = Z_n(J).$$

This completes the proof.

3.2 A Geometric Description of the Cartan Matrix

The above description of the Cartan matrix can be rephrased in geometric terms. To each label $J \in \{1,\dots,p\}^n$, we will associate a unit n-cube, such that the Cartan invariant c_{JK} can be calculated by counting the number of vertices that the cubes J and K share. This idea is analogous to the geometric interpretation obtained in the previous chapter for $p = 2$.

Begin by dividing $\mathbb{R}^n$ into unit n-cubes with corners at integer lattice points. Assign a label in the set $\mathbb{Z}^n$ to each cube according to the following rule: if a cube is centered at the half-integer lattice point $\mathbf{x} = (x_1,\dots,x_n)$, assign the label $J = (J_1,\dots,J_n)$, where

$$J_i = \frac{p}{2} + (-1)^{\lfloor x_{i+1}\rfloor}x_i.$$

Next, discard all cubes except for those with labels in the set $\{1, \ldots, p\}^n$. Also discard any cube labeled $(p, \ldots, p)$, which is the label of the Steinberg module. We will call this arrangement of labeled cubes in $\mathbb{R}^n$ the *even arrangement.*

We wish to define another arrangement of cubes in $\mathbb{R}^n$, the *odd arrangement*, which is identically labeled with the exception that

$$J_n = \frac{p}{2} - (-1)^{\lfloor x_1 \rfloor} x_n.$$

The even and odd arrangements will give the Cartan invariants of the two blocks of kG of positive defect; thus, a complete combinatorial picture of the Cartan invariants will involve the disjoint union of two copies of $\mathbb{R}^n$. For convenience, we define $\epsilon(i) = 1$, unless $i = n$ and we are in the odd arrangement, in which case $\epsilon(i) = -1$. With this notation, we have

$$J_i = \frac{p}{2} + \epsilon(i)(-1)^{\lfloor x_{i+1} \rfloor} x_i$$

for all i, and for either arrangement.

We will call a cube *interior* if its label J lies in the set $\{1, \ldots, p-1\}^n$, and *boundary* otherwise. From the formulas for a cube's label, we can see that a cube centered at $\mathbf{x}$ is interior if and only if $-\frac{p-2}{2} \leq x_i \leq \frac{p-2}{2}$ for all $i \in N$, and so the set of all interior cubes forms one large cube centered at the origin. A cube is *central* if $x_i = \pm 1/2$ for all i, or, equivalently, if the cube has the origin as a vertex.

Call a vertex $\mathbf{y} = (y_1, \ldots, y_n)$ of a cube *relevant* if $-\frac{p-1}{2} \leq y_i \leq \frac{p-1}{2}$ for all i. Thus, a vertex is relevant if and only if it is a vertex of some interior cube. Figure 3.1 shows the even and odd arrangements when $p = 5$, $n = 2$. Each cube is labeled appropriately, and the relevant vertices are shown as dots.

As one can see, there is some duplication in the labeling of the cubes. If we wish to put cubes in bijective correspondence with simple modules, we must compensate for this.

Proposition 17. In either arrangement, the cube centered at $\mathbf{x} = (x_1, \ldots, x_n)$ has the same label as the cube centered at $-\mathbf{x} = (-x_1, \ldots, -x_n)$. If a label appears in an arrangement, then it appears exactly twice.

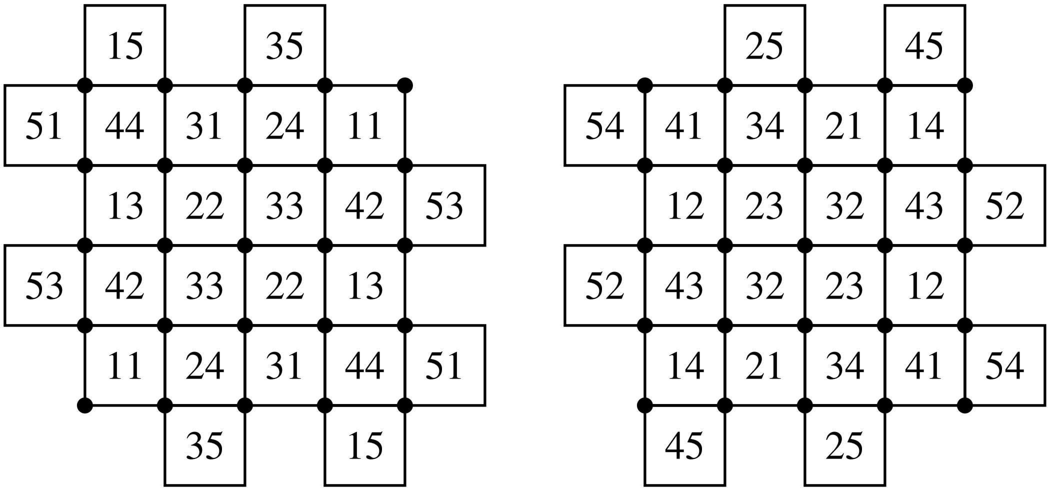


Figure 3.1: The even and odd arrangements for $q = 25$

Proof. If x_{i+1} is not an integer, then the parities of $\lfloor x_{i+1} \rfloor$ and $\lfloor -x_{i+1} \rfloor$ are always opposite. Thus, $(-1)^{\lfloor -x_{i+1} \rfloor} = -(-1)^{\lfloor x_{i+1} \rfloor}$, and so $(-1)^{\lfloor -x_{i+1} \rfloor}(-x_i) = (-1)^{\lfloor x_{i+1} \rfloor} x_i$. Thus, the cubes centered at $\mathbf{x}$ and $-\mathbf{x}$ have the same labels.

Suppose the labels assigned to the cubes centered at $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are equal, i.e. that $(-1)^{\lfloor x_{i+1} \rfloor} x_i = (-1)^{\lfloor y_{i+1} \rfloor} y_i$. If $\mathbf{x} \neq \mathbf{y}$, then we may assume without loss of generality that $x_1 \neq y_1$. But $(-1)^{\lfloor x_2 \rfloor} x_1 = (-1)^{\lfloor y_2 \rfloor} y_1$, so we conclude that $x_1 = -y_1$, and that the parities of $\lfloor x_2 \rfloor$ and $\lfloor y_2 \rfloor$ differ. But this implies that $x_2 \neq y_2$, and therefore we may repeat the argument to show that $x_2 = -y_2$. By induction, $\mathbf{x} = -\mathbf{y}$, and therefore no other cube shares this label. This proves the proposition. □

Let $\mathbb{R}^n/\{\pm 1\}$ be the topological space $\mathbb{R}^n/\sim$, where $x \sim y$ iff $x = \pm y$. It is an immediate consequence of the proposition that the label of a cube in the quotient space $\mathbb{R}^n/\{\pm 1\}$ is well-defined under the natural projection $\pi : \mathbb{R}^n \to \mathbb{R}^n/\{\pm 1\}$. Furthermore, in the quotient space, each label is used at most once. From now on, when we refer to the even or odd arrangement of cubes, we will mean the image of that arrangement in the quotient space $\mathbb{R}^n/\{\pm 1\}$. Whenever we refer to the "coordinates of the center of a cube labeled J" or the "coordinates of a relevant vertex", we will understand that these coordinates are only well-defined up to a choice of sign.

Now we are ready for the crucial observation which links these arrangements of cubes to the Cartan invariants of G:

Proposition 18. Let J and K be labels of cubes which are in the same arrangement, and let $\mathbf{x}$ and $\mathbf{y}$ be the coordinates of the centers of the cubes labeled J and K, respectively. Then:

$$J \underset{A}{\rightarrow} K \iff y_i = \begin{cases} x_i & \text{if } i \notin A \\ x_i \pm 1 & \text{if } i \in A. \end{cases}$$

Proof. ($\Leftarrow$) We have four cases, depending on whether i and $i+1$ are in A. In each case, the corresponding conditions on y_i and y_{i+1} give the correct formula for K_i :

$$\left\{\begin{matrix} y_i = x_i \\ y_{i+1} = x_{i+1} \end{matrix}\right\} \Rightarrow \ (-1)^{\lfloor y_{i+1} \rfloor} y_i = (-1)^{\lfloor x_{i+1} \rfloor} x_i \ \Rightarrow \ K_i = J_i$$

$$\left\{\begin{matrix} y_i = x_i \pm 1 \\ y_{i+1} = x_{i+1} \end{matrix}\right\} \Rightarrow \ (-1)^{\lfloor y_{i+1} \rfloor} y_i = (-1)^{\lfloor x_{i+1} \rfloor} x_i \pm 1 \ \Rightarrow \ K_i = J_i \pm 1$$

$$\left\{\begin{matrix} y_i = x_i \\ y_{i+1} = x_{i+1} \pm 1 \end{matrix}\right\} \Rightarrow \ (-1)^{\lfloor y_{i+1} \rfloor} y_i = -\,(-1)^{\lfloor x_{i+1} \rfloor} x_i \ \Rightarrow \ K_i = p - J_i$$

$$\left\{\begin{matrix} y_i = x_i \pm 1 \\ y_{i+1} = x_{i+1} \pm 1 \end{matrix}\right\} \Rightarrow \ (-1)^{\lfloor y_{i+1} \rfloor} y_i = -\,(-1)^{\lfloor x_{i+1} \rfloor} x_i \pm 1 \ \Rightarrow \ K_i = p - J_i \pm 1.$$

($\Rightarrow$) Working in this direction, we must be more careful about the sign ambiguity in choosing the coordinates of the centers of the cubes labeled J and K. Suppose we fix the coordinates $\mathbf{x}$ of one of the two cubes labeled J. If $1 \notin A$, we choose the coordinates $\mathbf{y}$ of the cube labeled K so that $\lfloor x_1 \rfloor$ and $\lfloor y_1 \rfloor$ have equal parities, and if $1 \in A$, we choose $\mathbf{y}$ so that $\lfloor x_1 \rfloor$ and $\lfloor y_1 \rfloor$ have opposite parities. This is always possible, because $\lfloor a \rfloor$ and $\lfloor -a \rfloor$ have opposite parities when a is a half-integer.

Suppose first that $1 \notin A$. If we also have $2 \notin A$, then $(-1)^{\lfloor y_2 \rfloor} y_1 = (-1)^{\lfloor x_2 \rfloor} x_1$, which implies that $y_1 = \pm x_1$. But $\lfloor x_1 \rfloor$ and $\lfloor y_1 \rfloor$ have equal parities, so we must have $y_1 = x_1$ as claimed. Moreover, this implies that $\lfloor x_2 \rfloor$ and $\lfloor y_2 \rfloor$ have equal parities. If, on the other hand, we have $2 \in A$, then $(-1)^{\lfloor y_2 \rfloor} y_1 = -(-1)^{\lfloor x_2 \rfloor} x_1$, which again implies that $y_1 = x_1$. However, we now have that $\lfloor x_2 \rfloor$ and $\lfloor y_2 \rfloor$ have opposite parities.

Now suppose that $1 \in A$. If we have $2 \notin A$, then $(-1)^{\lfloor y_2 \rfloor} y_1 = (-1)^{\lfloor x_2 \rfloor} x_1 \pm 1$, which implies that $y_1 = \pm x_1 \pm 1$. But $\lfloor x_1 \rfloor$ and $\lfloor y_1 \rfloor$ have opposite parities, so it must be the case that $y_1 = x_1 \pm 1$ as claimed. Moreover, this implies that $\lfloor x_2 \rfloor$ and $\lfloor y_2 \rfloor$ have equal parities. If, on the other hand, we have $2 \in A$, then $(-1)^{\lfloor y_2 \rfloor} y_1 = -(-1)^{\lfloor x_2 \rfloor} x_1 \pm 1$, which again implies that $y_1 = x_1 \pm 1$. However, we now have that $\lfloor x_2 \rfloor$ and $\lfloor y_2 \rfloor$ have opposite parities.

Thus, we see that if $2 \notin A$, then $\lfloor x_2 \rfloor$ and $\lfloor y_2 \rfloor$ have equal parities, and if $2 \in A$, $\lfloor x_2 \rfloor$ and $\lfloor y_2 \rfloor$ have opposite parities. Therefore, we may repeat the argument to show that $y_2 = x_2$ if $2 \notin A$, and $y_2 = x_2 \pm 1$ if $2 \in A$. Continuing in this way, we obtain the desired conclusion. □

We are now ready to give another description of the Cartan invariants of kG:

Proposition 19. Let $J \in (1, \ldots, p)$ be the label of a cube in either the even or odd arrangement. If $K \in (1, \ldots, p)$ is another such label, then $c_{JK} \neq 0$ if and only if the cube labeled J shares a vertex with a cube labeled K. In this case, the Cartan invariant equals the number of *relevant* vertices that the corresponding cubes share, with the understanding that the origin, if shared, is counted twice.[4]

Proof. Let $\mathbf{x}$ and $\mathbf{y}$ be the coordinates of the centers of the cubes labeled J and K, respectively. If the cubes labeled J and K share no vertices, then we must have $y_i \notin \{x_i, x_i \pm 1\}$ for some i. By the proposition, there does not exist an $A \subseteq N$ with $J \underset{A}{\to} K$, and therefore $c_{JK} = 0$.

Now suppose the cubes labeled J and K share at least one vertex. For the moment, suppose that at least one of the cubes is not central (below, we will deal with the case

[4] It must be emphasized that the even and odd arrangements exist in the space $\mathbb{R}^n/\{\pm 1\}$, and, therefore, the enumeration of relevant vertices shared by the cubes labeled J and K also takes place in this space. Referring to figure 3.1, we see that the Cartan invariant for $(2, 2)$ and $(3, 3)$ is *four*. The squares share *three* vertices: $\pm(1, 0)$, $\pm(0, 1)$, and $(0, 0)$, which is counted twice.

where both cubes are central). Then there is exactly one $A \subseteq N$ with $J \underset{A}{\rightarrow} K$, and, by the proposition, the cubes must share $2^{n-|A|}$ vertices. However, not all of these shared vertices are necessarily relevant. Specifically, for each i with $x_i = y_i = \pm\frac{p}{2}$, half of the shared vertices will be irrelevant. But if $x_i = \pm\frac{p}{2}$, then $J_i = \frac{p}{2} \pm \frac{p}{2} = 0$ or p; since no cube has a zero in its label, $J_i = p$. Conversely, if $J_i = p$, then $x_i = \pm\frac{p}{2}$, in which case y_i also equals $\pm\frac{p}{2}$ if and only if $i \notin A$ (by the proposition). Therefore, to compensate for the fact that the cubes labeled J and K may share irrelevant vertices, we see that we must divide the number of shared vertices by two whenever there is an $i \notin A$ such that $J_i = p$. Thus, $c_{JK} = 2^{n-|A|-\#\{i \notin A \,|\, J_i = p\}}$, which is equivalent to the formula in the previous section.

Finally, suppose that both cubes are central. Then every shared vertex is relevant; however, there are now two subsets A_1 and A_2 via which $J \rightarrow K$; furthermore, A_1 and A_2 are complements of each other. By the proposition, this implies that the cube labeled J is adjacent to the cube labeled K in two different ways; once in the coordinate directions in the set A_1, and once in the coordinate directions in the set A_2. If we count the shared vertices resulting from each of these two adjacencies, we obtain $2^{n-|A_1|}+2^{n-|A_2|}$ vertices, with the stated convention that the origin is counted twice. (No other vertex is counted twice, because A_1 and A_2 are complements of each other.) This number also agrees with the formula given in the previous section, which completes the proof. □

To show the value of this geometric interpretation, we prove a fact which is not obvious from previous descriptions of the Cartan matrix:

Corollary 20. As $p \rightarrow \infty$, the fraction of simple modules J satisfying $c_{JJ} = 2^n$ approaches 1.

Proof. If the cube labeled J is interior but not central, then the Cartan invariant is as stated. Clearly, as $p \rightarrow \infty$, the fraction of cubes which are interior and noncentral approaches 1. □

It is clear now that the even and odd arrangements correspond to the principal and nonprincipal blocks of kG of positive defect; however, which arrangement corresponds to which block is determined by an unexpected rule:

Proposition 21. If n is even, or $p = 1 \bmod 4$, then the even arrangement of cubes gives the Cartan invariants of the principal block of kG, and the odd arrangement gives the Cartan invariants of the nonprincipal block. If n is odd and $p = 3 \bmod 4$, then the situation is reversed.

Proof. In the even arrangement, the cube centered at $(1/2, \ldots, 1/2)$ is labeled $(\frac{p+1}{2}, \ldots, \frac{p+1}{2})$. The total weight of this label is thus $n \cdot \frac{(p+1)}{2}$, which is even if n is even or if $p = 3 \bmod 4$, and odd if n is odd and $p = 1 \bmod 4$. Moreover, the parity of the trivial representation, $(1, \ldots, 1)$, is the same as the parity of n. Thus, if n is even, then the even arrangement corresponds to the principal block, and if n is odd, then the even arrangement corresponds to the principal block if $p = 1 \bmod 4$, and the nonprincipal block if $p = 3 \bmod 4$. □

3.3 Factoring the Cartan Matrix

Once again, we will follow the route indicated in the introduction, and prove combinatorially that the decomposition matrix of kG is essentially determined by the Cartan matrix.

Main Theorem. There is a unique nonnegative integer matrix M, up to a permutation of rows, such that:

1. Every entry is a zero or one,

2. Every row contains a nonzero entry, and

3. $M^{\top} M = C$.

Clearly, the decomposition matrix of G satisfies the second and third conditions; by work of Srinivasan [12], the decomposition numbers of $\mathrm{SL}(2, p^n)$ are all zero or one when p is an odd prime. Therefore, an immediate consequence of the main theorem is that the unique matrix M is, in fact, the decomposition matrix.

We next describe a matrix E which satisfies the three conditions of the theorem. The columns of E are already labeled by the simple kG-modules. The rows of E are labeled by the disjoint union of the relevant vertices of the even and the odd arrangements, with one exception: for each arrangement, there are *two* rows of E labeled by the origin. Note that the arrangements, and thus the relevant vertices, are each taken to lie in the space $R^n/\{\pm 1\}$. To this, we add one more row labeled with the symbol St, which corresponds to the Steinberg module. Since each of the arrangements has $(p^n-1)/2$ relevant non-origin vertices, this gives us a total of p^n+4 rows in the matrix E, which equals the number of ordinary characters of G.

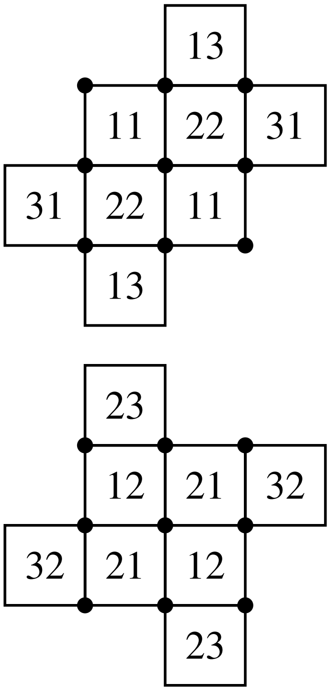
The entries of E are all zero or one, according to the rules:

$$e_{RJ} = \begin{cases} 1 & \text{if } R \neq \mathrm{St} \text{ and vertex } R \text{ belongs to the cube labeled } J \\ 0 & \text{if } R \neq \mathrm{St} \text{ and vertex } R \text{ does not belong to the cube labeled } J \\ 1 & \text{if } R = \mathrm{St} \text{ and } J = (p, \dots, p) \\ 0 & \text{if } R = \mathrm{St} \text{ and } J \neq (p, \dots, p). \end{cases}$$

Figure 3.2 shows the even and odd arrangements for $\mathrm{SL}(2, 9)$, with the Cartan and decomposition matrices for each block.

Proposition 22. The matrix E satisfies conditions 1–3 of the theorem.

Proof. Clearly, E satisfies condition 1 of the theorem. Since each relevant vertex belongs to at least one interior cube, condition 2 is also satisfied. Finally, if J and K are (non-Steinberg) column labels of E, then the J, K entry of $E^{\top}E$ is the number of rows which have a one in both column J and column K. By our definition of E, this is the number of relevant vertices which belong to both the cube labeled J, and the cube labeled K, with the convention that the origin is counted twice. Thus, E satisfies all three conditions of the theorem. □



C	11	22	13	31
11	5	4	1	1
22	4	5	2	2
13	1	2	2	1
31	1	2	1	2

D	11	22	13	31
$\pm(1,-1)$	1	0	0	0
$\pm(0,1)$	1	1	1	0
$\pm(1,1)$	0	1	1	1
$\pm(1,0)$	1	1	0	1
$(0,0)$	1	1	0	0
$(0,0)$	1	1	0	0

C	12	21	23	32
12	5	4	2	1
21	4	5	1	2
23	2	1	2	0
32	1	2	0	2

D	12	21	23	32
$\pm(1,-1)$	1	0	1	0
$\pm(0,1)$	1	1	1	0
$\pm(1,1)$	0	1	0	1
$\pm(1,0)$	1	1	0	1
$(0,0)$	1	1	0	0
$(0,0)$	1	1	0	0

Figure 3.2: The principal and nonprincipal blocks of $\mathrm{SL}(2,9)$

3.4 Proof of the Main Theorem

Our strategy for proving the uniqueness of the matrix M is to "build up" M by rows, using the argument from the previous chapter on each of the noncentral interior cubes. (The central cubes provide additional difficulties, since these cubes are associated to each other by more than one subset $A \subset N$.) Unfortunately, there are no noncentral interior cubes when $p = 3$, which means we will need to construct an entirely different argument for this case. With this in mind, we first deal with the case $p \geq 5$.

The heart of the argument is the following proposition:

Proposition 23. Let J be an interior noncentral cube centered at $\mathbf{x}$ in the even or odd arrangement. Then there exists an isometry $f : \mathbb{R}^n \to \mathbb{R}^n$, with $f(0) = \mathbf{x}$, which maps the arrangement $\mathcal{A}_n$ of cubes described at the end of the previous chapter into the current arrangement, with cubes mapping to cubes and relevant vertices mapping to relevant vertices.

Thus, $\mathcal{A}_n$ can be made to "fit into" the even or odd arrangement in such a way that any interior noncentral cube plays the role of the cube at the origin in $\mathcal{A}_n$. However, it will *not* usually be the case that the number of relevant vertices shared by a pair of cubes in the image will equal the corresponding number of shared relevant vertices in $\mathcal{A}_n$, because there are usually more relevant vertices in the image. That is, non-relevant vertices of $\mathcal{A}_n$ may map to relevant vertices in the current arrangement.

Proof. Let $\mathbf{x} = (x_1, \ldots, x_n)$ be the coordinates of the center of an interior cube in the even arrangement, and let $J = (J_1, \ldots, J_n)$ be its label. Define the isometry $f = (f_1, \ldots, f_n) : \mathbb{R}^n \to \mathbb{R}^n$ by:

$$f_i(t) = \begin{cases} x_i + t & \text{if } \lfloor x_{i+1} \rfloor \text{ is even} \\ x_i - t & \text{if } \lfloor x_{i+1} \rfloor \text{ is odd.} \end{cases}$$

Clearly, $f(0) = \mathbf{x}$. Now, from our description of $\mathcal{A}_n$ in the last chapter, $\mathbf{a} = (a_1, \ldots, a_n)$ is the center of a cube in $\mathcal{A}_n$ if and only if the following four conditions are satisfied:

- $a_i \in \{-1, 0, 1\}$,
- if $a_i = -1$, then $a_{i+1} = \pm 1$,
- if $a_i = 1$, then $a_{i+1} = 0$, and
- $a_i \neq -1$ for some $i \in N$.

Fix one such $\mathbf{a}$, and let $K = (K_1, \ldots, K_n)$ be the label of the cube centered at $f(\mathbf{a})$. With these restrictions on $\mathbf{a}$, we must show that $K \in \{1, \ldots, p\}^n$. We have:

$$K_i = \frac{p}{2} + (-1)^{\lfloor f_{i+1}(a_{i+1}) \rfloor} f_i(a_i) = \frac{p}{2} + (-1)^{\lfloor x_{i+1} \pm a_{i+1} \rfloor}(x_i \pm a_i).$$

Suppose first that $a_i = 0$. If so, then $K_i = \frac{p}{2} \pm x_i$. Since J is an interior cube, we have $-\frac{p-2}{2} \leq x_i \leq \frac{p-2}{2}$, which implies that $1 \leq K_i \leq p - 1$. Thus $K_i \in \{1, \ldots, p\}$.

Now suppose $a_i = 1$. Then $a_{i+1} = 0$, so $K_i = \frac{p}{2} + (-1)^{\lfloor x_{i+1} \rfloor}(x_i \pm 1)$, where the sign is positive if $\lfloor x_{i+1} \rfloor$ is even and negative if $\lfloor x_{i+1} \rfloor$ is odd. Thus, $K_i =$

$\frac{p}{2} + (-1)^{\lfloor x_{i+1} \rfloor} x_i + 1 = \frac{p}{2} \pm x_i + 1$, and therefore $2 \leq K_i \leq p$. So we again have $K_i \in \{1, \ldots, p\}$.

Finally, suppose $a_i = -1$, which implies that $a_{i+1} = \pm 1$. In this case, $K_i = \frac{p}{2} + (-1)^{\lfloor x_{i+1} \pm 1 \rfloor}(x_i \pm 1) = \frac{p}{2} - (-1)^{\lfloor x_{i+1} \rfloor}(x_i \pm 1)$, where the sign is negative if $\lfloor x_{i+1} \rfloor$ is even and positive if $\lfloor x_{i+1} \rfloor$ is odd. So $K_i = \frac{p}{2} - (-1)^{\lfloor x_{i+1} \rfloor} x_i + 1 = \frac{p}{2} \pm x_i + 1$, and again $K_i \in \{1, \ldots, p\}$.

It remains to show that $K \neq (p, \ldots, p)$. But $a_i = 0$ for some $i \in N$, and therefore $1 \leq K_i \leq p - 1$.

The proof is similar for the odd arrangement. □

Now, if it were true that any pair of cubes in $\mathcal{A}_n$ shared the same number of relevant vertices as the images of those cubes shared in the even or odd arrangements, then a submatrix of C would equal the Cartan matrix of $\mathrm{SL}(2, 2^n)$. In that event, we could appeal to the previous chapter to show that the columns of M corresponding to the cubes in the image of f were uniquely determined. However, as we've noted, cubes in the even and odd arrangements may share additional relevant vertices that are not present in $\mathcal{A}_n$.

Fortunately, we were able to prove the main theorem of chapter 2 with restricted assumptions. In the situation where every decomposition number is known to be a zero or one, we obtained a proof while only making use of the Cartan invariants c_{IJ}, where $\max(|I|, |J|) \leq 1$. Therefore, we could use the theorem from chapter 2 if we only knew that the number of shared vertices of a pair of cubes in $\mathcal{A}_n$ was equal to the corresponding number of shared vertices in the even or odd arrangements, for pairs of cubes I and J with $I = \varnothing$, or $I = \{k\}$. Since every vertex of the cube labeled $\varnothing$ in $\mathcal{A}_n$ is already relevant, this cube poses no problems. The cubes labeled $\{k\}$ are those that share an $(n-1)$-dimensional face with $\varnothing$, so we must show that the cubes in the even or odd arrangements which share an $n-1$-dimensional face with the cube labeled J also have the property that the number of relevant vertices they share with another cube in the image is the number of relevant vertices that the corresponding cubes in $\mathcal{A}_n$ share. Unfortunately, this is usually false.[5,6]

To remedy this problem, we introduce the idea of a *virtual cube.* Let Q be a formal $\mathbb{Z}$-linear combination of labels of simple modules:

$$Q = \sum_{i=1}^{q} u_i J_i.$$

If K is a label of another simple module, we can define a "Cartan invariant" of Q with K in the obvious way:

$$c_{QK} = \sum_{i=1}^{q} u_i c_{J_i K}.$$

Furthermore, if we associate a $\mathbb{Z}$-linear combination of relevant vertices to Q by counting each vertex of J_i a number of times equal to u_i, then this "Cartan invariant" clearly has the following meaning: c_{QK} is the number of vertices that K shares with Q, where each vertex of Q is counted a number of times equal to its multiplicity (and the origin counted for twice its multiplicity). For instance, referring to the principal block of SL$(2, 9)$ in figure 3.2, we see that if $K = (3, 1)$ and $Q = 4 \cdot (1, 3) + (2, 2) - 2 \cdot (1, 1)$, then $c_{QK} = 4c_{13,31} + c_{22,31} - 2c_{11,31} = 4 + 2 - 2 = 4$. Thus, a $\mathbb{Z}$-linear combination of simple modules can be made to behave just like a single simple module from the viewpoint of computing Cartan invariants. Finally, we note that if Q and R are both $\mathbb{Z}$-linear combinations of labels, then c_{QR} can be calculated by an obvious application of the distributive law.

Definition 24. A $\mathbb{Z}$-linear combination Q of simple modules (all in the same block) is a *virtual cube* if the associated formal sum of relevant vertices has the following properties:

1. Each vertex occurs with multiplicity zero or one, and

[5] This is actually true for the cube $J = (p-1, \ldots, p-1)$ in the even arrangement. For this one cube, the appropriate portion of the Cartan matrix is identical to the portion of the Cartan matrix of SL$(2, 2^n)$ with $\max(|I|, |J|) \leq 1$, and the argument from the previous chapter can be used directly. In this case, a submatrix of D is *equal to* the decomposition matrix of SL$(2, 2^n)$.

[6] This is also true when $n = 2$, in which case a much simpler argument suffices.

2. The vertices with multiplicity one, taken as a set, form the vertices of some k-dimensional unit cube, for some $k \leq n$.

Thus, going back to figure 3.2, we see that $Q = (1,1) - (2,2) + (1,3)$ is a virtual cube. In fact, it is exactly these types of alternating sums which will be useful to us.

Proposition 25. Every $(n-1)$-dimensional face of an interior cube is a virtual cube.

Proof. Let J be a labeled interior cube, and let $m \in N$. To avoid notational difficulties, we will show that *both* $(k-1)$-dimensional faces of J in the m-th coordinate direction are virtual cubes. Since J is interior, we have $1 \leq J_i \leq p-1$ for each $i \in N$.

Now, consider the set of all cubes whose centers differ from the center of J in only the m-th coordinate direction. We claim that all of these cubes are interior, with one exception; furthermore, this one boundary cube has a single p in its label, implying that its set of relevant vertices forms an $(n-1)$-dimensional cube.

To see this, note that the only such cubes which could be boundary are those with m-th coordinate $\pm\frac{p}{2}$. The label of such a cube K will be equal to J in every coordinate position except possibly the m-th and $(m-1)$-th. For these coordinate positions, we have $K_{m-1} = J_{m-1}$ or $p - J_{m-1}$, which is clearly in the range $1 \leq K_{m-1} \leq p-1$, and $K_m = \frac{p}{2} \pm \frac{p}{2}$. Furthermore, both of the signs occur, depending on whether the m-th coordinate of the cube labeled K is $\frac{p}{2}$ or $-\frac{p}{2}$. Thus, one of the two cubes has $K_m = p$, and is the boundary cube claimed; the other has $K_m = 0$, which means the cube doesn't exist.

We may now construct an obvious alternating sum of cubes, starting from the cube labeled J, and working in the m-th coordinate direction toward the cube labeled K. In this alternating sum, every relevant vertex will cancel out, except for those on the face of J where the alternating sum was started. If the sum started with J, then the virtual cube so constructed is the face of J which is farther away from K; if the alternating sum starts with the cube next to J in the direction of K, then the virtual cube constructed is the face of J which is closer to K. □

We are now in a position to salvage the argument proposed earlier. Let J be the label of an interior noncentral cube. Then there is an isometry f mapping $\mathcal{A}_n$ into the current arrangement, such that the cube labeled $\varnothing$ maps to the cube labeled J and relevant vertices map to relevant vertices. Since every vertex of cube $\varnothing$ is relevant, we know that if the cube labeled I in $\mathcal{A}_n$ maps to the cube labeled K, then $c_{\varnothing I} = c_{JK}$.

Now extend the range of f to include virtual cubes. If $B = \{b\}$ is a singleton label of a cube in $\mathcal{A}_n$, then B maps via f to some cube which shares an $(n-1)$-dimensional face with cube J. Replace the image of cube B with the virtual cube V corresponding to this shared $(n-1)$-dimensional face. In effect, this eliminates the relevant vertices of this cube which are not also vertices of J. Thus, if I is a cube in $\mathcal{A}_n$ mapping to the cube labeled K, we have $c_{BI} = c_{VK}$. This eliminates the obstruction to using the result from the previous chapter.

Next, we extend the matrix M to include columns formally labeled by the virtual cubes that we used above. Thus, when we apply the result from the previous chapter, we conclude that a portion of the matrix M is unique; this portion is a submatrix indexed by the columns involved in the above discussion (some real, some virtual), and by one row for each of the vertices of the cube J.

Next, we wish to leverage this knowledge of M into a unique determination of every column within the rows corresponding to the vertices of J. This is not difficult. Let K be some (real) cube. If $c_{JK} = 0$, then column K of M must be zeros within these rows, since column J has only ones in this set of rows. Suppose, then, that $c_{JK} = 2^r$. (Since J is not central, this Cartan invariant is always a power of two.) By examining the Cartan invariants c_{VK} for each virtual cube V which shares a face with J, we are able to uniquely determine column K of M, within the set of rows corresponding to vertices of J. In fact, this process is completely analogous to the determination of column I in the previous chapter, in the case when $|I| > 1$.

Thus, we are able to uniquely determine a subset of the rows of M. Since the matrix E described above gives one possible matrix that satisfies the conditions of the theorem, and we have just proved the uniqueness of certain rows of M, we conclude that these rows must be the same as the corresponding rows of E. Thus, this portion of M is an incidence matrix of relevant vertices and cubes. Repeating this argument for each noncentral interior cube J, we can fill in the matrix M row by row, one for each relevant vertex which is incident to one of these noncentral interior cubes. While doing this for some cube J, it may be the case that some of the rows so determined are already known. However, this presents no difficulty, since there is no harm in showing that a certain row of M is uniquely determined more than once. The existence of the matrix E satisfying the conditions of the theorem guarantees that all such unique determinations of a row will necessarily be the same.

Since we are only using noncentral cubes, we will never gain any information about the remaining rows of M, namely the rows which (in E) correspond to the origin. However, these two rows of E are the same, and therefore the undetermined entries in each column of M must be all zeros, or two ones and some number of zeros. (Recall that we are not assuming we know how many rows M has.) If c_{JJ} is already accounted for by the number of ones in column J of M, then every remaining entry of column J is a zero. If J is some column where this is not the case, then column J must have two more ones, which we place in two new rows. Finally, all such ones must be placed in the same two rows, since we can examine the Cartan invariants c_{JK}, where J and K are both rows which need two more ones. Any additional row beyond these two would necessarily be all zeros, which is not permitted. This proves the theorem. □

3.5 The Case $p = 3$

In this case, we face an additional difficulty: every cube is central or boundary. Therefore, when $\mathcal{A}_n$ is embedded into one of the arrangements in the way discussed above, the Cartan invariants of pairs of cubes in the image might bear little resemblance to the corresponding Cartan invariants in $\mathcal{A}_n$. Fortunately, the solution to this issue has already been discussed: virtual cubes. In order to repair the above argument, we will need to pare down the relevant vertices of cubes in the image to an absolute minimum, which means mapping every cube of $\mathcal{A}_n$ (except $\varnothing$) to a virtual cube which has no additional relevant vertices.

Proposition 26. Every k-dimensional face of an interior cube, for $k \geq 1$, is a virtual cube.

Proof. We prove this by induction on k, starting with $k = n$ and proceeding towards $k = 1$. The base case is trivial, because every n-dimensional interior cube is clearly a virtual cube.

Now suppose that every $(k+1)$-dimensional face of every interior cube is a virtual cube, and let F be a k-dimensional face of an interior cube. Suppose for the moment that there is a boundary cube J whose vertex set is a translate of the vertex set of F in a direction perpendicular to F. If this is so, then we can construct a sequence of $(k+1)$-dimensional faces $L_1, \ldots, L_m$ such that F lies only in L_1, the vertices of J lie only in L_m, and each pair (L_i, L_{i+1}) intersects in a k-dimensional face (which will be a perpendicular translate of F). In this case, the alternating sum $L_1 - L_2 + \cdots \pm L_m \mp J$ will be a $\mathbb{Z}$-linear combination of labels whose vertex set is F, and we will be done.

Thus, we must prove that there is a perpendicular translate of F which is the vertex set of some boundary cube. Let A be the set of coordinate directions that are perpendicular to F, and let K be the label of some (real) cube whose vertices include F. Translating the cube K in a direction perpendicular to F by one unit is equivalent to finding a cube K' for which $K \underset{B}{\rightarrow} K'$, for some subset $B \subseteq A$. Thus, such a perpendicular translate exists if and only if there is a sequence $K \underset{B_1}{\rightarrow} L_1 \underset{B_2}{\rightarrow} L_2 \ldots L_m$, where L_m is the desired boundary cube whose vertex set is a k-dimensional cube and each B_i is a subset of A.

Now, $k \geq 1$, so $A \neq N$. Without loss of generality, suppose that $1 \notin A$. We claim that we can successively translate the cube labeled K in coordinate directions in the set A, until we have $K_i = p$ for all $i \in A$. Let i be the largest element of A. If we translate K one unit in the i-th coordinate direction, we must modify K by replacing K_i with $K_i \pm 1$ (depending on whether we translate in the positive or negative direction along the i-th coordinate axis), and K_{i-1} with $p - K_{i-1}$. We do this, choosing to replace K_i with $K_i + 1$, until we have $K_i = p$. If we performed this translation operation an odd number of times, we will have replaced K_{i-1} with $p - K_{i-1}$; however, this is not a problem, because K was originally an interior cube, and thus we have $1 \leq K_{i-1} \leq p - 1$. This inequality still holds after an odd number of translations in the i-th coordinate direction.

Now we repeat the argument for the next largest element of A, and so on by induction. When we are done, we will have $K_i = p$ for all $i \in A$, and $1 \leq K_i \leq p-1$ for all $i \notin K$. Finally, since $1 \notin A$, there is no possibility that K_n will be inadvertently modified in the final step of the induction.

The resulting cube will have p in its label $|A| = n-k$ times, implying that it has the same number of vertices as the k-dimensional face F. Moreover, it was obtained by translation of a cube K containing F in directions perpendicular to F. This proves the proposition. □

This proposition would allow us to modify the function f discussed above even further, so that every cube except $\varnothing$ is mapped to a virtual cube in the even or odd arrangement. However, this is not sufficient to prove the theorem for $p = 3$, because the even and odd arrangements are in the space $\mathbb{R}^n/\{\pm 1\}$. Thus, if we carelessly map $\mathcal{A}_n$ into the even or odd arrangement, with $\varnothing$ mapping to a central cube, we may not have a one-to-one function on cubes and vertices. In fact, this is why we avoided the central cubes in the first place when proving the theorem for $p \geq 5$.

To circumvent this difficulty, we make the following observation: every cube in $\mathcal{A}_n$ except $\varnothing$ has at least one of its central coordinates x_i equal to 1. Therefore, it is possible to precompose f with a rotation so that every cube except $\varnothing$ in $\mathcal{A}_n$ maps to a virtual cube which lies on the boundary of the current arrangement. In other words, we arrange to map the relevant vertex $(-1/2, \ldots, -1/2)$ in $\mathcal{A}_n$ to the origin. With this modification, every cube except the image of $\varnothing$ avoids the origin, and we are guaranteed a one-to-one mapping of cubes and relevant vertices. Thus, the Cartan invariants in the image are now equal to the Cartan invariants in $\mathcal{A}_n$, with the single exception that $c_{\varnothing\varnothing}$ changes from 2^n to $2^n + 1$ in the image. In this case, it is clear that the result from the previous chapter still holds, with the row of the decomposition matrix corresponding to the trivial module occurring twice instead of once.

Applying this result, we obtain a portion of the matrix M (extended by the addition of columns for the virtual cubes we used) with rows corresponding to the relevant vertices in the image of f, and with columns corresponding to the single real cube and many virtual cubes which played a role in the calculation above. We now finish the argument just as in the case $p \geq 5$. □

APPENDIX: CYCLIC BLOCKS

In this appendix, we prove Proposition 1 from the introduction. Let B be a cyclic block of kG with Cartan matrix C, and assume the Brauer tree of B has no exceptional vertex, and is not a star with three edges. We will show that the matrix equation $D^{\mathsf{T}} D = C$ is sufficient to recover D, up to a permutation of rows.

Since the Brauer tree has no exceptional vertex, we have $c_{MM} = 2$ for any simple kG-module M. If M and N are distinct simple kG-modules, then $c_{MN} = 1$ if the edges M and N of the Brauer tree share a vertex, and $c_{MN} = 0$ otherwise.

The proposition is clearly true if the Brauer tree is a single edge, so assume there is more than one simple kG-module. We begin by finding a kG-module A with the property that, whenever $c_{AB} \neq 0$ and $c_{AC} \neq 0$, then $c_{BC} \neq 0$. The edge in the Brauer tree labeled A will necessarily have one endpoint not connected to any other edges. Let $\{B_1, \ldots, B_k\}$ be the simple modules with nonzero Cartan invariants with A. We know that each of the columns $\{A, B_1, \ldots, B_k\}$ of D has two ones, and each pair of these columns shares a single one in some row of D.

Suppose column A has ones in rows R_1 and R_2. If $k = 1$, then we may place ones in column B_1 in rows R_1 and R_3 without loss of generality. If $k \geq 2$, then we argue as follows: without loss of generality, place ones in column B_1 in rows R_1 and R_3. At this point, we have a nontrivial choice for which rows have ones in column B_2: we may place ones in rows R_1 and R_4, or in rows R_2 and R_3.

The latter choice must be eliminated, since it leads to a Brauer graph which contains a triangle. Since the Brauer tree is not a star with three edges, either $k > 2$, or there is an edge U which does not share a vertex with A, but does share a vertex with B_1 or B_2. If $k > 2$, then we observe that column B_3 must share exactly one one with columns A, B_1, and B_2, which is impossible in the latter case. If there is an edge U which shares a vertex with, say, edge B_1 but not with edge A nor edge B_2, then column B_3 has a one in some row which has a one in column B_1, but zeros in columns A and B_2. Again, this is impossible in the latter case.

Therefore, column B_2 has ones in rows R_1 and R_4. Continuing with the columns B_i for $i > 2$ (if any), we clearly see that each of these columns must have ones in rows R_1 and R_{i+2} (without loss of generality). Finally, if U is a simple module with $c_{AU} = 0$, we clearly have zeros in column U in rows R_1 and R_2.

Note that we have completely determined rows R_1 and R_2, and column A, of D. Furthermore, row R_2 contains a single one in column A. At this point, we can remove row R_2 and column A from the decomposition matrix, and recalculate a new matrix $C' = D^\top D$ which has one fewer rows and columns. Applying induction, there is a unique matrix D' such that ${D'}^\top D' = C'$.[7] Adding back row R_2 and column A recovers the original decomposition matrix, which is now uniquely determined. This proves the proposition.

A careful refinement of this argument would show that the proposition holds if B has an exceptional vertex of multiplicity two. If the multiplicity is three, we must also exclude the case of a single edge, in which case $C = [4]$. If the exceptional vertex has multiplicity four or larger, then the theorem is false for every Brauer tree B. For instance, if B is a star with four edges, with exceptional vertex of multiplicity four in the middle, then:

$$C = \begin{bmatrix} 5 & 4 & 4 & 4 \\ 4 & 5 & 4 & 4 \\ 4 & 4 & 5 & 4 \\ 4 & 4 & 4 & 5 \end{bmatrix},$$

[7] Of course, it is possible that we will arrive at a star with three edges after applying induction some number of times. However, in such a case, the *original* Brauer tree was not a star with three edges, so we may use a simple module whose column of D has already been determined in order to eliminate the possibility of a triangle in the Brauer graph.

which admits the decomposition matrices

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \qquad \text{and} \qquad D = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix}.$$

In general, we can replace any row of zeros and ones which appears four times with a single row of zeros and twos.

Moreover, the proposition is also false if the Brauer tree is a star with three edges. In this case, we see from the proof that there are two possible matrices D with $D^{\mathsf{T}}D = C$, namely

$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \text{and} \qquad D = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Of course, the second possibility can't be a decomposition matrix, since it is square.

REFERENCES

[1] J. L. ALPERIN, Projective Modules for $\mathrm{SL}(2, 2^n)$, *J. Pure Appl. Algebra* **15** (1979), 219–234.

[2] R. BRAUER AND C. NESBITT, On the Modular Characters of Groups, *Ann. of Math.* **42** (1941), 556–590.

[3] R. BURKHARDT, Die Zerlegungsmatrizen der Gruppen $\mathrm{PSL}(2, p^f)$, *J. Algebra* **40** (1976), 75–96.

[4] Y. CHENG, On the Cartan Invariants of $\mathrm{SL}(2, p^m)$, *Comm. in Algebra* **14** (1986), 507–515.

[5] J. H. CONWAY, R. T. CURTIS, S. P. NORTON, R. A. PARKER, AND R. A. WILSON, *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Oxford University Press, Oxford, 1985.

[6] P. W. A. M. VAN HAM, T. A. SPRINGER, AND M. VAN DER WEL, On the Cartan Invariants of $\mathrm{SL}_2(\mathbb{F}_q)$, *Comm. in Algebra* **10** (1982), 1565–1588.

[7] J. E. HUMPHREYS, Projective Modules for $\mathrm{SL}(2, q)$, *J. Algebra* **25** (1973), 513–518.

[8] ———, Cartan Invariants and Decomposition Numbers of Chevalley Groups, *Proc. Sympos. Pure Math.* **37** (1980), 347–351.

[9] A. V. JEYAKUMAR Principal Indecomposable Representations for the Group $\mathrm{SL}(2, q)$ *J. Algebra* **30** (1974), 444–458.

[10] H. KOSHITA, Quiver and Relations for $\mathrm{SL}(2, 2^n)$ in Characteristic 2, *J. Pure Appl. Algebra* **97** (1994), 313–324.

[11] ———, Quiver and Relations for $\mathrm{SL}(2, p^n)$ in Characteristic p With p Odd, *Comm. in Algebra* **26** (1998), 681–712.

[12] B. SRINIVASAN, On the Modular Characters of the Special Linear Group $\mathrm{SL}(2, p^n)$, *Proc. London Math. Soc.* **14** (1964), 101–114.

[13] B. S. UPADHYAYA, Composition Factors of the Principal Indecomposable Modules for the Special Linear Groups $\mathrm{SL}(2, q)$, *J. London Math. Soc.* **17** (1978), 437–445.