EINDHOVEN UNIVERSITY OF TECHNOLOGY
Department of Mathematics and Computing Science

MASTER'S THESIS

On the p-rank of the adjacency matrices of strongly regular graphs

C.A. van Eijl

Supervisor : Prof. dr. A.E. Brouwer

October 1991

Contents

Introduction

In this thesis we study the rank over the finite field of p elements, or p-rank, of the adjacency matrices of strongly regular graphs. Such matrices may be used as generator matrices for p-ary codes and in this connection the determination of the p-rank is of particular importance, since it is the dimension of the code.

For various incidence structures, the p-ranks of associated $(0,1)$ matrices have been investigated. As an example of such investigations that are explicitly related to error correcting codes, we mention the papers of Bagchi and Sastry [2] and Hamada [9], who deal with generalized polygons and block designs, respectively. However, also other problems give rise to the study of the p-rank of incidence matrices. For example, Linial and Rothschild [13] solve a set theoretical problem by determining the p-rank of the incidence matrix of subsets (see also Wilson [21]). Furthermore, self-dual codes associated with symmetric designs are investigated by Lander [12] in order to derive new results on the parameters of such designs. Bagchi, Brouwer and Wilbrink [1] and Brouwer and Haemers [3] give results on the p-rank of the adjacency matrices of some strongly regular graphs. As a matter of fact, these are the only papers known to us which deal with our subject.

Let A denote the adjacency matrix of a strongly regular graph. We shall not restrict our investigations to the p-rank of A, but study the p-rank of $A + \tau I$ for any integer τ. For most combinations of p and τ, the p-rank of $A + \tau I$ is completely determined by the parameters of the graph. For the remaining cases, it is really necessary to investigate the structure of the graph.

Linear algebra, coding theory and group theory play an important role in deriving results on the p-rank of a strongly regular graph[1]. Chapter 1 gives a survey of the concepts used from these areas. Besides that, it provides an introduction to the theory of strongly regular graphs.

The p-rank of an integral matrix is easily derived from its Smith normal form, which is the subject of Chapter 2. We shall determine the Smith normal form of the adjacency matrices of two infinite families of strongly regular graphs, namely, the lattice graphs and the triangular graphs.

In Chapter 3 the p-rank of strongly regular graphs with integral eigenvalues is considered. We isolate the combinations of p and τ for which the determination of the p-rank of $A + \tau I$ is nontrivial and give a general upper bound for these cases. Furthermore, it is investigated how the p-ranks of switching-equivalent graphs are related.

Chapter 4 deals with Paley graphs. For these graphs, the p-rank of $A + \tau I$ will be determined for every p and τ.

In Chapter 5 it is shown how character theory can be used to obtain a set of possible values for the p-rank of a graph. We also investigate for which graphs such a set is expected to be small.

In the last chapter we determine (bounds for) the p-rank of a considerable number of graphs, especially sporadic graphs. A table of the results concludes this chapter.

[1] By the rank of a graph we mean the rank of its adjacency matrix.

Chapter 1

Preliminaries

In this thesis many concepts from different areas of mathematics are used. Although most of them are elementary, we think it convenient for the reader to have a brief survey. Besides that, some notation is introduced and a few results on matrices and strongly regular graphs are given. The results are stated without proof, for which the reader is referred to the literature. As far as matrix theory is concerned, proofs can be found in any textbook, for example Marcus and Minc [16]. For the theory of strongly regular graphs we refer to the surveys of Cameron [5] and Seidel [19].

The first convention is that the letter p always denotes a prime. We assume that the reader is familiar with the basic notions from the theory of finite fields. If not, it suffices to study the first sections of Chapter 4 of MacWilliams and Sloane [15]. A finite field with q elements is denoted by $\mathbb{F}_q$.

1.1 Matrix theory

Let us first establish some notation. The set of all $n \times m$ matrices with entries in a field F is denoted by $F^{n\times m}$. We shall mainly deal with square matrices. Usually, the rows and columns of a matrix will be indexed by elements of a given set. A vector $\underline{x}$ always denotes a row vector.

The $n \times n$ identity matrix is denoted by I_n. Furthermore, O_n denotes the $n \times n$ all-zero matrix and J_n the all-one matrix of size n. The all-one and all-zero vector are written as $\underline{1}_n$ and $\underline{0}_n$, respectively. When no confusion can occur, the index n is omitted.

We write $\mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for a diagonal matrix of size n with diagonal elements α_i, $1 \leq i \leq n$. $\mathrm{Diag}(\alpha_1^{m_1}, \alpha_2^{m_2}, \ldots)$ denotes the matrix

$$\mathrm{diag}(\overbrace{\alpha_1, \ldots, \alpha_1}^{m_1}, \overbrace{\alpha_2, \ldots, \alpha_2}^{m_2}, \ldots).$$

Similarly, a block diagonal matrix consisting of n_1 blocks M_1, n_2 blocks M_2, etc., is denoted by $\mathrm{diag}(M_1^{n_1}, M_2^{n_2}, \ldots)$.

Denote by V the n-dimensional vectorspace over F. Let V_1 and V_2 be linear subspaces of V. The sum of V_1 and V_2 is denoted by $V_1 + V_2$. If $V_1 \cap V_2 = \{\underline{0}\}$, then we write $V_1 \oplus V_2$ for the direct sum of the two subspaces.

Now let F be a field and let M be an element of $F^{n\times n}$ for some integer n. The matrix M is said to be *nonsingular* if $\det(M) \neq 0$ and *singular* otherwise. The *characteristic polynomial* of M is the polynomial $p(z) = \det(M - zI)$. The *eigenvalues* of M are the zeros of $p(z)$. If λ is an eigenvalue of

M, then there exists a nonzero vector $\underline{x}$ such that $\underline{x}M = \lambda\underline{x}$. The vector $\underline{x}$ is called an *eigenvector* of M (belonging to λ). By the *algebraic multiplicity* of λ we mean its multiplicity as a root of $p(z)$. The *geometric multiplicity* is the dimension of the corresponding *eigenspace* $V_\lambda := \{\underline{x} \in V \mid \underline{x}M = \lambda\underline{x}\}$. The *spectrum* of M is the set of eigenvalues including their algebraic multiplicities.

The geometric multiplicity of λ is at most its algebraic multiplicity. If equality holds, then

$$\sum_{\lambda_i} \dim(V_{\lambda_i}) = n. \tag{1.1}$$

This is equivalent to the assertion that V has a basis consisting of the eigenvectors of M. In this case, we omit the adjective and speak about the multiplicity of the eigenvalue.

The matrix M is called *diagonalizable* if there exists a nonsingular matrix $S \in F^{n\times n}$ such that $S^{-1}MS = \Lambda$, where Λ is a diagonal matrix. M is diagonalizable if and only if (1.1) holds. If $M' \in F^{n\times n}$, $MM' = M'M$ and both matrices are diagonalizable, then they can be diagonalized by the same nonsingular matrix S.

Set $\langle \underline{x}_1, \ldots, \underline{x}_m \rangle := \{\sum_{i=1}^m \alpha_i \underline{x}_i | \alpha_i \in F\}$, the vectorspace over F generated by $\underline{x}_1, \ldots, \underline{x}_m$. We write $\mathcal{R}_F(M)$ for the *rowspace* of M over F, that is, the vectorspace generated by the rows of M. The *F-rank* of M is defined as the dimension of $\mathcal{R}_F(M)$. We use the notation $r_F(M)$. In the special case that $F = \mathbb{F}_q$, we write $r_q(M)$ and $\mathcal{R}_q(M)$ to denote the rank and rowspace of M over $\mathbb{F}_q$, respectively.

The *kernel* of M over F, denoted by $\mathcal{N}_F(M)$, is defined as

$$\mathcal{N}_F(M) := \{\underline{x} \mid \underline{x}M = \underline{0}\}.$$

We have

$$\dim \mathcal{R}_F(M) + \dim \mathcal{N}_F(M) = n.$$

Clearly, if λ is an eigenvalue of M, then $V_\lambda = \mathcal{N}_F(M - \lambda I)$.

M is said to be *equivalent* to M' if there exist two nonsingular elements P and Q of $F^{n\times n}$, such that $M = PM'Q$. Notation:

$$M_1 \simeq M_2.$$

If $r_F = r$, then $M \simeq \mathrm{diag}(1^r, 0^{n-r})$.

The following row operations are called *elementary*:

(i) interchanging rows;

(ii) adding a multiple of a row to another row;

(iii) multiplying a row by a nonzero element of F.

The elementary column operations are defined similarly. It is evident that if $M \simeq M'$, then M can be obtained from M' by applying a sequence of elementary row and column operations.

The *trace* of M is the sum of its diagonal elements and is denoted by $\mathrm{tr}(M)$. One easily sees that it satisfies the following property:

$$\mathrm{tr}(MM') = \mathrm{tr}(M'M), \quad M, M' \in F^{n\times n}.$$

If Ω is a set and $\Omega' \subset \Omega$, then the *characteristic vector* of Ω' is the vector $\underline{c}$ with coordinates indexed by the elements of Ω satisfying

$$c_\omega = \begin{cases} 1 & \text{if } \omega \in \Omega' \\ 0 & \text{otherwise.} \end{cases}$$

Finally, a *permutation matrix* is a square matrix which has precisely one 1 in each column and each row and zeros elsewhere.

1.2 Graph theory

1.2.1 General concepts

A (simple, undirected) *graph* Γ is a pair (V, E), where V is a finite nonempty set of elements called *vertices* and E is a finite set of unordered pairs of distinct vertices of V called *edges*. The number of vertices of Γ is called the *order* of Γ and is denoted by v. If $e = \{x, y\}$ is an edge of Γ, then x and y are said to be *adjacent* and e is said to be *incident* to x and y. For each vertex x in a graph Γ, the number of vertices adjacent to x is called the *valency* of x. A vertex of valency 0 is called an *isolated vertex*. If all the vertices of Γ have the same valency, then Γ is said to be a *regular* graph.

A *subgraph* of a graph Γ is a graph $\Delta = (V_1, E_1)$ such that $V_1 \subseteq V$ and $E_1 \subseteq E$. If V_1 is any subset of vertices of Γ, then the subgraph *induced* by V_1 is the subgraph of Γ obtained by taking the vertices in V_1 and joining those pairs of vertices of V_1 which are joined in Γ. An *induced subgraph* of Γ is a subgraph induced by some subset V_1 of V.

The *complement* of Γ (denoted by $\bar{\Gamma}$) is the graph with the same vertex set as Γ, but where two vertices are adjacent iff they are not adjacent in Γ.

A graph consisting of v isolated vertices is called a *coclique* of size v. Its complement is a regular graph of valency $v - 1$, which is called the *complete* graph or *clique* of size v.

Two graphs Γ and Δ are said to be *isomorphic* (written $\Gamma \cong \Delta$) if there is a one-to-one correspondence between their vertex sets which preserves the adjacency of vertices. An *automorphism* of Γ is a one-to-one mapping ϕ of V onto itself such that $\phi(x)$ and $\phi(y)$ are adjacent iff x and y are. The automorphisms of Γ form a group under composition, called the *automorphism group* of Γ. It is said to be *transitive* if it contains transformations mapping each vertex of Γ to every other vertex.

A graph Γ can be described by its (0,1) *adjacency matrix* A of size v defined by numbering the vertices and taking $a_{ij} = 1$ iff the vertices i and j are adjacent. By the *eigenvalues* of Γ, we mean the eigenvalues of A, which are independent of the numbering of the vertices. Since A is a symmetric matrix, its eigenvalues are real. Graphs with the same spectrum are called *cospectral*. Cospectral graphs are not necessarily isomorphic. Denote by B the adjacency matrix of $\bar{\Gamma}$, the complement of Γ, then

$$I_v + A + B = J_v.$$

When considering a graph Γ, its adjacency matrix will always be denoted by A_Γ, unless stated otherwise. If no confusion can occur, we simply write A.

1.2.2 Strongly regular graphs

A graph is called *strongly regular* if there exist integers k, λ and μ such that:

1. the graph is regular with valency k;
2. the number of vertices adjacent to two adjacent vertices is λ;
3. the number of vertices adjacent to two non-adjacent vertices is μ.

If Γ is a strongly regular graph (or *srg* for short) with parameters (v, k, λ, μ), then its complement $\bar{\Gamma}$ is also strongly regular with parameters

$$(\bar{v}, \bar{k}, \bar{\lambda}, \bar{\mu}) = (v, v - k - 1, v - 2k + \mu - 2, v - 2k + \lambda).$$

Usually, the valency of $\bar{\Gamma}$ is denoted by l. Disconnected graphs and their complements will be excluded, i.e. we assume $0 < \mu < k < v - 1$.

Let A be the adjacency matrix of Γ. For the rest of this section, A is regarded as an element of $\mathbb{R}^{v \times v}$. The matrix A satisfies

$$\begin{aligned} AJ &= kJ, \\ A^2 &= kI + \lambda A + \mu(J - I - A). \end{aligned} \tag{1.2}$$

We see that the all-one vector is an eigenvector of A with eigenvalue k. The adjacency matrix A has two other eigenvalues r and s ($r > s$), which are the solutions of $x^2 + (\mu - \lambda)x + (\mu - k) = 0$. Their multiplicities f and g satisfy

$$\begin{aligned} f + g &= v - 1, \\ k + fr + gs &= 0. \end{aligned}$$

Clearly, f and g can be expressed in terms of v, k, λ and μ. From the integrality of f and g, a strong necessary condition on the parameters of a srg is obtained. If $f = g$ (the so-called *half-case*), we have $v = 4\mu + 1$, $k = 2\mu$, $\lambda = \mu - 1$ and the graph has the same parameters as its complement. Otherwise, the eigenvalues r and s are integers.

For later use, we mention the following relations between k, λ, mu, r and s:

$$\lambda - \mu = r + s, \quad \mu = k + rs. \tag{1.3}$$

These relations immediately follow from the equality $x^2 + (\mu - \lambda)x + (\mu - k) = (x - r)(x - s)$.

Let $\mathcal{A}$ be the linear span of $\{I, A, B\}$ over $\mathbb{R}$, where B denotes the adjacency matrix of $\bar{\Gamma}$. The vectorspace $\mathcal{A}$ is closed with respect to ordinary matrix multiplication and is called the *adjacency algebra* or *Bose-Mesner algebra* of Γ. Since the matrices in $\mathcal{A}$ are symmetric and commute with each other, they can be simultaneously diagonalized. Therefore, $\mathcal{A}$ admits a (unique) basis of *minimal idempotents* $\{E_0, E_1, E_2\}$ satisfying

$$\begin{aligned} \sum_{i=0}^{2} E_i &= J, \\ E_i E_j &= \delta_{ij} E_i, \end{aligned} \tag{1.4}$$

where δ_{ij} denotes the Kronecker delta. The following tables list them as linear combinations of the basis $\{I, A, B\}$ and vice versa:

	I	A	B
vE_0	1	1	1
vE_1	f	$f\frac{r}{k}$	$-f\frac{r+1}{l}$
vE_2	g	$g\frac{s}{k}$	$-g\frac{s+1}{l}$

	E_0	E_1	E_2
I	1	1	1
A	k	r	s
B	l	$-r-1$	$-s-1$

From the right hand table and (1.4), we obtain that $AE_1 = rE_1$ and $AE_2 = sE_2$. The columns of the E_i span the eigenspaces of all the matrices of $\mathcal{A}$. Thus the rank of E_i equals the dimension of the ith eigenspace. It follows that $r(E_1) = f$ and $r(E_2) = g$, where $r(M)$ denotes the $\mathbb{R}$-rank of M.

The last concept discussed here is *switching*. Let $\Gamma = (V, E)$ be a (not necessarily strongly regular) graph and let V_1 be a nonempty proper subset of V. Set $V_2 := V \setminus V_1$. We construct a new graph $\Gamma' = (V, E')$ in the following way:

$$\begin{aligned}&\text{if } v_1, v_1' \in V_1, \text{ then } \{v_1, v_1'\} \in E' \text{ iff } \{v_1, v_1'\} \in E;\\ &\text{if } v_2, v_2' \in V_2, \text{ then } \{v_2, v_2'\} \in E' \text{ iff } \{v_2, v_2'\} \in E;\\ &\text{if } v_1 \in V_1, v_2 \in V_2, \text{ then } \{v_1, v_2\} \in E' \text{ iff } \{v_1, v_2\} \notin E.\end{aligned}$$

Γ and Γ' are said to be *switching-equivalent*. V_1 is called the *switching-set*.

It can be proven that if Γ is strongly regular, its parameters satisfy

$$v + 4rs + 2r + 2s = 0$$

and Γ' is regular, then Γ' is again a srg, either with different parameters, or with the same parameters but nonisomorphic to Γ, or isomorphic to Γ. If $V_1 = \{y \mid x \sim y\}$ for an arbitrary vertex x of Γ, then Γ' is the disjoint union of x and a srg with $k = 2\mu$.

1.3 Codes

We shall recall only a few basic concepts from coding theory here.

By a p-ary *linear code* C of length n and dimension k, we mean a k-dimensional subspace of the n-dimensional vectorspace over $\mathbb{F}_p$ provided with its standard basis. The elements of C are called *codewords*. A third parameter of the code is the *minimum distance* d, defined as

$$d := \min\{d(\underline{c}_1, \underline{c}_2) \mid \underline{c}_1, \underline{c}_2 \in C,\ \underline{c}_1 \neq \underline{c}_2\}\ ,$$

where the *Hamming distance* $d(\underline{x}, \underline{y})$ between two n-tuples $\underline{x}$ and $\underline{y}$ denotes the number of coordinates on which $\underline{x}$ and $\underline{y}$ differ. If C has minimum distance d, then C is a $\lceil \frac{d-1}{2} \rceil$-error correcting code.

If $\{\underline{c}_1, \ldots, \underline{c}_k\}$ is a basis for C, then the matrix

$$M_C = \begin{pmatrix} \underline{c}_1 \\ \vdots \\ \underline{c}_k \end{pmatrix}$$

is called a *generator matrix* for C.

The *dual* $C^\perp$ of C is defined as

$$C^\perp := \{\underline{x} \in \mathbb{F}_p^n \mid (\underline{c}, \underline{x}) = 0 \text{ for all } \underline{c} \in C\},$$

where $(\cdot, \cdot)$ denotes the ordinary inner product. The dimension of $C^\perp$ is $n - k$. The code C is said to be *self-orthogonal* if $C \subset C^\perp$. In case $C = C^\perp$, the code is called *self-dual*.

1.4 Groups

In this section a few elementary concepts from group theory are recalled. For more details we refer to Suzuki [20].

We assume the reader to be familiar with the concept of a group. Let G be a finite group with identity e. The number of elements of G is called the *order* of the group and denoted by $|G|$. If g is an element of G, then the *order* of g is defined as the smallest integer n for which $g^n = e$.

The set $\{g^{-1}g_1g \mid g \in G\}$ is called the *conjugacy class* of g_1. A subgroup H of G is called *normal* if $H^g := \{g^{-1}hg \mid h \in H\} = H$ for every $g \in G$. If H is a normal subgroup of G, then the *factor group* G/H is defined as the group of *cosets* $gH := \{gh \mid h \in H\}$ with multiplication $(g_1H)(g_2H) := (g_1g_2)H$. The *index* of H in G is the order of G/H.

Let G and G' be two groups. A function $f : G \longmapsto G'$ is called a *homomorphism* from G into G' if it satisfies

$$f(g_1)f(g_2) = f(g_1g_2) \text{ for all } g_1, g_2 \in G.$$

If f induces a one-to-one correspondence and is surjective, then f is said to be an *isomorphism*. In that case, we say that G and G' are *isomorphic* and write $G \simeq G'$.

If G acts on a set X, then the action of G is written on the right. Thus, if $x \in X$ and $g \in G$, then the image of x under g is denoted by xg. The *orbit* of x is defined as

$$\{xg \mid g \in G\}.$$

If X is itself an orbit, then G is called *transitive*.

A *ring* R is an additive abelian group (i.e. $x + y = y + x$ for all $x, y \in R$), together with a multiplication satisfying $(xy)z = x(yz)$, $x(y+z) = xy+xz$, $(x+y)z = xz+yz$ and which contains an identity element e such that $xe = ex = x$. Furthermore, let F be a field and V a vectorspace over F which is also a ring. If $(c\underline{u})\underline{v} = c(\underline{uv}) = \underline{u}(c\underline{v})$ for all $c \in F$ and $\underline{u}, \underline{v} \in V$, then V is called an *F-algebra*.

Chapter 2

The Smith normal form

Throughout this section, M denotes an $n \times n$ matrix with integral entries and $\mathbb{R}$-rank r. The Smith normal form of M is a diagonal matrix obtained from M by a sequence of elementary row and column operations over $\mathbb{Z}$, from which the p-rank of M is easily derived for all primes p. We first give definitions and prove some general results. In the second section, the Smith normal form of the adjacency matrices of triangular graphs and lattice graphs is calculated.

2.1 Definitions and results

For more details on the theory discussed here we refer to Newman [17].

Definitions M is called *unimodular* if $|\det(M)| = 1$. Two integral matrices M and N are said to be *unimodularly equivalent* (denoted by $M \sim N$) if there exist unimodular matrices P and Q such that $M = PNQ$.

Theorem 2.1 *M is unimodularly equivalent to a diagonal matrix $S = \mathrm{diag}(s_1, ..., s_r, 0, ..., 0)$, where r is the $\mathbb{R}$-rank of M and $s_i \mid s_{i+1}$, $1 \leq i \leq r-1$.*

PROOF. If M is the all-zero matrix, then there is nothing to prove. Hence, we assume that M contains a nonzero element, that can be brought to the (1,1) position by suitable row and column interchanges. Applying the Euclidean algorithm, this element may be replaced by the greatest common divisor of the elements of the first row and column. Now all these elements, except the (1,1) element, can be made zero. Denote this new matrix by $\bar{M}$. Clearly, $M \sim \bar{M}$. Suppose that $\bar{M}$ contains an element $\bar{m}_{ij}$ that is not divisible by $\bar{m}_{11}$. Adding the ith row to the first row and proceeding as described before, we finally reach a state where the element in the (1,1) position divides every element of the matrix, and all the other elements of the first row and column are zero.

The entire procedure is now repeated with the submatrix obtained by deleting the first row and column of $\bar{M}$. Since unimodularly equivalent matrices have the same rank, we eventually obtain a diagonal matrix with the required properties. □

Theorem 2.2 *The diagonal entries of the matrix S which is described by Theorem 2.1, are uniquely determined, up to sign.*

For the proof of this theorem we introduce the concept of the *determinantal divisors* of M, $d_i(M)$, $1 \leq i \leq n$. They are defined as the greatest common divisor of all determinants of $i \times i$ submatrices of M.

PROOF OF THE THEOREM. From the fact that unimodularly equivalent matrices have the same determinantal divisors (see [17] for a proof), it follows that

$$d_i(M) = \prod_{j=1}^{i} s_j\,, \quad 1 \le i \le r.$$

Thus $s_1 = d_1(M)$ and $s_i = d_i(M)/d_{i-1}(M)$, $2 \le i \le r$. Since the determinantal divisors are determined up to sign, the statement is proved. □

S is called the *Smith normal form* (SNF) of M. We shall use the notation $S(M)$. The s_i are known as the *invariant factors* of M.

The p-rank of M is easily derived from $S(M)$. Let $S(M) = \mathrm{diag}(s_1, \ldots, s_r, 0, \ldots, 0)$. Then $r_p(M) = r_p(S(M)) = r^*$, where r^* satisfies $p \nmid s_{r^*}$ and $p \mid s_{r^*+1}$. Clearly, we have $r_p(M) \le r$, the rank of M over the real field.

Example 2.1 Let us determine the SNF of $J_n - I_n$, the adjacency matrix of the complete graph of size n.

$$J_n - I_n = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & -1 & 0 & \cdots & 0 \\ 1 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & -1 \end{pmatrix} \sim \mathrm{diag}(1^{n-1}, n-1).$$

Thus

$$r_p(J_n - I_n) = \begin{cases} n-1 & \text{if } p \mid (n-1) \\ n & \text{otherwise.} \end{cases}$$

More generally, $S(J_n + \tau I_n) = \mathrm{diag}(1, \tau^{n-2}, \tau(\tau+n))$, $\tau \in \mathbb{Z}$.

If for M a unimodularly equivalent diagonal matrix is known, then $S(M)$ is easily determined. Let $S(M) = \mathrm{diag}(s_1, \ldots, s_r, 0, \ldots, 0)$ and let $p_1, p_2, \ldots, p_k$ be the complete set of primes which occur as divisors of the s_i. Thus for appropriate nonnegative integers e_{ij} we have

$$\begin{aligned} s_1 &= p_1^{e_{11}} p_2^{e_{12}} \cdots p_k^{e_{1k}}, \\ &\vdots \\ s_r &= p_1^{e_{r1}} p_2^{e_{r2}} \cdots p_k^{e_{rk}}. \end{aligned}$$

Since $s_i | s_{i+1}$, $1 \le i \le r-1$, the e_{ij} satisfy

$$0 \le e_{1j} \le e_{2j} \le \ldots \le e_{rj}, \quad 1 \le j \le k.$$

The set of prime powers $p_j^{e_{ij}}, 1 \le i \le r, 1 \le j \le k$, including repetitions, is called the set of *elementary divisors*. Given this set, the invariant factors can easily be reconstructed because of the ordering condition. If

$$e_j := \max_{1 \le i \le r} e_{ij}, \quad 1 \le j \le k,$$

then $s_r = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Deleting these primes from the set of elementary divisors, we determine s_{r-1} in the same way, and so on. This leads to the following theorem:

Theorem 2.3 *If $M \sim \Lambda = \mathrm{diag}(\lambda_1, \ldots, \lambda_r, 0, \ldots, 0)$, then the set of prime power factors of the $\lambda_i, 1 \leq i \leq r$, is equal to the set of elementary divisors of $S(M)$.*

PROOF. We first note that from Theorem 2.2 it follows that $S(M) = S(\Lambda)$. Let p be any prime that divides some $\lambda_i, 1 \leq i \leq r$. Order the λ_i according to ascending powers of p:

$$\begin{aligned} \lambda_{i_1} &= p^{e_1}\mu_1, \ (p, \mu_1) = 1, \\ &\vdots \\ \lambda_{i_r} &= p^{e_r}\mu_r, \ (p, \mu_r) = 1, \end{aligned}$$

so that $0 \leq e_1 \leq \ldots \leq e_r$. Then d_i, the i-th determinantal divisor of Λ, satisfies

$$d_i = p^{e_1 \cdots e_i}\mu, \ (p, \mu) = 1.$$

Thus, if s_i denotes the i-th invariant factor of $S(\Lambda)$, and hence of $S(M)$, then

$$\begin{aligned} s_1 &= d_1, \\ s_i &= d_i/d_{i-1} = p^{e_i}\bar{\mu}, \ (p, \bar{\mu}) = 1, \ 2 \leq i \leq r. \end{aligned}$$

Thus p^{e_i} is an elementary divisor, $1 \leq i \leq r$. Applying the same argument for all primes p which divide some λ_i, we obtain the result. □

2.2 Applications of the Smith normal form

The adjacency matrices of lattice graphs and triangular graphs have a very simple structure. This enables us to compute their SNF by hand.

The *lattice graph* $L_2(n)$ has as vertices the ordered pairs $(x, y) \in \{1, \ldots, n\}^2$, where two vertices are adjacent iff they have a common coordinate. $L_2(n)$ has parameters $(v, k, \lambda, \mu) = (n^2, 2(n-1), n-2, 2)$. For $n \neq 4$, $L_2(n)$ is unique, i.e. every graph with the same parameters is isomorphic to $L_2(n)$. For $n = 4$, there is exactly one nonisomorphic cospectral graph, the *Shrikhande graph* (see Cameron [5] for a description).

Proposition 2.4 *The SNF of the lattice graph $L_2(n)$ is equal to*

$$\mathrm{diag}(1^{2n-2}, 2^{(n-2)^2}, \{2(n-2)\}^{2n-3}, 2(n-1)(n-2)).$$

PROOF. Let A_n be the adjacency matrix of $L_2(n)$ with columns and rows indexed in the following

order: $(1,1),(1,2),\ldots,(1,n),(2,1),\ldots,(n,n)$. Then

$$A_n = \begin{pmatrix} J_n - I_n & I_n & I_n & \cdots & I_n \\ I_n & J_n - I_n & I_n & \cdots & I_n \\ I_n & I_n & J_n - I_n & \cdots & I_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ I_n & I_n & I_n & \cdots & J_n - I_n \end{pmatrix}$$

$$\sim \begin{pmatrix} O_n & -(n-2)J_n & 2I_n - J_n & \cdots & 2I_n - J_n \\ I_n & O_n & O_n & \cdots & O_n \\ O_n & 2I_n - J_n & J_n - 2I_n & \cdots & O_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ O_n & 2I_n - J_n & O_n & \cdots & J_n - 2I_n \end{pmatrix}$$

$$\sim \operatorname{diag}(I_n, (J_n - 2I_n)^{n-2}, 2(n-2)(J_n - I_n))$$

$$\sim \operatorname{diag}(1^{2n-2}, 2^{(n-2)^2}, \{2(n-2)\}^{2n-3}, 2(n-1)(n-2)) =: \Lambda_n.$$

Since $S(\Lambda_n) = \Lambda_n$, the result follows. □

For sake of completeness, we mention that $S(A_S) = S(A_4) = \operatorname{diag}(1^6, 2^4, 4^5, 12)$, where A_S denotes the adjacency matrix of the Shrikhande graph.

The *triangular graph* $T(n)$ has as vertices the 2-element subsets of $\{1,2,\ldots,n\}$. Two vertices are adjacent iff they are not disjoint as subsets. The parameters of $T(n)$ are $(v,k,\lambda,\mu) = (\frac{1}{2}n(n-1), 2(n-2), n-2, 4)$. $T(n)$ is unique except for $n = 8$. In that case, there are three nonisomorphic graphs, the *Chang graphs*. These will be discussed in the next chapter.

Proposition 2.5 *The SNF of the triangular graph $T(n)$ is equal to*

$$\begin{array}{ll} \operatorname{diag}(1^{n-2}, 2^{\frac{1}{2}(n-2)(n-3)}, \{2(n-4)\}^{n-2}, (n-2)(n-4)) & \text{if } 2 \mid n \\ \operatorname{diag}(1^{n-1}, 2^{\frac{1}{2}(n-1)(n-4)}, \{2(n-4)\}^{n-2}, 2(n-2)(n-4)) & \text{otherwise.} \end{array}$$

PROOF. Let A_n be the adjacency matrix of $T(n)$, corresponding to the following labelling of the rows and columns: $\{1,2\},\{1,3\},\ldots,\{1,n\},\{2,3\},\ldots,\{n-1,n\}$. Furthermore, let a_j^i denote the all-a matrix of size $i \times j$, $a \in \mathbb{Z}$. Then we have

$$A_n = \left(\begin{array}{c|c|c|c|c|c} J_{n-1} - I_{n-1} & \begin{matrix} 1_{n-2}^1 \\ I_{n-2} \end{matrix} & \begin{matrix} 0_{n-3}^1 \\ 1_{n-3}^1 \\ I_{n-3} \end{matrix} & \cdots & \begin{matrix} 0_2^{n-4} \\ 1_2^1 \\ I_2 \end{matrix} & \begin{matrix} 0_1^{n-3} \\ 1 \\ 1 \end{matrix} \\ \hline 1_1^{n-2} \quad I_{n-2} & J_{n-2} - I_{n-2} & \begin{matrix} 1_{n-3}^1 \\ I_{n-3} \end{matrix} & \cdots & \begin{matrix} 0_2^{n-5} \\ 1_2^1 \\ I_2 \end{matrix} & \begin{matrix} 0_1^{n-4} \\ 1 \\ 1 \end{matrix} \\ \hline 0_1^{n-3} \quad 1_1^{n-3} \quad I_{n-3} & 1_1^{n-3} \quad I_{n-3} & J_{n-3} - I_{n-3} & \cdots & \begin{matrix} 0_2^{n-6} \\ 1_2^1 \\ I_2 \end{matrix} & \begin{matrix} 0_1^{n-5} \\ 1 \\ 1 \end{matrix} \\ \hline \vdots & \vdots & \vdots & \ddots & \cdots & \cdots \\ \hline 0_{n-4}^2 \quad 1_1^2 \quad I_2 & 0_{n-5}^2 \quad 1_1^2 \quad I_2 & 0_{n-6}^2 \quad 1_1^2 \quad I_2 & \cdots & J_2 - I_2 & 1_1^2 \\ \hline 0_{n-3}^1 \quad 11 & 0_{n-4}^1 \quad 11 & 0_{n-5}^1 \quad 11 & \cdots & 11 & 0 \end{array}\right) \sim$$

$$\left(\begin{array}{c|c|c|c|c|c|c}
n-2 & 0^1_{n-2} & (n-4)^1_{n-2} & 2^1_{n-3} & \cdots & 22 & 2 \\
\hline
(n-4)^{n-2}_1 & O_{n-2} & (n-4)J_{n-2} & \begin{matrix}2^1_{n-3}\\ 2(J-I)_{n-3}\end{matrix} & \cdots & \begin{matrix}2^{n-5}_2\\ 00\\ 2(J_2-I_2)\end{matrix} & \begin{matrix}2^{n-4}_1\\ 0\\ 0\end{matrix} \\
\hline
0^{n-2}_1 & I_{n-2} & O_{n-2} & 0^{n-2}_{n-3} & \cdots & 0^{n-2}_2 & 0^{n-2}_1 \\
\hline
2^{n-3}_1 & 0^{n-3}_{n-2} & 0^{n-3}_1 \quad 2(J-I)_{n-3} & & & & \\
\hline
2^{n-4}_1 & 0^{n-4}_{n-2} & 0^{n-4}_1 \quad 2^{n-4}_1 \quad 2(J-I)_{n-4} & & & & \\
\hline
\vdots & \vdots & \vdots & & & 2I_{\frac{1}{2}(n-2)(n-3)} & \\
\hline
2^2_1 & 0^2_{n-2} & 2^2_{n-5} \quad 0^2_1 \quad 2(J_2-I_2) & & & & \\
\hline
2 & 0^1_{n-2} & 2^1_{n-4} \quad 00 & & & &
\end{array}\right)$$

$$\sim \operatorname{diag}(I_{n-2}, 2I_{\frac{1}{2}(n-2)(n-3)}, A_n^*),$$

where

$$A_n^* = \left(\begin{array}{c|c} (n-2)(n-4) & \{(n-4)^2\}^1_{n-2} \\ \hline \{(n-4)^2\}^{n-2}_1 & \begin{matrix}(n-4)(n-6)J_{n-2}\\ +2(n-4)I_{n-2}\end{matrix}\end{array}\right) \sim \left(\begin{array}{c|c} (n-2)(n-4) & \{(n-4)^2\}^1_{n-2} \\ \hline \{2(n-4)\}^{n-2}_1 & 2(n-4)(J-I)_{n-2}\end{array}\right)$$

$$\sim \left(\begin{array}{c|c} (n-2)(n-4) & \{-2(n-4)\}^1_{n-2} \\ \hline \{2(n-4)\}^{n-2}_1 & -2(n-4)I_{n-2}\end{array}\right) \sim \operatorname{diag}(\{2(n-4)\}^{n-2}, (n-2)(n-4)).$$

Thus $A_n \sim \operatorname{diag}(1^{n-2}, 2^{\frac{1}{2}(n-2)(n-3)}, \{2(n-4)\}^{n-2}, (n-2)(n-4)) =: \Lambda_n$. Applying Theorem 2.3, we obtain

$$S(A_n) = S(\Lambda_n) = \begin{cases} \Lambda_n & \text{if } 2 \mid n \\ \operatorname{diag}(1^{n-1}, 2^{\frac{1}{2}(n-1)(n-4)}, \{2(n-4)\}^{n-2}, 2(n-2)(n-4)) & \text{otherwise.} \end{cases}$$

□

We recall the fact that if $r_p(M) = r$, then M can be reduced over $\mathbb{F}_p$ to a diagonal matrix $\operatorname{diag}(1^r, 0^{n-r})$, the so-called *canonical form*. In general, there will only be a few primes p for which $r_p(M) < n$, since $r_p(M) = n$ unless p is a divisor of $\det(M)$. Hence in practice it will not be far more efficient to compute the SNF of M than to determine the canonical form for those primes p that divide $\det(M)$.

In the subsequent chapters we shall try to determine the p-rank of several (classes of) strongly regular graphs, without making use of the methods mentioned above. For some primes the rank can be calculated in a rather easy way; for other primes we can only derive bounds. In the proofs the next lemma will be frequently used.

Lemma 2.6 *Let M be a nonsingular matrix and suppose $p^k \parallel \det(M)$. Then $r_p(M) \geq n - k$. (By $p^k \parallel a$, $a \in \mathbb{Z}$, we mean that $p^k \mid a$, but $p^{k+1} \nmid a$.)*

PROOF. Since $\det(S(M)) = \det(M) \neq 0$, the diagonal elements s_i of $S(M)$ are unequal to zero for $1 \leq i \leq n$. Furthermore, because $s_i \mid s_{i+1}$, $1 \leq i \leq n-1$, at most k of the invariant factors are divisible by p. □

Chapter 3

On the p-rank of strongly regular graphs with integral eigenvalues

Let Γ be a srg of order v with integral eigenvalues k, r and s. In this chapter it is proven that the p-rank of A is completely determined by the parameters of Γ when p does not divide both r and s. For the remaining primes p, an upper bound for $r_p(A)$ is derived. A similar result is obtained for the p-rank of $A + \tau I$, $\tau \in \mathbb{Z}$. Furthermore, we examine how the p-ranks of switching-equivalent graphs are related.

3.1 Preliminaries

In this section a few elementary but useful lemmas from matrix theory are recalled. We omit the proofs, which can be found in any textbook on matrix theory (e.g. Marcus and Minc [16]).

Let M, M_1 and M_2 be $n \times n$ matrices with entries in some field F.

Lemma 3.1 *If $M = M_1 + M_2$, then*

$$|\, r_F(M_1) - r_F(M_2)\,| \leq r_F(M) \leq r_F(M_1) + r_F(M_2).$$

In particular, $|\, r_F(M) - r_F(J_n - M)\,| \leq 1$.

Lemma 3.2 *If $M = M_1 M_2$, then*

$$r_F(M_1) + r_F(M_2) - n \leq r_F(M) \leq \min(r_F(M_1), r_F(M_2))\,.$$

This lemma will mainly be used in one of the following forms:
(a) If $M_1 M_2 = O_n$, then $r_F(M_1) + r_F(M_2) \leq n$;
(b) If $M_1 M_2 = J_n$, then $r_F(M_1) + r_F(M_2) \leq n + 1$.

Lemma 3.3 *Let $\lambda_1, \ldots, \lambda_k, \lambda_i \in F$, $\lambda_i \neq \lambda_j$ for $i \neq j$, be the complete set of eigenvalues of M. Then the following are equivalent:*

1. $\prod_{i=1}^{k}(M - \lambda_i I) = O_n$
2. $\sum_{i=1}^{k} \dim(\mathcal{N}_F(M - \lambda_i I)) = n$.

3.2 General theorems

Throughout this section, let A be the adjacency matrix of a $srg\ \Gamma$ with parameters (v, k, λ, μ) and integral eigenvalues k, r, s with multiplicities $1, f$ and g, respectively. Denote the rank of A over $\mathbb{R}$ by $r(A)$.

Theorem 3.4 *Define* $\alpha_0 := k \pmod p$, $\alpha_1 := r \pmod p$, $\alpha_2 := s \pmod p$. *Then the following holds:*

(i) *if precisely one of* $\alpha_0, \alpha_1, \alpha_2$ *is equal to zero, say* α_i *with multiplicity* m_i, *then* $r_p(A) = v - m_i$;

(iia) *if* $\alpha_0 = 0$, $\alpha_1 = 0$ *and* $\alpha_2 \neq 0$, *then* $r_p(A) = g$;

(iib) *if* $\alpha_0 = 0$, $\alpha_1 \neq 0$ *and* $\alpha_2 = 0$, *then* $r_p(A) = f$;

(iii) *if* $\alpha_1 = 0$ *and* $\alpha_2 = 0$, *then* $r_p(A) \leq \min(f, g) + 1$.

PROOF. The characteristic polynomial of A over $\mathbb{F}_p$ is $(x - \alpha_0)(x - \alpha_1)^f(x - \alpha_2)^g$. Since the dimension of the kernel of A is at most the multiplicity of the eigenvalue 0 as a root of the characteristic polynomial of A, a lower bound for $r_p(A)$ is

$$r_p(A) \geq \epsilon_0 + \epsilon_1 f + \epsilon_2 g, \tag{3.1}$$

where $\epsilon_i = 0$ or 1, depending on whether α_i is equal to zero or not. This bound also follows immediately from Lemma 2.6.

Define $m := \max((1 - \epsilon_0), (1 - \epsilon_1)f, (1 - \epsilon_2)g)$. Suppose $m > 0$. Let α be the eigenvalue of A over $\mathbb{R}$ corresponding to m (thus $\alpha \in \{k, r, s\}$). Then an upper bound for $r_p(A)$ is

$$r_p(A) = r_p(A - \alpha I) \leq r(A - \alpha I) = v - m. \tag{3.2}$$

Combining (3.1) and (3.2) proves (i) and (iii).

Now assume $p \mid k$, $p \mid r$ and $p \nmid s$. By (1.2),

$$A(A - sI) = (k - \mu)I + (\lambda - \mu - s)A + \mu J.$$

From Section 1.2 we recall the following relations between the parameters:

$$\mu = k + rs \quad \text{and} \quad \lambda - \mu = r + s.$$

Thus, under the assumptions made,

$$A(A - sI) \equiv O \pmod p.$$

Combining (3.1) and Lemma 3.2 yields

$$v = g + (f + 1) \leq r_p(A) + r_p(A - \alpha_2 I) \leq v.$$

Thus $r_p(A) = g$ as claimed. Assertion (iib) is proven in a similar way. □

Hence, the only primes p for which the determination of $r_p(A)$ is nontrivial, are the primes that divide both r and s.

The question arises whether the upper bound in case (iii) is good or not. From the results in Chapter 6, we might conclude that the bound is often fairly good. However, most of the graphs that are examined, have small f or g (< 25), so we can not say anything in general.

Remark Sometimes a slightly better upper bound can be obtained in case (iii) as follows. Without

loss of generality, suppose $f < g$. Then according to the above theorem, $r_p(A) \leq f + 1$. Consider the minimal idempotent E_1 satisfying $r(E_1) = f$. Let c_1 be the smallest integer such that $c_1 E_1$ is an integral matrix, say

$$c_1 E_1 = c_{10} I + c_{11} A + c_{12} B\ ,\ \ c_{1i} \in \mathbb{Z}.$$

Suppose that $p \mid c_{10}, p \mid c_{12}$ and $p \nmid c_{11}$. Then $r_p(A) = r_p(c_1 E_1) \leq r(c_1 E_1) = f$.

The next theorem is a generalization of Theorem 3.4 for $A + \tau I$, $\tau \in \mathbb{Z}$. Its spectrum is $(k+\tau)^1, (r+\tau)^f, (s+\tau)^g$, where the multiplicities are written as exponents.

Theorem 3.5 *Define* $\alpha_0 := (k+\tau) \pmod p$, $\alpha_1 := (r+\tau) \pmod p$, $\alpha_2 := (s+\tau) \pmod p$. *Then the following holds:*

(i) *if precisely one of* $\alpha_0, \alpha_1, \alpha_2$ *is equal to zero, say* α_i *with multiplicity* m_i, *then* $r_p(A + \tau I) = v - m_i$;

(iia) *if* $\alpha_0 = 0, \alpha_1 = 0$ *and* $\alpha_2 \neq 0$, *then* $r_p(A + \tau I) = g + \epsilon$, *where* $\epsilon = 0$ *if* $p \mid \mu$ *and* 1 *otherwise;*

(iib) *if* $\alpha_0 = 0, \alpha_1 \neq 0$ *and* $\alpha_2 = 0$, *then* $r_p(A + \tau I) = f + \epsilon$, *where* $\epsilon = 0$ *if* $p \mid \mu$ *and* 1 *otherwise;*

(iii) *if* $\alpha_1 = 0$ *and* $\alpha_2 = 0$, *then* $r_p(A + \tau I) \leq \min(f, g) + 1$.

PROOF. We shall only prove (iia).

$$\begin{aligned}(A + \tau I)(A - sI) &= (k - \mu - \tau s)I + (\lambda - \mu + \tau - s)A + \mu J \\ &= -s(r+\tau)I + (r+\tau)A + \mu J \\ &\equiv \mu J \pmod p.\end{aligned}$$

From (i) it follows that $r_p(A - sI) = f + 1$ under the assumptions of (iia). Replacing A by $A + \tau I$ in (3.1) yields, together with Lemma 3.2,

$$g \leq r_p(A + \tau I) \leq g + r_p(\mu J).$$

Lemma 3.3 asserts that $r_p(A + \tau I) = g$ if and only if

$$(A + \tau I)(A - sI) \equiv O \pmod p.$$

Hence the conclusion holds. □

Thus, when studying the p-rank of $A + \tau I$ for a given $srg\ \Gamma$ with integral eigenvalues k, r and s, we may restrict ourselves to the values of p and τ for which both $r + \tau$ and $s + \tau$ are divisible by p. There is no known general strategy to determine (bounds for) the p-rank of $A + \tau I$. In the next section we give a few small lemmas which might be useful, especially if f or g is small. In that case, it is often easy to obtain a good lower bound from an induced subgraph, as is shown in Examples 3.1 and 3.2.

3.3 Bounds from subgraphs and examples

Let Γ be a *srg*, not necessarily with integral eigenvalues, and let $\tau \in \mathbb{Z}$. Suppose Γ contains an induced subgraph Γ' of order v'. Let A' be the adjacency matrix of Γ'. Then we obviously have $r_p(A + \tau I_v) \geq r_p(A' + \tau I_{v'})$. In particular, the following holds:

Lemma 3.6 *If Γ contains a clique of size n and $\tau \not\equiv 1 \pmod{p}$, then*

$$r_p(A + \tau I) \geq \begin{cases} n-1 & \text{if } p \mid (n+\tau-1) \\ n & \text{otherwise.} \end{cases}$$

PROOF. If Γ contains a clique of size n, then $J_n + (\tau - 1)I_n$ is a submatrix of $A + \tau I_v$. In Example 2.1 it was derived that $S(J_n + (\tau-1)I_n) = \mathrm{diag}(1, (\tau-1)^{n-2}, (\tau-1)(n+\tau-1))$, from which the result follows. □

If Γ contains a coclique of size n, then n is a lower bound for $r_p(A + \tau I)$ if τ is not divisible by p. On the other hand, Theorem 3.5 provides an upper bound for the size of a coclique in a *srg* with integral eigenvalues.

Proposition 3.7 *The size of a coclique in a strongly regular graph with integral eigenvalues is at most* $\min(f, g) + 1$.

PROOF. Let C be a coclique in a *srg* Γ and set $n := |C|$. Let p_1 and p_2 be two (not necessarily distinct) primes satisfying $p_1 | (r+1)$ and $p_2 | (s-1)$ (such primes exist since both r and s are different from zero). Then, under the assumption that the eigenvalues of Γ are all integers, we obtain from Theorem 3.5

$$n \leq r_{p_1}(A + I) \leq g + 1,$$
$$n \leq r_{p_2}(A - I) \leq f + 1.$$

Hence, the statement holds. □

In this way, we have almost proven the Cvetković bound for strongly regular graphs with integral eigenvalues. This bound asserts that the size of a coclique C in a graph Γ can not exceed the number of nonnegative (nonpositive) eigenvalues of Γ (see Cvetković, Doob and Sachs [7]). For a *srg* this yields $|C| \leq \min(f+1, g)$.

Our problem is related to another graph theoretic problem, namely the determination of the *chromatic number* of Γ. This number, usually denoted by $\chi(\Gamma)$, is defined as the minimal number of colors needed for a coloring of the vertices of Γ in which adjacent vertices have different colors.

If $\chi(\Gamma) = \chi$, then there is one coclique of size at least $\lceil v/\chi \rceil$ contained in Γ. Hence an upper bound for $\chi(\Gamma)$ provides a lower bound for $r_p(A + \tau I)$ when $p \nmid \tau$, and vice versa. However, general upper bounds for $\chi(\Gamma)$ do not give useful lower bounds for $r_p(A + \tau I)$.

When we study the p-rank of a given graph, both $r_p(A + \tau I)$ and $r_p(J - A - \tau I)$ will be considered. The relation between the two ranks is expressed by

$$\dim(\mathcal{R}_p(A + \tau I) + \langle \underline{1} \rangle) \;=\; \dim(\mathcal{R}_p(J - A - \tau I) + \langle \underline{1} \rangle). \tag{3.3}$$

In view of this, the following lemma turns out to be often useful.

Lemma 3.8 *If $p \nmid v$, $p \mid k$, then $r_p(J - A) = r_p(A) + 1$.*

PROOF. We have $\underline{1}(J - A) = (v - k)\underline{1} \not\equiv \underline{0} \pmod{p}$, thus $\underline{1} \in \mathcal{R}_p(J - A)$. Consider A as a generator matrix of a p-ary linear code C. Because $(\underline{r}, \underline{1}) = k \equiv 0 \pmod{p}$ holds for every row $\underline{r}$ of A, the dual code $C^{\perp}$ contains $\underline{1}$. As $(\underline{1}, \underline{1}) = v \not\equiv 0 \pmod{p}$, the all-one vector is not contained in $\mathcal{R}_p(A)$. The conclusion now follows from (3.3). □

A last lemma, before we discuss some examples:

Lemma 3.9 *The 2-rank of the adjacency matrix of any graph is even.*

For a proof of this lemma, we refer to the Appendix (A5).

Example 3.1 The *Clebsch graph* can be described in the following way: take as vertices all subsets of $\{1, \ldots, 5\}$ of even cardinality; two vertices are adjacent whenever their symmetric difference has cardinality 4. This yields a *srg* with parameters $(v, k, \lambda, \mu) = (16, 5, 0, 2)$. Its spectrum is $5^1, 1^{10}, (-3)^5$. From the discussion at the end of the previous section it follows that we only have to determine the 2-rank of $A + I$ and $B := J - A - I$.

By Theorem 3.5, we find $r_2(A + I) \leq 6$. Now consider the subgraph on the five vertices of cardinality 4 and the vertex $\{1, 2\}$. Let A' be the corresponding submatrix of A. Then

$$A' + I_6 = \left(\begin{array}{c|c} I_5 & \underline{x}^T \\ \hline \underline{x} & 1 \end{array}\right), \quad \text{where } \underline{x} = (00011).$$

Since $r_2(A + I_{16}) \geq r_2(A' + I_6) = 6$, we conclude that $r_2(A + I) = 6$.

Furthermore, $|r_2(A+I) - r_2(B)| \leq 1$ (Lemma 3.1) and $r_2(B)$ is even (Lemma 3.9), so $r_2(B) = 6$.

Example 3.2 The *Gewirtz graph* has parameters $(v, k, \lambda, \mu) = (56, 10, 0, 2)$ and is unique. Its spectrum is $10^1, 2^{35}, (-4)^{20}$. A construction of this graph is given in Chapter 6. Since $r - s = 6$, the only interesting cases are $r_2(A)$ and $r_3(A + I)$. In this example, we shall only determine $r_2(A)$. In Chapter 6, the other case is dealt with.

From the parameters of the graph we deduce that A contains a 20×20 submatrix A' of the following form:

$$A' = \left(\begin{array}{cc|c|c} 0 & 1 & \underline{1}_9 & \underline{0}_9 \\ 1 & 0 & \underline{0}_9 & \underline{1}_9 \\ \hline \underline{1}_9^t & \underline{0}_9^t & O_9 & I_9 \\ \hline \underline{0}_9^t & \underline{1}_9^t & I_9 & O_9 \end{array}\right).$$

Clearly, $r_2(A) \geq 18$.

Assume w.l.o.g. that

$$A = \left(\begin{array}{c|c} A' & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right).$$

Every row in $[A_{21}|A_{22}]$ has a zero in the first two columns, a one in exactly two of the columns $3, 4, \ldots, 11$ and a one in exactly two of the columns $12, 13, \ldots, 20$. Suppose $r_2(A) = 18$. Let $\underline{r}$ be a row of $[A_{21}|A_{22}]$. Then $\underline{r}$ can be expressed as the sum (modulo 2) of four of the rows $3, 4, \ldots, 20$. Since $k = 10$, one of these four rows must have at least three ones in common with $\underline{r}$. This contradicts $\mu = 2$. Hence, $18 < r_2(A) \leq 21$. Since $r_2(A)$ is even, it follows that $r_2(A) = 20$.

In Chapter 6 it will be proven that $\underline{1}$ can be written as the sum of an even number of rows of A. This implies that $\underline{1}$ is an element of both $\mathcal{R}_2(A)$ and $\mathcal{R}_2(J - A)$, hence $r_2(J - A) = r_2(A) = 20$.

3.4 Switching-equivalent graphs

In Section 2 it was shown that the p-rank of a *srg* with integral eigenvalues is completely determined by its spectrum when p does not divide both r and s. Hence cospectral graphs have the same p-rank for primes p satisfying this condition. However, this not necessarily holds when $p \mid r$ and $p \mid s$. For example, we shall see that the triangular graph $T(8)$ and the Chang graphs have different 2-ranks (Example 3.3). Clearly, isomorphic graphs have the same rank over any field $\boldsymbol{F}_p$, since labelling the rows and columns of a matrix in a different way does not change the rank.

Switching-equivalent graphs need not be isomorphic or even cospectral, but when the p-rank of one graph is known, there are only a few possible values for the p-rank of the other graph(s).

Lemma 3.10 *If Γ_1 and Γ_2 are switching-equivalent, then $|r_p(A_1) - r_p(A_2)| \leq 2$.*

PROOF. Assume that the rows and columns of A_1 and A_2 are labelled in the same way. Set $B_i := J - A_i - I$ for $i = 1, 2$. From the definition of switching as given in Chapter 1, it is readily seen that

$$B_2 - A_2 = D(B_1 - A_1)D,$$

where D is a diagonal matrix with $d_{ii} = -1$ if the ith row and column of A_1 are indexed by an element of the switching-set and 1 otherwise. This is equivalent to

$$J - 2A_2 = D(J - 2A_1)D. \tag{3.4}$$

For $p > 2$, the above-mentioned relation yields

$$r_p(J - 2A_2) = r_p(J - 2A_1),$$

from which the result is easily derived by Lemma 3.1.

If $p = 2$, relation (3.4) gives a trivial result, but in this case we can give a more explicit relation between $\mathcal{R}_2(A_1)$ and $\mathcal{R}_2(A_2)$. Denote by $\underline{c}$ the characteristic vector of the switching-set with respect to the labelling of the columns of A_1 and A_2. Then

$$\mathcal{R}_2(A_1) + \langle \underline{1}, \underline{c} \rangle = \mathcal{R}_2(A_2) + \langle \underline{1}, \underline{c} \rangle. \tag{3.5}$$

Hence, the assertion is also proven for $p = 2$. □

Of course, this lemma also holds when A_1 and A_2 are substituted by $A_1 + \tau I$ and $A_2 + \tau I$ for $\tau \in \mathbb{Z}$.

Lemma 3.11 *Let Γ be a srg on v vertices that is switching-equivalent to the disjoint union of a vertex and a srg Γ' on $v - 1$ vertices. Denote the eigenvalues of Γ by k, r and s.*
(a) *If $2 \mid r$ and $2 \mid s$, then $r_2(A_\Gamma) = r_2(A_{\Gamma'}) + \epsilon$, where $\epsilon = 2$ if $\underline{1} \in \mathcal{R}_2(A_\Gamma)$ and 0 otherwise.*
(b) *If $2 \mid (r+1)$ and $2 \mid (s+1)$, then $|r_2(A_\Gamma + I_v) - r_2(A_{\Gamma'} + I_{v-1})| \leq 1$.*

PROOF. W.l.o.g. assume that the first row of A_Γ, denoted by $\underline{r}$, is the characteristic vector of the switching-set V_1. Write A instead of A_Γ and denote by A^* the matrix obtained from A by switching with respect to V_1, that is, $A^* = \mathrm{diag}(0, A_{\Gamma'})$. Now (3.5) takes the following form:

$$\mathcal{R}_2(A + \tau I) + \langle \underline{1}, \underline{r} \rangle = \mathcal{R}_2(A^* + \tau I) + \langle \underline{1}, \underline{r} \rangle, \quad \tau = 0, 1.$$

(a) Since $\underline{r} \in \mathcal{R}_2(A)$ and $\underline{1} \notin \mathcal{R}_2(A^* + \langle \underline{r} \rangle)$, we have $\dim(\mathcal{R}_2(A) + \langle \underline{1} \rangle) = \dim(\mathcal{R}_2(A^*) + \langle \underline{r} \rangle) + 1$. Because both $r_2(A)$ and $r_2(A_{\Gamma'}) = r_2(A^*)$ are even (Lemma 3.9), the following holds:

- if $\underline{1} \in \mathcal{R}_2(A)$, then $r_2(A) = r_2(A_{\Gamma'}) + 2$ (and $\underline{r} \notin \mathcal{R}_2(A^*)$);
- if $\underline{1} \notin \mathcal{R}_2(A)$, then $r_2(A) = r_2(A_{\Gamma'})$ (and $\underline{r} \in \mathcal{R}_2(A^*)$).

(b) Denote by B and B' the adjacency matrices of $\bar{\Gamma}$ and $\bar{\Gamma}'$, respectively. If p divides both $r+1$ and $s+1$, then (a) applies to $r_2(B)$ and $r_2(B')$. In Section 1.2, we mentioned the fact that both v and the valency of Γ' are even. Hence, by Lemma 3.8, $r_2(A' + I_{v-1}) = r_2(B') + 1$.

If $\underline{1} \in \mathcal{R}_2(B)$, then $r_2(A + I_v) = r_2(B) - \delta_1$, where $\delta_1 = 0$ if $\underline{1} \in \mathcal{R}_2(A + I_v)$ and 1 otherwise. From this we get

$$r_2(A + I_v) + \delta_1 = r_2(B) \overset{(a)}{=} r_2(B') + 2 = r_2(A' + I_{v-1}) + 1. \tag{3.6}$$

If the all-one vector is not contained in $\mathcal{R}_2(B)$, a similar argument is used to derive that

$$r_2(A + I_v) - \delta_2 = r_2(B) \overset{(a)}{=} r_2(B') = r_2(A' + I_{v-1}), \tag{3.7}$$

where $\delta_2 = 1$ if $\underline{1} \in \mathcal{R}_2(A + I_v)$ and 0 otherwise. Combining (3.6) and (3.7) yields the result. □

To illustrate the foregoing, we calculate the 2-rank of the Schläfli graph and the Chang graphs, which can all be obtained from $T(8)$ by switching.

Example 3.3 The triangular graph $T(8)$ has been discussed in Chapter 2. Its vertex set is the set of unordered pairs of $\{1,\ldots,8\}$ and two pairs are adjacent whenever they are not disjoint. $T(8)$ has parameters $(v,k,\lambda,\mu) = (28,12,6,4)$, spectrum $12^1, 4^7, (-2)^{20}$ and its 2-rank is 6 (Proposition 2.5).

The Schläfli graph Γ_S is obtained from $T(8)$ by isolating one vertex through switching and then removing it. Its parameters are $(v,k,\lambda,\mu) = (27,16,10,8)$. The spectrum of Γ_S is $27^1, 4^6, (-2)^{20}$. It can be shown that the Schläfli graph is unique, i.e. every graph with the same parameters is isomorphic to it. Let A_S denote the adjacency matrix of Γ_S. Consider the adjacency matrix A_8 as shown in the previous chapter and take the first row as the characteristic vector of the switching set (i.e. switching is performed with respect to the the set $\{\{1,x\},\{2,x\} \mid 3 \le x \le 8\}$ and the vertex $\{1,2\}$ is isolated). Then the first six rows of A_S can be written as:

$$\left(\begin{array}{c|c|c|c|c} J_6 - I_6 & I_6 & \begin{matrix} 0_5^1 \\ J_5 - I_5 \end{matrix} & \cdots & \begin{matrix} 1_2^3 \\ 0_2^1 \\ J_2 - I_2 \end{matrix} \quad \begin{matrix} 1_1^4 \\ 0 \\ 0 \end{matrix} \end{array}\right).$$

We see that I_6 is a submatrix of A_S. Hence $r_2(A_S) \ge 6$ and equality holds because of Lemma 3.11 and the fact that $r_2(A_8) = 6$.

The Chang graphs C_i, $1 \le i \le 3$, are obtained from $T(8)$ by switching with respect to

(C_1) $\{\{1,2\},\{3,4\},\{5,6\},\{7,8\}\}$;
(C_2) $\{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,6\},\{6,7\},\{7,8\},\{1,8\}\}$;
(C_3) $\{\{1,2\},\{2,3\},\{1,3\},\{4,5\},\{5,6\},\{6,7\},\{7,8\},\{4,8\}\}$.

The Chang graphs all have the same parameters as $T(8)$. There are no other graphs with these parameters.

It is easy to give for every i, $1 \le i \le 3$, a submatrix A'_{C_i} of A_{C_i} of 2-rank 8. The submatrices are formed by the rows and columns labelled by $\{\{1,2\},\ldots,\{1,8\},\{x,y\}\}$, where $\{x,y\} = \{3,5\}$ for

C_1 and $\{x, y\} = \{2,4\}$ for C_2 and C_3.

$$A'_{C_1} = \left(\begin{array}{c|c|c} & & 1 \\ \hline & J_6 - I_6 & \underline{v}_1^T \\ \hline 1 & \underline{v}_1 & \end{array}\right), A'_{C_2} = \left(\begin{array}{c|c|c|c} & & 1 & \\ \hline & J_5 - I_5 & & \underline{v}_2^T \\ \hline 1 & & & 1 \\ \hline & \underline{v}_2 & 1 & \end{array}\right), A'_{C_3} = \left(\begin{array}{c|c|c|c} & 1 & & \\ \hline 1 & & & 1 \\ \hline & & J_5 - I_5 & \underline{v}_3^T \\ \hline & 1 & \underline{v}_3 & \end{array}\right),$$

where $\underline{v}_1 = (101000)$, $\underline{v}_2 = (01000)$ and $\underline{v}_3 = (10000)$. Hence $8 \leq r_2(A_{C_i}) \leq r_2(A_8) + 2 = 8$ for $1 \leq i \leq 3$, where the right hand inequality follows from Lemma 3.10. Of course, the upper bound is also obtained from Theorem 3.4.

Let $\underline{c}_1$ denote the characteristic vector of the switching-set of $T(8)$ and C_1. From Lemma 3.11 it follows that $\underline{1} \notin \mathcal{R}_2(A_8)$. Substituting this in (3.5) yields, together with the obtained results,

$$8 \geq \dim(\mathcal{R}_2(A_8) + \langle \underline{c}_1 \rangle) + 1 = \dim(\mathcal{R}_2(A_{C_1}) + \langle \underline{c}_1, \underline{1} \rangle) \geq 8,$$

which is only possible if $\langle \underline{c}_1, \underline{1} \rangle \subset \mathcal{R}_2(A_{C_1})$ and $\underline{c}_1 \notin \mathcal{R}_2(A_8)$. Examining A'_{C_1}, we see that $\sum_{i \in \{2,4,6,7,8\}} \underline{r}_{\{1,i\}} + \underline{r}_{\{3,5\}} \equiv \underline{1} \pmod 2$ must hold. Since $\underline{1}$ can be written as the sum of an even number of rows of A_{C_1}, this vector is also contained in $\mathcal{R}_2(J_{28} - A_{C_1})$. Hence $r_2(J_{28} - A_{C_1}) = r_2(A_{C_1}) = 8$. The same arguments can be used to derive that $r_2(J_{28} - A_{C_2}) = r_2(J_{28} - A_{C_3}) = 8$.

Lemma 3.8 yields that $r_2(J_{27} - A_S) = 7$. Finally, since I_7 is a submatrix of $J_{28} - A_8$ and $|r_2(J_{28} - A_8) - r_2(A_8)| \leq 1$, we conclude that $r_2(J_{28} - A_8) = 7$.

Chapter 4

On the p-rank of Paley graphs

Paley graphs are strongly regular graphs with half-case parameters. Hence, their eigenvalues are not necessarily integral. In this chapter we study the p-rank of $A_P + \sigma I$, where A_P denotes the adjacency matrix of a Paley graph and $\sigma \in \mathbb{Z}$. In fact, $r_p(A_P + \sigma I)$ will be completely determined for all values of p and σ. However, we first discuss a method that enables us to calculate the p-rank of a circulant in an easy way. This method is based upon results from algebraic coding theory, especially from the theory of cyclic codes.

4.1 Circulants

Definition A matrix of the form

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}$$

is called a *circulant.*

In this section it is shown how the p-rank of a circulant can be determined by regarding it as a generator matrix of a cyclic code.

Definition A linear code C is called *cyclic* if for every codeword $(c_0, c_1, \ldots, c_{n-1})$ the word $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also in C.

The theory of cyclic codes is based upon the identification of codewords with a set of polynomials. Let F be any finite field $\mathbb{F}_q$. Denote by $F[x]$ the set of polynomials in x with coefficients from F. The ring $R_n := F[x]/(x^n - 1)$ consists of the residue classes of $F[x]$ modulo $x^n - 1$. As a system of representatives we take the set of polynomials of $F[x]$ of degree less than n. Now the codeword $(c_0, c_1, \ldots, c_{n-1})$ is associated with the polynomial $c(x) = \sum_{i=0}^{n-1} c_i x^i$ in R_n. Then a cyclic shift corresponds to multiplying $c(x)$ by x in R_n.

Definitions A *principal ideal* $\mathcal{I}$ of R_n is a linear subspace of R_n consisting of all multiples of a fixed polynomial $g(x)$. We call $g(x)$ a *generator polynomial* of $\mathcal{I}$. This is denoted by $\mathcal{I} = \langle g(x) \rangle$.

$\mathcal{I}$ can be considered as a cyclic code of length n. The next theorem proves that every cyclic code is a principal ideal.

Theorem 4.1 ([15, p.190]) *Let C be a cyclic code of length n.*

(a) *There is a unique monic polynomial $g(x)$ of minimal degree in C.*
(b) *$g(x)$ is a generator polynomial of C.*
(c) *$g(x)$ is a factor of $x^n - 1$.*
(d) *Any $c(x) \in C$ can be written uniquely as $c(x) = f(x)g(x)$ in $F[x]$, where $f(x) \in F[x]$ has degree less than $n - r$, $r = \deg(g(x))$. The dimension of C is $n - r$.*

PROOF. (a) Suppose $g_1(x), g_2(x) \in C$ are monic and of minimal degree. Because C is linear, $g_1(x) - g_2(x)$ is in C. But $g_1(x) - g_2(x)$ has lower degree than $g_1(x)$ and $g_2(x)$, a contradiction, unless $g_1(x) = g_2(x)$.
(b) Suppose $c(x) \in C$. Write $c(x) = q(x)g(x) + r(x)$ in R_n, where $\deg(r(x)) < r$. Linearity yields that $r(x) \in C$, so $r(x) = 0$. Therefore, $c(x) \in \langle g(x) \rangle$.
(c) Write $x^n - 1 = h(x)g(x) + r(x)$ in $F[x]$, where $\deg(r(x)) < r$. This implies that $r(x) = -h(x)g(x) \in C$ in R_n, a contradiction unless $r(x) = 0$.
(d) From (b), it follows that any $c(x) \in C$, $\deg(c(x)) < n$, can be written as $q(x)g(x)$ in R_n. Thus

$$\begin{aligned} c(x) &= q(x)g(x) + e(x)(x^n - 1) && \text{in } F[x], \\ &= (q(x) + e(x)h(x))g(x) && \text{in } F[x], \\ &= f(x)g(x) && \text{in } F[x], \end{aligned}$$

where $\deg(f(x)) \leq n - r - 1$. Thus the code consists of multiples of $g(x)$ by polynomials of degree $\leq n - r - 1$, evaluated in $F[x]$. There are $n - r$ linearly independent multiples of $g(x)$, namely $g(x), xg(x), \ldots, x^{n-r-1}g(x)$. Thus the code has dimension $n - r$. □

Let A be a circulant of size n with entries in F. Then A can be considered as a generator matrix of a cyclic code C over F. If $(a_0, a_1, \ldots, a_{n-1})$ is a row of A and $a(x) := \sum_{i=0}^{n-1} a_i x^i$, then $C = \langle a(x) \rangle$. Write $\gcd(x, y)$ for the greatest common divisor of x and y. According to Theorem 4.1, there is a polynomial $g(x)$ which is a factor of $\gcd(x^n - 1, a(x))$ such that $C = \langle g(x) \rangle$. We claim that $g(x)$ is actually equal to $\gcd(x^n - 1, a(x))$.

Lemma 4.2 ([15, p.199]) *Let $g(x)$ be a factor of $x^n - 1$ and let C be the code generated by $g(x)$. Let $p(x) \in R_n$ be such that $\gcd(x^n - 1, p(x)) = 1$. Then $p(x)g(x)$ is also a generator polynomial for C.*

PROOF. It is evident that $\langle p(x)g(x) \rangle \subseteq \langle g(x) \rangle$ holds. If $h(x) = (x^n - 1)/g(x)$, then $\gcd(h(x), p(x)) = 1$. Hence, there exist polynomials $u(x)$ and $v(x)$ such that

$$\begin{aligned} 1 &= u(x)p(x) + v(x)h(x) && \text{in } F[x], \\ g(x) &= u(x)p(x)g(x) + v(x)(x^n - 1) && \text{in } F[x], \\ &= u(x)p(x)g(x) && \text{in } R_n. \end{aligned}$$

Thus $\langle g(x) \rangle \subseteq \langle p(x)g(x) \rangle$. We conclude that $C = \langle g(x) \rangle = \langle p(x)g(x) \rangle$. □

Continuing with the above notation, $r_F(A)$ is now easily determined from the foregoing.

Corollary 4.3 *The F-rank of A equals $n - \deg(g(x))$, where $g(x) = \gcd(a(x), x^n - 1)$.*

Example 4.1 Let A_n be the adjacency matrix of the n-gon:

$$A_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

Thus A_n is a circulant. Take $a(x) = 1 + x^2$.

Over $\mathbb{F}_2$ we have

$$\gcd(a(x), x^n + 1) = \begin{cases} x^2 + 1 & \text{if } n \text{ is even} \\ x + 1 & \text{if } n \text{ is odd.} \end{cases}$$

Thus $r_2(A_{2m}) = 2(m-1)$ and $r_2(A_{2m+1}) = 2m$.

Over $\mathbb{F}_p$, $p > 2$, we have

$$\gcd(a(x), x^n - 1) = \begin{cases} x^2 + 1 & \text{if } n \equiv 0 \pmod 4 \\ 1 & \text{otherwise.} \end{cases}$$

Hence $r_p(A_n) = n - 2$ if $n \equiv 0 \pmod 4$ and $r_p(A_n) = n$ otherwise.

4.2 Paley graphs

The *Paley graphs* are an infinite class of strongly regular graphs that satisfy $f = g$, hence their eigenvalues are not necessarily integral. They are defined in the following way. Take $F = \mathbb{F}_q$, where $q \equiv 1 \pmod 4$. The Paley graph $P(q)$ has vertex set F, with two different vertices x and y joined if and only if $x - y$ is a nonzero square in F. Since -1 is a square in F, the adjacency is well defined. $P(q)$ is strongly regular with parameters

$$v = q,\ k = \frac{1}{2}(q-1),\ \lambda + 1 = \mu = \frac{1}{4}(q-1),\ r = \frac{-1+\sqrt{q}}{2},\ s = \frac{-1-\sqrt{q}}{2},\ f = g = k.$$

Clearly, $P(q)$ has the same parameters as its complement $\bar{P}(q)$.

Lemma 4.4 *$P(q)$ and $\bar{P}(q)$ are isomorphic.*

PROOF. Write P and $\bar{P}$ instead of $P(q)$ and $\bar{P}(q)$. It is evident that two vertices x and y of $\bar{P}$ are adjacent iff $x - y$ is not a square. Now let a be a nonsquare in F and define the function $\phi : F \longmapsto F$ as $\phi(x) := ax$, $x \in F$. Let $\phi(P)$ be the graph with vertex set $\phi(F) = F$ where two vertices x and y are adjacent whenever $\phi^{-1}(x) \sim \phi^{-1}(y)$. Since $ax - ay$ is not a square iff $x - y$ is a nonzero square, it follows that $\phi(P) = \bar{P}$. Hence $P \cong \bar{P}$. □

We denote the adjacency matrix of $P(q)$ by $A(q)$. Combining Lemma 3.1 and Lemma 4.4 yields

Lemma 4.5 *For every prime p, $|r_p(A(q)) - r_p(A(q) + I)| \leq 1$.*

Let us first consider the case where q is a prime (congruent to 1 (mod 4)). Then $F = \{0, 1, \ldots, q-1\}$. If we number the rows and columns of $A(q)$ from 0 to $q-1$, then $A(q)$ is a circulant (suppose $a_{xy} = 1$, then $x - y$ is a square, thus $(x+1) - (y+1)$ is a square, hence $a_{(x+1) \bmod v, (y+1) \bmod v} = 1$). Thus the p-rank of $A(q)$ can be determined for any prime p by means of Corollary 4.3.

However, let us examine first for which primes p the determination of $r_p(A(q))$ might be nontrivial. Since $\det(A(q)) = \frac{1}{2}(q-1)(\frac{1}{4}(q-1))^{(q-1)/2} \neq 0$, Lemma 2.6 can be applied, which yields

(i) if $p \not| (q-1)$, then $r_p(A(q)) = q$;

(ii) if $4 \parallel (q-1)$, then $r_2(A(q)) = q-1$.

Hence, the calculation of $r_p(A(q))$ by application of Corollary 4.3 can be restricted to those primes p that divide $\frac{q-1}{4}$. The next table shows the values of $r_p(A(q))$ for $q < 100$ and $p \mid \frac{(q-1)}{4}$:

q	p	$r_p(A(q))$	q	p	$r_p(A(q))$
13	3	6	53	13	26
17	2	8	61	3,5	30
29	7	14	73	2,3	36
37	3	18	89	2,11	44
41	2,5	20	97	2,3	48

The values of $r_p(A(q))$ in the table suggest that $r_p(A(q)) = \frac{1}{2}(q-1)$ for $p \mid \frac{q-1}{4}$. It will be proven that this holds indeed.

In the introduction of this chapter we claimed that for all values of p and $\sigma \in \mathbb{Z}$ the p-rank of $A(q) + \sigma I$ could be completely determined. The next theorem shows that for most combinations of p and σ this can be attained by applying simple arguments from linear algebra. The remaining cases are dealt with in Theorem 4.9.

Theorem 4.6 *Let q be a prime power, $q \equiv 1 \pmod 4$. Denote by A the adjacency matrix of the Paley graph $P(q)$. Then the following holds:*

(a) *if $\sigma^2 - \sigma + \mu$ is not divisible by p, then*

$$r_p(A + \sigma I) = \begin{cases} q-1 & \text{if } p \mid (k+\sigma) \\ q & \text{otherwise;} \end{cases}$$

(b) *if $q \equiv 1 \pmod p$, then $r_p(A) = k$ and $r_p(A+I) = k+1$;*

(c) *if q is a square modulo p, $q \not\equiv 1 \pmod p$, then $r_p(A + \sigma_1 I) = r_p(A + \sigma_2 I) = \frac{1}{2}(q+1)$, where $\sigma_1, \sigma_2 \in \mathbb{F}_p$ satisfy $\sigma_1 + \sigma_2 \equiv 1 \pmod p$ and $\sigma_1\sigma_2 \equiv -\mu \pmod p$;*

PROOF. Let $\sigma \in \mathbb{Z}$. The matrix $A + \sigma I$ has eigenvalues $k + \sigma$, $\sigma + \frac{\sqrt{q}-1}{2}$ and $\sigma - \frac{\sqrt{q}+1}{2}$ and determinant $(k+\sigma)(\sigma^2 - \sigma - \mu)^{(q-1)/2}$. Assume that $\det(A + \sigma I) \neq 0$. Otherwise, replace $A + \sigma I$ by $A + (\sigma + p)I$.

Clearly, if $\det(A + \sigma I)$ is not divisible by p, then $r_p(A + \sigma I) = q$. Furthermore, if $p \mid (k+\sigma)$ and $p \not| (\sigma^2 - \sigma - \mu)$, then $r_p(A + \sigma I) = q - 1$. This is obvious if $p \parallel (k+\sigma)$. If $p^2 \mid (k+\sigma)$, then consider the matrix $A + (\sigma + p)I$. Since $p \parallel (k + \sigma + p)$ and $p \not| ((p+\sigma)^2 - (p+\sigma) - \mu)$, we get $r_p(A + \sigma I) = r_p(A + (\sigma + p)I) = q - 1$. Hence, assertion (a) is proven.

Now we turn to the case where $\sigma^2 - \sigma - \mu \equiv 0 \pmod p$. Let us first determine the $\sigma \in \mathbb{F}_p$ that satisfy $\sigma^2 - \sigma - \mu \equiv 0 \pmod p$.

If $p = 2$, then there is no solution for σ if μ is odd. If μ is even, then both 0 and 1 satisfy the equation.

If $p > 2$, then we must solve

$$\begin{aligned} \sigma^2 - \sigma - \mu &\equiv 0 \pmod p, \\ (2\sigma - 1)^2 &\equiv 4\mu + 1 \equiv q \pmod p. \end{aligned} \tag{4.1}$$

We distinguish three cases:

(1) if q is not a square modulo p, then (4.1) has no solutions;
(2) if $q \equiv 0 \pmod{p}$, the only solution is $\sigma \equiv \frac{1}{2}(p+1) \pmod{p}$;
(3) if q is a nonzero square modulo p, then (4.1) has two different solutions $\sigma_1, \sigma_2 \in \mathbb{F}_p$ satisfying $\sigma_1 + \sigma_2 \equiv 1 \pmod{p}$ and $\sigma_1\sigma_2 \equiv -\mu \pmod{p}$.

The statements (b) and (c) deal with the case of two different solutions σ_1 and σ_2 for (4.1). From

$$\begin{aligned}(A+\sigma_1 I)(A+\sigma_2 I) &= A^2 + (\sigma_1+\sigma_2)A + \sigma_1\sigma_2 I \\ &= (\mu + \sigma_1\sigma_2)I + (\sigma_1+\sigma_2-1)A + \mu J \\ &\equiv \mu J \pmod{p},\end{aligned}$$

and Lemma 3.2, it follows that

$$r_p(A+\sigma_1 I) + r_p(A+\sigma_2 I) \leq q + r_p(\mu J). \tag{4.2}$$

Suppose $p \mid \mu$. Then $\sigma_1 \equiv 0 \pmod{p}$, $\sigma_2 \equiv 1 \pmod{p}$ and

$$q = r_p(I) \leq r_p(A+I) + r_p(-A) \leq q. \tag{4.3}$$

From $p \mid \mu$ it follows that $p \mid v$, but $p \nmid (k+1)$. Thus by Lemma 3.8, we find $\underline{1} \in \mathcal{R}_p(A+I)$ and $\underline{1} \notin \mathcal{R}_p(A)$. Together with Lemma 4.5 this yields

$$r_p(A+I) = r_p(J-A-I) + 1 = r_p(A) + 1.$$

Substituting this in (4.3) gives $r_p(A) = \frac{1}{2}(q-1)$ and $r_p(A+I) = \frac{1}{2}(q+1)$, which proves (b).

Now suppose $p \nmid \mu$, while q is still a nonzero square (mod p). Then we have

$$q = r_p(I) \leq r_p(A+\sigma_1 I) + r_p(-A-\sigma_2 I) \overset{(4.2)}{\leq} q+1.$$

The left hand inequality holds, because $(\sigma_1 - \sigma_2)^2 \equiv q \not\equiv 0 \pmod{p}$.

The proof of (c) is completed by showing that $r_p(A+\sigma_i I) \geq \frac{1}{2}(q+1)$ for $i = 1,2$. Let $q \equiv \rho^2 \pmod{p}$, $\rho \in \mathbb{F}_p$. Suppose $p \mid (k+\sigma)$ for $\sigma = \sigma_1, \sigma_2$ and recall that σ satisfies (4.1). Then $k + \sigma \equiv \frac{1}{2}(q-1) + \frac{1}{2}(1 \pm \rho) \equiv 0 \pmod{p}$, which implies $\rho^2 \pm \rho \equiv 0 \pmod{p}$. In that case, $q \equiv 0 \pmod{p}$ or $q \equiv 1 \pmod{p}$, a contradiction. Thus $p \nmid (k+\sigma)$.

W.l.o.g. we assume that $\det(A+\sigma I) \neq 0$ for $\sigma = \sigma_1, \sigma_2$. Now Lemma 2.6 yields that if $p \parallel (\sigma^2 - \sigma - \mu)$, then $r_p(A+\sigma I) \geq \frac{1}{2}(q+1)$. If $p^2 \mid (\sigma^2 - \sigma - \mu)$, then $p \parallel ((p+\sigma)^2 - (p+\sigma) - \mu)$, since $2\sigma - 1 \equiv \pm\rho \pmod{p}$ and $\rho \not\equiv 0 \pmod{p}$. Hence again, we get $r_p(A+\sigma I) = r_p(A+(p+\sigma)I) \geq \frac{1}{2}(q+1)$. □

From the proof of this theorem it follows that there is one case left, namely, when there is exactly one solution for (4.1). Then p and σ satisfy $q \equiv 0 \pmod{p}$ and $\sigma \equiv \frac{1}{2}(p+1) \pmod{p}$. Applying the same arguments as in the proof of the above theorem does not yield good bounds. From

$$\begin{aligned}(A + \frac{1}{2}(p+1)I)^2 &= \frac{1}{4}p(p^{e-1} + p + 2)I + pA + \mu J \\ &\equiv \mu J \pmod{p},\end{aligned}$$

we obtain the upper bound

$$r_p(A + \frac{1}{2}(p+1)I) \leq \frac{1}{2}(q+1).$$

Furthermore, $\det(A + \frac{p+1}{2}I) = \frac{1}{2}p^{\frac{1}{2}(q+1)}(p^{e-1}+1)(\frac{1}{4}(p-p^{e-1})^{(q-1)/2}$. Hence only for $e = 1$ a nontrivial lower bound is yielded by Lemma 2.6.

We computed $r_p(A(p^e) + \frac{p+1}{2}I)$ for several small values of p and e. The values obtained in this way suggested that $r_p(A(p^e) + \frac{p+1}{2}I) = (\frac{p+1}{2})^e$. This has been proven by Brouwer (personal communication). The result is obtained by applying the following theorem to the matrix $2A(p^e)+I-J$.

Theorem 4.7 *Let F be a field and let $\mathcal{A}$ and $\mathcal{B}$ be two subsets of F. Set $m := |\mathcal{A}|$ and $n := |\mathcal{B}|$. Let M be an $m \times n$ matrix with the rows labelled by the elements of $\mathcal{A}$ and the columns by the elements of $\mathcal{B}$. Define the entries of M by*

$$M_{ab} := p(a,b),$$

where $p(x,y) := \sum_{i=0}^{d}\sum_{j=0}^{e} c_{ij}x^iy^j$ for d and e satisying $d < m$ and $e < n$. Define the subspace $S \subseteq F[y]$ by

$$S := \langle \sum_{j=0}^{e} c_{ij}y^j \mid 0 \le i \le d \rangle.$$

Then $r_F(M) = \dim(S)$.

PROOF. Set $V := F^{\mathcal{B}}$, that is, V is the vectorspace consisting of all maps from $\mathcal{B}$ into F. Define an evaluation map $E : F[y] \longmapsto V$ by

$$E(f(y))(b) := f(b), \quad \text{for all } b \in \mathcal{B}.$$

In fact, Ef is the restriction of f to $\mathcal{B}$ (notation: $f|_{\mathcal{B}}$). Define $R := \mathcal{R}_F(M)$. We claim that $S \cong R$, from which the result follows. In order to prove this, we show that

(1) $E|_S$ is injective;

(2) $E(S) = R$,

Indeed, combining (1) and (2) yields $S \cong E(S) = R$ as claimed.

We first show that the kernel of $E|_S$ contains the all-zero vector only. Let $f \in S$. Suppose $f(b) = 0$ for every $b \in \mathcal{B}$. Then f has n zeros. However, f is a polynomial of degree at most e. Since we assumed that $n > e$, this implies that $f(b)$ can not be zero for every $b \in \mathcal{B}$ unless the coefficients of f all equal zero. This proves (1).

Furthermore, let $\underline{r}_a$ be a row of M. The yth entry is $p(a,y) = \sum_i a^i \sum_j c_{ij}y^j$, which is a linear combination of elements of S. Thus $R \subseteq E(S)$.

We are left with the proof of $E(S) \subseteq R$, which is equivalent to $R^{\perp} \subseteq E(S)^{\perp}$. Let $\underline{r} \in R^{\perp}$. Denote its coordinate r_b by $r(b)$. Then $\underline{r}$ satisfies for every $a \in \mathcal{A}$

$$\sum_{b\in\mathcal{B}} r(b)p(a,b) = 0.$$

Thus

$$\sum_{i,j,b} r(b)c_{ij}a^ib^j = 0$$

for a in $\mathcal{A}$. Regard the left hand expression as a polynomial in a, then

$$\sum_{i=0}^{d} x^i \sum_{j,b} r(b)c_{ij}b^j = 0$$

for $x \in \mathcal{A}$. Since $d < m$, this polynomial can not have m zeros unless $\sum_{j,b} r(b)c_{ij}b^j = 0$ for every i, $0 \le i \le e$. But, in that case, $\underline{r}$ is contained in $E(S)^{\perp}$. Hence $R^{\perp} \subseteq E(S)^{\perp}$, which completes the

proof of the theorem. □

We shall apply this theorem to the matrix Q defined in the following way. Take $F = \mathbb{F}_q$, where q is the power of an odd prime p, say $q = p^e$. We introduce here the *Legendre symbol* χ that is defined for $x \in \mathbb{F}_q$ by

$$\chi(x) := \begin{cases} 1 & \text{if } x \text{ is a nonzero square in } \mathbb{F}_q \\ 0 & \text{if } x = 0 \\ -1 & \text{otherwise.} \end{cases}$$

Clearly, $\chi(x) = x^{(q-1)/2}$. Let Q be the $q \times q$ matrix with rows and columns indexed by the elements of $\mathbb{F}_q$ and entries $Q_{xy} := \chi(y - x)$. Then

$$Q_{xy} = (y-x)^{(q-1)/2} = \sum_{i=0}^{(q-1)/2} (-1)^i \begin{pmatrix} \frac{q-1}{2} \\ i \end{pmatrix} x^i y^{(-i+(q-1)/2)}.$$

Q is called a *Jacobsthal matrix*. It clearly satisfies the conditions of Theorem 4.7. In this case, the set S takes the following form:

$$S = \langle \begin{pmatrix} \frac{q-1}{2} \\ i \end{pmatrix} x^i \mid 0 \le i \le \tfrac{1}{2}(q-1) \rangle.$$

We obviously have

$$\dim(S) = |\{i \mid \begin{pmatrix} \frac{q-1}{2} \\ i \end{pmatrix} \not\equiv 0 \,(\mathrm{mod}\, p),\ 0 \le i \le \tfrac{1}{2}(q-1)\}|.$$

In order to compute this number, we need the following well-known result from number theory.

Theorem 4.8 (Lucas) *Let the p-ary expansions of l and k be $l = \sum_i l_i p^i$ and $k = \sum_i k_i p^i$, where $0 \le l_i, k_i \le p-1$. Then*

$$\begin{pmatrix} l \\ k \end{pmatrix} \equiv \prod_i \begin{pmatrix} l_i \\ k_i \end{pmatrix} \,(\mathrm{mod}\, p).$$

For a proof of this theorem we refer to Van Lint [14, p.47].

Recalling that $q = p^e$, one easily verifies that

$$\frac{1}{2}(q-1) = \sum_{i=0}^{e-1} \frac{1}{2}(p-1)p^i.$$

Furthermore, write $i = \sum_{j=0}^{e-1} i_j p^j$. For every i_j there are $\frac{p+1}{2}$ choices such that $\begin{pmatrix} \frac{p-1}{2} \\ i_j \end{pmatrix} \neq 0$. Thus, by Theorem 4.8, there are $(\frac{p+1}{2})^e$ possible values for i such that $\begin{pmatrix} \frac{q-1}{2} \\ i \end{pmatrix} \neq 0$. By Theorem 4.7, $r_q(Q) = \dim(S)$, hence

$$r_q(Q) = \left(\frac{p+1}{2}\right)^e.$$

Obviously, if $q \equiv 1 \pmod 4$ and A denotes the adjacency matrix of the Paley graph $P(q)$, then $Q = 2A + I - J$. From

$$Q^2 = qI - J \equiv -J \pmod p \text{ and } (2A + I)^2 = qI + (q-1)J \equiv -J \pmod p,$$

we obtain that both $\mathcal{R}_p(2A + I)$ and $\mathcal{R}_p(2A + I - J)$ contain the all-one vector, hence $r_p(A + 2I) = r_p(Q)$. Since the entries of Q are elements of both $\mathbb{F}_p$ and $\mathbb{F}_q$, we have $r_p(Q) = r_q(Q)$. Together with the obvious fact that $r_p(A + \frac{p+1}{2}I) = r_p(2A + I)$, this proves the following theorem.

Theorem 4.9 *Let A be the adjacency matrix of the Paley graph $P(q)$. If $q = p^e$, then $r_p(A + \frac{p+1}{2}I) = (\frac{p+1}{2})^e$.*

Hence for every Paley graph $P(q)$ with adjacency matrix A and for every combination of p and $\sigma \in \mathbb{Z}$, the p-rank of $A + \sigma I$ is given by Theorem 4.6 or Theorem 4.9.

Chapter 5

Bounds from character theory

Character theory provides a powerful tool for proving theorems on finite groups. By applying results from this theory to an automorphism group of a $srg\ \Gamma$, a set of possible values for the p-rank of A can be obtained. Of course, such a set will only be of help if it is small.

The aim of the first two sections is to introduce definitions and results from representation and character theory. We do not give many details and usually omit proofs; for an extensive treatment we refer to Isaacs [11]. The application of character theory to our problem is discussed in Section 3. Finally, a class of graphs is presented for which it is expected that a small set of possible values for $r_p(A)$ can be derived.

5.1 Group representations and modules

Throughout this chapter, G will denote a finite group with identity e. Furthermore, let F be a field. We denote by $GL(n, F)$ the group of all nonsingular elements of $F^{n\times n}$.

Definition An *F-representation* of G of *degree* n is a homomorphism $\Phi : G \longmapsto GL(n, F)$.

Example 5.1 Let G act on a finite set Ω. The *permutation representation* Π of G over F is defined in the following way: label the rows and columns of $\Pi(g)$, $g \in G$, by the elements of Ω and set

$$(\Pi(g))_{\omega_1,\omega_2} := \begin{cases} 1 & \text{if } \omega_1 g = \omega_2 \\ 0 & \text{otherwise.} \end{cases}$$

Thus Π maps each $g \in G$ to the appropriate permutation matrix. If we take $\Omega = G$, then Π is called the *regular F-representation* of G.

Denote by $F[G]$ the set of all formal sums $\sum_{g\in G} a_g g$, $a_g \in F$. If addition is performed componentwise and multiplication is defined as

$$(\sum_{g_1\in G} a_{g_1} g_1)(\sum_{g_2\in G} a_{g_2} g_2) := \sum_{g_1\in G}\sum_{g_2\in G} (a_{g_1} a_{g_2})(g_1 g_2),$$

then $F[G]$ can be considered as a ring with identity e. It is easy to see that $F[G]$ can also be considered as a vectorspace over F of dimension $|G|$. Since $(cx)y = c(xy) = x(cy)$ for all $c \in F$ and $x, y \in F[G]$, $F[G]$ is an F-algebra.

Definition Let V be a finite dimensional vectorspace over F. Suppose for every $\underline{v} \in V$ and $x \in F[G]$ that a unique $\underline{v}x \in V$ is defined. Assume for all $x, y \in F[G]$, $\underline{v}, \underline{w} \in V$ and $c \in F$ that

(a) $(\underline{v} + \underline{w})x = \underline{v}x + \underline{w}x$;
(b) $\underline{v}(x + y) = \underline{v}x + \underline{v}y$;
(c) $(\underline{v}x)y = \underline{v}(xy)$;
(d) $(c\underline{v})x = c(\underline{v}x) = \underline{v}(cx)$;
(e) $\underline{v}e = \underline{v}$.

Then V is called an $F[G]$-*module.*

There is a one-to-one correspondence between F-representations of G of degree n and $F[G]$-modules of dimension n. Let Φ be a representation of degree n and denote by V the n-dimensional vectorspace over F. Then

$$\underline{v}(\sum_{g \in G} a_g g) := \sum_{g \in G} a_g(\underline{v}\Phi(g)) \in V$$

holds for every $\sum_{g \in G} a_g g \in F[G]$. It is easily verified that V is an $F[G]$-module.

Conversely, if V is an $F[G]$-module, choose an F-basis $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n$ for V. Let $\Phi(g)$ be the element of $F^{n \times n}$ satisfying

$$\begin{pmatrix} \underline{v}_1 \\ \vdots \\ \underline{v}_n \end{pmatrix} \Phi(g) = \begin{pmatrix} \underline{v}_1 g \\ \vdots \\ \underline{v}_n g \end{pmatrix}.$$

Then Φ is an F-representation of G. Note that the representation depends on the basis.

Usually we shall explain ideas from the representation point of view. However, the foregoing implies that results for representations can be easily expressed in terms of modules (and vice versa). In the rest of this section we write 'modules' instead of '$F[G]$-modules' and 'representations' instead of 'F-representations'.

Two representations Φ and Ψ are said to be *similar* if there exists a nonsingular matrix P such that, for every $g \in G$,

$$P\Phi(g)P^{-1} = \Psi(g).$$

If Φ and Ψ correspond to modules V and W, respectively, then the representations are similar iff V and W are isomorphic, i.e. there exists an invertible linear transformation $\theta : V \longmapsto W$ satisfying $\theta(\underline{v}x) = \theta(\underline{v})x$ for all $\underline{v} \in V$ and $x \in F[G]$.

Let V be a module. A *submodule* U of V is a linear subspace of V that satisfies $\underline{u}x \in U$ for every $\underline{u} \in U$ and $x \in F[G]$. V is called *reducible* if V has a nontrivial submodule (that is, other than $\{\underline{0}\}$ or V). Otherwise, we say that V is *irreducible.* V is *completely reducible* if it can be written as a direct sum of irreducible submodules.

Theorem 5.1 ([11, p.4]) *Let G be a finite group and F a field whose characteristic does not divide $|G|$. Then every $F[G]$-module is completely reducible.*

This theorem is generally known as Maschke's Theorem.

It is evident that there exists a *composition series* for a module V, that is, a series of submodules of the form

$$V = V_0 \supset V_1 \supset V_2 \supset \ldots \supset V_t = 0$$

such that for each i the factor module V_{i-1}/V_i is a nonzero irreducible module. An irreducible module U is called an *irreducible constituent* of V of *multiplicity* m if $U \cong V_{i-1}/V_i$ for precisely m values of i. The *Jordan-Hölder Theorem* ([20, p.43]) asserts that the set of composition factors of V does not depend on the choice of composition series.

These concepts can be translated into the language of representations as follows. Let U be a proper nonzero submodule of a module V. Choose a basis b_U for U and extend it to a basis for V. By a suitable numbering of the basis vectors, the representation Φ associated with V takes the following form:

$$\Phi(g) = \left(\begin{array}{c|c} \Phi_2(g) & \Theta(g) \\ \hline 0 & \Phi_1(g) \end{array}\right), \quad g \in G. \tag{5.1}$$

Here Φ_1 is the representation corresponding to U with respect to b_U and Φ_2 is a representation corresponding to V/U. As far as (ir)reduciblility is concerned, the same terminology is used for representations as for the associated modules.

If there exists a submodule $W \subseteq V$ in the above situation so that $V = U \oplus W$, then, for an appropriate choice of basis of V, $\Phi = \mathrm{diag}(\Phi_1, \Phi_2')$, where Φ_2' is the representation corresponding to W. Hence, if Φ is a completely reducible representation, then Φ is similar to a representation in block diagonal form, where each block is an irreducible representation.

We see that the irreducible representations play an important rôle in representation theory. As a matter of fact, they can be considered as the building blocks for all representations. It can be proven (see [11, p.147]) that there exist only finitely many irreducible F-representations up to similarity.

Finally, let Φ be an F-representation of G and let $\bar{F}$ be a field containing F. Then Φ can also be considered as a $\bar{F}$-representation. It is entirely possible that Φ is irreducible over F, but reducible as an $\bar{F}$-representation. If Φ is irreducible for every field $\bar{F} \supseteq F$, then Φ is said to be *absolutely irreducible*.

Definition The field F is called a *splitting field* for G if every irreducible F-representation of G is absolutely irreducible.

5.2 Character theory

5.2.1 Generalities

For most applications of representations, it is not necessary to distinguish between similar representations. Therefore, it would be useful to have a function defined on the set of representations that distinguishes between nonsimilar irreducible representations, but has the same value for similar representations. A character is such a function.

Definition Let Φ be an F-representation of G. Then the *F-character* ϕ of G *afforded* by Φ is the function given by $\phi(g) = \mathrm{tr}(\Phi(g)), g \in G$.

If V is an $F[G]$-module corresponding to the F-representation Φ of G and Φ affords ϕ, then we also say that V affords ϕ. Let us first show that characters do indeed satisfy the required properties.

Proposition 5.2 *Let Φ and Ψ be F-representations that afford the characters ϕ and ψ, respectively. If Φ and Ψ are similar, then $\phi = \psi$.*

PROOF. If Φ and Ψ are similar representations, then $P^{-1}\Phi(g)P = \Psi(g)$ for some nonsingular matrix P. This shows that $\psi(g) = \mathrm{tr}(\Psi(g)) = \mathrm{tr}(P^{-1}\Phi(g)P) = \mathrm{tr}(\Phi(g)) = \phi(g)$ for every $g \in G$. Hence $\phi = \psi$. □

Theorem 5.3 ([11, p.155]) *Let F be any field. Then the characters afforded by nonsimilar irreducible F-representations of G are nonzero, distinct and linearly independent.*

Let us give some examples. In fact, these are the only characters that we shall deal with.

Example 5.2 The F-character afforded by the trivial representation $\Phi(g) = 1$, for every $g \in G$, is denoted by 1_G and is called the *principal F-character*. Obviously, $1_G(g) = 1$ for all $g \in G$.

Example 5.3 Consider the permutation representation Π defined in Example 5.1. If Π is considered as a representation over a field of characteristic 0, then the *permutation character* π afforded by Π is

$$\pi(g) = |\{\omega \in \Omega \mid \omega g = \omega\}|, \quad g \in G.$$

If $\Omega = G$, then the *regular character* ρ satisfies

$$\rho(g) = \begin{cases} |G| & \text{if } g = e \\ 0 & \text{otherwise.} \end{cases}$$

In the following proposition, some elementary properties of characters are proven:

Proposition 5.4 *Let Φ be an F-representation that affords the character ϕ. Denote by V the $F[G]$-module corresponding to Φ.*

(a) *The set of characters is closed under addition.*
(b) *If U is a proper nonzero submodule of V, then V affords the character $\phi_1 + \phi_2$, where ϕ_1 and ϕ_2 denote the character afforded by U and V/U, respectively.*
(c) *Characters are constant on the conjugate classes of the group.*

PROOF. (a) Define for $g \in G$

$$\Xi(g) := \left(\begin{array}{c|c} \Phi(g) & 0 \\ \hline 0 & \Psi(g) \end{array}\right).$$

Obviously, Ξ is also an F-representation of G and affords the character $\xi = \phi + \psi$.
(b) This follows from (5.1).
(c) $\phi(h^{-1}gh) = \mathrm{tr}(\Phi(h^{-1}gh)) = \mathrm{tr}(\Phi(h^{-1})\Phi(g)\Phi(h)) = \mathrm{tr}(\Phi(h^{-1})\Phi(h)\Phi(g)) = \mathrm{tr}(\Phi(g)) = \phi(g)$ for all $g, h \in G$. □

By the *exponent* of G we mean the least positive integer d such that $g^d = e$ for all $g \in G$. Naturally, $d \mid |G|$.

Lemma 5.5 *Let Φ be an F-representation of G of degree n affording the character ϕ and let $g \in G$. Let d denote the exponent of G. Suppose that the polynomial $x^d - 1$ splits into linear factors over F. Then $\Phi(g)$ is similar to a diagonal matrix $\mathrm{diag}(\epsilon_1, \ldots, \epsilon_n)$, where the ϵ_i satisfy $\epsilon_i^d = 1$, $1 \le i \le n$.*

PROOF. For each $g \in G$ we have $\Phi(g)^d = \Phi(g^d) = I_n$. Thus the eigenvalues ϵ_i of $\Phi(g)$ satisfy $\epsilon_i^d = 1$. By assumption, the ϵ_i are elements of F, hence $\Phi(g)$ is diagonalizable over F. This proves

the lemma. □

Thus, if F satisfies the condition of the above lemma, then $\phi(g)$ is the sum of the eigenvalues of $\Phi(g)$, counting multiplicities. We also deduce from this lemma that an algebraically closed field is a splitting field for every group.

5.2.2 Ordinary characters

This section deals with characters over $\mathbb{C}$, the so-called *ordinary characters*.

Lemma 5.6 ([11, p.16]) *The number of similarity classes of irreducible representations equals the number of conjugacy classes of G.*

Theorem 5.3 yields that this latter number is also the number of distinct characters afforded by irreducible representations. (In this section 'character' always means '$\mathbb{C}$-character' and the same holds for 'representation'.) These characters are called *irreducible* and the set of all irreducible $\mathbb{C}$-characters of G is denoted by $\mathrm{Irr}(G)$.

Since $\mathbb{C}$ has characteristic 0, it follows from Maschke's Theorem that every $\mathbb{C}$-representation Φ is completely reducible. Thus for the character ϕ afforded by Φ, we have $\phi = \sum_{\chi_i \in Irr(G)} n_i \chi_i$, where n_i denotes the multiplicity of the irreducible representation that affords χ_i as constituent of Φ. The χ_i with $n_i > 0$ are called the *irreducible constituents* of ϕ.

For later use we introduce the following concept:

Definition Let ϕ and ψ be $\mathbb{C}$-characters of G. Then

$$[\phi, \psi] := \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}$$

is called the *inner product* of ϕ and ψ.

We state without proof ([11, p.21]) that

$$[\chi_i, \chi_j] = \delta_{ij}, \quad \chi_i, \chi_j \in \mathrm{Irr}(G),$$

where δ_{ij} denotes the Kronecker delta. Hence, if $\phi = \sum_{\chi \in Irr(G)} n_i \chi_i$ is a character of G, then

$$[\phi, \phi] = \sum n_i^2. \tag{5.2}$$

The *degree* of an ordinary character is defined as the degree of the corresponding representation. Since $\Phi(e) = I_{deg(\Phi)}$ for every representation Φ, we can also say that the degree of a character ϕ is equal to $\phi(e)$.

Definition An *algebraic integer* is a complex number which is a root of a monic polynomial with integer coefficients.

The set of all algebraic integers forms a ring that we shall denote by R^*. For an ordinary character ϕ, we have $\phi(g) \in R^*$ for all $g \in G$. This holds because of Lemma 5.5 and the fact that $\mathbb{C}$ is

algebraically closed.

For a particular group G, the irreducible characters are usually presented in a *character table* as shown below. The rows are indexed by the irreducible characters; the columns correspond to the conjugacy classes of G. A class is denoted by the order of its elements. Classes of elements of the same order are distinguished by subscripts.

In [6], the so-called *Atlas*, the character tables of many finite groups are given.

Example 5.4(a) The character table of A_5, the alternating group of degree 5, has the following form:

Class :	1	2	3	5_1	5_2
χ_1 :	1	1	1	1	1
χ_2 :	4	0	1	−1	−1
χ_3 :	5	1	−1	0	0
χ_4 :	3	−1	0	α_1	α_2
χ_5 :	3	−1	0	α_2	α_1

where $\alpha_1 = \frac{1+\sqrt{5}}{2}$, $\alpha_2 = \frac{1-\sqrt{5}}{2}$.

5.2.3 Modular characters

The theory of modular characters is concerned with the connections between ordinary representations and representations over a field of characteristic p. We shall need only a few results from this theory. For proofs and more details the reader is referred to Chapter 15 of [11].

Throughout this section we fix a prime p. The (p-)modular characters are defined in a particular field F^* that is constructed in the following way. Choose a maximal ideal $\mathcal{I} \supseteq pR^*$ of R^* and set $F^* := R^*/\mathcal{I}$. Let $\theta : R^* \longmapsto F^*$ be defined as $\theta(r) := r\mathcal{I}$, $r \in R^*$. Furthermore, let $\mathcal{U} := \{\epsilon \in \mathbb{C} \mid \epsilon^n = 1 \text{ for some } n \in \mathbb{Z} \text{ with } p \not| n\}$. Clearly, $\mathcal{U} \subseteq \mathcal{R}^*$.

The field F^* has the following properties:

(a) F^* has characteristic p;

(b) F^* is algebraically closed;

(c) $\theta : \mathcal{U} \longmapsto F^* \setminus \{0\}$ is an isomorphism of multiplicative groups.

Definition If p divides the order of $g \in G$, then g is called *p-singular*. Otherwise, g is said to be *p-regular*.

Let Φ be an F^*-representation of G of degree n. Denote by $\mathcal{S}$ the set of p-regular elements of G. We define a function $\eta : \mathcal{S} \longmapsto R^*$ in the following way. Let ϕ denote the F^*-character afforded by Φ and let $g \in \mathcal{S}$. From Property (b) and Lemma 5.5 it follows that $\phi(g) = \sum_{i=1}^{n} \epsilon_i$, where the $\epsilon_i \in F^*$ denote the eigenvalues of $\Phi(g)$, counting multiplicities. Property (c) says that for each i, $1 \leq i \leq n$, there exists a unique $u_i \in \mathcal{U}$ such that $\theta(u_i) = \epsilon_i$. Define $\eta(g) := \sum_{i=1}^{n} u_i$.

Definition The function η is called the *modular character* or *Brauer character* of G afforded by Φ.

Strictly speaking, it is not correct to define η as *the* modular character afforded by Φ, since the maximal ideal $\mathcal{I}$ is not uniquely determined. To avoid this problem, we always assume that a particular

maximal ideal $\mathcal{I}$ has been fixed.

We notice that the modular characters are only defined on the p-regular elements of G. It can be proven that this is sufficient to reconstruct the full F^*-character afforded by Φ.

Similar F^*-representations afford equal modular characters and modular characters are constant on conjugacy classes. Both statements follow from the fact that similar representations have the same eigenvalues.

Let $\Phi_1, \ldots, \Phi_m$ be a set of representatives for the similarity classes of irreducible F^*-representations of G and let η_i be the modular character afforded by Φ_i. The η_i are called the *irreducible* modular characters and we write $\mathrm{IM}(G) = \{\eta_1, \ldots, \eta_m\}$.

Theorem 5.7 $|\mathrm{IM}(G)|$ *equals the number of conjugacy classes of p-regular elements of G. Furthermore, the irreducible modular characters are nonzero, distinct and linearly independent.*

Modular characters connect $\mathrm{Irr}(G)$ and the representations of characteristic p as is shown in the next theorem.

Theorem 5.8 *Let ϕ be an ordinary character of G and let $\hat{\phi}$ denote the restriction of ϕ to S, the set of p-regular elements of G. Then $\hat{\phi}$ is a modular character of G.*

Thus $\hat{\phi} = \sum_{\eta_i \in IM(G)} n_i \eta_i$, for some nonnegative integers n_i which are not all zero. The next theorem shows that the construction of p-modular character tables for G can be restricted to those primes p that are a divisor of $|G|$.

Theorem 5.9 *Suppose $p \nmid |G|$. Then* $\mathrm{IM}(G) = \mathrm{Irr}(G)$.

The *Modular Atlas* ([18]) provides for many finite groups G the tables of irreducible p-modular characters. As an example, the tables of p-modular characters of A_5 for $p = 2, 3, 5$ are presented. We establish the notation that the irreducible p-modular characters are denoted by χ_i^p.

Example 5.4(b) $G = A_5$

$p = 2$:

Cl:	1	3	5_1	5_2
χ_1^2:	1	1	1	1
χ_2^2:	2	−1	β_1	β_2
χ_3^2:	2	−1	β_2	β_1
χ_4^2:	4	1	−1	−1

$p = 3$:

Cl:	1	2	5_1	5_2
χ_1^3:	1	1	1	1
χ_2^3:	3	−1	$-\beta_1$	$-\beta_2$
χ_3^3:	3	−1	$-\beta_2$	$-\beta_1$
χ_4^3:	4	0	−1	−1

$p = 5$:

Cl:	1	2	3
χ_1^5:	1	1	1
χ_2^5:	3	−1	0
χ_3^5:	5	1	−1

where $\beta_1 = \frac{-1+\sqrt{5}}{2}$, $\beta_2 = \frac{-1-\sqrt{5}}{2}$.

In the following section we shall need the next lemma:

Lemma 5.10 *Let Φ be an F^*-representation which affords the modular character η. Then* $\eta(e) = \deg(\Phi)$.

PROOF. Recall that $\Phi(e) = I_{deg(\Phi)}$. Since $\mathcal{U}$ and F^* are isomorphic, we must have $\theta(1) = 1$. Hence, the conclusion holds. □

Inspired by this lemma, we define the *degree* of a modular character η afforded by the F^*-representation Φ in the same way as the degree of an ordinary character, i.e. $\deg(\eta) := \deg(\Phi)$.

5.3 Application to strongly regular graphs

Let us now explain how representation and character theory can be used to obtain more information on the p-rank of the adjacency matrix A of a srg Γ. For notational convenience, we shall only consider $r_p(A)$, but all results can be easily translated into results for the p-rank of $A + \sigma I$, $\sigma \in \mathbb{Z}$.

Let F be a field. Take for G an automorphism group of Γ. Then G acts as a permutation group on the vertex set V of Γ. Denote by Φ_F the permutation representation of G acting on V regarded as an F-representation. Consider also A as a matrix with entries in F.

Proposition 5.11 *$\Phi_F(g)$ commutes with A for every $g \in G$.*

PROOF. This follows from

$$(\Phi_F^T(g)A\Phi_F(g))_{ij} = (A)_{ig,jg} = (A)_{ij}$$

and the fact that $\Phi_F^T(g) = \Phi_F^{-1}(g)$. □

This proposition yields

$$\mathcal{R}_F(A) = \mathcal{R}_F(\Phi_F(g)A) = \mathcal{R}_F(A\Phi_F(g))$$

for every $g \in G$. Hence $\mathcal{R}_F(A)$ can be considered as a submodule of the $F[G]$-module corresponding to Φ_F.

Let us first deal with the case $F = \mathbb{C}$. Denote by $\mathcal{R}(A)$ the rowspace of A over $\mathbb{C}$ and by $r(A)$ the $\mathbb{C}$-rank of A. For the $\mathbb{C}$-representation of G acting on V we simply write Φ. Finally, $\Phi(A)$ denotes the $\mathbb{C}$-representation corresponding to the submodule $\mathcal{R}(A)$.

Let ϕ and $\phi(A)$ denote the characters afforded by Φ and $\Phi(A)$, respectively. Because $r(A) = v = \deg(\phi)$, we have $\phi = \phi(A)$. In $\mathbb{C}$ the minimal idempotents E_i, $0 \leq i \leq 2$, can be expressed as linear combinations of I, A and J. So from the above remark it follows that $\mathcal{R}(E_i)$ is a submodule of $\mathcal{R}(A)$, $0 \leq i \leq 2$. In fact,

$$\mathcal{R}(A) = \mathcal{R}(E_0) \oplus \mathcal{R}(E_1) \oplus \mathcal{R}(E_2),$$

hence Φ can be written as

$$\Phi = \mathrm{diag}(\Phi_0, \Phi_1, \Phi_2),$$

where $\Phi_i := \Phi(E_i)$. Denote by ϕ_i the character afforded by Φ_i and recall that $vE_0 = J$. Then

$$\phi = 1_G + \phi_1 + \phi_2, \text{ with } \deg(\phi_1) = f \text{ and } \deg(\phi_2) = g. \tag{5.3}$$

We now turn to fields of characteristic p. Let us first introduce some notation. Since p is not fixed, we write F_p^* and $\mathrm{IM}_p(G)$ instead of F^* and $\mathrm{IM}(G)$. Furthermore, Φ_p^* denotes the permutation representation of G considered as an F_p^*-representation and $\Phi_p^*(A)$ the representation associated with the submodule $\mathcal{R}_p^*(A)$, the rowspace of A over F_p^*. The notation $\mathcal{R}_p^*(A)$ should not be confused with $\mathcal{R}_p(A)$, which as usual denotes the rowspace of A over $\mathbb{F}_p$. Finally, if ϕ is an ordinary character, then $\hat{\phi}^p$ denotes the restriction of ϕ to the p-regular elements of G. Theorem 5.8 asserts that $\hat{\phi}^p$ is a p-modular character.

A first observation is that the p-rank of A equals its rank over F_p^*. Together with Lemma 5.10, this yields

$$r_p(A) = \dim \mathcal{R}_p^*(A) = \deg(\phi^p(A)), \tag{5.4}$$

where $\phi^p(A)$ denotes the p-modular character afforded by $\Phi_p^*(A)$. Now what can we say about $\phi^p(A)$?

Let ϕ^p denotes the p-modular character afforded by Φ_p^*. Since $\phi(g)$ is equal to the number of vertices fixed under the action of g, it follows from the next lemma that the character ϕ^p can be computed in a rather easy way.

Lemma 5.12 *Let $\hat{\phi}^p$ and ϕ^p be as defined above. Then $\hat{\phi}^p = \phi^p$.*

PROOF. Let g be a p-regular element of G. By definition, $\hat{\phi}^p(g) = \phi(g) = \mathrm{tr}(\Phi(g)) = \sum_{i=1}^{v} \epsilon_i$, where the ϵ_i denote the eigenvalues of $\Phi(g)$, counting multiplicities. Furthermore, let θ be as defined in Section 5.2.3. Then $\phi^p(g) = \sum_{i=1}^{v} \theta^{-1}(\eta_i)$, where the η_i denote the $(F_p^*$-)eigenvalues of $\Phi_p^*(g)$. But $\Phi_p^*(g) = \Phi(g)$ for every element g of G, so $\epsilon_i = \theta^{-1}(\eta_i)$ for all i, which proves the statement. □

Since $\mathcal{R}_p^*(A)$ is a submodule of the module associated with Φ_p^*, we can write ϕ^p as

$$\phi^p = \phi^p(A) + \phi_1^p$$

for some p-modular character ϕ_1^p. Hence a set of possible values for the p-rank of A is

$$\{ \sum_{\chi_i^p \in IM_p(G)} n_i \chi_i^p(e) \mid 0 \le n_i \le \hat{n}_i,\ 1 \le i \le |\mathrm{IM}_p(G)| \},$$

where $\hat{n}_i$ denotes the multiplicity of χ_i^p as constituent of ϕ^p. For the case that we are interested in, namely when p divides r and s, this set can be reduced to

$$\{ \sum_{\chi_i^p \in IM_p(G)} n_i \chi_i^p(e) \mid 0 \le n_i \le \hat{n}_i,\ 1 \le i \le |\mathrm{IM}_p(G)|, \sum n_i \chi_i^p(e) \le \min(f,g) + 1 \},$$

where the upper bound of Theorem 3.4 is used.

From now on it is assumed that $p \mid r$ and $p \mid s$. Under this assumption, a set smaller then the one above can be obtained by considering the minimal idempotents E_i, $0 \le i \le 2$.

Define $L_i := \{\underline{x} \mid \underline{x} \in \mathcal{R}(E_i) \cap \mathbb{Z}^v\}$ and $L_i^p := \{\underline{x} \,(\mathrm{mod}\, p) \mid \underline{x} \in L_i\}$, $0 \le i \le 2$.

Proposition 5.13 *L_i^p is a vectorspace over $\mathbb{F}_p$ of dimension $r(E_i)$.*

PROOF. Set $\rho := r(E_i)$. Let $\{\underline{x}_1, \ldots, \underline{x}_\rho\}$ be a $\mathbb{Z}$-basis of L_i. Then $\{\underline{x}_i \,(\mathrm{mod}\, p) \mid 1 \le i \le \rho\}$ is a basis for L_i^p. If $\underline{z} := \sum_{i=1}^{\rho} \alpha_i \underline{x}_i \in p\mathbb{Z}^v$, then $\frac{1}{p}\underline{z} \in L_i$, thus $\frac{1}{p}\underline{z} = \sum_{i=1}^{\rho} \beta_i \underline{x}_i$ for some $\beta_i \in \mathbb{Z}$. This implies that $p \mid \alpha_i$ for all i. From this it follows that $\dim(L_i^p) = \rho$. □

Let E_i^p be a basis for L_i^p. Consider $L_0^p = \langle \underline{1} \rangle$, L_1^p and L_2^p as p-ary linear codes. We recall from Chapter 1 that the minimal idempotents satisfy

$$E_i E_j = \delta_{ij} E_i \quad \text{and} \quad E_i^T = E_i.$$

Thus $(\underline{x}_1, \underline{x}_2) \equiv 0 \,(\mathrm{mod}\, p)$ for every $\underline{x}_1 \in L_1^p$ and $\underline{x}_2 \in L_2^p$. This implies $L_2^p \subset (L_1^p)^\perp$ and $\underline{1} \in (L_1^p)^\perp$. Since $\dim(L_1^p)^\perp = v - \dim(L_1^p) = g + 1$ and $g \le \dim(L_2^p + \langle \underline{1} \rangle) \le g + 1$, it follows that

$$\dim((L_1^p)^\perp / (L_2^p + \langle \underline{1} \rangle)) \le 1, \tag{5.5}$$

with equality iff $\underline{1} \in L_2^p$. From $AE_1 = rE_1$ and the assumption that $r \equiv 0 \pmod{p}$, we get

$$\mathcal{R}_p(A) \subset (L_1^p)^\perp. \tag{5.6}$$

Combining (5.5) and (5.6) yields

$$\dim(\mathcal{R}_p(A)/(\mathcal{R}_p(A) \cap L_2^p)) \leq 1. \tag{5.7}$$

By similar arguments we obtain

$$\dim(\mathcal{R}_p(A)/(\mathcal{R}_p(A) \cap L_1^p)) \leq 1. \tag{5.8}$$

So far everything has been considered over $\mathbb{F}_p$ instead of F_p^*. It is obvious that the above relations still hold when $\mathcal{R}_p(A)$, L_1^p and L_2^p are substituted by $\mathcal{R}_p^*(A)$, $\mathcal{R}_p^*(E_1^p)$ and $\mathcal{R}_p^*(E_2^p)$, respectively. The $\mathcal{R}_p^*(E_i^p)$, $0 \leq i \leq 2$, are also submodules of the module corresponding to Φ_p^*. Clearly, $\phi^p(E_0^p) = 1_G$, where 1_G is considered as a p-modular character. Write $\phi^p(E_1^p)$ and $\phi^p(E_2^p)$ as

$$\phi^p(E_1^p) = \sum_{\chi_i^p \in IM_p(G)} \gamma_{1i}\chi_i^p \quad \text{and} \quad \phi^p(E_2^p) = \sum_{\chi_i^p \in IM_p(G)} \gamma_{2i}\chi_i^p.$$

From (5.7) and (5.8) with $\mathcal{R}_p^*(A)$, $\mathcal{R}_p^*(E_1^p)$ and $\mathcal{R}_p^*(E_2^p)$ instead of $\mathcal{R}_p(A)$, L_1^p and L_2^p, respectively, and the above expressions, we obtain that $\phi^p(A)$ is an element of the set

$$\{\, \delta\chi_0^p + \sum_{\chi_i^p \in IM_p(G)} \gamma_i\chi_i^p \mid \delta \in \{0,1\},\ \chi_0^p(e) = 1,\ 0 \leq \gamma_i \leq \min(\gamma_{1i}, \gamma_{2i}),\ 1 \leq i \leq |\mathrm{IM}_p| \,\}. \tag{5.9}$$

This leads to the following theorem:

Theorem 5.14 *Let Γ be a srg with eigenvalues k, r and s and let G be a group of automorphisms of Γ. Denote by ϕ the ordinary character afforded by the permutation representation of G acting on Γ. Let the p-modular character χ_j^p be an irreducible constituent of $\hat{\phi}^p(E_i)$ with multiplicity n_{ij} for $i = 1, 2$. Thus*

$$\hat{\phi}^p(E_1) = \sum_{\chi_i^p \in IM_p(G)} n_{1i}\chi_i^p \quad \textit{and} \quad \hat{\phi}^p(E_2) = \sum_{\chi_i^p \in IM_p(G)} n_{2i}\chi_i^p,$$

If p divides r and s, then

$$r_p(A) \in \{\, \delta + \sum_{\chi_i^p \in IM_p(G)} n_i\chi_i^p(e) \mid \delta \in \{0,1\},\ 0 \leq n_i \leq \min(n_{1i}, n_{2i}),\ 1 \leq i \leq |\mathrm{IM}_p| \,\}.$$

PROOF. Let L_i^p, $i = 1, 2$, be as defined before. Let B_i be a $\mathbb{Z}$-basis for $\mathcal{R}(E_i)$ such that $B_i^p := \{\underline{x} \pmod{p} \mid \underline{x} \in B_i\}$ is a basis for L_i^p (cf. Proposition 5.13). Then $\phi^p(A)$ is an element of the set (5.9) with E_i^p substituted by B_i^p. Because $r_p(A) = \deg(\phi^p(A))$, it suffices to show that $\hat{\phi}^p(E_i) = \phi^p(B_i^p)$ for $i = 1, 2$.

Denote the $\mathbb{C}$-representation of G on the basis B_i by Ψ and the F_p^*-representation of G on B_i^p by Ψ_p^*. Let ψ denote the character afforded by Ψ and let ψ^p denote the p-modular character afforded by Ψ_p^*. By definition, $\hat{\phi}^p(E_i) = \hat{\psi}^p$ and $\phi^p(B_i^p) = \psi^p$. Since $\Psi(g) = \Psi_p^*(g)$ for all p-regular elements of G, we obtain from Lemma 5.12 that

$$\hat{\psi}^p = \psi^p.$$

Hence $\hat{\phi}^p(E_i) = \phi^p(B_i^p)$ for $i = 1, 2$, which proves the theorem. □

Remark The set of possible values for $r_p(A)$ as given in the above theorem always contains 1 and, in many cases, also 2. However, we shall never mention these possibilities, since for the graphs to be discussed, it will always be easy to find a submatrix of A of p-rank 3.

In general we want to determine both $r_p(A)$ and $r_p(J - A)$. In that case, the following lemma is often useful.

Lemma 5.15 *Let $\phi^p(A)$ be the character afforded by the permutation representation $\Phi_p^*(A)$ of G acting on Γ. If $\underline{1} \in \mathcal{R}_p(A)$, then the principal character 1_G (regarded as a p-modular character) is a constituent of $\phi^p(A)$.*

PROOF. Obviously, since $\langle \underline{1} \rangle$ is a submodule of $\mathcal{R}_p^*(A)$. □

Let us illustrate the foregoing with a small example. A more interesting example will be discussed at the end of the next section.

Example 5.5 The full automorphism group of the triangular graph $T(5)$ (cf. Section 2.2) is S_5, the symmetric group of degree 5. Thus the alternating group A_5 is also a group of automorphisms of the graph. Since the spectrum of $T(5)$ is $6^1, 1^4, (-2)^5$, the only interesting case is $r_3(A - I)$. Denote by ϕ the permutation character associated with the action of A_5 on the vertices of $T(5)$.

We first determine the irreducible constituents of ϕ by means of the table in Example 5.4(a). Since $\phi(e) = 10$, $\phi((12)(34)) = 2$, $\phi((123)) = 1$ and $\phi((12345)) = 0$, we find that $\phi = \chi_1 + \chi_2 + \chi_3$. By (5.3), $\phi(E_1) = \chi_2$ and $\phi(E_2) = \chi_3$.

From the tables in Example 5.4(b) we find that $\hat{\chi}_1^3 = \chi_1^3$, $\hat{\chi}_2^3 = \chi_4^3$ and $\hat{\chi}_3^3 = \chi_1^3 + \chi_4^3$. Hence, by Theorem 5.14, $\phi^3(A - I) = \chi_4^3$ or $\phi^3(A - I) = \chi_1^3 + \chi_4^3$. The rows of $A - I$ add up to $-\underline{1}$ (modulo 3), thus $\underline{1} \in \mathcal{R}_3(A - I)$. Now it follows from Lemma 5.15 that χ_1^3 is an irreducible constituent of $\phi^3(A - I)$. Thus $r_3(A - I) = 1 + \deg(\chi_4^3) = 5$. Taking A as in Proposition 2.5, a subgraph of $A - I$ of 3-rank 5 is readily found. Furthermore, $r_3(A - I) \leq 5$ by Theorem 3.5. Hence indeed, $r_3(A - I) = 5$. Finally, since $-J(J - A + I) \equiv J \pmod 3$, we also find that $r_3(J - A + I) = 5$.

5.4 Rank 3 graphs

Continuing with the notation of the previous section, it seems reasonable to assume that the set (5.9) will be large if Φ has many irreducible constituents. Let G act transitively on a finite set Ω. If G_ω, the subgroup of G fixing $\omega \in \Omega$, has ρ orbits on Ω, then G is said to be a *rank ρ group*. Denote by π the permutation character of G as defined in Example 5.3. Write π as $\pi = \sum_{\chi_i \in Irr(G)} n_i \chi_i$, where n_i denotes the multiplicity of χ_i as a constituent of π. In [11, p.68] it is proven that $[\pi, \pi] = \rho$, where $[\ ,\ ]$ denotes the inner product as defined in Section 2. From (5.2) we obtain that $\sum n_i^2 = \rho$. Hence π has at most ρ irreducible constituents. Thus if G is a group of automorphisms acting transitively on the vertex set of Γ and has low rank, then probably G gives rise to a small set of possible values for the p-rank of A. We now introduce a class of graphs for which such an automorphism group exists.

Let G and Ω be as defined above. If G is a rank 3 group of even order, then a srg Γ can be constructed from G in the following way. Take Ω as the vertex set of Γ. Denote the three orbits of G_ω, $\omega \in \Omega$ by $\{\omega\}$, Γ_ω and Δ_ω. Let two vertices ω_1 and ω_2 be adjacent whenever $\omega_1 \in \Gamma_{\omega_2}$. The adjacency is well defined, because from the assumption that $|G|$ is even, it follows that $\omega_1 \in \Gamma_{\omega_2}$ iff

$\omega_2 \in \Gamma_{\omega_1}$. Clearly, G is a transitive group of automorphisms of the graph. For obvious reasons, Γ is called a *rank 3 graph*.

Denote by Φ the permutation representation of G with respect to Ω. Write ϕ for the character afforded by Φ. From the above discussion it follows that ϕ has precisely three irreducible constituents, say $\phi = \chi_1 + \chi_2 + \chi_3$, $\chi_i \in \mathrm{Irr}(G)$. Now according to (5.3), we have $\chi_1 = 1_G$, $\deg(\chi_2) = f$ and $\deg(\chi_3) = g$. Hence for a rank 3 graph we expect the set (5.9) to be small when G is the group that defines the graph.

We conclude this chapter with an example in which we study the p-rank of three rank 3 graphs. We shall only give the groups from which these graphs are derived. By applying Theorem 5.14 to these groups, small sets of possible values for the p-rank are obtained. In some cases the actual value of the p-rank can be easily determined from this set; in other cases we need more information about the structure of the graph. The character tables of the groups involved can be found in the *Atlas* and the *Modular Atlas*. The degree of an irreducible character is written as a subscript. Characters of the same degree are distuinguished by letters.

Example 5.6 Let Γ be a rank 3 graph derived from the group G and let x be a vertex of Γ. It may happen that G_x has a rank 3 representation on the set Γ_x, which denotes the set of vertices adjacent to x. This process may occur several times and yield a so-called *rank 3 tower*.

In this example we shall investigate the p-rank of the first three elements of the *Suzuki tower*.

	v	k	λ	μ	r	s	f	g	G
Γ_1	36	14	4	6	2	-4	21	14	$G_2(2)$
Γ_2	100	36	14	12	6	-4	36	63	HJ
Γ_3	416	100	36	20	20	-4	65	350	$G_2(4)$
Γ_4	1782	416	100	96	20	-16	780	1001	Suz

The groups involved in this tower are the Chevalley groups $G_2(2)$ and $G_2(4)$, the sporadic Hall-Janko group and the sporadic Suzuki group. For more details on the rank 3 representations we refer to Hubaut [10].

The permutation representation of $G_2(2)$ acting on Γ_1 affords the ordinary character $\chi_1 + \chi_{14} + \chi_{21}$. From the *Modular Atlas* we obtain

$$\hat{\chi}_{14}^2 = \chi_{14}^2, \quad \hat{\chi}_{21}^2 = \chi_1^2 + \chi_6^2 + \chi_{14}^2$$

and

$$\hat{\chi}_{14}^3 = \chi_1^3 + \chi_{3a}^3 + \chi_{3b}^3 + \chi_7^3, \quad \hat{\chi}_{21}^3 = 2\chi_1^3 + \chi_{6a}^3 + \chi_{6b}^3 + \chi_7^3.$$

Theorem 5.14 yields that $14 \leq r_2(A_1), r_2(J - A_1) \leq 15$. Since $r_2(A_1)$ is even (Lemma 3.9) and $r_2(J - A_1)$ satisfies $r_2(J - A_1) \leq r(6I - 3A_1 + J) = r(E_2) = 14$, we conclude that $r_2(A_1) = r_2(J - A_1) = 14$.

For the 3-rank of $A_1 + I(-J)$ we can only deduce that $7 \leq r_3(A_1 + I(-J)) \leq 9$. However, this is a considerable improvement on the upper bound 15, which is obtained from Theorem 3.5.

For the *Hall-Janko graph* Γ_2 the interesting cases are $r_2(A_2)$ and $r_5(A_2 - I)$. With respect to HJ we have $\phi(E_1) = \chi_{36}$ and $\phi(E_2) = \chi_{63}$, which satisfy

$$\hat{\chi}_{36}^2 = \chi_{36}^2, \quad \hat{\chi}_{63}^2 = 3\chi_1^2 + 2\chi_{6a}^2 + 2\chi_{6b}^2 + \chi_{36}^2$$

and

$$\hat{\chi}^5_{36} = \chi^5_1 + \chi^5_{14} + \chi^5_{21}, \quad \hat{\chi}^5_{63} = \chi^5_1 + \chi^5_{21} + \chi^5_{41}.$$

From Theorem 5.14 and the fact that $r_2(A_2)$ is even, it immediately follows that $r_2(A_2) = 36$. Furthermore, we have $r_2(J-A_2) = 36+\epsilon$, where ϵ equals 0 or 1 depending on whether $\underline{1} \in \mathcal{R}_2(J-A_2)$ or not.

Looking only at the characters, we obtain that $21 \leq r_5(A_2 - I(-J)) \leq 23$. This result can be slightly improved in the following way. It is easily verified that

$$3(A_2 - I)^2 \equiv J \,(\mathrm{mod}\, 5) \text{ and } 3(I - A_2)(J - A_2 + I) \equiv J \,(\mathrm{mod}\, 5).$$

Hence χ^5_1 is a constituent of $\phi^5(A_2 - I(-J))$ by Lemma 5.15. Thus $22 \leq r_2(A_2 - I) = r_2(J - A_2 + I) \leq 23$.

As for Γ_3 we restrict ourselves to $r_2(A_3)$. The irreducible characters χ_{65} and χ_{350} of $G_2(4)$ satisfy

$$\hat{\chi}^2_{65} = \chi^2_1 + \chi^2_{14a} + \chi^2_{14b} + \chi^2_{36}, \quad \hat{\chi}^2_{350} = 6\chi^2_1 + 4\chi^2_{6a} + 4\chi^2_{6b} + \chi^2_{14a} + \chi^2_{14b} + 2\chi^2_{36} + \chi^2_{196}.$$

First of all, we notice that $r_2(A_3) > r_2(A_2) = 36$. The strict inequality can be seen in the following way. Since $\phi^2(A_2) = \chi^2_{36}$ (where χ^2_{36} is a character of HJ), Lemma 5.15 implies that $\underline{1}$ is not contained in $\mathcal{R}_2(A_2)$. The induced subgraph on a vertex of Γ_3 and its neighbours has adjacency matrix

$$\left(\begin{array}{c|c} 0 & \underline{1} \\ \hline \underline{1}^T & A_2 \end{array}\right).$$

Now it is evident that $r_2(A_2) = r_2(A_3)$ would imply that $\underline{1} \in \mathcal{R}_2(A_2)$. From $\mathcal{R}(E_1) = \mathcal{R}(16I + 4A_3 - J)$ it follows that χ^2_1 as constituent of $\hat{\chi}^2_{65}$ corresponds to $\langle\underline{1}\rangle$. This leads to the conclusion that $r_2(A_3) \in \{50, 64\}$ if $\mathcal{R}_2(A_3)$ does not contain the all-one vector and $r_2(A_3) \in \{38, 52, 66\}$ otherwise. Furthermore, $r_2(J - A_3) \in \{37, 38, 50, 51, 52, 64, 65, 66\}$.

Chapter 6

Results

In this chapter we shall determine (bounds for) the p-rank of a considerable number of strongly regular graphs. In most cases the theory of the previous chapters is not sufficient to determine the p-rank completely, hence we also have to examine the structure of the graph. A table of the results is given at the end of this chapter. All graphs discussed here are described in Brouwer and Van Lint [4] or Hubaut [10].

In general, the notation is the same as used in the previous chapters. The subscripts of the irreducible characters indicate their degree. The character tables of the groups involved can all be found in the *Atlas* or the *Modular Atlas*. Furthermore, 'subgraph' will always mean 'induced subgraph'.

The graphs that we consider are often constructed from other combinatorial objects. The reader who is not familiar with (some of) these concepts is referred to the Appendix. Besides definitions, results that are used in order to determine the p-rank are mentioned there. We refer to the Appendix by (An), where n indicates the section.

In this chapter we mainly deal with so-called *sporadic graphs*. These graphs are related to the *sporadic groups* by means of their group of automorphisms. Usually, the sporadic group acts as a rank 3 group on the vertex set of the corresponding graph. As for the greater part of the groups mentioned here we refer to the literature for a description, e.g. Suzuki [20].

6.1 The Higman-Sims family

The Steiner systems $S(4,7,23)$ and $S(3,6,22)$ (A1) give rise to many sporadic graphs. The three graphs of the Higman-Sims family are derived from $S(3,6,22)$. Each of them is a unique rank 3 graph.

The Higman-Sims graph Γ_{Hi} has parameters $(v,k,\lambda,\mu) = (100,22,0,6)$ and is obtained by the following construction. Take as vertex set the 22 points and 77 blocks of $S(3,6,22)$ and the symbol ∞. Join ∞ to all the points, join a point to the 21 blocks containing it and let two blocks be adjacent whenever they are disjoint. The subgraph on the 77 blocks is a srg with parameters $(v,k,\lambda,\mu) = (77,16,0,4)$ and is denoted by Γ_{π}. Let x_0 be a point of $S(3,6,22)$. The subgraph of Γ_{π} on the blocks not containing x_0 is again strongly regular with parameters $(v,k,\lambda,\mu) = (56,10,0,2)$. This graph is the *Gewirtz graph* which has already been discussed in Example 3.2. We shall denote it by Γ_G.

Label the first row of A_{Hi} by ∞, the next 22 rows by the points and the last 56 rows by the blocks

not containing x_0. Then A_{H_i} has the following form:

$$A_{H_i} = \left(\begin{array}{c|c|c} 0 & 1\ldots1 & 0\ldots0 \\ \hline \underline{1}^T & O_{22} & N_1 \\ \hline \underline{0}^T & N_1^T & A_\pi \end{array}\right), \quad \text{where } A_\pi = \left(\begin{array}{c|c} O_{21} & N_2 \\ \hline N_2^T & A_G \end{array}\right). \tag{6.1}$$

Let us start with the Gewirtz graph. Its spectrum is $10^1, 2^{35}, (-4)^{20}$. Hence the only interesting cases are $r_2(A_G)$ and $r_3(A_G + I)$. In Example 3.2 we derived that $r_2(A_G) = 20$. Furthermore, we claimed that $\underline{1}$ could be written as the sum of an even number of rows of A_G, which implied that $r_2(J - A_G) = 20$. This will be proven now.

Γ_G is a rank 3 graph derived from $PSL(3,4)$. The corresponding permutation representation affords the ordinary character $\chi_1 + \chi_{20} + \chi_{35}$. The 2-modular characters $\hat{\chi}^2_{20}$ and $\hat{\chi}^2_{35}$ satisfy

$$\hat{\chi}^2_{20} = 2\chi_1^2 + \chi_{9a}^2 + \chi_{9b}^2, \quad \hat{\chi}^2_{35} = \chi_1^2 + \chi_{8a}^2 + \chi_{8b}^2 + \chi_{9a}^2 + \chi_{9b}^2.$$

Since $r_2(A_G) = 20$, we have $\phi^2(A_G) = 2\chi_1^2 + \chi_{9a}^2 + \chi_{9b}^2$. The constituent χ_1^2 of χ_{35}^2 corresponds to the submodule $\langle\underline{1}\rangle$, because $24E_1 = 16I + 4A_G - J$, thus $\underline{1} \in L_1^2$. From this we conclude that $\underline{1} \in \mathcal{R}_2(A_G)$. Number the points of $S(3,6,22)$ from 1 to 22 and assume that the vertices of Γ_G do not contain 22. The rows of A_G labelled by the following blocks form a basis of $\mathcal{R}_2(A_G)$.

(1 2 5 12 18 19)*	(2 4 5 9 11 13)*	(3 7 8 9 10 13)*	(5 6 11 12 16 21)
(1 4 6 8 12 13)*	(2 5 6 8 10 15)*	(4 5 7 8 18 21)*	(5 7 10 11 17 19)*
(1 5 6 7 9 14)	(2 7 8 11 12 14)*	(4 6 9 10 17 21)*	(5 8 9 12 17 20)
(1 7 11 13 16 18)*	(3 4 5 10 12 14)*	(4 7 9 12 16 19)	(6 7 10 12 18 20)*
(1 9 10 11 12 15)*	(3 4 6 7 11 15)	(4 8 10 11 16 20)*	(6 8 9 11 18 19)

The sum of the rows indexed by the $*$-marked blocks equals $\underline{1}$ (modulo 2). This is easily verified from the submatrix of A_G corresponding to these blocks. Hence, $\underline{1}$ can indeed be written as the sum of an even number of rows of A_G.

Let us now examine the 3-rank of $A_G + I$. From the *Modular Atlas* we obtain

$$\hat{\chi}^3_{20} = 2\chi_1^3 + \chi_{19}^3, \quad \hat{\chi}^3_{35} = \chi_1^3 + \chi_{15}^3 + \chi_{19}^3.$$

So $r_3(J - A_G - I) \geq 19$. We claim that equality holds. The Gewirtz graph is a subgraph of a srg Γ on 112 vertices (the first subconstituent of the McLaughlin graph) that will be discussed in the next section. It will be shown that $r_3(J - A_\Gamma - I) \leq 19$. This proves our claim. From Lemma 3.8 we find $r_3(A_G + I) = r_3(J - A_G - I) + 1 = 20$.

We mention here that Brouwer and Haemers [3] have obtained the same results by different methods.

Γ_π has spectrum $16^1, 2^{55}, (-6)^{21}$, so we only have to determine $r_2(A_\pi)$. Obviously, $20 = r_2(A_G) \leq r_2(A_\pi) \leq r(22I - 11A_\pi + 2J) = r(E_2) = 21$ holds. By Lemma 3.9, $r_2(A_\pi)$ is even, hence $r_2(A_\pi) = 20$. From Lemma 3.8 it follows that $r_2(J - A_\pi) = 21$.

The spectrum of the Higman-Sims graph is $22^1, 2^{77}, (-8)^{22}$. Therefore, we consider $r_2(A_{H_i})$ and $r_5(A_{H_i} + 3I)$.

Examining the matrix A_{H_i} in (6.1), we observe that a row of A_{H_i} indexed by a point can not be expressed as the sum of rows labelled by blocks. From this, it follows that $20 = r_2(A_\pi) < r_2(A_{H_i}) \leq 23$. Because $r_2(A_{H_i})$ has to be even, we conclude that $r_2(A_{H_i}) = 22$. In order to

determine $r_2(J - A_{H_i})$, we consider the matrix $J - A_{H_i}$ in more detail. As in (6.1), let the first row be labelled by ∞. Furthermore, assume that the second row is indexed by x_0 and that the last 56 rows are indexed by the blocks not containing x_0. Thus the submatrix of $J - A_{H_i}$ on the last 56 rows and columns is $J - A_G$. Since $r_2(J - A_G) = 20$, we can choose 20 rows of $J - A_G$ that are linearly independent over $\mathbb{F}_2$. Denote these rows by $\underline{b}_i$, $1 \leq i \leq 20$, and let $\underline{a}_i$ be the corresponding row of $J - A_{H_i}$, thus $\underline{a}_i = (11; \underline{x}_i; \underline{b}_i)$. Denote the first row of $J - A_{H_i}$ by $\underline{a}_0$. Then $\underline{a}_0 = (10; \underline{x}_0; \underline{1})$. Obviously, $\dim(\langle \underline{a}_i \mid 0 \leq i \leq 20 \rangle) = 21$. Suppose that the second row can be expressed as a linear combination of the $\underline{a}_i$. Then for the first two coordinates the following must hold:

$$\lambda_0(10) + \textstyle\sum_{i=1}^{20} \lambda_i(11) \equiv (01) \pmod 2$$

and for the last 56 coordinates

$$\lambda_0 \underline{1} + \textstyle\sum_{i=1}^{20} \lambda_i \underline{b}_i \equiv \underline{1} \pmod 2.$$

Thus

$$\begin{aligned} \textstyle\sum_{i=1}^{20} \lambda_i &\equiv 1 \pmod 2, \\ \textstyle\sum_{i=1}^{20} \lambda_i \underline{b}_i &\equiv \underline{0} \pmod 2. \end{aligned}$$

Since the $\underline{b}_i$ form a basis for $\mathcal{R}_2(J - A_G)$, it follows from the second equation that $\lambda_i = 0$ for $1 \leq i \leq 20$, which contradicts the first equation. Hence, $r_2(J - A_{H_i}) \geq 22$. Together with the upper bound $r_2(J - A_{H_i}) \leq r(10I - 5A_{H_i} + J) = r(E_2) = 22$, this yields $r_2(J - A_{H_i}) = 22$.

For $r_5(A_{H_i} + 3I)$ we have $22 = r_5(A_{77} + 3I_{77}) < r_5(A_{H_i} + 3I_{100}) \leq 23$. The strict inequality is obtained by the same argument as used for the inequality $r_2(A_{77}) < r_2(A_{H_i})$. Thus $r_5(A_{H_i} + 3I) = 23$. Furthermore, from $(2I - A_{H_i})(J - A_{H_i} - 3I) \equiv J \pmod 5$, it follows that $r_5(A_{H_i} + 3I) \leq r_5(J - A_{H_i} - 3I)$. Together with the upper bound derived in Theorem 3.5, this yields $r_5(J - A_{H_i} - 3I) = 23$.

6.2 The McLaughlin graph and its subconstituents

The McLaughlin graph Γ_M is the unique graph with parameters $(v, k, \lambda, \mu) = (275, 112, 30, 56)$. It can be constructed in the following way. Denote the set of points of the Steiner system $S(4, 7, 23)$ by X and the set of blocks by $\mathcal{B}$. Let $\mathcal{B}_1$ be the set of blocks containing a fixed point x_0 and define $\mathcal{B}_2 := \mathcal{B} \setminus \mathcal{B}_1$. Take as vertex set of Γ_M the set $X \setminus \{x_0\} \cup \mathcal{B}$. Join a block $B_1 \in \mathcal{B}_1$ to all points that are nonincident to it; join a block of $\mathcal{B}_2$ to the points incident to it. Let two blocks of $\mathcal{B}_i$, $i = 1, 2$, be adjacent when they have a single point in common. Finally, a block $B_1 \in \mathcal{B}_1$ is joined to a block $B_2 \in \mathcal{B}_2$ whenever they intersect in three points. Γ_M is a rank 3 graph with the sporadic McLaughlin group as group of automorphisms.

The spectrum of Γ_M is $112^1, 2^{252}, (-28)^{22}$, so the interesting cases are $r_2(A_M)$, $r_3(A_M + I)$ and $r_5(A_M + 3I)$. Let ϕ be the character afforded by the permutation representation of the McLaughlin group acting on Γ_M, then

$$\phi = \chi_1 + \chi_{22} + \chi_{252}.$$

Because $\hat{\chi}_{22}^2 = \chi_{22}^2$ and the 2-rank of A_M is even (Lemma 3.9), it immediately follows that $r_2(A_M) = 22$. Furthermore $r_2(J - A_M) = 23$ by Lemma 3.8.

Clearly, the subgraph of Γ_M induced on the 22 points is a coclique. Thus $r_3(A_M + I) \geq 22$. We claim that in fact equality holds. Denote by $\mathcal{P}_B$ the set of points adjacent to the block B. Thus $|\mathcal{P}_B| = 16$ if $B \in \mathcal{B}_1$ and $|\mathcal{P}_B| = |B| = 7$ otherwise. Let B_i and B_i' be two different blocks of $\mathcal{B}_i$ for

$i = 1, 2$. From the above-mentioned construction of Γ_M we deduce that

$$\begin{array}{l}
\text{if } B_1 \sim B_1', \text{ then } |B_1 \cap B_1'| = 1 \text{ and } \{x_0\} \in B_1 \cap B_1', \text{ hence } |\mathcal{P}_1 \cap \mathcal{P}_1'| = 10; \\
\text{if } B_1 \not\sim B_1', \text{ then } |B_1 \cap B_1'| = 3 \text{ and } \{x_0\} \in B_1 \cap B_1', \text{ hence } |\mathcal{P}_1 \cap \mathcal{P}_1'| = 12; \\
\text{if } B_1 \sim B_2, \text{ then } |B_1 \cap B_2| = 3 \text{ and } \{x_0\} \notin B_1 \cap B_2, \text{ hence } |\mathcal{P}_1 \cap \mathcal{P}_2| = 4; \\
\text{if } B_1 \not\sim B_2, \text{ then } |B_1 \cap B_2| = 1 \text{ and } \{x_0\} \notin B_1 \cap B_2, \text{ hence } |\mathcal{P}_1 \cap \mathcal{P}_2| = 6; \\
\text{if } B_2 \sim B_2', \text{ then } |B_2 \cap B_2'| = 1 \text{ and } \{x_0\} \notin B_2 \cap B_2', \text{ hence } |\mathcal{P}_2 \cap \mathcal{P}_2'| = 1; \\
\text{if } B_2 \not\sim B_2', \text{ then } |B_2 \cap B_2'| = 3 \text{ and } \{x_0\} \notin B_2 \cap B_2', \text{ hence } |\mathcal{P}_2 \cap \mathcal{P}_2'| = 3.
\end{array}$$

Now it is easily verified that for every block B the row $\underline{r}_B$ satisfies

$$\underline{r}_B \equiv \sum_{p \in \mathcal{P}_B} \underline{r}_p \pmod 3.$$

Hence indeed $r_3(A_M + I) = 22$. Again Lemma 3.8 yields that $r_3(J - A_M - I) = r_3(A_M + I) - 1 = 21$.

By the *subconstituents* of a graph we mean the induced subgraphs on the vertex sets $\{x \mid x \sim y\}$ and $\{x \mid x \not\sim y\}$ for an arbitrary vertex y. The subconstituents of the McLaughlin graph are both strongly regular. We shall denote them by Γ_{112} and Γ_{162} and their parameters are (112, 30, 2, 10) and (162, 56, 10, 24), respectively. Thus

$$A_M = \left(\begin{array}{c|c|c} 0 & 1\ldots1 & 0\ldots0 \\ \hline \underline{1}^T & A_{112} & N \\ \hline \underline{0}^T & N^T & A_{162} \end{array}\right). \tag{6.2}$$

Now $r_5(A_M + 3I)$ is easily determined. The second subconstituent Γ_{162} has spectrum $56^1, 2^{140}, (-16)^{21}$. Hence, $22 \leq r_5(A_M + 3I) \leq 23$. Considering the matrix $A_M + 3I$ with A_M as in (6.2), we notice that the first row can not be written as the sum of some of the last 162 rows because of the first coordinate. Hence $r_5(A_M + 3I) = 23$. From $(2I - A_M)(J - A_M - 3I) \equiv J \pmod 5$, it follows that $r_5(A_M + 3I) \leq r_5(J - A_M - 3I)$. Together with the usual upper bound, this yields $r_5(J - A_M - 3I) = 23$. Let us now turn to the subconstituents of Γ_M.

We start with Γ_{112}. Since its spectrum is $30^1, 2^{90}, (-10)^{21}$, we shall consider $r_2(A_{112})$ and $r_3(A_{112} + I)$. However, let us first give a direct description of Γ_{112}. Choose two points x and y from the point set of $S(4, 7, 23)$. Take as vertices the 112 blocks that contain exactly one of these points. Join two blocks containing the same point when this is the only point they have in common. Join a block containing x to a block containing y iff they intersect in three points. This produces directly the srg (112, 30, 2, 10). Notice that the subgraph on the blocks containing x (y) is the Gewirtz graph.

We first consider $r_2(A_{112})$. The graph Γ_{112} is the point graph of the generalized quadrangle $GQ(3, 9)$ (A2). Bagchi, Brouwer and Wilbrink [1] have proven that the 2-rank of the adjacency matrix of the point graph of $GQ(q, q^2)$ for odd q equals $q^3 - q^2 + q + 1$. Hence $r_2(A_{112}) = 22$.

We prove that $r_2(J - A_{112}) = 22$ by showing that $\underline{1}$ can be written as an even number of rows of A_{112}. In $GQ(3, 9)$ every line is incident with four points. Take a line $l = \{x_1, x_2, x_3, x_4\}$. W.l.o.g. assume that the first four rows of A_{112} are indexed by the points x_i, $1 \leq i \leq 4$. Then from the parameters of the graph, it follows that these rows can be written as

$$\left[\begin{array}{l|l} 0111 & \underline{1}_{27} \\ 1011 & \quad \underline{1}_{27} \\ 1101 & \quad\quad \underline{1}_{27} \\ 1110 & \quad\quad\quad \underline{1}_{27} \end{array}\right].$$

This obviously proves the statement.

The last result can also be obtained in a different way, using the fact that $r_2(A_{112}) = r_2(A_M)$. Without loss of generality assume that the first 22 rows of A_{112} form a basis for $\mathcal{R}_2(A_{112})$. Set $\underline{a}_i := (1; \underline{b}_i; \underline{n}_i)$ for $1 \leq i \leq 22$, where $\underline{b}_i$ denotes the ith row of A_{112} and $\underline{a}_i$ is the corresponding row of A_M, with the latter as in (6.2). Because the $\underline{a}_i$ are a basis for $\mathcal{R}_2(A_M)$, there exist λ_i, $1 \leq i \leq 22$, such that

$$\sum_{i=1}^{22} \lambda_i \underline{a}_i \equiv (0; \underline{1}; \underline{0}) \pmod 2.$$

Thus $\sum \lambda_i \equiv 0 \pmod 2$ and $\sum \lambda_i \underline{b}_i \equiv \underline{1} \pmod 2$, which is equivalent to the assertion that $\underline{1}$ can be written as an even number of rows of A_{112}.

Let us now look at $r_3(J - A_{112} - I)$ and $r_3(A_{112} + I)$. It is clear from Lemma 3.8 that $r_3(A_{112} + I) = r_3(J - A_{112} - I) + 1$. For the Gewirtz graph Γ_G we derived before that $r_3(J - A_G - I) \geq 19$, so

$$19 \leq r_3(J - A_{112} - I) \leq r_3(J - A_M - I) = 21. \tag{6.3}$$

Set $\rho := r_3(J - A_{112} - I)$. Without loss of generality, assume that the first ρ rows of $J - A_{112} - I$ are linearly independent. Denote by $\underline{r}_i$ the ith row of $J - A_M - I$, with A_M as in (6.2). Let $S \subseteq \mathcal{R}_3(J - A_M - I)$ be defined as

$$S := \langle \underline{r}_i \mid 2 \leq i \leq \rho + 1 \rangle.$$

Then $\dim(S) = \rho$. One easily sees that the first row of $J - A_M - I$ is not contained in S, because otherwise the first ρ rows of $J - A_{112} - I$ would not be linearly independent. A row indexed by a block can not be contained in $S + \langle \underline{r}_1 \rangle$, because of the first coordinate. Thus $r_3(J - A_M - I) \geq r_3(J - A_{112} - I) + 2$. Combining this with (6.3), we conclude that $r_3(J - A_{112} - I) = 19$. This also proves that $r_3(J - A_G - I) = 19$.

The graph Γ_{162} can be constructed from the projective plane $PG(2,4)$ (A3) in the following way. Let the vertex set consist of the 21 points, the 21 lines and one class of 120 Fano subplanes. Join a point to a line when they are not incident; join a point to a Fano plane when they are incident; join a line to a Fano plane when they have two points in common and join two Fano planes when they intersect in one point.

$$A_{162} = \left(\begin{array}{c|c|c} O_{21} & N_1 & N_2 \\ \hline N_1^T & O_{21} & N_3 \\ \hline N_2^T & N_3^T & A' \end{array}\right) \begin{array}{l} \text{points} \\ \text{lines} \\ \text{Fano planes} \end{array} \tag{6.4}$$

This graph is a rank 3 graph derived from $PSU_4(3)$. Since Γ_{162} has spectrum $56^1, 2^{140}, (-16)^{21}$, the interesting cases are $r_2(A_{162})$ and $r_3(A_{162} + I)$.

We first consider $r_2(A_{162})$. Goethals and Seidel [8] have shown that the vertex set of Γ_{162} can be split into two halves such that the induced subgraphs on these halves both form a strongly regular graph on 81 vertices with spectrum $20^1, 2^{60}, (-7)^{20}$. Denote this graph by Γ_{81}. Then $20 = r_2(A_{81}) \leq r_2(A_{162}) \leq 21$. Because $r_2(A_{162})$ is even by Lemma 3.9, we conclude that $r_2(A_{162}) = 20$.

In order to determine the 2-rank of $J - A_{112}$, write the matrix as

$$J_{162} - A_{162} = \left(\begin{array}{c|c} J_{81} - A_{81} & N \\ \hline N^T & J_{81} - A_{81} \end{array}\right).$$

There are 61 ones in every column of $J_{81} - A_{81}$ and 45 ones in each column of N. Hence the sum of the rows of $[J_{81} - A_{81} \mid N]$ equals $\underline{1}$ (modulo 2). In order to find out whether $\underline{1}$ is contained in $\mathcal{R}_2(A_{162})$

or not, we look at the permutation character $\phi = \chi_1 + \chi_{21} + \chi_{140}$ yielded by the action of $PSU_4(3)$ on the vertices of Γ_{162}. From $r_2(A_{162}) = 20$ and

$$\hat{\chi}_{21} = \chi_1^2 + \chi_{20}^2, \quad \hat{\chi}_{140} = \chi_{20}^2 + \chi_{120}^2,$$

it follows that $\phi^2(A_{162}) = \chi_{20}^2$. We see that $\phi^2(A_{162})$ has no constituent of degree 1, thus, by Lemma 5.15, the all-one vector is not contained in $\mathcal{R}_2(A_{162})$. Hence $r_2(J - A_{162}) = 21$.

For the 3-rank of $A_{162} + I$ and $J - A_{162} - I$, we look at (6.4). It is evident that $r_3(A_{162} + I) \geq 21$. In $PG(2,4)$ every line is incident to 5 points and every Fano subplane is incident to 7 points. Thus N_1 has 16 ones in every column, while N_2 has 7 ones per column. So

$$\sum_{i=1}^{21} \underline{r}_i \equiv \underline{1} \,(\mathrm{mod}\, 3) \quad \text{and} \quad \sum_{i=1}^{21} (\underline{1} - \underline{r}_i) \equiv -\underline{1} \,(\mathrm{mod}\, 3),$$

where $\underline{r}_i$ denotes the ith row of $A_{162} + I$. This proves that $r_3(A_{162} + I) = r_3(J - A_{162} - I)$.

Let l be a line and f a Fano subplane. Denote by P_l the set of points not incident to l and by P_f the set of points incident to f (thus $|P_l| = 16$ and $|P_f| = 7$). From the construction of Γ_{162} it follows that

$$\begin{array}{llll} \text{if} & l \neq l', \text{ then} & |P_l \cap P_{l'}| & = 12; \\ \text{if} & l \sim f, \text{ then} & |P_l \cap P_f| & = 4; \\ \text{if} & l \not\sim f, \text{ then} & |P_l \cap P_f| & = 6; \\ \text{if} & f \sim f', \text{ then} & |P_f \cap P_{f'}| & = 1; \\ \text{if} & f \not\sim f', \text{ then} & |P_f \cap P_{f'}| & = 3. \end{array}$$

From this it follows that any row of $A_{162} + I$ can be written as a linear combination of the first 21 rows. Hence $r_3(A_{162} + I) = r_3(J - A_{162} - I) = 21$.

6.3 Graphs related to the McLaughlin graph by switching

Let Γ_M^* be the graph obtained by adjoining an isolated vertex to the McLaughlin graph. This graph can be switched into several interesting graphs one of which is strongly regular. The adjacency matrix A_M^* of Γ_M^* satisfies

$$\begin{array}{rcrcl} r_2(A_M^*) & = & r_2(J - A_M^*) - 1 & = & 22; \\ r_3(A_M^* + I) & = & r_3(J - A_M^* - I) + 1 & = & 22; \\ & & r_5(A_M^* - 2I) & = & 24. \end{array}$$

Define a graph Γ_{276}^* on the 23 points and 253 blocks of $S(4,7,23)$ by joining a point to the blocks containing it and joining two blocks whenever they intersect in one point. From the explicit construction of Γ_M as given in the previous section, it is immediately seen that isolating a point from Γ_{276}^* by switching produces Γ_M^*. Note that Γ_{276}^* is not strongly regular. However, the subgraph induced on the blocks is a srg with parameters $(v,k,\lambda,\mu) = (253,112,36,60)$. This graph is denoted by Γ_{253} and will be discussed in the next section.

Write the adjacency matrix of Γ_{276}^* as

$$A_{276}^* = \left(\begin{array}{c|c} O_{23} & N \\ \hline N^T & A_{253} \end{array}\right). \tag{6.5}$$

We shall investigate $r_2(A_{276}^*)$ and $r_3(A_{276}^* + I)$.

The submatrix N has 7 ones in each column and 77 ones in every row. Thus

$$\sum_{i=1}^{276} \underline{r}_i \equiv \underline{1} \,(\mathrm{mod}\, 2) \quad \text{and} \quad \sum_{i=1}^{276} (\underline{1} - \underline{r}_i) \equiv \underline{1} \,(\mathrm{mod}\, 2),$$

where $\underline{r}_i$ denotes the ith row of A^*_{276}. Hence $r_2(A^*_{276}) = r_2(J - A^*_{276})$. From Lemma 3.11 it follows that $r_2(A^*_{276}) = r_2(A_M) + 2 = 24$. Thus $r_2(A^*_{276}) = r_2(J - A^*_{276}) = 24$.

Furthermore, we prove that $r_3(A^*_{276} + I) = r_3(J - A^*_{276} - I) = 23$. Clearly, $r_3(A^*_{276} + I) \geq 23$, since I_{23} is a submatrix of $A^*_{276} + I$. Let x denote a point, B a block and X the point set of $S(4,7,23)$. Write $\underline{r}_x$ ($\underline{r}_B$) for the row of $A^*_{276} + I$ indexed by x (B). From the fact that two blocks of $S(4,7,23)$ intersect in 1 or 3 points, it follows that

$$\sum_{x \in B} \underline{r}_x \equiv \underline{r}_B \,(\mathrm{mod}\, 3).$$

So $r_3(A^*_{276} + I) = 23$. The proof is completed by observing that

$$\sum_{x \in X} \underline{r}_x \equiv \underline{1} \,(\mathrm{mod}\, 3) \quad \text{and} \quad \sum_{x \in X} (\underline{1} - \underline{r}_x) \equiv -\underline{1} \,(\mathrm{mod}\, 3),$$

The graphs Γ^*_M and Γ^*_{276} can be switched into a $srg\,\Gamma_{276}$ with parameters $(v,k,\lambda,\mu) = (276,140,58,84)$. This graph was first constructed by Goethals and Seidel [8]. Its spectrum is $140^1, 2^{252}, (-28)^{23}$. Hence the interesting cases are $r_2(A_{276})$, $r_3(A_{276} + I)$ and $r_5(A_{276} - 2I)$.

Let us start with $r_2(A_{276})$. In [8] the first six rows of A_{276} are given by

$$\left(J_6 - I_6 \mid D_0 \mid D_1 \mid \ldots \mid D_9 \right), \tag{6.6}$$

where $D_i := [d_i d_i \ldots d_i]$, $0 \leq i \leq 9$, is a 6×27 matrix and $[d_0 d_1 \ldots d_9]$ denotes the incidence matrix of the 2-(6,3,2) design (A1). Thus there are 3 ones in every column d_i, $0 \leq i \leq 9$. Hence

$$\sum_{i=1}^{6} \underline{r}_i \equiv \underline{1} \,(\mathrm{mod}\, 2) \quad \text{and} \quad \sum_{i=1}^{6} (\underline{1} - \underline{r}_i) \equiv \underline{1} \,(\mathrm{mod}\, 2),$$

where $\underline{r}_i$ denotes the ith row of (6.6). Thus $r_2(A_{276}) = r_2(J - A_{276})$ and $r_2(A_{276}) = r_2(A_M) + 2 = 24$ by Lemma 3.10.

For the 3-rank of $A_{276} + I$ and $J - A_{276} - I$, Lemma 3.10 yields

$$\begin{array}{rcccccccl} 22 & = & r_3(A^*_{276} + I) - 2 & \leq & r_3(A_{276} + I) & \leq & r_3(A^*_M + I) + 2 & \leq & 24, \\ 21 & = & r_3(J - A^*_{276} - I) - 2 & \leq & r_3(J - A_{276} - I) & \leq & r_3(J - A^*_M - I) + 2 & \leq & 23. \end{array}$$

For $r_5(A_{276} - 2I)$ we find the following bounds:

$$22 = r_5(A^*_M - 2I) - 2 \leq r_5(A_{276} - 2I) \leq 24,$$

where Theorem 3.5 provides the upper bound. The same bounds apply to $r_5(J - A_{276} + 2I)$, since $r_5(J - A_{276} + 2I) = r_5(A_{276} - 2I)$. This can be seen by consideration of

$$\left(J_6 + 2I_6 \mid D_0 \mid D_1 \mid \ldots \mid D_9 \right), \tag{6.7}$$

with the D_i as in (6.6). Denote the ith row of (6.7) by $\underline{r}_i$, then

$$\sum_{i=1}^{6} \underline{r}_i \equiv \underline{3} \,(\mathrm{mod}\, 5) \quad \text{and} \quad \sum_{i=1}^{6} (\underline{1} - \underline{r}_i) \equiv \underline{3} \,(\mathrm{mod}\, 5).$$

Thus $r_5(A_{276} - 2I) = r_5(J - A_{276} + 2I)$.

The above graphs are switching-equivalent to a graph that consists of 11 mutually nonadjacent triangles and 243 further vertices each of which is adjacent to exactly one vertex of each triangle (see [8] for more details). The subgraph on the 243 vertices is strongly regular with parameters $(v, k, \lambda, \mu) = (243, 110, 37, 60)$. This graph is called the Delsarte graph; we denote it by Γ_D. Its spectrum is $110^1, 2^{220}, (-25)^{22}$, hence we only have to consider $r_3(A_D + I)$. In [8] it is proven that Γ_D contains a subgraph on 162 vertices that can be switched into Γ_{162}, the second subconstituent of the McLaughlin graph. Hence $19 = r_3(A_{162} + I) - 2 \leq r_3(A_D + I) \leq 23$, where the lower bound is obtained by applying Lemma 3.10 and the upper bound is the bound derived in Theorem 3.5. Since $r_3(J - A_{162} - I) = r_3(A_{162} + I)$, the same bounds apply to $r_3(J - A_D + I)$.

6.4 Other graphs derived from $S(4, 7, 23)$

Most graphs discussed in this chapter are derived from the Steiner system $S(4, 7, 23)$. This also holds for the three *srg*s that are studied in this section. Their parameters are

$$\begin{array}{rcl} \Gamma_{253} : (v, k, \lambda, \mu) & = & (253, 112, 36, 60); \\ \Gamma_{176} : (v, k, \lambda, \mu) & = & (176, 70, 18, 34); \\ \Gamma_{120} : (v, k, \lambda, \mu) & = & (120, 42, 8, 18). \end{array}$$

We have seen Γ_{253} already as a subgraph of the graph Γ^*_{276}, which was discussed in the previous section. It is constructed by taking as vertices the blocks of $S(4, 7, 23)$ and joining the blocks intersecting in one point. Clearly, the subgraph on the blocks containing a fixed point is the graph Γ_{77} of the Higman-Sims family. The graph Γ_{253} has spectrum $112^1, 2^{230}, (-26)^{22}$, thus we shall investigate $r_2(A_{253})$ and $r_7(A_{253} - 2I)$.

Γ_{253} is a rank 3 graph derived from M_{23}. The associated permutation character is $\chi_1 + \chi_{22} + \chi_{230}$. From the *Modular Atlas* we obtain

$$\hat{\chi}^2_{22} = \chi^2_{11a} + \chi^2_{11b}, \quad \hat{\chi}^2_{230} = \chi^2_{11a} + \chi^2_{11b} + \chi^2_{44a} + \chi^2_{44b} + \chi^2_{120}$$

and

$$\hat{\chi}^7_{22} = \chi^7_{22}, \quad \hat{\chi}^7_{230} = \chi^7_{22} + \chi^7_{208}.$$

Since $r_2(A_{253}) \geq r_2(A_{77}) = 20$ and $r_2(A_{253})$ is even, we find $r_2(A_{253}) = 22$ by application of Theorem 5.14. Furthermore, Lemma 3.8 yields that $r_2(J - A_{253}) = r_2(A_{253}) + 1 = 23$.

We also obtain from Theorem 5.14 that $22 \leq r_7(A - 2I) \leq 23$. Since

$$\begin{array}{rcl} 3J(A_{253} - 2I) & \equiv & J \;\; (\mathrm{mod}\, 7), \\ -2J(J - A_{253} + 2I) & \equiv & J \;\; (\mathrm{mod}\, 7), \end{array}$$

it follows from Lemma 5.15 that χ^7_1 is an irreducible constituent both of $\phi^7(A_{253} - 2I)$ and of $\phi^7(J - A_{253} + 2I)$. We conclude that $r_7(A_{253} - 2I) = r_7(J - A_{253} + 2I) = 23$.

Γ_{176} is the subgraph of Γ_{253} on the blocks not containing a fixed point. Every other element of the point set of $S(4,7,23)$ is contained in 56 of the 176 blocks. The subgraph on the blocks containing a second fixed point is the Gewirtz graph. Deleting these blocks produces a graph on 120 vertices which is again strongly regular. This graph is Γ_{120}.

The spectrum of Γ_{176} is $70^1, 2^{154}, (-18)^{21}$. Therefore we shall consider $r_2(A_{176})$ and $r_5(A_{176}-2I)$. The Mathieu group M_{22} acts as a rank 3 group on the vertex set of Γ_{176}. The corresponding permutation character is $\chi_1 + \chi_{21} + \chi_{154}$. For χ_{21} and χ_{154} the following holds:

$$\hat{\chi}_{21}^2 = \chi_1^2 + \chi_{10a}^2 + \chi_{10b}^2, \quad \hat{\chi}_{154}^2 = 2\chi_1^2 + \chi_{10a}^2 + \chi_{10b}^2 + \chi_{34}^2 + \chi_{98}^2$$

and

$$\hat{\chi}_{21}^5 = \chi_{21}^5, \quad \hat{\chi}_{154}^5 = \chi_{21}^5 + \chi_{133}^5. \tag{6.8}$$

Using the facts that the Gewirtz graph Γ_G is a subgraph of Γ_{176} and that $r_2(A_G) = 20$, we find $r_2(A_{176}) = 20$ or $r_2(A_{176}) = 22$, depending on whether the all-one vector is contained in $\mathcal{R}_2(A_{176})$ or not. For the 2-rank of $J - A_{176}$, we obtain that $20 \leq r_2(J - A_{176}) \leq 22$.

We now prove that $r_5(A_{176} - 2I) = r_5(J - A_{176} + 2I) = 22$. Applying Theorem 5.14 to (6.8) yields $21 \leq r_7(A_{176} - 2I(-J)) \leq 22$. The rows of $A_{176} - 2I$ add up to $\underline{3}$ (modulo 5) and the same holds for the rows of $J - A_{176} + 2I$. Hence the assertion is true by Lemma 5.15.

The last graph discussed in this section has spectrum $42^1, 2^{99}, (-12)^{20}$, hence the interesting cases are $r_2(A_{120})$ and $r_7(A_{120} - 2I)$. $PSL(3,4)$ is a group of automorphisms for Γ_{120}. The permutation representation of its action on the vertices of the graph affords the character $\phi = \chi_1 + \chi_{20} + \chi_{35} + \chi_{64}$. For $\phi(E_1) = \chi_{35} + \chi_{64}$ and $\phi(E_2) = \chi_{20}$ we have

$$\hat{\phi}^2(E_1) = \chi_1^2 + \chi_{8a}^2 + \chi_{8b}^2 + \chi_{9a}^2 + \chi_{9b}^2 + \chi_{64}^2, \quad \hat{\phi}^2(E_2) = 2\chi_1^2 + \chi_{9a}^2 + \chi_{9b}^2 \tag{6.9}$$

and

$$\hat{\phi}^7(E_1) = \chi_{19}^7 + \chi_{35}^7 + \chi_{45}^7, \quad \hat{\phi}^7(E_2) = \chi_1^7 + \chi_{19}^7.$$

For the 7-rank of $A_{120} - 2I$ and $J - A_{120} + 2I$, we immediately obtain from

$$\begin{aligned} 3J(A_{120} - 2I) &\equiv J \pmod 7, \\ -2J(J - A_{120} + 2I) &\equiv J \pmod 7, \end{aligned}$$

and the constituents of $\hat{\phi}^7(E_1)$ and $\hat{\phi}^7(E_2)$ that $r_7(A_{120} - 2I) = r_7(J - A_{120} + 2I) = 20$.

Theorem 5.14 yields that $r_2(A_{120}) \in \{10, 18, 20\}$. Number the points of $S(4,7,23)$ from 1 to 23. Take as vertex set of Γ_{120} the set $\mathcal{B}'$ which is defined as the collection of blocks containing neither 1 nor 2. Assume that $\{1,2,3,4,5,6,7\}$ is a block of $S(4,7,23)$. Then every 3-subset of $\{3,4,5,6,7\}$ is contained in exactly four blocks of $\mathcal{B}'$. The blocks containing 3 and one of the 2-subsets of $\{4,5,6\}$ form a coclique of size 12; the same holds for the blocks containing 3, 7 and one of $\{4,5,6\}$. Let A' be the 24×24 submatrix of A_{120} corresponding to the 24 blocks described above. By a suitable labelling of the rows and columns, we get

$$A' = \left(\begin{array}{c|c} O & N \\ \hline N^T & O \end{array}\right). \tag{6.10}$$

The matrix N has the following form:

$$\begin{array}{c} \\ \{345\} \\ \{346\} \\ \{356\} \end{array} \begin{array}{c} \begin{array}{ccc} \{347\} & \{357\} & \{367\} \end{array} \\ \begin{pmatrix} & & N_1 \\ & N_2 & \\ N_3 & & \end{pmatrix} \end{array} \tag{6.11}$$

Every N_i, $1 \leq i \leq 3$, is a 4×4 matrix with two ones in each row and column. Thus $r_2(N_i) \geq 2$. Hence from (6.10) and (6.11) it follows that $r_2(A_{120}) \geq r_2(A') \geq 12$. This leads to the conclusion that $r_2(A_{120}) = 20$ if $\underline{1} \in \mathcal{R}_2(A_{120})$ and 18 otherwise. For the 2-rank of $J - A_{120}$ we find $18 \leq r_2(J - A_{120}) \leq 20$.

6.5 The Cameron graph

The Cameron graph Γ_C has parameters $(v, k, \lambda, \mu) = (231, 30, 9, 3)$ and is constructed from $S(3, 6, 22)$ in the following way: take as vertices the unordered pairs from the point set of the Steiner system and let two pairs be adjacent when they are disjoint and their union is contained in a block. Since its spectrum is $30^1, 9^{55}, (-3)^{175}$, we shall examine $r_3(A_C)$ and $r_2(A_C + I)$.

Clearly, M_{22} is a group of automorphisms of Γ_C. For the character ϕ afforded by the permutation representation of M_{22} acting on Γ_C, we find

$$\phi = \chi_1 + \chi_{21} + \chi_{55} + \chi_{154}.$$

Thus $\phi(E_1) = \chi_{55}$ and $\phi(E_2) = \chi_{21} + \chi_{154}$.

Let us first deal with $r_3(A_C)$. Then

$$\hat{\phi}^3(E_1) = \chi_{55}^3 \quad \text{and} \quad \hat{\phi}^3(E_2) = \chi_1^3 + \chi_{21}^3 + \chi_{49a}^3 + \chi_{49b}^3 + \chi_{55}^3.$$

Thus $55 \leq r_3(J - A_C) \leq r(21I + 7A_C - J) = r(E_1) = 55$. Furthermore, $r_3(A_C) = 55$ or 56, depending on whether $\underline{1}$ is contained in $\mathcal{R}_3(A_C)$ or not.

The 2-rank of $A_C + I$ is not as easily determined as the 3-rank of A_C, since

$$\hat{\phi}^2(E_1) = \chi_1^2 + \chi_{10a}^2 + \chi_{10b}^2 + \chi_{34}^2 \quad \text{and} \quad \hat{\phi}^2(E_2) = 3\chi_1^2 + 2\chi_{10a}^2 + 2\chi_{10b}^2 + \chi_{34}^2 + \chi_{98}^2.$$

Taking into account that $r_2(J - A_C - I) \leq r(21I + 7A_C - J) = r(E_1) = 55$ and $r_2(J - A_C - I)$ is even (Lemma 3.9), we obtain that $r_2(J - A_C - I) \in \{10, 20, 34, 44, 54\}$. By Lemma 3.8, $r_2(A_C + I) = r_2(J - A_C - I) + 1$.

The set of possible values for $r_3(A_C + I)$ can be reduced by examining the structure of the graph in more detail. Number the points of $S(3, 6, 22)$ from 1 to 22. The vertices $\{1, i\}$, $2 \leq i \leq 22$, form a coclique, hence $r_2(A_C + I) \geq 21$. Without loss of generality assume that $\{1, 2, 3, 4, 5, 6\}$ is a block of $S(3, 6, 22)$. We claim that

$$\underline{r}_{\{2,3\}} \notin \underline{r}_{\{1,4\}} + \underline{r}_{\{1,5\}} + \underline{r}_{\{1,6\}} \pmod 2.$$

From this it follows that $\mathcal{R}_2(A_C + I)$ is not generated by the rows $\underline{r}_{\{1,i\}}$, $2 \leq i \leq 22$. A counting argument shows that there are 20 pairs $\{x, y\}$ with $x, y \in \{7, \ldots, 22\}$ such that $\{1, 4, x, y\}$ is contained in a block and $\{2, 3, x, y\}$ not. Assume that $\{7, 8\}$ is such a pair. From the fact that two blocks of $S(3, 6, 22)$ intersect in 0 or 2 points, it follows that neither $\{1, 5, 7, 8\}$ nor $\{1, 6, 7, 8\}$ is contained in a block. Now $\underline{r}_{\{2,3\}}$ has a zero at the coordinate corresponding to $\{7, 8\}$, whereas the sum of the three rows mentioned above has a one at the same coordinate. Hence $r_2(A_C + I) > 21$. We conclude that $r_2(A_C + I) \in \{35, 45, 55\}$.

6.6 The Hoffmann-Singleton graph and related graphs

In Brouwer and Van Lint [4] it is shown that the vertex set of the Higman-Sims graph can be split into two halves such that the each of the induced subgraphs is a srg with parameters $(v, k, \lambda, \mu) =$

$(50,7,0,1)$. This graph is called the Hoffmann-Singleton graph and is denoted by Γ_{Ho}. The group $PSU_3(5^2)$ acts as rank 3 group on the vertex set of Γ_{Ho}. The action yields the permutation character $\chi_1 + \chi_{21} + \chi_{28}$.

Γ_{Ho} has spectrum $7^1, 2^{28}, (-3)^{21}$. Thus only $r_5(A_{Ho} - 2I)$ is of interest. The irreducible 5-modular constituents of $\hat{\chi}^5_{21}$ and $\hat{\chi}^5_{28}$ are

$$\hat{\chi}^5_{21} = 2\chi^5_1 + \chi^5_{19}, \quad \hat{\chi}^5_{28} = \chi^5_1 + \chi^5_8 + \chi^5_{19}.$$

Thus $19 \leq r_5(A_{Ho} - 2I) \leq 21$. The lower bound can be improved since

$$\begin{aligned} (A_{Ho} - 2I)^2 &\equiv J \pmod 5, \\ (2I - A_{Ho})(J - A_{Ho} + 2I) &\equiv J \pmod 5. \end{aligned}$$

So $\mathcal{R}_5(A_{Ho} - 2I)$ and $\mathcal{R}_5(J - A_{Ho} + 2I)$ both contain the all-one vector. Thus, by Lemma 5.15, $20 \leq r_5(A_{Ho} - 2I) = r_5(J - A_{Ho} + 2I) \leq 21$.

The action of $PSU_3(5^2)$ on the edges of Γ_{Ho} gives rise to a srg Γ_{175} with parameters $(v,k,\lambda,\mu) = (175,72,20,36)$. This graph is also produced by isolating a vertex of the graph Γ_{176} discussed in Section 4, and deleting it. Its spectrum is $72^1, 2^{153}, (-18)^{21}$. Therefore, we shall consider $r_2(A_{175})$ and $r_5(A_{175} - 2I)$.

The 2-rank of A_{175} is easily determined. We derived before that $r_2(A_{176}) = 20 + \epsilon$, where $\epsilon = 2$ if $\underline{1} \in \mathcal{R}_2(A_{176})$ and 0 otherwise. Now it immediately follows from Lemma 3.11 that $r_2(A_{175}) = 20$. Furthermore, $r_2(J - A_{175}) = 21$ by Lemma 3.8.

The group $PSU_3(5^2)$ is an automorphism group of Γ_{175}. The associated permutation character ϕ equals $\phi = \chi_1 + \chi_{21} + \chi_{28} + \chi_{125}$. Hence $\phi(E_1) = \chi_{28} + \chi_{125}$, $\phi(E_2) = \chi_{21}$ and

$$\hat{\phi}^5(E_1) = \chi^5_1 + \chi^5_8 + \chi^5_{19} + \chi^5_{125}, \quad \hat{\phi}^5(E_2) = 2\chi^5_1 + \chi^5_{19}.$$

Thus by Theorem 5.14, $19 \leq r_5(A_{175} - 2I(-J)) \leq 21$. Since

$$\begin{aligned} (A_{175} - 2I)^2 &\equiv J \pmod 5, \\ (2I - A_{175})(J - A_{175} + 2I) &\equiv J \pmod 5, \end{aligned}$$

it follows from Lemma 5.15 that $20 \leq r_5(A_{175} - 2I) = r_5(J - A_{175} + 2I) \leq 21$.

Γ_{176} can also be switched into a srg with parameters $(v,k,\lambda,\mu) = (176,90,38,54)$ and spectrum $90^1, 2^{153}, (-18)^{22}$. We denote this graph by Γ^*_{176}.

Applying Lemma 3.11, we find that $r_2(A^*_{176}) = 22$ if $\underline{1} \in \mathcal{R}_2(A^*_{176})$ and 20 otherwise. Then we also know that $20 \leq r_2(J - A^*_{176}) \leq 22$.

Since $k = 90$, the sum of the rows of $A^*_{176} - 2I$ equals $\underline{3}$ (modulo 5) and the same holds for the sum of the rows of $J - A^*_{176} + 2I$. By Theorem 3.5 and Lemma 3.10,

$$20 = r_5(A_{176} - 2I) - 2 \leq r_5(A^*_{176} - 2I) = r_5(J - A^*_{276} + 2I) \leq 23.$$

6.7 Graphs derived from the Golay codes

The Golay codes (A4) give rise to several srgs (see [4]). In this section we shall study three of them.

The Berlekamp-Van Lint-Seidel graph Γ_{BLS} has parameters $(v,k,\lambda,\mu) = (243,22,1,2)$ and is constructed in the following way. Take as vertices the $3^5 = 243$ cosets of the [11,6] ternary Golay

code and join two vertices when the corresponding cosets have representatives differing by a vector of weight one. Its spectrum is $22^1, 4^{132}, (-5)^{110}$, hence the only interesting case is $r_3(A_{BLS} - I)$. The Mathieu group M_{11} is a group of automorphisms of Γ_{BLS}. The permutation representation of its action on the graph affords the character $6\chi_1 + 6\chi_{10} + 3\chi_{44} + \chi_{45}$. Furthermore,

$$\begin{aligned} \phi(E_1) &= 3\chi_1 + 4\chi_{10} + \chi_{44} + \chi_{45}, \\ \phi(E_2) &= 2\chi_1 + 2\chi_{10} + 2\chi_{44}. \end{aligned}$$

The 3-modular characters $\hat{\phi}^3(E_1)$ and $\hat{\phi}^3(E_2)$ satisfy

$$\hat{\phi}^3(E_1) = 3\chi_1^3 + \chi_{5a}^3 + \chi_{5b}^3 + 5\chi_{10}^3 + \chi_{24}^3 + \chi_{45}^3, \quad \hat{\phi}^3(E_2) = 2\chi_1^3 + 2\chi_{5a}^3 + 2\chi_{5b}^3 + 4\chi_{10}^3 + 2\chi_{24}^3.$$

Now Theorem 5.14 yields the following set of possible values for $r_3(A_{BLS} - I)$:

$$\{\alpha_1 + 5(\alpha_2 + \alpha_3) + 10\alpha_4 + 24\alpha_5 \mid 0 \le \alpha_1 \le 3, 0 \le \alpha_2, \alpha_3, \alpha_5 \le 1, 0 \le \alpha_4 \le 4\}.$$

We shall reduce this set to

$$\{43 + 5(\alpha_2 + \alpha_3) + 24\alpha_5 \mid 0 \le \alpha_2, \alpha_3, \alpha_5 \le 1\}. \tag{6.12}$$

We first show that $\alpha_1 = 3$. Take as representatives of the cosets the vectors of weight ≤ 2. Let $1^a(-1)^b0^c$ denote a vector having a one at a, a minus one at b and a zero at c coordinates. Then by a suitable labelling of the rows and columns, $A_{BLS} - I$ can be written as

$$\left(\begin{array}{c|c|c|c|c|c} -1 & \underline{1} & \underline{1} & & & \\ \hline \underline{1}^T & -I_{11} & I_{11} & N_1 & & N_2 \\ \hline \underline{1}^T & I_{11} & -I_{11} & & N_1 & N_3 \\ \hline & N_1^T & & A' + I_{55} & N_4 & N_5 \\ \hline & & N_1^T & N_4^T & A' + I_{55} & N_6 \\ \hline & N_2^T & N_3^T & N_4^T & N_5^T & A'' + I_{110} \end{array}\right) \begin{array}{l} 0^{11} \\ 1^10^{10} \\ (-1)^10^{10} \\ 1^20^9 \\ (-1)^20^9 \\ 1^1(-1)^10^9 \end{array}$$

It is easily seen that N_1 has 2 ones in every column and that N_2 and N_3 have both 1 one per column. Thus $r_3(A_{BLS} - I)$ contains the following linearly independent vectors:

$$\begin{aligned} \underline{v}_1 &:= (-1; \underline{1}_{11}; \underline{1}_{11}; \underline{0}_{55}; \underline{0}_{55}; \underline{0}_{110}), \\ \underline{v}_2 &:= (-1; -\underline{1}_{11}; \underline{1}_{11}; -\underline{1}_{55}; \underline{0}_{55}; \underline{1}_{110}), \\ \underline{v}_3 &:= (-1; \underline{1}_{11}; -\underline{1}_{11}; \underline{0}_{55}; -\underline{1}_{55}; \underline{1}_{110}). \end{aligned}$$

These three vectors are all invariant under the action of M_{11} on the coordinates. This proves our claim. Since

$$-\underline{v}_1 + \underline{v}_2 + \underline{v}_3 \equiv \underline{1} \pmod 3$$

and $\underline{1} - \underline{v}_1$, $\underline{1} + \underline{v}_2$ and $\underline{1} + \underline{v}_3$ are contained in $\mathcal{R}_3(J - A_{BLS} + I)$, this also shows that $r_3(A_{BLS} - I) = r_3(J - A_{BLS} + I)$.

In order to prove that $\alpha_4 = 4$, we observe that every element of M_{11} maps a vector $1^a(-1)^b0^c$ to a vector $1^a(-1)^b0^c$. Consider the following four subspaces over $\mathbb{F}_3$:

$$\begin{aligned} R_{1a} &:= \langle \underline{r}_{1^10^{10}} \rangle, \\ R_{1b} &:= \langle \underline{r}_{(-1)^10^{10}} \rangle, \\ R_{2a} &:= \langle \underline{r}_i \mid 1 \le i \le 11 \rangle, \\ R_{2b} &:= \langle \underline{r}'_i \mid 1 \le i \le 11 \rangle, \end{aligned}$$

where $\underline{r}_i$ ($\underline{r}'_i$) denotes the sum of the rows corresponding to a vector $1^2 0^9$ ($(-1)^2 0^9$) and a 1 (-1) at the ith coordinate. These four subspaces are submodules of dimension 11 of the module corresponding to the permutation representation Φ of M_{11} on the vertex set of Γ_{BLS}. Let ϕ^3 be the (3-modular) character afforded by Φ, then

$$\phi^3(R_{1a}) = \phi^3(R_{1b}) = \phi^3(R_{2a}) = \phi^3(R_{2b}) = \chi_1^3 + \chi_{10}^3$$

($\underline{v}_1 + \underline{v}_3 \in R_{2a}$; $\underline{v}_1 + \underline{v}_2 \in R_{2b}$). Set $R := R_{1a} + R_{1b} + R_{2a} + R_{2b}$. It is easily verified that

$$\phi^3(R) = 2\chi_1^3 + 4\chi_{10}^3.$$

Hence indeed, $\alpha_4 = 4$.

We have proven that the set (6.12) contains the value of $r_3(A_{BLS} - I)$. It has been computed by Brouwer that the actual 3-rank of $A_{BLS} - I$ equals 67.

The Delsarte graph Γ_D with parameters $(v, k, \lambda, \mu) = (243, 110, 37, 60)$ has been introduced in Section 3 as a subgraph of a graph on 276 vertices related to the McLaughlin graph by switching. However, Γ_D can also be directly constructed in the following way. Take as vertices the codewords of the unique ternary Golay code of length 11 and dimension 5. Join two vertices when they have Hamming distance 6.

We derived before that $19 \leq r_3(A_D - I(-J)) \leq 23$. The lower bound can be slightly improved by using characters. The Mathieu group M_{11} is an automorphism group of Γ_D. Denote by ϕ the permutation character yielded by the action of M_{11} on the vertex set of Γ_D. Because $g = 22$, the irreducible constituents of $\phi(E_2)$ must have degree ≤ 22. The irreducible characters of M_{11} of degree ≤ 22 are χ_1, χ_{10a}, χ_{10b}, χ_{10c} and χ_{11}. They satisfy

$$\begin{aligned} \hat{\chi}_1^3 &= \chi_1^3, \\ \hat{\chi}_{10i}^3 &= \chi_{10i}^3 \quad \text{for } i \in \{a, b, c\}, \\ \hat{\chi}_{11}^3 &= \chi_1^3 + \chi_{5a}^3 + \chi_{5b}^3. \end{aligned}$$

Applying Theorem 5.14 to the above-mentioned relations and recalling that $r_3(A_D + I(-J)) \geq 19$, it follows that $r_3(A_D + I(-J)) \geq 20$.

We finally consider a rank 3 graph derived from M_{24}. This graph, which is denoted by Γ_{1288}, has parameters $(v, k, \lambda, \mu) = (1288, 792, 476, 504)$. Its spectrum is $792^1, 8^{1035}, (-36)^{252}$. Hence the interesting cases are $r_2(A_{1288})$ and $r_{11}(A_{1288} + 3I)$.

Let us first give an explicit description of Γ_{1288}. Take as vertices the cosets of $\{\underline{0}, \underline{1}\}$ in the extended binary Golay code which contain two dodecads. Join two cosets when they have Hamming distance 12.

The 11-rank of $A_{1288} + 3I$ is easily obtained from Theorem 5.14. Let ϕ denote the permutation character corresponding to the action of M_{24} on the vertex set of the graph. Then $\phi(E_1) = \chi_{1035}$ and $\phi(E_2) = \chi_{252}$. The irreducible constituents of $\hat{\phi}^{11}(E_1)$ and $\hat{\phi}^{11}(E_2)$ are given by

$$\hat{\phi}^{11}(E_1) = \chi_{229}^{11} + \chi_{806}^{11}, \quad \hat{\phi}^{11}(E_2) = \chi_{23}^{11} + \chi_{229}^{11}.$$

Thus, by Theorem 5.14, $229 \leq r_{11}(A_{1288} + 3I(-J)) \leq 230$. Since the sum of the rows of $A_{1288} + 3I$ ($J - A_{1288} - 3I$) equals $\underline{3}$ ($-\underline{2}$) (modulo 11), the all-one vector is contained both in $\mathcal{R}_{11}(A_{1288} + 3I)$ and in $\mathcal{R}_{11}(J - A_{1288} - 3I)$. So $r_{11}(A_{1288} + 3I) = r_{11}(J - A_{1288} - 3I) = 230$ by Lemma 5.15.

For the constituents of $\hat{\chi}^2_{252}$ and $\hat{\chi}^2_{1035}$ we find

$$\begin{aligned}\hat{\chi}^2_{252} &= 2\chi^2_{11a} + 2\chi^2_{11b} + \chi^2_{44a} + \chi^2_{44b} + \chi^2_{120},\\ \hat{\chi}^2_{1035} &= \hat{\chi}^2_{252} + 3\chi^2_1 + \chi^2_{44a} + \chi^2_{44b} + \chi^2_{220a} + \chi^2_{220b}.\end{aligned}$$

When not examining the structure of the graph in more detail, we can only conclude that $\hat{\phi}^2(A_{1288})$ is a constituent of $\hat{\phi}^2(E_1)$, which implies that the 2-rank of A_{1288} is an element of the set

$$\{\, 11(\alpha_1+\alpha_2) + 44(\alpha_3+\alpha_4) + 120\alpha_5 \mid 0 \le \alpha_{1,2} \le 2,\ 0 \le \alpha_{3,4,5} \le 1 \,\}.$$

6.8 Rank 3 graphs related to $S_{2m}(q)$

Infinite classes of strongly regular rank 3 graphs are derived from *classical groups*. For a survey we refer to [4] or [10]. Here we shall consider the p-rank of elements of one such class.

Let q be a prime power of p. Denote by $V_{2m,q}$ the $2m$-dimensional vectorspace over $\mathbb{F}_q$. Define the symplectic form $f_{2m,q} : V_{2m,q} \times V_{2m,q} \longmapsto \mathbb{F}_q$ (A5) by

$$f_{2m,q}((u_1,\ldots,u_{2m}),(v_1,\ldots,v_{2m})) := u_1v_2 - u_2v_1 + \ldots + u_{2m-1}v_{2m} - u_{2m}v_{2m-1}.$$

Denote by $P_{2m,q}$ the collection of points of the projective geometry $PG(2m-1,q)$. Take $P_{2m,q}$ as vertex set of a graph $\Gamma_{2m,q}$ and join two different vertices $\langle \underline{u} \rangle$ and $\langle \underline{v} \rangle$ by an edge iff $f_{2m,q}(\underline{u},\underline{v}) = 0$. Then $\Gamma_{2m,q}$ is a srg with parameters

$$v = \frac{q^{2m}-1}{q-1},\ k = \frac{q^{2m-1}-q}{q-1},\ \lambda + 2 = \mu = \frac{q^{2m-2}-1}{q-1},\ r = q^{m-1}-1,\ s = -q^{m-1}-1.$$

From the eigenvalues it follows that if q is even, then the only interesting case is $r_2(A+I)$. If q is odd, then $r_2(A)$ and $r_p(A+I)$ are the nontrivial cases (recall that p is such that $q = p^e$). $\Gamma_{2m,q}$ is a rank 3 graph derived from $S_{2m}(q)$.

If $q = 2$, then $r_2(A_{2m,2})$ is easily determined by induction. Let $\langle \underline{u} \rangle$, $\langle \underline{v} \rangle$ be two different elements of $P_{2m-2,2}$. Then

$$f_{2m,2}((\underline{u};u_{2m-1}u_{2m}),(\underline{v};v_{2m-1}v_{2m})) = f_{2m-2,2}(\underline{u},\underline{v}) + u_{2m-1}v_{2m} - u_{2m}v_{2m-1}.$$

Put $A' := A_{2m-2,2} + I_{2m-2}$. Then it follows from the above-mentioned relation that, by a suitable labelling of the rows and columns, $A_{2m,2} + I_{2m}$ can be expressed as

$$A_{2m,2} + I_{2m} = \left(\begin{array}{c|c|c|c|c|c|c}
A' & \underline{1}^T & A' & \underline{1}^T & A' & \underline{1}^T & A' \\ \hline
\underline{1} & 1 & \underline{1} & & & & \\ \hline
A' & \underline{1}^T & A' & & J-A' & & J-A' \\ \hline
\underline{1} & & & 1 & \underline{1} & & \\ \hline
A' & & J-A' & \underline{1}^T & A' & & J-A' \\ \hline
\underline{1} & & & & & 1 & \underline{1} \\ \hline
A' & & J-A' & & J-A' & \underline{1}^T & A'
\end{array}\right)\begin{array}{l}\langle(\underline{u};00)\rangle\\ \langle(\underline{0};10)\rangle\\ \langle(\underline{u};10)\rangle\\ \langle(\underline{0};01)\rangle\\ \langle(\underline{u};01)\rangle\\ \langle(\underline{0};11)\rangle\\ \langle(\underline{u};11)\rangle\end{array}$$

where $\langle \underline{u} \rangle$ denotes an element of $P_{2m-2,2}$. Performing suitable elementary row and column operations over $\mathbb{F}_2$ on $A_{2m,2} + I_{2m}$ we get

$$A_{2m,2} + I_{2m} \simeq \left(\begin{array}{c|c|c|c|c|c|c} A' & \underline{1}^T & A' & \underline{1}^T & A' & \underline{1}^T & A' \\ \hline \underline{1} & 1 & \underline{1} & & & & \\ \hline & & & \underline{1}^T & J & \underline{1}^T & J \\ \hline \underline{1} & & & 1 & \underline{1} & & \\ \hline & \underline{1}^T & J & & & \underline{1}^T & J \\ \hline \underline{1} & & & & & 1 & \underline{1} \\ \hline & & & \underline{1}^T & J & \underline{1}^T & J \end{array}\right)$$

$$\simeq \left(\begin{array}{cccc|c} A' & A' & A' & A' & \\ \hline 1 & 1 & & & \\ \hline & & 1 & 1 & \\ \hline 1 & & 1 & & \\ \hline & 1 & & 1 & \\ \hline 1 & & & 1 & \\ \hline & & & & O \end{array}\right)$$

$$\simeq \operatorname{diag}(A', 1^2, 0^{3\cdot 2^{2m-2}-2})$$

(note that the rows of A' add up to $\underline{1}$ (modulo 2)). Thus

$$r_2(A_{2m,2} + I_{2m}) = r_2(A_{2m-2,2} + I_{2m-2}) + 2 = \ldots = r_2(A_{4,2} + I_4) + 2m - 4. \tag{6.13}$$

The graph $A_{4,2}$ has the same parameters as the complement of the triangular graph $T(6)$. From the uniqueness of the latter, it follows that $r_2(A_{4,2} + I) = r_2(A_{T(8)}) + 1 = 5$ (Proposition 2.5). Substituting this in (6.13) yields

$$r_2(A_{2m,2} + I) = 2m + 1.$$

Finally, since $v = 2^{2m} - 1$ and $k = 2^{2m-1} - 2$ for $\Gamma_{2m,2}$, we find $r_2(J - A_{2m,2} - I) = 2m$ by Lemma 3.8.

For $q > 2$, the adjacency matrix $A_{2m,q}$ is not as easily described as for $q = 2$. In that case we have to look at the character obtained from the action of $S_{2m}(q)$ on the vertices of $\Gamma_{2m,q}$. Let us examine $\Gamma_{4,3}$ and $\Gamma_{4,5}$.

The action of $S_4(3)$ on the vertex set of $\Gamma_{4,3}$ yields the character $\chi_1 + \chi_{15} + \chi_{24}$. From the *Modular Atlas* we obtain

$$\hat{\chi}^2_{15} = \chi^2_1 + \chi^2_{14}, \quad \hat{\chi}^2_{24} = 2\chi^2_1 + \chi^2_{4a} + \chi^2_{4b} + \chi^2_{14}$$

and

$$\hat{\chi}^3_{15} = \chi^3_5 + \chi^3_{10}, \quad \hat{\chi}^3_{24} = \chi^3_{10} + \chi^3_{14}.$$

For $\Gamma_{4,3}$ we have $v = 40$ and $k = 12$, so it immediately follows from Lemma 3.8 and Theorem 5.14 that $r_3(A_{4,3} + I) = r_3(J - A_{4,3} - I) + 1 = 11$.

Concerning the 2-rank, we derive that $r_2(A_{4,3}) = 14$ or 16 depending on whether $\underline{1} \in \mathcal{R}_2(A_{4,3})$, and $14 \leq r_2(J - A_{4,3}) = r_2(8I - 4A_{4,3} + J) \leq r(E_2) = 15$.

The character afforded by the permutation representation of $S_4(5)$ acting on $\Gamma_{4,5}$ equals $\chi_1 + \chi_{65} + \chi_{90}$. We only examine the 2-rank of $A_{4,5}$, since the *Modular Atlas* does not give a table of the 5-modular irreducible characters of $S_4(5)$. For $\hat{\chi}^2_{65}$ and $\hat{\chi}^2_{90}$ we find

$$\hat{\chi}^2_{65} = \chi^2_1 + \chi^2_{64}, \quad \hat{\chi}^2_{90} = \chi^2_1 + \chi^2_{12a} + \chi^2_{12b} + \chi^2_{64}.$$

So $r_2(A_{4,3}) = 64$ or 66 depending on whether $\underline{1} \in \mathcal{R}_2(A_{4,3})$ or not, and $64 \leq r_2(J - A_{4,3}) = r_2(24I - 6A_{4,3} + J) \leq r(E_2) = 65$.

6.9 Table of the results

To conclude this chapter, we list the results on the p-rank of *srgs* that have been derived in this chapter or in the examples of Chapters 3 and 5. For results on the lattice and triangular graphs we refer to Chapter 2.

If a set of possible values for $r_p(A + \sigma I)$ is given, then 'idem' means that the same set holds for $r_p(J - A - \sigma I)$. The entry '(=)' denotes that $r_p(J - A - \sigma I) = r_p(A + \sigma I)$ and '(-1)' denotes that $r_p(J - A - \sigma I) = r_p(A + \sigma I) - 1$. Furthermore, the entry '$*$' in the last column indicates that this result is not derived in this thesis (but is given for sake of completeness). Finally, the graphs No. 25 have parameters $a_1 = 2^{2m} - 1$, $a_2 = 2^{2m-1} - 1$ and $a_3 + 2 = a_4 = 2^{2m-2} - 1$.

No.	v	k	λ	μ	p	σ	$r_p(A+\sigma I)$	$r_p(J-A-\sigma I)$	
1	16	5	0	2	2	1	6	6	Ex. 3.1
2	27	16	10	8	2	0	6	7	Ex. 3.3
					3	−1	7	7	*
3	36	14	4	6	2	0	14	14	Ex. 5.6
					3	1	$7 \le r \le 9$	idem	
4	40	12	2	4	2	0	14, 16	$14 \le r \le 16$	6.8
					3	1	11	10	
5	50	7	0	1	5	−2	20, 21	(=)	6.6
6	56	10	0	2	2	0	20	20	Ex. 3.2
					3	1	20	19	6.1
7	77	16	0	4	2	0	20	21	6.1
8	100	22	0	6	2	0	22	22	6.1
					5	−2	23	23	
9	100	36	14	12	2	0	36	35, 36	Ex. 5.6
					5	−1	22, 23	idem	
10	112	30	2	10	2	0	22	22	6.2
					3	1	20	19	
11	120	42	8	18	2	0	18, 20	$18 \le r \le 20$	6.4
					7	−2	20	20	
12	156	30	4	6	2	0	64, 66	64, 65	
13	162	56	10	24	2	0	20	21	6.2
					3	1	21	21	
14	175	72	20	36	2	0	20	21	6.6
					5	−2	20, 21	(=)	
15	176	70	18	34	2	0	20, 22	$20 \le r \le 22$	6.4
					5	−2	22	22	
16	176	90	38	54	2	0	20, 22	$20 \le r \le 22$	6.6
					5	−2	$20 \le r \le 23$	(=)	
17	231	30	9	3	2	1	35, 45, 55	(−1)	6.5
					3	0	55	55, 56	
18	243	22	1	2	3	−1	67	67	6.7
19	243	110	37	60	3	−1	$20 \le r \le 23$	idem	6.4, 6.7
20	253	112	36	60	2	0	22	23	6.4
					7	−2	23	23	
21	275	112	30	56	2	0	22	23	6.2
					3	1	22	21	
					5	−2	23	23	
22	276	140	58	84	2	0	24	24	6.3
					3	1	$22 \le r \le 24$	$21 \le r \le 23$	
					5	−2	23, 24	idem	
23	416	100	36	20	2	0	38, 50, 52, 64, 66	37, 38, 50, 51 52, 64, 65, 66	Ex. 5.6
24	1288	792	476	504	11	3	230	230	6.8
25	a_1	a_2	a_3	a_4	2	1	$2m+1$	$2m$	6.8

Appendix

A1 t-Designs

Let X be a set of v elements, called *points*, and $\mathcal{B}$ a collection of k-subsets of X, called *blocks*, such that every t-subset of X is contained in exactly λ blocks. The pair $(X, \mathcal{B})$ is called a *t-design* or, more precisely, a t-(v, k, λ) design.

If $\lambda = 1$, the design is called a *Steiner system*. Notation: $S(t, k, v)$. We shall only deal with the following Steiner systems:

	b_0	b_1	b_2	b_3	b_4	b_5	s
$S(5,8,24)$	759	253	77	21	5	1	4,2,0
$S(4,7,23)$	253	77	21	5	1		3,1
$S(3,6,22)$	77	21	5	1			2,0

The column b_i gives the number of blocks in which an arbitrary i-tuple is contained. Hence b_0 denotes the number of blocks. The last column gives the possible values for the intersection of two different blocks.

$S(4,7,23)$ is obtained from $S(5,8,24)$ by taking all blocks containing a fixed point and deleting this point. In the same way, $S(3,6,22)$ is derived from $S(4,7,23)$. The remaining blocks form a 3-(22,7,4) design. From this design we obtain a 2-(21,6,4) design and a 2-(21,7,12) design. The former can also be derived from $S(3,6,22)$ by deleting all blocks containing a fixed point.

v	k	t	b_0	b_1	b_2	b_3	s
22	7	3	176	56	16	4	3,1
21	7	2	120	40	12		3,1
21	6	2	56	16	4		2,0

An *automorphism* of a design is a permutation of the points such that blocks are carried into blocks. The sporadic *Mathieu groups* M_{24} and M_{23} are the full automorphism groups of $S(5,8,24)$ and $S(4,7,23)$, respectively; the Mathieu group M_{22} is a group of index 2 in the full automorphism group of $S(3,6,22)$.

A2 Partial geometries

A *partial geometry* with parameters (K, R, T) consists of a set of elements, called *points*, and a collection of K-subsets, called *lines*, such that

(i) every point is on R lines;
(ii) for every pair of points there is at most one line containing them both (if there exists such a line for a pair $\{x, y\}$, then x and y are said to be *collinear*);
(iii) if a point p is not on a line L, then p is collinear with exactly T points of L.

A partial geometry with $T = 1$ is called a *generalized quadrangle* $GQ(s,t)$, where $s := K - 1$ and $t := R - 1$.

The *point graph* of a partial geometry is defined as follows. Take the points as vertices and join two vertices by an edge iff they are collinear. This graph is strongly regular with parameters

$$v = KT^{-1}((K-1)(R-1)+T),\ k = R(K-1),\ \lambda = K-2+(R-1)(T-1),\ \mu = RT.$$

A3 Projective geometries

The *projective geometry* of dimension m over $\boldsymbol{F}_q$ can be defined as the collection of linear subspaces of the vectorspace $V := \boldsymbol{F}_q^{m+1}$. It is denoted by $PG(m,q)$. The 1-dimensional subspaces of V are called *points* and the 2-dimensional subspaces of V are called *lines*.

A *projective plane* is defined as a collection of points and lines satisfying
(i) for every pair of two points there is a unique line containing them both;
(ii) any two lines meet in a unique point;
(iii) there exist four points no three of which are on a line.

It is a Steiner system $S(2, n+1, n^2+n+1)$ for some $n \geq 2$, when taking the lines as blocks. A projective geometry of dimension 2 is a projective plane; the converse does not necessarily hold.

A *collineation* of $PG(m,q)$ is a permutation of the points carrying lines into lines. The full collineation group is denoted by $P\Gamma L(m+1,q)$. Every element of $GL(m+1,q)$, the group of nonsingular $(m+1)\times(m+1)$ matrices with entries in $\boldsymbol{F}_q$, induces a collineation of $PG(m,q)$. The *projective general linear group* $PGL(m+1,q)$ consists of all collineations induced by the elements of $GL(m+1,q)$. The subgroup induced by the matrices of determinant 1 is denoted by $PSL(m+1,q)$.

A *subplane* of a projective plane is a subset of points and lines which is itself a projective plane. The subplanes of order 2 in $PG(2,4)$ are called *Fano subplanes*. There are 360 Fano subplanes which fall into 3 orbits under the action of $PSL(3,4)$. Fano planes in the same orbit intersect in an odd number of points; those in different classes have an even number of points in common.

A4 The Golay codes

Several strongly regular graphs are derived from the *extended binary Golay code* $\mathcal{G}_{24}$ and the *ternary Golay code* $\mathcal{G}_{11}$. For an extensive treatment of the Golay codes, we refer to Chapter 20 of MacWilliams and Sloane [15].

The extended binary Golay code $\mathcal{G}_{24}$ is a [24,12] code with minimum distance 8. The 759 codewords of weight 8 form an $S(5,8,24)$ and are called *octads*. The 1288 codewords of weight 12 are called *dodecads*. The code is self-dual. The automorphism group of a code is formed by the permutations of the coordinates which map every codeword to a codeword. The Mathieu group M_{24} is the full automorphism group of $\mathcal{G}_{24}$.

$\mathcal{G}_{11}$ is a [11,6,5] code over $\boldsymbol{F}_3$ which contains its dual. The Mathieu group M_{11} is a group of automorphisms for the code. The dual $\mathcal{G}_{11}^{\perp}$ is a [11,5] code consisting of the all-zero word, 110 words of weight 6 and 132 words of weight 9.

Let C be an $[n, k]$ linear code over $\boldsymbol{F}_q$. For any vector $\underline{x}$, the set

$$\underline{x} + C := \{\underline{x} + \underline{c} \mid \underline{c} \in C\}$$

is called a *coset* of C. Two vectors $\underline{x}$ and $\underline{y}$ are in the same coset iff $\underline{x} - \underline{y}$ is a codeword. Two cosets are either disjoint or coincide. The $3^5 = 243$ cosets of $\mathcal{G}_{11}$ are uniquely represented by the 220 vectors of weight 2, the 22 vectors of weight 1 and the all-zero vector. This holds, because the minimum distance of the code equals 5, hence every vector of weight ≤ 2 must be in a coset containing no other word of weight ≤ 2.

A5 Symplectic forms

Let V be a vectorspace of finite dimension n over a field F. A bilinear form f on V is said to be *symplectic* if $f(\underline{u}, \underline{u}) = 0$ for every $\underline{u} \in V$. A symplectic form satisfies

$$f(\underline{u}, \underline{v}) = -f(\underline{v}, \underline{u})$$

for all $\underline{u}, \underline{v} \in V$.

A symplectic form f is called *degenerate* if there exists an element $\underline{u} \neq \underline{0}$ such that $f(\underline{u}, \underline{v}) = \underline{0}$ for all $\underline{v} \in V$. If f_1 and f_2 are both symplectic forms defined on V, then they are called *equivalent* if there exists a linear transformation θ on V such that $f_1(\underline{u}, \underline{v}) = f_2(\theta(\underline{u}), \theta(\underline{v}))$ for all $\underline{u}, \underline{v} \in V$.

Theorem *Let f be a nondegenerate symplectic form defined on a vectorspace V. Then* $\dim(V)$ *is even and f is equivalent to f^*, where f^* is defined as*

$$f^*((u_1, \ldots, u_n), (v_1, \ldots, v_n)) := u_1 v_2 - u_2 v_1 + u_3 v_4 - u_4 v_3 + \ldots + u_{n-1} v_n - u_n v_{n-1}.$$

For a proof of this theorem we refer to Suzuki [20, p.373].

A linear transformation θ on V is said to leave the form f *invariant* if for every $\underline{u}, \underline{v} \in V$

$$f(\theta(\underline{u}), \theta(\underline{v})) = f(\underline{u}, \underline{v}).$$

The *symplectic group* $S_n(q)$ consists of all $n \times n$ matrices over $\boldsymbol{F}_q$ leaving the nondegenerate symplectic form f^* invariant.

We conclude this section with the proof of Lemma 3.9 in which it is stated that the 2-rank of the adjacency matrix of any graph is even.

A matrix M with entries in a field F of characteristic $\neq 2$ satisfying $M = -M^T$, corresponds to the symplectic form f defined by

$$f(\underline{u}, \underline{v}) := \underline{u} M \underline{v}^T.$$

It is easily verified that f is indeed a symplectic form. If $\mathrm{char}(F) = 2$, then a symmetric matrix $M \in F^{n \times n}$ with zeros on the diagonal represents a symplectic form in a similar way.

The form f is nondegenerate on the rowspace of M over F. Thus, by the above-mentioned theorem, $\mathcal{R}_F(M)$ is even. The adjacency matrix of a graph is symmetric and its diagonal elements all equal zero, hence its 2-rank is even.

Bibliography

[1] Bagchi, B., A.E. Brouwer and H.A. Wilbrink, Notes on binary codes related to the $O(5,q)$ generalized quadrangle for odd q, *Geometriae Dedicata* **39** (1991), 339 - 355.

[2] Bagchi, B. and N.S.N. Sastry, Codes associated with generalized polygons, *Geometriae Dedicata* **27** (1988), 1 - 8.

[3] Brouwer, A.E. and W.H. Haemers, The Gewirtz graph - an exercise in the theory of graph spectra, to appear in *Eur. J. Comb.*

[4] Brouwer, A.E. and J.H. van Lint, Strongly regular graphs and partial geometries, in: *Enumeration and Design*, D.M. Jackson and S.A. Vanstone (eds.), Academic Press, Toronto, 1984, 85 - 122.

[5] Cameron, P.J., Strongly regular graphs, in: *Selected topics in graph theory*, L.W. Beineke and R.J. Wilson (eds.), Academic Press, London, 1978, 337 - 360.

[6] Conway, J.H., R.T. Curtis, R.P. Parker and R.A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

[7] Cvetković, D.M., M. Doob and H. Sachs, *Spectra of Graphs: Theory and Application*, Academic Press, New York, 1980.

[8] Goethals, J.M. and J.J. Seidel, The regular two-graph on 276 vertices, *Discrete Math.* **12** (1975), 143 - 158.

[9] Hamada, N., On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes, *Hiroshima Math. J.* **3** (1973), 153 - 226.

[10] Hubaut, X.L., Strongly regular graphs, *Discrete Math.* **13** (1975), 357 - 381.

[11] Isaacs, I.M., *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[12] Lander, E.S., *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, Cambridge, 1983.

[13] Linial, N. and B. Rothschild, Incidence matrices of subsets - a rank formula, *SIAM J. Alg. Discr. Meth.* **2** (1981), 333 - 340.

[14] Lint, J.H. van, *Introduction to Coding Theory*, Springer-Verlag, New York, 1982.

[15] MacWilliams, F.J. and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[16] Marcus, M. and H. Minc, *A Survey of Matrix Theory and Matrix Inequalities*, Allyn and Bacon, Boston, 1964.

[17] Newman, M., *Integral Matrices*, Academic Press, London, 1972.

[18] Parker, R.P., *Modular Atlas*, Preprint, 1989.

[19] Seidel, J.J., Strongly regular graphs, in: *Surveys in Combinatorics*, B. Bollobas (ed.), Proc. 7th British Comb. Conf., London Math. Soc. Lecture Note Series, No. 38, Cambridge 1979, 157 - 180.

[20] Suzuki, M., *Group Theory I*, Springer Verlag, Berlin, 1982.

[21] Wilson, R.M., A diagonal form for the incidence matrices of t-subsets *vs.* k-subsets, *Eur. J. Combinatorics* **11** (1990), 609 - 615.