Eigenvalues and root systems in finite geometry

Peter J. Cameron
School of Mathematics and Statistics
University of St Andrews
North Haugh
St Andrews, Fife KY16 9SS
UK
pjc20@st-andrews.ac.uk

Contents

Preface

These are the notes of lectures I gave at a summer school on Finite Geometry at the University of Sussex, organised by Fatma Karaoglu, in June 2017.

The notes are partly based on a lecture course on Advanced Combinatorics I gave at the University of St Andrews in the second semester of 2015–2016.

The central plank of the course is the determination of graphs which have the “strong triangle property”: there are two infinite families of such graphs and three sporadic examples, and they form one of the many occurrences of a pattern which appears throughout mathematics, the “ADE affair”. In other guises, this is the classification of the root systems with all roots of the same length, or the classification of generalised quadranges with line size 3, or the classification of the quadratic forms with Witt index 2 over the field of two elements. I pursue all of these leads. The first is connected with spectral graph theory, the second with the theory of generalised polygons, and the third is a precursor of the Buekenhout–Shult classification of polar spaces by their point–line structure.

Along the way, there are various interesting diversions to be followed.

CHAPTER 1

Graphs

1.1 The Friendship Theorem

Theorem 1.1 *In a finite society with the property that any two individuals have a unique common friend, there must be somebody who is everybody else's friend.*

This theorem was proved by Erdős, Rényi and Sós in the 1960s. We assume that friendship is an irreflexive and symmetric relation on a set of individuals: that is, nobody is his or her own friend, and if A is B's friend then B is A's friend. (It may be doubtful if these assumptions are valid in the age of social media – but we are doing mathematics, not sociology.)

In other words, the configuration of friendships is a *graph*; the people are vertices, and two people are joined by an edge if they are friends. We discuss this notion in a moment.

The graph in the conclusion to the Friendship Theorem, with each individual represented by a dot, and friends joined by a line, is as shown in Figure 1.1.

1.2 Graphs

The mathematical model for a structure of the type described in the Friendship Theorem is a *graph*.

A *simple graph* (one "without loops or multiple edges") can be thought of in various ways, for example:

- a set of vertices, with a symmetric and irreflexive relation called *adjacency*;

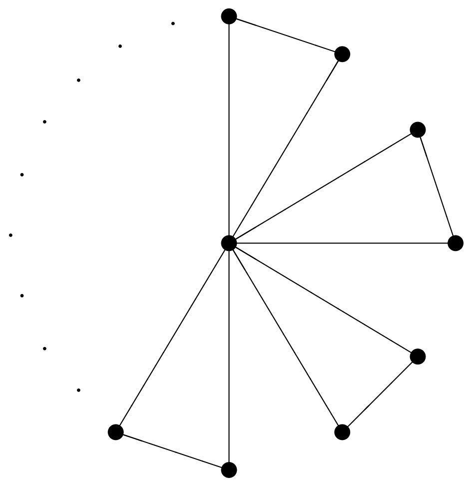


Figure 1.1: The Friendship graph

- a pair (V,E), where V is the set of vertices, and E a set of 2-element subsets called *edges*;
- an incidence structure (V,E), where each element of E is incident with two elements of V and there are no "repeated blocks".

In particular, a graph is a special sort of block design.

We write $v \sim w$ to denote that the vertices v and w are joined by an edge $\{v,w\}$. Sometimes we write the edge more briefly as vw.

More general graphs can involve weakenings of these conditions:

- We might allow *loops*, which are edges joining a vertex to itself.
- We might allow *multiple edges*, more than one edge connecting a given pair of vertices (so that the edges form a multiset rather than a set).
- We might allow the edges to be *directed*, that is, ordered rather than unordered pairs of vertices.
- Sometimes we might even allow "half-edges" which are attached to a vertex at one end, the other end being free.

But in these lectures, unless specified otherwise, graphs will be simple.

A few definitions:

- Two vertices are *neighbours* if there is an edge joining them. The *neighbourhood* of a vertex is the set of its neighbours. (Sometimes this is called the *open neighbourhood*, and the *closed neighbourhood* also includes the vertex.)

- The *valency* or *degree* of a vertex is the number of neighbours it has. A graph is *regular* if every vertex has the same valency.
- A *path* is a sequence $(v_0, v_1, \ldots, v_d)$ of vertices such that $v_{i-1} \sim v_i$ for $1 \leq i \leq d$. (We usually assume that all the vertices are distinct, except possibly the first and the last.)
- A graph is *connected* if there is a path between any two of its vertices. In a connected graph, the *distance* between two vertices is the length of the shortest path joining them, and the *diameter* of the graph is the maximum distance between two vertices. The vertex set of a connected graph, with the distance function, satifies the axioms for a metric space.
- A *cycle* is a path $(v_0, \ldots, v_d)$ with $d > 2$ in which $v_0, \ldots, v_{d-1}$ are distinct and $v_d = v_0$. (We exclude $d = 2$ which would represent a single edge.) A graph with no cycles is a *forest*; if it is also connected, it is a *tree*. In a graph which is not a forest, the *girth* is the number of vertices in a shortest cycle.
- The *complete graph* on a given vertex set is the graph in which all pairs of distinct vertices are joined; the *null graph* is the graph with no edges.
- The *complete bipartite graph* $K_{m,n}$ has vertex set partitioned into two subsets A and B, of sizes m and n; two vertices are joined if and only if one is in A and the other in B. So $K_{2,2}$ is the 4-cycle graph. More generally, a graph is *bipartite* if its vertex set can be partitioned into two subsets A and B such that every edge has one vertex in A and the other in B.
- The *complement* of a graph G is the graph $\overline{G}$ on the same vertex set, for which two vertices are joined in $\overline{G}$ if and only if they are not joined in G. (So the complement of a complete graph is a null graph.)
- Given a graph G, the *line graph* of G is the graph $L(G)$ whose vertices are the edges of G; two vertices of $L(G)$ are joined by an edge if and only if (as edges of G) they have a vertex in common. Figure 1.2 is an example.
- Given a graph with vertex set V, we consider square matrices whose rows and columns are indexed by the elements of V. (Such a matrix can be thought of as a function from $V \times V$ to the field of numbers being used. If $V = \{v_1, \ldots, v_n\}$, we assume that vertex v_i labels the ith row and column of the matrix. Now the *adjacency matrix* of the graph is the matrix A (with rows and columns indexed by V) with (v, w) entry 1 if $v \sim w$, and 0 otherwise. Note that the adjacency matrix of a graph is a real symmetric matrix, and so it is diagonalisable, and all its eigenvalues are real.

Further definitions will be introduced as required.

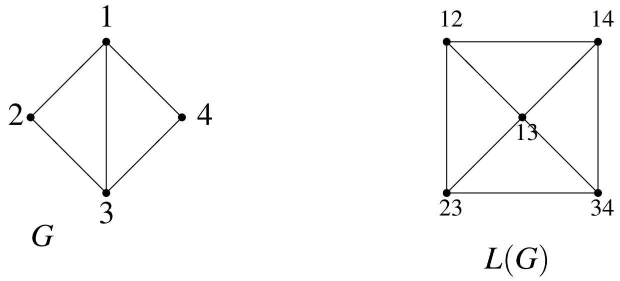


Figure 1.2: A graph and its line graph

For example, the triangle (a cycle with 3 vertices) has diameter 1 and girth 3; it is regular with valency 2. Its adjacency matrix is

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

1.3 Proof of the Friendship Theorem

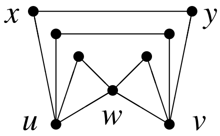
The proof of the Friendship Theorem 1.1 falls into two parts. First, we show that any counterexample to the theorem must be a regular graph; then, using methods from linear algebra, we show that the only regular graph satisfying the hypothesis is the triangle (which is not a counterexample).

Step 1: A counterexample is regular

Let G be a graph satisfying the hypothesis of the Friendship Theorem: that is, any two vertices have a unique common neighbour.

First we observe: *Any two non-adjacent vertices of G have the same valency.*

For let u and v be non-adjacent. They have one common neighbour, say w. Then u and w have a common neighbour, as do v and w. If x is any other neighbour of u, then x and v have a unique common neighbour y; then obviously y is a neighbour of v, and y and u have a unique common neighbour x. (The sequence (u,x,y,v) is a path.) So we have a bijection from the neighbourhood of u to the neighbourhood of y.



Now we have to show: *If G is not regular, then it satisfies the conclusion of the theorem.*

Suppose that a and b are vertices of G with different valencies. Then a and b are adjacent. Also, any further vertex x has different valency from either a or b, and so is joined to either a or b; but only one vertex, say c, is joined to both.

Suppose that the valency of c is different from that of a. Then any vertex which is not joined to a must be joined to both b and c. But there can be no such vertex, since a is the only common neighbour of b and c. So every vertex other than a is joined to a, and the assertion is proved. (The structure of the graph in this case must be a collection of triangles with one vertex identified, as in the diagram after the statement of the theorem.)

Step 2: A regular graph satisfying the hypotheses must be a triangle

Let G be a regular graph satisfying the statement of the theorem; let its valency be k.

Let A be the adjacency matrix of G, and let J denote the matrix (with rows and columns indexed by vertices of G) with every entry 1. We have $AJ = kJ$, since each entry in AJ is obtained by summing the entries in a row of A, and this sum is k, by regularity. We claim that

$$A^2 = kI + (J - I) = (k-1)I + J.$$

For the (u,w) entry in A^2 is the sum, over all vertices v, of $A_{uv}A_{vw}$; this term is 1 if and only if $u \sim v$ and $v \sim w$. If $u = w$, then there are k such v (all the neighbours of u), but if $u \neq w$, then by assumption there is a unique such vertex. So A^2 has diagonal entries k and off-diagonal entries 1, whence the displayed equation holds.

Now A is a real symmetric matrix, and so it is diagonalisable. The equation $AJ = kJ$ says that the all-1 vector j is an eigenvector of A with eigenvalue k. Any other eigenvector x is orthogonal to j, and so $Jx = 0$; thus, if the eigenvalue is θ, we have

$$\theta^2 x = A^2 x = ((k-1)I + J)x = (k-1)x,$$

so $\theta = \pm\sqrt{k-1}$.

Thus A has eigenvalues k (with multiplicity 1) and $\pm\sqrt{k-1}$ (with multiplicities f and g, say, where $f + g = n - 1$.

The sum of the eigenvalues of A is equal to its trace (the sum of its diagonal entries), which is zero since all diagonal entries are zero. Thus $k + f\sqrt{k-1} + g(-\sqrt{k-1}) = 0$. So $g - f = k/\sqrt{k-1}$.

Now $g - f$ must be an integer; so we conclude that $k-1$ is a square, say $k = s^2 + 1$, and that s divides k. This is only possible if $s = 1$. So $k = 2$, and the graph is a triangle, as claimed.

Remark The finiteness assumption in the Friendship Theorem is necessary; infinite "friendship graphs" failing the conclusion of the theorem exist in great profusion. They can be built by a free construction, as follows.

Start with a set of vertices. Now the construction proceeds in stages. At each stage, for each pair of vertices without a common neighbour, add a new vertex joined to both of them. After countably many stages, any two vertices have a unique common neighbour, added at the latest at the stage after both vertices appear.

More generally, we can start the construction with any graph (finite or infinite) in which each pair of vertices has at most one common neighbour. For those interested in such things, if the set we start with is infinite, then the cardinality of the final vertex set is the same as that of the starting set, so all infinite cardinalities are possible.

1.4 Moore graphs

Before proceeding to a general definition of the class of graphs to which such linear algebra methods apply, we give one further example, the classification of Moore graphs of diameter 2.

Theorem 1.2 *Let G be a regular graph having n vertices and valency k, where $k \geq 2$.*

(a) If G is connected with diameter 2, then $n \leq k^2 + 1$, with equality if and only if G has girth 5.

(b) If G has girth 5, then $n \geq k^2 + 1$, with equality if and only if G is connected with diameter 2.

Proof (a) Take a vertex v. It has k neighbours, each of which has $k-1$ neighbours apart from v. These vertices include all those whose distance from v is at most 2 (which, by assumption, is the whole graph). So $n \leq 1 + k + k(k-1) = k^2 + 1$.

If equality holds, then there is no duplication among these vertices. So, first, all neighbours of neighbours of v lie at distance 2 from v, and second, each is joined to just one neighbour of v. So there are no 3-cycles or 4-cycles, and the girth is 5.

(b) Similar argument: try it for yourself.

A graph which is regular of valency $k > 2$, is connected with diameter 2, and has girth 5 (and so has $k^2 + 1$ vertices) is called a *Moore graph* of diameter 2. (There is a similar result for diameter d and girth $2d+1$ which we will not require: here, "Moore graphs" have diameter 2.

Examples

(a) The 5-cycle is clearly the unique Moore graph with valency 2.

(b) There is a unique Moore graph with valency 3, the famous *Petersen graph*, shown below.

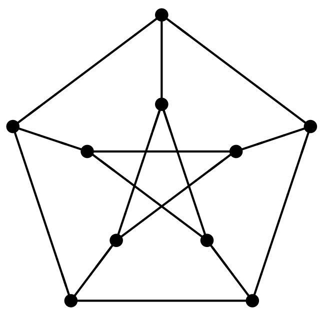


Figure 1.3: The Petersen graph

This celebrated graph has been a counterexample to many plausible conjectures in graph theory, and has even had a book devoted entirely to it and its properties (Derek Holton and John Sheehan, *The Petersen Graph*). We will say more about it in the next lecture.

It can be shown directly that there is no Moore graph of valency 4. (An outline of a proof is given in the second appendix below.) But we are going to prove the following theorem:

Theorem 1.3 *If there exists a Moore graph of valency k, then* $k = 2$, 3, 7, *or* 57.

There is a unique Moore graph of valency 7, the *Hoffman–Singleton graph*. I outline a construction of it in the appendix to this chapter. The existence of a Moore graph of valency 57 is unknown: this is one of the big open problems of extremal graph theory. Such a graph would have 3250 vertices, too large for computation! Graham Higman showed that it cannot have a vertex-transitive automorphism group.

Proof Suppose that G is a Moore graph of valency k, and let A be its adjacency matrix. We have

$$AJ = kJ, \qquad A^2 = kI + (J - I - A).$$

The first equation holds for any regular graph. The second asserts that the number of paths of length 2 from u to w is k if $u = w$, 0 if $u \sim w$ (since there are no triangles), and 1 otherwise (since there are no quadrilaterals but the diameter is 2.

As before, the all-1 vector is an eigenvector of A with eigenvalue k. Note that the second equation now gives $k^2 = k + (n - 1 - k)$, or $n = k^2 + 1$.) Any other eigenvector x is orthogonal to the all-1 vector, and so satisfies $Jx = 0$, from which we obtain the equation $\theta^2 = k - 1 - \theta$ for the eigenvalue θ, giving

$$\theta = \frac{-1 \pm \sqrt{4k-3}}{2}.$$

If these two eigenvalues have multiplicities f and g, we have

$$\begin{aligned} f + g &= k^2, \\ f(-1 + \sqrt{4k-3})/2 + g(-1 - \sqrt{4k-3})/2 &= -k. \end{aligned}$$

Multiplying the second equation by 2 and adding the first gives

$$(f - g)\sqrt{4k-3} = k^2 - 2k.$$

Now if $k = 2$, we have $f = g = 2$: this corresponds to a solution, the 5-cycle.

Suppose that $k > 2$. Then the right-hand side is non-zero, so $4k - 3$ must be a perfect square, say $4k - 3 = (2s - 1)^2$, so that $k = s^2 - s + 1$. Then our equation becomes $(f - g)(2s - 1) = (s^2 - s + 1)(s^2 - s - 1)$.

So $2s - 1$ divides $(s^2 - s + 1)(s^2 - s - 1)$. Multiplying the right-hand side by 16, and using the fact that $2s \equiv 1 \pmod{2s-1}$, we see that $2s - 1$ divides $(1 - 2 + 4)(1 - 2 - 4) = -15$, so that $2s - 1 = 1$, 3, 5, or 15. This gives $s = 1$, $s = 2$, $s = 3$ or $s = 8$, and so $k = 1$, 3, 7 or 57. The case $k = 1$ gives a graph which is a single edge, and doesn't satisfy our condition of having diameter 2, so we are left with the other three values.

1.5 Polarities of projective planes

The Friendship Theorem has a close link to finite geometry, which has been recognised from the time it was proved.

A *projective plane* is an incidence structure of points and lines satisfying the conditions

- any two points are incident with a unique line, and any two lines with a unique point;
- (nondegeneracy) there exist four points, no three collinear.

Exercise Show that, if the nondegeneracy condition is weakened to the statement that no point lies on all lines, and no line contains all points, the only additional structures that arise consist of a line L incident with all but one point P, and 2-point lines joining P to the points of L.

The class of projective planes is *self-dual*; the nondegeneracy condition implies its dual. However, not every individual projective plane is "self-dual" (isomorphic to its dual). We define a *duality* of a projective plane to be an isomorphism from the plane to its dual (a pair of bijections from points to lines and from lines to points which preserves incidence); it is a *polarity* if its square is the identity. A point P is *absolute* (with respect to a polarity π) if it is incident with its image P^π.

Theorem 1.4 *Any polarity of a finite projective plane has absolute points.*

Proof Suppose that π is a polarity with no absolute points. Form a graph whose vertices are the points of the plane, two vertices P and Q being adjacent if P is incident with Q^π (equivalently, Q is incident with P^π). Given any two points P and Q, let L be the line incident with both, and let $R = L^\pi$. Then R is the unique common neighbour of P and Q.

By the Friendship Theorem, there is a point collinear with all others; that is, the projective plane is degenerate.

Remark As we noted after the proof of the Friendship Theorem, this is false for infinite projective planes, which can be produced in great proliferation by a free construction.

1.6 Appendix: symmetric matrices

Recall that a *symmetric matrix* A is a real matrix satisfying $A = A^\top$, while an *orthogonal matrix* P satisfies $PP^\top = I$. The following result is basic.

Theorem 1.5 *Let A be a $n \times n$ real symmetric matrix. Then there is an orthogonal matrix P such that $P^{-1}AP$ is diagonal. Equivalently, there is an orthonormal basis for $\mathbb{R}^n$ consisting of eigenvectors of A.*

This is the extension we need.

Theorem 1.6 *Let $A_1, A_2, \ldots, A_m$ be $n \times n$ real symmetric matrices, and suppose that these matrices commute (that is, $A_iA_j = A_jA_i$ for $i, j = 1, \ldots, m$). Then there is an orthogonal matrix P such that $P^{-1}A_iP$ is diagonal for $i = 1, \ldots, m$. Equivalently, there is an orthonormal basis for $\mathbb{R}^n$ consisting of simultaneous eigenvectors of $A_1, \ldots, A_m$.*

Proof The proof of the theorem is by induction on m; the case $m = 1$ is just Theorem 1.5.

So suppose that the result holds for any set of $m-1$ matrices. That is, we can find an orthogonal matrix Q such that $Q^{-1}A_iQ$ is diagonal for $i = 1,\dots,m-1$.

We can partition the n coordinates in such a way that two coordinates j and k are in the same part of the partition whenever the jth and kth diagonal entries of $Q^{-1}A_iA$ are equal for all $i = 1,\dots,m-1$. This means that the space spanned by the basis vectors in a single part of the partition consists of all vectors which are eigenvectors for A_i with the corresponding diagonal element as eigenvalue for $i = 1,\dots,m-1$.

We lose no generality by grouping the parts of the partition so that they are consecutive: that is, we assume that

$$Q^{-1}A_iQ = \begin{pmatrix} \lambda_{i1}I_{r_1} & 0 & \dots & 0 \\ 0 & \lambda_{2i}I_{r_2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_{is}I_{r_s} \end{pmatrix}.$$

Thus s is the number of parts, $r_1,\dots,r_s$ are the sizes of the parts, and λ_{ij} is the eigenvalue of A_i on eigenvectors in the jth part, for $1 \le i \le m-1$ and $1 \le j \le s$.

Now consider the matrix $Q^{-1}A_mQ$. This commutes with all $Q^{-1}A_iQ$ for $i = 1,\dots,m-1$: for

$$(Q^{-1}A_mQ)(Q^{-1}A_iQ) = Q^{-1}A_mA_iQ = Q^{-1}A_iA_mQ = (Q^{-1}A_iQ)(Q^{-1}A_mQ).$$

Put $B_i = Q^{-1}A_iQ$ for all i. Note that B_i are symmetric matrices (using the fact that $Q^{-1} = Q^\top$).

Now suppose that v is a vector in the span of the jth part of the partition, so that $B_iv = \lambda_{ij}v$ for $i = 1,\dots,m-1$. Then

$$B_i(B_mv) = (B_iB_m)v = (B_mB_i)v = B_m(\lambda_{ij}v) = \lambda_{ij}(B_mv).$$

Thus B_mv is also a vector in the span of the jth part of the partition.

This implies that the matrix B_m has shape

$$B_m = \begin{pmatrix} C_1 & 0 & \dots & 0 \\ 0 & C_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & C_s \end{pmatrix},$$

where C_j is a $r_j \times r_j$ matrix.

Since B_m is symmetric, each of the C_j is symmetric. So there exist orthogonal matrices R_j, for $1 \le j \le s$, such that $R_j^{-1}C_jR_j$ is diagonal.

Put

$$R = \begin{pmatrix} R_1 & 0 & \dots & 0 \\ 0 & R_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & R_s \end{pmatrix},$$

abnd $P = QR$. Then

(a)

$$P^{-1}A_mP = R^{-1}B_mR = \begin{pmatrix} R_1^{-1}C_1R_1 & 0 & \dots & 0 \\ 0 & R_2^{-1}C_2R_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & R_s^{-1}C_sR_s \end{pmatrix}$$

is diagonal;

(b) Since $R_j^{-1}(\lambda_{ij}I)R_j = \lambda_{ij}I$, we have

$$P^{-1}A_iP = R^{-1}B_iR = \begin{pmatrix} \lambda_{i1}I & 0 & \dots & 0 \\ 0 & \lambda_{i2}I & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_{is}I \end{pmatrix}$$

is diagonal, for $i = 1, \dots, m-1$.

So we have succeeded in simultaneously diagonalising all the matrices by the orthogonal matrix P. □

In essence, we have diagonalised A_m without "un-diagonalising" $A_1, \dots, A_{m-1}$.

You might prefer a proof involving vectors rather than matrices; the argument is essentially the same but looks rather different.

This time we have m commuting self-adjoint linear operators on $V = \mathbb{R}^n$: ("self-adjoint" means $Av \cdot w = v \cdot Aw$, where $\cdot$ is the usual inner product. (An operator is self-adjoint if and only if the matrix representing it with respect to any orthonormal basis is symmetric.) Again the proof is by induction on m, the case $m = 1$ being Theorem 1.5.

So suppose we have m commuting self-adjoint linear operators on V, and by induction we have found an orthogonal decomposition

$$V = V_1 \oplus \cdots \oplus V_s$$

of V, such that, for each i, the space V_i consists of simultaneous eigenvectors of $A_1, \dots, A_{m-1}$, in such a way that two vectors belonging to different subspaces cannot have the same eigenvalues for all of $A_1, \dots, A_{m-1}$. Let λ_{ij} be the eigenvector of A_i on V_j.

Since the A_i commute, if $v \in V_j$, we have

$$A_i(A_m v) = A_m(A_i v) = A_m(\lambda_{ij} v) = \lambda_{ij}(A_m v).$$

Thus $A_m v$ is a simultanous eigenvector for $A_1, \ldots, A_{m-1}$, having the same eigenvalues as v; thus $A_m v \in V_j$.

So A_m maps V_j to itself. Clearly the restriction of A_m to V_j is self-adjoint. So by Theorem 1.5, there is an orthonormal basis for V_j consisting of eigenvectors of A_m. Clearly these vectors are still eigenvectors for $A_1, \ldots, A_{m-1}$.

Putting all these basis vectors together, and using the fact that V_j and V_k are orthogonal for $j \neq k$, we get an orthogonal matrix for the whole of V consisting of simultaneous eigenvectors of all of $A_1, \ldots, A_m$. □

A final note. If a set of symmetric matrices can be simultaneously diagonalised by an orthogonal matrix, then they must commute. For suppose that $P^{-1}A_iP = D_i$ is diagonal for $1 \leq i \leq m$. Then $A_i = PD_iP^{-1}$, and so

$$A_iA_j = (PD_iP^{-1})(PD_jP^{-1}) = PD_iD_jP^{-1} = PD_jD_iP^{-1} = A_jA_i,$$

since diagonal matrices commute.

Now the two theorems stated above both remain true if we replace the real numbers by the complex numbers, "symmetric" by "Hermitian", and "orthogonal" by "unitary". The proof is essentially the same: instead of transpose, simply use conjugate transpose.

But the converse is not true in this case; we need something a little more general. A complex matrix A is said to be *normal* if it commutes with its conjugate transpose: $A\overline{A}^\top = \overline{A}^\top A$. Now a normal matrix can be diagonalised by a unitary matrix. In general, a set of complex matrices can be diagonalised by a unitary matrix if and only if it consists of commuting normal matrices.

The proofs are left to you ...

1.7 Appendix: Moore graphs

This appendix leads you through an elementary proof of the nonexistence of a Moore graph of diameter 2 and valency 4.

Recall that a *Moore graph* of diameter 2 and valency k is a connected graph with diameter 2, girth 5, valency k, and having $k^2 + 1$ vertices. Let G be such a graph. Let $m = k - 1$.

(a) Let $\{u, v\}$ be an edge. Show that the remaining vertices consist of three sets:

- A, the set of neighours of u other than v; the vertices of A are not joined to one another or to v, and $|A| = m$.

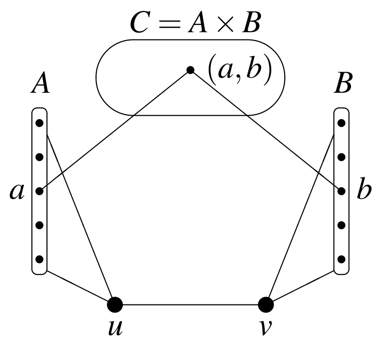
- B, the set of neighours of v other than u; the vertices of B are not joined to one another or to u, and $|B| = m$.
- C, the set of vertices remaining: each vertex in C has one neighbour in A and one in B, and each pair (a,b) with $a \in A$ and $b \in B$ corresponds to a unique vertex $c \in C$ in this manner, so that $|C| = m^2$.

Check that $2+m+m+m^2 = k^2+1$. See the figure below.

(b) Identify C with $A \times B$ in the obvious way. Show that each vertex (a,b) of C has $m-1$ neighbours in C, say $(a_1,b_1),\dots,(a_{m-1},b_{m-1})$, where $a,a_1,\dots,a_{m-1}$ are all distinct, as are $b,b_1,\dots,b_{m-1}$.

(c) Suppose that $m=2$, with $A = \{a_1,a_2\}$ and $B = \{b_1,b_2\}$. Show that the only possibility for the edges in C is from (a_1,b_1) to (a_2,b_2) and from (a_1,b_2) to (a_2,b_1). Deduce the uniqueness of the Petersen graph.

(d) Suppose that $m=3$, with $A = \{a_1,a_2,a_3\}$ and $B = \{b_1,b_2,b_3\}$. Suppose, without loss of generality, that (a_1,b_1) is joined to (a_2,b_2) and (a_3,b_3). Show that necessarily (a_2,b_2) is joined to (a_3,b_3), in contradiction to the fact that there are no triangles. Deduce the non-existence of the Moore graph with valency 4.



I mention briefly a construction of the Moore graph of valency 7: see Cameron and van Lint, *Designs, Graphs, Codes and their Links*, for further details. In this case, $|A| = |B| = 6$. We exploit the fact that the symmetric group of degree 6 has an *outer automorphism*: that is, it has two different actions on sets of size 6, which we can take to be A and B in our construction. These actions have the property that the element of S_6 acting as a transposition (a_1,a_2) on A acts on B as the product of three transpositions; if (b_1,b_2) is one of these three transpositions, then the element of S_6 acting on B as the transposition (b_1,b_2) acts on A as the product of three transpositions, one of which is (a_1,a_2).

Now we complete the graph by putting an edge from (a_1,b_1) to (a_2,b_2) whenever the above situation holds. Properties of the outer automorphism enable one to show that this graph is indeed a Moore graph of valency 7.

CHAPTER 2

Strongly regular graphs

In the preceding section we met two examples of “strongly regular graphs”: putative counterexamples to the Friendship Theorem, and Moore graphs. Now we examine this class of graphs in more details.

2.1 Strongly regular graphs

A graph G is *strongly regular* with parameters (n,k,λ,μ) if the following conditions hold:

- G has n vertices;
- G is regular with valency k;
- the number of common neighbours of two distinct vertices v and w is λ if $v \sim w$ and μ otherwise.

The parameters are not all independent. Fix a vertex u, and count pairs (v,w) of vertices where $u \sim v \sim w$ but $u \not\sim w$. If l denotes the number of vertices not joined to u, we have

$$k(k-\lambda-1) = l\mu,$$

so the parameters k,λ,μ determine l, and hence $n = 1+k+l$. The argument also gives us a divisibility condition: μ divides $k(k-\lambda-1)$.

A regular counterexample to the Friendship Theorem would be a strongly regular graph with $\lambda = \mu = 1$, while a Moore graph of diameter 2 is a strongly regular graph with $\lambda = 0$, $\mu = 1$. So, for example, the Petersen graph has parameters $(10,3,0,1)$.

Here are some strongly regular graphs.

- $L(K_m)$ is strongly regular with parameters $(m(m-1)/2, 2(m-2), m-2, 4)$. (This graph is called the *triangular graph* $T(m)$.)
  For clearly there are $m(m-1)/2$ vertices (edges of K_m. Given an edge vw, it is adjacent to all edges vx and wx with $x \neq v, w$ (so $2(m-2)$ of these). Two adjacent edges uv and uw are joined to vw and to all ux with $x \neq u, v, w$: $1+(m-3)$ of these; and finally, nonadjacent edges uv and wz have four common neighbours, uw, uz, vw and vz.
  Hoffman and Chang showed that, for $m \neq 8$, any strongly regular graph with the same parameters as $T(m)$ is isomorphic to $T(m)$; for $m = 8$, there are three exceptional graphs, the *Chang graphs.*. We will see the explanation for this later.
- $L(K_{m,m})$ is strongly regular with parameters $(m^2, 2(m-1), m-2, 2)$. (This graph is called the *square lattice graph* $L_2(m)$. It can be viewed as m^2 vertices in an $m \times m$ array, with vertices in the same row or column being adjacent.)
  Shrikhande showed that, for $m \neq 4$, a strongly regular graph with the same parameters as $L_2(m)$ is isomorphic to $L_2(m)$; for $m = 4$ there is a unique exception, the *Shrikhande graph*. Again we will see the reason later.

There are many more examples, derived from group-theoretic, geometric or combinatorial configurations; we will meet some of them later in this course. A strongly regular graph is a special case of a more general type of structure, an *association scheme*.

The disjoint union of complete graphs of size $k+1$ is strongly regular, with $\mu = 0$. Such a graph is sometimes called "trivial". Its complement is a *complete multipartite graph*, and is also strongly regular, with $\mu = k$. (Indeed, the complement of a strongly regular graph is again strongly regular – can you prove this?)

We now apply the eigenvalue methods we saw in the two examples. The adjacency matrix A has an eigenvalue k with eigenvector the all-1 vector j, as we see from the equation $AJ = kJ$. Any other eigenvector x can be taken to be orthogonal to j, and so satisfies $Jx = 0$; thus, if the eigenvalue is θ, we have

$$\theta^2 x = A^2 x = ((k-\mu)I + (\lambda-\mu)A)x = ((k-\mu)+\lambda-\mu)\theta x,$$

and so $\theta^2 - (\lambda-\mu)\theta - (k-\mu) = 0$.

The roots of this equation give the other eigenvalues of A, which (by convention) are denoted r and s. Their product is $-(k-\mu)$, which is negative (if $k \neq \mu$); so we assume that $r > 0$ and $s < 0$. We have

$$r, s = \tfrac{1}{2}\left(\lambda - \mu \pm \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}\right).$$

If r and s have multiplicities f and g, then we have

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

the second equation coming from the fact that the trace of A is 0.

These equations can be solved to give f and g, which must be non-negative integers:

Theorem 2.1 *If a strongly regular graph with parameters (n,k,λ,μ) exists, then the numbers*

$$f,g = \frac{1}{2}\left(n-1 \pm \frac{(n-1)(\mu-\lambda)-2k}{\sqrt{(\mu-\lambda)^2+4(k-\mu)}}\right)$$

are non-negative integers.

To analyse further, we divide strongly regular graphs into two types:

Type I, with $(n-1)(\mu-\lambda) = 2k$. In this case

$$n = 1 + \frac{2k}{\mu-\lambda} > 1+k,$$

so $0 < \mu-\lambda < 2$. So we must have $\mu-\lambda = 1$, which gives $\lambda = \mu+1$, $k = 2\mu$, $n = 4\mu+1$. Examples of graphs of this type include the 5-cycle (with $\mu = 1$) and $L_2(3)$ (with $\mu = 2$).

Type 2, with $(n-1)(\mu-\lambda) \neq 2k$. In this case, we see that $(\mu-\lambda)^2 - 4(k-\mu)$ must be a perfect square, say u^2; that u divides $(n-1)(\mu-\lambda)-2k$, and that the quotient is congruent to $n-1 \pmod 2$. This is the "general case": most parameter sets for strongly regular graphs fall into this case.

Example Consider the triangular graph, which has parameters $(m(m-1)/2, 2(m-2), m-2, 4)$. We have

$$\sqrt{(\mu-\lambda)^2+4(k-\mu)} = \sqrt{(m-6)^2+8(m-4)} = m-2,$$

and some further calculation gives the multiplicities of the eigenvalues as $m-1$ and $m(m-3)/2$, which are integers (as they should be).

Example Let us consider our previous examples.

We saw that a counterexample to the Friendship Theorem would be strongly regular, with $\lambda = \mu = 1$ and $n = k^2 - k + 1$. We find

$$\sqrt{(\mu - \lambda)^2 + 4(k - \mu)} = 2\sqrt{k-1},$$

so $k = s^2 + 1$, where s divides k; we reach the same contradiction as before unless $s = 0$.

A Moore graph of diameter 2 is strongly regular, with $\lambda = 0$, $\mu = 1$, and $n = k^2 + 1$. This time, Type 1 is possible, and corresponds to the 5-cycle. For Type 2, we have that $4k - 3$ is a perfect square, say $(2u - 1)^2$, where $2u - 1$ divides $k(k-2)$; again we reach the same conclusion as before.

2.1.1 Resources

Andries Brouwer keeps a list of parameter sets of strongly regular graphs on at most 1300 vertices at `http://www.win.tue.nl/~aeb/graphs/srg/srgtab.html`

A list of strongly regular graphs on at most 64 vertices is maintained by Ted Spence at `http://www.maths.gla.ac.uk/~es/srgraphs.php` (there may be many different graphs with the same parameters – note that the list is not quite complete, see the documentation).

2.2 Petersen, Clebsch and Schläfli graphs

Three important graphs which play an important role in these lectures are those named in the section title. They are strongly regular graphs having parameters respectively $(10,3,0,1)$, $(16,5,0,2)$, and $(27,10,1,5)$.

We already met the Petersen graph (and saw its portrait) in the last lecture. More formally, it is the complement of the line graph of K_5: in other words, its vertices can be labelled with the 2-element subsets of $\{1,2,3,4,5\}$, so that two vertices are joined if and only if their labels are disjoint.

Another construction of it is from the dodecahedral graph (the 1-skeleton of the dodecahedron). This graph has 20 vertices, falling into 10 “antipodal pairs” (lying at the maximum distance, namely 5, from each other). If we form a graph on 10 vertices by identifying antipodal vertices, we obtain the Petersen graph.

The *Clebsch graph* can be constructed as follows. Take a set A of size 5, say $\{1,2,3,4,5\}$. The vertices of the graph are the subsets of A of cardinality 1 or 2, together with an extra vertex $*$. Edges are as follows (we identify a singleton subset of A with an element of A):

- $*$ is joined to the five elements of A;
- an element of A is joined to a 2-subset of A containing it;
- two 2-subsets of A are joined if and only if they are disjoint.

A relatively small amount of checking shows that this graph is regular with valency 5 and contains no triangles, while two vertices at distance 2 have two common neighbours – in other words, it is strongly regular $(16,5,0,2)$.

Another construction is from the 5-dimensional cube (the graph whose vertices are all 5-tuples of zeros and ones, two vertices joined if they agree in all but one coordinate, in other words, their *Hamming distance* is 1). For each vertex, there is a unique antipodal vertex at distance 5 (obtained by changing the 0s into 1s and *vice versa*. Now, if we identify antipodal vertices, we obtain the Clebsch graph. This can be looked at another way. The set of 5-tuples containing an even number of ones (those with even Hamming weight) contains one vertex from each antipodal pair, so we can regard these tuples as the vertices of the Clebsch graph; two vertices are joined if they differ in all but one position.

Note that the graph on the set of vertices not adjacent to a fixed vertex in the Clebsch graph is the Petersen graph.

The *Schläfli graph* is defined in a somewhat similar way. The vertex set consists of three parts: a set of ten vertices falling into five 2-sets $\{a_i, b_i\}$ for $i = 1, \dots, 5$; the set of all 5-tuples of zeros and ones with even Hamming weight (an even number of ones); and one further vertex $*$. Edges are of three types:

- $*$ is joined to a_i and b_i for all i;
- a word w (a 5-tuple with even weight) is joined to a_i if $w_i = 0$, and to b_i if $w_i = 1$;
- two words are joined if they differ in all positions except one.

Again, checking shows that the graph is strongly regular $(27,10,1,5)$.

The graph on the set of vertices not adjacent to a fixed vertex in the Schläfli graph is the Clebsch graph.

Theorem 2.2 *Each of the Petersen, Clebsch and Schläfli graphs is the unique strongly regular graph with its parameters (up to isomorphism).*

Here is the proof of uniqueness of the Clebsch graph. The other two are left as exercises for you.

Let G be a strongly regular graph with parameters $(16,5,0,2)$. Let A be the set of five neighbours of a fixed vertex v, and B the set of non-neighbours. The induced subgraph on A is null, since $\lambda = 0$. Now $\mu = 2$, from which we conclude that any vertex in B has two neighbours in A, and any two vertices in A have a unique common neighbour in B. So vertices in B correspond to 2-element subsets of A. Now a vertex in B has two neighbours in A, and so three in B. Two adjacent vertices in B must be indexed by disjoint subsets, since otherwise we would have a triangle. Since there are three pairs disjoint from a given one, the edges in B are determined: two vertices are joined if and only if the pairs labelling them are disjoint. So everything is determined.

2.3 Partition into Petersen and Clebsch graphs

The Petersen graph has ten vertices, fifteen edges, and valency 3, and is arguably the most famous graph of all. The complete graph on ten vertices has 45 edges and valency 9. In 1983, Schwenk asked in the *American Mathematical Monthly* whether K_{10} could be partitioned into three Petersen graphs. Four years later he gave an elegant solution based on linear algebra:

Theorem 2.3 *It is not possible to partition the edges of the complete graph K_{10} into three copies of the Petersen graph.*

Proof The Petersen graph is strongly regular, with parameters $(10,3,0,1)$. Using the method of Chapter 1, it is routine to calculate its eigenvalues: they are 3 with multiplicity 1 (corresponding to the all-1 eigenvector); 1 with multiplicity 5; and -2 with multiplicity 4.

Suppose, more generally, that we can find two edge-disjoint copies P_1 and P_2 of the Petersen graph, and let G be the graph formed by the remaining edges; then G is clearly also a regular graph with valency 3. Let V_1 and V_2 be the 5-dimensional eigenspaces for P_1 and P_2. These two spaces are contained in the 9-dimensional space orthogonal to the all-1 vector j (the space of vectors with coordinate sum 0). So by the intersection-sum formula, $V_1 \cap V_2 \neq \{0\}$. Let v be a non-zero vector in this intersection.

Now the adjacency matrices A_1, A_2, B of P_1, P_2, G satisfy $A_1 + A_2 + B = J - I$, where J is the all-1 matrix. Since $Jv = 0$, we have

$$2v + Bv = A_1 v + A_2 v + Bv = Jv - Iv = -v,$$

so $Bv = -3v$ and B has an eigenvalue -3. So G cannot be isomorphic to the Petersen graph (which doesn't have an eigenvalue -3).

Indeed, it is known that a regular graph of valency 3 with an eigenvalue -3 is necessarily bipartite. (In general, let G be a connected regular graph with valency k. If G has an eigenvalue $-k$, then take an eigenvector x with eigenvalue $-k$, and partition the vertices into those with positive and negative sign; show that any edge goes between parts of this partition.)

The next question is: Can the edge set of K_{16} be partitioned into three copies of the Clebsch graph?

This time the answer is "yes", and this fact is significant in Ramsey theory, as we will briefly discuss. The construction is due to Greenwood and Gleason.

Here is the construction. Let F be the field $\mathrm{GF}(16)$. The multiplicative group of F is cyclic of order 15, and so has a subgroup A of order 5, which has three cosets, say A, B, C in the multiplicative group. Now define three graphs as follows: The vertex set is the set F; two vertices x, y are joined in the first, second, third graph respectively if $y - x$ lies in A, B, C respectively. Each graph has valency 5, since $|A| = |B| = |C| = 5$, and the three graphs are isomorphic (multiplication by an element of order 3 in the multiplicative group permutes them cyclically).

It can be shown that each of the three graphs is isomorphic to the Clebsch graph. Using the uniqueness, it is enough to show that they are all strongly regular with parameters $(16, 5, 0, 2)$. The first two parameters are clear.

Let a, b, c, d, e be the fifth roots of unity in $\mathrm{GF}(16)$. These five elements sum to zero: Any 5th root of unity ω except 1 itself satisfies

$$1 + \omega + \omega^2 + \omega^4 + \omega^5 = 0.$$

We claim that no proper subset sums to 0. Choose a subset of cardinality i. If $i = 1$, we would have (say) $a = 0$, which is not so. If $i = 2$, we would have (say) $a + b = 0$, so $b = a$ (as the characteristic is 2), which again is not so. If $i \geq 3$, then the complementary set would also sum to zero, which again is not so.

Now, if $(x_1, \dots, x_k)$ is a cycle in the graph with "connection set" A, then each of $x_2 - x_1, x_3 - x_2, \dots, x_1 - x_k$ would be a fifth root of unity, and these roots would sum to 0. So the graph contains no triangles; and the only 4-cycles are those of the form $(x, x + a, x + a + b, x + b)$ for $a, b \in A$. Thus indeed $\lambda = 0$ and $\mu = 2$.

Now, unlike what happened with the Petersen graph, if we remove the edges of two edge-disjoint Clebsch graphs from K_{16}, what remains must be another Clebsch graph:

Proposition 2.4 *The complement of two edge-disjoint Clebsch graphs in K_{16} is isomorphic to the Clebsch graph.*

Proof As in the Petersen proof, we let A_1 and A_2 be the adjacency matrices for the two Clebsch graphs, and B the matrix for what remains. So we have $A_1 + A_2 + B = J - I$.

This time we find that the Clebsch graph has eigenvalues 5 (multiplicity 1), 1 (multiplicity 10), and -3 (multiplicity 5). So each of A_1 and A_2 has a 10-dimensional space of eigenvectors with eigenvalue 1, contained in the 15-dimensional space orthogonal to the all-1-vector. These two spaces have intersection of dimension (at least) 5. If v is a vector in this space, then $A_1 v = A_2 v = I_v = v$, $Jv = 0$; so $Bv = -3v$. Thus B has eigenvalue -3 (with multiplicity 5) in addition to 5 (with multiplicity 1).

Let $r_1, \ldots, r_{10}$ be the remaining eigenvalues of B. Since the trace of B is 0, we have $5 + 5 \cdot (-3) + r_1 + \cdots + r_{10} = 0$, so

$$r_1 + \cdots + r_{10} = 10.$$

Moreover, the trace of B^2 is 80, since all of its diagonal elements are 5; thus $25 + 5 \cdot 9 + r_1^2 + \cdots + r_{10}^2 = 80$, so

$$r_1^2 + \cdots + r_{10}^2 = 10.$$

From this we see that

$$(r_1 - 1)^2 + \cdots + (r_{10} - 1)^2 = 0,$$

so $r_1 = \cdots = r_{10} = 1$. So B has the same spectrum as the Clebsch graph: eigenvalues 5, 1, -3 with multiplicities 1, 10 and 5 respectively.

This means that $B^2 + 2B - 3I$ vanishes on the space orthogonal to the all-1 vector, so that $B^2 + 2B - 3I$ is a multiple of the all-1 matrix J. The diagonal entries are $5 - 3 = 2$, so we have $B^2 + 2B - 3I = 2J$, so that

$$B^2 = 5I + 2(J - I - B).$$

This matrix equation shows that B is the adjacency matrix of a strongly regular graph, with $\lambda = 0$ and $\mu = 2$, so parameters $(16, 5, 0, 2)$.

We saw earlier that the only such graph is the Clebsch graph. The proof is done.

2.4 Ramsey's Theorem

Theorem 2.5 (The Party Theorem) *Given six people at a party, either three of them are mutual friends, or three of them are mutual strangers. Moreover, six is the smallest number with this property.*

Again, our concept of "friendship" is mathematical and not sociological; we assume that friendship is the adjacency relation of a graph, and that being strangers is the adjacency matrix of the complementary graph (in other words, two people are either friends or strangers, but not both).

Proof We have two things to do: to show that the assertion is true with six people but false for five. In this case, the latter is easily dealt with: the pentagon or 5-cycle is a graph on 5 vertices containing no triangle; its complement is also a 5-cycle and contains no triangle. (Think of the edges and diagonals of a 5-gon.)

Given six people at a party, select one of them, say A. Of the other five, according to the Pigeonhole Principle, either at least three are friends of A, or at least three are strangers to A. Let us consider the first case, and suppose that B, C, D are friends of A. (The other case is similar.) If any two of B, C, D (say B and C) are friends, then we have three mutual friends A, B, C. If not, then B, C, D are mutual strangers.

This theorem has a far-reaching generalisation, found in the 1930s. In order to state it, we use the languge of colourings rather than friendship.

Theorem 2.6 (Ramsey's Theorem) *Let $r, k, l_1, \ldots, l_r$ be given positive integers. Then there exists a positive integer N such that, if the k-subsets of $\{1, \ldots, N\}$ are coloured with r colours, say $c_1, \ldots, c_r$, then there is some i with $1 \leq i \leq r$ and a l_i subset L_i of $\{1, \ldots, N\}$ so that every k-subset of L_i has colour c_i.*

I will not prove the theorem here; the proof is just an elaboration of the argument we saw for the Party Theorem. A consequence of Ramsey's Theorem is that there is a smallest number N with the property of the theorem; we call this the *Ramsey number $R_k(l_1, \ldots, l_r)$*.

Thus, the Party Theorem tells us that $R_2(3, 3) = 6$.

Very few Ramsey numbers are known exactly (see the survey by Radzizowski in the *Electronic Journal of Combinatorics*). For example, it is known that $R_2(4, 4) = 18$, but $R_2(l, l)$ is not known for any larger value of l. In fact, Paul Erdős said that, if powerful aliens arrived and threatened to destroy the earth unless we told them the value of $R_2(5, 5)$, then we should put every mathematician and computer on the planet to work on the problem; but if they asked for $R_2(6, 6)$, our only hope would be to get them before they got us.

One of the few values that is known is:

Theorem 2.7 $R_2(3, 3, 3) = 17$.

Proof We suppose that the edges of K_{17} are coloured with three colours, say red, blue, green. Choose a vertex a. By the Pigeonhole Principle, there is a colour (let us say red) such that at least six vertices are joined to a by red edges – this is because $1 + 5 + 5 + 5 < 17$. Let b, c, d, e, f, g be vertices joined to a by red edges. If any of the edges within this set is red, we have a red triangle with a. If not, then $\{b, \ldots, g\}$ is a set of six vertices with edges coloured blue and green; by the Party Theorem, there is either a blue triangle or a green triangle within this set.

Now we have to show that 16 is not enough. For that we use the configuration of three edge-disjoint Clebsch graphs. Colour their edges red, blue and green respectively; since each is a Clebsch graph, there is no triangle of a single colour.

2.5 Regular two-graphs

Regular two-graphs are objects introduced by Graham Higman to study various doubly transitive permutation groups, especially the third Conway group. They have very close connections with strongly regular graphs, and also to other structures such as equiangular lines in Euclidean space (which are outside what I can talk about here, unfortunately).

A *regular two-graph* $(X,\mathscr{T})$ consists of a set X and a set $\mathscr{T}$ of 3-element subsets of X (which, to exclude degenerate cases, we assume is not the empty set and not the set of all 3-subsets of X) with the properties:

(a) any 4-element subset of X contains an even number of members of $\mathscr{T}$;

(b) any 2-element subset of X is contained in a constant number c of elements of $\mathscr{T}$ (in other terminology, $(X,\mathscr{T})$ is a 2-$(|X|,3,c)$ design).

Given a regular two-graph $(X,\mathscr{T})$, and a point $x \in X$, we define a graph G_x as follows: the vertex set is $X \setminus \{x\}$, and the vertices y and z are adjacent if and only if $\{x,y,z\} \in \mathscr{T}$.

Theorem 2.8 *If $(X,\mathscr{T})$ is a regular two-graph with parameter c, then for any $x \in X$, the graph G_x defined above is a strongly regular graph $(n-1,k,\lambda,\mu)$ with $n = |X|$, $k = c$, and $\mu = c/2$.*

Conversely, given a strongly regular graph G with $\mu = k/2$, there is a regular two-graph $(X,\mathscr{T})$, where X consists of the vertex set of X and a new isolated vertex x, and $\mathscr{T}$ consists of the triples $\{y,z,w\}$ containing an odd number an odd number of edges of G.

Proof We say that a 4-subset of X is *complete* if it contains four members of $\mathscr{T}$. Note that $\{x,y,z,w\}$ is complete if and only if $\{y,z,w\}$ is a triangle in G_x. (The forward implication is trivial; for the reverse, if $\{y,z,w\}$ is a triangle, then $\{x,y,z,w\}$ contains at least three members of $\mathscr{T}$, and so is complete.

We show that any triple in $\mathscr{T}$ is contained in a constant number d of 4-sets, where $|X| = 3c-2d$. Let $\{x,y,z\} \in \mathscr{T}$. For any further point w, either all of $\{x,y,w\}$, $\{x,z,w\}$ and $\{y,z,w\}$ are in $\mathscr{T}$ (this happens for d points w) or exactly one of them is (this happens $c-d-1$ times for any given triple). So $d+3(c-d-1) = |X|-3$ as required.

It now follows that G_x has valency $k = c$, and any two adjacent points have $\lambda = d$ common neighbours.

Now suppose that $\{x,y,z\} \notin \mathscr{T}$. Then, for any w, none or two of $\{x,y,w\}$, $\{x,z,w\}$, $\{y,z,w\}$ belong to $\mathscr{T}$; let the numbers of w realising two of the three pairs be α,β,γ. Then $\alpha+\beta=\alpha+\gamma=\beta+\gamma=c$, so that $\alpha=\beta=\gamma=c/2$. This shows that, if y and z are non-adjacent in G_x, they have $\mu=c/2$ common neighbours, as required.

The converse direction is more straightforward and is omitted.

Examples of strongly regular graphs which have $k=2\mu$ (and so give rise to regular two-graphs) include three graphs which will have a starring role in the rest of the lectures:

(a) the 3×3 grid (the line graph of $K_{3,3}$, with parameters $(9,4,1,2)$;

(b) the complement of the line graph of K_6, with parameters $(15,6,1,3)$;

(c) the Schläfli graph, with parameters $(27,10,1,5)$.

There are many more. Here is a class of examples, which I will not discuss further, the *Paley graphs*. Let F be a finite field of order q congruent to 1 (mod 4). Then half of the non-zero elements of F (including -1) are squares in F, and half are non-squares. The graph $P(q)$ has vertex set F; vertices x and y are joined if and only if $y-x$ is a square. (Since -1 is a square, the joining rule is symmetric.) The graph $P(q)$ is strongly regular, with parameters $(q,(q-1)/2,(q-5)/4,(q-1)/4)$. Note that $P(5)$ is the 5-cycle, while $P(9)$ is the 3×3 grid.

There is another connection between regular two-graphs and strongly regular graphs, that doesn't involve isolating a vertex. Given a graph G with vertex set X, we can construct a two-graph (a structure satisfying condition (a) of the definition of a regular two-graph) by the rule that $\mathscr{T}$ is the set of all 3-sets containing an odd number of edges of G.

Proposition 2.9 *If G is a regular graph which gives rise to a regular two-graph by the above construction, then G is strongly regular, and its parameters satisfy $n=2(2k-\lambda-\mu)$; the parameter of the two-graph is given by $c=n-2(k-\lambda)=2(k-\mu)$. Conversely, a strongly regular graph whose parameters satisfy this condition defines a regular two-graph.*

I leave the proof as an exercise. Among strongly regular graphs which satisfy the condition, we have

(a) the Petersen graph, the Clebsch graph;

(b) the 4×4 grid (the line graph of $K_{4,4}$);

(c) the line graphs of K_5 and K_8.

To conclude this section, here is a design-theoretic construction of a very important regular two-graph. This uses the famous 4-$(23,7,1)$ *Witt design*, with 23 points, 253 blocks, each block a set of seven points, and any four points contained in a unique block. It is known that there is a unique such design; it has the property that any two blocks intersect in 1 or 3 points.

Build a graph G, whose vertex set is $\mathscr{P} \cup \mathscr{B}$, where $\mathscr{P}$ and $\mathscr{B}$ are the point and block sets of the design. Here are the edges:

- Any two vertices in $\mathscr{P}$ are adjacent.
- A vertex in $\mathscr{P}$ and a vertex in $\mathscr{B}$ are adjacent if and only if they are incident.
- Two vertices in $\mathscr{B}$ are adjacent if and only if their intersection has cardinality 3.

Let X be the vertex set, and $\mathscr{T}$ the set of triples from X containing an odd number of edges of G. Counting arguments show that this is a regular two-graph with parameter $c = 162$. (For example, if $x, y \in \mathscr{P}$, then there are 21 further points of $\mathscr{P}$ (joined to both), 21 blocks containing both, and 120 blocks containing neither.)

The automorphism group of the two-graph is the third Conway group. (This construction was given by Graham Higman.)

The graph G_x we obtain from it is strongly regular with parameters $(275,162,105,81)$. This is the *McLaughlin graph*.

CHAPTER 3

The Strong Triangle Property

We begin with one further result which looks superficially similar to the Friendship Theorem. However, this result, the classification of graphs with the Strong Triangle Property, will lead us on to root systems, graphs with smallest eigenvalue -2, characterisation of quadrics over the field of two elements, and more besides.

3.1 The Strong Triangle Property

We say that a graph G has the *strong triangle property* if

> Every edge $\{u,v\}$ of G is contained in a triangle $\{u,v,w\}$ with the property that, for any vertex $x \notin \{u,v,w\}$, x is joined to exactly one of u,v,w.

Theorem 3.1 *A graph with the strong triangle property is one of the following:*

(a) a null graph;

(b) a Friendship Theorem graph (see Figure 1.1);

(c) one of three special graphs on 9, 15 *and* 27 *vertices.*

Remark The three special graphs are the line graph of $K_{3,3}$, the complement of the line graph of K_6, and the Schläfli graph; the three graphs we met in connection with regular two-graphs in the last section.

Proof Let G be such a graph. If G has no edges, then (a) holds, so we may assume there is at least one edge. Now we follow the proof of the Friendship Theorem, by showing that either (b) holds or the graph is regular.

First we claim that, if u and v are not joined, then they have the same valency. For, given any vertex u, the subgraph on the closed neighbourhood of u is a Friendship Theorem graph, consisting of (say) m triangles joined at a vertex, and so u has valency $2m$. Since v is not joined to u, it is joined to one vertex in each of these triangles; so the neighbourhood of v consists of at least m triangles, and v has valency at least $2m$. Reversing the roles of u and v gives the claim.

Suppose that the graph is not regular, and let a and b be vertices with different valencies. There is a third vertex c joined to both, as in the Friendship Theorem. Now c has different valency from at least one of a and b, say a. Any further vertex is joined to exactly one of a,b,c, and also to at least one of a and b and at least one of a and c; so it is joined to a, and we have a Friendship Theorem graph.

In the case when the graph is regular, we have that any two adjacent vertices have one common neighbour, while two non-adjacent vertices have m common neighbours, where $2m$ is the valency of the graph. So it is strongly regular, with parameters $n, 2m, 1, m$; and calculation shows that $n = 6m-3$. (Note that, since $k = 2\mu$, the graph will give rise to a regular two-graph.)

Our analysis of strongly regular graphs in Chapter 2 shows that the eigenvalues are $2m$, 1 and $-m$. If their multiplicities are 1, f, g, we get

$$\begin{aligned} 1+f+g &= 6m-3, \\ 2m+f-mg &= 0, \end{aligned}$$

so $(m+1)g = 8m-4$. Thus $m+1$ divides 12, that is, $m = 2$, 3, 5 or 11.

Further analysis shows that $m = 11$ is impossible while the graphs in the other three cases are unique. (There is a bare-hands argument which comes up with the values 2, 3, 5 without using the strongly regular graph conditions; alternatively, the next result in the theory of strongly regular graphs beyond what we did in the last lecture, the *Krein condition*, excludes the case $m = 11$.)

Here is the combinatorial argument. Let I be an index set for the set of triangles containing a given base point $*$; denote the two points of triangle i by $(i,0)$ and $(i,1)$. Now any point p not adjacent to $*$ is joined to one point in each triangle; so we can label p by a function $w_p : I \to \{0,1\}$, where p is adjacent to $(i, w_p(i))$ for all $i \in I$. Now let p and q be non-neighbours of $*$, and consider the possible relations between p and q.

- If p and q are adjacent, then w_p and w_q agree in one point and differ in all others: for the third point in the triangle containing p an q has the form (i,ε) for some $\varepsilon \in \{0,1\}$, whence $w_p(i) = w_q(i) = \varepsilon$ but there are no further agreements.

- If p and q are nonadjacent but have a common neighbour r not joined to $*$, then w_p and w_q agree in all but two positions; to see this, observe that all but two values are changed twice as we go from p to r to q.
- Otherwise, *every* triangle on p contains a neighbour of $*$ and a neighbour r of q, and these two must be equal since there is a path prq which cannot lie in the non-neighbourhood of $*$. So w_p and w_q agree everywhere: $w_p = w_q$.

But now, if $|I| > 2$, there is a path of length 3 in the set of non-neighbours of $*$, then all but three values of the function are changed three times, so the functions associated with the end points of the path agree in three points only. Since we covered all cases, "three" must be equal to "all of I" or "all but two points of I", and $|I| \leq 5$, as required.

Note the finiteness of I is not assumed here. So there are no infinite regular graphs with the strong triangle property, a fact we will meet again!

3.2 Root systems and the ADE affair

Root systems are geometric objects in Euclidean space, which crop up in many parts of mathematics including Lie algebras, singularity theory, mathematical physics, and graph theory.

In this section of the lectures, we will use graph theory to give the famous *ADE classification* of root systems in which all roots have the same length. This will then be used to determine the graphs whose adjacency matrix has least eigenvalue -2 or greater.

3.2.1 The definition

We work in the Euclidean space $V = \mathbb{R}^d$, with the standard inner product.

Given a non-zero vector $u \in V$, there is a unique hyperplane H_u through the origin which is perpendicular to u. We define the *reflection* r_u in this hyperplane to be the linear map which fixes every vector in H_u and maps u to $-u$.

The formula for this reflection is

$$r_u(x) = x - \frac{2(x.u)}{u.u}\,u.$$

For this map is clearly linear, and does map u to $-u$ and fixes every x satisfying $x.u = 0$.

A *root system* is a set S of non-zero vectors of $\mathbb{R}^d$ satisfying the four conditions

- $\langle S \rangle = V$ (S spans V);
- if $u, \lambda u \in S$, then $\lambda = \pm 1$;

- if $u, v \in S$, then $2(v.u)/(u.u)$ is an integer;
- for all $u \in S$, the reflection r_u maps S to itself.

We remark that the first condition is not crucial, since we could replace V by the subspace spanned by S to ensure that it holds. Also, the fourth condition implies the converse of the second (that is, if $u \in S$, then $r_u(u) = -u \in S$). Also, the third condition shows that $r_u(v)$ is an integer combination of u and v, for all $u, v \in S$. (This is called the *crystallographic condition*.)

Suppose that S_1 and S_2 are root systems in spaces V_1 and V_2. Then clearly $S_1 \cup S_2$ is a root system in the orthogonal direct sum of V_1 and V_2. Such a root system is called *decomposable*; if there is no orthogonal direct sum decomposition with S the union of its intersections with the two summands it is called *indecomposable*. Clearly, to classify all root systems, it suffices to classify the indecomposable ones, and take direct sums of them.

It turns out that the indecomposable root systems fall into four infinite families apart from five sporadic examples. I am not going to prove this, but will deal with the case where all the roots have the same length. First, here are the examples. We assume that $e_1, e_2, \ldots, e_n$ is an orthonormal basis for $\mathbb{R}^n$.

- $A_n = \{e_i - e_j : 1 \leq i, j \leq n+1, i \neq j\}$.
- $D_n = \{\pm e_i \pm e_j : 1 \leq i < j \leq n\}$.
- $E_8 = D_8 \cup \{\frac{1}{2}\sum_{i=1}^{8} \varepsilon_i e_i : \varepsilon_i = \pm 1, \prod_{i=1}^{8} \varepsilon_i = +1\}$.
- $E_7 = \{u \in E_8 : (e_1 - e_2).u = 0\}$.
- $E_6 = \{u \in E_8 : (e_1 - e_2).u = (e_2 - e_3).u = 0\}$.

It can be verified that each of these is a root system; the subscript gives the dimension. (Note that the vectors of A_n do not span the whole of $\mathbb{R}^{n+1}$, since each of them is orthogonal to the vector $e_1 + \cdots + e_{n+1}$; they span the n-dimensional space perpendicular to this vector.)

With a little more effort we can see that D_2 is decomposable (it consists of two vectors in each of two perpendicular directions), and D_3 is isomorphic to A_3; hence we consider D_n only for $n \geq 4$.

Root systems are beautiful symmetrical objects: Mark Ronan, in his recent book on the history of the finite simple group classification, refers to them as *multidimensional crystals*. Figure 3.1 shows A_2 and A_3.

Theorem 3.2 *An indecomposable root system in which all the roots have the same length is isomorphic to A_n ($n \geq 1$), D_n ($n \geq 4$), E_6, E_7 or E_8.*

We will prove this theorem after a small diversion. Using this result, it is not too hard to extend the theorem to deal with arbitrary root systems, as we will see.

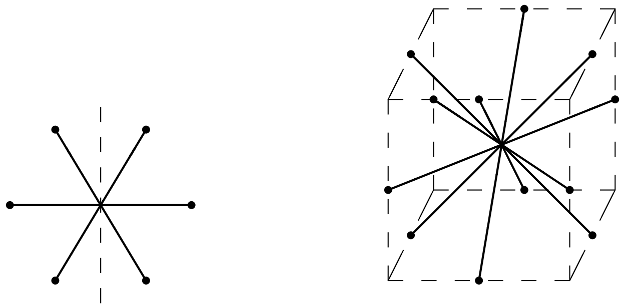


Figure 3.1: The root systems A_2 and A_3

3.2.2 Proof of Theorem 3.2

Suppose we have an indecomposable root system in $\mathbb{R}^d$ with all roots of the same length. Without loss of generality, we take this length to be $\sqrt{2}$; so $u.u = 2$ for every root u, and $u.v \in \{2, 1, 0, -1, -2\}$ for any roots u and v. This means that any two roots are at an angle 0°, 60°, 90°, 120° or 180°. In other words, the lines spanned by the roots make angles 90° or 60° with each other.

There exist two roots u, v with $u.v = -1$ (in other words, an angle 120°). Then $w = -u - v$ is also a root (it is $-r_u(v)$). We call six roots of the form $\pm u$, $\pm v$ and $\pm w$ a *star*. (They form a root system of type A_2 in the plane they span.)

Let S be a set of lines through the origin in Euclidean space $\mathbb{R}^d$, any two making an angle 90° or 60°. We say that S is *star-closed* if, whenever two lines $L_1, L_2 \in S$ are at angle 60°, the third line in their plane making an angle 60° with both is also in S. (See Figure 3.2.)

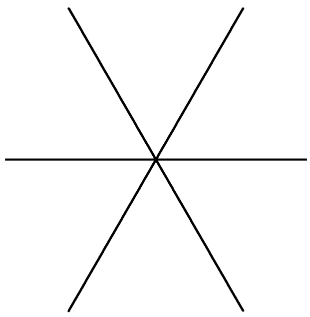


Figure 3.2: A star

Proposition 3.3 *Fix a positive number l. Then the vectors of length l in both directions along the lines of a set S form a root system if and only if the lines in S make angles* 90° *or* 60° *with each other and the set S is star-closed.*

This is hopefully obvious from the preceding remarks. We will classify the root systems by classifying the line systems with these properties instead.

If $\{\langle u\rangle, \langle v\rangle, \langle w\rangle\}$ is a star with $u+v+w=0$, then any further root is orthogonal to one or all of u, v, w. For $x.u, x.v, x.w \in \{-1,0,1\}$ and $x.u+x.v+x.w=0$.

Let A_u, A_v, A_w, B be the sets of lines spanned by roots which are orthogonal to just u, just v, just w, or all three, and choose spanning roots on these lines so that, for example, if $\langle x\rangle \in A_u$, then $x.v=+1$ and $x.w=-1$. Now form a graph G with vertex set A_u, in which two vertices are adjacent if the corresponding lines are perpendicular.

First we claim that any two spanning vectors of lines in A_u have non-negative inner product. For if x, y are two such and $x.y=-1$, then $\langle x+y\rangle \in A_u$, and $(x+y).v=2$, which forces $x+y=v$, a contradiction.

Next we claim that the graph G has the strong triangle property. For suppose that $\langle x\rangle$ and $\langle y\rangle$ are adjacent, so that $x.y=0$. Then $v-x$ and $w+y$ are roots, and $(v-x).(w+y)=1$; so $v-x-w-y=z$ is a root. Checking inner products, we find that $\langle z\rangle \in A_x$. Now $x+y+z=v-w$, and so

$$(t.x)+(t.y)+(t.z)=2$$

for all $\langle t\rangle \in A_u$. This means that exactly two of these three inner products are 1, so exactly one of the lines $\langle x\rangle$, $\langle y\rangle$ and $\langle z\rangle$ is perpendicular to $\langle t\rangle$ (and so joined to it in G).

Finally we claim that G determines the root system uniquely. For the graph structure of G determines the inner products of vectors spanning the lines in

$$\{\langle u\rangle, \langle v\rangle, \langle w\rangle\} \cup A_u;$$

and any other root can be obtained from these by closing under reflection.

Now it is readily checked that, for the root systems A_n, D_n, E_6, E_7 and E_8, the structure of the graph G is null, a Friendship graph, or one of the three exceptional graphs in Theorem 3.1. This completes the proof.

For example, take the root system A_n, and let $u=e_1-e_2$, $v=e_2-e_3$ and $w=e_3-e_1$. Then A_u consists of the lines spanned by vectors e_2-e_i for $i>3$, and no two of these are orthogonal, so G is the null graph.

3.3 Graphs with greatest eigenvalue ≤ 2

The most iconic representation of the ADE root systems is given by the famous “Coxeter–Dynkin diagrams”. Indeed, Francis Buekenhout suggested that they could be used in attempts to contact extraterrestrial civilisations, since any civilisation advanced enough to receive our transmissions has almost certainly met these ubiquitous diagrams!

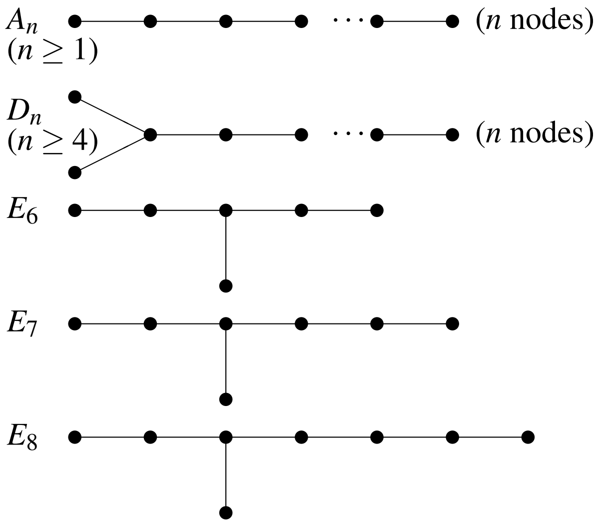


Figure 3.3: The ADE diagrams

Associated with each diagram is an “extended” diagram with one extra node: $\tilde{A}_n$ is an $(n+1)$-cycle; $\tilde{D}_n$ forks at both ends (if $n = 4$ it is a “star” with four arms); and $\tilde{E}_6$, $\tilde{E}_7$ and $\tilde{E}_8$ have arms where the numbers of edges are $(2,2,2)$, $(1,3,3)$ and $(1,2,5)$ respectively. (Add one to each of these numbers: the results should remind you of plane symmetry groups!)

I will not describe in detail how these are connected with the root systems. Here is their characterisation in graph-theoretic terms:

Theorem 3.4 *(a) A connected graph whose adjacency matrix has greatest eigenvalue less than* 2 *is a Coxeter–Dynkin diagram of type ADE, and conversely.*

(b) A connected graph whose adjacency matrix has greatest eigenvalue 2 *is an extended Coxeter–Dynkin diagram of type ADE, and conversely.*

Proof First a general observation. By the Perron–Frobenius Theorem, if G is a connected graph, then the largest eigenvalue of its adjacency matrix is a simple eigenvalue with an eigenvector having every entry positive; if the graph is regular, then the largest eigenvalue is the degree. Moreover, the only eigenvectors with every entry positive are multiples of this one.

Now show that each exteneded Dynkin diagram has largest eigenvalue 2. This is simply a case of writing down an eigenvector, that is, putting a number on each vertex such that the sum of the numbers on neighbours of v is twice the number on v. For $\tilde{A}_n$, this is easy: put 1 on each vertex. The eigenvector for $\tilde{E}_8$ is shown.

Thus, a graph with largest eigenvalue strictly less than 2 cannot contain any extended Dynkin diagram. In particular,

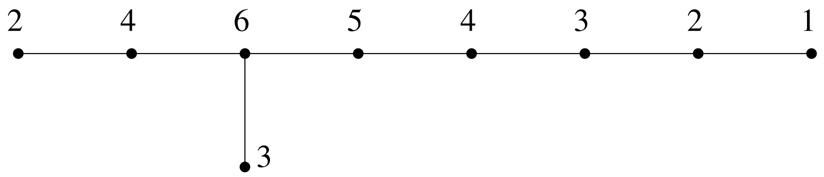


Figure 3.4: An eigenvector for $\tilde{E}_8$

- it contains no cycle, so it is a tree;
- it has no vertex of valency 4, and at most one of valency 3;
- there are restrictions on the lengths of the arms if there is a vertex of valency 3.

Only the Coxeter–Dynkin diagrams survive these conditions. This proves (a) one way round; the converse holds since these graphs are contained in the extended diagrams, which have greatest eigenvalue 2, as we saw. The proof of (b) is similar, just a little more elaborate.

The usual proof of the characterisation of ADE root systems by Cartan and Killing works by showing that such a system has a "fundamental basis", any two of whose vectors have non-positive inner product; such a basis is represented by a graph with greatest eigenvalue less than 2, and the argument above determines it.

3.4 Graphs with least eigenvalue ≥ -2

In this section, we use the classification of the root systems with all roots of the same length to determine the graphs G whose adjacency matrix $A(G)$ has least eigenvalue $A(G)$ or larger.

Note that, if G is a graph with at least one edge, then the sum of the eigenvalues of $A(G)$ is zero (the trace of $A(G)$, and hence G has both positive and negative eigenvalues. So, for non-null graphs, the smallest eigenvalue is negative.

3.4.1 Preliminaries

Theorem 3.5 *Let $A = (a_{ij})$ be a positive semidefinite real symmetric $n \times n$ matrix. Then there are vectors $v_1, \ldots, v_n \in \mathbb{R}^d$ with $v_i.v_j = a_{ij}$ for all i and j, where d is the rank of A.*

Proof From the theory of real quadratic forms we know that, if A is a real symmetric matrix, then there exists an invertible matrix P such that

$$PAP^\top = \begin{pmatrix} I_r & O & O \\ O & -I_s & O \\ O & O & O \end{pmatrix},$$

where $r+s$ and $r-s$ are the rank and signature of A. Since our matrix A is positive semidefinite, we have $s=0$, and so

$$PAP^\top = \begin{pmatrix} I_d & O \\ O & O \end{pmatrix}.$$

Put $Q = P^{-1}$. Then

$$A = Q\begin{pmatrix} I_d & O \\ O & O \end{pmatrix}Q^\top = Q_1Q_1^\top,$$

where Q_1 is the matrix consisting of the first d columns of Q. Now if v_i denotes the ith row of Q_1, the (i,j) entry of $A = Q_1Q_1^\top$ is equal to $v_i.v_j$, as required.

Here is an application, to point us in the direction we will go.

Proposition 3.6 *Let G be a connected graph with smallest eigenvalue* -1 *(or greater). Then G is a complete graph.*

Proof Let $A(G)$ be the adjacency matrix of G. By assumption, $A(G)+I$ is positive semi-definite, so there are vectors $v_1,\ldots,v_n$ with $v_i.v_j$ equal to the (i,j) entry. Thus we have

- $v_i.v_i = 1$, so v_i is a unit vector.
- if the ith and jth vertices are adjacent, then $v_i.v_j = 1$. But then $(v_i - v_j).(v_i - v_j) = 0$, and so $v_i = v_j$.

Since the graph is connected, all the vectors v_i are equal. So $v_i.v_j = 1$ for all pairs (i,j); this means that G is a complete graph.

Indeed, the complete graph K_n has eigenvalues $n-1$ (with multiplicity 1) and -1 (with multiplicity $n-1$).

3.4.2 Generalised line graphs

In this section we define generalised line graphs. The definition is due to Alan Hoffman, who proved the first version of the theorem given in the next section.

Our strategy is to represent a graph (if possible) by a set of vectors in Euclidean space, where $v_i.v_i = 2$ for all i, and

$$v_i.v_j = \begin{cases} 1 & \text{if vertices } i \text{ and } j \text{ are joined,} \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 3.7 *A graph has a Euclidean representation in the above sense if and only if its adjacency matrix has least eigenvalue -2 or greater.*

Proof Suppse the least eigenvalue of $A(G)$ has least eigenvalue -2 or greater. Then $2I + A(G)$ is positive semidefinite, and so represents the inner product of a set of vectors forming the required Euclidean representation. The other direction works in the same way.

So which graphs can be represented?

First we observe that any line graph has such a representation. Let G be a graph on n vertices $1,2,\ldots,n$. Take $e_1,e_2,\ldots,e_n$ to be an orthonormal basis for $\mathbb{R}^n$. Then, for each edge ij in the graph G, we take the vector $e_i + e_j$. It is clear that each vector has inner product 2 with itself, 1 with the vector $e_i + e_k$ representing an edge sharing a vertex with ij, and 0 otherwise; so our conditions are satisfied.

Note that the representing vectors all lie in the root system D_n.

Hoffman observed another class of graphs which are representable. The *cocktail party graph* $\mathrm{CP}(n)$ has $2n$ vertices, numbered $1,2,\ldots,2n$; every pair of vertices is joined by an edge except for the pairs $(2i-1),2i$ for $i = 1,2,\ldots,n$. (The name reflects a cocktail party attended by n couples, each person talks to everyone at the party except for his/her partner.)

The cocktail party graph can be represented in $\mathbb{R}^{n+1}$, with standard basis $e_0,e_1,\ldots,e_n$, in the following way: $2i-1 \mapsto e_0 + e_i$, $2i \mapsto e_0 - e_i$. Again we have a representation in a root system, this time D_{n+1}.

Hoffman combined these into the notion of a *generalised line graph*, defined as follows. Given a graph G with vertex set $1,2,\ldots,n$, and n non-negative integers $a_1,a_2,\ldots,a_n$, we define the graph $L(G;a_1,\ldots,a_n)$ as follows: take the disjoint union of the line graph of G with cocktail parties $\mathrm{CP}(a_1),\ldots,\mathrm{CP}(a_n)$, with some extra edges: a vertex of $L(G)$ corresponding to the edge ij in the graph G is joined to all vertices of the cocktail parties $\mathrm{CP}(a_i)$ and $\mathrm{CP}(a_j)$. Figure 3.5 shows a graph G and the generalized line graph $L(G;2,1,0,3)$.

A generalised line graph also has a Euclidean representation in the root system D_m, where $m = n + \sum_{i=1}^{n} a_i$, as follows. We label the basis $e_{i,k}$ where i runs from 1 to n, and for each i, k runs from 0 to a_i. Now for each edge ij of G, we choose the vector $e_{i,0} + e_{j,0}$ (these vectors represent the line graph of G). Then we add all edges $e_{i,0} \pm e_{i,k}$ where k runs from 1 to a_i; these represent the cocktail party $\mathrm{CP}(a_i)$, and it is easy to see that the extra edges are handled correctly as well.

Now we can state the main theorem.

Theorem 3.8 *Let G be a connected graph with least eigenvalue -2. Then either*

(a) G is a generalised line graph; or

(b) G is represented by a subset of the root system E_8.

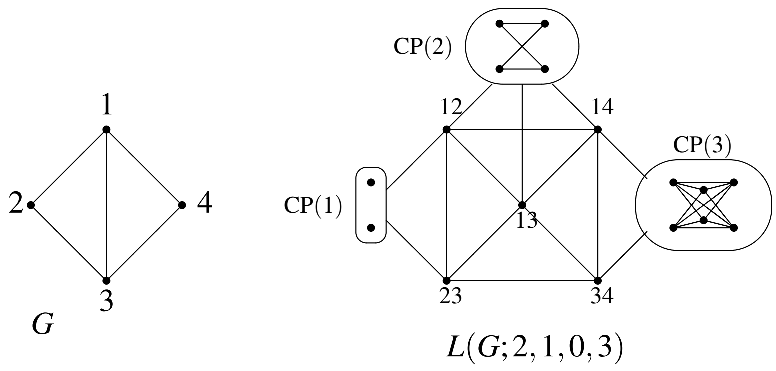


Figure 3.5: A generalised line graph

Remark In Hoffman's earlier version of the theorem, condition (b) simply said that the number of vertices of G is bounded above by a constant. In fact, it can be shown easily that a graph represented by a subset of E_8 has at most 36 vertices, and has valency at most 28; these bounds are best possible.

The proof depends on the following lemma.

Lemma 3.9 *Let S be a set of vectors in Euclidean space such that*

(a) $v.v = 2$ *for all* $v \in S$*;*

(b) $v.w \in \{-1,0,1\}$ *for all* $v,w \in S$ *with* $w \neq \pm v$.

Then S is a subset of a root system.

Proof We can adjoin to S the negatives of its vectors. Now suppose that $v,w \in S$ with $v.w = -1$. If $v+w \notin S$, we consider inner products:

- $(v+w).(v+w) = 2-2+2 = 2$.
- Take any vector $x \in S$. Then $x.(v+w) = x.v + x.w$, and each of $x.v$ and $x.w$ is in $\{-1,0,1\}$. If $x.v = x.w = 1$, then $x.(v+w) = 2$, and so

  $$(x-v-w).(x-v-w) = 2-2-2+2 = 0,$$

  so $x = v+w$, contrary to the assumption that $v+w \notin S$. A similar argument holds if $x.v = x.w = -1$. We conclude that we can add $v+w$ (and its negative) to S while preserving the hypotheses.

When this process terminates, we have a root system.

Proof of Theorem 3.8 To prove the theorem, take a graph with least eigenvalue -2 or greater. We know that it has a Euclidean representation, by a subset of a root system, and so we only need to examine the root systems. Moreover, since A_n is contained in D_{n+1}, we can assume that the root system is D_n (for some n) or E_8; so to complete the proof, we only need to examine the case where the embedding is into D_n.

So suppose G is a connected graph with a Euclidean representation as a subset of D_n. We know that the vectors in the representation have non-negative inner products with each other. In particular, a vector and its negative cannot both occur.

Suppose that both $e_i + e_j$ and $e_i - e_j$ occur in the representation. Then no other vector can involve e_j, and none can involve $-e_i$. Thus we obtain a cocktail party graph consisting of vectors $e_i \pm e_k$ for some values of k. We call the vector e_i the *index* of this cocktail party.

If we have $-e_i + e_j$ and $-e_i - e_j$, then we can change the sign of e_i to obtain a cocktail party of the previous form with index e_i.

Any other basis vector e_l occurs in only one of $\pm e_l \pm e_m$, and we may assume that it occurs with positive sign.

Then the vectors consist of a number of cocktail parties, and some vectors $e_i + e_l$ where each of e_i and e_l is either the index of a cocktail party of one of the additional vectors (which could be regarded as indices of empty cocktail parties). So we have reconstructed the graph, and it is a generalised line graph. (In detail, take the vertices of the graph G to be the indices of the cocktail parties, including trivial indices of empty cocktail parties; edges of G have the form il, where $v_i + v_l$ is a vector in our set. Now we have precisely the representing set of the generalised line graph $L(G; a_1, \ldots)$, where $\mathrm{CP}(a_i)$ is the cocktail party whose index is the ith vertex of G.)

Many characterisations of graphs by their eigenvalues can be deduced from this theorem. Here is an example, a theorem of Hoffman and Ray-Chaudhuri. (Originally, the theorem originally said "A sufficiently large connected regular graph ... is a line graph or a cocktail party graph".)

Theorem 3.10 *A connected regular graph whose ajacency matrix has least eigenvalue -2 or greater is a line graph, a cocktail party graph, or is represented by a subset of E_8.*

Proof All we need to do is to show that a generalised line graph cannot be regular unless it is either a line graph or a cocktail party graph. So consider a generalised line graph $L(G; a_1, \ldots, a_n)$, which has an edge ij and has $a_i > 0$. Let d_i and d_j be the valencies of i and j in G. Then the vertex corresponding to the edge ij has valency $(d_i - 1) + (d_j - 1) + 2a_i + 2a_j$, whereas a vertex in $\mathrm{CP}(a_i)$ has valency

$(2a_i - 2) + d_i$. These differ by $d_j + 2a_j$, where $d_j \geq 1$, a contradiction. So either G has one vertex and no edges (and we have just a cocktail party graph), or $a_i = 0$ for all i (and we have a line graph). The regular graphs represented by subsets of E_8 have been classified by Bussemaker, Cvetkovič and Seidel. There are 187 such graphs which are not line graphs or cocktail party graphs.

Another example is an even earlier theorem of Seidel (which, however, included a classification of all the exceptional graphs: there are exactly seven of them, the smallest being the Petersen graph). Seidel's theorem extended earlier results by Hoffman, Chang and Shrikhande. Indeed, the Shrikhande and Chang graphs we met earlier are represented in the root system E_8, as well as the other exceptions (the Petersen, Clebsch and Schläfli graphs).

Theorem 3.11 *A strongly regular graph whose adjacency matrix has least eigenvalue -2 is isomorphic to $L(K_m)$, $L(K_{m,m})$, or* $\mathrm{CP}(m)$*, or is one of finitely many exceptions.*

The theorem in this form now follows if we can show that the only strongly regular line graphs are $L(K_m)$, $L(K_{m,m})$, and $L(C_5) \cong C_5$; this is an exercise.

3.5 The other root systems

In addition to the root systems of types A_n, D_n, E_6, E_7 and E_8, there are further indecomposable root systems where roots can have different lengths.

Note that, if u and v are roots, with $v \neq \pm u$, then $2(u.v)/(u.u)$ and $2(u.v)/(v.v)$ are integers; their product is $4(u.v)^2/(u.u)(v.v)$, which is strictly less than 4, by the Cauchy–Schwarz inequality. So this product is 0, 1, 2 or 3. This means that, assuming v is longer than u, we have $|v| = \sqrt{2}|u|$ or $|v| = \sqrt{3}|u|$. In particular, we see that only two different lengths can occur, and they are in the ratio $\sqrt{2}$ or $\sqrt{3}$.

Now in such a mixed root system, the roots of fixed length form a root system (since reflections map them to themselves); this root system must be an orthogonal direct sum of root systems of type ADE. A little more thought shows that the possibilities are:

- two copies of A_2, length ratio $\sqrt{3}$ (this gives type G_2);
- a copy of D_n together with an orthonormal basis, length ratio $\sqrt{2}$ or $1/\sqrt{2}$ (this gives types B_n and C_n);
- two copies of D_4, length ratio $\sqrt{2}$ (this gives type F_4).

Thus we have the complete classification. B_2 and G_2 are shown below.

The root system F_4 can be represented (in terms of an orthonormal basis e_1, e_2, e_3, e_4) by the vectors

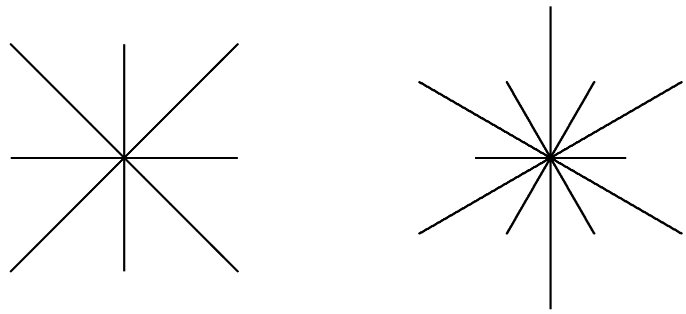


Figure 3.6: The root systems B_2 and G_2

- $\pm e_1$, $\pm e_2$, $\pm e_3$, $\pm e_4$ (8 vectors);
- $\pm e_i \pm e_j$ ($i \neq j$) (24 vectors);
- $(\pm e_1 \pm e_2 \pm e_3 \pm e_4)/2$ (16 vectors).

These root systems also have applications to spectral graph theory. A theorem of Whitney asserts that graphs G and G' on more than four vertices which have isomorphic line graphs must themselves be isomorphic. (An exception on four vertices is given by the two graphs in Figure 3.7.

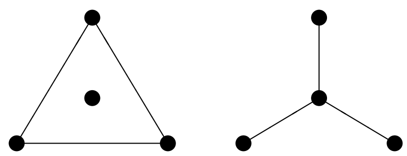


Figure 3.7: Graphs with isomorphic line graphs

This theorem can be extended to generalised line graphs. If $L(G;a_1,\ldots,a_n)$ and $L(H;b_1,\ldots,b_m)$ are isomorphic, and $n+\sum a_i > 4$, then G is isomorphic to H, so $m = n$, and $a_i = b_i$ for $i = 1,\ldots,n$.

This is proved by representing the edge set of a generalised line graph by a subset of a root system of type D_n as before. Now vertices correspond to unit vectors having inner product 0 or ± 1 with all the vectors of D_n. If $n > 4$, then adding in these vectors gives a root system of type B_n, and the vertices are uniquely defined. The exceptional cases correspond to the exceptional root system F_4.

Exercise In $\mathbb{R}^4$, with orthonormal basis $\{e_1,e_2,e_3,e_4\}$, the vectors $e_i + e_j$, for $1 \leq i < j \leq 4$, represent $L(K_4)$. Find another orthonormal basis f_1, f_2, f_3, f_4 relative to which these vectors have the form $f_1 \pm f_k$ f or $k = 2,3,4$ (representing $\mathrm{CP}(3) = L(K_1;3)$).

CHAPTER 4

Polar spaces

4.1 Vector spaces over GF(2)

Vector spaces over the field of two elements are particularly easy to recognise and pleasant to work in. If X denotes a basis for such a vector space, then an arbitrary vector v has coordinates 0 and 1 relative to X, and so defines a subset of X, the set of basis vectors which occur with coefficient equal to 1. The correspondence between the vector space and the power set of X is a bijection; addition of vectors corresponds to symmetric difference of subsets.

The projective space based on such a vector space is also easy to recognise. In general, the points and lines of the projective space based on a vector space V correspond to the 1-dimensional and 2-dimensional subspaces of V. Over GF(2), a 1-dimensional space has the form $\{0, v\}$ for some non-zero vector v, so points can be identified with elements of $V \setminus \{0\}$; any 2-dimensional subspace has the form $\{0, u, v, w\}$, where $w = u + v$, and so the lines can be identified with the triples of points having sum 0.

The Veblen–Young characterisation of projective space is also very simple.

Theorem 4.1 *An incidence structure of points and lines is a projective space over* GF(2) *if and only if it satisfies the following:*

(a) *any line contains exactly three points;*

(b) *two points lie on a unique line;*

(c) *if a line meets two sides of a triangle, not at a vertex, then it meets the third side also (see Figure 4.1).*

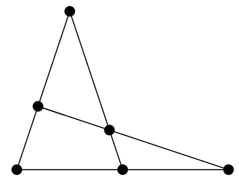


Figure 4.1: Veblen–Young axiom (c)

Proof To prove the theorem we have to reconstruct the vector space. The obvious way to do this is to define $V = P \cup \{0\}$, where P is the point set and 0 a new symbol; then define addition by

$$v+0=0+v=v, \quad v+v=0, \quad u+v=w \text{ if } \{u,v,w\} \text{ is a line,}$$

and scalar multiplication by

$$0.v = 0 \qquad 1.v = v,$$

and prove that this is a vector space over GF(2). The only thing that is not obvious is the associative law, which follows from condition (c).

However, I will give a different proof, which is a gentle introduction to the argument (of Jonathan Hall) we use later to recognise polar spaces over GF(2).

Let $\hat{V}$ be the vector space of functions from P to GF(2). This space has a basis consisting of the characteristic functions $\hat{x}$ of singleton subsets $\{x\}$ of P. Now let R be the subspace of $\hat{V}$ spanned by all vectors of the form $\hat{u}+\hat{v}+\hat{w}$, where $\{u,v,w\}$ is a line of the projective space, and $V = \hat{V}/R$. Let $\bar{x}$ be the image of $\hat{x}$ in V. We are going to show that

- the map $P \to V$ given by $x \mapsto \bar{x}$ is one-to-one, and its image is $V \setminus \{0\}$, where 0 is the zero of V;
- $\bar{u}+\bar{v}+\bar{w} = 0$ if and only if $\{u,v,w\}$ is a line.

The result will follow.

We show that, if S is a set of points with $\sum\{\bar{v} : v \in S\} = 0$, then $|S| \geq 3$, with equality if and only if S is a line. This clearly establishes the second point above. Suppose that it holds. Then clearly $\bar{x} \neq 0$ and $\bar{x}+\bar{y} \neq 0$ for all distinct x,y, so the first point holds too.

If a set S has sum zero as above, and two points x,y belong to S, then either the third point z on the line through xy belongs to S, or we can replace x and y by z to get a smaller set. So we may assume that $|S| = 1$, say $S = \{v\}$. Now $\bar{v} = 0$ means that there is a set $\mathscr{L}$ of lines such that the sum of the corresponding spanning vectors of R is $\hat{v}$; that is, v lies on an odd number of lines of $\mathscr{L}$ and every other point on an even number. Suppose that, subject to this, $|\mathcal{L}|$ is minimal. Then there is no triangle formed by lines of $\mathcal{L}$ (since we could replace $\{a,b,z\}$, $\{a,c,y\}$, $\{b,c,x\}$ by $\{x,y,z\}$, which is a line by the VY axiom).

The set $\mathcal{L}$ must contain a cycle. But any cycle can be shortened, which contradicts the fact that there are no triangles. For suppose that $\{a,b,c\}$, $\{c,d,e\}$, $\{e,f,g\}$ and $\{g,h,i\}$ are lines in $\mathcal{L}$. Let $\{c,g,j\}$ be the line on c and g. Then $\{d,f,j\}$ is a line; replacing $\{c,d,e\}$ and $\{e,f,g\}$ by $\{c,g,j\}$ and $\{d,f,j\}$ gives a shorter cycle, as claimed.

4.2 Quadratic and bilinear forms

Let V be a vector space over a field F. A *bilinear form* B on V is a function from $V \times V$ to F, which is linear in each variable (the other being fixed): that is,

$$\begin{array}{ll} B(v_1+v_2,w) = B(v_1,w)+B(v_2,w), & B(cv,w) = cB(v,w), \\ B(v,w_1+w_2) = B(v,w_1)+B(v,w_2), & B(v,cw) = cB(v,w) \end{array}$$

for all $v,\ldots, \in V$ and $c \in F$.

A bilinear form B has a left and a right radical, defined by

$$\begin{array}{rcl} L_B & = & \{v \in V : (\forall w \in V) B(v,w) = 0, \\ R_B & = & \{w \in V : (\forall v \in V) B(v,w) = 0. \end{array}$$

If V is finite-dimensional, the radicals have the same dimension. We say that B is *non-degenerate* if they are equal to $\{0\}$.

A bilinear form B is *reflexive* if $B(v,w) = 0$ if and only if $B(w,v) = 0$. Clearly the left and right radicals of a reflexive form are equal.

Theorem 4.2 *A non-degenerate reflexive bilinear form is either*

- symmetric*, that is,* $B(v,w) = B(w,v)$ *for all* $v,w \in V$*; or*
- alternating. *that is,* $B(v,v) = 0$ *for all* $v \in V$.

Note that, if B is alternating, then expanding $B(v+w,v+w) = 0$ we find that $B(v,w) = -B(w,v)$. In particular,

- if the characteristic of F is not 2, then only the zero form is both symmetric and alternating;
- if the characteristic is 2, then an alternating form is symmetric.

Non-degenerate alternating bilinear forms can be defined on V if and only if the dimension of V is even.

A *quadratic form* on a vector space V over F is a function $Q : V \to F$ satisfying the conditions

- $Q(cv) = c^2 Q(v)$ for all $c \in F$, $v \in V$;
- the function $B(v,w) = Q(v+w) - Q(v) - Q(w)$ is bilinear.

The bilinear form B is said to be obtained by *polarisation* of Q.

The behaviour depends on the characteristic of F:

- If the characteristic of F is not 2, then B is a symmetric bilinear form, and Q can be recovered from B by $Q(v) = \frac{1}{2}B(v,v)$.
- If the characteristic of F is 2, then B is an alternating bilinear form, and Q is not recoverable from Q.
- In the special case where F has two elements, the set of quadratic forms which polarise to a given alternating bilinear form is a coset of the space of linear forms on V (the dual space of V), so there are 2^n such quadratic forms, where $n = \dim(V)$.

A quadratic form Q (which polarises to B) is said to be *non-singular* if $Q(v) = 0$ and $B(v,w) = 0$ for all $w \in V$ imply $v = 0$. If the characteristic is not 2, then Q is non-singular if and only if B is non-degenerate. However, if the characteristic is 2, then it may happen that B has 1-dimensional radical and Q is non-zero on the nonzero vectors of the radical. Indeed, in the case where $|F| = 2$, the restriction of Q to the radical of B is a linear function, so its kernel has codimension 1; thus, for a non-singular form, the radical has dimension at most 1.

We conclude this brief survey with a result about defining forms by their values on a basis.

Proposition 4.3 *Let V be a vector space with basis $\{e_1, \ldots, e_n\}$.*

(a) We can define a bilinear form B on V by specifying the values $B(e_i, e_j)$ for $1 \le i, j \le n$.

(b) In characteristic 2, if we specify $B(e_i, e_i) = 0$ for all i and $B(e_i, e_j) = B(e_j, e_i)$ for all i, j, then B is alternating.

(c) In characteristic 2, given an alternating bilinear form B, we can define a quadratic form Q polarising to B by specifying the values $Q(e_i)$ for $1 \le i \le n$.

Proof (a) Given B on a basis, we define

$$B\left(\sum_i x_i e_i, \sum_j y_j e_j\right) = \sum_i \sum_j x_i y_j B(e_i, e_j).$$

(b) If $B(e_i, e_i) = 0$ for all i and the characteristic is 2, then

$$B\left(\sum_i x_i e_i, \sum_i x_i e_i\right) = 2 \sum_{i<j} x_i x_j B(e_i, e_j) = 0$$

because of the factor 2.

(c) Given the values of $Q(e_i)$, we have

$$Q(x_i e_i + x_j e_j) = x_i^2 Q(e_i) + x_y^2 Q(e_j) + x_i x_j B(e_i, e_j),$$

and similarly we extend Q to linear combinations of more than two basis vectors.

4.3 The Triangle Property

In this section, we give a generalisation of Theorem 3.1, the classification of graphs with the strong triangle property.

Theorem 4.4 *Let G be a graph with the triangle property. Then one of the following holds:*

(a) G is a null graph;

(b) there is a vertex of Γ joined to all others;

(c) G is the graph associated with a non-singular formed space over GF(2).

The theorem is due to Shult, with a refinement by Seidel. The proof given here is by Jonathan Hall: with small modifications it works for infinite graphs as well as finite ones.

Proof The null graph clearly satisfies the hypotheses; so we may assume that G is not null. We also assume that (b) does not hold, that is, there is no vertex joined to all others.

It follows from this assumption that, given an edge $\{u, v\}$, the third vertex w specified in the triangle property is unique. For suppose that the triangles $\{u, v, x\}$ and $\{u, v, y\}$ both satisfy the conditions of the triangle property. Then y is joined to u and v, and so also with x; so there is a triangle $\{x, y, z\}$ for some z, and both u

and v are joined to z. Any further point is joined to both or neither x and y, and so is joined to z, contradicting the assumption.

Let X be the vertex set of the graph G, and let $F = \mathrm{GF}(2)$. We begin with the vector space $\hat{V}$ of all functions from X to F, with pointwise operations. Let $\hat{x} \in \hat{V}$ be the characteristic function of the singleton set $\{x\}$. The functions $\hat{x}$, for $x \in X$, form a basis for $\hat{V}$. We define a bilinear form $\hat{B}$ on $\hat{V}$ by setting

$$\hat{B}(\hat{x},\hat{y}) = \begin{cases} 0 & \text{if } x = y \text{ or } x \text{ is joined to } y, \\ 1 & \text{otherwise,} \end{cases}$$

and extending linearly. Then we define a quadratic form $\hat{Q}$ by setting $\hat{Q}(\hat{x}) = 0$ for all $x \in X$ and extending to $\hat{V}$ by the rule

$$\hat{Q}(v+w) = \hat{Q}(v) + \hat{Q}(w) + \hat{B}(v,w).$$

Note that both $\hat{B}$ and $\hat{Q}$ are well-defined, by our remarks before the theorem.

Let R be the *radical* of $\hat{Q}$; that is, R is the *subspace*

$$\{v \in \hat{V} : \hat{Q}(v) = 0,\ \hat{B}(v,w) = 0 \text{ for all } w \in \hat{V}\},$$

and set $V = \hat{V}/R$. Then $\hat{B}$ and $\hat{Q}$ induce bilinear and quadratic forms B, Q on V: for example, we have $Q(v+R) = \hat{Q}(v)$ (and this is well-defined, that is, independent of the choice of coset representative). Now let $\bar{x} = \hat{x} + R \in V$.

We claim that the embedding $x \mapsto \bar{x}$ has the required properties; in other words, it is one-to-one; its image is the set of singular points of Q; and two vertices x, y are adjacent if and only if the corresponding vectors $\bar{x}, \bar{y}$ are orthogonal. We proceed in a series of steps.

Step 1 *Let $\{x,y,z\}$ be a special triangle, as in the statement of the triangle property. Then $\bar{x}+\bar{y}+\bar{z} = 0$.*

It is required to show that $r = \hat{x}+\hat{y}+\hat{z} \in R$. We have

$$\hat{B}(r,\hat{v}) = \hat{B}(\hat{x},\hat{v}) + \hat{B}(\hat{y},\hat{v}) + \hat{B}(\hat{z},\hat{v}) = 0$$

for all $v \in X$, by the triangle property; and

$$\hat{Q}(r) = \hat{Q}(\hat{x}) + \hat{Q}(\hat{y}) + \hat{Q}(\hat{z}) + \hat{B}(\hat{x},\hat{y}) + \hat{B}(\hat{y},\hat{z}) + \hat{B}(\hat{z},\hat{x}) = 0$$

by definition.

Step 2 *The map $x \mapsto \bar{x}$ is one-to-one on X.*

Suppose that $\bar{x} = \bar{y}$. Then $r = \hat{x} + \hat{y} \in R$. Hence $\hat{B}(\hat{x},\hat{y}) = 0$, and so x is joined to y. Let z be the third vertex of the special triangle containing x and y. Then $\hat{z} = \hat{x} + \hat{y} \in R$ by Step 1, and so z is joined to all other points of X, contrary to assumption.

Step 3 *Any quadrangle is contained in a* 3×3 *grid.*

Let $\{x,y,z,w\}$ be a quadrangle. Letting $\overline{x+y}=\bar{x}+\bar{y}$, etc., we see that $x+y$ is not joined to z or w, and hence is joined to $z+w$. Similarly, $y+z$ is joined to $w+x$; and the third point in the special triangle through each of these pairs is $x+y+z+w$, completing the grid. (See Fig. 4.2.)

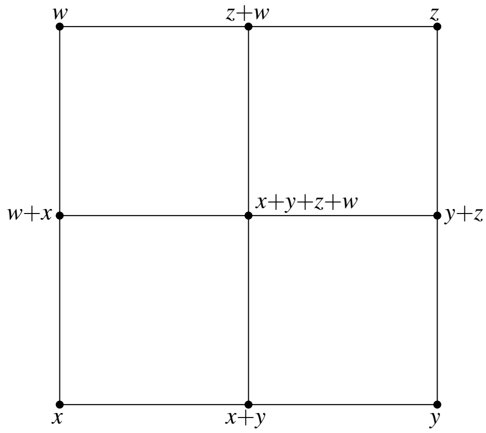


Figure 4.2: A grid

Step 4 *For any* $v\in V$*, write* $v=\sum_{i\in I}\bar{x}_i$*, where* $x_i\in X$*, and the number* $m=|I|$ *of summands is minimal (for the given* v*). Then*

(a) $m\leq 3$*;*

(b) the points x_i *are pairwise non-adjacent.*

This is the crucial step, and needs four sub-stages.

Substep 4.1 *Assertion (b) is true.*

If $x_i\sim x_j$, we could replace $\bar{x}_i+\bar{x}_j$ by the third point $\bar{x}_k$ of the special triangle, and obtain a shorter expression.

Substep 4.2 *If* T *is a special triangle containing* x_1*, and* y *a point of* T *which is adjacent to* x_2*, then* $y\sim x_i$ *for all* $i\in I$*.*

If not, let $T=\{x_1,y,z\}$, and suppose that $x_i\sim z$. Then x_i is joined to the third point w of the special triangle on x_2y. Let u be the third point of the special triangle on x_iw. Then $\bar{z}=\bar{x}_1+\bar{y}$, and $\bar{u}=\bar{w}+\bar{x}_i=\bar{y}+\bar{x}_2+\bar{x}_i$; so we can replace $\bar{x}_1+\bar{x}_2+\bar{x}_i$ by the shorter expression $\bar{z}+\bar{u}$.

Substep 4.3 *There are two points y, z joined to all x_i.*

Each special triangle on x_1 contains a point with this property, by Substep 4.2. It is easily seen that if x_1 lies in a unique special triangle, then one of the points on this line is adjacent to all others, contrary to assumption.

Substep 4.4 $m \leq 3$.

Suppose not. Considering the quadrangles $\{x_1, y, x_2, z\}$ and $\{x_3, y, x_4, z\}$, we find (by Step 3) points a and b with

$$\bar{x}_1 + \bar{y} + \bar{x}_2 + \bar{z} = \bar{a}, \qquad \bar{x}_3 + \bar{y} + \bar{x}_4 + \bar{z} = \bar{b}.$$

But then $\bar{x}_1 + \bar{x}_2 + \bar{x}_3 + \bar{x}_4 = \bar{a} + \bar{b}$, a shorter expression.

Step 5 *If $v \in V$, $v \neq 0$, and $Q(v) = 0$, then $v = \bar{x}$ for some $x \in X$.*

If not then, by Step 4, either $v = \bar{x} + \bar{y}$, or $v = \bar{x} + \bar{y} + \bar{z}$, where points x, y (and z) are (pairwise) non-adjacent. In the second case,

$$Q(v) = Q(\bar{x}) + Q(\bar{y}) + Q(\bar{z}) + B(\bar{x}, \bar{y}) + B(\bar{y}, \bar{z}) + B(\bar{z}, \bar{x}) = 0 + 0 + 0 + 1 + 1 + 1 = 1.$$

The other case is similar but easier.

Step 6 *$x \sim y$ if and only if $B(\bar{x}, \bar{y}) = 0$.*

This is true by definition, since $B(\bar{x}, \bar{y}) = \hat{B}(\hat{x}, \hat{y})$.

4.4 The Buekenhout–Shult Theorem

This section describes a wide generalisation of the material in the preceding section. I will give only a general description, with no proofs. Also we will consider only finite fields. (Additional complications arise in the infinite case!)

We met vector spaces carrying various kinds of forms (non-degenerate alternating bilinear forms, or non-singular quadratic forms). There is a third kind of form to be considered in conjunction with these, non-degenerate *Hermitian forms*. Such a form is *sesquilinear*, that is, linear in the first variable and semilinar in the second (this means there is an associated field automorphism σ such that

$$B(v, w_1 = w_2) = B(v, w_1) + B(v, w_2), \qquad B(v, cw) = c^\sigma B(v, w).$$

We pause to recall that the automorphism group of a finite field of order $q = p^r$ (wherer p is prime) is cyclic of order n, generated by the *Frobenius map* $x \mapsto x^p$.

A Hermitian form is a non-degenerate (that is, radical is zero) sesquilinear form satisfying $B(w, v) = B(v, w)^\sigma$, where σ is the associated field automorphism. It is immediate that $\sigma^2 = 1$, so that $q = q_0^2$ and σ is the map $x \mapsto x^{q_0}$.

Now alternating bilinear forms, quadratic forms, and Hermitian forms can be treated together. The geometry associated with such a form is called a *polar space*; its points, lines, ..., are the points, lines, ... of the projective space which are *totally isotropic* (in the case of bilinear or Hermitian forms) or *totally singular* (for quadratic forms), that is to say, the form vanishes on the subspace. The maximum vector space dimension of such a subspace is called the *Witt index* of the space. If the Witt index is r, then the vector space dimension n of V is at least $2r$, and is at most $2r+2$ (in the case of a quadratic form), $2r+1$ (for a Hermitian form), and $2r$ (for an alternating form). Thus there are six kinds of polar space. Those coming from a quadratic form are called *quadrics*, and are *elliptic*, *parabolic* or *hyperbolic* according as $n = 2r+2$, $n = 2r+1$, or $n = 2r$. (Remember that the geometric dimension is $n-1$.)

Now with a polar space we associate a graph as follows: the vertices are the points of the polar space; two vertices are joined if and only if they are orthogonal with respect to the sesquilinear form, that is, they are contained in a totally isotropic or totally singular line.

The *Buekenhout–Shult* theorem gives a unified characterisation of all these polar spaces, in the finite case, in terms of this graph.

Theorem 4.5 *Let G be a finite graph with the property that any edge of G is contained in a clique (a complete subgraph) C with $|C| > 2$ such that any vertex outside C is joined to one or all points of C. Then one of the following holds:*

- *G is a null graph;*
- *G has a vertex which is joined to all other vertices;*
- *G is the graph associated with a non-degenerate polar space.*

(Note that the polar spaces here include generalised quadrangles, which we will consider in the next section.)

Note how this theorem is a natural generalisation of the characterisation of graphs with the triangle property. Unlike that theorem, in this case the vector space is not constructed directly from the graph, but instead the entire polar space is reconstructed, and a theorem of Veldkamp and Tits is used to recognise it.

Note also that there is a version of the theorem not assuming finiteness. It is necessary to assume finite rank (that is, chains of subspaces, suitably defined, are required to be finite), and also there are some other types of spaces which have to be added to the list.

For an example of this, the lines in the 3-dimensional vector space over a field F carry the structure of a graph satisfying the hypothesis. (There are two types of cliques: the set of lines in a plane, and the set of lines in the pencil through a point. The hypothesis is easily checked.) If F is commutative, then this is isomorphic to the Klein quadric in 5-dimensional projective space. However, infinite fields need not be commutative. (A finite field is necessarily commutative, by Wedderburn's theorem.)

4.5 Generalised quadrangles

Generalised quadrangles form the "low-dimensional case" in the Buekenhout–Shult theorem just as projective planes do in the Veblen–Young theorem.

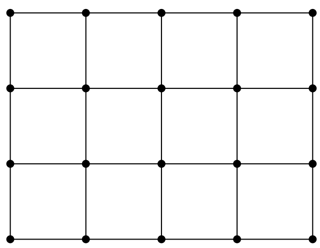
A *generalised quadrangle* is a geometry of *points* and *lines* having the properties

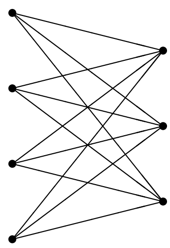
(a) two points lie on *at most* one line;

(b) given a line L and point p not on L, there is a unique point q on L collinear with p;

(c) any point lies on at least two lines, and any line contains at least two points.

This still allows some examples which, while not so silly, are not so interesting either:





The first example, a *rectangular grid*, has two lines through each point, but some lines have four points while others have five. The second example, a *complete bipartite graph*, has two points on each line, but some points lie on four lines and others on three.

It can be shown (I won't give the proof here) that it is the presence of lines with two points, or points on two lines, which allow this behaviour:

Theorem 4.6 *Suppose that a generalised quadrangle $\mathcal{Q}$ has at least three points on any line and at least three lines through any point. Then there are numbers (finite or infinite) s and t such that any line has $s+1$ points and any point lies on $t+1$ lines.*

Accordingly, we make a definition:

Definition A generalised quadrangle $\mathcal{Q}$ *has parameters* (s,t) if every line has $s+1$ points and every point lies on $t+1$ lines.

Thus we see that a rectangular grid has parameters if and only if it is square; and a complete bipartite graph has parameters if and only if the two parts of the partition have equal size. Any generalised quadrangle not of one of these forms necessarily has parameters.

There is a famous open problem here. Can we have a generalised quadrangle with parameters (s,t), where s is finite and $s>1$, while t is infinite? It is known that this is not possible for $s=2$, $s=3$, and $s=4$, though the arguments for the three cases are very different and the degree of difficulty increases rapidly. For larger values of s, the problem is open. We will look at the case $s=2$ shortly.

Theorem 4.7 *Let $\mathcal{Q}$ be a generalised quadrangle with parameters (s,t). Then*

(a) The number of points in $\mathcal{Q}$ is $(s+1)(st+1)$, and the number of lines is $(t+1)(st+1)$.

(b) The point graph *of $\mathcal{Q}$, whose vertices are the points of $\mathcal{Q}$, two vertices adjacent if they are collinear, is strongly regular, with parameters $((s+1)(st+1),(t+1)s,s-1,t+1)$.*

(c) A dual statement (with s and t exchanged) holds for the line graph *of $\mathcal{Q}$, whose vertices are the lines, two vertices adjacent if they intersect in a point.*

Proof We prove (a) and (b) together. Take a point p, and let $A(p)$ be the set of points collinear with p and $B(p)$ the set not collinear. Then p lies on $t+1$ lines, each with s further points, and there are no overlaps among these points; so $|A(p)|=(t+1)s$ is the number of neighbours of p.

Each neighbour q of p is joined to the $s-1$ further points on the line pq, and to no other points in $A(p)$ (since the geometry contains no triangles). So there are $(t+1)s-1-(s-1)=ts$ edges from q to points in $B(p)$. On the other hand, each point $r\in B(p)$ is joined to one point on each of the $t+1$ lines containing p; so p and r have $t+1$ common neighbours. This shows the strong regularity of the graph, and gives the stated parameters. Also, counting edges from $A(p)$ to $B(p)$, we have

$$|A(p)|\cdot st=|B(p)|\cdot(t+1),$$

and using $|A(p)|=(t+1)s$ we get $|B(p)|=s^2t$. So the total number of vertices is $1+(t+1)s+s^2t=(s+1)(st+1)$, as required.

Part (c) is proved (and the number of lines counted) by a similar argument with the roles of points and lines reversed, or more simply by observing that the *dual* of $\mathcal{Q}$ (the geometry whose points are the lines of $\mathcal{Q}$ and whose lines are the pencils of lines of $\mathcal{Q}$ through a point, is a generalised quadrangle with parameters (t,s).

We now turn our attention to the case $s = 2$.

Theorem 4.8 *Let $\mathcal{Q}$ be a (possibly degenerate) generalised quadrangle with three points on any line. Then the point graph of $\mathcal{Q}$ has the strong triangle property. Hence, if $\mathcal{Q}$ has parameters $(2,t)$, then $t = 1$, 2 or 4.*

Proof A line in $\mathcal{Q}$ corresponds to a triangle in the point graph; the second axiom for a generalised quadrangle shows that any further vertex is joined to a unique vertex in such a triangle. Thus the Strong Triangle Property holds. So the graph is null, a Friendship graph, or one of our three exceptions. The null and Friendship graphs are degenerate (the first has no lines, and the second has points lying on only one line); the other three cases give the three values of t in the theorem.

Remark A generalised quadrangle with three points on a line is equivalent to a graph with the strong triangle property. We saw while discussing that theorem that necessarily $t = 1$, 2 or 4.

More generally, it is known that the parameters (s,t) of a generalised quadrangle satisfy $t \leq s^2$ if $s > 1$, and dually $s \leq t^2$ if $t > 1$ (provided that s and t are finite!).

There is a rather limited range of parameters for which generalised quadrangles are known to exist. The following list includes all known examples. In the list, q denotes a prime power.

- $s = 1$ (regular complete bipartite graphs);
- $t = 1$ (square grids);
- $(s,t) = (q,q)$, (q,q^2), (q^2,q), (q^2,q^3), $q^3,q^2)$;
- $(s,t) = (q-1,q+1)$ or $(q+1,q-1)$.

4.6 Generalised polygons

Generalised polygons are a class of geometries introduced by the Belgian geometer Jacques Tits (winner of the Abel prize along with John Thompson a few years ago). They bear a similar relation to a more general class of things called *buildings* as projective planes do to projective spaces.

We now work towards the definition of a generalised n-gon, via a short detour.

We have several times considered structures with points and lines, or points and blocks. Sometimes (as with projective planes) we have considered a dual object, where lines become points and points become lines. We need a way of thinking about these which treats points and lines on the same footing.

An *incidence structure*, then, is a structure with points and lines, and an "incidence relation" between points and lines. If a point and a line are incident, we use the usual geometric language by saying that the point lies on the line. By doing this, we are implicitly thinking of a line as being identified with a set of points (namely, the points incident with it). But the incidence structure language tries to avoid doing this.

The *incidence graph*, or *Levi graph*, of an incidence structure $\mathscr{S}$ is the bipartite graph whose vertices are the points and lines of $\mathscr{S}$, with an edge between a point and a line if they are incident.

We can regard an ordinary n-gon as an incidence structure with n points and n lines. Its incidence graph is a $2n$-gon. (Point vertices are drawn as solid circles and line vertices as hollow squares.)

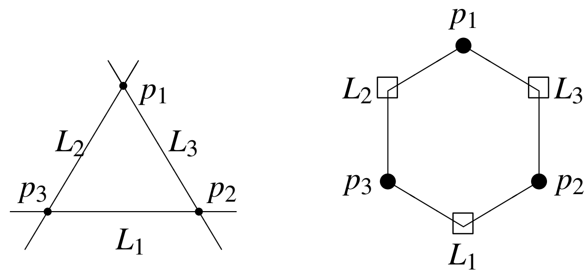


Figure 4.3 shows the incidence graph of the Fano plane: it has fourteen vertices, seven points and seven lines.

Recall that the *diameter* of a graph is the largest distance between two vertices, while the *girth* is the length of the shortest cycle. In a bipartite graph, any cycle has even length (since the vertices alternate between the two parts of the bipartition). So in a bipartite graph of diameter d in which all vertices have valency at least 2, the girth cannot be larger than $2d$. Note that

- if the incidence graph has girth 6 or greater, then two points lie on at most one line – for two points incident with two lines would be represented as a 4-cycle in the incidence graph;
- if the incidence graph has diameter 3 or less, then two points lie on at least one line – for two point vertices have even distance in the incidenc graph, necessarily 2, and so some line vertex is joined to both.

Definition A *generalised n-gon* is a geometry whose incidence graph has diameter n and girth $2n$, and all of its vertices have valency at least 2.

Theorem 4.9 *A generalised* 3*-gon is a (possibly degenerate) projective plane. (The allowed degenerate cases have all but one point on a single line; this includes the case of an ordinary triangle as shown above.)*

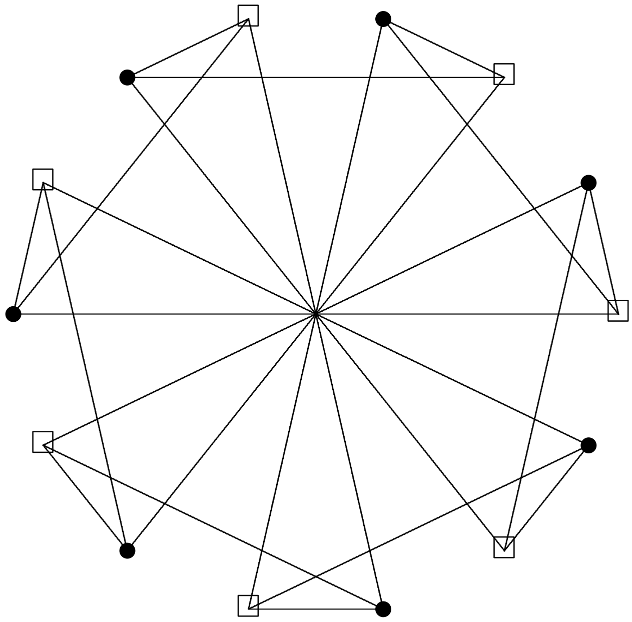


Figure 4.3: The incidence graph of the Fano plane

Proof The incidence graph of a generalised 3-gon has diameter 3 and girth 6. As we observed above, this means that two points lie on a unique line, and dually two lines meet in a unique point.

Go back to Figure 4.3 and check that the graph drawn there really does have diameter 3 and girth 6.

As a generalisation of our earlier theorem, if every vertex of the incidence graph has degree at least 3, then the geometry has *parameters* (s,t), in the sense that any line has $s+1$ points and any point lies on $t+1$ lines. However, we don't forbid one or both of the parameters to be 1.

Example A projective plane of order n is a generalised 3-gon with parameters (n,n).

Example An ordinary n-gon is a generalised n-gon with parameters $(1,1)$, and conversely.

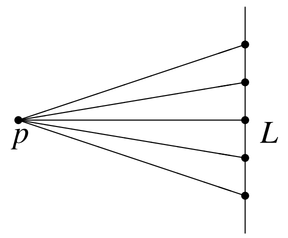
For "parameters $(1,1)$" mean that the incidence graph has valency 2, and so is a cycle; and the definition of a generalised n-gon shows that it must be a $2n$-cycle.

Example Our earlier definition of generalised quadrangles coincides with the new definition of generalised 4-gons.

Proposition 4.10 *If a generalised n-gon with n odd has parameters (s,t), then $s=t$.*

Proof Take two vertices at maximum distance in the incidence graph. One is a point p, and the other a line L. Now any point on L has a unique path to p of length $n-1$, whose penultimate step is a line on p; and in reverse, any line on p has a unique path to L of length $n-1$, whose penultimate step is a point on L. So there is a bijection between lines through p and points on L.

The diagram shows the case $n=3$. The lines through p are matched to the points on L by incidence. Note that this case refers to projective planes, which we have seen before.



The most important theorem about generalised polygons is the *Feit–Higman Theorem*, proved in 1964.

Theorem 4.11 *A finite generalised n-gon $\mathcal{G}$ with $n \geq 3$ and parameters (s,t) can exist only in the following cases:*

(a) $s=t=1$ *($\mathcal{G}$ is an ordinary n-gon);*

(b) $n=3$, 4, 6, 8 *or* 12 *(and if $n=12$, then $s=1$ or $t=1$).*

The proof uses the eigenvalue techniques we have used often in this course. I will prove one special case of the theorem.

Theorem 4.12 *A generalised 5-gon with parameters (s,t) exists only if $s=t=1$.*

Proof Suppose that $\mathcal{G}$ is a generalised 5-gon with parameters (s,t). Since 5 is odd, we know that $s=t$. Let G be the point graph of $\mathcal{G}$.

We claim that G is a strongly regular graph with parameters $(s^4+s^3+s^2+s+1, s(s+1), s-1, 1)$.

Take a point p. This lies on $s+1$ lines, each containing s further points, and without overlap. So $k=s(s+1)$.

Since the graph has no triangles, a neighbour q of p is joined to the $s-1$ further points on the line pq and no other neighbours of p. So $\lambda=s-1$.

Let r be a non-neighbour of p. Then the distance from p to r in the incidence graph is 4. (It cannot be greater, since the diameter is 5; and it cannot be less, since r is not collinear with p.) So there is at least one point joined to both p and r. But there cannot be more than one, since the existence of two such points a and b would create either a triangle or a quadrangle in $\mathscr{G}$, hence a circuit of length 6 or 8 in the incidence graph. So $\mu = 1$.

We calculate the number of vertices in the usual way.

Now we apply the eigenvalue conditions. The adjacency matrix A of G satisfies $A^2 = s(s+1)I + (s-1)A + (J - I - A)$. So it has eigenvalue $k = s(s+1)$ with multiplicity 1. The other eigenvalues satisfy $\theta^2 = s(s+1) + (s-1)\theta - 1 - \theta$, giving

$$\theta = \tfrac{1}{2}(s - 2 \pm s\sqrt{5}).$$

Since both eigenvalues are irrational, their multiplicities must be equal, and must each be $\frac{1}{2}s(s^3 + s^2 + s + 1)$. Thus the equation $\mathrm{Trace}(A) = 0$ gives

$$s(s+1) + \tfrac{1}{2}s(s+1)(s^2+1)(s-2) = 0.$$

This equation is satisfied when $s = 1$.

But if $s \geq 2$, then $s(s+1) > 0$ and $\frac{1}{2}s(s+1)^2(s-2) \geq 0$, so the equation cannot hold.

Remark An alternative way to finish the proof goes as follows. We saw in our discussion of strongly regular graphs that, if the eigenvalues of A are irrational, then we are in Type 1, where $n = 4\mu + 1$ holds. Here, $\mu = 1$, so $n = 5$.

Index