Random strongly regular graphs?

Peter J Cameron

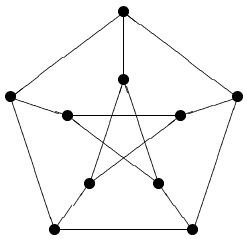
School of Mathematical Sciences
Queen Mary, University of London
London E1 4NS, U.K.
p.j.cameron@qmul.ac.uk

COMB01, Barcelona, 14 September 2001

Strongly regular graphs

A graph Γ is *strongly regular* with parameters v, k, λ, μ (or $\mathrm{srg}(v,k,\lambda,\mu)$) if

- there are v vertices;
- every vertex has k neighbours;
- two adjacent vertices have λ common neighbours;
- two non-adjacent vertices have μ common neighbours.



Graphs with 36 vertices

- There is a unique $\mathrm{srg}(36,10,4,2)$ up to isomorphism, the graph $L_2(6)$ (the line graph of $K_{6,6}$ (Shrikhande).
- There are exactly 32548 non-isomorphic $\mathrm{srg}(36,15,6,6)$ (McKay and Spence).

The first result reflects the search for nice characterisation theorems (in particular, uniqueness theorems) for strongly regular graphs. There are many examples of such theorems.

The second is a bit surprising in view of this.

Some more examples

(a) *complete multipartite graphs*: the vertex set is partitioned into n subsets of size m, and two vertices are adjacent if and only if they belong to different sets.

(b) *line graphs of Steiner systems*: the vertices are the blocks of a Steiner system $S(2,m,n)$ (that is, they are m-subsets of an n-set with the property that any two elements of the set lie in a unique block); two vertices are adjacent if and only if the corresponding blocks intersect.

(c) *Latin square graphs*: given $m-2$ mutually orthogonal Latin squares of order n, the vertices are the n^2 cells, two vertices adjacent if they lie in the same row or column or have the same entry in one of the squares.

(d) *Paley graphs*: the vertices are the elements of the field $\mathbb{F}_q$, where q is a prime power congruent to 1 mod 4; two vertices are adjacent if their difference is a square in F.

Neumaier's Theorem

The adjacency matrix of a (connected) strongly regular graph has the property that, apart from the valency of the graph (which is an eigenvalue with multiplicity 1), there are just two distinct eigenvalues, of which one is positive and the other negative. Moreover, if these eigenvalues are not both integers, then the parameters of the graph are "self-complementary", that is, the same as those of the complement. Paley graphs (with q a non-square) have this property.

The other three classes, in some sense, account for almost all strongly regular graphs, as a theorem of Neumaier shows:

Theorem 1 *Let m be an integer greater than 1. Then a strongly regular graph with smallest eigenvalue $-m$ is a complete multipartite graph with parts of size m, or arises from $m-2$ mutually orthogonal Latin squares or from a Steiner system with block size m, or is one of a finite list $\mathcal{L}(m)$ of graphs.*

The case $m = 2$

The case $m = 2$ of Neumaier's Theorem was proved by Seidel:

Theorem 2 *A strongly regular graph with smallest eigenvalue -2 is a complete multipartite graph with parts of size 2 (a* cocktail party graph*), a square lattice graph $L_2(n) = L(K_{n,n})$, a triangular graph $T(n) = L(K_n)$, or is the Petersen, Clebsch, Schläfli or Shrikhande graph or one of the three Chang graphs (with 10, 16, 27, 16, 28, 28, 28 vertices respectively.)*

So there are just seven exceptional graphs in $\mathcal{L}(2)$.

The case $m = 3$

When $m = 3$, one important difference is that, instead of having one graph $L_2(n)$ and one $T(n)$ for every n, there are as many as there are Latin squares or Steiner triple systems (counted up to a suitable notion of isomorphism).

The numbers of such objects of order n are very roughly n^{n^2} and $n^{n^2/6}$ respectively (where n is congruent to 1 or 3 mod 6 in the latter case). (Godsil and McKay gave estimates for the number of Latin squares, and Wilson for the number of Steiner triple systems.)

For $\mathrm{srg}(36, 15, 6, 6)$s, there are eleven $L_3(6)$ graphs; the other 32537 are in the list $\mathcal{L}(3)$ of exceptions.

Latin square graphs

For a Latin square L of order $n > 4$ and the corresponding Latin square graph Γ,

(a) the largest clique in Γ has size n, and there are exactly $3n$ cliques of this size;

(b) the second largest clique in Γ has size at most 4, with equality if and only if L contains an *intercalate* (a subsquare of order 2);

(c) the largest coclique in Γ has size at most n, with equality if and only if L has a transversal;

(d) the chromatic number of Γ is at least n, with equality if and only if L has an orthogonal mate.

So we are led to ask about the numbers of intercalates, transversals, and orthogonal mates of a typical Latin square.

Random Latin squares

There is a Markov chain method for selecting a random Latin square (and hence a random strongly regular graph with the appropriate parameters) from the uniform distribution. (Jacobson and Matthews).

Represent a Latin square as a function f from the set of ordered triples from $\{1,\dots,n\}$ to $\{0,1\}$ such that, for any $x,y \in \{1,\dots,n\}$, we have

$$\sum_{z\in\{1,\dots,n\}} f(x,y,z) = 1,$$

with analogous statements if we specify the entries in any other pair of coordinates. We allow also *improper Latin squares*, which are functions satisfying the displayed constraint but which take the value -1 exactly once (and the values 0 and 1 elsewhere). Now to take one step in the Markov chain starting at a function f, we do the following:

(a) If f is proper, choose (x,y,z) with $f(x,y,z) = 0$; if f is improper, start with the unique (x,y,z) such that $f(x,y,z) = -1$.

(b) Let x',y',z' be points such that

$$f(x',y,z) = f(x,y',z) = f(x,y,z') = 1.$$

(If f is proper, these points are unique; if f is improper, there are two choices for each of them.)

(c) Now increase the value of f by 1 on (x,y,z), (x,y',z'), (x',y,z'), and (x',y',z), and decrease it by 1 on (x',y,z), (x,y',z), (x,y,z'), and (x',y',z'). We obtain another proper or improper Latin square, according as $f(x',y',z') = 1$ or $f(x',y',z') = 0$ in the original.

This Markov chain is irreducible (in other words, we can move from any proper or improper Latin square to any other by a sequence of such moves), and the limiting distribution gives the same probability to any Latin square.

STS graphs

For a Steiner triple system S of order $n > 15$ and the corresponding STS graph Γ,

(a) the largest clique in Γ has size $(n-1)/2$, and there are exactly n cliques of this size;

(b) the second largest clique in Γ has size at most 7, with equality if and only if S contains a subsytem of order 7;

(c) the largest coclique in Γ has size at most $n/3$, with equality if and only if S has a spread;

(d) the chromatic number of Γ is at least $(n-1)/2$, with equality if and only if S is resolvable.

So we are led to look at subsystems, spreads and resolutions (parallelisms) of random Steiner triple systems.

Random STSs

There is a Markov chain for Steiner triple systems, almost identical to that of Jacobson and Matthews for Latin squares: simply replace ordered triples by unordered triples. Thus a Steiner triple system is a function from 3-sets to $\{0,1\}$ whose sum over the 3-sets containing any 2-set is 1, and an improper STS is a function taking the value -1 precisely once.

As far as I know, the connectedness of this Markov chain has not been proved. This is an interesting open problem! (Grannell and Griggs have recently shown that any two isomorphic STS lie in the same component.)

Sets of MOLS

There is no known method of choosing a random set of mutually orthogonal Latin squares.

Instead we can do the following: Start with a complete set of $q-1$ mutually orthogonal Latin squares of order q (corresponding to an affine plane of order q); then select $m-2$ of them at random (corresponding to m parallel classes in the plane). Even if we choose the Desarguesian plane, this construction produces many non-isomorphic graphs.

The isomorphism problem can be solved completely in some cases, for example, Desarguesian planes of prime order.

If q is odd and $m=(q+1)/2$, then the resulting graph has "self-complementary parameters" $n=q^2$, $k=(q^2-1)/2$, $\lambda=(q^2-5)/4$, $\mu=(q^2-1)/4$, so we obtain an analogue of "edge-probability $1/2$".

The Wallis–Fon-Der-Flaass graphs

Fon-Der-Flaass revived and extended an old construction of Wallis which produces superexponential numbers of strongly regular graphs for various parameter sets (all of which are exceptional in Neumaier's Theorem).

An affine design is a 2-design with the properties that any two blocks intersect in either zero or a constant number s of points; and each block together with all blocks disjoint from it forms a parallel class, of size m. So there are ms points in each block, and m^2s points altogether.

The number of parallel classes is $r=(m^2s-1)/(m-1)$; so $m-1$ divides $s-1$.

Let $I=\{1,\ldots,r+1\}$, and let $\{S_i : i\in I\}$ be arbitrary affine designs with parameters as above (where r is the number of parallel classes). Let $S_i=(V_i,B_i)$.

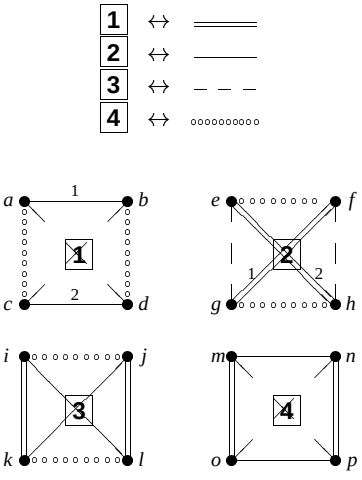
For every i, denote arbitrarily the parallel classes of S_i by symbols C_{ij}, $j\in I\setminus\{i\}$. For $v\in V_i$, let $b_{ij}(v)$ denote the block in the parallel class C_{ij} which contains v.

For every pair $i,j\in I$ with $i\neq j$, choose an arbitrary bijection $\sigma_{ij}:C_{ij}\to C_{ji}$; we require only that $\sigma_{ji}=\sigma_{ij}^{-1}$.

Construct a graph Γ on the vertex set $X=\bigcup_{i\in I}V_i$. The sets V_i will be independent (that is, no two vertices in the same V_i are joined). Two vertices $v\in V_i$ and $w\in V_j$ with $i\neq j$ are adjacent in Γ if and only if $w\in\sigma_{ij}(b_{ij}(v))$ (or, equivalently, $\sigma_{ij}(l_{ij}(v))=b_{ji}(w)$).

The graph so obtained is strongly regular $\mathrm{srg}(v,k,\lambda,\mu)$, where $v=m^2s(r+1)$, $k=msr$, $\lambda=\mu=s(r-1)$.

Example



$a\sim f$ $a\sim g$ $b\sim f$ $b\sim g$
$c\sim e$ $c\sim h$ $d\sim e$ $d\sim h$
etc.

Embeddings

These graphs allow us to embed all graphs in relatively small strongly regular graphs as induced subgraphs.

Theorem 3 *(a) Any graph with n vertices can be embedded in a strongly regular graph with at most $4n^2$ vertices;*

(b) There is a strongly regular graph with at most $2^{2(n+1)}$ vertices in which every graph on n vertices can be embedded.

This is done by choosing the affine designs to be affine spaces over the field $\mathbb{F}_2$. The vertex sets of the graphs are chosen from distinct sets V_i.

Existential closure

A graph is said to be n-existentially closed if, given any two disjoint sets U and W of vertices with $|U|+|W|=n$, there is a vertex v joined to every vertex in U and to no vertex in W. We write n-e.c. for short.

A n-e.c. graph obviously has at least 2^n+n vertices. On the other hand, the "first moment method" shows that, if $N > n^2 2^n$, there is a graph on N vertices which is n-e.c. (since the probability that a random graph is n-e.c. is positive).

The Paley graph $P(q)$ is known to be n-e.c. if $q > n^2 2^{2n-2}$. The proof uses the Hasse–Weil estimates for character values, so is not elementary.

Many existentially closed graphs

Using the analogous Paley designs in the Fon-Der-Flaass construction, Cameron and Stark showed:

Theorem 4 *Let q be a prime power congruent to 3 mod 4, satisfying $q \geq 16n^2 2^{2n}$. Then there exist $2^{\binom{q+1}{2}(1-O(q^{-1}\log q))}$ non-isomorphic strongly regular graphs $\mathrm{srg}((q+1)^2, q(q+1)/2, (q^2-1)/4, (q^2-1)/4)$ which have the n-e.c. property.*

Desiderata

It seems out of the question, with our present state of knowledge, to talk about random strongly regular graphs with specified parameters. For many parameter sets, we cannot even determine whether or not any graphs exist!

What we do instead is assume that we have a specific construction of strongly regular graphs. We must impose some requirements on this construction, if there is to be any chance of developing a theory of random objects.

(a) The construction should produce all (or all but a few) s.r.g.s with the relevant parameters. (We will relax that in some cases below but with the proviso that we are not truly considering "random strongly regular graphs"; these cases often allow us to develop methods which apply in other cases.)

(b) The construction should produce large numbers of s.r.g.s. If we are looking at a particular parameter set for which there is a unique graph, or only a few, then the issue of randomness doesn't apply.)

(c) We should be able to tell when two graphs produced by the construction are isomorphic. This is not always necessary: if the number of graphs is much larger than the order of the symmetric group, then isomorphisms don't affect the asymptotics too much.

(d) The construction should depend on a sequence of choices, or have some other form which lends itself to analysis by the tools of probability theory.

(e) The properties of the graphs constructed should be deducible from the choices made in the construction.

References

B. Bollobás and A. G. Thomason, Graphs which contain all small graphs, *Europ. J. Comb.*, **2** (1981), 13–15.

R. C. Bose, Strongly regular graphs, partial geometries, and partially balanced designs, *Pacific J. Math.* **13** (1963), 389–419.

P. J. Cameron and D. Stark, Strongly regular graphs with the n-e.c. property, submitted to *Discrete Math.*

D. G. Fon-Der-Flaass, New prolific constructions of strongly regular graphs, in preparation.

C. D. Godsil and B. D. McKay, Asymptotic enumeration of Latin rectangles, *J. Combinatorial Theory* (B) **48** (1990), 19-44.

M. T. Jacobson and P. Matthews, Generating uniformly distributed random Latin squares, *J. Combinatorial Design* **4** (1996), 405–437.

A. Neumaier, Strongly regular graphs with least eigenvalue $-m$, *Arch. Math.* **33** (1979), 392–400.

J. J. Seidel, Strongly regular graphs with $(-1,1,0)$ adjacency matrix having eigenvalue 3, *Linear Algebra Appl.* **1** (1968), 281–298.

W. D. Wallis, Construction of strongly regular graphs using affine designs, *Bull. Austral. Math. Soc.* **4** (1971), 41–49.

R. M. Wilson, Non-isomorphic Steiner triple systems, *Math. Z.* **135** (1974), 303–313.