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

Abstract

Strongly regular graphs lie on the cusp between highly structured and unstructured. For example, there is a unique strongly regular graph with parameters $(36,10,4,2)$, but there are 32548 non-isomorphic graphs with parameters $(36,15,6,6)$. (The first assertion is a special case of a theorem of Shrikhande, while the second is the result of a computer search by McKay and Spence.) In the light of this, it will be difficult to develop a theory of random strongly regular graphs!

For certain values of the parameters, we have at least one prerequisite for a theory of random objects: there should be very many of them (e.g. superexponentially many). Two other features we would like are a method to sample from the uniform distribution (this is known in a couple of special cases) and information about how various graph parameters behave as random variables on the uniform distribution. Very little is known but there are a few recent results and some interesting problems.

This paper develops no general theory, but explores a few examples and techniques which can be applied in some cases.

Thomason has developed a theory of "pseudo-random graphs" which he calls (p,α)-jumbled graphs. Some of these graphs are strongly regular, but they are very special strongly regular graphs. I conclude with some speculation about "random jumbled graphs".

1 Strongly regular graphs

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

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

The four parameters are not independent. A simple counting argument shows that $k(k-\lambda-1) = (v-k-1)\mu$. Many further necessary conditions are known. See [18] or [6] for a survey.

We now define several classes of strongly regular graphs which will be important.

(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 F with q elements, where q is a prime power congruent to 1 mod 4; two vertices are adjacent if their difference is a square in F.

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 [16] shows:

Theorem 1.1 *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.*

This theorem was proved by Seidel [17] in the case $m = 2$ with an explicit derivation of the list $\mathcal{L}(2)$:

Theorem 1.2 *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 $\mathcal{L}(2)$.

As a corollary to Neumaier's theorem, since the parameters of a strongly regular graph determine its eigenvalues, we see that a graph with the same parameters as one of Latin square or Steiner system type, where m is fixed, is of this type provided that $n > f(m)$ for some function f. (This was proved earlier by Bose [3], who gave explicit bounds.) Moreover, there is a function g such that, if a graph is of one of these types, the set of MOLS or the Steiner system is uniquely determined (up to a suitable notion of isomorphism) by the graph.

For example, of the 32548 $\mathrm{srg}(36,15,6,6)$ mentioned in the Abstract, eleven are of Latin square type; the rest belong to the list $\mathcal{L}(3)$.

2 Desiderata

Choosing a graph at n points at random from the uniform distribution is easy: select edges independently with probabiility $1/2$ from the set of all 2-sets of vertices.

Choosing a regular graph of valency k on n vertices (where kn is even) is now also well-understood, at least if k is not too large: see Wormald [24] for a survey.

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.) We will see several cases below where the number of non-isomorphic graphs is superexponential in the number of vertices.

(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. We will see instances where the "isomorphism problem" has a strong solution.

(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. This is a bit vague; but we do not know how to choose at random without some further information!

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

3 Latin squares and Steiner systems

It follows from the results in the first section that, for sufficiently large n,

- there is a unique $\mathrm{srg}(n^2, 2(n-1), n-2, 2)$, the *square lattice graph*;
- there is a unique $\mathrm{srg}(n(n-1)/2, 2(n-2), n-2, 4)$, the *triangular graph*.

In fact, results of Shrikhande and Hoffman show that $n > 4$ and $n > 8$ respectively suffice. Not much room for random graphs here!

The next case is more interesting. For sufficiently large n,

- a srg$(n^2, 3(n-1), n, 6)$ comes from a unique Latin square of order n, up to isotopy;

- a srg$(n(n-1)/6, 3(n-3)/2, (n+3)/2, 9)$ comes from a unique Steiner triple system of order n, up to isomorphism.

(In other words, the isomorphism problem has a strong solution in these cases.) Now the numbers of Latin squares, resp. Steiner triple systems, of order n (where n is congruent to 1 or 3 mod 6 in the latter case) is known to be about n^{n^2}, resp. $n^{n^2/6}$ (these estimates are asymptotic in the logarithm; see Wilson [23] for estimates for Steiner triple systems, and Godsil and McKay [10], McKay and Wanless [15], for Latin squares). So there are superexponentially many strongly regular graphs for these parameter sets.

Another feature of these cases is that it is known that almost all Latin squares and Steiner triple systems (and hence almost all strongly regular graphs of each of these types) admits no non-trivial automorphisms. (See Babai [1] for Steiner triple systems.)

Moreover, in each case there is a Markov chain method for selecting a random Latin square or Steiner triple system (and hence a random strongly regular graph with the appropriate parameters) from the uniform distribution. See Jacobson and Matthews [11] for Latin squares. We outline the method briefly. Represent a Latin square as a function f from the set of ordered triples from $\{1,\ldots,n\}$ to $\{0,1\}$ such that, for any $x,y \in \{1,\ldots,n\}$, we have

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

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.

Jacobson and Matthews show that 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 that the limiting distribution gives the same probability to any Latin square. However, the mixing time for this Markov chain is not known.

The analogous Markov chain for Steiner triple systems has an almost identical description, obtained simply by using 3-element subsets in place of ordered triples. To my knowledge it has not been written down anywhere; and, in particular, it has not been shown that the connectedness property holds (though this seems very likely to be so). Recently, Grannell and Griggs (personal communication) have shown that isomorphic Steiner triple systems lie in the same component.

So we can ask, how do various graph-theoretic parameters behave? It turns out that these particular strongly regular graphs do not very much resemble random graphs:

Proposition 3.1 *(a) For a Latin square L of order $n > 4$ and the corresponding Latin square graph Γ,*

- *the largest clique in Γ has size n, and there are exactly $3n$ cliques of this size;*
- *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);*
- *the largest coclique in Γ has size at most n, with equality if and only if L has a transversal;*
- *the chromatic number of Γ is at least n, with equality if and only if L has an orthogonal mate.*

(b) For a Steiner triple system S of order $n > 15$ and the corresponding Latin square graph Γ,

- *the largest clique in Γ has size $(n-1)/2$, and there are exactly n cliques of this size;*
- *the second largest clique in Γ has size at most 7, with equality if and only if S contains a subsytem of order 7;*

- *the largest coclique in* Γ *has size at most* $n/3$, *with equality if and only if* S *has a spread;*
- *the chromatic number of* Γ *is at least* $(n-1)/2$, *with equality if and only if* S *is resolvable.*

The precise details are not too important, but it is striking that the graph-theoretic parameters are closely related to those which have been considered in their own right. These results also focus our attention on the numbers of intercalates, transversals, and orthogonal mates of a random Latin square, and the numbers of Fano subsystems, spreads, and resoutions of a random Steiner triple system.

Some results about these are already known. For example, McKay and Wanless [14] show that a random Latin square of order n has $n^{(3/2-\varepsilon)}$ intercalates, and the probability of a random Latin square of order n not containing any intercalates is $O(\exp(-n^{(2-\varepsilon)})$, for any $\varepsilon > 0$.

One can consider other graph-theoretic properties such as expansion properties or Hamiltonicity. Sometimes these are trivial; for example, every Latin square graph is Hamiltonian. (Indeed, $L_2(n)$ is Hamiltonian if n is even, and has a Hamiltonian path between any two non-adjacent vertices if n is odd.)

4 Sets of MOLS

At present, we have no method for constructing a random Steiner triple system with block size greater than 3, or a random set of two or more MOLS.

A weaker procedure for MOLS is as follows. Take an affine plane of order n (corresponding to a complete set of $n-1$ MOLS). Then we obtain a s.r.g. of type $L_m(n)$ by choosing m of the $n+1$ parallel classes of the plane and joining two points by an edge if the line joining them is in a chosen class. This provides us with $\binom{n+1}{m}$ strongly regular graphs, though of course not all are non-isomorphic.

Even in the most favourable case, with $m = (n+1)/2$, this number is subexpobebtial. (This case gives strongly regular graphs with self-complementary parameters, the analogue of random graphs with edge-probability $1/2$.)

We sketch out here how the isomorphism problem can be settled in the simplest case, where $n = p$ is prime and the affine plane is coordinatised by $\mathrm{GF}(p)$. Related results have been found by Kantor [12] for other combinatorial structures.

In this case, choose a set S containing m of the $p+1$ subgroups of order p of $C_p \times C_p$. Select two of them, and let their cosets be the rows and columns of the square array: the remaining subgroups give rise to the Latin squares. The vertices of the graph are the elements of $C_p \times C_p$, two vertices adjacent if their difference lies in the union of the chosen subgroups. Call a graph obtained in this way the *standard graph* $\Gamma(S)$.

Clearly two sets of subgroups equivalent under the *projective linear group* $\mathrm{PGL}(2,p)$ (induced by the automorphism group of $C_p \times C_p$, acting on the *projective line* or set of subgroups of order p) define isomorphic standard graphs. We will prove the converse.

Theorem 4.1 *Let S and S' be sets of 1-dimensional subspaces of a 2-dimensional vector space over $\mathrm{GF}(p)$. Then $\Gamma(S)$ and $\Gamma(S')$ are isomorphic if and only if S and S' lie in the same orbit of $\mathrm{PGL}(2,p)$ on subsets of the projective line over $\mathrm{GF}(p)$.*

Proof Since $\mathrm{PGL}(2,p)$ is 3-transitive, the theorem is true if $s \leq 3$ or $s \geq p-2$; so suppose not.

Let P be the translation group of V. First we show that P is a Sylow subgroup of $G = \mathrm{Aut}(\Gamma)$. For suppose not. Let Q be a Sylow subgroup containing P. Then Q_v has p fixed points (since the fixed points form a block of imprimitivity for Q), and $p-1$ orbits of length p on the remaining points. Since $k = m(p-1) = (m-1)p + (p-m)$, a point v is joined to $m-1$ orbits and $p-m$ further points in the same block as v. Note that the graph on a block is neither complete nor null.

Now $N_Q(Q_v)$ is transitive on the fixed points but fixes the non-trivial orbits. So if w is another fixed point, then w is joined to the same $m-1$ orbits of length p. So, if v and w are nonadjacent points in the same block,

$$m(m-1) = |\Gamma(v) \cap \Gamma(w)| \geq (m-1)p,$$

a contradiction.

Now let θ be an isomorphism from $\Gamma(S)$ to $\Gamma(S')$. Then θ conjugates the translation group Q to a Sylow subgroup Q' of $\mathrm{Aut}(\Gamma(S'))$. By Sylow's Theorem, there is an automorphism of $\Gamma(S')$ which conjugates Q' back to Q. The composite is an isomorphism from $\Gamma(S)$ to $\Gamma(S')$ which normalises Q, and hence maps S to S', as required. ■

Corollary 4.2 *Let p be an odd prime. Then the number of standard strongly regular graphs on p^2 vertices is equal to the number of orbits of $\mathrm{PGL}(2,p)$ on the set of subsets of the projective line over $\mathrm{GF}(p)$, which is asymptotically $2^{p+1}/p^3$. The number of standard s.r.g.s with self-complementary parameters (that is, $m = (p+1)/2$) is asymptotically $c.2^p/p^{7/2}$).*

Proof By a simple calculation based on the orbit-counting lemma, almost all orbits of $\mathrm{PGL}(2,p)$ acting on subsets (or $(p+1)/2$-subsets) of the projective line are regular; and this group has order $(p+1)p(p-1) \sim p^3$. (The number of orbits can be computed exactly.) ∎

In fact, we can be considerably more precise. If $m = 1$ or $m = p$, then $\Gamma(S)$ or its complement is a disjoint union of p complete graphs of size p, so that $\mathrm{Aut}(\Gamma(S)) = C_p \wr C_p$ (in its imprimitive action). If $m = 2$ or $m = p-1$, then $\Gamma(S)$ or its complement is a square lattice graph, so that $\mathrm{Aut}(\Gamma(S)) = C_p \wr C_2$ (in its product action). In every other case, all automorphisms of $\Gamma(S)$ are induced by affine transformations:

Theorem 4.3 *Let $2 < m < p-1$, and let S be an m-set of subspaces of $V = V(2,p)$. Then the translation group $P = C_p \times C_p$ of V is a normal subgroup of $\mathrm{Aut}(\Gamma(S))$, and hence*

$$\mathrm{Aut}(\Gamma(S)) = ((C_p \times C_p) : C_{p-1}).H(S),$$

where $H(S)$ is the stabiliser of S in $\mathrm{PGL}(2,p)$. For almost all choices of S, we have $H(S) = 1$.

Proof Let $\Gamma = \Gamma(S)$. From the proof of Theorem 4.1, P is a Sylow subgroup of $G = \mathrm{Aut}(\Gamma)$.

If G is primitive but does not satisfy the conclusion, then a theorem of Wielandt [22] shows that either G is 2-transitive, or G is a rank 3 subgroup of $S_p \wr S_2$. Both are impossible here, by assumption. So we may assume that G is imprimitive.

Thus, $G \leq H \wr K$, where H and K are transitive permutation groups of degree p. (There is a block system C, and a block $C \in B$, such that $H = G_B^B$ and $K = G^C$.) By Burnside's Theorem [4], each of H and K is either soluble or 2-transitive.

Suppose first that H is insoluble. Every element of order p fixing the block B fixes every block in the system C; these elements generate an insoluble subgroup of H, which thus fixes all blocks and is 2-transitive on each block. So G_v has orbit lengths 1, $p-1$, x_i, $x_i(p-1)$, where $\sum x_i = p-1$.

Now $k = m(p-1)$. So a point $v \in B$ is joined to no or all further points of B; by complementation if necessary,we may assume the former. Thus either v is joined to all points of $m-1$ blocks and one point of each remaining block, or it is joined to all but one point of m blocks. Applying an automorphism of order p fixing all blocks, we see that for any other point $w \in B$, the same $s-1$ or s blocks contain all or all but one neighbours of w. Thus,

$$|\Gamma(v) \cap \Gamma(w)| = p(m-1) \text{ or } (p-2)m.$$

But $|\Gamma(v) \cap \Gamma(w)| = s(s-1)$, so we have a contradiction.

Now assume that K is insoluble but H is soluble. The kernel N of the action on blocks is soluble, of order pk (say), where $kl = p-1$. If $k > 1$, then the fixed points of N_v form a block transversal to C; using this block instead of B, we are back in the previous case. So $k = 1$. Then G is an extension of C_p by K, and the Sylow subgroup Q splits over C_p; so G splits over C_p. Replacing K by its simple minimal normal subgroup, we have $G = C_p \times K$. But then the K-orbits form a system of imprimitivity, which again falls into the previous case.

So both H and K are soluble. Now G has a normal subgroup G^* which projects onto a Sylow p-subgroup of K; and G^* has a normal (indeed characteristic) subgroup P. So P is normal in G. This proves the first part of the theorem.

Now, choosing a vertex v of Γ, there is a canonical identification of the vertex set with P so that G acts by affine transformations. The set S is determined as the set of subspaces which are cliques in the graph (the other subspaces are cocliques). So every linear automorphism fixes S, and (modulo scalars) lies in $H(S)$. Conversely, all translations and linear transformations fixing S induce automorphisms. So we are done. ■

5 A construction of Wallis and Fon-Der-Flaass

Wallis [21] constructed a large number of strongly regular graphs from affine designs. His construction was rediscovered and generalised by Fon-Der-Flaass [8], who observed that the construction gives superexponentially many non-isomorphic strongly regular graphs.

We briefly describe the construction. It depends on the existence of at least one *affine design* (this is a resolvable 2-design in which blocks from different parallel classes meet in a constant number of points). Let r be the number of parallel classes, and m the cardinality of the intersection of two non-parallel blocks. Then

Take $r+1$ such designs all with the same parameters (they may or may not be isomorphic), where r is the number of parallel classes of each design; number the parallel classes of the ith design as $\mathcal{C}_{ij}$, where $1 \leq j \leq r+1$, $j \neq i$. For each $i \neq j$, choose a bijection σ_{ij} between $\mathcal{C}_{ij}$ and $\mathcal{C}_{ji}$, where σ_{ij} and σ_{ji} are mutually inverse. Now the vertex set is the disjoint union of the point sets of the designs, and edges join all the points of a block in $\mathcal{C}_{ij}$ to the points of the corresponding block of $\mathcal{C}_{ji}$.

Figure 1 illustrates the construction in the smallest case, where the blocks of the affine design consist of all 2-subsets of a 4-set. The $r+1 = 4$ designs are associated with the four different styles used for indicating the parallel classes of

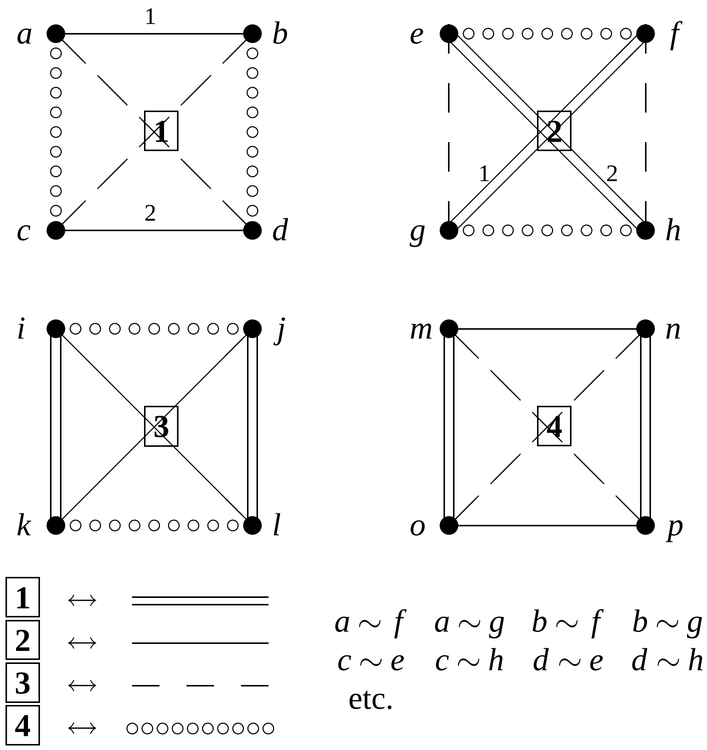

Figure 1: An example

lines; the small numbers 1 and 2 indicate the bijection between the parallel classes $\mathcal{C}_{12}$ and $\mathcal{C}_{21}$, which gives rise to the eight adjacencies listed.

The construction is prolific because of the choices involved: we can use arbitrary affine designs (and, for some parameters, there are more than exponentialy many of these); we can choose the numberings of the parallel classes in $(r!)^{r+1}$ ways; and, most significantly, we can choose the bijections in $(m!)^{r(r+1)/2}$ ways, where $m = n/k$ is the size of a parallel class. Different choices may produce isomorphic graphs, but Fon-Der-Flaass shows that, given the designs and the numberings of the parallel classes, at most $v^3 n!^2$ different choices of bijections give rise to a given isomorphism type of strongly regular graph, so that there are at least $2^{n^3 \log n(1+o(1))/2}$ non-isomorphic strongly regular graphs.

Fon-Der-Flaass has given a number of variants on this construction; they also produce many strongly regular graphs with various parameter sets.

6 Embeddings and existential closure

A simple property of random graphs is that they contain all "small" graphs as subgraphs. The graphs of Fon-Der-Flaass have similar properties:

Theorem 6.1 *(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.*

To prove part (a), we choose a representative point in each of the affine designs, and assume that it lies on the first block of each parallel class. Now the representative points in the ith and jth designs are adjacent if and only if σ_{ij} maps the first block of $\mathcal{C}_{ij}$ to the first block of $\mathcal{C}_{ji}$.

Now, for any n, there is a Hadamard design (an affine design with two blocks in each parallel class) with at most $2n-1$ parallel classes, and at mst $2n$ points; so the resulting strongly regular graph has at most $4n^2$ vertices.

The proof of (b) is similar.

The result is best possible apart from the constants: see [2]. In fact, it is conjectured that Hadamard designs exist on any number of points divisible by 4; the truth of this conjecture would reduce the constant 4 in part (a) to $1+o(1)$.

We turn to another property possessed by random graphs, but for which explicit models have been rare. We say that a graph has the *n-existential closure* propeprty (or, for short, is n-e.c.) if, given any set A of at most n vertices, and any subset B of A, there is a vertex outside A joined to all vertices in B and to none in $A\setminus B$.

Some of the interest in this property stems from the fact that there is a unique countable graph R which is n-e.c. for all n, namely the countable "random graph" or *Rado's graph* (see [5] for discussion). It follows that a first-order sentence ϕ (in the language of graph theory) which is true in R is provable from the set $\{\sigma_n : n \in \mathbb{N}\}$, where σ_n is the sentence asserting the n-e.c. property. As a result, ϕ is true in almost all finite graphs if and only if it is true in R, and we obtain the zero-one law for first-order properties of graphs due to Glebskii *et al.*[9].

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 $q > n^2 2^{2n-2}$ (see Bollobás and Thomason [2]). The proof uses the Hasse–Weil estimates for character values, so is not elementary.

More recently, Cameron and Stark [7] showed, using probabilistic methods, that superexponentially many of Wallis' graphs are n-e.c. More precisely:

Theorem 6.2 *Let q be a prime power congruent to* 3 *mod* 4*, and suppose that* $q \geq 16n^2 2^{2n}$*. Then there are at least* $2^{\binom{q+1}{2}(1-O(q^{-1}\log q))}$ *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.*

The graphs of this theorem are the ones obtained from the construction of Wallis and Fon-Der-Flaass. Both [8] and [7] use Hadamard designs for the affine designs. In [7], they must be of Paley type, for much the same reason that Paley graphs are n-e.c. for large n. If we use even one affine geometry over $\mathrm{GF}(2)$, the resulting graph is not even 4-e.c.

7 Jumbled graphs

Let p and α be real numbers. Thomason [20] defined a class of "pseudo-random" graphs, which he called (p,α)*-jumbled graphs*, as follows. iLet p and α be real numbers satisfying $0 < p < 1 \leq \alpha$. A graph G is (p,α)-jumbled if every induced subgraph H of G satisfies

$$|e(H) - p\binom{m(H)}{2}| \leq \alpha m(H),$$

where $m(H)$ and $e(H)$ are the numbers of vertices and edges of H.

The (p,α)-jumbled graphs behave in many ways like random graphs with edge probability p.

Thomason shows that strongly regular graphs provide examples of jumbled graphs, where p and α can be computed from the parameters of the graphs. His examples are very specific. However, our approach raises the possibility of considering a "random" jumbled graph chosen from a large set, and so perhaps of quantifying the extent to which jumbled graphs do model the properties of random graphs. I hope to return to this point in the future.

References

[1] L. Babai, Almost all Steiner triple systems are asymmetric, in *Topics in Steiner systems* (ed. C. C. Lindner and A. Rosa), *Ann. Discrete Math.* **7**, Elsevier, Amsterdam, 1979, pp. 37–39.

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

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

[4] W. Burnside, *Theory of Groups of Finite Order*, Dover Publ. (reprint), New York, 1955.

[5] P. J. Cameron, The random graph, in *The Mathematics of Paul Erdős*, (ed. J. Nešetřil and R. L. Graham), Springer, Berlin, 1996, pp. 331–351.

[6] P. J. Cameron, Strongly regular graphs, in preparation.

[7] P. J. Cameron and D. Stark, Strongly regular graphs with the n-e.c. property, in preparation.

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

[9] Y. V. Glebskii, D. I. Kogan, M. I. Liogon'kii and V. A. Talonov, Range and degree of realizability of formulas in the restricted predicate calculus, *Kibernetika* **2**(1969), 17–28.

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

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

[12] W. M. Kantor, Exponential numbers of two-weight codes, difference sets and symmetric designs, *Discrete Math.* **46** (1983), 95–98.

[13] B. D. McKay and E. Spence, in preparation; see `http://gauss.maths.gla.ac.uk/~ted/srgraphs.html`

[14] B. D. McKay and I. M. Wanless, Most Latin squares have many subsquares, *J. Combinatorial Theory* (A) **86** (1999), 323–347.

[15] B. D. McKay and I. M. Wanless, Maximising the permanent of $(0,1)$-matrices and the number of extensions of Latin rectangles, *Electronic J. Combinatorics* **5** (1998), #R5 (20pp).

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

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

[18] J. J. Seidel, Strongly regular graphs, *Surveys in combinatorics* (ed. B. Bollobás), pp. 157-180, Cambridge University Press, Cambridge, 1979.

[19] S. S. Shrikhande, The uniqueness of the L_2 association scheme, *Ann. Math. Statistics* **30** (1959), 781–798.

[20] A. G. Thomason, Pseudo-random graphs. *Ann. Discrete Math.* **33** (1987), 307–331.

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

[22] H. Wielandt, *Permutation Groups through Invariant Relations and Invariant Functions*, Ohio State Univ., Columbus, 1969.

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

[24] N. C. Wormald, Models of random regular graphs, pp. 239–298 in *Surveys in Combinatorics, 1999* (ed. J. D. Lamb and D. A. Preece), London Math. Soc. Lecture Notes Series **267**, Cambridge University Press, Cambridge, 1999.