A prolific construction of strongly regular graphs with the n-e.c. property

Peter J. Cameron and Dudley Stark

School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS, U.K.
P.J.Cameron@qmul.ac.uk, D.S.Stark@qmul.ac.uk

Submitted: October 18, 2001; Accepted: July 19, 2002.

Abstract

A graph is n-e.c. (n-existentially closed) if for every pair of subsets U, W of the vertex set V of the graph such that $U \cap W = \emptyset$ and $|U| + |W| = n$, there is a vertex $v \in V - (U \cup W)$ such that all edges between v and U are present and no edges between v and W are present. A graph is strongly regular if it is a regular graph such that the number of vertices mutually adjacent to a pair of vertices $v_1, v_2 \in V$ depends only on whether or not $\{v_1, v_2\}$ is an edge in the graph.

The only strongly regular graphs that are known to be n-e.c. for large n are the Paley graphs. Recently D. G. Fon-Der-Flaass has found prolific constructions of strongly regular graphs using affine designs. He notes that some of these constructions were also studied by Wallis. By taking the affine designs to be Hadamard designs obtained from Paley tournaments, we use probabilistic methods to show that many non-isomorphic strongly regular n-e.c. graphs of order $(q+1)^2$ exist whenever $q \geq 16n^2 2^{2n}$ is a prime power such that $q \equiv 3 \pmod 4$.

1 Introduction

The vertex set of a graph G will be denoted by $V = V(G)$ and the edge set by $E = E(G)$. The number of vertices is denoted by $N = |V|$.

We define a graph to be n-e.c. (n-existentially closed) if for every pair of subsets U, W of the vertex set V such that $U \cap W = \emptyset$ and $|U| + |W| = n$ there is a vertex $v \in V - (U \cup W)$ such that all edges between v and U are present and no edges between v and W are present.

A *strongly regular* $SR(N, K, \Lambda, M)$ graph is a regular graph such that the number of vertices adjacent to a pair of vertices $v_1, v_2 \in V$ depends only on whether or not $\{v_1, v_2\} \in E$. Denote the common degree of the vertices of G by K. Given $v \in V$, let

$\Gamma(v) = \{w \in V : \{w, v\} \in E\}$ denote the set of vertices in V adjacent to v. If v and w are vertices such that $\{w, v\} \in E$, then the number of vertices mutually adjacent to v and w is $|\Gamma(v) \cap \Gamma(w)| = \Lambda$, and if $\{w, v\} \notin E$, then $|\Gamma(v) \cap \Gamma(w)| = M$.

The only strongly regular graphs that are known to be n-e.c. for $n > 3$ are the Paley graphs, which are constructed from finite fields of size q where q is a prime power such that $q \equiv 1 \pmod 4$. Let $\mathbb{F}_q$ denote the finite field containing q elements, where q is a power of a prime. The vertices of the Paley graph P_q are the elements of $\mathbb{F}_q$ and there is an edge between two vertices x and y if and only if $x - y$ is a square in $\mathbb{F}_q$. The Paley graphs are n-e.c. whenever $q > n^2 2^{2n-2}$; see Bollobás and Thomason [3]. Recently Bonato, Holzmann and Kharaghani [4] have used Hadamard matrices to construct new 3-e.c. graphs.

Even more recently, D. G. Fon-Der-Flaass [6] has found prolific constructions of strongly regular graphs using affine designs. (He points out that some of these constructions appeared in Wallis [10].) His main construction appears as Construction 1 in Section 3. By taking the affine designs in Construction 1 to be Hadamard designs obtained from Paley tournaments (defined in Section 3) we use probabilistic methods to show that many non-isomorphic strongly regular n-e.c. graphs of certain orders exist.

Theorem 1.1 *Suppose that q is a prime power such that $q \equiv 3 \pmod 4$. There is a function $\varepsilon(q) = O(q^{-1} \log q)$ such that there exist $2^{\binom{q+1}{2}(1-\varepsilon(q))}$ non-isomorphic $SR((q+1)^2, q(q+1)/2, (q^2-1)/4, (q^2-1)/4)$ graphs which are n-e.c. whenever $q \geq 16n^2 2^{2n}$.*

The lower bound on q arises from the need to make the estimates in Theorem 3.2 below effective and the condition on the modulus of q is required because Paley tournaments are only defined on q vertices for q a prime power such that $q \equiv 3 \pmod 4$.

Theorem 1.1 will be proved by analysing randomly generated strongly regular graphs. The graphs are generated by Construction 2 (described in Section 3) when certain bijections and permutations are chosen uniformly at random. Lemma 3.3 in Section 3 shows that Construction 2 generates many non-isomorphic graphs. We then show that most of the graphs generated have the n-e.c. property in Section 4, thereby completing the proof of Theorem 1.1. The proof of the n-e.c. property uses bounds on the expected number of pairs of subsets U, W causing the graph not to be n-e.c.

2 Background

The n-e.c. property first occurred in the discussion of random graphs, in particular the zero-one law for first-order sentences [7]. Clearly this property can be expressed as a first-order sentence ϕ_n in the language of graph theory. Now it is well-known that

(a) the countable random graph R satisfies ϕ_n for all n (and is determined up to isomorphism by this);

(b) for fixed n, almost all finite graphs satisfy ϕ_n.

Now let θ be any sentence. Either θ or its negation holds in R; we may suppose the former. By compactness, θ is a logical consequence of a finite number of sentences ϕ_n; so θ holds in almost all finite graphs.

As usual, although almost all random graphs are n-e.c., it is not clear how to construct explicit examples!

3 Constructing random strongly regular graphs

An *affine design* is a 2-design with the following two properties:

(i) Every two blocks are either disjoint or intersect in a constant number r of points.

(ii) Each block together with all blocks disjoint from it forms a parallel class: a set of n mutually disjoint blocks partitioning all points of the design.

Define s to be $s = (r-1)/(n-1)$. The number of parallel classes is $p = n^2s + n + 1$ and each block in a parallel class contains $k = nr = n^2s - ns + n$ points. The following construction is described in Fon-Der-Flaass [6]. It originally appeared in Wallis [10]:

Construction 1 Let $\mathcal{S}_1, \ldots, \mathcal{S}_{p+1}$ be arbitrary affine designs with parameters (n, r, s); here $p = n^2s + n + 1$ is the number of parallel classes in each $\mathcal{S}_i$. Let $\mathcal{S}_i = (V_i, \mathcal{L}_i)$. Let $\mathcal{I} = \{1, \ldots, p+1\}$.

For every i, denote arbitrarily the parallel classes of $\mathcal{S}_i$ by symbols $\mathcal{L}_{ij}$, $j \in \mathcal{I} - \{i\}$. For $v \in V_i$, let $l_{ij}(v)$ denote the line in the parallel class $\mathcal{L}_{ij}$ which contains v.

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

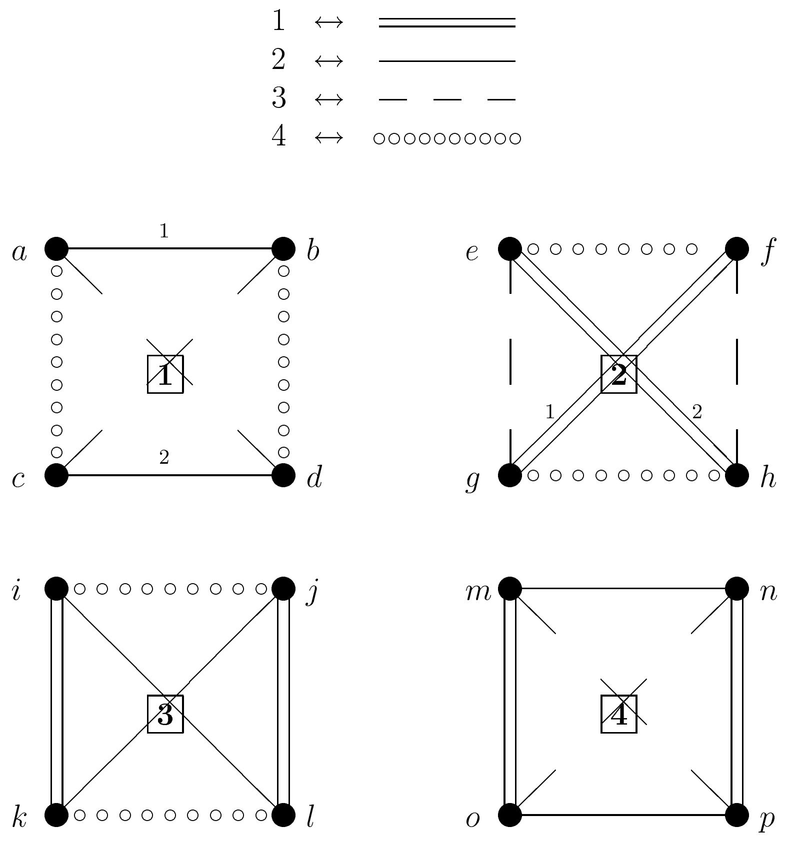
Construct a graph $\mathcal{G}_1 = \mathcal{G}_1((\mathcal{S}_i), (\sigma_{i,j}))$ on the vertex set $X = \cup_{i \in \mathcal{I}} V_i$. The sets V_i will be independent. Two vertices $v \in V_i$ and $w \in V_j$, $i \neq j$, are adjacent in $\mathcal{G}_1$ if and only if $w \in \sigma_{i,j}(l_{ij}(v))$ (or, equivalently, $\sigma_{i,j}(l_{ij}(v)) = l_{ji}(w)$).

Wallis and Fon-Der-Flaass go on to show that

Theorem 3.1 *The graph obtained in Construction 1 is strongly regular with parameters* (N, K, Λ, M), $N = n^2r(n^2s + n + 2)$, $K = nr(n^2s + n + 1)$, $\Lambda = M = r(n^2s + n)$.

Figure 1 shows the case $n = 2$, $r = 1$, $s = 0$, where we obtain a $(16, 6, 2, 2)$ strongly regular graph. Each of the four designs has as blocks all 2-subsets of a 4-set; the design $\mathcal{S}_i$ is labelled with a bold numeral i in a square. The top of the figure shows the numbering of the parallel classes; each style of line corresponds to a fixed second index. For example, the double lines in design $\mathcal{S}_i$ form the parallel class $\mathcal{L}_{i1}$. The small numerals show the correspondence between $\mathcal{L}_{12}$ and $\mathcal{L}_{21}$. The last two lines of the figure show some adjacencies in the graph: the two points of each block in $\mathcal{L}_{12}$ are adjacent to the two points of the corresponding block in $\mathcal{L}_{21}$.

In order for Construction 1 to produce strongly regular graphs with the n-e.c. property, it is necessary that for any V_i and for any pair of disjoint subsets U, W of V_i such that



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

Figure 1: The construction

$|U| + |W| = n$, there must be a vertex v with all edges between v and U present and no edges between v and W present. It is therefore necessary that there is a parallel class $\mathcal{L}_{ij}$ such that U and V are contained in two different (disjoint) blocks of $\mathcal{L}_{ij}$. To ensure that condition is satisfied our designs will be Hadamard designs constructed from *Paley tournaments.*

A tournament is a directed graph with no loops in which the underlying graph is the complete graph. Suppose that q is a prime power such that $q \equiv 3 \pmod 4$. Let $\mathbb{F}_q$ be the finite field on q elements. The vertices of the Paley tournament $\vec{P}_q$ are the elements of $\mathbb{F}_q$ and there is a directed edge from a vertex x to another vertex y if and only if $y - x$ is a square in $\mathbb{F}_q$. (The edges are directed because of the assumption on the modulus of q.) Let $A_q = (a_{i,j})$ be the adjacency matrix of $\vec{P}_q$, so that $a_{i,j} = +1$ if (i, j) is an edge of $\vec{P}_q$ and $a_{i,j} = -1$ if it is not. For $q = 3$, using $+$ in place of $+1$ and $-$ instead of -1, we have

$$A_q = \begin{pmatrix} 0 & + & - \\ - & 0 & + \\ + & - & 0 \end{pmatrix}.$$

Paley tournaments satisfy a version of the n-e.c. property given by Theorem 3.2, which is proved using quadratic residue characters as in the proof of Theorem 10, Section XIII.2, of Bollobás [2]. If U and W are disjoint sets of vertices of the Paley tournament $\vec{P}_q$, then we denote by $v(U, W)$ the number of vertices v not in $U \cup W$ such that (v, u) is a directed edge in $\vec{P}_q$ for each $u \in U$ and (w, v) is a directed edge in $\vec{P}_q$ for each $w \in W$ (so that (v, w) is not a directed edge).

Theorem 3.2 *Suppose that q is a prime power such that $q \equiv 3 \pmod 4$ and Let U and W be disjoint sets of vertices of the Paley tournament $\vec{P}_q$. and define n to be $n = |U|+|W|$. Then*

$$\left|v(U, W) - 2^{-n}q\right| \leq \frac{1}{2}\left(n - 2 + 2^{-n+1}\right) q^{1/2} + n/2.$$

Moreover, $v(U, W) > 0$ whenever $q > n^2 2^{2n-2}$.

Let I_q be the $q \times q$ identity matrix. Let $B_q = A_q - I_q$. Let C_q be the $(q+1) \times (q+1)$ matrix obtained by adding an initial row of 1's and a column of 1's. Then C_q is a Hadamard matrix. For $q = 3$ we have

$$B_3 = \begin{pmatrix} - & + & - \\ - & - & + \\ + & - & - \end{pmatrix}, \quad C_3 = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & - & - & + \\ + & + & - & - \end{pmatrix}.$$

For each q, the last q rows of C are the ± 1 incidence matrix of an affine design. Each parallel class contains two blocks, corresponding to $+$ and $-$. The columns correspond to the points of the design. Thus, from each Paley tournament $\vec{P}_q$ we get the incidence matrix D_q of a design on $q+1$ points with vertices corresponding to columns and parallel classes corresponding to rows, and with parameters $p = q$, $n = 2$, $r = (q+1)/4$, $s = (q-3)/4$ and $k = (q+1)/2$. In our running example

$$D_3 = \left(\begin{array}{cccc} + & - & + & - \\ + & - & - & + \\ + & + & - & - \end{array} \right).$$

The vertices are labelled from 1 to $q+1$.

One source of randomness in the graphs generated from Construction 1 comes from the labelling of the parallel classes in the second step. This is equivalent to randomly permuting the rows of D_q to get the incidence matrix of each $\mathcal{S}_i$, $i = 1, \ldots, q+1$. More precisely, if the incidence matrix of a design $\mathcal{S}_i$ is denoted by M_i, then the jth row of M_i is the $\pi_i(j)$th row of D_q for some permutation π_i. The total number of ways of choosing the π_i is $(q!)^{q+1}$,

The functions $\sigma_{i,j}$ in Construction 1 supply another source of randomness in the designs. Since there are $\binom{q+1}{2}$ functions to be chosen and 2 possibilities for each function (because $n = 2$), there is a total of $2^{\binom{q+1}{2}}$ possibilities for the $\sigma_{i,j}$. The fact that $(q!)^{q+1}$, grows more rapidly than $2^{\binom{q+1}{2}}$ may indicate that the choice of permutations adds more randomness to our construction than the choice of bijections.

Construction 2 is the version of Construction 1 that produces the graphs in Theorem 1.1.

Construction 2 Suppose that q is a prime power such that $q \equiv 3 \pmod 4$.

Choose permutations π_i, $1 \le i \le q+1$ independently and uniformly from the set of all permutations acting on $\{1, 2, \ldots, q\}$.

Let $\mathcal{S}_1, \ldots, \mathcal{S}_{q+1}$ be affine designs such that the point sets $V_1, \ldots, V_{q+1}$ are copies of $\{1, 2, \ldots, q+1\}$ and such that the jth row of M_i is the $\pi_i(j)$th row of D_q. Let $\mathcal{S}_i = (V_i, \mathcal{L}_i)$. Let $\mathcal{I} = \{1, \ldots, q+1\}$.

For every i, denote the parallel class of $\mathcal{S}_i$ corresponding to the jth row of M_i by symbols $\mathcal{L}_{ij}$, $j \in \mathcal{I} - \{i\}$. For $v \in V_i$, let $l_{ij}(v)$ denote the line in the parallel class $\mathcal{L}_{ij}$ which contains v. Each line in a parallel class consists of $(q+1)/2$ points and each parallel class consists of two lines.

For every pair i, j, $i \neq j$, choose an arbitrary bijection $\sigma_{i,j} : \mathcal{L}_{ij} \to \mathcal{L}_{ji}$ arbitrarily from the 2 possibilities; we only require that $\sigma_{j,i} = \sigma_{i,j}^{-1}$.

Construct a graph $\mathcal{G}_1 = \mathcal{G}_1((\mathcal{S}_i), (\sigma_{i,j}))$ on the vertex set $X = \cup_{i \in \mathcal{I}} V_i$. The sets V_i will be independent. Two vertices $v \in V_i$ and $w \in V_j$, $i \neq j$, are adjacent in $\mathcal{G}_1$ if and only if $w \in \sigma_{i,j}(l_{ij}(v))$ (or, equivalently, $\sigma_{i,j}(l_{ij}(v)) = l_{ji}(w)$).

Theorem 3.1 guarantees that Construction 2 produces graphs that are $SR((q+1)^2, q(q+1)/2, (q^2-1)/4, (q^2-1)/4)$.

Lemma 3.3 *Construction 2 produces at least $2^{\binom{q+1}{2}(1-\varepsilon(q))}$ non-isomorphic graphs.*

Proof The number of graphs generated by Construction 2 is $2^{\binom{q+1}{2}}(q!)^{q+1}$. To bound the number of graphs G isomorphic to a specific graph $\tilde{G}$, consider the following way of choosing vertices:

(i) Choose $q+1$ vertices in G corresponding to V_1 in $\tilde{G}$. This can be done in at most $(q+1)^{2(q+1)}$ ways. The vertices in G corresponding to the lines of the $\pi_i(1)$st parallel class of V_i in $\tilde{G}$ are now determined. In particular set of vertices corresponding to each V_i are determined.

(ii) Choose the correspondences to the vertices in G to those in each V_i, $2 \le i \le q+1$. This can be done in $((q+1)!)^q$ ways (and determines all π_i and all $\sigma_{i,j}$).

The number of isomorphism classes is at least

$$2^{\binom{q+1}{2}}(q!)^{q+1} / \left((q+1)^{2(q+1)}((q+1)!)^q\right) = 2^{\binom{q+1}{2}(1-\varepsilon(q))},$$

where $\varepsilon(q) = O\left(q^{-1}\log q\right)$. ■

4 Proof of the n-e.c. property

Fix a pair of disjoint subsets of vertices U, W in the graph in Construction 2 such that $|U|+|W|=n$. Let U_i be the set of points of V_i which are vertices in U and let W_i be the set of points of V_i which are vertices in W. Define $G_i = G_i(U,W)$ to be the labels of the parallel classes in the (unpermuted) design D_q for which all of the U_i are in one block and all of the W_i are in the other. The parallel classes in G_i are the ones which "separate" U_i and W_i. Define $\Gamma(U,W)$ to be

$$\Gamma(U,W) = \{i \in [1, q+1] : U_i = W_i = \emptyset\}.$$

If $i \in \Gamma(U,W)$, then $G_i = \{1,2,\ldots,q\}$. Define $n_i = |U_i| + |W_i|$ for $i \in [1, q+1]$.

Lemma 4.1 *For each $i \in [1, q+1]$,*

$$|G_i| \ge 2^{-n_i}q - n_i q^{1/2} - n_i.$$

Proof The conclusion of the lemma is trivially true for $i \in \Gamma(U,W)$. Observe that for $i \notin \Gamma(U,W)$,

$$|G_i| = \begin{cases} v(U_i,W_i) + v(W_i,U_i) & \text{if } \ 1 \notin U_i \cup W_i; \\ v(U_i - \{1\}, W_i) & \text{if } \ 1 \in U_i; \\ v(W_i - \{1\}, U_i) & \text{if } \ 1 \in W_i, \end{cases}$$

where $v(U,W)$ was defined just before Theorem 3.2. If $1 \notin U_i \cup W_i$, then Theorem 3.2 gives $v(U_i,W_i) \ge 2^{-n_i}q - \frac{1}{2}n_i q^{1/2} - \frac{n_i}{2}$, and the same lower bound holds for $v(W_i,U_i)$. Therefore $|G_i| \ge 2^{-n_i+1} - n_i q^{1/2} - n_i$ and the conclusion of the lemma follows. If $1 \in U_i$, then Theorem 3.2 gives $G_i = v(U_i - \{1\}, W_i) \ge 2^{-(n_i-1)}q - n_i q^{1/2} - n_i$. A similar argument is used for the case $1 \in W_i$. ■

Recall from Construction 2 that $\mathcal{I} = \{1,\ldots,q+1\}$. A design V_i with $i \in \Gamma(U,W)$ is said to be *good* for U, W if $\pi_k(i) \in G_k$ for each $k \in \mathcal{I} - \Gamma(U,W)$ and is said to be *bad* for U, W otherwise. The number of vertices in a design V_i good for U, W which are adjacent to all vertices in U and not adjacent to any vertices in W corresponds to the columns in D_q for which a set of $q+1-|\Gamma(U,W)| \leq n$ rows match a certain pattern of 0's and 1's. If $q > n^2 2^{2n-2}$, then Theorem 3.2 implies for each good design V_i there exists at least one (actually many) points of V_i satisfying the conditions of the n-e.c. property for U, W. Therefore, if $q > n^2 2^{2n-2}$, then a graph constructed with Construction 1 satisfies the n-e.c. property for U, W whenever some design V_i is good for U, W. Therefore, to prove that the graphs described by Construction 2 are n-e.c., it suffices to show that there exists at least one good design for every pair U, W.

For each $i \in \Gamma(U,W)$ let I_i be the indicator random variable

$$I_i = I\left[V_i \text{ is good for } U, W\right].$$

Define $X = X(U,W)$ to be

$$X = \sum_{i \in \Gamma(U,W)} I_i.$$

Let us say that a pair U, W is *bad* if there is no vertex $v \in V - (U \cup W)$ such that v is adjacent to all edges in U and adjacent to no edge in W. Let $\mathcal{N}_q(U,W)$ denote the event that the pair U, W is bad for the random graph in Construction 2. Then, by the previous paragraph,

$$\mathbb{P}(\mathcal{N}_q(U,W)) \leq \mathbb{P}(X=0). \tag{1}$$

The remaining part of the proof gets a lower bound on $\mathbb{P}(X > 0)$, hence an upper bound on $\mathbb{P}(X=0)$, by using a large deviations result from Poisson approximation theory. We begin with a lower bound on $\mathbb{E}X$.

Lemma 4.2 *Assume that $q \geq 16n^2 2^{2n}$. Then for U and W such that $|U|+|W| = n$,*

$$\mathbb{E}X \geq (q-n)\, 2^{-n} \exp\left(-4n 2^n q^{-1/2}\right).$$

Proof Fix a vertex $i \in \Gamma(U,W)$. Then

$$\begin{aligned}
\mathbb{E}X &\geq (q-n)\,\mathbb{E}I_i \\
&= (q-n)\prod_{j=1}^{q} \frac{|G_j|}{q} \\
&\geq (q-n)\prod_{j=1}^{q}\left(\frac{2^{-n_j}q - n_j q^{1/2} - n_j}{q}\right) \qquad (2)\\
&= (q-n)2^{-n}\prod_{j=1}^{q}\left(1 - \frac{n_j 2^{n_j}}{\sqrt{q}} - \frac{n_j 2^{n_j}}{q}\right) \\
&\geq (q-n)2^{-n}\prod_{j=1}^{q}\left(1 - \frac{2n_j 2^{n_j}}{\sqrt{q}}\right),
\end{aligned}$$

where we have used Lemma 4.1 at (2). Whenever $0 < x < 1/2$, $\log(1-x) \geq -2x$ and $1-x \geq e^{-2x}$, so

$$\begin{aligned}
\mathbb{E}X &\geq (q-n)2^{-n} \prod_{j=1}^{q} \exp\left(-\frac{4n_j 2^{n_j}}{\sqrt{q}}\right) \\
&\geq (q-n)2^{-n} \prod_{j=1}^{q} \exp\left(-\frac{4n_j 2^{n}}{\sqrt{q}}\right) \\
&= (q-n)2^{-n} \exp\left(-\frac{4n 2^{n}}{\sqrt{q}}\right). \quad \blacksquare
\end{aligned}$$

We now discuss a general result from Poisson approximation theory. Suppose that $(I_i;\, i \in \Gamma)$ are random variables with indices i in Γ, where Γ is some arbitrary set of indices. The probability law of the I_i conditioned on the event $\{I_i = 1\}$ is denoted by $\mathcal{L}(I_j;\, j \in \Gamma | I_i = 1)$. We say that the I_i are *negatively related* if for each $i \in \Gamma$ random variables $(J_{j,i};\, j \in \Gamma)$ can be defined on the same probability space as $(I_j;\, j \in \Gamma)$ in such a way that, firstly,

$$\mathcal{L}(J_{j,i};\, j \in \Gamma) = \mathcal{L}(I_j;\, j \in \Gamma | I_i = 1)$$

and, secondly,

$$J_{j,i} \leq I_j \textit{ for all } j \in \Gamma.$$

A special case of Theorem 2.R of the standard text [1] on Poisson approximation, which contains many more interesting results and examples, is

Theorem 4.3 *For any sum $Y = \sum_{i \in \Gamma} I_i$ of negatively related indicator variables*

$$\mathbb{P}(Y = 0) \leq 2e^{-\mathbb{E}X}.$$

The next lemma bounds the probability that the pair U, W is bad.

Lemma 4.4 *The probability of the event $\mathcal{N}_q$ is bounded above by*

$$\mathbb{P}(\mathcal{N}_q) \leq 2\exp\left(-(q-n)2^{-n}\exp\left(-\frac{4n2^n}{\sqrt{q}}\right)\right). \tag{3}$$

Proof We will show that $\mathbb{P}(X = 0)$ is bounded by the right hand side of (3) and then apply (1). Since $\mathbb{E}I_i = \mathbb{P}(I_i = 0)$, it suffices to prove that the variables $(I_i, i \in \Gamma)$ are negatively related and then apply Theorem 4.3 and Lemma 4.2.

We will now construct the random variables $J_{j,i}$ in the definition of negatively related indicators. If $I_i = 1$, then simply define $J_{j,i} = I_j$ for all $j \in \Gamma(U, W)$. The harder part is constructing $J_{j,i}$ when $I_i = 0$.

Fix $i \in \Gamma(U, W)$ and let k be an index taken over $\mathcal{I} - \Gamma(U, W)$. Conditional on $I_i = 1$, it follows from the definition of a design good for U, W (after Lemma 4.1) and the independence of the permutations π_k, that the $\pi_k(i)$ are uniformly distributed over the G_k and are mutually independent. If $I_i = 0$, then for each k such that $\pi_k(i) \notin G_k$ choose random elements $\gamma_k \in G_k$ such that the γ_k are independent and uniformly distributed over G_k. Replace each π_k for which $\pi_k(i) \notin G_k$ with $\phi_k \circ \pi_k$, where $\phi_k = (\pi_k(i)\ \ \gamma_k)$ is a transposition and $\phi \circ \pi(i) = \phi(\pi(i))$. Define $J_{j,i}$ for $j \in \Gamma(U,W)$ as in the definition of I_j, but using $\phi_k \circ \pi_k$ in place of π_k whenever $\pi_k(i) \notin G_k$. If $\pi_k(i) \in G_k$, then continue to use π_k.

In this construction the $J_{j,i}$ have the right distribution and are bounded by I_j, proving that the $(I_i, i \in \Gamma(U,W))$ are negatively related. ■

Proof of Theorem 1.1 Let Z be the expected number of bad pairs U, W and suppose that for $q \geq 16n^2 2^{2n}$. Using the immediate bounds $n \leq \log_2 q$ and $2^{-n} \geq 4nq^{-1/2} \geq 4q^{-1/2}$, we have

$$\begin{aligned}
\mathbb{E}Z &\leq \binom{(q+1)^2}{n} 2^n \cdot 2\exp\left(-(q-n)2^{-n}\exp\left(-\frac{4n2^n}{\sqrt{q}}\right)\right) \\
&\leq (q+1)^{2n} 2^n \cdot 2\exp\left(-(q-n)2^{-n}\exp\left(-\frac{4n2^n}{\sqrt{q}}\right)\right) \\
&\leq (q+1)^{2\log_2 q+1} \cdot 2\exp\left(-(q-\log_2 q)\frac{4e^{-1}}{\sqrt{q}}\right) \\
&\leq c_1 \exp\left(-c_2 q^{1/2}\right)
\end{aligned}$$

for some constants $c_1, c_2 > 0$. Since $\mathbb{P}(Z > 0) \leq \mathbb{E}Z$ for all nonnegative integer-valued random variables Z, we have the bound $\mathbb{P}(Z > 0) \leq c_1 \exp\left(-c_2 q^{1/2}\right)$ for the probability that there exist *any* bad pairs U, W for the graphs of Construction 2. The number of graphs without any bad pairs U, W is therefore at least $2^{\binom{q+1}{2}}(q!)^{q+1}\left\{1 - c_1\exp\left(-c_2 q^{1/2}\right)\right\}$. Theorem 1.1 results from the proof of Lemma 3.3 applied to those graphs. ■

5 Further remarks

We can obtain further strongly regular graphs with the e.c. property from our examples using switching (see Seidel [8]) as follows. Let v be any vertex of a n-e.c. graph Γ. Switch with respect to the neighbours of v, and delete v. The resulting graph Γ' is $(n-1)$-e.c. Moreover, if Γ is strongly regular with parameters $((q+1)^2, q(q+1)/2, (q^2-1)/4, (q^2-1)/4)$, then Γ' is strongly regular with parameters $(q(q+2), (q+1)^2/2, (q+1)^2/4, (q+1)^2/4)$.

The n-e.c. property in graphs produced by Construction 1 depends crucially on the designs used. If we use affine geometries in place of Paley designs, we can do no better than 3-e.c.:

Proposition 5.1 *Let $\mathcal{G}_1 = \mathcal{G}_1((\mathcal{S}_i), (\sigma_{i,j}))$ be a strongly regular graph produced by Construction 1. Suppose that at least one of the designs $\mathcal{S}_i$ is an affine geometry over $\mathbb{F}_2$. Then $\mathcal{G}_1$ does not satisfy 4-e.c.*

Proof Suppose that $\mathcal{S}_1$ is an affine geometry, and let v, w, x, y be an affine plane of $\mathcal{S}_1$. Then any hyperplane containing three of v, w, x, y contains the fourth; so every vertex joined to three of these vertices is also joined to the fourth. ■

Thomason [9] defined a class of "pseudo-random" graphs which he called *jumbled graphs*. He showed that these share many properties with random graphs. However, the n-e.c. property for large n is not such a property: in fact, one of Thomason's graphs arises from Construction 1 using affine geometries over $\mathbb{F}_2$.

The usual description of the graph $\mathcal{G}(n)$ is as follows. Let

$$Q(x) = x_1 x_{n+1} + x_2 x_{n+2} + \cdots + x_n x_{2n}$$

be a quadratic form on the vector space $V = \mathbb{F}_2^{2n}$. The vertex set of the graph is V, and vertices v, w are joined if and only if $Q(v - w) = 1$.

We re-formulate the definition as follows. Let $W = \mathbb{F}_2^n$. Then $V = W \oplus W$; we write a typical vector as (x, a), and let $W_a = \{(x, a) : x \in W\}$. Then $Q(x, a) = x \cdot a$ (the standard inner product).

Each set W_a is naturally bijective with $W = \mathbb{F}_2^n$, the point set of the affine geometry. A parallel class of hyperplanes in W is given by

$$H(c, i) = \{x \in W : x \cdot c = i\} \text{ for } i = 0, 1,$$

for each non-zero $c \in W$. Thus, we can label the parallel classes in W_a by vectors $b \neq a$, where the parallel class labelled by b is

$$\mathcal{L}_{ab} = \{(H(a + b, 0), a), (H(a + b, 1), a)\}.$$

Now the neighbours of (y, b) in W_a are precisely the points (x, a) which satisfy $(x - y) \cdot (a - b) = 1$. If $a = b$, there are no such vertices. If $a \neq b$, then $(x, a) \in ((H(a + b), i), a)$ and $(y, b) \in ((H(a + b), j), b)$ satisfy $x \cdot (a + b) = i$ and $y \cdot (a + b) = j$, so they are joined if and only if $i - j = 1$. Thus, choosing the bijection $\sigma_{a,b}$ to map $((H(a + b), i), a)$ to $((H(a + b), i + 1), b)$, we see that Construction 1 does produce this graph.

We conclude by noting that, even though $\mathcal{G}(n)$ fails to be 4-e.c., it has a much stronger version of the 3-e.c. property, considered by Cameron *et al.* [5]: for every pair of subsets U, W of the vertex set V such that $U \cap W = \emptyset$ and $|U| + |W| = 3$, the number of vertices $v \in V - (U \cup W)$ joined to every vertex in U and to none in W depends only on the induced subgraph on $U \cup W$ with distinguished subset U (and this number is non-zero provided that $n \geq 3$).

References

[1] Barbour, A. D., Holst, L. and Janson, S., *Poisson Approximation*, Oxford University Press, Oxford, 1992.

[2] Bollobás, B., *Random Graphs*. Academic Press, London, 1985.

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

[4] Bonato, A., Holzmann, W. H., Kharaghani, H., Hadamard matrices and strongly regular graphs with the 3-e.c. adjacency property, *Electronic J. Combinatorics*, **8(1)** (2001), #R1, 9pp.

[5] Cameron, P. J., Goethals, J.-M., Seidel, J. J., Strongly regular graphs having strongly regular subconstituents, *J. Algebra* **55** (1978), 257–280.

[6] Fon-Der-Flaass, D. G., New prolific constructions of strongly regular graphs. Preprint.

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

[8] Seidel, J. J., A survey of two-graphs, pp. 481–511 in *Proc. Internat. Coll. Teorie Combinatorie* (Roma 1973), Accad. Naz. Lincei, Roma, 1977.

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

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