2010

Computational and Theoretical Aspects of *N*-E.C. Graphs

Alexandru Costea
Wilfrid Laurier University

Your file Votre référence
ISBN: 978-0-494-64358-7
Our file Notre référence
ISBN: 978-0-494-64358-7

COMPUTATIONAL AND THEORETICAL ASPECTS OF N-E.C. GRAPHS

by

Alexandru Costea
BSc, Wilfrid Laurier University, 2006

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for
Master of Science and Finance

Wilfrid Laurier University
January 21 2010

The undersigned hereby certify that they have read and recommend to the Faculty of Mathematics for acceptance a thesis entitled "COMPUTATIONAL AND THEORETICAL ASPECTS OF N-E.C. GRAPHS" by Alexandru Costea in partial fulfillment of the requirements for the degree of Master of Science and Finance.

Dated: January 21 , 2010

Supervisor: _____
Professor Anthony Bonato

Readers: _____
Professor Joe Campolieti

_____
Professor Peter Danziger

_____
Professor Roderick Melnik

Table of Contents

List of Figures

Abstract

We consider graphs with the n-existentially closed adjacency property. For a positive integer n, a graph is *n-existentially closed* (or *n-e.c.*) if for all disjoint sets of vertices A and B with $|A \cup B| = n$ (one of A or B can be empty), there is a vertex z not in $A \cup B$ joined to each vertex of A and no vertex of B. Although the n-e.c. property is straightforward to define, it is not obvious from the definition that graphs with the property exist. In 1963, Erdős and Rényi gave a non-explicit, randomized construction of such graphs. Until recently, only a few explicit families of n-e.c. graphs were known such as Paley graphs. Furthermore, n-e.c. graphs of minimum order have received much attention due to Erdős' conjecture on the asymptotic order of these graphs. The exact minimum orders are only known for $n = 1$ and $n = 2$.

We provide a survey of properties and examples of n-e.c. graphs. Using a computer search, a new example of a 3-e.c. graph of order 30 is presented. Previously, no known 3-e.c. graph was known to exist of that order. We give a new randomized construction of n-e.c. vertex-transitive graphs, exploiting Cayley graphs. The construction uses only elementary probability and group theory.

Acknowledgements

I would like to acknowledge the support of my advisor Dr. Anthony Bonato. I would like to thank him for his guidance and instruction. I am grateful to the Department of Mathematics at Wilfrid Laurier University for the academic opportunities they have presented me, and for the family feeling that the department and university convey. A special thanks to Dr. Joe Campolieti, Dr. Peter Danziger, Dr. Roderick Melnik, for being part of my thesis committee. Finally, I would like to thank Dr. Gordon Royle and Dr. Ted Spence for help with the graph data sets used in Chapter 3.

Chapter 1

INTRODUCTION

1.1 Motivation and Background

The purpose of the thesis is to investigate adjacency properties of graphs. An *adjacency property* is a global property of a graph, where given a fixed subset of vertices S, there exists vertices outside of S joined to vertices of S in a predetermined way. Adjacency properties stem from a seminal paper on random graphs by Erdős and Rényi [14] published in 1963. One particular adjacency property that has received much recent attention is the n-e.c. property. For a positive integer n, a graph is *n-existentially closed* (or *n-e.c.*) if for all disjoint sets of vertices A and B with $|A \cup B| = n$ (one of A or B can be empty), there is a vertex z not in $A \cup B$ joined to each vertex of A and no vertex of B. We say that z is *correctly joined* (or *c.j.*) to A and B. A visual representation of this property is presented in Figure 1.1. Hence, for all n-subsets S of vertices,

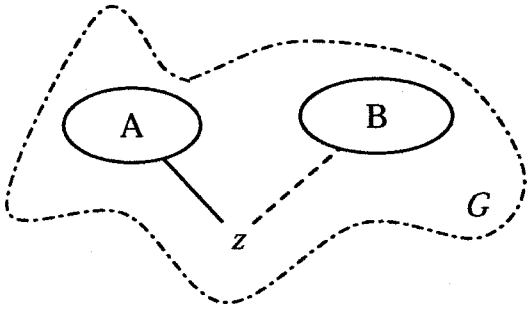


Figure 1.1: Abstract representation of the n-e.c. property.

there exist 2^n-many vertices joined to S in all possible ways. Although

the n-e.c. property is straightforward to define, it is not obvious from the definition that graphs with the property exist. Erdős and Rényi gave a non-explicit, randomized construction of such a graph in [14]. Explicit examples of n-e.c. graphs were later introduced in [7] who used graphs defined over certain finite fields. Almost all finite graphs are n-e.c. (in a sense to be made precise in Section 2.1) but, until recently, only a few explicit constructions were known. Furthermore, n-e.c. graphs of minimum order have received much attention due to Erdős' conjecture on the asymptotic order of these graphs. The exact minimum orders are only known for $n = 1$ and $n = 2$.

The n-e.c. graphs are an instance of *pseudo-random graphs*; that is, deterministic graphs which satisfy some of the properties of random $G(m, p)$ graphs (see [28]). Two key properties of random graphs with applications to real-world networks are universality and expansion. As we will prove in Theorem 2.4, an n-e.c. graph G is $(n+1)$-*universal*: that is, each graph of order at most $n + 1$ is isomorphic to an induced subgraph of G. Universal graphs have numerous applications in computer science. Several optimization problems in data representations (see [13]), data structures (see [24]), and circuit design (see [29]) surround problems on certain universal graphs. An *expander* graph has high connectivity properties. To be more precise, given a set S of vertices, define the *boundary* of S, written $\partial(S)$, to be the set of edges with one end in S, and the other outside S. Expander graphs require that for all "small" sets of vertices (where small usually means a fraction of the order of the graph), the ratio of the cardinality of $\partial(S)$ to the order of S is greater than or equal to some fixed positive constant. Expander graphs have several applications to theoretical computer science, design of robust computer networks, and the theory

of error-correcting codes (see [1], for example). Certain well-known families of n-e.c. graphs—such as Paley graphs and certain random Cayley graphs—are expanders [1]. The n-e.c. graphs witness a type of expansion described in Lemma 2.1.

The focus of the remainder of this chapter is to recall various notations and concepts from graph theory, probability theory and finite fields that will be used in later chapters. We conclude this introductory chapter with an outline of the remainder of the thesis.

1.2 Mathematical Concepts

Graphs are both highly useful and beautiful mathematical structures. This section provides some of the basic terminology and operations needed for the study of graphs and lists several useful families of graphs. Some families of graphs stem from other mathematical areas such as finite fields and probability theory. We present some of the graph concepts needed to describe such families of graphs. For a good reference on graph theory, see [30].

1.2.1 Graph Theory

A *graph* is a pair $G = (V(G), E(G))$ of sets such that $V(G)$ is non-empty, and $E(G)$ is a set of unordered pairs from $V(G)$. For simplicity, we often write $V(G) = V$ and $E(G) = E$. The elements of V are the *vertices* (or *nodes*) of the graph G and the elements of E are its *edges* defined in terms of the nodes. We take V (and hence, E) to be finite, unless otherwise stated. The usual way to picture a graph is by drawing a dot for each vertex and joining two of these dots by a line if the corresponding two vertices form an edge. As an example, in Figure 1.2 we give three

drawings of the *Petersen graph*. A graph is called *simple* if it consists of

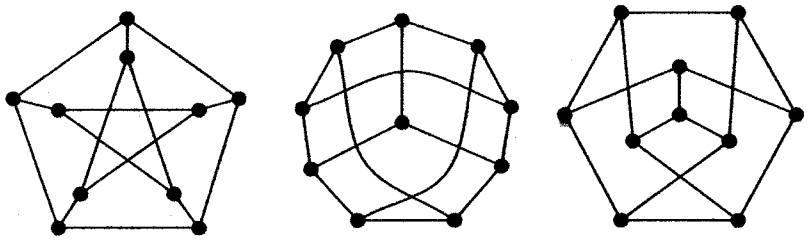


Figure 1.2: Three drawings of the Petersen graph.

no loops nor multiple edges, while an *undirected* graph forces E to be a symmetric relation. We will always consider simple, undirected graphs, unless we state otherwise. The number of vertices of a graph is its *order*, written $|V|$, while the number of edges, denoted by $|E|$ is its *size*. If $\{u, v\} \in E$, then we denote the edge by uv. We say that u is *joined* to v or that u is *adjacent* to v and write $u \sim v$. We say that u and v are both *incident* to the edge and that u and v are the *endpoints* of uv. The set E may be empty. For all graphs, as there are at most as many edges as distinct pairs of vertices, the following inequality holds:

$$|E| \leq \binom{|V|}{2}.$$

Graphs are often used in network analysis. In this context the term *network* may differ and is often referred to as a simple graph. Hence, a graph is also known as a *network*, especially with respect to real-world examples.

Given any subset $S \subset V$ in G, the *subgraph induced* by S in G, denoted by $G \restriction S$, has two vertices joined if and only if they are joined in G. Given a vertex x, the induced subgraph formed by deleting x is

denoted by $G - x$.

Certain special types of graphs play prominent roles in graph theory. For example, a *complete* graph of order n, denoted by K_n, has the property that each pair of distinct vertices are adjacent. A graph is *bipartite* if its vertices can be partitioned into two sets X_1 and X_2 such that any two adjacent vertices are not both in the same X_i, where $i = 1, 2$. A *complete bipartite* graph, written $K_{m,n}$, has $|X_1| = m$, and $|X_2| = n$, and each vertex of X_1 is joined to each vertex of X_2. Figure 1.3 depicts a complete graph and complete bipartite graph. The maximum integer r such that K_r is an induced subgraph of G is called the *clique number of* G, and is written $\omega(G)$. For example, $\omega(K_5) = 5$, while $\omega(K_{3,3}) = 2$.

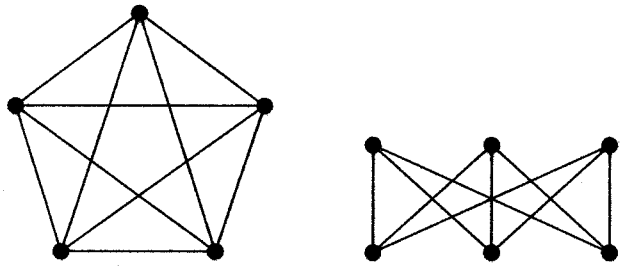


Figure 1.3: The complete graph K_5 and the complete bipartite graph $K_{3,3}$.

A *walk* in a graph consists of an alternating sequence of vertices and edges

$$x_0, e_1, x_1, \ldots, e_t, x_t \tag{1.1}$$

so that for all $1 \leq i \leq t$, $e_i = x_{i-1}x_i$. Note that vertices and edges may be repeated in a walk. To be explicit about the endpoints, we sometimes refer to (1.1) as an x_0,x_t-*walk*. A walk is *closed* if $x_0 = x_t$; otherwise, it is *open*. The number of edges is the *length* of the walk. A *path* is an open walk with no repeated vertex. A *cycle* is a closed walk with no repeated

vertex. The path of length n is P_n, and the cycle of length n is C_n.

A graph is *connected* if for each pair of vertices there is a path between them. The relation of being connected by a path is an equivalence relation on V, and the equivalence classes are the *connected components* of G. A graph which is not connected is called *disconnected*; a connected component consisting of a single vertex is called an *isolated vertex.* A vertex joined to all other vertices is called *universal.* The *complement* $\overline{G}$ of G is the graph whose vertex set is V and whose edges are the pairs of non-adjacent vertices of G.

The *distance* between u and v, written $d(u, v)$, is either the length of a shortest path connecting u and v (and 0 if $u = v$) or ∞ otherwise. Note that $d(u, v)$ turns each connected graph into a metric space. The *diameter* of a connected graph G, written $\text{diam}(G)$, is the maximum of all distances between distinct pairs of vertices. If the graph is disconnected, then $\text{diam}(G)$ is ∞.

The set of vertices joined to a given vertex $u \in V(G)$ is called the *neighbour* set of u, written $N(u)$. The cardinality of this set is called the *degree* of vertex u, denoted by $\deg_G(x)$. The following theorem is called the *First Theorem of Graph Theory* and it establishes a fundamental relationship between number of edges and the degrees of the vertices in a graph. The proof follows the one found in [30].

Theorem 1.1. *For a graph $G = (V, E)$ we have that*

$$\sum_{v \in V} \deg_G(v) = 2|E|. \tag{1.2}$$

Proof. Each edge is incident to two vertices, thus contributing to the degree of two distinct vertices. Counting the degrees of every vertex in

the graph, the equation (1.2) follows. □

A graph G is *k-regular* if $\deg_G(v) = k$ for all $v \in V$. For example, K_n is $(n-1)$-regular. A 3-regular graph with diameter 3 is given in Figure 1.4. The set $N^c(u)$ is the set of all vertices not joined to u excluding u itself.

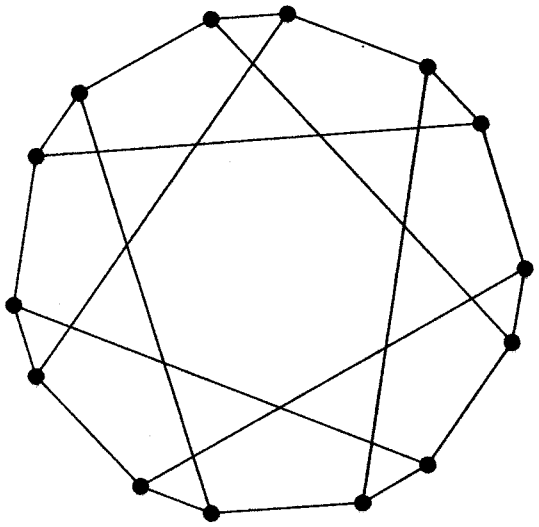


Figure 1.4: A 3-regular graph with diameter three.

We note that a partition of the vertex set of a graph is $\{u\}, N(u), N^c(u)$. Figure 1.5 illustrates this partition for a graph of order seven. A *k-colouring* of a graph is a vertex partition into k independent sets. The *chromatic number*, written $\chi(G)$, is the smallest integer k such G has a k-colouring.

An important concept in graph theory is the notion of isomorphism. A *homomorphism* f between graphs G and H is a function $f : V(G) \to V(H)$ which *preserves edges*; that is, if $xy \in E(G)$, then $f(x)f(y) \in E(H)$. We abuse notation and simply write $f : G \to H$. An *embedding* from G to H is an injective homomorphism $f : G \to H$ with the property that $xy \in E(G)$ if and only if $f(x)f(y) \in E(H)$. We will write $G \leq H$ if there is some embedding of G into H, and say that G *embeds in* H. An

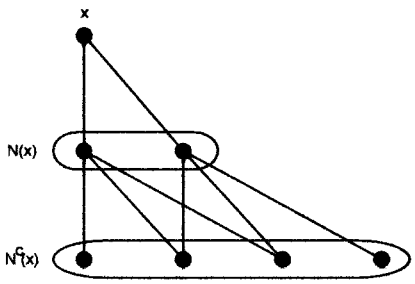


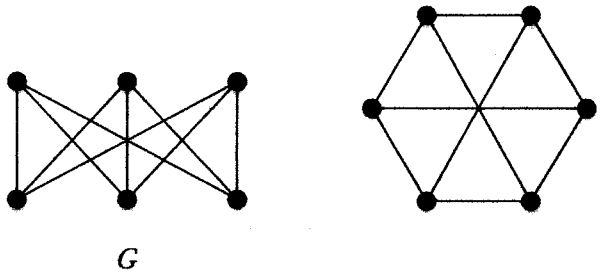
Figure 1.5: A 3-colouring of a graph.

isomorphism is a bijective embedding; if there is an isomorphism between two graphs, then we say they are *isomorphic*. We write $G \cong H$ if G and H are isomorphic. For an example, consider graphs G and H shown in Figure 1.6. It can be directly verified that the mapping f, given by

$$1 \to a, 2 \to e, 3 \to c, 4 \to f, 5 \to b, 6 \to d$$

is an isomorphism between G and H. (Note that the mapping is not unique.) The relation $\cong$ is an equivalence relation on the class of all graphs, whose equivalence classes are *isomorphism types* or *isotypes*. We will always identify a graph with its isomorphism type. An *automorphism* of a graph G is an isomorphism from G to itself; the set of all automorphisms forms a group under the operation of composition, written $\mathrm{Aut}(G)$. A graph G is *vertex-transitive* if for every pair of vertices u and v there is automorphism of G mapping u to v.

There are several ways to represent graphs. One common representation describing the relationship between vertices and edges is the so-called *adjacency matrix* representation. Suppose that G is a graph, and without loss of generality, assume that $V = \{1, 2, 3, \ldots, n\}$. Let A be a $n \times n$



G

Figure 1.6: Isomorphic graphs.

matrix, where the (i, j) entry of A is denoted by $a_{i,j}$. We define the *adjacency matrix* $A(G)$ of a graph G of order n to be the $n \times n$ matrix defined as follows:

$$a_{i,j} = \begin{cases} 0 & \text{if } i = j \text{ or } ij \notin E(G), \\ 1 & \text{otherwise.} \end{cases}$$

Notice that the adjacency matrix of a undirected graph is symmetric with 0's on the main diagonal. Figure 1.7 depicts the so-called *lattice graph of order* 12. The adjacency matrix $A(G)$ of G is given by

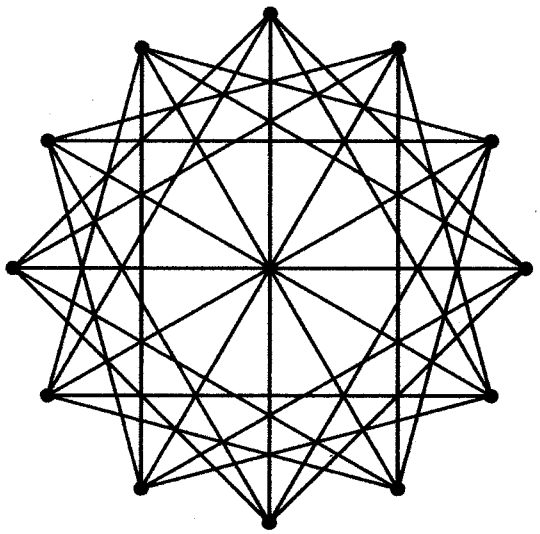


Figure 1.7: The lattice graph of order 12.

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

1.2.2 Discrete Probability Theory

We now present concepts from discrete probability theory that will be used in this thesis. This will help in proving results related to the random graph $G(n,p)$ in Chapter 2, and results on random Cayley graphs in Chapter 4.

The *probabilistic method* is a powerful tool for tackling many problems in discrete mathematics. Roughly speaking, the method works as follows: when attempting to prove that a structure with certain desired properties exists, one defines an appropriate probability space of structures and then shows that the desired properties hold in these structures with positive probability (or even better: with probability tending to 1 as the order of the structures tends to ∞).

For simplicity, we consider only finite, discrete probability spaces. A *probability space* $(\Omega, \mathcal{F}, \mathbb{P})$, consists of a finite set Ω, called the *sample*

space, $\mathcal{F}$ is the collection of all subsets of Ω, and *probability function* $\mathbb{P} : \Omega \to [0,1]$ satisfying $\sum_{\omega \in \Omega} \mathbb{P}(\omega) = 1$. A subset of the sample space Ω, is called an *event*. The function $\mathbb{P}$ must satisfy the following properties.

1. For all events $\omega \in \mathcal{F}$, $\mathbb{P}(\omega) \in [0,1]$ and $\mathbb{P}(\Omega) = 1$.

2. If $(A_i : i \in I)$ is a countable set of events that are pairwise disjoint, then

$$\mathbb{P}(\bigcup_{i \in I} A_i) = \sum_{i \in I} \mathbb{P}(A_i)$$

An important example for us of a probability space are random graphs. Roughly speaking, random graphs arise by choosing edges among pairs of distinct vertices independently with a given probability. To be more precise, the *random graph* $G(m,p)$ consists of the probability space $(\mathcal{G}_m, \mathcal{F}, \mathbb{P})$, where $\mathcal{G}_m$ is the set of all graphs with vertex set $[n] = \{1, 2, \ldots, m\}$, $\mathcal{F}$ is the family of all subsets of $\mathcal{G}_m$. Each graph is chosen independently (two events X and Y are *independent* if and only if $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$). There are $|\mathcal{G}_m| = 2^{\binom{m}{2}}$ graphs, so the probability function is given by

$$\mathbb{P}(G) = 2^{-\binom{m}{2}}, \text{ for all } G \subset \mathcal{G}_m.$$

A more general probability space on the set $\mathcal{G}_m$ may be obtained by fixing a real number $p \in (0,1)$ and choosing each edge with probability p. This space may be viewed as $\binom{m}{2}$ independent coin flips, one for each pair of vertices where the probability of success (that is, drawing an edge) is equal to p. The probability of one edge not drawing an edge is $1-p$ and so the probability function $\mathbb{P}$ is given by For every $G \in \mathcal{G}_m$

$$\mathbb{P}(G) = p^{|E(G)|}(1-p)^{\binom{m}{2}-|E(G)|} \tag{1.3}$$

Observe that in the special case where $p = 1/2$ that

$$\mathbb{P}(G) = \left(\frac{1}{2}\right)^{\binom{m}{2}}.$$

We say that an event holds *asymptotically almost surely* (a.a.s.) in $G(m,p)$ if it holds with probability tending to 1 as $m \to \infty$. For example, as we will prove in Theorem 2.1, $G(m,1/2)$ a.a.s. satisfies the n-e.c. property for a fixed positive integer n.

We will consider asymptotic results on probability spaces such as $G(m,p)$, so we recall asymptotic notation. Let f and g be functions whose domain is some fixed subset of $\mathbb{R}$. We write $f \in O(g)$ if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)}$$

exists and is finite. We will the standard notation and write $f = O(g)$. We write $f = \Omega(g)$ if $g = O(f)$, and $f = \Theta(g)$ if $f = O(g)$ and $f = \Omega(g)$. If

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0,$$

then $f = o(g)$. So if $f = o(1)$, then f tends to 0. We write $f \sim g$ if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

All logarithms are in base e, and written (keeping with the convention among random graph theorists) as $\log x$ (i.e. $\log x \equiv \ln x$). If $0 \leq m \leq n$ are integers with $n > 0$, then we will use the following inequality for binomial coefficients:

$$\binom{n}{m} \leq \left(\frac{n}{2}\right)^m \leq n^m.$$

1.2.3 Graphs from Algebra: Paley and Cayley Graphs

We will use abstract algebra to describe certain classes of graphs called *Paley* and *Cayley graphs*. As we will see, Paley graphs are derived from finite fields, while Cayley graphs are defined using groups.

The finite fields are classified by size; in particular, there is exactly one finite field up to isomorphism of size p^k for each prime p and positive integer k, written $GF(p^k)$ (where "GF" stands for *Galois Field*; see [18]). For further discussion of algebraic structures in the context of graph theory, please see [15].

Now let q be a prime power such that $q \equiv 1 \pmod 4$. The *Paley graph of order* q is the graph P_q whose vertices are the elements of the finite field $GF(q)$ in which two distinct vertices x and y are joined if and only if $x - y$ is a square in $GF(q)$. Since $q \equiv 1 \pmod 4$, it follows that -1 is a contained in the set of non-zero squares of $GF(q)$. In particular, the edge set $E(P_q)$ is a symmetric relation: $x - y$ is a square if and only if $y - x$ is a square.

As an example, consider the graph P_9. Let S be the set of all non-zero squares in $GF(9)$. We use the following representation of elements of the field with 9 elements:

$$GF(9) = \{a + bi : a, b \in \mathbb{Z}_3, i^2 = -1\}.$$

In particular,

$$GF(9) = \{0, 1, 2, i, 2i, 1 + i, 1 + 2i, 2 + i, 2 + 2i\}.$$

Computing all the non-zero squares we find that

$$S = \{1, 2, i, 2i\}.$$

See Figure 1.8, where vertices are labelled by the elements of $GF(9)$.

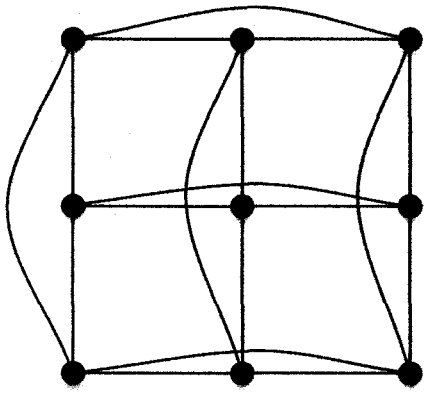


Figure 1.8: The graph P_9.

We now consider Cayley graphs. Let G be a group of order m and let S be a set of elements of G so that the *identity element*, written e, is not in S and S is *inverse-closed*: that is, if $g \in S$, then $g^{-1} \in S$. The set S is called the *connection set*. Define the *Cayley graph* $G(S)$ to have vertices the elements of G, with g joined to h if $gh^{-1} \in S$. Note that $G(S)$ is simple and undirected by the defining properties of S. If G is Abelian, then we use additive notation, so g^{-1} is written $-g$.

The following theorem shows that each Paley graph is a Cayley graph.

Theorem 1.2. *Let q be a prime power such that $q \equiv 1 \pmod 4$, and let S be the set of squares in $GF(q)$. Then S is inverse-closed.*

Proof. Write $-1 = b^2$, for a suitable $b \in GF(q)$ (which is possible by

the hypothesis on q). For $x \in S$, choose $a \in G$ such that $x = a^2$. Then

$$\begin{aligned} -x &= b^2 a^2 \\ &= (ba)^2. \end{aligned}$$

Hence, $-x$ is also a square and S is inverse-closed. □

1.3 Thesis Overview

We now summarize the contents of the remainder of the thesis. In Chapter 2 we will elaborate on basic properties of n-e.c. graphs, as well the existence of such graphs using probabilistic methods. We will present an overview of some of the known constructions of n-e.c. graphs. These explicit families of graphs with the property are derived from finite fields and finite geometry. Computational results on n-e.c. graphs are presented in Chapter 3. Given a graph, it can be easily verified in polynomial time whether the graph satisfies the n-e.c. property. (For example, it can be shown that the 3-e.c.-checking algorithm described in Appendix A.1 is of complexity $\Theta(n^4)$.) Finding graphs with a certain order that satisfy the n-e.c. property is difficult. Even for $n = 3$, it has proven difficult to check the 3-e.c. property for all graphs of a certain class of graphs. Thus, to aid in the search for 3-e.c. graphs, a computer search was conducted on certain small order vertex-transitive and strongly regular graphs. As a result, a new example of a 3-e.c. graph of order 30 will be presented. Previously, no 3-e.c. graph was known to exist of that order. In Chapter 4 a new construction for n-e.c. graphs using elementary probability and group theory will be given. We conclude with Chapter 5, in which we

will summarize the main results of the thesis, and state the main open problems surrounding n-e.c. graphs.

Chapter 2

EXISTENCE AND PROPERTIES OF N-E.C. GRAPHS

2.1 Introduction

In this chapter we consider the existence and properties of graphs with the n-e.c. adjacency property. Although the n-e.c. property is straightforward to define, it is not clear from the definition that graphs with the property exist. We now give a classic proof of Erdős and Rényi [14] which demonstrates that for a fixed integer $n > 0$, asymptotically almost surely $G(m, 1/2)$ is n-e.c.

Theorem 2.1. *Fix an integer $n \in \mathbb{N}$. The following then holds.*

1. *A.a.s. $G(m, \frac{1}{2})$ is n-e.c.*

2. *Let f be a positive real-valued function defined by*

$$f(m,n) = \binom{m}{n} 2^n \left(1 - \frac{1}{2^n}\right)^{m-n}. \tag{2.1}$$

If m is an integer chosen so that $f(m) < 1$, then there is an n-e.c. graph of order m.

Proof. Let $G = G(m, 1/2)$. For item (1), let A, B be two sets of vertices of G such that $A \cap B = \emptyset$ and $|A \cup B| = n$. Fix $z \notin A \cup B$. Then, by the independence of the choice of edges in G, the probability that z is

not joined correctly to A and B is

$$1 - \frac{1}{2^n}.$$

Hence, the probability that no vertex of G is joined correctly to A and B is

$$\left(1 - \frac{1}{2^n}\right)^{m-n}. \tag{2.2}$$

There are $\binom{m}{n}$ choices of an n-set of vertices X, and 2^n many partitions of X into sets A and B. Hence, by (2.2) it follows that the probability that G is not n-e.c. is at most

$$\begin{aligned}
\binom{m}{n} 2^n \left(1 - \frac{1}{2^n}\right)^{m-n} &\leq m^n 2^n \left(1 - \frac{1}{2^n}\right)^{m-n} \\
&= \exp\left(n \log m + n \log 2 + (m-n) \log\left(1 - \frac{1}{2^n}\right)\right) \\
&= o(1),
\end{aligned}$$

where the last equality follows since $\log\left(1 - \frac{1}{2^n}\right)$ is a negative constant.

For the proof of item (2), if m has the given property, then with positive probability, $G(m, \frac{1}{2})$ contains a n-e.c. graph with positive probability. □

Theorem 2.1 generalizes to $G(m,p)$, where $p \in (0,1)$ is fixed. We omit the more technical proof of this generalization, as our focus here is on proving the existence of n-e.c. graphs.

We now consider how large m must be for $G(m, \frac{1}{2})$ to be n-e.c. with positive probability. Using Theorem 2.1 (2), we plotted the function $f(m,n)$ considered as a two-variable function of both m and n (hence, the plot is three dimensional). See Figure 2.1.

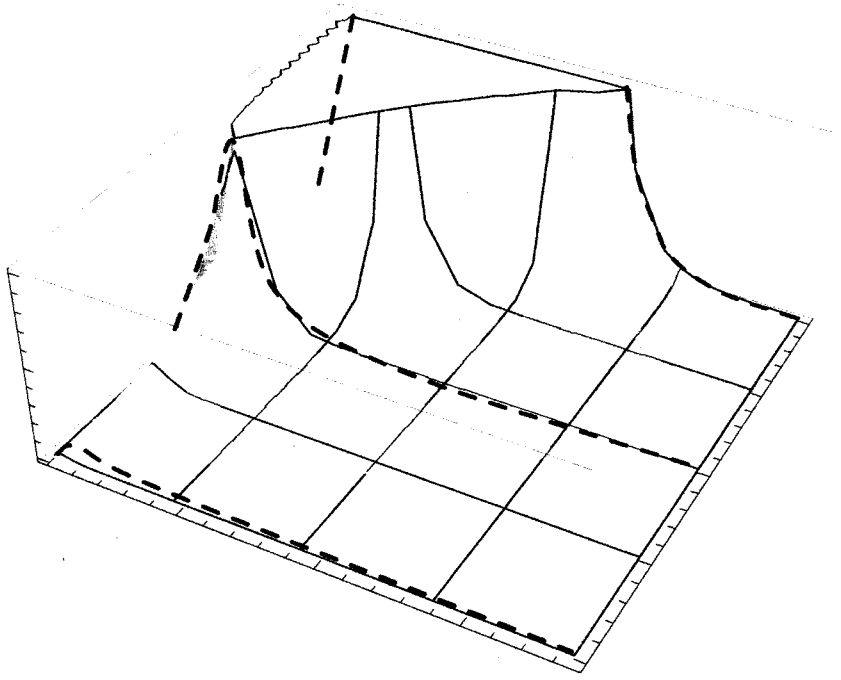


Figure 2.1: A plot of function $f(m,n)$ from Theorem 2.1 b).

As expected, as n increases, the value of m such that $G(m,\frac{1}{2})$ is n-e.c. with positive probability grows exponentially. Extrapolating from Figure 2.1, a plot n versus m (where the corresponding m value is found by solving the equation $\lceil f(m,n) \rceil = 1$) is shown in Figure 2.2. Note that whenever m is an integer satisfying $f(m,n) < 1$, then by the probabilistic method there is an n-e.c. graph of order m.

We now turn our attention to the minimum order of an n-e.c. graph. For a positive integer n, denote the minimum order of an n-e.c. graph by $m_{ec}(n)$. By Theorem 2.1 (2), n-e.c. graphs exist for all $n > 0$, and so the function $m_{ec}(n)$ is well-defined. It was determined in [9] that $m_{ec}(1) = 4$ and $m_{ec}(2) = 9$. In [9], it was shown that there are exactly three non-isomorphic 1-e.c. graphs of order four. Figure 2.3 shows these graphs in the following order $2K_2$ (which consists of two disjoint copies of K_2), the 4-cycle C_4, and the path with 4 vertices P_4.

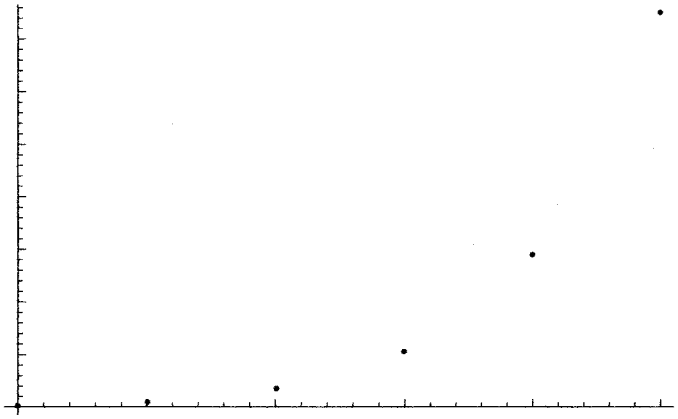


Figure 2.2: Number of vertices m needed for $G(m, 1/2)$ to be n-e.c.

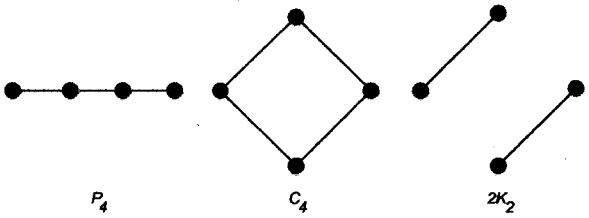


Figure 2.3: The 1-e.c. graphs of minimum order.

To describe the minimum order 2-e.c. graph, we need to define the *Cartesian product* of two graphs. The *Cartesian product* of G and H, written $G\Box H$, has vertices $V(G)\times V(H)$ and edges $(a,b)(c,d) \in E(G\Box H)$ if and only if $ac \in E(G)$ and $b = d$ or $a = c$ and $bd \in E(H)$. The notation stems from the fact that

$$K_2\Box K_2 \cong C_4.$$

The graph $K_3\Box K_3$, which is the unique 2-e.c. of minimum order (as proved in [9]), is shown in Figure 2.4.

Theorem 2.1 (2) supplies an asymptotic upper bound for $G(m, \frac{1}{2})$ to be n-e.c., which we describe in our next theorem.

Theorem 2.2. *If $m = O(n^2 2^n)$ and n is a sufficiently large integer, then*

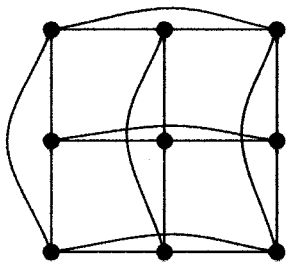


Figure 2.4: The unique 2-e.c. graph of minimum order.

with positive probability $G(m, \frac{1}{2})$ is n-e.c. In particular,

$$m_{ec}(n) = O(n^2 2^n).$$

Proof. Let $m = f(n)$ be the function defined as in (2.1). We must show that if $m = O(n^2 2^n)$, then $f(m) < 1$. Equivalently, we show that if $\epsilon > 0$ is fixed and $m = (\epsilon + 1)n^2 2^n$, then

$$\log f(m) < 0. \tag{2.3}$$

Now

$$\binom{m}{n} 2^n \left(1 - \frac{1}{2^n}\right)^{m-n} < m^n 2^n \left(1 - \frac{1}{2^n}\right)^{m-n}.$$

Hence, (2.3) is equivalent to showing that

$$n \log m + n \log 2 + (m - n) \log \left(1 - \frac{1}{2^n}\right) < 0. \tag{2.4}$$

For n sufficiently large we have that $\log\left(1 - \frac{1}{2^n}\right) \sim -\frac{1}{2^n}$. By this fact, by computation, and by the choice of m, (2.4) is equivalent to

$$n(\log(\epsilon + 1) + 2 \log n + \log 2) + n^2 \log 2 + \frac{n}{2^n} < (\epsilon + 1)n^2,$$

which is valid for large n as $\log 2 < 1$. □

The determination of $m_{ec}(n)$, where $n \geq 3$ is a difficult open problem. It was proved in [10] that $m_{ec}(n) = \Omega(n2^n)$. In fact, one of the deepest conjectures on n-e.c. graphs was given in Erdős et al. [10], which states that

$$m_{ec}(n) = \Theta(n2^n).$$

Hence, to prove the conjecture, we would need to present a family of n-e.c. graphs with order $O(n2^n)$.

There has been much research done in determining the minimum order of a 3-e.c. graph. The results of [9] show that

$$20 \leq m_{ec}(3) \leq 28.$$

A lower bound on the order of $m_{ec}(3)$ was found recently using complex computational methods. Based on 15,000 hours of CPU time, the authors of [16] demonstrated that $m_{ec}(3) \geq 24$.

2.2 Properties of n-e.c. Graphs

We now consider how n-e.c. graphs behave with respect to (among other things) the taking of complements and induced subgraphs. The following theorem is a part of folklore (see [8]) but we present a full proof for completeness.

Theorem 2.3. *Fix n a positive integer, and let $G = (V, E)$ be a fixed n-e.c. graph.*

1. *The graph G is m-e.c. for all $1 \leq m \leq n - 1$.*

2. *The graph G has order at least $n + 2^n$ and has at least $n2^{n-1}$ many edges.*

3. *The graph $\overline{G}$ is n-e.c.*

4. *If $n > 1$, then for each vertex x of G, each of the graphs*

$$G\backslash\{x\},\ \ G \restriction N(x),\ \ G \restriction N^c(x).$$

are $(n-1)$-e.c.

5. *If $n \geq 2$, then the graph G is connected with diameter 2.*

Proof. To prove (1), fix a positive integer $m \leq n-1$, and let $A, B \subseteq V$ be disjoint sets chosen so that $|A \cup B| = m$. Choose a set of vertices C disjoint from $A \cup B$ so that $|A \cup B \cup C| = n$. As G is n-e.c., there is a vertex $z \in V$ correctly joined to A and $B \cup C$. Then z is correctly joined to A and B, and so G is m-e.c.

For item (2), fix an n-set X of vertices in V. There are 2^n many distinct vertices correctly joined to X by the n-e.c. property. Hence

$$|V| \geq n + 2^n.$$

For each subset A of X with $|A| = i$, where $1 \leq i \leq n$, by the n-e.c. property there is a vertex z joined to A and no other vertices of X. Such a z contributes i edges for each subset A. Hence, the number of edges in G is at least the following

$$\sum_{i=0}^{n} i\binom{n}{i} = n2^{n-1},$$

using a standard equality for sums of binomial coefficients; see [11].

For (3), let $A, B \subseteq V(\overline{G})$. By the n-e.c. property there exists $z \in V(G)$ joined to B and not A. Vertex z will then be correctly joined to A, B in $\overline{G}$. This implies that $\overline{G}$ is n-e.c.

For (4), define $G' = G - x$, and let $A, B \subseteq V(G')$ be chosen such that $|A \cup B| = n - 1$. Define $A' = A \cup \{x\}$. By hypothesis there exists z correctly joined to A' and B. This implies $z \in V(G \backslash \{x\})$. Then G' is $(n-1)$-e.c.

Let $A, B \subseteq N(x)$ such that $|A \cup B| = n - 1$. Define $A' = A \cup \{x\}$. Then there exists z correctly joined to A' and B and $z \in N(x)$. Hence, $G \restriction N(x)$ is $(n-1)$-e.c.

Let $A, B \subseteq N^c(x)$ such that $|A \cup B| = n - 1$. Define $B' = B \cup \{x\}$. Then there exists z correctly joined to A and B' and $z \in N^c(x)$. Hence, $G \restriction N^c(x)$ is $(n-1)$-e.c.

To prove the final item (5), let x and y be distinct non-joined vertices in G. By the n-e.c. property, there is a vertex joined to both x and y. Hence, any two distinct vertices are connected by a path of length at most two. □

We consider one illustration of Theorem 2.3 below. Note that if G is 2-e.c., then by the Theorem 2.3 (4), it follows that $G \restriction N(x)$ and $G \restriction N^c(x)$ are 1-e.c. Hence, G has order at least 19. However, if G was of order 19, it would be 19-regular, which violates the First Theorem of Graph Theory (see equation (1.2)). It follows that

$$m_{ec}(3) \geq 20.$$

This argument was first given in [9].

2.3 Applications of n-e.c. Graphs

As mentioned in the introduction of Chapter 1, an n-e.c. graph G is $(n+1)$-universal. That is, each graph of order at most $n+1$ is isomorphic to an induced subgraph of G. We show this in Theorem 2.4. Universal graphs have numerous applications in computer science. Several optimization problems in data representations [13], data structures [24], and circuit design [29] surround problems on certain universal graphs.

Theorem 2.4. *For a fixed integer $n > 0$, if G is an n-e.c. graph, then G is $(n+1)$-universal. In particular $\chi(G), \omega(G) \geq n+1$.*

Proof. Let H be a graph of order at most $n+1$. We will prove that $H \leq G$ by induction on $|V(H)|$.

For the base case, we have that $|V(H)| = 1$. Hence, $H \cong K_1$ which embeds in G, as G has at least one vertex. Now assume that each graph of order at most k embeds in G, where $0 < k \leq n$ is a fixed integer. Fix H a graph of order $k+1$, and fix $x \in V(H)$. Consider $H' \cong H - x$. Then by the induction hypothesis $H' \leq G$. Say x has neighbours in H equalling the set A and non-neighbours B. Since G is n-e.c., it follows there exists $z \in V(G)$ correctly joined to vertices of A and B. It follows that

$$G \restriction (V(H \backslash \{x\}) \cup \{z\}) \cong H.$$

The final statements of the theorem on the clique and chromatic number follow since G contains the complete graph K_{n+1} as an induced subgraph. □

Expander graphs were first defined by Bassalygo and Pinsker, and their existence was first proved by Pinsker around 1970 (see [23]). The

property of being an expander seems significant in many mathematical, physical, and computational settings. For example, expander graphs are very useful in the design and analysis of communication networks; see [17]. As mentioned in Chapter 1, under certain conditions, n-e.c. graphs behave like expander graphs.

Lemma 2.1. *Let G be an n-e.c. graph, and let S be a set of vertices of G of order n. Then $|\partial(S)| \geq n$.*

Proof. Fix a vertex x of S. By the n-e.c. property, there is a vertex z_x joined to x and to no other vertex of S. Hence, the edge xz_x is in $\partial(S)$. Note that for $x \neq x'$, we have that $z_x \neq z_{x'}$. It follows that

$$|\partial(S)| \geq |\{xz_x : x \in S\}| = n,$$

and the proof of the lemma follows. □

2.4 Explicit Constructions of n-e.c. Graphs

This section describes various constructions for n-e.c. graphs. While we do not cover all known constructions, our discussion should provide further insight to the nature of the n-e.c. graphs.

Most of the known explicit n-e.c. graphs are strongly regular. Let k, $v > 0$, λ, and μ be non-negative integers. A k-regular graph G with v vertices, so that each pair of joined vertices has exactly λ common neighbours, and each pair of non-joined vertices has exactly μ common neighbours, is called a *strongly regular graph*; we say that G is $\mathrm{SRG}(v, k, \lambda, \mu)$. An example of a strongly regular graph is the 5-cycle, depicted in Figure 2.5.

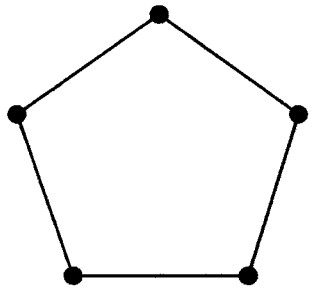


Figure 2.5: The 5-cycle is a SRG(5, 2, 0, 1).

2.4.1 Paley Graphs

The first family of explicit graphs that were discovered to contain n-e.c. graphs for all n were Paley graphs P_q. Recall from Chapter 1 that a Paley graph is a graph constructed on the points of a finite field such that two vertices are adjacent if and only if their difference is a non-zero square in the field. Chung, Graham, and Wilson (see [12]) proved that Paley graphs are contained in a class of graphs called quasi-random graphs, thereby showing that such Paley graphs share a large number of graph properties with random graphs.

Some of the main properties of Paley graphs are summarized in the following theorem, whose proof is omitted. A full proof may be found in [6].

Theorem 2.5. *Fix q a prime power with $q \equiv 1 \pmod 4$.*

1. The graph P_q is a SRG$(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.

2. The graph P_q is *self-complementary*; that is $P_q \cong \overline{P_q}$.

3. The graph P_q is vertex-transitive.

The following result on the n-e.c. properties of Paley graphs was proven independently in [5, 7]. The proof is beyond the scope of this

thesis, and so is omitted. It uses a famous result from number theory: Weil's proof of the Riemann hypothesis over finite fields.

Theorem 2.6. *If*

$$q > n^2 2^{2n-2},$$

then P_q is n-e.c.

Note that Theorem 2.6 demonstrates that sufficiently large Paley graphs are n-e.c. However, it only gives examples of prime power order.

As described in [2], one variation of a Paley graph is the cubic Paley graph. A *cubic Paley graph*, denoted by $P_q^{(3)}$ of order $q \equiv 1 \pmod 3$ has distinct vertices joined if their difference is the cube of an element of $GF(q)$. The condition $q \equiv 1 \pmod 3$ ensures that -1 is a cube in $GF(q)$, and so $P_q^{(3)}$ is a well-defined, undirected graph. As an example, the cubic Paley graph of order 19 shown in Figure 2.6.

A *quadruple Paley graph* $P_q^{(4)}$ of order $q \equiv 1 \pmod 8$ has two vertices joined if and only if their difference is a fourth power of an element of $GF(q)$. See Figure 2.7 for an example of a quadruple Paley graph.

These two variations of Paley graphs possess the n-e.c. property if q is large enough. The following result—proven in [2]—provides a lower bound on the size of q required for the Paley graph variations to be n-e.c.

Theorem 2.7. *1. If*

$$q > (2n2^{2n-1} - 2^{2n} + 1)2^n\sqrt{q} + 3n2^{-n}3^{2n-1},$$

then $P_q^{(3)}$ is n-e.c.

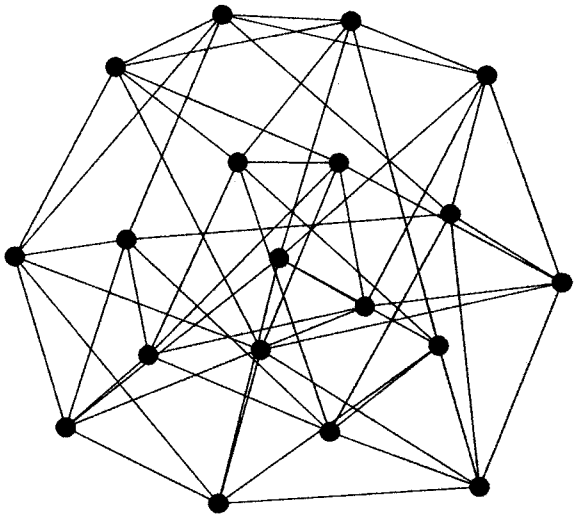


Figure 2.6: A cubic Paley graph of order 19.

2. If

$$q > (2n2^{2n-1} - 2^{2n} + 1)3^n\sqrt{q} + 4n3^{-n}4^{2n-1},$$

then $P_q^{(4)}$ *is n-e.c.*

There is another natural generalization of Paley graphs described as follows. Let $q = p^r$ be an odd prime power so that $q \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$. Let v be a generator under the multiplicative group of $GF(q)$. Define the graph $P^*(q)$ where the set of vertices are the elements of $GF(q)$ and two vertices are joined if their difference is of the form v^j, where $j \equiv 0 \pmod 4$ or $j \equiv 1 \pmod 4$. It can be shown that $P^*(q)$ is strongly regular, self-complementary, and vertex-transitive (see [21]). These graphs are n-e.c. given a large enough q. Using character sum estimates, the following result was proven in [20].

Theorem 2.8. *If* $q = p^r$ *is a prime power so that* $q \equiv 1 \pmod 4$, $p \equiv 3$

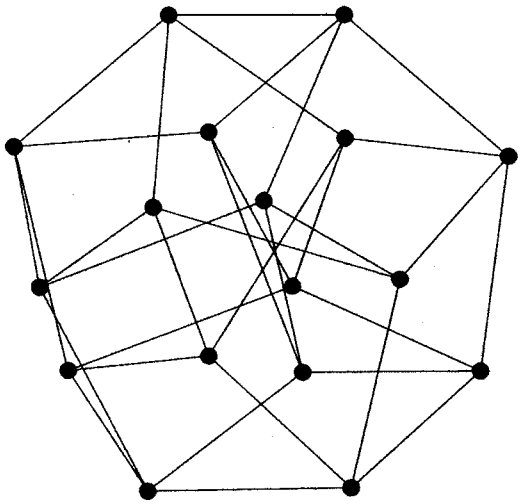


Figure 2.7: A quadruple Paley graph of order 17.

(mod 4), *and*

$$q > 8n^2 2^{8n},$$

then $P^*(q)$ *is* n*-e.c.*

2.4.2 Finite Geometry

Euclidean plane geometry investigates the incidence structure formed by points and lines in a plane. One important incidence structure is called an affine plane. Using affine plane geometry, we describe a recent construction from [8] of strongly regular n-e.c. graphs. This randomized construction will set the stage for our randomized Cayley graph construction of n-e.c. graphs in Chapter 4.

An *affine plane* is a pair $(A, \mathcal{L})$ satisfying the following properties, where A is a non-empty set of elements called *points* and $\mathcal{L}$ is a family of subsets of A called *lines*. First, any two points uniquely determine a line.

Second, given a line l and a point p, there is a unique line l' containing p parallel to l (where two lines are *parallel* if they are disjoint). The last property states that an affine plane has at least four points, no three which are on the same line. We denote a line by $\overline{pq}$, for the line between p and q.

As an example, let X be a two dimensional vector space over the field F. Consider elements of X as ordered pairs (x, y) where $x, y \in F$. For any $m, b \in F$ with $b \neq 0$, we will name the set

$$\{(x, y) : y = mx + b\}$$

a *line with slope* m. For any $a \in F$, we will call the set $\{(x, y) : x = a\}$ a *line with infinite slope*. If $\mathcal{L}$ is the set of all lines, then $(X, \mathcal{L})$ is a well-defined affine plane. Observe that two lines are parallel if they have the same slope. We note that parallelism is an equivalence relation on the set of lines. That is, it is reflexive, symmetric and transitive. Lines with same slope form a *parallel class*.

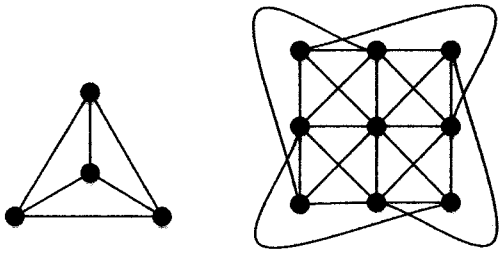
For any finite affine plane A, there is a positive integer $n \geq 2$ such that every line of A consists of exactly $n + 1$ lines and A has exactly n^2 points, $n^2 + n$ lines, and $n + 1$ parallel classes. We say that the affine plane is of *order* n. Every point in the affine plane is on $n + 1$ lines and each line is incident to n points. Given a line l in the affine plane there are $n - 1$ other lines parallel to l. Because each point is on $n + 1$ lines it follows that the affine plane contains $n + 1$ parallel classes. The proof of these and other results on affine planes may be found in [19].

The affine plane of order two is shown in part (a) of the following

figure. The set of points is $\{1, 2, 3, 4\}$. The six lines are

$$\{1, 2\}, \{3, 4\}, \{1, 3\}, \{2, 4\}, \{1, 4\}, \{2, 3\}$$

contained in three parallel classes. Similarly, the affine plane of order three shown in part (b) has 9 vertices, 12 lines, and four parallel classes.



(a) (b)

Figure 2.8: Affine planes of order two and three.

We now present a geometric construction of strongly regular graphs which is due to Delsart, Goethals and Turyn (see [26]). Fix a finite affine plane A. Let l_∞ be the line at infinity, which contains $q + 1$ elements. The elements of l_∞ may be identified with the slopes of lines in the affine plane. Let $S \subseteq l_\infty$. Define a graph $G(q, S, A)$ of order q with vertices representing the points of the affine plane A. Two vertices p and q are joined if and only if the line $\overline{pq}$ has a slope in S. We show now that $G(q, S, A)$ is strongly regular.

Theorem 2.9. *Fix an affine plane A of order q, and fix $S \subseteq l_\infty$. The graph $G(q, S, A)$ of order q is a*

$$\mathrm{SRG}(q^2, |S|(q-1), q-2+(|S|-1)(|S|-2), |S|(|S|-1)).$$

Proof. Vertices are the points of the affine plane and so there are q^2 vertices. Each vertex lies on $|S|$ lines, each with q points. Hence, we have

that

$$k = |S|(q-1).$$

To determine λ, fix distinct adjacent vertices x and y. There are $q-2$ vertices on the xy joined to x and y. A vertex z is joined to x, y if and only if the slopes determined by lines $\overline{xz}$ and $\overline{yz}$ are in S. There are $(|S|-1)(|S|-2)$ such choices for z. It follows that

$$\lambda = q - 2 + (|S|-1)(|S|-2).$$

The fact that

$$\mu = |S|(|S|-1)$$

follows in an analogous fashion. □

Let $\mathcal{G}(q, A)$ be the family of graphs $\mathcal{G}(q, S, A)$ for all choices of S; if $0 \leq k \leq q+1$ is fixed, then we write $\mathcal{G}(q, k, A)$ for the subfamily of all graphs in $\mathcal{G}(q, A)$ where $|S| = k$. In particular, fix A, an affine plane of even order $q \geq 8$, where the points are given by $GF(2^k)$. Choose S to contain $\frac{q}{2}$ slopes from l_∞. It follows that G is a

$$SRG\left(q^2, \frac{q(q-1)}{2}, \frac{q(q-2)}{4}, \frac{q(q-2)}{4}\right).$$

Considering all the subsets S of l_∞, with $|S| = \frac{q}{2}$ we can construct an equiprobable probability space, where each point of the probability space corresponds to a subset S (that is, each choice of S is made uniformly at random from all $\frac{q}{2}$ subsets of l_∞). This leads to a result, proven in [4], which states that as q approaches infinity, the probability that $\mathcal{G}(q, \frac{q}{2}, A)$ is n-e.c. tends to one. We formally state this result in the following theorem.

Theorem 2.10. *Let q be a power of 2, fix an affine plane A of order q, and fix n a positive integer. With probability tending to 1 as $q \to \infty$, $\mathcal{G}(q, \frac{q}{2}, A)$ is n-e.c.*

A different construction of explicit n-e.c. graphs was given recently by Bonato in [8]. Instead of fixing the order of $|S|$, a slope $m \in l_\infty$ is added independently to S with probability p, where $p \in (0,1)$ is fixed. Note that the probability that m is not in S is $1-p$. It follows that $\mathcal{G}(q, |S|, A)$ is a probability space, and $|S|$ is a random variable on this space. We denote this space by $\mathcal{G}(q, A)$. All choices of S lead to a strongly regular graph. We present a proof of the following result found in [8] as it will aid us in Chapter 4 to prove that Cayley graphs are n-e.c. We only consider the case $p = 1/2$.

Theorem 2.11. *([8]) Fix an affine plane A of order q, and fix n a positive integer. With probability tending to 1 as $q \to \infty$, $\mathcal{G}_{1/2}(q, A)$ is n-e.c.*

Proof. Let X and Y in G, with $|X \cup Y| = n$ and $X \cap Y = \emptyset$. Let $U = X \cup Y$. We prove that for sufficiently large q, with probability 1 there is a vertex z correctly joined to X and Y. To accomplish this, we construct a set P_U of points, disjoint from U, such that with probability 1, z is in P_U. We set $s = \lceil q^b \rceil$, where $b < 1$ is fixed.

Fix a point v of A. The *projection from v onto l_∞* is the map

$$\pi_v : A \backslash \{v\} \to \ell_\infty$$

taking a point x to the intersection of $\overline{vx}$ with ℓ_∞. Hence, $\pi_v(x)$ is the

slope of the line $\overline{vx}$. If V is a set of points, then let

$$\pi_v(V) = \bigcup_{x \in V} \pi_v(x).$$

For sufficiently large q, we inductively construct a set of points P_U distinct from U with the following properties.

1. If $p \in P_U$, then $|\pi_p(U)| = n$.

2. For all distinct p and q in P_U, $\pi_p(U) \cap \pi_q(U) = \emptyset$.

3. $|P_U| = s$.

Define $P_{U,1}$ by choosing any point $p_1 \notin U$ that is not on a line joining two points of U. For large q

$$n + \binom{n}{2}(q-2) < q^2,$$

so we may find such a p_1.

For a fixed positive $i \leq s-1$, suppose that $P_{U,i}$ has been constructed for large q, with $P_{U,i}$ containing $P_{U,1}$, and $|P_{U,i}| = i$. We would like to choose $p_{i+1} \notin U$ to be a point that is

(i) not on a line joining two points of U, and

(ii) not on a line joining a point of U to a point in

$$\bigcup_{j=1}^{i} \pi_{p_j}(U).$$

Condition (i) rules out points on $\binom{n}{2}$ lines, while (ii) rules out points on

$$ni + n(n-1)i$$

lines. For large q

$$n + \binom{n}{2}(q-2) + ni(q-1) + n(n-1)i(q-2) < n^2 q^{b+1} < q^2,$$

so we may find a suitable p_{i+1} satisfying items (1) and (2). Add p_{i+1} to $P_{U,i}$ to form $P_{U,i+1}$. Define

$$P_U = \bigcup_{i=1}^{s} P_{U,i}$$

so $|P_U| = s$, as desired.

For a fixed n-set U of vertices we estimate the probability that none of the vertices of P_U are correctly joined to U. By item (1), note that any z in P_U has the property that $\overline{zx}$ and $\overline{zy}$ have distinct slopes, where x, y are distinct points of U. Note also that zx is an edge of G if and only if $\pi_z(x) \in S$. Therefore, the probability that a given z in P_U is not joined correctly to X and Y is the positive constant

$$1 - \frac{1}{2^n}. \tag{2.5}$$

By item (2) in the defining properties of P_U, any two distinct points of P_U induce disjoint slope sets in ℓ_∞. In particular, the probability (2.5) independently holds for any choice of z in P_u. Hence, the probability that no z in P_U is correctly joined to X and Y is $(p_n)^{\lceil q^b \rceil}$. The probability

that $\mathcal{G}_p(q, A)$ is not n-e.c. is therefore at most

$$\begin{aligned}\binom{q^2}{n} 2^n (p_n)^{\lceil q^b \rceil} &\leq q^{2n} 2^n \left(1 - \frac{1}{2^n}\right)^{q^b} \\ &= \exp\left(2n \log q + n \log 2 + q^b \log\left(1 - \frac{1}{2^n}\right)\right) \\ &= o(1)\end{aligned}$$

where the last line follows since $\log\left(1 - \frac{1}{2^n}\right)$ is a negative constant. □

Determining the minimum order of n-e.c. graphs remains one of the most challenging problems surrounding such graphs. In our search for minimal order n-e.c. graphs, our focus has been on the case $n = 3$. The next chapter provides an overview of some classes of graphs that have been checked for the 3-e.c. property using a computer search.

Chapter 3

COMPUTATIONAL RESULTS

3.1 Introduction

The difficulty of determining if a graph is n-e.c. increases exponentially with n. For example, to check that a graph of order m is n-e.c., for each of the $\binom{m}{n}$ subsets S of vertices, we would need to find 2^n vertices joined to S in all the possible ways. This becomes difficult, if not impossible, to do by hand for large examples. The focus of this chapter is on computational results related to the minimum order of a 3-e.c. graph. We recall from Section 2.1 that

$$24 \leq m_{ec}(3) \leq 28$$

(the lower bound follows from [16], while the upper bound follows from [9]). We note that most of the known explicit n-e.c. graphs are strongly regular. For $n = 3$, in [3] it was shown that the Paley graph of order 29 is the minimum order 3-e.c. Paley graph. Few examples of strongly regular non-Paley n-e.c. graphs are known.

Recall from Section 1.2.1 that a graph G is *vertex-transitive* if any two distinct vertices of G, there is an automorphism mapping one to the other. An example of a vertex-transitive graph is the *k-cube* Q_k. The vertex set of Q_k is the set of all 2^k binary strings of length k, with two being adjacent if they differ in precisely one position. Figure 3.1 depicts the 3-cube Q_3 with vertices labelled by the binary strings of length 3.

Note that Q_k is bipartite, so it is not even 2-e.c. (recall by Theorem 2.3 that 2-e.c. graphs have chromatic number at least 3).

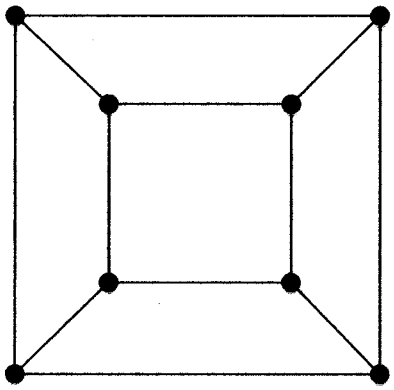


Figure 3.1: The 3-cube Q_3.

Strongly regular graphs were defined in Section 2.4. Paley graphs are an important instance of strongly regular graphs. In our computer search for a minimum order 3-e.c. graph, we focused on strongly regular graphs and the class of vertex-transitive graphs with orders between 24 to 30 (inclusive).

3.2 Data Sets and Results

Appendix A.1 describes the algorithm used for checking the 3-e.c. condition given an adjacency matrix of a graph as input. Lists containing all isotypes of small order vertex-transitive and strongly regular graphs are publicly available on-line. The data sets for the class of strongly regular graphs can be found in [27], while the data for the class of vertex-transitive graphs is available on-line at [25]. The data set is partitioned into different files based on the order of the graph. Each file consists of adjacency matrices encoded in the *g6* format. (More on this format can

be found at [25].) The search was conducted only on graphs of order 24 to 30 to determine if a minimum order 3-e.c. graph lies in one of these two classes. We note that the vertex-transitive graphs of orders 20 to 28 were checked for the 3-e.c. property in [9]. Although we did not determine the order of minimum order 3-e.c. graph, we found other results which we now report.

The following table summarizes the results of the computer search for 3-e.c. graphs. The numbers in the second and third columns represent the number of isomorphism types of graphs which are 3-e.c. The time required to check all the isotypes is presented along with number of isotypes checked for each order.

Order	**Vertex-Transitive**	**SRG**	**Isotypes**	**CPU hrs**
24	0	0	15506	8
25	0	0	464	0.29
26	0	0	4236	3.06
27	0	0	1434	1.16
28	2	0	25850	23.52
29	1	1	1182	1.19
30	2	0	46308	52

Before we discuss the results, we mention the numerical location of these graphs within the data sets. Hence, the numbers in the last two columns correspond to the positive integer assigned to the graphs.

Order	**Vertex-Transitive**	**Strongly Regular**
28	11440 and 15880	-
29	653	41
30	19022 and 24918	-

As $m_{ec}(3) \geq 24$, our results show that there are no 3-e.c. strongly regular or vertex-transitive graphs of order less than 28. The two 3-e.c. graphs of order 28 (first found in [9]) are not isomorphic and one is the complement of the other. (This can be verified using a software such as *Mathematica*, whereby isomorphism between the first found graph and the complement of the second found graph is verified. The command is 'IsomorphicQ') The adjacency matrix is shown below.

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

The 3-e.c. graph of order 29 found through our search is isomorphic to P_{29}, the Paley graph of order 29. This is shown in the following lemma.

Lemma 3.1. *There exists an unique* 3*-e.c. vertex-transitive graph of order* 29*, which is isomorphic to* P_{29}*.*

Proof. A complete list of vertex-transitive graphs of order 29 is provided in [25]. Using a computer search to determine all 3-e.c. graphs of order 29, it was discovered that only one graph possesses this property. We call this graph G. It is known that the Paley graph of order 29 is vertex-transitive and (see [3]) is 3-e.c. Hence, $G \cong P_{29}$. □

3.3 A New 3-e.c. Example of Order 30

In [22] it is mentioned that the existence of 3-e.c. graphs of order 30 is unknown. The 3-e.c. graphs of order 30 found through our search settles this problem. The two 3-e.c. graphs we found of order 30 are complements of each other. (This can be verified using *Mathematica.*) Below we present the adjacency matrix of one of these graphs.

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

Chapter 4

RANDOM CAYLEY GRAPHS

4.1 Introduction

We now consider Cayley graphs, which offer a combinatorial depiction of groups. They possess good expansion properties (see [17]) and, as we will prove in Theorem 4.1, under certain conditions they are n-e.c.

We recall the definition of Cayley graphs from Chapter 1. Given a group G, let S be a non-empty subset of G that is closed with respect to taking inverses, and does not contain the identity element e. The set S is called the *connection set.* The Cayley graph, denoted by $G(S)$, has vertices the elements of G, and $x, y \in E(G)$ if and only if $xy^{-1} \in S$.

Cayley graphs are an important class of vertex-transitive graphs. The following result is standard (see [15], for example), and we include a proof for completeness.

Lemma 4.1. *Every Cayley graph $G(S)$ is vertex-transitive.*

Proof. Fix vertices x and y in $V = G(S)$. Define $f : V \to V$ by

$$f(z) = zx^{-1}y,$$

where $z \in V$. Then

$$f(x) = xx^{-1}y = y.$$

Let $u, v \in V$. Note that

$$(uxy^{-1})(vxy^{-1})^{-1} = uv^{-1}.$$

From this it follows that $uv^{-1} \in S$ if and only if $f(u)f(v)^{-1} \in S$. Therefore, u is adjacent to v if and only if $f(u)$ is adjacent to $f(v)$. Hence, f is an automorphism of $G(S)$ mapping x to y. □

By the above lemma, $G(S)$ is a regular graph. As an example, consider $G(S)$ where $S = \emptyset$. The graph contains no edges. Similarly, if $S = G - e$, then $G(S)$ is a complete graph.

4.2 Random Cayley Graphs

Given a group G, we consider a way of randomly choosing the connection set S. We begin by defining a set S' to contain all the pairs (g, g^{-1}) from G, except for the pair (e, e). Fix a real number $p \in (0, 1)$. For each pair $(g, g^{-1}) \in S'$, elements g, g^{-1} are added independently and with probability p to S; with probability $(1-p)$, g, g^{-1} is not added to S. We note that S is a well-defined connection set since it inverse-closed and it does not contain the identity element. We name the corresponding probability space *the random Cayley graphs on the group G with probability p* and write $\mathcal{G}(p)$. While $|S|$ is a random variable in $\mathcal{G}(p)$, all choices of S give rise to Cayley graphs, and hence, vertex-transitive graphs. This follows directly from the definition of Cayley graphs. We prove the following result in the case when $p = 1/2$.

Theorem 4.1. *With probability tending to* 1 *as the order of the group G tends to ∞, $\mathcal{G}(1/2)$ is n-e.c., where n is a positive integer.*

Observe that Theorem 4.1 supplies a new randomized construction of vertex-transitive n-e.c. graphs, for all positive integer n.

Proof. Consider $G = \mathcal{G}(1/2)$ to have order m. Fix $X = \{x_1, x_2, \ldots, x_n\}$ an n-set of vertices $G(1/2)$. We need to find a vertex z correctly joined to X (regardless of the partition of X into two sets, say A and B). For $z \in X$ define $\sigma_X(z)$ to be the set of elements such that either $zx^{-1} \in S$ or $xz^{-1} \in S$. More precisely,

$$\sigma_X(z) = \{x \in G \mid zx^{-1} \in S \text{ or } x^{-1}z \in S\} \tag{4.1}$$

We would like to show we can construct a set U, disjoint from X, such that with probability tending to 1, there is a $z \notin U$ that is correctly joined to X. Equivalently, we show that with probability $o(1)$, there is no vertex in U correctly joined to X. We construct U such that $|U| = \lfloor \frac{m}{3n} \rfloor$, and impose the following restrictions on U.

1. For all distinct z and z' in U, $\sigma_X(z) \cap \sigma_X(z') = \emptyset$.

2. $|\sigma_X(z)| = n$.

Item (1) ensures the event that z is joined to a vertex x_i in X is independent of the event that z' is joined to x_i. Item (2) ensures that the events that z is joined to any particular x_i are mutually independent.

We inductively construct the set U_k whose union will be U. We choose U_1 to be a single vertex z_1 not in X with the property that $|\sigma_X(z_1)| = n$. We therefore eliminate elements in X and those z_1 such that $|\sigma_X(z_1)| < n$. For example, if it happens that $x_i^{-1}z_1 = z_1x_j^{-1}$ for some i and j, then we must eliminate z_1 from consideration. Each distinct pair of vertices from X eliminates at most one element of G. We may now find a suitable z_1

since

$$m - n - \binom{n}{2} > 0. \tag{4.2}$$

(Recall that n is a constant that does not depend on m.)

Suppose that U_k has been constructed for a fixed $k < \lfloor \frac{m}{n} \rfloor$, so that $|U_k| = k$, and the set U_k has elements satisfying items (1) and (2). Set $U_k = \{z_1, \ldots, z_k\}$. We choose z_{k+1} as the new element of U_k by eliminating elements from $V(G) \setminus U_k$. As in the base step, by considering all the pairs of vertices from X, $\binom{n}{2}$ vertices are eliminated. Each vertex $z \in U_k$ satisfies $|\sigma_X z| = n$. To ensure that $\sigma_X(z) \cap \sigma_X(z') = \emptyset$ for $z \in U_k$ and $z' \in U_{k+1}$, we must eliminate another $2kn$ vertices. For large m, we may find a suitable z_{k+1} since

$$m - n - k - \binom{n}{2} - 2kn > 0. \tag{4.3}$$

Add z_{k+1} to U_k, to form U_{k+1}. Define

$$U = \bigcup_{i=1}^{\lfloor \frac{m}{3n} \rfloor} U_k.$$

In particular, $|U| = \lfloor \frac{m}{3n} \rfloor$ as desired.

We now estimate the probability that none of the vertices of U are correctly joined to X, and show this tends to 0 as m tends to ∞. Given $z \in U$ and $x \in X$ we have by item (1) that

$$\mathbb{P}(z \text{ is c.j. to } X) = \frac{1}{2^n},$$

since each element in G is chosen independently with probability $1/2$.

Then

$$\mathbb{P}(\text{no } z \text{ is c.j. to } X) = 1 - \frac{1}{2^n}.$$

By items (1) and (2), we have that

$$\mathbb{P}(\text{no } z \text{ in } U \text{ is c.j. to } X) = \left(1 - \frac{1}{2^n}\right)^{\lfloor \frac{m}{3n} \rfloor}.$$

Hence, we have that the probability P of the event that G is not n-e.c. satisfies

$$\begin{aligned} P &\leq \binom{m}{n} 2^n \left(1 - \frac{1}{2^n}\right)^{\frac{m}{3n}} \\ &\leq m^n 2^n \left(1 - \frac{1}{2^n}\right)^{\frac{m}{3n}} \\ &= \exp\left(n \log m + n \log 2 + \left(\frac{m}{3n}\right) \log\left(1 - \frac{1}{2^n}\right)\right) \\ &= o(1), \end{aligned}$$

where the last equality follows since $\log\left(1 - \frac{1}{2^n}\right)$ is a negative constant.

□

We note that the proof of Theorem 4.1 generalizes to $p \in (0, 1)$. We omit this more technical proof in favour of the proof with $p = 1/2$, as we are focused on providing a new randomized construction of vertex-transitive n-e.c. graphs.

The proof of Theorem 4.1 gives an asymptotic upper bound for $\mathcal{G}(1/2)$ to be n-e.c.

Theorem 4.2. *If $m = O(n^3 2^n)$ and n is a sufficiently large integer, then with positive probability $\mathcal{G}(1/2)$ is n-e.c. In particular, there is a vertex-transitive n-e.c. graph of order $O(n^3 2^n)$.*

Proof. Let

$$f(m) = \binom{m}{n} 2^n \left(1 - \frac{1}{2^n}\right)^{\frac{m}{n}}$$

be the function defined as in proof of Theorem 4.1. We must show that if $m = O(n^3 2^n)$, then $f(m) < 1$. Equivalently, we show that if $\epsilon > 0$ is a fixed constant and $m = (\epsilon + 1)n^3 2^n$, then

$$\log f(m) < 0. \tag{4.4}$$

Now

$$\binom{m}{n} 2^n \left(1 - \frac{1}{2^n}\right)^{m/n} < m^n 2^n \left(1 - \frac{1}{2^n}\right)^{m/n}.$$

Hence, (4.4) is equivalent to showing that

$$n \log m + n \log 2 + \left(\frac{m}{n}\right) \log \left(1 - \frac{1}{2^n}\right) < 0. \tag{4.5}$$

By choice of m and computation, (4.5) is equivalent to

$$n(\log(\epsilon + 1) + 3 \log n + \log 2) + n^2 \log 2 < (\epsilon + 1)n^2,$$

which is valid for large n as $\log 2 < 1$. □

Chapter 5

CONCLUSION AND OPEN PROBLEMS

The main goal of the thesis was to investigate the n-e.c. property from both theoretical and computational perspectives. In our search for n-e.c. graphs, we have shown in Chapter 2 that a.a.s. the random graph $G(m,p)$ is n-e.c. and the order of the graph has an asymptotic upper bound given by $O(n^2 2^n)$. The computational results we provided focused on 3-e.c. graphs of small order. The results of Chapter 3 showed that there are no vertex-transitive or strongly regular 3-e.c. graphs of order less than 28. By our exhaustive search using a computer we have determined a new 3-e.c. graph of order 30. Previously, no 3-e.c. graph was known of that order. Finally in Chapter 4, we provided a new construction of n-e.c. graphs derived from random Cayley graphs $\mathcal{G}(p)$. We showed that the asymptotic order of the n-e.c. random Cayley graphs is $O(n^3 2^n)$.

We collect the open problems stated in this thesis.

1. Determine the precise value of $m_{ec}(3)$. More generally, determine the values of $m_{ec}(n)$, where $n \geq 3$.

   The determination of $m_{ec}(3)$ will likely use a mixture of computational and theoretical results on 3-e.c. graphs. Determining the exact order of $m_{ec}(n)$ for $n \geq 4$ appears to be a very difficult problem. Even determining the asymptotic order of this function presents a serious challenge, as summarized in the next problem.

2. Determine the asymptotic order of the function $m_{ec}(n)$. The conjecture of Erdős et al. [10] states that

$$m_{ec}(n) = \Theta(n2^n).$$

The conjecture of Erdős remains as one of the deepest problems in this area of graph theory. Random graphs give rise to n-e.c. graphs with order $\Theta(n^2 2^n)$ while our new random Cayley graph examples in Chapter 4 have order $\Theta(n^3 2^n)$. Even a seemingly modest improvement to order $\Theta(n^{2-c}2^n)$, where c is a fixed positive constant would represent a significant breakthrough. Although it is not clear, it is possible that the random graphs stemming from either affine planes or Cayley graphs may eventually be adapted to solve the conjecture.

3. Determine the integers m such that there is a 3-e.c. graph of order m.

By the results in [22] and Chapter 3, the only orders where we do not know whether a 3-e.c. graph exists are:

$$24, 25, 26, 27, 31, 33.$$

Appendix A

APPENDIX

A.1 Code to check for 3-e.c. property

```
checkNEC[adj_] := Module[
  {cond, i, j, k, v, r, count},

  Array[cond, 8];
  For[i = 1, i <= 8, i++,
   cond[i] = 0];

  For[i = 1, i <= 26, i++,
   For[j = i + 1, j <= 27, j++,
     For[k = j + 1, k <= 28, k++,
       For[v = 1, v <= 28, v++,
        If[i != v && j != v && k != v,

          If [adj[[i, v]] == 1 && adj[[j, v]] == 1 &&
            adj[[k, v]] == 1, cond[1] = 1];

          If [adj[[i, v]] == 1 && adj[[j, v]] == 1 &&
            adj[[k, v]] == 0, cond[2] = 1];
```

```
   If [adj[[i, v]] == 1 && adj[[j, v]] == 0 &&

     adj[[k, v]] == 1, cond[3] = 1];

   If [adj[[i, v]] == 1 && adj[[j, v]] == 0 &&
     adj[[k, v]] == 0, cond[4] = 1];

   If [adj[[i, v]] == 0 && adj[[j, v]] == 1 &&
     adj[[k, v]] == 1, cond[5] = 1];

   If [adj[[i, v]] == 0 && adj[[j, v]] == 1 &&
     adj[[k, v]] == 0, cond[6] = 1];

   If [adj[[i, v]] == 0 && adj[[j, v]] == 0 &&
     adj[[k, v]] == 1, cond[7] = 1];

   If [adj[[i, v]] == 0 && adj[[j, v]] == 0 &&
     adj[[k, v]] == 0, cond[8] = 1];
   ];
 ];
(*
For[r=1,r<=8,r++,
    If[cond[r]>=2 ,count+=1]
];
```

```
      If[count==8 && i==1,
      Print["(",i,j,k,")",cond[1],cond[2],cond[3],cond[4],cond[5],
      cond[6],cond[7],cond[8]];
      ];*)

      For[r = 1, r <= 8, r++,
       If[cond[r] == 0, Print["Not n-e.c."]; Return[]];
       cond[r] = 0;
       ];
      ];
    ];
  ];
  Print["Graph is 3-e.c. of order 28"];
  Print[adj]
  ]
```

A.2 Code for standard, cubic and quadruple Paley graphs

```
(* Standard Paley Construction Module*)

Paley[p_, r_] := Module[
   {adj, i, k, q, z, x, j, zPower, fldElem, pwrElem, elem, fld, S},

   q = p^r;
```

```
<< FiniteFields`;
<< GraphUtilities`;

adj = SparseArray[Array[0 &, {q, q}]];
If[PrimePowerQ[q] == False,
 Return["Parameter p expected to be prime."]];

(* Define the field *)
fld = GF[q];
(* Find all the non-zero elements of GF (q) *)

elem = PowerList[fld];
fldElem = {{0}};
pwrElem = {};

(* Find the inverse closed set and the elements of GF (q) in \
complex arithmetic *)
For[i = 1, i <= Length[elem], i++,
  z = elem[[i, 1]] + elem[[i, 2]] I;
  AppendTo[fldElem, {z}];
  zPower = Mod[z^2, p];
  AppendTo[pwrElem, {zPower}];
 ];
(* Inverse Closed Set Defined *)
S = DeleteDuplicates[pwrElem];

For[i = 1, i <=  q, i++,
```

```
    For[j = 1, j <= q, j++,
      For[k = 1, k <= Length[S], k++,
        If[
          Mod[(fldElem[[i]] - fldElem[[j]]), p] == Mod[S[[k]], p] &&
           i != j,
          adj[[i, j]] = 1;
          adj[[j, i]] = 1;
          ];
        ];
      ];
    ];
   Return[adj];
   ];

(*Cubic Paley Module*)

CubicPaley[p_] := Module[
   {adj, i, k, q, z, x, j, zPower, fldElem, F, S},

   << FiniteFields`;
   << GraphUtilities`;

   adj = SparseArray[Array[0 &, {p, p}]];

   If[Mod[p - 1, 3] != 0, Return["(p-1) mod 3 not satisfied."]];

   If[PrimePowerQ[p] == False,
```

```
 Return["Parameter p expected to be prime."]];

(* Define the field *)
fld = GF[p];
fldElem = PowerList[fld];
S = DeleteDuplicates[PowerMod[fldElem, 3, p]];
F = AppendTo[fldElem, {0}];

For[i = 1, i <=  p, i++,
 For[j = 1, j <= p, j++,
   For[k = 1, k <= Length[S], k++,
     If[Mod[(F[[i]] - F[[j]]), p] == Mod[S[[k]], p] && i != j,
       adj[[i, j]] = 1;
       adj[[j, i]] = 1;
       ];
     ];
   ];
 ];
Return[adj];
];

(* QUAD PALEY MODULE *)

  QuadPaley[p_] := Module[
{adj, i, k, q, z, x, j, zPower, fldElem, F, S},

<< FiniteFields`;
```

```
<< GraphUtilities`;

adj = SparseArray[Array[0 &, {p, p}]];

If[Mod[p - 1, 8] != 0, Return["(p-1) mod 8 not satisfied."]];

If[PrimePowerQ[p] == False,
 Return["Parameter p expected to be prime."]];

(* Define the field *)
fld = GF[p];
fldElem = PowerList[fld];
S = DeleteDuplicates[PowerMod[fldElem, 4, p]];
F = AppendTo[fldElem, {0}];

For[i = 1, i <=  p, i++,
 For[j = 1, j <= p, j++,
   For[k = 1, k <= Length[S], k++,
     If[Mod[(F[[i]] - F[[j]]), p] == Mod[S[[k]], p] && i != j,
       adj[[i, j]] = 1;
       adj[[j, i]] = 1;
       ];
     ];
   ];
 ];
Return[adj];
];
```

Bibliography

[1] N. Alon and J.H. Spencer, *The Probabilistic Method*, Wiley-Interscience, New York, 2000.

[2] W. Ananchuen, *On the adjacency properties of generalized Paley graphs*, Australasian Journal of Combinatorics **24** (2001), 129–148.

[3] W. Ananchuen and L. Caccetta, *On the adjacency properties of Paley graphs*, Networks **23** (1993), 227–227.

[4] C.A. Baker, A. Bonato, J.M.N. Brown, and T. Szőnyi, *Graphs with the n-e.c. adjacency property constructed from affine planes*, Discrete Mathematics **308** (2008), 901–912.

[5] A. Blass, G. Exoo, and F. Harary, *Paley graphs satisfy all first-order adjacency axioms*, Journal of Graph Theory **5** (1981), 435–439.

[6] B. Bollobás, *Random Graphs*, Cambridge University Press, Cambridge (2001).

[7] B. Bollobás and A. Thomason, *Graphs which contain all small graphs*, European Journal of Combinatorics **2** (1981), 13–15.

[8] A. Bonato, *The search for n-e.c. graphs*, Contributions to Discrete Mathematics **4** (2009), 40–53.

[9] A. Bonato and K. Cameron, *On an adjacency property of almost all graphs*, Discrete Mathematics **231** (2001), 103–119.

[10] L. Caccetta, P. Erdős, and K. Vijayan, *A property of random graphs*, Ars Combinatoria **19** (1985), 287–294.

[11] P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge, 1994.

[12] F.R.K. Chung, R.L. Graham, and R.M. Wilson, *Quasi-random graphs*, Combinatorica **9** (1989), 345–362.

[13] F.R.K. Chung, A.L. Rosenberg, and L. Snyder, *Perfect storage representations for families of data structures*, SIAM Journal on Algebraic and Discrete Methods **4** (1983), 548.

[14] P. Erdős and A. Rényi, *Asymmetric graphs*, Acta Mathematica Academiae Scientiarum Hungaricae **14** (1963), 295–315.

[15] C.D. Godsil and G. Royle, *Algebraic Graph Theory*, Springer, New York, 2001.

[16] P. Gordinowicz and P. Prałat, *The search for the smallest* 3*-e.c. graphs*, Journal of Combinatorial Mathematics and Combinatorial Computing, Preprint, 2009.

[17] S. Hoory, N. Linial, and A. Wigderson, *Expander graphs and their applications*, Bulletin of the American Mathematical Society **43** (2006), 439–561.

[18] J.M. Howie, *Field and Galois theory*, Springer Verlag, New York, 2006.

[19] Y.J. Ionin and M.S. Shrikhande, *Combinatorics of Symmetric Designs*, Cambridge Univ Press, Cambridge, 2006.

[20] A. Kisielewicz and W. Peisert, *Pseudo-random properties of self-complementary symmetric graphs*, Journal of Graph Theory **47** (2004), 310–316.

[21] N. Mullin, *Self-Complementary Arc-Transitive Graphs and Their Imposters*, (2009).

[22] O. Pikhurko and M. Singh, *Extremal existentially closed graphs*, Preprint, 2009.

[23] M.S. Pinsker, *On the complexity of a concentrator*, 7th International Telegraffic Conference, 1973, pp. 1–4.

[24] A.L. Rosenberg, L.J. Stockmeyer, and L. Snyder, *Uniform data encodings*, Theoretical Computer Science **11** (1980), 145–165.

[25] G. Royle, *Transitive graphs*, `http://units.maths.uwa.edu.au/~gordon/remote/trans/index.html`.

[26] J.J. Seidel, *A survey of two-graphs*, Proc. Int. Colloq. Teorie Combinatorie, pp. 481–511.

[27] T. Spence, *Strongly regular graphs on at most* 64 *vertices*, `http://www.maths.gla.ac.uk/~es/srgraphs.html`.

[28] A. Thomason, *Pseudo-random graphs*, Annals of Discrete Mathematics **33** (1987), 307–331.

[29] L.G. Valiant, *Universality considerations in VLSI circuits*, IEEE Transactions on Computers **30** (1981), 135–140.

[30] D.B. West, *Introduction to Graph Theory*, Prentice Hall, Upper Saddle River, NJ, 2001.