E.M. de Deckere

Understanding the bounds for the chromatic number of the Erdős-Rényi graph and its subgraphs

Master thesis, defended on August 25, 2009

Thesis advisors: Dr. Ir. Ing. M.J.P. Peeters (UvT), Prof. Dr. L.C.M. Kallenberg (UL)

Mathematisch Instituut, Universiteit Leiden

Contents

Preface

This thesis investigates the chromatic number of the Erdős-Rényi graph and its orthogonality subgraph. We try to understand the behavior of lower bounds and upper bounds for the chromatic number and we will make an attempt to improve the bounds by covering the vertex set of the Erdős-Rényi graph with suitable sized independent sets. Therefore independent sets of the Erdős-Rényi graph are of particular interest to us and we will give explicit constructions of them as well.

This thesis is in the field of discrete mathematics and combinatorial optimization and uses basic abstract (linear) algebra and try & search with the computer package MAGMA to obtain results.

I would like to thank Kallenberg, Peeters, Edixhoven, Bosma, Williford and Godsil voor non-published information and feedback.

Chapter 1

Introduction

We will introduce the discrete and algebraic structures needed for this thesis together with their properties.

1.1 Graphs

The graphs in this thesis are finite and undirected. Although we will rarely mention them explicitly the vertex set and the edge set of a graph $G = (V, E)$ are V and E respectively. Parallel edges are not allowed neither do we allow ***loops*** (that is edges that connect a vertex to itself) unless stated otherwise. Some terminology to start with:

- A ***clique*** is a subset of the vertex set of G such that every pair of vertices in the subset is adjacent. The size of the largest clique in G is named the ***clique number*** and is denoted by $\omega(G)$.
- An ***independent set*** (also known as ***coclique*** or ***stable set***) is a subset of the vertex set of G such that none of the vertices in the subset are adjacent. The size of the largest independent set is denoted by $\alpha(G)$.
- A ***k-coloring*** of G is a coloring of the vertex set with k colors such that every two vertices which are adjacent have a different color. An equivalent definition is that of partitioning the vertex set in k independent sets. The smallest number k such that a graph is still **k-colorable** is called the ***chromatic number*** and is denoted by $\gamma(G)$.

As an example the graph G from Figure 1.1 is given. The subset $\{2, 3, 6\}$ is a clique and it is of maximal cardinality so $\omega(G) = 3$. Note there is another clique which has maximal cardinality as well, it is the subset $\{2, 5, 6\}$. An example of an independent set is the subset $\{1, 6\}$, it is not of maximal cardinality as $\{1, 5, 4\}$ has size 3 and is an independent set as well. It is not difficult to see that $\alpha(G) = 3$. An example of a minimal coloring possible is $\{1, 6\}, \{3, 5\}, \{2, 4\}$ so $\gamma(G) = 3$.

A straightforward relation between $\alpha(G)$ and $\omega(G)$ is given by

$$\alpha(\overline{G}) = \omega(G),$$

where $\overline{G}$ is the complementary graph of G. In general determining $\omega(G)$, $\alpha(G)$ and $\gamma(G)$ is not an easy task. This has been given the mathematical formulation which can be found in many books among which [17] (it are the Theorems 64.1 and 64.2 and Corollary 64.1a).

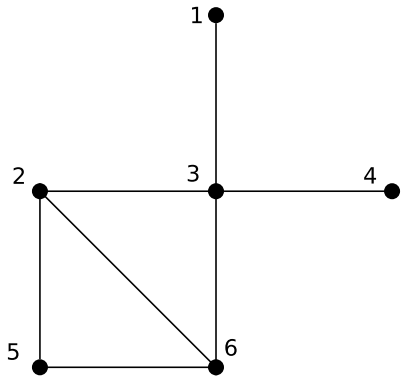

Figure 1.1: Example

Theorem 1.1. *In general determining $\omega(G)$, $\alpha(G)$ and $\gamma(G)$ is NP-complete.*

Some exceptions for which determining $\gamma(G)$ is easy:

- $\gamma(G) = 2$ when G is an even cycle and $\gamma(G) = 3$ when G is an odd cycle.
- $\gamma(G) = n$ in the case G is a clique on n vertices.
- $\gamma(G) = 2$ in the case G is bipartite and the edge set is non-empty..

We also have the well known 4-coloring theorem by Appel and Haken which states:

Theorem 1.2. *If G is planar then $\gamma(G) \leq 4$.*

However it is NP-complete to decide whether a planar graph is 3-colorable [3].

For every vertex $v \in V$ we define a vertex $w \in V$ to be a ***neighbor*** of v if w is adjacent to v. The ***degree*** $\deg(v)$ is the number of neighbors of v. A well known relation between the cardinality of the edge set E and the degree of the vertices of a graph without loops is

$$\sum_{v \in V} \deg(v) = 2|E|. \tag{1.1}$$

The ***diameter*** $d(G)$ of a graph is the maximum of lengths (that is the number of edges in a path) of all shortest paths between any two vertices in G:

$$d(G) = \max\{\text{length of shortest path between } v \text{ and } w : v, w \in V\}.$$

The example we gave at the beginning of this section has diameter 3. Given a graph G the ***adjacency matrix*** is the matrix A such that for two vertices u and v in G we have $A_{uv} = 1$ if u and v are adjacent and $A_{uv} = 0$ if u and v are *not* adjacent. Note the adjacency matrix is a real symmetric matrix. The adjacency matrix of our example is

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}. \tag{1.2}$$

The adjacency matrix may have 1s on the diagonal. This is the case when the graph has loops.

A ***(graph) isomorphism*** of graphs G and G' is a bijection $f : V \longrightarrow V'$ of the vertex sets such that for every *distinct* $u, w \in V$ holds

$$u \text{ and } w \text{ are adjacent} \iff f(u) \text{ and } f(w) \text{ are adjacent.}$$

A useful fact which helps us to reason on isomorphisms and images of isomorphisms is

$$\deg(v) = \deg(f(v)), \quad \text{for every } v \in V. \tag{1.3}$$

If $G = G'$ then f is called an ***(graph) automorphism***. The set of all automorphisms, we write $\mathrm{Aut}(G)$, of a graph is obviously a group and it is a subgroup of the symmetry group $\mathrm{Sym}(V)$ of V. The automorphism group of our example in the beginning of the section is

$$\langle (1\ 4), (2\ 6) \rangle.$$

Because the automorphism group acts on the vertex set of a graph we can use a result from the theory of groups to introduce a trick to find the order of the automorphism group of a graph. For every vertex $v \in V$ we have

$$|\mathrm{Aut}(G)| = |\mathrm{Aut}(G)_v| \cdot |\mathrm{Aut}(G)v|.$$

Here $\mathrm{Aut}(G)_v \subseteq \mathrm{Aut}(G)$ is the stabilizer of v and $\mathrm{Aut}(G)v \subseteq V$ the orbit of v. So by fixing a suitable vertex of G we might be able to find $|\mathrm{Aut}(G)|$. Applying this technique to our example we fix vertex $v = 1$ so $|\mathrm{Aut}(G)_v| = 2$ and $|\mathrm{Aut}(G)v| = 2$ giving us $|\mathrm{Aut}(G)| = 4$. Similarly we find $|\mathrm{Aut}(C_n)| = 2n$.

1.2 Groups and fields

This section recalls some results from basic abstract algebra which are worth mentioning regarding this thesis. The first result enables us to reason about the existence of rth roots of elements in $\mathbf{F}_q$ and can be found in almost any book on algebra. We give a short elegant proof from [11].

Proposition 1.3. *The group of units $\mathbf{F}_q^*$ of a finite field $\mathbf{F}_q$ is a cyclic group of order $q - 1$.*

Proof. We know $\mathbf{F}_q^*$ is, with respect to multiplication, an abelian group of order $q-1$. For each maximal primepower p^r dividing $q-1$ there is a subgroup $U_{p^r} \subseteq \mathbf{F}_q^*$ (**Sylow**). Write $\mathbf{F}_q^*$ as a product of these subgroups U_{p^r} (exercise 13 and the accompanying example in Chapter I of [11]).

First we will show each U_{p^r} is cyclic. Let $a \in U_{p^r}$ be an element of maximal order p^k. So for every $x \in U_{p^r}$ holds $x^{p^k} = 1$ and therefore all elements in U_{p^r} are roots of the polynomial equation

$$X^{p^k} = 1.$$

The cyclic group generated by a has p^k elements. If this cyclic group is not equal to U_{p^r} then our polynomial has more than p^k roots, which is impossible. So U_{p^r} is cyclic. Because the orders of the subgroups U_{p^r} are all coprime the product of them is cyclic (Proposition 4.3(v) in Chapter I of [11]) so $\mathbf{F}_q^*$ is cyclic. □

As a reminder. A generator of $\mathbf{F}_q^*$, where q is not a prime, can act as a solution of the minimum-polynomial which defines a finite field $\mathbf{F}_q$.

An $x \in \mathbf{F}$ (this definition is for infinite fields too) is called a ***square*** if there exists a $y \in \mathbf{F}$ such that $x = y^2$. An application of this definition and the previous proposition is the next proposition which is about the number of squares in a finite field.

Proposition 1.4. *Given arbitrary finite field $\mathbf{F}_q$.*

*(i) If q is even then every element in $\mathbf{F}_q$ is a square (we say $\mathbf{F}_q$ is **perfect**).*

(ii) If q is odd then there are exactly $(q+1)/2$ squares in $\mathbf{F}_q$.

(iii) If q is odd then for every $k \in \mathbf{F}_q$ there exists $c, d \in \mathbf{F}_q$ such that $c^2 + d^2 = k$.

Proof. We have:

(i) If q is even then $\mathbf{F}_q^* = \langle \alpha \rangle$ is a cyclic group of odd order $q-1$. If for arbitrary $\alpha^t \in \langle \alpha \rangle$ holds t is even then α^t is a square. If t is odd then

$$\alpha^t = \alpha^t \alpha^{q-1} = \alpha^{t+q-1}.$$

Now $t+q-1$ is even so there exists an integer j such that $2j = t+q-1$ so $(\alpha^j)^2 = \alpha^t$ so α^t is a square.

(ii) For q is odd $\mathbf{F}_q^* = \langle \alpha \rangle$ is of even order $q-1$. So there are $(q-1)/2$ elements in $\langle \alpha \rangle$ which are a square. The elements of the form α^{2t+1} are not a square as for every element α^i holds $(\alpha^i)^2 = \alpha^{2i+(q-1)m}$ where $2t+1$ is odd and $2i+(q-1)m$ is even for every i or m.

(iii) If you range over all $c \in \mathbf{F}_q$ then $k - c^2$ takes $(q+1)/2$ different values. As there are $(q-1)/2$ non-squares in $\mathbf{F}_q$ one of the values $k - c^2$ is a square so k can be written as the sum of two squares.

□

The argument used in the proof of Proposition 1.4(iii) is in combinatorics often referred to as *'the pigeonhole principle'*. Some other well known small results are:

Proposition 1.5. *Given a prime power $q = p^n$ we have*

(i) For an arbitrary element $x \in \overline{\mathbf{F}}_q$ (the algebraic closure of $\mathbf{F}_q$) holds: $x^q = x \iff x \in \mathbf{F}_q$.

(ii) For every $x, y \in \mathbf{F}_q$ holds $(x+y)^p = x^p + y^p$.

(iii) The automorphism group $\mathrm{Aut}(\mathbf{F}_q)$ is cyclic of order n and is generated by $x \mapsto x^p$.

Proof. We have:

(i) As $\mathbf{F}_q^*$ is, with respect to multiplication, a group of order $q-1$ we have for arbitrary $x \in \mathbf{F}_q^*$ that holds $x^{q-1} = 1$ so every $x \in \mathbf{F}_q$ satisfies

$$X^q = X. \tag{1.4}$$

Because every polynomial of degree q has q solutions in $\overline{\mathbf{F}}_q$ this means all the solutions of (1.4) are in $\mathbf{F}_q$. So an element in $\overline{\mathbf{F}}_q$ not in $\mathbf{F}_q$ won't satisfy (1.4).

(ii) The justification is that all, except two, binomial-coefficients in the expansion of $(x+y)^p$ are divisible by p. For $i = 0, p$ we have $\binom{p}{i} = 1$. For an integer i with $0 < i < p$ we have $\binom{p}{i}$ an integer which is divisible by p because as p is prime p does not divide $i!$ nor $(p-i)!$. Now p is the characteristic of $\mathbf{F}_q$ so $(x+y)^p = x^p + y^p$.

(iii) See Theorem 5.3 (Chapter V) in [11].

□

Note that we can apply the statement in Proposition 1.5(ii) repeatedly so for every integer k and any $x, y \in \mathbf{F}_q$ we have

$$(x+y)^{p^k} = x^{p^k} + y^{p^k}. \tag{1.5}$$

Now we have enough results for our last proposition.

Proposition 1.6. *Given an odd prime-power q.*

(i) $q \equiv 1 \bmod 4 \iff$ -1 is a square in $\mathbf{F}_q$.

(ii) $q \equiv 1, 3 \bmod 8 \iff$ -2 is a square in $\mathbf{F}_q$.

(iii) $q \equiv 1, 7 \bmod 8 \iff$ +2 is a square in $\mathbf{F}_q$.

Proof. Proof of the three cases:

(i) ($\Rightarrow$) $\mathbf{F}_q^*$ is a cyclic group of order $q - 1 = 4t$ (for an integer t) with respect to multiplication so there is a 4th root of unity $\zeta_4 \in \mathbf{F}_q$ for which holds $(\zeta_4^2)^2 = 1$ so $\zeta_4^2 = -1$ so -1 is a square in $\mathbf{F}_q$.

($\Leftarrow$) When $q \equiv 3 \bmod 4$ we have $q - 1 = 4t + 2$ (for an integer t) so there is no 4th root of unity in $\mathbf{F}_q$.

(ii) ($\Rightarrow$) There is an integer t such that $q = 8t + 1$ (this case is for $q \equiv 1 \bmod 8$). As $\mathbf{F}_{q^2}^*$ is a cyclic group of order $q^2 - 1 = 8(8t^2 + 2t)$ this means there is an 8th root of unity $\zeta_8 \in \mathbf{F}_{q^2}$. We have

$$(\zeta_8 + \zeta_8^3)^2 = \zeta_8^2 + 2\zeta_8^4 + \zeta_8^6 = -2.$$

This is easy to see because $(\zeta_8^4)^2 = 1$ and $(\zeta_8^2 + \zeta_8^6)^2 = 0$. By observing

$$(\zeta_8 + \zeta_8^3)^q =_{(1.5)} \zeta_8^q + \zeta_8^{3q} = \zeta_8^{8t+1} + \zeta_8^{24t+3} = \zeta_8 + \zeta_8^3,$$

and Proposition 1.5(i) we find $\zeta_8 + \zeta_8^3 \in \mathbf{F}_q$ so -2 is a square in $\mathbf{F}_q$.

($\Leftarrow$) When $q \equiv 5, 7 \bmod 8$ we have $\zeta_8 \in \mathbf{F}_{q^2}$ so $\zeta_8 + \zeta_8^3 \in \mathbf{F}_{q^2}$. But now (in both cases of q)

$$(\zeta_8 + \zeta_8^3)^q = \zeta_8^5 + \zeta_8^7 = -(\zeta_8 + \zeta_8^3) \neq \zeta_8 + \zeta_8^3$$

so (by Proposition 1.5(i)) $\zeta_8 + \zeta_8^3 \notin \mathbf{F}_q$ so -2 is not a square in $\mathbf{F}_q$.

(iii) This case goes similar to showing when -2 is a square but now consider the element $\zeta_8 + \zeta_8^{-1} \in \mathbf{F}_{q^2}$.

□

1.3 Linear algebra

We start with a well known useful result on the eigenvalues of a real symmetric matrix which can, for example, be found in [12] as an exercise.

Proposition 1.7. *If A is a real symmetric $n \times n$ matrix then every eigenvalue of A is real.*

Proof. Let $x \in \mathbf{C}^n$ be a vector. Define $\beta = \overline{x}^T A x$. Then

$$\overline{\beta} = \overline{\overline{x}^T A x} = x^T \overline{A} \overline{x} = x^T A \overline{x} = (x^T A \overline{x})^T = \overline{x}^T A^T x = \overline{x}^T A x = \beta.$$

So $\beta = \overline{x}^T A x$ is a real number. If x is an eigenvector corresponding to an eigenvalue $\lambda \in \mathbf{C}$ of A then we have $Ax = \lambda x$ and we compute

$$\overline{x}^T A x = \overline{x}^T \lambda x = \lambda \cdot \overline{x}^T x.$$

Because $\overline{x}^T A x$ is real and $\overline{x}^T x$ is real this implies λ is real. □

The previous proposition holds for Hermitian ($\overline{A} = A^T$) matrices too. For the proof we can use the same β. We have another result which can be found in most books on (linear)algebra. For every complex $n \times n$ matrix A with eigenvalues $\lambda_1, \ldots, \lambda_n$ (not all necessarily distinct), the sum of the eigenvalues equals the trace. That is

$$\mathrm{tr} A = \sum_{i=1}^{n} \lambda_i. \tag{1.6}$$

This is by the fact that for two square matrices A and B holds $\mathrm{tr}AB = \mathrm{tr}BA$ and **Jordan**'s decomposition theorem (Theorem 5.20 in [10]).

Given a vector space W. A subset $\mathcal{B} \subseteq W$ is a ***basis*** for W if $\langle \mathcal{B} \rangle = W$ and any $v_1, \ldots, v_k \in \mathcal{B}$ are linearly independent. The cardinality of a basis for W is called the ***dimension*** of W. If the cardinality is finite the we say W is ***finite dimensional***. In this thesis all vector spaces are finite dimensional.

Given a subspace of a finite dimensional vector space $V \subseteq W$ we can ***extend a basis*** of V to a basis of W by the following procedure. Pick a vector $w_1 \in V^c$. Next pick a vector $w_2 \in \langle V \cup \{w_1\} \rangle^c$. Repeat this till you have extended a basis of V to a basis of W with new extra basis vectors $w_1, w_2, \ldots, w_k$. This way we can construct a basis for V too by taking the vector space $\{0\}$ as a starting point.

The next proposition gives an overview of some statements about dimensions of vector spaces which can be found in many books such as in [10], [11] or [16].

Proposition 1.8. *Given subspace and finite dimensional vector space $V \subseteq W$.*

(i) $\dim(V) \leq \dim(W)$.

(ii) If $\dim(V) = \dim(W)$ *then* $V = W$.

(iii) $\dim(W) = \dim(V) + \dim(W/V)$

Proof. Basis extension is the key concept in the proofs of the items. □

A direct consequence of Proposition 1.8(ii) is the next proposition

Proposition 1.9. *Given a linear function $\psi : W \longrightarrow \widetilde{W}$ where W and $\widetilde{W}$ are finite dimensional and* $\dim(W) = \dim(\widetilde{W})$. *If ψ is injective then ψ is surjective.*

The following proposition allows us to reason on dimensions of two subspaces $U, S \subseteq W$ of a vector space. Here $U + S$ is the set of the sum of all elements in U and S and $U \oplus S$ is the direct sum.

Proposition 1.10. *Given subspaces and finite dimensional vector space $U, S \subseteq W$.*

(i) If $W = U \oplus S$ then $\dim(W) = \dim(U) + \dim(S)$.

(ii) $\dim(U) + \dim(S) = \dim(U + S) + \dim(U \cap S)$.

Proof. We have:

(i) Let $\mathcal{B}_U$ be a basis for U and $\mathcal{B}_S$ be a basis for S. Then by definition of direct sum $W = \langle \mathcal{B}_U \cup \mathcal{B}_S \rangle$. Pick an arbitrary linear combination $u \neq 0$ of $\mathcal{B}_U$ and an arbitrary linear combination $s \neq 0$ of $\mathcal{B}_S$. U and S are, with respect to addition, groups. As their intersection equals 0 (by definition) this implies $u \notin S$ and $s \notin U$ so $u + s \notin U \cup S$ so $u + s \neq 0$ so $\mathcal{B}_U \cup \mathcal{B}_S$ is linearly independent so $\mathcal{B}_U \cup \mathcal{B}_S$ is a basis for W.

(ii) *(About the notation in this proof. The symbols for sum and intersection have stronger binding than the symbol for the factor group)* By definition of direct sum (see notation index) we have

$$(U/U \cap S) \oplus (S/U \cap S) = U + S/U \cap S. \tag{1.7}$$

The set $U \cap S$ acts as a zero element in (1.7). From (1.7) and (i) we deduce

$$\dim(U/U \cap S) + \dim(S/U \cap S) = \dim(U + S/U \cap S) \tag{1.8}$$

From Proposition 1.8(iii) we deduce

$$\begin{aligned} \dim(U) &= \dim(U \cap S) + \dim(U/U \cap S), \\ \dim(S) &= \dim(U \cap S) + \dim(S/U \cap S). \end{aligned}$$

Combining these two identities with (1.8) we get our desired equality.

□

1.4 Bilinear forms

Given a vector space W over a field $\mathbf{F}$. By a ***bilinear form*** we define a function $W \times W \longrightarrow \mathbf{F}$, denoted by $\langle \cdot, \cdot \rangle$, such that for all $u, v, w \in W$ and all $c \in \mathbf{F}$ holds

(BF1) $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle$;

(BF2) $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$;

(BF3) $\langle cu, v \rangle = c\langle u, v \rangle$;

(BF4) $\langle u, cv \rangle = c\langle u, v \rangle$.

From our definition we immediately deduce (note we can use (BF1) and (BF2) or (BF3) and (BF4)) that for every $w \in W$ holds

$$\langle w, 0 \rangle = 0 = \langle 0, w \rangle.$$

From (BF1) we can proof the first identity.

$$\langle w, 0 \rangle = \langle w, 0 + 0 \rangle = \langle w, 0 \rangle + \langle w, 0 \rangle$$

so $\langle w, 0 \rangle = 0$. An example of a bilinear form on $x, y \in \mathbf{F}^n$ is the multiplication by an $n \times n$ matrix A over the field $\mathbf{F}$:

$$\langle x, y \rangle := x^T A y. \tag{1.9}$$

In fact, every bilinear form on a vector space $\mathbf{F}^n$ can be written as the multiplication with an $n \times n$ matrix over the field $\mathbf{F}$ like in (1.9). Now we list some definitions:

- A bilinear form is called ***symmetric*** if for all $v, w \in W$ holds $\langle v, w \rangle = \langle w, v \rangle$.
- A symmetric bilinear form is called ***non-degenerate*** if for every non-zero $v \in W$ there is a non-zero $w \in W$ such that $\langle v, w \rangle \neq 0$.

- Two vectors $v, w \in W$ are ***orthogonal*** if $\langle v, w\rangle = 0$. This not necessarily implies $\langle w, v\rangle = 0$ which can be seen by finding a counterexample:

$$v = \begin{bmatrix} 1 \\ -1 \end{bmatrix}, M = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}, w = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

  We have $v^T M w = 0$ there $w^T M v = -4$.

- Two subspaces $S, U \subseteq W$ are ***orthogonal subspaces***, and we write $S \perp U$, if for all $s \in S$ and all $u \in U$ holds $\langle s, u\rangle = 0$.

- The ***orthogonal complement*** of a subspace $U \subseteq W$ is the subset $U^\perp \subseteq W$ of all vectors $w \in W$ which are orthogonal to every vector in U:

$$U^\perp := \{w \in W : \langle w, u\rangle = 0 \text{ for all } u \in U\}.$$

  It is easy to verify $U^\perp$ is a subspace of W.

We continue with a short proposition.

Proposition 1.11. *Given a symmetric bilinear form induced by a symmetric matrix A on a vector space W. Then A is invertible $\iff$ the bilinear form is non-degenerate.*

Proof. We Have:

($\Rightarrow$) A is invertible. Pick an arbitrary non-zero vector $w \in W$. Because $w \neq 0$ there is an integer i such that $w^T e_i \neq 0$ (here e_i is the vector with the ith entry equal to 1 and the other entries equal to 0). Because A is invertible the equation $Ax = e_i$ has a non-zero solution $x \in W$. Now

$$\langle w, x\rangle = w^T A x = w^T e_i \neq 0$$

so the bilinear form is non-degenerate.

($\Leftarrow$) We prove the negation. If A is not invertible then there is a non-zero $x \in W$ such that $Ax = 0$ so the bilinear form is not non-degenerate.

□

The next proposition gives a relation between the dimensions of U, $U^\perp$ and W. Its proof can by found in [10] or [16].

Proposition 1.12. *If the symmetric bilinear-form on the finite dimensional vector space W is non-degenerate then for every subspace $U \subseteq W$ holds*

$$\dim(U) + \dim(U^\perp) = \dim(W).$$

Proof. We introduce the dual space U' of U. That is the set of all linear functions $U \longrightarrow \mathbf{F}$. Now introduce the function

$$\begin{array}{rcl} \psi : W & \longrightarrow & U' \\ w & \longmapsto & (u \mapsto \langle u, w\rangle). \end{array}$$

For the kernel and the image of ψ we claim

$$\begin{aligned} \ker \psi &= U^{\perp}, && (1.10)\\ \text{im } \psi &= U'. && (1.11) \end{aligned}$$

(1.10) follows from the definition of $U^{\perp}$. (1.11) requires some work. We start by choosing a subspace $\widetilde{U} \subseteq W$ (to construct $\widetilde{U}$ use the concept of basis extension to obtain basis vectors for $\widetilde{U}$) such that

$$W = U \oplus \widetilde{U}. \tag{1.12}$$

Next pick arbitrary $u' \in U'$ and define a function w' by

$$w' = \begin{cases} u' & \text{on } U, \\ 0 & \text{on } \widetilde{U}. \end{cases}$$

By (1.12) it is safe to say $w' \in W'$ (the dual space). Since the bilinear form $\langle \cdot, \cdot \rangle$ is non-degenerate the linear function

$$\begin{aligned} \varphi : W &\longrightarrow W' \\ w &\longmapsto (v \mapsto \langle v, w \rangle) \end{aligned}$$

is a surjection (see *supporting proof*). Thus we can choose $w \in W$ with $\varphi(w) = w'$. Then for all $u \in U$,

$$\psi(w)(u) = \langle u, w \rangle = \varphi(w)(u) = w'(u) = u'(u)$$

and hence $\psi(w) = u'$. Therefore im $\psi = U'$ and we conclude that

$$\begin{aligned} \dim(W) &= \dim(\ker \psi) + \dim(\text{im } \psi) && (1.13)\\ &= \dim(U^{\perp}) + \dim(U') \\ &= \dim(U^{\perp}) + \dim(U). \end{aligned}$$

(1.13) is Theorem 2.8 in [16].

supporting proof: We have $\dim(W) = \dim(W')$. This is because W has a finite basis $b_1, \ldots, b_n \in W$. So for all $T \in W'$ and every $c_1 b_1 + \cdots + c_n b_n \in W$ holds

$$T(c_1 b_1 + \cdots + c_n b_n) = c_1 T(b_1) + \cdots + c_n T(b_n).$$

As all $T(b_i)$ are scalars we can with fixed elements $b'_1, \ldots, b'_n \in \mathbf{F}_q$ and for every T suitable scalars $s_1, \ldots, s_n$ obtain any element from W'. The only way to create the zero-map is by picking $s_1, \ldots, s_n = 0$ so by definition our elements $b'_1, \ldots, b'_n$ form a basis and we have $\dim(W) = \dim(W')$.

Because φ is a homomorphism of (additive) groups with $\ker \varphi = 0$ (follows from the bilinear form which is non-degenerate) φ is injective so we can apply Proposition 1.9 to show φ is a surjection. $\square$

A small result which follows from this proposition is the following

Proposition 1.13. *For a symmetric non-degenerate bilinear form on a subspace and finite dimensional vector space $U \subseteq W$ holds $U^{\perp\perp} = U$.*

Proof. From Proposition 1.12 we deduce $\dim(U^{\perp\perp}) = \dim(U)$. We also have $U \subseteq U^{\perp\perp}$ so by Proposition 1.8(ii) we have equality. □

Now we give an example of a vector space W, a non-degenerate bilinear form and a subspace $U \subseteq W$ such that $U \cap U^{\perp}$ is non-zero (opposed to a real or complex inner-product space where the intersection equals 0). Take $W = \mathbf{R}^2$, a bilinear form defined on any $x, y \in \mathbf{R}^2$ by

$$\langle x, y \rangle := x^T \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} y = x_1 y_1 - x_2 y_2,$$

and the subspace $U = \{(c, c) : c \in \mathbf{R}\}$. Now $U^{\perp} = U$ so $U \cap U^{\perp}$ is non-zero.

Chapter 2

Projective planes

This chapter will introduce projective planes and their relation with subspaces of $\mathbf{F}_q^3$. This chapter is needed to show some important properties of our subject of study which we will present in the chapter after this one.

2.1 Projective planes an polarities

A ***projective plane*** Π is a finite set of ***points*** and a finite set of ***lines*** such that:

(PP1) Every pair of points are exactly on (set theoretic membership or inclusion) one line.

(PP2) Every pair of lines intersects (set theoretic intersection) in exactly one point.

(PP3) There are four points such that no three of them are on the same line.

An example of a projective plane is the vector space $\mathbf{F}_q^3$ where the 1-dimensional subspaces of $\mathbf{F}_q^3$ are the points and the 2-dimensional subspaces of $\mathbf{F}_q^3$ are the lines. For (PP2) one might want to use Proposition 1.10(ii). For (PP3) we can take the vectors $e_1, e_2, e_3, 1 \in \mathbf{F}_q^3$. In the literature $\mathbf{F}_q^3$, when viewed as a projective plane, is often referred to as $PG(2,q)$. Figure 2.1 shows $PG(2,2)$. See also [9] for an extensive treatise on projective planes.

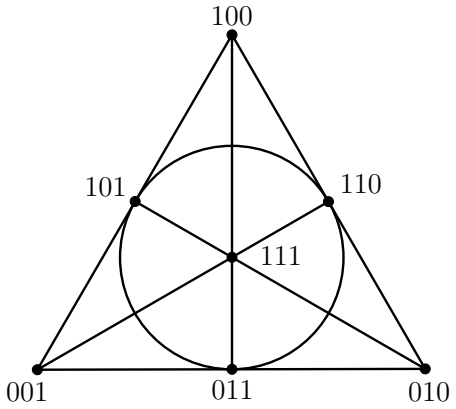

Figure 2.1: The projective plane $PG(2,2)$, also called the **Fano** plane

Proposition 2.1. *In every projective plane there are 4 lines such that no three of them intersects in the same point.*

Proof. By (PP3) there are four points A, B, C and D such that no three of them are on the same line. Therefore by (PP1) we have 4 *distinct* lines AB, BC, CD and DA. If any three of those lines (say AB, BC and CD) intersect in a point P then this would violate (PP2). So we have 4 lines such that no three of them intersect in one point. □

By the previous proposition lines of a projective plane Π can be seen as "points" and points of Π as "lines". We call this projective plane Π^* the ***dual*** of Π. In some cases reasoning on the dual Π^* might give us short proofs of propositions for Π.

Proposition 2.2. *Not all points are on two lines.*

Proof. Assume all points are on two lines $\mathcal{L}$ and $\mathcal{M}$. By (PP3) we have 4 distinct points L_1, L_2 on $\mathcal{L}$ and M_1, M_2 on $\mathcal{M}$. The lines L_1M_1 and L_2M_2 intersect by (PP2) in a point P not equal to L_1, L_2, M_1 or M_2 (by (PP3)). If P is on $\mathcal{L}$ then the line L_1M_1 intersects $\mathcal{L}$ twice, violating (PP2). If P is on $\mathcal{M}$ then the line L_1M_1 intersects $\mathcal{M}$ twice, violating (PP2) again. So there is a point not on $\mathcal{L}$ or $\mathcal{M}$. □

Another proposition is

Proposition 2.3. *For a projective plane we have:*

(i) Every line contains the same number of points.

(ii) Every point is on the same number of lines.

(iii) The number of lines which intersects a point equals the number of points on a line.

Proof. We have:

(i) Follows from Proposition 2.2 and (PP1) and (PP2).

(ii) By (i) and the dual.

(iii) Pick a line $\mathcal{L}$ and a point P not on $\mathcal{L}$. For every point on $\mathcal{L}$ there is by (PP1) a line which intersects that point and P. As every line P is on intersects, by (PP2), $\mathcal{L}$ this implies the number of lines which intersects a point equals the number of points on a line.

□

With Proposition 2.3 we have the next proposition:

Proposition 2.4. *For a projective plane we have:*

(i) On every line are $n+1$ points.

(ii) Every point is on $n+1$ lines.

(iii) There are n^2+n+1 points.

(iv) There are n^2+n+1 lines.

Proof. We have:

(i) By Proposition 2.3(i) we are free to say there are $n+1$ points on every line.

(ii) By (i) and the dual.

(iii) By the previous two items we have $n+1$ points on a line $\mathcal{L}$ and every point on $\mathcal{L}$ is on $n+1$ lines. So there are $(n+1)n$ lines which intersect $\mathcal{L}$ so including $\mathcal{L}$ there are n^2+n+1 lines.

(iv) By (iii) and the dual.

□

By Proposition 2.4 we say a projective plane is of ***order*** n.

Given a projective plane $\Pi = (X, L)$ (here X is the set of points, L is the set of lines) a ***polarity*** is a function $\phi : X \cup L \longrightarrow X \cup L$ such that holds:

(Po1) for every point $x \in X$ we have $\phi(x) \in L$;

(Po2) for every line $l \in L$ we have $\phi(l) \in X$;

(Po3) the composition $\phi^2 = \phi \circ \phi$ is the identity function on $X \cup L$.

On the projective plane $PG(2, q) = (X, L)$ (here X is the set of all 1-dimensional subspaces of $\mathbf{F}_q^3$ and L is the set of all 2-dimensional subspaces of $\mathbf{F}_q^3$) we define a polarity ϕ on any $U \in X \cup L$ by:

$$U \longmapsto U^{\perp} \tag{2.1}$$

From Proposition 1.12 we easily deduce that for any $U \in X \cup L$ holds

$$\begin{array}{ll} \dim(\phi(U)) = \dim(U^{\perp}) = 2 & \text{when } \dim(U) = 1, \\ \dim(\phi(U)) = \dim(U^{\perp}) = 1 & \text{when } \dim(U) = 2. \end{array}$$

This makes our ϕ satisfying (Po1) and (Po2). Proposition 1.13 makes our ϕ satisfies (Po3).

2.2 Subspaces of $\mathbf{F}_q^n$

In the previous section we gave $\mathbf{F}_q^3$ as an example of a projective plane. It satisfies:

(PP1′) For every two *distinct* 1-dimensional subspaces (points) X and Y there is exactly one 2-dimensional subspace (line) $\mathcal{U}$ such that $X, Y \subseteq \mathcal{U}$.

(PP2′) For every two *distinct* 2-dimensional subspaces (lines) $\mathcal{U}$ and $\mathcal{S}$ the intersection $\mathcal{U} \cap \mathcal{S}$ contains one unique 1-dimensional subspace (point).

(PP3′) There exist four *distinct* 1-dimensional subspaces (points) such that no three of them are contained in the same 2-dimensional subspace (line).

We can use the propositions from section 2.1 to learn about the subspaces of $\mathbf{F}_q^3$. This section contains two propositions to derive the same claims without the theory of projective planes.

Proposition 2.5. *The number of subspaces of dimension k in a vector space $\mathbf{F}_q^n$ is*

$$\frac{(q^n-1)\dots(q^2-1)(q-1)}{(q^k-1)\dots(q^2-1)(q-1)\cdot(q^{n-k}-1)\dots(q^2-1)(q-1)}.$$

Proof. By S we define a subset $S \subseteq \mathbf{F}_q^n$ with $|S| = k$ and all the vectors in S linearly independent (so S is a basis for a k-dimensional subspace). Then the number of subsets S contained in $\mathbf{F}_q^n$ is

$$\frac{(q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{k-1})}{k!}. \tag{2.2}$$

This is easy to see as we have q^n-1 choices for our first vector. This leaves us with q^n-q choices for our second vector. This goes on till we have the numerator of (2.2). See also the concept of basis extension mentioned in section 1.3. We avoid double counting by putting $k!$ in the denominator of (2.2).

From (2.2) we also deduce that the number of subsets $S \subseteq W \subseteq \mathbf{F}_q^n$ (here W is a subspace with $\dim(W) = k$) is

$$\frac{(q^k-1)(q^k-q)(q^k-q^2)\dots(q^k-q^{k-1})}{k!}. \tag{2.3}$$

If N is the total number of subspaces $W \subseteq \mathbf{F}_q^n$ of dimension k then combining (2.2) and (2.3) gives the following counting relation for S:

$$\frac{(q^k-1)\dots(q^k-q^{k-1})}{k!} \cdot N = \frac{(q^n-1)\dots(q^n-q^{k-1})}{k!}.$$

This is because (PP1′): an S can not be contained in two different subspaces. So we deduce

$$N = \frac{(q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)(q^k-q^2)\dots(q^k-q^{k-1})}.$$

By induction we can show N equals our desired identity. For $k = 1$ it is obvious the equality holds for all n. By multiplying with

$$\frac{q^k(q^{n+1}-1)}{q^k(q^{k+1}-1)},$$

we can proof that when the equality holds for n and k it becomes valid for $n+1$ and $k+1$. □

So with the previous proposition we can state the next proposition which summarizes the relation between 1-dimensional and 2-dimensional subspaces of $\mathbf{F}_q^3$.

Proposition 2.6. *For $\mathbf{F}_q^3$ we have:*

(i) q^2+q+1 *subspaces of dimension 1.*

(ii) q^2+q+1 *subspaces of dimension 2.*

(iii) Each 2-dimensional subspace has $q+1$ *subspaces of dimension 1.*

(iv) Every 1-dimensional subspace is contained in $q+1$ *subspaces of dimension 2.*

Proof. The items (i), (ii) and (iii) follow form the previous proposition. For the last item let N be the number of 2-dimensional subspaces of $\mathbf{F}_q^3$ which contain an arbitrary 1-dimensional subspace $U \subseteq \mathbf{F}_q^3$. Then, by the previous items and (PP1′), we have the following counting relation for N:

$$(q+1)N - N + 1 = q^2 + q + 1.$$

From this relation we deduce $N = q + 1$. □

2.3 Ovals of $PG(2, q)$

An ***oval*** $\mathcal{O}$ is a set of $n+1$ points in a projective plane Π of order n such that no three points in $\mathcal{O}$ are on the same line. Given a set $\mathcal{S}$ of points of $PG(2, q)$. A line which intersects $\mathcal{S}$ in

- 0 points is called an ***external line***;
- 1 point is called a ***unisecant***;
- 2 points is called a ***bisecant***.

With these new definitions we have the following proposition.

Proposition 2.7. *For q is odd: in $PG(2, q)$ every point not in an oval $\mathcal{O}$ lies on exactly two or no unisecants of $\mathcal{O}$.*

Proof. Lemma 8.10 in [8]. □

We will now introduce two other definitions. For odd q a point of $PG(2, q)$ is called ***external*** if it lies on two unisecants of an oval $\mathcal{O}$ in $PG(2, q)$. A point is called ***internal*** if it lies on no unisecants of $\mathcal{O}$. Now we can, for odd q, classify lines and points of $PG(2, q)$ with respect to an oval $\mathcal{O}$ by the following proposition:

Proposition 2.8. *Let q be odd. With respect to an oval $\mathcal{O}$ in $PG(2, q)$ we have:*

(i) $q + 1$ *unisecants;*

(ii) $q(q + 1)/2$ *bisecants;*

(iii) $q(q - 1)/2$ *external lines.*

Proof. We have:

(i) Let P be arbitrary point in $\mathcal{O}$, we have $|\mathcal{O}| = q + 1$ so by (PP1) we have q lines with P on it accompanied by another point from $\mathcal{O}$. By 2.4(ii) there must be one other line P is on, as $\mathcal{O}$ is an oval that line must be a unisecant. We have $q + 1$ such points so $q + 1$ unisecants.

(ii) There are $q(q + 1)/2$ ways to choose 2 out of $q + 1$ points. By (PP1) there is a line which intersects any 2 points in $\mathcal{O}$. By definition of oval any such line can not intersect other points of $\mathcal{O}$.

(iii) As we have a total of $q^2 + q + 1$ lines there are, by (i) and (ii), $q(q - 1)/2$ external lines.

□

For the points of $PG(2,q)$ we have

Proposition 2.9. *Let q be odd. With respect to an oval $\mathcal{O}$ in $PG(2,q)$ we have:*

(i) $q+1$ *points on* $\mathcal{O}$*;*

(ii) $q(q+1)/2$ *external points;*

(iii) $q(q-1)/2$ *internal points.*

Proof. We have:

(i) By definition.

(ii) There are $q(q+1)/2$ ways to choose 2 out of $q+1$ points of $\mathcal{O}$. So there are $q(q+1)/2$ ways to pick 2 unisecants. A pair of unisecants intersects in a point P (not in $\mathcal{O}$ as the lines are unisecants). There is by Proposition 2.7 no 3rd unisecant which intersects in P. So there are, by definition of external point, $q(q+1)/2$ external points.

(iii) We have q^2+q+1 points so from (i) and (ii) we deduce we have $q(q-1)/2$ internal points.

□

Next we present the useful Tables 2.1 and 2.2:

	Point of $\mathcal{O}$	External point	Internal point
Unisecant	1	q	0
Bisecant	2	$(q-1)/2$	$(q-1)/2$
External line	0	$(q+1)/2$	$(q+1)/2$

Table 2.1: How many points of each type lie on each line

The proof of Table 2.1 is:

Proof. We reason as follows to show there are $(q-1)/2$ external points on a bisecant: If we have a bisecant B with 2 points of $\mathcal{O}$ then there are $(q+1)-2 = q-1$ points of $\mathcal{O}$ not on B. The $q-1$ unisecants trough those points intersect B in an external point (because on every unisecant are q external points). As every external point is on exactly 2 unisecants (by Proposition 2.7) this implies there are $(q-1)/2$ external points on B.

Showing there are $(q+1)/2$ external points on every external line goes similar. □

Dually we have Table 2.2.

	Unisecant	Bisecant	External line
Point of $\mathcal{O}$	1	q	0
External point	2	$(q-1)/2$	$(q-1)/2$
Internal point	0	$(q+1)/2$	$(q+1)/2$

Table 2.2: How many lines of each type intersects each point

In the coming chapter we will give an example of an oval in $PG(2,q)$.

Chapter 3

Introduction to ER_q

Here we will introduce the Erdős-Rényi graph, the subject of our study, together with its properties.

3.1 Definition of the Erdős-Rényi graph

In this section we will describe the graph which plays a central role in this thesis: the Erdős-Rényi graph. The proofs of the propositions in this section will rely heavily upon Proposition 1.12.

On elements $x, y \in \mathbf{F}_q^3$ we have the bilinear form in which I is the identity matrix:

$$\langle x, y \rangle := x^T I y = x^T y. \tag{3.1}$$

We define the ***Erdős-Rényi graph*** ER_q as follows. Given the vector space $\mathbf{F}_q^3$ and the bilinear form defined by (3.1) on it. Then the vertex set of ER_q is the set of all 1-dimensional subspaces of $\mathbf{F}_q^3$. Two *distinct* 1-dimensional subspaces $U, V \subseteq \mathbf{F}_q^3$ are adjacent if and only if $U \perp V$. 1-dimensional subspaces $V \subseteq \mathbf{F}_q^3$ for which holds $V \perp V$ are called ***absolute points***. If we allow edges which connect the absolute points with themselves (we called these kind of edges loops in section 1.1) to be part of the edge set too then we write ER_q^o.

Most of the time we will not talk about 1-dimensional subspaces but about the non-zero left normalized (that is: the first non-zero element in a vector equals 1) element which represents the 1-dimensional subspace. Now two *distinct* vertices x and y are adjacent if and only if

$$\langle x, y \rangle = 0.$$

Given the symmetric matrix

$$I' := \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \tag{3.2}$$

we define on any two vertices $x = (x_0, x_1, x_2)$ and $y = (y_0, y_1, y_2)$ in ER_q a new bilinear form by

$$\langle x, y\rangle := x^T I' y = x^T \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix} y = x_0y_2 + x_2y_0 - x_1y_1.$$

Now this new bilinear form defines whether vertices are adjacent and absolute. This new graph ER_q^* allows us for easy algebraic manipulations.

An alternative definition is given by $PG(2, q) = (X, L)$ and the defined polarity ϕ from (2.1). We define ER_q by the vertex set equal to X and two *distinct* $U, S \in X$ adjacent if and only if $U \subseteq \phi(S) = S^\perp$.

The ***orthogonality graph*** OG_q is the subgraph of the Erdős-Rényi graph which is induced by all its non-absolute points.

Figures 3.2 and 3.1 give graphical examples for the case $q = 2$. Section A.1 contains an example of ER_3.

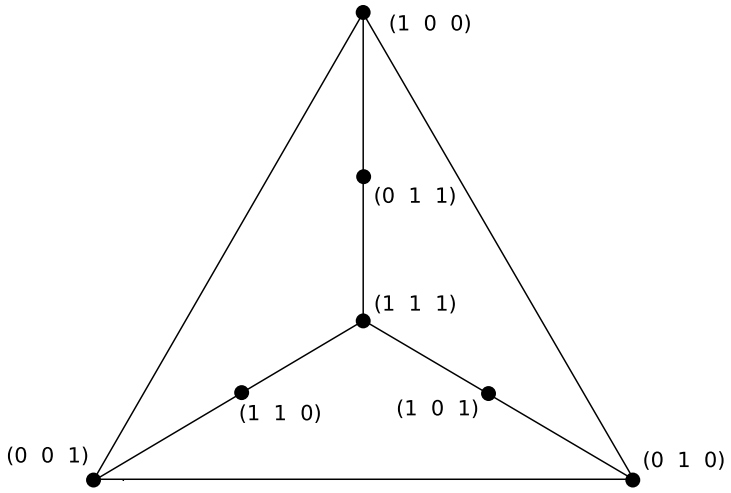

Figure 3.1: The Erdős-Rényi graph ER_2 with absolute points $(1, 1, 0), (1, 0, 1)$ and $(0, 1, 1)$

Our next proposition tells us that ER_q and ER_q^* are isomorph. As mentioned before, the bilinear form of ER_q^* allows us for easy algebraic manipulations. Therefore we will use this bilinear form most of the time in the thesis. **However we will always name the graph ER_q despite most of the times we mean ER_q^*.**

Proposition 3.1. *ER_q is isomorphic to ER_q^*.*

Proof. We need to find a matrix C such that $CI'C^T = \lambda I$ for a non-zero $\lambda \in \mathbf{F}_q$. We distinguish the following cases, the last three cases supported by the results from section 1.2:

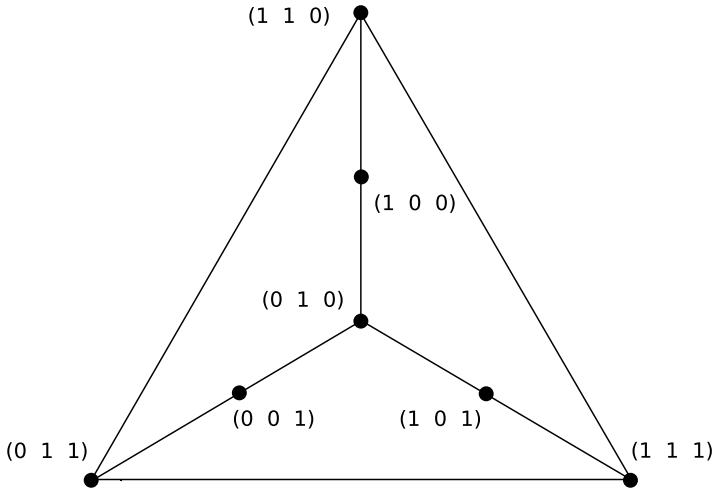

Figure 3.2: The Erdős-Rényi graph ER_2^* with absolute points $(1,0,0),(1,0,1)$ and $(0,0,1)$

($q \equiv 0 \bmod 2$)

$$C_2 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

($q \equiv 1 \bmod 4$) Pick an $i \in \mathbf{F}_q$ such that $i^2 = -1$.

$$C_1 = \begin{bmatrix} \frac{1+i}{2} & 0 & \frac{1-i}{2} \\ 0 & i & 0 \\ \frac{-1+i}{2} & 0 & -\frac{1+i}{2} \end{bmatrix}.$$

($q \equiv 3 \bmod 8$) Pick an $a \in \mathbf{F}_q$ such that $a^2 = -2$.

$$C_3 = \begin{bmatrix} \frac{a}{2} & a & \frac{a}{2} \\ -1 & -1 & -1 \\ -\frac{a}{2} & 0 & \frac{a}{2} \end{bmatrix}.$$

($q \equiv 7 \bmod 8$) Take $b, c, d, \in \mathbf{F}_q$ such that $b^2 = 2$, $c^2 + d^2 = -1$.

$$C_7 = \begin{bmatrix} \frac{1}{b} & 0 & \frac{1}{b} \\ -\frac{d}{b} & c & \frac{d}{b} \\ \frac{c}{b} & d & -\frac{c}{b} \end{bmatrix}.$$

Note $\lambda = 1$ in all four cases. □

The points $(1,0,0)$ and $(0,0,1)$ in ER_q^* are, for every q, absolute points so the set of absolute points is non-empty.

3.2 Basic properties

This section gives some basis properties of ER_q (using the bilinear form for ER_q^*) which can also be found in [18]. As our bilinear form is, by Proposition 1.11, non-degenerate we will use Proposition 1.12 in the proofs of the majority of the propositions in this section. Proposition 1.12 backs up our geometric intuition we have for ER_q.

So most of the proofs in this section are based on linear algebra over finite fields. This is a different approach compared to [18] where finite geometry is used. Another approach is to prove the propositions with elementary algebra. We will only do this for the next proposition as for all the other propositions our linear algebra proofs are much shorter. However we will mention when an elementary algebraic proof is possible.

Proposition 3.2. *ER_q has $q+1$ absolute points, q^2 non-absolute points for a total of q^2+q+1 points.*

Proof. In this proof we are, by the previous proposition, free to choose the alternative inner-product of ER_q^*. First we count the absolute points, that is the points $x = (x_0, x_1, x_2)$ for which holds

$$\langle x, x\rangle = 2x_0x_2 - x_1^2 = 0.$$

If q is a power of 2 then this equation reduces to $x_1^2 = 0$ so $x_1 = 0$. So all absolute points are of the form $(x_0, 0, x_2)$ and as they are normalized we have $q+1$ of them. If q is odd then $x_0 = 0$ implies $x_1 = 0$ and $x_2 = 1$ giving one solution. For $x_0 = 1$ we have $2x_2 = x_1^2$ where we are free to choose x_1 giving q additional solutions so we have a total of $q+1$ solutions.

We have a total of q^2+q+1 non-zero normalized elements in $\mathbf{F}_q^3$ (this is by Proposition 2.6(i)). Now we immediately deduce we have $(q^2+q+1)-(q+1) = q^2$ non-absolute points. □

The next proposition is on the degree of the vertices of ER_q.

Proposition 3.3. *The absolute points of ER_q have degree q while the non-absolute points have degree $q+1$.*

Proof. A vertex x in ER_q can be interpreted as a 1-dimensional subspace $U \subseteq \mathbf{F}_q^3$. So by Proposition 1.12 we have

$$\dim(U) + \dim(U^\perp) = 3.$$

So $U^\perp$ is 2-dimensional with (by Proposition 2.6(iii)) $q+1$ normalized points so if x is not absolute then x is adjacent to $q+1$ other vertices in ER_q. If x is absolute then $x \in U^\perp$ and therefore x is adjacent to q other vertices in ER_q. □

By making case distinction on $(1, x_1, x_2), (0, 1, x_2), (0, 0, 1) \in ER_q$ we can give an elementary algebraic proof of Proposition 3.3. From Proposition 3.3 we deduce the following result for the cardinality of the edge set of ER_q.

Proposition 3.4. *ER_q has $q(q+1)^2/2$ edges.*

Proof. By identity (1.1) and the previous propositions we have

$$\sum_{v \in V} \deg(v) = (q+1)q^2 + q(q+1) = q(q+1)^2 = 2|E|,$$

so we find ER_q has $q(q+1)^2/2$ edges. □

We do not have enough information to say anything about the cardinality of the edge set of the orthogonality subgraph. The following proposition helps us with it.

Proposition 3.5. *The absolute points from ER_q form an independent set.*

Proof. Pick two *distinct* absolute points x and y in ER_q. Because they are absolute we have

$$\langle x, x \rangle = 0 \text{ and } \langle y, y \rangle = 0.$$

Now x and y span a 2-dimensional subspace $U \subseteq \mathbf{F}_q^3$ so by Proposition 1.12 $\dim(U^\perp) = 1$. If x and y are adjacent then $\langle x, y \rangle = 0$. Now we reach a contradiction because $x, y \in U^\perp$ which is not possible because $U^\perp$ is of dimension 1 and x and y are different. So x and y are not adjacent and the absolute points form an independent set. □

By making a case distinction between even q and odd q we can give an elementary algebraic proof of the proposition above as well. So now we can deduce the orthogonality subgraph has $q(q+1)(q-1)/2$ edges.

Proposition 3.6. *We have:*

(i) Every two distinct adjacent *vertices x and y in ER_q have at most one common neighbor. We have: x is absolute or y is absolute $\iff$ x and y do* not *have a (unique) common neighbor.*

(ii) Every two distinct non-adjacent *vertices x and y in ER_q have a unique common neighbor.*

(iii) Every two distinct vertices x and y in ER_q^o have one unique common neighbor (possibly x or y itself as ER_q^o has loops).

Proof. Proposition 1.12 says that for every subspace $U \subseteq \mathbf{F}_q^3$ holds

$$\dim(U) + \dim(U^\perp) = 3.$$

Now every two distinct vertices x and y in ER_q are two distinct points in $\mathbf{F}_q^3$ which span a plane U which has dimension 2 so $U^\perp$ has dimension 1 so all elements in $U^\perp$ only differs a non-zero scalar $c \in \mathbf{F}_q$.

If x and y are adjacent and x or y is absolute then x or y is in $U^\perp$ so there is no common neighbor. If x nor y is absolute then there is a unique common neighbor. If x and y are not adjacent than x nor y is in $U^\perp$ so there is a unique common neighbor.

Because ER_q^o has loops x and y have a unique common neighbor, probably x or y it self. □

From the proposition above we immediately deduce ER_q is of diameter 2. We mention the link with the *'friendship theorem'* which can, for example, be found in [1]. It says that in any graph in which two distinct vertices have one unique common neighbor there is a vertex which is adjacent to all other vertices. ER_q^o satisfies this claim however it has loops and the friendship theorem is for graphs which does not have loops.

Proposition 3.7. *We have:*

(i) *ER_q contains a triangle which does not meet the absolute points.*

(ii) *Every absolute point is not contained in a triangle.*

(iii) *Every edge which does not have an absolute point as an endpoint is contained in a unique triangle.*

(iv) *ER_q does not contain C_4 as a subgraph.*

Proof. Using the bilinear form for ER_q (so we use the identity matrix) we have 3 non-absolute points which are adjacent to each other

$$(1,0,0) \quad (0,1,0) \quad (0,0,1),$$

and therefore form a triangle. The other items follow directly from Proposition 3.6. □

More properties of ER_q can be found in [18].

3.3 Absolute, external and internal points

This section is strongly supported by the results from section 2.3. For the absolute points $\mathcal{R}$ of ER_q we have the following proposition:

Proposition 3.8. *For the absolute points of ER_q we have:*

(i) *For even q the set $\mathcal{R}$ is a line.*

(ii) *For odd q the set $\mathcal{R}$ is an oval.*

Proof. See Proposition 3.20 and 3.21 in [18]. □

We will now define two other kind of points. But before we are allowed to do so a proposition which puts a relation between external points as defined in section 2.3 and non-absolute points adjacent to absolute points.

Proposition 3.9. *For odd q we have with respect to the oval $\mathcal{R}$ of absolute points:*

(i) *For an absolute point P we have $P^\perp$ is the unisecant P is on.*

(ii) *The set of non-absolute points of ER_q adjacent to an absolute point equals the set of external points of $PG(2,q)$.*

Proof. We have:

(i) When we have a unisecant it is one of the $q+1$ lines which an absolute point P is on. Also, as $P \subseteq P^\perp$, $P^\perp$ is one of the $q+1$ lines P is on. By Proposition 3.5 no other absolute point than P can be on $P^\perp$ so this proves our assertion.

(ii) By (i) and the fact that external point are the points on unisecant of $\mathcal{R}$ by Proposition 2.7.

□

So now we can apply our definitions of section 2.3 to ER_q. Given a non-absolute point x in ER_q. We say x is ***external*** if it is adjacent to an absolute point. We write $\mathcal{L}$ for the set of all external points of ER_q. We say x is ***internal*** if it is *not* adjacent to an absolute point. We write $\mathcal{M}$ for the set of all internal points of ER_q. The following two propositions shines some light on the structure of ER_q with respect to our new definitions.

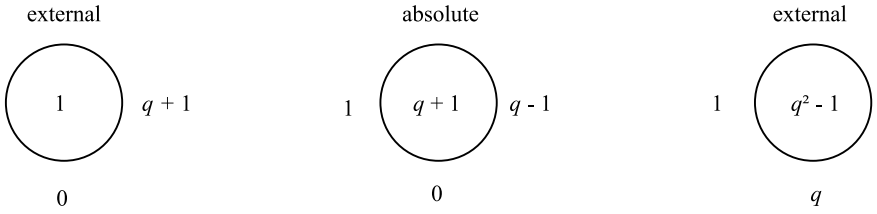

Figure 3.3: Supporting figure for Proposition 3.10

Proposition 3.10. *In case q is even we have*

(i) There is one non-absolute vertex, it is the vertex $S_0 = (0, 1, 0)$, that is adjacent with all absolute vertices.

(ii) Every non-absolute vertex not equal to S_0 is adjacent to exactly one absolute vertex.

So every non-absolute vertex is external.

Proof. As every vertex of the form $(1, 0, x)$ is absolute and $(0, 0, 1)$ is absolute as well we have $q+1$ absolute vertices this way and by Proposition 3.2 we have categorized them all.

The non-absolute vertex $(0, 1, 0)$ is adjacent to every absolute vertex and as $(0, 1, 0)$ has degree $q + 1$ and because we have $q + 1$ absolute vertices this implies $(0, 1, 0)$ is adjacent to absolute vertices only.

Now pick an arbitrary non-absolute vertex $(1, y_1, y_2)$ (so $y_1 \neq 0$). It is not adjacent to $(0, 0, 1)$, but the bilinear form with $(1, 0, x)$ gives $x + y_2 = 0$ so every non-absolute vertex of the form $(1, y_1, y_2)$ is adjacent to exactly one absolute vertex. The non-absolute point $(0, 1, y)$ (with $y \neq 0$) is not adjacent to any point $(1, 0, x)$ but it is adjacent to $(0, 0, 1)$ so every non-absolute vertex of the form $(0, 1, y)$ (with $y \neq 0$) is also adjacent to exactly one absolute vertex. □

For q is even we have that $\mathbf{F}_q$ is perfect so saying an x in ER_q is external is equivalent to saying that $\langle x, x\rangle = -\langle x, x\rangle$ is a non-zero square (as a reminder: we use the bilinear form for ER_q^*). When q is odd it is more difficult to obtain results. The proof of the following proposition relies on Proposition 3.9 and Table 2.1.

Proposition 3.11. *In case q is odd we have:*

(i) Given a vertex x in ER_q: x is external $\iff -\langle x, x\rangle$ is a non-zero square in $\mathbf{F}_q$.

(ii) There are $q(q + 1)/2$ external vertices. Every external vertex is adjacent to 2 absolute vertices, $(q - 1)/2$ other external vertices and $(q - 1)/2$ internal vertices.

(iii) There are $q(q-1)/2$ internal vertices. Every internal vertex is adjacent to $(q+1)/2$ other internal vertices and $(q + 1)/2$ external vertices.

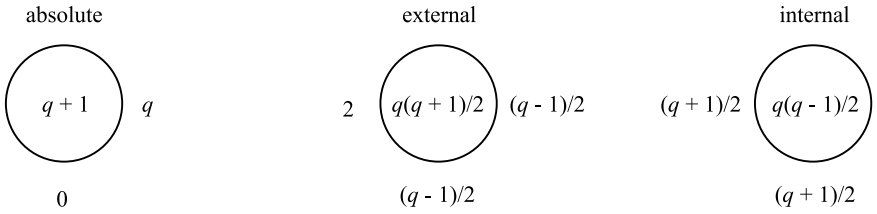

Figure 3.4: Supporting figure for Proposition 3.11

Proof. Pick a vertex of the form $(0, 1, x)$, note it is not absolute. We are going to count how many absolute vertices $(1, y_1, y_2)$ (note $2y_2 = y_1^2$) are adjacent to it. An absolute vertex is adjacent if and only if

$$x - y_1 = 0.$$

So given x there is one absolute point of the form $(1, y_1, y_2)$ which is adjacent to it. Also $(0, 1, x)$ is adjacent to the absolute point $(0, 0, 1)$ so every point of the form $(0, 1, x)$ is an external point adjacent to exactly 2 absolute vertices and we have q of them. Also

$$-\langle (0, 1, x), (0, 1, x)\rangle = 1$$

which is a square in $\mathbf{F}_q$.

Pick a non-absolute vertex of the form $(1, x_1, x_2)$, so $2x_2 \neq x_1^2$. We are going to count how many absolute vertices $(1, y_1, y_2)$ (note $2y_2 = y_1^2$) are adjacent to it. An absolute vertex is adjacent if and only if

$$y_2 + x_2 - x_1 y_1 = 0.$$

By substituting $y_1^2/2$ for y_2 we get

$$y_1^2 - 2x_1 y_1 + 2x_2 = 0.$$

We have the solutions

$$y_1 = x_1 \pm \sqrt{x_1^2 - 2x_2} = x_1 \pm \sqrt{-\langle x, x\rangle}. \tag{3.3}$$

This implies $(1, x_1, x_2)$ is external if and only if $-\langle x, x\rangle$ is a non-zero square. From (3.3) we also deduce that if $(1, x_1, x_2)$ is external then it is adjacent to exactly 2 absolute points. So any external point of ER_q is adjacent to exactly 2 absolute points.

From Proposition 2.9 and Proposition 3.9(ii) we deduce we have $q(q + 1)/2$ external points and therefore $q(q-1)/2$ internal points. Because an external point U is adjacent to 2 absolute points this implies $U^\perp$ is a bisecant with respect to $\mathcal{R}$ so U is, by Table 2.1, adjacent to $(q-1)/2$ external points and $(q-1)/2$ internal points.

For an internal point T we have $T^\perp$ contains no absolute points so it is an external line with respect to $\mathcal{R}$ so T is by Table 2.1 adjacent to $(q + 1)/2$ internal points and $(q + 1)/2$ external points. □

The proposition above can also be found in [15] which relies on results from [2]. To summarize. For odd q we can partition the vertex set of ER_q by

$$\begin{aligned}\mathcal{R} &= \{\text{vertices } x \text{ in } ER_q : \langle x,x\rangle = 0\},\\ \mathcal{L} &= \{\text{vertices } x \text{ in } ER_q : \langle x,x\rangle \neq 0, -\langle x,x\rangle \text{ is a square}\},\\ \mathcal{M} &= \{\text{vertices } x \text{ in } ER_q : \langle x,x\rangle \neq 0, -\langle x,x\rangle \text{ is a non-square}\}.\end{aligned}$$

When q is even $\mathcal{M} = \emptyset$ and for all $r \in \mathbf{F}_q$ holds $-x = x$ so this gives the partition

$$\begin{aligned}\mathcal{R} &= \{\text{vertices } x \text{ in } ER_q : \langle x,x\rangle = 0\},\\ \mathcal{L} &= \{\text{vertices } x \text{ in } ER_q : \langle x,x\rangle \text{ is a non-zero square}\}.\end{aligned}$$

3.4 An inequality

Given subfield and field $\mathbf{F}_q \subseteq \mathbf{F}_{q^2}$ we have that ER_q is a subgraph of ER_{q^2}. It is obvious we have

$$\gamma(ER_q) \leq \gamma(ER_{q^2}). \tag{3.4}$$

We wonder whether it would be possible to obtain a strict inequality. The following proposition supports us with this question.

Proposition 3.12. *We have:*

(i) There is no vertex y in ER_{q^2} which is not in ER_q and is adjacent to every vertex in ER_q.

(ii) There is no vertex y in OG_{q^2} which is not in OG_q and is adjacent to every vertex in ER_q.

Proof. From Proposition 3.7(i) we know ER_q and OG_3 have a triangle so if x is adjacent to every vertex in and ER_q and OG_q then it is adjacent to every vertex in the triangle and this would mean there are two different vertices which have 2 common neighbors which is by Proposition 3.6(iv) not true so a contradiction. □

If there was a vertex in ER_{q^2} not in ER_q which is adjacent to every vertex in ER_q then (3.4) would become a strict inequality. The proposition tells us no such vertex exist so whether (3.4) is strict is still open. In section 5.3 we will elaborate on

$$\gamma(OG_q) \leq \gamma(OG_{q^2}). \tag{3.5}$$

Chapter 4

Automorphisms of ER_q

A seperated chapter is dedicated to the automorphisms of the Erdős-Rényi graph.

4.1 Constructing some automorphisms

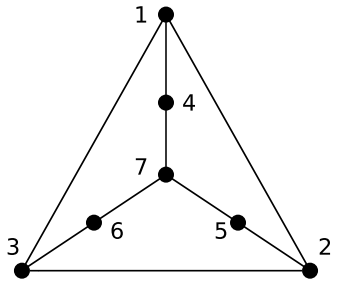

Figure 4.1: ER_2 with an alternate labeling

In this section we will present some info of the automorphism group of ER_q. The automorphism group of ER_2, when labeled according to Figure 4.1, is

$$\langle (1\ 2)(4\ 5), (2\ 3)(5\ 6) \rangle \simeq \mathrm{Sym}(3).$$

We will now construct some automorphisms of ER_q. Define the ***orthogonal group*** $O(n, \mathbf{F})$ to be the set of all $n \times n$ matrices N over a field $\mathbf{F}$ such that $N^T N = I$. It is a subgroup of the ***general linear group*** $GL(n, \mathbf{F})$ which is the set of all invertible $n \times n$ matrices over $\mathbf{F}$. The ***projective orthogonal group*** $PO(n, \mathbf{F})$ is the group $O(n, \mathbf{F})/\{cI : c \in \mathbf{F}^*\}$.

Now we can construct automorphisms of ER_q ourself. We need to find a 3×3 matrix M over $\mathbf{F}_q$ such that for a non-zero $\lambda \in \mathbf{F}_q$ holds $MI'M^T = \lambda I'$. By applying the determinant to this identity we have

$$\det(M)^2 = \det(MI'M^T) = \det(\lambda I') = \lambda^3.$$

So λ has to be square so we can distribute it over M and M^T. Therefore it is sufficient to take $\lambda = 1$ so we are interested in a 3×3 matrix M over $\mathbf{F}_q$ such that holds

$$MI'M^T = I'. \tag{4.1}$$

From the proof of Proposition 3.1 we can extract for each q a 3×3 matrix C over $\mathbf{F}_q$ such that we have the next two equivalent identities

$$\begin{aligned} CI'C^T &= I, & (4.2)\\ (C^{-1})(C^{-1})^T &= I'. & (4.3) \end{aligned}$$

Define for an $N \in O(3, \mathbf{F}_q)$ a matrix

$$M := C^{-1}NC.$$

By definition of $O(3, \mathbf{F}_q)$ and (4.2) and (4.3) it is easy to verify M satisfies (4.1) so we have constructed an element of $\mathrm{Aut}(ER_q)$. The next section tells whether we can construct all automorphisms this way.

4.2 All automorphisms

Proposition 4.1. *We have:*

(i) If q is even then $\mathrm{Aut}(ER_q) \simeq O(3, q) \rtimes \mathrm{Aut}(\mathbf{F}_q)$.

(ii) If q is odd then $\mathrm{Aut}(ER_q) \simeq PO(3, q) \rtimes \mathrm{Aut}(\mathbf{F}_q)$.

Proof. This is Theorem 2 in [15]. The proofs are spread out over section 3 and 6 in [15]. □

When q is even then $\mathcal{M} = \emptyset$ and the vertex S_0 in ER_q is the external vertices adjacent to all the absolute vertices (so is isolated from the other external vertices), see also Proposition 3.10.

Proposition 4.2. *We have:*

(i) When q is even then for every two vertices $x, y \in \mathcal{L}\backslash\{S_0\}$ there exists an $f \in \mathrm{Aut}(ER_q)$ such that $f(x) = y$.

(ii) When q is odd then for every external vertex x and y there is an $f \in \mathrm{Aut}(ER_q)$ such that $f(x) = y$. This holds for internal vertices too.

Proof. For odd q it is Corollary 4 in [15]. For even q it is section 6 from [15]. The proof of Corollary 4 in [15] is spread out over the whole article. □

Corollary 4 in [15] is also used to show that, for odd q, the graphs $G\mathcal{L}$ and $G\mathcal{M}$ induced by $\mathcal{L}$ and $\mathcal{M}$ are transitive (that is for every $x, y \in \mathcal{L}$ there is an $f \in \mathrm{Aut}(G\mathcal{L})$ such that $f(x) = y$, the same for $\mathcal{M}$).

Proposition 4.3. *The automorphism group $\mathrm{Aut}(ER_q)$ of ER_q acts on the vertex set of ER_q in the following way:*

(i) Let q be even. Then $\mathrm{Aut}(ER_q)$ partitions the vertex set of ER_q in three orbits $\mathcal{R}$, $\mathcal{L}\backslash\{S_0\}$ and $\{S_0\}$.

(ii) Let q be odd. Then $\mathrm{Aut}(ER_q)$ partitions the vertex set of ER_q in three orbits $\mathcal{R}$, $\mathcal{L}$ and $\mathcal{M}$.

Proof. We have:

(i) It is obvious that S_0 is an orbit on its own. By (1.3) and Proposition 3.3 we deduce that for every external vertex $x \in \mathcal{L}\backslash\{S_0\}$ and every $f \in \mathrm{Aut}(ER_q)$ holds that $f(x) \in \mathcal{L}\backslash\{S_0\}$. So by Proposition 4.2(ii) $\mathcal{L}\backslash\{S_0\}$ is an orbit.

For every absolute vertex x in ER_q we have $f(x)$ is absolute. This is because the absolute vertices have degree q there the non-absolute vertices have degree $q+1$. So by (1.3) we have $f(x)$ is absolute;

Next pick two arbitrary *distinct* absolute vertices r and r'. Pick two external *distinct* vertices $x, x' \neq S_0$ such that x is a neighbor of r and x' is a neighbor of r'. By Proposition 3.10(ii) every external vertex not equal to S_0 is adjacent to exactly one absolute vertex so x is not adjacent to r' nor is x' adjacent to r. By Proposition 4.2(i) there is an $f \in \mathrm{Aut}(ER_q)$ such that $f(x) = x'$ so by definition of automorphism $f(r) = r'$ so the absolute vertices $\mathcal{R}$ form a single orbit.

(ii) Pick an arbitrary $f \in \mathrm{Aut}(ER_q)$. Then

- for every absolute vertex x in ER_q we have $f(x)$ is absolute. This is the same argument as we used in (i);
- for every external vertex y in ER_q we have $f(y)$ is external. This is because y is, by definition of external, adjacent to an absolute vertex u. By definition of automorphism $f(y)$ and $f(u)$ are adjacent. The previous item tells us $f(u)$ is absolute so $f(y)$ is external;
- for every internal vertex z in ER_q we have $f(z)$ is internal. This is because f is a bijection and the previous two items.

So by Proposition 4.2(ii) we have found the orbits $\mathcal{L}$ and $\mathcal{M}$.

Next pick two arbitrary distinct absolute vertices r and r' in ER_q. If r and r' do not have a common neighbor then we pick arbitrary external neighbor x of r and arbitrary external neighbor x' of r' (so $x \neq x'$). By Proposition 4.2(ii) x can be mapped to y so by the definition of automorphism r is mapped to r'. If r and r' do have a common neighbor z (by Proposition 3.7(iv) it is unique) then pick arbitrary external neighbor x of r with $x \neq z$ and arbitrary external neighbor x' of r' with $x' \neq z$. As x can be mapped to x' and by definition of automorphism r can be mapped to r'. So the absolute vertices $\mathcal{R}$ are a single orbit under the automorphism group of ER_q.

□

We have enough results to construct automorphisms of ER_q ourself. However MAGMA has a build-in function called `AutomorphismGroup` which computes the automorphism group of a graph. The code is based on ideas of McKay which can be found in [13]. Info including an extensive manual is on the website

`http://cs.anu.edu.au/~bdm/nauty/`

Independent of [15] the partitioning of the vertex set of ER_q into three orbits by $\mathrm{Aut}(ER_q)$ was shown in [18] by cleverly constructing some automorphisms.

Chapter 5

Eigenvalues and bounds

This chapter puts a relation between eigenvalues and bounds on the chromatic number and the size of the largest independent set of a graph.

5.1 Eigenvalues

In section 1.1 we introduced the adjacency matrix of a graph. This brings us to the ***eigenvalues*** of a graph G which are the eigenvalues of the adjacency matrix of a graph. The eigenvalues of (1.2), the adjacency matrix of the graph we gave as an example in section 1.1, are

$$\sqrt{3}+1, \quad 1, \quad 0, \quad -\sqrt{3}+1, \quad -1, \quad -2.$$

Because the adjacency matrix has size 6 all multiplicities are 1. As a real symmetric $n \times n$ matrix A has (by Proposition 1.7) real eigenvalues $\lambda_i(A)$ we can write them in descending order

$$\lambda_1(A) \quad \geq \quad \lambda_2(A) \quad \geq \quad \ldots \quad \geq \quad \lambda_n(A). \tag{5.1}$$

When it is obvious which matrix we are talking about we will just write λ_i. By $\lambda_i(G)$ we mean of course the ith eigenvalue of the adjacency matrix of G. A short relation is

$$-\lambda_i(A) \quad = \quad \lambda_{n+1-i}(-A). \tag{5.2}$$

As the eigenvalues are labeled according to (5.1) and $u_1, \ldots, u_n$ is an orthonormal set of eigenvectors for A such that for every i holds $Au_i = \lambda_i u_i$ (see Theorem 8.4.5 in [4]) we can easily prove the following result by **Rayleigh**:

$$\begin{array}{lll} \dfrac{u^T A u}{u^T u} & \geq & \lambda_i, \quad \text{for non-zero } u \in \langle u_1, \ldots, u_i \rangle; \\ \dfrac{u^T A u}{u^T u} & \leq & \lambda_i, \quad \text{for non-zero } u \in \langle u_1, \ldots, u_{i-1} \rangle^{\perp} = \langle u_i, \ldots, u_n \rangle. \end{array}$$

We introduce a new definition. Consider two sequences of real numbers:

$$\begin{array}{ccccccc} \lambda_1 & \geq & \lambda_2 & \geq & \ldots & \geq & \lambda_n, \\ \mu_1 & \geq & \mu_2 & \geq & \ldots & \geq & \mu_m, \end{array}$$

with $n > m$. We say the second sequence ***interlace*** the first sequence if

$$\lambda_i \quad \geq \quad \mu_i \quad \geq \quad \lambda_{i+n-m}, \quad \text{for } i = 1, \ldots, m.$$

This gives rise to the following proposition which can be found in [7]:

Proposition 5.1. *Let S be a real $n \times m$ matrix with $n > m$ such that $S^T S = I$ and let A be a real symmetric $n \times n$ matrix. Let $B = S^T AS$. Then the eigenvalues of B interlace the eigenvalues of A.*

Proof. A has orthonormal eigenvectors $u_1, \ldots, u_n$. B has orthonormal eigenvectors $v_1, \ldots, v_m$. For arbitrary integer i with $1 \leq i \leq m$ we pick a non-zero vector

$$s_i \in \langle S^T u_1, \ldots, S^T u_{i-1} \rangle^\perp \cap \langle v_1, \ldots, v_i \rangle.$$

The intersection is non-zero because the dimension is at least 1. This is because $\langle S^T u_1, \ldots, S^T u_{i-1} \rangle$ has dimension *at most* $i-1$ so $\langle S^T u_1, \ldots, S^T u_{i-1} \rangle^\perp$ has (by Proposition 1.12) dimension *at least* $m + 1 - i$. As $\langle v_1, \ldots, v_i \rangle$ has dimension i we deduce by Proposition 1.10(ii) that the intersection has dimension at least 1 so there is a non-zero vector in the intersection.

So $Ss_i \in \langle u_1, \ldots, u_{n-1} \rangle^\perp$ (s_i is orthogonal to every element in $\langle S^T u_1, \ldots, S^T u_{i-1} \rangle$ therefore Ss_i is orthogonal to every element in $\langle u_1, \ldots, u_{n-1} \rangle$) and $s_i \in \langle v_1, \ldots, v_i \rangle$ so by Rayleigh we have

$$\lambda_i(A) \geq \frac{(Ss_i)^T A(Ss_i)}{(Ss_i)^T (Ss_i)} = \frac{s_i^T (S^T AS) s_i}{s_i^T s_i} = \frac{s_i^T B s_i}{s_i^T s_i} \geq \lambda_i(B).$$

Applying the above equation to $-A$ and $-B$ and using identity (5.2) we get

$$-\lambda_{n+1-i}(A) \quad = \quad \lambda_i(-A) \quad \geq \quad \mu_i(-B) \quad = \quad -\lambda_{m+1-i}(B).$$

From this we deduce $\lambda_{n+1-i}(A) \leq \lambda_{m+1-i}(B)$. Substituting $i = m + 1 - i'$ we get $\lambda_{n-m+i'}(A) \leq \lambda_{i'}(B)$ and therefore by definition the eigenvalues of B interlace the eigenvalues of A. □

From this we can deduce the following proposition.

Proposition 5.2. *If B is a principal submatrix of A then the eigenvalues of B interlace the eigenvalues of A.*

Proof. Use $S = [I \;\; O]^T$ in Proposition 5.1. □

We can see this proposition in action for ER_2 and its orthogonality subgraph OG_2. For the small adjacency matrix of OG_2 we can give exact results so the eigenvalues of OG_2 are

eigenvalue	multiplicity
-1	2
0	1
2	1

The eigenvalues of ER_2 are

eigenvalue	multiplicity
-1.86620	1
-1.61803	2
0.61803	2
1.21076	1
2.65544	1

An unpublished result by Godsil, which uses Rayleigh, is the following proposition.

Proposition 5.3. *Let G be a graph of average degree $\overline{d}$. Then*

$$\overline{d} \leq \lambda_1 \leq \Delta(G),$$

with (if G is connected) $\lambda_1 = \Delta(G)$ if and only if G is regular.

Proof. With A the adjacency matrix (of size n) and orthonormal eigenvectors $u_1, \ldots, u_n$we have $\mathbf{R}^n = \langle u_1, \ldots, u_n \rangle$ (so $1 \in \langle u_1, \ldots, u_n \rangle$) so with Rayleigh we find

$$\overline{d} = \frac{1^T A 1}{1^T 1} \leq \lambda_1.$$

For the second inequality let z be an eigenvector for λ_1, that is $Az = \lambda_1 z$. Then for every i holds

$$\lambda_1 z_i = \sum_{j \sim i} z_j. \tag{5.3}$$

If we choose i such that z_i is maximal and d_i is the degree of vertex i then $\lambda_1 z_i \leq d_i z_i$ and therefore $\lambda_1 \leq d_i \leq \Delta(G)$. Now assume G is connected. ($\Leftarrow$) because G is regular we have $\overline{d} = \Delta(G)$ so $\lambda_1 = \Delta(G)$. For ($\Rightarrow$) we have $\lambda_1 = \Delta(G)$ so by (5.3) we have

$$\Delta(G) z_i = \sum_{j \sim i} z_j. \tag{5.4}$$

If we choose z_i to be maximal in (5.4) then we immediately deduce G is regular. □

Another tool to reason on the eigenvalues is the following theorem.

Theorem 5.4. *Let A and B be real symmetric matrices of size m. Then*

$$\lambda_{i-j}(A) + \lambda_{1+j}(B) \geq \lambda_i(A+B) \geq \lambda_{i+j}(A) + \lambda_{m-j}(B).$$

for $i = 1, \ldots, m$ and $0 \leq j \leq \min(i-1, m-i)$.

Proof. Define

$$\begin{aligned} C &= \begin{bmatrix} A - \lambda_{i-j}(A) I & 0 \\ 0 & B - \lambda_{1+j}(B) I \end{bmatrix}, \\ S &= \frac{1}{2}\sqrt{2} \begin{bmatrix} I_m \\ I_m \end{bmatrix}. \end{aligned}$$

Then we have

$$\begin{aligned} \lambda_{i-j}(A - \lambda_{i-j}(A)I) &= 0, \\ \lambda_{1+j}(B - \lambda_{1+j}(B)I) &= 0. \end{aligned}$$

From this we deduce $\lambda_i(C) = \lambda_{i+1}(C) = 0$. A quick verification tells us

$$S^T C S = \frac{A + B - (\lambda_{i-j}(A) + \lambda_{i+j}(B))I}{2}.$$

With Proposition 5.1 we now have

$$\lambda_i(A + B) - \lambda_{i-j}(A) - \lambda_{1+j}(B) = 2\lambda_i(S^T C S) \leq 2\lambda_i(C) = 0.$$

If we replace A by $-A$ and B by $-B$ we obtain the second inequality. □

The proof of the previous proposition can be found in [7] and the theorem is originally from Weyl.

5.2 Applications to ER_q

Our first result is on the eigenvalues of ER_q^o and its proof can be found in [1] as well as in [18].

Proposition 5.5. *The eigenvalues of the adjacency matrix A of ER_q^o are $q+1$ (multiplicity 1) and $\pm\sqrt{q}$ (both cases multiplicity of $q(q+1)/2$).*

Proof. We first compute A^2. Because ER_q^o is $(q+1)$-regular and every two distinct vertices have one unique common neighbor (see Proposition 3.6(iii)) we have:

$$A^2 = \begin{bmatrix} q+1 & 1 & \dots & 1 \\ 1 & q+1 & \dots & 1 \\ \dots & \dots & & \dots \\ 1 & 1 & \dots & q+1 \end{bmatrix} = qI + J.$$

By adding all the rows of A^2 to the first row (note that A is of size q^2+q+1 by q^2+q+1) we get the matrix:

$$\begin{bmatrix} (q+1)^2 & (q+1)^2 & \dots & (q+1)^2 \\ 1 & q+1 & \dots & 1 \\ \dots & \dots & & \dots \\ 1 & 1 & \dots & q+1 \end{bmatrix}.$$

Subtracting the first row divided by $(q+1)^2$ from all other rows we have the upper triangular matrix:

$$\begin{bmatrix} (q+1)^2 & (q+1)^2 & \dots & (q+1)^2 \\ 0 & q & \dots & 0 \\ \dots & \dots & & \dots \\ 0 & 0 & \dots & q \end{bmatrix}.$$

This matrix has characteristic polynomial

$$(\lambda - (q+1)^2)(\lambda - q)^{q^2+q}.$$

Therefore A^2 has eigenvalues $(q+1)^2$ (multiplicity 1) and q (multiplicity q^2+q). As A is a symmetric matrix it can be written as $A = PDP^T$ for a diagonal matrix D with all the eigenvalues of A on the diagonal and a square matrix P such that $P^TP = I$. This implies $A^2 = PD^2P^T$. So A^2 and D^2 are similar and therefore (Theorem 4 in §5.2 of [12]) have the same eigenvalues. So D has q^2+q eigenvalues $\pm\sqrt{q}$ so A has q^2+q eigenvalues $\pm\sqrt{q}$. The other eigenvalue of A is $q+1$ (easy to check as the vector full of 1s is an eigenvector). So we have found all the eigenvalues of A. Because $\mathrm{tr}A = q+1$ the eigenvalues $\sqrt{q}$ and $-\sqrt{q}$ both have multiplicity $(q^2+q)/2$ by (1.6). □

We now have enough to make a claim about the eigenvalues of the orthogonality graph OG_q.

Proposition 5.6. *For every $q > 2$ we have for the eigenvalues of OG_q*

$$\lambda_1 = q, \quad \lambda_2 = \sqrt{q}, \quad \lambda_{q^2} = -\sqrt{q}.$$

Proof. We make case distinction.
If q is odd:
Partition the adjacency matrix of OG_q by a matrix A which is the adjacency matrix for all the internal vertices, B the matrix for adjacency relation between external and internal vertices and C is the matrix adjacency matrix for the external vertices. Then by Proposition 3.11 we have:

$$\left[\begin{array}{c|c} & \\ A & B \\ & \\ \hline & \\ B^T & C \\ & \end{array}\right] \left[\begin{array}{c} a \\ \dots \\ a \\ \hline b \\ \dots \\ b \end{array}\right] = \left[\begin{array}{c} (a+b)(q+1)/2 \\ \dots \\ (a+b)(q+1)/2 \\ \hline (a+b)(q-1)/2 \\ \dots \\ (a+b)(q-1)/2 \end{array}\right] = s \left[\begin{array}{c} a \\ \dots \\ a \\ \hline b \\ \dots \\ b \end{array}\right].$$

We derive the equalities

$$(a+b)(q+1) = 2sa, \tag{5.5}$$
$$(a+b)(q-1) = 2sb. \tag{5.6}$$

By adding them together we find $s = q$ so q is an eigenvalue of OG_q.

Because the adjacency matrix of OG_q is a principal submatrix of the adjacency matrix of ER_q^o we can use Proposition 5.2 to write down an interlacing relation.

$$\lambda_i \geq \mu_i \geq \lambda_{i+q+1}, \qquad \text{for } i = 1, \ldots, q^2.$$

By Proposition 5.5 we have $\lambda_2 = \sqrt{q}$ (multiplicity $q(q+1)/2$) so for $i = q(q+1)/2 - q$ we have $\lambda_{q(q+1)/2+1} = \sqrt{q}$ so

$$\mu_2 \quad = \quad \ldots \quad = \quad \mu_{q(q+1)/2-q} \quad = \quad \sqrt{q}.$$

We already stated q is an eigenvalue so now we can say

$$\mu_1 \quad = \quad q.$$

Analogue to finding $\sqrt{q}$ we can argue $-\sqrt{q}$ is an eigenvalue of OG_q:

$$\mu_{q(q+1)/2+2} \quad = \quad \ldots \quad = \quad \mu_{q^2} \quad = \quad -\sqrt{q}.$$

If q is even:
Analog as in the case of q is odd. □

From the proof above we can extract that the multiplicity of λ_2 and λ_{q^2} is at least $q(q-1)/2 - 1$. Also in the case q is odd we find that 0 is an eigenvalue (use $-a = b$ in (5.5) and (5.6)).

For ER_q we can give some useful bounds on some of its eigenvalues.

Proposition 5.7. *For the eigenvalues of the Erdős-Rényi graph we have:*

$$\begin{array}{rcccl} q & \leq & \lambda_1 & < & q+1; \\ \sqrt{q}-1 & \leq & \lambda_2 & \leq & \sqrt{q}; \\ -\sqrt{q}-1 & \leq & \lambda_n & \leq & -\sqrt{q}. \end{array}$$

Here $n = q^2 + q + 1$.

Proof. If A is the adjacency matrix of ER_q and A^o is the adjacency matrix of ER_q^o then we have a matrix H with 0s and 1s on the diagonal and 0 outside the diagonal such that $A + H = A^o$. As the eigenvalues of H are 1 (multiplicity $q+1$) and 0 (multiplicity q^2) we can use Theorem 5.4 to obtain the relations for the eigenvalues of ER_q. We demonstrate the case for λ_1. Choose $i = 1$. This implies $j = 0$. So we have

$$\lambda_1(A) + \lambda_1(H) \quad \geq \quad \lambda_1(A^o) \quad \geq \quad \lambda_1(A) + \lambda_n(H).$$

There $\lambda_1(H) = 1$, $\lambda_n(H) = 0$ and $\lambda_1(A^o) = q + 1$ we have

$$\lambda_1(A) + 1 \quad \geq \quad q + 1 \quad \geq \quad \lambda_1(A).$$

From this we easily deduce

$$q \quad \leq \quad \lambda_1(A) \quad \leq \quad q + 1.$$

Because ER_q is not regular by Proposition 5.3 we deduce $\lambda_1(A) \neq q + 1$. So we have $\lambda_1(A) < q + 1$. □

We would like to stress that Godsil (together with Royle) has, in unpublished conference notes, computed the characteristic polynomial of the adjacency matrices of ER_q and OG_q. They are respectively:

$$(x^3 - qx^2 - 2qx + q^2 + q)(x^2 + x + 1 - q)^q(x^2 - q)^{(q^2-q-2)/2},$$
$$(x - q)x(x + 1)^q(x^2 - q)^{(q^2-q-2)/2}.$$

5.3 Bounds

This section gives some bounds for the size of the maximum independent set and the chromatic number of ER_q. Some well known bounds to start with:

- $\alpha(G)\gamma(G) \geq n$ where n is the number of vertices of G.
- $\gamma(G) \leq \Delta(G) + 1$. This is easy to see. If we have $\Delta(G) + 1$ colors then for any vertex of G we can pick a color as the degree of the picked vertex equals $\Delta(G)$ or less.
- $\gamma(G) \leq \Delta(G)$ if G is not a complete graph or an odd cycle. This is a well known theorem by **Brooks**. A proof can be found in [17].
- $\omega(G) \leq \gamma(G)$.

Because of the last item we wonder whether lower bounds for $\omega(G)$ would help us finding a lower bound for $\gamma(G)$.

Proposition 5.8. *$\omega(ER_q) = 3$, that is, the largest clique in ER_q is a triangle.*

Proof. From Proposition 3.7(i) we have that ER_q contains a triangle so $\omega(ER_q) \geq 3$. proposition 3.7(iv) also says C_4 is not a subgraph so the largest clique can not exceed size 3 so $\omega(ER_q) \leq 3$ hence $\omega(ER_q) = 3$. □

So bounding $\gamma(ER_q)$ below by bounding $\omega(ER_q)$ would not give us any useful results. Some more advanced bounds which use the eigenvalues of a graph, labeled as in (5.1), for bounds on the chromatic number:

- **Wilf** bound: $\gamma(G) \leq 1 + \lambda_1$.

  Proof. When G' is an induced subgraph of G then (by Proposition 5.2) $\lambda_1(G') \leq \lambda_1(G)$. With this we can easily prove the induction hypothesis.

  If G has a vertex set of cardinality n then there exists a vertex v in G such that $\deg(v) \leq \lambda_1(G)$ (by Proposition 5.3). As $G - v$ has a vertex set of cardinality $n - 1$ it is colorable by $\lambda_1(G - v) + 1$ colors (induction hypothesis). So $G - v$ is colorable with $\lambda_1(G) + 1$ colors. Because $\deg(v) \leq \lambda_1(G)$ we have G is colorable with $\lambda_1(G) + 1$ colors (just join the vertex v and its initial edges with $G - v$). □

- **Hoffman** bound: $\gamma(G) \geq 1 - \lambda_1/\lambda_n$. A generalization of this bound can be found in [7].
- **Haemers** bound: if $\gamma(G)$ is bounded above by the multiplicity of λ_n then $\gamma(G) \geq 1 - \lambda_n/\lambda_2$. See also [7].

For bounds on the size of a maximum independent set we can use eigenvalues as well.

- If G is a d-regular graph on n vertices then a bound for $\alpha(G)$ can be found by a result of **Hoffman** and **Delsarte**

$$\alpha(G) \quad \leq \quad \frac{n\lambda_n}{\lambda_n - d}.$$

  A proof can be found in [5].

- **Godsil** and **Newman** [5] recently found the upper bound for a graph which can be made d-regular by adding a number of l loops to certain vertices.

$$\alpha(G) \quad \leq \quad n\frac{-\lambda_n + \sqrt{\lambda_n^2 + 4\frac{d-\lambda_n}{n}l}}{2(d-\lambda_n)}.$$

  Note the eigenvalue λ_n is the eigenvalue of the adjacency matrix of the graph we get by adding loops there the independence number is for the graph without loops.

- For a d-regular graph G on n vertices **Sarnak** says

$$\alpha(G) \quad \leq \quad \frac{n\lambda_2}{d}.$$

  A proof can be found in [5].

So by Proposition 5.7 Wilf gives us for ER_q an upper bound, which can also be deduced from Brooks and Proposition 3.3,

$$\gamma(ER_q) \quad \leq \quad q+1.$$

Similarly we have for the orthogonality subgraph OG_q:

$$\begin{array}{lcll} \gamma(OG_q) & \leq & q, & \text{if } q \text{ is even and } q \neq 2; \\ \gamma(OG_q) & \leq & q+1, & \text{if } q \text{ is odd.} \end{array} \tag{5.7}$$

For q is even we use that every external point is adjacent to exactly one absolute point (by Proposition 3.10) which gives $\Delta(OG_q) = q$, see Proposition 3.11 for q is odd. Hoffman and Proposition 5.7 tells us

$$1 + \frac{q}{\sqrt{q}+1} \quad \leq \quad \gamma(ER_q).$$

Similarly Hoffman and Proposition 5.6 gives us a slightly better bound

$$1 + \sqrt{q} \quad \leq \quad \gamma(OG_q) \quad \leq \quad \gamma(ER_q). \tag{5.8}$$

Summarized we have:

$$O(\sqrt{q}) \quad \leq \quad \gamma(ER_q) \quad \leq \quad O(q).$$

For ER_q the bound by Godsil and Newman turns out to be $\alpha(ER_q) \leq O(q\sqrt{q})$ (using Proposition 5.5). So combining it with the bound $\alpha(ER_q)\gamma(ER_q) \geq q^2 + q + 1$ we find $\gamma(ER_q) \geq O(\sqrt{q})$. A result we just obtained by Hoffman. We also have been able to partly solve (3.5). Because by (5.7) and (5.8) we have for even q

$$\gamma(OG_q) \quad < \quad \gamma(OG_{q^2}).$$

Chapter 6

Constructions of independent sets

This chapter is dedicated to constructions of independent sets in ER_q for all q.

6.1 Overview

As a coloring is a partition of the vertex set in disjoint independent sets we are particulary interested in independent sets in ER_q of suitable large size. The following theorem by [14] gives a lower bound for $\alpha(ER_q)$ of order $O(q\sqrt{q})$.

Theorem 6.1. *Given a prime power $q = p^n$. Then*

$$\begin{array}{lcll} \alpha(ER_q) & \geq & q\sqrt{q} - q + \sqrt{q} & \text{for } p = 2, \text{ } n \text{ is even;} \\ \alpha(ER_q) & \geq & \frac{q\sqrt{q}}{2\sqrt{2}} & \text{for } p = 2, \text{ } n \text{ is odd;} \\ \alpha(ER_q) & \geq & \frac{q\sqrt{q}+q+2}{2} & \text{for } p > 2, \text{ } n \text{ is even;} \\ \alpha(ER_q) & \geq & \frac{120q\sqrt{q}}{73\sqrt{73}} & \text{for } p > 2, \text{ } n \text{ is odd.} \end{array}$$

In all cases $\alpha(ER_q) \geq \frac{120q\sqrt{q}}{73\sqrt{73}} > 0.19239q\sqrt{q}$.

We also have the special case

Theorem 6.2. *If n is even for $q = 2^n$ then $\alpha(OG_q) = q\sqrt{q} - q + \sqrt{q}$.*

Which is a result from [14]. The sections which will follow prove Theorem 6.1 by giving explicit constructions of our desired independent sets which we obtained from [14]. This enables us to put them in MAGMA, a computer programming language dedicated for algebraic en discrete structures (see Appendix D.1). Together with the results from the previous section we now have

$$\alpha(ER_q) = O(q\sqrt{q}).$$

From the constructions we derive that for all $q \geq 3$ the independent sets do not have absolute points. The exception is when $p > 2$ and n is even. In that case the independent sets contain all the absolute points.

6.2 $p = 2$ and n is even

Here we give a proof for the case $p = 2$ and n is even (for $q = p^n$). We want to prove

$$\alpha(ER_q) \geq q\sqrt{q} - q + \sqrt{q}.$$

We start with an irreducible polynomial $x^2 + x + s$ over $\mathbf{F}_q$. First we elaborate on the existence of such an $s \in \mathbf{F}_q$. Introduce a function

$$\begin{array}{rcl} f : \mathbf{F}_q & \longrightarrow & \mathbf{F}_q \\ x & \longmapsto & x^2 + x \end{array}$$

We claim f is a homomorphism as for arbitrary $x, y \in \mathbf{F}_q$ holds

$$(x + y)^2 + (x + y) = x^2 + x + y^2 + y.$$

The kernel of f is the set $\{0, 1\}$, this is easy to see as $x^2 + x = x(x + 1)$ and $\mathbf{F}_q$ is a field. From undergraduate algebra we know

$$\mathbf{F}_q/\ker(f) = \mathbf{F}_q/\{0, 1\} \simeq f(\mathbf{F}_q).$$

This means $f(\mathbf{F}_q)$ is of index 2 in $\mathbf{F}_q$ and hence this proves the existence of an $s \in \mathbf{F}_q$ which is not in $f(\mathbf{F}_q)$ so for this s holds $x^2 + x + s$ is irreducible. From this we can easily state the following lemma:

Lemma 6.3. *Given an irreducible polynomial $x^2 + x + s$ over $\mathbf{F}_q$. Then the image under $x^2 + x + s$ is disjoint from the subfield $\mathbf{F}_{\sqrt{q}}$.*

Proof. The only extra we need is that $\mathbf{F}_{\sqrt{q}}$ is contained in the image of $x^2 + x$ (as defined by f). Pick arbitrary $c \in \mathbf{F}_{\sqrt{q}}$. Then $x^2 + x = c$ leads to $x^2 + x + c = 0$. As $c \in \mathbf{F}_{\sqrt{q}}$ and our polynomial is quadratic this means it has a solution in $\mathbf{F}_q$ and therefore the image of $x^2 + x$ contains $\mathbf{F}_{\sqrt{q}}$. □

Now let I be the set of points $(x_0, x_1, x_2) \in ER_q$ for which there exists a $\lambda \in \mathbf{F}_{\sqrt{q}}$ such that

$$x_2^2 + x_2x_0 + sx_0^2 + \lambda x_1^2 = 0. \tag{6.1}$$

Next we show $|I| = q\sqrt{q} - q + \sqrt{q}$. To do this we make a case distinction:

($\lambda = 0$) As the elements in I are normalized this means $x_0 = 0$ or $x_0 = 1$. $x_0 = 1$ would mean we would have a solution of $x_2^2 + x_2 + s = 0$ which is a contradiction. So we have $x_0 = 0$. So what is left is $x_2^2 = 0$, however this implies $x_1 = 1$ (because our elements are normalized) which gives us one point which satisfies (6.1).

($\lambda \neq 0$) We now make a second case distinction:

($x_0 = 0$) This immediately implies $x_1 = 1$ ($x_1 = 0$ would imply $x_2 = 0$, a contradiction as our elements are normalized) which leaves us with $x_2^2 + \lambda = 0$ which is (as our field has characteristic 2) equivalent to $x_2^2 = \lambda$ which gives us $\sqrt{q} - 1$ solutions $x_2 \in \mathbf{F}_q$ (for every non-zero $\lambda \in \mathbf{F}_{\sqrt{q}}$ a solution).

$(x_0 = 1)$ This implies $x_1^2 = \lambda^{-1}(x_2^2 + x_2 + s)$ and any choice of $\lambda \neq 0$ and x_2 uniquely determines x_1, yielding $q(\sqrt{q} - 1)$ solutions.

So we conclude we have $1 + \sqrt{q} - 1 + q(\sqrt{q} - 1) = q\sqrt{q} - q + \sqrt{q}$ solutions so $|I| = q\sqrt{q} - q + \sqrt{q}$.

We also claim I is an independent set. Assume two points (x_0, x_1, x_2) and (y_0, y_1, y_2) are adjacent. Then for some $\lambda, \tilde{\lambda} \in \mathbf{F}_{\sqrt{q}}$ the equations below are satisfied

$$\begin{aligned} x_2^2 + x_2x_0 + sx_0^2 + \lambda x_1^2 &= 0, \\ y_2^2 + y_2y_0 + sy_0^2 + \tilde{\lambda} y_1^2 &= 0, \\ x_2y_0 + x_0y_2 &= x_1y_1. \end{aligned}$$

Case distinction:

$(x_1 = 0)$ Then we have $x_2^2 + x_2x_0 + sx_0^2 = 0$. This forces $x_0 = 1$ which leads to a contradiction as our polynomial is irreducible.

$(\lambda = 0)$ Then we have $x_2^2 + x_2x_0 + sx_0^2 = 0$. This forces $(x_0, x_1, x_2) = (0, 1, 0)$. This means $y_1 = 0$. From this we obtain $y_2^2 + y_2y_0 + sy_0^2 = 0$ which is, as in the case of $x_1 = 0$, not possible.

$(y_1 = 0)$ Analogue as in the case of $x_1 = 0$.

$(\tilde{\lambda} = 0)$ Analogue as in the case of $\lambda = 0$.

$(\lambda, \tilde{\lambda}, x_1, y_1 \neq 0)$ We then rewrite the equations

$$\begin{aligned} \lambda^{-1}(x_2^2 + x_2x_0 + sx_0^2) &= x_1^2, \\ \tilde{\lambda}^{-1}(y_2^2 + y_2y_0 + sy_0^2) &= y_1^2, \\ x_2y_0 + x_0y_2 &= x_1y_1. \end{aligned}$$

Squaring the third equation and substituting, we get:

$$(x_2y_0 + x_0y_2)^2 = \frac{1}{\lambda\tilde{\lambda}}(x_2^2 + x_2x_0 + sx_0^2)(y_2^2 + y_2y_0 + sy_0^2).$$

The quantity $x_2y_0 + x_0y_2 \neq 0$ since $x_1, y_1 \neq 0$, therefore we obtain:

$$\lambda\tilde{\lambda} = \frac{(x_2^2 + x_2x_0 + sx_0^2)(y_2^2 + y_2y_0 + sy_0^2)}{(x_2y_0 + x_0y_2)^2}.$$

If $x_0 = 0$ then $y_0 = 1$ (by $x_2y_0 + x_0y_2 \neq 0$). This gives us $y_2^2 + y_2 + s = \lambda\tilde{\lambda}$ which is impossible by the lemma as $\lambda\tilde{\lambda} \in \mathbf{F}_{\sqrt{q}}$. Similarly $y_0 = 0$ also lead to a contradiction. For $x_0 = y_0 = 1$ we have

$$\lambda\tilde{\lambda} = \frac{(x_2^2 + x_2 + s)(y_2^2 + y_2 + s)}{(x_2 + y_2)^2}. \tag{6.2}$$

Note that $x_2 \neq y_2$. We write $y_2 = 1/w + x_2 = (1 + wx_2)/w$ for a $w \in \mathbf{F}_q$ and substitute it in (6.2). After expanding we get:

$$\begin{aligned}
\frac{(x_2^2 + x_2 + s)((\frac{1+wx_2}{w})^2 + \frac{1+wx_2}{w} + s)}{(x_2 + 1/w + x_2)^2} &= \\
w^2(x_2^2 + x_2 + s)\left(\left(\frac{1 + wx_2}{w}\right)^2 + \frac{1 + wx_2}{w} + s\right) &= \\
(x_2^2 + x_2 + s)((1 + wx_2)^2 + w(1 + wx_2) + sw^2) &= \\
(x_2^2 + x_2 + s)(1 + w^2x_2^2 + w + w^2x_2 + sw^2) &= \\
(x_2^2 + x_2 + s)(1 + w^2(x_2^2 + x_2 + s) + w) &= \\
(x_2^2 + x_2 + s) + w^2(x_2^2 + x_2 + s)^2 + w(x_2^2 + x_2 + s) &= \\
((x_2^2 + x_2 + s)w + x_2)^2 + ((x_2^2 + x_2 + s)w + x_2) + s &\in \mathbf{F}_{\sqrt{q}}.
\end{aligned}$$

(The member relation is by (6.2) and the fact that $\lambda, \tilde{\lambda} \in \mathbf{F}_{\sqrt{q}}$) This is impossible by Lemma 6.3.

All cases accounted for, we have that no two distinct points in I are adjacent. Then we have $\alpha(ER_q) \geq q\sqrt{q} - q + \sqrt{q}$ as desired.

6.3 $p = 2$ and n is odd

Here we give a proof for the case $p = 2$ and n is odd (for $q = p^n$). We want to prove

$$\alpha(ER_q) \geq \frac{q\sqrt{q}}{2\sqrt{2}}.$$

Let $\mu \in \mathbf{F}_q^*$ be a primitive element. Write $x \in \mathbf{F}_q$ in the form

$$x = x_0 + x_1\mu + x_2\mu^2 + \cdots + x_{n-1}\mu^{n-1}$$

where all $x_i \in \mathbf{F}_2$. Construct two sets where $m = (n-1)/2$

$$\begin{aligned}
S &= \{x \in \mathbf{F}_q : x_{n-1} = 0\}, \\
T &= \{x \in \mathbf{F}_q : x_m = 1, \text{if } i > m \text{ then } x_i = 0\}.
\end{aligned}$$

They have the following cardinality

$$\begin{aligned}
|S| &= 2^{n-1} = q/2, \\
|T| &= 2^m = \sqrt{q}/\sqrt{2}.
\end{aligned}$$

Then we have an independent set (we use the inner-product for ER_q^*)

$$I = \{(1, t, s) : t \in T, s \in S\}$$

of cardinality $|I| = |S||T| = \frac{q\sqrt{q}}{2\sqrt{2}}$.

6.4 $p > 2$ and n is even

Here we give a proof for the case $p > 2$ and n is even (for $q = p^n$). We want to prove

$$\alpha(ER_q) \geq \frac{q\sqrt{q} + q + 2}{2}.$$

Let $\mu \in \mathbf{F}_q^*$ be a primitive element. Introduce the set

$$R \quad = \quad \left\{ \mu^{(\sqrt{q}+1)k} : \text{integer } k \in \left[0, \frac{\sqrt{q}-3}{2}\right] \right\} \cup \{0\}.$$

It has the following properties:

- $|R| = (\sqrt{q}+1)/2$. As μ is primitive μ generates $\mathbf{F}_q^*$ (which has cardinality $q-1$) and the largest element in the interval is $(\sqrt{q}-3)/2$ for which holds

  $$(\sqrt{q}+1) \cdot \frac{\sqrt{q}-3}{2} \quad < \quad q-1,$$

  so if you range over the interval $[0, (\sqrt{q}-3)/2]$ you will get $(\sqrt{q}-3)/2 - 0 + 1 = (\sqrt{q}-1)/2$ different elements. Together with $|\{0\}| = 1$ we have $(\sqrt{q}+1)/2$ elements.

- For every non-zero $x \in R$ we have $-x \notin R$. We can proof this by using $-1 = \mu^{(q-1)/2}$ ($\langle \mu \rangle$ is a group of even order $q-1$). For arbitrary $k \in [0, (\sqrt{q}-3)/2]$ we have

  $$-x = \mu^{(q-1)/2} \cdot \mu^{(\sqrt{q}+1)k} = \mu^{(\sqrt{q}+1)(k+(\sqrt{q}-1)/2)} \notin R$$

  because $(k + (\sqrt{q}-1)/2) \notin \left[0, \frac{\sqrt{q}-3}{2}\right]$.

- R is isomorphic to a subset of $\mathbf{F}_{\sqrt{q}}$. Because $\mathbf{F}_{\sqrt{q}}^*$ is a subgroup of $\mathbf{F}_q^*$ of cardinality $\sqrt{q}-1$ and $\langle \mu^{\sqrt{q}+1} \rangle$ is also of cardinality $(q-1)/(\sqrt{q}+1) = \sqrt{q}-1$ this means $\langle \mu^{\sqrt{q}+1} \rangle = \mathbf{F}_{\sqrt{q}}^*$ which means R must be isomorphic to a subset of $\mathbf{F}_{\sqrt{q}}$.

We introduce another set

$$I \quad = \quad \left\{ \left(1, t, \frac{t^2 - \mu r}{2}\right) : t \in \mathbf{F}_q, r \in R \right\} \cup \{(0,0,1)\}.$$

We make two claims about it which complete the proof.

I is an independent set in ER_q. By using the inner-product for ER_q^* we have immediately that $(0,0,1)$ is not adjacent to any other vertex in I. Next pick two arbitrary vertices in I of the form

$$\left(1, t, \frac{t^2 - \mu r}{2}\right), \left(1, \tilde{t}, \frac{\tilde{t}^2 - \mu \tilde{r}}{2}\right).$$

By computing their inner-product (using the inner-product for ER_q^*) we set

$$\begin{aligned} 0 &= \frac{\tilde{t}^2 - \mu\tilde{r}}{2} - t\tilde{t} + \frac{t^2 - \mu r}{2} \qquad \text{which is equiv. to} \\ 0 &= \tilde{t}^2 - \mu\tilde{r} - 2t\tilde{t} + t^2 - \mu r \qquad \text{which is equiv. to} \\ \mu(\tilde{r} + r) &= \tilde{t}^2 - 2t\tilde{t} + t^2 \;=\; (t - \tilde{t})^2. \end{aligned}$$

We know $\tilde{r}+r$ is a square (as R is isomorphic to a subset of $\mathbf{F}_{\sqrt{q}}$, $\tilde{r}+r$ could be a square in $\mathbf{F}_{\sqrt{q}}$ and therefore in $\mathbf{F}_q$, in case it is not square in $\mathbf{F}_{\sqrt{q}}$ it is square in $\mathbf{F}_q$ because that is a quadratic extension of $\mathbf{F}_{\sqrt{q}}$) and because $(t-\tilde{t})^2$ is a square too $\mu(\tilde{r}+r)$ must be a square too. However this is only possible when $t = \tilde{t}$ and $-r = \tilde{r}$, which implies $r = \tilde{r} = 0$ so the two vertices we picked are equal so I is an independent set.

It is easy to see

$$|I| = |\mathbf{F}_q||R| + 1 = q \cdot \frac{\sqrt{q}+1}{2} + 1 = \frac{q\sqrt{q} + q + 2}{2}.$$

6.5 $p > 2$ and n is odd

Here we give a proof for the case $p > 2$ and n is odd (for $q = p^n$). We want to prove

$$\alpha(ER_q) \geq \frac{120q\sqrt{q}}{73\sqrt{73}}.$$

Let $\mu \in \mathbf{F}_q^*$ be a primitive element. Write $x \in \mathbf{F}_q$ in the form

$$x = x_0 + x_1\mu + x_2\mu^2 + \cdots + x_{n-1}\mu^{n-1}$$

where all $x_i \in \mathbf{F}_p$. Introduce the following subsets of $\mathbf{Z}$

$$\begin{aligned} A &= [\lceil p/6 \rceil, \lfloor p/2 \rfloor], \\ B &= [0, \lfloor \sqrt{p/3} \rfloor]. \end{aligned}$$

Next we construct two other sets where $m = (n-1)/2$

$$\begin{aligned} S &= \{x \in \mathbf{F}_q : x_{n-1} \in A\}, \\ T &= \{x \in \mathbf{F}_q : x_m \in B, \text{if } i > m \text{ then } x_i = 0\}. \end{aligned}$$

They have the following cardinality

$$\begin{aligned} |S| &= p^{n-1}|A|, \\ |T| &= p^m|B|. \end{aligned}$$

Now we have two claims

- For all $s, \tilde{s} \in S$ we have $(s+\tilde{s})_{n-1} \in [\lceil (p+1)/3 \rceil, p-1]$. This is easy to see in the case $p = 3$. For $p > 3$ it is sufficient to prove $\lceil (p+1)/3 \rceil \leq 2\lceil p/6 \rceil$ which can be shown by combining

$$\begin{aligned} \lceil (p+1)/3 \rceil &= \lceil p/3 \rceil, \\ \lceil p/3 \rceil &\leq 2\lceil p/6 \rceil. \end{aligned}$$

- For all $t, \tilde{t} \in T$ we have $(t\tilde{t})_{n-1} = t_m \tilde{t}_m \in [0, \lfloor p/3 \rfloor]$. This is easy to see because in general for all real $r \geq 0$ holds $\lfloor r \rfloor^2 \leq \lfloor r^2 \rfloor$ (write $r = k + l$ for an integer k and a real l with $0 \geq l < 1$).

As $\lfloor p/3 \rfloor < \lceil (p+1)/3 \rceil$ (for $p > 3$ write $p = 3j+1$ or $p = 3j+2$) the sets $[0, \lfloor p/3 \rfloor]$ and $[\lceil (p+1)/3 \rceil, p-1]$ are disjoint and therefore the following set

$$I = \{(1, t, s) : t \in T, s \in S\}$$

is an independent set (again we use the bilinear form for ER_q^*) of cardinality

$$|I| = |S||T| = |A||B|p^{m+n-1} = |A||B|\frac{qp^m}{p} = |A||B|\frac{q\sqrt{q}}{p\sqrt{p}}.$$

We will modify the term $|A||B|/p\sqrt{p}$ to something more useful. To do this we first introduce the bound bellow:

$$|A||B| \cdot \frac{1}{p\sqrt{p}} = \left(\left\lfloor \frac{p}{2} \right\rfloor - \left\lceil \frac{p}{6} \right\rceil + 1 \right) (\lfloor \sqrt{p/3} \rfloor + 1) \cdot \frac{1}{p\sqrt{p}} > \frac{p-1}{3} \cdot \frac{\sqrt{p}}{\sqrt{3}} \cdot \frac{1}{p\sqrt{p}} = \frac{1 - 1/p}{3\sqrt{3}}.$$

Justifications for the bound(s):

- Write $p/6 = r + j$ for an integer r and a real j with $0 < j \leq 1$, then

$$\begin{aligned} |A| = \left\lfloor \frac{p}{2} \right\rfloor - \left\lceil \frac{p}{6} \right\rceil + 1 = \frac{p-1}{2} - \lceil r + j \rceil + 1 = \\ \frac{p-1}{2} - (r+1) + 1 = \frac{p-1}{2} - r \geq \\ \frac{p-1}{2} - (r+j) + \frac{1}{6} = \frac{p-1}{2} - \frac{p}{6} + \frac{1}{6} = \frac{p-1}{3}. \end{aligned}$$

- For $|B|$ we have

$$|B| = \lfloor \sqrt{p/3} \rfloor + 1 > \sqrt{p/3}.$$

So $|A||B|/p\sqrt{p}$ is bounded below by the strict increasing function $(1 - 1/p)/3\sqrt{3}$ so $|A||B|/p\sqrt{p}$ attains a minimum. In [18] a computer search was done to find the minimum is attained at $p = 73$ where $|A||B|/p\sqrt{p} = 120/73\sqrt{73}$ so

$$\alpha(ER_q) \geq \frac{120q\sqrt{q}}{73\sqrt{73}}.$$

Chapter 7

Improved constructions for odd q

In the previous chapter we gave constructions for independent sets in ER_q bounded below by $O(q\sqrt{q})$. In this section we will introduce for odd q two new constructions. In practice these constructions provide us with independent sets in ER_q larger than the constructions from chapter 6, see Appendix B.2 for a comparison table. The constructions come from [18].

7.1 Method 1

Given a subset $R \subseteq \mathbf{F}_q$ such that every $r \in R$ is a non-square and for any *distinct* $r, \tilde{r} \in R$ holds $r + \tilde{r}$ is a non-square (note this implies for every $r \in R$ holds $-r \notin R$). We then construct the set

$$I := \{(1, t, (t^2 - r)/2) : t \in \mathbf{F}_q, r \in R \cup \{0\}\} \cup \{(0, 0, 1)\}.$$

Now pick arbitrary $(1, t, (t^2-r)/2), (1, \tilde{t}, (\tilde{t}^2-\tilde{r})/2) \in I$. If these two points are adjacent then

$$\begin{aligned} \langle (1, t, (t^2 - r)/2), (1, \tilde{t}, (\tilde{t}^2 - \tilde{r})/2) \rangle &= 0, \quad \Longleftrightarrow \\ t^2 - r + \tilde{t}^2 - \tilde{r} &= 2t\tilde{t}, \quad \Longleftrightarrow \\ t^2 - 2t\tilde{t} + \tilde{t}^2 &= \tilde{r} + r, \quad \Longleftrightarrow \\ (t - \tilde{t})^2 &= \tilde{r} + r \end{aligned} \tag{7.1}$$

For $r \neq \tilde{r}$, by construction of our R, (7.1) can not hold. So we assume $r = \tilde{r}$. This gives us

$$(t - \tilde{t})^2 = 2r. \tag{7.2}$$

We make case distinction on q.

- For $q \equiv 1, 7 \bmod 8$ we have (by Proposition 1.6(iii)) 2 is a square in $\mathbf{F}_q$. Now we write $2 = \mu^{2i}$ and $r = \mu^{2j+1}$ so 2μ is a non-square. So we can only satisfy (7.2) if $r = 0$ and $t = \tilde{t}$. So we conclude I is an independent set

- For $q \equiv 3, 5 \bmod 8$ we have 2 is not a square in $\mathbf{F}_q$ so $2r$ is a square. Now we deduce from (7.2):

$$\tilde{t} = t \pm \sqrt{2r}.$$

For $r = 0$ we find $t = \tilde{t}$. For $r \neq 0$ we conclude the point $(1, t, (t^2 - r)/2)$ is of degree 2 in I. So we conclude every vertex in I has degree 0 or 2. This implies I consists of isolated points or cycles, Figure 7.1 gives the MAGMA construction in the case $q = 11$. From this we can easily find a subset of I which is an independent set.

The appendix has MAGMA code which returns on a given q an independent set constructed with this method. It also contains code for finding an optimal R. One of the properties of I is that for every $x \in I$ holds

$$-\langle x, x \rangle = r \tag{7.3}$$

which equals 0 or a non-square by our construction of R so by Proposition 3.11(i) I does not contain external points. From (7.3) we also deduce I contains all the $q + 1$ absolute points.

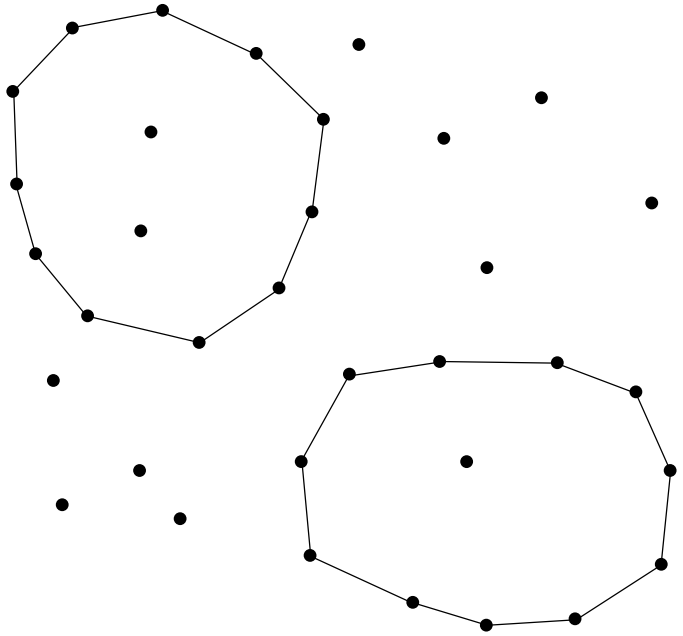

Figure 7.1: MAGMA construction of I for $q = 11$

7.2 Method 2

We start with a subset $R \subseteq \mathbf{F}_q$ such that for all *distinct* $r, \tilde{r} \in R$ holds $1 - r\tilde{r}$ is a non-square. This immediately implies $0 \notin R$. Now introduce the set

$$I := \{(1, t, rt^2/2) : t \in \mathbf{F}_q, r \in R\} \cup \{(0, 0, 1)\}.$$

Pick two points $(1, t, rt^2/2), (1, \tilde{t}, \tilde{r}\tilde{t}^2/2) \in I$. If these two points are adjacent then we have

$$\begin{aligned}
\langle (1, t, rt^2/2), (1, \tilde{t}, \tilde{r}\tilde{t}^2/2) \rangle &= 0, \iff \\
rt^2/2 + \tilde{r}\tilde{t}^2/2 &= t\tilde{t}, \iff \\
\tilde{r}\tilde{t}^2 - 2t\tilde{t} &= -rt^2, \iff \\
\tilde{t}^2 - \frac{2t\tilde{t}}{\tilde{r}} &= -\frac{rt^2}{\tilde{r}}, \iff \\
\left(\tilde{t} - \frac{t}{\tilde{r}}\right)^2 &= -\frac{rt^2}{\tilde{r}} - \frac{t^2}{\tilde{r}^2}, \iff \\
\left(\tilde{t} - \frac{t}{\tilde{r}}\right)^2 &= (1 - r\tilde{r}) \cdot \left(\frac{t}{\tilde{r}}\right)^2. \qquad (7.4)
\end{aligned}$$

Which is only possible if $1 - r\tilde{r}$ is a square. So when $r \neq \tilde{r}$ (7.4) will not hold, by construction of our R. Assume $r = \tilde{r}$. If $1 - r^2 = a^2$ for some $a \in \mathbf{F}_q$ then from (7.4) we derive

$$\left(\tilde{t} - \frac{t}{r}\right)^2 = \left(\frac{at}{r}\right)^2.$$

This equation has solutions

$$\tilde{t} = \left(\frac{1+a}{r}\right) t, \left(\frac{1-a}{r}\right) t.$$

by $(1+a)/r \cdot (1-a)/r = 1$ this becomes

$$\tilde{t} = \left(\frac{1+a}{r}\right) t, \left(\frac{1+a}{r}\right)^{-1} t.$$

So for a given $t \in \mathbf{F}_q$ there are two points in I adjacent to it. So every element in I has degree 0 or 2 (in I) so I contains only isolated points and cycles. Cycles have length l equal the order of $(1+a)/r$ in $\mathbf{F}_q^*$. If l is even then the cycle provides us with $l/2$ isolated points. If l is odd then the cycle provides us with $(l-1)/2$ isolated points. For a concrete construction we are free to pick any non-zero $t \in \mathbf{F}_q$ as a starting point.

Because $\mathbf{F}_q^*$ has a generating element μ we can write $t = \mu^i$ and $(1+a)/r = \mu^j$ for integers i and j. So a cycle looks like

$$\left\{ \left(\frac{1+a}{r}\right), \left(\frac{1+a}{r}\right)^2, \ldots, \left(\frac{1+a}{r}\right)^l \right\} = \{\mu^j, \mu^{2j}, \ldots, \mu^{lj}\}.$$

As the order is l we have $(q-1)/l$ cycles which can be constructed by scaling our initial cycle with $1, \mu, \mu^2, \ldots, \mu^{(q-1)/l-1}$.

Just as for method 1 we have implemented this construction in MAGMA too. We restrict ourself to sets R for which holds $1 \in R$ and with this restriction the code generates an R such that I contains a largest independent set. With the restriction that $1 \in R$ we have for every $x \in I$

$$-\langle x, x\rangle = t^2(1-r) \tag{7.5}$$

which equals 0 or a non-square by our construction of R so I does not contain external points just as in the case of method 1. From (7.5) we also deduce I contains all the $q+1$ absolute points.

By modifying our code and leaving the restriction $1 \in R$ out we did found larger independent sets. Our results are given in the table below which shows all odd $q \leq 150$ were leaving the restriction out gives us a larger independent set (note in that case $1 \notin R$).

q	$1 \in R$	$1 \notin R$
31	107	122
61	302	332
71	352	387
73	398	434
113	730	786
125	808	870
127	758	821
131	782	912
139	899	968
149	1038	1112

Chapter 8

Try and search

Opposed to the previous two chapters, where for all q we were able to give a construction of an independent set, we will in this chapter introduce some heuristics which can be used to find independent sets and colorings.

8.1 Heuristics

As finding a maximal clique, independent set or optimal coloring of the vertex set of a graph G on n vertices is NP-complete we introduce two heuristics. The results might not be optimal but gives us extra feedback for reasoning on independent sets and optimal colorings.

The first heuristic is for finding a large clique in G (applying the heuristic to $\overline{G}$ gives us an independent set in G). The concept is as follows:

1. Put the vertices of G in random order.
2. Create with the first vertex a clique of cardinality 1.
3. If the 2nd vertex is adjacent to all vertices in the clique then join the 2nd vertex with the clique.
4. Repeat the previous step for the 3rd, 4th, ..., nth vertex.

The algorithm can be repeated as many times as desirable, every time with a new random sequence of the vertices. This provides us with a lower-bound for $\omega(G)$.

The second heuristic is for finding an upper-bound for the chromatic number $\gamma(G)$ of a graph. The heuristic is called ***sequential coloring***. The concept of the algorithm is similar to that of finding a clique:

1. Put the vertices of G in random order.
2. Assuming the first i vertices are colored with k colors, try to color the $(i+1)$th vertex with one of the k colors (choose the smallest color available). If this is not possible then color the $(i+1)$th vertex with a new color $k+1$.
3. Repeat the previous step for $i = 1, 2, \ldots, n-1$.

We can repeat this as many times as we want, every time with a new random sequence of the vertices.

We implemented these heuristics in MAGMA. The programs can be found in the appendix. We optimized the algorithms as best as we can which might result in less readable code. The algorithms for finding a clique or an independent set will return the clique or independent set itself. The algorithm for the chromatic number will only return the number of colors which were used and it will always be $\Delta(G) + 1$ or less by the way the algorithm works.

8.2 Searching for good colorings

Given an independent set I of the graph OG_q we construct a set

$$V_q := \{f(I) : f \in \mathrm{Aut}(OG_q)\}.$$

Note $I \in V_q$ and every set in V_q is an independent set by definition of graph automorphism. With this set V_q we can construct a graph where two *distinct* vertices $f_i(I)$ and $f_j(I)$ are adjacent if and only if

$$|f_i(I) \cap f_j(I)| \leq k, \tag{8.1}$$

for a given integer $k \geq 0$. Finding suitable sized cliques in the graph might give us a coloring of the vertex set of G. We have made an attempt for the following cases:

($\mathbf{q = 3}$)
By inspection we find an independent set in OG_3 of size 3:

$$\{(110), (102), (120)\}.$$

See Appendix A.1 for a complete list of vertices and adjacency relations of OG_3 including a figure as well. The images of this independent set under all elements of $\mathrm{Aut}(OG_3)$ are:

$$\begin{aligned}
A &= \{(110), (102), (120)\},\\
B &= \{(010), (111), (012)\},\\
C &= \{(111), (101), (120)\},\\
D &= \{(111), (101), (012)\},\\
E &= \{(011), (121), (010)\},\\
F &= \{(110), (121), (101)\},\\
G &= \{(010), (111), (120)\},\\
H &= \{(011), (102), (120)\},\\
I &= \{(011), (121), (101)\},\\
J &= \{(011), (102), (012)\},\\
K &= \{(110), (102), (012)\},\\
L &= \{(110), (121), (010)\}.
\end{aligned}$$

Figure 8.1 shows whether independent sets (now seen as vertices themselves) meet ($k = 0$ in (8.1)). Any vertices from Figure 8.1 which form a clique of size 3 cover the whole vertexset of OG_3 so OG_3 is 3 colorable. .

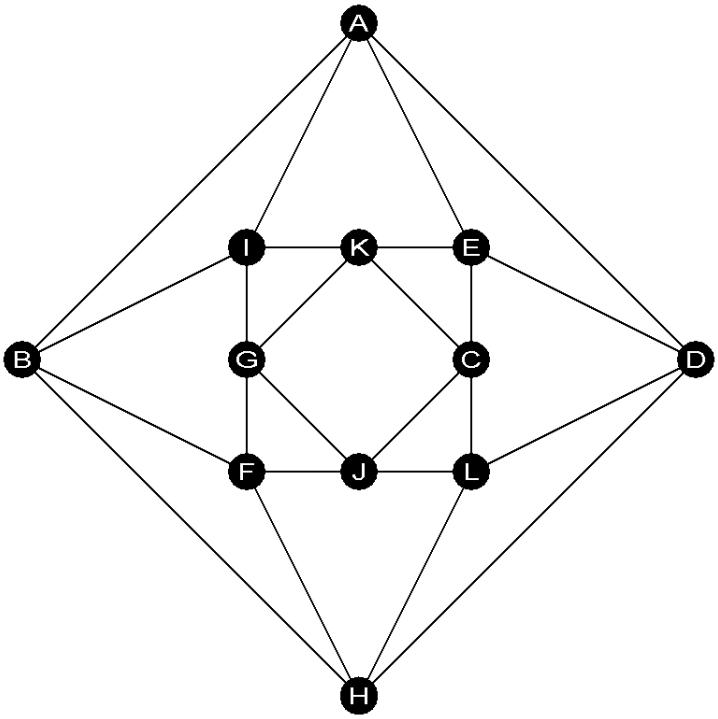

Figure 8.1: Independent sets of OG_3 and their intersection relation

($\mathbf{q = 9}$)

For $q = 9$ we found, by our heuristic from section 8.1, an independent set I in OG_9 with $|I| = 19$. There $4 \cdot 19 < 9^2$ and we were already able to color the vertexset of OG_9 with 5 colors by sequential coloring (see Appendix B.3) we will not obtain any new results this way. Other independent set constructions do not supply us with independent sets for OG_9 with more than 19 vertices. Method 2 gives us an independent of size 22 (see Appendix B.2) however it contains the 10 absolute points which are not part of OG_9.

($\mathbf{q = 11}$)

With our heuristic from section 8.1 we find an independent set I in OG_{11} with $|I| = 28$. Constructing a graph for various k in (8.1) we found the following clique sizes:

k	size clique
0	1
1	1
2	2
3	3
4	5
5	6

When $k = 2$ our procedure gives us a clique of size 2 with the union of the 2 subsets of the vertexset of OG_{11} equal to 54. Sequential coloring colored the re-

maning $11^2 - 54 = 67$ vertices with 4 colors so OG_{11} is $2 + 4 = 6$ colorable. When $k = 3$ our procedure gives us a clique of size 3 with the union of the 3 subsets of the vertexset of OG_{11} equal to 77. Sequential coloring colored the remaining $11^2 - 77 = 44$ vertices with 3 colors so OG_{11} is $3 + 3 = 6$ colorable. When $k = 4$ our procedure gives us a clique of size 5 with the union of the 3 subsets of the vertexset of OG_{11} equal to 105. In none of the cases we improved sequential coloring which colored the vertexset of OG_{11} with 6 colors (see Appendix B.3).

The construction from chapter 6 gives us an independent set of size 8. There OG_{11} has 121 vertices we will not be able to cover the vertexset with 6 independent sets as $8 \cdot 6 < 121$.

($\mathbf{q = 13}$)

We repeated the steps from the case when $q = 11$. We did not improve the sequential coloring algorithm which colored OG_{13} with 7 colors. Our table of clique sizes is:

k	size clique
0	1
1	3
2	3
3	4
4	5
5	5
6	8

($\mathbf{q = 16}$)

With an independent set I with $|I| = 44$, constructed by our heuristic from section 8.1, we construct the vertexset V_{16}. It turns out that $|V_{16}| = 16320$. It took MAGMA over 39 minutes to construct the corresponding edge set. When we apply our procedure to the independent set I with $|I| = 52$ from chapter 6 we have a much smaller vertexset of size 120 therefore we were able to give the next table:

k	size clique
0	1
1	1
2	1
3	1
4	4
5	4
6	4

The union of the 4 independent sets for $k = 4$ in (8.1) equals 187. Not coloring the whole vertexset of 256 vertices. Applying sequential coloring to the remaining vertices (that is the vertices that are not covered by the 4 independet sets) we were able to color them with 3 colors so OG_{16} is colorable with $3 + 4 = 7$ colors. An improvement over sequential coloring which had to use 8 colors (see Appendix B.3). Appendix C.1 gives every element of the coloring.

($\mathbf{q = 17}$)

Applying Method 1 from section 7 we obtain an independent set I with $|I| = 52$. Of the 52 vertices 18 of them are absolute so 34 are non-absolute. However as $8 \cdot 34 < 17^2$ and sequential coloring colors OG_{17} with 9 colors we fail in beating

sequential coloring.

Applying the sequential independent set heuristic from section 8.1 to OG_{17} gives us an independent set I with $|I| = 47$. If we choose $k = 3$ in (8.1) then we found 4 images of I in our graph which colored 171 vertices. The remaining $17^2 - 171 = 118$ vertices are 4 colorable by sequential coloring so OG_{17} is $4 + 4 = 8$ colorable, an improvement over sequential coloring which needed 9 colors. Appendix C.2 gives every element of the coloring.

We would like to state that for bigger q we needed more and more CPU-time. Therefore our search stops for $q = 17$. For odd q our Methods from chapter 7 only provides us with internal and absolute points so by Proposition 4.3(ii) we can not cover the external points.

Chapter 9

Motivation, conclusions and recommendations

This chapter shines some light on the motivation for our study of the Erdős-Rényi graph together with conlusions for further research.

9.1 Motivation

Given arbitrary field $\mathbf{F}$. Let G be a graph on n vertices. An $n \times n$ matrix over $\mathbf{F}$ with all diagonal elements non-zero and $A_{ij} = 0$ if i and j are adjacent in G is said to **fit** G.

A clique in G corresponds with a diagonal submatrix of A therefore $\text{rank}(A) \geq \omega(G)$. There also exists a matrix A that fits G for which holds $\text{rank}(A) = \gamma(G)$.

Proposition 9.1. *There exists a matrix A over $\mathbf{F}$ that fits G such that rank$(A) = \gamma(G)$.*

Proof. Let G be colored with $\gamma(G)$ colors. Now define the matrix A by

$$A_{ij} = \begin{cases} 1 & \text{if } i \text{ and } j \text{ are in the same color class,} \\ 0 & \text{otherwise.} \end{cases}$$

Note for all i holds $A_{ii} = 1$. Then A fits G (by definition) and $\text{rank}(A) = \gamma(G)$ (A can be partitioned as a block matrix with blocks of 1s on the diagonal and 0s outside the diagonal). □

Next we introduce a number which was first introduced by Haemers.

$$\eta(G) \quad = \quad \min\{\text{rank}(A) : \text{matrix } A \text{ over } \mathbf{F} \text{ which fits } G\}.$$

So by Proposition 9.1 we have

$$\omega(G) \quad \leq \quad \eta(G) \quad \leq_{(*)} \quad \gamma(G).$$

Notice the exact value $\eta(G)$ depends on the field $\mathbf{F}$. One of the questions that arises: how large can the gap (*) be? An approach to answer this question is by fixing a rank r and look what the largest chromatic number and its accompanying graph can be. The next two numbers M_1 and M_2 together with a theorem which is from unpublished notes from Peeters helps us with the answer of this new question.

$$
\begin{aligned}
M_1(\mathbf{F}, r) &= \max\{\gamma(G): \text{ all graphs } G \text{ on } n \text{ vertices} \\
&\qquad \text{such that there exists an } n \times n \text{ matrix } A \text{ over } \mathbf{F} \\
&\qquad \text{which fits } G, \text{ is symmetric and } \operatorname{rank}(A) \leq r\}, \\
M_2(\mathbf{F}, r) &= \max\{\gamma(G): \text{ all orthogonality graphs } G \text{ which are defined by a} \\
&\qquad \text{non-degenerate bilinear form on } \mathbf{F}^n\}.
\end{aligned}
$$

Theorem 9.2. *Given arbitray field* $\mathbf{F}$ *and arbitrary integer* $r > 0$*. Then*

$$M_1(\mathbf{F}, r) = M_2(\mathbf{F}, r).$$

Recall that an orthogonality graph is a graph where the vertex set are all the 1-dimensional subspaces $U \subseteq \mathbf{F}^m$ such that U is not orthogonal to itself (the ortogonality relation is defined by a non-degenerate bilinear form on $\mathbf{F}^m$) and two distinct subspaces U and S are adjacent if and only if $U \perp S$.

This thesis has special attention for the case $r = 3$ and the bilinear form defined by the matrix from (3.2).

9.2 Conclusions and recommendations

For further research we would suggest to try to tweak Methods 1 and 2 from chapter 7 such that you will get independent sets with external points. This might be a fruitful path to walk as the table from Appendix B.2 shows that, despite the independens sets contain the absolute points, they have still much more points than the independent sets generated by our heuristic from section 8.1.

The stuctured search we did in section 8.2 for OG_{16} and OG_{17} beats sequential coloring by 1. So one might want to consider this strategy when one wants to search for a good upperbound for ER_q or OG_q.

The table in Appendix B.3 with exact chromatic numbers for ER_q only has one value. The function in MAGMA which can find exact chromatic numbers appears to be somewhat slow. Using something like CPLEX or comparable strategies as described in [6] might be a better way to find exact chromatic numbers for small cases.

Figure 8.1 suggests the graphs which are constructued in section 8.2 have a beautiful structure. Further research might lead to large cliques.

Appendix A

An example

A.1 ER_3

This section will give some properties and facts of ER_3. The table bellow shows the vertices and the relation between them: + corresponds to adjacent vertices where blank means two vertices are not adjacent.

	1	1	1	1	1	1	1	1	1	0	0	0	0
	0	0	0	1	1	1	2	2	2	1	1	1	0
	0	1	2	0	1	2	0	1	2	0	1	2	1
1 0 0				+			+			+			
1 0 1			+			+			+	+			
1 0 2		+			+			+		+			
1 1 0	+				+				+		+		
1 1 1			+	+				+			+		
1 1 2		+					+				+		
1 2 0	+					+		+				+	
1 2 1			+		+		+					+	
1 2 2		+		+								+	
0 1 0	+	+	+										+
0 1 1				+	+	+							+
0 1 2							+	+	+				+
0 0 1										+	+	+	

The absolute points are $(1\ 0\ 0), (0\ 0\ 1), (1\ 2\ 2)$ and $(1\ 1\ 2)$. A graphical representation of OG_3 is given below

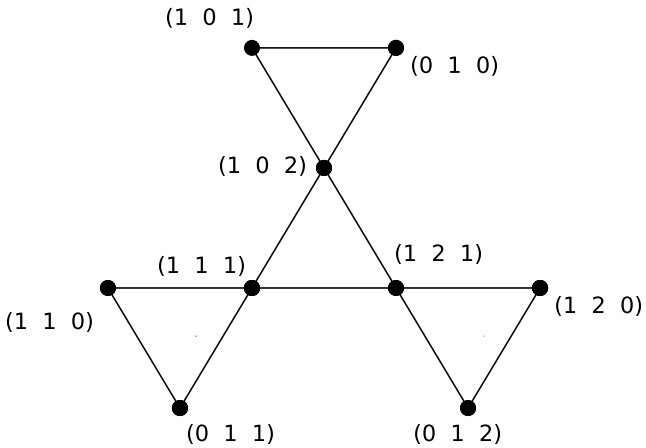

Figure A.1: The orthogonality graph OG_3

Appendix B

Independent set and coloring tables

B.1 Distribution of points in ER_q

This table shows how many absolute points $\mathcal{R}$, external points $\mathcal{L}$ and internal points $\mathcal{M}$ each graph ER_q contains. Propositions 3.2, 3.10, 3.11(ii) and 3.11(iii) tell us how much points of each type we have. See also the supporting Figures 3.3 and 3.4. When q is even we have

$$\begin{aligned} q+1 &\text{ absolute points,} \\ q^2 &\text{ external points.} \end{aligned}$$

When q is odd we have

$$\begin{aligned} q+1 &\text{ absolute points,} \\ q(q+1)/2 &\text{ external points,} \\ q(q-1)/2 &\text{ internal points.} \end{aligned}$$

This gives us the table

q	$\mathcal{R}$	$\mathcal{L}$	$\mathcal{M}$
3	4	6	3
4	5	16	0
5	6	15	10
7	8	28	21
8	9	64	0
9	10	45	36
11	12	66	55
13	14	91	78
16	17	256	0
17	18	153	136
19	20	190	171
23	24	276	253
25	26	325	300
27	28	378	351
29	30	435	406
31	32	496	465
32	33	1024	0
37	38	703	666
41	42	861	820
43	44	946	903
47	48	1128	1081
49	50	1225	1176

B.2 Independent sets

The table in this section gives sizes of independent sets in ER_q constructed by the various methods we have described in this thesis. Columns 2, 3 and 4 are chapter 6 and Methods 1 and 2 from chapter 7. The results from the last four columns are by our sequential heuristic from section 8.1 applied to the given graphs.

q	chapter 6	Method 1	Method 2	ER_q	OG_q	$G\mathcal{L}_q$	$G\mathcal{M}_q$
3	2	5	5	5	3	3	1
4	6	-	-	7	6	-	-
5	4	8	10	10	7	5	4
7	4	15	14	15	13	12	7
8	8	-	-	17	16	-	-
9	19	19	22	22	19	15	12
11	8	22	27	28	28	24	17
13	12	32	38	35	36	29	24
16	52	-	-	45	46	-	-
17	18	52	50	48	47	44	37
19	18	47	56	55	54	51	41
23	24	70	79	71	70	64	55
25	76	101	86	79	78	69	60
27	54	55	106	86	87	77	65
29	40	72	114	96	96	79	76
31	40	125	107	104	103	92	80
32	64	-	-	108	107	-	-
37	48	110	164	130	129	111	105
41	56	165	182	150	148	125	119
43	56	128	170	158	155	138	122
47	64	189	209	176	174	155	139
49	197	246	218	185	185	155	151
53	90	184	262	203	202	174	168
59	100	205	292	233	235	209	186
61	100	212	302	242	244	207	202
64	456	-	-	259	258	-	-
67	110	233	332	273	272	239	220
71	120	356	352	292	294	258	237
73	120	366	398	303	301	260	254
79	156	396	431	335	332	293	272
81	406	487	442	346	345	295	292
83	168	330	453	355	357	311	292
89	180	535	530	388	388	330	329
97	192	583	578	431	431	369	365

B.3 Bounds on chromatic numbers

This section has tables with bounds on the chromatic numbers of OG_q and ER_q. The 3rd column of each table is the Hoffman bound from section 5.3 applied to both graphs, giving us lower bounds for the chromatic numbers $\gamma(OG_q)$ and $\gamma(ER_q)$. Upperbounds are given by our sequential coloring heuristic from section 8.1 and the Wilf bound from section 5.3. The column with exact values of $\gamma(OG_q)$ are results from [6]. The column labeled by $\gamma(OG_q$ and $\gamma(ER_q)$ is the best interval we have for the chromatic concluding from other columns.

q	$\gamma(OG_q)$	Hoffman	exact	Sequential	Wilf	section 8.2
3	3	3	3	3	4	-
4	4	3	4	4	5	-
5	4	4	4	4	6	-
7	4	4	4	4	8	-
8	5	4	5	5	9	-
9	5	4	5	5	10	-
11	5-6	5	-	6	12	-
13	5-7	5	-	7	14	-
16	5-7	5	-	8	17	7
17	6-8	6	-	9	18	8
19	6-9	6	-	9	20	-
23	6-11	6	-	11	24	-
25	6-12	6	-	12	26	-

Next table is for ER_q. The only exact value comes from MAGMA, for larger q it took too much computer time.

q	$\gamma(ER_q)$	Hoffman	exact	Sequential	Wilf	section 8.2
3	4	3	4	4	4	-
4	$4^{(1)}$	3	-	4	5	-
5	4	4	-	4	6	-
7	4-5	4	-	5	8	-
8	5-6$^{(2)}$	4	-	6	9	-
9	5-6$^{(3)}$	4	-	6	10	-
11	5-7	5	-	7	12	-
13	5-8	5	-	8	14	-
16	5-8$^{(4)}$	5	-	9	17	-
17	6-9$^{(5)}$	5	-	9	18	-
19	6-10	6	-	10	20	-
23	6-12	6	-	12	24	-
25	6-12	6	-	12	26	-

(1) is because of $\gamma(OG_4) = 4$.
(2) is because of $\gamma(OG_8) = 5$.
(3) is because of $\gamma(OG_9) = 5$.
(4) is because of $\gamma(OG_{16})$ =5-7.
(5) is because of $\gamma(OG_{17}) \geq 6$.

Appendix C

Colorings

Two concrete colorings for OG_{16} and OG_{17}.

C.1 OG_{16}

(i) $\{ (1:\mu^8:\mu^{14}), (1:\mu^{14}:\mu^2), (1:\mu^7:1), (1:\mu^3:\mu), (1:\mu^{11}:\mu^{10}), (1:\mu^6:\mu^{10}), (0:1:1), (1:\mu^7:\mu^{13}), (1:\mu^{13}:\mu), (1:\mu^{12}:0), (1:\mu^4:\mu^8), (1:\mu^{12}:\mu^6), (1:\mu^9:\mu^8), (1:\mu^2:1), (1:\mu^{11}:\mu^5), (1:\mu^4:\mu^7), (1:\mu^6:\mu^5), (1:\mu:\mu^5), (1:\mu^{13}:\mu^{14}), (1:\mu^2:\mu^{13}), (1:\mu^9:\mu^7), (1:\mu^3:\mu^{14}), (1:\mu^8:\mu^3), (1:\mu^{14}:\mu^8), (1:\mu:\mu^{12}), (1:\mu^7:0), (1:\mu^8:\mu^4), (0:1:0), (1:\mu^2:0), (1:\mu^7:\mu^6), (1:\mu^4:\mu^2), (1:\mu^9:\mu^9), (1:\mu^{14}:\mu^7), (1:\mu^{11}:\mu^{12}), (1:\mu^6:\mu^{12}), (1:\mu^3:\mu^3), (1:\mu^2:\mu^6), (1:\mu^9:\mu^2), (1:\mu^4:\mu^9), (0:1:\mu^{10}), (1:\mu^{13}:\mu^4), (1:\mu^{12}:1), (1:\mu^{13}:\mu^3), (1:\mu^{11}:\mu^{11}), (1:\mu^6:\mu^{11}), (1:\mu^{12}:\mu^{13}), (1:\mu^3:\mu^4), (0:1:\mu^5), (1:\mu^8:\mu), (1:\mu:\mu^{11}), (1:\mu:\mu^{10}), (1:\mu^{14}:\mu^9) \};$

(ii) $\{ (1:\mu^{10}:\mu^{14}), (1:\mu^7:\mu^2), (1:\mu^8:\mu^{10}), (1:\mu^2:\mu^2), (1:\mu^9:\mu), (1:\mu^{14}:1), (1:\mu^9:\mu^{11}), (1:\mu^4:\mu), (1:\mu^3:0), (1:\mu^{14}:\mu^{13}), (1:\mu^2:\mu^9), (1:\mu^{13}:0), (1:\mu^4:\mu^{11}), (1:\mu^5:\mu^4), (1:\mu^3:\mu^{10}), (1:\mu^{13}:\mu^{10}), (1:1:\mu^6), (1:\mu^{12}:\mu^8), (1:\mu^{12}:\mu^7), (0:1:\mu^{11}), (1:1:\mu^{14}), (1:\mu^{10}:\mu^5), (0:1:\mu^6), (1:\mu^8:\mu^3), (1:\mu^{14}:\mu), (1:\mu^7:\mu^8), (1:\mu^{10}:\mu^4), (0:1:\mu), (0:1:0), (1:\mu^{14}:\mu^{11}), (1:1:\mu^5), (1:\mu^8:\mu^{12}), (1:\mu^7:\mu^7), (1:\mu^5:\mu^6), (1:\mu^3:\mu^3), (1:\mu^2:\mu^8), (1:\mu^{12}:\mu^9), (1:\mu^{12}:\mu^2), (1:\mu^{13}:\mu^3), (1:\mu^4:\mu^{13}), (1:1:\mu^4), (1:\mu^2:\mu^7), (1:\mu^5:\mu^{14}), (1:\mu^4:1), (1:\mu^3:\mu^{12}), (1:\mu^{13}:\mu^{12}), (1:\mu^9:\mu^{13}), (1:\mu^9:1), (1:\mu^8:0), (1:\mu^{10}:\mu^6), (1:\mu^7:\mu^9), (1:\mu^5:\mu^5) \};$

(iii) $\{ (1:\mu^7:\mu^3), (1:\mu^8:\mu^7), (1:\mu^7:\mu^4), (1:\mu^{11}:\mu^{14}), (1:\mu:\mu^{14}), (1:\mu^{11}:\mu^{10}), (1:\mu^6:\mu^{10}), (0:1:\mu^4), (1:\mu^6:\mu^{14}), (1:\mu^3:\mu^6), (1:1:\mu), (1:1:0), (1:\mu^{12}:\mu^{11}), (1:\mu^2:\mu^3), (1:\mu^{13}:\mu^6), (1:\mu^2:\mu^4), (1:\mu^{12}:\mu^8), (1:\mu^{13}:\mu^7), (1:\mu^5:\mu^{12}), (1:\mu:\mu^9), (1:\mu^{11}:\mu^2), (1:\mu^5:\mu^{13}), (1:\mu:\mu^2), (1:\mu^6:\mu^2), (1:\mu^8:\mu^5), (1:\mu^3:\mu^7), (1:\mu^{11}:\mu^9), (1:\mu^6:\mu^9), (1:\mu^7:\mu^8), (1:\mu^5:\mu), (0:1:0), (1:\mu^7:\mu^{11}), (1:\mu^5:0), (1:\mu^{10}:\mu^{12}), (1:\mu^8:1), (1:\mu^{10}:\mu^{13}), (1:\mu^2:\mu^{11}), (1:\mu^3:\mu^5), (0:1:\mu^{14}), (1:\mu^2:\mu^8), (1:\mu^{12}:\mu^4), (1:\mu^{13}:\mu^5), (1:\mu^{12}:\mu^3), (1:1:\mu^{12}), (1:\mu^{13}:1), (1:1:\mu^{13}), (1:\mu^{10}:\mu), (1:\mu^3:1), (1:\mu^{10}:0), (1:\mu:\mu^{10}), (1:\mu^8:\mu^6), (0:1:\mu^9) \};$

(iv) $\{ (1:\mu^7:\mu^3), (1:\mu^2:\mu^5), (1:\mu^7:\mu^5), (1:\mu^{14}:\mu^4), (1:\mu^5:\mu^2), (1:\mu^8:\mu^8), (1:\mu^3:\mu), (1:\mu^9:0), (1:\mu^9:\mu^6), (1:\mu^{14}:\mu^{12}), (1:\mu^{13}:\mu), (1:\mu^4:0), (1:\mu^2:\mu^3), (1:1:\mu^{11}), (1:\mu^{12}:\mu^{10}), (1:\mu^4:\mu^6), (1:\mu^5:1), (1:\mu^3:\mu^8), (1:\mu^{13}:\mu^8), (1:\mu^{12}:\mu^{14}), (1:1:\mu^7), (0:1:\mu^{11}), (1:\mu^8:\mu^9), (1:\mu^7:\mu^{10}),$

$(1 : \mu^{10} : \mu^2)$, $(0 : 1 : \mu^6)$, $(0 : 1 : \mu)$, $(0 : 1 : 0)$, $(1 : \mu^{14} : 0)$, $(1 : \mu^{10} : 1)$, $(1 : \mu^{14} : \mu^6)$, $(1 : 1 : \mu^2)$, $(1 : \mu^5 : \mu^{11})$, $(1 : \mu^8 : \mu^{13})$, $(1 : \mu^3 : \mu^9)$, $(1 : \mu^7 : \mu^{14})$, $(1 : \mu^2 : \mu^{10})$, $(1 : \mu^{13} : \mu^9)$, $(1 : \mu^{12} : \mu^5)$, $(1 : \mu^4 : \mu^{12})$, $(1 : \mu^{12} : \mu^3)$, $(1 : \mu^5 : \mu^7)$, $(1 : \mu^4 : \mu^4)$, $(1 : \mu^9 : \mu^{12})$, $(1 : 1 : 1)$, $(1 : \mu^2 : \mu^{14})$, $(1 : \mu^9 : \mu^4)$, $(1 : \mu^3 : \mu^{13})$, $(1 : \mu^{13} : \mu^{13})$, $(1 : \mu^8 : \mu)$, $(1 : \mu^{10} : \mu^{11})$, $(1 : \mu^{10} : \mu^7)$ };

(v) { $(1 : \mu^{11} : \mu^6)$, $(1 : \mu^6 : \mu^6)$, $(1 : \mu^{10} : \mu^{10})$, $(0 : 1 : \mu^2)$, $(1 : \mu : \mu^8)$, $(1 : \mu^{11} : \mu^8)$, $(1 : \mu^7 : \mu^{12})$, $(1 : \mu^4 : \mu^{10})$, $(1 : 1 : \mu^8)$, $(1 : \mu^{10} : \mu^9)$, $(1 : \mu^{11} : \mu^{13})$, $(1 : \mu^6 : \mu^{13})$, $(0 : 1 : \mu^8)$, $(1 : \mu^{13} : \mu^2)$, $(1 : \mu^{11} : \mu)$, $(1 : \mu : \mu^7)$, $(1 : \mu^{11} : 0)$, $(1 : \mu^3 : \mu^{11})$, $(0 : 1 : \mu^{12})$, $(1 : \mu^{11} : \mu^4)$, $(1 : \mu^{11} : 1)$, $(1 : \mu^{14} : \mu^{14})$, $(1 : 1 : \mu^9)$, $(1 : \mu : 0)$ }

(vi) { $(1 : \mu^{14} : \mu^5)$, $(1 : \mu^6 : 1)$, $(1 : \mu : \mu^3)$, $(0 : 1 : \mu^3)$, $(1 : \mu : \mu)$, $(1 : \mu^2 : \mu)$, $(1 : \mu^{11} : \mu^3)$, $(1 : \mu^6 : \mu^3)$, $(1 : \mu^{13} : \mu^{11})$, $(0 : 1 : \mu^7)$, $(1 : \mu^9 : \mu^5)$, $(1 : \mu^6 : \mu^7)$, $(1 : \mu^{12} : \mu)$ };

(vii) { $(1 : \mu^{10} : \mu^8)$, $(1 : \mu^{14} : \mu^3)$, $(1 : \mu^6 : \mu^8)$, $(1 : \mu^{11} : \mu^7)$, $(1 : \mu^5 : \mu^9)$, $(1 : \mu^5 : \mu^3)$, $(1 : \mu^2 : \mu^{12})$, $(1 : 1 : \mu^{10})$, $(1 : \mu^8 : \mu^2)$, $(1 : \mu^9 : \mu^{10})$, $(1 : \mu : \mu^4)$, $(1 : \mu : 1)$, $(1 : \mu^{10} : \mu^3)$, $(1 : \mu^{14} : \mu^{10})$, $(1 : \mu : \mu^{13})$, $(1 : \mu^4 : \mu^5)$, $(1 : \mu^3 : \mu^2)$, $(1 : \mu^9 : \mu^3)$, $(1 : \mu^5 : \mu^{10})$, $(1 : \mu^{12} : \mu^{12})$, $(1 : \mu^5 : \mu^8)$, $(1 : \mu : \mu^6)$, $(1 : \mu^8 : \mu^{11})$, $(1 : \mu^6 : \mu)$, $(1 : \mu^6 : 0)$, $(0 : 1 : \mu^{13})$, $(1 : \mu^4 : \mu^{14})$, $(1 : \mu^9 : \mu^{14})$, $(1 : \mu^7 : \mu)$, $(1 : \mu^6 : \mu^4)$, $(1 : \mu^4 : \mu^3)$, $(1 : 1 : \mu^3)$ }.

C.2 OG_{17}

(i) { $(1 : 8 : 0)$, $(1 : 15 : 14)$, $(1 : 3 : 3)$, $(1 : 3 : 0)$, $(1 : 10 : 6)$, $(1 : 10 : 5)$, $(1 : 15 : 15)$, $(1 : 10 : 3)$, $(1 : 12 : 8)$, $(1 : 7 : 12)$, $(1 : 7 : 11)$, $(1 : 2 : 1)$, $(1 : 4 : 4)$, $(0 : 1 : 14)$, $(1 : 16 : 7)$, $(1 : 11 : 7)$, $(1 : 1 : 14)$, $(1 : 1 : 11)$, $(1 : 11 : 8)$, $(1 : 6 : 10)$, $(1 : 8 : 16)$, $(1 : 8 : 1)$, $(1 : 13 : 13)$, $(1 : 3 : 4)$, $(1 : 9 : 8)$, $(0 : 1 : 5)$, $(1 : 6 : 2)$, $(1 : 1 : 15)$, $(1 : 1 : 2)$, $(1 : 13 : 4)$, $(1 : 15 : 10)$, $(1 : 8 : 5)$, $(1 : 12 : 3)$, $(1 : 4 : 13)$, $(1 : 2 : 7)$, $(1 : 9 : 9)$, $(1 : 16 : 13)$, $(1 : 6 : 16)$, $(1 : 3 : 12)$, $(1 : 1 : 6)$, $(1 : 9 : 14)$, $(1 : 9 : 13)$, $(0 : 1 : 0)$, $(1 : 1 : 10)$, $(1 : 16 : 3)$, $(1 : 3 : 15)$, $(1 : 13 : 9)$ };

(ii) { $(1 : 13 : 10)$, $(1 : 3 : 1)$, $(1 : 2 : 1)$, $(1 : 9 : 4)$, $(1 : 9 : 16)$, $(1 : 16 : 5)$, $(1 : 4 : 6)$, $(1 : 6 : 9)$, $(1 : 11 : 9)$, $(1 : 4 : 5)$, $(0 : 1 : 15)$, $(1 : 13 : 2)$, $(1 : 1 : 12)$, $(1 : 5 : 11)$, $(1 : 10 : 8)$, $(1 : 2 : 4)$, $(1 : 14 : 4)$, $(1 : 9 : 6)$, $(1 : 6 : 15)$, $(1 : 16 : 10)$, $(0 : 1 : 7)$, $(1 : 11 : 11)$, $(1 : 11 : 12)$, $(1 : 1 : 4)$, $(1 : 10 : 10)$, $(1 : 5 : 13)$, $(1 : 0 : 3)$, $(1 : 5 : 0)$, $(1 : 2 : 8)$, $(1 : 2 : 6)$, $(1 : 4 : 12)$, $(1 : 11 : 3)$, $(1 : 6 : 5)$, $(1 : 16 : 0)$, $(1 : 1 : 7)$, $(0 : 1 : 8)$, $(1 : 11 : 2)$, $(1 : 13 : 7)$, $(1 : 3 : 10)$, $(1 : 5 : 16)$, $(1 : 5 : 3)$, $(1 : 14 : 12)$, $(1 : 9 : 1)$, $(1 : 2 : 9)$, $(1 : 16 : 15)$, $(0 : 1 : 12)$, $(1 : 6 : 7)$ };

(iii) { $(1 : 13 : 10)$, $(1 : 3 : 2)$, $(1 : 3 : 14)$, $(1 : 10 : 5)$, $(1 : 5 : 5)$, $(1 : 5 : 6)$, $(1 : 0 : 8)$, $(1 : 7 : 10)$, $(1 : 16 : 5)$, $(1 : 16 : 8)$, $(1 : 14 : 1)$, $(0 : 1 : 1)$, $(1 : 13 : 15)$, $(1 : 13 : 12)$, $(1 : 13 : 14)$, $(1 : 8 : 14)$, $(1 : 3 : 16)$, $(0 : 1 : 2)$, $(1 : 15 : 6)$, $(1 : 3 : 4)$, $(1 : 10 : 7)$, $(1 : 7 : 15)$, $(1 : 7 : 1)$, $(0 : 1 : 6)$, $(1 : 8 : 6)$, $(1 : 10 : 12)$, $(1 : 5 : 14)$, $(1 : 5 : 12)$, $(1 : 0 : 14)$, $(1 : 12 : 16)$, $(1 : 12 : 2)$, $(1 : 4 : 0)$, $(1 : 16 : 1)$, $(0 : 1 : 9)$, $(1 : 13 : 7)$, $(1 : 15 : 0)$, $(1 : 0 : 6)$, $(1 : 12 : 7)$, $(1 : 5 : 15)$, $(1 : 10 : 0)$, $(1 : 0 : 4)$, $(1 : 14 : 10)$, $(1 : 16 : 4)$, $(1 : 16 : 16)$, $(1 : 4 : 2)$, $(1 : 11 : 4)$, $(1 : 15 : 16)$ };

(iv) { $(1 : 8 : 12)$, $(1 : 10 : 3)$, $(1 : 0 : 9)$, $(1 : 12 : 9)$, $(1 : 14 : 0)$, $(1 : 4 : 6)$, $(1 : 11 : 10)$, $(1 : 8 : 14)$, $(1 : 1 : 0)$, $(1 : 8 : 4)$, $(1 : 1 : 12)$, $(1 : 8 : 3)$, $(1 : 15 : 7)$, $(1 : 3 : 5)$, $(1 : 7 : 3)$, $(1 : 7 : 15)$, $(1 : 2 : 5)$, $(1 : 2 : 3)$, $(1 : 16 : 11)$, $(1 : 14 : 5)$, $(0 : 1 : 5)$, $(1 : 6 : 14)$, $(1 : 3 : 9)$, $(1 : 3 : 7)$, $(1 : 15 : 9)$, $(1 : 0 : 16)$, $(1 : 7 : 6)$, $(1 : 9 : 11)$, $(1 : 9 : 10)$, $(1 : 11 : 14)$, $(1 : 11 : 15)$, $(1 : 16 : 0)$, $(1 : 6 : 3)$, $(1 : 6 : 4)$, $(1 : 15 : 13)$,

$(1:3:11)$, $(1:10:14)$, $(1:12:6)$, $(1:4:16)$, $(1:14:11)$, $(1:9:12)$, $(0:1:13)$, $(1:4:14)$, $(1:4:15)$, $(1:16:2)$, $(1:1:10)$, $(1:15:16)$ };

(v) { $(1:15:12)$, $(1:0:10)$, $(1:7:13)$, $(1:2:15)$, $(1:9:0)$, $(1:11:5)$, $(1:10:4)$, $(1:2:13)$, $(1:14:14)$, $(1:1:1)$, $(1:12:12)$, $(1:7:14)$, $(1:6:0)$, $(1:13:16)$, $(1:13:3)$, $(1:5:1)$, $(1:4:11)$, $(1:8:10)$, $(1:16:12)$, $(1:13:6)$, $(1:7:9)$, $(1:2:11)$, $(1:10:13)$, $(1:11:6)$, $(1:5:2)$, $(1:6:8)$, $(1:15:3)$, $(1:6:6)$, $(1:8:11)$, $(1:14:2)$, $(0:1:3)$, $(1:9:2)$, $(1:1:13)$, $(1:5:10)$, $(1:4:9)$, $(1:1:16)$, $(1:7:5)$ };

(vi) { $(1:12:10)$, $(1:15:4)$, $(1:2:16)$, $(1:14:15)$, $(1:12:11)$, $(1:7:0)$, $(1:7:4)$, $(1:9:5)$, $(1:6:12)$, $(0:1:4)$, $(1:1:5)$, $(1:9:7)$, $(1:8:8)$, $(1:0:15)$, $(1:14:6)$, $(1:11:13)$, $(1:11:0)$, $(1:13:5)$, $(1:7:8)$, $(1:11:16)$, $(1:2:12)$, $(0:1:10)$, $(1:9:3)$, $(1:13:0)$, $(1:15:5)$, $(1:5:7)$ };

(vii) { $(1:2:14)$, $(1:5:8)$, $(1:6:13)$, $(0:1:16)$, $(1:6:11)$, $(1:15:8)$, $(1:13:1)$, $(1:0:1)$, $(1:0:12)$, $(1:4:7)$, $(1:12:13)$, $(1:14:7)$, $(1:7:2)$, $(1:10:9)$, $(1:1:3)$, $(1:0:13)$, $(1:3:8)$, $(1:10:11)$, $(1:0:2)$, $(1:7:7)$, $(1:4:10)$, $(1:14:8)$, $(0:1:11)$, $(1:8:9)$, $(1:8:7)$, $(1:10:1)$, $(1:14:9)$, $(1:2:10)$, $(1:10:2)$, $(1:2:0)$, $(1:4:3)$, $(1:8:13)$, $(1:5:9)$, $(1:0:11)$ };

(viii) { $(1:10:15)$, $(1:14:16)$, $(1:12:15)$, $(1:14:3)$, $(1:13:11)$, $(1:0:5)$, $(1:3:6)$, $(1:15:11)$, $(1:12:14)$, $(1:12:1)$, $(1:12:5)$, $(1:4:1)$, $(1:16:6)$, $(1:1:8)$, $(1:8:2)$, $(1:12:0)$, $(1:15:1)$, $(1:0:7)$, $(1:16:14)$ }.

Appendix D

MAGMA

D.1 The MAGMA language

MAGMA is an imperative programming language with in-build mathematical structures from the field of algebra and discrete mathematics. The homepage which is also a resource for help and documentation contains a free online demo:

`http://magma.maths.usyd.edu.au/magma/`

Basic structures are sets and lists. Creating and assigning these two structures can be done by

```
> set  := {1, 2, 3};
> list := [1 .. 100];
```

Here we used a console and not the demo on the website. Some basic operations we can do

```
> set; // print the set
{ 1, 2, 3 }
> list[50]; // return the element at position 50
50
> #set; // gives the cardinality of the set
3
```

Taking the union of (multiple) sets is done by the `join` function.

```
> {1, 2} join {1, 3, 5};
{ 1, 2, 3, 5 }
> &join [ {1, 2}, {1, 3, 5}, {6} ];
{ 1, 2, 3, 5, 6 }
```

Taking the intersection is done by the `meet` function. Now we give the construction our Erdős-Rényi graph is based on: a 3-dimensional vector space over $\mathbf{F}_q$ ($q = 4$ in our code).

```
> F<mu> := FiniteField(4);
> W     := VectorSpace(F, 3);
> W ! [0, 1, 0];
(    0     1     0)
> mu    := PrimitiveElement(F);
> mu^3;
1
```

Two new concepts here. By `V ! [0, 1, 0]` we construct the element $(0, 1, 0)$ in our vector space. With `F<mu>` we capture the root of the minimal-polynomial which defines $\mathbf{F}_q$ and call it `mu`. A function can return multiple values:

```
> IsPrimePower(25);
true 5 2
> _, p, n := IsPrimePower(64);
> p, n;
2 6
```

The construction of sets is almost identical to what we now from mathematics:

```
> { x : x in [2 .. 100] | IsEven(x)  and  IsSquare(x) };
{ 4, 16, 36, 64, 100 }
```

Graphs are important for our research. We will show how we constructed the example in section 1.1:

```
> V := {1 .. 6};
> E := { {1, 3}, {2, 3}, {2, 6}, {2, 5}, {3, 4}, {3, 6}, {5, 6} };
> G := Graph< V | E >;
> G;
Graph
Vertex  Neighbors

1       3 ;
2       3 5 6 ;
3       1 2 4 6 ;
4       3 ;
5       2 6 ;
6       2 3 5 ;
```

For relation testing MAGMA uses the following code:

Mathematics	MAGMA
$<$	`lt`
$\leq$	`le`
$=$	`eq`
$\geq$	`ge`
$>$	`gt`

We might want to do arithmetic with the vertices of our graph. However when a graph is created the vertex set will lose some of its structure. We make a subset of the vertex set of the graph we just constructed:

```
> T := { v : v in VertexSet(G) | Degree(v) eq 3 }; T;
{ 2, 6 }
```

Picking a vertex out of `T` and do arithmetic with it will give an error. However we know the mathematical structure the graph is created from. We can just recall that structure and ask whether elements from it are in `T`.

```
> S := { n : n in {1 .. 6} | n in T }; S;
{ 2, 6 }
> Representative(S) + 1;
3
```

A word of warning is in its place. When we let MAGMA calculate the eigenvalues it will only find the eigenvalues in the ring for which we defined the entries of the matrix. That means for the adjacency matrix (1.2) of our example we would, without instructing MAGMA, find eigenvalues -2, -1, 0 and 1. So we have to tell MAGMA the entries of the adjacency matrix are in `RealField()`, the real field $\mathbf{R}$. A trick which speeds up the calculation process for computing the eigenvalues of large matrices is given by Bosma, the code can be found in the appendix and is called `BosmaTruuk`.

D.2 Source code

This section contains the MAGMA source code which was used doing our research. The link below provides the code in a more suitable file format:

`http://www.math.leidenuniv.nl/~edeckere/thesis/`

This MAGMA code constructs the cocliques from section 6, $q \geq 3$.

```
function CreateCoclique( q )
        _, p, n := IsPrimePower(q);
        F<mu>   := FiniteField(q);
        mu      := PrimitiveElement(F);
        V       := VectorSpace(F, 3);


        if ( p eq 2 and IsEven( n ) ) then
                FF      := FiniteField( 2 ^ (n div 2) );

                S       := Set(F) diff { x^2 + x : x in F };
                s       := Representative(S);

                I       := { V ! [1, x1, x2] : x1 in F, x2 in F
                        |
                                exists(u){ lambda : lambda in
                                   FF | x2^2 + x2 + s + lambda
                                   * x1^2 eq 0 } } join
                           { V ! [0,  1, x2] :          x2 in F
                                |
                                exists(u){ lambda : lambda in
                                   FF | x2^2          + lambda
                                          eq 0 } };
        end if;



        if ( p eq 2 and IsOdd( n ) ) then
                m := (n - 1) div 2;


                // Construct S
                S := {0, 1};

                for i in [1 .. n - 2] do
```

```
                S := { rr + r * mu ^ i : rr in S, r in
                    {0, 1} };
        end for;

        // construct T
        T := {0, 1};

        for i in [1 .. m - 1] do
                T := { rr + r * mu ^ i : rr in T, r in
                    {0, 1} };
        end for;

        T := { rr + mu ^ m : rr in T};

        //
        I := { V ! [1, t, s] : t in T, s in S };
end if;



if ( p gt 2 and IsEven( n ) ) then
        _, Rootq      := IsSquare( q );
        R               := { mu ^ ((Rootq + 1) * k) : k
            in [0 .. (Rootq - 3) div 2] } join { 0 };
        I               := { V ! [1, t, (t^2 - mu*r)/2]
            : t in F, r in R } join { V ! [0, 0, 1] };
end if;



if ( p gt 2 and IsOdd( n ) ) then
        m := (n - 1) div 2;

        A := [Ceiling( p/6 ) .. Floor( p/2 )];
        B := [0 .. Floor( SquareRoot( p/3 ) )];

        if (n eq 1) then
                S       := A;
                T       := B;
        else
                // construct S
                S := [0 .. p - 1];

                for i in [1 .. n - 2] do
                        S := { rr + r * mu ^ i : rr in
                            S, r in [0 .. p - 1] };
                end for;

                S := { rr + r * mu ^ (n - 1) : rr in S,
                    r in A };

                // construct T
```

```
                        T := [0 .. p - 1];

                        for i in [1 .. m - 1] do
                                T := { rr + r * mu ^ i : rr in
                                    T, r in [0 .. p - 1] };
                        end for;

                        T := { rr + r * mu ^ m : rr in T, r in
                            B};
                end if;

                I := { V ! [1, t, s] : t in T, s in S };
        end if;



        return I;
end function;
```

MAGMA code with several functions, most of them have an (in)direct relation to ER_q.

```
// A function which returns all the prime powers between m and
   mm
function PrimePowers(m, mm)
        return [ n : n in [m .. mm] | IsPrimePower(n) ];
end function;



// Some functions about adjacency for ERq using the
   innerproduct of ERq*
function BilinearForm( PuntA, PuntB )
        return PuntA[1] * PuntB[3] - PuntA[2] * PuntB[2] +
           PuntA[3] * PuntB[1];
end function;



function Adjacent( PuntA, PuntB )
        return BilinearForm( PuntA, PuntB ) eq 0;
end function;



function IsAbsolute( Punt )
        t       := BilinearForm( Punt, Punt );

        return t eq 0;
end function;
```

```
function IsExternal( Punt )
        t       := BilinearForm( Punt, Punt );

        return t ne 0 and IsSquare(-t);
end function;



function IsInternal( Punt )
        t       := BilinearForm( Punt, Punt );

        return t ne 0 and (not IsSquare(-t));
end function;



// Functions related to (co)clique testing, the first is for
   any graph, the second is dedicated for
// elements in VectorSpace(Fq, 3)
function IsClique(C)
        return forall(u, v){ <u, v> : u, v in C | u eq v  or  u
            adj v};
end function;



function IsIndependentSet(I)
        return forall(u, v){ <u, v> : u, v in I | u eq v  or  u
            notadj v};
end function;



function IsCliqueFast(C)
        return forall(u, v){ <u, v> : u, v in C | u eq v  or
           Adjacent(u, v) };
end function;



function IsIndependentSetFast(I)
        return forall(u, v){ <u, v> : u, v in I | u eq v  or
           not Adjacent(u, v) };
end function;



// Two functions who return ERq and the orthogonality subgraph
function NormPoints(q)
        F<mu>   := FiniteField(q);
        mu      := PrimitiveElement(F);
        W       := VectorSpace(F, 3);
```

```
        return { Normalize(w) : w in W | w ne 0 }, mu;
end function;



function ER_Graph( q )
        V       := NormPoints(q);
        E       := { {u, v} : u in V, v in V | u ne v  and
            Adjacent(u, v) };

        return Graph< V | E >;
end function;



function Ortho_Graph( q )
        V       := NormPoints(q);
        V       := { v : v in V | not IsAbsolute(v) }; //
            filter the absolute points out of V
        E       := { {u, v} : u in V, v in V | u ne v  and
            Adjacent(u, v) };

        return Graph< V | E >;
end function;



function ExternalPointGraph(q);
        V       := NormPoints(q);
        V       := { v : v in V | IsExternal(v) }; // filter
            the non-external points out of V
        E       := { {u, v} : u in V, v in V | u ne v  and
            Adjacent(u, v) };

        return Graph< V | E >;
end function;



function InternalPointGraph(q);
        V       := NormPoints(q);
        V       := { v : v in V | IsInternal(v) }; // filter
            the non-internal points out of V
        E       := { {u, v} : u in V, v in V | u ne v  and
            Adjacent(u, v) };

        return Graph< V | E >;
end function;
```

```
// A trick bij W. Bosma (Radboud University) for finding the
   eigenvalues of a matrix
function BosmaTruuk(M);
        C                       := CharacteristicPolynomial(M);
        eigenval        := Roots(C, RealField(10));

        return Sort(eigenval);
end function;
```

The two methods from section 7, q must be odd. The functions return the independent set itself.

```
// for a subset of the vertex set which is a cycle (>= 3 or
   equal 1) it returns the maximum independent set.
function CycleCoclique(C)
        if #C eq 1 then
                Answ    := C;
        else
                v       := Representative(C);   // pick a
                   vertex out of the vertex-set of C
                Answ    := { v };
                C       := C diff (Neighbours(v) join {v}); //
                   remove v and its two neighbours out of C

                while #C gt 0 do
                        _       := exists(w){ w : w in C | #(
                           Neighbours(w) meet C) le 1 }; //
                           finds an element in C which has
                           degree
                        // 0 or 1. Watch out, it find the
                           element in C, not in G as in G the
                           degree will always be 2.
                        C       := C diff (Neighbours(w) join {
                           w});
                        Answ    := Answ join { w };
                end while;
        end if;

        return Answw;
end function;



function Method1(q)
        F<mu>   := FiniteField(q);
        mu      := PrimitiveElement(F);
        W       := VectorSpace(F, 3);

        // Construct our biggest R
        V       := { y : y in F | not IsSquare(y) };
        E       := { {y, z} : y, z in V | not IsSquare(y + z)
           and  y ne z };
        G       := Graph< V | E >;
```

```
        if Order(G) eq 0 then
                RR      := {};
        else
                RR      := MaximumClique(G);
        end if;

        // Find a largest independent set
        R       := { r : r in V | r in RR };
        I       := { W ! [1, t, (t^2 - r)/2] : t in F, r in R
            join {0} } join { W ! [0, 0, 1] };

        if not IsSquare(F ! 2) then
                GI      := Graph< I | { {u, v} : u, v in I | u
                    ne v  and  Adjacent(u, v) } >;
                Temp    := &join [ CycleCoclique(Comp) : Comp
                    in Components(GI) ];
                I       := { v : v in I | v in Temp };
        end if;

        return I;
end function;



function Method2(q)
        F<mu>   := FiniteField(q);
        mu      := PrimitiveElement(F);
        W       := VectorSpace(F, 3);

        // Construct candidate subsets R
        V       := { y : y in F | not IsSquare(1 - 1*y) and y
            ne 0 }; // we assume 1 is in R.
        E       := { {y, z} : y, z in V | not IsSquare(1 - y*z)
             and y ne z };
        G       := Graph< V | E >;

        A       := AllCliques(G);

        // find a largest independent set
        MaxI    := {};

        for RR in A do
                R       := { x : x in V | x in RR } join { 1 };
                R1      := { x : x in R | not IsSquare(1 - x^2
                    ) or x eq 1 };   // these elements satisfy
                    our criteria
                R2      := R diff R1;
                I_A     := { W ! [1, t, r * t^2 / 2] : t in F,
                    r in R1 };
                I_B     := {};
```

```
                for r in R2 do
                        _, ra           := IsSquare(1 - r^2);
                        keyElem := (1 + ra)/r;
                        ora             := Order(keyElem);

                        Z               := ora mod 2;   //
                            replaces an if-then-else (on even/
                            odd) construction
                        Cykel           := { keyElem ^ (2*i +
                            1) : i in [0 .. (ora - Z)/2 - 1] };
                            // create one cykel
                        Cykels  := [ { mu ^ j * x : x in Cykel
                            } : j in [0 .. (#F - 1)/ora - 1] ];
                            // create all cykels

                        union   := &join Cykels;

                        I_Bb    := { W ! [1, t, r*t^2/2] : t in
                             union }; // create with current r
                            the subset
                        I_B     := I_B join I_Bb;
                end for;

                I       := I_A join I_B join {W ! [0, 0, 1]};

                if #I gt #MaxI then
                        MaxI    := I;
                end if;
        end for;

        return MaxI;
end function;
```

Three heuristics which work for any graph. The first algorithm finds a large clique, it returns the clique set it self. The second algorithm finds a large independent set. The third algorithm performs sequential coloring and only returns the coloring number. The user can, by passing a number of seconds to it, decide how long the algorithm will run. 60 seconds is a good starting point.

```
function SequentialClique(G, seconds)
        V       := Set(VertexSet(G));
        best    := [ Representative(V) ]; // a clique (of size
            1) to start with.
        t       := Cputime();

        while (Cputime(t) le seconds) do
                perm            := Random(Sym(V)); // Random
                    permutation
                W               := [ v ^ perm : v in V ]; //
                    Random permutation of the vertices
                clique  := [ W[1] ];
                counter := 2;
```

```
                while (counter le #V) do
                        // Tests wetter the sellected (by
                           counter) vertex in the sequence W is
                            adjacent
                        // to any other vertex in the
                           independent set
                        if forall{ w : w in clique | w adj W[
                           counter] } then
                                Append(~clique, W[counter]);
                        end if;

                        counter := counter + 1;
                end while;

                if (#clique gt #best) then
                        best    := clique;
                end if;
        end while;

        return Set(best);
end function;




function SequentialCoclique(G, seconds)
        I       := SequentialClique(Complement(G), seconds);

        return Set({ v : v in VertexSet(G) | v in I });
end function;




function SequentialColoring(G, seconds)
        V       := Set(VertexSet(G));
        best    := #V;  // The best number of colors to start
           with
        t       := Cputime();

        while Cputime(t) le seconds do
                perm            := Random(Sym(V)); // Random
                   permutation
                W               := [ v ^ perm : v in V ]; //
                   Random permutation of the vertices
                Colors  := [1];
                MaxColors       := 1;

                while (MaxColors lt best  and  #Colors lt #V)
                   do
                        // Set of the non-available colors
```

```
                        NonAvailable    := Set([ Colors[j] : j
                            in [1 .. #Colors] | W[#Colors + 1]
                            adj W[j] ]);
                        // Set of the available colors
                        Available               := {1 ..
                            MaxColors} diff NonAvailable;

                        if IsEmpty(Available) then
                                MaxColors := MaxColors + 1;
                                Append(~Colors, MaxColors);
                        else
                                Append(~Colors, Minimum(
                                    Available));
                        end if;
                end while;

                best := Minimum(best, MaxColors);
        end while;

        return best;
end function;
```

Notation index

Sets

$\emptyset$ The empty set.

$|S|$ If S is a finite set then $|S|$ is the number of elements in S.

$U \backslash S$ The set $\{u \in U : u \notin S\}$.

S^c Given S as a subset of a larger set U then S^c is the complement of S in U. That is $S^c = \{u \in U : u \notin S\}$.

$\mathrm{Sym}(X)$ The set of all bijections $X \longrightarrow X$.

$\mathrm{Sym}(n)$ The set of all bijections $\{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$.

Numbers

$\lceil r \rceil$ The ceiling of a real number r. That is the smallest integer n such that $r \leq n$.

$\lfloor r \rfloor$ The floor of a real number r. That is the largest integer n such that $r \geq n$.

$\overline{z}$ The complex conjugate of a complex number z.

Algebra

$\mathbf{F}$ Field.

$\mathbf{R}$ Field of real numbers.

$\mathbf{C}$ Field of complex numbers.

$\mathbf{F}_q$ Finite field of q elements.

$\mathbf{F}^*$ The group of units. That is the set of all non-zero x in the field $\mathbf{F}$.

$\overline{\mathbf{F}}$ The algebraic closure of the field $\mathbf{F}$.

G/H The ***factor group*** of G and a normal subgroup H.

$\rtimes$ The ***semi-direct product***.

Graphs

$\overline{G}$ Graph complement. The graph $\overline{G}$ has the same vertex set V as G but now any two vertices $u, v \in V$ are adjacent if and only if they are not adjacent in G.

$\mathrm{Aut}(G)$ The automorphism group of a graph.

$i \sim j$ Vertex i is adjacent to vertex j.

ER_q The Erdős-Rényi graph.

ER_q^* The Erdős-Rényi graph with a different bilinear form.

ER_q^o The Erdős-Rényi graph with loops to the absolute vertices.

OG_q The orthogonality graph.

$\mathcal{R}$ The absolute points.

$\mathcal{L}$ The external points.

$\mathcal{M}$ The internal points.

$G\mathcal{L}_q$ The graph induced by all the external points.

$G\mathcal{M}_q$ The graph induced by all the internal points.

$\Delta(G)$ The maximum degree of a vertex in G.

$\alpha(G)$ The size of the largest independent set in G.

$\omega(G)$ The size of the largest clique in G.

$\gamma(G)$ The chromatic number of G.

C_n Cycle of n vertices.

$G - v$ The subgraph of $G = (V, E)$ induced by the vertices $V \backslash \{v\}$.

$\lambda_i(G)$ The ith eigenvalue of a graph G where $\lambda_1(G)$ is the largest eigenvalue and $\lambda_n(G)$ the smallest.

Linear Algebra

$U^\perp$ The orthogonal complement of a subspace $U \subseteq W$.

e_i The vector with the ith entry equal to 1 and the other entries equal to 0.

J Matrix where every entry equals 1.

$U + S$ When $U, S \subseteq W$ are subspaces then the sum $U + S$ is the set $\{u + s : u \in U, s \in S\}$.

$U \oplus S$ When $U, S \subseteq W$ are subspaces and $U + S = W$ and $U \cap S = 0$ then $U \oplus S$ is notation for W. We call $U \oplus S$ the ***direct sum***.

M^T The transposed of a matrix M.

$\langle \cdot, \cdot \rangle$ Bilinear form.

$U \perp S$ U is orthogonal to S.

$\overline{M}$ The matrix by taking the complex conjugate of all the entries in M.

$\langle U \rangle$ For a subset U of a vector space this is the set of all linear combinations of every finite subset of U. We will occasionally omit the set brackets.

Projective Planes

$PG(2, q)$ The projective plane where points are defined by 1-dimensional subspaces of $\mathbf{F}_q^3$ and lines by 2-dimensional subspaces of $\mathbf{F}_q^3$.

Bibliography

[1] M. Aigner and G.M. Ziegler. *Proofs from The Book*. Springer, 3rd edition, 2004.

[2] R. Baer. Polarities in finite projective planes. *Bulletin of the American Mathematical Society*, 52:77–93, 1946.

[3] M. R. Garey, D. S. Johnson, and L. Stockmeyer. Some simplified NP-complete graph problems. *Theoretical Computer Science*, 1:237–267, 1976.

[4] C. Godsil and G. Royle. *Algebraic Graph Theory*. Springer, 2001.

[5] C.D. Godsil and M.W. Newman. Eigenvalue bounds for independent sets. *Journal of Combinatorial Theory*, 98:721–734, 2008.

[6] B. Gorissen. Exploring the relation between ranks and graph coloring. 2008. BSc thesis.

[7] W.H. Haemers. *Eigenvalue techniques in design and graph theory*. PhD thesis, 1980.

[8] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford University Press, 2nd edition, 1998.

[9] D.R. Hughes and F.C. Piper. *Projective Planes*. Springer-Verlag, 1973.

[10] A.W. Knapp. *Basic Algebra*. Birkhäuser, 2006.

[11] S. Lang. *Algebra*. Springer, revised 3rd edition, 2004.

[12] D.C. Lay. *Linear Algebra and its applications*. Addison-Wesley, 2nd edition, 2000.

[13] B.D. McKay. Practical graph isomorphism. *Congressus Numerantium*, 30:45–87, 1981.

[14] D. Mubayi and J. Williford. On the independence number of the Erdős-Rényi graph and projective norm graphs and a related hypergraph. *Journal of Graph Theory*, 56:113–127, 2007.

[15] T.D. Parsons. Graphs from projective planes. *Aequationes Mathematicae*, 14(1-2):167–189, 1976.

[16] S. Roman. *Advanced Linear Algebra*. Springer, 2nd edition, 2005.

[17] A. Schrijver. *Combinatorial Optimization*. Springer, 2003.

[18] J. Williford. *Constructions in Finite Geometry with applications to Graphs*. PhD thesis, 2004.