ON THE INDEPENDENCE NUMBER OF THE ERDŐS-RÉNYI AND PROJECTIVE NORM GRAPHS AND A RELATED HYPERGRAPH

DHRUV MUBAYI* AND JASON WILLIFORD

Abstract. The Erdős-Rényi and Projective Norm graphs are algebraically defined graphs that have proved useful in supplying constructions in extremal graph theory and Ramsey theory. Their eigenvalues have been computed and this yields an upper bound on their independence number. Here we show that in many cases, this upper bound is sharp in order of magnitude.

Our result for the Erdős-Rényi graph has the following reformulation: the maximum size of a family of mutually non-orthogonal lines in a vector space of dimension three over the finite field of order q is of order $q^{3/2}$.

We also prove that every subset of vertices of size greater than $q^2/2 + q^{3/2} + O(q)$ in the Erdős-Rényi graph contains a triangle. This shows that an old construction of Parsons is asymptotically sharp. Several related results and open problems are provided.

1. Introduction

The independence number $\alpha(G)$ of a graph or hypergraph G is the maximum size of a subset of vertices of G that contains no edge. The eigenvalues of the adjacency matrix of a graph provide an upper bound on its independence number. The aim of this paper is to examine the tightness of these bounds when applied to several well-known families of graphs. The particular graphs considered are the Erdős-Rényi and Projective Norm graphs, and various subgraphs of these. We also consider a related hypergraph obtained from the Erdős-Rényi graph that has recently proved useful in extremal hypergraph theory.

Given a graph G and any set $I \subset V(G)$ let $e(I, I)$ be the number of ordered pairs of vertices in I which are adjacent. The aforementioned eigenvalue bound, found, for example, in [4], gives the following.

Theorem 1. *Let λ be the second largest eigenvalue in absolute value of the adjacency matrix of a d-regular graph G (possibly with loops) with n vertices. Then $|e(I, I) - \frac{d}{n}|I|^2| \leq \lambda|I|$. In particular, if I contains no edges, except for possibly loops, then $|I| \leq (\lambda + 1)n/d$.*

1.1. The Projective Norm Graphs.

Let $t > 1$ be a positive integer, F_q be the finite field of order q and F_q^* be the multiplicative group of F_q. The *norm* from $F_{q^{t-1}}$ to F_q is the function $N : F_{q^{t-1}} \to F_q$ defined by $N(X) = X^{1+q+\cdots+q^{t-2}}$.

*Research supported in part by National Science Foundation grant DMS-0400812, and an Alfred P. Sloan Research Fellowship.

Definition. Fix an integer $t \geq 2$ and a prime power q. The Projective Norm graph $G = G_{q,t}$ has vertex set $V(G) = F_{q^{t-1}} \times F_q^*$ with two vertices $(A, a), (B, b) \in V(G)$ adjacent when $N(A + B) = ab$.

For a graph G let $ex(n, G)$ deonte the largest number of edges of any graph on n vertices which has no copy of G as a subgraph. Let $R_k(G_1, \ldots, G_k)$ denote the smallest integer n such that any edge coloring in k colors of K_n must contain an i colored copy of G_i for some $1 \leq i \leq k$, and let $R_k(G) = R_k(G, \ldots, G)$. The graphs $G_{q,t}$ were first constructed by Alon, Rónyai and Szabó to give improved lower bounds for the Turán function $ex(n, K_{t,s})$ and the Ramsey numbers $R_k(K_{t,s})$ where $t \geq 2$ and $s \geq (t-1)! + 1$ (see [3]). In [22] T. Szabó found the eigenvalues of $G_{q,t}$ to be $\pm q^{(t-1)/2}, \pm 1, 0$ and $q^{t-1} - 1$. This was done independently by Alon and Rödl in [2], who used these eigenvalues to provide tight bounds for $R_k(K_{t,s}, \ldots, K_{t,s}, K_m)$ where again $t \geq 2$ and $s \geq (t-1)! + 1$ (see [3]).

The projective norm graph $G_{q,t}$ has $n = q^t - q^{t-1}$ vertices, and degree $q^{t-1} - 1$. Using the results of [2, 22] for its eigenvalues and Theorem 1, we obtain for fixed $t \geq 2$

$$\alpha(G_{q,t}) \leq \frac{(q^t - q^{t-1})(q^{(t-1)/2} + 1)}{q^{t-1} - 1} = (1 + o(1))q^{(t+1)/2} \qquad \text{as } q \to \infty. \tag{1.1}$$

Our first result shows that (1.1) gives the correct order of magnitude for all odd t.

Theorem 2. *Let $t > 1$ be an odd integer and q an odd prime power. Then*

$$\alpha(G_{q,t}) \geq \frac{q^{(t+1)/2} - q^{(t-1)/2}}{2}.$$

Thus as $q \to \infty$,

$$(1/2 + o(1))q^{(t+1)/2} < \alpha(G_{q,t}) < (1 + o(1))q^{(t+1)/2}.$$

The problem of determining whether (1.1) is sharp for even t seems to be more difficult.

Open Problem 1. Find a construction of an independent set of size $Cq^{(t+1)/2}$, C a constant, for even values of $t > 2$ or q a power of 2.

1.2. **The Erdős-Rényi Graph.** We will pay special attention to the Projective Norm graphs in the case $t = 2$. The graph $G_{q,2}$ is a large induced subgraph of a well-known graph called the Erdős-Rényi graph which we denote ER_q. Since the graph ER_q is of independent interest, we begin by explaining its construction and connection to $G_{q,2}$.

Let q be a prime power and V be a 3-dimensional vector space over a finite field F_q. The projective geometry $PG(2, q)$ is the triple $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ where $\mathcal{P}$ is the set of all 1-dimensional subspaces of V which we call points, $\mathcal{L}$ is the set of all 2-dimensional subspaces which we call lines, and the incidence relation $\mathcal{I}$ is containment. Points of $PG(2, q)$ will be represented by left-normalized vectors, vectors whose left-most non-zero entry is 1, and which span the 1-dimensional space in question. Similarly lines will be represented by left-normalized vectors which span the orthogonal complement of the corresponding 2-dimensional subspace of V. We use round brackets for points and square brackets for lines to avoid confusion. Therefore a point (x_0, x_1, x_2) is on a line $[y_0, y_1, y_2]$ if and only if $x_0y_0 + x_1y_1 + x_2y_2 = 0$. A *polarity* ϕ of a projective plane $PG(2, q)$ is a bijective map from $\mathcal{P} \cup \mathcal{L}$ to itself that maps

points to lines and lines to points and reverses incidence (meaning $p \in l$ if and only if $\phi(l) \in \phi(p)$) and with the property that ϕ^2 is the identity map on π. A point p is called absolute with respect to the polarity ϕ if $p \in \phi(p)$. The *polarity graph* of $PG(2,q)$ with respect to a polarity ϕ is the simple graph (V,E) with vertex set equal to $\mathcal{P}$ such that for $x,y \in \mathcal{P}$ with $x \neq y$, $\{x,y\} \in E$ if and only if $x \in \phi(y)$. (It should be noted that polarity graphs can alternately be defined with loops at each of the absolute points).

The projective plane $PG(2,q)$ is known to have the orthogonal polarity $\phi_o : (x_0,x_1,x_2) \mapsto [x_0,x_1,x_2]$ and if q is a perfect square the unitary polarity $\phi_u : (x_0,x_1,x_2) \mapsto [x_0^{\sqrt{q}},x_1^{\sqrt{q}},x_2^{\sqrt{q}}]$. Any other polarity of $PG(2,q)$ is projectively equivalent to one of these forms (see [18]).

Definition. For q a prime power, the Erdős-Rényi graph ER_q is the orthogonal polarity graph of $PG(2,q)$. Formally, the vertex set of ER_q is the set of points of $PG(2,q)$ with two distinct vertices (x_0,x_1,x_2) and (y_0,y_1,y_2) adjacent if and only if $x_0y_0+x_1y_1+x_2y_2 = 0$. We define ER_q^o to be the graph ER_q with loops attached to the absolute points.

The graph ER_q was introduced in this form by Erdős and Rényi in [8] to give constructive examples of graphs with small maximum degree, relatively few edges and diameter 2. The graph ER_q plays a notable role in extremal graph theory. Recall that if G is a graph, $ex(n,G)$ denotes the greatest number of edges a graph on n vertices can have without containing G as a subgraph. Any graph on n vertices with $ex(n,G)$ edges and which has no copy of G as a subgraph is called extremal. The asymptotic behavior of $ex(n,G)$ is well understood if G is not bipartite; however, very little is known when G is bipartite (see [5] and [10] and the references therein). Of particular interest is the behavior of $ex(n,C_{2k})$ where C_{2k} denotes a cycle of length 2k. In [9] Erdős, Rényi and Sós proved that $ex(n,C_4)$ is asymptotic with $\frac{1}{2}n^{3/2}$ using the graphs ER_q for constructive lower bounds (this was done independently by Brown in [6]). Füredi later demonstrated in [12], [13] and [14] that the graphs ER_q are extremal. Such exact results are relatively rare in extremal graph theory. The graph ER_q has also been used to solve a similar problem for hypergraphs (see [19]). These hypergraphs will be dealt with in the last section.

Many of our results require algebraic manipulations for which ER_q is not suited. This leads us to the following

Definition. For q an odd prime power, ER_q^* is the graph whose vertex set is $V(ER_q)$ with two vertices (x_0,x_1,x_2) and (y_0,y_1,y_2) adjacent if and only if $x_0y_2 - x_1y_1 + x_2y_0 = 0$.

Several of our calculations will be aided by the following fact:

Proposition 3. *The graph ER_q^* is isomorphic to ER_q.*

The connection between the projective norm graph $G_{q,2}$ and ER_q is given by the following Proposition.

Proposition 4. *The graph $G_{q,2}$ is isomorphic to an induced subgraph of ER_q.*

ER_q has q^2+q+1 vertices while $G_{q,2}$ has q^2-q. As $G_{q,2}$ is an induced subgraph of ER_q missing $2q+1$ of the vertices of ER_q, their independence numbers are equal up to a linear (in q) error term. The question of determining the independence

number of ER_q can be phrased as a simple question about vector spaces which seems independently interesting:

What is the maximum number of mutually non-orthogonal 1-dimensional subspaces of a 3-dimensional vector space over F_q?

The eigenvalues of ER_q^o are well known to be $\pm\sqrt{q}, q+1$ (see [1]). It is clear that the maximum size of a set of vertices of ER_q^o with no edges except for possibly loops is equal to $\alpha(ER_q)$. From Theorem 1, and noting that there are $q+1$ loops in ER_q^o, we obtain $\alpha(ER_q) \leq q^{3/2}+q+\frac{\sqrt{q}+1}{q+1}$. Since one of our results will be close to exact, we will introduce a bound due to Hoffman (see [17]) which is sharper than Theorem 1 with respect to lower order terms. However, this bound only bounds the size of the largest independent set which has no loops, so we must add the number of loops to the result. This bound states that if λ is the smallest eigenvalue of the adjacency matrix of a d-regular n-vertex graph G, then

$$\alpha(G) \leq \frac{-n\lambda}{d-\lambda}$$

In the case of ER_q we must add $q+1$ to the bound, which after simplification gives us:

$$\alpha(ER_q) \leq q^{3/2}+\sqrt{q}+1$$

Godsil and Newman generalize this bound if a restricted number of absolute points are allowed, see [15] for details. We will establish that the Hoffman bound gives the correct magnitude for $\alpha(ER_q)$.

Theorem 5. *Let p be a prime, n a positive integer and $q=p^n$. Then*

$$\alpha(ER_q) \geq \begin{cases} \frac{q^{3/2}+q+2}{2} & \text{for } p \text{ odd, } n \text{ even} \\ \frac{120q^{3/2}}{73\sqrt{73}} & \text{for } p \text{ odd, } n \text{ odd} \\ \frac{q^{3/2}}{2\sqrt{2}} & \text{for } p=2, \ n \text{ odd} \\ q^{3/2}-q+\sqrt{q} & \text{for } p=2, \ n \text{ even} \end{cases}$$

In all cases, $\alpha(ER_q) \geq \frac{120q^{3/2}}{73\sqrt{73}} > .19239\, q^{3/2}$.

For even powers of 2 we can state exactly the size of the largest independent set which contains no absolute points.

Theorem 6. *Let q be an even power of 2. Then the size of the largest independent set of ER_q containing no absolute vertex is $q^{3/2}-q+\sqrt{q}$.*

Given the level of precision in the previous result, it is natural to ask the following:

Open Problem 2. Construct an independent set I in ER_q for all q which are not even powers of two such that $|I| = q^{3/2}+O(q)$, or prove that no such set exists.

1.3. **The Polarity Graph U_q.** We next consider a graph closely related to ER_q whose independence number can be found exactly for all q which are even powers of primes.

Definition. Let q be a square prime power. The *unitary polarity graph* U_q of $PG(2,q)$ is the graph with vertex set $V(ER_q)$ with two vertices (x_0,x_1,x_2) and (y_0,y_1,y_2) adjacent if and only if $x_0y_0^{\sqrt{q}}+x_1y_1^{\sqrt{q}}+x_2y_2^{\sqrt{q}}=0$.

As stated earlier, the graph U_q is the only other polarity graph which $PG(2,q)$ admits. U_q is similar to ER_q in that it has no 4-cycles and has diameter 2 (see [23] for a similar argument for ER_q). However, it has fewer edges than ER_q and so does not play the same role in extremal graph theory. Consequently, U_q is not as well known as ER_q. As in ER_q, there are absolute points. The graph formed by deleting the absolute vertices of U_q will be denoted by U_q^-. U_q has precisely $q^{3/2}+1$ such absolute points, and these form an independent set in the graph U_q. We will show that this is the unique maximum independent set of U_q. This is in stark contrast to the graph ER_q for which exact results remain elusive. To get the level of precision necessary in the upper bound of $\alpha(U_q)$ we will use a combinatorial bound as opposed to eigenvalue methods.

Theorem 7. *Let q be a prime power. Then $\alpha(U_q) = q^{3/2}+1$, with the set of absolute points being the unique independent set of size $q^{3/2}+1$.*

It is interesting to note that the largest independent set in U_q consists of all the absolute points of U_q, while the best construction for ER_q contains no absolute points. With the independence number of U_q resolved, it would be interesting to see what is the magnitude of the largest independent set I of U_q^- (which contains no absolute points). Using the Hoffman bound and the fact that U_q has the same eigenvalues as ER_q, we have the inequality

$$\alpha(U_q^-) \leq q^{3/2} - q + \sqrt{q}.$$

From direct computation, this bound is not tight. For $q = 4, 9$ we have upper bounds of 6 and 21 while $\alpha(U_4^-) = 4$ and $\alpha(U_9^-) = 19$. A better upper bound and new constructive techniques are required to see if the size of I can also be found exactly as $\alpha(U_q)$.

1.4. **The Erdős-Rényi Hypergraph of Triangles.** In [19] Lazebnik, and Verstraëte (using an idea of Lovász) construct a series of hypergraphs $\mathcal{H}_q$ of girth 5. These hypergraphs are used to determine the asymptotics of the Turán number $T_3(n,8,4)$, defined as the maximum number of edges in a 3-graph on n vertices in which no set of 8 vertices spans more than 4 edges.

Definition. Let q be an odd prime power. $\mathcal{H}_q$ is the 3-graph whose vertex set is the set of nonabsolute points of $V(ER_q)$ and edge set is the set of triangles in ER_q.

It is apparent from the construction of $\mathcal{H}_q$ that $\alpha(\mathcal{H}_q)$ is the order of the largest triangle-free induced subgraph of ER_q which contains no absolute points. In [21] Parsons constructs such a subgraph which has $\binom{q+1}{2}$ vertices if $q \equiv 3 \ (mod\ 4)$ and $\binom{q}{2}$ vertices if $q \equiv 1 \ (mod\ 4)$ (Parsons' aim was to study the automorphism groups of these subgraphs). We will show that Parsons' construction is asymptotically tight using eigenvalue techniques.

Theorem 8. *Let q be an odd prime power. Then $\alpha(\mathcal{H}_q) \leq q^2/2 + q^{3/2} + O(q)$. Thus in particular,*

$$\alpha(\mathcal{H}_q) = (1/2 + o(1))q^2.$$

Having shown that Parson's graphs are asymptotically tight, we conjecture the following.

Conjecture 1. Let q be an odd prime power. Then $\alpha(\mathcal{H}_q) = \binom{q}{2}$ if $q \equiv 1 \,(mod\ 4)$ and $\alpha(\mathcal{H}_q) = \binom{q+1}{2}$ if $q \equiv 3 \,(mod\ 4)$.

The only constructions known of size roughly $q^2/2$ are for odd q.

Open Problem 3. Let q be a power of 2. Find an induced subgraph of ER_q which is triangle free and has at least $q^2/2 + O(q^{3/2})$ vertices.

The proofs of all stated results are in the following sections, labelled according to the graphs they pertain to.

2. The Projective Norm Graph $G_{q,t}$

Proof of Theorem 2. Recall that $t > 1$ is odd, q is an odd prime power, and we are to show that $\alpha(G_{q,t}) \geq \frac{q^{(t+1)/2} - q^{(t-1)/2}}{2}$. Let μ be a primitive element of $F_{q^{t-1}}$ and set

$$E = \{\mu^{s(q^{(t-1)/2}+1)} : s \in [1, q^{(t-1)/2} - 1]\} \cup \{0\}.$$

Since $t-1$ is even, there is a subfield $F_{q^{(t-1)/2}}$ of $F_{q^{t-1}}$ which consists of those $x \in F_{q^{t-1}}$ which satisfy $x^{q^{(t-1)/2}} = x$. It is easy to verify this property for elements of E and therefore E is closed under addition. One also notes that every element x of E is a square in $F_{q^{t-1}}$ since x is 0 or $x = (\mu^{s(q^{(t-1)/2}+1)/2})^2$ for some $s \in [1, q^{(t-1)/2} - 1]\}$. Let $S = \{\mu x : x \in E\}$ and let T be the set of all nonzero squares in F_q. We will show that $I = S \times T$ is an independent set in $G_{q,t}$.

First observe that S is closed under addition because E is, and every element of S is a nonsquare as it is the product of μ and a square. Also, T is closed under multiplication as the product of two nonzero squares in F_q is a nonzero square in F_q. Let $A, B \in S$ and $a, b \in T$. Then $A + B$ is a nonsquare in $F_{q^{t-1}}$ and therefore $N(A+B)$ is a nonsquare in F_q. As ab is a square in F_q, we must have $N(A+B) \neq ab$ and therefore I is an independent set of size $|S||T| = q^{(t-1)/2}(q-1)/2 = (q^{(t+1)/2} - q^{(t-1)/2})/2$.

□

3. The Erdős-Rényi Graph ER_q

In this section we completely prove Theorem 5. We begin be proving Propositions 3 and 4, both of which are needed in the proof of Theorem 5.

Proof of Proposition 3. We must show that ER_q^* is isomorphic to ER_q, where ER_q^* is the graph with the same vertex set as ER_q but with two vertices x and y connected when $x_0y_2 - x_1y_1 + x_2y_0 = 0$.

We need a change of basis of V which transforms the form $x_0y_0 + x_1y_1 + x_2y_2 = 0$ into $x_0y_2 - x_1y_1 + x_2y_0 = 0$. This requires a 3 by 3 matrix C where $CMC^T = \lambda I, \lambda \in F_q, \lambda \neq 0$, where $M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. We explicitly give matrices C satisfying these properties.

If q is a power of 2, we use the matrix $C_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$. If q is odd, let a, b, c, d, i be such that $a^2 = -2, b^2 = 2, c^2 + d^2 = -1, i^2 = -1$ (when they exist). We use

the following change of variables for $q \equiv 1 \pmod 4$ and $q \equiv 3, 7 \pmod 8$ which we label C_1, C_3, C_7 respectively:

$$C_1 = \begin{pmatrix} \frac{(1+i)}{2} & 0 & \frac{(1-i)}{2} \\ 0 & i & 0 \\ \frac{(-1+i)}{2} & 0 & -\frac{(1+i)}{2} \end{pmatrix} C_3 = \begin{pmatrix} \frac{a}{2} & a & \frac{a}{2} \\ -1 & -1 & -1 \\ \frac{-a}{2} & 0 & \frac{a}{2} \end{pmatrix} C_7 = \begin{pmatrix} \frac{1}{b} & 0 & \frac{1}{b} \\ \frac{-d}{b} & c & \frac{d}{b} \\ \frac{c}{b} & d & \frac{-c}{b} \end{pmatrix}$$

□

Proof of Proposition 4. We must show that $G_{q,2}$ is isomorphic to a subgraph of ER_q. Recall that $G_{q,2}$ has vertex set $V(G) = F_q \times F_q^*$ with two vertices $(A, a), (B, b) \in V$ adjacent when $N(A + B) = ab$. As the norm from F_q to itself is trivial, the norm may be omitted and we have that two vertices are connected when $A + B = ab$. Having established that ER_q and ER_q^* are isomorphic, now take the set W of vertices of ER_q^* of the form $(1, x_1, x_2)$ where $x_1 \neq 0$. Let H_q be the subgraph of ER_q^* induced by W. We form a map $\phi : H_q \to G_{q,2}$ defined by $\phi : (1, x_1, x_2) \mapsto (x_2, x_1)$. This map is an isomorphism as two vertices x, y of H_q are adjacent if and only if $x_2 - x_1y_1 + y_2 = 0$, which is equivalent to $x_2 + y_2 = x_1y_1$.

□

Proof of Theorem 5. Let p be prime, $n > 0$, and $q = p^n$. We prove all cases here except when $p = 2$ and n is even. For this case we obtain sharper results, which we postpone to the next subsection. By virtue of Proposition 3 we will work with ER_q^* instead of ER_q. Let μ be a primitive element of F_q.

Case (i): $p > 2$ and n is even. Let $R = \left\{\mu^{(\sqrt{q}+1)k} : k \in \left[0, \frac{\sqrt{q}-3}{2}\right]\right\} \cup \{0\}$. Then R is isomorphic to a subset of $F_{\sqrt{q}}$ which has the property that for $x, y \in R$, $x = -y$ implies that $x = y = 0$. This follows as $-1 = \mu^{(q-1)/2}$. If $x \neq 0$ then $x = \mu^{(\sqrt{q}+1)k}$ where $k \in \left[0, \frac{\sqrt{q}-3}{2}\right]$, and $-x = \mu^{(\sqrt{q}+1)k}\mu^{(q-1)/2} = \mu^{(\sqrt{q}+1)(k+(\sqrt{q}-1)/2)} \notin R$ since $(k + (\sqrt{q} - 1)/2) \notin \left[0, \frac{\sqrt{q}-3}{2}\right]$.

We claim that

$$I = \{(1, t, t^2/2 - \mu r/2) : t \in F_q, r \in R\} \cup \{(0, 0, 1)\}$$

is an independent set of size $\frac{q^{3/2}+q+2}{2}$.

By way of contradiction, if $(1, t, t^2/2 - \mu r_1/2), (1, s, s^2/2 - \mu r_2/2) \in I$ are two adjacent vertices then $st = t^2/2 - \mu r_1/2 + s^2/2 - \mu r_2/2$. This yields $\mu(r_1 + r_2) = t^2 - 2st + s^2 = (t - s)^2$. As the right hand side of the equation is a square, equality is possible only if $r_1 = -r_2$ and $s = t$. However, the only element of R whose additive inverse is also in R is 0. Therefore, $r_1 = r_2$ implying that these two vertices are not distinct, a contradiction.

Case (ii): $p > 2$ and n is odd. Write $x \in F_q$ in the form

$$x = \sum_{i=0}^{n-1} x_i \mu^i$$

where $x_i \in F_p$. Let A be the set of all integers in the interval $[\lceil p/6 \rceil, \lfloor p/2 \rfloor]$ and B be the set of all integers in the interval $[0, \lfloor \sqrt{p/3} \rfloor]$. We let our sets S and T be the following with $m = \frac{n-1}{2}$:

$$S = \{x : x_{n-1} \in A\}$$

$$T = \{y : y_i = 0 \text{ if } i > m \text{ and } y_m \in B\}$$

For $w, x \in S$ we have $(w+x)_{n-1} \in \left[\lceil \frac{p+1}{3} \rceil, p-1\right]$. For $y, z \in T$ we have

$$yz = \left(\sum_{i=0}^{m} y_i \mu^i\right)\left(\sum_{j=0}^{m} z_j \mu^j\right) = \sum_{i=0}^{n-1}\sum_{j=0}^{i} y_{i-j} z_j \mu^i$$

This gives us $(yz)_{n-1} = (y_m)(z_m) \in \left[0, \lfloor \frac{p-1}{3} \rfloor\right]$. Then $I = \{(1,t,s) : s \in S \text{ and } t \in T\}$ is an independent set with:

$$|I| = \left(\left\lfloor \frac{p}{2} \right\rfloor - \left\lceil \frac{p}{6} \right\rceil + 1\right)\left(\left\lfloor \sqrt{\frac{p}{3}} \right\rfloor + 1\right)\left(\frac{q^{3/2}}{p\sqrt{p}}\right) > \frac{1-\frac{1}{p}}{3\sqrt{3}}\left(q^{\frac{3}{2}}\right)$$

Since the constants are bounded below by $\frac{1-\frac{1}{p}}{3\sqrt{3}}\left(q^{\frac{3}{2}}\right)$, it is clear that there is a prime which yields the worst constant. In [23] a search using the software package Magma was done to determine that the worst case is when $p = 73$ which gives the constant $\frac{120}{73\sqrt{73}}$.

Case (iii): $p = 2$ and n is odd. Let $m = \frac{n-1}{2}$ and consider the following sets:

$$S = \{x : x_{n-1} = 0\}$$

$$T = \{y : y_i = 0 \text{ if } i > m \text{ and } y_m = 1\}$$

Then $I = \{(1,t,s) : s \in S \text{ and } t \in T\}$ is an independent set of size $\frac{q^{3/2}}{2\sqrt{2}}$. The remaining case where n is even and $p = 2$ will be verified in the following subsection.

The case where n and p are both odd yields the smallest constants. All cases considered, this verifies that $\alpha(ER_q) \geq \frac{120q^{3/2}}{73\sqrt{73}}$.

□

3.1. **Even powers of 2.** We now prove that when $q = 2^n$, n even, $\alpha(ER_q) \geq q^{3/2} - q + \sqrt{q}$. Our construction uses a special Denniston maximal arc, for more information on maximal arcs see [7],[11], and [20]. The coordinatization of the arc will be similar to that of Mathon's (see [20]). The following lemma is based on a result in [7]. We pay special attention to the subfield $F_{\sqrt{q}}$.

Lemma 9. *Let q be an even power of 2 and x^2+x+s be an irreducible polynomial over F_q. Then the image of x^2+x+s is a coset of an additive subgroup of index 2 of F_q which is disjoint from the subfield $F_{\sqrt{q}}$.*

Proof. As noted in [7], for fields of characteristic two, the polynomial x^2+x has the property that for $x, y \in F_q$ $x^2+x+y^2+y = (x+y)^2+(x+y)$ and is therefore an endomorphism of the additive group of F_q with kernel $\{0,1\}$. The image of a polynomial of the form x^2+x+c where c is a constant is therefore a subgroup of index 2 or the coset of a subgroup of index 2, depending on whether or not c is in the image of x^2+x. Since every polynomial of the form x^2+x+c with $c \in F_{\sqrt{q}}$ splits in F_q, the equation $x^2+x+c = 0$ has a solution in F_q, therefore, $x^2+x = c$ has a solution in F_q. This implies that the image of x^2+x contains the entire subfield $F_{\sqrt{q}}$. However, the image of x^2+x does not contain s due to the fact that x^2+x+s is irreducible (since any solution to $x^2+x = s$ is a solution to

$x^2+x+s=0$); therefore, the image of x^2+x+s is a coset of the image of x^2+x. It follows that the image of x^2+x+s is disjoint from $F_{\sqrt{q}}$. □

Proof of Theorem 6. Let x^2+x+s be an irreducible polynomial over F_q. Let I be the set of all points $(x_0,x_1,x_2)\in ER_q$ for which there exists $\lambda\in F_{\sqrt{q}}$ such that $x_2^2+x_2x_0+sx_0^2+\lambda x_1^2=0$. Then by a result of Denniston [7] the set I is a maximal arc of order $\sqrt{q}$. It can be argued combinatorially that $|I|=q^{3/2}-q+\sqrt{q}$ using that I is a maximal arc, but here we count the size of the set directly. If $\lambda=0$, we must have $x_0=0$ (if $x_0=1$ we would have a solution to $x_2^2+x_2+s=0$, a contradiction) and hence $x_2=0$. This implies $x_1=1$, and we have only one solution. In the case where $\lambda\neq 0$, we then condition on whether $x_0=0$ or 1. If $x_0=0$, then $x_1=1$ (as $x_1=0$ implies $x_2=0$ which is impossible). We then have $x_2^2=\lambda$ which gives us $\sqrt{q}-1$ solutions as every choice of a nonzero λ uniquely determines x_2^2 and hence x_2 (as squaring is a field automorphism over fields of characteristic two). Lastly if $\lambda\neq 0$ and $x_0=1$, then $x_1^2=\lambda^{-1}(x_2^2+x_2+s)$ and any choice of $\lambda\neq 0$ and x_2 uniquely determines x_1, yielding $q(\sqrt{q}-1)$ solutions. Altogether we have $1+\sqrt{q}-1+q(\sqrt{q}-1)=q^{3/2}-q+\sqrt{q}$ solutions, therefore, $|I|=q^{3/2}-q+\sqrt{q}$.

We claim that this particular arc forms an independent set in ER_q^*. Assume two points (x_0,x_1,x_2) and (y_0,y_1,y_2) are connected. Then for some $\lambda_1,\lambda_2\in F_{\sqrt{q}}$ the three equations below are satisfied:

$$x_2^2+x_2x_0+sx_0^2+\lambda_1x_1^2=0$$
$$y_2^2+y_2y_0+sy_0^2+\lambda_2y_1^2=0$$
$$x_2y_0+x_0y_2=x_1y_1$$

If $\lambda_1=0$ or $x_1=0$, then we have that $x_2^2+x_2x_0+sx_0^2=0$ which forces $x_0=x_2=0$ as otherwise $\frac{x_2}{x_0}$ is a root of the polynomial x^2+x+s which is impossible. We have an immediate contradiction if $x_1=0$, as $(0,0,0)$ is not a vertex of ER_q. If $\lambda_1=0$ then we must have $x_1=1$ and therefore $y_1=0$. Then we obtain $y_2^2+y_2y_0+sy_0^2=0$ which forces $y_0=y_2=0$, which implies $(y_1,y_2,y_3)=(0,0,0)$, a contradiction. If $\lambda_1,\lambda_2,x_1,y_1\neq 0$, then we may rewrite the above equations to obtain:

$$\frac{1}{\lambda_1}(x_2^2+x_2x_0+sx_0^2)=x_1^2$$
$$\frac{1}{\lambda_2}(y_2^2+y_2y_0+sy_0^2)=y_1^2$$
$$x_0y_2+x_2y_0=x_1y_1$$

Squaring the third equation and substituting we get:

$$(x_2y_0+x_0y_2)^2=\frac{1}{\lambda_1\lambda_2}(x_2^2+x_2x_0+sx_0^2)(y_2^2+y_2y_0+sy_0^2)$$

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

$$\frac{(x_2^2+x_2x_0+sx_0^2)(y_2^2+y_2y_0+sy_0^2)}{(x_2y_0+x_0y_2)^2}=\lambda_1\lambda_2$$

If $x_0=0$, then $x_1=y_0=1$ and we have $y_2^2+y_2+s=\lambda_1\lambda_2$, which is impossible by Lemma 9. Similarly, $y_0=0$ also leads to a contradiction. The last case to consider is $x_0=y_0=1$, which yields the equation:

$$\frac{(x_2^2+x_2+s)(y_2^2+y_2+s)}{(x_2+y_2)^2}=\lambda_1\lambda_2\in F_{\sqrt{q}}$$

Noting that $y_2 \neq x_2$, we substitute $y_2 = 1/w + x_2$. After expanding we have the equation:

$$(x_2^2 + x_2 + s)^2 w^2 + (x_2^2 + x_2 + s)w + x_2^2 + x_2 + s \in F_{\sqrt{q}}$$

which is equivalent to:

$$((x_2^2 + x_2 + s)w + x_2)^2 + ((x_2^2 + x_2 + s)w + x_2) + s \in F_{\sqrt{q}}$$

This is impossible by Lemma 9. All cases accounted for, we have that no two points of I are adjacent. Then we have $\alpha(ER_q) \geq q^{3/2} - q + \sqrt{q}$, as desired.

□

4. The Unitary Polarity Graph of $PG(2, q)$

In the next proof, we use the fact that all polarity graphs of projective planes or order q have diameter 2, no 4-cycles, and that all vertices have degree $q+1$ except for the absolute points, which have degree q.

Proof of Theorem 7. Let I be an independent set of maximum size. Let E_I be the edges of U_q with an endvertex in I, and $\deg_I(v)$ be the number of neighbors in I of a vertex v, respectively. Let a be the number of absolute points contained in I (this implies $a \leq q^{3/2} + 1$). Then

$$E_I = (q+1)(|I| - a) + qa = (q+1)|I| - a.$$

We wish to count the number of 2-paths which have both endpoints in I. As U_q has diameter 2 and no 4-cycles, we must have exactly $\binom{|I|}{2}$ such paths. We obtain the equation:

$$\binom{|I|}{2} = \sum_{v \in V} \binom{|\Gamma_I(v)|}{2} = \sum_{v \in V} \binom{\deg_I(v)}{2}$$

By Jensen's inequality we have

$$\binom{|I|}{2} = \sum_{v \in V} \binom{\deg_I(v)}{2} \geq (|V| - |I|)\binom{E_I/(|V| - |I|)}{2}$$

$$= (q^2 + q + 1 - |I|)\binom{((q+1)|I| - a)/(q^2 + q + 1 - |I|)}{2}$$

$$\geq (q^2 + q + 1 - |I|)\binom{((q+1)|I| - q^{3/2} - 1)/(q^2 + q + 1 - |I|)}{2}$$

Equality holds throughout if and only if $a = q^{3/2} + 1$. This leads to the inequality

$$|I|^3 + 2q|I|^2 - f(q)|I| + g(q) \leq 0.$$

where $f(q) = q^3 + 2q^{5/2} + q^2 + 3q^{3/2} + 3q + 3$ and $g(q) = (q^{3/2} + 1)(q^2 + q^{3/2} + q + 2)$. The largest root of this equation is precisely $q^{3/2} + 1$, therefore $\alpha(U_q) \leq q^{3/2} + 1$. If equality holds, $a = q^{3/2} + 1$, and therefore I is the set of absolute points of U_q.

□

5. The Hypergraph $\mathcal{H}_q$

Proof of Theorem 8. We are to show that $\alpha(\mathcal{H}_q) \leq q^2/2 + q^{3/2} + O(q)$. To facilitate the proof we will use a few facts about the graph ER_q^o: the graph is $q+1$ regular on q^2+q+1 vertices, every edge which does not have an absolute endvertex is contained in a unique triangle (see [19]), and a nonabsolute vertex is connected to either 0 or 2 absolute vertices. Recall that the vertex set of $\mathcal{H}_q$ is the set of nonabsolute points in $V(ER_q)$.

Let I be an independent set in $\mathcal{H}_q$ and let $J = V(\mathcal{H}_q)\backslash I$. By Theorem 1 we have that

$$e(I,I) \geq \left(\frac{q+1}{q^2+q+1}\right)|I|^2 - \sqrt{q}|I|.$$

Similarly,

$$e(J,J) \geq \left(\frac{q+1}{q^2+q+1}\right)|J|^2 - \sqrt{q}|J|.$$

As every vertex has degree at most $q+1$, we must have

$$e(I,J) \leq |J|(q+1) - \left(\frac{q+1}{q^2+q+1}\right)|J|^2 + \sqrt{q}|J|.$$

As every edge in I lies in a unique triangle, we must have that $e(I,I) \leq e(I,J)$, and this leads to:

$$\left(\frac{q+1}{q^2+q+1}\right)|I|^2 - \sqrt{q}|I| \leq |J|(q+1) - \left(\frac{q+1}{q^2+q+1}\right)|J|^2 + \sqrt{q}|J|.$$

Substituting $|J| = q^2 - |I|$ and multiplying by q^2+q+1 we have:

$$(2q+2)\,|I|^2 + \left(-q^3+2q+1\right)|I| - q^2(q^{5/2}+q^2+q^{3/2}+2q+\sqrt{q}+1) \leq 0.$$

The roots of this equation are:

$$\frac{q^3 - 2q - 1 \pm \sqrt{f(q)}}{4(q+1)}$$

where

$$f(q) = q^6 + 8q^{\frac{11}{2}} + 8q^5 + 16q^{\frac{9}{2}} + 20q^4 + 16q^{\frac{7}{2}} + 22q^3 + 8q^{\frac{5}{2}} + 12q^2 + 4q + 1.$$

It follows then from the series expansion of this root that $\alpha(\mathcal{H}_q) \leq q^2/2 + q^{3/2} + O(q)$. □

6. Acknowledgments

The second author would like to thank Felix Lazebnik who was his thesis advisor during a portion of this research. Thanks also to Gary Ebert for fruitful discussions about Finite Geometry and norms, Chris Godsil and Mike Newman for their discussions on eigenvalue bounds, and to Benny Sudakov for bringing the problem to the attention of Felix Lazebnik, who in turn passed it on to the author. The authors would also like to thank the referees for their helpful comments.

References

[1] M. Aigner, G. M. Ziegler, *Proofs from The Book* Second edition. Springer-Verlag, Berlin, 2001.

[2] N. Alon, V. Rödl, Asymptotically tight bounds for some multicolor Ramsey numbers. *Combinatorica*, to appear

[3] N. Alon, L. Rónyai, T. Szabó, Norm-graphs: variations and applications. *J. Combin. Theory Ser. B* 76 (1999), no. 2, 280–290.

[4] N. Alon, J. Spencer, The Probabilistic Method, Wiley, 2000

[5] B. Bollobás, *Extremal graph theory.* Academic Press, London, 1978.

[6] Brown, W. G. On graphs that do not contain a Thomsen graph. *Canad. Math. Bull.* 9 (1966) 281–285.

[7] R. H. F. Denniston, Some maximal arcs in finite projective planes. *J. Combinatorial Theory* 6 (1969), 317–319.

[8] P. Erdős, A. Rényi, On a problem in the theory of graphs. *Publ. Math. Inst. Hungar. Acad. Sci.* 7A 1962 623–641.

[9] P. Erdős, A. Rényi, V.T. Sos, On a problem of graph theory. *Studia Sci. Math. Hungar.* 1 (1966) 215–235.

[10] P. Erdős, M. Simonovits, Compactness results in extremal graph theory. *Combinatorica* 2 (1982), no. 3, 275–288.

[11] F. Fiedler, *Maximal Arcs in* $PG(2, 2^m)$. PhD thesis, University of Delaware, May 2004.

[12] Z. Füredi, Graphs without Quadrilaterals. *Journal of Combinatorial Theory, Series B* 34 (1983), 187–190.

[13] Z. Füredi, On the Number of Edges of Quadrilateral-Free Graphs. *Journal of Combinatorial Theory, Series B* 68 (1996), 1–6.

[14] Z. Füredi, Quadrilateral-free graphs with maximum number of edges. *preprint*

[15] M. Newman, *Independent Sets and Eigenspaces.* PhD thesis, University of Waterloo, December 2004.

[16] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford, New York, 1998.

[17] A. J. Hoffman, On eigenvalues and colorings of graphs. *1970 Graph Theory and its Applications (Proc. Advanced Sem., Math. Research Center, Univ. of Wisconsin, Madison, Wis., 1969)*, Academic Press, New York.

[18] D. Hughes, F. Piper, *Projective planes.* Graduate Texts in Mathematics Vol. 6. Springer-Verlag, New York-Berlin, 1973, pp 45-49.

[19] F. Lazebnik, J. Verstraëte, On Hypergraphs of Girth Five. *Electronic Journal of Combinatorics* 10 (2003), R25.

[20] R. Mathon, New maximal arcs in Desarguesian planes. *J. Combin. Theory Ser. A* 97 (2002), no. 2, 353–368.

[21] T.D. Parsons, Graphs from projective planes. *Aequationes Math.* 14 (1976), no. 1-2, 167–189.

[22] T. Szabó, On the spectrum of projective norm-graphs. *Inform. Process. Lett.* 86 (2003), no. 2, 71–74.

[23] J. Williford, *Constructions in Finite Geometry with Applications to Graphs.* PhD thesis, University of Delaware, August 2004.

(Dhruv Mubayi) Department of Mathematics, Statistics, and Computer Science, University of Illinois, Chicago, IL 60607

(Jason Williford) Department of Mathematics and Computer Science, Albion College, Albion, MI 49224