SIAM J. DISCRETE MATH.
Vol. 21, No. 2, pp. 329–348

GRAPH POWERS, DELSARTE, HOFFMAN, RAMSEY, AND SHANNON*

NOGA ALON† AND EYAL LUBETZKY‡

Abstract. The kth p-power of a graph G is the graph on the vertex set $V(G)^k$, where two k-tuples are adjacent iff the number of their coordinates which are adjacent in G is not congruent to 0 modulo p. The clique number of powers of G is polylogarithmic in the number of vertices; thus graphs with small independence numbers in their p-powers do not contain large homogeneous subsets. We provide algebraic upper bounds for the asymptotic behavior of independence numbers of such powers, settling a conjecture of [N. Alon and E. Lubetzky, *Combinatorica*, 27 (2007), pp. 13–33] up to a factor of 2. For precise bounds on some graphs, we apply Delsarte's linear programming bound and Hoffman's eigenvalue bound. Finally, we show that for any nontrivial graph G, one can point out specific induced subgraphs of large p-powers of G with neither a large clique nor a large independent set. We prove that the larger the Shannon capacity of $\overline{G}$ is, the larger these subgraphs are, and if G is the complete graph, then some p-power of G matches the bounds of the Frankl–Wilson Ramsey construction, and is in fact a subgraph of a variant of that construction.

Key words. graph powers, Delsarte's linear programming bound, eigenvalue bounds, Ramsey theory, cliques and independent sets

AMS subject classifications. 05C69, 05D10, 05E35, 94B65

DOI. 10.1137/060657893

1. Introduction.

The kth Xor graph power of a graph G, $G^{\oplus k}$, is the graph whose vertex set is the Cartesian product $V(G)^k$, where two k-tuples are adjacent iff an odd number of their coordinates is adjacent in G. This product was used in [21] to construct edge colorings of the complete graph with two colors, containing a smaller number of monochromatic copies of K_4 than the expected number of such copies in a random coloring.

In [4], the authors studied the independence number, α, and the clique number, ω, of high Xor powers of a fixed graph G, motivated by problems in coding theory: cliques and independent sets in such powers correspond to maximal codes satisfying certain natural properties. It is shown in [4] that while the clique number of $G^{\oplus k}$ is linear in k, the independence number $\alpha(G^{\oplus k})$ grows exponentially: the limit $\alpha(G^{\oplus k})^{\frac{1}{k}}$ exists and is in the range $[\sqrt{|V(G)|}, |V(G)|]$. Denoting this limit by $x_\alpha(G)$, the problem of determining $x_\alpha(G)$ for a given graph G proves to be extremely difficult, even for simple families of graphs. Using spectral techniques, it is proved in [4] that $x_\alpha(K_n) = 2$ for $n \in \{2, 3, 4\}$, where K_n is the complete graph on n vertices, and it is conjectured that $x_\alpha(K_n) = \sqrt{n}$ for every $n \geq 4$. The best upper bound given in [4] on $x_\alpha(K_n)$ for $n \geq 4$ is $n/2$.

*Received by the editors April 21, 2006; accepted for publication (in revised form) November 20, 2006; published electronically April 27, 2007.
http://www.siam.org/journals/sidma/21-2/65789.html

†School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, and Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, 69978, Israel (nogaa@tau.ac.il). This author's research was supported in part by the Israel Science Foundation, by a U.S.–Israeli BSF grant, by NSF grant CCR-0324906, by a Wolfensohn fund, and by the State of New Jersey.

‡School of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, 69978, Israel (lubetzky@tau.ac.il). This author's research was partially supported by a Charles Clore Foundation Fellowship.

The graph product we introduce in this work, which generalizes the Xor product, is motivated by Ramsey theory. In [9], Erdős proved the existence of graphs on n vertices without cliques or independent sets of size larger than $O(\log n)$ vertices, and that in fact almost every graph satisfies this property. Ever since, there have been many attempts to provide explicit constructions of such graphs. Throughout the paper, without being completely formal, we call a graph "Ramsey" if it has neither a "large" clique nor a "large" independent set. The famous Ramsey construction of Frankl and Wilson [10] provided a family of graphs on n vertices, FW_n, with a bound of $\exp\left(\sqrt{(2+o(1))\log n \log\log n}\right)$ on the independence and clique numbers, using results from extremal finite set theory. Thereafter, constructions with the same bound were produced in [3] using polynomial spaces and in [11] using low degree matrices. Recently, the old Frankl–Wilson record was broken in [6], where the authors provided, for any $\varepsilon > 0$, a polynomial-time algorithm for constructing a Ramsey graph on n vertices without cliques or independent sets on $\exp\left((\log n)^{\varepsilon}\right)$ vertices. The disadvantage of this latest revolutionary construction is that it involves a complicated algorithm, from which it is hard to tell the structure of the resulting graph.

Relating the above to graph products, the Xor product may be viewed as an operator, $\oplus_k$, which takes a fixed input graph G on n vertices and produces a graph on n^k vertices, $H = G^{\oplus k}$. The results of [4] imply that the output graph H satisfies $\omega(H) \le nk = O(\log(|V(H)|))$, and that if G is a nontrivial d-regular graph, then H is d'-regular, with $d' \to \frac{1}{2}|V(H)|$ as k tends to infinity. Thus, $\oplus_k$ transforms any nontrivial d-regular graph into a random looking graph, in the sense that it has an edge density of roughly $\frac{1}{2}$ and a logarithmic clique number. However, the lower bound $\alpha(H) \ge \sqrt{|V(H)|}$, which holds for every even k, implies that $\oplus_k$ cannot be used to produce good Ramsey graphs.

In order to modify the Xor product into a method for constructing Ramsey graphs, one may try to reduce the high lower bound on the independence numbers of Xor graph powers. Therefore, we consider a generalization of the Xor graph product, which replaces the modulo 2 (adjacency of two k-tuples is determined by the parity of the number of adjacent coordinates) with some possibly larger modulo $p \in \mathbb{N}$. Indeed, we show that by selecting a larger p, the lower bound on the independence number, $\alpha(H)$, is reduced from $\sqrt{|V(H)|}$ to $|V(H)|^{1/p}$, at the cost of a polynomial increase in $\omega(H)$. The generalized product is defined as follows.

DEFINITION 1.1. *Let $k, p \in \mathbb{N}$. The kth p-power of a graph G, denoted by $G^{k_{(p)}}$, is the graph whose vertex set is the Cartesian product $V(G)^k$, where two k-tuples are adjacent iff the number of their coordinates which are adjacent in G is not congruent to 0 modulo p, that is,*

$$(u_1, \dots, u_k)\ (v_1, \dots, v_k) \in E(G^k) \quad \textit{iff} \quad |\{i : u_i v_i \in E(G)\}| \not\equiv 0 \pmod{p}.$$

Throughout the paper, we use the abbreviation G^k for $G^{k_{(p)}}$ when there is no danger of confusion.

In section 2 we show that the limit $\alpha(G^k)^{\frac{1}{k}}$ exists and equals $\sup_k \alpha(G^k)^{\frac{1}{k}}$; denote this limit by $x_\alpha^{(p)}$. A simple lower bound on $x_\alpha^{(p)}$ is $|V(G)|^{1/p}$, and algebraic arguments show that this bound is nearly tight for the complete graph: $x_\alpha^{(p)}(K_n) = O(n^{1/p})$. In particular, we obtain that

$$\sqrt{n} \le x_\alpha(K_n) = x_\alpha^{(2)}(K_n) \le 2\sqrt{n-1},$$

improving the upper bound of $n/2$ for $n \ge 4$ given in [4], and determining that the

behavior of x_α for complete graphs is as stated in Question 4.1 of [4] up to a factor of 2.

For the special case $G = K_n$, it is possible to apply coding theory techniques in order to bound $x_\alpha^{(p)}(G)$. The problem of determining $x_\alpha^{(p)}(K_n)$ can be translated into finding the asymptotic maximum size of a code over the alphabet $[n]$, in which the Hamming distance between any two codewords is divisible by p. The related problem for *linear* codes over a field has been well studied: see, e.g., [23] for a survey on this subject. However, as we later note in section 2, the general nonlinear case proves to be quite different, and the upper bounds on linear divisible codes do not hold for $x_\alpha^{(p)}(K_n)$. Yet, other methods for bounding sizes of codes are applicable. In section 3 we demonstrate the use of Delsarte's linear programming bound in order to obtain precise values of $\alpha(K_3^{k_{(3)}})$. We show that $\alpha(K_3^{k_{(3)}}) = 3^{k/2}$ whenever $k \equiv 0 \pmod 4$, while $\alpha(K_3^{k_{(3)}}) < \frac{1}{2}3^{k/2}$ for $k \equiv 2 \pmod 4$; hence the series $\alpha(K_3^{k+1_{(3)}})/\alpha(K_3^{k_{(3)}})$ does not converge to a limit.

Section 4 gives a general bound on $x_\alpha^{(p)}$ for d-regular graphs in terms of their eigenvalues, using Hoffman's eigenvalue bound. The eigenvalues of p-powers of G are calculated using tensor products of matrices over $\mathbb{C}$, in a way somewhat similar to performing a Fourier transform on the adjacency matrix of G. This method may also be used to derive tight results on $\alpha(G^{k_{(p)}})$, and we demonstrate this on the above-mentioned case of $p = 3$ and the graph K_3, where we compare the results with those obtained in section 3 by the Delsarte bound.

Section 5 shows, using tools from linear algebra, that indeed the clique number of $G^{k_{(p)}}$ is polylogarithmic in k, and thus p-powers of graphs attaining the lower bound of $x_\alpha^{(p)}$ are Ramsey. We proceed to show a relation between the Shannon capacity of the complement of G, $c(\overline{G})$, and the Ramsey properties of p-powers of G. Indeed, for any nontrivial graph G, we can point out a large Ramsey-induced subgraph of some p-power of G. The larger $c(\overline{G})$ is, the larger these Ramsey subgraphs are. When $G = K_p$ for some prime p, we obtain that $H = K_p^{p^2{}_{(p)}}$ is a Ramsey graph matching the bound of Frankl and Wilson, and in fact, H contains an induced subgraph which is a modified variant of FW_{N_1} for some N_1 and is contained in another variant of FW_{N_2} for some N_2. The method of proving these bounds on $G^{k_{(p)}}$ provides yet another (simple) proof for the Frankl–Wilson result.

2. Algebraic lower and upper bounds on $x_\alpha^{(p)}$. In this section, we define the parameter $x_\alpha^{(p)}$ and provide lower and upper bounds for it. The upper bounds follow from algebraic arguments, using graph representation by polynomials.

2.1. The limit of independence numbers of p-powers. The following lemma establishes that $x_\alpha^{(p)}$ exists and gives simple lower and upper bounds on its range for graphs on n vertices.

LEMMA 2.1. *Let G be a graph on n vertices, and let $p \geq 2$. The limit of $\alpha(G^{k_{(p)}})^{\frac{1}{k}}$ as $k \to \infty$ exists, and, denoting it by $x_\alpha^{(p)}(G)$, it satisfies*

$$n^{1/p} \leq x_\alpha^{(p)}(G) = \sup_k \alpha(G^{k_{(p)}})^{\frac{1}{k}} \leq n.$$

Proof. Observe that if I and J are independent sets of G^k and G^l, respectively, then the set $I \times J$ is an independent set of G^{k+l}, as the number of adjacent coordinates between any two k-tuples of I and between any two l-tuples of J is 0 (mod p). Therefore, the function $g(k) = \alpha(G^k)$ is supermultiplicative and strictly positive, and

we may apply Fekete's lemma (cf., e.g., [15, p. 85]) to obtain that the limit of $\alpha(G^k)^{\frac{1}{k}}$ as $k \to \infty$ exists, and satisfies

$$\lim_{k\to\infty} \alpha(G^k)^{\frac{1}{k}} = \sup_k \alpha(G^k)^{\frac{1}{k}}. \tag{2.1}$$

Clearly, $\alpha(G^k) \le n^k$, and it remains to show the lower bound on $x_\alpha^{(p)}$. Notice that the following set is an independent set of G^p:

$$I = \{\ (u, \ldots, u)\ :\ u \in V(G)\} \subset G^p,$$

since for all $u, v \in V(G)$ there are either 0 or p adjacent coordinates between the two corresponding p-tuples in I. By (2.1), we obtain that $x_\alpha^{(p)}(G) \ge |I|^{1/p} = n^{1/p}$. □

2.2. Bounds on $x_\alpha^{(p)}$ of complete graphs. While the upper bound $|V(G)|$ on $x_\alpha^{(p)}(G)$ is clearly attained by an edgeless graph, proving that a family of graphs attains the lower bound requires some effort. The next theorem states that complete graphs achieve the lower bound of Lemma 2.1 up to a constant factor.

THEOREM 2.2. *The following holds for all integers $n, p \ge 2$:*

$$x_\alpha^{(p)}(K_n) \le 2^{H(1/p)}(n-1)^{1/p}, \tag{2.2}$$

where $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function. In particular, $x_\alpha^{(p)}(K_n) = \Theta(n^{1/p})$. In the special case where $n = p = q^r$ for some prime q and $r \ge 1$, the lower bound roughly matches the upper bound:

$$p^{\frac{2}{p+1}} \le x_\alpha^{(p)}(K_p) \le \left(\mathrm{e}p^2\right)^{1/p}.$$

Taking $p = 2$ and noting that $H(\frac{1}{2}) = 1$, we immediately obtain the following corollary for Xor graph products, which determines the asymptotic behavior of x_α for complete graphs.

COROLLARY 2.3. *For all $n \ge 2$, the complete graph on n vertices satisfies*

$$\sqrt{n} \le x_\alpha(K_n) \le 2\sqrt{n-1}.$$

Proof of Theorem 2.2. The upper bound will follow from an argument on polynomial representations, an approach which was used in [3] to bound the Shannon capacity of certain graphs. Take $k \ge 1$, and consider the graph $H = K_n^k$. For every vertex of H, $u = (u_1, \ldots, u_k)$, we define the following polynomial in $\mathbb{R}[x_{i,j}]$, where $i \in [k]$, $j \in [n]$:

$$f_u(x_{1,1}, \ldots, x_{k,n}) = \prod_{t=1}^{\lfloor k/p \rfloor} \left(k - tp - \sum_{i=1}^{k} x_{i,u_i}\right). \tag{2.3}$$

Next, give the following assignment of values for $\{x_{i,j}\}$, x_v, to each $v = (v_1, \ldots, v_k) \in V(H)$:

$$x_{i,j} = \delta_{v_i,j}, \tag{2.4}$$

where δ is the Kronecker delta. Definitions (2.3) and (2.4) imply that for every two such vertices $u = (u_1, \ldots, u_k)$ and $v = (v_1, \ldots, v_k)$ in $V(H)$,

$$f_u(x_v) = \prod_{t=1}^{\lfloor k/p \rfloor} \left(k - tp - \sum_{i=1}^{k} \delta_{u_i,v_i}\right) = \prod_{t=1}^{\lfloor k/p \rfloor} \left(|\{i\ :\ u_i \ne v_i\}| - tp\right). \tag{2.5}$$

Notice that, by the last equation, $f_u(x_u) \neq 0$ for all $u \in V(H)$, and consider two distinct nonadjacent vertices $u, v \in V(H)$. The Hamming distance between u and v (considered as vectors in $\mathbb{Z}_n^k$) is by definition 0 (mod p) (and is not zero). Thus, (2.5) implies that $f_u(x_v) = 0$.

Recall that for all u, the assignment x_u gives values $x_{i,j} \in \{0, 1\}$ for all i, j, and additionally $\sum_{j=1}^{n} x_{i,j} = 1$ for all i. Therefore, it is possible to replace all occurrences of $x_{i,n}$ by $1 - \sum_{j=1}^{n-1} x_{i,j}$ in each f_u, and then proceed and reduce the obtained result modulo the polynomials,

$$\bigcup_{i \in [k]} \left(\{x_{i,j}^2 - x_{i,j} : j \in [n]\} \ \cup \ \{x_{i,j} x_{i,l} : j, l \in [n], j \neq l\} \right),$$

without affecting the value of the polynomials on the above-defined substitutions. In other words, after replacing $x_{i,n}$ by $1 - \sum_{j<n} x_{i,j}$, we repeatedly replace $x_{i,j}^2$ by $x_{i,j}$, and let all the monomials containing $x_{i,j} x_{i,l}$ for $j \neq l$ vanish. This gives a set of multilinear polynomials $\{\tilde{f}_u\}$ satisfying

$$\begin{cases} \tilde{f}_u(x_u) \neq 0 & \text{for all } u \in V(H), \\ \tilde{f}_u(x_v) = 0 & \text{for } u \neq v,\ uv \notin E(H), \end{cases}$$

where the monomials of $\tilde{f}_u$ are of the form $\prod_{t=1}^{r} x_{i_t, j_t}$ for some $0 \leq r \leq \lfloor \frac{k}{p} \rfloor$, a set of pairwise distinct indices $\{i_t\} \subset [k]$, and indices $\{j_t\} \subset [n-1]$.

Let $\mathcal{F} = \mathrm{Span}(\{\tilde{f}_u : u \in V(H)\})$, and let I denote a maximum independent set of H. A standard argument shows that $F = \{\tilde{f}_u : u \in I\}$ is linearly independent in $\mathcal{F}$. Indeed, suppose that $\sum_{u \in I} a_u \tilde{f}_u(x) = 0$; then substituting $x = x_v$ for some $v \in I$ gives $a_v = 0$. It follows that $\alpha(H) \leq \dim \mathcal{F}$, and thus

$$\alpha(H) \leq \sum_{r=0}^{\lfloor k/p \rfloor} \binom{k}{r} (n-1)^r \leq \left(2^{H(1/p)} (n-1)^{1/p} \right)^k, \tag{2.6}$$

where in the last inequality we used the fact that $\sum_{i \leq \lambda n} \binom{n}{i} \leq 2^{nH(\lambda)}$ (cf., e.g., the remark following Corollary 4.2 in [2], and also [5, p. 242]). Taking the kth root and letting k grow to ∞, we obtain

$$x_\alpha^{(p)}(K_n) \leq 2^{H(1/p)} (n-1)^{1/p},$$

as required.

In the special case of K_p (that is, $n = p$), note that $2^{H(\frac{1}{p})} = p^{\frac{1}{p}} (\frac{p}{p-1})^{\frac{p-1}{p}} \leq (\mathrm{e}p)^{\frac{1}{p}}$ and hence in this case $x_\alpha^{(p)}(K_p) \leq (\mathrm{e}p^2)^{1/p}$. If $p = q^r$ is a prime-power, we can provide a nearly matching lower bound for $x_\alpha^{(p)}(K_p)$ using a construction of [4], which we shortly describe for the sake of completeness.

Let $\mathcal{L}$ denote the set of all lines with finite slopes in the affine plane $GF(p)$, and write down the following vector w_ℓ for each $\ell \in \mathcal{L}$, $\ell = ax + b$ for some $a, b \in GF(p)$:

$$w_\ell = (a, ax_1 + b, ax_2 + b, \ldots, ax_p + b),$$

where $x_1, \ldots, x_p$ denote the elements of $GF(p)$. For every two distinct lines ℓ, ℓ', if $\ell \| \ell'$, then $w_\ell, w_{\ell'}$ has a single common coordinate (the slope a). Otherwise, $w_\ell, w_{\ell'}$ has a single common coordinate, which is the unique intersection of ℓ, ℓ'. In any case,

we obtain that the Hamming distance of w_ℓ and $w_{\ell'}$ is p; hence $W = \{w_\ell : \ell \in \mathcal{L}\}$ is an independent set in K_p^{p+1}. By (2.1), we deduce that

$$x_\alpha^{(p)}(K_p) \geq p^{\frac{2}{p+1}},$$

completing the proof. □

Remark 2.4. The proof of Theorem 2.2 used representation of the vertices of K_n^k by polynomials of kn variables over $\mathbb{R}$. It is possible to prove a similar upper bound on $x_\alpha^{(p)}(K_n)$ using a representation by polynomials of k variables over $\mathbb{R}$. To see this, use the natural assignment of $x_i = v_i$ for $v = (v_1, \ldots, v_k)$, denoting it by x_v, and assign the following polynomial to $u = (u_1, \ldots, u_k)$:

$$f_u(x_1, \ldots, x_k) = \prod_{t=1}^{\lfloor k/p \rfloor} \left(k - tp - \sum_{i=1}^{k} \prod_{\substack{j=1 \\ j \neq u_i}}^{n} \frac{x_i - j}{u_i - j} \right). \tag{2.7}$$

The expression $\prod_{j \neq u_i} \frac{x_i - j}{u_i - j}$ is the monomial of the Lagrange interpolation polynomial and is equal to δ_{x_i, u_i}. Hence, we obtain that $f_u(x_u) \neq 0$ for any vertex u, whereas $f_u(x_v) = 0$ for any two distinct nonadjacent vertices u, v. As the Lagrange monomials yield values in $\{0, 1\}$, we can convert each f_u to a multilinear combination of these polynomials, $\tilde{f}_u$, while retaining the above properties. Note that there are n possibilities for the Lagrange monomials (determined by the value of u_i), and it is possible to express one as a linear combination of the rest. From this point, a calculation similar to that in Theorem 2.2 for the dimension of $\mathrm{Span}(\{\tilde{f}_u : u \in V\})$ gives the upper bound (2.2).

Remark 2.5. The value of $\alpha(K_n^{k_{(p)}})$ corresponds to a maximum size of a code C of k-letter words over $\mathbb{Z}_n$, where the Hamming distance between any two codewords is divisible by p. The case of *linear* such codes when $\mathbb{Z}_n$ is a field, that is, we add the restriction that C is a linear subspace of $\mathbb{Z}_n^k$, has been thoroughly studied; it is equivalent to finding a linear subspace of $\mathbb{Z}_n^k$ of maximal dimension, such that the Hamming weight of each element is divisible by p. It is known for this case that if p and n are relatively prime, then the dimension of C is at most k/p (see [22]), and hence the size of C is at most $n^{k/p}$. However, this bound does not hold for the nonlinear case (notice that this bound corresponds to the lower bound of Lemma 2.1). We give two examples of this:

1. Take $p = 3$ and $n = 4$. The divisible code bound implies an upper bound of $4^{1/3} \approx 1.587$, and yet $x_\alpha^{(3)}(K_4) \geq \sqrt{3} \approx 1.732$. This follows from the geometric construction of Theorem 2.2, which provides an independent set of size 9 in $K_3^{4_{(3)}} \subset K_4^{4_{(3)}}$, using only the coordinates $\{0, 1, 2\}$ (this result can be slightly improved by adding an all-3 vector to the above construction in the 12th power).
2. Take $p = 3$ and $n = 2$. The linear code bound is $2^{1/3} \approx 1.26$, whereas the following construction shows that $\alpha(K_2^{12_{(3)}}) \geq 24$, implying that $x_\alpha^{(3)}(K_2) \geq 24^{1/12} \approx 1.30$. Let $\{v_1, \ldots, v_{12}\}$ denote the rows of a binary Hadamard matrix of order 12 (such a matrix exists by Paley's theorem; cf., e.g., [12]). For all $i \neq j$, v_i and v_j have precisely 6 common coordinates, and hence the set $I = \{v_i\} \cup \{\overline{v}_i\}$ (where $\overline{v}_i$ denotes the complement of v_i modulo 2) is an independent set of size 24 in $K_2^{12_{(3)}}$. In fact, I is a maximum independent set

of $K_2^{12_{(3)}}$, as Delsarte's linear programming bound (described in section 3) implies that $\alpha(K_2^{12_{(3)}}) \le 24$.

2.3. The value of $x_\alpha^{(3)}(K_3)$. While the upper bound of Theorem 2.2 on $x_\alpha^{(p)}(K_n)$ is tight up to a constant factor, the effect of this constant on the independence numbers is exponential in the graph power, and we must resort to other techniques in order to obtain more accurate bounds. For instance, Theorem 2.2 implies that

$$1.732 \approx \sqrt{3} \le x_\alpha^{(3)}(K_3) \le 2^{H(\frac{1}{3})2^{\frac{1}{3}}} = \frac{3}{2^{1/3}} \approx 2.381.$$

In sections 3 and 4, we demonstrate the use of Delsarte's linear programming bound and Hoffman's eigenvalue bound for the above problem, and in both cases obtain the exact value of $\alpha(K_3^{k_{(3)}})$ under certain divisibility conditions. However, if we are merely interested in the value of $x_\alpha^{(3)}(K_3)$, a simpler consideration improves the bounds of Theorem 2.2 and shows that $x_\alpha^{(3)}(K_3) = \sqrt{3}$.

LEMMA 2.6. *For any $k \ge 1$, $\alpha(K_3^{k_{(3)}}) \le 3 \cdot \sqrt{3}^k$, and in particular $x_\alpha^{(3)}(K_3) = \sqrt{3}$.*

Proof. Treating vertices of K_3^k as vectors of $\mathbb{Z}_3^k$, notice that every two vertices $x = (x_1, \ldots, x_k)$ and $y = (y_1, \ldots, y_k)$ satisfy

$$\sum_{i=1}^{k} (x_i - y_i)^2 \equiv |\{i : x_i \ne y_i\}| \pmod 3,$$

and hence if I is an independent set in K_3^k, then

$$\sum_i (x_i - y_i)^2 \equiv 0 \pmod 3 \text{ for all } x, y \in I.$$

Let I denote a maximum independent set of K_3^k, and let $I_c = \{x \in I : \sum_i x_i^2 \equiv c \pmod 3\}$ for $c \in \{0, 1, 2\}$. For every $c \in \{0, 1, 2\}$ we have

$$\sum_i (x_i - y_i)^2 = 2c - 2x \cdot y \equiv 0 \pmod 3 \text{ for all } x, y \in I_c,$$

and hence $x \cdot y = c$ for all $x, y \in I_c$. Choose c for which $|I_c| \ge |I|/3$, and subtract an arbitrary element $z \in I_c$ from all the elements of I_c. This gives a set J of size at least $|I|/3$, which satisfies

$$x \cdot y = 0 \text{ for all } x, y \in J.$$

Since $\mathrm{Span}(J)$ is a self-orthogonal subspace of $\mathbb{Z}_3^k$, its dimension is at most $k/2$, and hence $|J| \le 3^{k/2}$. Altogether, $\alpha(K_3^k) \le 3 \cdot \sqrt{3}^k$, as required. □

3. Delsarte's linear programming bound for complete graphs. In this section, we demonstrate how Delsarte's linear programming bound may be used to derive precise values of independence numbers in p-powers of complete graphs. As this method was primarily used on binary codes, we include a short proof of the bound for a general alphabet.

3.1. Delsarte's linear programming bound. The linear programming bound follows from the relation between the distance distribution of codes and the Krawtchouk polynomials, defined as follows.

DEFINITION 3.1. *Let $n \in \mathbb{N}$ and take $q \geq 2$. The Krawtchouk polynomials $\mathcal{K}_k^{n;q}(x)$ for $k = 0, \ldots, n$ are defined by*

$$\mathcal{K}_k^{n;q}(x) = \sum_{j=0}^{k} \binom{x}{j}\binom{n-x}{k-j}(-1)^j(q-1)^{k-j}. \tag{3.1}$$

DEFINITION 3.2. *Let C be an n-letter code over the alphabet $\{1, \ldots, q\}$. The distance distribution of C, $B_0, B_1, \ldots, B_n$, is defined by*

$$B_k = \frac{1}{|C|}|\{(w_1, w_2) \in C^2 : \delta(w_1, w_2) = k\}| \quad (k = 0, \ldots, n),$$

where δ denotes the Hamming distance.

The Krawtchouk polynomials $\{\mathcal{K}_k^{n;q}(x)\}$ are sometimes defined with a normalizing factor of q^{-k}. Also, it is sometimes customary to define the distance distribution with a different normalizing factor, letting $A_k = \frac{B_k}{|C|}$, in which case A_k is the probability that a random pair of codewords has a Hamming distance k.

The Krawtchouk polynomials $\{\mathcal{K}_k^{n;q} : k = 0, \ldots, n\}$ form a system of orthogonal polynomials with respect to the weight function $w(x) = \frac{n!}{\Gamma(1+x)\Gamma(n+1-x)}(q-1)^x$, where Γ is the gamma function. For further information on these polynomials see, e.g., [20].

Delsarte [7] (see also [18]) presented a remarkable method for bounding the maximal size of a code with a given set of restrictions on its distance distribution. This relation is given in the next proposition, for which we include a short proof.

PROPOSITION 3.3. *Let C be a code of n-letter words over the alphabet $[q]$, whose distance distribution is $B_0, \ldots, B_n$. The following holds:*

$$\sum_{i=0}^{n} B_i \mathcal{K}_k^{n;q}(i) \geq 0 \quad \textit{for all } k = 0, \ldots, n. \tag{3.2}$$

Proof. Let $G = \mathbb{Z}_q^n$, and for every two functions $f, g : G \to \mathbb{C}$, define (as usual) their inner product $\langle f, g\rangle$ and their delta-convolution, $f * g$, as

$$\langle f, g\rangle = \int_G f(x)\overline{g(x)}dx = \frac{1}{|G|}\sum_{T\in G} f(T)\overline{g(T)},$$

$$(f * g)(s) = \int_G f(x)\overline{g(x-s)}dx.$$

Denoting the Fourier expansion of f by $f = \sum_{S\in G}\widehat{f}(S)\chi_S$, where $\chi_S(x) = \omega^{S\cdot x}$ and ω is the qth root of unity, it follows that for any $k = 0, \ldots, n$,

$$\sum_{S\in G:|S|=k}\widehat{f}(S) = \frac{1}{|G|}\sum_{i=0}^{n}\mathcal{K}_k^{n;q}(i)\sum_{T\in G:|T|=i} f(T), \tag{3.3}$$

where $|S|$ and $|T|$ denote the Hamming weights of $S, T \in G$. Since the delta-convolution satisfies

$$\widehat{f * g}(S) = \widehat{f}(S)\widehat{\overline{g}(S)},$$

every f satisfies

$$\widehat{f * f}(S) = |\widehat{f}(S)|^2 \geq 0. \tag{3.4}$$

Let f denote the characteristic function of the code C, $f(x) = \mathbf{1}_{\{x \in C\}}$, and notice that

$$(f * f)(S) = \frac{1}{|G|} \sum_{T \in G} f(T)\overline{f(T-S)} = \frac{1}{|G|}|\{T : T, T-S \in C\}|,$$

and thus

$$B_i = \frac{|G|}{|C|} \sum_{T:|T|=i} (f * f)(T). \tag{3.5}$$

Putting together (3.3), (3.4), and (3.5), we obtain

$$0 \leq \sum_{S:|S|=k} \widehat{f * f}(S) = \frac{1}{|G|} \sum_{i=0}^{n} \mathcal{K}_k^{n;q}(i) \sum_{T:|T|=i} (f * f)(T) = \frac{|C|}{|G|^2} \sum_{i=0}^{n} \mathcal{K}_k^{n;q}(i) B_i,$$

as required. □

Let $F \subset [n]$ be a set of forbidden distances between distinct codewords. Since $|C| = \sum_i B_i$, the following linear program provides an upper bound on the size of any code with no pairwise distances specified by F:

$$\text{maximize } \sum_i B_i \text{ subject to the constraints}$$

$$\begin{cases} B_0 = 1, \\ B_i \geq 0 \quad \text{for all } i, \\ B_i = 0 \quad \text{for all } i \in F, \\ \sum_{i=0}^{n} B_i \mathcal{K}_k^{n;q}(i) \geq 0 \quad \text{for all } k = 0, \ldots, n. \end{cases}$$

By examining the dual program, it is possible to formulate this bound as a minimization problem. The following proposition has been proved in various special cases (cf., e.g., [8], [16]). For the sake of completeness, we include a short proof of it.

PROPOSITION 3.4. *Let C be a code of n-letter words over the alphabet $[q]$, whose distance distribution is $B_0, \ldots, B_n$. Let $P(x) = \sum_{k=0}^{n} \alpha_k \mathcal{K}_k^{n;q}(x)$ denote an n-degree polynomial over $\mathbb{R}$. If $P(x)$ has the two properties*

$$\alpha_0 > 0 \quad \textit{and } \alpha_i \geq 0 \quad \textit{for all } i = 1, \ldots, n, \tag{3.6}$$

$$P(d) \leq 0 \quad \textit{whenever } B_d > 0 \textit{ for } d = 1, \ldots, n, \tag{3.7}$$

then $|C| \leq P(0)/\alpha_0$.

Proof. The MacWilliams transform of the vector $(B_0, \ldots, B_n)$ is defined as follows:

$$B'_k = \frac{1}{|C|} \sum_{i=0}^{n} \mathcal{K}_k^{n;q}(i) B_i. \tag{3.8}$$

By the Delsarte inequalities (stated in Proposition 3.3), $B'_k \geq 0$, and furthermore

$$B'_0 = \frac{1}{|C|} \sum_{i=0}^{n} \mathcal{K}_0^{n;q}(i) B_i = \frac{1}{|C|} \sum_i B_i = 1.$$

Therefore, as (3.6) guarantees that $\alpha_i \geq 0$ for $i > 0$, we get

$$\sum_{k=0}^{n} \alpha_k B'_k \geq \alpha_0. \tag{3.9}$$

On the other hand, $B_0 = 1$, and by (3.7), whenever $B_i > 0$ for some $i > 0$ we have $P(i) \leq 0$, and thus

$$\sum_{i=0}^{n} B_i P(i) \leq P(0). \tag{3.10}$$

Combining (3.9) and (3.10) with (3.8) gives

$$\alpha_0 \leq \sum_{k=0}^{n} \alpha_k B'_k = \frac{1}{|C|} \sum_{i=0}^{n} B_i \sum_{k=0}^{n} \alpha_k \mathcal{K}_k^{n;q}(i) = \frac{1}{|C|} \sum_{i=0}^{n} B_i P(i) \leq \frac{P(0)}{|C|},$$

and the result follows. □

We proceed with an application of the last proposition in order to bound the independence numbers of p-powers of complete graphs. In this case, the distance distribution is supported by $\{i : i \equiv 0 \pmod p\}$, and in section 3.2 we present polynomials which satisfy the properties of Proposition 3.4 and provide tight bounds on $\alpha(K_3^{k_{(3)}})$.

3.2. Improved estimations of $\alpha(K_3^{k_{(3)}})$. Recall that the geometric construction of Theorem 2.2 describes an independent set of size p^2 in $K_p^{p+1_{(p)}}$ for every p, which is a prime-power. In particular, this gives an independent set of size $3^{k/2}$ in $K_3^{k_{(3)}}$ for every $k \equiv 0 \pmod 4$. Using Proposition 3.4 we are able to deduce that indeed $\alpha(K_3^k) = 3^{k/2}$ whenever $k \equiv 0 \pmod 4$, whereas for $k \equiv 2 \pmod 4$ we prove that $\alpha(K_3^k) < \frac{1}{2} 3^{k/2}$.

THEOREM 3.5. *The following holds for any even integer k:*

$$\begin{cases} \alpha(K_3^k) = 3^{k/2}, & k \equiv 0 \pmod 4, \\ \frac{1}{3} 3^{k/2} \leq \alpha(K_3^k) < \frac{1}{2} 3^{k/2}, & k \equiv 2 \pmod 4. \end{cases}$$

Proof. Let k be an even integer, and define the following polynomials:

$$P(x) = \frac{2}{3} 3^{k/2} + \sum_{\substack{t=1 \\ t \not\equiv 0 (\mathrm{mod}\ 3)}}^{k} \mathcal{K}_t^{k;3}(x), \tag{3.11}$$

$$Q(x) = \frac{2}{3} 3^{k/2} + \sum_{\substack{t=0 \\ t \equiv 0 (\mathrm{mod}\ 3)}}^{k} \mathcal{K}_t^{k;3}(x). \tag{3.12}$$

Clearly, both P and Q satisfy (3.6), as $\mathcal{K}_0^{n;q} = 1$ for all n, q. It remains to show that P, Q satisfy (3.7) and to calculate $P(0), Q(0)$. As the following calculation will prove useful later on, we perform it for a general alphabet q and a general modulo p.

Denoting the qth root of unity by $\omega = \mathrm{e}^{2\pi i/q}$, we have

$$\begin{aligned}\sum_{\substack{t=0\\ t\equiv 0 (\mathrm{mod}\ p)}}^{k} \mathcal{K}_t^{k;q}(s) &= \sum_{\substack{t=0\\ t\equiv 0 (\mathrm{mod}\ p)}}^{k} \sum_{j=0}^{t} \binom{s}{j}\binom{k-s}{t-j}(-1)^j (q-1)^{t-j} \\ &= \sum_{j=0}^{s} \binom{s}{j}(-1)^j \sum_{\substack{l=0\\ j+l\equiv 0 (\mathrm{mod}\ p)}}^{k-s} \binom{k-s}{l}(q-1)^l \\ &= \sum_{j=0}^{s} \binom{s}{j}(-1)^j \sum_{l=0}^{k-s} \binom{k-s}{l}(q-1)^l \frac{1}{q}\sum_{t=0}^{q-1} \omega^{(j+l)t} \\ &= \delta_{s,0}\cdot q^{k-1} + \frac{1}{q}\sum_{t=1}^{q-1}(1+(q-1)\omega^t)^{k-s}(1-\omega^t)^s, \end{aligned} \tag{3.13}$$

where the last equality is by the fact that $\sum_{j=0}^{s}\binom{s}{j}(-1)^j = \delta_{s,0}$, and therefore the summand for $t=0$ vanishes if $s\neq 0$ and is equal to q^{k-1} if $s=0$. Repeating the above calculation for $t \not\equiv 0 \pmod p$ gives

$$\begin{aligned}\sum_{\substack{t=0\\ t\not\equiv 0 (\mathrm{mod}\ p)}}^{k} \mathcal{K}_t^{k;q}(s) &= \sum_{j=0}^{s} \binom{s}{j}(-1)^j \sum_{l=0}^{k-s} \binom{k-s}{l}(q-1)^l \left(1 - \frac{1}{q}\sum_{t=0}^{q-1}\omega^{(j+l)t}\right) \\ &= \delta_{s,0}\cdot(q^k - q^{k-1}) - \frac{1}{q}\sum_{t=1}^{q-1}(1+(q-1)\omega^t)^{k-s}(1-\omega^t)^s. \end{aligned} \tag{3.14}$$

Define

$$\xi_s = \frac{1}{q}\sum_{t=1}^{q-1}(1+(q-1)\omega^t)^{k-s}(1-\omega^t)^s,$$

and consider the special case $p=q=3$. The fact that $\omega^2 = \overline{\omega}$ implies that

$$\xi_s = \frac{2}{3}\mathrm{Re}\left((1+2\omega)^{k-s}(1-\omega)^s\right) = \frac{2}{3}\mathrm{Re}\left((\sqrt{3}i)^{k-s}(\sqrt{3}\mathrm{e}^{-\frac{\pi}{6}i})^s\right) = \frac{2}{3}\sqrt{3}^k\cos\left(\frac{\pi k}{2} - \frac{2\pi s}{3}\right), \tag{3.15}$$

and for even values of k and $s\equiv 0 \pmod 3$ we deduce that

$$\xi_s = \frac{2}{3}3^{k/2}(-1)^{k/2}. \tag{3.16}$$

Therefore, $\xi_s = \frac{2}{3}3^{k/2}$ whenever $s\equiv 0 \pmod 3$ and $k\equiv 0 \pmod 4$, and (3.14) gives the following for any $k\equiv 0 \pmod 4$:

$$\begin{aligned} P(0) &= \frac{2}{3}3^{k/2} + \frac{2}{3}3^k - \xi_0 = \frac{2}{3}3^k, \\ P(s) &= \frac{2}{3}3^{k/2} - \xi_s = 0 \quad \text{for any } 0\neq s\equiv 0 \pmod 3. \end{aligned}$$

Hence, $P(x)$ satisfies the requirements of Proposition 3.4 and we deduce that for any $k\equiv 0 \pmod 4$,

$$\alpha(K_3^k) \leq \frac{P(0)}{\frac{2}{3}3^{k/2}} = 3^{k/2}.$$

As mentioned before, the construction used for the lower bound on $x_\alpha^{(p)}(K_3)$ implies that this bound is indeed tight whenever $4 \mid k$.

For $k \equiv 2 \pmod 4$ and $s \equiv 0 \pmod 3$ we get $\xi_s = -\frac{2}{3}3^{k/2}$, and by (3.13) we get

$$Q(0) = \frac{2}{3}3^{k/2} + 3^{k-1} + \xi_0 = 3^{k-1},$$
$$Q(s) = \frac{2}{3}3^{k/2} + \xi_s = 0 \quad \text{for any } 0 \neq s \equiv 0 \pmod 3.$$

Again, $Q(x)$ satisfies the requirements of Proposition 3.4 and we obtain the following bound for $k \equiv 2 \pmod 4$:

$$\alpha(K_3^k) \leq \frac{Q(0)}{\frac{2}{3}3^{k/2}+1} = \frac{3^k}{2 \cdot 3^{k/2}+3} < \frac{1}{2}3^{k/2}.$$

To conclude the proof, take a maximum independent set of size $\sqrt{3}^l$ in K_3^l, where $l = k-2$, for a lower bound of $\frac{1}{3}3^{k/2}$. □

4. Hoffman's bound on independence numbers of p-powers. In this section we apply spectral analysis in order to bound the independence numbers of p-powers of d-regular graphs. The next theorem generalizes Theorem 2.9 of [4] by considering tensor powers of adjacency matrices whose values are pth roots of unity.

THEOREM 4.1. *Let G be a nontrivial d-regular graph on n vertices, whose eigenvalues are $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$, and let $\lambda = \max\{\lambda_2, |\lambda_n|\}$. The following holds for any $p \geq 2$:*

(4.1)
$$x_\alpha^{(p)}(G) \leq \max\left\{\sqrt{n^2 - 2\left(1-\cos\left(\frac{2\pi}{p}\right)\right)d(n-d)}, \lambda\sqrt{2-2\cos\left(\frac{2\pi}{p}\left\lfloor\frac{p}{2}\right\rfloor\right)}\right\}.$$

Proof. Let $A = A_G$ denote the adjacency matrix of G, and define the matrices B_t for $t \in \mathbb{Z}_p$ as follows:

$$B_t = J_n + (\omega^t - 1)A, \tag{4.2}$$

where $\omega = \mathrm{e}^{2\pi i/p}$ is the pth root of unity, and J_n is the all-ones matrix of order n. In other words,

$$(B_t)_{uv} = \omega^{tA_{uv}} = \begin{cases} \omega^t & \text{if } uv \in E(G), \\ 1 & \text{if } uv \notin E(G). \end{cases}$$

By the definition of the matrix tensor product $\otimes$, it follows that for all $u = (u_1, \ldots, u_k)$ and $v = (v_1, \ldots, v_k)$ in G^k,

$$(B_t^{\otimes k})_{u,v} = \omega^{t|\{i \,:\, u_i v_i \in E(G)\}|},$$

and

$$\sum_{t=0}^{p-1}(B_t^{\otimes k})_{u,v} = \begin{cases} p & \text{if } |\{i : u_i v_i \in E(G)\}| \equiv 0 \pmod p, \\ 0 & \text{otherwise.} \end{cases}$$

Recalling that $uv \in E(G^k)$ iff $|\{i : u_i v_i \in E(G)\}| \not\equiv 0 \pmod p$, we get

$$A_{G^k} = J_{n^k} - \frac{1}{p}\sum_{t=0}^{p-1} B_t^{\otimes k} = \frac{p-1}{p}J_{n^k} - \frac{1}{p}\sum_{t=1}^{p-1} B_t^{\otimes k}. \tag{4.3}$$

The above relation enables us to obtain expressions for the eigenvalues of G^k and then apply the following bound, proved by Hoffman (see [13], [17]): every regular nontrivial graph H on N vertices, whose eigenvalues are $\mu_1 \geq \cdots \geq \mu_N$, satisfies

$$\alpha(H) \leq \frac{-N\mu_N}{\mu_1 - \mu_N}. \tag{4.4}$$

Recall that J_n has a single nonzero eigenvalue of n corresponding to the all-ones vector $\underline{1}$. Hence, (4.2) implies that $\underline{1}$ is an eigenvector of B_t with an eigenvalue of $n + (\omega^t - 1)d$, and the remaining eigenvalues of B_t are $\{(\omega^t - 1)\lambda_i : i > 1\}$. By well-known properties of tensor products, we obtain that the largest eigenvalue of $H = G^k$ (which is its degree of regularity) is

$$\begin{aligned}\mu_1 &= n^k - \frac{1}{p}\sum_{t=0}^{p-1}(n + (\omega^t - 1)d)^k = n^k - \frac{1}{p}\sum_{j=0}^{k}\binom{k}{j}(n-d)^{k-j}d^j\sum_{t=0}^{p-1}\omega^{jt} \\ &= n^k - \sum_{\substack{j=0 \\ j\equiv 0 (\mathrm{mod}\ p)}}^{k}\binom{k}{j}(n-d)^{k-j}d^j, \end{aligned} \tag{4.5}$$

and the remaining eigenvalues are of the form

$$\mu(\lambda_{i_1}, \ldots, \lambda_{i_s}) = -\frac{1}{p}\sum_{t=1}^{p-1}(n + (\omega^t - 1)d)^{k-s}\prod_{j=1}^{s}(\omega^t - 1)\lambda_{i_j}, \tag{4.6}$$

where $0 < s \leq k$ and $1 < i_j \leq n$ for all j (corresponding to an eigenvector which is a tensor-product of the eigenvectors of λ_{i_j} for $j = 1, \ldots, s$ and $\underline{1}^{\otimes k-s}$). The following holds for all such choices of s and $\{\lambda_{i_j}\}$:

$$\begin{aligned}|\mu(\lambda_{i_1}, \ldots, \lambda_{i_s})| &\leq \max_{1\leq t\leq p-1}\left|(n + (\omega^t - 1)d)^{k-s}\prod_{i=1}^{s}(\omega^t - 1)\lambda_{i_j}\right| \\ &\leq \max_{1\leq t\leq p-1}|n + (\omega^t - 1)d|^{k-s}(|\omega^t - 1|\lambda)^s \\ &\leq \max_{1\leq t\leq p-1}\left(\max\{|n + (\omega^t - 1)d|, \lambda|\omega^t - 1|\}\right)^k.\end{aligned}$$

Since for any $1 \leq t \leq p-1$ we have

$$|n + (\omega^t - 1)d|^2 = n^2 - 2\left(1 - \cos\left(\frac{2\pi t}{p}\right)\right)d(n-d) \leq n^2 - 2\left(1 - \cos\left(\frac{2\pi}{p}\right)\right)d(n-d),$$

$$|\omega^t - 1|^2 = 2 - 2\cos\left(\frac{2\pi t}{p}\right) \leq 2 - 2\cos\left(\frac{2\pi}{p}\left\lfloor\frac{p}{2}\right\rfloor\right),$$

it follows that

$$|\mu(\lambda_{i_1}, \ldots, \lambda_{i_s})| \leq (\max\{\rho_1, \rho_2\})^k,$$

where

$$\rho_1 = \sqrt{n^2 - 2\left(1 - \cos\left(\frac{2\pi}{p}\right)\right)d(n-d)},$$

$$\rho_2 = \lambda\sqrt{2 - 2\cos\left(\frac{2\pi}{p}\left\lfloor\frac{p}{2}\right\rfloor\right)}.$$

By the same argument, (4.5) gives

$$|\mu_1| \geq n^k - \rho_1^k,$$

and applying Hoffman's bound (4.4), we get

$$\alpha(G^k) \leq \frac{-n^k \mu_{n^k}}{\mu_1 - \mu_{n^k}} \leq \frac{(\max\{\rho_1, \rho_2\})^k}{1 - (\frac{\rho_1}{n})^k + (\frac{\max\{\rho_1,\rho_2\}}{n})^k}. \tag{4.7}$$

To complete the proof, we claim that $\max\{\rho_1, \rho_2\} \leq n$, and hence the denominator in the expression above is $\Theta(1)$ as $k \to \infty$. Clearly, $\rho_1 \leq n$, and a simple argument shows that $\lambda \leq n/2$ and hence $\rho_2 \leq n$ as well. To see this, consider the matrix A^2 whose diagonal entries are d; we have

$$nd = \operatorname{tr} A^2 = \sum_i \lambda_i^2 \geq d^2 + \lambda^2,$$

implying that $\lambda \leq \sqrt{d(n-d)} \leq \frac{n}{2}$. Altogether, taking the kth root and letting k tend to ∞ in (4.7), we obtain that $x_\alpha^{(p)}(G) \leq \max\{\rho_1, \rho_2\}$, as required. □

Examples. For $p = 2, 3$ the above theorem gives

$$x_\alpha^{(2)}(G) \leq \max\{|n - 2d|, 2\lambda\},$$
$$x_\alpha^{(3)}(G) \leq \max\{\sqrt{n^2 - 3d(n-d)}, \sqrt{3}\lambda\}.$$

Since the eigenvalues of K_3 are $\{2, -1, -1\}$, this immediately provides another proof for the fact that $x_\alpha^{(3)}(K_3) \leq \sqrt{3}$. Note that, in general, the upper bounds derived in this method for $x_\alpha^{(p)}(K_n)$ are useful only for small values of n, and tend to n as $n \to \infty$, whereas by the results of section 2 we know that $x_\alpha^{(p)}(K_n) = \Theta(n^{1/p})$.

Consider $d = d(n) = \frac{n}{2} + O(\sqrt{n})$, and let $G \sim G_{n,d}$ denote a random d-regular graph on n vertices. By the results of [14], $\lambda = \max\{\lambda_2, |\lambda_n|\} = O(n^{3/4})$, and thus Theorem 4.1 implies that $x_\alpha^{(2)}(G) = O(n^{3/4})$, and $x_\alpha^{(3)}(G) \leq (1+o(1))\frac{n}{2}$. We note that one cannot hope for better bounds on $x_\alpha^{(3)}$ in this method, as ρ_1 attains its minimum at $d = \frac{n}{2}$.

Remark 4.2. The upper bound (4.1) becomes weaker as p increases. However, if p is divisible by some $q \geq 2$, then clearly any independent set of $G^{k_{(p)}}$ is also an independent set of $G^{k_{(q)}}$, and in particular $x_\alpha^{(p)}(G) \leq x_\alpha^{(q)}(G)$. Therefore, when applying Theorem 4.1 on some graph G, we can replace p by the minimal $q \geq 2$, which divides p. For instance, $x_\alpha^{(4)}(G) \leq x_\alpha^{(2)}(G) \leq \max\{|n - 2d|, 2\lambda\}$, whereas substituting $p = 4$ in (4.1) gives the slightly weaker bound $x_\alpha^{(4)}(G) \leq \{\sqrt{(n-d)^2 + d^2}, 2\lambda\}$.

Remark 4.3. In the special case $G = K_n$, the eigenvalues of G are $\{n - 1, -1, \ldots, -1\}$, and the general expression for the eigenvalues of G^k in (4.6) takes the form (note that $\lambda_{i_j} = -1$ for all $1 \leq j \leq s$)

$$\mu(s) = -\frac{1}{p} \sum_{t=1}^{p-1} (1 + (n-1)\omega^t)^{k-s} (1 - \omega^t)^s,$$

and as $s > 0$, we obtain the following from (3.14):

$$\mu(s) = \sum_{\substack{t=0 \\ t \not\equiv 0 (\mathrm{mod}\ p)}}^{k} \mathcal{K}_t^{k;q}(s).$$

Similarly, comparing (4.5) to (3.14) gives

$$\mu_1 = \sum_{\substack{t=0 \\ t\not\equiv 0 (\mathrm{mod}\ p)}}^{k} \mathcal{K}_t^{k;q}(0).$$

It is possible to deduce this result directly, as K_n^k is a Cayley graph over $\mathbb{Z}_n^k$ with the generator set $S = \{x : |x| \not\equiv 0 \pmod p\}$, where $|x|$ denotes the Hamming weight of x. It is well known that the eigenvalues of a Cayley graph are equal to the character sums of the corresponding group elements. Since for any $k = 0, \ldots, n$ and any $x \in \mathbb{Z}_n^k$ the Krawtchouk polynomial $\mathcal{K}_k^{n;q}$ satisfies

$$\mathcal{K}_k^{n;q}(|x|) = \sum_{y\in\mathbb{Z}_n^k : |y|=k} \chi_y(x),$$

the eigenvalue corresponding to $y \in \mathbb{Z}_n^k$ is

$$\mu(y) = \sum_{x\in S} \chi_x(y) = \sum_{\substack{t=0 \\ t\not\equiv 0 \pmod p}}^{k} \sum_{x:|x|=t} \chi_x(y) = \sum_{\substack{t=0 \\ t\not\equiv 0 \pmod p}}^{k} \mathcal{K}_t^{k;q}(|y|).$$

Remark 4.4. The upper bound on $x_\alpha^{(p)}$ was derived from an asymptotic analysis of the smallest eigenvalue μ_{n^k} of G^k. Tight results on $\alpha(G^k)$ may be obtained by a careful analysis of the expression in (4.6). To illustrate this, we consider the case $G = K_3$ and $p = 3$. Combining the previous remark with (3.14) and (3.15), we obtain that the eigenvalues of $K_3^{k_{(3)}}$ are

$$\mu_1 = \frac{2}{3}3^k - \frac{2}{3}\sqrt{3}^k \cos\left(\frac{\pi k}{2}\right),$$
$$\mu(s) = -\frac{2}{3}\sqrt{3}^k \cos\left(\frac{\pi k}{2} - \frac{2\pi s}{3}\right) \quad \text{for } 0 < s \le k.$$

Noticing that $\mu(s)$ depends only on the values of $s \pmod 3$ and $k \pmod 4$, we can determine the minimal eigenvalue of G^k for each given power k and deduce that

$$\alpha(G^k) \le 3^{k/2} \qquad \text{if } k \equiv 0 \pmod 4,$$
$$\alpha(G^k) \le \frac{3^{k+1}}{3 + 2\cdot 3^{(k+1)/2}} < \frac{1}{2}3^{(k+1)/2} \qquad \text{if } k \equiv 1 \pmod 2,$$
$$\alpha(G^k) \le \frac{3^k}{3 + 2\cdot 3^{k/2}} < \frac{1}{2}3^{k/2} \qquad \text{if } k \equiv 2 \pmod 4,$$

matching the results obtained by the Delsarte linear programming bound.

5. Ramsey subgraphs in large *p*-powers of any graph. In order to prove a polylogarithmic upper bound on the clique sizes of p-powers of a graph G, we use an algebraic argument, similar to the method of representation by polynomials described in the section 2. We note that the same approach provides an upper bound on the size of independent sets. However, for this latter bound, we require another property, which relates the problem to strong graph products and to the Shannon capacity of a graph.

The kth *strong* power of a graph G (also known as the *and* power), denoted by $G^{\wedge k}$, is the graph whose vertex set is $V(G)^k$, where two distinct k-tuples $u \neq v$ are adjacent iff each of their coordinates is either equal or adjacent in G:

$$(u_1,\dots,u_k)(v_1,\dots,v_k) \in E(G^{\wedge k}) \text{ iff for all } i=1,\dots,k:\ u_i = v_i \text{ or } u_iv_i \in E(G).$$

In 1956, Shannon [19] related the independence numbers of strong powers of a fixed graph G to the effective alphabet size in a zero-error transmission over a noisy channel. Shannon showed that the limit of $\alpha(G^{\wedge k})^{\frac{1}{k}}$ as $k \to \infty$ exists and equals $\sup_k \alpha(G^{\wedge k})^{\frac{1}{k}}$, by supermultiplicativity; this limit is denoted by $c(G)$, the Shannon capacity of G. It follows that $c(G) \geq \alpha(G)$, and in fact equality holds for all perfect graphs. However, for nonperfect graphs, $c(G)$ may exceed $\alpha(G)$, and the smallest (and most famous) example of such a graph is C_5, the cycle on 5 vertices, where $\alpha(C_5) = 2$ and yet $c(C_5) \geq \alpha(C_5^{\wedge 2})^{\frac{1}{2}} = \sqrt{5}$. The seemingly simple question of determining the value of $c(C_5)$ was solved only in 1979 by Lovász [17], who introduced the ϑ-function to show that $c(C_5) = \sqrt{5}$.

The next theorem states the bound on the clique numbers of $G^{k_{(p)}}$ and relates the Shannon capacity of $\overline{G}$, the complement of G, to bounds on independent sets of $G^{k_{(p)}}$.

THEOREM 5.1. *Let G denote a graph on n vertices and let $p \geq 2$ be a prime. The clique number of $G^{k_{(p)}}$ satisfies*

$$\omega(G^{k_{(p)}}) \leq \binom{kn+p-1}{p-1}, \tag{5.1}$$

and if I is an independent set of both $G^{k_{(p)}}$ and $\overline{G}^{\wedge k}$, then

$$|I| \leq \binom{kn+\lfloor \frac{k}{p} \rfloor}{\lfloor \frac{k}{p} \rfloor}. \tag{5.2}$$

Moreover, if in addition G is regular, then

$$\omega(G^{k_{(p)}}) \leq \binom{k(n-1)+p}{p-1}, \quad |I| \leq \binom{k(n-1)+\lfloor \frac{k}{p} \rfloor + 1}{\lfloor \frac{k}{p} \rfloor}. \tag{5.3}$$

The above theorem implies that if S is an independent set of $\overline{G}^{\wedge k}$, then any independent set I of $G^{k_{(p)}}[S]$, the induced subgraph of $G^{k_{(p)}}$ on S, satisfies inequality (5.2). For large values of k, by definition there exists such a set S of size roughly $c(\overline{G})^k$. Hence, there are induced subgraphs of $G^{k_{(p)}}$ of size tending to $c(\overline{G})^k$ whose clique number and independence number are bounded by the expressions in (5.1) and (5.2), respectively.

In the special case $G = K_n$, the graph $\overline{G}^{\wedge k}$ is an edgeless graph for any k, and hence

$$\alpha(K_n^{k_{(p)}}) \leq \binom{k(n-1)+\lfloor \frac{k}{p} \rfloor + 1}{\lfloor \frac{k}{p} \rfloor} \leq \left(ep(n-1)+\mathrm{e}+o(1)\right)^{k/p},$$

where the $o(1)$-term tends to 0 as $k \to \infty$. This implies an upper bound on $x_\alpha^{(p)}(K_n)$ which nearly matches the upper bound of Theorem 2.2 for large values of p.

Proof. Let $g_1 : V(G) \to \mathbb{Z}_p^m$ and $g_2 : V(G) \to \mathbb{C}^m$, for some integer m, denote two representations of G by m-dimensional vectors satisfying the following for any (not necessarily distinct) $u, v \in V(G)$:

$$\begin{cases} g_i(u) \cdot g_i(v) = 0 & \text{if } uv \in E(G) \\ g_i(u) \cdot g_i(v) = 1 & \text{otherwise} \end{cases} \quad (i = 1, 2). \tag{5.4}$$

It is not difficult to see that such representations exist for any graph G. For instance, the standard basis of n-dimensional vectors is such a representation for $G = K_n$. In the general case, it is possible to construct such vectors inductively, in a way similar to a Gram–Schmidt orthogonalization process. To see this, define the lower diagonal $|V(G)| \times |V(G)|$ matrix M as follows:

$$M_{k,i} = \begin{cases} -\sum_{j=1}^{i-1} M_{k,j} M_{i,j}, & i < k,\ v_i v_k \in E(G), \\ 1 - \sum_{j=1}^{i-1} M_{k,j} M_{i,j}, & i < k,\ v_i v_k \notin E(G), \\ 1, & i = k, \\ 0, & i > k. \end{cases}$$

The rows of M satisfy (5.4) for any distinct $u, v \in V(G)$, and it remains to modify the inner product of any vector with itself into 1 without changing the inner products of distinct vectors. This is clearly possible over $\mathbb{Z}_p$ and $\mathbb{C}$ using additional coordinates.

Consider $G^{k_{(p)}}$, and define the vectors $w_u = g_1(u_1) \circ \cdots \circ g_1(u_k)$ for $u = (u_1, \ldots, u_k) \in V(G^k)$, where $\circ$ denotes vector concatenation. By definition

$$w_u \cdot w_v \equiv k - |\{i : u_i v_i \in E(G)\}| \pmod{p}$$

for any $u, v \in V(G^k)$, and hence if S is a maximum clique of G^k, then $w_u \cdot w_v \not\equiv k \pmod{p}$ for any $u, v \in S$. It follows that if B is the matrix whose columns are w_u for $u \in S$, then $C = B^t B$ has values which are $k \pmod{p}$ on its diagonal and entries which are not congruent to k modulo p anywhere else. Clearly, $\operatorname{rank}(C) \leq \operatorname{rank}(B)$, and we claim that $\operatorname{rank}(B) \leq kn$, and that, furthermore, if G is regular, then $\operatorname{rank}(B) \leq k(n-1)+1$. To see this, notice that as the dimension of $\operatorname{Span}(\{g_1(u) : u \in V\})$ is at most n, the dimension of the span of $\{w_u : u \in G^k\}$ is at most kn. If in addition G is regular, define $z = \sum_{u \in V} g_1(u)$ (assuming without loss of generality that $z \neq 0$), and observe that by (5.4), each of the vectors w_u is orthogonal to the following $k-1$ linearly independent vectors:

$$\{z \circ (-z) \circ \underline{0}^{\circ(k-2)},\ \underline{0} \circ z \circ (-z) \circ \underline{0}^{\circ(k-3)}, \ldots,\ \underline{0}^{\circ(k-2)} \circ z \circ (-z)\}. \tag{5.5}$$

Similarly, the vectors $w'_u = g_2(u_1) \circ \cdots \circ g_2(u_k)$ satisfy the following for any $u, v \in V(G^k)$:

$$w'_u \cdot w'_v = k - |\{i : u_i v_i \in E(G)\}|.$$

Let I denote an independent set of $G^{k_{(p)}}$, which is also an independent set of $\overline{G}^{\wedge k}$. By the definition of $\overline{G}^{\wedge k}$, every $u, v \in I$ shares a coordinate i such that $u_i v_i \in E(G)$, and combining this with the definition of $G^{k_{(p)}}$, we obtain

$$0 < |\{i : u_i v_i \in E(G)\}| \equiv 0 \pmod{p} \text{ for any } u, v \in I.$$

Therefore, for any $u \neq v \in I$,

$$w'_u \cdot w'_v = k - tp \text{ for some } t \in \left\{1, \ldots, \left\lfloor \frac{k}{p} \right\rfloor\right\},$$

and if B' is the matrix whose columns are w'_u for $u \in I$, then $C' = B'^t B'$ has the entries k on its diagonal and entries of the form $k - tp$, $0 < t \le \lfloor \frac{k}{p} \rfloor$, anywhere else. Again, the definition of g_2 implies that $\mathrm{rank}(C') \le kn$, and in case G is regular, $\mathrm{rank}(C') \le k(n-1)+1$ (each w'_u is orthogonal to the vectors of (5.5) for $z = \sum_{u \in V} g_2(u)$).

Define the following polynomials:

$$f_1(x) = \prod_{\substack{j \in \mathbb{Z}_p \\ j \not\equiv k \pmod p}} (j - x), \qquad f_2(x) = \prod_{t=1}^{\lfloor \frac{k}{p} \rfloor} (k - tp - x). \tag{5.6}$$

By the discussion above, the matrices D, D' obtained by applying f_1, f_2 on each element of C, C', respectively, are nonzero on the diagonal and zero anywhere else, and, in particular, they are of full rank: $\mathrm{rank}(D) = |S|$ and $\mathrm{rank}(D') = |I|$. Recalling that the ranks of C and C' are at most kn, and at most $k(n-1)+1$ if G is regular, the proof is completed by the following simple lemma of [1].

LEMMA 5.2 (see [1]). *Let $B = (b_{i,j})$ be an $n \times n$ matrix of rank d, and let $P(x)$ be an arbitrary polynomial of degree k. Then the rank of the $n \times n$ matrix $(P(b_{i,j}))$ is at most $\binom{k+d}{k}$. Moreover, if $P(x) = x^k$, then the rank of $(P(b_{i,j}))$ is at most $\binom{k+d-1}{k}$.* □

For large values of k, the upper bounds provided by the above theorem are

$$\omega(H) \le \binom{(1+o(1))kn}{p},$$
$$\alpha(H) \le \binom{(1+o(1))kn}{k/p}.$$

This gives the following immediate corollary, which states that large p-powers of any nontrivial graph G contain a large induced subgraph without large homogeneous sets.

COROLLARY 5.3. *Let G be some fixed nontrivial graph and fix a prime p.*

1. *Let S denote a maximum clique of G, and set $\lambda = \log \omega(G) = \log \alpha(\overline{G})$. For any k, the induced subgraph of $G^{k_{(p)}}$ on S^k, $H = G^{k_{(p)}}[S^k]$, is a graph on $N = \exp(k\lambda)$ vertices which satisfies*

$$\omega(H) = O(\log^p N), \qquad \alpha(H) \le N^{(1+o(1))\frac{\log(np)+1}{p\lambda}}.$$

2. *The above formula holds when taking $\lambda = \frac{\log \alpha(\overline{G}^{\wedge \ell})}{\ell}$ for some $\ell \ge 1$ dividing k, S a maximum clique of $\overline{G}^{\wedge \ell}$, and $H = G^{k_{(p)}}[S^{k/\ell}]$. In particular, for sufficiently large values of k, $G^{k_{(p)}}$ has an induced subgraph H on $N = \exp\big((1-o(1))k \log c(\overline{G})\big)$ vertices satisfying*

$$\omega(H) = O(\log^p N), \qquad \alpha(H) \le N^{(1+o(1))\frac{\log(np)+1}{p \log c(\overline{G})}}.$$

Remark 5.4. In the special case $G = K_n$, where n, p are large and $k > p$, the bound on $\omega(K_n^k)$ is $\binom{(1+o(1))kn}{p}$, whereas the bound on $\alpha(K_n^k)$ is $\binom{(1+o(1))kn}{k/p}$. Hence, the optimal mutual bound on these parameters is obtained at $k = p^2$. Writing $H = K_n^k$, $N = n^k = n^{p^2}$, and $p = n^c$ for some $c > 0$, we get

$$p = \sqrt{\frac{(2c + o(1)) \log N}{\log \log N}}$$

and

$$\max\{\omega(H), \alpha(H)\} \leq ((1+o(1))epn)^p = \exp\left(\left(\frac{1+c}{\sqrt{2c}} + o(1)\right)\sqrt{\log N \log\log N}\right).$$

The last expression is minimized for $c = 1$, and thus the best Ramsey construction in p-powers of K_n is obtained at $p = n$ and $k = p^2$, giving a graph H on N vertices with no independence set or clique larger than $\exp\left((1+o(1))\sqrt{2\log N \log\log N}\right)$ vertices. This special case matches the bound of the Frankl–Wilson Ramsey construction, and is in fact closely related to that construction, as we next describe.

The graph FW_N, where $N = \binom{p^3}{p^2-1}$ for some prime p, is defined as follows: its vertices are the N possible choices of (p^2-1)-element sets of $[p^3]$, and two vertices are adjacent iff the intersection of their corresponding sets is congruent to -1 modulo p. Observe that the vertices of the graph $K_n^{k_{(p)}}$ for $n = p$ and $k = p^2$, as described above, can be viewed as k-element subsets of $[kn]$, where the choice of elements is restricted to precisely one element from each of the k subsets $\{(j-1)n+1, \ldots, jn\}$, $j \in [k]$ (the jth subset corresponds to the jth coordinate of the k-tuple). In this formulation, the intersection of two sets corresponds to the number of common coordinates between the corresponding k-tuples. As $k = p^2 \equiv 0 \pmod{p}$, it follows that two vertices in $K_p^{p^2_{(p)}}$ are adjacent iff the intersection of their corresponding sets is not congruent to 0 modulo p. Altogether, we obtain that $K_p^{p^2_{(p)}}$ is an induced subgraph of a slight variant of FW_N, where the differences are in the cardinality of the sets and the criteria for adjacency.

Another relation between the two constructions is the following: one can identify the vertices of $K_2^{p^3_{(p)}}$ with all possible subsets of $[p^3]$, where two vertices are adjacent iff the intersection of their corresponding sets is not congruent to 0 modulo p. In particular, $K_2^{p^3_{(p)}}$ contains all the (p^2-1)-element subsets of $[p^3]$, a variant of FW_N for the above value of N (the difference lies in the criteria for adjacency).

We note that the method of proving Theorem 5.1 can be applied to the graph FW_N, giving yet another simple proof for the properties of this well-known construction.

Acknowledgment. The authors would like to thank Simon Litsyn and Benny Sudakov for useful discussions.

REFERENCES

[1] N. Alon, *Problems and results in extremal combinatorics.* I, Discrete Math., 273 (2003), pp. 31–53.

[2] N. Alon, *Probabilistic methods in extremal finite set theory*, in Extremal Problems for Finite Sets, Bolyai Soc. Math. Stud. 3, P. Frankl, Z. Füredi, G. O. H. Katona, and D. Miklós, eds., Visegrád, Hungary, 1991, pp. 39–57.

[3] N. Alon, *The Shannon capacity of a union*, Combinatorica, 18 (1998), pp. 301–310.

[4] N. Alon and E. Lubetzky, *Codes and Xor graph products*, Combinatorica, 27 (2007), pp. 13–33.

[5] N. Alon and J. H. Spencer, *The Probabilistic Method*, 2nd ed., Wiley, New York, 2000.

[6] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson, 2-*source dispersers for sub-polynomial entropy and Ramsey graphs beating the Frankl-Wilson construction*, in Proceedings of the 38th ACM Symposium on Theory of Computing, 2006, pp. 671–680.

[7] P. Delsarte, *Bounds for unrestricted codes by linear programming*, Philips Res. Rep., 27 (1972), pp. 272–289.

[8] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl., 10 (1973), pp. 1–97.

[9] P. Erdős, *Some remarks on the theory of graphs*, Bull. Amer. Math. Soc., 53 (1947), pp. 292–294.
[10] P. Frankl and R. Wilson, *Intersection theorems with geometric consequences*, Combinatorica, 1 (1981), pp. 357–368.
[11] V. Grolmusz, *Low rank co-diagonal matrices and Ramsey graphs*, Electron. J. Combin., 7 (2000).
[12] M. Hall, *Combinatorial Theory*, 2nd ed., Wiley, New York, 1986.
[13] A. J. Hoffman, *On eigenvalues and colorings of graphs*, in Graph Theory and Its Applications, B. Harris, ed., Academic Press, New York, London, 1970, pp. 79–91.
[14] M. Krivelevich, B. Sudakov, V. Vu, and N. Wormald, *Random regular graphs of high degree*, Random Structures Algorithms, 18 (2001), pp. 346–363.
[15] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed., Cambridge University Press, Cambridge, UK, 2001.
[16] S. Litsyn, *New upper bounds on error exponents*, IEEE Trans. Inform. Theory, 45 (1999), pp. 385–398.
[17] L. Lovász, *On the Shannon capacity of a graph*, IEEE Trans. Inform. Theory, 25 (1979), pp. 1–7.
[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North–Holland, Amsterdam, 1977.
[19] C. E. Shannon, *The zero-error capacity of a noisy channel*, IRE Trans. Inform. Theory, 2 (3) (1956), pp. 8–19.
[20] G. Szegő, *Orthogonal Polynomials*, 4th ed., Amer. Math. Soc. Colloq. Publ. 23, AMS, Providence, RI, 1975.
[21] A. Thomason, *Graph products and monochromatic multiplicities*, Combinatorica, 17 (1997), pp. 125–134.
[22] H. N. Ward, *Divisible codes*, Arch. Math. (Basel), 36 (1981), pp. 485–494.
[23] H. N. Ward, *Divisible codes: A survey*, Serdica Math. J., 27 (2001), pp. 263–278.