Codes and Xor graph products

Noga Alon* Eyal Lubetzky †

November 20, 2005

Abstract

What is the maximum possible number, $f_3(n)$, of vectors of length n over $\{0,1,2\}$ such that the Hamming distance between every two is even? What is the maximum possible number, $g_3(n)$, of vectors in $\{0,1,2\}^n$ such that the Hamming distance between every two is odd? We investigate these questions, and more general ones, by studying Xor powers of graphs, focusing on their independence number and clique number, and by introducing two new parameters of a graph G. Both parameters denote limits of series of either clique numbers or independence numbers of the Xor powers of G (normalized appropriately), and while both limits exist, one of the series grows exponentially as the power tends to infinity, while the other grows linearly. As a special case, it follows that $f_3(n) = \Theta(2^n)$ whereas $g_3(n) = \Theta(n)$.

1 Introduction

The *Xor product* of two graphs, $G = (V,E)$ and $H = (V', E')$, is the graph whose vertex set is the Cartesian product $V \times V'$, where two vertices (u, u') and (v, v') are connected iff either $uv \in E$, $u'v' \notin E'$ or $uv \notin E$, $u'v' \in E'$, i.e., the vertices are adjacent in precisely one of their two coordinates. This product is commutative and associative, and it follows that for any $n \geq 1$, the product of $G_1, \ldots, G_n$ is the graph whose vertex set is $\prod V(G_i)$, where two vertices are connected iff they are adjacent in an *odd* number of coordinates. Throughout this paper, let $G \cdot H$ denote the Xor product of G and H, and let G^n denote the Xor product of n copies of G.

The Xor graph product was studied in [12], where the author used its properties 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. See also [5],[6],[13] for more about this problem.

*Schools of Mathematics and Computer Science, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, 69978, Israel. Email: nogaa@tau.ac.il. Research supported in part by a USA-Israeli BSF grant, by the Israel Science Foundation and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University.

†Department of Computer Science, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, 69978, Israel. Email: lubetzky@tau.ac.il.

Examine K_3, the complete graph on 3 vertices. Each vertex of K_3^n can be naturally represented by a vector in $\{0,1,2\}^n$, and two vertices are connected in K_3^n iff their representing vectors differ in an odd number of coordinates, or equivalently, have an odd Hamming distance. Thus, a set of vectors in $\{0,1,2\}^n$, in which every two vectors have an even Hamming distance, represents an independent set in K_3^n; similarly, a set of vectors of $\{0,1,2\}^n$ in which each pair has an odd Hamming distance represents a clique in K_3^n, and hence:

$$f_3(n) = \alpha(K_3^n)$$

$$g_3(n) = \omega(K_3^n)$$

where $\alpha(G)$ denotes the independence number of G and $\omega(G)$ denotes the clique number of G. Studying the series of independence numbers and the series of clique numbers of powers of a fixed graph G provides several interesting questions and results. Both series, when normalized appropriately, converge, however one has an exponential growth while the other grows linearly.

In section 2 we show that the series of independence numbers, when normalized, converges to its supremum, which we denote by $x_\alpha(G)$:

$$x_\alpha(G) = \lim_{n\to\infty} \sqrt[n]{\alpha(G^n)} = \sup_n \sqrt[n]{\alpha(G^n)}$$

We calculate this parameter for several families of graphs and multi-graphs, and study some of its properties.

In section 3 we show, this time using a linear normalization, that the series $\omega(G^n)/n$ converges as well. We denote its limit by $x_\omega(G)$:

$$x_\omega(G) = \lim_{n\to\infty} \frac{\omega(G^n)}{n} = \sup_n \frac{\omega(G^n)-2}{n+1}$$

Determining the value of x_α and x_ω for K_3 and for a general complete graph K_r gives the asymptotic behavior of $f_3(n)$ and $g_3(n)$, and similarly, of $f_r(n)$ and $g_r(n)$, defined analogously with r replacing the alphabet size of 3. For a general G, it seems that merely approximating x_α and x_ω can be extremely difficult. Both parameters are non-monotone with respect to the addition of edges to the graph, and we use combinatorial ideas, tools from linear algebra and spectral techniques in order to provide bounds for them for different graphs.

2 Independence numbers of Xor powers

2.1 The independence series and x_α

We begin with an immediate observation: for every two graphs G and H, and every two independent sets $I \subset V(G)$ and $J \subset V(H)$, $I \times J$ is an independent set of $G \cdot H$. Therefore, the function

$f(n) = \alpha(G^n)$ is super-multiplicative: $f(m+n) \geq f(m)f(n)$, and by Fekete's lemma (c.f., e.g., [10], p. 85), we deduce that

$$\exists \lim_{n\to\infty} \sqrt[n]{f(n)} = \sup_n \sqrt[n]{f(n)}$$

Let $x_\alpha(G)$ denote this limit.

We note that the definition of the Xor product and of x_α applies to multi-graphs as well: indeed, since only the parity of the number of edges between two vertices dictates their adjacency, we can assume that there are no multiple edges, however there may be (self) loops in the graph. The function $f(n) = \alpha(G^n)$ remains super-multiplicative (notice that an independent set I of G^n can never contain a vertex $v = (v_1, \ldots, v_n)$ with an odd number of coordinates $\{v_{i_j}\}$, which have loops). However, in the single scenario where every vertex of G has a loop, $\alpha(G) = 0$ and we cannot apply Fekete's lemma (indeed, in this case, $f(2n+1) = 0$ and $f(2n) \geq 1$ for all n). In all other cases, $x_\alpha(G)$ is well defined. Furthermore, if we negate the adjacency matrix of G, obtaining the multi-graph complement $\overline{G}$ (u and v are adjacent in $\overline{G}$ iff they are disconnected in G, including the case $u = v$), we get $x_\alpha(G) = x_\alpha(\overline{G})$, as long as $x_\alpha(\overline{G})$ is also defined. To see this fact, take the even powers $2k$ of the independence series, in which two vertices are adjacent in G^{2k} iff they are adjacent in $\overline{G}^{2k}$.

Proposition 2.1. *For every multi-graph $G = (V, E)$ satisfying $\alpha(G) > 0$, $x_\alpha(G)$ is well defined. Furthermore, if in addition $\alpha(\overline{G}) > 0$, where $\overline{G}$ is the multi-graph-complement of G, then $x_\alpha(G) = x_\alpha(\overline{G})$.*

2.2 General bounds for x_α

It is obvious that $x_\alpha(G) \leq |V(G)|$, and this upper bound is tight, for instance, for the edgeless graph. For the lower bound, the following simple fact holds:

Claim 2.2 (Uniform lower bound). *Let $G = (V, E)$ be a multi-graph satisfying $\alpha(G) > 0$. Then:*

$$x_\alpha(G) \geq \sqrt{|V|} \tag{1}$$

Proof. Let $I \subset V(G^2)$ denote the set $\{(v, v) \mid v \in V\}$. Clearly, I is an independent set of G^2 of size $|V|$, thus $x_\alpha(G) \geq |V|^{\frac{1}{2}}$ (and similarly, for all k we get an explicit independent set of size $|V|^k$ in G^{2k}). ■

For a better understanding of the parameter $x_\alpha(G)$, we next show several infinite families of graphs which attain either the lower bound of (1) or the upper bound of $|V(G)|$. While, trivially, the edgeless graph G on n vertices satisfies $x_\alpha(G) = n$, it is interesting that complete bipartite graphs also share this property:

Claim 2.3. *Let $K_{m,n}$ denote the complete bipartite graph with color classes of sizes m, n, where $m \geq n$. Then for every $k \geq 1$, $K^k_{m,n}$ is a complete bipartite graph with color classes W_0, W_1 of* *sizes:*

$$|W_0| = \frac{1}{2}\left((m+n)^k + (m-n)^k\right) \quad , \quad |W_1| = \frac{1}{2}\left((m+n)^k - (m-n)^k\right)$$

Therefore, $x_\alpha(K_{m,n}) = m + n$.

Proof. Let $G = K_{m,n}$, $m \geq n$, and denote its color classes by U_0, U_1, where $|U_0| = m$. For every vertex $v = (v_1, \ldots, v_k) \in V(G^k)$, define a vector $w_v \in \{0,1\}^k$, in the following manner: $(w_v)_i = 0$ iff $v_i \in U_0$. By the definition of the Xor product (recall that G is a complete bipartite graph), the following holds for every $u, v \in V(G^k)$:

$$uv \notin E(G^k) \iff |\{1 \leq i \leq k \mid (w_u)_i \neq (w_v)_i\}| = 0 \pmod 2$$

Equivalently, performing addition and dot-product over $GF(2^k)$:

$$uv \notin E(G^k) \iff (w_u + w_v) \cdot \underline{1} = 0 \tag{2}$$

Let W_0 denote the set of all vertices in $v \in V(G^k)$ such that the Hamming weight of w_v is even, and let W_1 denote the set of all those whose corresponding vectors have an odd Hamming weight. In other words, we partition the vertices of G^k into two sets, according to the parity of the number of times a coordinate was taken from U_0. Notice that:

$$|W_0| = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2i} n^{2i} m^{k-2i} = \frac{1}{2}\left((m+n)^k + (m-n)^k\right) ,$$

and similarly:

$$|W_1| = \frac{1}{2}\left((m+n)^k - (m-n)^k\right)$$

To see that G^k is a complete bipartite graph with color classes W_0, W_1, argue as follows: take $u, v \in W_i$ ($i \in \{0,1\}$); clearly, we have:

$$(w_u + w_v) \cdot \underline{1} = w_u \cdot \underline{1} + w_v \cdot \underline{1} = i + i = 0 ,$$

hence, by (2), W_0 and W_1 are both independent sets. Next, for every $u \in W_0$ and $v \in W_1$, we have:

$$(w_u + w_v) \cdot \underline{1} = 0 + 1 = 1 ,$$

implying that u and v are adjacent. This completes the proof. ∎

The previous claim shows that $x_\alpha(K_{n,n}) = 2n = n x_\alpha(K_2)$. This is a special case of the following property of x_α:

Claim 2.4. *Let $G = (V, E)$ be a graph on the vertex set $V = [n]$. We define the r-blow-up of G, $G[r]$, as the n-partite graph whose color groups are $(V_1, \ldots, V_n)$, where for all i, $|V_i| = r$, and two vertices $x \in V_i$ and $y \in V_j$ are connected iff $ij \in E$. Then:*

$$x_\alpha(G[r]) = r \cdot x_\alpha(G)$$

Furthermore, every maximum independent set of $G[r]^k$ is an r-blow-up of a maximum independent set of G^k.

Proof. Let $T : V(G[r]) \to V(G)$ be the mapping from each vertex in $G[r]$ to its corresponding vertex in G (i.e., if $x \in V_i$, then $T(x) = i$), and define $T^{\circ k} : V(G[r]^k) \to V(G^k)$ by

$$T^{\circ k}(v_1, \dots, v_k) = (T(v_1), \dots, T(v_k))$$

Then, by the definition of $G[r]$, $T^{\circ k}(G[r]^k)$ is isomorphic to G^k, and furthermore, a set I is independent in $G[r]^k$ iff $T^{\circ k}(I)$ is independent in G^k. This implies that every maximum independent set of $G[r]^k$ can be obtained by taking a maximum independent set of G^k and expanding each coordinate in each of the r possible ways. In particular:

$$\alpha(G[r]^k)^{\frac{1}{k}} = \left(r^k \alpha(G^k)\right)^{\frac{1}{k}} = r \cdot \alpha(G^k)^{\frac{1}{k}}$$

and the desired result follows. ■

A simple algebraic consideration provides an example for a family of multi-graphs which attain the lower bound - the Hadamard multi-graphs (see , e.g., [10] for further information on Sylvester-Hadamard matrices):

Claim 2.5. *Let H_{2^n} be the multi-graph whose adjacency matrix is the Sylvester-Hadamard matrix on 2^n vertices: two (not necessarily distinct) vertices u and v, represented as vectors in $GF(2^n)$, are adjacent iff their dot product equals 1. Then: $x_\alpha(H_{2^n}) = 2^{n/2}$*

Proof. Let $H = H_{2^n}$. Notice that exactly 2^{n-1} vertices have loops, and in particular there is a non-empty independent set in H and x_α is defined. Examine H^k; by definition, $u = (u_1, \dots, u_k)$ and $v = (v_1, \dots, v_k)$ are adjacent in H^k iff $\sum_i u_i \cdot v_i = 1 \pmod 2$. This implies, by the definition of the Hadamard multi-graph, that:

$$H_{2^n}^k = H_{2^{nk}}$$

We are thus left with showing that $H = H_{2^n}$ satisfies $\alpha(H) \leq \sqrt{|H|}$, and this follows from the fact that an independent set in H is a self-orthogonal set of vectors in $GF(2^n)$, hence the rank of its span is at most $n/2$ and thus:

$$\alpha(H) \leq 2^{n/2} = \sqrt{|H|} \ ,$$

as needed. ■

Note that the result above is also true for multi-graphs whose adjacency matrix is a general-type Hadamard matrix, H_n; this can be proved using spectral analysis, in a way similar to the treatment of strongly-regular graphs in the next subsection. As another corollary of the analysis of strongly-regular graphs in the next subsection, we will show that the Paley graph P_q, defined there, has q vertices and satisfies $x_\alpha(P_q) \leq \sqrt{q} + 1$, hence there exists a family of simple graphs which roughly attain the general lower bound on x_α.

2.3 Properties of x_α and bounds for codes

The normalizing factor applied to the independence series when calculating x_α depends only on the current graph power, therefore restricting ourselves to an induced subgraph of a graph G immediately gives a lower bound for $x_\alpha(G)$. It turns out that x_α cannot drastically change with the addition of a single vertex to the graph - each added vertex may increase x_α by at most 1. However, x_α is non-monotone with respect to the addition of edges. The next few claims summarize these facts.

Claim 2.6. *Let $G = (V, E)$ be a multi-graph, and let H be an induced subgraph on $U \subset V$, satisfying $\alpha(H) > 0$. Then:*

$$x_\alpha(H) \le x_\alpha(G) \le x_\alpha(H) + |V| - |U|$$

Proof. The first inequality is trivial, since we can always restrict our choice of coordinates in independent sets of G^k to vertices of U. In order to prove the second inequality, it is enough to prove the case of $|U| = |V| - 1$. Denote by v the single vertex of $V \setminus U$, and assume that v does not have a loop. Let I be a maximum independent set of G^k. For every pattern of i appearances of v in the coordinates of vertices of I, the set of all vertices of I containing this pattern (and no other appearances of v) is an independent set. This set remains independent in H^{k-i}, after omitting from each of these vertices its i appearances of v, hence its size is at most $\alpha(H^{k-i})$. Since $x_\alpha(H)$ is the supremum of $\sqrt[n]{\alpha(H^n)}$, we get the following bound for I:

$$|I| \le \sum_{i=0}^{k} \binom{k}{i} \alpha(H^{k-i}) \le \sum_{i=0}^{k} \binom{k}{i} x_\alpha(H)^{k-i} = (x_\alpha(H) + 1)^k \ .$$

Taking the k-th root gives $x_\alpha(G) \le x_\alpha(H) + 1$.

We are left with the case where v has a loop. If H has no loops, then every vertex of I must have an even number of appearances of v in its coordinates (as an independent set cannot contain loops). Hence, every pattern of i appearances of v in the coordinates of vertices of I still represents an independent set in H^{k-i}, and the calculation above is valid. In fact, it gives that

$$|I| \le \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{i} \alpha(H^{k-2i}) = \frac{1}{2}\left((x_\alpha(H) + 1)^k + (x_\alpha(H) - 1)^k \right) < (x_\alpha + 1)^k \ .$$

If H does contain loops, then $\alpha(\overline{H}) > 0$, and we can apply the previous argument to $\overline{G}$ with respect to $\overline{H}$ and v (which does not have a loop in $\overline{G}$), obtaining:

$$x_\alpha(G) = x_\alpha(\overline{G}) \le x_\alpha(\overline{H}) + 1 = x_\alpha(H) + 1 \ ,$$

where the last equality holds since $\alpha(H) > 0$, guaranteeing that at least one vertex of H does not have a loop. ■

Notice that, by the last claim, we can apply the vertex-exposure Martingale on the random graph $\mathcal{G}_{n,\frac{1}{2}}$, and obtain a concentration result for x_α (see for example [3], Chapter 7):

Corollary 2.7. *Almost surely, that is, with probability that tends to 1 as n tends to infinity, the random graph $G = \mathcal{G}_{n,\frac{1}{2}}$ satisfies*

$$|x_\alpha(G) - \mathbb{E}x_\alpha(G)| \leq O(\sqrt{n})$$

A counterexample for edge-addition monotonicity exists already when $|V| = 3$, as the next claim shows.

Claim 2.8. *x_α is non-monotone with respect to the addition of edges.*

Proof. Let $G = (V, E)$ be the graph on three vertices $V = \mathbb{Z}_3$ and one edge $E = \{(0,1)\}$. We show that $x_\alpha(G) = 2$, thus if we *remove* the single edge (creating the empty graph on 3 vertices) or *add* the edge $(1,2)$ (creating the complete bipartite graph $K_{1,2}$) we increase x_α to a value of 3. In fact, up to an automorphism of the graph G in each coordinate, there is exactly one maximum independent set of G^k, which is $\{(v_1, \ldots, v_k) : v_i \in \{0,2\}\}$.

The proof is by induction on k, stating that every maximum independent set of G^k is the Cartesian product of either $\{0,2\}$ or $\{1,2\}$ in each of the coordinates (it is obvious that this set is indeed independent). The case $k = 1$ is trivial. For $k > 1$, let I be a maximum independent set of G^k, and notice that by the construction of the independent set above, we have $|I| = \alpha(G^k) \geq 2^k$. Let A_i ($i \in \mathbb{Z}_3$) be the set of vertices of I whose first coordinate is i. We denote by A'_i the set of vertices of G^{k-1} formed by omitting the first coordinate from A_i. Since $A_i \subset I$ is independent, so is A'_i for every i. However, every vertex of A'_0 is adjacent to every vertex of A'_1 (again since I is independent).

Note that, by induction, $|A_i| = |A'_i| \leq 2^{k-1}$. Clearly, this implies that if either A_0 or A_1 are empty, we are done, and I is the Cartesian product of a maximum independent set $I' \subset G^{k-1}$ of size 2^{k-1}, with either $\{0,2\}$ or $\{1,2\}$. Indeed, if for instance A_1 is empty, then both A'_0 and A'_2 are maximum independent sets of G^{k-1} (otherwise, the size of I would be strictly less than 2^k), with the same automorphism of G in each coordinate (otherwise I would not be independent - consider the two vertices which contain 2 in all coordinates except the one where the automorphism is different).

Assume therefore that $A_0, A_1 \neq \emptyset$. By a similar argument, $A_2 \neq \emptyset$, otherwise $|I| \geq 2^k$ would imply that both A'_0 and A'_1 are maximum independent sets in G^{k-1} (of size 2^{k-1} each), and by induction, both contain the vector $\underline{2}$, contradicting the independence of I. We therefore have:

$$|I| = \sum_i |A_i| = \sum_i |A'_i| < \left(|A'_0| + |A'_2|\right) + \left(|A'_1| + |A'_2|\right) \leq 2 \cdot 2^{k-1} = 2^k$$

The last inequality is by the fact that $A'_2 \cap A'_0 = A'_2 \cap A'_1 = \emptyset$, since, for instance, all vertices in A'_0 are adjacent to all vertices in A'_1 but disconnected from all vertices in A'_2. We therefore obtained a contradiction to the fact that $|I| \geq 2^k$. ∎

We next prove a general upper bound for x_α of regular graphs. As a corollary, this will determine $x_\alpha(K_3)$ and give the asymptotic behavior of the function $f_3(n)$, mentioned in the abstract.

Theorem 2.9. *Let G be a loopless nontrivial d-regular graph on n vertices, and let $d = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ denote the eigenvalues of G. Then:*

$$x_\alpha(G) \leq \max\{|n-2d|, 2|\lambda_2|, 2|\lambda_n|\}$$

Proof. We use spectral analysis to bound the independence numbers of powers of the graph G. Denote by $A = A_G$ the adjacency matrix of G, and let $B = B_G = (-1)^A$, i.e.:

$$B_{ij} \stackrel{def}{=} \begin{cases} -1 & ij \in E(G) \\ 1 & ij \notin E(G) \end{cases}$$

Notice that $B_{G \cdot H} = B_G \otimes B_H$, where $\otimes$ denotes the tensor-product:

$$(B_G \otimes B_H)_{(u,v),(u',v')} = B_{G\,u,v} \cdot B_{H\,u',v'} = \begin{cases} -1 & (u,v)(u',v') \in E(G \cdot H) \\ 1 & (u,v)(u',v') \notin E(G \cdot H) \end{cases}$$

Our aim in using B_G is to obtain expressions for the eigenvalues of A_{G^k}, and then use the following bound, proved by Hoffman: every regular graph H with eigenvalues $\mu_1 \geq \ldots \geq \mu_m$ satisfies:

$$\alpha(H) \leq \frac{-|H|\mu_m}{\mu_1 - \mu_m} \tag{3}$$

(see [7], [11]). Recall that the eigenvalues of A are:

$$\lambda(A) = \{d = \lambda_1, \ldots, \lambda_n\}$$

By definition, $B_G = J_n - 2A_G$, where J_n is the all 1-s matrix of order n, and fortunately, the single non-zero eigenvalue of J_n (the eigenvalue n) corresponds to an eigenvector of $\underline{1}$, which is also an eigenvector of A (with the eigenvalue d). Thus, if we denote the spectrum of B by Λ:

$$\Lambda = \lambda(B) = \{n - 2d, -2\lambda_2, \ldots, -2\lambda_n\}$$

Define $\Lambda^k = \{\mu_1\mu_2\ldots\mu_k : \mu_i \in \Lambda\}$. As usual with tensor-products (c.f., e.g., [2]), we use the fact that:

$$\lambda(B^{\otimes k}) = \{\lambda_{i_1}\lambda_{i_2} \cdot \ldots \cdot \lambda_{i_k} \mid \lambda_{i_j} \in \lambda(B)\} = \Lambda^k$$

Returning to A_{G^k}, we have $A_{G^k} = \frac{1}{2}(J_{n^k} - B_{G^k})$, and $\underline{1}$ is an eigenvector of B_{G^k} corresponding to the eigenvalue $(n-2d)^k$. Hence, $\underline{1}$ is an eigenvector of A_{G^k} with an eigenvalue of:

$$\lambda_M = \frac{n^k - (n-2d)^k}{2}$$

Since this is the regularity degree of G^k, by the Perron-Frobenius theorem it is also its largest eigenvalue. The remaining eigenvalues of A_{G^k} are $\left\{-\frac{1}{2}\mu : \mu \in \Lambda^k, \mu \neq (n-2d)^k\right\}$. Hence, if we define:

$$\beta(k) = \max\left\{\Lambda^k \setminus \{(n-2d)^k\}\right\}$$

then the minimal eigenvalue of A_{G^k}, λ_m, equals $-\frac{1}{2}\beta(k)$. Applying (3) gives:

$$\alpha(G^k) \leq \frac{-n^k \lambda_m}{\lambda_M - \lambda_m} = \frac{\beta(k)}{1-(1-\frac{2d}{n})^k + \beta(k)/n^k} \tag{4}$$

Examine the right hand side of (4). The term $\left(1-\frac{2d}{n}\right)^k$ tends to zero as k tends to infinity, since G is simple and hence $1 \leq d \leq n-1$. Considering $\beta(k)$, notice that for sufficiently large values of k, in order to obtain the maximum of $\Lambda^k \setminus \{(n-2d)^k\}$, one must choose the element of Λ whose absolute value is maximal with plurality at least $k-2$ (the remaining two choices of elements should possibly be used to correct the sign of the product, making sure the choice made is not the one corresponding to the degree of G^k). Therefore, if we set $r = \max\{|n-2d|, 2|\lambda_2|, 2|\lambda_n|\}$, we get $\beta(k) = \Theta(r^k)$. To bound r, we use the following simple argument, which shows that

$$\lambda = \max\{|\lambda_2|, \ldots, |\lambda_n|\} \leq \frac{n}{2}$$

(equality is precisely in the cases where G is complete bipartite with $d = \frac{n}{2}$). Indeed, the square of the adjacency matrix A of G has the values d on its diagonal (as G is d-regular), hence:

$$d^2 + \lambda^2 \leq \sum_i \lambda_i^2 = \mathrm{tr}(A^2) = nd \ ,$$

implying that:

$$\lambda \leq \sqrt{d(n-d)} \leq \frac{n}{2}$$

Therefore, either $r = 2\lambda \leq n$ or $r = |n-2d| < n$, and in both cases we obtain that $\beta(k)/n^k = O(1)$. Taking the k-th root in (4), gives:

$$x_\alpha(G) \leq \lim_{k\to\infty} \sqrt[k]{\beta(k)} = r \ ,$$

as required. ∎

Note that the above proof in fact provides upper bounds for the independence numbers of every power k of a given regular graph G (not only for the asymptotic behavior as k tends to infinity) by calculating $\beta(k)$ and applying (4).

Corollary 2.10. *For the complete graphs K_3 and K_4, $x_\alpha(K_3) = x_\alpha(K_4) = 2$*

Proof. It is easy and well known that the eigenvalues of the complete graph K_n on $n \geq 2$ vertices are: $\{n-1, -1, \ldots, -1\}$. By Theorem 2.9, we have, for every $n \geq 2$:

$$x_\alpha(K_n) \leq \max\{n-2, 2\}$$

For $n = 3$, this implies $x_\alpha(K_3) \leq 2$, and for $n \geq 4$ this implies $x_\alpha(K_n) \leq n-2$. The lower bounds for K_3 and K_4 follow from the fact that $x_\alpha(K_2) = 2$.

We note that (4) gives the following bounds on $\alpha(K_n^k)$ for every $k \geq 1$:

$$\alpha(K_3^k) \leq \frac{2^k}{1-\left(-\frac{1}{3}\right)^k+\left(\frac{2}{3}\right)^k} \quad ,$$

$$\alpha(K_n^k) \leq \frac{2(n-2)^{k-1}}{1-(\frac{2-n}{n})^k+\frac{2}{n}(\frac{n-2}{n})^{k-1}} \quad , \quad n \geq 4 \quad , \quad 2 \nmid k \quad ,$$

$$\alpha(K_n^k) \leq \frac{2(n-2)^{k-1}}{1-(\frac{2-n}{n})^k+\frac{4}{n^2}(\frac{n-2}{n})^{k-2}} \quad , \quad n \geq 4 \quad , \quad 2 \mid k \quad .$$

■

Recalling the motivation of the codes considered in the introduction, the last claim implies that

$$f_3(n) = \Theta(2^n)$$

$$f_4(n) = \Theta(2^n)$$

In other words, extending the alphabet from 3 letters to 4 does not increase the maximal asymptotic size of the required code, and both cases are asymptotically equivalent to using a binary alphabet. However, adding additional letters to the alphabet does increase this asymptotic size, as it is immediate by Claim 2.2 that $f_5(n)$ is at least $\Omega(\sqrt{5}^n)$. Using a simple probabilistic argument (similar to the one used in [2]), we can derive an upper bound for $x_\alpha(K_5)$ from the result on K_4 :

Claim 2.11. *Let G be a vertex transitive graph, and let H be an induced subgraph of G. Then:*

$$x_\alpha(G) \leq x_\alpha(H)\frac{|G|}{|H|}$$

Combining this with Corollary 2.10, we get:

Corollary 2.12. *For all $m < n$, $x(K_n) \leq \frac{x_\alpha(K_m)}{m}n$, and in particular, $\sqrt{5} \leq x_\alpha(K_5) \leq \frac{5}{2}$.*

Proof of claim. Let I be a maximum independent set of G^k, and let $\sigma_1, \sigma_2, \ldots, \sigma_k$ denote random automorphisms of G, chosen independently and uniformly out of all the automorphisms of G. The permutation τ, which maps $v = (v_1, \ldots, v_k) \in G^k$ to $(\sigma_1(v_1), \ldots, \sigma_k(v_k))$, is an automorphism of G^k, and moreover, if we fix a vertex v in G^k, then $\tau(v)$ is uniformly distributed over all the vertices of G^k. Let S be an induced copy of H^k in G^k, and notice that by the properties of τ,

$$\mathbb{E}|\tau(S) \cap I| = |I|\frac{|S|}{|G^k|} = |I|\left(\frac{|H|}{|G|}\right)^k$$

On the other hand, I is an independent set, therefore $|\tau(S) \cap I| \leq \alpha(H^k) \leq (x_\alpha(H))^k$. Choose an automorphism τ for which this random variable attains at least its expected value of $\mathbb{E}|\tau(S) \cap I|$, and it follows that:

$$|I| \leq \left(x_\alpha(H)\frac{|G|}{|H|}\right)^k$$

■

While the best upper bound we have for K_n, when $n \geq 5$, is $n/2$, the last corollary, as well as some simple observations on the first few powers of complete graphs, lead to the following conjecture:

Conjecture 2.13. *For every $n \geq 4$, the complete graph on n vertices satisfies $x_\alpha(K_n) = \sqrt{n}$.*

It seems possible that the Delsarte linear programming bound (c.f., e.g., [9]) may provide improved upper bounds for $\alpha(K_n^k)$ when $n \geq 4$, but it does not seem to supply a proof of the last conjecture.

As another corollary of Theorem 2.9, we can derive bounds for x_α of strongly-regular graphs. Recall that a strongly-regular graph G with parameters (n, d, λ, μ) is a d-regular graph on n vertices, where the co-degree (the number of common neighbors) of every two adjacent vertices is λ, and the co-degree of every two non-adjacent vertices is μ. The eigenvalues of such a graph are d and the solutions to the quadratic equation $x^2 + (\mu - \lambda)x + (\mu - k) = 0$ (c.f., e.g. [4], Chapter 10). As an example, we consider the Paley graphs:

Corollary 2.14. *The Paley graph P_q (where q is a prime power, $q = 1 \pmod 4$) satisfies $\sqrt{q} \leq x_\alpha(P_q) \leq \sqrt{q} + 1$.*

Proof. Recall that P_q has a vertex set $V(P_q) = GF(q)$ and $i, j \in V$ are connected iff $i - j$ is a quadratic residue in $GF(q)$. It is easy to check that P_q is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ strongly regular graph (c.f., e.g., [4]). Hence, its largest eigenvalue is $\frac{q-1}{2}$, and its remaining eigenvalues are the solutions of the equation $x^2 + x - \frac{q-1}{4} = 0$, i.e., $\{\frac{-1 \pm \sqrt{q}}{2}\}$. By Theorem 2.9:

$$x_\alpha(P_q) \leq \max\{1, \sqrt{q} + 1\} = \sqrt{q} + 1$$

■

We conclude this section with another example of an extremal problem on codes, which can easily be translated to the terms of x_α: let $\tilde{f}_3(n)$ be the maximum size of a set of words over $\mathbb{Z}_3^n$, where for every two not necessarily distinct words u, v, the Hamming weight of their sum $u + v$ (addition is performed modulo 3) is even. Determining $\tilde{f}_3(n)$ asymptotically becomes relatively simple, once the problem is translated to the problem of determining $x_\alpha(H)$ for an appropriate multi-graph H. This graph H has a vertex set $V = \mathbb{Z}_3$, where 0 is connected to both 1 and -1, and there are loops on the vertices $1, -1$. It is easy to confirm that a maximum independence set in H^n corresponds to a code of maximum size, meeting the requirements mentioned above. This is an induced subgraph of H_4, the Hadamard graph on 4 vertices (assign the vertices $\{0, 1, -1\}$ the values $\{11, 01, 10\}$ respectively), hence $x_\alpha(H) \leq x_\alpha(H_4) = 2$. The lower bound is immediate, and therefore, $\tilde{f}_3(n) = \Theta(2^n)$.

3 Clique numbers of Xor powers

3.1 The clique series and x_ω

In the previous section, we examined independent sets in Xor powers of graphs; the behavior of cliques in Xor powers of graphs proves to be significantly different.

Theorem 3.1. *For every graph $G = (V, E)$, the limit of $\frac{\omega(G^n)}{n}$ as n tends to infinity exists. Let $x_\omega(G)$ denote this limit. Then:*

$$0 \leq x_\omega(G) = \sup_n \frac{\omega(G^n) - 2}{n+1} \leq |V|$$

Proof. Let G and H denote two simple graphs, and let $\{v_1, \ldots, v_r\}$ and $\{u_1, \ldots, u_s\}$ be maximum cliques in G and H respectively. The following set is a clique in the graph $G \cdot H \cdot K_2$, where the vertex set of K_2 is $\{0, 1\}$:

$$\{v_2, \ldots, v_r\} \times \{u_1\} \times \{0\} \quad \cup \quad \{v_1\} \times \{u_2, \ldots, u_s\} \times \{1\} \tag{5}$$

Thus, the following inequality applies to every two simple graphs G and H:

$$\omega(G \cdot H \cdot K_2) \geq \omega(G) + \omega(H) - 2 \tag{6}$$

Note that there are graphs G and H for which equation (6) is tight. For example, take both G and H to be powers of K_2. The graph K_2^n is triangle free (recall that by Claim 2.3, K_2^n is bipartite), therefore, $\omega(K_2^{k+l}) = 2 = \omega(K_2^k) + \omega(K_2^l) - 2$.

Consider a graph G, and define $g(n) = \omega(G^n)$. If G contains no edges, then each of its powers is an edgeless graph, and $g(n) = 1$ for all n. Otherwise, it contains a copy of K_2, hence equation (6) implies that for every $m, n \geq 1$:

$$g(m + n + 1) \geq g(m) + g(n) - 2$$

Defining, for every $n \geq 1$,

$$\hat{g}(n) = g(n-1) - 2$$

gives:

$$\hat{g}(m+n) = g(m+n-1) - 2 \geq g(m-1) + g(n-1) - 4 = \hat{g}(m) + \hat{g}(n)$$

Therefore, the function $\hat{g}$ is super-additive, and by Fekete's lemma, the limit of the series $\frac{\hat{g}(n)}{n}$ exists and equals its supremum. We note that this applies for edgeless graphs as well, where this limit equals 0. Denote this limit by x_ω:

$$x_\omega(G) = \lim_{n\to\infty} \frac{\omega(G^n)}{n} = \sup_n \frac{\omega(G^n) - 2}{n+1} \tag{7}$$

It remains to show that $x_\omega(G) \leq |V|$. We first need the following definition: A function $f : V \to \mathbb{Z}_2^k$ (for some $k \geq 1$) will be called a **proper representation** of G, if there is a $b_f \in \{0, 1\}$, such that for every (not necessarily distinct) $u, v \in V$, $uv \in E$ iff $f(u) \cdot f(v) = b_f$. The dimension of the representation, $\dim(f)$, is defined to be $\dim(f(V))$ in $\mathbb{Z}_2^k$.

The upper bound for x_ω is given by the following lemma:

Lemma 3.2. *If $G = (V, E)$ has a proper representation f, then $x_\omega(G) \leq \dim(f)$.*

Proof. Let $x \circ y$ denote the concatenation of the vectors x and y. By the definition of the Xor product, for every two graphs G and H, if g is a proper representation of G and h is a proper representation of H, then $g \circ h$, which maps each vector $(u, v) \in V(G \cdot H)$ to $g(u) \circ h(v)$, is a proper representation of $G \cdot H$, with $b_{g \circ h} = b_g + b_h + 1 \pmod 2$. Clearly, $\dim(g \circ h) \leq \dim(g) + \dim(h)$.

Suppose f is a proper representation of G of dimension d, and let g denote the k-fold concatenation of f. Allowing $\dim(g)$ to be at most $kd + 1$ we may assume that $b_g = 0$ (by adding a new coordinate of 1 to all vectors if necessary). Let S be a maximum clique in G^k, $|S| = s$. We define B to be the matrix whose s columns are $\{g(v) : v \in S\}$. Since S is a clique, and g is a proper representation of G^k with $b_g = 0$, then $B^t B = I$. The rank of $B^t B$ is thus s, hence:

$$s = \text{rank}(B^t B) \leq \text{rank}(B) \leq \dim(g) \leq kd + 1$$

We conclude that for every k, $\frac{\omega(G^k)}{k} \leq d + \frac{1}{k}$, and the result follows. ∎

To prove that $x_\omega(G) \leq |V|$, it suffices to show that there exists a proper representation for every G (the dimension of the span of n vectors can never exceed n). Set $|V| = n$ and $|E| = m$, and examine the function $f : V \to \mathbb{Z}_2^m$, which maps each vertex v to its corresponding row in the incidence matrix of G. For every $u \neq v \in V$, either $uv \in E$, in which case there is a single index at which $f(u) = f(v) = 1$, or $uv \notin E$ and there is no such index. Hence $f(u) \cdot f(v) = 1$ iff $uv \in E$ (and in particular, this applies to the dot product in $\mathbb{Z}_2^m$ as well). All that remains in order to turn f into a proper representation of G (with $b_f = 1$) is to adjust the values of $f(u) \cdot f(u)$ to 0 for every $u \in V$. Note that $f(u) \cdot f(u)$ is precisely the degree of u modulo 2, hence the vertices which requires adjusting are precisely those of odd degree. Let $S = \{v_1, \ldots, v_s\}$ denote the set of vertices of odd degree (clearly, s is even). We adjust the representation as follows: add s new coordinates to all vectors. For every $u \notin S$, set all of its new coordinates to 0. For v_i, $1 \leq i \leq s$, set the i-th new coordinate to 1 and the remaining new coordinates to 0. In this manner, we reversed the parity of the v_i vectors, while preserving the dot product of v_i and v_j, guaranteeing this is a proper representation of G. This completes the proof of Theorem 3.1. ∎

Remark: Lemma 3.2 can give better upper bounds for various graphs, by constructing proper representations of dimension strictly smaller than $|V|$. For instance, for every Eulerian graph $G = (V, E)$, the incidence matrix is a proper representation of G (there is no need to modify the parity of any of the vertices, since the degrees are all even). Since each column has precisely two occurrences of the value 1, the sum of all rows is 0 in $GF(2)$, hence the rank of the matrix is at most $|V| - 1$. More generally, if G has k Eulerian connected components, then $x_\omega(G) \leq |V| - k$ (by creating a dependency in each set of rows corresponding to an Eulerian component). Finally, since the matrix whose rows are the vectors of the proper representation, B, satisfies either $BB^t = A$ or $BB^t = A + J$ (operating over $GF(2)$), where A is the adjacency matrix of G), then every proper representation f satisfies $\dim(f) \geq \min\{\text{rank}(A), \text{rank}(A+J)\}$ over $GF(2)$. In particular, if both A and $A+J$ are of full rank over $GF(2)$, then there cannot exist a proper representation which gives a better bound than $|V|$.

We now wish to extend our definition of x_ω to multi-graphs. Recall that without loss of generality, there are no parallel edges, hence a clique in a multi-graph G is a set where every two distinct vertices are adjacent, however, it contains no loops. We note that if we were to examine sets in G, where each two vertices are adjacent, and in addition, each vertex has a loop, then this notion would be equivalent to independent sets in the multi-graph complement $\overline{G}$, and would thus be treated by the results in the previous section.

Notice that equation (6) remains valid, by the same argument, when G and H are multi-graphs. It therefore follows that if a graph G satisfies $\omega(G) \geq 2$, or equivalently, if there are two adjacent vertices in G, each of which does not have a loop, then x_ω is well defined and satisfies equation (7).

If $\omega(G) = 0$, then every vertex of G has a loop, hence $\omega(G^{2n+1}) = 0$ and yet $\omega(G^{2n}) \geq 1$ for every n, thus the series $\frac{g(n)}{n}$ alternates between zero and non zero values. Indeed, it is easy to come up with examples for such graphs where this series does not converge (the disjoint union of 3 loops is an example: the second power, which is exactly the square lattice graph $L_2(3)$, contains a copy of K_3, hence the subseries of even indices does not converge to 0).

If $\omega(G) = 1$, then either the graph is simple (and hence edgeless), or there exist two vertices a and b, such that a has a loop and b does not. In this case, we can modify the clique in (5) to use the induced graph on $\{a, b\}$ instead of a copy of K_2:

$$\{v_2, \ldots, v_r\} \times \{u_1\} \times \{aba\} \quad \cup \quad \{v_1\} \times \{u_2, \ldots, u_s\} \times \{aab\} \tag{8}$$

We can therefore slightly modify the argument used on simple graphs, and obtain a similar result. The function $g(n)$ now satisfies the inequality:

$$g(m + n + 3) \geq g(m) + g(n) - 2$$

hence we can define $\hat{g}$ as:

$$\hat{g}(n) = g(n - 3) - 2$$

and obtain the following definition for x_ω:

$$x_\omega(G) = \lim_{n\to\infty} \frac{\omega(G^n)}{n} = \sup_n \frac{\omega(G^n) - 2}{n + 3} \tag{9}$$

Altogether, we have shown that x_ω, the limit of $\frac{g(n)}{n}$, exists for every multi-graph G satisfying $\omega(G) > 0$. Examining the even powers of G, it is clear that two possibly equal vertices u and v are adjacent in G^{2n} iff they are adjacent in $\overline{G}^{2n}$ (where $\overline{G}$ is the multi-graph complement of

G, as defined in the previous section). Hence, we obtain the following proposition, analogous to Proposition 2.1:

Proposition 3.3. *For every multi-graph $G = (V, E)$ satisfying $\omega(G) > 0$, $x_\omega(G)$ is well defined. Furthermore, if in addition $\omega(\overline{G}) > 0$, where $\overline{G}$ is the multi-graph-complement of G, then $x_\omega(G) = x_\omega(\overline{G})$.*

We note that the upper bound of $|V|$ in Theorem 3.1 applies to multi-graphs as well: Lemma 3.2 does not rely on the fact that G has no loops, and in the constructions of proper representations for G, we have already dealt with the scenario of having to modify the value of $f(u_i) \cdot f(u_i)$ for a subset of the vertices $\{u_i\} \subset V$. The loops merely effect the choice of the vertices whose parity we need to modify.

3.2 Properties of x_ω and bounds for codes

While defining x_ω in the previous section, we commented that the lower bound of 0 is trivially tight for edgeless graphs. It is interesting to state that $x_\omega(G)$ may be 0 even if the graph G is quite dense: recall that the powers of complete bipartite graphs are complete bipartite (Claim 2.3). Therefore, for every $k \geq 1$, $\omega(K_{m,n}^k) = 2$, and $x_\omega(K_{m,n}) = 0$.

It is now natural to ask whether $x_\omega(G) = 0$ holds for every (not necessarily complete) bipartite graph. This is false, as the following example shows: take P_4, the path on 4 vertices, $w - x - y - z$. The set $\{(w, x), (y, y), (z, y)\}$ is a triangle in P_4^2, hence (7) implies that $x_\omega(P_4) \geq \frac{1}{3} > 0$. However, adding the edge (w, z) completes P_4 into a cycle $C_4 = K_{2,2}$, which satisfies $x_\omega(K_{2,2}) = 0$ by the discussion above. This proves the following property of x_ω:

Claim 3.4. *x_ω is non-monotone with respect to the addition of edges.*

Recall the motivation of examining $g_3(n)$, the maximal number of vectors in $\{0, 1, 2\}^n$ such that the Hamming distance between every two is odd. We already noted in the introduction that $g_3(n) = \omega(K_3^n)$; it is now clear from the lower and upper bounds we have presented for x_ω that $g_3(n) = \Theta(n)$, and more generally, that when the alphabet is $\{0, \ldots, r - 1\}$ for some fixed r, $g_r(n) = \Theta(n)$. The following holds for general complete graphs:

Theorem 3.5. *The complete graph K_r ($r \geq 3$) satisfies:*

$$x_\omega(G) = (1 - o(1))\, r \ ,$$

where the $o(1)$-term tends to 0 as r tends to infinity.

Proof. We first prove the following lemma, addressing the case of r being a prime power:

Lemma 3.6. *Let $r = p^k$ for some prime $p \geq 3$ and $k \geq 1$. Then:*

$$r - 1 - \frac{r}{r + 2} \leq x_\omega(K_r) \leq r - 1$$

Proof. The upper bound of $r-1$ is derived from the remark following Theorem 3.1 (r is odd and hence K_r is Eulerian). For the lower bound, argue as follows: let $\mathcal{L}$ denote the set of all lines with finite slopes in the affine plane $GF(p^k)$. Let $\{x_1, \ldots, x_{p^k}\}$ denote the elements of $GF(p^k)$, and represent each such line $\ell \in \mathcal{L}$, $\ell = ax + b$ by the vector:

$$f(\ell) = (a, ax_1 + b, ax_2 + b, \ldots, ax_{p^k} + b)$$

(i.e., represent ℓ by its slope followed by the y-coordinates of its set of points). Every two distinct lines $\ell_1, \ell_2 \in \mathcal{L}$ are either parallel ($a_1 = a_2$ and $b_1 \neq b_2$) or intersect in precisely one point ($x = (b_1 - b_2)(a_2 - a_1)^{-1}$). In both cases, precisely one coordinate in $f(\ell_1), f(\ell_2)$ is equal, hence the Hamming distance between them is p^k. Since p is odd, the above set of vectors forms a clique of size $|\mathcal{L}| = p^{2k}$ in $K_{p^k}^{p^k+1}$. Equation (7) yields:

$$x_\omega(K_{p^k}) \geq \frac{p^{2k} - 2}{(p^k + 1) + 1} = p^k - 1 - \frac{p^k}{p^k + 2} \ ,$$

as required. ■

There exists a $\frac{1}{2} < \Theta < 1$ such that for every sufficiently large n, the interval $[n - n^\Theta, n]$ contains a prime number (see, e.g., [8] for $\Theta = 23/42$). Combining this fact with the lower bound of the above lemma immediately implies the asymptotic result for every sufficiently large r. ■

Remark: Lemma 3.6 gives a lower bound of 1.4 for $x_\omega(K_3)$. Using a computer search, we improved this lower bound to 1.7 (compared to the upper bound of 2), by finding a clique of size 19 in K_3^9.

It is not difficult to see that the upper bounds of proper representations, given for cliques, can be extended to complete r-partite graphs, by assigning the same vector to all the vertices in a given color class. This is a special case of the following property, analogous to Claim 2.4:

Claim 3.7. *Let $G = (V, E)$ be a graph on the vertex set $V = [n]$. The r-blow-up of G, $G[r]$ (see Claim 2.4 for the definition) satisfies:*

$$x_\omega(G[r]) = x_\omega(G)$$

Furthermore, every maximum clique of $G[r]^k$ corresponds to a maximum clique of the same size of G^k.

Proof. Define the *pattern* of a vertex $v = (v_1, \ldots, v_k) \in G[r]^k$ to be the vector $w_v = (w_1, \ldots, w_k) \in G^k$, such that every coordinate of v belongs in $G[r]$ to the color class of the corresponding coordinate of w_v in G (i.e., v_i belongs to the independent set of size r which corresponds to w_i in $G[r]$). Let S be a maximum clique of $G[r]^k$; then every vertex $v \in S$ has a unique pattern in S (by definition, two vertices sharing the same pattern are disconnected in every coordinate). Thus, we can fix a vertex in each color class of $G[r]$ (note that this is an induced copy of G in $G[r]$), and without loss of generality, we can assume that these are the only vertices used in every $v \in S$. This completes the proof of the claim. ■

Corollary 3.8. *Every complete r-partite graph G satisfies $\frac{r}{2} - 1 \leq x_\omega(G) \leq r$, and in addition, $x_\omega(G) = (1 - o(1))\, r$, where the $o(1)$-term tends to 0 as r tends to infinity.*

We have so far seen that for every graph G on n vertices and a maximum clique of size r, $\Omega(r) \leq x_\omega(G) \leq O(n)$. For complete graphs, $x_\omega(G) = (1 - o(1))r$, and one might suspect that $x_\omega(G)$ cannot be significantly larger than r. The following claim settles this issue, by examining self complementary Ramsey graphs (following the ideas of [1]):

Claim 3.9. *For every $n \in \mathbb{N}$ there is a graph G on n vertices, such that $\omega(G) < 2\lceil \log_2(n) \rceil$ and yet $x_\omega(G) \geq \frac{n-5}{3}$.*

Proof. In section 2.2 of [1], the authors prove the following lemma:

Lemma 3.10 ([1]). *For every n such that $4 \mid n$ there is a self-complementary graph G on n vertices satisfying $\alpha(G) < 2\lceil \log_2(n) \rceil$.*

Set $n = 4m + r$ $(0 \leq r \leq 3)$, and let G be the disjoint union of a self-complementary graph H on $4m$ vertices, and r isolated vertices. By the lemma,

$$\omega(G) < 2\lceil \log_2(n) \rceil$$

Furthermore, if τ is an isomorphism mapping H to its complement, the set $\{(v, \tau(v)) : v \in V(H)\}$ is a clique of size $4m$ in G^2, since for every $u \neq v$, $uv \in E(G)$ iff $\tau(u)\tau(v) \notin E(G)$. Hence:

$$x_\omega(G) \geq \frac{\omega(G^2) - 2}{3} \geq \frac{n - r - 2}{3} \geq \frac{n - 5}{3}$$

■

We note that a slightly weaker result can be proved rather easily and without using the lemma on self-complementary Ramsey graphs, by taking the disjoint union of a Ramsey graph and its complement. The lower bound on x_ω is again derived from a clique in G^2 of the form $\{(v, \tilde{v})\}$ where $\tilde{v}$ is the vertex corresponding to v in the complement graph. This construction gives, for every even $n \in \mathbb{N}$, a graph G on n vertices, satisfying $\omega(G) \leq 2\log_2(n)$ and yet $x_\omega(G) \geq \frac{n/2-2}{3} = \frac{n-4}{6}$.

4 Open problems

We conclude with several open problems related to x_α and x_ω:

Question 4.1. *Does every complete graph on $n \geq 4$ vertices, K_n, satisfy $x_\alpha(K_n) = \sqrt{n}$?*

Question 4.2. *What is the expected value of x_α for the random graph $\mathcal{G}_{n,\frac{1}{2}}$? What is the expected value of x_ω for the random graph $\mathcal{G}_{n,\frac{1}{2}}$?*

Question 4.3. *What is the precise value of $x_\omega(K_n)$ for $n \geq 3$?*

Question 4.4. *Is the problem of deciding whether $x_\alpha(G) > k$, for a given graph G and a given value k, decidable? Is the problem of deciding whether $x_\omega(G) > k$, for a given graph G and a given value k, decidable?*

Acknowledgement We would like to thank Benny Sudakov and Simon Litsyn for fruitful discussions.

References

[1] N. Alon and A. Orlitsky, Repeated communication and Ramsey graphs, IEEE Transactions on Information Theory 41 (1995), 1276-1289.

[2] N. Alon, I. Dinur, E. Friedgut and B. Sudakov, Graph products, fourier analysis and spectral techniques, Geometric and Functional Analysis 14 (2004), 913-940.

[3] N. Alon and J. H. Spencer, The Probabilistic Method, Second Edition, Wiley, New York, 2000.

[4] C. Godsil and G. Royle, Algebraic Graph Theory, volume 207 of Graduate Text in Mathematics, Springer, New York, 2001.

[5] P. Erdős, On the number of complete subgraphs contained in certain graphs, Publ. Math. Inst. Hung. Acad. Sci., VII, ser. A 3 (1962), 459-464.

[6] F. Franek and V. Rödl, 2-colorings of complete graphs with a small number of monochromatic K_4 subgraphs, Discrete Math. 114 (1993), 199-203.

[7] A. J. Hoffman, On eigenvalues and colorings of graphs, B. Harris Ed., Graph Theory and its Applications, Academic, New York and London, 1970, 79-91.

[8] H. Iwaniec and J. Pintz, Primes in short intervals, Monatsh. Math. 98 (1984), 115-143.

[9] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[10] J.H. van Lint and R.M. Wilson, A Course in Combinatorics. Second Edition. Cambridge University Press, Cambridge, 2001.

[11] L. Lovász, On the Shannon capacity of a graph, IEEE Transactions on Information Theory IT-25, pages 1-7, 1979.

[12] A. Thomason, Graph products and monochromatic multiplicities, Combinatorica 17 (1997), 125-134.

[13] A. Thomason, A disproof of a conjecture of Erdős in Ramsey theory, J. London Math. Soc. 39 (1989), 246-255.