On metric properties of maps between Hamming spaces and related graph homomorphisms

Yury Polyanskiy[a]

[a]*Department of Electrical Engineering and Computer Science, MIT, Cambridge, MA 02139 USA.*

Abstract

A mapping of k-bit strings into n-bit strings is called an (α, β)-map if k-bit strings which are more than αk apart are mapped to n-bit strings that are more than βn apart. This is a relaxation of the classical problem of constructing error-correcting codes, which corresponds to $\alpha = 0$. Existence of an (α, β)-map is equivalent to existence of a graph homomorphism $\bar{H}(k, \alpha k) \to \bar{H}(n, \beta n)$, where $H(n, d)$ is a Hamming graph with vertex set $\{0, 1\}^n$ and edges connecting vertices differing in d or fewer entries.

This paper proves impossibility results on achievable parameters (α, β) in the regime of $n, k \to \infty$ with a fixed ratio $\frac{n}{k} = \rho$. This is done by developing a general criterion for existence of graph-homomorphism based on the semi-definite relaxation of the independence number of a graph (known as the Schrijver's θ-function). The criterion is then evaluated using some known and some new results from coding theory concerning the θ-function of Hamming graphs. As an example, it is shown that if $\beta > 1/2$ and $\frac{n}{k}$ – integer, the $\frac{n}{k}$-fold repetition map achieving $\alpha = \beta$ is asymptotically optimal.

Finally, constraints on configurations of points and hyperplanes in projective spaces over $\mathbb{F}_2$ are derived.

Keywords: Error-correcting codes, graph homomorphism, Schrijver's θ-function, projective geometry over $\mathbb{F}_2$

Email address: yp@mit.edu (Yury Polyanskiy)

Preprint submitted to Elsevier *April 29, 2016*

1. Introduction

Hamming space $\mathbb{F}_2^k$ of binary k-strings, equipped with the Hamming distance is one of the classical objects studied in combinatorics. Its properties that received significant attention are the maximal packing densities, covering numbers, isoperimetric inequalities, list-decoding properties, etc. In this paper we are interested in studying metric properties of maps $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$ between Hamming spaces of different dimensions.

Indeed, frequently one is interested in embedding $\mathbb{F}_2^k$ into $\mathbb{F}_2^n$ "expansively", i.e. so that points that were far apart in $\mathbb{F}_2^k$ remain far apart in $\mathbb{F}_2^n$. Two immediate examples of such maps are: the error-correcting codes with rate k/n and minimum distance d satisfy

$$|x - x'| > 0 \implies |f(x) - f(x')| \geq d\,,$$

where here and below $|z| = \|z\|_0 = |\{i : z_i \neq 0\}|$ is the Hamming weight of the vector. Another example is the repetition coding with $f(x)$ mapping x into $\frac{n}{k}$ repetitions of x. This map satisfies:

$$|x - x'| > \alpha k \implies |f(x) - f(x')| > \alpha n\,. \tag{1}$$

With these two examples in mind, we introduce the main concept of this paper.

Definition 1. *A map $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$ is called an $(\alpha, \beta; k, n)$-map (or simply an (α, β)-map) if αk and βn are integers and for all $x, x' \in \mathbb{F}_2^k$ we have either*

$$|f(x) - f(x')| > \beta n \quad \text{or} \quad |x - x'| \leq \alpha k\,, \tag{2}$$

where $\mathbb{F}_2^k$ is the Hamming space of dimension k over the binary field.

We next define the Hamming graphs $H(n, d)$ for integer $d \in [0, n]$ as follows:

$$V(H(n,d)) = \mathbb{F}_2^n, \quad E(H(n,d)) = \{(x, x') : 0 < |x - x'| \leq d\}\,. \tag{3}$$

By $V(G)$, $E(G)$ and $\alpha(G)$ we denote the vertices of G, the edges of G and the cardinality of the maximal independent set of G. All graphs in this paper are simple (without self-loops and multiple edges). By $\bar{G}$ we denote the (simple) graph obtained by complementing $E(G)$ and deleting self-loops.

The relevance of Hamming graphs to this paper comes from the simple observation:

$$\exists(\alpha, \beta; k, n)\text{-map} \qquad \Longleftrightarrow \qquad \bar{H}(k, \alpha k) \to \bar{H}(n, \beta n)\,,$$

where $G \to H$ denotes the existence of a graph homomorphism (see Section 3 for definition).

This paper focuses on proving negative results showing impossibility of certain parameters (α, β). Note that there are a variety of methods that we can use to disprove existence of graph homomorphisms. For example, by computing the shortest odd cycle we can prove

$$\bar{H}(2,0) \not\to \bar{H}(4,2) \not\to \bar{H}(6,4) \not\to \bar{H}(8,6) \not\to \cdots\,.$$

In this paper, however, we are interested in the methods that provide some useful information in the asymptotic regime of $k \to \infty$, $\frac{n}{k} \to \rho > 0$ and fixed (α, β).

1.1. More on the concept of an (α, β)-map

Our original motivation for Definition 1 was the following. Suppose the map $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$ is used to protect the k data bits against noise. If the points $x, x' \in \mathbb{F}_2^k$ are far apart but $f(x)$ and $f(x')$ are close, i.e. if a map fails to satisfy (2), then $f(x)$ may be confused with $f(x')$ in a noisy environment. Consequently, this would lead to a severe discrepancy if x' is reported instead of x.

Below we briefly discuss how (α, β)-property relates to some previously studied concepts.

First, a $(0, \beta)$-map is simply an error-correcting code of rate k/n and minimum distance $1+\beta n$. Thus, (α, β)-condition is a *relaxation of the minimum-distance property:* the separation of $1+\beta n$ is only guaranteed for data vectors x, x' that were $1 + \alpha k$ apart to start with. Practically, data may have some structure guaranteeing some separation between feasible data-vectors (e.g. if x is English test, changing one letter is unlikely to result in a grammatically correct phrase).

Second, in the inverse problem of reconstructing x from a noisy version $y = f(x) + z$, one may proceed by computing a pre-image of the Hamming ball of radius $\beta n/2$ around y. Then the (α, β)-condition guarantees that the points in the pre-image will all be close to each other.

Third, an (α, β)-map can be used to convert a code with (normalized) minimal distance $> \alpha$ to a code of minimal distance $> \beta$ at the expense of losing a factor k/n in rate. This observation leads, on one hand, to a non-trivial bound on achievable parameters (α, β), see (9) below. On the other hand, it also suggests that (α, β)-maps could be employed for adapting properties of a fixed mother code to the changing noise environment.

Fourth, an (α, β)-map with $n < k$ can be seen as a type of hashing in which one wants the hashes of dissimilar strings to be also dissimilar. In fact, the (α, β)-condition is weakening of the locality-sensitive hashing condition [1, 2].

Finally, relaxation of the minimum-distance property taken in Definition 1 may be motivated by availability of the redundancy in the k-bit data. In information theory transmitting such data across a noisy channel is known as the joint source-channel coding (JSCC) problem. Combinatorial variation, cf. [3, 4], can be stated as follows: say that $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$ is a (D, δ)-JSCC if there exists a decoder map $g : \mathbb{F}_2^n \to \mathbb{F}_2^k$ with the property

$$\forall x \in \mathbb{F}_2^k, z \in \mathbb{F}_2^n : \quad |f(x) - z| \le \delta n \quad \implies \quad |x - g(z)| \le Dk\,.$$

The operational meaning is that a (D, δ)-JSCC reduces the (adversarial) noise of strength δ in n-space to (adversarial) noise of strength D in k-space. A special case of $D = \epsilon\delta$ was introduced by Spielman [5] under the name of *error-reducing* codes. The connection to Def. 1 comes from the simple observation:

$$f \text{ is a } (D, \delta)\text{-JSCC} \quad \implies \quad f \text{ is a } (2D, 2\delta)\text{-map}\,.$$

Thus, every impossibility result for (α, β)-maps implies impossibility results for (D, δ)-JSCC and Spielman's error-reducing codes.

2. Main results

For $\alpha = 0$ the best known bound to date is due to McEliece et al [6]. It says that any set $S \subset \mathbb{F}_2^n$ with $|y - y'| \ge \delta n$ for all $y, y' \in S, y \ne y'$ satisfies

$$\frac{1}{n} \log |S| \le R_{LP2}(\delta) + o(1)\,, \tag{4}$$

where $R_{LP2}(\delta) = 0$ for $\delta \ge 1/2$ and for $\delta < 1/2$:

$$R_{LP2}(\delta) = \min(1 - h(\alpha) + h(\beta))\,, \tag{5}$$

where $h(x) = -x\log x - (1-x)\log(1-x)$ and the minimum is taken over all $0 \le \beta \le \alpha \le 1/2$ satisfying

$$2\frac{\alpha(1-\alpha) - \beta(1-\beta)}{1 + 2\sqrt{\beta(1-\beta)}} \le \delta\,.$$

For distances $\delta < 0.273$ the solution is given by $\alpha = 1/2$ and $R_{LP2}(\delta)$ has a simpler expression:

$$R_{LP1}(\delta) = h(1/2 - \sqrt{\delta(1-\delta)})\,. \tag{6}$$

Thus from (4) we get

$$\exists (0, \beta;\, k, n)\text{-map} \qquad \Longrightarrow \quad k/n \lesssim R_{LP2}(\beta)\,.$$

A natural question is whether going from $\alpha = 0$ to $\alpha > 0$ may enable larger rates $k/n > R_{LP2}(\beta)$.

The first impulse could be that the answer is negative. Indeed, note that for $\alpha < 1/2$ there is $2^{k+o(k)}$ points x' s.t. $|x - x'| > \alpha k$. Thus it may seem that for $\alpha < 1/2$ this relaxation yields no improvements (asymptotically) compared to $\alpha = 0$. This observation is incorrect for two reasons. First, we do not require f to be injective — thus although all points $f(x')$ are far from $f(x)$, they may not all be distinct. Second, even though each x has many x' satisfying $|x - x'| > \alpha k$, we in fact need a collection $S \subset \mathbb{F}_2^k$ s.t. $|x - x'| > \alpha k$ for all *pairs* $x, x' \in S$. Only then we may conclude that $f(S)$ is code in $\mathbb{F}_2^n$ with large minimal distance.

Thus, S needs to be an independent set in $H(k, \alpha k)$. How large can it be? To that end, we recall Turan's theorem, cf. [7, Theorem IV.6]:

$$\mathbb{\alpha}(G) \ge \frac{|V(G)|^2}{2(|E(G)| + |V(G)|)}\,. \tag{7}$$

Counting the number of edges of the graph $H(k, \alpha k)$ via Stirling's formula we get $|E(H(k, \alpha k))| = 2^k \sum_{j=0}^{\alpha k} \binom{k}{j} = 2^{k + kh(\alpha) + o(k)}$. Therefore,

$$\mathbb{\alpha}(H(k, \alpha k)) \ge \frac{(2^k)^2/2}{|E(H(k, \alpha k))| + 2^k} = 2^{k(1-h(\alpha)) + o(k)}\,. \tag{8}$$

Consequently, if an (α, β)-map exists then comparing (4) and (8) we get

$$k(1 - h(\alpha)) + o(k) \le nR_{LP2}(\beta) + o(n)\,. \tag{9}$$

One natural way to improve the bound would be to notice that graphs $H(k, \alpha k)$ have a lot of extra structure and perhaps simplistic estimate (8) via Turan's theorem can be improved. Unfortunately, despite decades of work the lower bound (8), known as the Gilbert-Varshamov bound, is asymptotically the best known. (For non-binary alphabets, however, better bounds exist [8].)

Instead, the next theorem improves (9) by establishing how another graph-function (the θ-function, see (21) below) behaves under graph homomorphisms, and then applying known results on θ-function for Hamming graphs established by Samorodnitsky [9, 10] and McEliece et al. [6].

Theorem 1. *For every $\epsilon > 0$ there exist a sequence $\delta_m \to 0$ s.t. if an $(\alpha, \beta; k, n)$-map exists with $\alpha \geq \epsilon$ and $\beta \geq \epsilon$ then*

$$kR_{Sam}(\alpha) + k\delta_k \leq nR_{LP2}(\beta) + n\delta_n \tag{10}$$

and

$$k\left(1 - h\left(\frac{\alpha}{2}\right)\right) + k\delta_k \leq n\left(1 - h\left(\frac{\beta}{2}\right)\right) + n\delta_n\,, \tag{11}$$

where

$$R_{Sam}(\alpha) = \frac{1}{2}\max\left(1 - h(\alpha) + R_{LP1}(\alpha), h(1 - 2\sqrt{\alpha(1-\alpha)})\right) \tag{12}$$

for $\alpha < 1/2$ and zero otherwise.

Remark 1. *The bound* (10) *is better for $n/k > 1$, while* (11) *is better for $n/k < 1$. See Section 5 for evaluations.*

Note that by virtue of relying only on the number of edges in $\bar{H}(k, \alpha k)$ the bound in (9) is robust in the sense that whenever (α, β) violate (9), there will be great many pairs of x, x' that violate (2). Here is a similar strengthening of Theorem 1.

Theorem 2. *For every $\epsilon > 0$ there exist a sequence $\delta_m \to 0$ with the following property. For every map $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$, every $S \subset \mathbb{F}_2^k$ of size $|S| > 2^{k(1-\epsilon+\delta_k)+n\delta_n}$ and every $\alpha, \beta \in [\epsilon, 1]$ satisfying*

$$kR_{Sam}(\alpha) - k\epsilon \geq nR_{LP2}(\beta) \tag{13}$$

or

$$k\left(1-h\left(\frac{\alpha}{2}\right)\right)-k\epsilon \geq n\left(1-h\left(\frac{\beta}{2}\right)\right) \tag{14}$$

there exists a pair $x, x' \in S$ such that

$$|x-x'| > \alpha k \quad \textit{and} \quad |f(x)-f(x')| \leq \beta n\,. \tag{15}$$

In particular, there are at least $2^{k(1+\epsilon-\delta_k)-n\delta_n}$ un-ordered pairs $\{x,x'\} \subset \mathbb{F}_2^k$ satisfying (15).

Next we consider an improved bound for the case of $\beta > 1/2$. Notice that by Plotkin bound [11, Chapter 2.2] we have

$$\alpha(H(n,\beta n)) \leq 1 + \frac{n}{2\beta n + 2 - n}\,.$$

In particular, $\bar{H}(n,\beta n)$ does not contain K_4 whenever $\beta > 2/3$. Therefore, any graph G which contains K_4 cannot map into $\bar{H}(n,\beta n)$. For example:

$$\bar{H}(3,1) \not\to \bar{H}(n,\beta n) \qquad \forall n \in \mathbb{Z}_+, \beta > 2/3\,.$$

The following elaborates on this idea:

Theorem 3. *For every $\epsilon > 0$ there exists $\delta_m \to 0$ such that if there exists an $(\alpha,\beta;k,n)$ map with $\beta > \frac{1}{2}$ and $\alpha \in [\frac{1}{2}+\epsilon; 1-\epsilon]$ then*

$$\alpha \geq \beta + \frac{(2\beta-1)^2}{2}\delta_k\,. \tag{16}$$

Furthermore, for any map $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$, any $\beta > 1/2$ and $\alpha \in [\frac{1}{2}+\epsilon; 1-\epsilon]$ and any set $S \subset \mathbb{F}_2^k$ of size

$$|S| > 2^k \frac{\frac{2\beta}{2\beta-1}}{\frac{2\alpha}{2\alpha-1} - \delta_k}$$

there exists a pair of points $x, x' \in S$ satisfying (15).

Remark 2. *Considering the argument preceding the theorem, it should not be so surprising that the relation between* α *and* β *in* (16) *is independent of the rate* $\frac{k}{n}$*. The significance of* (16) *is that for the case of* $\frac{n}{k} \in \mathbb{Z}$ *this bound is (asymptotically) optimal, as the example of the repetition map* (1) *clearly shows. For linear* (α, β)*-maps the result was shown in [4, Theorem 8] by studying properties of the generator matrix.*

When applied to linear maps $\mathbb{F}_2^k \to \mathbb{F}_2^n$ Theorems 2 and 3 have the following geometric interpretations:

Corollary 4. *For every* $\epsilon > 0$ *there exists a sequence* $\delta_\ell \to 0$ *with the following property. Fix any two lists of (possibly repeated) points* $u_1, \dots, u_k$ *and* $v_1, \dots, v_n$ *in projective space* $\mathbb{P}^{m-1}(\mathbb{F}_2)$ *s.t. that they are not all contained in a codimension 1 hyperplane. Fix any* $\alpha, \beta \in [\epsilon, 1]$ *s.t.*

$$m > k(1 - R_{Sam}(\alpha) + \delta_k) + n(R_{LP2}(\beta) + \delta_n) \tag{17}$$

or

$$m > k(h(\alpha/2) + \delta_k) + n(1 - h(\beta/2) + \delta_n)\,. \tag{18}$$

There exists a hyperplane H *of codimension 1 in* $\mathbb{P}^{m-1}$ *such that*

$$\#\{j : v_j \in H\} \geq (1-\beta)n\,, \quad \#\{i : u_i \in H\} < (1-\alpha)k \text{ or } = k\,. \tag{19}$$

Corollary 5. *For every* $\epsilon > 0$ *there exists* $\delta_\ell \to 0$ *with the following property. Fix any two lists of (possibly repeated) points* $u_1, \dots, u_k$ *and* $v_1, \dots, v_n$ *in projective space* $\mathbb{P}^{m-1}(\mathbb{F}_2)$ *s.t. that they are not all contained in a codimension 1 hyperplane. Fix any* $\beta > 1/2$ *and* $\alpha \in [\frac{1}{2} + \epsilon; 1 - \epsilon]$ *s.t.*

$$m > k + \log_2 \frac{2\beta}{2\beta - 1} - \log_2 \left(\frac{2\alpha}{2\alpha - 1} - \delta_k \right)\,. \tag{20}$$

Then there exists a hyperplane H *of codimension 1 in* $\mathbb{P}^{m-1}$ *satisfying* (19).

Note that by identifying homogeneous coordinates with affine coordinates we can establish set-isomorphism $\mathbb{P}^{m-1}(\mathbb{F}_2)$ and $\mathbb{F}_2^m \setminus \{0\}$. Thus, previous corollaries can be equivalently restated in terms of $\mathbb{F}_2^m$. For example, for any $\epsilon > 0$, all k sufficiently large and all n: *Fix some basis of* $\mathbb{F}_2^k$ *and arbitrary non-zero points* $v_1, \dots, v_n \in \mathbb{F}_2^k$*. Then there exists a* $(k-1)$*-subspace containing* $\geq \frac{n}{4}$ *v-points and* $< \left(\frac{1}{4} + \epsilon\right) k$ *basis vectors.* Note that this is a manifestly

$\mathbb{F}_2$-property since over large fields one could select v-points (when $n > 4k$) so that no $\frac{n}{4}$ of them are contained in a $(k-1)$-subspace.

The rest of the paper is organized as follows: Section 3 proves a few results on graph homomorphisms. In Section 4 these results are applied to prove Theorems 1-3 and Corollaries 4-5. We conclude in Section 5 with discussion, numerical evaluations and some open problems.

3. Graph homomorphisms

Let us introduce notation to be used in the remainder of the paper:

$$\theta_S(G) \stackrel{\triangle}{=} \max\{\operatorname{tr} JM : \operatorname{tr} M = 1, M \succeq 0, M|_{E(G)} = 0, M_{v,v'} \geq 0 \ \forall v, v'\} \quad (21)$$

$$= \min\{\lambda_{\max}(C) : C = C^T, C|_{E(G)^c} \geq 1\} \quad (22)$$

$$\theta_L(G) \stackrel{\triangle}{=} \max\{\operatorname{tr} JM : \operatorname{tr} M = 1, M \succeq 0, M|_{E(G)} = 0\} \quad (23)$$

$$= \min\{\lambda_{\max}(C) : C = C^T, C|_{E(G)^c} = 1\}\,, \quad (24)$$

where M is a positive-semidefinite matrix of order $|V(G)|$, J is an all-one matrix of the same size, $\lambda_{\max}(\cdot)$ denotes the maximal eigenvalue and $M|_S$ denotes a subset $\{M_{i,j} : (i,j) \in S\}$ of the entries of matrix M, so that $M|_{E(G)} = \{M_{i,j} : i \sim j \text{ in } G\}$. $\theta_S(G)$ and $\theta_L(G)$ are the Schrijver and Lovász θ-functions, respectively[1].

We recall a few properties of the θ-function (one may consult [12] for more):

- Both θ-functions are typically used to upper bound the independence number of a graph:

$$\alpha(G) \leq \theta_S(G) \leq \theta_L(G)\,. \quad (25)$$

- $\theta_L(\cdot)$, while yielding a looser bound on $\alpha(\cdot)$, is multiplicative under strong product of graphs[2] as shown in [13]:

$$\theta_L(G \boxtimes H) = \theta_L(G)\theta_L(H)\,. \quad (26)$$

[1] Other authors write $\theta(G)$ for $\theta_L(G)$ and any of $\theta'(G)$, $\theta_{1/2}(G)$ or $\theta^-(G)$ for $\theta_S(G)$.

[2] The strong product $G \boxtimes H$ is a simple graph with vertex set given by $V(G) \times V(H)$ and edges $(g_1, h_1) \sim (g_2, h_2) : (g_1 \sim g_2 \text{ or } g_1 = g_2)$ and $(h_1 \sim h_2 \text{ or } h_1 = h_2)$.

- For a vertex transitive graphs, we also have reciprocity [13]:

$$\theta_L(G)\theta_L(\bar{G}) = |V(G)|\,. \tag{27}$$

Our main technical contribution in this section is the following partial generalization of (26)-(27) to θ_S:

Lemma 6. *Let G be vertex transitive, then*

$$\theta_S(G \boxtimes H) \le \frac{|V(G)|}{\theta_S(\bar{G})}\theta_S(H)\,. \tag{28}$$

Proof is given at the end of this section. We next discuss its application to existence of graph homomorphisms.

The graph homomorphism $f : X \to Y$ is a map of vertices of X to vertices of Y such that endpoints of each edge of X map to the endpoints of some edge in Y. If there exists any graph homomorphism between X and Y we will write $X \to Y$. The problem of finding $f : X \to Y$ is known as Y-coloring problem.

For establishing properties of graph homomorphisms it is convenient to introduce *homomorphic product* [14][3]: graph $X \ltimes Y$ is a simple graph with vertices $V(X) \times V(Y)$ and $(x_1, y_1) \sim (x_2, y_2)$ if $x_1 = x_2$ or $x_1 \sim x_2, y_1 \not\sim y_2$. From (25) and definition of $X \ltimes Y$ we have:

$$\alpha(X \ltimes Y) \le \theta_S(X \ltimes Y) \le \theta_L(X \ltimes Y) \le |V(X)|$$

and

$$\alpha(X \ltimes Y) = |V(X)| \quad \iff \quad X \to Y\,.$$

We overview some of the well-known tools for proving $X \not\to Y$:

- (No-Homomorphism Lemma [15]) If $X \to Y$ and Y is vertex transitive then
$$\frac{\alpha(X)}{|V(X)|} \ge \frac{\alpha(Y)}{|V(Y)|}\,. \tag{29}$$

- (Monotonicity of $\bar{\alpha}$) If $X \to Y$ then
$$\alpha(\bar{X}) \le \alpha(\bar{Y}) \tag{30}$$

[3]Note that [14] instead defines hom-product $X \circ Y$ which corresponds to $\overline{X \ltimes Y}$.

- (Monotonicity of $\bar{\theta}$) If $X \to Y$ then

$$\theta_L(\bar{X}) \le \theta_L(\bar{Y}) \tag{31}$$
$$\theta_S(\bar{X}) \le \theta_S(\bar{Y})\,. \tag{32}$$

- (Homomorphic product) If $X \to Y$ then

$$\theta_S(X \ltimes Y) = |V(X)| \tag{33}$$
$$\theta_L(X \ltimes Y) = |V(X)|\,. \tag{34}$$

Note that (31)-(34) give necessary conditions for $X \to Y$. Although, generally not tight, these conditions can be understood as elegant relaxations (semi-definite, fractional, quantum etc) of the graph homomorphism problem, cf. [16, 14, 17, 18, 19].

Inequalities (29)-(34) are useful for showing $X \not\to Y$. If $X \not\to Y$ it is natural to ask for a quantity measuring to what extent X fails to homomorphically map into Y. One such quantity is $\alpha(X \ltimes Y)$, since

$$\alpha(X \ltimes Y) = \max\{|V(G)| : G\text{– induced subgraph of } X \text{ s.t. } G \to Y\}\,. \tag{35}$$

Indeed, by construction any independent set S in $X \ltimes Y$ has at most one point in each fiber $\{x_0\} \times Y$ and thus projection $V(G) \triangleq \mathrm{proj}_1(S)$ onto X always yields an induced subgraph $G \subset X$ satisfying $G \to Y$. With (35) in mind, the next set of results will allow us to assess the degree of failure of $X \not\to Y$.

Theorem 7. *If X is vertex transitive, then*

$$\alpha(X \ltimes Y) \le |V(X)| \frac{\alpha(\bar{Y})}{\alpha(\bar{X})} \tag{36}$$
$$\theta_S(X \ltimes Y) \le |V(X)| \frac{\theta_S(\bar{Y})}{\theta_S(\bar{X})} \tag{37}$$
$$\theta_L(X \ltimes Y) \le |V(X)| \frac{\theta_L(\bar{Y})}{\theta_L(\bar{X})} = \theta_L(X)\theta_L(\bar{Y})\,. \tag{38}$$

If Y is vertex transitive, then

$$\alpha(X \ltimes Y) \le |V(Y)| \frac{\alpha(X)}{\alpha(Y)} \tag{39}$$

$$\theta_S(X \ltimes Y) \le |V(Y)| \frac{\theta_S(X)}{\theta_S(Y)} \tag{40}$$

$$\theta_L(X \ltimes Y) \le |V(Y)| \frac{\theta_L(X)}{\theta_L(Y)} = \theta_L(X)\theta_L(\bar{Y})\,. \tag{41}$$

Remark 3. *One may view* (36)-(38) *as a quantitative version of criteria* (30)-(32) *and* (39)-(41) *as a quantitative version of no-homomorphism lemma* (29)*. Note also that the right-most versions of* (38) *and* (41) *hold without any transitivity assumptions [14, Theorem 17]: For any X, Y*

$$\theta_L(X \ltimes Y) \le \theta_L(X)\theta_L(\bar{Y})\,. \tag{42}$$

Proof. The proof relies on the following simple observation: The strong product $X \boxtimes \bar{Y}$ of X and $\bar{Y}$ – is a subgraph of $X \ltimes Y$. Thus by edge-monotonicity:

$$\alpha, \theta_S, \theta_L(X \ltimes Y) \le \alpha, \theta_S, \theta_L(X \boxtimes \bar{Y})\,.$$

From here the results on α and θ_S follow from Lemma 6 with $G = X$, $H = \bar{Y}$ (for (36) and (37)) or $G = \bar{Y}$ and $H = X$ (for (39) and (40)). For θ_L the equality parts of (38) and (41) follow from the results of Lovász (26) and (27). □

One of the classically useful methods in coding theory is the Elias-Bassalygo reduction: From a given code in $\mathbb{F}_2^n$ one selects a large subcode sitting on a Hamming sphere of a given radius. One then bounds minimum distance (or other) parameters for the packing problem in the Johnson graph $J(n, d, w)$. It so happens that taking a simple dual certificate for $\theta_S(J(n, d, w))$ and transporting the bound back to the full space results in excellent bounds, which are hard (but possible – see Rodemich theorem in [20, p. 27]) to obtain by direct SDP methods in the full space. Succinctly, we may summarize this as follows: If G' is an induced subgraph of a vertex transitive G then

$$\alpha(G), \theta_S(G), \theta_L(G) \le \frac{|V(G)|}{|V(G')|}\alpha(G'), \theta_S(G'), \theta_L(G') \quad \text{resp.}$$

Here is a version of the similar method for the graph-homomorphism problem and for the problem of finding independent sets in $G \boxtimes H$:

Proposition 8. *Let G be a vertex transitive graph and G' its induced subgraph. Then*

$$\alpha(G \boxtimes H) \le \frac{|V(G)|}{|V(G')|}\alpha(G' \boxtimes H) \tag{43}$$

$$\theta_S(G \boxtimes H) \le \frac{|V(G)|}{|V(G')|}\theta_S(G' \boxtimes H) \tag{44}$$

and same for θ_L.

Proof. Let Γ be the group of automorphisms of G. The action of Γ naturally extends to the action on $G \boxtimes H$ via:

$$\gamma(g,h) \triangleq (\gamma(g), h)\,.$$

Let S be the maximal independent set of $G \boxtimes H$. Consider the chain:

$$\alpha(G' \boxtimes H) \ge \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma} |\gamma(S) \cap G' \boxtimes H| \tag{45}$$

$$= \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma, g, g', h} 1\{\gamma(g) = g'\}1\{(g',h)\in S\}1\{g \in G'\} \tag{46}$$

$$= \frac{|S|\,|V(G')|}{|V(G)|}, \tag{47}$$

where (45) follows since each $\gamma(S)\cap G' \boxtimes H$ is an independent set of $G' \boxtimes H$, (46) is obvious, and (47) is because by the transitivity of the action of Γ: $\sum_\gamma 1\{\gamma(g) = g'\} = \frac{|\Gamma|}{V(G)}$. Clearly, (47) is equivalent to (43).

For (44) let $M = (M_{g_1h_1,g_2h_2}, g_1, g_2 \in G, h_1, h_2 \in H)$ be the maximizer in (21). Symmetrizing over Γ if necessary we may assume that

$$M_{gh_1,gh_2} = M_{g'h_1,g'h_2} \qquad \forall g, g' \in G, h_1, h_2 \in H \tag{48}$$

$$M_{g_1h_1,g_2h_2} = M_{\gamma(g_1)h_1,\gamma(g_2)h_2} \qquad \forall g_1, g_2 \in G, h_1, h_2 \in H, \forall\gamma\in\Gamma \tag{49}$$

Last equation also implies that the subspace spanned by vectors $1_G \otimes (\cdot)$ is an eigenspace of M. Here and below $1_G, 1_H$ are all-one vectors of dimensions $|V(G)|$ and $|V(H)|$ respectively. And $1_{G'}$ is a zero/one vector of dimension $|V(G)|$ having ones in coordinates corresponding to vertices in G'.

Set

$$\tilde{M}_{g_1h_1,g_2h_2} = \frac{|V(G)|}{|V(G')|} M_{g_1h_1,g_2h_2} \quad \forall g_1, g_2 \in G', h_1, h_2 \in H\,.$$

One easily verifies that $\tilde{M}$ is a feasible choice for the primal program (21) for $\theta_S(G' \boxtimes H)$. To compute $\operatorname{tr} J\tilde{M}$ we notice that

$$\operatorname{tr} J\tilde{M} = \frac{|V(G)|}{|V(G')|} \left(M 1_{G'} \otimes 1_H, 1_{G'} \otimes 1_H \right)\,, \tag{50}$$

where $(\cdot, \cdot)$ is a standard inner product on $\mathbb{R}^{|V(G)|} \otimes \mathbb{R}^{|V(H)|}$. Finally, observe that orthogonal decomposition

$$1_{G'} \otimes 1_H = c 1_G \otimes 1_H + (1_{G'} - c 1_G) \otimes 1_H\,, \qquad c = \frac{|V(G')|}{|V(G)|}$$

remains orthogonal after application of M, cf. (48). Therefore, we get by positivity $M \succeq 0$ that

$$(M 1_{G'} \otimes 1_H, 1_{G'} \otimes 1_H) \geq c^2 (M 1_G \otimes 1_H, 1_G \otimes 1_H) = c^2 \operatorname{tr} JM\,,$$

which together with (50) completes the proof of (44). $\square$

Corollary 9. *Let X' and Y' be induced subgraphs of X and Y, respectively. If X is vertex transitive then*

$$\alpha(X \ltimes Y) \leq \frac{|V(X)|}{|V(X')|} \alpha(X' \ltimes Y)\,.$$

If Y is vertex transitive then

$$\alpha(X \ltimes Y) \leq \frac{|V(Y)|}{|V(Y')|} \alpha(X \ltimes Y')\,.$$

Proof (Lemma 6). We will give an explicit proof by exhibiting a choice of $\tilde{C}$ in (22) for computing $\theta_S(G \boxtimes H)$.

Let M be the optimal (primal) solution of (21) for $\theta_S(\bar{G})$ and let C be the optimal (dual) solution of (22) for $\theta_S(H)$. We know:

$$\operatorname{tr} JM = \theta_S(\bar{G}), \lambda_{\max}(C) = \theta_S(H)\,.$$

and also from the vertex-transitivity of G without loss of generality we may assume that

$$M_{g,g} = \frac{1}{|V(G)|}, M1 = \frac{\operatorname{tr} JM}{|V(G)|} 1\,,$$

where 1 is an all-one vector. We now define[4]

$$\hat{C} \triangleq c_1 I + c_2 M \otimes (C - \lambda_{\max}(C) I - J) + J\,, \tag{51}$$

where as before J denotes the square matrix of all ones (of different dimension depending on context) and

$$c_1 \triangleq \frac{\lambda_{\max}(C)|V(G)|}{\operatorname{tr} JM}, \quad c_2 = \frac{|V(G)|^2}{\operatorname{tr} JM}\,. \tag{52}$$

We will prove that $\hat{C}$ is a feasible choice in the (dual) problem (22) for $\theta_S(G \boxtimes H)$. Then we can conclude that since $M \succeq 0$ and $C - \lambda_{\max}(C) I \preceq 0$ that

$$\hat{C} \preceq c_1 I - c_2 M \otimes J + J = c_1 I - (c_2 M - J) \otimes J \preceq c_1 I \tag{53}$$

since by construction $c_2 M - J \succeq 0$ (recall that M and J commute). Thus,

$$\lambda_{\max}(C) \le c_1 = \frac{|V(G)|\theta_S(H)}{\theta_S(\bar{G})}$$

proving (37). To verify that $\hat{C}$ is feasible dual assignment, we need to show

$$\hat{C}_{gh,g'h'} \ge 1 \quad \forall g, h, g', h' : \begin{cases} g = g', h = h', & \text{or} \\ g \ne g', g \not\sim g', & \text{or} \\ h \ne h', h \not\sim h'\,, \end{cases} \tag{54}$$

which follows since $E(G \boxtimes H)^c$ consists of all self-loops and edges connecting pairs that are non-adjacent (and non-identical) in either G or H-coordinate.

To verify (54) we recall that M and C satisfy

$$M_{g,g'} \ge 0 \quad \forall g, g' \tag{55}$$
$$M_{g,g'} = 0 \quad \forall g \not\sim g' \text{ and } g \ne g' \tag{56}$$
$$C_{h,h'} \ge 1 \quad \forall h \not\sim h' \tag{57}$$

[4]This choice may appear mysterious, but notice that if we define $D = C - \lambda_{\max}(C) I - J$ and assuming $\lambda_{\max}(\hat{C}) = c_1$ we could write (51) as $\hat{D} = c_2 M \otimes D$, which is more natural.

Then verification proceeds in a straightforward manner. For example, in the first case in (54) we have

$$\begin{aligned}\hat{C}_{gh,gh} &= c_1 + \frac{c_2}{|V(G)|}(C_{h,h} - \lambda_{\max}(C) - 1) + 1 \\ &\geq c_1 - \frac{c_2 \lambda_{\max}(C)}{|V(G)|} + 1 = 1\end{aligned}$$

because $C_{h,h} \geq 1$ and by (52). The two remaining cases are checked similarly.

$\square$

4. Proofs of main results

Before going into details of the proofs, we make a clarifying remark. Our main goal is to improve the simple bound (9), which (we remind) was obtained by noticing that independent sets of $H(k, \alpha k)$ transform under (α, β)-maps into independent sets of $H(n, \beta n)$. The improvement comes by noticing that (α, β)-maps also transform any matrix M in (21) feasible for $H(k, \alpha k)$ into a matrix M' feasible for $H(n, \beta n)$. Good feasible matrices for $H(k, \alpha k)$ were found previously in [9, 10]. We proceed to formal details.

Proof (Theorems 1 and 2). Clearly, it is sufficient to prove Theorem 2. We quote the following results of Kleitman [21], McEliece et al [6] and the joint lower bound of Samorodnitsky [9] and Navon-Samorodnitsky [10]:

$$\frac{1}{m} \log \alpha(\bar{H}(n, \lambda m)) = h(\lambda/2) + \delta_m(\lambda) \tag{58}$$

$$\frac{1}{m} \log \theta_S(H(m, \lambda m)) \leq R_{LP2}(\lambda) + \delta_m(\lambda) \tag{59}$$

$$\frac{1}{m} \log \theta_S(H(m, \lambda m)) \geq R_{Sam}(\lambda) - \delta_m(\lambda)\,, \tag{60}$$

where the remainder term $\delta_m(\lambda) \to 0$ uniformly on compacts in $\lambda \in (0, 1]$.

Take $\alpha, \beta \geq \epsilon$ and $k, n \in \mathbb{Z}_+$. Define $\delta_m = \sup_{\lambda \in [\epsilon, 1]} \delta_m(\lambda)$. Assume that (13) holds. Consider arbitrary $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$. Notice that if S is a set which does not contain any pair satisfying (15), then the set

$$\{(x, y) : x \in S, y = f(x)\}$$

is an independent set of $\bar{H}(k, \alpha k) \ltimes \bar{H}(n, \beta n)$. (This is also clear from (35) as f defines a homomorphism $S \to \bar{H}(n, \beta n)$ if S is viewed as induced subgraph of $\bar{H}(k, \alpha k)$.) Thus it is sufficient to show

$$\alpha(\bar{H}(k, \alpha k) \ltimes \bar{H}(n, \beta n)) \le 2^{k(1-\epsilon)+n\delta_n+k\delta_k}$$

This follows from the following chain:

$$\begin{aligned} \alpha(\bar{H}(k, \alpha k) \ltimes \bar{H}(n, \beta n)) &\le 2^k \frac{\theta_S(H(n, \beta n))}{\theta_S(H(k, \alpha k))} && (61)\\ &\le 2^{k+nR_{LP2}(\beta)-kR_{Sam}(\alpha)+n\delta_n+k\delta_k} && (62)\\ &\le 2^{k(1-\epsilon)+n\delta_n+k\delta_k}, && (63) \end{aligned}$$

where (61) is from (37), (62) is from (59) and (60) and (63) is from (13).

If instead of (13) the pair (α, β) satisfies (14) then the argument is the same except in (61) we should apply (39) and (58) to get:[5]

$$\alpha(\bar{H}(k, \alpha k) \ltimes \bar{H}(n, \beta n)) \le 2^{k+n(1-nh(\beta/2)+\delta_n)-k(1-h(\alpha/2)-\delta_k)}$$

and the rest of the proof is the same.

Finally, to show the statement about the number of pairs satisfying (15) define a graph G with vertices $\mathbb{F}_2^k$ and $x \sim x'$ if (15) holds. We have already shown

$$\alpha(G) \le 2^{k(1-\epsilon)+n\delta_n+k\delta_k}.$$

Then from Turan's theorem we have

$$|E(G)| \ge \frac{|V(G)|}{2} \left(\frac{|V(G)|}{\alpha(G)} - 1 \right) \ge 2^{k(1+\epsilon-\delta_k)-n\delta_n}$$

(after enlarging δ_k slightly). □

---

[5]Note that another result of Samorodnitsky [22, Proposition 1.2] shows that up to factors $2^{o(m)}$ we have

$$\theta_L(\bar{H}(m, \lambda m)) \approx \theta_S(\bar{H}(m, \lambda m)) \approx \alpha(\bar{H}(m, \lambda m)) = 2^{mh(\lambda/2)+o(m)}.$$

Therefore here we could still operate with θ_S only and apply (40). We chose to use α's because Kleitman's theorem (58) has explicit non-asymptotic form and thus for finite k, n results in a better bound.

Proof (Theorem 3). The argument follows step by step the proof of Theorem 3 except that at (61) we use the (almost) exact value of $\theta_S(H(n,d))$ for $d > n/2$ found in the Lemma below.

Lemma 10. *For any $\lambda \in (1/2, 1)$ there exists $\delta_n(\lambda) \ge 0$ s.t.*

$$\frac{2\lambda}{2\lambda - 1} - \delta_n(\lambda) \le \theta_S(H(n, \lfloor \lambda n \rfloor)) \tag{64}$$

$$\le \frac{2\lambda}{2\lambda - 1}\,. \tag{65}$$

Furthermore, $\delta_n(\lambda) \to 0$ uniformly on compacts of $(1/2, 1)$.

Proof. We need to introduce the standard definitions from linear programming bounds in coding theory, cf. [11, Ch. 17]. Any polynomial $f(x) \in \mathbb{R}[x]$ of degree $\le n$ can be represented as

$$f(x) = 2^{-n} \sum_{j=0}^{n} \hat{f}(j) K_j^{(n)}(x)\,,$$

where Krawtchouk polynomials are defined as

$$K_j^{(n)}(x) \triangleq \sum_{k=0}^{n} (-1)^j \binom{x}{k} \binom{n-x}{j-k} \tag{66}$$

and, for example, $K_0^{(n)}(x) = 1$, $K_1^{(n)}(x) = n - 2x$.

It is a standard result [23, Theorem 3] that for the Hamming graphs the semidefinite program (21) becomes a linear program. We put it here in the following form:

$$\theta_S(H(n,d))$$
$$= \max\left\{ \frac{\hat{f}(0)}{f(0)} : \hat{f} \ge 0, f(x) = 0, x \in [1,d] \cap \mathbb{Z}, f(x) \ge 0, x \in [0,n] \cap \mathbb{Z} \right\} \tag{67}$$

$$= \min\left\{ 2^n \frac{g(0)}{\hat{g}(0)} : \hat{g} \ge 0, g(x) \le 0, x \in [d+1, n] \cap \mathbb{Z}, \hat{g}(0) > 0 \right\} \tag{68}$$

where f and g are polynomials of degree at most n.

The upper bound (65) is a standard Plotkin bound (see [11, Ch. 17, §4]): taking $g(x) = 2(d+1-x)$ we notice that

$$g(x) = K_1^{(n)}(x) + (2(d+1)-n)K_0^{(n)}(x)\,.$$

Thus $\hat{g}(0) = 2^n(2d+2-n)$ and we get for $d = \lfloor \lambda n \rfloor$

$$\theta_S(H(n,d)) \le \frac{2(d+1)}{2d+2-n} \le \frac{2\lambda}{2\lambda-1}\,.$$

For the lower bound (65) we assume that $d = \lfloor \lambda n \rfloor$,

$$\lambda \in [1/2-\epsilon, 1-\epsilon] \tag{69}$$

and n is sufficiently large (for all small n we may take $\delta_n(\lambda) = \frac{2\lambda}{2\lambda-1}$). We first consider the case of d – odd.

Consider the polynomial $f(x) = 2^{-n}\sum_{\omega=0}^n K_\omega^{(n)}(x)$ with coefficients given by

$$\hat{f}(\omega) = K_0^{(n)}(\omega) + r\binom{n}{d+1}^{-1} K_{d+1}^{(n)}(\omega)\,, \omega = 0,1,\dots,n \tag{70}$$

where $r \in (0,1)$ is to be determined. To compute values of this polynomial, we employ the orthogonality relation for Krawtchouk polynomials, cf. [24, (34)]:

$$\sum_{\omega=0}^n K_\ell^{(n)}(\omega)K_\omega^{(n)}(x) = 2^n 1\{x=\ell\}, \qquad \forall x,\ell \in [0,n]\cap\mathbb{Z}$$

From here we get

$$f(x) = \begin{cases} 1, & x = 0 \\ r\binom{n}{d+1}^{-1}, & x = d+1 \\ 0, & \text{all other } x \in [0,n]\cap\mathbb{Z}\,. \end{cases}$$

We note that this $f(x)$ was guessed by studying Levenshtein's codes that attain Plotkin bound [11, Chapter 2, Theorem 8].

To verify that $f(x)$ is a (asymptotically!) feasible solution of (67) we need to check $\hat{f}(\omega) \ge 0$. First, let $m = n-d-1 \le n/2$ and notice that [24, (31)-(32)]

$$K_{d+1}^{(n)}(\omega) = (-1)^\omega K_m^{(n)}(\omega) = (-1)^{(n-\omega)+(m-n)} K_m^{(n)}(n-\omega)\,.$$

Therefore, since $n - m$ is even it is sufficient to verify

$$(-1)^\omega K_m^{(n)}(\omega) \geq -\frac{1}{r}\binom{n}{m} \tag{71}$$

for all $\omega \in [0, n/2] \cap \mathbb{Z}$. For $\omega = 0$ this is obvious, for $\omega = 1$ we have [24, (13)]

$$K_m^{(n)}(1) = \frac{n-2m}{n}\binom{n}{m}$$

and thus taking

$$r = \frac{n}{n-2m}$$

makes (71) hold at $\omega = 1$.

It is known that $K_m^{(n)}(x)$ has m real roots with the smallest root x_1 satisfying [24, (71)]

$$x_1 \geq \frac{n}{2} - \sqrt{m(n-m)}\,. \tag{72}$$

Therefore, polynomial $K_m^{(n)}(x)$ is decreasing on $(-\infty, x_1]$ and hence (71) must also hold for all odd $\omega \in [1, x_1]$ (for even $\omega \leq x_1$, inequality (71) holds just by considering the signs). In view of (72) we only need to show (71) for $\xi n \leq \omega \leq n/2$, where

$$\xi = \frac{1}{2} - \sqrt{\lambda(1-\lambda)}\,. \tag{73}$$

In this range, we will show a stronger bound

$$|K_m^{(n)}(x)| \leq \frac{1}{r}\binom{n}{m}\,. \tag{74}$$

The following bound is well known [24, (87)][6]:

$$|K_m^{(n)}(\omega)| \leq 2^{\frac{n}{2}}\binom{n}{m}^{\frac{1}{2}}\binom{n}{\omega}^{-\frac{1}{2}}\,.$$

Note that by the constraint (69) ξ is bounded away from 0 and thus we can estimate

$$\binom{n}{m}\binom{n}{\omega}^{-1} \leq 2^{n(h(\lambda)-h(\xi)+\delta_n')}$$

[6]To get an explicit estimate on $\delta_n(\lambda)$ in (64), we could use the non-asymptotic bound in [25, Lemma 4], which also holds for $\omega < \xi n$.

for some sequence δ'_n that only depends on ϵ. Thus comparing the exponents on both sides of (71) we see that it will hold provided that

$$r^{-2} \geq 2^{n(1-h(\lambda)+h(\xi))+n\delta'_n} . \tag{75}$$

But notice that by (73) the exponent in parenthesis is exactly the gap between the Gilbert-Varshamov bound $1-h(1-\lambda))$ and the first linear programming bound $R_{LP1}(1-\lambda)$, cf. (6). There exists $\epsilon' > 0$ separating these two bounds for all λ's in (69). Thus, the right-hand side of (75) is exponentially decreasing $2^{-\epsilon' n+n\delta'_n}$ and hence for sufficiently large n it must hold. This completes the proof that $f(x)$ in (70) is a feasible choice in (67). Therefore, we have shown that for all n sufficiently large

$$\theta_S(H(n,d)) \geq 1 + r = \frac{2d+2}{2d+2-n}$$

if d is odd and

$$\theta_S(H(n,d)) \geq \theta_S(H(n,d+1)) \geq \frac{2d+4}{2d+4-n}$$

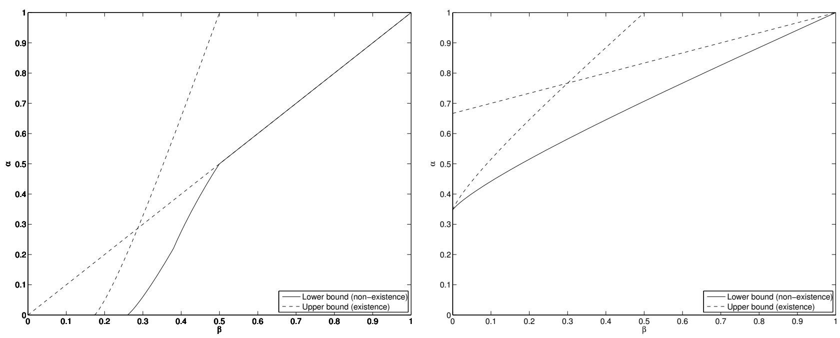
if d is even. □

Proof (Corollaries 4 and 5). Assume to the contrary that one found α, β and $u_1, \ldots, u_k, v_1, \ldots, v_n \in \mathbb{P}^{m-1}$ s.t. there is no hyperplane satisfying (19). Then as explained in Section 5.5 below (see (81)), there is an independent set of size 2^m in $\bar{H}(k, \alpha k) \boxtimes H(n, \beta n)$. By inspecting the proofs of Theorem 2 and 3 we notice that they prove three different upper bounds on $\alpha(\bar{H}(k, \alpha k) \boxtimes H(n, \beta n))$ that are equal to exponentiation of the left-hand sides of (17), (18) and (20) respectively. Therefore, m cannot satisfy any of (17),(18) or (20) – a contradiction. □

5. Discussion and open problems

5.1. Evaluation

In this section we evaluate our bounds. We consider the asymptotic setting $k \to \infty$ and $n = \rho k$ where ρ is fixed. In Fig. 1(a) ($\rho = 3$) and Fig. 1(b) ($\rho = 1/3$) we plot the various bounds on the region of asymptotically feasible pairs (α, β):



(a) $\rho = 3$ (b) $\rho = \frac{1}{3}$

Figure 1: Bounds on minimal possible α for a given $\beta \in (0,1)$ in the asymptotics $n, k \to \infty$ and $\frac{n}{k} = \rho$.

- For $\rho = 3$ the lower bound for $0 < \alpha < 1/2$ is (10) from Theorem 1; for $1/2 \le \alpha \le 1$ is Theorem 3.
- For $\rho = 1/3$ the lower bound (for all α) is (11). In this case the other two bounds, (10) and (16), are strictly worse.
- For $\rho = 3$ the straight dashed line denotes performance of the repetition map (1).
- For $\rho = \frac{1}{3}$ the straight dashed line denotes performance of the *majority-vote* map. Namely $f : \mathbb{F}_2^{3n} \to \mathbb{F}_2^n$ gives a majority vote for every one of 3-bit blocks. It is clear that for all x, x' we have:

  $$|f(x) - f(x')| \le \beta n \qquad \Longrightarrow \qquad |x - x'| \le \frac{2+\beta}{3} n$$

  Indeed any pair of 3-bit strings for which majority-vote agrees can be at most Hamming distance 2 away (as 001 and 010).
- Finally, the curved dashed line corresponds to the *separation map* defined as follows. Fix $\alpha \in (0,1)$ and cover $\mathbb{F}_2^k$ with balls of radius $\alpha k/2$. It is sufficient to have $2^{k(1-h(\alpha/2))+o(k)}$ such balls. Also consider a packing of balls of radius $\beta n/2$ in $\mathbb{F}_2^n$. By Gilbert-Varshamov bound we know that we can select at least $2^{n(1-h(\beta))+o(n)}$ such balls. Thus whenever

  $$k(1 - h(\alpha/2)) + o(k) \le n(1 - h(\beta)) + o(n)$$

we can construct the map $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$ that maps every point inside an $\alpha k/2$ ball to a center of the corresponding packing ball. Clearly, such map will be an (α, β) map. Thus, asymptotically all pairs of (α, β) s.t. $\beta \le 1/2$ and

$$1 - h(\alpha/2) \ge \rho(1 - h(\beta))$$

are achievable.

Note that as $\beta \nearrow \frac{1}{2}$ the bound (10) becomes:

$$\alpha \ge \frac{1}{2} - \sqrt{\rho}\left(\frac{1}{2} - \beta\right) + o(1 - 2\beta)\,, \qquad \beta \to \frac{1}{2}\,. \tag{76}$$

This is a significant improvement over what the simple bound (9) yields:

$$\alpha \ge \frac{1}{2} - \sqrt{\frac{\rho}{2\log_2 e}(1 - 2\beta)\log_2\frac{1}{1 - 2\beta}} + o(h((1/2 - \beta)^2)), \qquad \beta \to \frac{1}{2}\,.$$

In particular, (76) has finite slope at $\alpha = \beta = \frac{1}{2}$ and furthermore as $\rho \searrow 1$ the slope-discontinuity at $(1/2, 1/2)$, see Fig. 1(a), disappears. This last effect is a consequence of the Navon-Samorodnitsky [10] part of the bound (12).

5.2. On list-decodable codes

One of the more interesting conclusions that we can draw from our bounds is the following. It is well known that there is only finitely many balls of radius $\ge n(1/4 + \epsilon)$ that can be packed inside $\mathbb{F}_2^n$ without overlapping (Plotkin bound). However, if one allows these balls to cover each point with multiplicity at most 3 then it is possible to pack exponentially many balls [26]. Thus, if one is allowed to decode into lists of size 3, it is possible to withstand adversarial noise of weight $1/4 + \epsilon$ while still having non-zero communication rate.

By setting $\beta = 1/2 + 2\epsilon$ and applying Theorem 3 we figure out, however, that no matter how the balls are labeled by k-bit strings, at least one ball of radius $1/4 + \epsilon$ will contain a pair of points whose labels differ in at least $(1/2 + 2\epsilon)k$ positions. So although list-decoding allows one to overcome the $1/4$ barrier, there is no hope (in the worst case) to recover any information bits from the labels. This is only true beyond the radius $1/4$, since of course, below $1/4$ one can use codes with list-1. Loosely speaking, we have a "phase-transition" in the communication problem at noise-level $1/4$.

5.3. Linear programming bound

It is possible to write a linear program for $\theta_S(\bar{H}(k,\alpha k) \ltimes \bar{H}(n,\beta n))$ similarly to the standard Delsarte's program (67)-(68). To that end, for an arbitrary polynomial $f(x,y)$ of degree at most k in x and at most n in y we can write it as

$$f(x,y) = 2^{-n-k} \sum_{i=0}^{k} \sum_{j=0}^{n} \hat{f}(i,j) K_i^{(k)}(x) K_j^{(n)}(y)\,,$$

where $K_i^{(k)}(x)$ and $K_j^{(n)}(y)$ are Krawtchouk polynomials (66). With this definition of the Fourier transform $\hat{f}$ we have:

$$\begin{aligned} &\theta_S(\bar{H}(k,\alpha k) \ltimes \bar{H}(n,\beta n)) \\ &= \max\left\{ \frac{\hat{f}(0,0)}{f(0,0)} : \hat{f} \geq 0, f(x,y) = 0 \forall (x,y) \in \mathcal{D} \setminus (0,0) \right\} && (77) \\ &= \min\left\{ 2^{k+n} \frac{g(0,0)}{\hat{g}(0,0)} : \hat{g} \geq 0, g(x,y) \leq 0, \forall (x,y) \in \mathcal{D}^c \setminus (0,0) \right\} && (78) \end{aligned}$$

where f, g are bi-variate polynomials of degree at most (k,n), and

$$\mathcal{D} \stackrel{\triangle}{=} \{(x,y) : x \in [0,k] \cap \mathbb{Z}, y \in [0,n] \cap \mathbb{Z}, (x = 0, y \neq 0) \text{ or } (x > \alpha k, y \leq \beta n)\} \tag{79}$$

$$\mathcal{D}^c \stackrel{\triangle}{=} \{(x,y) : x \in [0,k] \cap \mathbb{Z}, y \in [0,n] \cap \mathbb{Z}, (0 < x \leq \alpha k) \text{ or } (x \neq 0, y > \beta n)\} \tag{80}$$

The bound used in Theorem 2 states

$$\theta_S(\bar{H}(k,\alpha k) \ltimes \bar{H}(n,\beta n)) \leq 2^{k + nR_{LP2}(\beta) - kR_{Sam}(\alpha) + o(n) + o(k)}$$

This bound corresponds to the following choice of $g(x,y)$ in (78):

$$g(x,y) = f_1(x) g_1(y)\,,$$

where $f_1(x)$ is the Samorodnitsky assignment [9] in the primal for $\theta_S(H(k,\alpha k))$ and $g_1(y)$ is a standard choice of McEliece-Rodemich-Rumsey-Welch [6] in the dual for $\theta_S(H(n,\beta n))$. In fact, any primal f_1 and any dual g_1 give a candidate for $g(x,y)$. Thus, we have

$$\theta_S(\bar{H}(k,\alpha k) \ltimes \bar{H}(n,\beta n)) \leq 2^{k+n} \frac{f_1(0)}{\hat{f}_1(0)} \frac{g_1(0)}{\hat{g}_1(0)}\,.$$

Optimizing over all f_1 and g_1 we get

$$\theta_S(\bar{H}(k,\alpha k) \ltimes \bar{H}(n,\beta n)) \le 2^k \frac{\theta_S(H(n,\beta n))}{\theta_S(H(k,\alpha k))}\,.$$

(This, of course, is exactly how the bound was obtained in Lemma 6.)

We were not able to find any choice of $g(x,y)$ in the dual problem (78) that beats the product $f(x)g(y)$. This seems to be the most natural direction for improvement. Another open problem is to find an upper bound on $\alpha(\bar{H}(k,\alpha k) \ltimes \bar{H}(n,\beta n))$ that does not follow from an upper bound on $\alpha(\bar{H}(k,\alpha k) \boxtimes \bar{H}(n,\beta n))$ or to prove that these are asymptotically equivalent.

5.4. On repetition & majority-vote

By looking at Fig. 1(a) we can see that relaxation of the minimum-distance property, cf. Def. 1, that we consider in this paper allows one to have non-zero rate even at "minimum distance" $\beta > 1/2$. However, in this case $\alpha \ge \beta$ (Theorem 3) and furthermore repetition map (1) is optimal (provided $n/k \in \mathbb{Z}$). This raises a number of questions:

- Can one show that any (α,β)-map in high-β regime is structured similarly to a repetition map?
- For the case when $n/k \notin \mathbb{Z}$ (e.g. $\rho = 3/2$), how do we asymptotically achieve $\alpha \approx \beta$?
- The corresponding situation with majority-vote maps is even worse, here we need $\frac{k}{n}$ be an odd integer. What is the counterpart for even $\frac{k}{n}$?
- Finally, how do we smoothly interpolate between the "non-smooth" separation construction (that is not even injective) and the repetition map?

In fact the last question was our main practical motivation for looking into the concept of (α,β)-maps. We do not have any good candidates at this point.

5.5. On linear codes

A natural approach to construct good (α, β) maps is to restrict to linear maps $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$. A linear f is (α, β) if

$$|x| > \alpha k \quad \Longrightarrow \quad |f(x)| > \beta n\,.$$

Instead of working with this condition, we get a more invariant notion by considering the graph of f that is just a linear subspace of $L \subset \mathbb{F}_2^{k+n}$. Different conditions can be stated on L that will ensure that L defines an (α, β)-map, or that it gives an independent set in $\bar{H}(k, \alpha k) \ltimes \bar{H}(n, \beta n)$, or even an independent set in $\bar{H}(k, \alpha k) \boxtimes H(n, \beta n)$.

We state these conditions for a general field $\mathbb{F}$ and also in a geometric language of [27]. The extension of the concept of an (α, β)-map, cf. Definition 1, and Hamming graphs $H_{\mathbb{F}}(n, d)$, cf. (3), to arbitrary field $\mathbb{F}$ is obvious.

Suppose that we have (not necessarily distinct) points

$$u_1, \ldots, u_k, v_1, \ldots v_n \in \mathbb{P}^{m-1}$$

where $\mathbb{P}^{m-1}$ is a projective space of dimension $m - 1$ over the field $\mathbb{F}$. For every codimension 1 hyperplane H define

$$Z_v(H) \triangleq \#\{j : v_j \in H\}, \quad Z_u(H) \triangleq \#\{i : u_i \in H\}\,.$$

By writing these two collections of points in homogeneous coordinates we get a $m \times (k + n)$ matrix over $\mathbb{F}$, whose row-span gives the linear subspace $L \subset \mathbb{F}^{k+n}$. We then have the following statements:

1. If points $\{u_i, v_j, i \in [k], j \in [n]\}$ are not contained in any (codimension 1) hyperplane $H \subset \mathbb{P}^{m-1}$ and satisfy

$$\forall H : Z_v(H) \geq (1 - \beta)n \implies k > Z_u(H) \geq (1 - \alpha)k$$

then

$$\alpha(\bar{H}_{\mathbb{F}}(k, \alpha k) \boxtimes H_{\mathbb{F}}(n, \beta n)) \geq |\mathbb{F}|^m\,. \tag{81}$$

2. If points $\{u_i, i \in [k]\}$ are not contained in any (codimension 1) hyperplane $H \subset \mathbb{P}^{m-1}$ and

$$\forall H : Z_v(H) \geq (1 - \beta)n \implies Z_u(H) \geq (1 - \alpha)k$$

then

$$\alpha(\bar{H}_{\mathbb{F}}(k, \alpha k) \ltimes \bar{H}_{\mathbb{F}}(n, \beta n)) \geq |\mathbb{F}|^m \tag{82}$$

(note that assumption implies $k \geq m$ here).

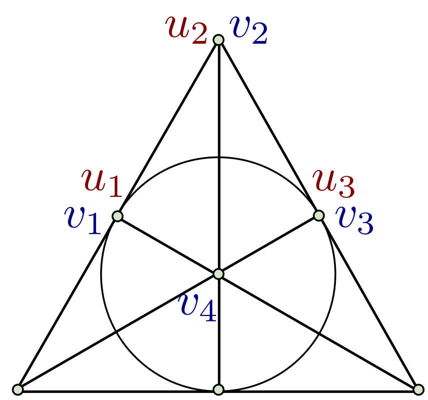


Figure 2: Construction of the optimal $(\frac{2}{3}, \frac{3}{4}; 3, 4)$-map by selecting seven points on the binary projective plane.

3. If in addition to previous assumption we also have $k = m$, i.e. points $\{u_i, i \in [k]\}$ span $\mathbb{P}^{k-1}$, then there exists a linear (α, β)-map and thus

$$\bar{H}_{\mathbb{F}}(k, \alpha k) \to \bar{H}_{\mathbb{F}}(n, \beta n)\,.$$

Note that if $\{u_i\}$ span $\mathbb{P}^{k-1}$ and $\alpha = 0$ then condition (82) simply states that one cannot include more than $(1-\beta)n$ points from $\{v_j, j \in [n]\}$ into any hyperplane – i.e. a standard geometric condition for $[n,k,d]_q$-systems, cf. [27]. Similarly to how $[n,k,d]_q$ systems exactly correspond to $[n,k,d]_q$ linear codes, existence of points $\{u_i, v_j\}$ satisfying (81) and assumptions in item 3 is *equivalent* to existence of an $\mathbb{F}$-linear $(\alpha, \beta; k, n)$-map.

As an example, consider $\mathbb{F} = \mathbb{F}_2$. We will construct a linear map $\mathbb{F}_2^3 \to \mathbb{F}_2^4$ by selecting seven points on the binary projective plane $\mathbb{P}_2^2$: u_1, u_2, u_3 are any points spanning $\mathbb{P}^2$,

$$v_1 = u_1, v_2 = u_2, v_3 = u_3$$

and finally put v_4 to be the only point not contained in any of the lines $(v_1, v_2), (v_1, v_3), (v_2, v_3)$. See Fig. 2 for an illustration. It is easy to see that condition (82) holds with $\alpha = \frac{2}{3}$ and $\beta = \frac{3}{4}$, thus

$$\bar{H}(3, 2) \to \bar{H}(4, 3)\,.$$

Computing (78) with smaller α and larger β shows that the code of Fig. 2 is optimal.

Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant No CCF-13-18620. Author is grateful to the support of Simons Institute for the Theory of Computing (UC Berkeley), at which this work was finished. Discussions with Prof. A. Mazumdar, A. Samorodnitsky and participants of the program on information theory at the Simons Institute were helpful.

[1] P. Indyk, R. Motwani, Approximate nearest neighbors: towards removing the curse of dimensionality, in: Proc. 30th ACM Symp. Theory Comp. (STOC), ACM, 1998, pp. 604–613.

[2] A. Andoni, P. Indyk, Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions, in: Proc. of 47th Ann. IEEE Symp. Found. Comp. Sci. (FOCS'2006), IEEE, 2006, pp. 459–468.

[3] Y. Kochman, A. Mazumdar, Y. Polyanskiy, The adversarial joint source-channel problem, in: Proc. 2012 IEEE Int. Symp. Inf. Theory (ISIT), Cambridge, MA, 2012.

[4] A. J. Young, Y. Polyanskiy, Converse and duality results for combinatorial source-channel coding in binary Hamming spaces, in: Proc. 2015 IEEE Int. Symp. Inf. Theory (ISIT), Hong Kong, China, 2015.

[5] D. Spielman, Linear-time encodable and decodable error-correcting codes, IEEE Trans. Inf. Theory 42 (6) (1996) 1723–1731.

[6] R. McEliece, E. Rodemich, H. Rumsey, L. Welch, New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities, IEEE Trans. Inf. Theory 23 (2) (1977) 157–166.

[7] B. Bollobás, Modern graph theory, Vol. 184, Springer Science & Business Media, 2013.

[8] M. A. Tsfasman, S. Vlădut, T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, Mathematische Nachrichten 109 (1) (1982) 21–28.

[9] A. Samorodnitsky, On the optimum of Delsarte's linear program, J. Comb. Th., Ser. A 96 (2001) 261–287.

[10] M. Navon, A. Samorodnitsky, On Delsarte's linear programming bounds for binary codes, in: Proc. 46th Annual IEEE Symp.Found. Comp. Sci. (FOCS), IEEE Computer Society, 2005, pp. 327–338.

[11] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1997.

[12] M. X. Goemans, Semidefinite programming in combinatorial optimization, Mathematical Programming 79 (1-3) (1997) 143–161.

[13] L. Lovász, On the Shannon capacity of a graph, IEEE Trans. Inf. Theory 25 (1) (1979) 1–7.

[14] R. Bačík, S. Mahajan, Semidefinite programming and its applications to NP problems, in: Computing and Combinatorics, Springer, 1995, pp. 566–575.

[15] M. O. Albertson, K. L. Collins, Homomorphisms of 3-chromatic graphs, Discr. Math. 54 (2) (1985) 127–132.

[16] U. Feige, L. Lovász, Two-prover one-round proof systems: Their power and their problems, in: Proc. 24th ACM Symp. Theory Comp. (STOC), ACM, 1992, pp. 733–744.

[17] D. E. Roberson, Variations on a theme: Graph homomorphisms, Ph.D. thesis, University of Waterloo (2013).

[18] D. E. Roberson, L. Mancinska, Graph homomorphisms for quantum players, arXiv preprint arXiv:1212.1724.

[19] T. Cubitt, L. Mancinska, D. Roberson, S. Severini, D. Stahlke, A. Winter, Bounds on entanglement assisted source-channel coding via the lovász ϑ number and its variants, IEEE Trans. Inf. Theory (11) (2014) 7330–7344.

[20] P. Delsarte, Application and generalization of the MacWilliams transform in coding theory, Proc. 15th Sympos. Inform. Theory in the Benelux 9 (1994) 44.

[21] D. J. Kleitman, On a combinatorial conjecture of Erdös, J. Comb. Theory 1 (2) (1966) 209–214.

[22] A. Samorodnitsky, Extremal properties of solutions for Delsarte's linear program, preprint.
URL `http://www.cs.huji.ac.il/~salex/papers/old_sq_measure.ps`

[23] A. Schrijver, A comparison of the Delsarte and Lovász bounds, IEEE Trans. Inf. Theory 25 (4) (1979) 425–429.

[24] I. Krasikov, S. Litsyn, Survey of binary Krawtchouk polynomials, DIMACS series: Codes and association schemes 56 (2001) 199–212.

[25] Y. Polyanskiy, Hypercontractivity of spherical averages in Hamming space, Arxiv preprint arXiv:1309.3014.

[26] V. Blinovsky, Bounds for codes in the case of list decoding of finite volume, Prob. Peredachi Inform. 22 (1) (1986) 7–19.

[27] M. A. Tsfasman, S. G. Vlădut, D. Nogin, Algebraic geometric codes: basic notions, Vol. 139, American Mathematical Soc., 1990.