Electronic Colloquium on Computational Complexity, Report No. 151 (2026)

Sparse polynomials and orthogonal representations of combinatorial graphs

Pavel Hrubeš*, Siddharth Iyer*

May 2026

Abstract

We give quantitative bounds on the sparsity of a real polynomial with non-negative coefficients vanishing on a slice of the Boolean cube $\{\pm 1\}^n$. We obtain similar bounds on the dimension of real orthogonal representations of (the complement of) Johnson-type graphs. The estimates are related to the classical problem about coloring of $\mathbb{R}^n$, as well as the existence of error-correcting codes. We also give a simple combinatorial application to k-fold Hadamard matrices.

1 Introduction

A classical problem about coloring of $\mathbb{R}^n$ asks what is the minimum number $\chi(\mathbb{R}_n)$ of colors needed to color $\mathbb{R}^n$ so that no two points of distance one share the same color. It is easy to see that $\chi(\mathbb{R}_n)$ is finite. Furthermore, Larman and Rogers have shown it can be bounded as $\chi(\mathbb{R}_n) \leq 2^{O(n)}$ [14]. An exponential lower bound $\chi(\mathbb{R}_n) \geq 2^{\Omega(n)}$ was proved by Frankl and Wilson in [5]. It is open to determine the function $\chi(\mathbb{R}_n)$ exactly. A similar problem has been investigated in the case of the sphere $S_r^{n-1} \subseteq \mathbb{R}^n$ of radius r. In this setting, Raigorodskii has shown that $\chi(S_r^{n-1})$ grows exponentially with n for any fixed $r > 1/2$ [21] (see also [20] and references within).

Both the lower bounds of Frankl-Wilson and Raigorodskii proceed by lower-bounding the chromatic number of a finite combinatorial graph embedded in $\mathbb{R}^n$ or S_r^{n-1}, respectively. In the case of [5], the graph is the Johnson graph $J(n, t, \ell)$ whose vertices are t-element subsets of n-element universe, and they are connected with an edge iff their intersection has size ℓ.

In this paper, we consider *orthogonal representations* of Johnson-type graphs. A (real) orthogonal representation of a graph G is a map ψ which assigns to every vertex v a non-zero vector $\psi(v) \in \mathbb{R}^m$ so that $\psi(v)$ and $\psi(v')$ are orthogonal whenever $v \neq v'$ are not adjacent in G. The smallest m for which such

*Institute of Mathematics of ASCR, Prague, Czech Republic. hrubes@math.cas.cz, iyer@math.cas.cz. This work was supported by Czech Science Foundation GAČR grant 25-16311S.

ISSN 1433-8092

a representation exists will be denoted $\dim_{\mathbb{R}}(G)$. This quantity is a natural generalization of the chromatic number in the sense that

$$\dim_{\mathbb{R}}(\overline{G}) \leq \chi(G)\,.$$

Orthogonal representations were introduced in the seminal paper of Lovász [16]. Representations of combinatorial Kneser-type graphs were studied by Haviv in [7]. We will prove exponential lower bounds on the dimension of real orthogonal representations of (the complement of) of Johnson-type graphs, such as $J(2n, n, \ell)$ with a suitable ℓ. A specific application to the coloring of $\mathbb{R}^n$ is the following: suppose that $\psi : \mathbb{R}^n \to \mathbb{R}^m \setminus \{0\}$ is a map such that for every $x, y \in \mathbb{R}^n$ of distance one, $\psi(x)$ and $\psi(y)$ are orthogonal. Then m grows exponentially with n.

The graphs we consider are graphs over the vertex set $\{\pm 1\}^n$ where two distinct x, y are connected if and and only if their Hadamard product, $x \circ y$, lies outside some prescribed set $S \subseteq \{\pm 1\}^n$. They can also be thought of as Cayley graphs over the group $\mathbb{Z}_2^n$. It turns out that one can obtain orthogonal representation for such graphs from polynomials $f(x)$ with real, non-negative coefficients that vanish when $x \in S$. The dimension of such a representation is precisely the number of non-zero coefficients in $f(x)$.

This leads us to the following question regarding the sparsity of polynomials with non-negative coefficients. Suppose $f \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]$ is a non-trivial polynomial with non-negative coefficients which vanishes on a prescribed subset $S \subseteq \{\pm 1\}^n$. How many non-zero coefficients must f contain? We give some generic bounds for this problem. In Theorem 1, we show that f must contain exponentially many non-zero coefficients in the specific case of S being a slice of the hypercube. The statement is reminiscent of the Hegedus lemma [8, 23]. It is also related to error-correcting codes (cf. Section 3.2). In Section 3.3, we will give combinatorial applications of Theorem 1 to generalized Hadamard matrices.

The above question is also related to problems in Fourier analysis of functions on the Boolean cube $\{\pm 1\}^n$ of an independent interest. A polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$ as above, can be regarded as a function $f : \{\pm 1\}^n \to \mathbb{R}$. Then, the coefficients of the polynomial are precisely the Fourier coefficients of the function. Our lower bound on the sparsity of f is, after a suitable normalization, a lower bound on the ℓ_1-norm of the Fourier spectrum of f given by $\sum_{S \subseteq [n]} |\hat{f}(S)|$. We note that estimates on the ℓ_p-norms on the Fourier spectra of f has been studied in [15, 25, 2, 11] with several applications, for example, in circuit lower bounds, in learning theory, and in the construction of pseudorandom generators.

2 Main results

Let $\{\pm 1\}^n_k$ denote the set of $x \in \{\pm 1\}^n$ with precisely k (-1)'s.

Theorem 1. *Let $f \in \mathbb{R}[x_1, \ldots, x_n]$ be a non-zero polynomial with non-negative real coefficients. Assume that $f(x) = 0$ for every $x \in \{\pm 1\}^n_k$ where $0 < k \le n/2$ is even. Then f has at least*

$$\Delta(n,k) := \frac{1}{2k} \cdot 2^{\frac{n}{2}\cdot\left(h(k/n)+h\left(1/2-\sqrt{(k/n)(1-k/n)}\right)-1\right)}$$

non-zero coefficients.

The bound $\Delta(n,k)$ is stated in terms of binary entropy function $h(\cdot)$, and is somewhat difficult to parse. We observe that

$$\Delta(n,k) \ \ge \ \Omega(n^{k/2}), \text{ if } k \text{ is fixed and } n \text{ goes to infinity,} \tag{1}$$

$$\Delta(n,k) \ \ge \ \frac{1}{2k} \cdot 2^{\frac{c \cdot k^2}{n}\cdot\left(\frac{1}{2}-\frac{k}{n}\right)^2}, \text{ if } 0 < k < n/2, \tag{2}$$

for an absolute constant $c > 0$.

An s-dimensional orthogonal representation of a graph $G = (V, E)$ over a field $\mathbb{F}$ is a map $\psi : V \to \mathbb{F}^s$ such that

(*i*). $\langle \psi(v), \psi(v) \rangle \neq 0$, for every $v \in V$,

(*ii*). $\langle \psi(v), \psi(v') \rangle = 0$, for every distinct non-adjacent v, v' in G.

The smallest s such that an orthogonal representation of G exists will be denoted $\dim_{\mathbb{F}}(G)$.

We turn to the applications for the aforementioned Johnson-type graphs. $J_{\pm 1}(n, \ell)$ is the graph with vertex-set $\{\pm 1\}^n$ such that distinct $x, y \in \{\pm 1\}^n$ are adjacent iff $\langle x, y \rangle = \ell$. This condition can be satisfied only if $\ell = n - 2k$ for some natural number k. Equivalently, x, y are adjacent in $J_{\pm 1}(n, n-2k)$ iff their Hamming distance is k - or their Euclidean distance is $2\sqrt{k}$. This makes $J_{\pm 1}(n, n-2k)$ a unit distance graph in $\mathbb{R}^n$.

For orthogonal representations of $J_{\pm 1}(n, \ell)$ we obtain the same bound as in Theorem 1:

Theorem 2. *Let $0 < k \le n/2$ be even. Then $\dim_{\mathbb{R}}(\overline{J_{\pm 1}(n, n-2k)})$ is at least $\Delta(n,k)$.*

An application of the estimate from Equation (2) is the following:

$$\dim_{\mathbb{R}}(\overline{J_{\pm 1}(n, \ell)})) \ge \frac{1}{n-\ell} \cdot 2^{\Omega\left(\frac{\ell^2}{n}\cdot\left(1-\frac{\ell}{n}\right)^2\right)}, \tag{3}$$
$$\text{if } 0 < \ell < n \text{ and } n \equiv \ell \bmod 4.$$

Let S^{n-1}_r be the sphere of radius r, $S^{n-1}_r := \{x \in \mathbb{R}^n : ||x||_2 = r\}$, and $S^{n-1} := S^{n-1}_1$.

Corollary 3. *(i). Let $0 < \delta < 1$ be fixed. Let $\psi : S^{n-1} \to \mathbb{R}^m \setminus \{0\}$ be a map such that for all $x, y \in S^{n-1}$, $\langle \psi(x), \psi(y) \rangle = 0$ whenever $\langle x, y \rangle = \delta$. Then $m = 2^{\Omega(n)}$.*

(ii). Let $r > \frac{1}{\sqrt{2}}$ be fixed. Let $\psi : S_r^{n-1} \to \mathbb{R}^m \setminus \{0\}$ be a map such that for all $x, y \in S_r^{n-1}$, $\langle \psi(x), \psi(y)\rangle = 0$ whenever $||x-y||_2 = 1$. Then $m = 2^{\Omega(n)}$.

That such maps exist with an exponential but finite m follows from the result of [14] on coloring of $\mathbb{R}^n$. The assumption $\delta > 0$ is necessary in part (i): if $\delta \leq 0$, we can take $\psi(x) = (x, \sqrt{|\delta|})$ which gives $m = n+1$. Similarly for the assumption $r > \frac{1}{\sqrt{2}}$ in part (ii). In contrast, Raigorodskii shows that $\chi(S_r^{n-1})$ is exponential whenever $r > 1/2$.

Another application is to standard Johnson graphs. Recall that $J(n,t,\ell)$ is the graph with vertices being t-element subsets of $[n]$ such that distinct A, B are adjacent iff $|A \cap B| = \ell$. Note that $J(n,t,\ell)$ is isomorphic to an induced subgraph of $J_{\pm 1}(n, n-4(t-\ell))$ as follows. Identify t-sets with ± 1 strings where the number of -1's is precisely t. Then, the Hamming distance between two strings is $2(t-\ell)$ iff the corresponding sets intersect in ℓ elements.

Corollary 4. *Let $0 < \delta_0 < \delta_1 < \frac{1}{2}$ be fixed. Then for all natural numbers n and ℓ with $\delta_0 n \leq \ell \leq \delta_1 n$, $\dim_{\mathbb{R}}(\overline{J(2n,n,\ell)}) \geq 2^{\Omega(n)}$.*

Organization. Theorem 1 will be proved in Section 3.1. Tightness of the bound will be discussed in Section 3.2. Section 3.3 gives combinatorial applications of Theorem 1. In Section 4, we prove Theorem 2 and Corollaries 4, 4.

Notation. $\{\pm 1\}^n_k$ is the set of $x \in \{\pm 1\}^n$ with precisely k (-1)'s. $\overline{1}^n$ is the vector $(1, \ldots, 1)$ of length n, $\overline{1}^n_k$ is the vector $(-1, \ldots, -1, 1, \ldots, 1)$ with k (-1)'s.

Given $x, y \in \mathbb{F}^n$, $\langle x, y\rangle$ denotes their inner product $\sum_i x_i y_i$. $x \circ y \in \{\pm 1\}^n$ is their Hadamard product $(x_1 y_1, \ldots, x_n y_n)$. We denote the set $\{1, \ldots, n\}$ by $[n]$.

3 Polynomials with non-negative coefficients

We will be interested in the sparsity of polynomials vanishing on a prescribed subset S of $\{\pm 1\}^n$.

Given a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ its *sparsity*, $\mathrm{spar}(f)$ is the number of non-zero coefficients of f. Since we care about the behaviour of f on the Boolean cube, our polynomials are without loss of generality multilinear, of the form $f = \sum_{A \subseteq [n]} c_A \prod_{i \in A} x_i$. The sparsity is then the size of the set $\{c_A : A \subseteq [n], c_A \neq 0\}$.

Given $S \subseteq \{0,1\}^n \setminus \{\overline{1}^n\}$, we define $\mathrm{spar}_{\mathbb{F}}(S)$ as the smallest s so that there exists an s-sparse polynomial f vanishing on S but with $f(\overline{1}^n) \neq 0$. If $\mathbb{F} = \mathbb{R}$, we define $\mathrm{spar}_+(S)$ analogously with the additional requirement that f has non-negative coefficients.

The following proposition illustrates the expressive power of polynomials with non-negative coefficients on $\{\pm 1\}^n$, and also underscores the special role of the point $\overline{1}^n$.

Proposition 5. *Let $g : \{\pm 1\}^n \to \mathbb{R}$. Then there exists a polynomial $f \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]$ such that $f(x) = g(x)$ for every $x \in \{\pm 1\}^n \setminus \{\overline{1}^n\}$.*

Proof. Let $\widehat{g}$ be the unique multilinear polynomial in $\mathbb{R}[x_1, \ldots, x_n]$ such that $\widehat{g}(x) = g(x)$ for every $x \in \{\pm 1\}^n$. Let

$$h(x) := \prod_{i=1}^{n} (1 + x_i)\,.$$

Observe that $h(x)$ vanishes on $\{\pm 1\}^n$ except for $x = \overline{1}^n$, and that all its coefficients are positive. Hence we can take $a > 0$ sufficiently large so that $ah + \widehat{g}$ has non-negative coefficients and agrees with g on $\{\pm 1\}^n \setminus \{\overline{1}^n\}$. $\square$

Note that it is not in general possible to achieve equality on all $\{\pm 1\}^n$: if g is non-zero and f has non-negative coefficients then f must be positive on $\overline{1}^n$.

Remark 6. *(i). The polynomial $\sum x_i - (n - 2k)$ vanishes on $\{\pm 1\}^n_k$ which shows that $\mathrm{spar}_{\mathbb{F}}(\{\pm 1\}^n_k) \leq n + 1$ if $k > 0$.*

(ii). Similarly, if $k \geq n/2$, the above polynomial has non-negative coefficients and hence $\mathrm{spar}_+(\{\pm 1\}^n_k) \leq n + 1$.

(iii). The polynomial $\prod_i x_i + 1$ vanishes on every x with an odd number of (-1)'s. Hence $\mathrm{spar}_+(\bigcup_{k\ odd} \{\pm 1\}^n_k) = 2$.

In particular, (i) and (iii) show that the assumptions $k \leq n/2$ and that k is even are necessary in Theorem 1.

In order to bound $\mathrm{spar}_+(S)$, we introduce the following linear programming relaxation of $\mathrm{spar}_+(S)$.

Given $S \subseteq \{\pm 1\}^n \setminus \{\overline{1}^n\}$, let $W(S)$ be the smallest w such that there exists $f \in \mathbb{R}_{\geq 0}[x_1, \ldots, x_n]$ such that

(i). $f(\overline{1}^n) = w$,

(ii). $f(x) = -1$, for every $x \in S$.

Observe that if a polynomial f has non-negative coefficients then $f(\overline{1}^n)$ is the ℓ_1-norm of the vector of its coefficients.

Lemma 7. *If $S \subseteq \{\pm 1\}^n \setminus \{\overline{1}^n\}$ then $W(S) + 1 \leq \mathrm{spar}_+(S)$.*

Proof. Let f be a non-zero polynomial with non-negative coefficients vanishing on S and sparsity s. We can write

$$f = \sum_{A \in \mathcal{A}} c_A \prod_{i \in A} x_i\,,$$

where $\mathcal{A} \subseteq [n]$ has size s and c_A are positive. Let B be some $A \in \mathcal{A}$ for which c_A is maximal. Let

$$f' = \sum_{A \in \mathcal{A}} c_B^{-1} c_A \prod_{i \in A \triangle B} x_i\,.$$

Then f' also vanishes on S. This is because, over $\{\pm 1\}^n$, we can write $f' = c_B^{-1}(\prod_{i\in B} x_i)f$. By the choice of B we have $f'(\overline{1}^n) \le s$. Finally, the constant term of f' equals one. Hence the polynomial $f'-1$ has non-negative coefficients, equals -1 on S, and its value on $\overline{1}^n$ is at most $s-1$. This shows $W(S) \le s-1$. $\square$

In the special case of $S = \{\pm 1\}^n_k$, we obtain the following characterisation of W. Let S_n^ℓ be the elementary symmetric polynomial of degree ℓ, namely

$$S_n^\ell = \sum_{A\subseteq[n],|A|=\ell}\prod_{i\in A} x_i\,.$$

Lemma 8. *The minimum in $W(\{\pm 1\}^n_k)$ is achieved by a scalar multiple of an elementary symmetric polynomial. In other words,*

$$W(\{\pm1\}^n_k) = \min_{\ell\in[n]:S_n^\ell(\overline{1}^n_k)<0} S_n^\ell(\overline{1}^n)|S_n^\ell(\overline{1}^n_k)|^{-1}\,.$$

Proof. Let f be a polynomial with non-negative coefficients such that $f(x) = -1$ for every $x \in \{\pm1\}^n_k$ and $f(\overline{1}^n) = w$ is minimal. We can assume that f is symmetric. Otherwise, we can take the polynomial

$$\frac{1}{n!}\sum_{\sigma\in SL_n}\sigma(f)\,,$$

where $\sigma(f) = f(x_{\sigma(1)},\ldots,x_{\sigma(n)})$. Consequently we can write $f = \sum_\ell c_\ell S_n^\ell$ with c_ℓ non-negative. Since $f(\overline{1}^n)$ is minimal, the terms with $S_n^\ell(\overline{1}^n_k) > 0$ must be zero and

$$f = \sum_{\ell:S_n^\ell(\overline{1}^n_k)<0} c_\ell S_n^\ell\,.$$

Since $f(\overline{1}^n_k) = -1$, f is a convex linear combination of the polynomials $S_n^\ell(x)|S_n^\ell(\overline{1}^n_k)|^{-1}$ with $S_n^\ell(\overline{1}^n_k) < 0$. Hence $f(\overline{1}^n)$ equals $S_n^\ell(\overline{1}^n)|S_n^\ell(\overline{1}^n_k)|^{-1}$ for some ℓ. $\square$

3.1 A lower bound on W from Krawchouk polynomials

In order to estimate the minumum in Lemma 8, we will apply known bounds on *Krawchouk polynomials.* For $n \in \mathbb{N}$ and $j \in \{0, 1, \ldots, n\}$, the Krawchouk polynomial is the univariate polynomial

$$\mathcal{K}_j(x) := \sum_{r=0}^{j}(-1)^r\cdot\binom{x}{r}\cdot\binom{n-x}{j-r}\,, \tag{4}$$

where $\binom{x}{r} := \frac{x(x-1)\cdots(x-r+1)}{r!}$. The polynomials were introduced in [13]. For us, it is important that Krawchouk polynomials capture the value of the elementary symmetric polynomial on a given slice of the hypercube:

$$S_n^\ell(\overline{1}^n_k) = \sum_{r=0}^{\ell}(-1)^r\cdot\binom{k}{r}\cdot\binom{n-k}{\ell-r} = \mathcal{K}_\ell(k)\,. \tag{5}$$

We collect some useful facts regarding Krawchouk polynomials [18, 24, 19].

Fact 9. *(i). [18] $\mathcal{K}_j$ has degree j. It has j simple real roots that lie in the interval $[n/2 - \sqrt{j \cdot (n-j)}, n/2 + \sqrt{j \cdot (n-j)}]$.*

(ii). $\mathcal{K}_j(\ell)/\binom{n}{j} = \mathcal{K}_\ell(j)/\binom{n}{\ell}$.

(iii). [19] For $x \in [n/2 - \sqrt{j \cdot (n-j)}, n/2 + \sqrt{j \cdot (n-j)}]$,

$$|\mathcal{K}_j(x)| \leq 2^{\frac{n}{2} \cdot (h(j/n) + 1 - h(x/n)))}.$$

(iv). If $j = \delta n$, the first root of $\mathcal{K}_j$ is located roughly at $n(\frac{1}{2} - \sqrt{\delta(1-\delta)})$. More precisely, for any $\epsilon > 0$ and n sufficiently large, the smallest root of $K_{\delta n}$ is at most $n(1/2 - \sqrt{\delta(1-\delta)} + \epsilon)$ (see Appendix A, proof of Equation A.20 in [18]).

(v). If z_i is the i-th root of $K_j(x)$ then the interval $[z_i, z_{i+1}]$ contains an integer (see [24] Theorem 3.41.2).

We will also use the following estimate on binomial coefficients: it holds that

$$\sqrt{\frac{n}{8k(n-k)}} \cdot 2^{nh(k/n)} \leq \binom{n}{k}, \text{for all } k \in [n-1]. \tag{6}$$

Lemma 10. *If $0 < k \leq n/2$ is even then*

$$W(\{\pm 1\}^n_k) \geq \frac{1}{2k} \cdot 2^{\frac{n}{2} \cdot \left(h(k/n) - 1 + h\left(1/2 - \sqrt{(k/n)(1-k/n)}\right)\right)}.$$

Proof. By Lemma 8, we have

$$W(\{\pm 1\}^n_k) = \min_{\ell \in [n]: S^\ell_n(\bar{1}^n_k) < 0} S^\ell_n(\bar{1}^n) |S^\ell_n(\bar{1}^n_k)|^{-1} = \min_{\ell \in [n]: S^\ell_n(\bar{1}^n_k) < 0} \binom{n}{\ell} |S^\ell_n(\bar{1}^n_k)|^{-1}.$$

Using Equation (5) and Fact 9 part (ii), we obtain

$$\begin{aligned} W(\{\pm 1\}^n_k) &= \min_{\ell \in [n]: \mathcal{K}_\ell(k) < 0} \binom{n}{\ell} \cdot |\mathcal{K}_\ell(k)|^{-1} \\ &= \min_{\ell \in [n]: \mathcal{K}_k(\ell) < 0} \binom{n}{k} |\mathcal{K}_k(\ell)|^{-1} \\ &= \binom{n}{k} \cdot \min_{\ell \in [n]: \mathcal{K}_k(\ell) < 0} |\mathcal{K}_k(\ell)|^{-1}. \end{aligned}$$

By Fact 9 part (i), $\mathcal{K}_k(x)$ has k simple roots that lie in the interval $I = [n/2 - \sqrt{k(n-k)}, n/2 + \sqrt{k(n-k)}]$. Since k is even, it is easy to see that $\mathcal{K}_k(0), \mathcal{K}_k(n) > 0$ and so $\mathcal{K}_k(x) \geq 0$ for every $x \notin I$. For any $x \in I$, we can use the bound (iii)

$$|\mathcal{K}_k(x)| \leq 2^{\frac{n}{2} \cdot (h(k/n) + 1 - h(x/n)))}.$$

If $k \leq n/2$, the inequality (6) gives $\binom{n}{k} \geq 2^{n \cdot h(k/n)}/2k$. Consequently,

$$\begin{aligned} W(\{\pm 1\}^n_k) &\geq \frac{2^{n \cdot h(k/n)}}{2k} \cdot \min_{x \in I} 2^{-\frac{n}{2} \cdot (h(k/n)+1-h(x/n)))} \\ &= \frac{2^{\frac{n}{2} \cdot (h(k/n)-1)}}{2k} \cdot \min_{x \in I} 2^{\frac{n}{2} \cdot h(x/n))} \\ &\geq \frac{1}{2k} \cdot 2^{\frac{n}{2} \cdot \left(h(k/n)-1+h\left(1/2-\sqrt{(k/n)(1-k/n)}\right)\right)}, \end{aligned}$$

where the last inequality follows by observing that the binary entropy function $h(x)$ is symmetric around $x = 1/2$ and increasing on $(0, 1/2)$. □

Proof of Theorem 1. The theorem follows from Lemmas 7 and 10. □

Proof of the estimate (1). We can write

$$\Delta(n,k) = \frac{1}{2k} \cdot 2^{\frac{n}{2} h(k/n))} \cdot 2^{\frac{n}{2} \cdot \left(h\left(1/2-\sqrt{(k/n)(1-k/n)}\right)-1\right)}.$$

Recall that the binary entropy function satisfies the inequality $h(p) \geq 4p(1-p)$, for $p \in (0,1)$. If $p = 1/2 - \gamma$, we then have $h(1/2-\gamma) \geq 1 - 4\gamma^2$. Hence

$$h\left(1/2 - \sqrt{(k/n)(1-k/n)}\right) - 1 \geq -(4k/n)\,(1-k/n) \geq -4\frac{k}{n}.$$

Since $2^{nh(k/n)} \geq \binom{n}{k}$, we obtain

$$\Delta(n,k) \geq \frac{1}{2k} \cdot 2^{\frac{n}{2} h(k/n)} 2^{\frac{n}{2} \cdot \frac{-4k}{n}} \geq \frac{1}{2k} \cdot \sqrt{\binom{n}{k}} \cdot 2^{-2k} = \Omega(n^{k/2}).$$

for k fixed. □

Proof of the estimate (2). Let $z := 1/2 - k/n$. Then, $z \in [0, 1/2]$ and

$$\begin{aligned} h\left(\frac{k}{n}\right) + h\left(\frac{1}{2} - \sqrt{\frac{k}{n} \cdot \left(1 - \frac{k}{n}\right)}\right) - 1 &= h\left(\frac{1}{2} - z\right) + h\left(\frac{1}{2} - \sqrt{\frac{1}{4} - z^2}\right) - 1 \\ &= c \cdot (z^2(1-4z^2), \end{aligned}$$

for some absolute constant $c > 0$, by Claim 24. Hence

$$\Delta(n,k) \geq \frac{1}{2k} \cdot 2^{\frac{cn}{2} \cdot \left(\frac{1}{2} - \frac{k}{n}\right)^2 \left(\frac{k}{n}\right)^2} \geq \frac{1}{2k} \cdot 2^{\frac{c' \cdot k^2}{n} \cdot \left(\frac{1}{2} - \frac{k}{n}\right)^2}.$$

The proof of Claim 24 is delegated to the Appendix. □

3.2 Some upper bounds

Linear spaces over $\mathbb{F}_2$ and error-correcting codes. Recall that $C \subseteq \mathbb{F}_2^n$ is an $[n, t, d]$ binary linear code if C is a t-dimensional subspace and every non-zero element in C has Hamming weight at least d. Let $\{\pm 1\}^n_{\leq k} := \bigcup_{0<\ell\leq k} \{\pm 1\}^n_\ell$.

Lemma 11. *If there exists an $[n, t, d]$ binary linear code C, then* $\mathrm{spar}_+(\{\pm 1\}^n_{\leq d-1}) \leq 2^{n-t}$.

Proof. Let $w^1, \ldots, w^{n-t}$ be $n - t$ linearly independent vectors in the dual code $C^\perp := \{w : \langle w, z\rangle = 0, \forall z \in C\}$. Such vectors exist since the dimension of $C^\perp$ is $n - \dim(C) = n - t$. Since C has distance d, no non-zero $z \in \mathbb{F}_2^n$ with Hamming weight at most $d - 1$ is contained in C, and consequently, there exists w^i such that $\langle w^i, z\rangle = 1$. Consider the real polynomial

$$f(x) = \prod_{i=1}^{n-t} \left(1 + \prod_{j:w^i_j=1} x_j\right).$$

We can identify any $x \in \{\pm 1\}^n$ with $x^* \in \mathbb{F}_2^n$ by setting $x^*_i = 1$ iff $x_i = -1$. The number of 1s in x^* is precisely the number of -1s in x. Hence, if $x \in \{\pm 1\}^n_{\leq d-1}$ then $\langle w^i, x^*\rangle = 1$ for some w^i, and we have $\prod_{j:w^i_j=1} x_j = (-1)^{\langle w_i, x^*\rangle} = -1$, and $f(x) = 0$. The bound on the sparsity follows from the dimension of $C^\perp$. □

Remark 12. *Lemma 11 can be stated for an arbitrary set $S \subseteq \{\pm 1\}^n \setminus \{\bar{1}^n\}$. An identical proof shows that if there exists a subspace $C \subseteq \mathbb{F}_2^n$ of dimension t which is disjoint from $S^* := \{x^* : x \in S\}$, then* $\mathrm{spar}_+(S) \leq 2^{n-t}$. *This can be used to show that* $\mathrm{spar}_+(S) \leq O(|S|)$.

The following matches the estimate (1) from Theorem 1.

Proposition 13. $\mathrm{spar}_+(\{\pm 1\}^n_{2k}) \leq \mathrm{spar}_+(\{\pm 1\}^n_{\leq 2k}) \leq O(n^k)$.

Proof. Bose–Chaudhuri–Hocquenghem [9, 1] code is a binary linear code with parameters $[2^m - 1, 2^m - km - 1, 2k + 1]$. Applying Lemma 11 to BCH codes we obtain $\mathrm{spar}_+(\{\pm 1\}^n_{\leq 2k}) \leq 2^{km} = O(n^k)$ since $n = 2^m - 1$ for this choice of parameters. □

An LP relaxation similar to our W was applied to codes in [4]. Krawchouk polynomials were used in this context by McEliece et. al. in [18], by Rao and Sprumont in [22], and Krasikov and Litsyn in [12].

A construction from Krawchouk polynomials. We construct non-negative polynomials of a particular sparsity that vanishes on certain slices of the cube using estimates on the roots of Krawchouk polynomials.

Proposition 14. *Given $\gamma \in (0, 1/2)$ and $k = n(\frac{1}{2} - \gamma)$ with n sufficiently large,*

$$\mathrm{spar}_+(\{\pm 1\}^n_k) \leq 2^{n(h(2\gamma^2)+o(1))}.$$

Proof. From Remark 6 (*iii*), it suffices to prove the statement for k even. We minimize ℓ so that the elementary symmetric polynomial S_n^ℓ is non-positive on $\{\pm1\}_k^n$. Then the polynomial $S_n^\ell(x) + |S_n^\ell(\overline{1}_k^n)|$ has non-negative coefficients, vanishes on $\{\pm1\}_k^n$ and its sparsity is at most $\binom{n}{\ell} + 1 \le 2^{n(h(\ell/n)+o(1))}$.

Indeed, when $x \in \{\pm1\}_k^n$, by Equation (5) we have $S_n^\ell(x) = S_n^\ell(\overline{1}_k^n) = \mathcal{K}_\ell(k)$. It suffices to minimize ℓ so that $\mathcal{K}_\ell(k) \le 0$. By Fact 9 (*ii*) the sign of $\mathcal{K}_\ell(k)$ is the same as the sign of $\mathcal{K}_k(\ell)$. By Fact 9 (*i*), we know that $\mathcal{K}_k(x)$ has k real, simple roots $z_1 < \ldots < z_k$. For even k, it is easy to check from Equation (4) that the leading coefficient of $\mathcal{K}_k(x)$ is positive, which implies that $\mathcal{K}_k(x)$ is non-negative in $(-\infty, z_1]$ and non-positive in $[z_1, z_2]$. Item (*iv*) gives that for any $\epsilon > 0$ and n large enough, $0 \le z_1 \le n/2 - \sqrt{k \cdot (n-k)} + \epsilon n/2$. Moreover, from Item (*v*) there exists an integer in $[z_1, z_2]$, and hence $\mathcal{K}_k(\lceil z_1 \rceil) \le 0$. Substituting $k = n(\frac{1}{2} - \gamma)$, we see that $\ell \le \lceil z_1 \rceil \le n(1 - \sqrt{1-4\gamma^2})/2 + \epsilon n + 1 \le 2n\gamma^2 + \epsilon n + 1$. The statement follows since ϵ can be arbitrarily small. □

Remark 15. *Since* $h(p) \le -2p\log(p)$ *for* $p \in (0, 1/2]$*, the bound from Proposition 14 gives* $\mathrm{spar}_+(\{\pm1\}^n_{n(\frac{1}{2}-\gamma)}) \le 2^{O(n\gamma^2 \log(1/\gamma))}$*. On the other hand, for* γ *bounded away from one, the estimate (2) from Theorem 1 gives* $\mathrm{spar}_+(\{\pm1\}^n_{n(\frac{1}{2}-\gamma)}) \ge 2^{\Omega(n\gamma^2)}$*. The two estimates match up to the* $\log(1/\gamma)$ *term in the exponent.*

3.3 Combinatorial applications

Theorem 16. *Let* $k \ge 2$ *be a fixed even integer. Let* $\mathcal{A} \subseteq 2^{[n]}$ *be a non-empty set of subsets of* $[n]$ *such that every* k*-element subset of* $[n]$ *has odd intersection with precisely half of the elements of* $\mathcal{A}$*. Then* $|\mathcal{A}| \ge \Omega(n^{k/2})$*.*

Proof. Let f be the polynomial

$$f := \sum_{A \in \mathcal{A}} \prod_{i \in A} x_i \,.$$

Then f vanishes on $\{\pm1\}_k^n$ and apply Theorem 1 with the estimate (1). □

For vectors $v^1, \ldots, v^k \in \mathbb{R}^n$ their *generalised inner product* equals

$$\sum_{i \in [n]} (v_i^1 \cdots v_i^k) \,.$$

An $n \times m$ matrix $M \in \{\pm1\}^{n \times m}$ will be called a *k-fold Hadamard matrix* if every set of k rows of M has generalised inner product equal to zero.

Theorem 17. *Let* $k \ge 2$ *be a fixed even integer. Then every* k*-fold Hadamard matrix with* n *rows has at least* $\Omega(n^{k/2})$ *columns.*

Proof. Given a j-th column of M, let $A_j \subseteq [n]$ be the set $\{i \in [n] : M_{i,j} = -1\}$. Then $\mathcal{A} = \{A_j : j \in [m]\}$ satisfies the assumption of the previous theorem: for any $S \subseteq [n]$ of size k,

$$\sum_j (-1)^{|A_j \cap S|} = \sum_j \prod_{i \in S} (-1)^{|A_j \cap \{i\}|} = \sum_j \prod_{i \in S} M_{i,j} = 0,$$

as M is a k-fold Hadamard matrix. Hence $m \geq \Omega(n^{k/2})$. $\square$

4 Orthogonal representations

We now focus on orthogonal representations of Johnson-type graphs and prove Theorem 2.

Given $S \subseteq \{\pm 1\}^n \setminus \{\overline{1}^n\}$, define the graph G_S as follows. The vertex set of G_S is $\{\pm 1\}^n$. Vertices $x, y \in \{\pm 1\}^n$ are adjacent in G_S iff $x \circ y \in S$, where $\circ$ is the Hadamard product. We note that G_S is a Cayley graph over the group $\{\pm 1\}^n$ with Hadamard product as the group operation (a.k.a. the group $\mathbb{Z}_2^n$) and generator set S.

We will show that

$$W(S) + 1 \leq \dim_{\mathbb{R}}(\overline{G_S}) \leq \operatorname{spar}_+(S)\,, \tag{7}$$

which allows to apply results from previous sections to $\dim_{\mathbb{R}}(\overline{G_S})$.

Remark 18. *G_S (and more generally, any Cayley graph) is vertex-transitive. If $S = \{\pm 1\}^n_k$, it is also edge-transitive. If t is as in Remark 12, the chromatic number can be bounded as $\chi(\overline{G_S}) \leq 2^{n-t}$.*

We first establish the easier inequality in Equation (7).

Proposition 19. $\dim_{\mathbb{C}}(\overline{G_S}) \leq \operatorname{spar}_{\mathbb{C}}(S)$ *and* $\dim_{\mathbb{R}}(\overline{G_S}) \leq \operatorname{spar}_+(S)$.

Proof. Let $f = \sum_{A \in \mathcal{A}} c_A \prod_{i \in A} x_i$ be a polynomial vanishing on S with sparsity $s = |\mathcal{A}|$ and $f(\overline{1}^n) \neq 0$. Given $x \in \{\pm 1\}^n$, let $\psi(x) \in \mathbb{C}^s$ be the vector whose coordinates are indexed by elements of $\mathcal{A}$ and

$$\psi(x)_A = c_A^{1/2} \prod_{i \in A} x_i\,.$$

The definition guarantees

$$\langle \psi(x), \psi(y) \rangle = \sum_{A \in \mathcal{A}} \left(c_A^{1/2} \prod_{i \in A} x_i \right) \left(c_A^{1/2} \prod_{i \in A} y_i \right) = f(x \circ y)\,.$$

By assumption, $f(x \circ y) = 0$ whenever $x \circ y \in S$ and $f(x \circ x) = f(\overline{1}^n) \neq 0$. Hence ψ is an orthogonal representation of $\overline{G_S}$ over $\mathbb{C}$. If f has non-negative coefficients, we obtain an orthogonal representation over $\mathbb{R}$. $\square$

The second inequality in (7) is proved by relating $\operatorname{spar}_+(S)$ to Lovász Θ-function [16]. We use the following definition[1] of $\Theta(G)$: $\Theta(G)$ is the minimum θ such that there exists a PSD matrix $M \in \mathbb{R}^{V \times V}$ with

(i). $M_{v,v} = \theta - 1$,

[1] It is equivalent to the standard one by Theorem 3 of [16], see also [6].

(ii). $M_{v,v'} = -1$, for distinct v, v' not adjacent in G.

Recall [16, 17]

$$\omega(\overline{G}) \leq \Theta(G) \leq \dim_{\mathbb{R}}(G) \leq \chi(\overline{G})\,, \tag{8}$$

where ω is the size of a largest clique in a graph and χ is the chromatic number.

Let $f \in \mathbb{R}[x_1, \ldots, x_n]$. Define the $2^n \times 2^n$ matrix $M(f)$ as follows. Rows and columns are indexed by $\{\pm 1\}^n$ (in an arbitrary but fixed order) and $M(f)_{y,z} = f(y \circ z)$.

Lemma 20. *$M(f)$ is a PSD matrix iff f has non-negative coefficients.*

Proof. For a single monomial $\prod_{i \in A} x_i$, we have

$$M(\prod_{i \in A} x_i) = v(A)v(A)^t\,,$$

where $v(A) \in \mathbb{R}^{2^n}$ is a column vector with entries indexed by $y \in \{\pm 1\}^n$ with $v(A)_y = \prod_{i \in A} y_i$. If $f = \sum_A c_A \prod_{i \in A} x_i$, we then have

$$M(f) = \sum_A c_A v(A)v(A)^t\,.$$

Since $v(A)v(A)^t$ is PSD, so is $M(f)$ provided all the coefficients are non-negative. Conversely, assume that some c_A is negative. Observe that for every $B \neq A$, $v(A)^t v(B) = 0$. This means

$$v(A)^t M(f) v(A) = c_A (v(A)^t v(A))^2 < 0$$

and $M(f)$ is not a PSD matrix. □

Remark 21. *It also holds that rk$(M(f)) = \mathrm{spar}(f)$, for a multilinear f.*

Lemma 22. $W(S) + 1 = \Theta(\overline{G_S})$.

Proof. The inequality $\Theta(\overline{G_S}) \leq W(S) + 1$ follows from Lemma 20: if f is a polynomial with non-negative coefficients satisfying (i), (ii) from the definition of W then $M(f)$ is a PSD matrix satisfying (i), (ii) from the definition of Θ with $\theta - 1 = w$.

To prove the opposite inequality, let M be a $2^n \times 2^n$ matrix indexed with elements of $\{\pm 1\}^n$ such that $M_{x,x} = \theta - 1$ and $M_{x,y} = -1$ if $x \circ y \in S$. For $z \in \{\pm 1\}^n$, let M^z be the matrix with $M^z_{x,y} = M_{z \circ x, z \circ y}$. It is obtained by applying the same permutation to rows and columns of M and hence it is a PSD matrix. Let

$$N := 2^{-n} \sum_{z \in \{\pm 1\}^n} M^z\,.$$

Then $N_{x,x} = \theta - 1$, $N_{x,y} = -1$ if $x \circ y \in S$ and moreover $N^z = N$ for every z.

We claim there exists $f : \{\pm 1\}^n \to \mathbb{R}$ such that for every x, y, $N_{x,y} = f(x \circ y)$. To see that, define an equivalence relation $\sim$ on $\{\pm 1\}^n \times \{\pm 1\}^n$ by

$$(x, y) \sim (x', y') \text{ iff there exists } z \in \{\pm 1\}^n\,,\ (x', y') = (z \circ x, z \circ y)\,.$$

Since $N^z = N$ for every z, the value of $N_{x,y}$ is determined by the $\sim$ equivalence class of (x, y). Moreover, one can see that

$$(x, y) \sim (x', y') \text{ iff } x \circ y = x' \circ y' .$$

This means that indeed $N_{x,y}$ can be written as $f(x \circ y)$.

Finally, we can write f as a multilinear polynomial and since N is PSD, f has non-negative coefficients. By the properties of N, $f(\overline{1}^n) = \theta - 1$ and $f(x) = -1$ for every $x \in S$. Hence $W(S) \leq \Theta(\overline{G_S}) - 1$. □

Remark 23. *Lemma 22 can be extended to undirected graphs on an arbitrary finite Abelian group H by replacing Fourier analysis over $\mathbb{Z}_2^n$ with Fourier analysis over H.*

Given H and $S \subseteq H$ that is symmetric ($S = -S$), the Cayley graph $G = Cay(H, S)$ over H generated by S is undirected. A similar proof as in Lemma 22 shows that

$$\Theta(\overline{G}) \geq \inf_{f:H\to\mathbb{R}} \{f(0)-1 : \forall x \in S, f(x) = -1 \textit{ and } \langle f, \chi\rangle \geq 0, \forall \textit{ characters } \chi : H \to \mathbb{C}\}.$$

This in turn gives a lower bound on $\dim_{\mathbb{R}}(\overline{G})$. A similar formulation of the Θ-function was derived in [3].

Proof of Theorem 2. In the notation of this section, we have

$$J_{\pm1}(n, n - 2k) = G_S \text{ with } S = \{\pm1\}^n_k .$$

The previous lemma then gives $\Theta(\overline{J_{\pm1}(n, n - 2k)}) = W(\{\pm1\}^n_k)+1$ and, by (8),

$$\dim_{\mathbb{R}}(\overline{J_{\pm1}(n, n - 2k)}) \geq W(\{\pm1\}^n_k) .$$

The bound then follows from Lemma 10. □

Proof of Corollary 3. It is sufficient to prove part (i), part (ii) easily follows.

Let ℓ be the largest integer such that $\ell \leq \delta(n - 1)$ and $\ell = n \mod 4$. Since $\ell \leq \delta(n - 1)$, there exist $\alpha, \beta \in \mathbb{R}$ with

$$\alpha^2(n - 1) + \beta^2 = 1 , \ \alpha^2\ell + \beta^2 = \delta .$$

Given $x \in \{\pm1\}^{n-1}$, let $x' \in \mathbb{R}^n$ be the vector $(\alpha x, \beta)$. The choice of α, β guarantees that $x' \in S^{n-1}$ and $\langle x', y'\rangle = \delta$ iff $\langle x, y\rangle = \ell$. Hence the map ψ gives an orthogonal representation of $\overline{J_{\pm1}(n - 1, \ell)}$. If $0 < \delta < 1$, we can apply Theorem 2 and the estimate (3) to conclude that $m \geq 2^{\Omega(n)}$. □

Proof of Corollary 4. Recall from the discussion in Section 2 that $J(n, t, \ell)$ is isomorphic to an induced subgraph of $J_{\pm1}(n, n - 4(t - \ell))$ by restricting to only those strings where the number of -1's is exactly t. We refer to this induced subgraph by $J_{\pm1}(n, t, n - 4(t - \ell))$.

We claim that for every n and ℓ

$$\dim_{\mathbb{R}}(\overline{J_{\pm1}(n, \ell)}) \leq \dim_{\mathbb{R}}(\overline{J_{\pm1}(2n, n, 2\ell)}) . \tag{9}$$

Indeed, let $\psi : \{\pm 1\}^{2n} \to \mathbb{R}$ be an orthogonal representation of $\overline{J_{\pm 1}(2n, n, 2\ell)}$. Given $x \in \{\pm 1\}^n$ let $\psi'(x) := \psi(x, -x)$. Then ψ' is an orthogonal representation of $\overline{J_{\pm 1}(n, \ell)}$): if $x, y \in \{\pm 1\}^n$ satisfy $\langle x, y\rangle = \ell$ then $\langle (x, -x), (y, -y)\rangle = 2\ell$. This means that $\langle \psi(x, -x), \psi(y, -y)\rangle = 0$ and hence $\langle \psi'(x), \psi'(y)\rangle = 0$, proving (9).

The rest is an application of Theorem 2 and the estimate (2).

$\square$

Quantitatively, the reduction (9) is quite lossy and applies to a limited scope of parameters. Observing that $\dim_{\mathbb{R}}(\overline{J_{\pm 1}(n, \ell)}) \leq \sum_{t=0}^{n} \dim_{\mathbb{R}}(\overline{J_{\pm 1}(n, t, \ell)})$ shows

$$\dim_{\mathbb{R}}(\overline{J_{\pm 1}(n, t, \ell)}) \geq \frac{\dim_{\mathbb{R}}(\overline{J_{\pm 1}(n, \ell)})}{n} \text{ for some } t.$$

This can give better estimates for a wider range of parameters. The caveat is that we are not given t explicitly.

5 Open problems

We end the play with some open problems.

Problem 1. *Show that* $\dim_{\mathbb{R}}(\overline{J(n, 3, 1)}) \geq \Omega(n^2)$.

Problem 2. *Let S be the union of $\{\pm 1\}^n_k$ over all $0 < k \leq n$ divisible by 4. Determine* $\dim_{\mathbb{C}}(\overline{G_S})$ *or* $\dim_{\mathbb{R}}(\overline{G_S})$.

Problem 3. *Given $\delta \in [0, 1)$, let c_δ be the infimum c such that there exists a map is in Corollary 3 part (i) with $m \leq O(2^{cn})$. Then $c_0 = 0$ and the Corollary shows that $c_\delta > 0$ if $\delta > 0$. Is it the case that* $\lim_{\delta \to 0_+} c_\delta = 0$*?*

Some comments are in order. In Problem 1, the trivial bounds are

$$\Omega(n) \leq \dim_{\mathbb{R}}(\overline{J(n, 3, 1)}) \leq O(n^2)\,.$$

Over complex numbers, one has $\dim_{\mathbb{C}}(\overline{J(n, 3, 1)}) \leq n+1$. In contrast, $\dim_{\mathbb{F}}(\overline{J(n, 3, 1)}) \geq \Omega(n^2)$ over a field of characteristic two. In Problem 2, one has the bound $\dim_{\mathbb{F}}(\overline{G_S}) \geq \Omega(2^{n/2})$ over any field. This follows from the observation that G_S contains a clique of size[2] $\Omega(2^{n/2})$. Over complex numbers, an upper bound $\dim_{\mathbb{C}}(\overline{G_S}) \leq O(2^{cn})$ with some constant $c < 1$ can be proved as in [10]. The correct value of the constant is unknown. Over $\mathbb{R}$, no such non-trivial upper bound is known.

Acknowledgement. We thank Yuval Filmus and Ishay Haviv for useful comments.

[2]If n is even, the clique consists of all vectors of the form (x, x) where $x \in \{\pm 1\}^{n/2}$ has an even number of (-1)'s.

References

[1] R.C. Bose and D.K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 1960.

[2] E. Chattopadhyay, P. Hatami, K. Hosseini, and S. Lovett. Pseudorandom generators from polarizing random walks. *Theory of Computing*, 2019.

[3] E. DeCorte, de Laat D., and Vallentin F. Fourier analysis on finite groups and the lovász θ-number of cayley graphs. *Experimental Mathematics*, 2014.

[4] P. Delsarte. *An Algebraic Approach to the Association Schemes of Coding Theory*. Philips Research Reports Supplements. Philips Research Laboratories, 1973.

[5] P. Frankl and R.M. Wilson. Intersetcion theorems with geometric consequences. *Combinatorica*, 1:357–368, 1981.

[6] M. Goemans. Semidefinite programming in combinatorial optimization. *Mathematical Programming*, 79:143–161, 1997.

[7] I. Haviv. Topological bounds on the dimension of orthogonal representations of graphs. *European Journal of Combinatorics*, 81:84–97, 2019.

[8] G. Hegedüs. Balancing sets of vectors. *Studia Scientiarum Mathematicarum Hungarica*, 47(3):333–349, 2009.

[9] A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffres*, 1959.

[10] P. Hrubeš. A subquadratic upper bound on sum-of-squares composition formulas. *Computational Complexity Conference, CCC*, 2024.

[11] S. Iyer, A. Rao, V. Reis, T. Rothvoss, and A. Yehudayoff. Tight bounds on the fourier growth of bounded functions on the hypercube. *CoRR*, abs/2107.06309, 2021.

[12] I. Krasikov and S. Litsyn. On the accuracy of the binomial approximation to the distance distribution of codes. *IEEE Trans. Inform. Theory*, 41(5):1472–1474, 1995.

[13] M. Krawtchouk. Sur une généralisation des polynômes d'Hermite. *C. R. Acad. Sci., Paris*, 189:620–622, 1929.

[14] D.G. Larman and C. A. Rogers. The realization of distances within sets in euclidean space. *Mathematika*, 19:1–24, 1972.

[15] N. Linial, Y. Mansour, and N. Nisan. Constant depth circuits, fourier transform, and learnability. *J. ACM*, 1993.

[16] L. Lovász. On the Shannon capacity of a graph. *IEEE Trans. Inform. Theory*, 25(1):1–7, 1979.

[17] L. Lovász. Orthogonal representations II: Minimal dimension. Lectures at ETH Zürich, 2014.

[18] R. McEliece, E. Rodemich, H. Rumsey, and L. Welch. New upper bounds on the rate of a code via the delsarte-macwilliams inequalities. *IEEE Transactions on Information Theory*, 1977.

[19] Y. Polyanskiy. Hypercontractivity of spherical averages in hamming space. *SIAM Journal on Discrete Mathematics*, 2019.

[20] R. Prosanov. Chromatic numbers of spheres. *Discrete Mathematics*, 341:3123–3133, 2018.

[21] A. M. Raigorodskii. On the chromatic numbers of spheres in $\mathbb{R}^n$. *Combinatorica*, 32(1):111–123, 2012.

[22] A. Rao and O. Sprumont. A criterion for decoding on the binary symmetric channel. *Advances in Mathematics of Communications*, 19(2):437–477, 2025.

[23] S. Srinivasan. A robust version of hegedűs's lemma, with applications. *TheoretiCS*, 2, 2023.

[24] G. Szegő. *Orthogonal Polynomials*. American Mathematical Society, 1959.

[25] A. Tal. Tight Bounds on the Fourier Spectrum of AC0. In *32nd Computational Complexity Conference (CCC 2017)*, Leibniz International Proceedings in Informatics (LIPIcs), pages 15:1–15:31, 2017.

[26] Wikipedia contributors. Binary entropy function. `https://en.wikipedia.org/wiki/Binary_entropy_function#Taylor_series`, 2026. Accessed: 2026-07-17.

A Proof of Claim 24

Claim 24. *For $z \in [0, 1/2]$ it holds that*

$$h\left(\frac{1}{2} - z\right) + h\left(\frac{1}{2} - \sqrt{\frac{1}{4} - z^2}\right) - 1 \geq c(z^2(1 - 4z^2))\,,$$

where $c > 0$ is an absolute constant.

Proof. We recall the standard expression for the Taylor series of the binary entropy function abut 1/2 [26]

$$h(1/2 - x) = 1 - \frac{1}{\ln 2} \sum_{i \geq 1} \frac{(2x)^{2i}}{2i \cdot (2i-1)}.$$

Replacing x once with z and again with $\sqrt{1/4 - z^2}$ we get

$$
\begin{aligned}
&h\left(\frac{1}{2} - z\right) + h\left(\frac{1}{2} - \sqrt{\frac{1}{4} - z^2}\right) - 1 \\
&= 1 - \frac{1}{\ln 2}\left[\sum_{i \geq 1} \frac{(2z)^{2i}}{2i \cdot (2i-1)} + \frac{(1-4z^2)^i}{2i \cdot (2i-1)}\right] \\
&= \frac{1}{\ln 2}\left[\sum_{i \geq 1} \frac{1}{2i \cdot (2i-1)} - \frac{(2z)^{2i}}{2i \cdot (2i-1)} - \frac{(1-4z^2)^i}{2i \cdot (2i-1)}\right] \quad (\ln 2 = \textstyle\sum_{i \geq 1} \frac{1}{2i(2i-1)}) \\
&= \frac{1}{\ln 2}\left[\sum_{i \geq 1} \frac{1 - (4z^2)^i - (1-4z^2)^i}{2i \cdot (2i-1)}\right] \\
&\geq \frac{8z^2 - 32z^4}{12 \cdot \ln 2} \qquad \text{(since } (1 - x^i) \geq (1-x)^i, \forall i \geq 1 \text{ and } x \in [0,1]) \\
&\geq c \cdot z^2(1 - 4z^2), \qquad \text{(for some absolute constant } c)
\end{aligned}
$$

where in the penultimate step we only keep the term corresponding to $i = 2$ and drop the rest. □

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il