Electronic Colloquium on Computational Complexity, Report No. 344 (2026)

Complex-analytic lower bounds for completions of Gap Hamming

Kaave Hosseini*

Abstract

Gap Hamming is the promise problem of distinguishing pairs of n-bit binary strings at Hamming distance at most $n/4$ from those at distance at least $3n/4$. We show that every completion of Gap Hamming to a total function has normalized trace norm and factorization norm at least $2^{\Omega(n)}$, exponentially improving previous bounds on these parameters. The proof uses polynomial division and Jensen's inequality from complex analysis and applies to arbitrary real completions.

Moreover, we show every Boolean completion has approximate factorization norm at least $n^{\Omega(1)}$ and approximate nonnegative rank at least $\exp(\Omega(\log^2 n))$. These latter results use Hadamard's interpolation theorems and Beckner's imaginary hypercontractivity (Annals of Mathematics '75). As an immediate application, the randomized communication complexity of any Boolean completion is $\Omega(\log^2 n)$. This improves the previous $\Omega(\log\log n)$ lower bound of Blondal, Hatami, Hatami, Lalov, and Tretiak (STOC 2026). As another application in noninteractive ε-locally private learning, the partial class needs only $O(\varepsilon^{-2})$ samples, while every Boolean completion requires $n^{\Omega(1)}/\varepsilon^2$.

1 Introduction

Given $x, y \in \{0,1\}^n$, let $d_H(x,y)$ denote the number of coordinates on which x and y differ. We assume that n is divisible by 4. The Gap Hamming problem with thresholds $n/4$ and $3n/4$ is the partial function

$$\mathrm{GHD}^n_{n/4}(x,y) = \begin{cases} 0 & d_H(x,y) \le n/4, \\ 1 & d_H(x,y) \ge 3n/4, \\ * & \text{otherwise.} \end{cases}$$

A *Boolean completion* of $\mathrm{GHD}^n_{n/4}$ is a total Boolean matrix obtained by replacing each $*$ with either 0 or 1. Let $X(\cdot)$ be a complexity measure of Boolean matrices. The following question template is related to a remarkable range of applications:

How large must $X(M)$ be for every Boolean completion M of $\mathrm{GHD}^n_{n/4}$?

The measures $X(\cdot)$ studied include *real rank* [Hav18]; *VC dimension* [AHHM22, BKT26, CMW25], *list replicability* and *Littlestone dimension* [BHH+26, CMW25]; *sign-rank* and certain topological invariants [HHM23, FHV26], *margin complexity* aka *discrepancy* [BHH+26]; *rectangle-overlay* and *equality-oracle complexity* [PSS14, CLV19]; and *randomized communication complexity* [BHH+26, FGHH25, GHR+26]. Since $\mathrm{GHD}^n_{n/4}(x,y)$ depends only on $x \oplus y$, it can also be viewed as the XOR lift of the partial Gap Majority function. Boolean completions of the form $M(x,y) = f(x \oplus y)$ correspond to functions f called *approximate majorities*. They have been

*Department of Computer Science, University of Rochester. Email: kaave.hosseini@rochester.edu.

ISSN 1433-8092

studied in terms of *constant-depth circuit size* [ABO84, Vio09, KS18, Coo20], *approximate degree* [BKT20], *certifying-polynomial degree* over $\mathbb{F}_2$ [KS18], *randomized decision-tree size* [CDM25], and *unambiguous randomized parity-query complexity* [Gav25].

The goal of this paper is to study exact and approximate *normalized trace norms* and *factorization norms*, as well as *approximate nonnegative rank*, using a new complex analytic approach that may be of independent interest. We discuss some applications later.

The *normalized trace norm* of a $2^n \times 2^n$ matrix M is $\|M\|_{\mathrm{ntr}} = 2^{-n} \sum_{i=1}^{2^n} \sigma_i(M)$, where $\sigma_i(M)$ are its singular values. The *factorization norm* is

$$\gamma_2(M) = \inf_{M_{xy}=\langle u_x, v_y\rangle} \Big(\max_x \|u_x\|_2\Big)\Big(\max_y \|v_y\|_2\Big),$$

where the infimum is over factorizations of the entries of M as inner products of real vectors. One has $\|M\|_{\mathrm{ntr}} \le \gamma_2(M)$ (see Fact 8). These were introduced to communication complexity in [LMSS07, LS09] and have been used study the power and limitations of fingerprinting in randomized communication [CHHS23, CHH$^+$25, GHR25]. The *approximate normalized trace norm* is defined by

$$\|M\|_{\mathrm{ntr},1/3} = \inf\{\|P\|_{\mathrm{ntr}} : P \in \mathbb{R}^{2^n \times 2^n},\ \|P - M\|_\infty \le 1/3\}.$$

and if M is partial, the approximation requirement is only on specified entries. Similarly define the *approximate factorization norm* denoted by $\gamma_{2,1/3}(M)$. The logarithms of these approximate norms give lower bounds on bounded-error quantum communication complexity, even with prior entanglement; see Razborov [Raz03] for the approximate trace norm and Linial and Shraibman [LS09] for the approximate factorization norm. For a nonnegative matrix P, its *nonnegative rank* $\mathrm{rank}_+(P)$ is the least r such that $P(x,y) = \sum_{j=1}^r f_j(x) g_j(y)$ with nonnegative functions f_j, g_j. Define $\mathrm{rank}_{+,1/3}(M)$ similar to the previous approximate definitions. Nonnegative rank was introduced into communication complexity by Yannakakis [Yan91]. Its approximate version is a useful tool for lower bounds on randomized communication complexity and is closely related to the *smooth rectangle bound* [KMSY14]. Finally, let $\mathrm{rank}_{1/3}(M)$ be the minimum rank of a real matrix P with $\|P - M\|_\infty \le 1/3$. For every total Boolean matrix M,

$$\|M\|_{\mathrm{ntr},1/3} \le \gamma_{2,1/3}(M) \le 2\sqrt{\mathrm{rank}_{1/3}(M)} \le 2\sqrt{\mathrm{rank}_{+,1/3}(M)}.$$

The middle inequality follows from John's theorem $\gamma_2(P) \le \|P\|_\infty \sqrt{\mathrm{rank}(P)}$ [LMSS07] and $\|P\|_\infty \le 2$ for every such approximant P.

1.1 Main results

A *real completion* of $\mathrm{GHD}^n_{n/4}$ allows the star entries to take arbitrary real values.

Theorem 1. *Every real completion M of $\mathrm{GHD}^n_{n/4}$ satisfies $\|M\|_{\mathrm{ntr}} \ge 2^{\Omega(n)}$.*

As discussed before, this immediately implies $\gamma_2(M) \ge 2^{\Omega(n)}$. For Boolean completions, a polynomial lower bound $\gamma_2(M) \ge n^{\Omega(1)}$ follows from the recent theorem of Balla, Hambardzumyan, and Tomon that Boolean matrices of small γ_2 norm contain large monochromatic rectangles, together with standard Hamming-cube isoperimetry [Kle66, KS93]. The proof of Theorem 1 uses polynomial division and Jensen's inequality from complex analysis. We give a sketch of the proof in the bounded case in Section 1.2.

Unlike the exact norm, there are bounded completions of Gap Hamming with constant approximate factorization norm. Indeed, let $D(x,y) = d_H(x,y)/n$. Then D approximates $\mathrm{GHD}^n_{n/4}$ within error $1/4$ on every specified entry. Moreover,

$$D(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i(1-y_i) + (1-x_i)y_i), \tag{1}$$

so $\gamma_2(D) \le 2$. In contrast, we show every *Boolean* completion has large approximate normalized trace norm, hance approximate factorization norm.

Theorem 2. *Every Boolean completion M of $\mathrm{GHD}^n_{n/4}$ satisfies $\|M\|_{\mathrm{ntr},1/3} \ge n^{\Omega(1)}$.*

For comparison, the margin bound of Blondal et al. [BHH+26, Section 4] implies $\gamma_{2,1/3}(M) = \Omega((\log n)^{1/4})$. The polynomial lower bound of Theorem 2 is significantly more involved than proof of Theorem 1. It is interesting to see if the lower bound here is tight.

Question 3. *Is there a Boolean completion M of $\mathrm{GHD}^n_{n/4}$ such that $\gamma_{2,1/3}(M) \le n^{O(1)}$?*

Nevertheless, we improve the lower bounds in the case of approximate non-negative rank. The bounded completion D in (1) has $\mathrm{rank}_+(D) \le 2n$, but for Boolean completions, we obtain the following quasipolynomial lower bound.

Theorem 4. *Every Boolean completion M of $\mathrm{GHD}^n_{n/4}$ satisfies $\mathrm{rank}_{+,1/3}(M) \ge \exp(\Omega(\log^2 n))$.*

It would be interesting to see if this complex analytic framework is strong enough to give exponential lower bounds here.

Question 5. *Does every Boolean completion M of $\mathrm{GHD}^n_{n/4}$ satisfy $\mathrm{rank}_{+,1/3}(M) \ge 2^{\Omega(n)}$?*

1.1.1 Application in private learning

In supervised learning, there is an unknown distribution D over labeled examples (y,b), where y is a data point and $b \in \{0,1\}$ is its label. A learner receives independent examples from D and must output a Boolean classifier h that predicts the label of a new data point. In agnostic learning, the labels need not agree with any classifier in the given concept class $\mathcal{C}$. The goal is to output h satisfying

$$L_D(h) \le \min_{c\in\mathcal{C}} L_D(c) + \alpha, \qquad L_D(h) = \Pr_{(y,b)\sim D}[h(y) \ne b],$$

with probability at least $2/3$. The output h need not belong to $\mathcal{C}$. In locally private learning, the learner does not see the examples directly. Instead, each example (y,b) is held by a separate user, who computes a randomized message from it and sends that message to the learner. The message need not itself be a labeled example. For instance, a user may be asked to evaluate a publicly specified classifier on their example and send a randomized bit indicating whether its prediction was correct. The ε-local privacy requirement ensures that changing the user's entire labeled example changes the probability of any message event by at most a factor of e^{ε}. The learner must construct h using only the received messages. The protocol is *noninteractive* if all users' randomization rules are fixed before any messages are received.

We consider concept classes obtained from partial Boolean matrices. Each row is a classifier that may output 0, 1, or the undefined symbol $*$. In the learning benchmark, an undefined prediction counts as an error [AHHM22], although the learner itself must output a total Boolean classifier h. Completing the matrix replaces every star by a Boolean value, making each reference classifier at

least as accurate as before. Consequently, the learner must compete with a potentially better class of classifiers.

This raises a natural question: can a partial concept class be much easier to learn privately than every Boolean completion? We answer this affirmatively using Gap Hamming. Its rows define the partial class

$$c_x(y) = \mathrm{GHD}^n_{n/4}(x, y), \qquad x \in \{0,1\}^n.$$

For any Boolean completion M of $\mathrm{GHD}^n_{n/4}$, the corresponding total concept class is

$$\mathcal{C}_M = \{y \mapsto M(x, y) : x \in \{0,1\}^n\}.$$

We show that the partial class can be learned with $O(\varepsilon^{-2})$ samples, whereas every Boolean completion requires $n^{\Omega(1)}/\varepsilon^2$ samples, at a fixed excess error. For the upper bound, public randomness selects a constant-size family of candidate classifiers. Each user evaluates one prescribed candidate on their own labeled example and sends a randomized bit reporting whether it made an error. These messages allow the learner to estimate the candidates' errors and select the best one.

For the lower bound, Edmonds, Nikolov, and Pitassi [ENP22] relate the sample complexity of noninteractive locally private agnostic learning to the approximate γ_2 norm of the sign-valued concept matrix. At a fixed sufficiently small excess error, an approximate γ_2 norm of B gives a sample lower bound of $\Omega(B^2/\varepsilon^2)$. Combining this result with Theorem 2 gives the separation.

Corollary 6. *There is an absolute $\alpha_0 > 0$ such that, for every $0 < \varepsilon \le 1$, the partial class formed by the rows of $\mathrm{GHD}^n_{n/4}$ admits a noninteractive ε-locally private agnostic learner with excess error α_0 using $O(\varepsilon^{-2})$ samples. For every Boolean completion M, learning $\mathcal{C}_M$ under the same requirements needs $n^{\Omega(1)}/\varepsilon^2$ samples.*

This improves the lower bound $\Omega(\sqrt{\log n}/\varepsilon^2)$ obtained from the margin complexity bound of Blondal, Hatami, Hatami, Lalov, and Tretiak [BHH+26, Section 4], proved using topological methods.

1.1.2 Application in pseudodeterministic communication

Let $R^{\mathrm{pub}}_{1/3}(M)$ denote the minimum worst-case number of bits communicated by a public-coin randomized protocol that computes M with error at most $1/3$ on every input. A randomized protocol for a partial function only needs to be correct on the promised inputs. For $\mathrm{GHD}^n_{n/4}$, there is a simple protocol of cost $O(1)$; the parties use public randomness to choose a uniform coordinate i. Alice sends x_i, and Bob outputs $x_i \oplus y_i$. The probability of output 1 is $d_H(x, y)/n$, so the protocol uses one bit and errs with probability at most $1/4$ on every promised input.

A *pseudodeterministic* protocol must additionally produce, with high probability, a fixed Boolean answer on every input. Equivalently, it computes some Boolean completion of the partial function. The sampling protocol for $\mathrm{GHD}^n_{n/4}$ is not of this kind, because on inputs in the middle of the gap it gives both answers with comparable probabilities. Thus the constant-cost protocol for the promise problem does not settle the randomized complexity of its Boolean completions.

Blondal et al. [BHH+26] showed that every Boolean completion requires $\Omega(\log \log n)$ randomized communication. Göös et al. [GHR+26] established an exponential separation between randomized and pseudodeterministic communication for another partial function, and conjectured that Gap Hamming itself requires $\Omega(n)$ pseudodeterministic communication.

Theorem 4 gives the following exponential improvement, using the standard relation [LMdW23, Theorems 1 and 5]

$$\log \mathrm{rank}_{+,1/3}(M) \le O(R^{\mathrm{pub}}_{1/3}(M) + \log n).$$

Corollary 7. *Every Boolean completion M of $\mathrm{GHD}^n_{n/4}$ satisfies $R^{\mathrm{pub}}_{1/3}(M) = \Omega((\log n)^2)$.*

1.2 Proof ideas

We outline the proof of Theorem 1 in the special case of bounded completions. The reader may consult the notation given in the next section. Let $M \in [0,1]^{2^n \times 2^n}$ be a bounded completion of $\mathrm{GHD}^n_{n/4}$. A standard symmetrization gives a function $f : \{0,1\}^n \to [0,1]$

$$f(w) = \mathbb{E}_{x \in \{0,1\}^n} M(x, x \oplus w),$$

which satisfies $f(w) = 0$ for $|w| \le n/4$ and $f(w) = 1$ for $|w| \ge 3n/4$. Consider the polynomial

$$p(z) = \sum_{S \subseteq [n]} \widehat{f}(S) z^{|S|}$$

and note that for $z \in \mathbb{C}$ with $|z| \le 1$

$$|p(z)| \le \sum_{S \subseteq [n]} |\widehat{f}(S)| \le \|M\|_{\mathrm{ntr}}. \tag{2}$$

Moreover, we have $p(1) = f(0) = 0$ and $p(-1) = f(1^n) = 1$. It is easy to show that $|p(z)| \le e^{-\Omega(n)}$ on an arc of the unit circle around 1 of length $\Omega(1)$. On the opposite arc around -1, we likewise have $|1 - p(z)| \le e^{-\Omega(n)}$. Moreover, w.l.o.g assume that $p(0) \ge 1/2$ (otherwise use $1 - p(-z)$, whose absolute value is at most $1 + \|M\|_{\mathrm{ntr}}$ on the unit disk). Jensen's inequality (Lemma 9) states that the value of $\log p(0)$ (which is at least $-\log 2$) is upper bounded by the average of $\log |p(z)|$ over the entire unit circle. Since $\log |p(z)| < -\Omega(n)$ on the arc of length $\Omega(1)$ around 1, there must be a point z^* on the unit circle where $\log |p(z^*)| \ge \Omega(n)$ which implies the statement of the theorem.

For the approximate parameters, note that a constant entrywise error will make the above argument useless. In this case, we rely on Booleanity of the completions and use majority amplification to reduce the error exponentially. However, we need several more tools to proceed, including Hadamard's three-lines theorem and three-circles theorem. So we postpone the proof sketch of Theorem 2 to Section 4. For the approximate nonnegative rank result we need Beckner's imaginary hypercontractivity [Bec75] to get quasipolynomial bound.

2 Preliminaries

On the cube we use the uniform distribution, so $\mathbb{E}_x f(x) = 2^{-n} \sum_x f(x)$ and $\|f\|_{L^p} = \left(\mathbb{E}_x |f(x)|^p\right)^{1/p}$. For a matrix A, we write $\|A\|_\infty$ for its largest absolute entry, $\|A\|_F$ for its Frobenius norm, and $\|A\|_{\mathrm{op}}$ for its largest singular value. The all-ones matrix is J. All logarithms are natural unless a base is indicated.

2.1 Matrix norms

For $\varepsilon \ge 0$, the approximate factorization norm is

$$\gamma_{2,\varepsilon}(M) = \inf\{\gamma_2(P) : P \in \mathbb{R}^{2^n \times 2^n},\ \|P - M\|_\infty \le \varepsilon\}.$$

It is nonincreasing in ε. We also use the following standard properties; see [LMSS07, LS09, HHH23].

Fact 8. *For real $2^n \times 2^n$ matrices A and B,*

$$\|A\|_{\mathrm{ntr}} \le \gamma_2(A), \qquad \|A\|_{\mathrm{ntr}} \le \frac{\sqrt{\mathrm{rank}(A)}}{2^n}\,\|A\|_F. \tag{3}$$

Moreover, $\gamma_2(J) = 1$, $\gamma_2(cA) = |c|\,\gamma_2(A)$ for $c \in \mathbb{R}$, and

$$\gamma_2(A+B) \le \gamma_2(A) + \gamma_2(B), \qquad \gamma_2(A \circ B) \le \gamma_2(A)\gamma_2(B).$$

Here $A \circ B$ denotes the entrywise product.

2.2 Fourier analysis and noise profiles

For $x \in \{0,1\}^n$ and $S \subseteq [n]$, define the Fourier character $\chi_S(x) = (-1)^{\sum_{i\in S} x_i}$. These characters form an orthonormal basis; for a real function f on the cube, put

$$\widehat{f}(S) = \mathbb{E}_x[f(x)\chi_S(x)], \qquad \|\widehat{f}\|_1 = \sum_{S\subseteq[n]} |\widehat{f}(S)|.$$

For $A(x,y) = f(x \oplus y)$, Fourier expansion gives $A(x,y) = \sum_S \widehat{f}(S)\chi_S(x)\chi_S(y)$. Each matrix $(\chi_S(x)\chi_S(y))_{x,y}$ has factorization norm 1, so $\gamma_2(A) \le \|\widehat{f}\|_1$ by the triangle inequality. See [O'D14, Chapters 1–2] for background. For a real matrix A, define $h_A(w) = \mathbb{E}_x A(x, x\oplus w)$. It's easy to see from convexity of the trace norm and its invariance under row and column permutations that

$$\|\widehat{h}_A\|_1 \le \|A\|_{\mathrm{ntr}}. \tag{4}$$

For $z \in \mathbb{C}$, define the *noise profile* of A by

$$\begin{aligned} F_A(z) &= \sum_{w\in\{0,1\}^n} h_A(w)\Big(\frac{1+z}{2}\Big)^{n-|w|}\Big(\frac{1-z}{2}\Big)^{|w|} \\ &= \sum_{S\subseteq[n]} \widehat{h}_A(S) z^{|S|}, \end{aligned} \tag{5}$$

where the second identity follows by Fourier expansion. This is a polynomial of degree at most n, linear in A, with $F_J = 1$. For $|z| \le 1$, inequality (4) gives

$$|F_A(z)| \le \|A\|_{\mathrm{ntr}}. \tag{6}$$

2.3 Complex analysis

Write $z = x + iy$ with $x, y \in \mathbb{R}$ and $i^2 = -1$. We denote its real and imaginary parts by $\mathrm{Re}\, z = x$ and $\mathrm{Im}\, z = y$, and its modulus by $|z| = \sqrt{x^2+y^2}$. A function is *holomorphic* on an open set if it is complex differentiable at every point of that set. Every polynomial is holomorphic. We use $\log|f(z)|$, the real logarithm of the modulus, with $\log 0 = -\infty$.

Jensen's inequality relates the value of a holomorphic function at the center of a disk to its values on the boundary. Here it will force large values somewhere on the circle if the function is very small on an arc but nonzero at the center.

Lemma 9 (Jensen's inequality [Ahl79, Chapter 5, Section 3.1])**.** *Let q be holomorphic on a neighborhood of the closed unit disk. Then*

$$\log|q(0)| \le \frac{1}{2\pi}\int_0^{2\pi} \log|q(e^{i\theta})|\, d\theta, \tag{7}$$

where $\log 0 = -\infty$.

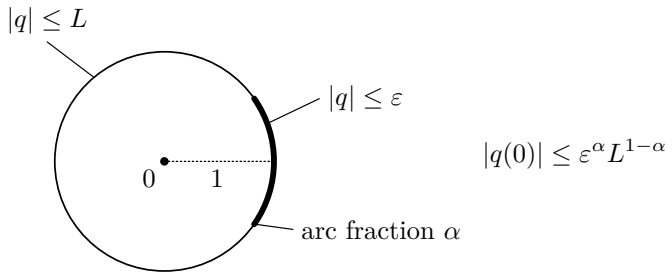

Figure 1: Jensen's inequality (Lemma 9). If $|q| \le \varepsilon$ on the bold arc, which occupies a fraction α of the unit circle, and $|q| \le L$ on the remaining arc, then $|q(0)| \le \varepsilon^{\alpha} L^{1-\alpha}$. A nonzero value at the center therefore limits how small q can be on an arc unless it is large elsewhere.

For the approximate bounds, we use Hadamard's theorems to interpolate between bounds on parallel lines and on concentric circles. See [Rud87, Theorem 12.8].

Lemma 10 (Hadamard's three-lines theorem)**.** *Let g be holomorphic in $0 < \operatorname{Im} w < 1$, bounded and continuous on the closed strip. Suppose $0 < \varepsilon \le L$ and, for every $u \in \mathbb{R}$,*

$$|g(u)| \le \varepsilon, \qquad |g(u+i)| \le L.$$

Then, for every $u \in \mathbb{R}$ and $0 \le t \le 1$,

$$|g(u+it)| \le \varepsilon^{1-t} L^{t}. \tag{8}$$

Roughly speaking, this theorem says that if an analytic function is very small on one boundary of a strip and bounded on the other boundary, then it must remain small sufficiently close to the first boundary.

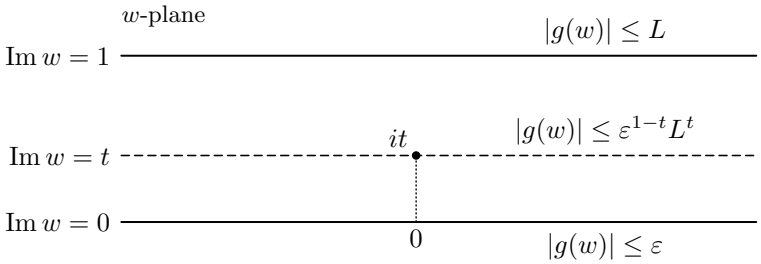

Figure 2: Hadamard's three-lines theorem (Lemma 10). Bounds ε and L on the two boundary lines give the bound $\varepsilon^{1-t} L^{t}$ on every intermediate line $\operatorname{Im} w = t$, for $0 \le t \le 1$.

Lemma 11 (Hadamard's three-circles theorem)**.** *Let q be holomorphic on a neighborhood of the disk $|z-a| \le 4r$, where $r > 0$, and write $M(t) = \max_{|z-a|\le t} |q(z)|$. Then*

$$M(2r) \le \sqrt{M(r)M(4r)}. \tag{9}$$

For the nonnegative-rank bound we also use the complex noise operator. For a function $g : \{0,1\}^d \to \mathbb{C}$ and $z \in \mathbb{C}$, define

$$(T_z g)(x) = \sum_{S \subseteq [d]} z^{|S|} \widehat{g}(S) \chi_S(x).$$

The following inequality controls this operator at imaginary parameters.

Lemma 12 (Beckner's imaginary hypercontractivity [Bec75])**.** *For $0 < |t| \le 1$, let $p = 1 + t^2$ and $p' = p/(p-1)$. For every $g : \{0,1\}^d \to \mathbb{C}$,*

$$\|T_{it} g\|_{L^{p'}} \le \|g\|_{L^p}.$$

Finally we need the following basic observation about growth of polynomials with a zero of high multiplicity. A polynomial q has a *zero of order at least m* at a if $(z-a)^m$ divides $q(z)$. The following coefficient bound controls its size near such a zero.

Lemma 13. *Suppose $q(z) = \sum_{j=0}^{n} c_j z^j$ has a zero of order at least m at 1, where $1 \le m \le n$, and put $B = \sum_j |c_j|$. For $|z| \le 1$,*

$$|q(z)| \le B \left(\frac{en|z-1|}{m} \right)^m. \tag{10}$$

Proof. Write $q(z) = (1-z)^m h(z)$ with $h(z) = \sum_{\ell=0}^{n-m} b_\ell z^\ell$. Using the power series

$$(1-z)^{-m} = \sum_{k \ge 0} \binom{m+k-1}{m-1} z^k \qquad (|z| < 1),$$

and comparing the coefficients of z^ℓ in $h(z) = q(z)(1-z)^{-m}$, we get

$$b_\ell = \sum_{j=0}^{\ell} \binom{m+\ell-j-1}{m-1} c_j.$$

Summing absolute values and then the binomial coefficients yields

$$\sum_{\ell=0}^{n-m} |b_\ell| \le \sum_{j=0}^{n-m} |c_j| \binom{n-j}{m} \le B \binom{n}{m}.$$

For $|z| \le 1$, this bounds $|h(z)|$. Using $\binom{n}{m} \le (en/m)^m$, we obtain the lemma. □

3 Proof of Theorem 1

The lower bound in Theorem 1 follows from Theorem 14 and (4), applied to $f(w) = \mathbb{E}_x M(x, x \oplus w)$.

Theorem 14. *Let $f : \{0,1\}^n \to \mathbb{R}$ satisfy $f(w) = 0$ for $|w| \le n/4$ and $f(w) = 1$ for $|w| \ge 3n/4$. Then*

$$\|\widehat{f}\|_1 \ge \frac{1}{4}\, 2^{\,n/(32\pi e)}.$$

Proof. Put $L = \|\widehat{f}\|_1 \ge |f(1^n)| = 1$ and

$$p(z) = \sum_S \widehat{f}(S) z^{|S|} = \sum_w f(w) \Big(\frac{1+z}{2}\Big)^{n-|w|} \Big(\frac{1-z}{2}\Big)^{|w|}.$$

Every nonzero term has $|w| > n/4$, so $(1-z)^{n/4}$ divides p. Applying the same observation to $1-f$ shows that $(1+z)^{n/4}$ divides $1-p$. Replace p by $1-p$ if necessary so that $p(0) \ge 1/2$. If its zero is now at -1, replace $p(z)$ by $p(-z)$. Thus p has degree at most n and a zero of order at least $n/4$ at 1. The sum of the absolute values of its coefficients is at most $1 + L \le 2L$. By Lemma 13, on the arc $\{e^{i\theta} : |\theta| \le 1/(8e)\}$,

$$|p(e^{i\theta})| \le 2L(4e|e^{i\theta} - 1|)^{n/4} \le 2L\, 2^{-n/4}.$$

This arc has normalized length $1/(8\pi e)$, while $|p| \le 2L$ on the whole unit circle. Applying Lemma 9 and bounding the integral separately on the arc and its complement gives

$$-\log 2 \le \frac{1}{2\pi} \int_0^{2\pi} \log |p(e^{i\theta})|\, d\theta \le \log(2L) - \frac{n \log 2}{32\pi e}.$$

Rearranging gives $L \ge \frac{1}{4}\, 2^{\,n/(32\pi e)}$. □

Remark 15 (General thresholds). If the thresholds $n/4$ and $3n/4$ are replaced by k and $n-k$, where $0 \le k < n/2$ is an integer, the same proof gives asymptotically tight bounds of $\|M\|_{\mathrm{ntr}} \ge \frac{1}{4}\exp(\Omega(k^2/n))$ for every real completion. One uses a zero of order $k+1$ and the arc $\{e^{i\theta} : |\theta| \le (k+1)/(2en)\}$.

4 Approximate bounds and applications

We first give the proof overviews before giving the detailed proofs.

Proof idea for approximate factorization norm. We explain the proof of the polynomial lower bound on approximate factorization norm. The goal is to show that every Boolean completion M of $\mathrm{GHD}^n_{n/4}$ satisfies $\gamma_{2,1/3}(M) \ge n^{\Omega(1)}$. Suppose that there is a real matrix P such that $\|P - M\|_\infty \le \frac{1}{3}$ for every x, y. In the exact proof, we had a polynomial $F_M(z)$ that is exponentially small near $z = 3/4$ and close to 1 at $z = -3/4$. But, we do not have a similar approximation for P because there is a $1/3$ additive error. So we first run a *majority amplification* to improve the error. This is the only part where Booleanity of M is used. First, rescale P to make sure it takes values in $[0,1]$, and say $P(x,y) \le \frac{2}{5}$ if $M(x,y) = 0$ and $P(x,y) \ge \frac{3}{5}$ if $M(x,y) = 1$. Interpret $P(x,y)$ as the probability that a coin comes up heads. Flip this coin $50s$ times, and output 1 if at least half of the results are heads. Let $A_s(x,y)$ be the probability that this majority is 1. By concentration

$$\|A_s - M\|_\infty \le e^{-s}. \tag{11}$$

We get exponentially small error, however factorization norm of A_s can increase compared to that of P. But since factorizaiton norm is submultiplicative under entrywise products and majority probability $A_s(x,y)$ is a polynomial of degree $50s$ in $P(x,y)$ we get

$$\gamma_2(A_s) \le \gamma_2(P)^{O(s)}. \tag{12}$$

The rest of the proof uses complex analysis to show that Equation (11) and Equation (12) imply that $\gamma_2(P) \geq n^{\Omega(1)}$. From Equation (11), for $t \in [-1,1]$, we get $|F_{A_s}(t) - F_M(t)| \leq e^{-s}$ and Equation (12) implies $|F_{A_s}(z)| \leq \gamma_2(P)^{O(s)}$ for $|z| \leq 1$. Thus we have polynomials F_{A_s} that converge exponentially fast to F_M on the real interval. To guarantee that F_M will stay bounded on a strip around $[-3/4, 3/4]$ as well. We apply Hadamard's three-lines theorem to the differences $F_{A_s} - F_{A_{s-1}}$ which implies each of them should be small on a complex strip around the real interval $[-3/4, 3/4]$ and summing the resulting estimates shows that F_M itself is bounded this strip. More precisely, we obtain $|F_M(z)| \leq O(\gamma_2(P))$ throughout a strip of width $\delta = \Omega\left(\frac{1}{\log(\gamma_2(P))}\right)$. Therefore, if $\gamma_2(P)$ were small, F_M would be bounded on a relatively wide strip. Next we use the Hadamard three-circle theorem to rule this out. Remember we already have $|F_M(z)| \leq e^{-\Omega(n)}$ near $z = \frac{3}{4}$, whereas $F_M(-3/4) \geq \frac{1}{2}$. Suppose that $|F_M(z)| \leq L$ for some L throughout the complex strip of width δ around $[-3/4, 3/4]$. We use Hadamard's three-circles theorem to propagate the smallness from $3/4$ toward $-3/4$ through a sequence of overlapping disks. If the maximum of $|F_M|$ on the current small disk is m_j, the three-circles theorem gives $m_{j+1} \leq \sqrt{m_j L}$. Starting with $m_0 \leq e^{-\Omega(n)}$, after $N = O(1/\delta)$ steps we obtain $m_N \leq L \exp\left(-\Omega\left(\frac{n}{2^N}\right)\right)$. But the final disk contains $-3/4$, where $F_M(-3/4) \geq 1/2$. Overall, it implies $n \leq 2^{O(1/\delta)} \log(2L)$. Substituting gives $\gamma_2(P) \geq n^{\Omega(1)}$.

Approximate trace norm. Suppose P approximates M within $1/3$. Using some standard arguments, we can remove some rows and columns to get P' and M' such that $\|P' - M'\|_\infty \leq \frac{1}{3}$ where P' has $\gamma_2(P') \leq O(\|P\|_{\text{ntr}})$ and still make sure the same argument as before goes through using the noise profile $F_{M'}$.

Approximate nonnegative rank. Beckner's imaginary hypercontractivity and majority amplification implies that a bounded matrix A of nonnegative rank at most R satisfies $|F_{A_s}(a+ib)| \leq 3^{O(s)} R^{O(sb^2)}$ when $|a| \leq 7/8,\ |b| \leq 1/8$. The saving is obtained from the quadratic dependence on b in the exponent. The rest of the argument is similar as before.

4.1 Approximate factorization norm

We establish a slightly more general statement, which will also be useful for approximate normalized trace norm.

Proposition 16. *Let $n \geq 200$ and let M be a Boolean $2^n \times 2^n$ matrix. Suppose $F_M(-3/4) \geq 1/2$ and that*

$$|F_M(z)| \leq e^{-n/200}$$

for every z in the disk $|z - 3/4| \leq 1/16$. Then $\gamma_{2,1/3}(M) \geq n^{\Omega(1)}$.

Majority amplification. Let M be Boolean and fix a real matrix P with $\|P - M\|_\infty \leq 1/3$. Put $U = \frac{3P+J}{5}$. For a positive integer m, let

$$Q_m(t) = \sum_{j=\lceil m/2 \rceil}^{m} \binom{m}{j} t^j (1-t)^{m-j},$$

so ties are counted as 1. For every integer $s \geq 1$, define A_s entrywise by $A_s(x,y) = Q_{50s}(U(x,y))$. The entries of U lie in $[0, 2/5]$ where $M = 0$ and in $[3/5, 1]$ where $M = 1$. Interpreting Q_m as the probability that at least half of m independent coin flips are 1, Hoeffding's inequality with $m = 50s$ gives

$$\|A_s - M\|_\infty \leq e^{-s}. \tag{13}$$

Since the weights defining $F_A(t)$ are nonnegative and sum to 1 for real $t \in [-1,1]$, we obtain, throughout this interval,

$$|F_{A_s}(t) - F_M(t)| \le e^{-s}. \tag{14}$$

If $\gamma_2(P) \ge 2$, then submultiplicativity and $\gamma_2(U) + \gamma_2(J-U) \le 2 + 2\gamma_2(P)$ give

$$\gamma_2(A_s) \le \gamma_2(P)^{O(s)}. \tag{15}$$

Thus, throughout the unit disk, $|F_{A_s}(z)| \le \gamma_2(P)^{O(s)}$. For later use, writing $Q_m(t) = \sum_j c_j t^j$, we also have

$$\sum_j |c_j| \le \sum_{k=\lceil m/2 \rceil}^{m} \binom{m}{k} 2^{m-k} \le 3^m. \tag{16}$$

The complex-analytic arguments. Next we show the noise profile to be exponentially small near $3/4$, but large at $-3/4$.

Lemma 17. *If $n \ge 200$ and M is a $[0,1]$-valued completion of $\mathrm{GHD}^n_{n/4}$, then $F_M(-3/4) \ge 3/4$. Moreover, for every z satisfying $|z - 3/4| \le 1/16$,*

$$|F_M(z)| \le e^{-n/200}. \tag{17}$$

Proof. Recall that $0 \le h_M \le 1$, that $h_M(w) = 0$ for $|w| \le n/4$, and that $h_M(w) = 1$ for $|w| \ge 3n/4$. Write $z = 3/4 + u$. By Cauchy–Schwarz in (5), using as reference measure the binomial distribution of parameter $1/8$,

$$|F_M(3/4+u)| \le e^{-n/64} \left(\frac{|7/8 + u/2|^2}{7/8} + \frac{|1/8 - u/2|^2}{1/8} \right)^{n/2},$$

where Hoeffding's inequality was used for the binomial tail. The quantity in parentheses equals $1 + 16|u|^2/7$, and hence for $|u| \le 1/16$ the right-hand side is at most $e^{-n/200}$. The same argument applied to $1 - M$ at $-3/4$ gives $1 - F_M(-3/4) \le e^{-n/64} \le 1/4$. □

We prove the proposition using Hadamard's three-lines theorem and three-circles theorem.

Proof of Proposition 16. Fix P with $\|P - M\|_\infty \le 1/3$. If $\gamma_2(P) < 2$, the argument below with 2 in place of $\gamma_2(P)$ gives $\log n = O(1)$, so this case can be absorbed into the implicit constant in the conclusion. We may therefore assume that $\gamma_2(P) \ge 2$.

By (14) and (15),

$$|F_{A_s}(t) - F_M(t)| \le e^{-s} \quad (t \in [-1,1]), \qquad |F_{A_s}(z)| \le \gamma_2(P)^{O(s)} \quad (|z| \le 1).$$

We first extend the convergence to a complex strip. Put $\delta = \frac{c}{\log \gamma_2(P)}$, where $c > 0$ is a sufficiently small absolute constant. Fix $|a| \le 3/4 + \delta$, and for $s \ge 2$ define

$$g_s(w) = (F_{A_s} - F_{A_{s-1}}) \left(a + \frac{1}{32} \sin w \right).$$

On the real axis, $|g_s| \le e^{-\Omega(s)}$, while throughout $0 \le \operatorname{Im} w \le 1$ we have $|g_s| \le \gamma_2(P)^{O(s)}$. Hadamard's three-lines theorem therefore gives

$$|F_{A_s}(a+ib) - F_{A_{s-1}}(a+ib)| \le e^{-\Omega(s)}$$

for $|b| \le \delta$, provided c is sufficiently small. Since F_{A_1} is bounded by $\gamma_2(P)^{O(1)}$ on the unit disk, summing in s shows that, for some $L = \gamma_2(P)^{O(1)}$,

$$|F_M(z)| \le L \qquad (z \in S_\delta), \qquad S_\delta = \{z : |\operatorname{Re} z| \le 3/4 + \delta,\ |\operatorname{Im} z| \le \delta\}.$$

We now propagate the exponentially small value near $3/4$ across this strip. Put $r = \delta/4$ and choose $N = O(1/\delta)$ points $a_0 = 3/4, \dots, a_N = -3/4$ on the real axis with $|a_{j+1} - a_j| \le r$. Let

$$m_j = \max_{|z - a_j| \le r} |F_M(z)|.$$

The $4r$-disk around a_j lies in S_δ, and the next r-disk lies inside the current $2r$-disk. Hence Hadamard's three-circles theorem gives

$$m_{j+1} \le \sqrt{m_j L}.$$

By the hypotheses of the proposition, $m_0 \le e^{-n/200}$ and $m_N \ge \frac{1}{2}$. Iterating the preceding inequality gives

$$\frac{1}{2} \le L \exp\left(-\Omega\left(\frac{n}{2^N}\right)\right).$$

Therefore

$$\log n = O(N + \log\log L) = O(\log \gamma_2(P)),$$

since $N = O(1/\delta) = O(\log \gamma_2(P))$. Thus $\gamma_2(P) \ge n^{\Omega(1)}$. Taking the infimum over P proves the proposition. □

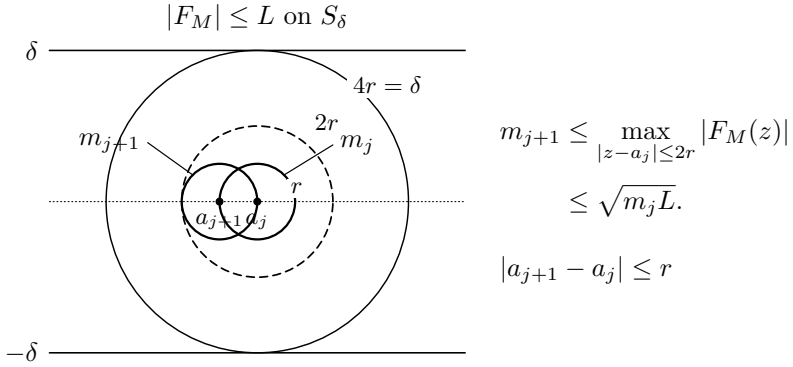

Figure 3: One step in propagation through overlapping disks. Here $m_j = \max_{|z-a_j|\le r} |F_M(z)|$ and $r = \delta/4$. Moving the center by at most r puts the next r-disk inside the $2r$-disk. Hadamard's three-circles theorem between radii r and $4r$ gives $m_{j+1} \le \sqrt{m_j L}$. Repeating this step carries the estimate from $3/4$ to $-3/4$.

4.2 Approximate normalized trace norm

Proof of Theorem 2. Fix $\|P - M\|_\infty \le 1/3$ and assume $n \ge 200$. Factor $P = VW^\top$ by its singular value decomposition so that $\|V\|_F^2 = \|W\|_F^2 = 2^n \|P\|_{\mathrm{ntr}}$. Retain the rows $\mathcal{X}$ of V and $\mathcal{Y}$ of W whose squared norms are at most $8\|P\|_{\mathrm{ntr}}$. By Markov's inequality, $|\mathcal{X}^c|, |\mathcal{Y}^c| \le 2^n/8$. Set

$$P'(x,y) = \mathbf{1}_{\mathcal{X}}(x)\mathbf{1}_{\mathcal{Y}}(y)P(x,y), \qquad M'(x,y) = \mathbf{1}_{\mathcal{X}}(x)\mathbf{1}_{\mathcal{Y}}(y)M(x,y).$$

Then $\|P' - M'\|_\infty \le 1/3$, and the restricted factors give

$$\gamma_2(P') \le 8\|P\|_{\mathrm{ntr}}. \tag{18}$$

Moreover, M' is Boolean and still vanishes for Hamming distance at most $n/4$, so the disk estimate of Lemma 17 holds for $F_{M'}$. For every w, $0 \le h_M(w) - h_{M'}(w) \le (|\mathcal{X}^c| + |\mathcal{Y}^c|)/2^n \le 1/4$. Averaging with the nonnegative weights in (5) gives $F_{M'}(-3/4) \ge F_M(-3/4) - 1/4 \ge 1/2$. Thus M' satisfies Proposition 16, so

$$8\|P\|_{\mathrm{ntr}} \ge \gamma_2(P') \ge \gamma_{2,1/3}(M') \ge n^{\Omega(1)}.$$

Taking the infimum over P proves the theorem. □

4.3 Approximate nonnegative rank

The quasipolynomial improvement comes from the following lemma.

Lemma 18. *For $d \ge 0$ and $R \ge 1$, whenever $A \in [0,1]^{2^d \times 2^d}$ has $\mathrm{rank}_+(A) \le R$, then for $|a| \le 7/8$ and $|b| \le 1/8$,*

$$|F_A(a + ib)| \le R^{O(b^2)}. \tag{19}$$

Proof. First consider the imaginary axis. Write $A = \sum_{j=1}^R f_j g_j^\top$ with nonnegative factors. Because $A \le 1$, we may rescale them so that $0 \le f_j, g_j \le 1$. Let $\mu_j = (\mathbb{E} f_j)(\mathbb{E} g_j)$; then $\sum_j \mu_j = \mathbb{E} A \le 1$. For $0 < |t| \le 1$, set $p = 1 + t^2$ and $p' = p/(p-1)$. By Fourier orthogonality and Hölder's inequality,

$$\begin{aligned} |F_{f_j g_j^\top}(it)| &= |\mathbb{E}_x f_j(x)(T_{it} g_j)(x)| \\ &\le \|f_j\|_{L^p} \|T_{it} g_j\|_{L^{p'}} \\ &\le \|f_j\|_{L^p} \|g_j\|_{L^p} \\ &\le \mu_j^{1/p}, \end{aligned}$$

where the second inequality is Beckner's imaginary hypercontractivity (Lemma 12). By concavity and $\sum_j \mu_j \le 1$,

$$|F_A(it)| \le \sum_j \mu_j^{1/p} \le R^{1-1/p} \le R^{t^2}. \tag{20}$$

To move to $a + ib$, write for bits u, v

$$K_z(u,v) = \frac{1 + z(-1)^{u+v}}{4}, \qquad F_A(z) = \sum_{x,y} A(x,y) \prod_{i=1}^d K_z(x_i, y_i).$$

For $a \ne 0$ put $t = b/(1 - |a|)$. Then

$$K_{a+ib} = |a| K_{\mathrm{sgn}(a)} + (1 - |a|) K_{it}. \tag{21}$$

Expanding the product expresses $F_A(a + ib)$ as a convex combination of profiles $F_{A'}(it)$, where A' is obtained by fixing some coordinate pairs to equal or opposite bits. Such restrictions retain the same entry bound and nonnegative-rank bound. As $|t| \le 1$, the imaginary-axis estimate gives

$$|F_A(a + ib)| \le R^{t^2} \le R^{O(b^2)}.$$

The case $a = 0$ is covered directly by (20). □

Proof of Theorem 4. Assume $n \geq 200$ and fix a nonnegative 1/3-approximant P to M. Put $R = \mathrm{rank}_+(P)$. Then $U = (3P + J)/5$ has nonnegative rank at most $R + 1 \leq 2R$. For every integer $s \geq 1$, set $m = 50s$ and define $A_s(x, y) = Q_m(U(x, y))$. By (14), $|F_{A_s}(t) - F_M(t)| \leq e^{-s}$ for real $|t| \leq 7/8$.

Writing $Q_m(t) = \sum_{j=0}^{m} c_j t^j$, we have $\sum_j |c_j| \leq 3^m$ and $\mathrm{rank}_+(U^{\circ j}) \leq (2R)^j$. Every entrywise power $U^{\circ j}$ lies in $[0, 1]$, so Lemma 18 gives

$$|F_{A_s}(a + ib)| \leq 3^{O(s)} R^{O(sb^2)}. \tag{22}$$

Put $\rho = \Theta(1/\sqrt{\log R})$, with a sufficiently small absolute implied constant. Then (22) gives $|F_{A_s}(a + ib)| \leq e^{O(s)}$ for $|a| \leq 7/8$ and $|b| \leq \rho$. Applying the three-lines calculation from the proof of Proposition 16, for $s \geq 2$, to

$$(F_{A_s} - F_{A_{s-1}})\left(a + \frac{\rho}{2} \sin w\right)$$

shows that F_M is bounded by an absolute constant on a strip of width $\delta = \Theta(\rho)$. Lemma 17 and the same three-circles propagation then give

$$\log n = O(1/\delta) = O(\sqrt{\log R}).$$

Hence $\mathrm{rank}_+(P) \geq \exp(\Omega((\log n)^2))$. □

4.4 Private learning

Proof of Corollary 6. Lower bound. The lower bound immediately follows from Edmonds, Nikolov, and Pitassi [ENP22, Theorem 4] who give the sample lower bound $\Omega((\gamma_{2,1/5}(M) - 1)^2/\varepsilon^2)$ at some absolute excess error $\alpha_0 > 0$, with confidence 2/3.

Upper bound for the partial class. Fix $0 < \alpha < 1$, choose an odd $t \geq 8 \log(12/\alpha)$, and publicly sample $I = (i_1, \ldots, i_t)$ uniformly from $[n]^t$. Writing $x_I = (x_{i_1}, \ldots, x_{i_t})$, consider the 2^t predictors indexed by $z \in \{0, 1\}^t$:

$$h_z(y) = \mathbf{1}\{d_H(z, y_I) > t/2\}.$$

For every promised (x, y), Hoeffding's inequality gives $\Pr_I[h_{x_I}(y) \neq \mathrm{GHD}^n_{n/4}(x, y)] \leq e^{-t/8}$. For an optimal partial row, the expected D-mass of disagreement on its defined entries is therefore at most $e^{-t/8} \leq \alpha/12$. By Markov's inequality, with probability at least 5/6 some h_z has loss at most the partial optimum plus $\alpha/2$.

Assign a disjoint group of users to each z. Each user applies ε-randomized response to $\mathbf{1}\{h_z(y) \neq b\}$, reporting it correctly with probability $e^\varepsilon/(1 + e^\varepsilon)$. Correcting the bias and applying Hoeffding's inequality and a union bound estimates all 2^t losses within $\alpha/4$, with probability at least 5/6, using $O(2^t(t + 1)/(\varepsilon^2\alpha^2))$ samples. Selecting the smallest estimate adds at most $\alpha/2$, so the excess error is at most α with probability at least 2/3. The messages are noninteractive and protect the full labeled example. Taking $\alpha = \alpha_0$ gives $O(\varepsilon^{-2})$ samples. □

Acknowledgments. We thank Daniel Štefankovič for useful conversations. We thank the Simons Institute for the Theory of Computing at UC Berkeley, where this work was conducted while the author was a long-term participant in the program on Pseudorandomness and HDX.

AI statement. The author formulated the problems and applications. LLMs gave an initial complex analytic proof for exact factorization norm, and helped in simplifying and extending the arguments to the other parameters, and during the writing of the manuscript.

References

[ABO84] Miklós Ajtai and Michael Ben-Or. A theorem on probabilistic constant depth computations. In *Proceedings of the 16th Annual ACM Symposium on Theory of Computing (STOC)*, pages 471–474, 1984.

[AHHM22] Noga Alon, Steve Hanneke, Ron Holzman, and Shay Moran. A theory of PAC learnability of partial concept classes. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 658–671, 2022.

[Ahl79] Lars V. Ahlfors. *Complex Analysis*. McGraw–Hill, third edition, 1979.

[Bec75] William Beckner. Inequalities in Fourier analysis. *Annals of Mathematics*, 102(1):159–182, 1975.

[BHH+26] Ari Blondal, Hamed Hatami, Pooya Hatami, Chavdar Lalov, and Sivan Tretiak. Borsuk–Ulam and replicable learning of large-margin halfspaces. In *Proceedings of the 58th Annual ACM Symposium on Theory of Computing (STOC)*, pages 529–540, 2026.

[BKT20] Mark Bun, Robin Kothari, and Justin Thaler. The polynomial method strikes back: Tight quantum query bounds via dual polynomials. *Theory of Computing*, 16(10):1–71, 2020.

[BKT26] Romain Bourneuf, Antonin Kiladjian, and Stéphan Thomassé. Ramsey obstructions to disambiguation, 2026. arXiv:2609.16359.

[CDM25] Arkadev Chattopadhyay, Yogesh Dahiya, and Meena Mahajan. Pseudo-deterministic query complexity of search problems. *Computational Complexity*, 34:20, 2025.

[CHH+25] Tsun-Ming Cheung, Hamed Hatami, Kaave Hosseini, Aleksandar Nikolov, Toniann Pitassi, and Morgan Shirley. A lower bound on the trace norm of Boolean matrices and its applications. In *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, volume 325 of *Leibniz International Proceedings in Informatics*, pages 37:1–37:15, 2025.

[CHHS23] Tsun-Ming Cheung, Hamed Hatami, Kaave Hosseini, and Morgan Shirley. Separation of the factorization norm and randomized communication complexity. In *38th Computational Complexity Conference (CCC 2023)*, volume 264 of *Leibniz International Proceedings in Informatics*, pages 1:1–1:16, 2023.

[CLV19] Arkadev Chattopadhyay, Shachar Lovett, and Marc Vinyals. Equality alone does not simulate randomness. In *34th Computational Complexity Conference (CCC)*, volume 137 of *Leibniz International Proceedings in Informatics*, pages 14:1–14:11, 2019.

[CMW25] Bogdan Chornomaz, Shay Moran, and Tom Waknine. Spherical dimension. In *Proceedings of the 38th Conference on Learning Theory (COLT)*, volume 291 of *Proceedings of Machine Learning Research*, pages 1259–1313, 2025.

[Coo20] Joshua Cook. Size bounds on low depth circuits for promise majority. Report TR20-122, Electronic Colloquium on Computational Complexity, 2020.

[ENP22] Alexander Edmonds, Aleksandar Nikolov, and Toniann Pitassi. Learning versus refutation in noninteractive local differential privacy. In *Advances in Neural Information Processing Systems*, volume 35, 2022.

[FGHH25] Yuting Fang, Mika Göös, Nathaniel Harms, and Pooya Hatami. Constant-cost communication is not reducible to k-Hamming distance. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing (STOC)*, pages 565–571, 2025.

[FHV26] Florian Frick, Kaave Hosseini, and Aliaksei Vasileuski. A $\mathbb{Z}_2$-topological framework for sign-rank lower bounds, 2026. arXiv:2604.01510.

[Gav25] Dmytro Gavinsky. Unambiguous parity-query complexity. *Random Structures & Algorithms*, 66(3):e70010, 2025.

[GHR25] Mika Göös, Nathaniel Harms, and Artur Riazanov. Equality is far weaker than constant-cost communication. *arXiv preprint arXiv:2507.11162*, 2025.

[GHR+26] Mika Göös, Nathaniel Harms, Artur Riazanov, Anastasia Sofronova, Dmitry Sokolov, and Weiqiang Yuan. Pseudodeterministic communication complexity. In *Proceedings of the 58th Annual ACM Symposium on Theory of Computing (STOC)*, pages 2030–2039, 2026.

[Hav18] Ishay Haviv. On minrank and forbidden subgraphs. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2018)*, volume 116 of *Leibniz International Proceedings in Informatics*, pages 42:1–42:14, 2018.

[HHH23] Lianna Hambardzumyan, Hamed Hatami, and Pooya Hatami. Dimension-free bounds and structural results in communication complexity. *Israel Journal of Mathematics*, 253:555–616, 2023.

[HHM23] Hamed Hatami, Kaave Hosseini, and Xiang Meng. A Borsuk–Ulam lower bound for sign-rank and its applications. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC)*, pages 463–471, 2023.

[Kle66] Daniel J. Kleitman. On a combinatorial conjecture of Erdős. *Journal of Combinatorial Theory*, 1(2):209–214, 1966.

[KMSY14] Gillat Kol, Shay Moran, Amir Shpilka, and Amir Yehudayoff. Approximate nonnegative rank is equivalent to the smooth rectangle bound. In *Automata, Languages, and Programming (ICALP 2014), Part I*, volume 8572 of *Lecture Notes in Computer Science*, pages 701–712. Springer, 2014.

[KS93] Daniel J. Kleitman and Leonard J. Schulman. Minimally distant sets of lattice points. *European Journal of Combinatorics*, 14(3):231–240, 1993.

[KS18] Swastik Kopparty and Srikanth Srinivasan. Certifying polynomials for $\mathrm{AC}^0[\oplus]$ circuits, with applications to lower bounds and circuit compression. *Theory of Computing*, 14(12):1–24, 2018.

[LMdW23] Olivier Lalonde, Nikhil S. Mande, and Ronald de Wolf. Tight Bounds for the Randomized and Quantum Communication Complexities of Equality with Small Error. In *43rd IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2023)*, volume 284 of *Leibniz International Proceedings in Informatics*, pages 32:1–32:18, 2023.

[LMSS07] Nati Linial, Shahar Mendelson, Gideon Schechtman, and Adi Shraibman. Complexity measures of sign matrices. *Combinatorica*, 27(4):439–463, 2007.

[LS09] Nati Linial and Adi Shraibman. Lower bounds in communication complexity based on factorization norms. *Random Structures & Algorithms*, 34(3):368–394, 2009.

[O'D14] Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.

[PSS14] Periklis A. Papakonstantinou, Dominik Scheder, and Hao Song. Overlays and limited memory communication. In *Proceedings of the 29th IEEE Conference on Computational Complexity (CCC)*, pages 298–308, 2014.

[Raz03] Alexander A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya: Mathematics*, 67(1):145–159, 2003.

[Rud87] Walter Rudin. *Real and Complex Analysis*. McGraw–Hill, third edition, 1987.

[Vio09] Emanuele Viola. On approximate majority and probabilistic time. *Computational Complexity*, 18(3):337–375, 2009.

[Yan91] Mihalis Yannakakis. Expressing combinatorial optimization problems by linear programs. *Journal of Computer and System Sciences*, 43(3):441–466, 1991.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il