Electronic Colloquium on Computational Complexity, Report No. 16 (2019)

THE HARDEST HALFSPACE

ALEXANDER A. SHERSTOV

Abstract. We study the approximation of halfspaces $h : \{0,1\}^n \to \{0,1\}$ in the infinity norm by polynomials and rational functions of any given degree. Our main result is an explicit construction of the "hardest" halfspace, for which we prove polynomial and rational approximation lower bounds that match the trivial upper bounds achievable for all halfspaces. This completes a lengthy line of work started by Myhill and Kautz (1961).

As an application, we construct a communication problem with essentially the largest possible gap, of n versus $2^{-\Omega(n)}$, between the sign-rank and discrepancy. Equivalently, our problem exhibits a gap of $\log n$ versus $\Omega(n)$ between the communication complexity with *unbounded* versus *weakly unbounded* error, improving quadratically on previous constructions and completing a line of work started by Babai, Frankl, and Simon (FOCS 1986). Our results further generalize to the k-party number-on-the-forehead model, where we obtain an explicit separation of $\log n$ versus $\Omega(n/4^n)$ for communication with unbounded versus weakly unbounded error. This gap is a quadratic improvement on previous work and matches the state of the art for number-on-the-forehead lower bounds.

* Computer Science Department, UCLA, Los Angeles, CA 90095. ✉ sherstov@cs.ucla.edu
Supported by NSF CAREER award CCF-1149018 and an Alfred P. Sloan Foundation Research Fellowship.

ISSN 1433-8092

Contents

1. Introduction

Representations of Boolean functions by real polynomials play a central role in theoretical computer science. The notion of *approximating* a Boolean function $f\colon \{0,1\}^n \to \{-1,+1\}$ pointwise by polynomials of given degree has been particularly fruitful. Formally, let $E(f,d)$ denote the minimum error in an infinity-norm approximation of f by a real polynomial of degree at most d:

$$E(f,d) = \min_p \{\|f-p\|_\infty : \deg p \leqslant d\}.$$

This quantity clearly ranges between 0 and 1 for any function $f\colon \{0,1\}^n \to \{-1,+1\}$. In more detail, we have $0 = E(f,n) \leqslant E(f,n-1) \leqslant \cdots \leqslant E(f,0) \leqslant 1$, where the first equality holds because any such f is representable exactly by a polynomial of degree at most n. The study of the polynomial approximation of Boolean functions dates back to the pioneering work in the 1960s by Myhill and Kautz [59] and Minsky and Papert [57]. This line of research has grown remarkably over the decades, with numerous connections discovered to other subjects in theoretical computer science. Lower bounds for polynomial approximation have complexity-theoretic applications, whereas upper bounds are a tool in algorithm design. In the former category, polynomial approximation has enabled significant progress in circuit complexity [17, 10, 48, 49, 73, 15], quantum query complexity [13, 1, 7, 23], and communication complexity [20, 65, 22, 73, 75, 66, 52, 26, 70, 15, 79, 78]. On the algorithmic side, polynomial approximation underlies many of the strongest results obtained to date in computational learning [82, 45, 44, 37, 61, 8], differentially private data release [84, 25], and algorithm design in general [55, 36, 72].

1.1. The hardest halfspace. Myhill and Kautz's work [59] six decades ago, and many of the papers that followed [59, 58, 81, 62, 16, 33, 76, 77, 83], focused on *halfspaces*. Also known as a linear threshold function, a halfspace is any function $h\colon \{0,1\}^n \to \{-1,+1\}$ representable as $h(x) = \operatorname{sgn}(\sum_{i=1}^n z_i x_i - \theta)$ for some fixed reals $z_1, z_2, \ldots, z_n, \theta$. The fundamental question taken up in this line of research is: how well can halfspaces be approximated by polynomials of given degree? An early finding, due to Muroga [58], was the upper bound

$$E(h,1) \leqslant 1 - \frac{1}{n^{\Theta(n)}} \tag{1.1}$$

for every halfspace h in n variables. In words, every halfspace can be approximated pointwise by a linear polynomial to error just barely smaller than the trivial bound of 1. Many authors pursued matching lower bounds on $E(h,1)$ for specific halfspaces h, culminating in an explicit construction by Håstad [33] that matches Muroga's bound (1.1).

The study of $E(h,d)$ for $d \geqslant 2$ proved to be challenging. For a long time, essentially the only result was the lower bound $E(h,d) \geqslant 1 - 2^{-\Theta(n/d^2)+1}$ due to Beigel [16], where h is the so-called *odd-max-bit* halfspace. Paturi [62] proved the incomparable lower bound $E(h,\Theta(n)) \geqslant 1/3$, where h is the majority function on n bits. Much later, the bound $E(h,\Theta(\sqrt{n})) \geqslant 1 - 2^{-\Theta(\sqrt{n})}$ was obtained in [76] for an explicit halfspace. This fragmented state of affairs persisted until the question was resolved completely in [77], with an *existence proof* of a halfspace h such that $E(h,d) \geqslant 1-2^{-\Theta(n)}$ for $d=1,2,\ldots,\Theta(n)$. This result is clearly as strong as one could hope for, since it essentially matches Muroga's upper bound for approximation by *linear* polynomials. The work in [77] further determined the minimum error, denoted $R(h,d)$, to which this h can be approximated by a degree-d rational function, showing that this quantity too is as large for h as it can be for any halfspace. Explicitly constructing a halfspace with these properties is our main technical contribution:

Theorem 1.1. *There is an algorithm that takes as input an integer $n \geqslant 1$, runs in time polynomial in n, and outputs a halfspace $h_n\colon \{0,1\}^n \to \{-1,+1\}$ with*

$$\begin{aligned} E(h_n,d) &\geqslant 1-2^{-\Omega(n)}, && d=1,2,\ldots,\lfloor cn\rfloor,\\ R(h_n,d) &\geqslant 1-2^{-\Omega(n/d)}, && d=1,2,\ldots,\lfloor cn\rfloor, \end{aligned}$$

where $c>0$ is an absolute constant.

Classic bounds for the approximation of the sign function imply that for any d, the lower bounds in Theorem 1.1 are essentially the best possible for any halfspace on n variables (see Sections 5.1 and 5.2 for details). Thus, the construction of Theorem 1.1 is the "hardest" halfspace from the point of view of approximation by polynomials and rational functions.

Theorem 1.1 is not a de-randomization of the existence proof in [77], which incidentally we are still unable to de-randomize. Rather, it is based on a new and simpler approach, presented in detail at the end of this section. Given the role that halfspaces play in theoretical computer science, we see Theorem 1.1 as answering a basic question of independent interest. In addition, Theorem 1.1 has applications to communication complexity and computational learning, which we now discuss.

1.2. Discrepancy vs. sign-rank. Consider the standard model of randomized communication [50], which features players Alice and Bob and a Boolean function $F\colon X\times Y \to \{-1,+1\}$. On input $(x,y)\in X\times Y$, Alice and Bob receive the arguments x and y, respectively. Their objective is to compute F on any given input with minimal communication. To this end, each player privately holds an unlimited supply of uniformly random bits which he or she can use in deciding what message to send at any given point in the protocol. The *cost* of a protocol is the total number of bits exchanged by Alice and Bob in a worst-case execution. The *ϵ-error randomized communication complexity of F*, denoted $R_\epsilon(F)$, is the least cost of a protocol that computes F with probability of error at most ϵ on every input.

Our interest in this paper is in communication protocols with error probability close to that of random guessing, $1/2$. There are two standard ways to define the complexity of a function F in this setting, both inspired by probabilistic polynomial time for Turing machines [31]:

$$\mathrm{UPP}(F) = \inf_{0\leqslant\epsilon<1/2} R_\epsilon(F)$$

and

$$\mathrm{PP}(F) = \inf_{0\leqslant\epsilon<1/2} \left\{ R_\epsilon(F) + \log_2\left(\frac{1}{\frac12-\epsilon}\right)\right\}.$$

The former quantity, introduced by Paturi and Simon [63], is called the communication complexity of F with *unbounded error*, in reference to the fact that the error probability can be arbitrarily close to 1/2. The latter quantity, proposed by Babai et al. [11], includes an additional penalty term that depends on the error probability. We refer to $\mathrm{PP}(F)$ as the communication complexity of F with *weakly unbounded error*. For all functions $F\colon \{0,1\}^n \times \{0,1\}^n \to \{-1,+1\}$, one has the trivial bounds $\mathrm{UPP}(F) \leqslant \mathrm{PP}(F) \leqslant n+2$. These two complexity measures give rise to corresponding *complexity classes* in communication complexity theory, defined in the seminal paper of Babai et al. [11]. Formally, UPP is the class of families $\{F_n\}_{n=1}^{\infty}$ of communication problems $F_n\colon \{0,1\}^n \times \{0,1\}^n \to \{-1,+1\}$ whose unbounded-error communication complexity is at most polylogarithmic in n. Its counterpart PP is defined analogously for the complexity measure PP.

These two models of large-error communication are synonymous with two central notions in communication complexity: *sign-rank* and *discrepancy*, defined formally in Sections 2.8 and 2.9. In more detail, Paturi and Simon [63] proved that the communication complexity of any problem with unbounded error is characterized up to an additive constant by the sign-rank of its communication matrix, $[F(x,y)]_{x,y}$. Analogously, Klauck [40, 41] showed that the communication complexity of any problem $F\colon \{0,1\}^n \times \{0,1\}^n \to \{-1,+1\}$ with weakly unbounded error is essentially characterized in terms of the discrepancy of F. Discrepancy and sign-rank enjoy a rich mathematical life [54, 71, 74, 56] outside communication complexity, which further motivates the study of PP and UPP as fundamental complexity classes.

Communication with weakly unbounded error is by definition no more powerful than unbounded-error communication, and for twenty years after the paper of Babai et al. [11] it was unknown whether this containment is proper. Buhrman et al. [22] and the author [71] answered this question in the affirmative, independently and with unrelated techniques. These papers exhibited functions $F\colon \{0,1\}^n \times \{0,1\}^n \to \{-1,+1\}$ with an exponential gap between communication complexity with unbounded error versus weakly unbounded error: $\mathrm{UPP}(F) = O(\log n)$ in both works, versus $\mathrm{PP}(F) = \Omega(n^{1/3})$ in [22] and $\mathrm{PP}(F) = \Omega(\sqrt{n})$ in [71]. In complexity-theoretic notation, these results show that $\mathsf{PP} \subsetneq \mathsf{UPP}$. A simpler alternate proof of the result of Buhrman et al. [22] was given in [75] using the pattern matrix method. More recently, Thaler [83] exhibited another, remarkably simple communication problem $F\colon \{0,1\}^n \times \{0,1\}^n \to \{-1,+1\}$, with communication complexity $\mathrm{UPP}(F) = O(\log n)$ and $\mathrm{PP}(F) = \Omega(n/\log n)^{2/5}$.

To summarize, the strongest explicit separation of communication complexity with unbounded versus weakly unbounded error prior to our work was the separation of $O(\log n)$ versus $\Omega(\sqrt{n})$ from twelve years ago [71]. The *existence* of a communication problem with a quadratically larger gap, of $O(\log n)$ versus $\Omega(n)$, follows from the work in [77]. This state of affairs parallels other instances in communication complexity, such as the P versus BPP question in multiparty communication [14], where the best existential separations are much stronger than the best explicit ones. There is considerable interest in communication complexity in explicit separations because they provide a deeper and more complete understanding of the complexity classes, whereas the lack of a strong explicit separation indicates a basic gap in our knowledge. As an application of Theorem 1.1, we obtain:

THEOREM 1.2. *There is a communication problem* $F_n\colon \{0,1\}^n\times\{0,1\}^n \to \{-1,+1\}$, *defined by*

$$F_n(x,y) = \operatorname{sgn}\left(w_0 + \sum_{i=1}^{n} w_i x_i y_i\right) \tag{1.2}$$

for some explicitly given reals $w_0, w_1, \ldots, w_n$, *such that*

$$\begin{aligned} \mathrm{UPP}(F_n) &\leqslant \log n + O(1), \\ \mathrm{PP}(F_n) &= \Omega(n). \end{aligned}$$

Moreover,

$$\begin{aligned} &\mathrm{rk}_\pm(F_n) \leqslant n+1, \\ &\mathrm{disc}(F_n) = 2^{-\Omega(n)}. \end{aligned}$$

Theorem 1.2 gives essentially the strongest possible separation of the communication classes PP and UPP, improving quadratically on previous constructions and matching the previous nonconstructive separation. Another compelling aspect of the theorem is the simple form (1.2) of the communication problem in question. The last two bounds in Theorem 1.2 state that F_n has sign-rank at most $n+1$ and discrepancy $2^{-\Omega(n)}$, which is essentially the strongest possible separation. The best previous construction [71] achieved sign-rank $O(n)$ and discrepancy $2^{-\Omega(\sqrt{n})}$.

We further generalize Theorem 1.2 to the *number-on-the-forehead k-party model*, the standard formalism of multiparty communication. Analogous to two-party communication, the k-party model has its own classes UPP_k and PP_k of problems solvable efficiently by protocols with unbounded error and weakly unbounded error, respectively. Their formal definitions can be found in Section 2.8. In this setting, we prove:

THEOREM 1.3. *There is a k-party communication problem* $F_n\colon (\{0,1\}^n)^k \to \{-1,+1\}$, *defined by*

$$F_n(x_1,x_2,\ldots,x_k) = \operatorname{sgn}\left(w_0 + \sum_{i=1}^{n} w_i x_{1,i} x_{2,i} \cdots x_{k,i}\right)$$

for some explicitly given reals $w_0, w_1, \ldots, w_n$, *such that*

$$\begin{aligned} \mathrm{UPP}(F_n) &\leqslant \log n + O(1), \\ \mathrm{PP}(F_n) &= \Omega\left(\frac{n}{4^k}\right), \\ \mathrm{disc}(F_n) &= \exp\left(-\Omega\left(\frac{n}{4^k}\right)\right). \end{aligned}$$

Theorem 1.3 gives essentially the strongest possible explicit separation of the k-party communication complexity classes UPP_k and PP_k for up to $k \leqslant (0.5-\epsilon)\log n$

parties, where $\epsilon > 0$ is an arbitrary constant. The previous best explicit separation [27, 80] of these classes was quadratically weaker, with communication complexity $\Omega(\sqrt{n}/4^k)$ for unbounded error and $O(\log n)$ for weakly unbounded error. The communication lower bound in Theorem 1.3 reflects the state of the art in the area, in that the strongest lower bound for any explicit communication problem $F\colon (\{0,1\}^n)^k \to \{-1,+1\}$ to date is $\Omega(n/2^k)$ due to Babai et al. [12].

1.3. Computational learning. A *sign-representing polynomial* for a given function $f\colon \{0,1\}^n \to \{-1,+1\}$ is any real polynomial p such that $f(x) = \operatorname{sgn} p(x)$ for all x. The minimum degree of a sign-representing polynomial for f is called the *threshold degree* of f, denoted $\deg_\pm(f)$. Clearly $0 \leqslant \deg_\pm(f) \leqslant n$ for every Boolean function f on n variables. The reader can further verify that sign-representation is equivalent to pointwise approximation with error strictly less than, but arbitrarily close to, the trivial error of 1. Sign-representing polynomials are appealing from a learning standpoint because they immediately lead to efficient learning algorithms. Indeed, any function of threshold degree d is by definition a linear combination of $N = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d}$ monomials and can thus be viewed as a halfspace in N dimensions. As a result, f can be PAC learned [86] under arbitrary distributions in time polynomial in N, using a variety of halfspace learning algorithms.

The study of sign-representing polynomials started fifty years ago with the seminal monograph of Minsky and Papert [57], who examined the threshold degree of several common functions. Since then, the threshold degree approach has yielded the fastest known PAC learning algorithms for notoriously hard concept classes, including DNF formulas [45] and AND-OR trees [8]. Conspicuously absent from this list of success stories is the concept class of *intersections of halfspaces*. While solutions are known to several restrictions of this learning problem [18, 51, 87, 9, 44, 46, 43], no algorithm has been discovered for PAC learning the intersection of even two halfspaces in time faster than $2^{\Theta(n)}$. Known hardness results, on the other hand, only apply to polynomially many halfspaces or to proper learning, e.g., [19, 3, 47, 39].

This state of affairs has motivated a quest to determine the threshold degree of the intersection of two halfspaces [57, 61, 42, 76, 77]. Prior to our work, the best lower bound was $\Omega(\sqrt{n})$ for an explicit intersection of two halfspaces [76], complemented by a tight but highly nonconstructive $\Omega(n)$ lower bound [77]. Using Theorem 1.1, we prove:

THEOREM 1.4. *There is an (explicitly given) halfspace $h_n\colon \{0,1\}^n \to \{-1,+1\}$ such that*

$$\deg_\pm(h_n \wedge h_n) = \Omega(n).$$

The symbol $h_n \wedge h_n$ above stands for the intersection of two copies of h_n on disjoint sets of variables. In other words, Theorem 1.4 constructs an explicit intersection of two halfspaces whose threshold degree is asymptotically maximal, $\Omega(n)$. While the nonconstructive $\Omega(n)$ lower bound of [77] already ruled out the threshold degree approach as a way to learn intersections of halfspaces, we see Theorem 1.4 as contributing a key qualitative piece of the puzzle. Specifically, it constructs a small and simple family of intersections of two halfspaces that are off-limits to all known algorithmic approaches (namely, the family obtained by applying $h_n \wedge h_n$ to different subsets of the variables $x_1, x_2, \ldots, x_{4n}$).

1.4. Proof overview. Our solution has two main components: the construction of a sparse set of integers that appear random modulo m, and the univariatization of a multivariate Boolean function. We describe each of these components in detail.

Discrepancy of integer sets. Let $m \geqslant 2$ be a given integer. Key to our work is the notion of *m-discrepancy*, which quantifies the pseudorandomness or aperiodicity modulo m of any given multiset of integers. It is largely unrelated to the notion of discrepancy in communication complexity (Section 1.2). Formally, the m-discrepancy of a nonempty multiset $Z = \{z_1, z_2, \ldots, z_n\}$ is defined as

$$\operatorname{disc}(Z, m) = \max_{k=1,2,\ldots,m-1} \left| \frac{1}{n} \sum_{j=1}^{n} \omega^{k z_j} \right|,$$

where ω is a primitive m-th root of unity. This fundamental quantity arises in combinatorics and theoretical computer science, e.g., [30, 69, 2, 38, 64, 5]. The identity $1 + \omega + \omega^2 + \cdots + \omega^{m-1} = 0$ for any m-th root of unity $\omega \neq 1$ implies that the set $Z = \{0, 1, 2, \ldots, m-1\}$ achieves the smallest possible m-discrepancy: $\operatorname{disc}(Z, m) = 0$. Much sparser sets with small m-discrepancy can be shown to exist using the probabilistic method (Fact 3.3 and Corollary 3.4). Specifically, one easily verifies for any constant $\epsilon > 0$ the existence of a set $Z \subseteq \{0, 1, 2, \ldots, m-1\}$ with m-discrepancy at most ϵ and cardinality $O(\log m)$, an exponential improvement in sparsity compared to the trivial set $\{0, 1, 2, \ldots, m-1\}$. We are aware of two efficient constructions of sparse sets with small m-discrepancy, due to Ajtai et al. [2] and Katz [38]. The approach of Ajtai et al. is elementary except for an appeal to the prime number theorem, whereas Katz's construction relies on deep results in number theory. Neither work appears to directly imply the kind of optimal de-randomization that we require, namely, an algorithm that runs in time polynomial in $\log m$ and produces a multiset of cardinality $O(\log m)$ with m-discrepancy bounded away from 1. We obtain such an algorithm by adapting the approach of Ajtai et al. [2].

The centerpiece of the construction of Ajtai et al. [2] is what the authors call the *iteration lemma*, stated in this paper as Theorem 3.6. Its role is to reduce the construction of a sparse set with small m-discrepancy to the construction of sparse sets with small p-discrepancy, for primes $p \ll m$. Ajtai et al. [2] proved their iteration lemma for m prime, but we show that their argument readily generalizes to arbitrary moduli m. By applying the iteration lemma in a recursive manner, one reaches smaller and smaller primes. The authors of [2] continue this recursive process until they reach primes p so small that the trivial construction $\{0, 1, 2, \ldots, p-1\}$ can be considered sparse. We proceed differently and terminate the recursion after just two stages, at which point the input size is small enough for brute force search based on the probabilistic method. The final set that we construct has size logarithmic in m and m-discrepancy a small constant, as opposed to the superlogarithmic size and $o(1)$ discrepancy in the work of Ajtai et al. [2].

We note that this modified approach additionally gives the first explicit circulant expander on n vertices of degree $O(\log n)$, which is optimal and improves on the previous best degree bound of $(\log^* n)^{O(\log^* n)} \cdot O(\log n)$ due to Ajtai et al. [2]. Background on circulant expanders, and the details of our expander construction, can be found in Section 5.6.

Univariatization. We now describe the second major component of our proof. Consider a halfspace $h_n(x) = \operatorname{sgn}(\sum z_i x_i - \theta)$ in Boolean variables $x_1, x_2, \ldots, x_n$, where the coefficients can be assumed without loss of generality to be integers. Then the linear form $\sum z_i x_i - \theta$ ranges in the discrete set $\{\pm 1, \pm 2, \ldots, \pm N\}$, for some integer N proportionate to the magnitude of the coefficients. As a result, one can approximate h_n to any given error ϵ by approximating the sign function to ϵ on $\{\pm 1, \pm 2, \ldots, \pm N\}$. This approach works for both rational approximation and polynomial approximation. We think of it as the *black-box* approach to the approximation of h_n because it uses the linear form $\sum z_i x_i - \theta$ rather than the individual bits. There is no reason to expect that the black-box construction is anywhere close to optimal. Indeed, there are halfspaces [76, Section 1.3] that can be approximated to arbitrarily small error by a rational function of degree 1 but require a black-box approximant of degree $\Omega(n)$. Surprisingly, we are able to construct a halfspace h_n with exponentially large coefficients for which the black-box approximant is essentially optimal. As a result, tight lower bounds for the rational and polynomial approximation of h_n follow immediately from the univariate lower bounds for approximating the sign function on $\{\pm 1, \pm 2, \pm 3, \ldots, \pm 2^{\Theta(n)}\}$. The role of h_n is to reduce the multivariate problem taken up in this work to a well-understood univariate question, hence the term *univariatization*.

The construction of h_n involves several steps. First, we study the probability distribution of the weighted sum $z_1 X_1 + z_2 X_2 + \cdots + z_n X_n$ modulo m, where $z_1, z_2, \ldots, z_n$ are given integers and the bits $X_1, X_2, \ldots, X_n \in \{0, 1\}$ are chosen uniformly at random. We show that the distribution is exponentially close to uniform whenever the multiset $\{z_1, z_2, \ldots, z_n\}$ has m-discrepancy bounded away from 1. For the next step, fix any multiset $\{z_1, z_2, \ldots, z_n\}$ with small m-discrepancy and consider the linear map $L\colon \{0,1\}^n \to \mathbb{Z}_m$ given by $L(x) = \sum z_i x_i$. At this point in the proof, we know that for uniformly random $X \in \{0,1\}^n$, the probability distribution of $L(X)$ is exponentially close to uniform. This implies that the characteristic functions of $L^{-1}(0), L^{-1}(1), \ldots, L^{-1}(m-1)$ have approximately the same Fourier spectrum up to degree cn, for some constant $c > 0$. We substantially strengthen this conclusion by proving that there are probability distributions $\mu_0, \mu_1, \ldots, \mu_{m-1}$, supported on $L^{-1}(0), L^{-1}(1), \ldots, L^{-1}(m-1)$, respectively, such that the Fourier spectra of $\mu_0, \mu_1, \ldots, \mu_{m-1}$ are *exactly* the same up to degree cn. Our proof relies on a general tool from [77, Theorem 4.1], proved there using the Gershgorin circle theorem.

As our final step, we use $\mu_0, \mu_1, \ldots, \mu_{m-1}$ to construct a halfspace in terms of $z_1, z_2, \ldots, z_n$ whose approximation by rational functions and polynomials gives corresponding approximants for the sign function on the discrete set $\{\pm 1, \pm 2, \ldots, \pm m\}$. More generally, for any tuple $z_1, z_2, \ldots, z_n$, we define an associated halfspace and prove a lower bound on m in terms of the discrepancy of the multiset $\{z_1, z_2, \ldots, z_n\}$. Combining this result with the efficient construction of an integer set with small m-discrepancy for $m = 2^{\Theta(n)}$, we obtain an explicit halfspace $h_n\colon \{0,1\}^n \to \{-1, +1\}$ whose approximation by polynomials and rational functions is equivalent to the univariate approximation of the sign function on $\{\pm 1, \pm 2, \pm 3, \ldots, \pm 2^{\Theta(n)}\}$. Theorem 1.1 now follows by appealing to known lower bounds for the polynomial and rational approximation of the sign function. To obtain the exponential separation of communication complexity with unbounded versus weakly unbounded error (Theorem 1.2), we use the *pattern matrix method* [73, 75] to "lift" the lower bound of Theorem 1.1 to a discrepancy bound. Finally, our result on the threshold degree of the intersection of two halfspaces (Theorem 1.4) works by combining the rational approximation lower bound of Theorem 1.1 with a structural result from [76] on the sign-representation of arbitrary functions of the form $f \wedge f$.

A key technical contribution of this paper is the identification of m-discrepancy as a pseudorandom property that is weak enough to admit efficient de-randomization and strong enough to allow the univariatization of the corresponding halfspace. The previous, existential result in [77] used a completely different and more complicated pseudorandom property based on affine shifts of the Fourier transform on $\{0,1\}^n$, which we have not been able to de-randomize. Apart from the construction of a low-discrepancy set, our proof is simpler and more intuitive than the existential proof in [77].

2. Preliminaries

We start with a review of the technical preliminaries. The purpose of this section is to make the paper as self-contained as possible, and comfortably readable by a broad audience. The expert reader should therefore skim this section for notation or skip it altogether.

2.1. Notation.

There are two common arithmetic encodings for the Boolean values: the traditional encoding *false* ↔ 0, *true* ↔ 1, and the Fourier-motivated encoding *false* ↔ 1, *true* ↔ −1. Throughout this manuscript, we use the former encoding for the domain of a Boolean function and the latter for the range. With this convention, Boolean functions are mappings $\{0,1\}^n \to \{-1,+1\}$ for some n. For Boolean functions $f\colon \{0,1\}^n \to \{-1,+1\}$ and $g\colon \{0,1\}^m \to \{-1,+1\}$, we let $f \circ g$ denote the coordinatewise composition of f with g. Formally, $f \circ g\colon (\{0,1\}^m)^n \to \{-1,+1\}$ is given by

$$(f \circ g)(x_1, x_2, \ldots, x_n) = f\left(\frac{1-g(x_1)}{2}, \frac{1-g(x_2)}{2}, \ldots, \frac{1-g(x_n)}{2}\right), \qquad (2.1)$$

where the linear map on the right-hand side serves the purpose of switching between the distinct arithmetizations for the domain versus range. A *partial function* f on a set X is a function whose domain of definition, denoted $\operatorname{dom} f$, is a nonempty proper subset of X. We generalize coordinatewise composition $f \circ g$ to partial Boolean functions f and g in the natural way. Specifically, $f \circ g$ is the Boolean function given by (2.1), with domain the set of all inputs $(\ldots, x_i, \ldots) \in (\operatorname{dom} g)^n$ for which $(\ldots, (1-g(x_i))/2, \ldots) \in \operatorname{dom} f$.

We use the following two versions of the sign function:

$$\operatorname{sgn} x = \begin{cases} -1 & \text{if } x < 0, \\ 0 & \text{if } x = 0, \\ 1 & \text{if } x > 0, \end{cases} \qquad \widetilde{\operatorname{sgn}}\, x = \begin{cases} -1 & \text{if } x < 0, \\ 1 & \text{if } x \geqslant 0. \end{cases}$$

For a subset $\mathscr{X} \subseteq \mathbb{R}$, we let $\operatorname{sgn}|_{\mathscr{X}}$ denote the restriction of the sign function to $\mathscr{X}$. A *halfspace* for us is any Boolean function $h\colon \{0,1\}^n \to \{-1,+1\}$ given by

$$h(x) = \operatorname{sgn}\left(\sum_{i=1}^n w_i x_i - \theta\right)$$

for some reals $w_1, w_2, \ldots, w_n, \theta$. The *majority function* $\mathrm{MAJ}_n\colon \{0,1\}^n \to \{-1,+1\}$ is the halfspace defined by

$$\begin{aligned}\mathrm{MAJ}_n(x) &= -\operatorname{sgn}\left(\sum_{i=1}^n x_i - \frac{n}{2} - \frac{1}{4}\right)\\ &= \begin{cases} -1 & \text{if } x_1 + x_2 + \cdots + x_n > n/2,\\ 1 & \text{otherwise.}\end{cases}\end{aligned}$$

Some authors define MAJ_n only for n odd, in which case the tiebreaker term $1/4$ can be omitted.

The complement and the power set of a set S are denoted as usual by $\overline{S}$ and $\mathscr{P}(S)$, respectively. The symmetric difference of sets S and T is $S \oplus T = (S \cap \overline{T}) \cup (\overline{S} \cap T)$. Throughout this manuscript, we use brace notation as in $\{z_1, z_2, \ldots, z_n\}$ to specify *multisets* rather than sets. The *cardinality* $|Z|$ of a finite multiset Z is defined as the total number of element occurrences in Z, with each element counted as many times as it occurs. The equality and subset relations on multisets are defined analogously, with the number of element occurrences taken into account. For example, $\{1,1,2\} = \{1,2,1\}$ but $\{1,1,2\} \neq \{1,2\}$. Similarly, $\{1,2\} \subseteq \{1,1,2\}$ but $\{1,1,2\} \not\subseteq \{1,2\}$.

The infinity norm of a function $f\colon \mathscr{X} \to \mathbb{R}$ is denoted $\|f\|_\infty = \sup_{x\in\mathscr{X}} |f(x)|$. For real-valued functions f and g and a nonempty finite subset $\mathscr{X}$ of their domain, we write

$$\langle f, g\rangle_{\mathscr{X}} = \frac{1}{|\mathscr{X}|} \sum_{x \in \mathscr{X}} f(x) g(x).$$

We will often use this notation with $\mathscr{X}$ a nonempty *proper* subset of the domain of f and g. We let $\ln x$ and $\log x$ stand for the natural logarithm of x and the logarithm of x to base 2, respectively. The binary entropy function $H\colon [0,1] \to [0,1]$ is given by $H(p) = -p\log p - (1-p)\log(1-p)$ and is strictly increasing on $[0, 1/2]$. The following bound is well known [35, p. 283]:

$$\sum_{i=0}^k \binom{n}{i} \leqslant 2^{H(k/n)n}, \qquad\qquad k = 0, 1, 2, \ldots, \left\lfloor \frac{n}{2} \right\rfloor. \tag{2.2}$$

For a complex number x, we denote the real part, imaginary part, and complex conjugate of x as usual by $\mathrm{Re}(x)$, $\mathrm{Im}(x)$, and $\overline{x}$, respectively. We typeset the imaginary unit $\mathbf{i}$ in boldface to distinguish it from the index variable i.

For an arbitrary integer a and a positive integer m, recall that $a \bmod m$ denotes the unique element of $\{0, 1, 2, \ldots, m-1\}$ that is congruent to a modulo m. For an integer $m \geqslant 2$, the symbols $\mathbb{Z}_m$ and $\mathbb{Z}_m^*$ refer to the ring of integers modulo m and the multiplicative group of integers modulo m, respectively. For a multiset $Z = \{z_1, z_2, \ldots, z_n\}$ of integers, we adopt the standard notation

$$-Z = \{-z_1, \ldots, -z_n\}, \tag{2.3}$$
$$aZ = \{az_1, \ldots, az_n\}, \tag{2.4}$$
$$Z + b = \{z_1 + b, \ldots, z_n + b\}, \tag{2.5}$$
$$Z \bmod m = \{z_1 \bmod m, \ldots, z_n \bmod m\}. \tag{2.6}$$

Note that the multisets in (2.3)–(2.6) each have cardinality n, the same as the original set Z. We often use these shorthands in combination, as in $(aZ + b) \bmod m = \{(az_1 + b) \bmod m, \ldots, (az_n + b) \bmod m\}$.

For a logical condition C, we use the Iverson bracket

$$\mathbf{I}[C] = \begin{cases} 1 & \text{if } C \text{ holds,} \\ 0 & \text{otherwise.} \end{cases}$$

The following concentration inequality, due to Hoeffding [34], is well-known.

Fact 2.1 (Hoeffding's Inequality). *Let $X_1, X_2, \ldots, X_n$ be independent random variables with $X_i \in [a_i, b_i]$. Let*

$$p = \sum_{i=1}^{n} \mathbf{E}\, X_i.$$

Then

$$\mathbf{P}\left[\left|\sum_{i=1}^{n} X_i - p\right| \geqslant \delta\right] \leqslant 2\exp\left(-\frac{2\delta^2}{\sum_{i=1}^{n}(b_i - a_i)^2}\right).$$

In Fact 2.1 and throughout this paper, we typeset random variables using capital letters.

2.2. Number-theoretic preliminaries. For positive integers a and b that are relatively prime, $(a^{-1})_b \in \{1, 2, \ldots, b-1\}$ denotes the multiplicative inverse of a modulo b. The following fact is well-known and straightforward to verify; cf. [2].

Fact 2.2. *For any positive integers a and b that are relatively prime,*

$$\frac{(a^{-1})_b}{b} + \frac{(b^{-1})_a}{a} - \frac{1}{ab} \in \mathbb{Z}. \tag{2.7}$$

Proof. We have $a(a^{-1})_b + b(b^{-1})_a \equiv b(b^{-1})_a \equiv 1 \pmod{a}$, and analogously $a(a^{-1})_b + b(b^{-1})_a \equiv a(a^{-1})_b \equiv 1 \pmod{b}$. Thus, $a(a^{-1})_b + b(b^{-1})_a - 1$ is divisible by both a and b. Since a and b are relatively prime, we conclude that $a(a^{-1})_b + b(b^{-1})_a - 1$ is divisible by ab, which is equivalent to (2.7). ∎

Recall that the *prime counting function* $\pi(x)$ for a real argument $x \geqslant 0$ evaluates to the number of prime numbers less than or equal to x. In what follows, it will be clear from the context whether π refers to $3.14159\ldots$ or the prime counting function. The asymptotic growth of the latter is given by the *prime number theorem*, which states that $\pi(n) \sim n/\ln n$. Many explicit bounds on $\pi(n)$ are known, such as the following theorem of Rosser [68].

FACT 2.3 (Rosser). *For $n \geqslant 55$,*

$$\frac{n}{\ln n + 2} < \pi(n) < \frac{n}{\ln n - 4}.$$

The number of distinct prime divisors of a natural number n is denoted $\nu(n)$. We will need the following first-principles bound on $\nu(n)$, which is asymptotically tight for infinitely many n.

FACT 2.4. *The number of distinct prime divisors of n obeys*

$$(\nu(n)+1)! \leqslant n. \tag{2.8}$$

In particular,

$$\nu(n) \leqslant (1+o(1))\frac{\ln n}{\ln \ln n}. \tag{2.9}$$

Proof. An integer $n \geqslant 1$ has by definition $\nu(n)$ distinct prime divisors. Letting p_k denote the k-th prime, we have

$$\begin{aligned}\ln n &\geqslant \ln p_1 p_2 \ldots p_{\nu(n)}\\ &\geqslant \sum_{k=1}^{\nu(n)} \ln(k+1)\\ &\geqslant \int_1^{\nu(n)} \ln x \, dx\\ &= \nu(n)\ln\nu(n) - \nu(n) + 1,\end{aligned}$$

where the second step uses the trivial estimate $p_k \geqslant k+1$. The second step in this derivation settles (2.8), whereas the last step settles (2.9). ∎

2.3. Matrix analysis. For an arbitrary set X such as $X = \mathbb{C}$ or $X = \{-1, 1\}$, the symbol $X^{n\times m}$ denotes the family of $n \times m$ matrices with entries in X. The symbols I_n and $J_{n,m}$ stand for the order-n identity matrix and the $n \times m$ matrix of all ones, respectively. When the dimensions of the matrix are clear from the context, we omit the subscripts and write simply I or J. The shorthand $\operatorname{diag}(d_1, d_2, \ldots, d_n)$ refers to the diagonal matrix with entries $d_1, d_2, \ldots, d_n$ on the diagonal:

$$\operatorname{diag}(d_1, d_2, \ldots, d_n) = \begin{bmatrix} d_1 & 0 & \cdots & 0\\ 0 & d_2 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & d_n\end{bmatrix}.$$

For a matrix $M = [M_{i,j}]$, recall that its complex conjugate is given by $\overline{M} = [\overline{M_{i,j}}]$. The transpose and conjugate transpose of M are denoted M^T and $M^* = \overline{M}^T$, respectively. The conjugation, transpose, and conjugate transpose operations apply as a special case to vectors, which we view as matrices with a single column. We use the familiar matrix norms $\|M\|_\infty = \max|M_{ij}|$ and $\|M\|_1 = \sum|M_{ij}|$. Again, these definitions carry over to vectors as a special case. A matrix $M \in \mathbb{C}^{n\times n}$ is called *unitary* if $MM^* = M^*M = I$.

A *circulant matrix* is any matrix $C \in \mathbb{C}^{m\times m}$ of the form

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{m-2} & c_{m-1} \\ c_{m-1} & c_0 & c_1 & \cdots & c_{m-3} & c_{m-2} \\ c_{m-2} & c_{m-1} & c_0 & \cdots & c_{m-4} & c_{m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_2 & c_3 & c_4 & \cdots & c_0 & c_1 \\ c_1 & c_2 & c_3 & \cdots & c_{m-1} & c_0 \end{bmatrix} \tag{2.10}$$

for some $c_0, c_1, \ldots, c_{m-1} \in \mathbb{C}$. Thus, every row of C is obtained by a circular shift of the previous row one entry to the right. We let $\operatorname{circ}(c_0, c_1, \ldots, c_{m-1})$ denote the right-hand side of (2.10). In this notation, $\operatorname{circ}(1, 0, \ldots, 0) = I$ and $\operatorname{circ}(1, 1, \ldots, 1) = J$. The eigenvalues and eigenvectors of a circulant matrix are well-known and straightforward to determine. For the reader's convenience, we include the short derivation below in Fact 2.5 and Corollary 2.6.

FACT 2.5. *Let $C = \operatorname{circ}(c_0, c_1, \ldots, c_{m-1})$ be a circulant matrix. Then for every m-th root of unity ω, the vector*

$$\begin{bmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{m-1} \end{bmatrix} \tag{2.11}$$

is an eigenvector of C with eigenvalue $\sum_{j=0}^{m-1} c_j\omega^j$.

Proof. Let v denote the vector in (2.11). Then for $k = 1, 2, 3, \ldots, m$,

$$\begin{aligned}(Cv)_k &= \sum_{j=0}^{m-1} c_{(j-k+1) \bmod m}\, \omega^j \\ &= \left(\sum_{j=0}^{m-1} c_{(j-k+1) \bmod m}\, \omega^{j-k+1}\right) v_k \\ &= \left(\sum_{j=0}^{m-1} c_{(j-k+1) \bmod m}\, \omega^{(j-k+1) \bmod m}\right) v_k \\ &= \left(\sum_{j=0}^{m-1} c_j\omega^j\right) v_k,\end{aligned}$$

where the third step uses $\omega^m = 1$. ∎

As a corollary to Fact 2.5, one recovers the full complement of eigenvalues for any circulant matrix C and furthermore learns that C is unitarily similar to a diagonal matrix. In the statement below, recall that a *primitive m-th root of unity* is any generator, such as $\exp(2\pi\mathbf{i}/m)$, for the multiplicative group of the roots of $x^m - 1 \in \mathbb{Q}[x]$.

Corollary 2.6. *Let $C = \operatorname{circ}(c_0, c_1, \ldots, c_{m-1})$ be a circulant matrix. Let ω be a primitive m-th root of unity. Then the matrix*

$$W = [\omega^{jk}/\sqrt{m}]_{j,k=0,1,\ldots,m-1}$$

is unitary and satisfies

$$W^*CW = \operatorname{diag}\left(\sum_{j=0}^{m-1} c_j, \sum_{j=0}^{m-1} c_j\omega^j, \sum_{j=0}^{m-1} c_j\omega^{2j}, \ldots, \sum_{j=0}^{m-1} c_j\omega^{(m-1)j}\right). \tag{2.12}$$

In particular, the eigenvalues of C, counting multiplicities, are

$$\sum_{j=0}^{m-1} c_j\omega^{kj}, \qquad k = 0, 1, 2, \ldots, m-1.$$

Proof. For $k, k' = 0, 1, \ldots, m-1$, we have

$$\begin{aligned}\sum_{j=0}^{m-1} \frac{\omega^{jk}}{\sqrt{m}} \cdot \frac{\overline{\omega^{jk'}}}{\sqrt{m}} &= \frac{1}{m}\sum_{j=0}^{m-1} \omega^{j(k-k')} \\ &= \begin{cases} 1 & \text{if } k = k', \\ 0 & \text{otherwise,} \end{cases}\end{aligned}$$

where the second step is valid because ω is primitive and in particular $\omega^k \neq \omega^{k'}$. We conclude that

$$WW^* = W^*W = I. \tag{2.13}$$

Fact 2.5 implies that

$$CW = W \operatorname{diag}\left(\sum_{j=0}^{m-1} c_j, \sum_{j=0}^{m-1} c_j\omega^j, \sum_{j=0}^{m-1} c_j\omega^{2j}, \ldots, \sum_{j=0}^{m-1} c_j\omega^{(m-1)j}\right),$$

which in light of (2.13) is equivalent to (2.12). ∎

2.4. Polynomial approximation. Recall that the *total degree* of a multivariate real polynomial $p\colon \mathbb{R}^n \to \mathbb{R}$, denoted $\deg p$, is the largest degree of any monomial of p. We use the terms "degree" and "total degree" interchangeably in this paper. Let $f\colon \mathscr{X} \to \mathbb{R}$ be a given function with domain $\mathscr{X} \subseteq \mathbb{R}^n$. For any $d \geqslant 0$, define

$$E(f,d) = \inf_p \|f - p\|_\infty,$$

where the infimum is over real polynomials p of degree at most d. In words, $E(f,d)$ is the least error in a pointwise approximation of f by a polynomial of degree no greater than d. The *ϵ-approximate degree of f* is the minimum degree of a polynomial p that approximates f pointwise within ϵ:

$$\|f - p\|_\infty \leqslant \epsilon.$$

In this overview, we focus on the polynomial approximation of the sign function. We start with an elementary construction of an approximant due to Buhrman et al. [21].

FACT 2.7 (Buhrman et al.). *For any $N > 1$ and $0 < \epsilon < 1$, the sign function can be approximated on $[-N,-1] \cup [1,N]$ pointwise to within ϵ by a polynomial of degree*

$$O\left(N^2 \log \frac{2}{\epsilon}\right).$$

The degree upper bound in Fact 2.7 is not tight. Indeed, a quadratically stronger bound of $O(N \log(2/\epsilon))$ follows in a straightforward manner from Jackson's theorem in approximation theory [67, Theorem 1.4]. Our applications do not benefit from this improvement, however, and we opt for the construction of Buhrman et al. [21] because of its striking simplicity. For the reader's convenience, we provide their short proof below.

Proof (adapted from Buhrman et al.) For a positive integer d, consider the degree-d univariate polynomial

$$B_d(t) = \sum_{i=\lceil d/2 \rceil}^{d} \binom{d}{i} t^i (1-t)^{d-i}.$$

In words, $B_d(t)$ is the probability of observing at least as many heads as tails in a sequence of d independent coin flips, each coming up heads with probability t. By Hoeffding's inequality (Fact 2.1) for sufficiently large $d = O(N^2 \log(2/\epsilon))$, the polynomial B_d sends $[0, \frac{1}{2} - \frac{1}{2N}] \to [0, \frac{\epsilon}{2}]$ and similarly $[\frac{1}{2} + \frac{1}{2N}, 1] \to [1 - \frac{\epsilon}{2}, 1]$. As a result, the shifted and scaled polynomial $2B_d\left(\frac{1}{2N} \cdot t + \frac{1}{2}\right) - 1$ approximates the sign function pointwise on $[-N,-1] \cup [1,N]$ within ϵ. ∎

On the lower bounds side, Paturi proved that low-degree polynomials cannot approximate the majority function well. He in fact obtained analogous results for all symmetric functions, but the special case of majority will be sufficient for our purposes.

Theorem 2.8 (Paturi). *For some constant $c > 0$ and all integers $n \geqslant 1$,*

$$E(\mathrm{MAJ}_n, cn) \geqslant \frac{1}{3}.$$

The constant $1/3$ in Paturi's theorem can be replaced by any other in $(0,1)$. His result is of interest to us because along with Fact 2.7, it implies a lower bound for the approximation of the sign function on the discrete set of points $\{\pm 1, \pm 2, \ldots, \pm N\}$ for any N.

Proposition 2.9. *For all positive integers N and d,*

$$E(\operatorname{sgn}|_{\{\pm 1, \pm 2, \ldots, \pm N\}}, d) \geqslant 1 - O\left(\frac{d}{N}\right)^{1/2}.$$

Proof. Abbreviate $\epsilon = E(\operatorname{sgn}|_{\{\pm 1, \pm 2, \ldots, \pm N\}}, d)$ and fix a polynomial p of degree at most d that approximates the sign function on $\{\pm 1, \pm 2, \ldots, \pm N\}$ within ϵ. Fact 2.7 gives a polynomial s of degree $O(1/(1-\epsilon)^2)$ that sends $[-1-\epsilon, -1+\epsilon] \to [-4/3, -2/3]$ and $[1-\epsilon, 1+\epsilon] \to [2/3, 4/3]$. Then the composition of these two approximants obeys

$$\max_{t = \pm 1, \pm 2, \ldots, \pm N} |\operatorname{sgn}(t) - s(p(t))| \leqslant \frac{1}{3}.$$

This in turn gives an approximant for the majority function on $n = \lfloor (N-1)/2 \rfloor$ bits:

$$\begin{aligned}
&\max_{x \in \{0,1\}^n} \left| \mathrm{MAJ}_n(x) - s\left(p\left(2\sum_{j=1}^n (-1)^{x_j} + 1\right)\right)\right| \\
&\qquad = \max_{x \in \{0,1\}^n} \left| \operatorname{sgn}\left(2\sum_{j=1}^n (-1)^{x_j} + 1\right) - s\left(p\left(2\sum_{j=1}^n (-1)^{x_j} + 1\right)\right)\right| \\
&\qquad \leqslant \max_{t = \pm 1, \pm 2, \ldots, \pm N} |\operatorname{sgn}(t) - s(p(t))| \\
&\qquad \leqslant \frac{1}{3}.
\end{aligned}$$

In view of Paturi's lower bound for the majority function (Theorem 2.8), the approximant $s(p(2\sum(-1)^{x_j} + 1))$ must have degree $\Omega(n) = \Omega(N)$. But this composition is a polynomial in $x \in \{0,1\}^n$ of degree $\deg s \cdot \deg p = O(d/(1-\epsilon)^2)$. We conclude that $d/(1-\epsilon)^2 \geqslant \Omega(N)$, whence $\epsilon \geqslant 1 - O(d/N)^{1/2}$. □

2.5. Rational approximation. Consider a rational function $r(x) = p(x)/q(x)$, where p and q are polynomials on $\mathbb{R}^n$. We refer to the degrees of p and q as the *numerator degree* and *denominator degree*, respectively, of r. The *degree* of r is, then, the maximum of the numerator and denominator degrees. For a function $f\colon X \to \mathbb{R}$ with domain $X \subseteq \mathbb{R}^n$, we define

$$R(f, d_0, d_1) = \inf_{p,q} \sup_{x \in X} \left| f(x) - \frac{p(x)}{q(x)} \right|, \tag{2.14}$$

where the infimum is over multivariate polynomials p and q of degree at most d_0 and d_1, respectively, such that q does not vanish on X. In words, $R(f, d_0, d_1)$ is the least error in an approximation of f by a multivariate rational function with numerator degree and denominator degree at most d_0 and d_1, respectively. We will be mostly working with $R(f, d_0, d_1)$ in the regimes $d_0 = d_1$ and $d_0 \gg d_1$. In the former regime, we use the shorthand

$$R(f, d) = R(f, d, d).$$

As a limiting case of the latter regime, we have

$$E(f, d) = R(f, d, 0).$$

The study of the rational approximation of the sign function dates back to the seminal work by Zolotarev [89] in the 1870s. The problem was revisited almost a century later by Newman [60], who proved the following result.

Fact 2.10 (Newman). *For any $N > 1$ and any integer $d \geqslant 1$,*

$$R(\operatorname{sgn}|_{[-N,-1]\cup[1,N]}, d) \leqslant 1 - \frac{1}{N^{1/d}}.$$

For a recent exposition of Newman's construction, we refer the reader to [76, Theorem 2.4]. As an important special case, Newman's work gives upper bounds for the rational approximation of the sign function on the discrete set $\{\pm1, \pm2, \ldots, \pm N\}$. Newman's upper bounds were sharpened and complemented with matching lower bounds in [76, Eq. (2.2) and Theorem 5.1], to the following effect.

Theorem 2.11 (Sherstov). *For any positive integers N and d,*

$$R(\operatorname{sgn}|_{\{\pm1,\pm2,\ldots,\pm N\}}, d) = \begin{cases} 1 - N^{-\Theta(1/d)} & \text{if } 1 \leqslant d \leqslant \log N, \\ 2^{-\Theta(d/\log(N/d))} & \text{if } \log N < d < N/2. \end{cases}$$

Among other things, Theorem 2.11 implies the following result on the rational approximation of the majority function [76, Eq. (2.2) and Theorems 5.1, 5.9].

Theorem 2.12 (Sherstov). *For any positive integers n and d,*

$$R(\mathrm{MAJ}_n, d) = \begin{cases} 1 - n^{-\Theta(1/d)} & \text{if } 1 \leqslant d \leqslant \log n, \\ 2^{-\Theta(d/\log(n/d))} & \text{if } \log n \leqslant d < \lfloor n/4 \rfloor. \end{cases}$$

2.6. Sign-representation. Let $f\colon X \to \{-1, +1\}$ be a given function, where $X \subset \mathbb{R}^n$ is finite. The *threshold degree* of f, denoted $\deg_\pm(f)$, is the least degree of a polynomial $p(x)$ such that $f(x) \equiv \operatorname{sgn} p(x)$. For functions $f\colon X \to \{-1, +1\}$ and $g\colon Y \to \{-1, +1\}$, we let the symbol $f \wedge g$ stand for the function $X \times Y \to \{-1, +1\}$ given by $(f \wedge g)(x, y) = f(x) \wedge g(y)$. Note that in this notation, f and $f \wedge f$ are completely different functions, the former having domain X and the latter $X \times X$. The following ingenious observation, due to Beigel et al. [17], relates the notions of sign-representation and rational approximation for conjunctions of Boolean functions.

THEOREM 2.13 (Beigel et al.). *Let $f\colon X \to \{-1,+1\}$ and $g\colon Y \to \{-1,+1\}$ be given functions, where $X, Y \subseteq \mathbb{R}^n$. Let d be any integer with*

$$R(f,d) + R(g,d) < 1.$$

Then

$$\deg_\pm(f \wedge g) \leqslant 4d.$$

Proof (adapted from Beigel et al.). Fix arbitrary rational functions $p_1(x)/q_1(x)$ and $p_2(y)/q_2(y)$ of degree at most d such that

$$\sup_X \left| f(x) - \frac{p_1(x)}{q_1(x)} \right| + \sup_Y \left| g(y) - \frac{p_2(y)}{q_2(y)} \right| < 1.$$

Then

$$\begin{aligned} f(x) \wedge g(y) &\equiv \operatorname{sgn}(1 + f(x) + g(y)) \\ &\equiv \operatorname{sgn}\left(1 + \frac{p_1(x)}{q_1(x)} + \frac{p_2(y)}{q_2(y)}\right). \end{aligned}$$

Multiplying through by the positive quantity $q_1(x)^2 q_2(y)^2$ gives the desired sign-representing polynomial: $f(x) \wedge g(y) \equiv \operatorname{sgn}\{q_1(x)^2 q_2(y)^2 + p_1(x) q_1(x) q_2(y)^2 + p_2(y) q_2(y) q_1(x)^2\}$. ∎

The construction of Theorem 2.13 is somewhat ad hoc, and there is no particular reason to believe that it gives a sign-representing polynomial of asymptotically optimal degree. Remarkably, it does. The following converse to the theorem of Beigel et al. was established in [76, Theorem 3.16].

THEOREM 2.14 (Sherstov). *Let $f\colon X \to \{-1,+1\}$ and $g\colon Y \to \{-1,+1\}$ be given functions, where $X, Y \subset \mathbb{R}^n$ are arbitrary finite sets. Assume that f and g are not identically false. Let $d = \deg_\pm(f \wedge g)$. Then*

$$R(f, 4d) + R(g, 2d) < 1.$$

2.7. Symmetrization. Let S_n denote the symmetric group on n elements. For $\sigma \in S_n$ and $x \in \{0,1\}^n$, we denote $\sigma x = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in \{0,1\}^n$. For $x \in \{0,1\}^n$, we define $|x| = x_1 + x_2 + \cdots + x_n$. A function $\phi\colon \{0,1\}^n \to \mathbb{R}$ is called *symmetric* if $\phi(x) = \phi(\sigma x)$ for every $x \in \{0,1\}^n$ and every $\sigma \in S_n$. Equivalently, ϕ is symmetric if $\phi(x)$ is uniquely determined by $|x|$. Symmetric functions on $\{0,1\}^n$ are intimately related to univariate polynomials, as borne out by Minsky and Papert's *symmetrization argument* [57].

PROPOSITION 2.15 (Minsky and Papert). *Let $p\colon \{0,1\}^n \to \mathbb{R}$ be a polynomial of degree d. Then there is a univariate polynomial p^* of degree at most d such that for all $x \in \{0,1\}^n$,*

$$\mathop{\mathbf{E}}_{\sigma \in S_n} p(\sigma x) = p^*(|x|).$$

Minsky and Papert's result generalizes to block-symmetric functions, as pointed out in [66, Proposition 2.3]:

Proposition 2.16 (Razborov and Sherstov). *Let $n_1, \ldots, n_k$ be positive integers. Let $p\colon \{0,1\}^{n_1} \times \cdots \times \{0,1\}^{n_k} \to \mathbb{R}$ be a polynomial of degree d. Then there is a polynomial $p^*\colon \mathbb{R}^k \to \mathbb{R}$ of degree at most d such that for all $x_1 \in \{0,1\}^{n_1}, \ldots, x_k \in \{0,1\}^{n_k}$,*

$$\mathop{\mathbf{E}}_{\sigma_1 \in S_{n_1}, \ldots, \sigma_k \in S_{n_k}} p(\sigma_1 x_1, \ldots, \sigma_k x_k) = p^*(|x_1|, \ldots, |x_k|).$$

Proposition 2.16 follows in a straightforward manner from Minsky and Papert's Proposition 2.15 by induction on the number of blocks k.

2.8. Communication complexity. An excellent reference on communication complexity is the monograph by Kushilevitz and Nisan [50]. In this overview, we will limit ourselves to key definitions and notation. We adopt the *randomized number-on-the-forehead model*, due to Chandra et al. [24]. The model features k communicating players, tasked with computing a (possibly partial) Boolean function F on the Cartesian product $X_1 \times X_2 \times \cdots \times X_k$ of some finite sets $X_1, X_2, \ldots, X_k$. A given input $(x_1, x_2, \ldots, x_k) \in X_1 \times X_2 \times \cdots \times X_k$ is distributed among the players by placing x_i, figuratively speaking, on the forehead of the i-th player (for $i = 1, 2, \ldots, k$). In other words, the i-th player knows the arguments $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k$ but not x_i. The players communicate by sending broadcast messages, taking turns according to a protocol agreed upon in advance. Each of them privately holds an unlimited supply of uniformly random bits, which he can use along with his available arguments when deciding what message to send at any given point in the protocol. The protocol's purpose is to allow accurate computation of F everywhere on the domain of F. An *ϵ-error protocol* for F is one which, on every input $(x_1, x_2, \ldots, x_k) \in \operatorname{dom} F$, produces the correct answer $F(x_1, x_2, \ldots, x_k)$ with probability at least $1 - \epsilon$. The *cost* of a protocol is the total bit length of the messages broadcast by all the players in the worst case.[1] The *ϵ-error randomized communication complexity* of F, denoted $R_\epsilon(F)$, is the least cost of an ϵ-error randomized protocol for F. As a special case of this model for $k = 2$, one recovers the original two-party model of Yao [88] reviewed in the introduction.

We focus on randomized protocols with probability of error close to that of random guessing, $1/2$. There are two natural ways to define the communication complexity of a multiparty problem F in this setting. The *communication complexity of F with unbounded error*, introduced by Paturi and Simon [63], is the quantity

$$\operatorname{UPP}(F) = \inf_{0 \leqslant \epsilon < 1/2} R_\epsilon(F).$$

The error probability in this formalism is "unbounded" in the sense that it can be arbitrarily close to $1/2$. Babai et al. [11] proposed an alternate quantity, which includes an additive penalty term that depends on the error probability:

$$\operatorname{PP}(F) = \inf_{0 \leqslant \epsilon < 1/2} \left\{ R_\epsilon(F) + \log \frac{1}{\frac{1}{2} - \epsilon} \right\}.$$

[1] The contribution of a b-bit broadcast to the protocol cost is b rather than $k \cdot b$.

We refer to $\mathrm{PP}(F)$ as the *communication complexity of F with weakly unbounded error.* These two complexity measures naturally give rise to corresponding complexity classes UPP_k and PP_k in multiparty communication complexity [11], both inspired by Gill's probabilistic polynomial time for Turing machines [31]. Formally, let $\{F_{n,k}\}_{n=1}^{\infty}$ be a family of k-party communication problems $F_{n,k}\colon (\{0,1\}^n)^k \to \{-1,+1\}$, where $k = k(n)$ is either a constant or a function. Then $\{F_{n,k}\}_{n=1}^{\infty} \in \mathsf{UPP}_k$ if and only if $\mathrm{UPP}(F_{n,k}) \leqslant \log^c n$ for some constant c and all $n \geqslant c$. Analogously, $\{F_{n,k}\}_{n=1}^{\infty} \in \mathsf{PP}_k$ if and only if $\mathrm{PP}(F_{n,k}) \leqslant \log^c n$ for some constant c and all $n \geqslant c$. By definition,

$$\mathsf{PP}_k \subseteq \mathsf{UPP}_k.$$

It is standard practice to abbreviate $\mathsf{PP} = \mathsf{PP}_2$ and $\mathsf{UPP} = \mathsf{UPP}_2$. The following well-known fact, whose proof in the stated generality is available in [80, Fact 2.4], gives a large class of communication problems that are efficiently computable with unbounded error.

FACT 2.17. *Let $F\colon (\{0,1\}^n)^k \to \{-1,+1\}$ be a k-party communication problem such that $F(x) = \operatorname{sgn} p(x)$ for some polynomial p with ℓ monomials. Then*

$$\mathrm{UPP}(F) \leqslant \lceil \log \ell \rceil + 2.$$

In the setting of $k = 2$ parties, Paturi and Simon [63] showed that unbounded-error communication complexity has a natural matrix-analytic characterization. For a matrix M without zero entries, the *sign-rank* of M is denoted $\mathrm{rk}_\pm(M)$ and defined as the minimum rank of a real matrix R such that $\operatorname{sgn} R_{i,j} = \operatorname{sgn} M_{i,j}$ for all i,j. In words, the sign-rank of M is the minimum rank of a real matrix that has the same sign pattern as M. We extend the notion of sign-rank to communication problems $F\colon X \times Y \to \{-1,+1\}$ by defining $\mathrm{rk}_\pm(F) = \mathrm{rk}_\pm(M_F)$, where $M_F = [F(x,y)]_{x \in X, y \in Y}$ is the characteristic matrix of F. The following classic result due to Paturi and Simon [63, Theorem 3] relates two-party unbounded-error communication complexity to sign-rank.

THEOREM 2.18 (Paturi and Simon). *Let $F\colon X \times Y \to \{-1,+1\}$ be a two-party communication problem. Then*

$$\log \mathrm{rk}_\pm(F) \leqslant \mathrm{UPP}(F) \leqslant \log \mathrm{rk}_\pm(F) + 2.$$

2.9. Discrepancy. A k-dimensional *cylinder intersection* is a function $\chi\colon X_1 \times X_2 \times \cdots \times X_k \to \{0,1\}$ of the form

$$\chi(x_1, x_2, \ldots, x_k) = \prod_{i=1}^{k} \chi_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k),$$

where $\chi_i\colon X_1 \times \cdots \times X_{i-1} \times X_{i+1} \times \cdots \times X_k \to \{0,1\}$. In other words, a k-dimensional cylinder intersection is the product of k functions with range $\{0,1\}$, where the i-th function does not depend on the i-th coordinate but may depend arbitrarily on the other $k-1$ coordinates. Introduced by Babai et al. [12], cylinder intersections are the fundamental building blocks of communication protocols and for that reason play a central role in the theory. For a (possibly partial) Boolean function F on $X_1 \times X_2 \times \cdots \times X_k$ and a probability distribution P on $X_1 \times X_2 \times \cdots \times X_k$, the *discrepancy of F with respect to P* is given by

$$\operatorname{disc}_P(F) = \sum_{x \notin \operatorname{dom} F} P(x) + \max_{\chi} \left| \sum_{x \in \operatorname{dom} F} F(x) P(x) \chi(x) \right|,$$

where the maximum is over cylinder intersections χ. The minimum discrepancy over all distributions is denoted

$$\operatorname{disc}(F) = \min_P \operatorname{disc}_P(F).$$

Upper bounds on a function's discrepancy give lower bounds on its randomized communication complexity, a classic technique known as the *discrepancy method* [28, 12, 50].

Theorem 2.19. *Let F be a (possibly partial) Boolean function on $X_1 \times X_2 \times \cdots \times X_k$. Then for $0 \leqslant \epsilon \leqslant 1/2$,*

$$2^{R_\epsilon(F)} \geqslant \frac{1 - 2\epsilon}{\operatorname{disc}(F)}.$$

A proof of Theorem 2.19 in the stated generality is available in [79, Theorem 2.9]. Combining this theorem with the definition of $\operatorname{PP}(F)$ gives the following corollary.

Corollary 2.20. *Let F be a (possibly partial) Boolean function on $X_1 \times X_2 \times \cdots \times X_k$. Then*

$$\operatorname{PP}(F) \geqslant \log \frac{2}{\operatorname{disc}(F)}.$$

2.10. Pattern matrix method. Theorem 2.19 and Corollary 2.20 highlight the role of discrepancy in proving lower bounds on randomized communication complexity. Apart from a few canonical examples [50], discrepancy is a challenging quantity to analyze. The *pattern matrix method* is a technique that gives tight bounds on the discrepancy and communication complexity for a large class of communication problems. The technique was developed in [73, 75] for two-party communication complexity and has since been generalized by several authors to the multiparty setting. We now review the strongest form [79, 78] of the pattern matrix method, focusing our discussion on discrepancy bounds.

Set disjointness is the k-party communication problem of determining whether k given subsets of the universe $\{1, 2, \ldots, n\}$ have empty intersection, where, as usual, the i-th party knows all the sets except for the i-th. Identifying the sets with their characteristic vectors, set disjointness corresponds to the Boolean function $\operatorname{DISJ}_{n,k} \colon (\{0,1\}^n)^k \to \{-1, +1\}$ given by

$$\operatorname{DISJ}_{n,k}(x_1, x_2, \ldots, x_k) = \neg \bigvee_{i=1}^{n} x_{1,i} \wedge x_{2,i} \wedge \cdots \wedge x_{k,i}\,. \tag{2.15}$$

The partial function $\mathrm{UDISJ}_{n,k}$ on $(\{0,1\}^n)^k$, called *unique set disjointness*, is defined as $\mathrm{DISJ}_{n,k}$ with domain restricted to inputs $x \in (\{0,1\}^n)^k$ such that $x_{1,i} \wedge x_{2,i} \wedge \cdots \wedge x_{k,i} = 1$ for at most one coordinate i. In set-theoretic terms, this restriction corresponds to requiring that the k sets either have empty intersection or intersect in a unique element.

The pattern matrix method pertains to the communication complexity of *composed* communication problems. Specifically, let G be a (possibly partial) Boolean function on $X_1 \times X_2 \times \cdots \times X_k$, representing a k-party communication problem, and let $f\colon \{0,1\}^n \to \{-1,+1\}$ be given. The coordinatewise composition $f \circ G$ is then a k-party communication problem on $X_1^n \times X_2^n \times \cdots \times X_k^n$. We are now in a position to state the pattern matrix method for discrepancy bounds [79, Theorem 5.7].

Theorem 2.21 (Sherstov). *For every Boolean function $f\colon \{0,1\}^n \to \{-1,+1\}$, all positive integers m and k, and all reals $0 < \gamma < 1$,*

$$\operatorname{disc}(f \circ \mathrm{UDISJ}_{m,k}) \leqslant \left(\frac{\mathrm{e} \cdot 2^k n}{\deg_{1-\gamma}(f)\sqrt{m}}\right)^{\deg_{1-\gamma}(f)} + \gamma\,.$$

This theorem makes it possible to prove communication lower bounds by leveraging the existing literature on polynomial approximation. In follow-up work, the author improved Theorem 2.21 to an essentially tight upper bound [78, Theorem 5.7]. However, we will not need this sharper version.

3. Discrepancy of integer sets

Let $m \geqslant 2$ be an integer modulus. Key to our work is the notion of *m-discrepancy*, which quantifies the pseudorandomness or aperiodicity of any given multiset of integers modulo m. The m-discrepancy of a nonempty multiset $Z = \{z_1, z_2, \ldots, z_n\}$ of arbitrary integers is defined as

$$\operatorname{disc}(Z, m) = \max_{k=1,2,\ldots,m-1} \left| \frac{1}{n} \sum_{j=1}^{n} \omega^{k z_j} \right|,$$

where ω is a primitive m-th root of unity; the right-hand side is obviously the same for any such ω. By way of terminology, we emphasize that the notion of m-discrepancy just defined is unrelated to the notion of *discrepancy* from Section 2.9. As a matter of convenience, we define

$$\operatorname{disc}(\varnothing, m) = 0. \tag{3.1}$$

The notion of m-discrepancy has a long history in combinatorics and theoretical computer science, e.g., [30, 69, 2, 38, 64, 5]. The m-discrepancy of an integer multiset Z has a natural interpretation in terms of the discrete Fourier transform on $\mathbb{Z}_m$. Specifically, consider the *frequency vector* $(f_0, f_1, \ldots, f_{m-1})$ of Z, where f_j is the total number of element occurrences in Z that are congruent to j modulo m. Applying the discrete Fourier transform to $(f_j)_{j=0}^{m-1}$ produces the sequence $(\sum_{j=0}^{m-1} f_j \exp(-2\pi \mathbf{i} kj/m))_{k=0}^{m-1} = (\sum_{j=1}^{n} \exp(-2\pi \mathbf{i} k z_j/m))_{k=0}^{m-1}$, which is a permutation of $(n, \sum_{j=1}^{n} \omega^{z_j}, \ldots, \sum_{j=1}^{n} \omega^{(m-1)z_j})$. Summarizing, the m-discrepancy of Z

coincides up to a normalizing factor with the largest absolute value of a nonconstant Fourier coefficient of the frequency vector of Z.

3.1. Basic properties. We collect a few elementary properties of m-discrepancy. To start with, we quantify the "continuity" of $\operatorname{disc}(Z,m)$ in the first argument. By way of notation, we remind the reader that the cardinality $|Z|$ of a multiset Z is found by summing, for each distinct element $z \in Z$, the number of times z occurs in Z.

Proposition 3.1. *Fix a natural number $m \geqslant 2$. Then for any nonempty finite multisets Z, Z' of integers with $Z' \subseteq Z$,*

$$1 + \operatorname{disc}(Z', m) \leqslant (1 + \operatorname{disc}(Z, m)) \cdot \frac{|Z|}{|Z'|}. \tag{3.2}$$

Proof. Abbreviate $n = |Z|$ and $n' = |Z'|$, and fix an enumeration $z_1, z_2, \ldots, z_n$ of the elements of Z such that $Z' = \{z_1, z_2, \ldots, z_{n'}\}$. Then for a primitive m-th root of unity ω,

$$\begin{aligned} n \operatorname{disc}(Z, m) &= \max_{k=1,2,\ldots,m-1} \left| \sum_{j=1}^{n} \omega^{k z_j} \right| \\ &\geqslant \max_{k=1,2,\ldots,m-1} \left\{ \left| \sum_{j=1}^{n'} \omega^{k z_j} \right| - \sum_{j=n'+1}^{n} \left| \omega^{k z_j} \right| \right\} \\ &= \max_{k=1,2,\ldots,m-1} \left| \sum_{j=1}^{n'} \omega^{k z_j} \right| - (n - n') \\ &= n' \operatorname{disc}(Z', m) - (n - n'), \end{aligned}$$

which directly implies (3.2). ∎

The m-discrepancy of Z is invariant under a variety of operations on Z, such as shifting the elements of Z by any given integer or multiplying the elements of Z by an integer relatively prime to m. For our purposes, the following observation will be sufficient.

Proposition 3.2. *Fix a natural number $m \geqslant 2$ and a nonempty finite multiset Z of integers. Then*

$$\operatorname{disc}(-Z, m) = \operatorname{disc}(Z, m).$$

Proof. The claim is immediate from the definition of m-discrepancy because ω is a primitive m-th root of unity if and only if ω^{-1} is. ∎

3.2. Existential bounds. Since the m-discrepancy of a multiset remains unchanged when one reduces its elements modulo m, we can focus without loss of generality on multisets with elements in $\{0, 1, 2, \ldots, m-1\}$. The identity $1+\omega+\omega^2+\cdots+\omega^{m-1} = 0$ for any m-th root of unity $\omega \neq 1$ implies that $Z = \{0, 1, 2, \ldots, m-1\}$

achieves the smallest possible m-discrepancy: $\operatorname{disc}(Z,m)=0$. The problem of constructing *sparse* nonempty multisets with small discrepancy has seen considerable work. Their existence is straightforward to verify, as follows.

Fact 3.3. *Fix $0<\epsilon<1$ and an integer $m\geqslant 2$. Let Z be a random multiset of size n whose elements are chosen independently and uniformly at random from $\{0,1,2,\ldots,m-1\}$. Then*

$$\mathbf{P}\left[\operatorname{disc}(Z,m)\geqslant\epsilon\right]\leqslant 4m\exp\left(-\frac{n\epsilon^2}{8}\right).$$

Fact 3.3 has been proved in one form or another by many authors, e.g., [30, 69, 5]. For the reader's convenience, we include a short proof below.

Proof of Fact 3.3. Let $Z_1,Z_2,\ldots,Z_n$ be independent random variables, each distributed uniformly in $\{0,1,2,\ldots,m-1\}$. For any m-th root of unity $\omega\neq 1$, we have $|\omega^{Z_j}|=1$ and $\mathbf{E}\,\omega^{Z_j}=0$ for $j=1,2,\ldots,n$. Hence, $\operatorname{Re}(\omega^{Z_1}),\operatorname{Re}(\omega^{Z_2}),\ldots,\operatorname{Re}(\omega^{Z_n})$ are independent random variables with range in $[-1,1]$ and expectation 0, and likewise for $\operatorname{Im}(\omega^{Z_1}),\operatorname{Im}(\omega^{Z_2}),\ldots,\operatorname{Im}(\omega^{Z_n})$. As a result,

$$\begin{aligned}\mathbf{P}\left[\left|\frac{1}{n}\sum_{j=1}^{n}\omega^{Z_j}\right|\geqslant\epsilon\right]&\leqslant\mathbf{P}\left[\left|\operatorname{Re}\left(\frac{1}{n}\sum_{j=1}^{n}\omega^{Z_j}\right)\right|\geqslant\frac{\epsilon}{2}\right]\\&\qquad+\mathbf{P}\left[\left|\operatorname{Im}\left(\frac{1}{n}\sum_{j=1}^{n}\omega^{Z_j}\right)\right|\geqslant\frac{\epsilon}{2}\right]\\&\leqslant 4\exp\left(-\frac{n\epsilon^2}{8}\right),\end{aligned}$$

where the second step uses Hoeffding's inequality (Fact 2.1). Applying the union bound across all m-th roots of unity $\omega\neq 1$, we conclude that the probability that $\operatorname{disc}(\{Z_1,Z_2,\ldots,Z_n\},m)\geqslant\epsilon$ is at most $4(m-1)\exp(-n\epsilon^2/8)$. ∎

In some applications, one is restricted to working with *subsets* of $\{0,1,2,\ldots,m-1\}$ as opposed to arbitrary *multisets* with possibly repeated elements. We record a version of Fact 3.3 for this setting.

Corollary 3.4. *Fix $0<\epsilon<1$ and an integer $m\geqslant 2$. Let Z be a random multiset of size $n\leqslant m$ whose elements are chosen independently and uniformly at random from $\{0,1,2,\ldots,m-1\}$. Then with probability at least*

$$\left(1-\frac{n}{m}\right)^n-4m\exp\left(-\frac{n\epsilon^2}{8}\right),\tag{3.3}$$

the elements of Z are nonzero and pairwise distinct, and obey $\operatorname{disc}(Z,m)\leqslant\epsilon$.

Proof. The probability that Z does not contain 0 or repeated elements is easily seen to be $\prod_{i=1}^{n}\frac{m-i}{m}\geqslant(1-\frac{n}{m})^n$. As a result, the claim follows from Fact 3.3. ∎

In all of our applications, the error parameter $\epsilon > 0$ will be a small constant. In this regime, Corollary 3.4 guarantees the existence of a set $Z \subseteq \{1, 2, \ldots, m-1\}$ with m-discrepancy at most ϵ and cardinality $O(\log m)$, an exponential improvement in sparsity compared to the trivial set $\{0, 1, 2, \ldots, m-1\}$. No further improvement is possible: it is well known that any nonempty multiset with m-discrepancy bounded away from 1 has cardinality $\Omega(\log m)$. This classical lower bound has a remarkable variety of proofs, e.g., using random walks [5], sphere packing arguments [29], and diophantine approximation [53]. We include here a particularly simple and self-contained proof, adapted from Leung et al. [53]. Unlike all other technical statements in this paper, Fact 3.5 is not used in the proof of our main result and is provided solely for completeness.

Fact 3.5 (Leung et al.). *Fix a natural number $m \geqslant 2$. Let $Z = \{z_1, z_2, \ldots, z_n\}$ be a multiset of integers. Then*

$$\operatorname{disc}(Z, m) \geqslant 1 - \frac{2\pi}{\lfloor (m-1)^{1/n} \rfloor}.$$

Proof (adapted from [53]). The proof is based on a classic technique from simultaneous diophantine approximation. For a nonnegative real number x, let $\operatorname{frac}(x)$ denote the fractional part of x. Abbreviate $q = \lfloor (m-1)^{1/n} \rfloor$ and consider the q intervals

$$\left[0, \frac{1}{q}\right), \left[\frac{1}{q}, \frac{2}{q}\right), \left[\frac{2}{q}, \frac{3}{q}\right), \ldots, \left[\frac{q-1}{q}, 1\right). \tag{3.4}$$

By the pigeonhole principle, there must be a pair of distinct integers $k', k'' \in \{0, 1, 2, \ldots, q^n\}$ such that

$$\operatorname{frac}\left(\frac{z_1 k'}{m}\right), \operatorname{frac}\left(\frac{z_2 k'}{m}\right), \ldots, \operatorname{frac}\left(\frac{z_n k'}{m}\right)$$

are in the same intervals of (3.4) as

$$\operatorname{frac}\left(\frac{z_1 k''}{m}\right), \operatorname{frac}\left(\frac{z_2 k''}{m}\right), \ldots, \operatorname{frac}\left(\frac{z_n k''}{m}\right),$$

respectively. Without loss of generality, $k' > k''$. Then the integer $k = k' - k''$ obeys

$$k \in \{1, 2, \ldots, m-1\}, \tag{3.5}$$

$$\left| \frac{z_j k}{m} - u_j \right| \leqslant \frac{1}{q}, \qquad j = 1, 2, \ldots, n \tag{3.6}$$

for some $u_1, u_2, \ldots, u_n \in \mathbb{Z}$. Now

$$\begin{aligned}
\operatorname{disc}(Z,m) &\geqslant \frac{1}{n}\left|\sum_{j=1}^{n}\exp\left(2\pi\mathbf{i}\cdot\frac{kz_j}{m}\right)\right| \\
&\geqslant 1-\frac{1}{n}\sum_{j=1}^{n}\left|1-\exp\left(2\pi\mathbf{i}\cdot\frac{kz_j}{m}\right)\right| \\
&= 1-\frac{1}{n}\sum_{j=1}^{n}\left|1-\exp\left(2\pi\mathbf{i}\cdot\left(\frac{kz_j}{m}-u_j\right)\right)\right| \\
&\geqslant 1-\frac{1}{n}\sum_{j=1}^{n}2\pi\left|\frac{kz_j}{m}-u_j\right| \\
&\geqslant 1-\frac{2\pi}{q},
\end{aligned}$$

where the first step uses the definition of m-discrepancy; the second step applies the triangle inequality; the third step is valid by periodicity; the fourth step uses the bound $|1-\exp(2\pi x\mathbf{i})| = \sqrt{2-2\cos(2\pi x)} \leqslant 2\pi|x|$ for all real x; and the final step is immediate from (3.6). ∎

3.3. An explicit construction. We now turn to the problem of efficiently constructing sparse sets with small m-discrepancy. Two such constructions are known to date, due to Ajtai et al. [2] and Katz [38]. The approach of Ajtai et al. is elementary except for an appeal to the prime number theorem. Katz's construction, on the other hand, relies on deep results in number theory. Neither work appears to directly imply the kind of optimal de-randomization that we require, namely, an algorithm that runs in time polynomial in $\log m$ and produces a multiset of cardinality $O(\log m)$ with m-discrepancy bounded away from 1. We obtain such an algorithm by adapting the approach of Ajtai et al. [2]. The following technical result plays a central role.

Theorem 3.6 (cf. Ajtai et al.). *Fix an integer $R \geqslant 1$ and a real number $P \geqslant 2$. Let m be an integer with $m \geqslant P^2(R+1)$. Fix a set $S_p \subseteq \{1, 2, \ldots, p-1\}$ for each prime $p \in (P/2, P]$ with $p \nmid m$, such that all S_p have the same cardinality. Consider the multiset*

$$\begin{aligned}
S = \{(r + s\cdot(p^{-1})_m) \bmod m :& \\
& r = 1, \ldots, R; \quad p \in (P/2, P] \text{ prime with } p \nmid m; \quad s \in S_p\}.
\end{aligned}$$

Then the elements of S are pairwise distinct and nonzero. Moreover,

$$\operatorname{disc}(S,m) \leqslant \frac{c}{\sqrt{R}} + \frac{c\log m}{\log\log m}\cdot\frac{\log P}{P} + \max_p\{\operatorname{disc}(S_p, p)\}$$

for some (explicitly given) constant $c \geqslant 1$ independent of P, R, m.

Ajtai et al. [2] proved a special case of Theorem 3.6 for m prime, but their argument readily generalizes to arbitrary moduli m as just stated. For the reader's convenience, we provide a complete proof of Theorem 3.6 in Appendix A. The theorem's purpose is to reduce the construction of a sparse set with small m-discrepancy to the construction of sparse sets with small p-discrepancy, for primes $p \ll m$. By applying Theorem 3.6 in a recursive manner, one reaches smaller and smaller primes. The authors of [2] continue this recursive process until they reach primes p so small that the trivial construction $\{1, 2, 3, \ldots, p-1\}$ can be considered sparse. We proceed differently and terminate the recursion after just two stages, at which point the input size is small enough for brute force search based on Corollary 3.4. The final set that we construct has size logarithmic in m and m-discrepancy a small constant, as opposed to the superlogarithmic size and $o(1)$ discrepancy in the work of Ajtai et al. [2]. A detailed exposition of our algorithm follows.

Theorem 3.7. *Let $0 < \epsilon \leqslant 1$ be given. Then there is an algorithm that takes as input an integer $m \geqslant 2$, runs in time polynomial in $\log m$, and outputs a nonempty set $Z \subseteq \{0, 1, 2, \ldots, m-1\}$ with*

$$\begin{aligned} &\operatorname{disc}(Z, m) \leqslant \epsilon, \\ &|Z| \leqslant C_\epsilon \log m, \end{aligned}$$

where $C_\epsilon \geqslant 1$ is a constant. Moreover, the constant C_ϵ and the algorithm are given explicitly.

Proof. Set $\delta = \epsilon/(11c)$, where $c \geqslant 1$ is the explicit constant from Theorem 3.6. Define

$$\begin{aligned} P' &= \frac{1}{\delta} \ln\left(\frac{1}{\delta}\ln m\right), \\ P'' &= \frac{1}{\delta}\ln m. \end{aligned}$$

We may assume that

$$P' \geqslant \frac{1}{\delta^2}, \tag{3.7}$$

$$P' > 4\left\lceil \frac{8\ln 8P'}{\delta^2}\right\rceil^2, \tag{3.8}$$

$$P'' \geqslant 2P'^2\left\lceil \frac{1}{\delta^2} + 1\right\rceil, \tag{3.9}$$

$$m \geqslant P''^2\left\lceil \frac{1}{\delta^2} + 1\right\rceil, \tag{3.10}$$

$$\pi(P') > \pi\left(\frac{P'}{2}\right), \tag{3.11}$$

$$\pi(P'') - \pi\left(\frac{P''}{2}\right) > \nu(m), \tag{3.12}$$

where π is the prime counting function and ν is the number of distinct prime divisors function. Indeed, if any of (3.7)–(3.10) is violated, then by elementary calculus m is bounded in terms of $1/\delta = O(1)$ and therefore the trivial set $Z = \{0, 1, 2, \ldots, m-1\}$ satisfies $\operatorname{disc}(Z, m) = 0$ and $|Z| = O(1)$. Analogously, the explicit bounds for π and ν in Facts 2.3 and 2.4 ensure that (3.11) and (3.12) can fail only if m is bounded in terms of $1/\delta = O(1)$, so that we may again output $Z = \{0, 1, 2, \ldots, m-1\}$.

Assuming (3.7)–(3.12), our construction of Z has three stages. In the first and second stages, we construct sparse sets $S_p \subseteq \{1, 2, \ldots, p-1\}$ with small p-discrepancy for all primes $p \in (P'/2, P']$ and $p \in (P''/2, P'']$, respectively. In the final stage, we construct the set Z in the theorem statement. We ensure that each stage runs in time polynomial in $\ln m$.

Stage 1. For every prime $p' \in (P'/2, P']$, Corollary 3.4 along with (3.8) guarantees the existence of a set $S_{p'} \subseteq \{1, 2, \ldots, p'-1\}$ with

$$|S_{p'}| = \left\lceil \frac{8 \ln 8P'}{\delta^2} \right\rceil, \qquad \text{prime } p' \in (P'/2, P'], \tag{3.13}$$

$$\operatorname{disc}(S_{p'}, p') \leqslant \delta, \qquad \text{prime } p' \in (P'/2, P']. \tag{3.14}$$

The primes in $(P'/2, P']$ can be identified by the trivial algorithm in time polynomial in $P' = O(\ln \ln m)$. For each such prime p', we can find a set $S_{p'}$ with the above properties in time $P'^{O(|S_{p'}|)} = o(\ln m)$ by trying out all candidate sets.

Stage 2. Apply the construction of Theorem 3.6 with parameters $P = P'$ and $R = \lceil 1/\delta^2 \rceil$ to the sets constructed in Stage 1 to obtain a set $S_{p''} \subseteq \{1, 2, \ldots, p''-1\}$ for each prime $p'' \in (P''/2, P'']$. This choice of parameters is legitimate by (3.9). By (3.13), the new sets have the same cardinality, namely,

$$|S_{p''}| = R \left\lceil \frac{8 \ln 8P'}{\delta^2} \right\rceil \left(\pi(P') - \pi\left(\frac{P'}{2}\right) \right), \qquad \text{prime } p'' \in (P''/2, P''].$$

The prime number theorem (Fact 2.3) implies that $|S_{p''}| = O(P') = O(\ln \ln m)$. In view of (3.7), (3.14), and $P'' = \exp(\delta P')$, the new sets have

$$\operatorname{disc}(S_{p''}, p'') \leqslant 6c\delta, \qquad \text{prime } p'' \in (P''/2, P'']. \tag{3.15}$$

We now show that Stage 2 runs in time polynomial in $\ln m$. To start with, the primes in $(P''/2, P'']$ can be identified by the trivial algorithm in time polynomial in $P'' = O(\ln m)$. For any such prime p'', the construction of the corresponding set $S_{p''}$ in Theorem 3.6 amounts to $O(|S_{p''}|) = O(\ln \ln m)$ arithmetic operations in the field $\mathbb{F}_{p''}$ of size $|\mathbb{F}_{p''}| = O(\ln m)$, and therefore can be carried out in time polynomial in $\ln \ln m$.

Stage 3. Apply the construction of Theorem 3.6 with parameters $P = P''$ and $R = \lceil 1/\delta^2 \rceil$ to the sets constructed in Stage 2 to obtain a set $S_m \subseteq \{1, 2, \ldots, m-1\}$.

This choice of parameters is legitimate by (3.10). This new set has cardinality

$$|S_m| = R^2 \left\lceil \frac{8\ln 8P'}{\delta^2} \right\rceil \left(\pi(P') - \pi\left(\frac{P'}{2}\right)\right) \\ \times \left|\left\{p'' \text{ prime} : p'' \in \left(\frac{P''}{2}, P''\right] \text{ and } p'' \nmid m\right\}\right|,$$

which in view of (3.11) and (3.12) guarantees that S_m is nonempty. Simplifying,

$$\begin{aligned} |S_m| &\leqslant \left\lceil \frac{1}{\delta^2} \right\rceil^2 \left\lceil \frac{8\ln 8P'}{\delta^2} \right\rceil \cdot \pi(P') \cdot \pi(P'') \\ &= O\left(\ln P' \cdot \frac{P'}{\ln P'} \cdot \frac{P''}{\ln P''}\right) \\ &= O(\ln m), \end{aligned}$$

where the second step applies the prime number theorem (Fact 2.3). The multiplicative constant in this asymptotic bound on $|S_m|$ can be easily recovered from the explicit bounds in Fact 2.3. Using (3.9), (3.15), and $m = \exp(\delta P'')$, we further obtain

$$\operatorname{disc}(S_m, m) \leqslant 11c\delta.$$

Since $\delta = \epsilon/(11c)$, the set $Z = S_m$ satisfies the requirements of the theorem. Finally, the construction of S_m in Stage 3 amounts to $O(|S_m|) = O(\ln m)$ arithmetic operations in the ring $\mathbb{Z}_m$ and therefore can be carried out in time polynomial in $\ln m$. □

4. Univariatization

Consider a halfspace $h_n(x) = \operatorname{sgn}(\sum z_i x_i - \theta)$ in Boolean variables $x_1, x_2, \ldots, x_n \in \{0,1\}$, where the coefficients can be assumed without loss of generality to be integers. Then the linear form $\sum z_i x_i - \theta$ ranges in the discrete set $\{\pm 1, \pm 2, \ldots, \pm N\}$, for some integer N proportionate to the magnitude of the coefficients. As a result, one can approximate h_n to any given error ϵ by approximating the sign function to ϵ on $\{\pm 1, \pm 2, \ldots, \pm N\}$. This approach works for both rational approximation and polynomial approximation. Needless to say, there is no reason to expect that the degree of the approximant in this naïve construction is anywhere close to optimal. Perhaps the most dramatic example is the *odd-max-bit function*, defined by $\mathrm{OMB}_n(x) = \operatorname{sgn}(1 + \sum_{i=1}^n (-2)^i x_i)$. A moment's thought reveals that OMB_n can be approximated to any given error $\epsilon > 0$ by a rational function of degree 1, whereas the naïve construction produces an approximant of degree $\Omega(n)$.

Surprisingly, we are able to construct a halfspace $h_n(x) = \operatorname{sgn}(\sum z_i x_i - \theta)$ with exponentially large coefficients for which the naïve construction is essentially optimal. Specifically, we show that a rational approximant for h_n with given error and given numerator and denominator degrees implies an analogous *univariate* rational approximant for the sign function on $\{\pm 1, \pm 2, \pm 3, \ldots, \pm 2^{\Theta(n)}\}$. As a result, tight lower bounds for the rational and polynomial approximation of h_n follow immediately from the univariate lower bounds for the sign function. The construction of h_n, carried out in this section, is the centerpiece of our paper. The role of h_n is to reduce the multivariate problem taken up in this work to a well-understood univariate question, whence the title of this section. We have broken down the proof into four steps, corresponding to subsections 4.1–4.4 below.

4.1. Distribution of a linear form modulo m. We start by studying the probability distribution of the weighted sum $z_1X_1+z_2X_2+\cdots+z_nX_n$ modulo m, where $z_1, z_2, \ldots, z_n$ are given integers and $X_1, X_2, \ldots, X_n \in \{0,1\}$ are chosen uniformly at random. We will show that the distribution is close to uniform whenever the multiset $\{z_1, z_2, \ldots, z_n\}$ has small m-discrepancy. This result uses the following classical fact on linear forms modulo m.

Fact 4.1 (cf. Gould [32]; Thathachar [85]). *Fix a natural number $m \geqslant 2$ and a multiset $Z = \{z_1, z_2, \ldots, z_n\}$ of integers. Let ω be a primitive m-th root of unity. Then*

$$\left|\mathop{\mathbf{P}}_{X\in\{0,1\}^n}\left[\sum_{j=1}^{n} z_jX_j \equiv s \pmod m\right] - \frac{1}{m}\right| \leqslant \frac{1}{m}\sum_{k=1}^{m-1}\left|\prod_{j=1}^{n}\frac{1+\omega^{kz_j}}{2}\right|, \qquad s\in\mathbb{Z}. \tag{4.1}$$

Proof (adapted from [85, Lemma 13]). The fraction of vectors $X \in \{0,1\}^n$ that satisfy the equation $\sum_{j=1}^{n} z_jX_j \equiv s \pmod m$ can be computed directly, as follows:

$$\begin{aligned}
\mathop{\mathbf{P}}_{X\in\{0,1\}^n}\left[\sum_{j=1}^{n} z_jX_j \equiv s \pmod m\right] &= \mathop{\mathbf{E}}_{X\in\{0,1\}^n} \mathbf{I}\left[\sum_{j=1}^{n} z_jX_j \equiv s \pmod m\right] \\
&= \mathop{\mathbf{E}}_{X\in\{0,1\}^n} \frac{1}{m}\sum_{k=0}^{m-1}\omega^{k(\sum_{j=1}^{n} z_jX_j - s)} \\
&= \mathop{\mathbf{E}}_{X\in\{0,1\}^n} \frac{1}{m}\sum_{k=0}^{m-1}\omega^{-ks}\prod_{j=1}^{n}\omega^{kz_jX_j} \\
&= \frac{1}{m}\sum_{k=0}^{m-1}\omega^{-ks}\mathop{\mathbf{E}}_{X\in\{0,1\}^n}\prod_{j=1}^{n}\omega^{kz_jX_j} \\
&= \frac{1}{m}\sum_{k=0}^{m-1}\omega^{-ks}\prod_{j=1}^{n}\frac{1+\omega^{kz_j}}{2} \\
&= \frac{1}{m}+\frac{1}{m}\sum_{k=1}^{m-1}\omega^{-ks}\prod_{j=1}^{n}\frac{1+\omega^{kz_j}}{2}.
\end{aligned}$$

This implies (4.1) because $|\omega^{-ks}| = 1$ for all $k, s \in \mathbb{Z}$. ∎

In the original version of this manuscript, we proved (4.1) using a different, matrix-analytic argument, which we include as Appendix B. The short and elegant proof above was pointed out to us by T. S. Jayram, who kindly allowed us to include it.

We now simplify the right-hand side of (4.1) and relate it to m-discrepancy.

Lemma 4.2. *Fix a natural number $m \geqslant 2$ and a multiset $Z = \{z_1, z_2, \ldots, z_n\}$ of integers. Then for all $s \in \mathbb{Z}$,*

$$\left| \mathop{\mathbf{P}}_{X\in\{0,1\}^n}\left[\sum_{j=1}^n z_jX_j \equiv s \pmod{m}\right] - \frac{1}{m}\right| \leqslant \left(\frac{1+\operatorname{disc}(Z,m)}{2}\right)^{n/2}.$$

Proof. Let ω be a primitive m-th root of unity. For $k = 1, 2, \ldots, m-1$, we have

$$\begin{aligned}\left|\prod_{j=1}^n \frac{1+\omega^{kz_j}}{2}\right| &= \left(\prod_{j=1}^n \frac{(1+\omega^{kz_j})\overline{(1+\omega^{kz_j})}}{4}\right)^{1/2}\\ &= \left(\prod_{j=1}^n \frac{1+\operatorname{Re}(\omega^{kz_j})}{2}\right)^{1/2}\\ &\leqslant \left(\frac{1}{n}\sum_{j=1}^n \frac{1+\operatorname{Re}(\omega^{kz_j})}{2}\right)^{n/2}\\ &= \left(\frac{1}{2}+\frac{1}{2}\operatorname{Re}\left(\frac{1}{n}\sum_{j=1}^n\omega^{kz_j}\right)\right)^{n/2}\\ &\leqslant \left(\frac{1}{2}+\frac{1}{2}\left|\frac{1}{n}\sum_{j=1}^n\omega^{kz_j}\right|\right)^{n/2},\end{aligned}$$

where the second step uses $|\omega| = 1$, and the third step follows by convexity since $1 + \operatorname{Re}(\omega^{kz_j}) \geqslant 0$. Maximizing over k, we arrive at

$$\begin{aligned}\max_{k=1,2,\ldots,m-1}\left|\prod_{j=1}^n \frac{1+\omega^{kz_j}}{2}\right| &\leqslant \left(\frac{1}{2}+\frac{1}{2}\max_{k=1,2,\ldots,m-1}\left|\frac{1}{n}\sum_{j=1}^n\omega^{kz_j}\right|\right)^{n/2}\\ &= \left(\frac{1+\operatorname{disc}(Z,m)}{2}\right)^{n/2}.\end{aligned}$$

In view of Fact 4.1, the proof is complete. ∎

4.2. Fooling distributions. Let $Z = \{z_1, z_2, \ldots, z_n\}$ be a multiset with m-discrepancy bounded away from 1. Consider the linear map $L\colon \{0,1\}^n \to \mathbb{Z}_m$ given by $L(x) = \sum z_ix_i$. We have shown that for uniformly random $X \in \{0,1\}^n$, the probability distribution of $L(X)$ is exponentially close to uniform. This implies, for some constant $c > 0$, that the sets $L^{-1}(0), L^{-1}(1), \ldots, L^{-1}(m-1)$ cannot be reliably distinguished by a real polynomial of degree up to cn. More precisely, the characteristic functions of $L^{-1}(0), L^{-1}(1), \ldots, L^{-1}(m-1)$ have approximately the same Fourier spectrum up to degree cn. We will now substantially strengthen this conclusion by proving that there are probability distributions $\mu_0, \mu_1, \ldots, \mu_{m-1}$, supported on $L^{-1}(0), L^{-1}(1), \ldots, L^{-1}(m-1)$, respectively, such that the Fourier spectra of $\mu_0, \mu_1, \ldots, \mu_{m-1}$ are *exactly* the same up to degree cn. To use a technical term, these distributions *fool* any polynomial p of degree up to cn, in that $\mathbf{E}_{\mu_0} p = \mathbf{E}_{\mu_1} p = \cdots = \mathbf{E}_{\mu_{m-1}} p$. Our proof relies on the following technical result [77, Theorem 4.1].

THEOREM 4.3 (Sherstov). *Let $f, \chi_1, \ldots, \chi_k \colon \mathscr{X} \to \{-1,+1\}$ be given functions on a finite set $\mathscr{X}$. Suppose that*

$$\sum_{i=1}^{k} |\langle f, \chi_i \rangle_{\mathscr{X}}| < \frac{1}{2}, \tag{4.2}$$

$$\sum_{\substack{j=1\\ j\neq i}}^{k} |\langle \chi_i, \chi_j \rangle_{\mathscr{X}}| \leqslant \frac{1}{2}, \qquad i = 1, 2, \ldots, k. \tag{4.3}$$

Then there exists a probability distribution μ on $\mathscr{X}$ such that

$$\mathop{\mathbf{E}}_{\mu} [f(x)\chi_i(x)] = 0, \qquad i = 1, 2, \ldots, k.$$

By way of notation, we remind the reader that $\langle f, g \rangle_{\mathscr{X}} = \frac{1}{|\mathscr{X}|} \sum_{x \in \mathscr{X}} f(x)g(x)$ for any real-valued functions f and g and a nonempty subset $\mathscr{X}$ of their domain. In words, Theorem 4.3 states that if $\chi_1, \chi_2, \ldots, \chi_k$ each have small correlation with f and, in addition, have small pairwise correlations, then a distribution exists with respect to which f is completely uncorrelated with $\chi_1, \chi_2, \ldots, \chi_k$. We are now in a position to prove the existence of the promised fooling distributions. In the statement that follows, recall that $H(p) = -p \log p - (1-p)\log(1-p)$ is the binary entropy function.

LEMMA 4.4. *Fix $\delta \in [0, 1/2)$ and a nonempty multiset $Z = \{z_1, z_2, \ldots, z_n\}$ of integers. Let m be an integer with*

$$2 \leqslant m \leqslant \left(\frac{2(1-2\delta)}{1 + \operatorname{disc}(Z, m)} \right)^{(\frac{1}{2}-\delta)n} 2^{-H(\delta)n-2}. \tag{4.4}$$

Define

$$\mathscr{X}_s = \left\{ x \in \{0,1\}^n : \sum_{j=1}^{n} z_j x_j \equiv s \pmod{m} \right\}, \qquad s \in \mathbb{Z}. \tag{4.5}$$

Then each $\mathscr{X}_s$ is nonempty. Moreover, there is a probability distribution μ_s on $\mathscr{X}_s$ (for each s) such that

$$\mathop{\mathbf{E}}_{X\sim\mu_s} p(X) = \mathop{\mathbf{E}}_{X\sim\mu_{s'}} p(X) \tag{4.6}$$

for all $s, s' \in \mathbb{Z}$ and all real polynomials $p\colon \{0,1\}^n \to \mathbb{R}$ of degree at most δn.

Proof. For a subset $A \subseteq \{1,2,\ldots,n\}$, define $\chi_A\colon \{0,1\}^n \to \{-1,+1\}$ by $\chi_A(x) = (-1)^{\sum_{i\in A} x_i}$. The centerpiece of the proof is the following claim.

Claim 4.5. *For every $s \in \mathbb{Z}$ and every nonempty proper subset $A \subset \{1,2,\ldots,n\}$,*

$$\mathscr{X}_s \neq \varnothing, \tag{4.7}$$

$$|\langle \chi_A, 1\rangle_{\mathscr{X}_s}| \leqslant 2m \left(\frac{1+\operatorname{disc}(Z,m)}{2}\cdot\frac{n}{n-|A|}\right)^{\frac{n-|A|}{2}}. \tag{4.8}$$

We will proceed with the main proof and settle the claim after we are finished. Fix $s \in \mathbb{Z}$ arbitrarily. Let $\mathscr{A}$ denote the family of nonempty subsets of $\{1,2,\ldots,n\}$ of cardinality at most δn. Recall from (2.2) that

$$|\mathscr{A}| \leqslant 2^{H(\delta)n} - 1. \tag{4.9}$$

As a result,

$$\begin{aligned}\sum_{A\in\mathscr{A}} |\langle \chi_A, 1\rangle_{\mathscr{X}_s}| &\leqslant |\mathscr{A}| \cdot \max_{1\leqslant |A|\leqslant \delta n} |\langle \chi_A, 1\rangle_{\mathscr{X}_s}| \\ &\leqslant (2^{H(\delta)n}-1)\cdot 2m \max_{1\leqslant k\leqslant \delta n}\left(\frac{1+\operatorname{disc}(Z,m)}{2}\cdot\frac{n}{n-k}\right)^{\frac{n-k}{2}} \\ &= (2^{H(\delta)n}-1)\cdot 2m \left(\frac{1+\operatorname{disc}(Z,m)}{2(1-\delta)}\right)^{\frac{(1-\delta)n}{2}} \\ &< \frac{1}{2}, \end{aligned} \tag{4.10}$$

where the second step uses (4.9) and Claim 4.5; the third step is valid because $1+\operatorname{disc}(Z,m) < 2(1-\delta)$ by (4.4); and the final step is immediate from (4.4). An analogous calculation shows that for every $A \in \mathscr{A}$,

$$\begin{aligned}\sum_{A'\in\mathscr{A}\setminus\{A\}} |\langle \chi_A, \chi_{A'}\rangle_{\mathscr{X}_s}| &= \sum_{\substack{A'\in\mathscr{A}\\ A'\neq A}} |\langle \chi_{A\oplus A'}, 1\rangle_{\mathscr{X}_s}| \\ &\leqslant (2^{H(\delta)n}-1)\cdot 2m \left(\frac{1+\operatorname{disc}(Z,m)}{2(1-2\delta)}\right)^{\frac{(1-2\delta)n}{2}} \\ &< \frac{1}{2}, \end{aligned} \tag{4.11}$$

where the second step follows from (4.9) and Claim 4.5, and the last step uses (4.4).

Recall from Claim 4.5 that each $\mathscr{X}_s$ is nonempty. Applying Theorem 4.3 with (4.10) and (4.11) to the functions χ_A $(A \in \mathscr{A})$ and $f = 1$, we infer the existence of a probability distribution μ_s on $\mathscr{X}_s$ such that

$$\mathop{\mathbf{E}}_{X \sim \mu_s} \chi_A(X) = 0, \qquad\qquad A \in \mathscr{A}. \tag{4.12}$$

Now that the probability distributions μ_s have been constructed for each $s \in \mathbb{Z}$, consider an arbitrary polynomial $p\colon \{0,1\}^n \to \mathbb{R}$ of degree at most δn. Then $p = \sum_{|A| \leqslant \delta n} p_A \chi_A$ for some reals p_A. As a result, (4.12) implies that $\mathbf{E}_{\mu_s} p = p_\varnothing$ for all $s \in \mathbb{Z}$, thereby settling (4.6). ∎

Proof of Claim 4.5. By symmetry, we may assume that $A = \{1, 2, \ldots, k\}$ for some $0 < k < n$. Let $X = (X_1, X_2, \ldots, X_n)$ be a random variable with uniform distribution on $\{0,1\}^n$. Then

$$\begin{aligned}
\frac{|\mathscr{X}_s|}{2^n} &\geqslant \frac{1}{m} - \left| \frac{|\mathscr{X}_s|}{2^n} - \frac{1}{m} \right| \\
&= \frac{1}{m} - \left| \mathop{\mathbf{P}}_{X}[X \in \mathscr{X}_s] - \frac{1}{m} \right| \\
&\geqslant \frac{1}{m} - \left(\frac{1 + \operatorname{disc}(Z, m)}{2} \right)^{n/2} \\
&\geqslant \frac{1}{2m},
\end{aligned} \tag{4.13}$$

where the last two steps follow from Lemma 4.2 and (4.4), respectively. This settles (4.7). Moreover,

$$\begin{aligned}
&\frac{|\mathscr{X}_s|}{2^n}|\langle \chi_A, 1\rangle_{\mathscr{X}_s}| \\
&\qquad = \left| \mathop{\mathbf{E}}_{X} \chi_{\{1,2,\dots,k\}}(X)\cdot \mathbf{I}[X\in\mathscr{X}_s]\right| \\
&\qquad = \left| \sum_{x\in\{0,1\}^k} \frac{(-1)^{x_1+\dots+x_k}}{2^k}\, \mathbf{P}[x_1\dots x_k X_{k+1}\dots X_n\in\mathscr{X}_s]\right| \\
&\qquad = \left| \sum_{x\in\{0,1\}^k} \frac{(-1)^{x_1+\dots+x_k}}{2^k} \left(\mathbf{P}[x_1\dots x_k X_{k+1}\dots X_n\in\mathscr{X}_s] - \frac{1}{m}\right)\right| \\
&\qquad \leqslant \frac{1}{2^k}\sum_{x\in\{0,1\}^k} \left| \mathbf{P}[x_1\dots x_k X_{k+1}\dots X_n\in\mathscr{X}_s] - \frac{1}{m}\right| \\
&\qquad = \frac{1}{2^k}\sum_{x\in\{0,1\}^k} \left| \mathbf{P}\left[\sum_{j=k+1}^{n} z_j X_j \equiv s - \sum_{j=1}^{k} z_j x_j \pmod m\right] - \frac{1}{m}\right| \\
&\qquad \leqslant \left(\frac{1+\operatorname{disc}(\{z_{k+1}, z_{k+2}, \dots, z_n\}, m)}{2}\right)^{(n-k)/2} \\
&\qquad \leqslant \left(\frac{1+\operatorname{disc}(Z,m)}{2}\cdot\frac{n}{n-k}\right)^{(n-k)/2}, \qquad (4.14)
\end{aligned}$$

where the third step uses $k \geqslant 1$; the next-to-last step is legitimate by Lemma 4.2; and the last step applies Proposition 3.1. Now (4.8) is immediate from (4.13) and (4.14). □

4.3. The univariate reduction. At last, we present a generic construction of a halfspace whose approximation by rational functions and polynomials gives corresponding approximants for the sign function on the discrete set $\{\pm1, \pm2, \dots, \pm m\}$. In more detail, let $z_1, z_2, \dots, z_n$ be given integers. For any such n-tuple, we define an associated halfspace and prove a lower bound on m in terms of the discrepancy of the multiset $\{z_1, z_2, \dots, z_n\}$. The following first-principles calculation will be helpful.

Proposition 4.6. *Let $a_1, a_2, \dots, a_k \in \mathbb{R}$ and $b_1, b_2, \dots, b_k > 0$. Then*

$$\min \frac{a_i}{b_i} \leqslant \frac{\mathbf{E}\, a_i}{\mathbf{E}\, b_i} \leqslant \max \frac{a_i}{b_i}. \qquad (4.15)$$

Proof. Abbreviate $m = \min a_i/b_i$ and $M = \max a_i/b_i$. Since each b_i is positive, we obtain $mb_i \leqslant a_i \leqslant Mb_i$. Taking a weighted sum of these inequalities, we arrive at $m\,\mathbf{E}\, b_i \leqslant \mathbf{E}\, a_i \leqslant M\,\mathbf{E}\, b_i$, which is equivalent to (4.15). □

We have:

THEOREM 4.7. *Fix $\delta \in [0, 1/2)$ and a nonempty multiset $Z = \{z_1, z_2, \ldots, z_n\}$ of integers. Let m be an integer with*

$$2 \leqslant m \leqslant \left(\frac{2(1-2\delta)}{1+\operatorname{disc}(Z,m)}\right)^{\left(\frac{1}{2}-\delta\right)n} 2^{-H(\delta)n-2}. \tag{4.16}$$

Define $f\colon \{0,1\}^n \times \{0,1\}^n \to \{-1,+1\}$ by

$$f(x,y) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{j=1}^{n} (z_j \bmod m) x_j - m \sum_{j=1}^{n} y_j\right).$$

Then

$$R(f, d_0, d_1) \geqslant R(\operatorname{sgn}|_{\{\pm 1, \pm 2, \ldots, \pm m\}}, 2d_0, 2d_1)$$

for all $d_0, d_1 = 0, 1, 2, \ldots, \lfloor \delta n/2 \rfloor$.

Proof. Fix $0 < \epsilon < 1$ arbitrarily for the remainder of the proof, and suppose that $R(f, d_0, d_1) < \epsilon$ for some $d_0, d_1 \leqslant \delta n/2$. Our goal is to show that

$$R(\operatorname{sgn}|_{\{\pm 1, \pm 2, \ldots, \pm m\}}, 2d_0, 2d_1) < \epsilon. \tag{4.17}$$

The proof is algorithmic and involves three steps. Given any approximant for f, we will first manipulate it to control the sign behavior in the numerator and denominator, then symmetrize it with respect to y, and finally—the arduous part of the proof—symmetrize it with respect to x. The result of these manipulations will be a univariate approximant for the sign function.

Step 1: Original approximant. Since $R(f, d_0, d_1) < \epsilon$, there are polynomials p and q of degree at most d_0 and d_1, respectively, with

$$\left| f(x,y) - \frac{p(x,y)}{q(x,y)} \right| < \epsilon$$

for all $x, y \in \{0,1\}^n$. This inequality is equivalent to

$$1 - \epsilon < \frac{p(x,y)}{q(x,y)} f(x,y) < 1 + \epsilon. \tag{4.18}$$

Observe that for all $x, y \in \{0,1\}^n$, we have $p(x,y) \neq 0$ and $q(x,y) \neq 0$, where the former is a consequence of $\epsilon < 1$ and the latter follows from the definition of a rational approximant. As a result, (4.18) gives

$$1 - \epsilon < \frac{p(x,y)q(x,y)f(x,y)}{q(x,y)^2} < 1 + \epsilon, \tag{4.19}$$

$$1 - \epsilon < \frac{p(x,y)^2}{p(x,y)q(x,y)f(x,y)} < 1 + \epsilon. \tag{4.20}$$

Step 2: Symmetrization on y. The fractions in (4.19) and (4.20) have positive numerators and denominators. Therefore, Proposition 4.6 implies that

$$1-\epsilon < \frac{\mathbf{E}_{\sigma\in S_n}[p(x,\sigma y)q(x,\sigma y)f(x,\sigma y)]}{\mathbf{E}_{\sigma\in S_n}[q(x,\sigma y)^2]} < 1+\epsilon, \tag{4.21}$$

$$1-\epsilon < \frac{\mathbf{E}_{\sigma\in S_n}[p(x,\sigma y)^2]}{\mathbf{E}_{\sigma\in S_n}[p(x,\sigma y)q(x,\sigma y)f(x,\sigma y)]} < 1+\epsilon. \tag{4.22}$$

Minsky and Papert's symmetrization technique (Proposition 2.15) ensures the existence of polynomials p^*, q^*, r^* of degree at most $2d_0$, $2d_1$, and d_0+d_1, respectively, such that for all $x, y \in \{0,1\}^n$,

$$\begin{aligned}
\mathop{\mathbf{E}}_{\sigma\in S_n}[p(x,\sigma y)^2] &\equiv p^*(x,|y|),\\
\mathop{\mathbf{E}}_{\sigma\in S_n}[q(x,\sigma y)^2] &\equiv q^*(x,|y|),\\
\mathop{\mathbf{E}}_{\sigma\in S_n}[p(x,\sigma y)q(x,\sigma y)] &\equiv r^*(x,|y|).
\end{aligned}$$

Moreover,

$$f(x,\sigma y) \equiv f^*(x,|y|)$$

for all $\sigma \in S_n$, where $f^*\colon \{0,1\}^n \times \{0,1,2,\ldots,n\} \to \{-1,+1\}$ is given by

$$f^*(x,t) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{j=1}^{n} (z_j \bmod m)x_j - mt\right).$$

Now (4.21) and (4.22) simplify to

$$1-\epsilon < \frac{r^*(x,t)f^*(x,t)}{q^*(x,t)} < 1+\epsilon, \tag{4.23}$$

$$1-\epsilon < \frac{p^*(x,t)}{r^*(x,t)f^*(x,t)} < 1+\epsilon \tag{4.24}$$

for all $x \in \{0,1\}^n$ and $t = 0,1,2,\ldots n$. The numerators and denominators of these fractions are again positive, being averages of positive numbers.

Step 3: Symmetrization on x. We have reached the most demanding part of the proof, where we symmetrize the approximants obtained so far with respect to x. For $s \in \mathbb{Z}$, let $\mathscr{X}_s \subseteq \{0,1\}^n$ be given by (4.5). Then Lemma 4.4 guarantees that each $\mathscr{X}_s$ is nonempty, and additionally provides a probability distribution μ_s on $\mathscr{X}_s$ (for each $s \in \mathbb{Z}$) such that for every polynomial $P\colon \{0,1\}^n \to \mathbb{R}$,

$$\deg P \leqslant \delta n \quad\implies\quad \mathop{\mathbf{E}}_{\mu_s} P(x) = \mathop{\mathbf{E}}_{\mu_{s'}} P(x) \qquad \forall s, s' \in \mathbb{Z}. \tag{4.25}$$

Now fix an integer $s \in [-m-1, m-1]$. On the support of μ_s, we have

$$\begin{aligned}\sum_{j=1}^{n}(z_j \bmod m)x_j - s &\in [0 \cdot n - m + 1, (m-1)\cdot n + m + 1] \cap m\mathbb{Z} \\ &\subseteq (-m, (n+1)m) \cap m\mathbb{Z} \\ &= \{0, m, 2m, \ldots, nm\},\end{aligned}$$

where the second step is valid because $n \geqslant 2$ by (4.16). It follows that on the support of μ_s, the linear form

$$\ell(x,s) = \frac{1}{m}\left(\sum_{j=1}^{n}(z_j \bmod m)x_j - s\right)$$

ranges in $\{0, 1, 2, \ldots, n\}$, forcing $f^*(x, \ell(x,s)) = \operatorname{sgn}(s + \frac{1}{2})$. Now (4.23) and (4.24) imply that

$$\begin{aligned}1 - \epsilon &< \frac{r^*(x, \ell(x,s)) \operatorname{sgn}(s+\frac{1}{2})}{q^*(x, \ell(x,s))} < 1 + \epsilon, \\ 1 - \epsilon &< \frac{p^*(x, \ell(x,s))}{r^*(x, \ell(x,s)) \operatorname{sgn}(s+\frac{1}{2})} < 1 + \epsilon\end{aligned}$$

for all integers $s \in [-m-1, m-1]$ and all x in the support of μ_s. Since the numerators and denominators of these fractions are positive, Proposition 4.6 allows us to pass to expectations with respect to $x \sim \mu_s$ to obtain

$$\begin{aligned}1 - \epsilon &< \frac{\mathbf{E}_{x\sim\mu_s}[r^*(x, \ell(x,s))] \operatorname{sgn}(s+\frac{1}{2})}{\mathbf{E}_{x\sim\mu_s}[q^*(x, \ell(x,s))]} < 1 + \epsilon, \\ 1 - \epsilon &< \frac{\mathbf{E}_{x\sim\mu_s}[p^*(x, \ell(x,s))]}{\mathbf{E}_{x\sim\mu_s}[r^*(x, \ell(x,s))] \operatorname{sgn}(s+\frac{1}{2})} < 1 + \epsilon,\end{aligned}$$

or equivalently

$$\left|\frac{\mathbf{E}_{x\sim\mu_s}[r^*(x, \ell(x,s))]}{\mathbf{E}_{x\sim\mu_s}[q^*(x, \ell(x,s))]} - \operatorname{sgn}\left(s + \frac{1}{2}\right)\right| < \epsilon, \tag{4.26}$$

$$\left|\frac{\mathbf{E}_{x\sim\mu_s}[p^*(x, \ell(x,s))]}{\mathbf{E}_{x\sim\mu_s}[r^*(x, \ell(x,s))]} - \operatorname{sgn}\left(s + \frac{1}{2}\right)\right| < \epsilon, \tag{4.27}$$

for all integers $s \in [-m-1, m-1]$.

Consider the univariate polynomials

$$\begin{aligned}p^{**}(s) &= \mathop{\mathbf{E}}_{x\sim\mu_s}[p^*(x, \ell(x,s))], \\ q^{**}(s) &= \mathop{\mathbf{E}}_{x\sim\mu_s}[q^*(x, \ell(x,s))], \\ r^{**}(s) &= \mathop{\mathbf{E}}_{x\sim\mu_s}[r^*(x, \ell(x,s))].\end{aligned}$$

Equations (4.26) and (4.27) show that $r^{**}(s-1)/q^{**}(s-1)$ and $p^{**}(s-1)/r^{**}(s-1)$ approximate $\operatorname{sgn} s$ pointwise on $\{\pm1,\pm2,\ldots,\pm m\}$ to error less than ϵ. Moreover, (4.25) ensures that the degrees of p^{**},q^{**},r^{**} are at most the degrees of p^*,q^*,r^*, respectively. We conclude that

$$R(\operatorname{sgn}|_{\{\pm1,\pm2,\ldots,\pm m\}},d_0+d_1,2d_1)<\epsilon,$$
$$R(\operatorname{sgn}|_{\{\pm1,\pm2,\ldots,\pm m\}},2d_0,d_0+d_1)<\epsilon.$$

These complementary bounds force (4.17) and thereby complete the proof. ∎

4.4. The master theorem. We now combine Theorem 4.7 with the efficient construction, in Theorem 3.7, of an integer set with small m-discrepancy for $m=2^{\Theta(n)}$. The result is an explicit halfspace $h_n\colon\{0,1\}^n\to\{-1,+1\}$ whose approximation by polynomials and rational functions is asymptotically equivalent to the univariate approximation of the sign function on $\{\pm1,\pm2,\pm3,\ldots,\pm2^{\Theta(n)}\}$. We refer to this result as our *master theorem* since all our main theorems are derived from it.

THEOREM 4.8. *For some constant $c'>0$, there is an algorithm that takes as input an integer $n\geqslant1$, runs in time polynomial in n, and outputs a halfspace $h_n\colon\{0,1\}^n\to\{-1,+1\}$ with*

$$R(h_n,d_0,d_1)\geqslant R\left(\operatorname{sgn}|_{\{\pm1,\pm2,\pm3,\ldots,\pm2^{\lfloor c'n\rfloor}\}},2d_0,2d_1\right) \tag{4.28}$$

for all $d_0,d_1=0,1,2,\ldots,\lfloor c'n\rfloor$. Moreover, the constant c' and the algorithm are given explicitly.

Proof. Let

$$c'=\min\left\{\frac{1}{200},\frac{1}{2C_{1/10}}\right\}, \tag{4.29}$$

where $C_{1/10}\geqslant1$ is the constant defined in Theorem 3.7. On input n, the construction of h_n is as follows. For $n<1/c'$, the sought property (4.28) amounts to $R(h_n,0,0)\geqslant R(\operatorname{sgn}|_{\{-1,1\}},0,0)$, which is in turn equivalent to $R(h_n,0,0)\geqslant1$ and holds trivially for the halfspace $h_n(x)=(-1)^{x_1}$.

We now turn to the nontrivial case, $n\geqslant1/c'$. Abbreviate $m=2^{\lfloor c'n\rfloor}$. Then the algorithm of Theorem 3.7 constructs, in time polynomial in n, a nonempty multiset Z with m-discrepancy

$$\operatorname{disc}(Z,m)\leqslant\frac{1}{10} \tag{4.30}$$

and cardinality $|Z|\leqslant n/2$. Observe that for any integer $k\geqslant1$, the union of k copies of Z is a multiset with m-discrepancy $\operatorname{disc}(Z,m)$ and cardinality $k|Z|$. Therefore, we may assume without loss of generality that

$$\frac{n}{4}\leqslant|Z|\leqslant\frac{n}{2}. \tag{4.31}$$

We let

$$h_n(x) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{j=1}^{|Z|}(z_j \bmod m)x_j - m\sum_{j=|Z|+1}^{2|Z|} x_j\right),$$

where $z_1, z_2, z_3, \ldots, z_{|Z|}$ denote the elements of the multiset Z. Taking $\delta = 1/25$, we have from (4.29) and (4.31) that

$$c'n \leqslant \frac{\delta|Z|}{2}. \tag{4.32}$$

Moreover,

$$\begin{aligned} m &\in [2, 2^{c'n}] \\ &\subseteq [2, 2^{n/200}] \\ &\subseteq \left[2, \left(\frac{2(1-2\delta)}{1+\operatorname{disc}(Z,m)}\right)^{(\frac{1}{2}-\delta)\cdot|Z|} 2^{-H(\delta)\cdot|Z|-2}\right], \end{aligned}$$

where the second step applies (4.29), and the third step uses (4.30), (4.31), and $n \geqslant 1/c' \geqslant 200$. As a result, Theorem 4.7 implies (4.28) for all $d_0, d_1 \leqslant \delta|Z|/2$. In view of (4.32), the proof is complete. ∎

5. Main results

Using the halfspace h_n constructed in our master theorem, we will now establish the main results of this paper.

5.1. Polynomial approximation. Prior to our work, the strongest lower bound for the approximation of an explicit halfspace $f_n\colon \{0,1\}^n \to \{-1,+1\}$ by polynomials was $E(f_n, c\sqrt{n}) \geqslant 1 - 2^{-c\sqrt{n}}$ for an absolute constant $c > 0$, proved in [76, 77]. The result that we are about to prove is a quadratic improvement on previous work, with respect to both degree and error. As we will discuss shortly, this new result is essentially the best possible.

Theorem 5.1 (Polynomial approximation). *Let $h_n\colon \{0,1\}^n \to \{-1,+1\}$ be the halfspace constructed in Theorem 4.8. Then for some constant $c > 0$ and all n,*

$$E(h_n, cn) > 1 - 2^{-cn}. \tag{5.1}$$

Proof. Let $c' > 0$ be the constant in Theorem 4.8. Then

$$\begin{aligned} E(h_n, c'n) &\geqslant E(\operatorname{sgn}|_{\{\pm1,\pm2,\pm3,\ldots,\pm2^{\lfloor c'n\rfloor}\}}, 2\lfloor c'n\rfloor) \\ &\geqslant 1 - O\left(\frac{n}{2^{c'n}}\right)^{1/2}, \end{aligned}$$

where the first step corresponds to taking $d_0 = \lfloor c'n\rfloor$ and $d_1 = 0$ in Theorem 4.8, and the second step is immediate from Proposition 2.9. This implies (5.1) for $c > 0$ small enough. ∎

Theorem 5.1 is essentially as strong as one could hope for. First of all, any function in n Boolean variables can be approximated to zero error by a polynomial of degree at most n, i.e., at most a constant factor larger than what is assumed in (5.1). Moreover, a classic result due to Muroga [58] implies that for every halfspace, the error bound in (5.1) is almost achieved by polynomials of degree 1:

Fact 5.2. *There is an absolute constant $c > 0$ such that for every n and every halfspace $h\colon \{0,1\}^n \to \{-1,+1\}$,*

$$E(h,1) \leqslant 1 - n^{-cn}.$$

Proof. Muroga [58] showed that every halfspace $h\colon \{0,1\}^n \to \{-1,+1\}$ can be represented as $h(x) = \operatorname{sgn}(\sum_{j=1}^n z_jx_j - \theta)$ for some integers $z_1, z_2, \ldots, z_n, \theta$ whose absolute values sum to $n^{O(n)}$. It follows that

$$\begin{aligned} E(h,1) &\leqslant \max_{x\in\{0,1\}^n} \left| h(x) - \frac{1}{|\theta| + \sum_{j=1}^n |z_j|} \left(\sum_{j=1}^n z_jx_j - \theta \right) \right| \\ &\leqslant 1 - \frac{1}{|\theta| + \sum_{j=1}^n |z_j|} \\ &\leqslant 1 - n^{-O(n)}. \end{aligned}$$ □

5.2. Rational approximation. We now show that the halfspace h_n constructed in our master theorem cannot be approximated pointwise to any small constant except by rational functions of degree $\Omega(n)$. This degree lower bound matches the trivial upper bound and is a quadratic improvement on the previous best construction [76, 77]. More generally, we derive a lower bound on the approximation of h_n by rational functions of any given degree d, and this lower bound too is essentially the best possible for any halfspace. Details follow.

Theorem 5.3 (Rational approximation). *Let $h_n\colon \{0,1\}^n \to \{-1,+1\}$ be the halfspace constructed in Theorem 4.8. Then for some constant $c > 0$ and all n,*

$$R(h_n, d) \geqslant 1 - \exp\left(-\frac{cn}{d}\right), \qquad d = 1, 2, \ldots, \lfloor cn \rfloor. \tag{5.2}$$

Proof. Let $c' > 0$ be the constant in Theorem 4.8. Then for $d = 1, 2, \ldots, \lfloor c'n \rfloor$, we have

$$\begin{aligned} R(h_n, d) &\geqslant R(\operatorname{sgn}|_{\{\pm 1, \pm 2, \pm 3, \ldots, \pm 2^{\lfloor c'n \rfloor}\}}, 2d) \\ &\geqslant 1 - \exp\left(-\Theta\left(\frac{n}{d}\right)\right), \end{aligned}$$

where the first step corresponds to taking $d_0 = d_1 = d$ in Theorem 4.8, and the second step is immediate from Theorem 2.11. This implies (5.2) for $c > 0$ small enough. □

We now show that the lower bounds on the approximation error in Theorem 5.3 are essentially the best possible for any halfspace.

FACT 5.4. *There exists an absolute constant $c > 0$ such that for every n and every halfspace $h\colon \{0,1\}^n \to \{-1,+1\}$,*

$$R(h,d) \leqslant 1 - \exp\left(-\frac{cn\log n}{d}\right), \qquad d = 1,2,\ldots,n.$$

Proof. As already mentioned, Muroga [58] showed that $h(x) \equiv \operatorname{sgn} p(x)$ for some linear polynomial $p(x)$ that ranges in $[-N,-1]\cup[1,N]$, where $N = \exp(cn\log n)$ for some absolute constant $c > 0$. This makes it possible to obtain a rational approximant for $h(x)$ by taking any rational approximant for the sign function on $[-N,-1]\cup[1,N]$ and composing it with $p(x)$. We conclude that for any integer d,

$$\begin{aligned} R(h,d) &\leqslant R(\operatorname{sgn}|_{[-N,-1]\cup[1,N]}, d) \\ &\leqslant 1 - \frac{1}{N^{1/d}} \\ &= 1 - \exp\left(-\frac{cn\log n}{d}\right), \end{aligned}$$

where the second step uses Newman's rational approximation (Fact 2.10). ∎

5.3. Threshold degree. Here, we use the halfspace h_n constructed in our master theorem to study the degree required to sign-represent intersections of halfspaces. Our result is a lower bound of $\Omega(n)$ for the intersection $h_n \wedge h_n$ of two independent copies of h_n. This result improves quadratically on the previous best construction [76, 77] and matches the trivial upper bound of $O(n)$ for sign-representing any Boolean function in n variables.

THEOREM 5.5. *Let $h_n\colon \{0,1\}^n \to \{-1,+1\}$ be the halfspace constructed in Theorem 4.8. Then*

$$\deg_\pm(h_n \wedge h_n) = \Omega(n).$$

Proof. Abbreviate $D_n = \deg_\pm(h_n \wedge h_n)$. Taking $f = g = h_n$ in Theorem 2.14 shows that $R(h_n, 4D_n) < 1/2$, which by Theorem 5.3 forces $D_n = \Omega(n)$. ∎

Theorem 5.5 should be contrasted with the result of Beigel et al. [17] that the conjunction of any constant number of majority functions on $\{0,1\}^n$ has threshold degree $O(\log n)$. We now derive a lower bound of $\Omega(\sqrt{n\log n})$ on the threshold degree of the intersection of an explicitly given halfspace and a majority function, improving quadratically on the previous best construction [76, 77]. As we discuss shortly, the new construction is optimal up to a logarithmic factor.

THEOREM 5.6. *Let $h_n\colon \{0,1\}^n \to \{-1,+1\}$ be the halfspace constructed in Theorem 4.8. Then*

$$\deg_\pm(h_n \wedge \mathrm{MAJ}_n) = \Omega(\sqrt{n\log n}). \tag{5.3}$$

Proof. Abbreviate $D_n = \deg_\pm(h_n \wedge \mathrm{MAJ}_n)$. Then $R(h_n, 4D_n) + R(\mathrm{MAJ}_n, 2D_n) < 1$ by Theorem 2.14. The lower bounds for the rational approximation of h_n and MAJ_n in Theorems 2.12 and 5.3 now imply that $D_n = \Omega(\sqrt{n\log n})$. ∎

Remark 5.7. The construction of Theorem 5.6 is essentially the best possible, in that

$$\deg_{\pm}(h \wedge \mathrm{MAJ}_n) = O(\sqrt{n}\log n) \tag{5.4}$$

for every halfspace $h\colon \{0,1\}^n \to \{-1,+1\}$. Indeed, taking $d = C\sqrt{n}\log n$ in Theorem 2.12 and Fact 5.4 for a large enough constant $C \geqslant 1$ yields $R(h, C\sqrt{n}\log n) + R(\mathrm{MAJ}_n, C\sqrt{n}\log n) < 1$, which in turn implies (5.4) in view of Theorem 2.13.

5.4. Threshold density. In addition to threshold degree, several other complexity measures are of interest when sign-representing Boolean functions by real polynomials. One such complexity measure is *threshold density*, defined as the least k for which a given function can be sign-represented by a linear combination of k parity functions. Formally, for a given function $f\colon \{0,1\}^n \to \{-1,+1\}$, its threshold density $\mathrm{dns}(f)$ is the minimum size $|\mathscr{S}|$ of a family $\mathscr{S} \subseteq \mathscr{P}(\{1,2,\ldots,n\})$ such that

$$f(x) \equiv \operatorname{sgn}\left(\sum_{S\in\mathscr{S}} w_S(-1)^{\sum_{j\in S} x_j}\right)$$

for some reals w_S. It is clear from the definition that $\mathrm{dns}(f) \leqslant 2^n$ for all functions $f\colon \{0,1\}^n \to \{-1,+1\}$, and we will now construct a pair of halfspaces whose intersection has threshold density $2^{\Theta(n)}$. Prior to our work, the best construction [76] had threshold density $2^{\Theta(\sqrt{n})}$.

To proceed, we recall a technique due to Krause and Pudlák [48] that transforms Boolean functions with high threshold degree into Boolean functions with high threshold density. Their transformation works in a black-box manner and sends a function $f\colon \{0,1\}^n \to \{-1,+1\}$ to the function $f^{\mathrm{KP}}\colon (\{0,1\}^n)^3 \to \{-1,+1\}$ defined by

$$f^{\mathrm{KP}}(x,y,z) = f(\ldots, (\overline{z_i} \wedge x_i) \vee (z_i \wedge y_i), \ldots).$$

The threshold degree of f and the threshold density of f^{KP} are related as follows [48, Proposition 2.1].

Theorem 5.8 (Krause and Pudlák). *For every function $f\colon \{0,1\}^n \to \{-1,+1\}$,*

$$\mathrm{dns}(f^{\mathrm{KP}}) \geqslant 2^{\deg_{\pm}(f)}.$$

We are now in a position to obtain the claimed density results.

Theorem 5.9. *There is an (explicit) algorithm that takes as input an integer $n \geqslant 1$, runs in time polynomial in n, and outputs a halfspace $H_n\colon \{0,1\}^n \to \{-1,+1\}$ such that*

$$\mathrm{dns}(H_n \wedge H_n) = 2^{\Omega(n)}, \tag{5.5}$$

$$\mathrm{dns}(H_n \wedge \mathrm{MAJ}_n) = 2^{\Omega(\sqrt{n\log n})}. \tag{5.6}$$

Proof. For any function $f\colon \{0,1\}^n \to \{0,1\}$, standard arithmetization gives

$$f^{\mathrm{KP}}(x,y,z) = f\left(\ldots, \frac{1}{2}(x_i + y_i + x_i \oplus z_i - y_i \oplus z_i), \ldots\right), \tag{5.7}$$

where $a \oplus b \in \{0,1\}$ denotes as usual the XOR of a and b. Similarly, one has

$$\mathrm{MAJ}_n^{\mathrm{KP}}(x,y,z) = \mathrm{MAJ}_{4n}(x, y, x \oplus z, \overline{y \oplus z}), \tag{5.8}$$

where the XOR and complement operations are applied bitwise.

Let $h_n\colon \{0,1\}^n \to \{-1,+1\}$ be the halfspace from Theorem 5.5, so that $h_n \wedge h_n$ has threshold degree $\Omega(n)$. By Theorem 5.8, the function $(h_n \wedge h_n)^{\mathrm{KP}} = h_n^{\mathrm{KP}} \wedge h_n^{\mathrm{KP}}$ has threshold density $2^{\Omega(n)}$. Observe from (5.7) that $h_n^{\mathrm{KP}} \wedge h_n^{\mathrm{KP}}$ is the result of starting with the intersection $H_{4n} \wedge H_{4n}$ of two explicitly given halfspaces in $4n$ variables each, and replacing their input variables with appropriately chosen parity functions. This replacement cannot increase the threshold density because the parity of several parity functions is another parity function. We conclude that $\mathrm{dns}(H_{4n} \wedge H_{4n}) = 2^{\Omega(n)}$. This completes the proof of (5.5).

The proof of (5.6) is closely analogous. Specifically, recall from Theorem 5.6 that $h_n \wedge \mathrm{MAJ}_n$ has threshold degree $\Omega(\sqrt{n \log n})$. By Theorem 5.8, the function $(h_n \wedge \mathrm{MAJ}_n)^{\mathrm{KP}} = h_n^{\mathrm{KP}} \wedge \mathrm{MAJ}_n^{\mathrm{KP}}$ has threshold density $\exp(\Omega(\sqrt{n \log n}))$. It follows from (5.7) and (5.8) that $h_n^{\mathrm{KP}} \wedge \mathrm{MAJ}_n^{\mathrm{KP}}$ is the result of starting with the intersection $H_{4n} \wedge \mathrm{MAJ}_{4n}$ for an explicit halfspace H_{4n} in $4n$ variables, and replacing the input variables with appropriately chosen parity functions or their negations. This replacement cannot increase the threshold density because the parity of several parity functions is another parity function. We conclude that $\mathrm{dns}(H_{4n} \wedge \mathrm{MAJ}_{4n}) = \exp(\Omega(\sqrt{n \log n}))$. This completes the proof of (5.6). ∎

Both lower bounds in Theorem 5.9 are essentially the best possible for any halfspace $H_n\colon \{0,1\}^n \to \{-1,+1\}$. Indeed, the first lower bound is tight by definition, while the second lower bound nearly matches the upper bound of $\exp(O(\sqrt{n} \log^2 n))$ that follows from Remark 5.7.

5.5. Communication complexity. Using the pattern matrix method, we will now "lift" the approximation lower bound of Theorem 5.1 to communication complexity. As a result, we will obtain an explicit separation of k-party communication complexity with unbounded and weakly unbounded error (which for $k = 2$ is equivalent to a separation of sign-rank and discrepancy). Our application of the pattern matrix method is based on the fact that the unique set disjointness function $\mathrm{UDISJ}_{m,k}$ has an exact representation on its domain as a polynomial with a small number of monomials; cf. [75, Section 10], [83, Section 4.2.3], and [80, Section 3.1]. Specifically, define $\mathrm{UDISJ}^*_{m,k}\colon (\{0,1\}^m)^k \to \mathbb{R}$ by

$$\mathrm{UDISJ}^*_{m,k}(x) = -1 + 2\sum_{i=1}^{m} x_{1,i} x_{2,i} \cdots x_{k,i}\,.$$

Then

$$\mathrm{UDISJ}_{m,k}(x) = \mathrm{UDISJ}^*_{m,k}(x), \qquad\qquad x \in \operatorname{dom} \mathrm{UDISJ}_{m,k}. \tag{5.9}$$

THEOREM 5.10. *For some constant $C>1$ and all positive integers n and k, there is an (explicitly given) k-party communication problem $F_{n,k}\colon(\{0,1\}^n)^k\to\{-1,+1\}$ such that*

$$\begin{aligned}\mathrm{UPP}(F_{n,k}) &\leqslant \log n+4, &(5.10)\\ \mathrm{PP}(F_{n,k}) &\geqslant \left\lfloor\frac{n}{C\cdot 4^k}\right\rfloor, &(5.11)\\ \mathrm{disc}(F_{n,k}) &\leqslant \exp\left(-\left\lfloor\frac{n}{C\cdot 4^k}\right\rfloor\right). &(5.12)\end{aligned}$$

Moreover,

$$F_{n,k}(x_1,x_2,\ldots,x_k)=\operatorname{sgn}\left(w_0+\sum_{i=1}^{n}w_ix_{1,i}x_{2,i}\cdots x_{k,i}\right) \tag{5.13}$$

for some explicitly given reals $w_0,w_1,\ldots,w_n$.

Proof. Let $h_n\colon\{0,1\}^n\to\{-1,+1\}$ be the halfspace constructed in Theorem 4.8. Then by definition, $h_n(x)=\operatorname{sgn}p_n(x)$ for a linear polynomial $p_n\colon\mathbb{R}^n\to\mathbb{R}$. Moreover, Theorem 5.1 ensures that

$$\deg_{1-2^{-cn}}(h_n)\geqslant cn \tag{5.14}$$

for some constant $c>0$ independent of n. Abbreviate $m=\lceil 2^{k+1}\mathrm{e}/c\rceil^2$ and consider the k-party communication problem $F'_{n,k}\colon(\{0,1\}^{nm})^k\to\{-1,+1\}$ given by

$$F'_{n,k}=\widetilde{\operatorname{sgn}}\;p_n\left(\frac{1-\mathrm{UDISJ}^*_{m,k}}{2},\frac{1-\mathrm{UDISJ}^*_{m,k}}{2},\ldots,\frac{1-\mathrm{UDISJ}^*_{m,k}}{2}\right), \tag{5.15}$$

where the right-hand side features the coordinatewise composition of the polynomial p_n with n independent copies of the polynomial $(1-\mathrm{UDISJ}^*_{m,k})/2$. The identity (5.9) implies that $F'_{n,k}$ coincides with $h_n\circ\mathrm{UDISJ}_{m,k}$ on the domain of the latter. Therefore,

$$\begin{aligned}\mathrm{disc}(F'_{n,k}) &\leqslant \mathrm{disc}(h_n\circ\mathrm{UDISJ}_{m,k})\\ &\leqslant 2^{-cn}+2^{-cn}\\ &=2\cdot 2^{-cn},\end{aligned} \tag{5.16}$$

where the second step uses (5.14) and the pattern matrix method (Theorem 2.21). Applying the discrepancy method (Corollary 2.20), we obtain

$$\begin{aligned}\mathrm{PP}(F'_{n,k}) &\geqslant \log\frac{2}{\mathrm{disc}(F'_{n,k})}\\ &\geqslant cn.\end{aligned} \tag{5.17}$$

To complete the proof, define the functions $F_{n,k}$ for any positive integers n and k by

$$F_{n,k} = \begin{cases} F'_{\lfloor n/\lceil 2^{k+1}\mathrm{e}/c\rceil^2\rfloor,k} & \text{if } n \geqslant \lceil 2^{k+1}\mathrm{e}/c\rceil^2, \\ 0 & \text{otherwise.} \end{cases}$$

Then (5.11)–(5.13) are immediate from (5.15)–(5.17), whereas (5.10) is a consequence of (5.13) and Fact 2.17. ∎

Theorem 5.10 gives an explicit separation $\mathsf{PP}_k \subsetneq \mathsf{UPP}_k$ for up to $k \leqslant (0.5-\epsilon)\log n$ parties, where $\epsilon > 0$ is an arbitrary constant. The special case $k = 2$ can be equivalently stated as an explicit separation of sign-rank and discrepancy:

Corollary 5.11. *There is an (explicitly given) family* $\{F_n\}_{n=1}^{\infty}$ *of communication problems* $F_n\colon \{0,1\}^n \times \{0,1\}^n \to \{-1,+1\}$ *with*

$$\operatorname{rk}_{\pm}(F_n) \leqslant n+1, \tag{5.18}$$

$$\operatorname{disc}(F_n) = 2^{-\Omega(n)}, \tag{5.19}$$

$$\operatorname{UPP}(F_n) \leqslant \log n + 4, \tag{5.20}$$

$$\operatorname{PP}(F_n) = \Omega(n). \tag{5.21}$$

Moreover,

$$F_n(x,y) = \operatorname{sgn}\left(w_0 + \sum_{i=1}^{n} w_i x_i y_i\right) \tag{5.22}$$

for some explicitly given reals $w_0, w_1, \ldots, w_n$.

Proof. Equations (5.19)–(5.22) result from setting $k = 2$ in Theorem 5.10. The new item, (5.18), is immediate from (5.22). ∎

Theorem 5.10 and Corollary 5.11 settle Theorems 1.3 and 1.2, respectively, from the introduction.

5.6. A circulant expander. Consider a d-regular undirected graph G on n vertices, with adjacency matrix A. Since A is symmetric, it has n real eigenvalues (counting multiplicities). We denote these eigenvalues by $\lambda_1(G) \geqslant \lambda_2(G) \geqslant \cdots \geqslant \lambda_n(G)$ and define $\lambda(G) = \max\{|\lambda_2(G)|, |\lambda_3(G)|, \ldots, |\lambda_n(G)|\}$. It is well known and straightforward to verify that $\lambda_1(G) = d$ and $|\lambda_i(G)| \leqslant d$ for $i = 2, 3, \ldots, n$. We say that G is an ϵ-*expander* if $\lambda(G) \leqslant \epsilon d$. This spectral notion is intimately related to key graph-theoretic and stochastic properties of G, such as vertex expansion and the convergence rate of a random walk on G to the uniform distribution. One is typically interested in ϵ-expanders that are d-regular for d as small as possible, where $0 < \epsilon < 1$ is a constant. The existence of expanders with strong parameters can be verified using the probabilistic method [6], and explicit constructions are known as well.

In this section, we study the problem of constructing *circulant* expanders. Formally, a graph is *circulant* if its adjacency matrix is circulant. It is clear that a circulant graph is d-regular for some d, meaning that every vertex has out-degree d and in-degree d. We focus on circulant graphs that are undirected and have no self-loops, which corresponds to adjacency matrices that are symmetric and have zeroes on the diagonal. It is well known [5] that for any $0 < \epsilon < 1$ and all large enough n, there exists a circulant ϵ-expander on n vertices of degree $O(\log n)$. This degree bound is asymptotically optimal [5, 29, 53], and the problem of constructing such circulant expanders explicitly has been studied by several authors [4, 2, 5]. The best construction prior to our work, due to Ajtai et al. [2], achieves degree $(\log^* n)^{O(\log^* n)} \log n$. In this section, we construct a circulant ϵ-expander of optimal degree, $O(\log n)$, for any constant $0 < \epsilon < 1$. By way of terminology, recall that the adjacency matrix of a circulant graph on n vertices is $\operatorname{circ}(\mathbf{1}_S)$ for some subset $S \subseteq \{0, 1, 2, \ldots, n-1\}$. With this in mind, we say that an algorithm *constructs a circulant graph on n vertices in time $T(n)$* if the algorithm outputs in time $T(n)$ the elements of the associated subset S. The formal statement of our result follows.

Theorem 5.12. *Let $0 < \epsilon < 1$ be given. Then there is an (explicitly given) algorithm that takes as input an integer $n \geqslant 2$ and constructs in time polynomial in $\log n$ an undirected simple d-regular circulant graph G_n on n vertices, where*

$$1 \leqslant d \leqslant O(\log n), \tag{5.23}$$

$$\lambda(G_n) \leqslant \max\left\{\epsilon, \frac{1}{n-1}\right\} d. \tag{5.24}$$

Proof. Let C_ϵ be the constant from Theorem 3.7. We first consider the trivial case when $2(C_\epsilon \log n)^2 \geqslant n$, which means that n is bounded by an explicit constant. In this case, we take G_n to be the complete graph on n vertices. It is clear that G_n is a d-regular circulant graph for $d = n-1$. The adjacency matrix of G_n is $\operatorname{circ}(0, 1, 1, \ldots, 1)$, whose eigenvalues by Corollary 2.6 are $n-1, -1, -1, \ldots, -1$. In particular, $\lambda(G_n) = 1 = d/(n-1)$. This settles (5.24), whereas (5.23) holds trivially because d and n are bounded by a constant.

We now turn to the nontrivial case when $2(C_\epsilon \log n)^2 < n$. The algorithm of Theorem 3.7 constructs, in time polynomial in $\log n$, a set $Z \subseteq \{0, 1, 2, \ldots, n-1\}$ with

$$\operatorname{disc}(Z, n) \leqslant \epsilon, \tag{5.25}$$

$$1 \leqslant |Z| \leqslant C_\epsilon \log n. \tag{5.26}$$

For any $z, z' \in Z$, the linear congruence $z + \Delta \equiv -(z' + \Delta) \pmod{n}$ has at most two solutions $\Delta \in \{0, 1, 2, \ldots, n-1\}$. Recalling that $2|Z|^2 < n$ in the case under consideration, we conclude that there exists $\Delta \in \{0, 1, 2, \ldots, 2|Z|^2\}$ with

$$z + \Delta \not\equiv -(z' + \Delta) \pmod{n}, \qquad\qquad z, z' \in Z. \tag{5.27}$$

Moreover, such Δ can clearly be found by brute force search in time polynomial in $|Z| = O(\log n)$. Equation (5.27) now implies that no two elements of the multiset $(Z \cup \Delta) \cup (-Z - \Delta)$ are congruent modulo n, and in particular no element of $Z \cup \Delta$ is congruent to 0 modulo n.

We define G_n to be the undirected graph with vertex set $\{0, 1, 2, \ldots, n-1\}$ in which (i, j) is an edge if and only if $i - j$ is congruent modulo n to an element of $(Z + \Delta) \cup (-Z - \Delta)$. The roles of i and j in this definition are symmetric, making G_n an undirected graph. It is obvious that the adjacency matrix of G_n is circulant. Furthermore, G_n has no self-loops because by construction no element of $Z \cup \Delta$ is congruent to 0 modulo n. Since the elements of $(Z + \Delta) \cup (-Z - \Delta)$ are pairwise distinct modulo n, the degree of G_n is $|(Z + \Delta) \cup (-Z - \Delta)| = 2|Z|$. Now (5.23) follows from (5.26). To settle the remaining property (5.24), observe that the first row of the adjacency matrix of G_n is the characteristic vector of the set $((Z+\Delta)\cup(-Z-\Delta)) \bmod n$. As a result, Corollary 2.6 implies that the eigenvalues of the adjacency matrix of G_n are

$$\sum_{z \in Z+\Delta} \omega^{kz} + \sum_{z \in -Z-\Delta} \omega^{kz}, \qquad\qquad k = 0, 1, 2, \ldots, n-1,$$

where ω is a primitive n-th root of unity. Setting $k = 0$ yields the largest eigenvalue, $2|Z|$. The other eigenvalues are bounded by

$$\begin{aligned}
\lambda(G_n) &= \max_{k=1,2,\ldots,n-1} \left| \sum_{z \in Z+\Delta} \omega^{kz} + \sum_{z \in -Z-\Delta} \omega^{kz} \right| \\
&\leqslant \max_{k=1,2,\ldots,n-1} \left| \sum_{z \in Z+\Delta} \omega^{kz} \right| + \max_{k=1,2,\ldots,n-1} \left| \sum_{z \in -Z-\Delta} \omega^{kz} \right| \\
&= 2|Z| \operatorname{disc}(Z, n).
\end{aligned}$$

Along with (5.25), this proves (5.24). ∎

Acknowledgments

I am thankful to Mark Bun, T. S. Jayram, Ryan O'Donnell, Rocco Servedio, and Justin Thaler for valuable comments on this work. Special thanks to T. S. Jayram for allowing me to include his short and elegant proof of Fact 4.1.

References

[1] S. Aaronson and Y. Shi, *Quantum lower bounds for the collision and the element distinctness problems*, J. ACM, 51 (2004), pp. 595–605, doi:10.1145/1008731.1008735.

[2] M. Ajtai, H. Iwaniec, J. Komlós, J. Pintz, and E. Szemerédi, *Construction of a thin set with small Fourier coefficients*, Bulletin of the London Mathematical Society, 22 (1990), pp. 583–590, doi:10.1112/blms/22.6.583.

[3] M. Alekhnovich, M. Braverman, V. Feldman, A. R. Klivans, and T. Pitassi, *The complexity of properly learning simple concept classes*, J. Comput. Syst. Sci., 74 (2008), pp. 16–34, doi:10.1016/j.jcss.2007.04.011.

[4] N. Alon, *Eigenvalues, geometric expanders, sorting in rounds, and Ramsey theory*, Combinatorica, 6 (1986), pp. 207–219, doi:10.1007/BF02579382.

[5] N. Alon and Y. Roichman, *Random Cayley graphs and expanders*, Random Struct. Algorithms, 5 (1994), pp. 271–285, doi:10.1002/rsa.3240050203.

[6] N. Alon and J. Spencer, *The Probabilistic Method*, John Wiley & Sons, 3rd ed., 2008.

[7] A. Ambainis, *Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range*, Theory of Computing, 1 (2005), pp. 37–46, doi:10.4086/toc.2005.v001a003.

[8] A. Ambainis, A. M. Childs, B. Reichardt, R. Špalek, and S. Zhang, *Any AND-OR formula of size N can be evaluated in time $N^{1/2+o(1)}$ on a quantum computer*, SIAM J. Comput., 39 (2010), pp. 2513–2530, doi:10.1137/080712167.

[9] R. I. Arriaga and S. Vempala, *An algorithmic theory of learning: Robust concepts and random projection*, Mach. Learn., 63 (2006), pp. 161–182, doi:10.1007/s10994-006-6265-7.

[10] J. Aspnes, R. Beigel, M. L. Furst, and S. Rudich, *The expressive power of voting polynomials*, Combinatorica, 14 (1994), pp. 135–148, doi:10.1007/BF01215346.

[11] L. Babai, P. Frankl, and J. Simon, *Complexity classes in communication complexity theory*, in *Proceedings of the Twenty-Seventh Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 1986, pp. 337–347, doi:10.1109/SFCS.1986.15.

[12] L. Babai, N. Nisan, and M. Szegedy, *Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs*, J. Comput. Syst. Sci., 45 (1992), pp. 204–232, doi:10.1016/0022-0000(92)90047-M.

[13] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, *Quantum lower bounds by polynomials*, J. ACM, 48 (2001), pp. 778–797, doi:10.1145/502090.502097.

[14] P. Beame, M. David, T. Pitassi, and P. Woelfel, *Separating deterministic from nondeterministic NOF multiparty communication complexity*, in *Proceedings of the Thirty-Fourth International Colloquium on Automata, Languages and Programming* (ICALP), 2007, pp. 134–145, doi:10.1007/978-3-540-73420-8_14.

[15] P. Beame and T. Huynh, *Multiparty communication complexity and threshold circuit size of* AC^0, SIAM J. Comput., 41 (2012), pp. 484–518, doi:10.1137/100792779.

[16] R. Beigel, *Perceptrons, PP, and the polynomial hierarchy*, Computational Complexity, 4 (1994), pp. 339–349, doi:10.1007/BF01263422.

[17] R. Beigel, N. Reingold, and D. A. Spielman, *PP is closed under intersection*, J. Comput. Syst. Sci., 50 (1995), pp. 191–202, doi:10.1006/jcss.1995.1017.

[18] A. Blum and R. Kannan, *Learning an intersection of a constant number of half-spaces over a uniform distribution*, J. Comput. Syst. Sci., 54 (1997), pp. 371–380, doi:10.1006/jcss.1997.1475.

[19] A. Blum and R. L. Rivest, *Training a 3-node neural network is NP-complete*, Neural Networks, 5 (1992), pp. 117–127, doi:10.1016/S0893-6080(05)80010-3.

[20] H. Buhrman and R. de Wolf, *Communication complexity lower bounds by polynomials*, in *Proceedings of the Sixteenth Annual IEEE Conference on Computational Complexity* (CCC), 2001, pp. 120–130, doi:10.1109/CCC.2001.933879.

[21] H. Buhrman, I. Newman, H. Röhrig, and R. de Wolf, *Robust polynomials and quantum algorithms*, Theory Comput. Syst., 40 (2007), pp. 379–395, doi:10.1007/s00224-006-1313-z.

[22] H. Buhrman, N. K. Vereshchagin, and R. de Wolf, *On computation and communication with small bias*, in *Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity* (CCC), 2007, pp. 24–32, doi:10.1109/CCC.2007.18.

[23] M. Bun, R. Kothari, and J. Thaler, *The polynomial method strikes back: Tight quantum query bounds via dual polynomials*, in *Proceedings of the Fiftieth Annual ACM Symposium on Theory of Computing* (STOC), 2018, pp. 297–310, doi:10.1145/3188745.3188784.

[24] A. K. Chandra, M. L. Furst, and R. J. Lipton, *Multi-party protocols*, in *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing* (STOC), 1983, pp. 94–99, doi:10.1145/800061.808737.

[25] K. Chandrasekaran, J. Thaler, J. Ullman, and A. Wan, *Faster private release of marginals on small databases*, in *Proceedings of the Fifth Conference on Innovations in Theoretical Computer Science* (ITCS), 2014, pp. 387–402, doi:10.1145/2554797.2554833.

[26] A. Chattopadhyay and A. Ada, *Multiparty communication complexity of disjointness*, in Electronic Colloquium on Computational Complexity (ECCC), January 2008. Report TR08-002.

[27] A. Chattopadhyay and N. S. Mande, *Separation of unbounded-error models in multi-party communication complexity*, Theory of Computing, 14 (2018), pp. 1–23, doi:10.4086/toc.2018.v014a021.

[28] B. Chor and O. Goldreich, *Unbiased bits from sources of weak randomness and probabilistic communication complexity*, SIAM J. Comput., 17 (1988), pp. 230–261, doi:10.1137/0217015.

[29] J. Friedman, R. Murty, and J.-P. Tillich, *Spectral estimates for Abelian Cayley graphs*, Journal of Combinatorial Theory, Series B, 96 (2006), pp. 111–121, doi:10.1016/j.jctb.2005.06.012.

[30] Z. Galil, R. Kannan, and E. Szemerédi, *On nontrivial separators for k-page graphs and simulations by nondeterministic one-tape Turing machines*, J. Comput. Syst. Sci., 38 (1989), pp. 134–149, doi:10.1016/0022-0000(89)90036-6.

[31] J. Gill, *Computational complexity of probabilistic Turing machines*, SIAM J. Comput., 6 (1977), pp. 675–695, doi:10.1137/0206049.

[32] H. W. Gould, *Combinatorial Identities: A Standardized Set of Tables Listing 500 Binomial Coefficient Summations*, Morgantown Printing and Binding Co., 1972.

[33] J. Håstad, *On the size of weights for threshold gates*, SIAM J. Discret. Math., 7 (1994), pp. 484–492, doi:10.1137/S0895480192235878.

[34] W. Hoeffding, *Probability inequalities for sums of bounded random variables*, Journal of the American Statistical Association, 58 (1963), pp. 13–30, doi:10.1080/01621459.1963.10500830.

[35] S. Jukna, *Extremal Combinatorics with Applications in Computer Science*, Springer-Verlag, Berlin, 2001, doi:10.1007/978-3-662-04650-0.

[36] J. Kahn, N. Linial, and A. Samorodnitsky, *Inclusion-exclusion: Exact and approximate*, Combinatorica, 16 (1996), pp. 465–477, doi:10.1007/BF01271266.

[37] A. T. Kalai, A. R. Klivans, Y. Mansour, and R. A. Servedio, *Agnostically learning halfspaces*, SIAM J. Comput., 37 (2008), pp. 1777–1805, doi:10.1137/060649057.

[38] N. M. Katz, *An estimate for character sums*, Journal of the American Mathematical Society, 2 (1989), pp. 197–200, doi:10.2307/1990974.

[39] S. Khot and R. Saket, *On the hardness of learning intersections of two halfspaces*, J. Comput. Syst. Sci., 77 (2011), pp. 129–141, doi:10.1016/j.jcss.2010.06.010.

[40] H. Klauck, *Lower bounds for quantum communication complexity*, in *Proceedings of the Forty-Second Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 2001, pp. 288–297, doi:10.1109/SFCS.2001.959903.

[41] H. Klauck, *Lower bounds for quantum communication complexity*, SIAM J. Comput., 37 (2007), pp. 20–46, doi:10.1137/S0097539702405620.

[42] A. R. Klivans, *A Complexity-Theoretic Approach to Learning*, PhD thesis, MIT, 2002.

[43] A. R. Klivans, P. M. Long, and A. K. Tang, *Baum's algorithm learns intersections of halfspaces with respect to log-concave distributions*, in *Proceedings of the Thirteenth International Workshop on Randomization and Computation* (RANDOM), 2009, pp. 588–600, doi:10.1007/978-3-642-03685-9_44.

[44] A. R. Klivans, R. O'Donnell, and R. A. Servedio, *Learning intersections and thresholds of halfspaces*, J. Comput. Syst. Sci., 68 (2004), pp. 808–840, doi:10.1016/j.jcss.2003.11.002.

[45] A. R. Klivans and R. A. Servedio, *Learning DNF in time $2^{\tilde{O}(n^{1/3})}$*, J. Comput. Syst. Sci., 68 (2004), pp. 303–318, doi:10.1016/j.jcss.2003.07.007.

[46] A. R. Klivans and R. A. Servedio, *Learning intersections of halfspaces with a margin*, J. Comput. Syst. Sci., 74 (2008), pp. 35–48, doi:10.1016/j.jcss.2007.04.012.

[47] A. R. Klivans and A. A. Sherstov, *Cryptographic hardness for learning intersections of halfspaces*, J. Comput. Syst. Sci., 75 (2009), pp. 2–12, doi:10.1016/j.jcss.2008.07.008. Preliminary version in *Proceedings of the Forty-Seventh Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 2006.

[48] M. Krause and P. Pudlák, *On the computational power of depth-2 circuits with threshold and modulo gates*, Theor. Comput. Sci., 174 (1997), pp. 137–156, doi:10.1016/S0304-3975(96)00019-9.

[49] M. Krause and P. Pudlák, *Computing Boolean functions by polynomials and threshold circuits*, Comput. Complex., 7 (1998), pp. 346–370, doi:10.1007/s000370050015.

[50] E. Kushilevitz and N. Nisan, *Communication complexity*, Cambridge University Press, 1997.

[51] S. Kwek and L. Pitt, *PAC learning intersections of halfspaces with membership queries*, Algorithmica, 22 (1998), pp. 53–75, doi:10.1007/PL00013834.

[52] T. Lee and A. Shraibman, *Disjointness is hard in the multiparty number-on-the-forehead model*, Computational Complexity, 18 (2009), pp. 309–336, doi:10.1007/s00037-009-0276-2.

[53] K. H. Leung, V. Nguyen, and W. So, *Nonexistence of a circulant expander family*, Bulletin of the Australian Mathematical Society, 83 (2011), pp. 87–95, doi:10.1017/S0004972710001644.

[54] N. Linial, S. Mendelson, G. Schechtman, and A. Shraibman, *Complexity measures of sign matrices*, Combinatorica, 27 (2007), pp. 439–463, doi:10.1007/s00493-007-2160-5.

[55] N. Linial and N. Nisan, *Approximate inclusion-exclusion*, Combinatorica, 10 (1990), pp. 349–365, doi:10.1007/BF02128670.

[56] N. Linial and A. Shraibman, *Learning complexity vs communication complexity*, Combinatorics, Probability & Computing, 18 (2009), pp. 227–245, doi:10.1017/S0963548308009656.

[57] M. L. Minsky and S. A. Papert, *Perceptrons: An Introduction to Computational Geometry*, MIT Press, Cambridge, Mass., 1969.

[58] S. Muroga, *Threshold Logic and Its Applications*, John Wiley & Sons, New York, 1971.

[59] J. Myhill and W. H. Kautz, *On the size of weights required for linear-input switching functions*, IRE Trans. on Electronic Computers, 10 (1961), pp. 288–290, doi:10.1109/TEC.1961.5219204.

[60] D. J. Newman, *Rational approximation to $|x|$*, Michigan Math. J., 11 (1964), pp. 11–14.

[61] R. O'Donnell and R. A. Servedio, *New degree bounds for polynomial threshold functions*, Combinatorica, 30 (2010), pp. 327–358, doi:10.1007/s00493-010-2173-3.

[62] R. Paturi, *On the degree of polynomials that approximate symmetric Boolean functions*, in *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing* (STOC), 1992, pp. 468–474, doi:10.1145/129712.129758.

[63] R. Paturi and J. Simon, *Probabilistic communication complexity*, J. Comput. Syst. Sci., 33 (1986), pp. 106–123, doi:10.1016/0022-0000(86)90046-2.

[64] A. Razborov, E. Szemerédi, and A. Wigderson, *Constructing small sets that are uniform in arithmetic progressions*, Combinatorics, Probability and Computing, 2 (1993), pp. 513–518, doi:10.1017/S0963548300000870.

[65] A. A. Razborov, *Quantum communication complexity of symmetric predicates*, Izvestiya of the Russian Academy of Sciences, Mathematics, 67 (2002), pp. 145–159.

[66] A. A. Razborov and A. A. Sherstov, *The sign-rank of AC^0*, SIAM J. Comput., 39 (2010), pp. 1833–1855, doi:10.1137/080744037. Preliminary version in *Proceedings of the Forty-Ninth Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 2008.

[67] T. J. Rivlin, *An Introduction to the Approximation of Functions*, Dover Publications, New York, 1981.

[68] B. Rosser, *Explicit bounds for some functions of prime numbers*, American Journal of Mathematics, 63 (1941), pp. 211–232.

[69] I. Z. Ruzsa, *Essential components*, Proceedings of the London Mathematical Society, 53-54 (1987), pp. 38–56, doi:10.1112/plms/s3-54.1.38.

[70] A. A. Sherstov, *Communication lower bounds using dual polynomials*, Bulletin of the EATCS, 95 (2008), pp. 59–93.

[71] A. A. Sherstov, *Halfspace matrices*, Computational Complexity, 17 (2008), pp. 149–178, doi:10.1007/s00037-008-0242-4. Preliminary version in *Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity* (CCC), 2007.

[72] A. A. Sherstov, *Approximate inclusion-exclusion for arbitrary symmetric functions*, Computational Complexity, 18 (2009), pp. 219–247, doi:10.1007/s00037-009-0274-4. Preliminary version in *Proceedings of the Twenty-Third Annual IEEE Conference on Computational Complexity* (CCC), 2008.

[73] A. A. Sherstov, *Separating AC^0 from depth-2 majority circuits*, SIAM J. Comput., 38 (2009), pp. 2113–2129, doi:10.1137/08071421X. Preliminary version in *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing* (STOC), 2007.

[74] A. A. Sherstov, *Communication complexity under product and nonproduct distributions*, Computational Complexity, 19 (2010), pp. 135–150, doi:10.1007/s00037-009-0285-1. Preliminary version in *Proceedings of the Twenty-Third Annual IEEE Conference on Computational Complexity* (CCC), 2008.

[75] A. A. Sherstov, *The pattern matrix method*, SIAM J. Comput., 40 (2011), pp. 1969–2000, doi:10.1137/080733644. Preliminary version in *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing* (STOC), 2008.

[76] A. A. Sherstov, *The intersection of two halfspaces has high threshold degree*, SIAM J. Comput., 42 (2013), pp. 2329–2374, doi:10.1137/100785260. Preliminary version in *Proceedings of the Fiftieth Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 2009.

[77] A. A. Sherstov, *Optimal bounds for sign-representing the intersection of two halfspaces by polynomials*, Combinatorica, 33 (2013), pp. 73–96, doi:10.1007/s00493-013-2759-7. Preliminary version in *Proceedings of the Forty-Second Annual ACM Symposium on Theory of Computing* (STOC), 2010.

[78] A. A. Sherstov, *Communication lower bounds using directional derivatives*, J. ACM, 61 (2014), pp. 1–71, doi:10.1145/2629334. Preliminary version in *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing* (STOC), 2013.

[79] A. A. Sherstov, *The multiparty communication complexity of set disjointness*, SIAM J. Comput., 45 (2016), pp. 1450–1489, doi:10.1137/120891587. Preliminary version in *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing* (STOC), 2009.

[80] A. A. Sherstov, *On multiparty communication with large versus unbounded error*, Theory of Computing, 14 (2018), pp. 1–17, doi:10.4086/toc.2018.v014a022.

[81] K.-Y. Siu and J. Bruck, *On the power of threshold circuits with small weights*, SIAM J. Discrete Math., 4 (1991), pp. 423–435, doi:10.1137/0404038.

[82] J. Tarui and T. Tsukiji, *Learning DNF by approximating inclusion-exclusion formulae*, in *Proceedings of the Fourteenth Annual IEEE Conference on Computational Complexity* (CCC), 1999, pp. 215–221, doi:10.1109/CCC.1999.766279.

[83] J. Thaler, *Lower bounds for the approximate degree of block-composed functions*, in *Proceedings of the Forty-Third International Colloquium on Automata, Languages and Programming* (ICALP), 2016, pp. 17:1–17:15, doi:10.4230/LIPIcs.ICALP.2016.17.

[84] J. Thaler, J. Ullman, and S. P. Vadhan, *Faster algorithms for privately releasing marginals*, in *Proceedings of the Thirty-Ninth International Colloquium on Automata, Languages and Programming* (ICALP), 2012, pp. 810–821, doi:10.1007/978-3-642-31594-7_68.

[85] J. S. Thathachar, *On separating the read-k-times branching program hierarchy.* ECCC Report TR98-002, 1998, `https://eccc.weizmann.ac.il/report/1998/002`. Extended abstract in *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing* (STOC), 1998.

[86] L. G. Valiant, *A theory of the learnable*, Commun. ACM, 27 (1984), pp. 1134–1142, doi:10.1145/1968.1972.

[87] S. Vempala, *A random-sampling-based algorithm for learning intersections of halfspaces*, J. ACM, 57 (2010), p. 32, doi:10.1145/1857914.1857916.

[88] A. C.-C. Yao, *Some complexity questions related to distributive computing*, in *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing* (STOC), 1979, pp. 209–213, doi:10.1145/800135.804414.

[89] E. I. Zolotarev, *Application of elliptic functions to questions of functions deviating least and most from zero*, Izvestiya Imp. Akad. Nauk, 30 (1877).

Appendix A. The iteration lemma of Ajtai et al.

The purpose of this appendix is to provide a detailed and self-contained proof of Theorem 3.6, which we restate below for the reader's convenience.

Theorem. *Fix an integer $R \geqslant 1$ and a real number $P \geqslant 2$. Let m be an integer with*

$$m \geqslant P^2(R+1).$$

Fix a set $S_p \subseteq \{1, 2, \ldots, p-1\}$ for each prime $p \in (P/2, P]$ with $p \nmid m$, such that all S_p have the same cardinality. Consider the multiset

$$S = \{(r + s \cdot (p^{-1})_m) \bmod m : \\ r = 1, \ldots, R; \quad p \in (P/2, P] \text{ prime with } p \nmid m; \quad s \in S_p\}.$$

Then the elements of S are pairwise distinct and nonzero. Moreover,

$$\operatorname{disc}(S,m) \leqslant \frac{c}{\sqrt{R}} + \frac{c\log m}{\log\log m}\cdot\frac{\log P}{P} + \max_p\{\operatorname{disc}(S_p,p)\} \tag{A.1}$$

for some (*explicitly given*) *constant $c \geqslant 1$ independent of P, R, m.*

This result is a slight generalization of the *iteration lemma* of Ajtai et al. [2], which corresponds to the special case for m prime. We closely follow their proof but provide ample detail to make it more accessible. We have structured the presentation around five key milestones, corresponding to Sections A.1–A.5 below. Before proceeding, the reader may wish to review the number-theoretic preliminaries in Section 2.2.

A.1. Shorthand notation. In the remainder of this manuscript, we adopt the shorthand

$$e(x) = \exp(2\pi x\mathbf{i}),$$

where $\mathbf{i}$ is the imaginary unit. We will need the following bounds, illustrated in Figure A.1:

$$|1-e(x)| \leqslant 2\pi x, \qquad 0\leqslant x\leqslant 1, \tag{A.2}$$

$$|1-e(x)| \geqslant 4\min(x,1-x), \qquad 0\leqslant x\leqslant 1. \tag{A.3}$$

To verify these bounds, write $|1-e(x)| = |1-\exp(2\pi x\mathbf{i})| = \sqrt{2-2\cos(2\pi x)}$ and apply elementary calculus.

We let $\mathscr{P}$ denote the set of prime numbers $p \in (P/2, P]$ with $p \nmid m$. In this notation, the multiset S is given by

$$S = \{(r + s\cdot(p^{-1})_m) \bmod m : p\in\mathscr{P},\ s\in S_p,\ r = 1,2,\ldots,R\}.$$

There are precisely $\pi(P)-\pi(P/2)$ primes in $(P/2,P]$, of which at most $\nu(m)$ are prime divisors of m. Therefore,

$$|\mathscr{P}| \geqslant \pi(P) - \pi\left(\frac{P}{2}\right) - \nu(m). \tag{A.4}$$

A.2. Elements of S are nonzero and distinct. As our first step, we verify that the elements of S are nonzero modulo m. Consider any $r\in\{1,2,\ldots,R\}$, any prime $p\in(P/2,P]$ with $p\nmid m$, and any $s\in S_p$. Then $pr+s\in[1, PR+P-1]\subseteq[1,m)$. This means that $pr+s\not\equiv 0 \pmod m$, which in turn implies that $r+s\cdot(p^{-1})_m\not\equiv 0$ $\pmod m$.

We now show that the multiset S contains no repeated elements. For this, consider any $r,r'\in\{1,2,\ldots,R\}$, any primes $p,p'\in\mathscr{P}$, and any $s\in S_p$ and $s'\in S_{p'}$ such that

$$r + s\cdot(p^{-1})_m \equiv r' + s'\cdot(p'^{-1})_m \pmod m. \tag{A.5}$$

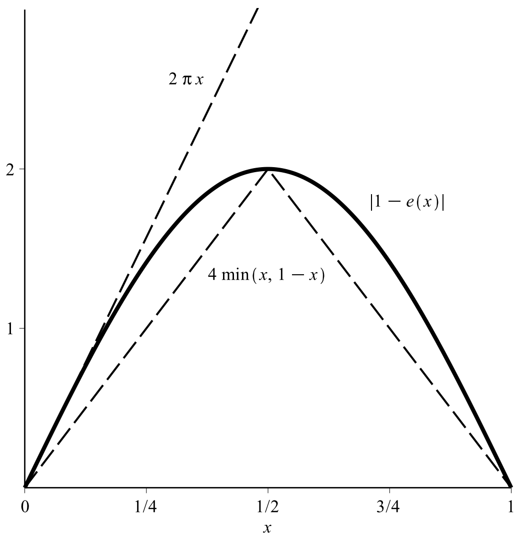

Figure A.1: A graph of $|1 - e(x)|$ and its approximations by piecewise linear functions.

Our goal is to show that $p = p', r = r', s = s'$. To this end, multiply (A.5) through by pp' to obtain

$$r \cdot pp' + s \cdot p' \equiv r' \cdot pp' + s' \cdot p \pmod{m}. \tag{A.6}$$

The left-hand side and right-hand side of (A.6) are integers in $[1, RP^2 + (P-1)P] \subseteq [1, m)$, whence

$$r \cdot pp' + s \cdot p' = r' \cdot pp' + s' \cdot p. \tag{A.7}$$

This implies that $p \mid s \cdot p'$, which in view of $s < p$ and the primality of p and p' forces $p = p'$. Now (A.7) simplifies to

$$r \cdot p + s = r' \cdot p + s', \tag{A.8}$$

which in turn yields $s \equiv s' \pmod{p}$. Recalling that $s, s' \in \{1, 2, \ldots, p-1\}$, we arrive at $s = s'$. Finally, substituting $s = s'$ in (A.8) gives $r = r'$.

A.3. Correlation for *k* small. So far, we have shown that the elements of S are distinct and nonzero. Recall that our objective is to bound the m-discrepancy of this set. Put another way, we must bound the exponential sum

$$\left| \sum_{s \in S} e\left(\frac{k}{m} \cdot s\right) \right| \tag{A.9}$$

for all $k = 1, 2, \ldots, m-1$. This subsection and the next provide two complementary bounds on (A.9). The first bound, presented below, is preferable when k is close to zero modulo m.

Claim A.1. *Let $k \in \{1,2,\ldots,m-1\}$ be given. Then*

$$\left|\sum_{s\in S} e\left(\frac{k}{m}\cdot s\right)\right| \\ \leqslant \left(\frac{2\pi\min(k,m-k)}{m} + \max_{p\in\mathscr{P}}\{\operatorname{disc}(S_p,p)\} + \frac{\nu(k)+\nu(m-k)}{|\mathscr{P}|}\right)|S|.$$

Proof. Let $\mathscr{P}'$ be the set of those primes in $\mathscr{P}$ that do not divide k or $m-k$. Then clearly

$$|\mathscr{P}\setminus\mathscr{P}'| \leqslant \nu(k)+\nu(m-k). \tag{A.10}$$

We have

$$\begin{aligned}
&\left|\sum_{s\in S} e\left(\frac{k}{m}\cdot s\right)\right| \\
&\quad= \left|\sum_{r=1}^{R}\sum_{p\in\mathscr{P}}\sum_{s\in S_p} e\left(\frac{k}{m}\cdot(r+s\cdot(p^{-1})_m\right)\right| \\
&\quad\leqslant \sum_{r=1}^{R}\sum_{p\in\mathscr{P}}\left|\sum_{s\in S_p} e\left(\frac{k}{m}\cdot(r+s\cdot(p^{-1})_m\right)\right| \\
&\quad= R\sum_{p\in\mathscr{P}}\left|\sum_{s\in S_p} e\left(\frac{ks\cdot(p^{-1})_m}{m}\right)\right| \\
&\quad\leqslant R\sum_{p\in\mathscr{P}'}\left|\sum_{s\in S_p} e\left(\frac{ks\cdot(p^{-1})_m}{m}\right)\right| + R\sum_{p\in\mathscr{P}\setminus\mathscr{P}'}\left|\sum_{s\in S_p} e\left(\frac{ks\cdot(p^{-1})_m}{m}\right)\right| \\
&\quad\leqslant R\sum_{p\in\mathscr{P}'}\left|\sum_{s\in S_p} e\left(\frac{ks\cdot(p^{-1})_m}{m}\right)\right| + R\sum_{p\in\mathscr{P}\setminus\mathscr{P}'}|S_p|.
\end{aligned} \tag{A.11}$$

We proceed to bound the two summations in (A.11). Bounding the second summation is straightforward:

$$\begin{aligned}
R\sum_{p\in\mathscr{P}\setminus\mathscr{P}'}|S_p| &= R\cdot\frac{|\mathscr{P}\setminus\mathscr{P}'|}{|\mathscr{P}|}\sum_{p\in\mathscr{P}}|S_p| \\
&= \frac{|\mathscr{P}\setminus\mathscr{P}'|}{|\mathscr{P}|}\cdot|S| \\
&\leqslant \frac{\nu(k)+\nu(m-k)}{|\mathscr{P}|}\cdot|S|,
\end{aligned} \tag{A.12}$$

where the first step is valid because all sets S_p have the same cardinality, and the last step uses (A.10).

The other summation in (A.11) requires more work. For $p \in \mathscr{P}'$ and $K \in \{k, k-m\}$, we have

$$\begin{aligned}
&\left|\sum_{s\in S_p} e\left(\frac{ks\cdot(p^{-1})_m}{m}\right)\right| \\
&\qquad = \left|\sum_{s\in S_p} e\left(\frac{Ks\cdot(p^{-1})_m}{m}\right)\right| \\
&\qquad = \left|\sum_{s\in S_p} e\left(-\frac{Ks\cdot(m^{-1})_p}{p}\right) e\left(\frac{Ks}{pm}\right)\right| \\
&\qquad \leqslant \left|\sum_{s\in S_p} e\left(-\frac{Ks\cdot(m^{-1})_p}{p}\right)\left(e\left(\frac{Ks}{pm}\right)-1\right)\right| + \left|\sum_{s\in S_p} e\left(-\frac{Ks\cdot(m^{-1})_p}{p}\right)\right| \\
&\qquad \leqslant \left|\sum_{s\in S_p} e\left(-\frac{Ks\cdot(m^{-1})_p}{p}\right)\left(e\left(\frac{Ks}{pm}\right)-1\right)\right| + \operatorname{disc}(S_p,p)\cdot|S_p| \\
&\qquad \leqslant \sum_{s\in S_p}\left|e\left(\frac{Ks}{pm}\right)-1\right| + \operatorname{disc}(S_p,p)\cdot|S_p| \\
&\qquad = \sum_{s\in S_p}\left|e\left(\frac{|K|s}{pm}\right)-1\right| + \operatorname{disc}(S_p,p)\cdot|S_p| \\
&\qquad \leqslant |S_p|\cdot\frac{2\pi|K|}{m} + \operatorname{disc}(S_p,p)\cdot|S_p|,
\end{aligned}$$

where the second step uses Fact 2.2 and the relative primality of p and m; the third step applies the triangle inequality; the fourth step follows from $p \nmid |K|$, and the last step is valid by (A.2) and $s < p$. We have shown that

$$\left|\sum_{s\in S_p} e\left(\frac{ks\cdot(p^{-1})_m}{m}\right)\right| \leqslant \frac{2\pi\min(k,m-k)}{m}\cdot|S_p| + \operatorname{disc}(S_p,p)\cdot|S_p|$$

for $p \in \mathscr{P}'$. Summing over $\mathscr{P}'$,

$$\begin{aligned}
&R \sum_{p\in\mathscr{P}'} \left| \sum_{s\in S_p} e\left(\frac{ks\cdot(p^{-1})_m}{m}\right)\right| \\
&\qquad\qquad \leqslant R \sum_{p\in\mathscr{P}'} \left(\frac{2\pi\min(k,m-k)}{m}\cdot|S_p| + \operatorname{disc}(S_p,p)\cdot|S_p|\right) \\
&\qquad\qquad \leqslant R \sum_{p\in\mathscr{P}} \left(\frac{2\pi\min(k,m-k)}{m}\cdot|S_p| + \operatorname{disc}(S_p,p)\cdot|S_p|\right) \\
&\qquad\qquad \leqslant \left(\frac{2\pi\min(k,m-k)}{m} + \max_{p\in\mathscr{P}}\{\operatorname{disc}(S_p,p)\}\right) R \sum_{p\in\mathscr{P}} |S_p| \\
&\qquad\qquad = \left(\frac{2\pi\min(k,m-k)}{m} + \max_{p\in\mathscr{P}}\{\operatorname{disc}(S_p,p)\}\right) |S|. \qquad (A.13)
\end{aligned}$$

By (A.11)–(A.13), the proof of the claim is complete. ∎

A.4. Correlation for k large. We now present an alternative bound on the exponential sum (A.9), which is preferable to the bound of Claim A.1 when k is far from zero modulo m.

Claim A.2. *Let $k \in \{1,2,\ldots,m-1\}$ be given. Then*

$$\left|\sum_{s\in S} e\left(\frac{k}{m}\cdot s\right)\right| \leqslant \frac{m}{2R\min(k,m-k)}\cdot|S|.$$

Proof:

$$\begin{aligned}
\left|\sum_{s\in S} e\left(\frac{k}{m}\cdot s\right)\right| &= \left|\sum_{p\in\mathscr{P}}\sum_{s\in S_p}\sum_{r=1}^{R} e\left(\frac{k}{m}\cdot(r+s\cdot(p^{-1})_m)\right)\right| \\
&\leqslant \sum_{p\in\mathscr{P}}\sum_{s\in S_p}\left|\sum_{r=1}^{R} e\left(\frac{k}{m}\cdot(r+s\cdot(p^{-1})_m)\right)\right| \\
&= \sum_{p\in\mathscr{P}}\sum_{s\in S_p}\left|\sum_{r=1}^{R} e\left(\frac{kr}{m}\right)\right| \\
&= \sum_{p\in\mathscr{P}}\sum_{s\in S_p}\frac{|1-e(kR/m)|}{|1-e(k/m)|} \\
&\leqslant \sum_{p\in\mathscr{P}}\sum_{s\in S_p}\frac{2}{|1-e(k/m)|} \\
&\leqslant \sum_{p\in\mathscr{P}}\sum_{s\in S_p}\frac{m}{2\min(k,m-k)} \\
&= \frac{m}{2R\min(k,m-k)}\cdot|S|,
\end{aligned}$$

where the last two steps use (A.3) and $|S| = R\sum_{p\in\mathscr{P}} |S_p|$, respectively. □

A.5. Finishing the proof. Facts 2.3 and 2.4 imply that

$$\pi(P) - \pi\left(\frac{P}{2}\right) \geqslant \frac{P}{C\log P} \qquad (P \geqslant C), \tag{A.14}$$

$$\max_{k=1,2,\ldots,m} \nu(k) \leqslant \frac{C\log m}{\log\log m}, \tag{A.15}$$

where $C \geqslant 1$ is a constant independent of R, P, m. Moreover, C can be easily calculated from the explicit bounds in Facts 2.3 and 2.4. We will show that the theorem conclusion (A.1) holds with $c = 4C^2$. We may assume that

$$P \geqslant C, \tag{A.16}$$

$$\frac{C\log m}{\log\log m} \leqslant \frac{P}{2C\log P}, \tag{A.17}$$

since otherwise the right-hand side of (A.1) exceeds 1 and the theorem is trivially true. By (A.4), (A.14), (A.15), and (A.17), we obtain

$$|\mathscr{P}| \geqslant \frac{P}{2C\log P},$$

which along with (A.15) gives

$$\begin{aligned}\max_{k=1,2,\ldots,m-1} \frac{\nu(k)+\nu(m-k)}{|\mathscr{P}|} &\leqslant \frac{2C\log m}{\log\log m}\cdot\frac{2C\log P}{P}\\ &= \frac{c\log m}{\log\log m}\cdot\frac{\log P}{P}.\end{aligned} \tag{A.18}$$

Claims A.1 and A.2 ensure that for every $k = 1, 2, \ldots, m-1$,

$$\begin{aligned}\left|\sum_{s\in S} e\left(\frac{k}{m}\cdot s\right)\right| &\leqslant \Bigg(\min\left(\frac{2\pi\min(k,m-k)}{m}, \frac{m}{2R\min(k,m-k)}\right)\\ &\qquad + \max_{p\in\mathscr{P}}\{\operatorname{disc}(S_p,p)\} + \frac{\nu(k)+\nu(m-k)}{|\mathscr{P}|}\Bigg)|S|\\ &\leqslant \left(\sqrt{\frac{\pi}{R}} + \max_{p\in\mathscr{P}}\{\operatorname{disc}(S_p,p)\} + \frac{\nu(k)+\nu(m-k)}{|\mathscr{P}|}\right)|S|\\ &\leqslant \left(\frac{c}{\sqrt{R}} + \max_{p\in\mathscr{P}}\{\operatorname{disc}(S_p,p)\} + \frac{\nu(k)+\nu(m-k)}{|\mathscr{P}|}\right)|S|.\end{aligned}$$

Substituting the estimate from (A.18), we conclude that

$$\begin{aligned}&\max_{k=1,2,\ldots,m-1}\left|\sum_{s\in S} e\left(\frac{k}{m}\cdot s\right)\right|\\ &\qquad\leqslant \left(\frac{c}{\sqrt{R}} + \max_{p\in\mathscr{P}}\{\operatorname{disc}(S_p,p)\} + \frac{c\log m}{\log\log m}\cdot\frac{\log P}{P}\right)|S|.\end{aligned}$$

This conclusion is equivalent to (A.1). The proof of Theorem 3.6 is complete.

Appendix B. An alternate proof of Fact 4.1

The purpose of this appendix is to give an alternate, matrix-analytic proof of Fact 4.1.

Fact (restatement of Fact 4.1). *Fix a natural number $m \geqslant 2$ and a multiset $Z = \{z_1, z_2, \ldots, z_n\}$ of integers. Let ω be a primitive m-th root of unity. Then*

$$\left| \mathop{\mathbf{P}}_{X\in\{0,1\}^n}\left[\sum_{j=1}^n z_jX_j \equiv s \pmod m\right] - \frac{1}{m}\right| \leqslant \frac{1}{m}\sum_{k=1}^{m-1}\left|\prod_{j=1}^n \frac{1+\omega^{kz_j}}{2}\right|, \qquad s\in\mathbb{Z}. \tag{B.1}$$

Proof. For any integer z, consider the circulant matrix

$$T_z = \frac{1}{2}\operatorname{circ}(\underbrace{1,0,\ldots,0}_{m}) + \frac{1}{2}\operatorname{circ}(\underbrace{\overbrace{0,\ldots,0}^{z \bmod m},1,0,\ldots,0}_{m}).$$

By Corollary 2.6, the matrix $W = [\omega^{jk}/\sqrt{m}]_{j,k=0,1,\ldots,m-1}$ obeys

$$WW^* = I, \tag{B.2}$$

$$W^*T_zW = \operatorname{diag}\left(1, \frac{1+\omega^z}{2}, \frac{1+\omega^{2z}}{2}, \ldots, \frac{1+\omega^{(m-1)z}}{2}\right), \qquad z\in\mathbb{Z}. \tag{B.3}$$

In particular,

$$\begin{aligned}
&W^*T_{-z_n}T_{-z_{n-1}}\cdots T_{-z_1}W\\
&\qquad= (W^*T_{-z_n}W)(W^*T_{-z_{n-1}}W)\cdots(W^*T_{-z_1}W)\\
&\qquad= \prod_{j=1}^n \operatorname{diag}\left(1, \frac{1+\omega^{-z_j}}{2}, \frac{1+\omega^{-2z_j}}{2}, \ldots, \frac{1+\omega^{-(m-1)z_j}}{2}\right)\\
&\qquad= \operatorname{diag}\left(1, \prod_{j=1}^n\frac{1+\omega^{-z_j}}{2}, \prod_{j=1}^n\frac{1+\omega^{-2z_j}}{2}, \ldots, \prod_{j=1}^n\frac{1+\omega^{-(m-1)z_j}}{2}\right),
\end{aligned}$$

where the first two steps use (B.2) and (B.3), respectively. Applying (B.2) yet again, we arrive at

$$\begin{aligned}
&T_{-z_n}T_{-z_{n-1}}\cdots T_{-z_1}\\
&\quad= W\operatorname{diag}\left(1, \prod_{j=1}^n\frac{1+\omega^{-z_j}}{2}, \prod_{j=1}^n\frac{1+\omega^{-2z_j}}{2}, \ldots, \prod_{j=1}^n\frac{1+\omega^{-(m-1)z_j}}{2}\right)W^*\\
&\quad= \frac{1}{m}J + \sum_{k=1}^{m-1}\prod_{j=1}^n\frac{1+\omega^{-kz_j}}{2}W_kW_k^*,
\end{aligned}$$

where $W_1, W_2, \dots, W_{m-1}$ denote the last $m-1$ columns of W. Since the components of each W_k are bounded in absolute value by $1/\sqrt{m}$, we conclude that

$$\left\| T_{-z_n} T_{-z_{n-1}} \cdots T_{-z_1} - \frac{1}{m} J \right\|_\infty \leqslant \frac{1}{m} \sum_{k=1}^{m-1} \left| \prod_{j=1}^{n} \frac{1 + \omega^{-kz_j}}{2} \right|. \tag{B.4}$$

We are now in a position to prove (B.1). Let $X = (X_1, X_2, \dots, X_n)$ be a random variable distributed uniformly in $\{0,1\}^n$. Consider the random variables $Y_0, Y_1, Y_2, \dots, Y_n$ given by $Y_k = (z_1 X_1 + z_2 X_2 + \cdots + z_k X_k) \bmod m$. The sequence $Y_0, Y_1, Y_2, \dots, Y_n$ has a natural interpretation in terms of an n-step random walk in $\mathbb{Z}_m$. Specifically, the random walk starts at $Y_0 = 0$ and evolves according to

$$Y_k = \begin{cases} Y_{k-1} & \text{with probability } 1/2, \\ (Y_{k-1} + z_k) \bmod m & \text{with probability } 1/2. \end{cases}$$

In particular, the k-th step of the random walk has transition probability matrix

$$\frac{1}{2} \begin{bmatrix} 1 &&&&&& \\ & 1 &&&&& \\ && 1 &&&& \\ &&& 1 &&& \\ &&&& \ddots && \\ &&&&& 1 & \\ &&&&&& 1 \end{bmatrix} + \frac{1}{2} \begin{array}{c} \begin{array}{ccccccc} \multicolumn{3}{c}{\overbrace{\hphantom{1 \quad 1 \quad 1}}^{-z_k \bmod m}} &&&& \end{array} \\ \begin{bmatrix} &&& 1 &&& \\ &&&& 1 && \\ &&&&& \ddots & \\ &&&&&& 1 \\ 1 &&&&&& \\ & \ddots &&&&& \\ && 1 &&&& \end{bmatrix} \end{array},$$

where the unspecified entries are zero, and the rows and columns correspond in the usual manner to the values $0, 1, \dots, m-1$. In the notation of the opening paragraph of the proof, this matrix is precisely T_{-z_k}. Letting $p_0, p_1, \dots, p_n$ be the m-dimensional vectors that represent the probability distributions of $Y_0, Y_1, \dots, Y_n$, respectively, we obtain the recursive relations $p_k = T_{-z_k} p_{k-1}$. Therefore,

$$p_n = T_{-z_n} T_{-z_{n-1}} \cdots T_{-z_1} p_0.$$

Now

$$\begin{aligned}
\left\| p_n - \begin{bmatrix} \frac{1}{m} & \frac{1}{m} & \cdots & \frac{1}{m} \end{bmatrix}^T \right\|_\infty &= \left\| T_{-z_n} T_{-z_{n-1}} \cdots T_{-z_1} p_0 - \frac{1}{m} J p_0 \right\|_\infty \\
&\leqslant \left\| T_{-z_n} T_{-z_{n-1}} \cdots T_{-z_1} - \frac{1}{m} J \right\|_\infty \|p_0\|_1 \\
&= \left\| T_{-z_n} T_{-z_{n-1}} \cdots T_{-z_1} - \frac{1}{m} J \right\|_\infty \\
&\leqslant \frac{1}{m} \sum_{k=1}^{m-1} \left| \prod_{j=1}^{n} \frac{1+\omega^{-kz_j}}{2} \right| \\
&= \frac{1}{m} \sum_{k=1}^{m-1} \left| \prod_{j=1}^{n} \frac{1+\omega^{kz_j}}{2} \right|,
\end{aligned}$$

where the next-to-last step uses (B.4). This conclusion is obviously equivalent to (B.1). □