

Sign-rank Can Increase under Intersection

MARK BUN, Boston University, USA

NIKHIL S. MANDE, CWI, The Netherlands

JUSTIN THALER, Georgetown University, USA

The communication class UPP^{cc} is a communication analog of the Turing Machine complexity class PP . It is characterized by a matrix-analytic complexity measure called sign-rank (also called dimension complexity), and is essentially the most powerful communication class against which we know how to prove lower bounds.

For a communication problem f , let $f \wedge f$ denote the function that evaluates f on two disjoint inputs and outputs the AND of the results. We exhibit a communication problem f with $\text{UPP}^{\text{cc}}(f) = O(\log n)$, and $\text{UPP}^{\text{cc}}(f \wedge f) = \Theta(\log^2 n)$. This is the first result showing that UPP communication complexity can increase by more than a constant factor under intersection. We view this as a first step toward showing that UPP^{cc} , the class of problems with polylogarithmic-cost UPP communication complexity, is not closed under intersection.

Our result shows that the function class consisting of intersections of two majorities on n bits has dimension complexity $n^{\Omega(\log n)}$. This matches an upper bound of (Klivans, O'Donnell, and Servedio, FOCS 2002), who used it to give a quasipolynomial time algorithm for PAC learning intersections of polylogarithmically many majorities. Hence, fundamentally new techniques will be needed to learn this class of functions in polynomial time.

CCS Concepts: • **Theory of computation** → **Communication complexity; Boolean function learning;**

Additional Key Words and Phrases: Sign rank, dimension complexity, communication complexity, learning theory

ACM Reference format:

Mark Bun, Nikhil S. Mande, and Justin Thaler. 2021. Sign-rank Can Increase under Intersection. *ACM Trans. Comput. Theory* 13, 4, Article 24 (August 2021), 17 pages.

<https://doi.org/10.1145/3470863>

1 INTRODUCTION

The unbounded-error communication complexity model UPP^{cc} was introduced by Paturi and Simon [26] as a natural communication analog of the Turing Machine complexity class PP . In a

A preliminary version of this article [8] appeared in the proceedings of the 46th International Colloquium on Automata, Languages and Programming (ICALP), 2019.

This work was done while M. Bun was at Princeton University and at the Simons Institute for the Theory of Computing, supported by a Google Research Fellowship.

This work was done while N. S. Mande was a postdoc at Georgetown University.

Authors' addresses: M. Bun, MCS 114, 111 Cummington Mall, Boston University, Boston, MA 02215, USA; email: mbun@bu.edu; N. S. Mande, L216, Science Park 123 1098 XG, CWI, Amsterdam, The Netherlands; email: nsm@cwi.nl; J. Thaler, Department of Computer Science, St. Mary's Hall, Room 354, 3700 Reservoir Road NW, Georgetown University, Washington, DC 20057, USA; email: justin.thaler@georgetown.edu.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2021 Association for Computing Machinery.

1942-3454/2021/08-ART24 \$15.00

<https://doi.org/10.1145/3470863>

UPP^{cc} communication protocol for a Boolean function $f(x, y)$, there are two parties, one with input x and one with input y . The two parties engage in a private-coin randomized communication protocol, at the end of which they are required to output $f(x, y)$ with probability strictly greater than $1/2$. The cost of the protocol is the number of bits exchanged by the two parties. As is standard, we use the notation UPP^{cc} not only to denote the communication model, but also the class of functions solvable in the model by protocols of cost polylogarithmic in the size of the input.

Observe that success probability $1/2$ can be achieved with no communication by random guessing, so the UPP^{cc} model merely requires a strict improvement over this trivial solution. Owing to this liberal acceptance criterion, UPP^{cc} is a very powerful communication model, essentially the most powerful one against which we know how to prove lower bounds. In particular, UPP^{cc} is powerful enough to simulate many other models of computing, and this makes UPP^{cc} *lower bounds* highly useful. As one example, any function $f(x, y)$ computable by a Threshold-of-Majority circuit of size s has UPP^{cc} complexity at most $O(\log s)$, and this connection has been used to translate UPP^{cc} lower bounds into state-of-the-art lower bounds against threshold circuits (see, for example, References [9, 11, 13, 27, 33]).

UPP^{cc} also happens to be characterized by a natural matrix-analytic complexity measure called *sign-rank* [26]. Here, the sign-rank of a matrix $M \in \{-1, 1\}^{N \times N}$ is the minimum rank of a real matrix whose entries agree in sign with M . Equivalently, $\text{sr}(M) := \min_A \text{rk}(A)$, where the minimum is over all matrices A such that $A_{i,j} \cdot M_{i,j} > 0$ for all $i, j \in [N]$. Paturi and Simon [26] showed the following tight connection between UPP^{cc} and sign-rank: If we associate a function $f(x, y)$ with the matrix $M = [f(x, y)]_{x,y}$, then the UPP^{cc} communication complexity of f equals $\log(\text{sr}(M)) \pm \Theta(1)$.

While lower bounds on UPP^{cc} complexity (equivalently, sign-rank) are useful in complexity theory, *upper bounds* on these quantities imply state-of-the-art learning algorithms, including the fastest known algorithms for PAC learning DNFs and read-once formulas [3, 22]. More specifically, suppose we want to learn a concept class C of functions mapping $\{-1, 1\}^n$ to $\{-1, 1\}$. C is naturally associated with a $|C| \times 2^n$ matrix M , whose i th row equals the truth table of the i th function in C . Then, assuming a standard representation of points in \mathbb{R}^n , C can be distribution-independently PAC learned in time polynomial in the sign-rank of M . (The sign-rank of M is often referred to in the learning theory literature as the *dimension complexity* of C .) Moreover, the resulting learning algorithm is robust to random classification noise, a property not satisfied by the handful of known PAC learning algorithms that are *not* based on dimension complexity.

For the purpose of our work, one particularly important application of the dimension-complexity approach to PAC learning was derived by Klivans et al. [21], who showed that the concept class consisting of intersections of two majority functions has dimension complexity at most $\binom{n}{O(\log n)} \leq n^{O(\log n)}$. They thereby obtained a quasipolynomial time algorithm for PAC learning intersections of two majority functions.¹ Prior to our work, it was consistent with current knowledge that the dimension complexity of this concept class is in fact $\text{poly}(n)$, which would yield a polynomial time PAC learning algorithm for intersections of constantly many majority functions.

1.1 Our Results

Despite considerable effort, progress on understanding sign-rank (equivalently, UPP^{cc}) has been slow. Our lack of knowledge is highlighted via the following well-known open question (cf. Göös et al. [18]). Throughout, for any function $f: \{-1, 1\}^n \rightarrow \{-1, 1\}$, $f \wedge f$ denotes the function on

¹ In fact, their algorithm runs in quasipolynomial time for intersections of polylogarithmic many majorities.

twice as many inputs obtained by evaluating f on two disjoint inputs and outputting -1 only if both copies of f evaluate to -1 , i.e., $(f \wedge f)(x_1, x_2) := f(x_1) \wedge f(x_2)$.

QUESTION 1. *Is the class UPP^{cc} closed under intersection? In other words, suppose the function $f(x, y) : \{-1, 1\}^n \times \{-1, 1\}^n \rightarrow \{-1, 1\}$ satisfies $\text{UPP}^{\text{cc}}(f) = O((\log n)^c)$ for some constant c . Is there always some constant c_1 (which may depend on c) such that $\text{UPP}(f \wedge f) \leq O((\log n)^{c_1})$? More generally and informally, if $\text{UPP}^{\text{cc}}(f)$ is “small,” does this imply any non-trivial upper bound on $\text{UPP}^{\text{cc}}(f \wedge f)$?*

Prior to our work, essentially nothing was known about Question 1. In particular, we are not aware of prior work ruling out the possibility that $\text{UPP}^{\text{cc}}(f \wedge f) \leq O(\text{UPP}^{\text{cc}}(f))$. However, for reasons that will become apparent in Section 1.2, there is good reason to suspect that there exists a function f with $\text{UPP}^{\text{cc}}(f) = O(\log n)$, yet $\text{UPP}^{\text{cc}}(f \wedge f) \geq \Omega(n)$. While we do not obtain a full resolution of Question 1, we do show for the first time that UPP^{cc} complexity can increase significantly under intersection.

Babai, Frankl, and Simon [4] observed that there are two natural communication complexity analogs of the Turing machine class PP , namely, PP^{cc} and UPP^{cc} . It is well known [5] that PP^{cc} is closed under intersection. Our work can be viewed as a first step towards showing that, in contrast, UPP^{cc} is *not* closed under intersection.

THEOREM 1.1. *There is a function $f(x, y) : \{-1, 1\}^n \times \{-1, 1\}^n \rightarrow \{-1, 1\}$ such that $\text{UPP}^{\text{cc}}(f) = O(\log n)$, yet $\text{UPP}^{\text{cc}}(f \wedge f) = \Theta(\log^2 n)$.*

In fact, for each fixed $x \in \{-1, 1\}^n$, the function $f(x, y)$ from Theorem 1.1 simply outputs the majority of some subset of the bits of y . This yields the following corollary:

COROLLARY 1.2. *Let C be the concept class in which each concept is the intersection of two majorities on n bits. Then C has dimension complexity $n^{\Theta(\log n)}$.*

Corollary 1.2 shows that the dimension complexity upper bound of Klivans et al. [21] is tight for intersections of two majorities, and new approaches will be needed to PAC learn this concept class in polynomial time. For context, we remark that learning intersections of majorities is a special case of the more general problem of learning intersections of many *halfspaces*.² The latter is a central and well-studied challenge in learning theory, as intersections of halfspaces are powerful enough to represent any convex set, and they contain many basic problems (like learning DNFs) as special cases. In contrast to the well-understood problem of learning a single halfspace, for which many efficient algorithms are known, no $2^{o(n)}$ -time algorithm is known for PAC learning even the intersection of two halfspaces. There have been considerable efforts devoted to showing that learning intersections of halfspaces is a hard problem [6, 12, 20, 23], but these results apply only to intersections of many halfspaces or make assumptions about the form of the output hypothesis of the learner. Our work can be seen as a new form of evidence that learning intersections of even two majorities is hard.

1.2 Our Techniques

UPP^{cc} has a *query complexity* analog, denoted UPP^{dt} and defined as follows: A UPP^{dt} algorithm is a randomized algorithm that on input x , queries bits of x , and must output $f(x)$ with probability strictly greater than $1/2$; the cost of the protocol is the number of bits of x queried. How UPP^{dt} behaves under intersection is now well understood. More specifically, it is known [31] that there is a function $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ (in fact, a halfspace) such that $\text{UPP}^{\text{dt}}(f) = O(1)$, yet

²A halfspace is any function of the form $\text{sgn}(\sum_{i=1}^n w_i \cdot x_i + w_0)$ for some real numbers w_0, \dots, w_n .

$\text{UPP}^{\text{dt}}(f \wedge f) = \Theta(n)$. Define the Majority function, which we denote by MAJ, to be -1 if at least half of its input bits are -1 . It is also known [30] that MAJ satisfies $\text{UPP}^{\text{dt}}(\text{MAJ}) = O(1)$, yet $\text{UPP}^{\text{dt}}(\text{MAJ} \wedge \text{MAJ}) = \Theta(\log n)$. Our goal in this article is, to the extent possible, to show that the UPP^{cc} communication model behaves similarly to its query complexity analog.

Over the course of the last decade, there has been considerable progress in proving *lifting theorems* [16, 17, 28]. These theorems seek to show that if a function f has large complexity in some query model \mathcal{C} , then for some “sufficiently complicated” function g on a “small” number of inputs, the composition $f \circ g$ has large complexity in the associated communication model (ideally, $\mathcal{C}^{\text{cc}}(f \circ g) \gtrsim \mathcal{C}^{\text{dt}}(f)$).

Unfortunately, a “generic” lifting theorem for UPP complexity is not known. That is, it is not known how to take an arbitrary function f with high UPP^{dt} complexity, and by composing it with a function g on a small number of inputs, yield a function with high UPP^{cc} complexity.

However, as we now explain, some significant partial results have been shown in this direction. It is well-known that $\text{UPP}^{\text{dt}}(f)$ is equivalent to an approximation-theoretic notion called *threshold degree*, denoted $\text{deg}_{\pm}(f)$ (see Appendix B.1 for the definition). The threshold degree of f can in turn be expressed as the value of a certain (exponentially large) linear program. Linear programming duality then implies that one can prove lower bounds on $\text{deg}_{\pm}(f)$ by exhibiting good solutions to the dual linear program. We refer to such dual solutions as *dual witnesses* for threshold degree. Sherstov [29] and Razborov and Sherstov [27] showed that if $\text{deg}_{\pm}(f)$ is large, and moreover this can be exhibited by a dual witness satisfying a certain *smoothness* condition, then there is a function g defined on a constant number of inputs such that $f \circ g$ does have large UPP^{cc} complexity. Several recent works [7, 9, 10, 33] have managed to prove new UPP^{cc} lower bounds by constructing, for various functions f , smooth dual witnesses exhibiting the fact that $\text{deg}_{\pm}(f)$ is large.

Our key technical contribution is to bring this approach to bear on the function $F(x, y) = \text{MAJ}(x) \wedge \text{MAJ}(y)$. A familiarity with Sherstov’s work [30] is helpful to understand our proof. Specifically, we show that the (known) threshold degree lower bound $\text{deg}_{\pm}(F) \geq \Omega(\log n)$ can be exhibited by a smooth dual witness.

We do this as follows: Sherstov [30] showed that for any function $f: \{-1, 1\}^n \rightarrow \{-1, 1\}$, the threshold degree of the function $F = f \wedge f$ is characterized by the *rational approximate degree* of f , i.e., the least total degree of real polynomials p and q such that $|f(x) - p(x)/q(x)| \leq 1/3$ for all $x \in \{-1, 1\}^n$. He then showed that the rational approximate degree of MAJ is $\Omega(\log n)$, thereby concluding that $F(x, y)$ has threshold degree $\Omega(\log n)$.

From Sherstov’s arguments, one can derive a dual witness ψ for the fact that the rational approximate degree of MAJ is $\Omega(\log n)$, and then transform ψ into a dual witness ϕ for the fact that $F(x, y)$ has threshold degree $\Omega(\log n)$. Unfortunately, neither ψ nor ϕ satisfies the type of smoothness condition required by Razborov and Sherstov’s machinery to yield UPP^{cc} lower bounds.

The smoothness condition required for the Razborov-Sherstov machinery to work essentially states that the mass of the dual witness ψ has to be “relatively large” (a reasonably large fraction of what mass the uniform distribution would have placed) on a “large” set of inputs (the fraction of inputs that do not have large mass has to be small).

To construct a *smooth* dual witness ψ' for F , our primary technical contribution is to construct a *smooth* dual witness ϕ' for the fact that the rational approximate degree of MAJ is $\Omega(\log n)$. We then apply a different transformation, due to Sherstov [32], of ϕ' into a dual witness for the fact that the threshold degree of F is $\Omega(\log n)$, and we show that this transformation *preserves the smoothness* of ψ' .

In a nutshell, our smooth dual witness for MAJ is obtained in two steps: First, we define for all inputs u whose Hamming weight lies in $[n/2 - \lfloor n^{2/3} \rfloor, n/2 + \lfloor n^{2/3} \rfloor]$, a dual witness ϕ'_u that places

a large mass on u and not too much mass on other points. Next, we define the final dual witness ϕ' to be a certain weighted average over u of all the dual witnesses thus obtained. The resulting mass on $\phi'(x)$ for each x of Hamming weight in $[n/2 - \lfloor n^{2/3} \rfloor, n/2 + \lfloor n^{2/3} \rfloor]$ is large enough, and the fraction of inputs whose Hamming weight is not in $[n/2 - \lfloor n^{2/3} \rfloor, n/2 + \lfloor n^{2/3} \rfloor]$ is small enough, to allow us to use the Razborov-Sherstov framework (Theorem 2.3) to prove the desired sign-rank lower bound on the pattern matrix of F .

1.3 Organization

In Section 2, we review some required preliminaries. In Section 3, we state our main technical contribution: a smooth dual witness for the hardness of rationally approximating the sign function (Theorem 3.1). We then show how to extend this to a smooth dual witness for rationally approximating Majority in Theorem 3.2. Finally, in Theorem 3.3, we use this to construct a smooth dual witness for the threshold degree of the intersection of two Majorities and use the Razborov-Sherstov framework to conclude on a lower bound on the sign-rank of the pattern matrix of the intersection of two Majorities. We prove Theorem 3.1 in Section 4. We summarize our results and state some open questions in Section 5.

2 PRELIMINARIES

All logarithms in this article are taken base 2. We use the notation $\exp(x)$ to denote e^x , where e is Euler's number. Given any finite set X and any functions $f, g : X \rightarrow \mathbb{R}$, define $\|f\|_1 := \sum_{x \in X} |f(x)|$ and $\langle f, g \rangle := \sum_{x \in X} f(x)g(x)$. We refer to $\|f\|_1$ as the ℓ_1 -norm of f . For any $x \in \{-1, 1\}^n$, we use the notation $|x|$ to denote the *Hamming weight* of x , which is the number of -1 's in the string x .

Paturi and Simon [26] showed the following equivalence between the sign-rank of a matrix and the UPP^{cc} cost of its corresponding communication game.

THEOREM 2.1. *For any $F : \{-1, 1\}^{2n} \times \{-1, 1\}^n \rightarrow \{-1, 1\}$, let M_F denote its communication matrix, defined by $M_F(x, y) = F(x, y)$. Then, $\text{UPP}^{\text{cc}}(F) = \log \text{sr}(M_F) \pm O(1)$.*

Let n, N be positive integers such that n divides N . Partition the set $[N] := \{1, \dots, N\}$ into n disjoint blocks $\{1, 2, \dots, N/n\}, \{N/n + 1, \dots, 2N/n\}, \dots, \{(n-1)N/n + 1, \dots, N\}$. Define the set $\mathcal{P}(N, n)$ to be the collection of subsets of $[N]$ that contain exactly one element from each block. For $x \in \{-1, 1\}^N$ and $S \in \mathcal{P}(N, n)$, let $x|_S = (x_{s_1}, \dots, x_{s_n})$, where $s_1 < s_2 < \dots < s_n$ are the elements of S .

Definition 2.2 (Pattern Matrix). For any function $\phi : \{-1, 1\}^n \rightarrow \mathbb{R}$, the (N, n, ϕ) -pattern matrix M is defined as follows:

$$M = [\phi(x|_S \oplus w)]_{x \in \{-1, 1\}^N, (S, w) \in \mathcal{P}(N, n) \times \{-1, 1\}^n},$$

where $x|_S \oplus w$ denotes the bitwise XOR of the strings $x|_S$ and w . Note that M is a $2^N \times (N/n)n^{2^n}$ matrix.

In a breakthrough result, Forster [13] proved that an upper bound on the spectral norm of a sign matrix implies a lower bound on its sign-rank. Razborov and Sherstov [27] established a generalization of Forster's theorem [13] that can be used to prove sign-rank lower bounds for pattern matrices. Specifically, we require the following result, implicit in their work [27, Theorem 1.1].

THEOREM 2.3 (IMPLICIT IN [27]). *Let $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ be any Boolean function and $\alpha > 1$ be a real number. Suppose there exists a function $\phi : \{-1, 1\}^n \rightarrow \mathbb{R}$ satisfying the following conditions:*

- $\sum_{x \in \{-1, 1\}^n} |\phi(x)| = 1$.

- For all polynomials p of degree at most d , $\sum_{x \in \{-1, 1\}^n} \phi(x)p(x) = 0$.
- $f(x) \cdot \phi(x) \geq 0 \forall x \in \{-1, 1\}^n$.
- $|\phi(x)| \geq \gamma$ for all but a Δ fraction of inputs $x \in \{-1, 1\}^n$.

Then, the sign-rank of the (N, n, f) -pattern matrix M can be bounded below as

$$\text{sr}(M) \geq \frac{\gamma}{\frac{1}{2^n} \left(\frac{n}{N}\right)^{d/2} + \gamma\Delta}.$$

We require the following well-known combinatorial identity:

CLAIM 2.4. For every polynomial p of degree less than $2n$, we have $\sum_{t=-n}^n (-1)^t \binom{2n}{n+t} p(t) = 0$.

Recall from Section 1.2 that the rational ϵ -approximate degree of f is the least degree of two polynomials p and q such that $|f(x) - p(x)/q(x)| \leq \epsilon$ for all x in the domain of f . Sherstov [32, Theorem 6.9] showed that a dual witness to the rational approximate degree of any function f can be converted to a threshold degree dual witness for $\text{OR}_n \circ f$. Implicit in his theorem is the fact that a smooth dual witness to the rational approximate degree of f can be converted to a smooth dual witness for the threshold degree of $\text{OR}_n \circ f$. More precisely, the following result is established by the proof of [32, Theorem 6.9]³:

THEOREM 2.5 (SHERSTOV [32]). Let $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ be any function. Let F denote $\text{OR}_t \circ f : \{-1, 1\}^{nt} \rightarrow \{-1, 1\}$, and $\delta > 0$ be any real number.

Suppose there exist functions $\psi_0, \psi_1 : \{-1, 1\}^n \rightarrow \mathbb{R}$ that are not identically 0 and satisfy the following properties:

$$f(x) = 1 \implies \psi_0(x) \geq \delta |\psi_1(x)|, \quad (1)$$

$$f(x) = -1 \implies \psi_1(x) \geq \delta |\psi_0(x)|, \quad (2)$$

$$\deg(p) < d \implies \langle \psi_0, p \rangle = 0 \text{ and } \langle \psi_1, p \rangle = 0. \quad (3)$$

Then for any $0 < \epsilon < \min\{\delta, 1\}$, there exist functions $A, B : \{-1, 1\}^{nt} \rightarrow \mathbb{R}$ such that $\Psi = \frac{1}{\delta}A - \frac{1}{\epsilon}B$ satisfies the following properties:

$$\deg(p) \leq \min\{\lfloor \epsilon^2 t \rfloor, d\} \implies \langle \Psi, p \rangle = 0. \quad (4)$$

$$F(x) \cdot \Psi(x_1, \dots, x_t) \geq (\delta - \epsilon)^{2t} \prod_{i=1}^t |\psi_0(x_i)| \text{ for all } x \in \{-1, 1\}^{nt}. \quad (5)$$

$$|A(x_1, \dots, x_t)| \leq \prod_{i=1}^t |\psi_0(x_i)| \text{ for all } x = (x_1, \dots, x_t) \in \{-1, 1\}^{nt}. \quad (6)$$

$$|B(x_1, \dots, x_t)| \leq \prod_{i:f(x_i)=0} |\psi_0(x_i)| \cdot \prod_{i:f(x_i)=1} \delta \psi_1(x_i) + \prod_{i=1}^t (|\psi_0(x_i)| - \delta \psi_1(x_i))$$

for all $x = (x_1, \dots, x_t) \in \{-1, 1\}^{nt}$. (7)

3 A SMOOTH DUAL WITNESS FOR MAJORITY

Our main technical contribution in this article is captured in Theorem 3.1 below. This theorem constructs a smooth dual witness R for the hardness of rationally approximating the sign function

³ In Theorem 2.5, the functions ψ_1 and ψ_0 together form a dual witness for the fact that the rational δ -approximate degree of f is at least d , while Ψ is a dual witness to the fact that $\deg_{\pm}(F) \geq d$. See Appendix B for details. However, we will not exploit this interpretation of Theorem 2.5 in our analysis.

on $\{0, \pm 1, \dots, \pm n\}$ (cf. Appendix B for details of this interpretation of Theorem 3.1). We defer the proof until Section 4.

THEOREM 3.1. *Let $1 \leq d \leq \frac{1}{3} \log n$ and let n be odd. There exists a function $R : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$ such that*

$$\bullet \sum_{t=-n}^n |R(t)| = 1. \quad (8)$$

- For $\delta = \exp(-18/(n^{1/(6d)}))$ and every $t = 1, 2, \dots, n$,

$$R(t) \geq \delta |R(-t)|. \quad (9)$$

- If $p : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$ is any polynomial of degree less than $d - 2$, then

$$\langle R, p \rangle = 0. \quad (10)$$

- For every $t \in \{0, \pm 1, \pm 2, \dots, \pm \lfloor n^{2/3} \rfloor\}$, we have

$$|R(t)| \geq \Omega\left(\frac{1}{n^{20}}\right). \quad (11)$$

The following theorem shows how to convert the (univariate) function R from Theorem 3.1 into a dual witness for the (multivariate) MAJ function:

THEOREM 3.2. *Let $1 \leq d \leq \frac{1}{3} \log n$ and let n be odd. Let $R : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$ be any function obtained in Theorem 3.1. Then, the multivariate polynomial $R' : \{-1, 1\}^{2n} \rightarrow \mathbb{R}$ defined by $R'(x) = R(n - |x|) / \binom{2n}{|x|}$ satisfies the following properties:*

$$\bullet \|R'\|_1 = 1. \quad (12)$$

- For $\delta = \exp(-18/(n^{1/(6d)}))$ and every $t = 1, 2, \dots, n$,

$$R'(x) \geq \delta |R'(y)| \quad (13)$$

for any $x, y \in \{-1, 1\}^{2n}$ such that $|x| = n - t$, $|y| = n + t$.

- For any polynomial p of degree at most $d - 2$,

$$\langle R', p \rangle = 0. \quad (14)$$

- For all $x \in \{-1, 1\}^{2n}$ such that $n - \lfloor n^{2/3} \rfloor \leq |x| \leq n + \lfloor n^{2/3} \rfloor$,

$$|R'(x)| \geq \Omega\left(\frac{1}{n^{20} \cdot 2^{2n}}\right). \quad (15)$$

PROOF. To establish Equation (12), observe:

$$\begin{aligned} \|R'\|_1 &= \sum_{x \in \{-1, 1\}^{2n}} |R'(x)| = \sum_{t=0}^{2n} \left(\sum_{x \in \{-1, 1\}^{2n}: |x|=t} |R'(x)| \right) \\ &= \sum_{t=0}^{2n} \binom{2n}{t} |R(n-t)| / \binom{2n}{t} = \sum_{t=-n}^n |R(t)| = 1, \end{aligned}$$

where the last equality follows from Equation (8). Equation (13) follows directly from Equation (9) and the definition of R' .

To establish Equation (14), consider any polynomial $p : \{-1, 1\}^{2n} \rightarrow \mathbb{R}$ of degree at most $d - 2$. For any permutation $\sigma \in S_{2n}$, define the polynomial p_σ by $p_\sigma(x_1, \dots, x_{2n}) = p(x_{\sigma(1)}, \dots, x_{\sigma(2n)})$. Note that, since R' is symmetric, $\langle R', p_\sigma \rangle = \langle R', p \rangle$ for all $\sigma \in S_{2n}$. Define $q = \mathbb{E}_{\sigma \in S_{2n}} [p_\sigma]$. Note that q is symmetric and $\langle R', p \rangle = \langle R', q \rangle$. It is a well-known fact (cf. Reference [25]) that q can be

written as a polynomial q' of degree at most $d - 2$ in the variable $\sum_{i=1}^{2n} x_i$, and so can R' . Hence, $\langle R', p \rangle = \langle R', q \rangle = \sum_{t=0}^{2n} \binom{2n}{t} \frac{R(n-t)}{\binom{2n}{t}} \cdot q'(t) = 0$, where the final equality holds by Equation (10).

To establish Equation (15), observe that by Equation (11) and the definition of R' , we have that for all $x \in \{-1, 1\}^{2n}$ such that $|x| \in [n - \lfloor n^{2/3} \rfloor, n + \lfloor n^{2/3} \rfloor]$, $|R'(x)| \geq \Omega\left(\frac{1}{n^{20} \cdot \binom{2n}{|x|}}\right) \geq \Omega\left(\frac{1}{n^{20} \cdot 2^{2n}}\right)$. \square

We are ready to derive a lower bound on the sign-rank of the $(4n^2, 4n, \text{OR}_2 \circ \text{MAJ}_{2n})$ -pattern matrix.

THEOREM 3.3. *The $(4n^2, 4n, \text{OR}_2 \circ \text{MAJ}_{2n})$ -pattern matrix M satisfies $\text{sr}(M) \geq n^{\Omega(\log n)}$.*

PROOF. Let F denote the function $\text{OR}_2 \circ \text{MAJ}_{2n}$ in this proof. Set $d = (\log n)/100$ and consider the function $R : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$ obtained via Theorem 3.1. Define the function $R' : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$ by $R'(t) = R(-t)$. Define the functions $\psi_0, \psi_1 : \{-1, 1\}^{2n} \rightarrow \mathbb{R}$ by $\psi_1(x) = R(n - |x|)/\binom{2n}{|x|}$, and $\psi_0(x) = R'(n - |x|)/\binom{2n}{|x|}$. We now verify that ψ_0, ψ_1 satisfy the conditions in Theorem 2.5 for $\delta = \exp(-18/(n^{1/(6d)})) = \exp(-18/n^{100/(6 \cdot 100)}) = \exp(-18/2^{100/6}) > 0.99$. Set $\varepsilon = \delta \cdot c$, where $c > 0$ is a constant such that $0.99 > \delta \cdot c > 1/\sqrt{2}$.

- By the definitions of ψ_0, ψ_1 and Equation (13), Properties (1) and (2) in the statement of Theorem 2.5 are satisfied.
- Equation (14) implies that $\langle \psi_0, p \rangle = \langle \psi_1, p \rangle = 0$ for any polynomial p of degree at most $d - 2$, and hence Property (3) is satisfied.

Moreover, Equation (15) implies that $|\psi_0(x)|, |\psi_1(x)| \geq \Omega\left(\frac{1}{n^{20} \cdot 2^{2n}}\right)$ for all $x \in \{-1, 1\}^{2n}$ such that $n - \lfloor n^{2/3} \rfloor \leq |x| \leq n + \lfloor n^{2/3} \rfloor$, and Equation (12) implies $\|\psi_0\|_1 = \|\psi_1\|_1 = 1$. Theorem 2.5 now implies the existence of a function Ψ satisfying the following properties:

- By Equation (4), $\deg(p) < \min\{\lfloor 2\varepsilon^2 \rfloor \cdot ((\log n)/100 - 2), (\log n)/100 - 2\} \implies \langle \Psi, p \rangle = 0$. Since $\varepsilon > 1/\sqrt{2}$, this implies that

$$\deg(p) < (\log n)/100 - 2 \implies \langle \Psi, p \rangle = 0.$$

- By Equation (5), $\Psi(x) \cdot F(x) \geq 0$ for all $x \in \{-1, 1\}^{2n} \times \{-1, 1\}^{2n}$.
- We now note that the functions A and B obtained in Theorem 2.5 have ℓ_1 -norm at most a constant. Since $\|\psi_0\|_1 = \|\psi_1\|_1 = 1$, we use Equation (6) to conclude that

$$\sum_{x_1, x_2 \in \{-1, 1\}^{2n} \times \{-1, 1\}^{2n}} |A(x_1, x_2)| \leq \sum_{x_1 \in \{-1, 1\}^{2n}} |\psi_0(x_1)| \cdot \sum_{x_2 \in \{-1, 1\}^{2n}} |\psi_0(x_2)| = 1.$$

By Equation (7), we have

$$\sum_{x_1, x_2 \in \{-1, 1\}^{2n}} |B(x_1, x_2)| \leq \max\{\|\psi_0\|_1, \delta\|\psi_1\|_1\}^2 + \|\psi_0\|_1^2 + \delta\|\psi_0\|_1\|\psi_1\|_1 + \delta^2\|\psi_1\|_1^2,$$

which is at most a constant, since $\delta = O(1)$.

Combined with the fact that ε is a constant, we conclude $\|\Psi\|_1 \leq \frac{1}{\delta}\|A\|_1 + \frac{1}{\varepsilon}\|B\|_1 \leq O(1)$.

- By Equation (5), $F(x) \cdot \Psi(x_1, x_2) \geq (\delta - \varepsilon)^4 |\psi_0(x_1)| \cdot |\psi_0(x_2)| \forall x \in \{-1, 1\}^{4n}$. This implies that for $|x_1|, |x_2| \in [n - \lfloor n^{2/3} \rfloor, n + \lfloor n^{2/3} \rfloor]$,

$$|\Psi(x_1, x_2)| \geq \Omega\left(\frac{1}{n^{40} \cdot 2^{4n}}\right),$$

since $\delta - \varepsilon = \Omega(1)$.

- By a standard Chernoff bound, the number of inputs in $\{-1, 1\}^{2n} \times \{-1, 1\}^{2n}$ such that $|x_1|, |x_2| \in [n - \lfloor n^{2/3} \rfloor, n + \lfloor n^{2/3} \rfloor]$ is at least $(1 - 2 \exp(-n^{1/3}/3)) \cdot 2^{4n}$.

Plugging $f = \text{OR}_2 \circ \text{MAJ}_{2n}$ and $\phi = \frac{\Psi}{\|\Psi\|_1}$ into Theorem 2.3, we conclude that the sign-rank of the $(4n^2, 4n, \text{OR}_2 \circ \text{MAJ}_{2n})$ pattern matrix M is bounded below as

$$\text{sr}(M) \geq \Omega\left(\frac{\frac{1}{n^{40}} \cdot \frac{1}{2^{4n}}}{\left(\frac{1}{n^{(\log n/200)-1}} \cdot \frac{1}{2^{4n}}\right) + \left(\frac{1}{n^{40}} \cdot \frac{1}{2^{4n}} \cdot 2 \exp(-n^{1/3}/3)\right)}\right) \geq n^{\Omega(\log n)}. \quad \square$$

We are now ready to prove Theorem 1.1.

PROOF OF THEOREM 1.1. Note that the function $\text{AND} \circ \text{MAJ}(x) = \overline{\text{OR} \circ \text{MAJ}(\bar{x})}$. Consider the dual witness $\phi = \frac{\Psi}{\|\Psi\|_1}$ obtained for the threshold degree of $\text{OR}_2 \circ \text{MAJ}_{2n}$ in the previous proof. Note that the function ϕ' defined by $\phi'(x) = -\phi(\bar{x})$ acts as a dual witness for the threshold degree of $\text{AND}_2 \circ \text{MAJ}_{2n}$ and satisfies all the conditions in Theorem 2.3 with the same parameters as in the proof of Theorem 3.3. Proceeding in exactly the same way as in the previous proof, we conclude that sign-rank of the $(4n^2, 4n, \text{AND}_2 \circ \text{MAJ}_{2n})$ pattern matrix M' is bounded below as

$$\text{sr}(M') \geq n^{\Omega(\log n)}. \quad (16)$$

Denote by f the communication game corresponding to the $(2n^2, 2n, \text{MAJ}_{2n})$ pattern matrix. For completeness, we now sketch a standard UPP^{cc} protocol of cost $O(\log n)$ for f . Note that Alice holds $2n^2$ input bits, and Bob holds a $(2n \cdot \log n)$ -bit string indicating the “relevant bits” in each block of Alice’s input and a $2n$ -bit string w . Bob sends Alice the index of a uniformly random relevant bit using $\log(2n^2)$ bits of communication. Alice responds with her value b of that input bit, and Bob outputs $b \oplus w_i$. It is easy to check that this is a valid UPP^{cc} protocol, and it has cost $O(\log n)$.

One can verify by the definition of pattern matrices (Definition 2.2) that the communication game corresponding to the $(4n^2, 4n, \text{AND}_2 \circ \text{MAJ}_{2n})$ pattern matrix M' equals $f \wedge f$. By Theorem 2.1 and Equation (16), we obtain that

$$\text{UPP}(f \wedge f) = \Theta(\log \text{sr}(M')) = \Omega(\log^2 n).$$

As mentioned in Section 1, the result of Klivans et al. [21] implies that $\text{sr}(M') = n^{O(\log n)}$. Thus, the function f satisfies $\text{UPP}^{\text{cc}}(f) = O(\log n)$, but $\text{UPP}^{\text{cc}}(f \wedge f) = \Theta(\log^2 n)$. \square

Corollary 1.2 follows immediately from the previous proof and the definition of pattern matrices.

4 PROOF OF THEOREM 3.1

The rest of this article is dedicated towards proving Theorem 3.1.

SKETCH OF PROOF: The starting point of our proof is Sherstov’s [30, Theorem 5.3] construction of a dual witness for the hardness of rationally approximating the sign function on $\{0, \pm 1, \dots, \pm n\}$. This satisfies all the requirements of Theorem 3.1 except for the smoothness requirement in Equation (11). However, this dual witness does place a significant proportion of its ℓ_1 -mass on values close to 0. To ensure the required smoothness, we consider a suitably weighted average of several affine transformations of this dual witness. This ensures smoothness while still preserving the other requirements in Theorem 3.1.

We now formally describe the main auxiliary construction and prove some preliminary facts about it.

Let $\Delta = \lfloor n^{1/(3d)} \rfloor \geq 2$. Fix any $u \in \{1, \dots, \lfloor n^{2/3} \rfloor - 1, \lfloor n^{2/3} \rfloor\}$. Define the set

$$S_u = \{\pm u, \pm u\Delta, \pm u\Delta^2, \dots, \pm u\Delta^{d-1}\}.$$

Define the polynomial $r_u : \{0, \pm 1, \dots, \pm n\} \rightarrow \mathbb{R}$ by

$$r_u(t) = \frac{1}{(2n)!} \prod_{i=0}^{d-1} (t - (u\Delta^i \sqrt{\Delta})) \prod_{s \notin S_u} (t - s).$$

When $u = 1$, this corresponds to Sherstov's construction.

Since n is odd, notice that $\text{sgn}(r_u(t)) = (-1)^t$, for $t \in \{u, u\Delta, u\Delta^2, \dots, u\Delta^{d-1}\}$, and $r_u(t) = 0$ for $t \notin S_u$.

Define

$$p_u(t) = \binom{2n}{n+t} r_u(t) = \begin{cases} (-1)^{n-t} \cdot \frac{\prod_{i=0}^{d-1} (t - (u\Delta^i \sqrt{\Delta}))}{\prod_{\substack{s \in S_u \\ s \neq t}} (t - s)} & \text{if } t \in S_u \\ 0 & \text{otherwise.} \end{cases}$$

The following claim tells us that for any $u \in \{1, \dots, \lfloor n^{2/3} \rfloor\}$, the function p_u places a reasonably large mass on input $-u$:

CLAIM 4.1.

$$|p_u(-u)| \geq \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{-(d-1)^2/2}.$$

PROOF. We calculate

$$\begin{aligned} |p_u(-u)| &= \frac{u(\sqrt{\Delta} + 1)}{2u} \cdot \prod_{i=1}^{d-1} \frac{u(\Delta^i \sqrt{\Delta} + 1)}{u^2(\Delta^i + 1)(\Delta^i - 1)} \quad (\text{pairing terms corresponding to } u\Delta^i \text{ and } -u\Delta^i) \\ &= \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \prod_{i=1}^{d-1} \frac{\Delta^{i+\frac{1}{2}} + 1}{\Delta^{2i} - 1} \geq \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{(d-1)/2} \cdot \prod_{i=1}^{d-1} \frac{\Delta^i}{\Delta^{2i}} \\ &= \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{-(d-1)^2/2}. \quad \square \end{aligned}$$

The next claim tells us that the mass placed by p_u on other points in its support is small.

CLAIM 4.2. For every $j = 1, 2, \dots, d-1$,

$$|p_u(-u\Delta^j)| \leq e^4 \cdot \Delta^{-(j^2-3j-2)/2} \cdot \left(\frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{-(d-1)^2/2} \right).$$

PROOF. We calculate

$$\begin{aligned} |p_u(-u\Delta^j)| &= \frac{u(\Delta^j \sqrt{\Delta} + \Delta^j)}{2u\Delta^j} \cdot \prod_{i=0}^{j-1} \frac{u(\Delta^i \sqrt{\Delta} + \Delta^i)}{u^2(\Delta^i + \Delta^j)(\Delta^j - \Delta^i)} \cdot \prod_{i=j+1}^{d-1} \frac{u(\Delta^i \sqrt{\Delta} + \Delta^i)}{u^2(\Delta^i + \Delta^j)(\Delta^i - \Delta^j)} \\ &\quad (\text{pairing terms corresponding to } u\Delta^i \text{ and } -u\Delta^i) \\ &\leq \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \prod_{i=0}^{j-1} \frac{\sqrt{\Delta}}{\Delta^j - \Delta^i} \cdot \prod_{i=j+1}^{d-1} \frac{\sqrt{\Delta}}{\Delta^i - \Delta^j} \end{aligned}$$

$$\begin{aligned}
&\leq \frac{\sqrt{\Delta} + 1}{2} \cdot (\sqrt{\Delta} \cdot u^{-1})^{d-1} \cdot \prod_{i=0}^{j-1} \frac{\Delta^{j-i} \cdot \Delta^{-j}}{\Delta^{j-i} - 1} \cdot \prod_{i=j+1}^{d-1} \frac{\Delta^{-i} \cdot \Delta^{i-j}}{\Delta^{i-j} - 1} \\
&\leq \frac{\sqrt{\Delta} + 1}{2} \cdot (\sqrt{\Delta} \cdot u^{-1})^{d-1} \cdot \prod_{i=0}^{j-1} \Delta^{-j} \cdot \prod_{i=j+1}^{d-1} \Delta^{-i} \cdot \left(\prod_{k=1}^{\infty} \frac{\Delta^k}{\Delta^k - 1} \right)^2 \\
&\leq \frac{\sqrt{\Delta} + 1}{2} \cdot (\sqrt{\Delta} \cdot u^{-1})^{d-1} \cdot \Delta^{-j^2 - (d(d-1) - (j+2)(j+1))/2} \cdot \exp\left(2 \sum_{k=1}^{\infty} \frac{1}{\Delta^k - 1}\right) \\
&\hspace{15em} \text{(since } 1 + x \leq e^x \text{ for all } x \in \mathbb{R}) \\
&\leq \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{-(j^2 - 3j - 2)/2} \cdot \Delta^{-(d-1)^2/2} \cdot \exp\left(4 \sum_{k=1}^{\infty} \frac{1}{\Delta^k}\right) \hspace{5em} \text{(since } \Delta \geq 2) \\
&\leq e^4 \cdot \frac{\sqrt{\Delta} + 1}{2} \cdot u^{-(d-1)} \cdot \Delta^{-(j^2 - 3j - 2)/2} \cdot \Delta^{-(d-1)^2/2}. \hspace{5em} \text{(again using } \Delta \geq 2)
\end{aligned}$$

□

The following claim tells us that for each u and j , the masses placed by r_u (and hence p_u) on $u\Delta^j$ and $-u\Delta^j$ are comparable.

CLAIM 4.3. *For every $j = 0, 1, \dots, d-1$, we have*

$$\begin{aligned}
&|r_u(-u\Delta^j)| \geq |r_u(u\Delta^j)| \geq \exp(-18/\sqrt{\Delta}) |r_u(-u\Delta^j)| \\
&\text{and } |p_u(-u\Delta^j)| \geq |p_u(u\Delta^j)| \geq \exp(-18/\sqrt{\Delta}) |p_u(-u\Delta^j)|.
\end{aligned}$$

PROOF. We may write the ratio

$$\frac{|p_u(u\Delta^j)|}{|p_u(-u\Delta^j)|} = \frac{|r_u(u\Delta^j)|}{|r_u(-u\Delta^j)|} = \prod_{i=0}^{j-1} \frac{u(\Delta^j - \Delta^i \sqrt{\Delta})}{u(\Delta^j + \Delta^i \sqrt{\Delta})} \cdot \prod_{i=j}^{d-1} \frac{u(\Delta^i \sqrt{\Delta} - \Delta^j)}{u(\Delta^j + \Delta^i \sqrt{\Delta})}.$$

This is a product of terms smaller than 1, yielding the first inequality. For the second, we follow Sherstov's argument [30, Theorem 5.3] and note that this product is at least

$$\begin{aligned}
&\left(\prod_{i=1}^{\infty} \frac{\Delta^{i/2} - 1}{\Delta^{i/2} + 1} \right)^2 \geq \exp\left(-5 \sum_{i=1}^{\infty} \frac{1}{\Delta^{i/2}}\right) \hspace{5em} \text{since } (a-1)/(a+1) > \exp(-2.5/a) \text{ for } a \geq \sqrt{2} \\
&= \exp\left(\frac{-5}{\sqrt{\Delta}} \sum_{i=0}^{\infty} \frac{1}{\Delta^{i/2}}\right) \geq \exp\left(\frac{-5}{\sqrt{\Delta}} \cdot \frac{1}{1 - 1/\sqrt{2}}\right) \hspace{5em} \text{since } \Delta \geq 2 \\
&\geq \exp\left(-\frac{18}{\sqrt{\Delta}}\right). \hspace{15em} \square
\end{aligned}$$

Putting the three claims together, we obtain the following conclusion, which states that the mass placed by p_u on $-u$ and u is a relatively large fraction of its ℓ_1 -norm:

LEMMA 4.4. $|p_u(-u)| \geq \|p_u\|_1 / (8\Delta^2 e^4)$ and $|p_u(-u)| \geq |p_u(u)| \geq \frac{\exp(-18/\sqrt{\Delta}-4)}{8\Delta^2} \cdot \|p_u\|_1$.

PROOF. We bound the ratio

$$\begin{aligned}
\frac{\|p_u\|_1}{|p_u(-u)|} &\leq 2 \sum_{j=0}^{d-1} \frac{|p_u(-u\Delta^j)|}{|p_u(-u)|} && \text{by the first inequality in Claim 4.3} \\
&\leq 2 \left(1 + \sum_{j=0}^{d-1} e^4 \Delta^{-(j^2-3j-2)/2} \right) && \text{by Claims 4.1 and 4.2} \\
&\leq 2 + 2e^4 \left(\sum_{j=0}^3 \Delta^{-(j^2-3j-2)/2} + \sum_{j=4}^{\infty} \Delta^{-(j^2-3j-2)/2} \right) \\
&\leq 8\Delta^2 \cdot e^4 \cdot \sum_{k=1}^{\infty} \Delta^{-k} \leq 8 \cdot \Delta^2 \cdot e^4. && \text{since } \Delta \geq 2
\end{aligned}$$

By the above and the second inequality in Claim 4.3,

$$|p_u(u)| \geq \exp(-18/\sqrt{\Delta}) |p_u(-u)| \geq \frac{\exp(-18/\sqrt{\Delta} - 4)}{8\Delta^2} \cdot \|p_u\|_1. \quad \square$$

We are now ready to prove Theorem 3.1.

PROOF OF THEOREM 3.1. Define $P(t) = \sum_{u=1}^{\lfloor n^{2/3} \rfloor} u^{20} \cdot \frac{p_u(t)}{\|p_u\|_1}$. We claim that the function $R : \{0, \pm 1, \dots, \pm n\} \rightarrow \{-1, 1\}$ defined by $R(t) = \frac{(-1)^t P(t)}{\|P\|_1}$ satisfies the conditions in Theorem 3.1.

- Clearly, $\sum_{t=-n}^n |R(t)| = 1$, i.e., R satisfies Equation (8).
- By Claim 4.3, for every $u = 1, \dots, \lfloor n^{2/3} \rfloor$ and every $t = 1, \dots, n$, $(-1)^t p_u(t) \geq \delta |p_u(-t)|$ for $\delta = \exp(-18/\sqrt{\Delta}) = \exp(-18/n^{(1/6d)})$. Therefore, for all such t , we also have $(-1)^t P(t) \geq \delta |P(t)|$, which implies $R(t) \geq \delta |R(-t)|$ for every $t = 1, 2, \dots, n$.
- We have

$$R(t) = \frac{(-1)^t P(t)}{\|P\|_1} = \frac{(-1)^t}{\|P\|} \sum_{u=1}^{\lfloor n^{2/3} \rfloor} u^{20} \cdot \frac{p_u(t)}{\|p_u\|_1} = \frac{(-1)^t}{\|P\|_1} \binom{2n}{n+t} \sum_{u=1}^{\lfloor n^{2/3} \rfloor} u^{20} \cdot \frac{r_u(t)}{\|p_u\|_1}.$$

Since each r_u is a polynomial of degree at most $(2n+1) - d$, Claim 2.4 implies that for any polynomial p of degree at most $d-2$, $\langle R, p \rangle = 0$.

- It now remains to verify the smoothness condition. Fix a point $v \in \{1, \dots, \lfloor n^{2/3} \rfloor\}$. Since $\text{sgn}(p_u(v)) = (-1)^v$ for all u and for all $v > 0$, we have that

$$\begin{aligned}
\frac{|P(v)|}{\|P\|_1} &\geq v^{20} \cdot \frac{|p_v(v)| \cdot \|p_v\|_1^{-1}}{\sum_{u=1}^{\lfloor n^{2/3} \rfloor} u^{20}} \geq \frac{\exp(-18/\sqrt{\Delta} - 4)/8\Delta^2}{[n^{2/3}] \cdot ([n^{2/3}])^{20}} && \text{by Lemma 4.4} \\
&\geq \frac{\exp(-18/\sqrt{2} - 4)}{8n^{15}} \geq \frac{e^{-15}}{8n^{15}}. && \text{since } n^{1/3} \geq \Delta = \lfloor n^{1/3d} \rfloor \geq 2
\end{aligned}$$

If $v < 0$, then the argument needs some more care, because we do not have the guarantee that $\text{sgn}(p_u(v)) = (-1)^v$. The large mass placed by p_{-v} on the point v plays a crucial role.

$$\begin{aligned}
|P(v)| &\geq \frac{(-v)^{20} \cdot |p_{-v}(v)|}{\|p_{-v}\|_1} - \sum_{\substack{u=1 \\ u \neq v}}^{\lfloor n^{2/3} \rfloor} u^{20} \cdot \frac{p_u(-v)}{\|p_u\|_1} \\
&\geq \frac{(-v)^{20}}{8\Delta^2 e^4} - \sum_{j=1}^{\lfloor \log_{\Delta}(-v) \rfloor} (-v\Delta^{-j})^{20} \cdot \frac{p_{-v\Delta^{-j}}(v)}{\|p_{-v\Delta^{-j}}\|_1} \\
&\quad \text{by Lemma 4.4, the definition of } p_u \text{ and its support} \\
&\geq (-v)^{20} \left[\frac{1}{8\Delta^2 e^4} - e^4 \sum_{j=1}^{\infty} \Delta^{-20j} \cdot \Delta^{-(j^2+3j+2)/2} \right] \quad \text{by Claims 4.1 and 4.2} \\
&= (-v)^{20} \left[\frac{1}{8\Delta^2 e^4} - e^4 \sum_{j=1}^{\infty} \Delta^{(-j^2-37j+2)/2} \right] \geq (-v)^{20} \left[\frac{1}{8\Delta^2 e^4} - e^4 \sum_{j=1}^{\infty} \Delta^{-18j} \right] \\
&\geq (-v)^{20} \left[\frac{1}{8\Delta^2 e^4} - \frac{e^4}{\Delta^{17}} \right] = (-v)^{20} \left[\frac{\Delta^{15} - 8e^8}{8\Delta^{17} e^4} \right] \geq \frac{20}{\Delta^{17}} \geq \frac{20}{n^6}. \\
&\quad \text{since } n^{1/3} \geq \Delta \geq 2 \text{ and } (-v) \geq 1
\end{aligned}$$

Thus, we have that for $v < 0$,

$$\frac{|P(v)|}{\|P\|_1} \geq \frac{20}{n^6 \sum_{u=1}^{\lfloor n^{2/3} \rfloor} u^{20}} \geq \frac{20}{n^6 \lfloor n^{2/3} \rfloor \cdot (\lfloor n^{2/3} \rfloor)^{20}} \geq \frac{20}{n^{20}}. \quad \square$$

5 CONCLUSION

We have exhibited a communication problem f with $\text{UPP}^{\text{cc}}(f) = O(\log n)$, and $\text{UPP}^{\text{cc}}(f \wedge f) = \Theta(\log^2 n)$. This is the first result showing that **UPP** communication complexity can increase by more than a constant factor under intersection. As a consequence, we have concluded that the dimension-complexity-based quasipolynomial time PAC learning algorithm of Reference [21] for learning intersections of polylogarithmically many majorities is optimal. That is, new learning algorithms not based on dimension complexity will be required to learn this class in polynomial time.

A glaring open question left by our work is whether the class of problems with polylogarithmic UPP^{cc} complexity is closed under intersection. Our results represent an important first step in this direction. It would also be very interesting to extend our result that dimension-complexity-based algorithms cannot PAC learn intersections of two majorities in polynomial time, to rule out an even larger class of learning algorithms. Specifically, it would be very interesting to show that no algorithm working in the important *statistical query* model [19] can learn this concept class in polynomial time.

APPENDICES

A OTHER RELATED WORK ON SIGN RANK

Alon, Frankl, and Rödl [1] proved lower bounds on the sign-rank of random matrices. The first nontrivial lower bounds for explicit matrix families was obtained in the breakthrough work of Forster [13], who proved strong lower bounds on the sign-rank of any sign matrix with small spectral norm. Several subsequent works improved and generalized Forster's method and studied

the relationship of sign-rank to other important complexity measures in learning theory and circuit complexity [2, 14, 15, 24]. As previously mentioned, Sherstov [29] and Razborov and Sherstov [27] showed that a smooth dual witness for the fact that a function has large threshold degree implies that a related function has large sign-rank. Razborov and Sherstov used this result to great effect, constructing a smooth dual witnesses for the large threshold degree of a certain DNF, and thereby giving an AC^0 function with exponential sign-rank. This answered an old question of Babai, Frankl, and Simon [4]. Recent works have quantitatively strengthened these sign-rank lower bounds for AC^0 [9, 10, 33]. Another work, due to Bouland et al. [7], managed to apply the methods to *simpler* functions within AC^0 and thereby resolved several old open questions about the power of statistical zero knowledge proofs.

B THRESHOLD DEGREE, RATIONAL APPROXIMATE DEGREE, SIGN-RANK, AND DUALITY

In this appendix, we define threshold degree and introduce its dual formulation, and also introduce the dual formulation of rational approximate degree. We also explain the connection between the threshold degree, rational approximate degree, and the sign-rank of pattern matrices. The material in this appendix is standard and provided only for intuition; none of it is actually required to prove the results in this article.

B.1 Threshold Degree and Its Dual Formulation

The *threshold degree* of a Boolean function $f: \{-1, 1\}^n \rightarrow \{-1, 1\}$, denoted $\deg_{\pm}(f)$, is the least degree of a real polynomial p that sign-represents f , i.e., $p(x) \cdot f(x) > 0$ for all $x \in \{-1, 1\}^n$.

To describe the dual formulation of threshold degree, we need to introduce some terminology.

Definition B.1. Let $\psi: \{-1, 1\}^n \rightarrow \mathbb{R}$ be any real-valued function on the Boolean hypercube. Recall (see Section 2) that, given another function $p: \{-1, 1\}^n \rightarrow \mathbb{R}$, we let $\langle \psi, p \rangle := \sum_{x \in \{-1, 1\}^n} \psi(x) \cdot p(x)$, and refer to $\langle \psi, p \rangle$ as the *correlation* of ψ with p . Also, $\|\psi\|_1 := \sum_{x \in \{-1, 1\}^n} |\psi(x)|$, and we refer to $\|\psi\|_1$ as the ℓ_1 -norm of ψ . If $\langle \psi, p \rangle = 0$ for all polynomials p of degree at most d , we say that ψ has *pure high degree* at least d .

The following standard theorem provides the aforementioned dual formulation of threshold degree:

THEOREM B.2. *Let $f: \{-1, 1\}^n \rightarrow \{-1, 1\}$. Then $\deg_{\pm}(f) > d$ if and only if there is a real function $\psi: \{-1, 1\}^n \rightarrow \mathbb{R}$ such that:*

- (1) (*Pure high degree*): ψ has pure high degree at least d .
- (2) (*Non-triviality*): $\|\psi\|_1 > 0$.
- (3) (*Sign Agreement*): $\psi(x) \cdot f(x) \geq 0$ for all $x \in \{-1, 1\}^n$.

ψ is called a *dual polynomial* for the fact that $\deg_{\pm}(f) > d$.

The relationship between threshold degree and sign-rank of pattern matrices. Suppose that $\deg_{\pm}(f) = d$. Then it is not hard to see that the (N, n, f) -pattern matrix M has sign-rank at most $\binom{N}{d} \leq N^d$. This is because each entry $M_{x, (S, w)}$ of M can be written as the sign of a linear combination of monomials in x , where each monomial in the linear combination has degree at most d . Theorem 2.3 shows that this sign-rank upper bound is essentially tight, so long as there is a dual polynomial ψ for that fact that $\deg_{\pm}(f) \geq d$, such that ψ satisfies an extra smoothness condition.

B.2 Rational Approximate Degree and Its Dual Formulation

In Section 1.2, we defined the rational ϵ -approximate degree of f to be the least total degree of real polynomials p and q such that $|f(x) - p(x)/q(x)| \leq \epsilon$ for all x in the domain of f . The functions ψ_0 and ψ_1 appearing in Theorem 2.5 constitute a dual witness to the large rational approximate degree of f . However, to describe the duality theory of rational approximate degree, it is helpful to introduce a related notion, due to Sherstov [32].

Definition B.3 (Sherstov [32] Definition 6.4). For $d_0, d_1 > 0$ and a function $f: \{-1, 1\}^n \rightarrow \{-1, 1\}$, define $R(f, d_0, d_1)$ as the infimum over all $\epsilon > 0$ for which there exist polynomials p_0, p_1 of degree at most d_0, d_1 , respectively, such that:

- $f(x) = 1 \implies |p_1(x)| < \epsilon \cdot p_0(x)$,
- $f(x) = -1 \implies |p_0(x)| < \epsilon \cdot p_1(x)$.

The relationship between rational approximate degree and Definition B.3. Sherstov [32] showed that, for constant $\epsilon > 0$, the rational ϵ -approximate degree of f is at most $O(d)$ if and only if there is some constant $c > 0$ such that $R(f, c \cdot d, c \cdot d) \leq \epsilon$. And unlike rational approximate degree itself, $R(f, d_0, d_1)$ has a clean dual characterization.

THEOREM B.4 (SHERSTOV [32] THEOREM 6.6). For $d_0, d_1 > 0$ and a function $f: \{-1, 1\}^n \rightarrow \{-1, 1\}$, $R(f, d_0, d_1) \geq \epsilon$ if and only if there exist $\psi_0, \psi_1: \{-1, 1\}^n \rightarrow \mathbb{R}$ such that

- $\psi_0(x) \geq \epsilon |\psi_1(x)|$ for all $x \in f^{-1}(1)$.
- $\psi_1(x) \geq \epsilon |\psi_0(x)|$ for all $x \in f^{-1}(-1)$.
- ψ_0 has pure high degree at least d_0 .
- ψ_1 has pure high degree at least d_1 .
- $\|\psi_0\|_1, \|\psi_1\|_1 > 0$.

The Connection between Rational Approximate Degree and Threshold Degree of Intersections. Let $F = f \wedge g$. Beigel et al. [5] famously showed that if f has rational approximate degree at most d , then F has threshold degree at most $O(d)$ (see Reference [32, Section 1.2] for a lucid explanation of this upper bound). The dual formulations of threshold degree (Theorem B.2) and rational approximate degree (Theorem B.4) together allow us to interpret Theorem 2.5 as showing that the upper bound of Beigel et al. is tight. That is, Theorem 2.5 shows that if f has rational δ -approximate degree at least d for an appropriate value of δ , then F has threshold degree at least d . In fact, Theorem 2.5 explicitly translates a dual witness to the high rational approximate degree of f into a dual witness to the high threshold degree of F .

REFERENCES

- [1] Noga Alon, Peter Frankl, and Vojtech Rödl. 1985. Geometrical realization of set systems and probabilistic communication complexity. In *Proceedings of the 26th Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 277–280. DOI: <https://doi.org/10.1109/SFCS.1985.30>
- [2] Noga Alon, Shay Moran, and Amir Yehudayoff. 2016. Sign rank versus VC dimension. In *Proceedings of the 29th Conference on Learning Theory (COLT)*. JMLR.org, 47–80. Retrieved from <http://jmlr.org/proceedings/papers/v49/alon16.html>.
- [3] Andris Ambainis, Andrew M. Childs, Ben W. Reichardt, Robert Špalek, and Shengyu Zhang. 2010. 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, 6 (2010), 2513–2530. DOI: <https://doi.org/10.1137/080712167>
- [4] László Babai, Peter Frankl, and Janos Simon. 1986. Complexity classes in communication complexity theory (preliminary version). In *Proceedings of the 27th Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 337–347. DOI: <https://doi.org/10.1109/SFCS.1986.15>
- [5] Richard Beigel, Nick Reingold, and Daniel A. Spielman. 1995. PP Is closed under intersection. *J. Comput. Syst. Sci.* 50, 2 (1995), 191–202. DOI: <https://doi.org/10.1006/jcss.1995.1017>

- [6] Arnab Bhattacharyya, Suprovat Ghoshal, and Rishi Saket. 2018. Hardness of learning noisy halfspaces using polynomial thresholds. In *Proceedings of the Conference On Learning Theory (COLT)*. PMLR, 876–917. Retrieved from <http://proceedings.mlr.press/v75/bhattacharyya18a.html>.
- [7] Adam Bouland, Lijie Chen, Dhiraj Holden, Justin Thaler, and Prashant Nalini Vasudevan. 2017. On the power of statistical zero knowledge. In *Proceedings of the 58th IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 708–719. DOI : <https://doi.org/10.1109/FOCS.2017.71>
- [8] Mark Bun, Nikhil S. Mande, and Justin Thaler. 2019. Sign-rank can increase under intersection. In *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming (ICALP)*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 30:1–30:14. DOI : <https://doi.org/10.4230/LIPIcs.ICALP.2019.30>
- [9] Mark Bun and Justin Thaler. 2016. Improved bounds on the sign-rank of AC^0 . In *Proceedings of the 43rd International Colloquium on Automata, Languages, and Programming (ICALP)*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 37:1–37:14. DOI : <https://doi.org/10.4230/LIPIcs.ICALP.2016.37>
- [10] Mark Bun and Justin Thaler. 2019. The large-error approximate degree of AC^0 . In *Proceedings of the Conference on Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 55:1–55:16. DOI : <https://doi.org/10.4230/LIPIcs.APPROX-RANDOM.2019.55>
- [11] Arkadev Chattopadhyay and Nikhil S. Mande. 2018. A short list of equalities induces large sign rank. In *Proceedings of the 59th IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 47–58. DOI : <https://doi.org/10.1109/FOCS.2018.00014>
- [12] Vitaly Feldman, Parikshit Gopalan, Subhash Khot, and Ashok Kumar Ponnuswami. 2006. New results for learning noisy parities and halfspaces. In *Proceedings of the 47th IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE, IEEE Computer Society, 563–574.
- [13] Jürgen Forster. 2002. A linear lower bound on the unbounded error probabilistic communication complexity. *J. Comput. Syst. Sci.* 65, 4 (2002), 612–625. DOI : [https://doi.org/10.1016/S0022-0000\(02\)00019-3](https://doi.org/10.1016/S0022-0000(02)00019-3)
- [14] Jürgen Forster, Matthias Krause, Satyanarayana V. Lokam, Rustam Mubarakzjanov, Niels Schmitt, and Hans Ulrich Simon. 2001. Relations between communication complexity, linear arrangements, and computational complexity. In *Proceedings of the 21st Conference on Foundations of Software Technology and Theoretical Computer Science*. Springer, 171–182. DOI : https://doi.org/10.1007/3-540-45294-X_15
- [15] Jürgen Forster and Hans Ulrich Simon. 2006. On the smallest possible dimension and the largest possible margin of linear arrangements representing given concept classes. *Theor. Comput. Sci.* 350, 1 (2006), 40–48. DOI : <https://doi.org/10.1016/j.tcs.2005.10.015>
- [16] Mika Göös, Pritish Kamath, Toniann Pitassi, and Thomas Watson. 2019. Query-to-communication lifting for P^{NP} . *Comput. Complex.* 28, 1 (2019), 113–144. DOI : <https://doi.org/10.1007/s00037-018-0175-5>
- [17] Mika Göös, Toniann Pitassi, and Thomas Watson. 2017. Query-to-communication lifting for BPP. In *Proceedings of the 58th IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 132–143. DOI : <https://doi.org/10.1109/FOCS.2017.21>
- [18] Mika Göös, Toniann Pitassi, and Thomas Watson. 2018. The landscape of communication complexity classes. *Comput. Complex.* 27, 2 (2018), 245–304. DOI : <https://doi.org/10.1007/s00037-018-0166-6>
- [19] Michael Kearns. 1998. Efficient noise-tolerant learning from statistical queries. *J. ACM* 45, 6 (1998), 983–1006.
- [20] Subhash Khot and Rishi Saket. 2011. On the hardness of learning intersections of two halfspaces. *J. Comput. Syst. Sci.* 77, 1 (2011), 129–141.
- [21] Adam R. Klivans, Ryan O’Donnell, and Rocco A. Servedio. 2004. Learning intersections and thresholds of halfspaces. *J. Comput. Syst. Sci.* 68, 4 (2004), 808–840. DOI : <https://doi.org/10.1016/j.jcss.2003.11.002>
- [22] Adam R. Klivans and Rocco A. Servedio. 2004. Learning DNF in time $2^{O(n^{1/3})}$. *J. Comput. Syst. Sci.* 68, 2 (2004), 303–318. DOI : <https://doi.org/10.1016/j.jcss.2003.07.007>
- [23] Adam R. Klivans and Alexander A. Sherstov. 2009. Cryptographic hardness for learning intersections of halfspaces. *J. Comput. Syst. Sci.* 75, 1 (2009), 2–12.
- [24] Nati Linial, Shahar Mendelson, Gideon Schechtman, and Adi Shraibman. 2007. Complexity measures of sign matrices. *Combinatorica* 27, 4 (2007), 439–463.
- [25] Marvin Minsky and Seymour Papert. 1969. *Perceptrons*. The MIT Press.
- [26] Ramamohan Paturi and Janos Simon. 1986. Probabilistic communication complexity. *J. Comput. Syst. Sci.* 33, 1 (1986), 106–123. DOI : [https://doi.org/10.1016/0022-0000\(86\)90046-2](https://doi.org/10.1016/0022-0000(86)90046-2)
- [27] Alexander A. Razborov and Alexander A. Sherstov. 2010. The sign-rank of AC^0 . *SIAM J. Comput.* 39, 5 (2010), 1833–1855. DOI : <https://doi.org/10.1137/080744037>
- [28] Alexander A. Sherstov. 2011. The pattern matrix method. *SIAM J. Comput.* 40, 6 (2011), 1969–2000. DOI : <https://doi.org/10.1137/080733644>

- [29] Alexander A. Sherstov. 2011. The unbounded-error communication complexity of symmetric functions. *Combinatorica* 31, 5 (2011), 583–614. DOI : <https://doi.org/10.1007/s00493-011-2580-0>
- [30] Alexander A. Sherstov. 2013. The intersection of two halfspaces has high threshold degree. *SIAM J. Comput.* 42, 6 (2013), 2329–2374. DOI : <https://doi.org/10.1137/100785260>
- [31] Alexander A. Sherstov. 2013. Optimal bounds for sign-representing the intersection of two halfspaces by polynomials. *Combinatorica* 33, 1 (2013), 73–96. DOI : <https://doi.org/10.1007/s00493-013-2759-7>
- [32] Alexander A. Sherstov. 2018. Breaking the Minsky-Papert barrier for constant-depth circuits. *SIAM J. Comput.* 47, 5 (2018), 1809–1857. DOI : <https://doi.org/10.1137/15M1015704>
- [33] Alexander A. Sherstov and Pei Wu. 2019. Near-optimal lower bounds on the threshold degree and sign-rank of AC^0 . In *Proceedings of the 51st ACM SIGACT Symposium on Theory of Computing (STOC)*. ACM, 401–412. DOI : <https://doi.org/10.1145/3313276.3316408>

Received May 2020; revised February 2021; accepted April 2021