Electronic Colloquium on Computational Complexity, Report No. 138 (2016)

ON MULTIPARTY COMMUNICATION WITH LARGE VERSUS UNBOUNDED ERROR

ALEXANDER A. SHERSTOV

Abstract. The communication complexity of F with *unbounded error* is the limit of the ϵ-error randomized complexity of F as $\epsilon \to 1/2$. Communication complexity with *weakly bounded error* is defined similarly but with an additive penalty term that depends on $1/2 - \epsilon$. Explicit functions are known whose two-party communication complexity with unbounded error is exponentially smaller than with weakly bounded error. Chattopadhyay and Mande (ECCC Report TR16-095) recently generalize this exponential separation to the number-on-the-forehead multiparty model, using a rather technical proof from first principles.

We show how to derive such an exponential separation from known two-party work, achieving stronger parameters along the way. We present several proofs for this result, some as short as half a page. Our strongest separation is a k-party communication problem $F\colon (\{0,1\}^n)^k \to \{0,1\}$ that has complexity $O(\log n)$ with unbounded error and $\Omega(n/4^k)$ with weakly bounded error.

* 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

The *number-on-the-forehead* model, due to Chandra et al. [11], is the most powerful model of multiparty communication. The model features k communicating players and a Boolean function $F\colon X_1 \times X_2 \times \cdots \times X_k \to \{-1,+1\}$ with k arguments. An input $(x_1, x_2, \ldots, x_k)$ is distributed among the k players by giving the ith player the arguments $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k$ but not x_i. This arrangement can be visualized as having the k players seated in a circle with x_i written on the ith player's forehead, whence the name of the model. Number-on-the-forehead is the canonical model in the area because any other way of assigning arguments to the players results in a less powerful model—provided of course that one does not assign all the arguments to some player, in which case there is never a need to communicate.

The players communicate according to a protocol agreed upon in advance. The communication occurs in the form of broadcasts, with a message sent by any given player instantly reaching everyone else. The players' objective is to compute F on any given input with minimal communication. To this end, each player privately holds an unbounded supply of uniformly random bits which he can use in deciding what message to send at any given point in the protocol. The *cost* of a protocol is the total bit length of all the messages broadcast in the worst-case execution. The *ϵ-error randomized communication complexity* $R_\epsilon(F)$ of a given function F is the least cost of a protocol that computes F with probability of error at most ϵ on every input. Number-on-the-forehead communication complexity is a natural subject of study in its own right, in addition to its applications to circuit complexity, pseudorandomness, and proof complexity [2, 37, 19, 26, 6].

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

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

and

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

The former quantity, introduced by Paturi and Simon [24], is called the *unbounded-error* communication complexity of F, in reference to the fact that the error probability can be arbitrarily close to $1/2$. The latter quantity, proposed by Babai et al. [1], includes an additional penalty term that depends on the error probability. For lack of a better word, we refer to $\mathsf{PP}(F)$ as the *large-error* communication complexity of F. Both of these complexity measures give rise to complexity classes in communication complexity theory [1]. Formally, UPP_k is the class of families $\{F_{n,k}\}_{n=1}^{\infty}$ of k-party communication problems $F_{n,k}\colon (\{0,1\}^n)^k \to \{-1,+1\}$ whose unbounded-error communication complexity is at most polylogarithmic in n. Its

counterpart PP_k is defined analogously for the complexity measure PP. The authors of [24] and [1] focused on two-party communication ($k = 2$). In the generalization just described, $k = k(n)$ can be an arbitrary constant or a growing function of n.

1.1. Previous work. Large-error communication is by definition no more powerful than unbounded-error communication, and for twenty years it was unknown whether this containment is proper. Buhrman et al. [9] and the author [29] answered this question for two-party communication, 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 large- versus unbounded-error communication complexity: $\mathrm{UPP}(F) = O(\log n)$ in both works, versus $\mathrm{PP}(F) = \Omega(n^{1/3})$ in [9] and $\mathrm{PP}(F) = \Omega(\sqrt{n})$ in [29]. In complexity-theoretic notation, these results show that $\mathsf{PP}_2 \subsetneq \mathsf{UPP}_2$.

The analyses by Buhrman et al. [9] and the author [29] were quite specialized. The former was based on a subtle lemma from Razborov's quantum lower bound [25] for set disjointness, whereas the latter was built around an earlier result of Goldmann et al. [18] on the discrepancy of a low-degree polynomial threshold function. In subsequent work, the author developed a general technique called the *pattern matrix method* [30, 31], which makes it possible to obtain communication lower bounds from simpler, approximation-theoretic complexity measures of Boolean functions. We used the pattern matrix method in [31] to give a simple alternate proof of the separation due to Buhrman et al. [9]. Following up, Thaler [36] and Bun and Thaler [10] used the pattern matrix-based approach to obtain quantitatively improved results. The strongest known separation [10] features, for any constant $\delta > 0$, a function $F\colon \{0,1\}^n \times \{0,1\}^n \to \{-1,+1\}$ with $\mathrm{UPP}(F) = O(\log n)$ and $\mathrm{PP}(F) = \Omega(n^{\frac{2}{3}-\delta})$.

The surveyed work on large- versus unbounded-error communication complexity focused on the two-party model. Recent years saw a resurgence of interest in *multiparty* communication complexity classes, with numerous separations established over the past decade [3, 21, 13, 16, 4, 17]. In a new contribution to this line of work, Chattopadhyay and Mande [14] revisit the large- versus unbounded-error question in the multiparty setting. They generalize the original two-party separation [29] to $k \geqslant 3$ parties, exhibiting a k-party communication problem $F\colon (\{0,1\}^n)^k \to \{-1,+1\}$ with $\mathrm{UPP}(F) = O(\log n)$ and $\mathrm{PP}(F) = \Omega(\sqrt{n}/4^k - \log n - k)$. Thus, the proper containment $\mathsf{PP}_k \subsetneq \mathsf{UPP}_k$ continues to hold for up to $k \approx 0.25 \log_2 n$ players.

1.2. Our results. Chattopadhyay and Mande's analysis is a rather technical and lengthy generalization of the two-party argument, although it is admittedly self-contained. The purpose of our manuscript is to show how to derive the proper containment $\mathsf{PP}_k \subsetneq \mathsf{UPP}_k$ from two-party work in an almost trivial manner, achieving stronger parameters along the way. The key is to use the pattern matrix-based approach to the problem [31, 36, 10], as opposed to the earlier two-party work [18, 29] which forms the basis for Chattopadhyay and Mande's result.

In more detail, we present three short proofs separating large- and unbounded-error multiparty communication complexity, all of which work by applying the pattern matrix method to a result from polynomial approximation. To start with, we give a half-a-page proof that $\mathsf{PP}_k \subsetneq \mathsf{UPP}_k$ for up to $k \approx 0.5 \log_2 n$ players,

constructing an explicit function with an exponential gap between large- versus unbounded-error complexity. The proof of this qualitative result is presented in Section 3.1 and is virtually identical to the previous analyses in the two-party setting [31, 36, 10]. By applying the pattern matrix method to more recent work in approximation theory, we are able to give quantitatively improved separations. Our strongest result is the following nonconstructive theorem.

THEOREM 1.1 (Nonconstructive separation). *There exists a k-party communication problem $H\colon (\{0,1\}^n)^k \to \{-1,+1\}$ with*

$$\begin{aligned} \mathrm{UPP}(H) &= O(\log n), \\ \mathrm{PP}(H) &= \Omega\left(\frac{n}{4^k}\right). \end{aligned}$$

Moreover,

$$H(x) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{i=1}^{n} w_i x_{1,i} x_{2,i} \cdots x_{k,i}\right) \tag{1.1}$$

for some fixed $w_1, w_2, \ldots, w_n \in \{0, \pm 1, \pm 2, \ldots, \pm(2^n - 1)\}$.

Recall that no nontrivial lower bounds are currently known for multiparty communication with $k \geqslant \log_2 n$ players. Therefore, Theorem 1.1 with its linear lower bound for up to $k \approx 0.5 \log_2 n$ represents the state of the art in the area. By using additional input bits, it is straightforward to obtain an *explicit* function that contains every function of the form (1.1) as a subfunction. Specifically, Theorem 1.1 implies the following constructive separation with quadratically weaker parameters.

COROLLARY 1.2. *Let $F\colon \{0,1\}^{n+\sqrt{n}} \times (\{0,1\}^{\sqrt{n}})^{k-1} \to \{-1,+1\}$ be the k-party communication problem given by*

$$F(x) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{i=1}^{\sqrt{n}} \left((-1)^{x_{1,i,\sqrt{n}}} \sum_{j=0}^{\sqrt{n}-1} 2^j x_{1,i,j}\right) x_{2,i} x_{3,i} \ldots x_{k,i}\right).$$

Then

$$\begin{aligned} \mathrm{UPP}(F) &= O(\log n), \\ \mathrm{PP}(F) &= \Omega\left(\frac{\sqrt{n}}{4^k}\right). \end{aligned}$$

The function in this corollary has a pleasing closed form. Coincidentally, it is almost the same as Chattopadhyay and Mande's function [14], in which the individual bits $x_{i,j}$ have domain ± 1 rather than $0, 1$. The communication lower bound in Corollary 1.2 is already an improvement on [14] and is tight for any fixed k. We are able to obtain a stronger constructive separation, as follows.

THEOREM 1.3 (Constructive separation). *For any constant $\delta > 0$, there is an (explicitly given) k-party communication problem $F\colon (\{0,1\}^n)^k \to \{-1,+1\}$ such that*

$$\begin{aligned} \mathrm{UPP}(F) &= O(\log^3 n), \\ \mathrm{PP}(F) &= \Omega\left(\frac{n}{4^k k^2}\right)^{\frac{2}{3}-\delta}. \end{aligned}$$

The proof of this theorem is as short as our qualitative separation but uses Bun and Thaler's recent result [10] on polynomial approximation. The separation in Theorem 1.3 is polynomially stronger than Chattopadhyay and Mande's and continues to hold for larger k.

In summary, this paper reflects the author's view that a proof should be as modular and general as possible. It was this aesthetic that motivated the pattern matrix method in the first place and here allowed us to obtain stronger results with shorter proofs. On the other hand, Chattopadhyay and Mande's treatment is preferable if a first-principles proof is desired.

1.3. Paper organization. The remainder of this paper is organized as follows. Section 2 gives a leisurely overview of the technical preliminaries, which the expert reader may wish to skim or skip altogether. We then prove our qualitative, constructive, and nonconstructive results in Sections 3.1–3.3.

2. PRELIMINARIES

There are two common arithmetic encodings for the Boolean values: the traditional encoding *false* $\leftrightarrow 0$, *true* $\leftrightarrow 1$, and the more recent Fourier-inspired encoding *false* $\leftrightarrow 1$, *true* $\leftrightarrow -1$. Throughout this manuscript, we use the former encoding for the domain of a Boolean function and the latter for the range. In particular, Boolean functions for us 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

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

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 $(\ldots, (1-g(x_i))/2, \ldots) \in \operatorname{dom} f$.

The analytic notation that we use is entirely standard. For a function $f\colon X \to \mathbb{R}$ on an arbitrary finite set X, we let $\|f\|_\infty = \max_{x \in X} |f(x)|$ denote the infinity norm of f. Euler's number is denoted $\mathrm{e} = 2.7182\ldots$. The sign function is given as usual

by

$$\operatorname{sgn} x = \begin{cases} -1, & x < 0, \\ 0, & x = 0, \\ 1, & x > 0. \end{cases}$$

For a subset $X \subseteq \mathbb{R}$, we let $\operatorname{sgn}|_X$ denote the restriction of the sign function to X. In other words, $\operatorname{sgn}|_X \colon X \to \{-1, 0, +1\}$ is the mapping that sends $x \mapsto \operatorname{sgn} x$. We let $\log x$ stand for the logarithm of x to base 2.

2.1. Approximation by polynomials. 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 $f \colon X \to \mathbb{R}$ be a given function, for a finite subset $X \subset \mathbb{R}^n$. For any $d \geqslant 0$, define

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

where the minimum is over real polynomials p of degree at most d. In words, $E(f, d)$ is the minimum error in a pointwise approximation of f by a polynomial of degree no greater than d. The *ϵ-approximate degree* of f, denoted $\deg_\epsilon(f)$, is the least degree of a real polynomial p such that $\|f - p\|_\infty \leqslant \epsilon$. Any polynomial p with this property is said to be a *uniform approximant*, or *pointwise approximant*, to f with error ϵ. Observe that

$$\deg_\epsilon(f) = \min\{d : E(f, d) \leqslant \epsilon\}.$$

The study of approximate degree as a complexity measure was initiated by Nisan and Szegedy [22]. It has since found a variety of applications in theoretical computer science, including circuit complexity, quantum query complexity, communication complexity, and computational learning theory; see [28, 33, 36, 10] and the references therein. Applications motivate the study of ϵ-approximate degree for the full range of ϵ, including low-error approximation $\epsilon = o(1)$, large-error approximation $\epsilon = 1 - o(1)$, and constant-error approximation (ϵ bounded away from 0 and 1). The standard choice of error parameter in constant-error approximation is $\epsilon = 1/3$, an aesthetically motivated constant that is replaceable by any other in $(0, 1)$ without changing the theory in any significant way. Specifically, the following result of Buhrman et al. [8, p. 384] gives an efficient way to reduce the error in a pointwise approximation of a Boolean function at the expense of a modest multiplicative increase in the degree of the approximant.

FACT 2.1 (Buhrman et al.). *For all functions $f \colon X \to \{-1, +1\}$ on a finite subset $X \subset \mathbb{R}^n$,*

$$\deg_\delta(f) \leqslant O\left(\frac{1}{(1-\epsilon)^2} \log \frac{2}{\delta}\right) \cdot \deg_\epsilon(f), \qquad 0 < \delta < \epsilon < 1.$$

While Fact 2.1 is sufficient for our purposes, we note that it is not optimal. For example, one can improve the dependence on ϵ quadratically, from $1/(1-\epsilon)^2$ to $1/(1-\epsilon)$, by appealing to Jackson's theorem [27, Theorem 1.4]. An advantage of Fact 2.1 is its short and elegant proof, which we include for the reader's convenience.

Proof (adapted from Buhrman et al.) Consider the degree-d univariate polynomial

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

In words, $B_d(t)$ is the probability of observing more heads than tails in a sequence of d independent coin flips, each coming up heads with probability t. By the Chernoff bound for sufficiently large

$$d = O\left(\frac{1}{(1-\epsilon)^2} \log \frac{2}{\delta}\right),$$

B_d sends $[0, \frac{\epsilon}{1+\epsilon}] \to [0, \frac{\delta}{2}]$ and similarly $[1 - \frac{\epsilon}{1+\epsilon}, 1] \to [1 - \frac{\delta}{2}, 1]$. In particular, if a given Boolean function $f(x)$ is approximated pointwise within ϵ by a polynomial $p(x)$, then $f(x)$ is approximated pointwise within δ by $2B_d(\frac{1}{2+2\epsilon}p(x) + \frac{1}{2}) - 1$. □

2.2. Approximation of specific functions. Among the first findings in this line of work was Paturi's tight lower bound [23] for the constant-error approximation of the sign function. Specifically, Paturi showed that approximating the sign function on $\{\pm 1, \pm 2, \pm 3, \ldots, \pm n\}$ pointwise to within $1/3$ requires a polynomial of linear degree.

THEOREM 2.2 (Paturi).

$$\deg_{1/3}(\operatorname{sgn}|_{\{\pm 1, \pm 2, \pm 3, \ldots, \pm n\}}) = \Omega(n).$$

Paturi in fact proved the stronger result that the majority function on n bits has $1/3$-approximate degree $\Omega(n)$, but Theorem 2.2 will suffice for our purposes. On the large-error side, Beigel [7] constructed the following function in his seminal work on perceptrons. Its remarkable feature is that low-degree polynomials can represent it in sign but cannot approximate it uniformly except with error exponentially close to 1.

THEOREM 2.3 (Beigel). *Let* $f_n \colon \{0,1\}^n \to \{-1,+1\}$ *be given by*

$$f_n(x) = \operatorname{sgn}\left(1 + \sum_{i=1}^{n} (-2)^i x_i\right).$$

Then for all $1 \leqslant d \leqslant \sqrt{n}$,

$$E(f_n, d) > 1 - \exp\left(-\Omega\left(\frac{n}{d^2}\right)\right).$$

To be precise, Beigel phrased his proof in terms of a related approximation-theoretic quantity known as *threshold weight*. A proof of Theorem 2.3 as it is stated here is available, e.g., in Thaler [36, Section 1.2.2]. Thaler in fact obtained a far-reaching generalization of Beigel's result, with the following consequence of interest for our purposes [36, Sections 4.1.3, 4.2.3].

THEOREM 2.4 (Thaler). *There exists an (explicitly given) function* $f_n\colon \{0,1\}^n \to \{-1,+1\}$ *such that*

$$E\left(f_n, \left(\frac{n}{\log n}\right)^{2/5}\right) > 1 - \exp\left(-\Omega\left(\frac{n}{\log n}\right)^{2/5}\right)$$

and $f_n(x) = \operatorname{sgn} p(x)$ *for a real polynomial* p *of degree* $O(\log n)$.

Bun and Thaler [10, Theorem 2 and Remark 3] recently obtained a stronger yet result, as follows.

THEOREM 2.5 (Bun and Thaler). *Let* $\delta > 0$ *be an arbitrary constant. Then for each* $n \geqslant 2$, *there exists an (explicitly given) function* $f_n\colon \{0,1\}^n \to \{-1,+1\}$ *such that*

$$E\left(f_n, n^{\frac{2}{3}-\delta}\right) > 1 - 2^{-n}$$

and $f_n(x) = \operatorname{sgn} p(x)$ *for a real polynomial* p *of degree* $O(\log^2 n)$.

To our knowledge, Theorem 2.5 is the strongest known construction of a function that is easy to sign-represent but hard to approximate pointwise. Any future improvements on Bun and Thaler's theorem will automatically translate in corresponding improvements on Theorem 1.3 in this paper.

2.3. Multiparty communication. An excellent reference on communication complexity is the monograph by Kushilevitz and Nisan [20]. 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. [11]. 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 ith player (for $i = 1, 2, \ldots, k$). In other words, the ith 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.

2.4. Communication with unbounded error. 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 *unbounded-error communication complexity* of F, introduced by Paturi and Simon [24], is the quantity

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

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

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

We refer to $\mathrm{PP}(F)$ as the *large-error communication complexity* of F. These two complexity measures naturally give rise to corresponding classes UPP_k and PP_k in multiparty communication complexity [1], inspired both by the Turing machine class PP. 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 growing function. Then $\{F_{n,k}\}_{n=1}^\infty \in \mathsf{UPP}_k$ if and only if $\mathrm{UPP}(F_{n,k}) \leqslant \log^c(n+k)$ for some constant c and all $n \geqslant c$. Analogously, $\{F_{n,k}\}_{n=1}^\infty \in \mathsf{PP}_k$ if and only if $\mathrm{PP}(F_{n,k}) \leqslant \log^c(n+k)$ for some constant c and all $n \geqslant c$. By definition,

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

The following well-known result, cf. [24], gives a large class of communication problems that are efficiently computable with unbounded error.

FACT 2.6 (cf. Paturi and Simon). *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*

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

For the reader's convenience, we include a folklore proof of this result.

Proof. For a subset S, let x_S denote the product of the variables indexed by S. By hypothesis,

$$F(x) = \operatorname{sgn} \left(\sum_{i=1}^{\ell} a_{S_i} x_{S_i} \right)$$

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

for some subsets $S_1, S_2, \ldots, S_\ell$ and some reals $a_{S_1}, a_{S_2}, \ldots, a_{S_\ell}$. Consider the following communication protocol, which involves only two of the k players. The first player chooses a random index i according to the probability distribution $|a_{S_i}|/(|a_{S_1}| + |a_{S_2}| + \cdots + |a_{S_\ell}|)$, and broadcasts i. He then collaborates with the second player to compute the corresponding monomial x_{S_i} on the input in question. Finally, they output a random element of $\{-1, +1\}$ with expected value $\operatorname{sgn}(a_{S_i} x_{S_i})$.

It is straightforward to verify that this protocol can be implemented using at most $\lceil \log \ell \rceil + 2$ bits of communication. For correctness, the output on a given input x has expected value

$$\frac{1}{|a_{S_1}| + |a_{S_2}| + \cdots + |a_{S_\ell}|} \sum_{i=1}^{\ell} a_{S_i} x_{S_i},$$

which agrees in sign with $F(x)$. Therefore, the protocol computes $F(x)$ correctly with probability greater than $1/2$. □

2.5. Discrepancy. Our main result involves proving, for communication problems F of interest, an upper bound on $\mathrm{UPP}(F)$ and a lower bound on $\mathrm{PP}(F)$. The former requires direct construction; the latter relies on technical machinery which we now review. 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 ith function does not depend on the ith coordinate but may depend arbitrarily on the other $k-1$ coordinates. Introduced by Babai et al. [2], 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 the discrepancy give lower bounds on randomized communication complexity, a classic technique known as the *discrepancy method* [15, 2, 20].

THEOREM 2.7 (Discrepancy method). *Let F be a (possibly partial) Boolean function on $X_1 \times X_2 \times \cdots \times X_k$. Then*

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

A proof of Theorem 2.7 in the stated generality is available in [32, Theorem 2.9]. Combining this theorem with the definition of $\mathrm{PP}(F)$ gives the following corollary.

COROLLARY 2.8. *Let F be a (possibly partial) Boolean function on $X_1 \times X_2 \times \cdots \times X_k$. Then*

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

2.6. Pattern matrix method. Theorem 2.7 and Corollary 2.8 highlight the role of discrepancy in proving lower bounds on randomized communication complexity. Apart from a few canonical examples [20], 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 class of communication problems. The technique was developed in [30, 31] in the context of two-party communication complexity and has since been generalized by several authors to the multiparty setting [21, 13, 16, 5, 12, 32, 35]. We now review the strongest form [32, 35] 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 ith party knows all the sets except for the ith. Identifying the sets with their characteristic vectors, set disjointness corresponds to the Boolean function $\mathrm{DISJ}_{n,k} \colon (\{0,1\}^n)^k \to \{-1,+1\}$ given by

$$\mathrm{DISJ}_{n,k}(x_1, x_2, \ldots, x_k) = \neg \bigvee_{i=1}^{n} x_{1,i} \wedge x_{2,i} \wedge \cdots \wedge x_{k,i}. \tag{2.2}$$

The partial function $\mathrm{UDISJ}_{n,k}$ on $(\{0,1\}^n)^k$, called *unique set disjointness*, is defined as the restriction of $\mathrm{DISJ}_{n,k}$ 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. The two theorems that follow were proved in [32, Theorem 5.7] and [35, Theorem 5.7], respectively.

THEOREM 2.9 (Sherstov). *For every Boolean function $f\colon \{0,1\}^n \to \{-1,+1\}$, all positive integers m and k, and all reals $0 < \gamma < 1$,*

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

THEOREM 2.10 (Sherstov). *For every Boolean function $f\colon \{0,1\}^n \to \{-1,+1\}$, all positive integers m and k, and all reals $0 < \gamma < 1$,*

$$\operatorname{disc}(f \circ \mathrm{UDISJ}_{m,k}) \leqslant \left(\frac{c2^k k}{\sqrt{m}}\right)^{\deg_{1-\gamma}(f)/2} + \gamma,$$

where $c \geqslant 1$ is an absolute constant.

The same bounds clearly apply to the discrepancy of $f \circ \mathrm{DISJ}_{m,k}$, an extension of $f \circ \mathrm{UDISJ}_{m,k}$. In typical usage, Theorem 2.10 is significantly stronger than Theorem 2.9 unless the approximate degree $\deg_{1-\gamma}(f)$ is large, e.g., linear in the number of variables n. On the other hand, Theorem 2.9 is significantly easier to prove. Both theorems reduce the discrepancy analysis to the study of simpler, approximation-theoretic properties of Boolean functions. This makes it possible to prove communication lower bounds by leveraging the existing literature on polynomial approximation, such as Theorems 2.2–2.5.

3. Main results

We are now in a position to establish the proper containment $\mathsf{PP}_k \subsetneq \mathsf{UPP}_k$ for up to $k \approx 0.5 \log n$ players. We present three distinct proofs for this separation. All of them apply the pattern matrix method to a relevant result on polynomial approximation, in a manner closely analogous to the two-party work [31, 36, 10]. The key new element is the observation that the unique set disjointness function has an exact representation on its domain as a polynomial with a small number of monomials. 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

$$\mathrm{UDISJ}_{m,k}(x) = \mathrm{UDISJ}^*_{m,k}(x), \qquad x \in \operatorname{dom} \mathrm{UDISJ}_{m,k}. \tag{3.1}$$

Section 3.1 presents our simplest and shortest proof of $\mathsf{PP}_k \subsetneq \mathsf{UPP}_k$. We follow up in Sections 3.2 and 3.3 with quantitatively stronger separations, settling the main constructive and nonconstructive results of this paper. Sections 3.1–3.3 are independent and can be read in any order.

3.1. A qualitative separation. Of the two variants of the multiparty pattern matrix method (Theorems 2.9 and 2.10), the latter is more technically demanding than the former. Similarly, the literature on the polynomial approximation of Boolean functions spans a broad spectrum of technical sophistication. Here, we combine the *simplest* variant of the pattern matrix method with the *simplest* theorem on polynomial approximation. Our proof is virtually identical to the previous proofs in the two-party setting, e.g., [31, Section 10] and [36, Section 4.2.3]. The only point of departure, (3.1), is to check that the inner gadget remains a sparse polynomial as the number of parties grows.

THEOREM 3.1. *For all 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*

$$\mathrm{UPP}(F_{n,k}) = O(\log n), \tag{3.2}$$

$$\mathrm{PP}(F_{n,k}) = \Omega\left(\frac{n}{4^k}\right)^{1/7}. \tag{3.3}$$

Moreover,

$$F_{n,k}(x) = \operatorname{sgn}\left(w_0 + \sum_{i=1}^{n} w_i x_{1,i} x_{2,i} \cdots x_{k,i}\right) \tag{3.4}$$

for fixed reals $w_0, w_1, \ldots, w_n$.

Proof. Let $f_n\colon \{0,1\}^n \to \{-1,+1\}$ be the function defined in Theorem 2.3. Then $f_n(x) = \operatorname{sgn} p(x)$ for a linear polynomial $p\colon \{0,1\}^n \to \mathbb{R}$, and

$$\deg_{1-\exp(-cn^{1/3})}(f_n) \geqslant n^{1/3} \tag{3.5}$$

for some constant $c > 0$. Abbreviate $m = \lceil 2^{k+1} e n^{2/3} \rceil^2$ and consider the k-party communication problem $F'_{n,k}\colon (\{0,1\}^{nm})^k \to \{-1,+1\}$ given by

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

where the right-hand side features the coordinatewise composition of p with n independent copies of $\mathrm{UDISJ}^*_{m,k}$. The identity (3.1) implies that $F'_{n,k}$ coincides with $f_n \circ \mathrm{UDISJ}_{m,k}$ on the domain of the latter. Therefore,

$$\begin{aligned}
\mathrm{PP}(F'_{n,k}) &\geqslant \mathrm{PP}(f_n \circ \mathrm{UDISJ}_{m,k}) \\
&\geqslant \log \frac{2}{\mathrm{disc}(f_n \circ \mathrm{UDISJ}_{m,k})} \\
&\geqslant \log \frac{2}{2^{-n^{1/3}} + \exp(-cn^{1/3})} \\
&= \Omega(n^{1/3}),
\end{aligned}$$

where the second step uses Corollary 2.8 and the third step follows from (3.5) by the pattern matrix method (Theorem 2.9). Now (3.3) and (3.4) are immediate by letting $F_{n,k} = F'_{\lfloor (n/4^{k+4})^{3/7} \rfloor, k}$, whereas (3.2) follows from (3.4) by Fact 2.6. □

Theorem 3.1 is not as strong as our main results, to be established shortly. It is nevertheless of qualitative interest because of its corollary:

COROLLARY. *Let $\epsilon > 0$ be an arbitrary constant. Then for $k \leqslant (0.5 - \epsilon) \log n$,*

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

3.2. The constructive separation. We now prove our main constructive separation of PP_k and UPP_k, stated as Theorem 1.3 in the Introduction. The proof is as short as that of the qualitative separation in Section 3.1. This time, however, we must appeal to the stronger version of the pattern matrix method as well as to Bun and Thaler's recent result on polynomial approximation.

THEOREM (restatement of Theorem 1.3). *Let $\delta > 0$ be an arbitrary constant. Then for all 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*

$$\begin{aligned} \mathrm{UPP}(F_{n,k}) &= O(\log^3 n), \\ \mathrm{PP}(F_{n,k}) &= \Omega\left(\frac{n}{4^k k^2}\right)^{\frac{2}{3}-\delta}. \end{aligned}$$

Proof. Abbreviate $m = \lceil 4c2^k k \rceil^2$, where $c \geqslant 1$ is the constant from Theorem 2.10. Let $f_n \colon \{0,1\}^n \to \{-1,+1\}$ be the function defined in Theorem 2.5, so that

$$\deg_{1-2^{-n}}(f_n) \geqslant n^{\frac{2}{3}-\delta} \tag{3.6}$$

and $f_n(x) = \operatorname{sgn} p(x)$ for a polynomial $p \colon \{0,1\}^n \to \mathbb{R}$ of degree $O(\log^2 n)$. Consider the k-party communication problem $F'_{n,k} \colon (\{0,1\}^{nm})^k \to \{-1,+1\}$ given by

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

where the right-hand side features the coordinatewise composition of p with n independent copies of $\mathrm{UDISJ}^*_{m,k}$. It is clear that the resulting composed polynomial features at most $(n+1)^{\deg p} \cdot (m+1)^{\deg p} = 2^{O(\log^3 nm)}$ monomials, whence

$$\mathrm{UPP}(F'_{n,k}) = O(\log^3 nm) \tag{3.7}$$

by Fact 2.6. On the other hand, (3.1) implies that $F'_{n,k}$ coincides with $f_n \circ \mathrm{UDISJ}_{m,k}$ on the domain of the latter. Therefore,

$$\begin{aligned}\mathrm{PP}(F'_{n,k}) &\geqslant \mathrm{PP}(f_n \circ \mathrm{UDISJ}_{m,k}) \\ &\geqslant \log \frac{2}{\mathrm{disc}(f_n \circ \mathrm{UDISJ}_{m,k})} \\ &\geqslant \log \frac{2}{2^{-\deg_{1-2^{-n}}(f_n)} + 2^{-n}} \\ &= \Omega(n^{\frac{2}{3}-\delta}),\end{aligned} \tag{3.8}$$

where the second step uses Corollary 2.8, the third step follows by the pattern matrix method (Theorem 2.10), and the final step uses (3.6). Letting $F_{n,k} = F'_{\lfloor n/m \rfloor,k}$, the proof is complete in view of (3.7) and (3.8). □

3.3. The nonconstructive separation. We close with a nonconstructive separation of PP_k and UPP_k, which quantitatively is our strongest. The main new ingredient here is an approximation-theoretic result [34, Theorem 5.1] on random halfspaces. Informally, it states that approximating a random halfspace in n Boolean variables is at least as hard as approximating the sign function on an exponentially larger domain, $\{\pm 1, \pm 2, \pm 3, \ldots, \pm \exp(\Omega(n))\}$.

THEOREM 3.2 (Sherstov). *Let $0 < \alpha < 1$ be a sufficiently small absolute constant. Then there exist reals $w_1, w_2, \ldots, w_n \in \{0, 1, 2, \ldots, 2^n - 1\}$ such that the function $f_n \colon \{0,1\}^n \times \{0, 1, 2, \ldots, n\} \to \{-1, +1\}$ given by*

$$f_n(x,t) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{i=1}^{n} w_i x_i - 2^{\lfloor \alpha n \rfloor + 1} t\right) \tag{3.9}$$

obeys

$$E(f_n, d) \geqslant E(\operatorname{sgn}|_{\{\pm 1, \pm 2, \pm 3, \ldots, \pm 2^{\lfloor \alpha n \rfloor}\}}, d), \qquad d = 0, 1, \ldots, \lfloor \alpha n \rfloor.$$

This result was proved in [34] in the greater generality of approximation by rational functions. The special case of polynomial approximation, stated above, corresponds to fixing $q = 1$ in the proof of [34, Theorem 5.1].

COROLLARY 3.3. *There exist reals $w_1, w_2, \ldots, w_{n+1} \in \{0, 1, 2, \ldots, 2^n - 1\}$ such that the function $h_n \colon \{0,1\}^{2n} \to \{-1, +1\}$ given by*

$$h_n(x) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{i=1}^{n} w_i x_i - w_{n+1} \sum_{i=n+1}^{2n} x_i\right) \tag{3.10}$$

obeys

$$E(h_n, cn) > 1 - \exp(-cn),$$

where $c > 0$ is an absolute constant.

Proof. Let $0 < \alpha < 1$ be the absolute constant from Theorem 3.2, and abbreviate $S = \operatorname{sgn}|_{\{\pm 1, \pm 2, \pm 3, \ldots, \pm 2^{\lfloor \alpha n \rfloor}\}}$. Theorem 2.2 and Fact 2.1 imply that

$$\Omega(2^{\lfloor \alpha n \rfloor}) \leqslant \deg_{1/3}(S) \leqslant O\left(\frac{1}{(1 - E(S, \lfloor \alpha n \rfloor))^2}\right) \cdot \lfloor \alpha n \rfloor,$$

whence

$$E(S, \lfloor \alpha n \rfloor) \geqslant 1 - \Omega\left(\frac{\lfloor \alpha n \rfloor}{2^{\lfloor \alpha n \rfloor}}\right)^{1/2}. \tag{3.11}$$

Now fix $w_1, w_2, \ldots, w_n$ whose existence is guaranteed by Theorem 3.2, and set $w_{n+1} = 2^{\lfloor \alpha n \rfloor + 1}$. Let f_n and h_n be given by (3.9) and (3.10). Then

$$\begin{aligned} E(h_n, \lfloor \alpha n \rfloor) &= E(f_n, \lfloor \alpha n \rfloor) \\ &\geqslant E(S, \lfloor \alpha n \rfloor). \end{aligned}$$

where the first step holds by a standard symmerization argument (see, e.g., [34, Proposition 2.6]) and the second step is immediate from Theorem 3.2. This completes the proof in view of (3.11). □

We are now in a position to prove our nonconstructive separation, stated as Theorem 1.1 in the Introduction.

THEOREM (restatement of Theorem 1.1). *There exists a k-party communication problem $H_{n,k} \colon (\{0,1\}^n)^k \to \{-1, +1\}$ with*

$$\mathrm{UPP}(H_{n,k}) = O(\log n), \tag{3.12}$$

$$\mathrm{PP}(H_{n,k}) = \Omega\left(\frac{n}{4^k}\right). \tag{3.13}$$

Moreover,

$$H_{n,k}(x) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{i=1}^{n} w_i x_{1,i} x_{2,i} \cdots x_{k,i}\right) \tag{3.14}$$

for some fixed $w_1, w_2, \ldots, w_n \in \{0, \pm 1, \pm 2, \ldots, \pm(2^n - 1)\}$.

Proof. Let $h_n \colon \{0,1\}^{2n} \to \{-1, +1\}$ be the function whose existence is assured by Corollary 3.3. Then

$$\deg_{1 - \exp(-cn)}(h_n) \geqslant cn \tag{3.15}$$

for some constant $c > 0$, and moreover $h_n(x) = \operatorname{sgn} p(x)$ for a linear polynomial $p \colon \{0,1\}^{2n} \to \mathbb{R}$ with constant term $1/2$ and all other coefficients integers bounded

in absolute value by $2^n - 1$. Abbreviate $m = \lceil 2^{k+2}\mathrm{e}/c \rceil^2$ and consider the k-party communication problem $H'_{n,k} \colon (\{0,1\}^{2nm})^k \to \{-1,+1\}$ given by

$$H'_{n,k} = \operatorname{sgn} p \left(\frac{1 - \mathrm{UDISJ}^*_{m,k}}{2}, \frac{1 - \mathrm{UDISJ}^*_{m,k}}{2}, \ldots, \frac{1 - \mathrm{UDISJ}^*_{m,k}}{2} \right),$$

where the right-hand side features the coordinatewise composition of p with $2n$ independent copies of $\mathrm{UDISJ}^*_{m,k}$. The identity (3.1) implies that $H'_{n,k}$ coincides with $h_n \circ \mathrm{UDISJ}_{m,k}$ on the domain of the latter. Therefore,

$$\begin{aligned}
\mathrm{PP}(H'_{n,k}) &\geqslant \mathrm{PP}(h_n \circ \mathrm{UDISJ}_{m,k}) \\
&\geqslant \log \frac{2}{\operatorname{disc}(h_n \circ \mathrm{UDISJ}_{m,k})} \\
&\geqslant \log \frac{2}{2^{-cn} + \exp(-cn)} \\
&= \Omega(n),
\end{aligned}$$

where the second step uses Corollary 2.8 and the third step follows from (3.15) by the pattern matrix method (Theorem 2.9). A moment's thought shows that $H'_{\lfloor n/(4m) \rfloor,k}$ is a subfunction of some $H_{n,k}$ in the theorem statement, whence (3.13) and (3.14). The remaining property (3.12) follows from (3.14) by Fact 2.6. □

It is noteworthy that the previous theorem, despite being nonconstructive, implies the following constructive result with quadratically weaker parameters.

Corollary (restatement of Corollary 1.2). *Let $F_{n,k} \colon \{0,1\}^{n+\sqrt{n}} \times (\{0,1\}^{\sqrt{n}})^{k-1} \to \{-1,+1\}$ be the k-party communication problem given by*

$$F_{n,k}(x) = \operatorname{sgn} \left(\frac{1}{2} + \sum_{i=1}^{\sqrt{n}} \left((-1)^{x_{1,i,\sqrt{n}}} \sum_{j=0}^{\sqrt{n}-1} 2^j x_{1,i,j} \right) x_{2,i} x_{3,i} \ldots x_{k,i} \right).$$

Then

$$\mathrm{UPP}(F_{n,k}) = O(\log n), \tag{3.16}$$

$$\mathrm{PP}(F_{n,k}) = \Omega\left(\frac{\sqrt{n}}{4^k} \right). \tag{3.17}$$

Proof. In the notation of the previous theorem, every $H_{\sqrt{n},k}$ is a subfunction of $F_{n,k}$. Therefore, (3.17) follows from (3.13), whereas (3.16) is immediate by Fact 2.6. □

Acknowledgments

The author is thankful to Arkadev Chattopadhyay and Nikhil Mande for a stimulating discussion and helpful feedback on an earlier version of this manuscript.

References

[1] 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.

[2] 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.

[3] 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.

[4] P. Beame, M. David, T. Pitassi, and P. Woelfel, *Separating deterministic from randomized multiparty communication complexity*, Theory of Computing, 6 (2010), pp. 201–225, doi:10.4086/toc.2010.v006a009.

[5] 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.

[6] P. Beame, T. Pitassi, and N. Segerlind, *Lower bounds for Lovász-Schrijver systems and beyond follow from multiparty communication complexity*, SIAM J. Comput., 37 (2007), pp. 845–869, doi:10.1137/060654645.

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

[8] 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.

[9] 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.

[10] M. Bun and J. Thaler, *Approximate degree and the complexity of depth three circuits*, in Electronic Colloquium on Computational Complexity (ECCC), 2016. Report TR16-121.

[11] 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.

[12] A. Chattopadhyay, *Circuits, Communication, and Polynomials*, PhD thesis, McGill University, 2008.

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

[14] A. Chattopadhyay and N. Mande, *Small error versus unbounded error protocols in the NOF model*, in Electronic Colloquium on Computational Complexity (ECCC), September 2016. Report TR16-095, Revision 1.

[15] 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.

[16] M. David, T. Pitassi, and E. Viola, *Improved separations between nondeterministic and randomized multiparty communication*, ACM Transactions on Computation Theory (TOCT), 1 (2009), doi:10.1145/1595391.1595392.

[17] D. Gavinsky and A. A. Sherstov, *A separation of* NP *and* coNP *in multiparty communication complexity*, Theory of Computing, 6 (2010), pp. 227–245, doi:10.4086/toc.2010.v006a010.

[18] M. Goldmann, J. Håstad, and A. A. Razborov, *Majority gates vs. general weighted threshold gates*, Computational Complexity, 2 (1992), pp. 277–300, doi:10.1007/BF01200426.

[19] J. Håstad and M. Goldmann, *On the power of small-depth threshold circuits*, Computational Complexity, 1 (1991), pp. 113–129, doi:10.1007/BF01272517.

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

[21] 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.

[22] N. Nisan and M. Szegedy, *On the degree of Boolean functions as real polynomials*, Computational Complexity, 4 (1994), pp. 301–313, doi:10.1007/BF01263419.

[23] 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.

[24] 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.

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

[26] A. A. Razborov and A. Wigderson, $n^{\Omega(\log n)}$ *lower bounds on the size of depth-3 threshold circuits with AND gates at the bottom*, Inf. Process. Lett., 45 (1993), pp. 303–307, doi:10.1016/0020-0190(93)90041-7.

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

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

[29] 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.

[30] 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.

[31] 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.

[32] A. A. Sherstov, *The multiparty communication complexity of set disjointness*, in *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing* (STOC), 2012, pp. 525–544, doi:10.1145/2213977.2214026.

[33] A. A. Sherstov, *Making polynomials robust to noise*, Theory of Computing, 9 (2013), pp. 593–615, doi:10.4086/toc.2013.v009a018. Preliminary version in *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing* (STOC), 2012.

[34] 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.

[35] 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.

[36] J. Thaler, *Lower bounds for the approximate degree of block-composed functions*, in Electronic Colloquium on Computational Complexity (ECCC), 2014. Report TR14-150, Revision 3.

[37] A. C.-C. Yao, *On* ACC *and threshold circuits*, in *Proceedings of the Thirty-First Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 1990, pp. 619–627, doi:10.1109/FSCS.1990.89583.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de