THEORY OF COMPUTING, Volume 14 (22), 2018, pp. 1–17
www.theoryofcomputing.org

On Multiparty Communication with Large versus Unbounded Error

Alexander A. Sherstov*

Received September 3, 2016; Revised March 24, 2017; Published December 28, 2018

Abstract: The *unbounded-error* communication complexity of a Boolean function F is the limit of the ε-error randomized complexity of F as $\varepsilon \to 1/2$. Communication complexity with *weakly unbounded error* is defined similarly but with an additive penalty term that depends on $1/2 - \varepsilon$. Explicit functions are known whose two-party communication complexity with unbounded error is logarithmic compared to their complexity with weakly unbounded error. Chattopadhyay and Mande (ECCC Report TR16-095, Theory of Computing 2018) recently generalized this exponential separation to the number-on-the-forehead multiparty model. We show how to derive such an exponential separation from known two-party work, achieving a quantitative improvement along the way. We present several proofs here, some as short as half a page.

In more detail, we construct a k-party communication problem $F\colon (\{0,1\}^n)^k \to \{0,1\}$ that has complexity $O(\log n)$ with unbounded error and $\Omega(\sqrt{n}/4^k)$ with weakly unbounded error, reproducing the bounds of Chattopadhyay and Mande. In addition, we prove a quadratically stronger separation of $O(\log n)$ versus $\Omega(n/4^k)$ using a nonconstructive argument.

ACM Classification: F.1.3, F.2.3

AMS Classification: 68Q17, 68Q15

Key words and phrases: lower bounds, separation of complexity classes, multiparty communication complexity, unbounded-error communication complexity, PP, UPP

A preliminary version of this paper appeared in ECCC TR16-138.

*The author was supported in part by NSF CAREER award CCF-1149018 and an Alfred P. Sloan Foundation Research Fellowship.

 DOI: 10.4086/toc.2018.v014a022

1 Introduction

The *number-on-the-forehead* model, due to Chandra et al. [9], 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 i-th 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 i-th 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 a worst-case execution. The *ε-error randomized communication complexity* $R_\varepsilon(F)$ 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, 32, 17, 23, 5].

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 standard ways to define the complexity of F in this setting, both inspired by probabilistic polynomial time for Turing machines:

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

and

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

The former quantity, introduced by Paturi and Simon [21], is called the communication complexity of F with *unbounded error*, in reference to the fact that the error probability can be arbitrarily close to $1/2$. The latter quantity, proposed by Babai et al. [1], includes an additional penalty term that depends on the error probability. We refer to $\mathrm{PP}(F)$ as the communication complexity of F with *weakly unbounded error*. 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 [21] and [1] studied 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. [8] and the author [24] 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 communication complexity with unbounded error versus weakly unbounded error: $\mathrm{UPP}(F) = O(\log n)$ in both works, versus $\mathrm{PP}(F) = \Omega(n^{1/3})$ in [8] and $\mathrm{PP}(F) = \Omega(\sqrt{n})$ in [24]. In complexity-theoretic notation, these results show that $\mathsf{PP}_2 \subsetneq \mathsf{UPP}_2$.

The analyses by Buhrman et al. [8] and the author [24] were quite specialized. The former was based on a subtle lemma from Razborov's quantum lower bound [22] for set disjointness, whereas the latter was built around an earlier result of Goldmann et al. [16] on the discrepancy of a low-degree polynomial threshold function. In subsequent work, the author developed a general technique called the *pattern matrix method* [25, 26], 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 [26] to give a simple alternate proof of the separation due to Buhrman et al. [8]. Following up, Thaler [31] used the pattern matrix method to exhibit a communication problem $F\colon \{0,1\}^n \times \{0,1\}^n \to \{-1,+1\}$ computable in AC^0 with communication complexity $\mathrm{UPP}(F) = O(\log n)$ and $\mathrm{PP}(F) = \Omega(n/\log n)^{2/5}$. Thaler's result improves on the previous separation by an AC^0 function, due to Buhrman et al. [8].

The surveyed work on communication complexity with unbounded and weakly unbounded error considered the two-party model. The past few years saw a resurgence of interest in *multiparty* communication complexity classes, with numerous separations established over the past decade [19, 11, 14, 3, 15]. Recently, Chattopadhyay and Mande [12] revisited the unbounded versus weakly unbounded question in the multiparty setting. They generalized the original two-party separation [24] 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

The purpose of our paper is to show how to derive the proper containment $\mathsf{PP}_k \subsetneq \mathsf{UPP}_k$ in an almost trivial manner from previous two-party work. The key is to use the pattern matrix-based approach to the problem [26, 31], as opposed to the earlier two-party work [16, 24] which forms the basis for Chattopadhyay and Mande's result.

In more detail, we present three short proofs separating multiparty communication complexity with unbounded versus weakly unbounded error, 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, by constructing an explicit function with an exponential gap between the complexity with unbounded error versus weakly unbounded error. 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 [26, 31]. 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 is a k-party communication problem* $H\colon (\{0,1\}^n)^k \to \{-1,+1\}$ *with*

$$\mathrm{UPP}(H) = O(\log n) \qquad \textit{and} \qquad \mathrm{PP}(H) = \Omega\left(\frac{n}{4^k}\right).$$

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

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. This yields our third result, which is our main constructive separation.

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

$$\mathrm{UPP}(F) = O(\log n) \qquad \textit{and} \qquad \mathrm{PP}(F) = \Omega\left(\frac{\sqrt{n}}{4^k}\right).$$

Ignoring cosmetic differences, the function in this corollary is the same as the functions used in our original two-party separation [24] and in the proof of Chattopadhyay and Mande [12]. Quantitatively, Corollary 1.2 reproduces the bounds proved by Chattopadhyay and Mande, whereas Theorem 1.1 gives a quadratically stronger nonconstructive result.

1.3 Paper organization

The remainder of this paper is organized as follows. Section 2 gives a leisurely review of the technical preliminaries, which the expert reader may wish to skim or skip altogether. We then prove our three separations 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 $\deg_\varepsilon(f)$, is the least degree of a real polynomial p such that $\|f - p\|_\infty \leqslant \varepsilon$. Any polynomial p with this property is said to be a *uniform approximant*, or *pointwise approximant*, to f with error ε. Observe that

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

A common choice of error parameter is $\varepsilon = 1/3$, an aesthetically motivated constant that is replaceable by any other in $(0, 1)$ without the theory changing in any significant way. Specifically, the following result of Buhrman et al. [7, 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 any function $f \colon X \to \{-1, +1\}$ on any finite subset $X \subset \mathbb{R}^n$,*

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

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

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

In words, $B_d(t)$ is the probability of observing 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

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

B_d sends

$$\left[0, \frac{\varepsilon}{1+\varepsilon}\right] \to \left[0, \frac{\delta}{2}\right] \qquad \text{and similarly} \qquad \left[1 - \frac{\varepsilon}{1+\varepsilon}, 1\right] \to \left[1 - \frac{\delta}{2}, 1\right].$$

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

$$2B_d\left(\frac{1}{2+2\varepsilon} p(x) + \frac{1}{2}\right) - 1. \qquad \square$$

2.2 Approximation of specific functions

Among the first findings in this line of work was Paturi's tight lower bound [20] 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 [6] 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 [31, Section 1.2.2].

2.3 Multiparty communication

An excellent reference on communication complexity is the monograph by Kushilevitz and Nisan [18]. 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. [9]. The model features k communicating players, tasked with computing a (possibly partial) Boolean function F on the Cartesian product $X_1 \times X_2 \times \cdots \times X_k$ of some finite sets $X_1, X_2, \ldots, X_k$. A given input $(x_1, x_2, \ldots, x_k) \in X_1 \times X_2 \times \cdots \times X_k$ is distributed among the players by placing x_i, figuratively speaking, on the forehead of the i-th player (for $i = 1, 2, \ldots, k$). In other words, the i-th player knows the arguments $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k$ but not x_i. The players communicate by sending broadcast messages, taking turns according to a protocol agreed upon in advance. Each of them privately holds an unlimited supply of uniformly random bits, which he can use along with his available arguments when deciding what message to send at any given point in the protocol. The protocol's purpose is to allow accurate computation of F everywhere on the domain of F. An *ε-error protocol* for F is one which, on every input $(x_1, x_2, \ldots, x_k) \in \operatorname{dom} F$, produces the correct answer $F(x_1, x_2, \ldots, x_k)$ with probability at least $1 - \varepsilon$. 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 $R_\varepsilon(F)$, is the least cost of an ε-error randomized protocol for F.

2.4 Communication with unbounded and weakly 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 *communication complexity of F with unbounded error*, introduced by Paturi and Simon [21], is the quantity

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

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:

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

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

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

The following result, proved in the setting of $k = 2$ parties by Paturi and Simon [21, Theorem 2], gives a large class of communication problems that are efficiently computable with unbounded error.

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

Fact 2.4 (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 proof of this result.

Proof of Fact 2.4. For a subset $S \subseteq \{1,2,\dots,n\} \times \{1,2,\dots,k\}$, let x_S denote the product of the variables indexed by S. By hypothesis,

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

for some subsets $S_1, S_2, \dots, S_\ell$ and some reals $a_{S_1}, a_{S_2}, \dots, a_{S_\ell}$. 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 $|a_{S_i}|/(|a_{S_1}| + |a_{S_2}| + \dots + |a_{S_\ell}|)$, and broadcasts i. He then collaborates with the second player to 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

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

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 is done using Fact 2.4; the latter relies on technical machinery which we now review. A k-dimensional *cylinder intersection* is a function $\chi\colon X_1 \times X_2 \times \dots \times X_k \to \{0,1\}$ of the form

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

where $\chi_i\colon X_1 \times \dots \times X_{i-1} \times X_{i+1} \times \dots \times X_k \to \{0,1\}$. In other words, a k-dimensional cylinder intersection is the product of k functions with range $\{0,1\}$, where the i-th function does not depend on the i-th coordinate but may depend arbitrarily on the other $k-1$ coordinates. Introduced by Babai et al. [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 $X_1 \times X_2 \times \dots \times X_k$ and a probability distribution P on $X_1 \times X_2 \times \dots \times X_k$, 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* [13, 2, 18].

Theorem 2.5 (Discrepancy method)**.** *Let F be a (possibly partial) Boolean function on $X_1 \times X_2 \times \cdots \times X_k$. Then*

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

A proof of Theorem 2.5 in the stated generality is available in [29, Theorem 2.9]. Combining this theorem with the definition of $\mathrm{PP}(F)$ gives the following corollary.

Corollary 2.6. *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 2.5 and Corollary 2.6 highlight the role of discrepancy in proving lower bounds on randomized communication complexity. Apart from a few canonical examples [18], 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 [25, 26] for two-party communication complexity and has since been generalized by several authors to the multiparty setting, e. g., [19, 11, 14, 4, 10, 29, 28]. We now review the strongest form [29, 28] of the pattern matrix method, focusing our discussion on discrepancy bounds.

Set disjointness is the k-party communication problem of determining whether k given subsets of the universe $\{1,2,\ldots,n\}$ have empty intersection, where, as usual, the i-th party knows all the sets except for the i-th. Identifying the sets with their characteristic vectors, set disjointness corresponds to the Boolean function $\mathrm{DISJ}_{n,k}\colon (\{0,1\}^n)^k \to \{-1,+1\}$ 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 [29, Theorem 5.7].

Theorem 2.7 (Sherstov)**.** *For every Boolean function $f\colon \{0,1\}^n \to \{-1,+1\}$, all positive integers m and k, and all reals $0 < \gamma < 1$,*

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

This theorem makes it possible to prove communication lower bounds by leveraging the existing literature on polynomial approximation. In follow-up work, the author improved Theorem 2.7 to an essentially tight upper bound [28, Theorem 5.7]. However, we will not need this sharper version.

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 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 [26, 31]. 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

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

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.

3.1 A qualitative separation

The literature on the polynomial approximation of Boolean functions spans a broad spectrum of technical sophistication. Here, we combine the pattern matrix method with a particularly well-known and basic result on polynomial approximation. Our proof is virtually identical to the previous proofs in the two-party setting, e. g., [26, Section 10] and [31, 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 positive integers n and k, there is an (explicitly given) k-party communication problem $F_{n,k}\colon (\{0,1\}^n)^k \to \{-1,+1\}$ such that*

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

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

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 $m = \lceil 2^{k+1} \mathrm{e} \cdot n^{2/3} \rceil^2$ 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 2.6 and the third step follows from (3.5) by the pattern matrix method (Theorem 2.7). 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 2.4. □

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

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

3.2 The nonconstructive separation

We now turn to a nonconstructive separation of PP_k and UPP_k, which quantitatively is our strongest. The main new ingredient here is an approximation-theoretic result [27, Theorem 5.1] for halfspaces. Informally, it states that approximating a certain 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 3.3 (Sherstov)**.** *Let $0 < \alpha < 1$ be any sufficiently small absolute constant. Then there exist integers $w_1, w_2, \ldots, w_n \in \{0,1,2,\ldots,2^n-1\}$ such that the Boolean function $f_n \colon \{0,1\}^n \times \{0,1,2,\ldots,n\} \to \{-1,+1\}$ given by*

$$f_n(x,t) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{i=1}^{n} w_i x_i - 2^{\lfloor \alpha n \rfloor + 1} t\right) \tag{3.6}$$

obeys

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

This result was proved in [27] 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 [27, Theorem 5.1].

Corollary 3.4. *There exist integers $w_1, w_2, \ldots, w_{n+1} \in \{0,1,2,\ldots,2^n-1\}$ such that the Boolean function $h_n \colon \{0,1\}^{2n} \to \{-1,+1\}$ given by*

$$h_n(x) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{i=1}^{n} w_i x_i - w_{n+1} \sum_{i=n+1}^{2n} x_i\right) \tag{3.7}$$

obeys

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

where $c > 0$ is an absolute constant.

Proof. Let $0 < \alpha < 1$ be a sufficiently small absolute constant from Theorem 3.3, 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

$$E(S, \lfloor \alpha n \rfloor) \geqslant 1 - \Omega\left(\frac{\lfloor \alpha n \rfloor}{2^{\lfloor \alpha n \rfloor}}\right)^{1/2}. \tag{3.8}$$

Now fix $w_1, w_2, \ldots, w_n$ whose existence is guaranteed by Theorem 3.3, and set $w_{n+1} = 2^{\lfloor \alpha n \rfloor + 1}$. Let f_n and h_n be given by (3.6) and (3.7). 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 symmetrization argument (see, e. g., [27, Proposition 2.6]) and the second step is immediate from Theorem 3.3. This completes the proof in view of (3.8). □

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

Theorem 3.5 (restatement of Theorem 1.1)**.** *There is a k-party communication problem*

$$H_{n,k} \colon (\{0,1\}^n)^k \to \{-1,+1\}$$

with

$$\mathrm{UPP}(H_{n,k}) = O(\log n) \qquad \textit{and} \tag{3.9}$$

$$\mathrm{PP}(H_{n,k}) = \Omega\left(\frac{n}{4^k}\right). \tag{3.10}$$

Moreover,

$$H_{n,k}(x) = \operatorname{sgn}\left(\frac{1}{2} + \sum_{i=1}^{n} w_i x_{1,i} x_{2,i} \cdots x_{k,i}\right) \tag{3.11}$$

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 3.4. Then

$$\deg_{1-\exp(-cn)}(h_n) \geqslant cn \tag{3.12}$$

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,

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

where the second step uses Corollary 2.6 and the third step follows from (3.12) by the pattern matrix method (Theorem 2.7). 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 (3.10) and (3.11). The remaining property (3.9) follows from (3.11) by Fact 2.4. □

3.3 The constructive separation

Despite being nonconstructive, Theorem 3.5 implies the following constructive result, which is our strongest constructive separation of PP_k and UPP_k.

Corollary 3.6 (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*

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

Then

$$\mathrm{UPP}(F_{n,k}) = O(\log n) \qquad \textit{and} \tag{3.13}$$

$$\mathrm{PP}(F_{n,k}) = \Omega\left(\frac{\sqrt{n}}{4^k}\right). \tag{3.14}$$

Proof. In the notation of Theorem 3.5, every $H_{\sqrt{n},k}$ is a restriction of $F_{n,k}$. Indeed, every $H_{\sqrt{n},k}$ can be obtained from $F_{n,k}$ by appropriately fixing $x_{1,i,0}, x_{1,i,1}, \dots, x_{1,i,\sqrt{n}-1} \in \{0, x_{1,i}\}$ and $x_{1,i,\sqrt{n}} \in \{0,1\}$. As a result, (3.14) follows from (3.10), whereas (3.13) is immediate by Fact 2.4. □

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] LÁSZLÓ BABAI, PETER FRANKL, AND JANOS SIMON: Complexity classes in communication complexity theory. In *Proc. 27th FOCS*, pp. 337–347. IEEE Comp. Soc. Press, 1986. [doi:10.1109/SFCS.1986.15] 2, 7

[2] LÁSZLÓ BABAI, NOAM NISAN, AND MARIO SZEGEDY: Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *J. Comput. System Sci.*, 45(2):204–232, 1992. Preliminary version in STOC'89. [doi:10.1016/0022-0000(92)90047-M] 2, 8, 9

[3] PAUL BEAME, MATEI DAVID, TONIANN PITASSI, AND PHILIPP WOELFEL: Separating deterministic from randomized multiparty communication complexity. *Theory of Computing*, 6(1):201–225, 2010. Preliminary version in ICALP'07. [doi:10.4086/toc.2010.v006a009] 3

[4] PAUL BEAME AND DANG-TRINH HUYNH-NGOC: Multiparty communication complexity and threshold circuit size of AC^0. *SIAM J. Comput.*, 41(3):484–518, 2012. Preliminary version in FOCS'09. [doi:10.1137/100792779] 9

[5] PAUL BEAME, TONIANN PITASSI, AND NATHAN SEGERLIND: Lower bounds for Lovász-Schrijver systems and beyond follow from multiparty communication complexity. *SIAM J. Comput.*, 37(3):845–869, 2007. Preliminary version in ICALP'05. [doi:10.1137/060654645] 2

[6] RICHARD BEIGEL: Perceptrons, PP, and the polynomial hierarchy. *Comput. Complexity*, 4(4):339–349, 1994. Preliminary version in SCT'92. [doi:10.1007/BF01263422] 6

[7] HARRY BUHRMAN, ILAN NEWMAN, HEIN RÖHRIG, AND RONALD DE WOLF: Robust polynomials and quantum algorithms. *Theory Comput. Syst.*, 40(4):379–395, 2007. Preliminary version in STACS'05. [doi:10.1007/s00224-006-1313-z, arXiv:quant-ph/0309220] 5

[8] HARRY BUHRMAN, NIKOLAI K. VERESHCHAGIN, AND RONALD DE WOLF: On computation and communication with small bias. In *Proc. 22nd IEEE Conf. on Computational Complexity (CCC'07)*, pp. 24–32. IEEE Comp. Soc. Press, 2007. [doi:10.1109/CCC.2007.18] 3

[9] ASHOK K. CHANDRA, MERRICK L. FURST, AND RICHARD J. LIPTON: Multi-party protocols. In *Proc. 15th STOC*, pp. 94–99. ACM Press, 1983. [doi:10.1145/800061.808737] 2, 7

[10] ARKADEV CHATTOPADHYAY: *Circuits, Communication, and Polynomials*. Ph. D. thesis, McGill University, 2008. eScholarship@McGill. 9

[11] ARKADEV CHATTOPADHYAY AND ANIL ADA: Multiparty communication complexity of disjointness. *Electron. Colloq. on Comput. Complexity (ECCC)*, January 2008. [ECCC:TR08-002] 3, 9

[12] ARKADEV CHATTOPADHYAY AND NIKHIL MANDE: Separation of unbounded-error models in multi-party communication complexity. *Theory of Computing*, 14(21), 2018. Preliminary version ECCC TR16-095. [doi:10.4086/toc.2018.v014a021] 3, 4

[13] BENNY CHOR AND ODED GOLDREICH: Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM J. Comput.*, 17(2):230–261, 1988. Preliminary version in FOCS'85. [doi:10.1137/0217015] 9

[14] MATEI DAVID, TONIANN PITASSI, AND EMANUELE VIOLA: Improved separations between nondeterministic and randomized multiparty communication. *ACM Trans. Comput. Theory*, 1(2/5), 2009. Preliminary version in RANDOM'08. [doi:10.1145/1595391.1595392] 3, 9

[15] DMITRY GAVINSKY AND ALEXANDER A. SHERSTOV: A separation of NP and coNP in multiparty communication complexity. *Theory of Computing*, 6(10):227–245, 2010. [doi:10.4086/toc.2010.v006a010, arXiv:1004.0817] 3

[16] MIKAEL GOLDMANN, JOHAN HÅSTAD, AND ALEXANDER A. RAZBOROV: Majority gates vs. general weighted threshold gates. *Comput. Complexity*, 2(4):277–300, 1992. Preliminary version in SCT'92. [doi:10.1007/BF01200426] 3

[17] JOHAN HÅSTAD AND MIKAEL GOLDMANN: On the power of small-depth threshold circuits. *Comput. Complexity*, 1(2):113–129, 1991. Preliminary version in FOCS'90. [doi:10.1007/BF01272517] 2

[18] EYAL KUSHILEVITZ AND NOAM NISAN: *Communication Complexity*. Cambridge University Press, 1997. 7, 9

[19] TROY LEE AND ADI SHRAIBMAN: Disjointness is hard in the multiparty number-on-the-forehead model. *Comput. Complexity*, 18(2):309–336, 2009. Preliminary version in CCC'08. [doi:10.1007/s00037-009-0276-2] 3, 9

[20] RAMAMOHAN PATURI: On the degree of polynomials that approximate symmetric Boolean functions. In *Proc. 24th STOC*, pp. 468–474. ACM Press, 1992. [doi:10.1145/129712.129758] 6

[21] RAMAMOHAN PATURI AND JANOS SIMON: Probabilistic communication complexity. *J. Comput. System Sci.*, 33(1):106–123, 1986. Preliminary version in FOCS'84. [doi:10.1016/0022-0000(86)90046-2] 2, 7

[22] ALEXANDER A. RAZBOROV: Quantum communication complexity of symmetric predicates. *Izv. Math.*, 67(1):145–159, 2003. [doi:10.1070/IM2003v067n01ABEH000422, arXiv:quant-ph/0204025] 3

[23] ALEXANDER A. RAZBOROV AND AVI WIGDERSON: $n^{\Omega(\log n)}$ lower bounds on the size of depth-3 threshold circuits with AND gates at the bottom. *Inform. Process. Lett.*, 45(6):303–307, 1993. Version available at CiteSeer. [doi:10.1016/0020-0190(93)90041-7] 2

[24] ALEXANDER A. SHERSTOV: Halfspace matrices. *Comput. Complexity*, 17(2):149–178, 2008. Preliminary version in CCC'07. [doi:10.1007/s00037-008-0242-4] 3, 4

[25] ALEXANDER A. SHERSTOV: Separating AC^0 from depth-2 majority circuits. *SIAM J. Comput.*, 38(6):2113–2129, 2009. Preliminary version in STOC'07. [doi:10.1137/08071421X] 3, 9

[26] ALEXANDER A. SHERSTOV: The pattern matrix method. *SIAM J. Comput.*, 40(6):1969–2000, 2011. Preliminary version in STOC'08. [doi:10.1137/080733644] 3, 9, 10

[27] ALEXANDER A. SHERSTOV: Optimal bounds for sign-representing the intersection of two halfspaces by polynomials. *Combinatorica*, 33(1):73–96, 2013. Preliminary version in STOC'10. [doi:10.1007/s00493-013-2759-7] 12, 13

[28] ALEXANDER A. SHERSTOV: Communication lower bounds using directional derivatives. *J. ACM*, 61(6):1–71, 2014. Preliminary version in STOC'13. [doi:10.1145/2629334] 9, 10

[29] ALEXANDER A. SHERSTOV: The multiparty communication complexity of set disjointness. *SIAM J. Comput.*, 45(4):1450–1489, 2016. Preliminary version in STOC'12. [doi:10.1137/120891587] 9

[30] ALEXANDER A. SHERSTOV: On multiparty communication with large versus unbounded error. *Electron. Colloq. on Comput. Complexity (ECCC)*, 23:138, 2016. [ECCC:TR16-138]

[31] JUSTIN THALER: Lower bounds for the approximate degree of block-composed functions. In *Proc. 43rd Internat. Colloq. on Automata, Languages and Programming (ICALP'16)*, pp. 17:1–17:15. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016. [doi:10.4230/LIPIcs.ICALP.2016.17, ECCC:TR14-150] 3, 6, 10

[32] ANDREW CHI-CHIH YAO: On ACC and threshold circuits. In *Proc. 31st FOCS*, pp. 619–627. IEEE Comp. Soc. Press, 1990. [doi:10.1109/FSCS.1990.89583] 2

AUTHOR

Alexander A. Sherstov
Associate professor
University of California, Los Angeles
sherstov@cs.ucla.edu
http://www.cs.ucla.edu/~sherstov

ABOUT THE AUTHOR

ALEXANDER A. SHERSTOV, known to his friends and colleagues as Sasha, is an associate professor of computer science at the University of California, Los Angeles. Prior to joining UCLA, Sasha obtained his Ph. D. at the University of Texas at Austin under the direction of Adam Klivans and spent two years as a postdoctoral scholar at Microsoft Research. He has broad research interests in theoretical computer science, including computational complexity theory, computational learning theory, and quantum computing.