# Separating Deterministic from Randomized Multiparty Communication Complexity

Paul Beame*
University of Washington
beame@cs.washington.edu

Matei David†
University of Toronto
matei@cs.toronto.edu

Toniann Pitassi†
University of Toronto
toni@cs.toronto.edu

Philipp Woelfel‡
University of Calgary
pwoelfel@cpsc.ucalgary.ca

September 4, 2008

*Supported by NSF grant CCR-0514870
†Supported by NSERC
‡Supported by DFG grant WO 1232/1-1

**Abstract**

We solve some fundamental problems in the number-on-forehead (NOF) $k$-player communication model. We show that there exists a function which has at most logarithmic communication complexity for randomized protocols with a one-sided error probability of 1/3 but which has linear communication complexity for deterministic protocols. The result is true for $k = n^{O(1)}$ players, where $n$ is the number of bits on each players' forehead. This separates the analogues of RP and P in the NOF communication model. We also show that there exists a function which has constant randomized complexity for public coin protocols but at least logarithmic complexity for private coin protocols. No larger gap between private and public coin protocols is possible. Our lower bounds are existential and we do not know of any explicit function which allows such separations. However, for the 3-player case we exhibit an explicit function which has $\Omega(\log \log n)$ randomized complexity for private coins but only constant complexity for public coins.

It follows from our existential result that any function that is complete for the class of functions with polylogarithmic nondeterministic $k$-player communication complexity does not have polylogarithmic deterministic complexity. We show that the set intersection function, which is complete in the number-in-hand model, is not complete in the NOF model under cylindrical reductions.

# 1 Introduction

The question of how much communication is necessary in order to compute a function $f : X_1 \times \cdots \times X_k \to O$ when its input is distributed between $k$ computationally unbounded players was first introduced in [Yao79] and it has since been shown to have many diverse applications in complexity theory. The case of $k = 2$ players has been studied extensively [KN97]. For two or more players, we are interested in the "number-on-forehead" model (NOF), first introduced by Chandra, Furst and Lipton in [CFL83]. In this model, the input is partitioned into $k$ parts, so that player $i$ can see all parts except for the $i^{\text{th}}$ part (since it is 'written on his forehead').

The number-on-forehead communication model is a fascinating and complex model that is not well understood when $k \geq 3$. The complexity of the situation arises from the fact that every part of the input is seen by multiple players. As the number of players increases, the sharing becomes increasingly generous. During the execution of a protocol, the set of inputs consistent with a particular message sequence is described by a so-called cylinder intersection. Cylinder intersections appear difficult to understand combinatorially.

Lower bounds for multiparty complexity in the number-on-forehead model are connected to a major open problem in complexity theory: it has been established that superlogarithmic communication complexity lower bounds in the NOF model for any explicit function with polylogarithmically many players would imply explicit lower bounds for $\mathsf{ACC}^0$ [BT91, HG91]. The best lower bound obtained so far is $\Omega(n/2^k)$, which breaks down when the number of players is greater than logarithmic [BNS92, CT93, Raz00, FG06]. Lower bounds in this model have many other important applications as well, including: constructions of pseudorandom generators for space bounded computation, constructions of universal traversal sequences, time-space tradeoffs [BNS92], circuit complexity bounds [HG91, NW93, Nis93], and proof complexity bounds [BPS05].

The motivation for our work is to pursue a broader understanding of the NOF complexity model. In particular, we would like to answer some of the basic questions that are still open for this model, but have well-known solutions in the 2-player model. For $k \geq 3$, we consider the three usual versions of communication complexity: deterministic, randomized and nondeterministic complexity. Are there functions separating these three different complexity measures? Surprisingly, the relationships between these complexity measures have not been resolved previously, even for $k = 3$.

Our main result is that for any $k$ that is $n^{O(1)}$ there is a function with $n$ bits on each players' forehead that is computable with a logarithmic communication by a randomized $k$-player communication protocol with 1-sided error but which requires linear complexity for deterministic protocols. We obtain this result nonconstructively by showing that deterministic protocols for a certain class of *simple* functions have a nice normal form and then establishing a lower bound for such function via a counting argument over protocols in normal form. We thus separate the randomized 1-sided error and deterministic $k$-player NOF communication complexity classes $\mathsf{RP}^{cc}_k$ and $\mathsf{P}^{cc}_k$. As a corollary of our lower bounds, we also establish an optimal separation between the public and private coin randomized NOF models.

These bounds are nonconstructive but, for $k$ at most logarithmic in the input size, we can also give *explicit* families of simple functions with $\Omega(\log n)$ deterministic $k$-player complexity in the NOF model. (We believe that they have superpolylogarithmic deterministic complexity.) The best previous lower bound for any explicitly defined simple function is the $\Omega(\log \log n)$ lower bound from [BGG06] for the Exact-T function (originally investigated in [CFL83]) in the special case of $k = 3$ players. As a corollary of our bound we obtain that our function families have $\Omega(\log \log n)$ complexity for randomized private coin protocols (with constant error probability) but only $O(1)$ complexity for public coin protocols.

The problem of separating deterministic from nondeterministic NOF complexity is particularly inter-

esting because of its connection to proof complexity. In recent work [BPS05], it has been shown that for $k = 3$, $(\log n)^{\omega(1)}$ lower bounds on the randomized NOF complexity of set intersection, which has nondeterministic NOF complexity $O(\log n)$, implies lower bounds for polynomial threshold proof systems, such as the Lovász-Schrijver proof systems, as well as the Chvátal cutting planes proof system. Recent work of Chattopadhyay and Ada , Lee and Shraibman, and Beame and Huynh-Ngoc [**?**, **?**, **?**] give lower bounds on the randomized complexity of the set disjointness function for up to $(\log n)^{1/3}$ players, thus separating the NOF communication complexity analogs of RP and NP. David, Pitassi and Viola [**?**] improve this separation by exhibiting a (different) function that is in NP but not in RP for up to $k = \epsilon \log n$ players for any $\epsilon < 1$. See the excellent survey article by Sherstov [**?**] for more details on this line of work.

This brings us to our second question: is there a 'complete' problem for the class of problems with efficient NOF nondeterministic algorithms under a suitable notion of reduction? Given our separation result, such a function would automatically be hard for deterministic protocols. Following [BFS86], it is not hard to see that set intersection is complete under communication-free reductions for the number-in-hand (NIH) model and in [BPS05] it had been assumed that the same holds for the number-on-forehead (NOF) model. (The number-in-hand model is an alternative generalization of the 2-player model in which each player gets his part of the input in his hand, and thus each player sees only his own part.) However, we prove that under communication-free reductions, set intersection is not complete in the NOF model.

## 2 Definitions and Preliminaries

In the NOF multiparty communication complexity model of computation [CFL83] there are $k$ players, numbered 1 to $k$, that are trying to collaborate to compute a function $f_{k,n} : X_1 \times \ldots \times X_k \to \{0,1\}$ where each $X_i = \{0,1\}^n$. In general, we allow $k$ to be a function of $n$. The $kn$ input bits are partitioned into $k$ sets, each of size $n$. For $(x_1, \ldots, x_k) \in \{0,1\}^{kn}$, and for each $i$, player $i$ knows the values of all of the inputs except for $x_i$ (which conceptually is thought of as being placed on player $i$'s forehead).

The players exchange bits according to an agreed-upon protocol, by writing them on a public blackboard. A *protocol* specifies, for every possible blackboard contents, whether or not the communication is over, the output if over and the next player to speak if not. A protocol also specifies what each player writes as a function of the blackboard contents and of the inputs seen by that player. The *cost* of a protocol is the maximum number of bits written on the blackboard.

In a *deterministic protocol*, the blackboard is initially empty. A *public-coin randomized protocol* of cost $c$ is simply a probability distribution over deterministic protocols of cost $c$, which can be viewed as a protocol in which the players have access to a shared random string. A *private-coin randomized protocol* is a protocol in which each player has access to a private random string. A *nondeterministic protocol* is a randomized private coin protocol with 1-sided error (only false negatives) and an error probability less than 1.

The *deterministic communication complexity of* $f_{k,n}$, written $D_k(f_{k,n})$, is the minimum cost of a deterministic protocol for $f_{k,n}$ that always outputs the correct answer. For $0 \leq \epsilon < 1/2$, let $R^{\text{pub}}_{k,\epsilon}(f_{k,n})$ denote the minimum cost of a public-coin randomized protocol for $f_{k,n}$ which, for every input, makes an error with probability at most $\epsilon$ (over the choice of the deterministic protocols). The *public-coin randomized communication complexity of* $f_{k,n}$ is $R^{\text{pub}}_k(f_{k,n}) = R^{\text{pub}}_{k,1/3}(f_{k,n})$. Let $R_{k,\epsilon}(f_{k,n})$ denote the minimum cost of a private-coin randomized protocol for $f_{k,n}$ which, for every input, makes an error with probability at most $\epsilon$ (over the choice of the private random strings). The *private-coin randomized communication complexity of* $f_{k,n}$ is $R_k(f_{k,n}) = R_{k,1/3}(f_{k,n})$. For both public-coin and private-coin complexities we add a superscript 1 if we require that the protocol makes error only on 1-inputs (i.e., false-negatives), and superscript 0 if we

require that the protocol makes error only on 0-inputs (i.e., false-positives). For example, $R^{0,\text{pub}}_{k,\epsilon}(f_{k,n})$ is the minimum cost of a $k$-player public-coin protocol for $f_{k,n}$ which is always correct on 1-inputs and makes error at most $\epsilon$ on 0-inputs. The *nondeterministic communication complexity of* $f_{k,n}$, written $N_k(f_{k,n})$, is the minimum cost of a nondeterministic protocol for $f_{k,n}$.

For a function $k = k(n)$, for a function family $f = (f_{k(n),n})_{n\in\mathbb{N}}$, and for any complexity measure $C$ defined above, we write $C_k(f)$ for the function $(C_k(f))(n) = C_{k(n)}(f_{k(n),n})$.

Since the general model laid out above is very powerful, we are also interested in communication restrictions. A player is *oblivious* in a certain protocol if the message he writes on the board is a function of the inputs he sees, but not a function of the messages sent by other players. Since we are interested in the best protocol, we may safely assume that all oblivious players write first, and then non-oblivious players continue to communicate using the information written by the former. A protocol in which all players are oblivious is called *simultaneous*. The simultaneous multiparty model was studied in [BGKL04], who proved new lower bounds, as well as surprising upper bounds in this model.

Since any function $f_{k,n}$ can be computed using only $n$ bits of communication, following [BFS86], for sequences of functions $f = (f_{k,n})_{n\in\mathbb{N}}$, communication protocols are considered "efficient" or "polynomial" if only polylogarithmically many bits are exchanged. Accordingly, let $\mathsf{P}^{cc}_k$ denote the class of function families $f$ for which $D_k(f)$ is $(\log n)^{O(1)}$, let $\mathsf{NP}^{cc}_k$ denote the class of function families $f$ with nondeterministic complexity $(\log n)^{O(1)}$, and let $\mathsf{RP}^{cc}_k$ denote the class of function families $f$ for which $R^1_k(f_n)$ is $(\log n)^{O(1)}$. The classes $\mathsf{BPP}^{cc}_k$, $\mathsf{coRP}^{cc}_k$ and $\mathsf{coNP}^{cc}_k$ can be defined similarly to their computational complexity counterparts.

The following are some important function families.

DEFINITION 2.1. *The* equality *function family, written* $\mathrm{EQ} = (\mathrm{EQ}_{k,n})_{n\in\mathbb{N}}$*, is defined by* $\mathrm{EQ}(x_1,\ldots,x_k) = 1$ *if and only if* $x_1 = \cdots = x_k$*. The* inequality *function family is* $\mathrm{INEQ} = (\mathrm{INEQ}_{k,n})_{n\in\mathbb{N}}$*, with* $\mathrm{INEQ}_{k,n} = 1 - \mathrm{EQ}_{k,n}$.

*The* set intersection *function family, written* $\mathrm{INT} = (\mathrm{INT}_{k,n})_{n\in\mathbb{N}}$*, is defined by* $\mathrm{INT}_{k,n}(x_1,\ldots,x_k) = 1$ *if and only if there exists some* $i \in [n]$ *such that* $x_{1,i} = \cdots = x_{k,i} = 1$*. The* set disjointness *function family is* $\mathrm{DISJ} = (\mathrm{DISJ}_{k,n})_{n\in\mathbb{N}}$*, with* $\mathrm{DISJ}_{k,n} = 1 - \mathrm{INT}_{k,n}$.

Multiparty communication complexity lower bounds are proven by analyzing properties of functions on *cylinder intersections*.

DEFINITION 2.2. *An* $i$-cylinder $C_i$ *in* $X_1 \times \ldots \times X_k$ *is a set such that for all* $x_1 \in X_1, \ldots, x_k \in X_k, x'_i \in X_i$ *we have* $(x_1,\ldots,x_i,\ldots,x_k) \in C_i$ *if and only if* $(x_1,\ldots,x'_i,\ldots,x_k) \in C_i$*. A* cylinder intersection *is a set of the form* $\bigcap_{i=1}^k C_i$ *where each* $C_i$ *is an* $i$*-cylinder in* $X_1 \times \cdots \times X_k$.

# 3 Separating $\mathsf{P}^{cc}_k$ from $\mathsf{RP}^{cc}_k$

## 3.1 Oblivious Players, Simple Functions, and a Normal Form

We will be interested in a special type of Boolean functions for which we can show that, without loss of generality, one of the players is oblivious. For sets $X_1,\ldots,X_k$ a function $f : X_1 \times \cdots \times X_k \to \{0,1\}$ is *simple for player* $i$ if for all $(x_1,\ldots,x_{i-1},x_{i+1},\ldots x_k) \in X_1 \times \cdots \times X_{i-1} \times X_{i+1} \times \cdots \times X_k$ there exists at most one $x^*_i \in X_i$ such that $f(x_1,\ldots,x_{i-1},x^*_i,x_{i+1},\ldots,x_k) = 1$.

If $f$ is simple for player $i$ then it is reducible with no communication to 2-player $n$-bit equality EQ. Player $i$ can compute the unique value for the input on its forehead for which the output could be 1 (if it exists), and any other player sees that input. All the players have to do is to decide whether these strings

are equal. We know that $R^0_{2,1/n}(\mathrm{EQ})$ is $O(\log n)$ and $R^{0,\mathrm{pub}}_2(\mathrm{EQ})$ is $O(1)$ [KN97]. Therefore we get the following.

**Lemma 3.1.** *For all $k$ and all simple functions $f$ on $kn$ bits, $R^0_{k,1/n}(f)$ is $O(\log n)$ and $R^{0,pub}_k(f)$ is $O(1)$. In particular, $f \in \mathsf{coRP}^{cc}_k$.*

The following theorem shows that if a function is simple for one player then this player can act obliviously with only a small increase in the deterministic communication complexity.

**Theorem 3.2.** *Let $f : X_1 \times \cdots \times X_k \to \{0,1\}$ be a function that is simple for player $i$ and has $D_k(f) = d$. Then there is a protocol $P'$ for $f$ in which player $i$ first sends $d$ bits and then all players $j \in \{1,\ldots,k\} - \{i\}$ simultaneously send exactly one bit $b_j$ such that $f(x_1,\ldots,x_k) = 1$ if and only if all bits $b_j = 1$.*

*Proof.* Let $f$ be simple for player 1. Let $P$ be a protocol for $f$ with complexity $d$. We describe protocol $P'$ on input $(x_1,\ldots,x_k)$. Assume that player 1, call her Alice, sees the partial input $(x_2,\ldots,x_k)$ on the other players' foreheads. Let $x_1^*$ be the input in $X_1$ such that $f(x_1^*, x_2 \ldots, x_k) = 1$, if it exists. If such an input does not exist, then let $x_1^*$ be an arbitrary input in $X_1$. Alice "simulates" protocol $P$ for the input $(x_1^*, x_2, \ldots, x_k)$, i.e., she writes on the blackboard exactly the string $I^*$ that would have been written by players $1,\ldots,k$ if protocol $P$ were executed for the input. Then each player $r$, $2 \le r \le k$, verifies that $I^*$ is consistent with what that player would have sent in protocol $P$ if it had seen $(x_1,\ldots,x_{r-1},x_{r+1},\ldots,x_k)$ on the other players' foreheads. More precisely, the player (say Bob) reads the bits $I_1^*, I_2^*, \ldots,$ of $I^*$, until he has read a partial message $I_1^* \ldots I_j^*$ upon which, in protocol $P$, it would be Bob's turn to write the next bit. Then Bob checks whether the bit he would write does in fact coincide with $I_{j+1}^*$. This is repeated until Bob has read all bits from $I^*$. In addition the player checks whether the output of protocol $P$ is 1, if $I^*$ is the blackboard contents. If Bob does not find an error (and the output of $P$ is 1 for blackboard contents $I^*$), then he accepts, i.e. sends bit $b_r = 1$. Otherwise he rejects, i.e. sends $b_r = 0$.

Consider an input $(x_1,\ldots,x_k)$, and let $I^*$ be the message sent by Alice for that input. If there is no $x_1^*$ such that $f(x_1^*, x_2 \ldots, x_k) = 1$, then the blackboard contents $I^*$ would imply an output of 0 in protocol $P$. Hence, the other players all reject, which is correct because obviously $f(x_1,\ldots,x_k) = 0$ in this case. Now assume that there is a (unique) $x_1^*$ such that $f(x_1^*, x_2 \ldots, x_k) = 1$, and hence $I^*$ is the blackboard contents for protocol $P$ on the input $(x_1^*, x_2 \ldots, x_k)$. If $x_1 = x_1^*$, then clearly all players $2,\ldots,k$ accept. Hence, $P'$ correctly computes a 1. Next, assume that $x_1 \neq x_1^*$, and hence $f(x_1,\ldots,x_k) = 0$. Let $I$ be the blackboard contents in protocol $P$ on input $(x_1,\ldots,x_k)$. Since $f(x_1,\ldots,x_k) \neq f(x_1^*, x_2, \ldots, x_k)$, obviously $I \neq I^*$. Let $j$ be the index of the first bit in $I$ that is different from $I^*$. Note that, at any time before the $j$th bit is written to the blackboard, the information Alice obtains from the blackboard and the other players' foreheads is the same for the inputs $(x_1,\ldots,x_k)$ and $(x_1^*, x_2, \ldots, x_k)$. Therefore, Alice does not write the $j$-th bit in protocol $P$. Hence, there must be some other player $r > 1$ whose messages in $P$ on input $(x_1,\ldots,x_k)$ differ from $I^*$. This player sends $b_r = 0$ in the protocol $P'$, and thus protocol $P'$ is correct for this input. □

## 3.2 Representing Simple Functions by Colorings and Cylinder Intersections

Most lower bound proofs for $D_k(f)$ use the fact shown in [BNS92] that any $k$-player protocol with complexity $d$ for a function $f$ yields a partitioning of the input into $O(2^d)$ disjoint cylinder intersections on which $f$ is constant. For $k \ge 3$ players, the known techniques for proving lower bounds on the number of cylinder intersections needed for such a partitioning are discrepancy-based and inherently yield lower bounds even for randomized protocols. Therefore, these techniques are not suitable for proving good lower bounds for functions with low randomized communication complexity.

For simple functions we obtain different, although related, structures. These structures seem to be better suited for lower bound proofs for functions in $\mathsf{RP}_k^{cc}$, as they will allow us to separate this class from $\mathsf{P}_k^{cc}$ and to prove $\Omega(\log n)$ lower bounds for explicit functions.

Throughout this section, $f : X_1 \times \cdots \times X_k \to \{0,1\}$ is simple for player 1. For any natural number $D$ and a set $S$, a *$D$-coloring* of $S$ is a mapping $c : S \to [D]$. Since $f$ is simple for player 1 (Alice), there exists a function $g : X_2 \times \cdots \times X_k \to X_1 \cup \{\perp\}$, where $g(x_2, \ldots, x_k) = \perp$ if $f(x_1, \ldots, x_k) = 0$ for all $x_1 \in X_1$, and otherwise $g(x_2, \ldots, x_k) = x_1^*$, where $x_1^*$ is the the unique element in $X_1$ with $f(x_1^*, x_2, \ldots, x_k) = 1$. In fact, any such mapping $g$ uniquely defines the simple function $f$.

Assume that $f$ can be computed by a $d$-bit protocol $P$. The special protocol $P'$ for $f$, derived in Theorem 3.2, can be characterized by a coloring of $X_2 \times \cdots \times X_k$ and cylinder intersections in $X_2 \times \cdots \times X_k$, as follows. Let $c$ be the $2^d$-coloring of $X_2 \times \cdots \times X_k$, where $c(x_2, \ldots, x_k)$ is the message Alice sends in $P'$ if she sees $(x_2, \ldots, x_k)$. Consider a fixed message $m$ from Alice and a fixed value $a \in X_1$ on Alice's forehead. The subset of points in $X_2 \times \cdots \times X_k$ for which all other players accept if they see $a$ on Alice's forehead and receive message $m$ is a cylinder intersection $I_{m,a}$. Note, each such cylinder intersection $I_{m,a}$ may also contain points that are not colored $m$. However, it is not possible that a point $p = (x_2, \ldots, x_k) \in I_{m,a}$ has color $m$ but $g(p) \neq a$ because then Alice would send message $m$ if she saw $p$ and the other players would all accept if they saw $a$ on Alice's forehead. Hence, $(a, x_2, \ldots, x_k)$ would be accepted by $P'$, a contradiction. We obtain the following.

**Lemma 3.3.** *Every function $f$ that is simple for player 1 and has $k$-player communication complexity $d$ can be uniquely represented by cylinder intersections $I_{m,a} \in X_2 \times \cdots \times X_k$, for $m \in [2^d]$, $a \in X_1$, and a $2^d$-coloring $c$ of $X_2 \times \cdots \times X_k$, such that $\forall a \in X_1, y \in X_2 \times \cdots \times X_k$: $f(a,y) = 1 \Leftrightarrow y \in I_{c(y),a}$. In particular, $I_{m,a}$ contains all points $y \in X_2 \times \cdots \times X_k$ with color $c(y) = m$ and $f(a,y) = 1$, but no point $y'$ with color $c(y') = m$ and $f(a,y') = 0$.*

*Proof.* We have already seen how to obtain $c$ and the cylinder intersections $I_{m,a}$ from the function $f$. This representation is unique because for any input $(a,p)$ with $a \in X_1$ and $p \in X_2 \times \cdots \times X_k$ we can retrieve the function value $f(a,p)$ by checking whether $p \in I_{c(p),a}$. □

### 3.3 The Lower Bound

In the following we consider a family of functions which have logarithmic communication complexity for private-coin randomized protocols with one-sided error and error probability bounded by 1/3. Using Lemma 3.3 we give an upper bound on the number of different deterministic protocols for the functions in that class in order to show that at least one such function requires at least linear deterministic communication complexity.

For positive integers $n$, $m$ and $t$, let $G_{t,n,m}$ be the set of all mappings $g : \{0,1\}^{n \cdot t} \to \{0,1\}^m$. For any function $g \in G_{k-1,n,m}$, define $f_g : \{0,1\}^m \times \{0,1\}^{n \cdot (k-1)}$ by $f_g(x_1, \ldots, x_k) = 1$ if and only if $g(x_2, \ldots, x_k) = x_1$. By Lemma 3.1, for all $g \in G_{k,n,n/2}$, $f_g \in \mathsf{coRP}_k^{cc}$.

**Theorem 3.4.** *There exists $g \in G_{k-1,n,n/2}$ such that $D_k(f_g)$ is $\Omega(n - \log k)$. In particular, $f_g \notin \mathsf{P}_k^{cc}$.*

**Corollary 3.5.** *$\mathsf{P}_k^{cc} \neq \mathsf{RP}_k^{cc}$ for any $k$ that is $n^{O(1)}$.*

*Proof of Theorem 3.4.* Any function $g \in G_{k-1,n,m}$ has a domain of size $2^{(k-1)n}$ and a range of size $2^m$. Therefore, it is not possible to encode every such function $g$ with less than $m \cdot 2^{(k-1)n}$ bits. Note that if two functions $g, g'$ are different, then $f_g$ and $f_{g'}$ are different, too.

Clearly, for all $g \in G_{k-1,n,m}$, $f_g$ is simple for Alice. Assume that for all $g$, $f_g$ has $D_k(f_g) \leq d$. Then by Lemma 3.3, every such function $f_g$ can be uniquely represented by a $2^d$-coloring of $\left(\{0,1\}^n\right)^{k-1}$ and $2^m \cdot 2^d$ cylinder intersections in $\left(\{0,1\}^n\right)^{k-1}$. The $2^d$-coloring of $\left(\{0,1\}^n\right)^{k-1}$ can be encoded with $d \cdot 2^{(k-1)n}$ bits. The number of $i$-cylinders in $X_1 \times \cdots \times X_t$ is $2^{\Pi_{j \neq i}|X_j|}$. Hence, $(k-1) \cdot 2^{(k-2)n}$ bits suffice for a unique encoding of any cylinder intersection in $\left(\{0,1\}^n\right)^{k-1}$. Thus, the total number of bits in which any function $f_g$, $g \in G_{k-1,n,m}$, can be encoded is bounded above by

$$d \cdot 2^{(k-1)n} + 2^{d+m} \cdot (k-1) \cdot 2^{(k-2)n} \;=\; d \cdot 2^{(k-1)n} + (k-1) \cdot 2^{d+m+(k-2)n}$$

As we have seen above, the number of bits needed to describe a function $f_g$ for $g \in G_{k-1,n,m}$ is at least $m \cdot 2^{(k-1)n}$. Therefore, if for all $f_g$ a protocol with complexity $d$ exists, then

$$d \cdot 2^{(k-1)n} + (k-1) \cdot 2^{d+m+(k-2)n} \;\geq\; m \cdot 2^{(k-1)n}.$$

This is equivalent to $2^d \geq 2^{n-m} \cdot (m-d)/(k-1)$. Hence, $d \;\geq\; \min\{m-1,\; n-m-\log(k-1)\}$, which for $m = \left\lfloor (n - \log k)/2 \right\rfloor$ is at least $(n - \log k)/2 - O(1)$. □

### 3.4 Separating Public from Private Coins

We now consider the difference between public-coin and private-coin randomized protocols. Trivially, any private-coin protocol can be simulated by tossing the coins in public, so for all $f$ and $k$, $R_k^{\text{pub}}(f) \leq R_k(f)$. In the other direction, Newman [New91, KN97] provides a simulation of a public-coin protocol by a private-coin protocol. (Although it is stated for the special case of 2 players, the proof works for any number of players.)

**Proposition 3.6** ([New91])**.** *There is a $c > 0$ such that for every $k \geq 2$ and function $f : \{0,1\}^{kn} \to \{0,1\}$, $R_k(f) \leq R_k^{pub}(f) + c\lceil \log_2 n \rceil$.*

We see that the maximum gap between the public-coin and private-coin randomized complexities of $f$ is $\Theta(\log n)$, and it is achieved when $R_k^{\text{pub}}(f)$ is $O(1)$ and $R_k(f)$ is $\Theta(\log n)$. The natural question arises, is there a function that achieves this gap? Our results allow us to answer this question affirmatively.

In order to obtain lower bounds, we need the following extension of Lemma 3.8 in [KN97] to $k$ players.

**Lemma 3.7.** *If $k^{1/\delta} < D_k(f)$ for some $\delta < 1$, then $R_k(f)$ is $\Omega(\log D_k(f))$.*

*Proof.* We first claim the following holds:

$$D_k(f) \leq (k-1) \cdot 2^{R_{k,\epsilon}(f)} \cdot \left(1 + \log(k-1) + \log\left(\frac{1}{2} - \epsilon\right)^{-1} + R_{k,\epsilon}(f)\right)$$

Provided we prove the above statement, assume that $R_k(f) \leq (1-\delta)/2 \cdot \log(D_k(f))$. Then,

$$\begin{aligned} D_k(f) &= O\left(D_k(f)^{\delta} \cdot D_k(f)^{(1-\delta)/2} \cdot (\delta \cdot \log(D_k(f)) + (1-\delta)/2 \cdot \log(D_k(f)))\right) \\ &= O\left(D_k(f)^{(1+\delta)/2} \cdot \log(D_k(f))\right) \end{aligned}$$

Since $\delta < 1$, this is a contradiction. Hence, $R_k(f) = \Omega(\log D_k(f))$.

The proof of our initial claim follows the same idea as the proof of Lemma 3.8 in [KN97]. Let $c = R_{k,\epsilon}(f)$ and consider the $\epsilon$-error randomized protocol $P$ that achieves $c$. Let $t = 1 + \log(k-1) - \log(1/2 - \epsilon) + c$. We construct a deterministic protocol $P'$ for $f$, of cost $(k-1) \cdot 2^c \cdot t$ as follows.

For every player $i$ and every leaf $l$ of the randomized protocol $P$, let $p_i(l)$ denote the probability player $i$ responds according to the path leading to $l$ (over their own private random strings). Player $i$ (for $1 \leq i \leq k-1$) computes, for every leaf $l$, the real number $p_i(l)$ and publishes $p_i^*(l)$, a $t$-bit approximation of $p_i(l)$. This introduces an error of at most $\phi = 2^{-t}$ for every such value.

Player $k$ now computes, for every $l$, the value $\left(\prod_{i=1}^{k-1} p_i^*(l)\right) \cdot p_k(l)$. Since $p_i^*(l) \in \{p_i(l) - \phi, p_i(l) + \phi\}$ and since $p_i(l) \leq 1$, we get

$$\left(\prod_{i=1}^{k-1} p_i^*(l)\right) \cdot p_k(l) \in \{\prod_{i=1}^{k} p_i(l) - ((1+\phi)^{k-1} - 1), \prod_{i=1}^{k} p_i(l) + ((1+\phi)^{k-1} - 1)\}.$$

Each leaf of the randomized protocol is associated with an output (0 or 1). Player $k$ now estimates the probability of an output in the randomized protocol by summing over the estimates of the probabilities for each leaf corresponding to that output. Finally, player $k$ decides to output in $P'$ the value that has a probability higher than 1/2.

In the original protocol $P$, an error is made with probability at most $\epsilon$. For the deterministic simulation to work, we need to make sure that the extra error introduced by the rounding process is less than $1/2 - \epsilon$. Since each estimate has error at most $(1+\phi)^{k-1} - 1$ and there are at most $2^c$ leaves, we need to make sure that $2^c \cdot ((1+\phi)^{k-1} - 1) < (1/2 - \epsilon)$. Equivalently, we need $(1+\phi)^{k-1} < 1 + (1/2 - \epsilon)/2^c$.

We choose $t = 1 + \log(k-1) - \log(1/2 - \epsilon) + c$, so $\phi = 2^{-t} = \frac{1/2-\epsilon}{2 \cdot (k-1) \cdot 2^c}$. We know that, for $0 \leq x < 1/2$, we have $(1 + x/(k-1))^{k-1} \leq e^x \leq 1 + 2 \cdot x$. Moreover, $(1/2 - \epsilon)/(2 \cdot 2^c) < 1/2$. Therefore,

$$(1+\phi)^{k-1} < 1 + 2 \cdot \frac{1/2 - \epsilon}{2 \cdot 2^c} = 1 + (1/2 - \epsilon)/2^c.$$

This completes the argument that the deterministic protocol $P'$ works and, thus, the proof of the Lemma. □

**Corollary 3.8.** *Let $\delta < 1$. For all $k$ such that $k < n^\delta$, there exists a $kn$-bit function $f$ such that $R_k^{pub}(f)$ is $O(1)$ and $R_k(f)$ is $\Theta(\log n)$.*

*Proof.* By Theorem 3.4 there is a function $f$ that is simple for player 1 such that $D_k(f)$ is $\Omega(n)$. By Lemma 3.7, $R_k(f)$ is $\Omega(\log n)$. By Lemma 3.1, $R_k(f)$ is $O(\log n)$ and $R_k^{\text{pub}}(f)$ is $O(1)$. □

# 4 Lower Bounds for Explicit Simple Functions

The separations in Section 3.3 are nonconstructive. We conjecture that there also exist *explicit* families of simple functions that give a linear or near linear separation between deterministic and one-sided error randomized $k$-player NOF communication complexities. In this section, we give two constructions of explicit families of simple functions, thus in $\mathsf{coRP}_k^{cc}$, that, we believe, might be outside $\mathsf{P}_k^{cc}$ for $k \geq 3$. While we are unable to prove the super-polylogarithmic ($(\log n)^{\omega(1)}$) deterministic communication complexity lower bounds required to place them outside $\mathsf{P}_k^{cc}$, we are, however, able to prove much weaker logarithmic ($\Omega(\log n)$) lower bounds. As a corollary, we obtain a separation between deterministic and public coin randomized communication complexities for explicit families of simple functions, though this is much weaker than our conjecture.

We begin in Section 4.1, by giving a family of simple functions for the case where we have only $k = 3$ players. This construction does not immediately generalize for $k > 3$ players, but we present it first because it is both simple enough and illustrative of a certain "mixing" property (made precise later) that plays a

crucial role in our arguments. We then prove the lower bound $D_k(f) = \Omega(\log n)$ for, in fact, *any* function family $f$ that satisfies this mixing property. In Section 4.2, we present a different family of simple functions, that can be defined for any $k \geq 3$, and we show that this family satisfies the same mixing property that we use in Section 4.1, thus allowing us to obtain a similar lower bound.

## 4.1 A Function Family for $k = 3$ Players

In the case of $k = 3$ players, our construction is based on universal families of hash functions. We begin with an informal description of our arguments.

Given a universal family $H$ of hash functions from $A$ to $B$, our three player function $f$ is defined on the set $B \times H \times A$ as follows. The second player holds a hash function $h \in H$, the third player holds an input $x \in A$, and $h(x) \in B$ is the unique value for the input of the first player that makes $f$ evaluate to 1. The key "mixing" property that this construction satisfies is closely related to the Hash Mixing Lemma from [MNT93], and says that, for every large rectangle $R \subseteq H \times A$ and every $b \in B$, if we visualize $R$ as a matrix where the entry at location $(h, x)$ has value $h(x)$, then the number of $b$-valued entries in $R$ is very close to uniform, that is, $|R|/|B|$. After making these definitions precise, we use the mixing property combined with the characterization of a deterministic protocol for $f$ from Lemma 3.3, to give some evidence as to why we believe $D_k(f)$ might be large. We subsequently prove in Theorem 4.4 that $D_k(f) = \Omega(\log n)$ for any function $f$ that satisfies the mixing property.

**Definition of the Family.** We write $\mathbb{F}_q$ for the finite field of $q$ elements when $q$ is a prime power. Let $n \geq 4$ be a positive integer, and let $m = n^{1/2}$. For $x \in \{0,1\}^n$ and $a \in \{0,1\}^{n+m-1}$, let $a \circ x$ be the $m$-bit string $z$ whose $i$-th bit is defined by $z_i = \sum_{j=1}^{n} x_j a_{(i-1)+j} \mod 2$. For two $m$-bit strings $z$ and $b$, let $z \oplus b$ be the bitwise exclusive-or of the two strings. For $(a, b) \in \mathbb{F}_{2^{n+m-1}} \times \mathbb{F}_{2^n}$, let $h_{a,b} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be defined by $h_{a,b}(x) = (a \circ x) \oplus b$. [MNT93] show that $H^{n,m} = \{h_{a,b} \mid a \in \mathbb{F}_{2^{n+m-1}}, b \in \mathbb{F}_{2^n}\}$ is a universal family of hash functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. We are now ready to define our family of simple functions for $k = 3$ players.

DEFINITION 4.1. *Let $f = (f_{3,N})_{N \in \mathbb{N}}$ be the family of functions defined as follows. For $N$ large enough, let $n = N/3$, let $m = n^{1/2}$, and note that $|H^{n,m}| \leq 2^{2n+m-1} \leq 2^N$. Let $f_{3,N} : \mathbb{F}_m \times H^{n,m} \times \mathbb{F}_n \to \{0,1\}$ be defined by $f_{3,N}(y, h, x) = 1$ if and only if $y = h(x)$.*

Clearly, $f_{3,N}$ is simple for player 1, so by Lemma 3.1, $R^0_{3,1/N}(f) = O(\log N)$ and $R^{0,\text{pub}}_3(f) = O(1)$.

**Mixing Property.** The following is a "mixing" property of $f$, that we will be use to prove lower bounds on $D_3(f)$.

DEFINITION 4.2 (Mixing Property). *Let $f = (f_{k,N})_{N \in \mathbb{N}}$ be a family of functions simple for player 1. Let $m = \log |X_1|$. Note that, in general, $k = k(N)$ and $m = m(N)$. Let $Z = X_2 \times \cdots \times X_k$ and let $g : Z \to X_1 \cup \{\perp\}$ be the unique function such that $f_{k,N}(x_1, x_2, \ldots, x_k) = 1$ if and only if $x_1 = g(x_2, \ldots, x_k)$. We say that the family $f$ has a* mixing property *if the following holds. For large enough $N$, for every cylinder intersection $I \subseteq Z$ with $|I| \geq |Z| \cdot 2^{-2m}$, and for every $x_1 \in X_1$, when $(x_2, \ldots, x_k)$ is drawn uniformly from $I$,*

$$\Pr[g(x_2, \ldots, x_k) = x_1] \leq 2 \cdot \frac{1}{2^m} = 2^{-m+1}.$$

*Note.* In the condition $|I| \geq |Z| \cdot 2^{-2m}$, the choice of $-2m$ as an exponent might seem arbitrary. As it is, Definition 4.2 allows us to prove Theorem 4.4. But, in fact, for both the construction in this section, and for the construction in Section 4.2, we could prove an even stronger mixing property, one that would apply to even smaller rectangles: for every $\alpha$, for large enough $N$ (now a function of $\alpha$), for every cylinder intersection $I$ with $|I| \geq |Z| \cdot 2^{-\alpha m}$, the same property as above would be required of $I$. However, we do not know how to use this stronger mixing property to prove a larger lower bound than the one in Theorem 4.4.

In the special case when $f$ is the family from Definition 4.1, we have $k = 3$, so we can visualize $Z = H^{n,m} \times \mathbb{F}_{2^n}$ as a 2-dimensional matrix in which rows correspond to hash functions $h \in H^{n,m}$, columns correspond to inputs $x \in \mathbb{F}_{2^n}$, and the entry at row $h$ and column $x$ is $Z_{h,x} = h(x) \in \mathbb{F}_{2^m}$. Furthermore, cylinder intersections in 2 dimensions are rectangles. With this interpretation, the mixing property says that for every large rectangle $R \subseteq Z$, more precisely, when $|R| \geq |Z| \cdot 2^{-m}$, the number of $y$-entries in $R$ is at most twice the expected number if $R$ was filled at random with values from $\mathbb{F}_{2^m}$. The fact that $f$ has this property follows directly from the Hash Mixing Lemma in [MNT93].

**Lemma 4.3.** *The function family $f = (f_{3,N})_{N \in \mathbb{N}}$ from Definition 4.1 has the mixing property from Definition 4.2.*

*Proof.* Since $H^{n,m}$ is a universal family of hash functions, by Lemma 13 in [MNT93], for every rectangle $R \subseteq Z$ and for every $y \in \mathbb{F}_{2^m}$, when $(h, x)$ are drawn uniformly from $R$, we have

$$\Pr[h(x) = y] \leq \frac{1}{|\mathbb{F}_{2^m}|} + \left( \frac{|H^{n,m}|}{|R| \cdot |\mathbb{F}_{2^m}|} \right)^{1/2} = 2^{-m} + \left( \frac{|Z|}{|R|} \cdot 2^{-n-m} \right)^{1/2}.$$

When $|R| \geq |Z| \cdot 2^{-2m}$, as in Definition 4.2, we have $\Pr[h(x) = y] \leq 2^{-m} + 2^{-n/2+m/2}$. Since $n/2 \geq 3m/2$ for large enough $n$, we get $\Pr[h(x) = y] \leq 2^{-m+1}$. □

**Evidence Towards a Conjecture.** The following is not a precise argument, but we consider it evidence towards why we believe that the deterministic communication complexity of $f$ could have to be large. Let $d = D_3(f)$. By Lemma 3.3, there exists a $2^d$-coloring $c$ of $Z$ and there are $2^{d+m}$ rectangles $R_{\ell,y} \subseteq M$, for $\ell \in [2^d]$ and $y \in \mathbb{F}_m$, such that

$$\forall (y, h, x) \in \mathbb{F}_m \times H^{n,m} \times \mathbb{F}_n : \quad (h, x) \in R_{c(h,x),y} \Leftrightarrow h(x) = y.$$

In keeping with the matrix interpretation of $Z$, we say that $(h, x) \in Z$ is *an $(\ell, y)$-entry in $Z$* if and only if $c(h, x) = \ell$ and $h(x) = y$. For a subset $S \subseteq Z$, let $\#_{(\ell,y)}(S)$ denote the number of $(\ell, y)$-entries in $S$ and let $\rho_{(\ell,y)}(S) = \#_{(\ell,y)}(S)/|S|$ denote the density of $(\ell, y)$-entries in $S$. We use the notation $(\ell, \cdot)$ and $(\cdot, y)$ to refer to all entries with color $\ell$ and all entries with value $y$, respectively. For every $(\ell, y) \in [2^d] \times \mathbb{F}_{2^m}$, let

$$B_{\ell,y} = R_{\ell,y} \setminus \bigcup_{y' \neq y} R_{\ell,y'}.$$

We call this set the *boundary* of the rectangle $R_{\ell,y}$. Note that, by definition of the coloring, all $(\ell, y)$-entries in $Z$ are in $B_{\ell,y}$.

Now, let red be a color with $\rho_{(\text{red},\cdot)}(Z) \geq 1/2^d$. When $y$ is chosen uniformly at random from $\mathbb{F}_{2^m}$,

$$\mathrm{E}[\#_{(\cdot,y)}(B_{\text{red},y})] \geq \mathrm{E}[\#_{(\text{red},y)}(B_{\text{red},y})] = \mathrm{E}[\#_{(\text{red},y)}(Z)] = \frac{\#_{(\text{red},\cdot)}(Z)}{2^m} \geq \frac{|Z|}{2^{m+d}}.$$

Furthermore, for various $y$, the sets $B_{\text{red},y}$ are disjoint, so

$$\mathrm{E}[|B_{\text{red},y}|] \leq \frac{|Z|}{2^m}.$$

If we fixed a $y$ for which both quantities above are within constant factors of their expectations (this is imprecise, but we believe it could be made precise), we would obtain a pair $(\text{red}, y)$ such that $\rho_{(\cdot,y)}(B_{\text{red},y}) \geq \Omega(1/2^d)$, whereas the mixing property in Definition 4.2 says that, if $R_{\text{red},y}$ is large enough, $\rho_{(\cdot,y)}(R_{\text{red},y}) \leq O(1/2^m)$. The smaller $d$ is, the larger the gap between these numbers. The reason this situation does not immediately translate into a lower bound for $d$ in terms of $m$ is that $B_{\text{red},y}$ is far from a rectangle, so its density of $(\cdot, y)$-entries could be much larger than that of the rectangle $R_{\text{red},y}$. However, we also consider this as evidence that $d$ might have to be large.

**A Weaker Lower Bound.** In the following Theorem, we show that any family $f = (f_{k,N})_{N\in\mathbb{N}}$ of simple functions that satisfies the mixing property from Definition 4.2 has deterministic communication complexity at least logarithmic in $m = m(N)$, the size of the input of player 1.

We describe the proof idea for the case of $k = 3$ players, when we can view $Z$ as a matrix, but the proof itself works in general for $k \geq 3$. Let $d = D_3(f)$ and consider the $2^d$-coloring $c$ of the matrix $Z$ given by Lemma 3.3. The proof proceeds by inductively decreasing the number of colors available and shrinking the matrix. During each step, we introduce a number of "holes" in the matrix (entries that are colored in the original matrix with one of the removed colors). We show that eventually there are no colors left to use, but the matrix still does not consist only of holes. Even if we were able to shrink the matrix by, say, a factor of 2 in order to remove every color, there are still $2^d$ colors to remove, so at the end we would have shrunk the matrix by a factor of $2^{2^d}$. Since the matrix $Z$ has size $2^{m^{O(1)}}$, this technique can only produce lower bounds of the form $d = \Omega(\log m)$.

**Theorem 4.4.** *Let $f = (f_{k,N})_{N\in\mathbb{N}}$ be a family of functions simple for player 1, with $f_{k,N} : X_1 \times \cdots \times X_k \to \{0, 1\}$, that satisfies the mixing property in Definition 4.2. Let $m = m(N) = \log |X_1|$ be the size of the input of player 1. Then, $D_k(f) = \Omega(\log m)$.*

*Proof.* Let $d = D_k(f)$. Let $Z = X_2 \times \cdots \times X_k$ and let $g : Z \to X_1 \cup \{\perp\}$ be the unique function such that $f_{k,N}(y, x_2, \ldots, x_k) = 1$ if and only if $y = g(x_2, \ldots, x_k)$. By Lemma 3.3, there is a $2^d$-coloring $c$ of $Z$ and there are $2^{d+m}$ cylinder intersections $I_{\ell,y}$, for $(\ell, y) \in [2^d] \times X_1$, such that

$$\forall (y, x_2, \ldots, x_k) \in X_1 \times Z, \quad (x_2, \ldots, x_k) \in I_{c(x_2,\ldots,x_k),y} \Leftrightarrow g(x_2, \ldots, x_k) = y.$$

We say that a point $(x_2, \ldots, x_k)$ has *color* $c(x_2, \ldots, x_k)$ and *value* $g(x_2, \ldots, x_k)$. For a set $S \subseteq Z$, let $\#_{(\ell,y)}(S)$ denote the number of points $(x_2, \ldots, x_k) \in S$ with color $\ell$ and value $y$.

Assume there exists some $\epsilon < 1$ such that for all $m$, $d \leq \epsilon \cdot \log m$. We will derive a contradiction.

For large enough $m$, we prove by induction that for all $0 \leq i \leq 2^d$, there exists a cylinder intersection $I_i \subseteq Z$ and a set of "holes" $H_i \subseteq I_i$ such that:

- $|I_i| \geq |Z| \cdot 2^{-i(d+2)}$;
- $|H_i| \leq i \cdot |Z| \cdot 2^{-m+1}$; and
- the initial coloring induces a coloring of the points in $I_i \setminus H_i$ with $2^d - i$ colors.

Assuming we have established this inductive statement, letting $i = 2^d$, we see that we must have $I_{2^d} \setminus H_{2^d} = \emptyset$, for any points in this set would have been uncolored in the original coloring. For large enough $m$,

$$|I_{2^d}| \geq |Z| \cdot 2^{-2^d(d+2)} \geq |Z| \cdot 2^{-m^\epsilon(\epsilon \cdot \log m + 2)} > |Z| \cdot 2^{-m+\epsilon \cdot \log m + 1} \geq |Z| \cdot 2^{-m+d+1}.$$

Since $|H_{2^d}| \leq 2^d \cdot |Z| \cdot 2^{-m+1}$, we get $I_{2^d} \setminus H_{2^d} \neq \emptyset$, which is a contradiction.

We now prove the inductive statement. For $i = 0$, let $I_0 = Z$ and let $H_0 = \emptyset$. Then, $c$ is a coloring of $I_0 \setminus H_0$ with $2^d$ colors. Now assume the inductive statement is true for some $0 \leq i < 2^d$. We have

$$|I_i \setminus H_i| \geq |Z| \cdot \left(2^{-i(d+2)} - i \cdot 2^{-m+1}\right) > |Z| \cdot \left(2^{-i(d+2)} - 2^{-m+d+1}\right) > |Z| \cdot 2^{-i(d+2)-1},$$

where in the last inequality we used $m - d - 1 > m^\epsilon(\epsilon \cdot \log m + 2) > i(d+2)$, for large enough $m$.

Let $(\ell, y)$ be the most popular color-value pair in $I_i \setminus H_i$. There are at most $2^{m+d}$ such pairs, so

$$\#_{(\ell,y)}(I_i \setminus H_i) \geq |I_i \setminus H_i| \cdot 2^{-m-d} \geq |Z| \cdot 2^{-i(d+2)-1-m-d} = |Z| \cdot 2^{-(i+1)(d+2)-m+1}.$$

Let $I_{i+1} = I_i \cap I_{\ell,y}$, which is a cylinder intersection in $Z$ because both $I_i$ and $I_{\ell,y}$ are. By the property of the coloring $c$ in Lemma 3.3, all points in $Z$ with color-value $(\ell, y)$ are in $I_{\ell,y}$. Hence,

$$|I_{i+1}| \geq \#_{(\ell,y)}(I_i \setminus H_i) \geq |Z| \cdot 2^{-(i+1)(d+2)-m+1}.$$

Note that $(i+1)(d+2) - 1 \leq m^\epsilon(\epsilon \log m + 2) - 1 < m$, so $|I_{i+1}| \geq |Z| \cdot 2^{-2m}$. Then, by the mixing property in Definition 4.2, $\#_{(\cdot,y)}(I_{i+1})/|I_{i+1}| \leq 2^{-m+1}$, so $|I_{i+1}| \geq \#_{(\cdot,y)}(I_{i+1}) \cdot 2^{-m+1}$. Also, $\#_{(\cdot,y)}(I_{i+1}) \geq \#_{(\ell,y)}(I_{i+1}) \geq \#_{(\ell,y)}(I_i \setminus H_i)$. Putting these together, we get

$$|I_{i+1}| \geq \#_{(\ell,y)}(I_i \setminus H_i) \cdot 2^{m-1} \geq |Z| \cdot 2^{-(i+1)(d+2)-m+1} \cdot 2^{m-1} = |Z| \cdot 2^{-(i+1)(d+2)},$$

establishing the first part of the inductive statement.

Let $H_{i+1} = H_i \cup \{(x_2, \ldots, x_k) \in I_{i+1} \mid c(x_2, \ldots, x_k) = \ell\}$. By induction hypothesis, points in $I_i \setminus H_i$ are colored with at most $2^d - i$ colors. Since $\ell$ is no longer available, we see that all points left in $I_{i+1} \setminus H_{i+1}$ must now be colored with at most $2^d - i - 1$ colors, establishing the third part of the inductive statement.

Finally, by the property of $c$ in Lemma 3.3, all points in $I_{\ell,y}$ that have color $\ell$ must have value $y$. In the entire set $Z$, by the mixing property, there are at most $|Z| \cdot 2^{-m+1}$ points with value $y$. Then, $|H_{i+1}| \leq |H_i| + |Z| \cdot 2^{-m+1} \leq (i+1) \cdot |Z| \cdot 2^{-m+1}$, establishing the second part of the inductive statement. □

**Corollary 4.5.** *The function family $f = (f_{3,N})_{N \in \mathbb{N}}$ from Definition 4.1 satisfies $D_3(f) = \Omega(\log N)$. Furthermore, $f$ provides a separation between public-coin and private-coin communication complexity, as $R_3^{pub}(f) = O(1)$ and $R_3(f) = \Omega(\log \log N)$.*

*Proof.* By Lemma 4.3, $f$ has the mixing property. By Theorem 4.4, $D_3(f) = \Omega(\log m)$. By definition of $f$, $m = (N/3)^{1/2}$, so $D_3(f) = \Omega(\log N)$.

Since $f_{3,N}$ is simple for player 1, by Lemma 3.1, $R_3^{\text{pub}}(f) = O(1)$. Finally, by Lemma 3.7, $R_3(f) = \Omega(\log \log N)$. □

## 4.2 A Function Family for $k \geq 3$ Players

To design a family of functions for the case of $k \geq 3$ players, we use a construction from [**?**].

Let $k \geq 3$, and let $n$, $m$ be positive integers with $m \geq \log_2 n$. Let $\beta_1, \ldots, \beta_n$ be distinct elements of $\mathbb{F}_{2^m}$ and define $v_i = (\beta_1^{i-1}, \ldots, \beta_n^{i-1})$ for $1 \leq i \leq n$. Let $g^{n,m} : ((\mathbb{F}_{2^m})^n)^{k-1} \to \mathbb{F}_{2^m}$ be defined by $g^{n,m}(x_2, \ldots, x_k) = \sum_{i=1}^{n} \prod_{j=2}^{k} \langle v_i, x_j \rangle$, where operations are over $\mathbb{F}_{2^m}$.

DEFINITION 4.6. *Let $f = (f_{k,N})_{N \in N}$ be defined as follows. Let $n = N^{1/2}$ and let $m = n^{1/2}$. Let $f_{k,N} : \mathbb{F}_{2^m} \times (\mathbb{F}_{2^m})^n \times \cdots \times (\mathbb{F}_{2^m})^n$ be defined by $f_{k,N}(x_1, \ldots, x_k) = 1$ if and only if $g^{n,m}(x_2, \ldots, x_k) = x_1$.*

We claim that this function family satisfies the mixing property from Definition 4.2, and hence, that we can apply Theorem 4.4 to obtain a lower bound on its deterministic communication complexity. To show this, we need the following technical result, which is the natural analogue of the Hash Mixing Lemma [MNT93] over cylinder intersections.

**Lemma 4.7.** *Let $f$ be the function family from Definition 4.6. Let $Z = ((\mathbb{F}_{2^m})^n)^{k-1}$. For every cylinder intersection $I \subseteq Z$ and for every $y \in \mathbb{F}_{2^m}$, when $(x_2, \ldots, x_k)$ is drawn uniformly from $Z$,*

$$\left| \Pr[g(x_2, \ldots, x_k) = y \text{ and } (x_2, \ldots, x_k) \in I] - 2^{-m} \cdot \frac{|I|}{|Z|} \right| \leq 2^{-(m-2)n/4^{k-1}}.$$

Before proving Lemma 4.7, we show its consequences.

**Corollary 4.8.** *When $k \leq (1/3) \log n$, the function family from Definition 4.6 satisfies the mixing property from Definition 4.2.*

*Proof.* Let $I \subseteq Z$ be a cylinder intersection with $|I| \geq |Z| \cdot 2^{-2m}$ and let $y \in \mathbb{F}_{2^m}$. By Lemma 4.7, when $(x_2, \ldots, x_k)$ are drawn uniformly from $I$,

$$\Pr[g(x_2, \ldots, x_k) = y] \leq 2^{-m} + \frac{|Z|}{|I|} \cdot 2^{-(m-2)n/4^{k-1}} \leq 2^{-m} + 2^{-(m-2)n/4^{k-1}+2m}.$$

When $k \leq (1/3) \log n$, $4^{k-1} < n^{2/3}$. Then, $(m-2)n/4^{k-1} - 2m > (m-2)n^{1/3} - 2m > m$ for large enough $n$. In this case, $\Pr[g(x_2, \ldots, x_k) = y] \leq 2^{-m+1}$, as required in Definition 4.2. □

**Corollary 4.9.** *When $k \leq (1/6) \log N$, the function family $f$ from Definition 4.6 has $D_k(f) = \Omega(\log N)$. Furthermore, $f$ provides a separation between public-coin and private-coin communication complexities, as $R_k^{pub}(f) = O(1)$ and $R_k(f) = \Omega(\log \log N)$.*

*Proof.* Since $k \leq (1/6) \log N$ and $n = N^{1/2}$ in the definition of $f$, we have $k \leq (1/3) \log n$. By Corollary 4.8, the function family $f$ satisfies the mixing property from Definition 4.2. By Theorem 4.4, $D_k(f) = \Omega(\log m)$. Since $m = N^{1/4}$, we get $D_k(f) = \Omega(\log N)$.

Since $f_{k,N}$ is simple for player 1, by Lemma 3.1, $R_k^{\text{pub}}(f) = O(1)$. Finally, by Lemma 3.7, $R_k(f) = \Omega(\log \log N)$. □

*Proof of Lemma 4.7.* We extend the ideas of Raz [Raz00] and Beame and Vee [**?**]. We write $g$ for $g^{n,m}$ to reduce clutter. As shown in [**?**], for $(x_2, \ldots, x_k)$ uniformly chosen in $Z$ and any two sets $A_0, A_1 \in \mathbb{F}_{2^m}$ with $|A_0| = |A_1|$,

$$|\Pr[g(x_2, \ldots, x_k) \in A_0] - \Pr[g(x_2, \ldots, x_k) \in A_1]| \leq (4/2^m)^{n/2^{k-1}} = 2^{-(m-2)n/2^{k-1}}.$$

Now for any function $h : Z \to \{0,1\}$ define $\Delta(h) = E[(-1)^{h(x_2,\ldots,x_k)}]$ where the expectation is over choices of $(x_2,\ldots,x_{k-1}) \in Z$. If $h$ is $\mathbb{F}_2$-multilinear, as observed in [**?**, **?**], the argument in [Raz00] shows that $\Delta(h)^{1/2^{k-1}}$ is an upper bound on the discrepancy under the uniform distribution of $h$ on any cylinder intersection $I$. For a given $I$ this discrepancy is

$$\begin{aligned}\Gamma_I(h) &= |\Pr[h(x_2,\ldots,x_k) = 0 \text{ and } (x_2,\ldots,x_k) \in I] \\ &\quad - \Pr[h(x_2,\ldots,x_k) = 1 \text{ and } (x_2,\ldots,x_k) \in I]|.\end{aligned}$$

For each $S \subseteq [m]$ define function $g_S : Z \to \{0,1\}$ as $\bigoplus_{i\in S} \varphi(g(x_2,\ldots,x_k))_i$ where $\varphi$ is an $\mathbb{F}_2$-linear bijection from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2^m$. Therefore, for each $S$ the function $g_S$ is linear. Set $A_{S,b} = \{\vec{y} \in \mathbb{F}_{2^m} \mid \bigoplus_{i\in S} \varphi(\vec{y})_i = b\}$ for $b \in \{0,1\}$, If $S \neq \emptyset$ then $|A_{S,0}| = |A_{S,1}|$ and so by definition,

$$\begin{aligned}\Delta(g_S) &= |\Pr[g_S(x_2,\ldots,x_k) = 0] - \Pr[g_S(x_2,\ldots,x_k) = 1]| \\ &= |\Pr[g(x_2,\ldots,x_k) \in A_{S,0}] - \Pr[g(x_2,\ldots,x_k) \in A_{S,1}]| \\ &\leq 2^{-(m-2)n/2^{k-1}}.\end{aligned}$$

Fix some cylinder intersection $I$ on $Z$. It follows that for $S \neq \emptyset$ the discrepancy of $g_S$ on $I$,

$$\begin{aligned}\Gamma_I(g_S) &= |\Pr[g_S(x_2,\ldots,x_k) = 0 \text{ and } (x_2,\ldots,x_k) \in I] \\ &\quad - \Pr[g_S(x_2,\ldots,x_k) = 1 \text{ and } (x_2,\ldots,x_k) \in I]| \\ &\leq 2^{-(m-2)n/4^{k-1}}.\end{aligned}$$

Now define the function $p : \mathbb{F}_2^m \to \mathbb{R}$ given by

$$p(y) = \Pr[\varphi(g(x_2,\ldots,x_k)) = y \text{ and } (x_2,\ldots,x_k) \in I].$$

Clearly, $\sum_{y\in\mathbb{F}_2^m} p(y) = \Pr[I]$. Consider the Fourier transform of $p$ over $\mathbb{F}_2^m$ and write $p = \sum_{S\subseteq[m]} \hat{p}_S \chi_S$ where $\chi_S(y) = \prod_{i\in S}(-1)^{y_i}$ and $\hat{p}_S = \frac{1}{2^m}\sum_{y\in\mathbb{F}_2^m} p(y)\chi_S(y)$. Observe that by definition $|\hat{p}_S|$ is precisely $\Gamma_I(g_S)/2^m$ and thus $\hat{p}_S$ is $\Pr[I]/2^m$ for $S = \emptyset$ and has absolute value at most $2^{-m}2^{-(m-2)n/4^{k-1}}$ for all other $S \subseteq [m]$. If we define $q(y) = \Pr[I]/2^m$ for all $y \in \mathbb{F}_2^m$ then it is easy to see that $\hat{q}_\emptyset = \Pr[I]/2^m$ and $\hat{q}_S = 0$ for $\emptyset \subset S \subseteq [m]$. Define function $r = p - q$. Then by the linearity of the transform, $\hat{r}_\emptyset = 0$ and $|\hat{r}_S| \leq 2^{-m}2^{-(m-2)n/4^{k-1}}$ for all other $S \subseteq [m]$. By Parseval's equality, $||r||_2 = ||\hat{r}||_2$ and thus

$$||r||_2^2 \leq \sum_{y\in\mathbb{F}_2^m} 2^{-2m}2^{-2(m-2)n/4^{k-1}} = 2^{-m}2^{-2(m-2)n/4^{k-1}}$$

and thus $||r||_2 \leq 2^{-m/2}2^{-(m-2)n/4^{k-1}}$. Since $r$ has $2^m$ dimensions, $||p-q||_1 = ||r||_1 \leq 2^{m/2}||r||_2 \leq 2^{-(m-2)n/4^{k-1}}$. In particular, this implies that for any $y \in \mathbb{F}_2^m$,

$$|\Pr[\phi(g(x_2,\ldots,x_k)) = y \text{ and } (x_2,\ldots,x_k) \in I] - \Pr[I]/2^m| \leq 2^{-(m-2)n/4^{k-1}},$$

which is what we wanted to prove. □

# 5 On Complete Problems for $\mathsf{NP}_k^{cc}$

An alternative approach to separating $\mathsf{P}_k^{cc}$ from $\mathsf{RP}_k^{cc}$ with an explicit function is to find a function that is complete in some sense. If we can prove for some explicit function that it is "at least as hard" as any function in $\mathsf{RP}_k^{cc}$, then by our separation result we can conclude that it is not in $\mathsf{P}_k^{cc}$. The set intersection function is complete for the class analogous to $\mathsf{NP}_k^{cc}$ in the number-in-hand (NIH) model, and thus also for $\mathsf{NP}_2^{cc}$. In this section, we prove that this function is not complete for $\mathsf{NP}_k^{cc}$ for $k \geq 3$.

In two-player communication complexity, Babai, Frankl, and Simon [BFS86] defined a natural notion of a reduction between problems called a 'rectangular' reduction that does not require any communication to compute.

DEFINITION 5.1. *For $k = 2$, let $f : X_1 \times X_2 \to \{0,1\}$ and $g : X_1' \times X_2' \to \{0,1\}$. A pair of functions $\varphi_1, \varphi_2$ with $\varphi_i : X_i \to X_i'$ is a* rectangular reduction *of $f$ to $g$, written $f \sqsubseteq g$, if and only if $f(x_1, x_2) = g(\varphi_1(x_1), \varphi_2(x_2))$.*

Furthermore, they defined an appropriate 'polynomially-bounded' version of rectangular reduction for function families.

DEFINITION 5.2. *For function families $f = \{f_n\}$ and $g = \{g_n\}$ where $f_n, g_n : (\{0,1\}^n)^2 \to \{0,1\}$, we write $f \sqsubseteq_p g$ if and only if there is a function $m : \mathbb{N} \to \mathbb{N}$ such that for every $n$, $f_n \sqsubseteq g_{m(n)}$ and $m(n)$ is $2^{(\log n)^{O(1)}}$.*

**Proposition 5.3** ([BFS86])**.** *Let $f$ and $g$ be function families. If $f \sqsubseteq_p g$ and $g \in \mathsf{P}_2^{cc}$ then $f \in \mathsf{P}_2^{cc}$. If $f \sqsubseteq_p g$ and $g \in \mathsf{NP}_2^{cc}$ then $f \in \mathsf{NP}_2^{cc}$.*

DEFINITION 5.4. *A function family $g$ is* complete for $\mathsf{NP}_2^{cc}$ under rectangular reductions *if and only if $g \in \mathsf{NP}_2^{cc}$ and for all $f \in \mathsf{NP}_2^{cc}$, $f \sqsubseteq_p g$.*

Recall the set intersection function INT from Definition 2.1 Clearly, $\mathrm{INT} \in \mathsf{NP}_k^{cc}$. Babai, Frankl and Simon observed the following:

**Proposition 5.5** ([BFS86])**.** INT *is complete for $\mathsf{NP}_2^{cc}$ under rectangular reductions.*

For $k \geq 3$, rectangular reductions extend to *cubic reductions* in the NIH model of communication complexity. Moreover, it is easy to see that the completeness result of Proposition 5.5 continues to hold in the NIH model under cubic reductions. One might conjecture that INT is also complete for $\mathsf{NP}_k^{cc}$ under a natural extension of rectangular reductions in the NOF model. Such a notion of reduction should not require any communication between the players. This yields the following definition:

DEFINITION 5.6. *Given $f : X_1 \times \cdots \times X_k \to \{0,1\}$ and $g : X_1' \times \cdots \times X_k' \to \{0,1\}$ we say that functions $\varphi_1, \ldots, \varphi_k$ are a* cylindrical reduction *of $f$ to $g$ if and only if for every $(x_1, \ldots, x_k) \in X_1 \times \cdots \times X_k$ there is an $(x_1', \ldots, x_k') \in X_1' \times \cdots \times X_k'$ such that for all $i \in [k]$, $\varphi_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k) = (x_1', \ldots, x_{i-1}', x_{i+1}', \ldots, x_k')$ and $f(x_1, \ldots, x_k) = g(x_1', \ldots, x_k')$. Thus, each $\varphi_i$ maps the NOF view of the $i$-th player on input $(x_1, \ldots, x_k)$ for $f$ to the NOF view of the $i$-th player on input $(x_1', \ldots, x_k')$ for $g$.*

We show that cylindrical reductions must be of a special form, given by the natural no-communication reductions associated with the number-in-hand model.

DEFINITION 5.7. *Given $f : X_1 \times \cdots \times X_k \to \{0,1\}$ and $g : X_1' \times \cdots \times X_k' \to \{0,1\}$ we say that functions $(\psi_1, \ldots, \psi_k)$ are a* cubic reduction *of $f$ to $g$ if and only $\psi_i : X_i \to X_i'$ for every $i$, and $f(x_1, \ldots, x_k) = g(\psi_1(x_1), \ldots, \psi_k(x_k))$.*

**Lemma 5.8.** *If $(\varphi_1, \ldots, \varphi_k)$ is a cylindrical reduction of $f$ to $g$ then there is a cubic reduction $(\psi_1, \ldots, \psi_k)$ of $f$ to $g$ such that, for all $i$,*

$$\varphi_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k) = (\psi_1(x_1), \ldots, \psi_{i-1}(x_{i-1}), \psi_{i+1}(x_{i+1}), \ldots, \psi_k(x_k)).$$

*Proof.* We prove by induction on $k$ that any consistent cylindrical reduction (whether or not it correctly reduces $f$ to $g$) must be cubic. The claim is trivial for $k = 2$. Assume that $k > 2$. Consider $(x_1, \ldots, x_k)$ and let $(x'_1, \ldots, x'_k)$ be the output of the cylindrical reduction on $x$. Let $y_k \in X_k$. The requirement that $\varphi_k(x_1, \ldots, x_{k-1}) = (x'_1, \ldots, x'_{k-1})$ and the fact that the views output by the $\varphi_i$ for $i < k$ must be consistent with this output implies that for $i < k$,

$$\varphi_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k-1}, x_k) = (x'_1, \ldots, x'_{i-1}, x'_{i+1}, \ldots, x'_{k-1}, x'_k)$$

and

$$\varphi_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k-1}, y_k) = (x'_1, \ldots, x'_{i-1}, x'_{i+1}, \ldots, x'_{k-1}, y'_k)$$

for some $y'_k \in X'_k$. Thus the first $k-2$ coordinates of the output of $\varphi_i$ are independent of the last coordinate of its input. Since $x = (x_1, \ldots, x_k)$ and $y_k$ were chosen arbitrarily, for any such input we can define functions $(\varphi'_1, \ldots, \varphi'_{k-1})$ where $\varphi'_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k-1})$ consists of the first $k-2$ coordinates of $\varphi_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k-1}, y_k)$ for any $y_k \in X_k$. These form a consistent map on $k-1$ coordinates and therefore by the inductive hypothesis there are $(\psi_1, \ldots, \psi_{k-1})$ such that

$$\varphi'_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k-1}) = (\psi_1(x_1), \ldots, \psi_{i-1}(x_{i-1}), \psi_{i+1}(x_{i+1}), \ldots, \psi_{k-1}(x_{k-1}))$$

and therefore for $i < k$ and any $x_1, \ldots, x_k \in X_k$,

$$\varphi_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k-1}, x_k) = (\psi_1(x_1), \ldots, \psi_{i-1}(x_{i-1}), \psi_{i+1}(x_{i+1}), \ldots, \psi_{k-1}(x_{k-1}), x'_k)$$

for some $x'_k = \phi_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$ for some function $\phi_i$; i.e., $\varphi_i$ acts component-wise on all but the $k$-th coordinate. Now, since $k > 2$ there is some $j \notin \{i, k\}$ and, by symmetry, the same inductive argument can be applied to characterize $\varphi_i$ for all $i \neq j$ so that $\varphi_i$ acts component-wise on all but the $j$-th coordinate. Moreover, the inductive argument implies that there are functions $\psi'_1, \ldots, \psi'_{j-1}, \psi'_{j+1}, \ldots, \psi'_k$ that give this component-wise behavior. Defining $\psi'_j = \psi_j$ and $\psi_k = \psi'_k$ we see that we must have $\psi'_i = \psi_i$ for all $i \in [k]$. Therefore for $i < k$, $\varphi_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k) = (\psi_1(x_1), \ldots, \psi_{i-1}(x_{i-1}), \psi_{i+1}(x_{i+1}), \ldots, \psi_k(x_k))$. Since $k$ was arbitrarily chosen, the same applies for $i = k$ and the result follows by induction. □

DEFINITION 5.9. *The set $A \subseteq X_1 \times \cdots \times X_k$ is a* cube *if $A = A_1 \times \ldots \times A_k$ for some sets $A_i \subseteq X_i$, for all $i \in [k]$.*

**Lemma 5.10.** *If there is a cylindrical reduction of $f : X_1 \times \cdots \times X_k \to \{0, 1\}$ to $\mathrm{INT}_{k,m}$ then $f^{-1}(1)$ is a union of $m$ cubes.*

*Proof.* By Lemma 5.8, there are functions $(\psi_1, \ldots, \psi_k)$ such that

$$f(x_1, \ldots, x_k) = \mathrm{INT}_{k,m}(\psi_1(x_1), \ldots, \psi_k(x_k)).$$

Thus $(x_1, \ldots, x_k) \in f^{-1}(1)$ if and only if there is some $i \in [m]$ such that the $i$-th coordinate of each of $\psi_1(x_1), \ldots, \psi_k(x_m)$ is 1. For $j \in [k]$ let $A_{i,j} = \{x_j \mid \text{ the } i\text{-th coordinate of } \psi_j(x_j) \text{ is } 1\} \subseteq X_j$. Therefore $A_{i,1} \times \ldots \times A_{i,k}$ is a cube for each $i \in [m]$ and $f^{-1}(1) = \bigcup_{i \in [m]} A_{i,1} \times \ldots \times A_{i,k}$ as required. □

**Theorem 5.11.** *There is a function $f : (\{0,1\}^n)^3 \to \{0,1\}$ with deterministic 3-player NOF communication complexity at most 3 such that any cylindrical reduction of $f$ to $\mathrm{INT}_{3,m}$ requires $m > 2^{n-3}$.*

*Proof.* For $x, y, z \in \{0,1\}^n$, define $f(x,y,z)$ to be 1 if and only if $x$, $y$, and $z$ are pairwise orthogonal in $\mathbb{F}_2^n$. There is a trivial 3-player NOF protocol for $f$ in which 3 bits are exchanged, namely, each player checks that the inputs it sees are orthogonal. We now show that any way to write $f^{-1}(1)$ as a union of cubes must contain exponentially many cubes since each cube can only cover an exponentially small portion of $f^{-1}(1)$.

For $u, v \in \{0,1\}^n$, let $h(u,v) = 1$ iff $\langle x, y\rangle = 0$ in $\mathbb{F}_2^n$. Then $f(x,y,z) = h(x,y)h(y,z)h(x,z)$. Consider the uniform distribution $\mu$ over $\{0,1\}^{3n}$.

We first show that $f^{-1}(1)$ is a set of probability more than 1/8. Under $\mu$, for each pair $u, v \in \{x,y,z\}$, the probability that $h(u,v) = 1$ is $1/2 + 1/2^n > 1/2$ (consider whether or not $u = 0^n$). We claim that the probability that $f(x,y,z) = 1$ is at least 1/8. Suppose that $x \neq 0^n$. Then the probability that $y$ is orthogonal to $x$ is precisely 1/2. Now, $z$ is orthogonal to the span $\langle\{x,y\}\rangle$ with probability at least $1/4$. So, conditioned on $x \neq 0^n$, the probability that $f(x,y,z) = 1$ is at least 1/8. If $x = 0^n$ then the probability that $f(x,y,z) = 1$ is precisely the probability that $y$ and $z$ are orthogonal which is at least $1/2$. Therefore the probability that $f(x,y,z) = 1$ is more than $1/8$ overall.

Now since $f(x,y,z) = h(x,y)h(y,z)h(x,z)$, any cube $C = A_1 \times A_2 \times A_3$ with $C \subseteq f^{-1}(1)$ must, in particular, have, $A_1 \times A_2 \subseteq h^{-1}(1)$. Thus every $x \in A_1$ must be orthogonal to every $y \in A_2$ and so the dimensions of their spans must satisfy $\dim(\langle A_1\rangle)+\dim(\langle A_2\rangle) \leq n$. Therefore $|A_1 \times A_2| \leq |\langle A_1\rangle \times \langle A_2\rangle| \leq 2^{\dim(\langle A_1\rangle)+\dim(\langle A_2\rangle)} \leq 2^n$ so $|C| \leq 2^n \cdot |A_3| \leq 2^{2n}$ and the probability that $(x,y,z) \in C$ is at most $2^{-n}$. The claimed result follows immediately. □

This argument can be extended to other functions $h : \{0,1\}^{2n} \to \{0,1\}$ that have only small 1-monochromatic rectangles. It suffices that $h(x,y)h(y,z)h(x,z)$ be 1 on a large fraction of inputs. Also, although the above Lemma is stated only for $k = 3$ it is easy to see that the same bounds hold for larger $k$.

Given that any function $f(x,y,z)$ of the form $h_1(x,y)h_2(x,z)h_3(y,z)$ has communication complexity at most 3, it seems unlikely that any function is complete for $\mathsf{NP}_3^{cc}$ under efficient reductions that do not require communication.

# 6 Open Problems

In this paper we have separated the NOF communication complexity analogs of the complexity classes $\mathsf{P}_k^{cc}$ and $\mathsf{RP}_k^{cc}$ for up to $k = n^{O(1)}$ players. This is somewhat surprising because the only method for proving any lower bound for an explicit function is the discrepancy method, which only seems to work for up to $k = \log n$ players. A major open problem is to prove this separation for an explicit function in $\mathsf{P}_k^{cc}$.

As mentioned earlier, a similar separation has recently been proven between the NOF communication complexity analogs of $\mathsf{RP}_k^{cc}$ and $\mathsf{NP}_k^{cc}$ for up to $k = \epsilon \log n$ players for all $\epsilon < 1$. It is open whether or not this separation continues to hold for more players, even for nonexplicit functions.

# References


[BFS86] László Babai, Péter Frankl, and János Simon. Complexity classes in communication complexity theory (preliminary version). In *27th Annual Symposium on Foundations of Computer Science*, pages 337–347, Toronto, Ontario, Canada, 1986. IEEE.

[BGG06] Richard Beigel, William I. Gasarch, and James Glenn. The multiparty communication complexity of exact-: Improved bounds and new problems. In Rastislav Kralovic and Pawel Urzyczyn, editors, *MFCS*, volume 4162 of *Lecture Notes in Computer Science*, pages 146–156. Springer, 2006.

[BGKL04] László Babai, Anna Gál, Peter G. Kimmel, and Satyanarayana V. Lokam. Communication complexity of simultaneous messages. *SIAM J. Comput.*, 33(1):137–166, 2004.

[BNS92] László Babai, Noam Nisan, and Márió Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *J. Comput. Syst. Sci.*, 45(2):204–232, 1992.

[BPS05] Paul Beame, Toniann Pitassi, and Nathan Segerlind. Lower bounds for lovász-schrijver systems and beyond follow from multiparty communication complexity. In *ICALP*, pages 1176–1188, 2005.

[BT91] Richard Beigel and Jun Tarui. On acc. In *Proceedings of the 32nd annual symposium on Foundations of computer science*, pages 783–792, Los Alamitos, CA, USA, 1991. IEEE Computer Society Press.

[CFL83] Ashok K. Chandra, Merrick L. Furst, and Richard J. Lipton. Multi-party protocols. In *STOC '83: Proceedings of the fifteenth annual ACM symposium on Theory of computing*, pages 94–99, New York, NY, USA, 1983. ACM Press.

[CT93] Fan R. K. Chung and Prasad Tetali. Communication complexity and quasi randomness. *SIAM J. Discret. Math.*, 6(1):110–125, 1993.

[FG06] Jeff Ford and Anna Gál. Hadamard tensors and lower bounds on multiparty communication complexity. In *Complexity of Boolean Functions*, 2006.

[HG91] J. Håstad and M. Goldmann. On the power of small-depth threshold circuits. *Computational Complexity*, 1(2):113–129, 1991.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, New York, NY, USA, 1997.

[MNT93] Yishay Mansour, Noam Nisan, and Prasoon Tiwari. The computational complexity of universal hashing. *Theor. Comput. Sci.*, 107(1):121–133, 1993.

[New91] Ilan Newman. Private vs. common random bits in communication complexity. *Inf. Process. Lett.*, 39(2):67–71, 1991.

[Nis93] Noam Nisan. The communication complexity of threshold gates. In *Proc. of "Combinatorics, Paul Erdos is Eighty"*, pages 301–315, 1993.

[NW93] Noam Nisan and Avi Wigderson. Rounds in communication complexity revisited. *SIAM J. Comput.*, 22(1):211–219, 1993.

[Raz00] Ran Raz. The bns-chung criterion for multi-party communication complexity. *Comput. Complex.*, 9(2):113–122, 2000.

[Yao79] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing(preliminary report). In *STOC '79: Proceedings of the eleventh annual ACM symposium on Theory of computing*, pages 209–213, New York, NY, USA, 1979. ACM Press.