There are no zero-hard problems in multiparty communication complexity

László Babai and Denis Pankratov
University of Chicago

October 23, 2013

Abstract

Beame *et al.* (*Theory of Computing,* 2010) suggest that the multiparty communication complexity analogue of NP may not have any complete families in the number-on-forehead (NOF) model under the natural (cylindrical, polynomially bounded) reductions. We confirm this in a strong sense. Let us call a family $F = (f_n)$ of k-party communication problems (one problem for every input length n) *zero-hard* if all families of k-party communication problems solvable with zero communication (cylinders) admit polynomially bounded reductions to F. We show that for $k \geq 3$ there are no zero-hard families of k-party communication problems. Furthermore, we initiate a study of reduction concepts that "allow communication." We arrive at a definition of a reduction with t bits of *total communication*, which is analogous to the Cook reduction in the classical Turing Machine world. We show that this more powerful reduction does not allow complete families of problems even for low complexity classes.

The purpose this note is conceptual clarification; the proofs are by simple counting arguments, much in the spirit of Beame *et al.*.

1 Introduction

We write NP_k^{cc} to denote the analogue of NP in k-party communication complexity. Beame *et al.* point out that finding an explicit NP_k^{cc}-complete family of communication problems would turn lower bounds, obtained via counting, into lower bounds for explicit functions. They suggest [3, Section 5], however, that for $k \geq 3$ players, NP_k^{cc}-complete families may not exist. We confirm this in a strong form.

Throughout this paper we talk about the "number-on-forehead" (NOF) model of communication complexity, introduced by Chandra, Furst, and Lipton [4], unless the "number-in-hand" (NIH) model is specifically indicated. We shall assume that the number of players is $k \geq 3$, unless the 2-player model is specifically discussed.

We use the notation and terminology of [3] with one slight difference in the concept of termination of the communication protocol (see the beginning of Section 2). Moreover, we shall be consistent in making a distinction between a "communication problem" (a finite object which refers to a communication function over a fixed finite domain) and a "family of communication problems," consisting of one communication problem for each input length n.

Babai, Frankl, and Simon [1] introduced complexity classes of families of 2-party communication problems, analogous to Turing machine complexity classes such as P, NP, BPP, Σ_r, Π_r, $\#\mathsf{P}$; and defined "rectangular reductions" between families of 2-party communication problems. One of the results of [1] asserts that the "set intersection" problem (a family) is NP_2^{cc}-complete under "polynomially-bounded" (see definition in Section 2) rectangular reductions.

Beame *et al.* [3] generalize these complexity classes and the reduction concept to multiparty communication and observe that the NP_2^{cc}-completeness result of [1] extends to the NP_k^{cc}-completeness of k-party set-intersection in the NIH model, but not in the far more interesting NOF model. In fact they prove, for $k = 3$ players, that even certain functions of communication complexity at most 2 cannot be reduced to set-intersection without an exponential blowup in the input length. Based on this evidence and on further thoughts on functions with similarly low complexity, they suggest that "it seems unlikely that any function is complete for NP_3^{cc} under efficient reductions that do not require communication."

Building on the insight of Beame *et al.*, we show that indeed, for $k \geq 3$, no family of k-party communication problems is *hard* even for a trivial subclass of NP_k^{cc}. This subclass consists of the families of *cylinders*, i. e., functions that do not depend on some player's input, so that that player knows the answer with zero communication. We would call a family of functions hard for this class a "zero-hard family." Alas, no zero-hard families exist. It follows that no complexity class that contains the families of cylinders has a complete family of problems.

The absence of zero-hard families witnesses the weakness of the reduction concept under consideration. One way to increase the power of the reduction, already suggested by the wording of the question of Beame *et al.*, is to allow communication. We introduce two natural definitions of such reductions - one permitting precommunication, and one permitting oracle access. The later is analogous to the Cook reduction in the classical Turing Machine world. We consider the class of families of problems (f_n) such that f_n requires $t(n)$ bits of communication. We show that this class does not admit hard problems under the above reductions even if we allow $O(t(n))$ bits of communication.

The rest of the paper is organized as follows. In Section 2 we study the reduction concepts defined by Beame *et al.* and prove the main result of this paper. In Section 3 we introduce the reduction concept with precommunication and generalize our results about the reduction without communication to the new reduction concept. In Section 4 we show that similar results hold for even a more powerful reduction concept with communication.

2 Reductions Without Communication

For the basic definitions, we refer the reader to [3].

A (k, n)-communication problem is a function $f : (\{0,1\}^n)^k \to \{0,1\}$. Here k is the number of players and each player's input has n bits. A *family of k-party communication problems* is a sequence $(f_n \mid n \in \mathbb{N})$ where f_n is a (k, n)-communication problem.

Following Yao's original convention [6] (see also Lovász [5]) and deviating from [3], we say that a communication game ends when *one of the players*, specified by the protocol, knows the answer. This is indeed the natural termination rule; this way, for instance, if each player has an n-bit input, the communication cost of the trivial protocol is n bits, rather than $n+1$ when a player has to broadcast the answer. In any case, the difference between the two conventions is at most 1 bit. But this difference will have a philosophical significance; under this definition, it is natural to consider the problems that require zero communication. These are the problems that do not depend on the input of one of the players. Following [2], we call such a problem a *cylinder*, or an i-cylinder if the i-th player's input is irrelevant.

Beame *et al.* [3, Section 5] introduce two reduction concepts, "cylindrical reductions," which map the NOF view of the world to another such view, and "cubic reductions," which map the NIH view of the world to another such view. Somewhat surprisingly, they prove that the two reduction concepts are equivalent; every cylindrical reduction can be expressed as a cubic reduction ([3, Lemma 5.7]). So it suffices to recall their definition of *cubic* reductions [3, Definition 5.6].

Definition 2.1. Given the communication problems $f : X_1 \times \cdots \times X_k \to \{0,1\}$ and $g : Y_1 \times \cdots \times Y_k \to \{0,1\}$, we say that a k-tuple $(\psi_1, \ldots, \psi_k)$ of functions, $\psi_i : X_i \to Y_i$, is a *cubic reduction* of f to g if for all $(x_1, \ldots, x_k) \in X_1 \times \cdots \times X_k$ we have $f(x_1, \ldots, x_k) = g(\psi_1(x_1), \ldots, \psi_k(x_k))$.

In our context, we have $X_i = \{0,1\}^n$ and $Y_i = \{0,1\}^q$.

Given a reduction concept between k-party communication problems, we say that a family (f_n) of k-party communication problems has a "polynomially-bounded" reduction to a family (g_n) of k-party communication problems if there is a *quasipolynomially bounded* ($\exp((\log n)^{O(1)})$ "stretch function" $q : \mathbb{N} \to \mathbb{N}$ such that for all sufficiently large n the communication problem f_n reduces to $g_{q(n)}$ in the given sense. (As argued in [1], $\log n$ is the natural notion of "input length," and the analogue of "polynomial time" should allow increasing this quantity polynomially, hence the quasipolynomial increase in n.)

For a class $\mathcal{C}$ of families of k-party communication problems, we say that a family (f_n) of k-party communication problems is *"$\mathcal{C}$-hard"* if every family in $\mathcal{C}$ has a polynomially bounded reduction to the family (f_n). If, in addition, (f_n) belongs to the class $\mathcal{C}$, we say that it is *"$\mathcal{C}$-complete."*

We shall use these concepts relative to either of the two equivalent types of reductions between communication problems introduced in [3] ("cubic" and "cylindrical" reductions).

We show that if every 1-cylinder reduces to a given function g then the domain of g must be exponentially large. In fact, this remains true even if each 1-cylinder reduces to some member of a rather large set of functions g_i. We need this generalization for the subsequent diagonal argument.

Lemma 2.2. *For all $k, n, q, m \in \mathbb{N}$, if there exists a set $\{g_i \mid i = 1, \ldots, m\}$ of m communication problems $g_i : (\{0,1\}^{q_i})^k \to \{0,1\}$ where $q_i \leq q$ (with at most q-bit inputs) such that every 1-cylinder $C : (\{0,1\}^n)^k \to \{0,1\}$ (with n-bit inputs) has a cubic reduction to one of the g_i then $q \geq \frac{2^{n(k-2)}}{k} - \frac{\log m}{k2^n}$. In particular, if $m \leq 2^{2^{n(k-1)-1}}$ then $q \geq \frac{2^{n(k-2)}}{2k} > 2^{(n-1)(k-2)-2}$.*

Proof. The number of 1-cylinders $C : (\{0,1\}^n)^k \to \{0,1\}$ is $2^{2^{n(k-1)}}$. On the other hand, the number of cubic reductions $(u_1, \ldots, u_k)$, where $u_i : \{0,1\}^n \to \{0,1\}^{q_i}$, is at most 2^{kq2^n}. They give rise to at most $m2^{kq2^n}$ functions $g_i(u_1(x_1), \ldots, u_k(x_k))$. Since every 1-cylinder has a cubic reduction to some g_i, every 1-cylinder must occur among the functions $g_i(u_1(x_1), \ldots, u_k(x_k))$. Consequently, $2^{2^{n(k-1)}} \leq m2^{kq2^n}$ and therefore $q \geq \frac{2^{n(k-2)}}{k} - \frac{\log m}{k2^n}$. □

Definition 2.3. We let $\mathcal{C}_1^k$ denote the *class of families* of k-party 1-cylinders.

Theorem 2.4. *Let (f_n) be a family of communication problems such that every family from $\mathcal{C}_1^k$ reduces to (f_n). Then there exists a family $(C_n) \in \mathcal{C}_1^k$ that requires the corresponding stretch function $q : \mathbb{N} \to \mathbb{N}$ to satisfy $q(n) \geq 2^{(n-1)(k-2)-2}$.*

Proof. We shall define the family (C_n) non-constructively for each n.

Consider the set of functions $S_n := \{f_\ell \mid \ell < 2^{(n-1)(k-2)-2}\}$. Clearly, we have $|S_n| < 2^{(n-1)(k-2)-2} < 2^{2^{n(k-1)-1}}$. Moreover, every 1-cylinder with n-bit inputs that has a cubic reduction to one of the functions from S_n has a corresponding stretch $q < 2^{(n-1)(k-2)-2}$. Thus by Lemma 2.2, there exists a cylinder C_n that cannot be cubically reduced to any of the $f_\ell \in S_n$. We combine thus defined cylinders into a single family (C_n).

It follows that if a cubic reduction of the family $(C_n \mid n \in \mathbb{N})$ to the family (f_n) exists then the corresponding function q must satisfy $q(n) \geq 2^{(n-1)(k-2)-2}$. □

Corollary 2.5. *If $k \geq 3$ then there is no $\mathcal{C}_1^k$-hard family of communication problems.*

The lower bound on the stretch function q provided by Theorem 2.4 is almost matched by the trivial upper bound, which we present next.

Lemma 2.6. *There is a family of communication problems (f_ℓ) such that every family from $\mathcal{C}_1^k$ reduces to (f_ℓ) with the stretch function $q : \mathbb{N} \to \mathbb{N}$ satisfying $q(n) \leq \lceil \frac{2^{n(k-1)}}{k-1} \rceil + n$. Moreover, the family (f_ℓ) is itself in $\mathcal{C}_1^k$.*

Proof. The number of 1-cylinders $C_n : \{0,1\}^{nk} \to \{0,1\}$ is $2^{2^{n(k-1)}}$. Thus each such cylinder has a name that can be described in binary by a string of length $2^{n(k-1)}$. We denote the name of C_n by $\langle C_n \rangle$. Now, we are ready to describe a cubic reduction $(u_{1,C_n}, \ldots, u_{k,C_n})$ from C_n to f_ℓ (to be defined later):

- $u_{1,C_n}(x_1) = 0^{\lceil \frac{2^{n(k-1)}}{k-1} \rceil} \cdot x_1$, where $\cdot$ denotes the concatenation,
- $u_{j,C_n}(x_j) = \langle C_n \rangle_j \cdot x_j$, where $j \in \{2, \ldots, k\}$ and $\langle C_n \rangle_j$ denotes the substring of $\langle C_n \rangle$ spanning from index $(j-2)\lceil \frac{2^{n(k-1)}}{k-1} \rceil + 1$ to $(j-1)\lceil \frac{2^{n(k-1)}}{k-1} \rceil$ (except possibly for $j = k$, when the substring may be shorter, in which case we can inflate the substring by appending 0s to the end).

Now it is clear how the family (f_ℓ) should be defined. We define f_ℓ only for ℓ for which there exists n such that $\ell = \lceil \frac{2^{n(k-1)}}{k-1} \rceil + n$. For input $(y_1, \ldots, y_k)$ let $\widehat{y_i}$ be the substring of y_i consisting of the last n bits and $\widetilde{y_i}$ be the remaining part of y_i. Then define E to be the substring of $\widetilde{y_2} \cdot \widetilde{y_3} \cdots \widetilde{y_k}$ consisting of the first $2^{n(k-1)}$ bits. Let C_n be the cylinder such that $\langle C_n \rangle = E$. Finally

$$f_\ell(y_1, \ldots, y_k) := C_n(\widehat{y_1}, \ldots, \widehat{y_k}).$$

Observe that $(f_\ell) \in \mathcal{C}_1^k$. In addition, for every 1-cylinder C_n we have

$$C_n(x_1, \ldots, x_k) = f_\ell(u_{1,C_n}(x_1), \ldots, u_{k,C_n}(x_k)),$$

where $\ell = \lceil \frac{2^{n(k-1)}}{k-1} \rceil + n$. □

3 Reductions with Precommunication

Let π be a protocol computing some k-party function on n-bit inputs. For each $(x_1, \ldots, x_k) \in \{0,1\}^{nk}$, we use $\pi(x_1, \ldots, x_k)$ to denote the *communication transcript*, i. e., the concatenation of all messages exchanged during the execution of π on $(x_1, \ldots, x_k)$. First we introduce the notion of "communication-constructible" functions, which plays the central role in our definition of reductions with precommunication.

Definition 3.1. Let $f : \{0,1\}^{nk} \to \{0,1\}^t$ be a k-party communication problem with n-bit inputs. We say that f is *communication-constructible* if there exists a (NOF) protocol π such that for each $(x_1, \ldots, x_k) \in \{0,1\}^{nk}$ we have $f(x_1, \ldots, x_k) = \pi(x_1, \ldots, x_k)$.

If a function $f : \{0,1\}^{nk} \to \{0,1\}^t$ is communication-constructible, then $f^i : \{0,1\}^{nk} \to \{0,1\}^i$, obtained by restricting output of f to a prefix of length i, is also communication-constructible. This follows by simply truncating protocol π for f to the first i bits of communication. This implies that the fraction of non-communication-constructible functions is monotonically non-decreasing in t. Thus most functions are not communication-constructible, as even for $t = 1$ most of the functions require n bits of communication by a classical

counting argument. Using this observation one can derive a trivial upper bound on the number of communication constructible function. Next we give a weak, but sufficient for our purposes, upper bound on the number of communication-constructible functions.

Proposition 3.2. *The number of communication-constructible functions* $\{0,1\}^{nk} \to \{0,1\}^t$ *is at most*

$$2^{(2^{n(k-1)}+\log k)(2^t-1)}.$$

Proof. Let $f : \{0,1\}^{nk} \to \{0,1\}^t$ be a communication-constructible function. A t-bit protocol π for f can be viewed as a complete binary tree of depth t (see Figure 1). Each internal node u is labeled by a pair (P_u, f_u), where $P_u \in [k]$ and $f_u : X^{k-1} \to \{0,1\}$. The leaves do not have labels. The players use this

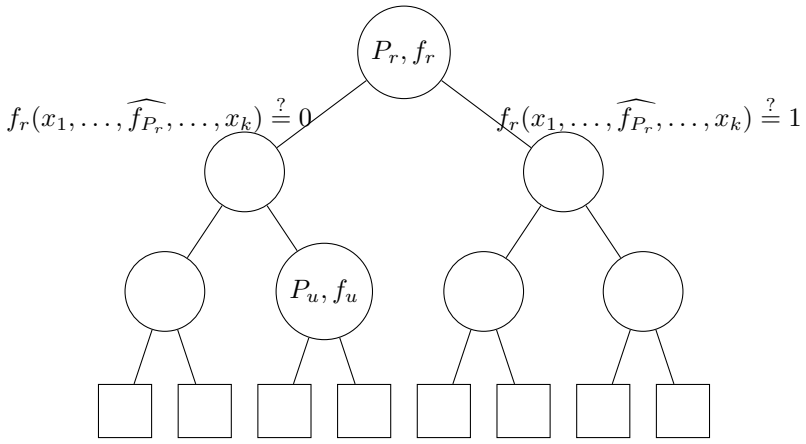

Figure 1: Representation of a k-party t-bit communication protocol π for a communication-constructible function as a labeled complete binary tree.

tree and the labeling for computing $h(x_1, \ldots, x_k)$ in an obvious way. Starting at the root r, player P_r evaluates f_r on the given inputs and writes the result on the public blackboard. The players proceed to the corresponding subtree.

Since the set of communication-constructible functions can be mapped injectively into a set of the labeled trees as above, it suffices to count the number of such trees to establish the claim. Now, for each internal node u the number of possible labels of u is at most $k2^{2^{n(k-1)}} = 2^{2^{n(k-1)}+\log k}$. The number of internal nodes is $2^t - 1$. □

Note that in spite of over-counting the above bound is meaningful for $t \leq n + \log \frac{n}{2}$. As we shall later see, for our purposes we may assume that $t \leq n$.

Remark 3.3. Observe that by our termination condition for t-bit k-party protocols with n-bit inputs that compute some Boolean function the tree from the

proof of Proposition 3.2 should have leaves labelled the same way as the internal nodes. Thus, we conclude that the number of such protocols is at most $2^{(2^{n(k-1)}+\log k)(2^{t+1}-1)}$.

The notion of communication-constructible functions might be of interest on its own; however, our motivation for introducing it was to give the following definition of reductions with precommunication.

Definition 3.4. Let $f : \{0,1\}^{nk} \to \{0,1\}$ and $g : \{0,1\}^{qk} \to \{0,1\}$ be two k-party Boolean functions. We say that f *cylindrically reduces to* g *with* t *bits of precommunication* if there exist functions $h : \{0,1\}^{nk} \to \{0,1\}^t$ and $\psi_i : \{0,1\}^{n(k-1)+t} \to \{0,1\}^{q(k-1)}$ for $i \in [k]$ such that

1. *(precommunication)* h is communication-constructible,
2. *(consistency)* for each $(x_1, \ldots, x_k) \in \{0,1\}^{nk}$ and $z \in \{0,1\}^t$ there exists $(y_1, \ldots, y_k) \in \{0,1\}^{qk}$ such that for each i we have[1] $\psi_i(x_1, \ldots, \widehat{x_i}, \ldots, x_k, z) = (y_1, \ldots, \widehat{y_i}, \ldots, y_k)$, i. e., the ith player computes $(y_1, \ldots, \widehat{y_i}, \ldots, y_k)$ given precommunication string z,
3. *(validity)* for each $(x_1, \ldots, x_k) \in \{0,1\}^{nk}$, if $z = h(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ is defined as above then $f(x_1, \ldots, x_k) = g(y_1, \ldots, y_k)$.

Note: the vector $(y_1, \ldots, y_k)$ is unique.

This notion is a formal description of the following simple idea that generalizes the notion of reduction without communication: before mapping the NOF view of inputs of f to the NOF view of inputs of g, the players are allowed to perform some precommunication during which the players learn t bits of information. These t bits are then available to the players in the computation of the new NOF view.

Definition 3.5. We define the *cubic reduction with* t *bits of precommunication* analogously to the cylindrical reduction by replacing in Definition 3.4 each function $\psi_i : \{0,1\}^{n(k-1)+t} \to \{0,1\}^{q(k-1)}$ with $\phi_i : \{0,1\}^{n+t} \to \{0,1\}^q$, where $\phi_i(x_i, z) = y_i$.

Remark 3.6. One could argue that it would be more natural to introduce and use the notion of NIH communication-constructible functions in the definition of cubic reductions with t bits of precommunication. With such a definition the cubic and cylindrical reductions would not be equivalent, and our main interest is in the NOF model. We are only interested in the NIH reduction concepts to the extent that they are equivalent to NOF reductions concepts and aid our counting arguments.

Remark 3.7. In Definition 3.4 we could have asked to enforce the consistency constraints only for $z = h(x_1, \ldots, x_k)$. However, this does not seem to be enough to guarantee the equivalence of the two reduction concepts.

[1] The hat symbol means that the corresponding component is deleted from the vector.

Now we show that the two reduction concepts, cubic and cylindrical, are equivalent, just as was the case for reductions without communication [3, Section 5].

Proposition 3.8. *Let $f : \{0,1\}^{nk} \to \{0,1\}$ and $g : \{0,1\}^{qk} \to \{0,1\}$ be two k-party functions. Then f cylindrically reduces to g with t bits of precommunication if and only if f cubically reduces to g with t bits of precommunication.*

Proof. Consider the following alternative characterization of a cylindrical reduction from f to g with t bits of precommunication: it is a set Ψ of at most 2^t cylindrical reductions from f to g without communication (each with stretch q) together with a communication-constructible function h that allows the players to agree (using t bits of precommunication) on a specific $(\psi_1, \ldots, \psi_k) \in \Psi$ to use in the reduction step. Analogous characterization holds for the cubic reduction with t bits of precommunication - simply replace the set Ψ of cylindrical reductions without communication with a set of Φ of cubic reductions without communication. By the result of Beame *et al.* [3] we can transform each cylindrical reduction without communication $(\psi_1, \ldots, \psi_k) \in \Psi$ into a cubic reduction without communication $(\phi_1, \ldots, \phi_k) \in \Phi$, and vice versa. Function h is left unchanged. □

From now on, we shall write "f reduces to g with t bits of precommunication", understanding that it could mean either cylindrical or cubic reduction, whichever we prefer more in that particular case.

Definition 3.9. For $t \in \mathbb{N}$, let $\mathcal{A}_t^k$ denote the class of k-party communication problems that are solvable by a t-bit protocol. When $t : \mathbb{N} \to \mathbb{N}$ is a function, we use $\mathfrak{A}_t^k$ to denote the class of *families* (f_n) *of k-party communication problems* such that for each n we have $f_n \in \mathcal{A}_{t(n)}^k$.

In the rest of this section we show that reductions with precommunication exhibits the following sharp threshold phenomenon. While there is a trivial $\mathfrak{A}_t^k$-hard family under reductions with $t(n)+1$ bits of precommunication, there is no $\mathfrak{A}_t^k$-hard family under reductions with $t(n)$ bits of precommunication.

Proposition 3.10. *For every $t : \mathbb{N} \to \mathbb{N}$ such that $t(n) \leq n$ there exists $\mathfrak{A}_t^k$-hard family of communication problems (τ_n) with respect to the reductions with $t(n)+1$ bits of precommunication. Moreover, $(\tau_n) \in \mathcal{C}_1^k$ and the stretch function is $q(n) = 1$ for every $(f_n) \in \mathfrak{A}_t^k$.*

Proof. Define (τ_n) to be the family of projection functions on the second coordinate, i. e., $\tau_n : \{0,1\}^{nk} \to \{0,1\}$ is defined by $(x_1, \ldots, x_k) \mapsto x_2$. Let $(f_n) \in \mathfrak{A}_t^k$. To reduce (f_n) to (τ_n) the players compute the value of the function f_n and broadcast the answer using $t(n)+1$ bits in the precommunication phase of the reduction. The functions ϕ_i simply map the players' inputs to the answer bit, which then gets output by τ_1. In particular, we have $q(n) = 1$. Observe that from the entire family (τ_n) only τ_1 is used. □

Lemma 3.11. *Let $g : \{0,1\}^{qk} \to \{0,1\}$ be a k-party Boolean function. The number of distinct functions on n-bit inputs reducible with t bits of precommunication to g is at most*

$$2^{(2^{n(k-1)}+\log k)(2^t-1)+qk2^{n+t}}.$$

Proof. A function *cubically* reducible to g with t bits of precommunication is completely determined by the two components h and the ϕ_i. The number of distinct h is given by Proposition 3.2 and is at most $2^{(2^{n(k-1)}+\log k)(2^t-1)}$. The total number of the $\phi_i : \{0,1\}^{n+t} \to \{0,1\}^q$ ($i \in [k]$) is $2^{qk2^{n+t}}$. □

We present an analogue of Lemma 2.2 for the reductions with precommunication.

Lemma 3.12. *For all $k, n, q, m, t \in \mathbb{N}$, such that $t < n$, if there exists a set $\{g_i \mid i = 1, \ldots, m\}$ of m communication problems $g_i : (\{0,1\}^{q_i})^k \to \{0,1\}$ where $q_i \leq q$ (with at most q-bit inputs) such that every function $f : (\{0,1\}^n)^k \to \{0,1\}$ from $\mathcal{A}_t^k$ (with n-bit inputs) is reducible to one of the g_i with t bits of precommunication then $q \geq \frac{2^{n(k-2)-t}}{k} - \frac{\log m}{k2^{n+t}} - 1$. In particular, if $m \leq 2^{2^{n(k-1)-1}}$ then $q \geq \frac{2^{n(k-2)-t}}{2k} - 1 \geq 2^{(n-1)(k-2)-t-2}$.*

Proof. By Lemma 3.11 the number of distinct functions reducible to one of the functions from the set $\{g_i\}$ is at most $m2^{(2^{n(k-1)}+\log k)(2^t-1)+qk2^{n+t}}$. Observe that the functions $f : \{0,1\}^t \times \{0,1\}^{n(k-1)} \to \{0,1\}$ are solvable with t bits of communication, thus they appear in $\mathcal{A}_t^k$. Thus, $|\mathcal{A}_t^k| \geq 2^{2^{n(k-1)+t}}$. Consequently, $2^{2^{n(k-1)+t}} \leq m2^{(2^{n(k-1)}+\log k)(2^t-1)+qk2^{n+t}}$ and $q \geq \frac{2^{n(k-2)-t}}{k} - \frac{\log m}{k2^{n+t}} - \frac{(2^t-1)\log k}{k2^{n+t}} \geq \frac{2^{n(k-2)-t}}{k} - \frac{\log m}{k2^{n+t}} - 1$. □

The proof of the following theorem is analogous to the proof of Theorem 2.4.

Theorem 3.13. *Let $t : \mathbb{N} \to \mathbb{N}$ be such that $t(n) < n$, and let (f_n) be a family of communication problems such that every $(g_n) \in \mathfrak{A}_t^k$ reduces to (f_n) with $t(n)$ bits of precommunication. Then there exists a family $(g_n) \in \mathfrak{A}_t^k$ that requires the corresponding stretch function $q : \mathbb{N} \to \mathbb{N}$ to satisfy $q(n) \geq 2^{(n-1)(k-2)-t(n)-2}$.*

We immediately obtain the following corollaries.

Corollary 3.14. *For each $\epsilon \in (0,1)$ and for each $t : \mathbb{N} \to \mathbb{N}$ such that $t(n) \leq (1-\epsilon)n$, there is no $\mathfrak{A}_t^3$-hard family of communication problems with respect to reductions with $t(n)$ bits of precommunication.*

Corollary 3.15. *For each $k \geq 4$ and for each $t : \mathbb{N} \to \mathbb{N}$ such that $t(n) < n$ there is no $\mathfrak{A}_t^k$-hard family of communication problems with respect to reductions with $t(n)$ bits of precommunication.*

Proposition 3.16. *For every $t : \mathbb{N} \to \mathbb{N}$, there is a family of communication problems (f_ℓ) such that every family from $\mathfrak{A}_t^k$ reduces to (f_ℓ)* without communication *with the stretch function $q : \mathbb{N} \to \mathbb{N}$ satisfying $q(n) \leq 2^{n(k-1)+t(n)+1}$ for $n \geq 3$. Moreover, the family (f_ℓ) is itself in $\mathfrak{A}_{\frac{\log \ell}{k}}^k$.*

Proof. Let $(g_n) \in \mathfrak{A}_t^k$. Then there is a $t(n)$-bit protocol π for computing g_n. In the cubic reduction, player i maps x_i to $(x_i, <\pi>)$, where $<\pi>$ is the name of the protocol π. By Remark 3.3, this stretches the input to size at most $(2^{n(k-1)}+\log k)(2^{t(n)+1}-1)+n \leq 2^{n(k-1)+t(n)+1}$ for $n \geq 3$. The family to which we reduce is the "universal family" (U_ℓ) defined by $U_\ell((x_1, <\pi>), \ldots, (x_k, <\pi>)) =$ output of π on $(x_1, \ldots, x_k)$, where $\ell = (2^{n(k-1)}+\log k)(2^{t(n)+1}-1)+n$. Observe that the communication complexity of U_ℓ is bounded above by $t(n)$. Since $\ell \geq 2^{n(k-1)+t(n)} \geq 2^{t(n)k}$, we have $(U_\ell) \in \mathfrak{A}^k_{\frac{\log \ell}{k}}$. □

Remark 3.17. Using a similar idea, if we allow $t(n)$ bits of precommunication in the above proposition then we can put the family (f_ℓ) in a class of problems solvable with 0 bits of communication. The players choose a $t(n)$-bit protocol and run it on their inputs, as the precommunication step. In the reduction step, they append the name of the protocol together with the transcript to their inputs. The family to which we reduce is a "universal family with transcript" (UT_ℓ) defined by $UT_\ell((x_1, T, <\pi>), \ldots, (x_k, T, <\pi>)) =$ output of π on $(x_1, \ldots, x_k)$, where $T = \pi(x_1, \ldots, x_k)$. Note that the stretch function satisfies $q(n) \leq (2^{n(k-1)} + \log k)(2^{t(n)+1} - 1) + t(n) + n \leq 2^{n(k-1)+t(n)+2}$ for $n \geq 3$.

4 Reductions with Rounds of Communication

The reduction concept described in Section 2 is a communication complexity analogue of the *Karp reduction* from the Turing Machine world. In the current section we describe the reduction concept which is analogous to the *Cook reduction*. When f reduces to g via a Cook reduction it means that we can solve

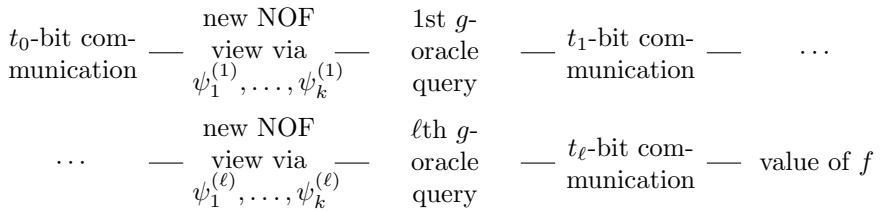

Figure 2: Reduction of f to g with ℓ rounds of communication, i. e., ℓ queries to the g-oracle.

f with the help of an oracle for g. This has a rather intuitive interpretation in the communication complexity world (see Figure 2). More precisely:

Definition 4.1. We say that a function $f : \{0,1\}^{nk} \to \{0,1\}$ reduces to $g : \{0,1\}^{qk} \to \{0,1\}$ with ℓ rounds and t bits of total communication if there exists $t_0, \ldots, t_\ell \in \mathbb{N}$, $h_i : \{0,1\}^{nk+i+\sum_{j=0}^{i-1} t_j} \to \{0,1\}^{t_i}$ $(0 \leq i \leq \ell-1)$, $h_\ell : \{0,1\}^{nk+\ell+\sum_{j=0}^{\ell-1} t_j} \to \{0,1\}$ and $\psi_j^{(i)} : \{0,1\}^{n(k-1)+(i-1)+\sum_{s=0}^{i-1} t_s} \to \{0,1\}^{q(k-1)}$ $(i \in [\ell], j \in [k])$ such that

1. $\ell + \sum_{i=0}^{\ell} t_i = t$,
2. for each $0 \leq i \leq \ell - 1$, h_i is communication-constructible, where the last $i + \sum_{j=0}^{i-1} t_j$ bits are interpreted as a shared string among the players,
3. communication complexity of h_ℓ is t_ℓ,
4. for each $i \in [\ell]$ the functions $(\psi_1^{(i)}, \ldots, \psi_k^{(i)})$ produce a consistent new NOF view on all inputs,
5. for each $(x_1, \ldots, x_k) \in \{0,1\}^{nk}$, after the computation is performed in the obvious way as per Figure 2 the protocol h_ℓ outputs $f(x_1, \ldots, x_k)$.

Definition 4.2. We say that $f : \{0,1\}^{nk} \to \{0,1\}$ reduces to $g : \{0,1\}^{qk} \to \{0,1\}$ with t bits of *total communication* if there exists $0 \leq \ell \leq t$ such that f reduces to g with ℓ rounds and t bits of total communication.

Observe that in Definition 4.1 each query to the g-oracle costs one bit of communication. In contrast, the reduction without rounds from Section 3 allows querying g for free. This difference is motivated by the following argument. If we expand g-oracle into a communication protocol for g, then after each query (= run of the protocol) we are only guaranteed that a single player knows the answer to the query. A query to g in the definition from Section 3 happens only once and at the end. Moreover, in that definition the output of the query matches the output of the function, which is sufficient to terminate the protocol for f without any extra bits of communication. However, if we allow rounds then the players should perform postcommunication with the assumption that *all of them* know the answer. This would require a player who knows the answer to a query from the run of a protocol for g to broadcast it. Thus, in case of rounds of communication we can visualize the g-oracle as writing the answers to the queries on the board, and everything that's written on the board is counted towards the communication cost.

In the rest of this section we show that this seemingly much more powerful reduction concept with t bits of total communication does not allow hard problems even for low complexity classes.

Lemma 4.3. *Let $f : \{0,1\}^{qk} \to \{0,1\}$ be a k-party communication problem. The number of functions on n inputs reducible to g with ℓ rounds and t bits of total communication is at most*

$$2^{2^{n(k-1)+t+4}+kq2^{n+t}}.$$

Proof. Let $t_0, \ldots, t_\ell$ be such that

$$t_i \geq 0 \text{ and } \ell + \sum_{i=0}^{\ell} t_i = t. \tag{1}$$

We shall give a bound $b(t_0, \ldots, t_\ell)$ on the number of functions that are reducible to g using t_i bits of communication in round $i+1$ of the ℓ-round reduction.

This bound will be of the form $b(t_0, \ldots, t_\ell) = \prod_{i=0}^{\ell} c_i$, where c_i is the number of choices available in the ith round of reduction. Similarly to Lemma 3.11, we have

$$\log c_i \leq (2^{n(k-1)+i+\sum_{j=0}^{i-1} t_j} + \log k)(2^{t_i} - 1) + kq2^{n+i+\sum_{j=0}^{i} t_i}$$

for $0 \leq i \leq \ell - 1$.

The last step in the reduction is postcommunication. Similarly to Remark 3.3, we have

$$\log c_\ell \leq (2^{n(k-1)+\ell+\sum_{i=0}^{\ell-1} t_i} + \log k)(2^{t_\ell+1} - 1).$$

Thus

$$\log b(t_0, \ldots, t_\ell) \leq 2^{n(k-1)+t+3} + kq2^{n+t}.$$

The total number of functions that are reducible to g is at most $\sum_{t_0,\ldots,t_\ell} b(t_0, \ldots, t_\ell)$, where $t_0, \ldots, t_\ell$ satisfy (1). Since the number of solutions to (1) is $\binom{t}{\ell} \leq t^\ell$ we have

$$\sum_{t_0,\ldots,t_\ell} b(t_0, \ldots, t_\ell) \leq t^\ell 2^{2^{n(k-1)+t+3}+kq2^{n+t}} \leq 2^{2^{n(k-1)+t+4}+kq2^{n+t}}.$$

□

Corollary 4.4. *Let $f : \{0,1\}^{qk} \to \{0,1\}$ be a k-party communication problem. The number of functions on n inputs reducible to g with t bits of total communication is at most*

$$2^{2^{n(k-1)+t+5}+kq2^{n+t}}.$$

Having this corollary, the following theorem follows easily using steps similar to the ones in Section 3.

Theorem 4.5. *Let $t : \mathbb{N} \to \mathbb{N}$ be such that $0 \leq t(n) < n - 6$, and let (f_n) be a family of communication problems such that every $(g_n) \in \mathfrak{A}^k_{t+6}$ reduces to (f_n) with $t(n)$ bits of total communication. Then there exists a family $(g_n) \in \mathfrak{A}^k_{t+6}$ that requires the corresponding stretch function $q : \mathbb{N} \to \mathbb{N}$ to satisfy $q(n) \geq 2^{(n-5)(k-2)+5}$.*

Proof. Similar to the proof of Theorem 2.4. □

Corollary 4.6. *For each $t : \mathbb{N} \to \mathbb{N}$ such that $t(n) < n-6$ there is no $\mathfrak{A}^k_{t+6}$-hard family of communication problems with respect to reductions with $t(n)$ bits of total communication.*

References

[1] László Babai, Péter Frankl, and Janos Simon. Complexity classes in communication complexity theory. In *FOCS '86: Proc. 27th Symp. on Foundations of Comp. Sci.*, pages 337–347, 1986.

[2] László Babai, Noam Nisan, and Mario Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *J. Computer and System Science*, 45(2):204–232, 1992. Preliminary version appeared in 21st STOC, 1989.

[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.

[4] Ashok K. Chandra, Merrick L. Furst, and Richard J. Lipton. Multi-party protocols. In *STOC '83: Proc.* 15^{th} *ACM STOC*, pages 94–99, 1983.

[5] László Lovász. Communication complexity: a survey. In Bernhard Korte, László Lovász, Hans Jürgen Prömel, and Alexander Schrijver, editors, *Paths, Flows, and VLSI-Layout*, pages 235–265. Springer-Verlag New York, Inc., 1990.

[6] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). In *Proc. 11th STOC*, pages 209–213. ACM, 1979.