Nondeterministic Communication Complexity with Help and Graph Functions

Adi Shraibman
The School of Computer Science
The Academic College of Tel Aviv-Yaffo
adish@mta.ac.il

Abstract

We define nondeterministic communication complexity in the model of communication complexity with help of Babai, Hayes and Kimmel [2]. We use it to prove logarithmic lower bounds on the NOF communication complexity of explicit graph functions, which are complementary to the bounds proved by Beame, David, Pitassi and Woelfel [3].

1 Introduction

The Number On the Forehead model (NOF) in communication complexity presents some of the more interesting and more challenging open questions in communication complexity. In this model $k \geq 2$ players are each given an input $x_i \in X_i$ $(i = 1, \ldots, k)$, and they require to compute a function $f : X_1 \times X_2 \times \cdots \times X_k \to \{0, 1\}$. Initially every player sees all the inputs except their own. The players then communicate by taking turns in writing one bit (0 or 1) on a blackboard. The communication ends when all the players know the value of $f(x_1, \ldots, x_k)$. The *cost* of a protocol is the maximal number of bits the players write on the blackboard during the computation of $f(x_1, \ldots, x_k)$, over all choices of inputs $(x_1, \ldots, x_k)$. The *deterministic communication complexity* of f, denoted $D_k(f)$, is equal to the minimal cost of a protocol for f.

We also denote by $N_k^1(f)$ the nondeterministic communication complexity of f in the k-players NOF model. Nondeterministic protocols are more powerful than deterministic ones. In addition to the input that is distributed between the players in the NOF fashion, in nondeterministic communication complexity the players also have access to a number of bits given by an all powerful prover. On input $(x_1, \ldots, x_k)$ such that $A(x_1, \ldots, x_k) = 1$ a correct protocol is required to have at least one nondeterministic choice (proof) for which the output of the protocol is 1. If $A(x_1, \ldots, x_k) = 0$ then all nondeterministic choices must lead to the output 0.

In randomized communication complexity the players are allowed to use random bits. The inputs are distributed as in the deterministic model, and the

players communicate the same way by writing on a blackboard. The next bit of each player is dependent on the part of the input that he sees, previous communication, and the random bits. At the end of the communication the players deduce the output from the communication transcript. Note that the output is now a random variable. It is required that the players deduce the correct value of $f(x_1, \ldots, x_k)$ with probability at least $2/3$ for every input $(x_1, \ldots, x_k)$.

A fundamental problem in multiparty communication complexity, as in many computational models, is to study the power of randomization. Beame, David, Pitassi and Woelfel [3] showed a non-constructive separation between randomized and nondeterministic NOF communication complexity. In fact they showed this gap in a very simple family of functions they called *graph functions*. A function $f : [n]^{k-1} \times [N] \to \{0,1\}$ [1] is a graph function if for every $(x_1, \ldots, x_{k-1})$ there is a unique $y \in N$ such that $f(x_1, \ldots, x_{k-1}, y) = 1$.

An advantage of graph functions, observed in [3] is that the randomized communication complexity of any graph function is $O(1)$. Thus, in order to separate randomized from nondeterministic communication complexity it is enough to prove a large lower bound on the nondeterministic communication complexity of any graph function. Beame et al [3] used an elegant counting argument to prove that most graph functions $f : [n]^{k-1} \times [N] \to \{0,1\}$ with $N \cong \sqrt{\frac{n}{k}}$ have nondeterministic communication complexity $\Omega(\log \frac{n}{k})$. It remains a challenging problem though to present an explicit function exhibiting a large gap, even for $k = 3$.

Another nice aspect of graph functions is that they can be alternatively viewed as a $(k-1)$-dimensional object. A graph function $f : [n]^{k-1} \times [N] \to \{0,1\}$ is associated with the function $A : [n]^{k-1} \to [N]$ defined by $A(x_1, \ldots, x_{k-1}) = y$ for the unique $y \in [N]$ satisfying $f(x_1, \ldots, x_{k-1}, y) = 1$. We let $A = Base(f)$ denote this base function, and also write $f = Lift(A)$. [2]

It is particularly hard to prove lower bounds for high-dimensional permutations and linjections [8] which are a special type of graph functions. For these functions $N \geq n$ while the results of [3] as well as ours apply only when $N \ll n$. For illustration, two-dimensional permutations are the class of functions $f : [n]^3 \to \{0,1\}$ for which $Base(f)$ is a Latin square. Improving the known lower bounds for permutations (even two-dimensional) imply strong applications even beyond the scope of communication complexity.

The highest lower bound for the communication complexity of an explicit graph function $f : [n]^{k-1} \times [N] \to \{0,1\}$ is $\Omega(\log \log n)$ proved in [3]. For permutations the best lower bound is $\Omega(\log \log \log n)$ for $k = 3$ proved in [8], and also in [4] for Exact-T functions which are a special type of permutations. These bounds are also closely related to the results of [6] and to Proposition 4.3 in [1]. For $k > 3$ the best lower bound for the communication complexity of any permutation is $\Omega(log^* n)$ [8].

The aim of this manuscript is to present another approach for proving lower bounds on the deterministic and nondeterministic communication complexity

[1] We assume here that the input space is $[n]^{k-1} \times [N]$. This is just for simplicity of presentation, and all the definitions and results hold for a general input space.

[2] In [3] a different notation is used, they write g instead of A and $f = graph^g$. We use the notation $f = Lift(A)$ since we consider other lift options in Section 6.

of graph functions. In particular we give an alternative proof to the $\Omega(\log\log n)$ bound of [3]. The bounds of [3], both constructive and non-constructive, use an observation that a nondeterministic protocol for a graph function can always be put in a special *normal form*. Namely, a graph function always has a very simple type of protocol in which one of the players is oblivious and the others send only one bit. This protocol was also previously used for a specific graph function by Chandra, Furst and Lipton in [5] and for a more general family of permutations in [4].

One way to tackle the problem of proving lower bounds on the deterministic and nondeterministic communication complexity of explicit graph functions, is to consider a relaxation of the model. The above mentioned one-way protocol for graph functions suggests to use the model of *communication complexity with help* defined by Babai, Hayes and Kimmel [2]. In this model k players wish to evaluate a function $A : [n]^k \to [N]$. A deterministic communication protocol with help is similar to the NOF protocol described earlier, with the addition of a "helper". Before the players start the communication on inputs $(x_1, \ldots, x_k)$, the helper sends them a help string of at most b bits, which can depend on any part of the input. The cost of a protocol is the maximal, over all inputs, of the length of the communication transcript, plus the length of the help string. The deterministic communication complexity with b help bits, denoted by $D^h_{k,b}(A)$, is the minimal cost of such a protocol for A.

Note that communication complexity with help is different than nondeterministic communication complexity in that the players in this model do not need to verify the information given by the helper, this is simply free information. Obviously, the helper can simply announce the value of the function with $\log N$ bits of information. Thus the interesting question is how much communication is needed when the helper gives less than $\log N$ bits.

Babai et al [2] used communication complexity with help in order to prove lower bounds on the one-way communication complexity of explicit functions. To prove the lower bounds they have defined a concept of multicolor discrepancy and used it as a lower bound for $D^h_{k,b}(A)$. They then computed the multicolor discrepancy of certain functions, thus providing lower bounds for the deterministic communication complexity with help of these functions. We exploit these bounds and translate them also to lower bounds on the deterministic complexity of explicit graph functions.

Let $f : [n]^{k-1} \times [N] \to \{0,1\}$ be a graph function, and let $A = Base(f)$. It is easy to check that $D_k(f) \leq D^h_{k-1,b}(A)+1$, for any natural number b. This upper bound holds even for the one-way model, where the last player sends a message and then the players communicate as usual but without the participation of the last player. Indeed the one-way NOF communication complexity model with k players is stronger than the model with help and $k-1$ players, since on input $(x_1, \ldots, x_k)$ the first $(k-1)$ players see the value on the forehead of the k-th player, which is essentailly $A(x_1, \ldots, x_{k-1})$, and need only validate it. In communication complexity with help on the other hand, the k-th player is replaced by the helper, and the rest of the players are required to compute $A(x_1, \ldots, x_{k-1})$.

Our first result is that for graph functions, the gap between these two models

cannot be arbitrary though, which makes this relaxation useful.

Theorem. *Let* $f : [n]^{k-1} \times [N] \to \{0,1\}$ *be a graph function and let* $A = Base(f)$. *Then*

$$D_k(f) \geq \min\{D^h_{k-1,b}(A) - (k-1)N, b\}.$$

The above lower bound, combined with the mentioned results of [2], can give a lower bound of $\Omega(\log\log n)$ on the deterministic communication complexity of explicit graph functions, matching the bound of [3].

Theorem. *There is an explicit graph function* $f : [n]^{k-1} \times [N] \to \{0,1\}$ *such that*

$$D_k(f) \geq \log N \geq \Omega(\log\log n - k).$$

Even though the above bound is tight, it is only applicable when N is at most $c \log n$ for some constant $c < 1$. The reason for this limitation is that the protocol that gives the lower bound iterates over all values $y \in [N]$ in order to find the unique value for which $f(x_1, \ldots, x_{k-1}, y) = 1$. A natural approach to break this barrier is to define and use nondeterministic communication complexity with help, which we do in Section 3. The bound $N^1_k(f) \leq N^h_{k-1,b}(A) + 1$ still naturally holds, and on the other hand we prove the following lower bound.

Theorem. *For every graph function* $f : [n]^{k-1} \times [N] \to \{0,1\}$ *it holds that*

$$N^1_k(f) \geq \min\{N^h_{k-1,b}(A) - \log N - k + 1, b\},$$

where $A = Base(f)$.

Nondeterministic communication complexity with help captures better the communication complexity of graph functions, and provides a lower bound that allows a much wider range for N. In fact, a tight lower bound for $N^h_{k-1,b}(A)$ can provide a tight lower bound for the communication complexity of the corresponding graph function $f : [n]^{k-1} \times [N] \to \{0,1\}$, as long as $N \ll n$. Recall that currently only exponentially smaller lower bounds are known. This makes proving lower bounds for this model an interesting question. The first place to look for such lower bounds, is to rely on the known bounds for the deterministic model. In the classical two players boolean model it is known that $D_2(f) \leq O(N^1_2(f)N^1_2(\bar{f}))$ for every function $f : [n]^2 \to \{0,1\}$. But the proof breaks down for communication complexity with help. Even for regular protocols, it is not clear whether this bound can be generalized to $k \geq 3$ players in the NOF model. It is also an interesting and nontrivial question whether multicolor discrepancy provides a good lower bound for nondeterministic communication complexity with help. The much weaker bound on nondeterministic communication complexity via deterministic complexity [7, Ex. 2.6] though, can be adapted also to the case of communication complexity with help.

Theorem. *Let* $A : [n]^k \to [N]$ *be a function and let* $b < \log N$ *be a natural number. Let* $D^h_{k,b}(A) = b + c_d$ *where* b *is the number of help bits and* c_d *is*

the number of subsequent bits of communication, in an optimal communication protocol. Similarly let $N^h_{k,b}(A) = b + c_n$, *then* [3]

$$c_d \leq (k-1)2^{c_n} + c_n.$$

This yields:

Theorem. *Let* $f : [n]^{k-1} \times [N] \to \{0,1\}$ *be a graph function, let* $A = Base(f)$, *and let* $b = \log N - 1$. *Then*

$$N^1_k(f) \geq \min\left\{\log\left(D^h_{k-1,b}(A) - \log N\right) - \log k - k, \log N\right\}.$$

Together with the discrepancy lower bound of [2], the above inequality implies that $N^1_k(f) \geq \Omega(\log\log n)$ for any graph function $f : [n]^{k-1} \times [N] \to \{0,1\}$ with a base function that has multicolor discrepancy smaller than $\frac{1}{N^{1+\Omega(1)}}$, similarly to the bounds of [3]. The techniques of [3] are different though and the underlying statement is complementary to ours. They prove that an optimal protocol requires $\Omega(\log\log n)$ help bits when the discrepancy is smaller than $\frac{1}{N^{1+\Omega(1)}}$. Our bound on the other hand says that regardless of the number of help bits, even if $\log N - 1$ help bits are given, the subsequent communication between the players has complexity $\Omega(\log\log n)$. We describe previous results in more detail in Section 5.

Finally, in Section 6 we briefly consider alternative Lift options for $A : [n]^k \to [N]$, other than the corresponding graph function.

2 Graph functions and deterministic communication complexity with help

We first prove the following lower bound and then apply it to give lower bounds on explicit graph functions.

Theorem 1. *Let* $f : [n]^{k-1} \times [N] \to \{0,1\}$ *be a graph function and let* $A = Base(f)$. *Then*

$$D_k(f) \geq \min\{D^h_{k-1,b}(A) - (k-1)N, b\}.$$

Proof. If $D_k(f) > b$ then we are done. Otherwise assume that $D_k(f) \leq b$, we show that in this case

$$D^h_{k-1,b}(A) \leq D_k(f) + (k-1)N.$$

To prove this lower bound, let P be an optimal communication protocol for f. We define the following protocol for A: On input $(x_1, \ldots, x_{k-1})$ the players iterate over all values $y \in [N]$, and check whether y is equal to $A(x_1, \ldots, x_{k-1})$. In

[3] According to the definition, the number of help bits can be smaller than b, we thus need to justify why there is always an optimal protocol with exactly b help bits. We remark on that at the end of Section 4.1.

each iteration, the players use as help-bits the transcript $\mathcal{T}$ of the run of the protocol P on $(x_1, \ldots, x_{k-1}, A(x_1, \ldots, x_{k-1}))$. Each player compares his actions according to the transcript $\mathcal{T}$ with his actions according to P on $(x_1, \ldots, x_{k-1}, y)$, and announces whether or not they agree. If for some player these actions do not agree this must mean that $y \neq A(x_1, \ldots, x_k)$.

Otherwise, since the actions of the k-th player do not depend on the k-th input, $\mathcal{T}$ is the transcript of a run of P both on $(x_1, \ldots, x_{k-1}, y)$ as well as on the input $(x_1, \ldots, x_{k-1}, A(x_1, \ldots, x_{k-1}))$. Since the transcript of the protocol determines its output, and A is a graph function, the players can find this way the unique value y for which $y = A(x_1, \ldots, x_k)$.

This protocol uses N rounds of communication, one round for each value $y \in [N]$. In each round the protocol uses $k-1$ bits of communication. In addition the protocol uses $D_k(f)$ help bits (Recall we have assumed that $D_k(f) \leq b$). Thus, $D^h_{k-1,b}(A) \leq (k-1)N + D_k(f)$ as required. □

Babai et al [2] proved a lower bound on distributional communication complexity with help in terms of multicolor discrepancy. They also gave explicit functions with low discrepancy.

Multicolor discrepancy Let $A : X \to Y$ be a function. For a subset $S \subset X$ and an element $y \in Y$, define

$$disc(A, S, y) = \left| |A^{-1}(y) \cap S| - |S|/|B| \right| / |X|.$$

The discrepancy of a set S is

$$disc(A, S) = \max_{y \in Y} disc(A, S, y).$$

The discrepancy of a set system $\mathcal{F}$ is defined as

$$disc(A, \mathcal{F}) = \max_{S \in \mathcal{F}} disc(A, S).$$

In words, discrepancy measures how much the size of $A^{-1}(y) \cap S$ deviates from what is expected from a random function A.

We are interested in the case where $X = [n]^{k-1}$, $Y = [N]$ and $\mathcal{F}$ is the family of cylinder intersections. We denote the discrepancy of a function $A : [n]^{k-1} \to [N]$ simply by $disc_{k-1}(A)$. The following bound is proved in [2].

Theorem 2 ([2]). *For every function* $A : [n]^{k-1} \to [N]$ [4]

$$D^h_{k-1,b}(A) \geq \log \left(\frac{1 - (2^b/N)}{disc_{k-1}(A)} \right).$$

An example of an explicit function with small discrepancy is

Definition 3 ([2]). *Let q be a prime power, and let d be a positive integer. Let M_d be the space of $d \times d$ matrices over $\mathbb{F}_q$. The function $T_{q,d,k} : M_d^k \to \mathbb{F}_q$ is defined by*

$$T_{q,d,k}(B_1, \ldots, B_k) = Tr(B_1 \cdot B_2 \cdot \ldots \cdot B_k).$$

[4] The result of [2] holds for distributional communication complexity with help, but we only need the deterministic model.

Lemma 4 ([2]). $-\log disc_k(T_{q,d,k}) \geq \Omega(\frac{d^2 \log q}{k^2 2^k})$.

Combining these facts with Theorem 1 gives:

Corollary 5. *Let N be a prime power, k be an integer, and take $d = c \cdot k^{3/2} 2^{k/2} \cdot \sqrt{\frac{N}{\log N}}$ for large enough c. Let $A = T_{N,d,k}$ and $f = Lift(A)$, then*

$$D_k(f) \geq \log N \geq \Omega(\log \log n - k),$$

where the domain of f is $[n]^{k-1} \times [N]$.

Proof. By Theorem 2 and Lemma 4

$$D^h_{k-1}(A) \geq c_1 \frac{d^2 \log N}{k^2 2^k},$$

for some constant $c_1 > 0$. But $c_1 \frac{d^2 \log N}{k^2 2^k} = c_1 c^2 kN$, therefore if we choose $c = c_1^{-1/2}$ then $c_1 c^2 = 1$ and $D^h_{k-1}(A) \geq kN$.

By Theorem 1

$$D_k(f) \geq \min\{\log N, D^h_{k-1}(A) - (k-1)N\}.$$

Thus

$$D_k(f) \geq \min\{\log N, N\} = \log N.$$

Finally notice that $n = 2^{d^2 \log N} = 2^{c^2 k^3 2^k N}$, is the size of the first $k-1$ players input space. Thus

$$\log \log n = \log N + k + 3 \log k + 2 \log c.$$

□

3 Nondeterministic communication complexity with help

The protocol in the proof of Theorem 1 iterates over values $y \in [N]$ in search of the correct value. This iteration adds an additive factor to the complexity, that is linear in N. It seems natural to consider nondeterministic complexity for such a search problem, as there is a potential of getting exponentially better lower bounds, and also improving the dependency on N. In this section we define nondeterministic communication complexity with help and use it to prove lower bounds on the deterministic NOF communication complexity of graph functions.

We define *nondeterministic communication complexity with help* of a function $A : [n]^k \to [N]$ similarly to deterministic communication. The difference is that the communication after receiving the help bits is nondeterministic. Namely, on input $(x_1, \ldots, x_k)$, after receiving the help string, the players also receive a proof from an all powerful prover, and are then required to compute the value of $A(x_1, \ldots, x_k)$. The output of the computation can either be the correct value or "don't know". It is required that for every input there is at least one choice of a nondeterministic string for which the protocol outputs the correct answer. We denote by $N^h_{k,b}(A)$ the nondeterministic communication complexity with help of A with b help bits. We also let $N_k(A) = N^h_{k,0}(A)$, be the nondeterministic communication complexity of A.

3.1 Bounds

Theorem 6. *Let $f : [n]^{k-1} \times [N] \to \{0,1\}$ be a graph function and let $A = Base(f)$. Then*

$$N^1_k(f) \geq \min\{N^h_{k-1,b}(A) - \log N - k + 1, b\}.$$

The proof is similar to the proof of Theorem 1, excluding the fact that here the deterministic search is replaced with a nondeterministic choice.

Proof. If $N^1_k(f) > b$ then the bound follows. Assume therefore that $N^1_k(f) \leq b$. We prove that in this case

$$N^h_{k-1,b}(A) \leq N^1_k(f) + \log N + k - 1.$$

The proof works by defining an efficient communication protocol for $N^h_{k-1,b}(A)$ based on a protocol for $N^1_k(f)$. Let P be an optimal nondeterministic communication protocol for f. We define the following protocol for A. On inputs $(x_1, \ldots, x_{k-1})$ the players guess an output $y \in [N]$, and then verify whether this is really the output. To verify whether y is the output, the players use as help-bits a transcript $\mathcal{T}$ of a run of the protocol P on input $(x_1, \ldots, x_{k-1}, A(x_1, \ldots, x_{k-1}))$, with nondeterministic choices that achieve the correct answer. Each player compares his actions according to the transcript $\mathcal{T}$ with his actions according to P on inputs $(x_1, \ldots, x_k, y)$, and announces whether or not they agree. If for some player these actions do not agree this must mean that $y \neq A(x_1, \ldots, x_{k-1})$ and thus the protocol outputs "don't know".

Otherwise, since the actions of the k-th player do not depend on the k-th input, $\mathcal{T}$ is the transcript of a run of P both on inputs $(x_1, \ldots, x_{k-1}, y)$ and on inputs $(x_1, \ldots, x_{k-1}, A(x_1, \ldots, x_{k-1}))$. By our choice of nondeterministic bits, and since the transcript of the protocol determines its output, if the protocol accepts it must be that $y = A(x_1, \ldots, x_{k-1})$. Note that here we use the fact that P makes only one-sided mistakes.

Finally, notice that this protocol uses $\log N + (k-1)$ bits of communication, and $N^1_k(f)$ help bits. We therefore conclude that $N^h_{k-1,b}(A) \leq N^1_k(k) + \log N + k - 1$. □

As in the deterministic and one-way models, it also holds that:

Theorem 7. *Let $f : [n]^{k-1} \times [N] \to \{0,1\}$ be a graph function and let $A = Base(f)$, then*

$$N^1_k(f) \leq N^h_{k-1,b}(A) + 1.$$

Proof. Given an input $(x_1, \ldots, x_k)$, the k-th player sees all inputs on the other player's foreheads, $(x_1, \ldots, x_{k-1})$. Thus, the last player can compute the help string and send it to the other players. The first $k-1$ players then use an optimal protocol for $N^h_{k-1,b}(A)$ to compute $A(x_1, \ldots, x_{k-1})$. If the result of the protocol is "don't know" then the first player outputs 0. After the first $k-1$ players compute $A(x_1, \ldots, x_{k-1})$ they compare it with x_k. If these quantities are equal the first player outputs 1, otherwise he outputs 0. This protocol requires $N^h_{k-1,b}(A) + 1$ bits of communication. Note that there is no restriction on b here. □

4 Lower bounds for explicit graph functions

We show in this section a lower bound on nondeterministic communication complexity with help in terms of deterministic complexity with help. This bound is a natural extension of the exponential bound known for the binary case of the two players traditional model [7, Ex. 2.6]. This bound enables to prove lower bounds on explicit graph functions for which the base function has relatively low multicolor discrepancy.

4.1 Partial functions

An alternative way to view communication complexity with b help bits is that we are allowed to partition the input space into at most 2^b parts and compute the complexity of the partial function confined to any of the parts, separately. The communication complexity with help is equal to the maximal complexity over these partial problems, plus the logarithm of the size of the partition.

For the formal definition we first recall the definition of the communication complexity of a partial function. Let $A : [n]^k \to [N]$ be a function and $S \subset [n]^k$ a subset of the inputs. The communication complexity of A restricted to S, denoted $CC(A, S)$, where CC is any communication complexity model, is defied similarly to $CC(A)$ with the exception that a protocol only needs to be correct on inputs that belong to S.

Now, let $A : [n]^k \to [N]$ be a function, and let b be a natural number, the communication complexity $D^h_{k,b}(A)$ is equal to

$$\min_{\mathcal{S}} \left(t + \max_{i=1,\ldots,2^t} D_k(A, S_i) \right),$$

where the minimum is over all partitions $\mathcal{S}$ of $[n]^k$ into 2^t subsets $\{S_1, S_2, \ldots, S_{2^t}\}$, with $t \leq b$. The partition $\mathcal{S}$ is defined by the help bits, all inputs in a single part S_i share the same help string.

The nondeterministic communication complexity $N^h_{k,b}(A)$ is defined similarly as

$$\min_{\mathcal{S}} \left(t + \max_{i=1,\ldots,2^t} N_k(A, S_i) \right).$$

The major difficulty in proving lower bounds on nondeterministic communication complexity with help is that the rectangles can intersect also outside the subset S_i, where there is no restriction on the value of the entries.

The number of help bits We note that we can assume without loss of generality that the number of help bits is exactly b. That is, the size of the partition is 2^b. We exhibit that on $N^h_{k-1,b}(A)$, the proof for $D^h_{k-1,b}(A)$ is similar.

Proof. Let P be an optimal communication protocol for $N^h_{k-1,b}(A)$. Let P_H be the help player's protocol and P_C the subsequent communication protocol. Namely, on input $(x_1, \ldots, x_{k-1})$ first the help player sends $P_H(x_1, \ldots, x_{k-1})$ to the players and then the transcript of their communication is given by $P_C(x_1, \ldots, x_{k-1})$. Let $N^h_{k-1,b}(A) = h + c$ where h is the maximal length of

a help string, and c is the maximal length of a transcript of P_C. Then, if $h < b$, we can change the protocols and add to the help string the initial $b-h$ communication bits of the transcript given by P_C, since the helper knows everything. Thus, we can assume without loss of generality that $h = b$. □

4.2 Cylinder intersections

A key definition in multiparty communication complexity is that of a cylinder intersection. We say that $C \subseteq X_1 \times \cdots \times X_k$ is a *cylinder in the i-th coordinate* if membership in C does not depend on the i-th coordinate. Namely, for every $x, x' \in X_i$ there holds $(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_k) \in C$ iff $(a_1, \ldots, a_{i-1}, x', a_{i+1}, \ldots, a_k) \in C$. A cylinder intersection is a set C of the form $C = \cap_{i=1}^{k} C_i$ where C_i is a cylinder in the i-th coordinate.

Following are some well known basic facts regarding the relation between cylinder intersections and communication complexity:

Lemma 8 ([7]). *There holds*

1. *Let $C = \cap_{i=1}^{k} C_i$ be a cylinder intersection in $X_1 \times \cdots \times X_k$ and let $\mathbf{x} \in X_1 \times \cdots \times X_k$. Then $\mathbf{x} \in C$ if and only if $\mathbf{x} \in C_i$ for all $i \in [k]$.*
2. *The above fact gives a one round protocol to determine membership in a cylinder intersection $C = \cap_{i=1}^{k} C_i$. Given an input $\mathbf{x} \in X_1 \times \cdots \times X_k$ player i checks whether $\mathbf{x} \in C_i$, and transmits 1 if it is true and 0 otherwise. It holds that $\mathbf{x} \in C$, if and only if all players transmitted 1.*
3. *Let $A : [n]^k \to [N]$ be a function, and let $S \subset [n]^k$ be a subset of the entries. An optimal protocol for $N_k(A, S)$ induces a cover of $[n]^k$ by at most $2^{N_k(A,S)}$ cylinder intersections that are monochromatic with respect to A on S.*

4.3 Determinism versus nondeterminism

Theorem 9. *Let $A : [n]^k \to [N]$ be a function and let $b < \log N$ be a natural number. Let $D^h_{k,b}(A) = b + c_d$ where b is the number of help bits and c_d is the number of subsequent bits of communication, in an optimal communication protocol. Similarly let $N^h_{k,b}(A) = b + c_n$, then*

$$c_d \leq (k-1)2^{c_n} + c_n.$$

Theorem 9 is a direct consequence of the following lemma.

Lemma 10. *Let $A : [n]^k \to [N]$ be a function and let $S \subset [n]^k$, then*

$$D_k(A, S) \leq (k-1)2^{N_k(A,S)} + N_k(A, S).$$

Proof of Lemma 10. Let $\chi = 2^{N_k(A,S)}$ and let $\{C^j\}_{j=1}^{\chi}$ be an optimal cover for $N_k(A, S)$ that exists by Lemma 8 (part 3). That is, a cover of $[n]^2$ into χ cylinder intersections that are monochromatic on S with respect to A.

On input $(x_1, \ldots, x_k) \in S$ the players then do the following:

1. For $i = 1, \ldots, k$: Player i computes the vector $V_i \in \{0,1\}^\chi$, whose jth coordinate is equal to 1 if and only if $(x_1, \ldots, x_k)$ belongs to C_i^j
2. The i-th player writes V_i on the blackboard, for $i = 1, \ldots, k-1$.
3. The k-th player publishes the index of a cylinder intersection C^j that contains $(x_1, \ldots, x_k)$.

Since $\{C^j\}_{j=1}^\chi$ is a cover for $N_k(A, S)$, there exists a cylinder intersection C_j that contains $(x_1, \ldots, x_k)$. By Lemma 8 (part 1), C_j contains $(x_1, \ldots, x_k)$ if and only if the jth coordinate of V_i is equal to 1 for every $i = 1, \ldots, k$. Since $\{C^j\}_{j=1}^\chi$ is also monochromatic on S, the above protocol is correct, and when it ends all players know $A(x_1, \ldots, x_k)$.

The first step requires no communication, the second step uses $(k-1)\chi$ bits, and in the last step the k-th player writes $\log \chi$ bits on the board. The total number of bits in a communication is $(k-1)\chi + \log \chi$. Since $\chi = 2^{N_k(A,S)}$ the claim follows. □

Proof of Theorem 9. Let $H = 2^b$ and let $\mathcal{S} = \{S_1, S_2, \ldots, S_H\}$ be a partition that achieves the optimal complexity for $N_{k,b}^h(A)$. Namely,

$$c_n = \max_{i=1,\ldots,H} N_k(A, S_i).$$

By Lemma 10, for every $i = 1, \ldots, H$ it holds that

$$D_k(A, S_i) \leq (k-1)2^{N_k(A,S_i)} + N_k(A, S_i) \leq (k-1)2^{c_n} + c_n.$$

In particular

$$c_d \leq \max_{i=1,\ldots,H} D_k(A, S_i) \leq (k-1)2^{c_n} + c_n.$$

□

4.4 A weak lower bound via multicolor discrepancy

We prove a weak lower bound using deterministic communication complexity with help, the lower bound via multicolor discrepancy then follows from Lemma 2.

Theorem 11. *Let $f : [n]^{k-1} \times [N] \to \{0,1\}$ be a graph function, let $A = Base(f)$, and let $b = \log N - 1$. Then*

$$N_k^1(f) \geq \min\left\{\log\left(D_{k-1,b}^h(A) - \log N\right) - \log k - k, \log N\right\}.$$

Proof. Let $N_{k-1,b}^h(A) = (\log N - 1) + c_n$, where c_n is the number of communication bits after the help string is given, similarly let $D_{k-1,b}^h(A) = (\log N - 1) + c_d$. Recall from the remark at the bottom of Section 4.1, we can assume without loss of generality that the number of help bits is exactly $b = \log N - 1$.

By Theorem 9, it holds that

$$c_d \leq (k-1)2^{c_n} + c_n \leq k2^{c_n}.$$

Thus,

$$c_n \geq \log c_d - \log k \geq \log\left(D^h_{k-1,b}(A) - \log N\right) - \log k.$$

Finally note that by Theorem 6,

$$N^1_k(f) \geq \min\{N^h_{k-1,b}(A) - (\log N - 1) - k, \log N\} = \min\{c_n - k, \log N\}.$$

□

5 Previous results, a closer look

In this section we review previous results in more detail. We start with a few more of the properties of graph functions, that we need in order to describe the previous results. A pleasant aspect of the study of graph functions is that the communication complexity is completely characterized by *stars*. For simplicity we describe this notion for the case $k = 3$. A star is a triplet $(x, y, z'), (x', y, z), (x, y', z)$ of points in $[n]\times[n]\times[N]$ such that $x \neq x'$, $y \neq y'$ and $z \neq z'$. In the 2-dimensional case stars become what is called an *A-star* [8]. The star $(x, y, z'), (x', y, z), (x, y', z)$ correspond to the A-star $(x, y), (x', y), (x, y')$, which is a triplet of distinct points such that $A(x', y) = A(x, y') = z$ and $A(x, y) = z' \neq z$.

Let $f : [n]^{k-1} \times [N] \to \{0, 1\}$ be a graph function and let $A = Base(f)$. The communication complexity of f, $D_k(f)$, is equal almost precisely to the minimal number of colors needed to color the entries of A so that no A-star is monochromatic [5, 4, 8]. It is also observed in [3] (see also [8]) that $D_k(f)$, $N^1_k(f)$ and $D^1_k(f)$ are equivalent up to a small additive factor. Hence, any result on the deterministic communication complexity of a graph function also holds (perhaps with slight change) for the nondeterministic and one-way complexity, and vice versa.

As mentioned earlier previous known bounds are: (i) a lower bound of $\Omega(\log\log n)$ for the communication complexity of explicit graph functions $f : [n]^{k-1} \times [N] \to \{0, 1\}$ with $N \ll n$ [3], (ii) an $\Omega(\log\log\log n)$ lower bounds for the communication complexity of any two-dimensional permutation [1, 6, 4, 8]. For higher-dimensional permutations the best lower bound is $\Omega(log^* n)$ [8], but it is outside the scope of techniques discussed here.

All the above mentioned lower bounds, either for graph functions [3] or for two-dimensional permutations [1, 6, 4, 8] use the following general lower bound technique. For simplicity we sketch the technique for the case $k = 3$. Let $f : [n]^2 \times [N] \to \{0, 1\}$ be a graph function, and let $A = Base(f)$. Assume that $D_3(f) \leq \log L$ for some natural number L. This means that it is possible to color the entries of A with L colors, so that no A-star is monochromatic. Following is an outline of a general lower bound technique for L:

1. Let $E = [n]^2$ and $V = \emptyset$.
2. While E contains entries whose value does not appear in V, do:
   (a) Pick v, the most frequent value from $[N] \setminus V$ that appears in E.
   (b) Pick $c \in [L]$, the most abundant color among E's v-entries.
   (c) Let $S \subset E$ be the subset of entries with value v and color c. Clearly, $|S| \geq |E|/(NL)$.
   (d) Let $\bar{S}$ be the minimal combinatorial rectangle that contains S.
   (e) Set $E = \bar{S}$, $V = V \cup \{v\}$.

The heart of this lower bound technique is the fact that the entries of $\bar{S} \setminus S$ cannot be colored by the color c or else there would be a monochromatic A-star. Thus L, the number of required colors, is at least the number of iterations of the above loop. To prove a lower bound on the number of such iterations, it is necessary to prove a lower bound on the size of the enclosing combinatorial rectangle $\bar{S}$. This bound on $\bar{S}$ determines the quality of the bound on L achieved using the above technique.

The lower bounds of [3] on the deterministic communication complexity of explicit graph functions, and the lower bounds in [8] on the deterministic communication complexity of permutations, and also related bounds [4], [6] and [1, Proposition 4.3], all follow the above scheme. In [3] they use multicolor discrepancy [2] to bound the size of $\bar{S}$, while in [8] and the related works, the structural properties of a permutation are used to this end.

The structural properties of permutations imply that $|\bar{S}| = |S|^2$, which gives the lower bound $\Omega(\log\log\log n)$. Discrepancy on the other hand gives better estimates on $\bar{S}$ and yields the bound $\Omega(\log\log n)$ on the communication complexity, which is perhaps the limit of this general technique. Another strong advantage of using discrepancy is that the bound works also for $k > 3$, and not only for $k = 3$. But the use of discrepancy seems limited to the case where $N \ll n$. Thus, improving the known lower bounds on explicit graph functions as well as specifically the much more limited bounds known for permutations, seems to require new ideas.

Note that even though the results of [3] are similar to ours regarding the lower bound that is achieved on the communication complexity of explicit graph functions, the techniques are different. In fact the statements are in a way complementary as we now explain. Let $f : [n]^{k-1} \times [N] \to \{0,1\}$ be a graph function whose base function has discrepancy smaller than $O(\frac{1}{N^{1+\epsilon}})$, for some $\epsilon > 0$. Let $N^h_{k-1,b}(Base(f)) = h + c$, where h is the size of the help string and c is the length of communication needed after the help string is given. In [3] it is proved that as long as h is much smaller than a constant times $\log\log n$ then c is significantly larger than $\log N$. The bounds via nondeterministic communication complexity with help on the other hand says that regardless of h, it might even be that $h = \log N - 1$, c is at least $\Omega(\log\log n)$.

6 One round communication complexity and communication complexity with help

Let $A : [n]^{k-1} \to [N]$ be a function. We have defined $f = Lift(A)$ as the graph function associated with A, and showed that $D_k(f)$ is strongly related to the nondeterministic communication complexity with help of A. In a way, when we go from A to f we represent the value in each entry of A by a boolean vector which is the unary representation of this value. Denote this representation by $f = Lift_U(A)$, it is possible to consider other representations as well:

1. $f = Lift_B(A)$ is the function $f : [n]^{k-1} \times [N] \to \{0,1\}$ where $f(x_1, \ldots, x_{k-1}, i)$ is equal to the ith bit in the binary representation of $A(x_1, \ldots, x_{k-1})$.
2. $f = Lift_{GT}(A)$ is the function $f : [n]^{k-1} \times [N] \to \{0,1\}$ satisfying $f(x_1, \ldots, x_k - 1, y) = 1$ iff $A(x_1, \ldots, x_{k-1}) \geq y$.

The representation $f = Lift_B(A)$ was considered in [2] in order to prove lower bounds on the one-way communication complexity of f in the NOF model, denoted $D^1_k(f)$. In fact, they mention this was one of the motivations for their paper. Similarly to the unary representation, it is not hard to check that $D^1_k(f) \leq D^h_{k-1,b}(A) + 1$. It is proved in [2] that this relation goes both ways as long as b is not too large.

Lemma 12 ([2]). *Let $A : [n]^{k-1} \to [N]$ be a function, and let $f = Lift_B(A)$. Then*

$$D^1_k(f) \geq \min\{\frac{1}{b} D^h_{k-1,b}(A), b\}.$$

In the binary representation the last dimension of f is small, $\log N$. This was an advantage for [2] as one of their main applications was to show that $D^1(f)$ can vary significantly when different players are allowed to speak first. But for the purpose of separating deterministic from randomized communication complexity this is a disadvantage, since then $D_k(f)$ is bounded by $\log \log N$. A way to remedy this is to consider the representation $f = Lift_{GT}(A)$.

The representation $f = Lift_{GT}(A)$ is useful for our purposes since the dimensions are not limited and also $R_k(f) \leq \log \log N$ by a simple reduction to the two players "greater than" function. Similarly to the binary representation, the communication complexity with help of A is also closely related to one-way communication complexity of f. It is again not hard to verify that $D^1_k(f) \leq D^h_{k-1,\log N - 1}(A) + 1$, and on the other hand:

Lemma 13. *Let $A : [n]^{k-1} \to [N]$ be a function, and let $f = Lift_{GT}(A)$. Then*

$$D^1_k(f) \geq \min\{\frac{1}{\log N} D^h_{k-1,\log N - 1}(A), \log N\}.$$

Proof. If $D^1_k(f) \geq \log N$ then we are done. Otherwise, Alice and Bob perform a binary search for the value of $A(x_1, \ldots, x_{k-1})$. They use as a help string the transcript of the k-th player on input $(x_1, \ldots, x_{k-1}, A(x_1, \ldots, x_{k-1}))$, in an optimal protocol for $D^1_k(f)$.

Note that the transcript of the k-th player is independent of the k-th input, and also independent of the other players transcript (as the protocol is one-way).

Thus the players can use this transcript to compute $f(x_1, \ldots, x_{k-1}, y)$ for any $y \in [N]$. Each such computation would require at most $D^1_k(f)$ bits of computation. Using a binary search and at most $D^1_k(f) \log N$ bits of communication, the players can compute this way the value of $A(x_1, \ldots, x_{k-1})$. □

A simple observation is that $D^1_k(Lift_U(A)) \leq 2D^1_k(Lift_{GT}(A))$. Similarly, it also holds that $D_k(Lift_U(A)) \leq 2D_k(Lift_{GT}(A))$ which means that the vast majority of functions $f = Lift_{GT}(A)$ are also good candidates for separating randomized from deterministic communication complexity, as graph functions are.

7 Discussion and open problems

Proving lower bounds on the deterministic communication complexity of explicit graph functions $f : [n]^{k-1} \times [N] \to \{0, 1\}$ is one of the most elementary open problems in the Number On The Forehead model. Still, proving such a bound would most likely require new techniques that will help with other problems in this area as well, and in fact also in other areas. The deterministic NOF communication complexity of permutations and linjections for example, which are a special family of graph functions, have strong relations with well studied problems in other mathematical fields, and proving lower bound therein can have very interesting consequences such as lower bounds for the multidimensional Szemerédi theorem and *corners theorems*, lower bounds on the density of Ruzsa-Szemerédi graphs, a combinatorial proof for the Hales-Jewett theorem, and more. See e.g. [5, 4, 8, 9] for more details.

The best open problems are to prove stronger lower bound than $\Omega(\log \log n)$ on any explicit graph function, improve the $\Omega(\log \log \log n)$ lower bound for a two-dimensional permutation, or the much weaker bounds for higher-dimensional permutations. But there are also other related problems that are interesting, we list a few of them:

1. Determine the relation between nondeterministic communication complexity with help, and multicolor discrepancy.
2. Determine the relation between nondeterministic communication complexity with help, and deterministic communication complexity with help.
3. What is the maximal gap between $D^1_k(Lift_{GT}(A))$ and $D_k(Lift_{GT}(A))$ for a function $A : [n]^{k-1} \to [N]$? Any relation would enable to use Lemma 13 to lower bound $D_k(Lift_{GT}(A))$.
4. Find an explicit function $A : [n]^2 \to [N]$ with small discrepancy and large enough N, for which the gap between $D^1_k(Lift_{GT}(A))$ and $D_k(Lift_{GT}(A))$ is small.
5. What is the maximal gap between $D^1_k(Lift_U(A))$ and $D^1_k(Lift_{GT}(A))$ for a function $A : [n]^{k-1} \to [N]$? Again, if there is a strong relation then Lemma 13 gives a bound on $D_k(Lift_U(A))$ since for graph functions one-way communication is as strong as regular protocols.

6. Find an explicit function $A : [n]^2 \to [N]$ with small discrepancy and large enough N, for which the gap between $D^1_k(Lift_U(A))$ and $D^1_k(Lift_{GT}(A))$ is small.

References

[1] N. Alon, A. Moitra, and B. Sudakov. Nearly complete graphs decomposable into large induced matchings and their applications. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 1079–1090. ACM, 2012.

[2] L. Babai, T. Hayes, and P. Kimmel. The cost of the missing bit: communication complexity with help. *Combinatorica*, 21:455–488, 2001.

[3] P. Beame, M. David, T. Pitassi, and P. Woelfel. Separating deterministic from randomized nof multiparty communication complexity. In *Proceedings of the 34th International Colloquium On Automata, Languages and Programming*, Lecture Notes in Computer Science. Springer-Verlag, 2007.

[4] R. Beigel, W. Gasarch, and J. Glenn. The multiparty communication complexity of exact-t: Improved bounds and new problems. In *International Symposium on Mathematical Foundations of Computer Science*, pages 146–156. Springer, 2006.

[5] A. Chandra, M. Furst, and R. Lipton. Multi-party protocols. In *Proceedings of the 15th ACM Symposium on the Theory of Computing*, pages 94–99. ACM, 1983.

[6] R. Graham and J. Solymosi. Monochromatic equilateral right triangles on the integer grid. In *Topics in discrete mathematics*, pages 129–132. Springer, 2006.

[7] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.

[8] N. Linial and A. Shraibman. On the communication complexity of high-dimensional permutations. *arXiv preprint arXiv:1706.02207*, 2017.

[9] A. Shraibman. A note on multiparty communication complexity and the hales-jewett theorem. *arXiv preprint arXiv:1706.02277*, 2017.