Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 16 (2022)

Super-cubic lower bound for generalized Karchmer–Wigderson games

Artur Ignatiev[*], Ivan Mihajlin[†], Alexander Smal[‡]

December 6, 2022

Abstract

In this paper, we prove a super-cubic lower bound on the size of a communication protocol for generalized Karchmer–Wigderson game for an explicit function $f : \{0,1\}^n \to \{0,1\}^{\log n}$. Lower bounds for original Karchmer–Wigderson games correspond to De Morgan formula lower bounds, thus the best known size lower bound is cubic. The generalized Karchmer–Wigderson games are similar to the original ones, so we hope that our approach can provide an insight for proving better lower bounds on the original Karchmer–Wigderson games, and hence for proving new lower bounds on De Morgan formula size.

To achieve super-cubic lower bound we adapt several techniques used in formula complexity to communication protocols, prove communication complexity lower bound for a composition of several functions with a multiplexer relation, and use a technique from [17] to extract the "hardest" function from it. As a result, in this setting we are able to show that there is a relatively small set of functions such that at least one of them does not have a small protocol. The resulting lower bound of $\tilde{\Omega}(n^{3.156})$ is significantly better than the bound obtained from the counting argument.

1 Introduction

1.1 Background

The circuit complexity of Boolean functions is one of the classical areas of complexity theory. Initially, the study of this area was considered as an easier way to prove $\mathsf{P} \neq \mathsf{NP}$. In fact, proving bounds on circuit size seems to be much easier than proving bounds on the number of steps that some Turing machine does. The desire to prove lower bounds on circuit complexity has attracted many brilliant researchers. The seeming simplicity of this problem turned out to be deceiving. From the Shannon's counting argument we know that a random Boolean function on n inputs has circuit complexity at least $2^{n-o(n)}$ with probability almost 1. At the same time, we do not know any explicit function that does not have linear-sized circuits. Despite over 60 years of attempts, it is still not clear how to prove even more modest lower bounds — we do not know explicit functions

[*]St.Petersburg University, Russia; HSE University, St.Petersburg, Russia, artur.ignatev23924@gmail.com

[†]St.Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences, Russia, ivmihajlin@gmail.com

[‡]St.Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences, Russia; Technion, Haifa, Israel, smal@pdmi.ras.ru

ISSN 1433-8092

that does not have circuits of size less than $4n$. The best known lower bound for unrestricted Boolean circuits shows that there is a function that can not be computed by a circuit of size less than $(3+\epsilon)n$ [4, 16]. A slightly better lower bound of $5n-o(n)$ [10] can be obtained if we consider circuits without parity gates.

The desire to learn how to prove lower bounds on circuits motivates us to study more restricted models. One of the most important such models is De Morgan formulas. In contrast to circuit complexity, in formula complexity we know how to prove superlinear lower bounds. Moreover, we know that there is an explicit function that does not have formulas of size $\tilde{\Omega}(n^3)$ [7]. This lower bound is the result of more than 40 years of research starting with works of Subbotovskaya [20] and Khrapchenko [14]. Improving this lower bound is the central challenge in formula complexity.

Karchmer, Raz, and Wigderson [12] suggested an approach for proving super-polynomial formula size lower bound for a Boolean function from class P. The idea of this approach is to study the formula complexity of *the block-composition* of Boolean functions.

Definition 1. Let $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ be Boolean functions. *The block-composition* $f \diamond g : \{0,1\}^{nm} \to \{0,1\}$ is defined by

$$(f \diamond g)(x_1, \ldots, x_m) = f(g(x_1), \ldots, g(x_m)),$$

where $x_1, \ldots, x_m \in \{0,1\}^n$.

Let $\mathrm{D}(f)$ denote the minimal depth of De Morgan formula for function f. It is easy to show that $\mathrm{D}(f \diamond g) \leq \mathrm{D}(f) + \mathrm{D}(g)$ by constructing a formula for $f \diamond g$ by substituting every variable in a formula for f with a copy of formula for g. Karchmer, Raz, and Wigderson [12] conjectured that this upper bound is roughly optimal.

Conjecture 2 (The KRW conjecture)**.** *Let $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ be non-constant functions. Then*

$$\mathrm{D}(f \diamond g) \approx \mathrm{D}(f) + \mathrm{D}(g).$$

If the conjecture is true then there is a polynomially computable function that does not have De Morgan formula of polynomial size, and hence $\mathsf{P} \not\subseteq \mathsf{NC}^1$. Consider the function $h : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, which interprets its first input as a truth table of a function $f : \{0,1\}^{\log n} \to \{0,1\}$ and computes the value of the block-composition of $\log n / \log\log n$ functions f on its second input (note that '$\diamond$' is associative):

$$h(f, x) = (\underbrace{f \diamond \cdots \diamond f}_{\log n/\log\log n})(x).$$

It is not hard to see that $h \in \mathsf{P}$. To show that $h \notin \mathsf{NC}^1$, let $\tilde{f}$ be a function with maximal depth complexity. By Shannon's counting argument $\tilde{f}$ has depth complexity roughly $\log n$. Assuming the KRW conjecture, $\tilde{f} \diamond \cdots \diamond \tilde{f}$ has depth complexity roughly $\log n \cdot (\log n / \log\log n) = \omega(\log n)$, and hence $\tilde{f} \diamond \cdots \diamond \tilde{f} \notin \mathsf{NC}^1$. Any formula for h must compute $\tilde{f} \diamond \cdots \diamond \tilde{f}$ if we hard-wire $f = \tilde{f}$ in it, so $h \notin \mathsf{NC}^1$. This argument is especially attractive since it does not seem to break any known meta mathematical barriers such as the concept of "natural proofs" by Razborov and Rudich [19] (the function h is very special, so the argument does not satisfy "largeness" property). It is worth noting that the proof would work even assuming some weaker version of the KRW conjecture, like $\mathrm{D}(f \diamond g) \geq \mathrm{D}(f) + \epsilon \cdot \mathrm{D}(g)$ or $\mathrm{D}(f \diamond g) \geq \epsilon \cdot \mathrm{D}(f) + \mathrm{D}(g)$ for some $\epsilon > 0$. Also, it is not necessary to prove the KRW conjecture for all pairs of functions — it would be enough to show that for every f there exists a hard function g such that $\mathrm{D}(f \diamond g) \approx \mathrm{D}(f) + \mathrm{D}(g)$.

The seminal work of Karchmer and Wigderson [13] established a correspondence between De Morgan formulas for non-constant Boolean function f and communication protocols for the Karchmer–Wigderson game for f.

Definition 3. *The Karchmer–Wigderson game (KW game)* for Boolean function $f : \{0,1\}^n \to \{0,1\}$ is the following communication problem: Alice gets an input $x \in \{0,1\}^n$ such that $f(x) = 0$, and Bob gets as input $y \in \{0,1\}^n$ such that $f(y) = 1$. Their goal is to find a coordinate $i \in [n]$ such that $x_i \neq y_i$. The KW game can be considered as a communication problem for *the Karchmer–Wigderson relation for* f:

$$\mathrm{KW}_f = \{(x, y, i) \mid x, y \in \{0,1\}^n, i \in [n], f(x) = 0, f(y) = 1, x_i \neq y_i\}.$$

Karchmer and Wigderson showed that the communication complexity of KW_f is exactly equal to the formula depth complexity of f. This correspondence allows us to use communication complexity methods for proving formula depth lower bounds. In fact, Conjecture 2 can be reformulated in terms of communication complexity of the Karchmer–Wigderson game for the block-composition of two arbitrary Boolean functions. Let $\mathrm{CC}(R)$ denote deterministic communication complexity of relation R. This leads to the following reformulation of the KRW conjecture.

Conjecture 4 (The KRW conjecture (reformulation))**.** *Let $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ be non-constant functions. Then*

$$\mathrm{CC}(\mathrm{KW}_{f \diamond g}) \approx \mathrm{CC}(\mathrm{KW}_f) + \mathrm{CC}(\mathrm{KW}_g).$$

The study of Karchmer–Wigderson games had already been shown to be a potent tool in the monotone setting — the monotone KW games were used to separate then monotone counterpart of classes NC^1 and NC^2 [12]. Therefore, there is reason to believe that the communication complexity perspective might help to prove new lower bounds in the non-monotone setting.

In a series of works [3, 8, 6, 2] several steps were taken towards proving the KRW conjecture. In the last paper of this series [2] the authors presented an alternative proof for the block-composition of an arbitrary function with the parity function in the framework of the Karchmer–Wigderson games (this result was originally proved in [7] using an entirely different approach). Their result gives an alternative proof of the cubic formula size lower bound for Andreev's function [7].

In [17], the authors proposed a new conjecture, the XOR-KRW conjecture, which is a relaxation of the KRW conjecture. This relaxation is still strong enough to imply $\mathsf{P} \not\subseteq \mathsf{NC}^1$ if proven. They also presented a weaker version of this conjecture that might be used for breaking n^3 lower bound for De Morgan formulas. The conjecture employs an alternative composition operation.

Definition 5. For any $n, m, k \in \mathbb{N}$ with $k \mid n$, and functions $f : \{0,1\}^n \to \{0,1\}$ and $g_1, \ldots, g_m : \{0,1\}^k \to \{0,1\}^k$ *the XOR-composition* $f \boxplus_m g : \{0,1\}^{nm} \to \{0,1\}$ is defined by

$$(f \boxplus_m (g_1, \ldots, g_m))(x_{1,1}, \ldots, x_{n/k,m}) = \\ f\left(g_1(x_{1,1}) \oplus \cdots \oplus g_m(x_{1,m}), \ldots, g_1(x_{n/k,1}) \oplus \cdots \oplus g_m(x_{n/k,m})\right),$$

where $x_{i,j} \in \{0,1\}^k$ for all $i \in [n/k]$ and $j \in [m]$, and $\oplus$ denotes bit-wise XOR.

The authors suggested the following general version of the XOR-KRW conjecture and showed that it implies separation of P and NC^1.

Conjecture 6 (The XOR-KRW conjecture)**.** *There exist $m \in \mathbb{N}$ and $\epsilon > 0$, such that for all natural $n, k \in \mathbb{N}$ with $k \mid n$, and every non-constant $f : \{0,1\}^n \to \{0,1\}$, there exists $g : \{0,1\}^k \to \{0,1\}^k$ such that $\mathrm{D}(f \boxplus_m g) \geq \mathrm{D}(f) + \epsilon k - O(1)$.*

In [17], the authors suggested focusing on the specific case of $k = n$ and $m = 2$, which might be enough to prove a super-cubic formula size lower bound for a specific formula. In this setting, the authors considered a communication problem that correspond to a universal relation XOR-composed with the Karchmer–Wigderson relation for some function $g : \{0,1\}^n \to \{0,1\}^n$ and proved $1.5n - o(n)$ lower bound on its communication complexity. As an implication of this result, the authors showed the same lower bound on the communication complexity of a universal relation block-composed with the Karchmer–Wigderson relation for some function $g : \{0,1\}^n \to \{0,1\}$.

In this work, we extend the latter result in multiple directions. First of all, we refine the lower bound from [17] such that it works for arbitrary $m \geq 2$. Second, we use this lower bound to prove a super-cubic lower bound on the size of communication protocol for a generalized Karchmer–Wigderson game for some function $f : \{0,1\}^n \to \{0,1\}^{\log n}$.

Definition 7. *The generalized Karchmer–Wigderson game (generalized KW game)* for function $f : \{0,1\}^n \to \{0,1\}^r$ is the following communication problem: Alice gets an input $x \in \{0,1\}^n$, Bob gets $y \in \{0,1\}^n$, and they are promised that $f(x) \neq f(y)$. Their goal is to find a coordinate $i \in [n]$ such that $x_i \neq y_i$. This problem corresponds to a communication problem for *the generalized Karchmer–Wigderson relation for f*:

$$\mathrm{KW}_f = \{(x, y, i) \mid x, y \in \{0,1\}^n, i \in [n], f(x) \neq f(y), x_i \neq y_i\}.$$

We show that the following theorem holds.

Theorem 8. *There exists a function $f : \{0,1\}^n \to \{0,1\}^{\log n}$ such that any communication protocol for generalized Karchmer–Wigderson game for f has size at least $\tilde{\Omega}(n^{3.156})$.*

To achieve this we extend Håstad's technique [7] to work with communication protocols for generalized Karchmer–Wigderson games.

A universal relation of size n [3] is exactly the generalized Karchmer–Wigderson game for the identity function $\mathrm{Id}_n : \{0,1\}^n \to \{0,1\}^n$: $\mathrm{U}_n = \{(x, y, i) \mid x, y \in \{0,1\}^n, i \in [n], x_i \neq y_i\}$. It is known, that U_m requires m bit of communication. So, one can show that generalized Karchmer–Wigderson game for a function $\{0,1\}^n \to \{0,1\}^m$ that computes Id_m of the first m bits of its input also requires m bits of communication. For this reason it is crucial that we focus on the regime of $\{0,1\}^n \to \{0,1\}^{\log n}$, where such an informal argument gives a relatively low bound.

1.2 Organization of the paper

In Section 2, we prove a lower bound for the XOR-composition of Id_n with multiple functions. In Section 3, we use the results of Section 2 to prove the super-cubic lower bound on the protocol size. Section 4 contains a conclusion and a list of open problems. Some parts of the proofs are presented in appendix. In Appendix A, we present the proof of Technical Lemma used in Section 2. In Appendix B, we show that any formula balancing technique that preserves monotonicity can be also used for communication protocols. In Appendix C, we define restrictions for generalized Karchmer–Wigderson games and show that we can use The Main Shrinkage Theorem from [7] to bound the expected size of a protocol after it has been hit with a random restriction.

2 Lower bound for $\mathrm{CC}(\mathrm{KW}_{\mathrm{Id}_n \boxplus_m g})$

In this section, we abuse the notation in the following way: talking about communication complexity of a generalized Karchmer–Wigderson game for some function f we write $\mathrm{CC}(f)$ instead of $\mathrm{CC}(\mathrm{KW}_f)$, and use the same notation to denote a XOR-composition of functions and the corresponding generalized Karchmer–Wigderson game.

We are going to only focus on the special case of XOR-composition with $k = n$ and prove the following theorem. (Note that Id_n can be replaced with any permutation function.)

Theorem 9. *For all $n, m \in \mathbb{N}$, there exists $g : \{0,1\}^n \to \{0,1\}^n$ such that*

$$\mathrm{CC}(\mathrm{Id}_n \boxplus_m g) \geq (2 - 2^{-m+1})n - O(\log n).$$

It is convenient for the proof to extend the definition of XOR-composition to allow m different functions instead of one function applied to m arguments.

Definition 10. For any $n, m \in \mathbb{N}$ and functions $f, g_1 \dots, g_m : \{0,1\}^n \to \{0,1\}^n$ *the XOR-composition* $f \boxplus (g_1, \dots, g_m) : \{0,1\}^{nm} \to \{0,1\}^n$ is defined by

$$\big(f \boxplus (g_1, \dots, g_m)\big)(x_1, \dots, x_m) = f\big(g_1(x_1) \oplus \dots \oplus g_m(x_m)\big),$$

where $x_i \in \{0,1\}^n$ for all $i \in [m]$ and $\oplus$ denotes bit-wise XOR.

We prove Theorem 9 by showing a lower bound for such an extended XOR-composition.

Theorem 11. *For all $n, m \in \mathbb{N}$ there exist $g_1, \dots, g_m : \{0,1\}^n \to \{0,1\}^n$ such that*

$$\mathrm{CC}(\mathrm{Id}_n \boxplus (g_1, \dots, g_m)) \geq (2 - 2^{-m+1})n - O(\log n).$$

A specific case of this theorem for $m = 2$ was proved in [17, Theorem 21]. To show that Theorem 11 implies Theorem 9 we need the following lemma.

Lemma 12. *For all $n, m \in \mathbb{N}$ and functions $g_1, \dots, g_m \in \{0,1\}^n \to \{0,1\}^n$, there exist a function $g \in \{0,1\}^{n'} \to \{0,1\}^{n'}$ for $n' = n + \lceil \log m \rceil$ such that*

$$\mathrm{CC}(\mathrm{Id}_{n'} \boxplus_m g) \geq \mathrm{CC}(\mathrm{Id}_n \boxplus (g_1, \dots, g_m)).$$

Proof. Consider function g' defined by the following equation: $g'(x, y) = g_{\overline{y}+1}(x) \circ 0^{\lceil \log n \rceil}$, where $x \in \{0,1\}^n$, $y \in \{0,1\}^{\lceil \log m \rceil}$, '$\circ$' denotes concatenation of bit strings, and $\overline{y}$ denotes a number with a binary expansion y. It is easy to see that for all $x_1, \dots, x_m \in \{0,1\}^n$,

$$(\mathrm{Id}_{n'} \boxplus_m g')\big((x_1, 0_2), \dots, (x_m, (m-1)_2)\big) = \big(\mathrm{Id}_n \boxplus (g_1, \dots, g_m)\big)(x_1, \dots, x_m) \circ 0^{\lceil \log n \rceil},$$

where k_2 defines binary expansion of k of length $\lceil \log m \rceil$. Since $\mathrm{Id}_n \boxplus (g_1, \dots, g_m)$ is a subfunction of $\mathrm{Id}_{n'} \boxplus g'$, the lower bound applies. $\square$

Proof of Theorem 9 assuming Theorem 11. Let $\tilde{n} = n - \lceil \log m \rceil$. By Theorem 11 there exist functions $g_1, \ldots, g_m : \{0,1\}^{\tilde{n}} \to \{0,1\}^{\tilde{n}}$ such that

$$\mathrm{CC}(\mathrm{Id}_{\tilde{n}} \boxplus (g_1, \ldots, g_m)) \geq (2 - 2^{-m+1})\tilde{n} - O(\log \tilde{n}) = (2 - 2^{-m+1})n - O(\log n).$$

Now we apply Lemma 12 to get the desired bound:

$$\mathrm{CC}(\mathrm{Id}_n \boxplus_m g') \geq \mathrm{CC}(\mathrm{Id}_{\tilde{n}} \boxplus (g_1, \ldots, g_m)) \geq (2 - 2^{-m+1})n - O(\log n). \qquad \square$$

2.1 Proof of Theorem 11

In the proof of this theorem, we need to consider communication complexity in *half-duplex communication model with zero.* The idea of half-duplex communication was introduced in [9] and later developed in [1]. In half-duplex communication model, every player can send messages in every round, but if both players send simultaneously, then their messages get lost. That allows them to "mix" classical communication protocols (see proof of Lemma 16). Formally speaking, every round each player chooses one of three actions: 'send 0', 'send 1', or 'receive'. If one of the players sends while the other receives then communication works like in the classical model. If both players send simultaneously then both messages get lost (and players do not know about it). If both players receive simultaneously they get zeroes.

In [17], the authors introduced *partially half-duplex communication.* In partially half-duplex communication problems the players receive inputs divided in two parts: Alice receives (f, x), Bob receives (g, y). They can use half-duplex communication but with a restriction: if $f = g$ then the communication must have only *classical* rounds (every round one of the players sends some bit and the other one receives).

We are going to prove a lower bound for $\mathrm{Id}_n \boxplus (g_1, \ldots, g_m)$ by induction on m. Assume that we have already proven a lower bound for some value of m. To prove a lower bound for $m+1$ we take the following steps:

- prove a lower bound on partially half-duplex communication complexity for an intermediate communication problem where g_{m+1} is replaced with *a multiplexer relation* (see Definition 13 and Lemma 15),
- argue that if the intermediate communication problem is hard for partially half-duplex communication then there is a "hardest" function g_{m+1} such that if we hard-wire it into the multiplexer then the resulting communication problem has the same lower bound (see Lemma 16).

Remark. Starting from here, we will always consider *non-promise* communication problems. For generalized Karchmer–Wigderson games this means that if the promise is broken, i.e., $f(x) = f(y)$, then the players are allowed to output a special symbol '$\perp$'. It is not hard to see that communication complexity of non-promise Karchmer–Wigderson game differs by no more than two from communication complexity of the promise version: the players can use a protocol for promise version and then verify the answer using additional two bits of communication. Since the complexity differs only by an additive constant, this will not affect our lower bounds.

We start with the definition of an intermediate communication problem.

Definition 13. For any $n, m \in \mathbb{N}$ and functions $f, g_1, \ldots, g_m : \{0,1\}^n \to \{0,1\}^n$ *the XOR-composition with a multiplexer* $f \boxplus (g_1, \ldots, g_m, \mathrm{Mux})$ defines the following communication problem: Alice is given $x_1, \ldots, x_m, z_a \in \{0,1\}^n$ and some function $h_a : \{0,1\}^n \to \{0,1\}^n$, Bob is given $y_1, \ldots, y_m, z_b \in \{0,1\}^n$ and some function $h_b : \{0,1\}^n \to \{0,1\}^n$. Their goal is to find $i \in [(m+1)n]$ such that $(x_1 \circ \cdots \circ x_m \circ z_a)_i \neq (y_1 \circ \cdots \circ y_m \circ z_b)_i$. If $h_a \neq h_b$ or $g_1(x_1) \oplus \cdots \oplus g_m(x_m) \oplus h_a(z_a) = g_1(y_1) \oplus \cdots \oplus g_m(y_m) \oplus h_b(z_b)$ then the players are allowed to output $\perp$.

For the remaining of the section we fix n. Let $\mathcal{P}_n$ be the set of all permutations of $\{0,1\}^n$, and $N = 2^n$, $\mathcal{X}_m = \mathcal{P}_n \times \{0,1\}^{nm} \times \{0,1\}^n$. To simplify the formulas we are going to use $\vec{x}$ and $\vec{y}$ to denote $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$, respectively. In the same manner we denote $g_1, \ldots, g_m$ with $\vec{g}$ and use $\vec{g} \otimes \vec{x}$ as a shortcut for $g_1(x_1) \oplus \cdots \oplus g_m(x_m)$. We use $\mathrm{CC}_{A \times B}$ and $\mathrm{CC}^{phd}_{A \times B}$ to denote the communication complexity of a communication problem restricted to a rectangle $A \times B$.

The proof is by induction on m. The following lemma plays the role of an induction hypothesis.

Lemma 14. *For all $m, k \in \mathbb{N}$, $k \leq n-3$, there exist functions $g_1, \ldots, g_m \in \mathcal{P}_n$ such that for any set $S \subset \{0,1\}^{nm}$ of size $2^{-k}N^m$,*

$$\mathrm{CC}_{S \times S}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m)) \geq (2 - 2^{-m+1})n - k - O(\log n).$$

The base case for $m = 1$ can be proved using to Shannon's counting argument but we do not prove it as our proof of the first induction step does not depend on it (see the proof of Lemma 15).

Assuming Lemma 14 for $m > 1$ or nothing for $m = 1$ we follow the ideas from [17] and prove a lower bound on partially half-duplex communication complexity of the XOR-composition with a multiplexer, the communication problem with one of the functions replaced by the multiplexer relation. A half-duplex protocol for $\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{Mux})$ is called *partially half-duplex* if it has the following property: whenever Alice and Bob are given the same function they are not allowed to perform non-classical communication. In other words, in a partially half-duplex protocol Alice and Bob never send or receive simultaneously if $h_a = h_b$. Let CC^{phd} denote partially half-duplex communication complexity.

Lemma 15. *For all $m, k \in \mathbb{N}$, $k \leq n-3$, there exist functions $g_1, \ldots, g_m \in \mathcal{P}_n$ such that for any set $S \in \mathcal{X}_m$ of size $2^{-k}N^{m+1}N!$,*

$$\mathrm{CC}^{phd}_{S \times S}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{Mux})) \geq \left(2 - 2^{-m}\right)n - k - O(\log n).$$

This lemma generalizes a lemma proved in [17, Lemma 46]. After we prove Lemma 15 for some value of m we use the following "extraction" lemma to replace the multiplexer relation with a function. This lemma is the main reason why we need (partially) half-duplex communication.

Lemma 16. *If $\mathrm{CC}^{phd}_{S \times S}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{Mux})) \geq \gamma$ on any rectangle $S \times S$ with $|S| \geq \delta|\mathcal{P}_n|$ for some $\gamma, \delta > 0$ then exists $g_{m+1} \in \mathcal{P}_n$ such that*

$$\mathrm{CC}_{S' \times S'}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, g_{m+1})) \geq \gamma - \lceil \log n \rceil - 2$$

for any set $S' \subset \{0,1\}^{nm}$ of size at least δ.

Proof. We prove by contradiction. Suppose that for every every function $h \in \mathcal{P}_n$ there is a rectangle $S_h \times S_h$ such that $|S_h| \geq \delta$ and

$$\mathrm{CC}_{S_h \times S_h}\big(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, h)\big) \leq d < \gamma - \lceil \log n \rceil - 2$$

for some $d \in \mathbb{N}$. Let $S = \bigcup_{h \in \mathcal{P}_n} \{(h, \vec{x}, z) \mid (\vec{x}, z) \in S_h\}$. It is easy to see that $|S| \geq \delta |\mathcal{P}_n|$. We are going to show that in this case $\mathrm{CC}^{phd}_{S \times S}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{Mux})) < \gamma$.

Consider the following half-duplex protocol for $\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{Mux})$. Alice, who is given $\vec{x}$, z_a, and h_a, follows the protocol Π_{h_a} using $(\vec{x}, z_a)$ as her input. Meanwhile Bob, who is given $\vec{y}$, z_b, and h_b, follows the protocol Π_{h_b} using $(\vec{y}, z_b)$ as his input. If $h_a \neq h_b$ they might use different protocols, which is fine because we are in the half-duplex communication model. When Alice reaches some leaf of Π_{h_a} she starts receiving until the end of round d. Bob does the same thing. After d rounds of communication Alice has a candidate i for the answer of the game, which is a valid output if $h_a = h_b$. Bob has a candidate j, that is equal to i if $h_a = h_b$. Now Alice and Bob just need to check that indeed $(\vec{x}, z_a)_i \neq (\vec{y}, z_b)_j$ and $i = j$, which can be done in $\lceil \log n \rceil + 2$ rounds of communication. They output i if both conditions are true, and $\perp$ otherwise. The total number of rounds of this half-duplex protocol is $d + \lceil \log n \rceil + 2 < \gamma$. $\square$

Together Lemma 15 and Lemma 16 immediately imply Lemma 14 for $m + 1$.

Proof of Lemma 14. We prove the statement of the lemma for $m + 1$ functions. Apply Lemma 16 for the result of Lemma 15 with $\delta = 2^{-k} N^{m+1}$ and $\gamma = \big(2 - 2^{-m}\big)n - O(\log n)$. $\square$

That concludes the induction step. Theorem 11 follows from Lemma 14 by setting $k = 0$.

Proof of Theorem 11. By Lemma 14 for $k = 0$, we have

$$\mathrm{CC}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m)) \geq (2 - 2^{-m+1})n - O(\log n). \qquad \square$$

It remains for us to prove Lemma 15.

2.2 Proof of Lemma 15

The proof of Lemma 15 has many similarities with the proof of the main result of [17]. The main technical novelty of the following proof is that we have found a way to make the proof inductive. In [17], there is a dichotomy between two communication complexity reductions: a reduction from deterministic equality and a reduction from non-deterministic non-equality. In this proof, we replace the reduction from deterministic equality with an inductive step.

The proof is split in two parts. In the first part, given a protocol we will find a large enough collection of subrectangles in it. All the nodes corresponding to these subrectangles will have equal *partial transcripts*. In the classical communication model, *a partial transcript* of a node of the protocol is a bit string consisting of all the messages that are sent on the path from the root to this node. For a partially half-duplex protocol we can also define a partial transcript of a node in the same way if all the preceding communication of the node is classical. An important difference is that in the classical model a partial transcript uniquely defines a node. In the half-duplex model the same partial transcript of length d can correspond to at most 2^d nodes of the protocol, e.g. a partial transcript "00" can correspond to 4 different nodes: a node where both messages were sent by Alice, a node where both messages were send by Bob, and two nodes where both players sent messages in different order.

Lemma 17. *For any partially half-duplex protocol Π for $\mathrm{Id}_n \boxplus (g_1, \dots, g_m, \mathrm{Mux})$ on a rectangle $S \times S$, $|S| \geq 2^{-k} N^{m+1} N!$, there exists a rectangle of inputs $R \times R$, $R \subset S$, $|R| \geq 8N^m N!$, and a string $T \in \{0,1\}^{n-k-3}$, such that if Alice and Bob are given the same input from R then the transcript of the first $n-k-3$ rounds is equal to T.*

Proof. Let $D = \{((h, \vec{x}, y), (h, \vec{x}, y)) \mid (h, \vec{x}, y) \in \mathcal{S}\}$ be the subset of inputs where player's inputs are identical. First, we need to notice that if Alice and Bob are given inputs from D, then they perform only classical communication. Consider the first $n-k-3$ rounds of communication. There are at most 2^{n-k-3} different transcripts of length $n-k-3$, so there is a transcript T that corresponds to at least $|D|/2^{n-k-3} = 8N^m N!$ inputs from D. Let R be the set of all these inputs. $\square$

Let us emphasize again, that the set S constructed here is not consolidated in a single node of the protocol. All the elements of S have the same transcript of the first $n-k-3$ rounds but these transcripts do not include the information who sends each of the messages, so in fact the same transcripts can correspond to different nodes of the protocol. Note that any two inputs from S with the same function g necessarily belong to the same node of the protocol as all the rounds are classical.

The last thing that we need for the proof of Lemma 15 is the "technical lemma". The following combinatorial object is useful for understanding the structure of subsets of inputs.

Definition 18. For a subset of inputs $S \subseteq \mathcal{X}_m$ we define *a domain graph* to be a bipartite graph $G_S = (U_S, V_S, E_S)$, such that $U_S \subseteq \mathcal{P}_n$, $V_S \subseteq \{0,1\}^{n(m+1)}$, and $(h, (\vec{x}, y)) \in E_S \iff (h, \vec{x}, y) \in S$.

The following "technical lemma" is a generalization of [17, Lemma 39].

Lemma 19. *Let $S \subseteq \mathcal{X}_m$ be a subset of inputs such that $|S| \geq N^m \cdot N!$, and let $G_S = (U_S, V_S, E_S)$ be a domain graph of S. If $\min_{h \in U_S}\{\deg_{G_S}(h)\} \geq 4N^m$ and*

$$\forall h \in \mathcal{P}_n,\ \forall y \in \{0,1\}^n,\ \left|\{\vec{x} \mid (h, (\vec{x}, y)) \in E_S\}\right| \leq N^{m-\alpha} \tag{1}$$

for some $\alpha > 0$, then there is a set $H \subseteq U_S$ of size $2^{\Omega(N^\alpha)}$ such that for all distinct $h_1, h_2 \in H$, there exist $(\vec{x}, y)$: $(h_1, \vec{x}, y) \in S$, $(h_2, \vec{x}, y) \in S$, and $h_1(y) \neq h_2(y)$.

The proof of Lemma 19 repeats almost verbatim the proof of the original lemma [17, Lemma 39]. We present it in Appendix A.

Now we are ready to prove Lemma 15 by showing that if $\mathrm{Id}_n \boxplus (g_1, \dots, g_m, \mathrm{Mux})$ has a short protocol then we can either contradict induction hypothesis by extracting a short protocol for $\mathrm{Id}_n \boxplus (g_1, \dots, g_m)$ or non-deterministically solve non-equality more efficiently than it is possible.

Lemma 15. *For all $m, k \in \mathbb{N}$, $k \leq n-3$, there exist functions $g_1, \dots, g_m \in \mathcal{P}_n$ such that for any set $S \in \mathcal{X}_m$ of size $2^{-k} N^{m+1} N!$,*

$$\mathrm{CC}^{phd}_{S \times S}(\mathrm{Id}_n \boxplus (g_1, \dots, g_m, \mathrm{Mux})) \geq \left(2 - 2^{-m}\right)n - k - O(\log n).$$

Proof. Let $\alpha = 1 - 2^{-m}$. Suppose that Π is a partially half-duplex protocol for $\mathrm{Id}_n \boxplus (g_1, \dots, g_m, \mathrm{Mux})$ of depth d. Let R be the set provided by Lemma 17. Let $S' = R \setminus \{(h, \vec{x}, y) \mid \deg_{G_S}(h) < 4N^m\}$, so $|S'| > 4N^m N!$. Let $G_{S'} = (U_{S'}, V_{S'}, E_{S'})$ be a domain graph of S'. The minimal degree of the vertices in $U_{S'}$ is at least $4N^m$.

Suppose that there is $h \in \mathcal{P}_n$ and $y \in \{0,1\}^n$ such that $\left|\{\vec{x} \mid (h,(\vec{x},y)) \in E_{S'}\}\right| > N^{m-\alpha}$. Let $S_{h,y} = \{(h,\vec{x},y) \mid (h,(\vec{x},y)) \in E_{S'}\}$. We can extract from Π a classical protocol Π' of depth at most $d-n+k+3$ that solves $\mathrm{Id}_n \boxplus (g_1,\ldots,g_m,\mathrm{Mux})$ on $S_{h,y} \times S_{h,y}$. This follows from the fact that Π is partially half-duplex, so it has only classical rounds on inputs from $S_{h,y} \times S_{h,y}$. Let $W = \{x_1,\ldots,x_m \mid (h,(x_1,\ldots,x_m,y)) \in E_{S'}\}$.

- If $m=1$ then the protocol Π' can be used to solve an equality problem on a set W. Given inputs $x_a, x_b \in W$, Alice and Bob simulate the protocol for Π' on $S' \times S'$ for inputs (h,x_a,y) and (h,x_b,y). If the protocol outputs $\perp$ then the players output 1, otherwise they output 0. For inputs (h,x_a,y) and (h,x_b,y), the protocol outputs $\perp$ if and only if $x_a = x_b$, so this reduction gives a correct protocol for EQ_W of the same depth. Any protocol for EQ_W has depth at least $\log|W| \geq \log(N^{1/2}) = n/2$. By the reduction, the same lower bound applies for the protocol for Π on $S' \times S'$. Thus, we have $d \geq n-k-3+n/2 = (2-2^{-m})n-k-3$.

- If $m>1$ then we can use the protocol Π' to solve $\mathrm{Id}_n \boxplus (g_1,\ldots,g_m)$ on the rectangle $W \times W$. By the induction hypothesis (Lemma 14) we know that

$$\begin{aligned}\mathrm{CC}_{W\times W}(\mathrm{Id}_n \boxplus (g_1,\ldots,g_m)) &\geq (2-\alpha-2^{-m+1})n - O(\log n)\\ &= (2-1+2^{-m}-2^{-m+1})n - O(\log n)\\ &= \alpha n - O(\log n).\end{aligned}$$

  Thus, we have $d \geq n-k-3+\alpha n - O(\log n) = (2-2^{-m})n-k-O(\log n)$.

Otherwise, if $\left|\{\vec{x} \mid (h,(\vec{x},y)) \in E_{S'}\}\right| \leq N^{m-\alpha}$ for all $h \in \mathcal{P}_n$ and $y \in \{0,1\}^n$, we apply Lemma 19 to construct a set H of size at least $2^{\Omega(N^\alpha)}$. In this case, the protocol for $\mathrm{Id}_n \boxplus (\vec{g},\mathrm{Mux})$ on $S' \times S'$ can be used to non-deterministically solve NEQ_H with additive overhead of $O(\log n)$. The reduction from NEQ_H to $\mathrm{Id}_n \boxplus (\vec{g},\mathrm{Mux})$ is similar to the reduction used in [17].

Let $R_{h_a,h_b} = \{((h_a,\vec{x}_a,y_a),(h_b,\vec{x}_b,y_b)) \in S' \times S' \mid \vec{g} \otimes \vec{x}_a \oplus h_a(y_a) \neq \vec{g} \otimes \vec{x}_b \oplus g_b(y_b)\}$. We consider the following three situations and show that they are the necessary and sufficient conditions for $h_a, h_b \in H$ to be different:

- There are $\vec{x}_a, \vec{x}_b, y_a, y_b$ such that the protocol Π performs non-classical communication in the first $n-k-3$ rounds on input $((h_a,\vec{x}_a,y_a),(h_b,\vec{x}_b,y_b))$. The partial transcript T of the first $n-k-3$ rounds of Π is fixed by Lemma 17, but it does not include an information about who sends each message, so the same transcript can be produced by different rounds. Such a difference can only exists if $h_a \neq h_b$ — for every fixed $h_a = h_b$ the protocol has only classical rounds, and hence a partial transcript uniquely defines who sends in each round.

- The protocol Π performs a non-classical round on some input from R_{h_a,h_b}. If $h_a = h_b$ then Π can only perform classical rounds by the definition of partially half-duplex communication.

- Π performs only classical rounds on some input from R_{h_a,h_b} and outputs $\perp$.

We can argue that one of this conditions is satisfied iff $h_a \neq h_b$. Indeed, suppose that $h_a \neq h_b$. If the first or the second condition is satisfied we are done, so let's assume that it is not. The first $n-k-3$ rounds of Π on inputs from R_{h_a,h_b} are already known, so we can skip them and only consider the rounds of Π after that. We also know that all the next rounds are going to be classical. By construction of H there exists $\vec{x}, y$, such that $(h_a,\vec{x},y)$ and $(h_b,\vec{x},y)$ belong to S', and also $\vec{g} \otimes \vec{x} \oplus h_a(y) \neq \vec{g} \otimes \vec{x} \oplus h_b(y)$. By the definition of $\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{Mux})$ the protocol Π has to output $\perp$, and hence satisfy the third condition.

Now suppose that $h_a = h_b$. Then neither of the conditions could be satisfied. The first condition fails as in this case a partial transcript uniquely defines who sends in each round. The second condition fails by the definition of partially half-duplex protocol. The third one fails by the definition of $\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{Mux})$.

Now we can use this property to solve NEQ_H. Alice and Bob guess which of the condition is satisfied, guess a proof of it, and then verify it.

- To prove the first condition the players guess the difference in the first $n-k-3$ rounds. Verification requires only $\log n$ bits of communication.
- For the second condition the players guess a number $t \in [d-n+k+3]$, a string $s \in \{0,1\}^t$, a number $i \in [n]$, and bits p, q. Then they verify that there exist pairs $(\vec{x}_a, y_a)$ and $(\vec{x}_b, y_b)$ such that:
  - $p = \left(\vec{g} \otimes \vec{x}_a \oplus h_a(y_a)\right)_i \neq \left(\vec{g} \otimes \vec{x}_b \oplus g_b(y_b)\right)_i = 1-p$,
  - both players are consisted with s being an extension of the partial transcript T on inputs $((h_a, \vec{x}_a, y_a), (h_b, \vec{x}_b, y_b))$, meaning that if a player wants to send a bit in some round, this bit is equal to corresponding bit in s,
  - in the next round after the rounds described in s, the protocol Π performs a non-classical round: either both send (in case $q = 1$) or both receive (in case $q = 0$).

  All together the size of the witness in this case is $d - n + k + O(\log n)$.
- For the third condition the players guess a string $s \in \{0,1\}^{d-n+k+3}$, a number $i \in [n]$, and a bit p. Then they verify that there exist pairs $(\vec{x}_a, y_a)$ and $(\vec{x}_b, y_b)$ such that:
  - $p = \left(\vec{g} \otimes \vec{x}_a \oplus h_a(y_a)\right)_i \neq \left(\vec{g} \otimes \vec{x}_b \oplus g_b(y_b)\right)_i = 1-p$,
  - both players are consisted with s being an extension of the partial transcript T on inputs $(h_a, \vec{x}_a, y_a), (h_b, \vec{x}_b, y_b)$, meaning that if a player wants to send a bit in some round, this bit is equal to corresponding bit in s,
  - the transcript ends in a leaf labeled with $\perp$.

  All together the size of the witness in this case is $d - n + k + O(\log n)$.

This reduction shows that NEQ_H can be non-deterministically solved with a protocol of size $d - n + k + O(\log n)$. Thus, the depth of the protocol Π is at least

$$\begin{aligned} n - k + \mathrm{NCC}(\mathrm{NEQ}_H) - O(\log n) &\geq n - k + \log\log|H| - O(\log n) \\ &\geq n - k + \log N^{\alpha} - O(\log\log(N)) \\ &= n - k + \alpha n - O(\log n), \end{aligned}$$

where NCC stands for non-deterministic communication complexity. $\square$

3 Super-cubic lower bound

Now we have all the ingredients to prove a super-cubic lower bound. First of all we need to reformulate the lower bound on $\mathrm{Id}_n \boxplus_m g$ (Theorem 9) in terms of protocol size.

Lemma 20. *For all $n, m \in \mathbb{N}$, there exists $g : \{0,1\}^n \to \{0,1\}^n$ such that any communication protocol Π for $\mathrm{Id}_n \boxplus_m g$,*

$$\log_2 \mathrm{L}(\Pi) \geq \frac{(2 - 2^{-m+1})n}{1.73} - O(\log n).$$

To get a protocol size lower bound from a protocol depth lower bound we need a protocol balancing technique. In Appendix B, we show that any De Morgan formula balancing technique that preserves monotonicity can be applied for communication protocols as well. And hence we can use balancing technique by Khrapchenko [15, 11].

For any $m \geq 16$ that gives us $\log_2 L(\Pi) > 1.156n$. So we fix $m = 16$. Now we are going to feed this lower bound into the following variant of Andreev's function.

Definition 21. For all $n, m \in \mathbb{N}$, $n > m \log n$, and functions $f, g : \{0,1\}^{\log n} \to \{0,1\}^{\log n}$ *the XOR-composed Andreev's function* $\mathrm{Andr}_{n,m}$ is defined by

$$\mathrm{Andr}_{n,m}(f, g, x_1, \dots, x_{m \log n}) = (f \boxplus_m g)\big(\oplus(x_1), \cdots, \oplus(x_{m \log n})\big),$$

where $x_i \in \{0,1\}^{\frac{n}{m \log n}}$ for $i \in [m \log n]$, and $\oplus(x)$ denotes the sum of all bits of x modulo 2.

Theorem 22. *Any communication protocol for the generalized Karchmer–Wigderson game for $\mathrm{Andr}_{n,16}$ has size at least $\Omega(n^{3.156}(\log n)^{-7/2}(\log\log n)^{-2})$.*

Note that the input length of $\mathrm{Andr}_{n,m}$ is $\Theta(n \log n)$. It is also important that there is a natural polynomial time algorithm for $\mathrm{Andr}_{n,m}$, so it is an explicit function. The proof of this theorem is almost identical to the original proof of Håstad [7, Theorem 8.1] with only difference that we now hard-wire functions $\mathrm{Id}_{\log n}$ and g provided by Lemma 20. It's not entirely obvious what restrictions mean in terms of communication protocols. In Appendix C, we explain that Håstad's technique, which was used for formulas, can be carried over to the case of communication protocols.

Proof. Assume that we have a protocol of size L for generalized KW game for $\mathrm{Andr}_{n,16}$. We know that there is a function $\mathrm{Id}_{\log n} \boxplus_{16} g$ on $16 \log n$ variables that requires protocol of size at least $n^{1.156}$. We fix the first two inputs to $\mathrm{Andr}_{n,16}$ with the description of $\mathrm{Id}_{\log n}$ and g provided by Lemma 20. This might decrease the size of the protocol, but it is not clear by how much and hence we just note that the resulting protocol is of size at most L.

Apply an R_p-restriction with $p = \frac{32 \log n \log\log n}{n}$ on the protocol. By Theorem 28 the resulting protocol will be of expected size at most $O(n^{-2}(\log n)^{7/2}(\log\log n)^2 L + 1)$. The probability that all variables in a particular group are fixed is bounded by

$$(1-p)^{\frac{n}{16 \log n}} \leq e^{-\frac{pn}{16 \log n}} \leq (\log n)^{-2}.$$

Since there are only $16 \log n$ groups, with probability $1 - o(1)$ there remains at least one live variable in each group. Now since a positive random variable is at most twice its expected with probability at least $1/2$, it follows that there is a positive probability that we have at most twice the expected remaining size and some live variable in each group. It follows that

$$n^{-2}(\log n)^{7/2}(\log\log n)^2 L \geq \Omega(n^{1.156}).$$

Hence $L \geq \Omega\big(n^{3.156}(\log n)^{-7/2}(\log\log n)^{-2}\big)$. $\square$

Theorem 8. *There exists a function $f : \{0,1\}^n \to \{0,1\}^{\log n}$ such that any communication protocol for generalized Karchmer–Wigderson game for f has size at least $\tilde{\Omega}(n^{3.156})$.*

Proof. Let $f' = \mathrm{Andr}_{n',16}$ for $n' = \frac{n}{2\log n}$. The input length of f' is $\frac{2n(\log n - \log\log n)+n}{2\log n} < n$. The output length of f' is $\log n - \log\log n - 1 < \log n$. Let $f : \{0,1\}^n \to \{0,1\}^{\log n}$ be a function obtained from f' by adding the appropriate number of dummy input and output bits. By Theorem 22 any protocol for generalized Karchmer–Wigderson game for f has size at least

$$\Omega\big(n^{3.156}(\log n)^{-6.656}(\log\log n)^{-2}\big) = \tilde{\Omega}(n^{3.156}). \qquad \square$$

4 Conclusion

We hope that our approach can provide an insight for proving better lower bounds on the original Karchmer–Wigderson games, and hence for proving new lower bounds on De Morgan formula size. We propose the following list of open problems.

- Show a better lower bound for block-composition of a universal relation and some function. In [17], the special case of Theorem 9 of $m = 2$ was used to show $1.5n - O(\log n)$ lower bound on $\mathrm{U}_n \diamond f_n$. Is it possible to show a better lower bound from Theorem 9 with $m > 2$?

- Can we show nontrivial lower bounds for generalized Karchmer–Wigderson games for functions from $\{0,1\}^n \to \{0,1\}^m$ for all m? For $m = o(\log n)$ we can not prove $n^{3+\varepsilon}$ bound without proving the same kind of bound for formula size, so that might be a bit too ambitious. For $m = \alpha \log n$ for $\alpha \leq 1$ one can adapt the proof from this paper to get a bound of the form $n^{3+O(\alpha)}$. But for $m = \alpha \log n$ for large enough α the best lower bound we know is just m. Is it possible to show a better bound?

- Show n^4 lower bound for generalized Karchmer–Wigderson games for function from $\{0,1\}^n \to \{0,1\}^{\log n}$. The reason for presented lower bound being $\tilde{\Omega}(n^{3.156})$ is that we balance the protocol to get size lower bound from depth lower bound. If one can avoid this step and get lower bounds for size directly, the lower bound will grow up greatly.

- Are there interesting upper and lower bounds for generalized Karchmer–Wigderson outside of the scope of KRW conjecture? It looks that in this setting in might be possible to develop new approaches that might turn to be useful to prove formula lower bounds.

References

[1] Yuriy Dementiev, Artur Ignatiev, Vyacheslav Sidelnik, Alexander Smal, and Mikhail Ushakov. New bounds on the half-duplex communication complexity. In *SOFSEM 2021*, volume 12607 of *LNCS*, pages 233–248. Springer, 2021. doi:10.1007/978-3-030-67731-2_17.

[2] Irit Dinur and Or Meir. Toward the KRW composition conjecture: Cubic formula lower bounds via communication complexity. In *CCC 2016*, volume 50 of *LIPIcs*, pages 3:1–3:51. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016. doi:10.4230/LIPIcs.CCC.2016.3.

[3] Jeff Edmonds, Russell Impagliazzo, Steven Rudich, and Jirí Sgall. Communication complexity towards lower bounds on circuit depth. *Comput. Complex.*, 10(3):210–246, 2001. doi:10.1007/s00037-001-8195-x.

[4] Magnus Gausdal Find, Alexander Golovnev, Edward A. Hirsch, and Alexander S. Kulikov. A better-than-$3n$ lower bound for the circuit complexity of an explicit function. In *FOCS 2016*, pages 89–98. IEEE Computer Society, 2016. doi:10.1109/FOCS.2016.19.

[5] Anna Gál. A characterization of span program size and improved lower bounds for monotone span programs. *Comput. Complex.*, 10(4):277–296, 2001. doi:10.1007/s000370100001.

[6] Dmitry Gavinsky, Or Meir, Omri Weinstein, and Avi Wigderson. Toward better formula lower bounds: The composition of a function and a universal relation. *SIAM J. Comput.*, 46(1):114–131, 2017. doi:10.1137/15M1018319.

[7] Johan Håstad. The shrinkage exponent of de morgan formulas is 2. *SIAM J. Comput.*, 27(1):48–64, 1998. doi:10.1137/S0097539794261556.

[8] Johan Håstad and Avi Wigderson. Composition of the universal relation. In *DIMACS*, volume 13, pages 119–134. DIMACS/AMS, 1990. URL: http://dimacs.rutgers.edu/Volumes/Vol13.html.

[9] Kenneth Hoover, Russell Impagliazzo, Ivan Mihajlin, and Alexander V. Smal. Half-duplex communication complexity. In *ISAAC 2018*, volume 123 of *LIPIcs*, pages 10:1–10:12. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. doi:10.4230/LIPIcs.ISAAC.2018.10.

[10] Kazuo Iwama and Hiroki Morizumi. An explicit lower bound of $5n - o(n)$ for boolean circuits. In *MFCS 2002*, volume 2420 of *LNCS*, pages 353–364. Springer, 2002. doi:10.1007/3-540-45687-2_29.

[11] Stasys Jukna. *Boolean Function Complexity - Advances and Frontiers*, volume 27 of *Algorithms and combinatorics*. Springer, 2012. doi:10.1007/978-3-642-24508-4.

[12] Mauricio Karchmer, Ran Raz, and Avi Wigderson. Super-logarithmic depth lower bounds via the direct sum in communication complexity. *Computational Complexity*, 5(3/4):191–204, 1995. doi:10.1007/BF01206317.

[13] Mauricio Karchmer and Avi Wigderson. Monotone circuits for connectivity require super-logarithmic depth. In *STOC 1988*, pages 539–550. ACM, 1988. doi:10.1145/62212.62265.

[14] Valeriy Mihailovich Khrapchenko. Complexity of the realization of a linear function in the class of II-circuits. *Mathematical Notes of the Academy of Sciences of the USSR*, 9(1):21–23, 1971.

[15] Valeriy Mihailovich Khrapchenko. On a relation between the complexity and the depth of formula. *Methods of Discrete Analysis in Synthesis of Control Systems*, 32:76–94, 1978.

[16] Jiatu Li and Tianqi Yang. $3.1n - o(n)$ circuit lower bounds for explicit functions. *Electron. Colloquium Comput. Complex.*, page 23, 2021. URL: https://eccc.weizmann.ac.il/report/2021/023.

[17] Ivan Mihajlin and Alexander Smal. Toward better depth lower bounds: The XOR-KRW conjecture. In *CCC 2021*, volume 200 of *LIPIcs*, pages 38:1–38:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.CCC.2021.38.

[18] Alexander A. Razborov. Applications of matrix methods to the theory of lower bounds in computational complexity. *Comb.*, 10(1):81–93, 1990. doi:10.1007/BF02122698.

[19] Alexander A. Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24–35, 1997.

[20] Bella Abramovna Subbotovskaya. Realization of linear functions by formulas using $\wedge$, $\vee$, $\neg$. In *Doklady Akademii Nauk*, volume 136-3, pages 553–555. Russian Academy of Sciences, 1961.

A Proof of Technical Lemma

Lemma 19. *Let $S \subseteq \mathcal{X}_m$ be a subset of inputs such that $|S| \geq N^m \cdot N!$, and let $G_S = (U_S, V_S, E_S)$ be a domain graph of S. If $\min_{h \in U_S}\{\deg_{G_S}(h)\} \geq 4N^m$ and*

$$\forall h \in \mathcal{P}_n,\ \forall y \in \{0,1\}^n,\ \left|\{\vec{x} \mid (h, (\vec{x}, y)) \in E_S\}\right| \leq N^{m-\alpha} \tag{1}$$

for some $\alpha > 0$, then there is a set $H \subseteq U_S$ of size $2^{\Omega(N^\alpha)}$ such that for all distinct $h_1, h_2 \in H$, there exist $(\vec{x}, y)$: $(h_1, \vec{x}, y) \in S$, $(h_2, \vec{x}, y) \in S$, and $h_1(y) \neq h_2(y)$.

Proof. We are going to construct a rooted tree $T(S)$ such that

- each leaf ℓ is labeled with a set of functions $F_\ell \subseteq U_S$,
- each internal node v is labeled with a pair $(\vec{x}_v, y_v) \in V_S$,
- for every leaf ℓ labeled with F_ℓ and every its ancestor labeled with $(\vec{x}, y)$ there exists $a \in \{0,1\}^n$ such that $\forall h \in F_\ell$, $h(y) = a$ and $(h, \vec{x}, y) \in S$.
- for every two leaves labeled with F_1 and F_2, and their lowest common ancestor labeled with $(\vec{x}, y)$: $F_1 \cap F_2 = \emptyset$ and for all $h_1 \in F_1$, $h_2 \in F_2$, such that $h_1(y) \neq h_2(y)$,
- the number of leaves is a least $\frac{3^{N^\alpha}}{N}$.

Having such a tree, the set H is constructed by taking one function from every leaf. Indeed, the structure of the tree guarantees that for every $h_1, h_2 \in H$, $h_1 \neq h_2$, there exist $(\vec{x}, y)$, the label of the least common ancestor of corresponding leaves, such that $(h_1, \vec{x}, y) \in S$, $(h_2, \vec{x}, y) \in S$, and $h_1(y) \neq h_2(y)$.

The tree is defined recursively. For a set $Z \subseteq S$, let $T(Z)$ be a (non-empty) rooted tree. Let $G_Z = (U_Z, V_Z, E_Z)$ be a domain graph of Z. If $\min_{h \in U_Z}\{\deg_{G_Z}(h)\} \geq 2N^{m-1}$ then the rooted tree $T(Z)$ consists of a root node labeled with $(\vec{x}_Z, y_Z)$, where $(\vec{x}_Z, y_Z)$ is a vertex of maximal degree in V_Z, and a set of subtrees — for every $a \in \{0,1\}^n$ such that $\exists h \in U_Z : (h, \vec{x}_Z, y_Z) \in Z$, $h(y_Z) = a$ there is a subtree $T(Z_a)$ attached to the root node, where

$$Z_a = \{(h, \vec{x}, y) \mid (h, \vec{x}, y) \in Z, y \neq y_Z, h(y_Z) = a\}$$

Otherwise $T(Z)$ consists of one leaf node labeled with U_Z.

We are going to lower bound the number of leaves in $T(S)$ by lower bounding the number of nodes at depth $N^\alpha + 1$. Let z be some node of $T(S)$ at depth $d \leq N^\alpha$ labeled with $(\vec{x}_Z, y_Z)$ that corresponds to a root node of a subtree $T(Z)$ for some $Z \subseteq S$. Let $G_Z = (U_Z, V_Z, E_Z)$ be a domain graph of Z. Due to the condition (1) the minimal degree of vertices in U_Z can be lower bounded by $4N^m - dN^{m-\alpha} \geq 3N^m$. At the same time $|V_Z| \leq N(N-d)$. Let $T(Z_{a_1}), \ldots, T(Z_{a_k})$ — be the subtrees attached to z. Note that $\pi_1(Z_{a_i}) \cap \pi_1(Z_{a_j}) = \emptyset$ for all $i \neq j$, so the number of functions appearing in $Z_{a_1}, \ldots, Z_{a_k}$ is exactly the number of functions in Z defined on $(\vec{x}_Z, y_Z)$. Given that (x_Z, y_Z) is a vertex of maximal degree in V_Z, the number of functions in the subtrees can be lower bounded as follows,

$$\left|\pi_1(Z_{a_1}) \sqcup \cdots \sqcup \pi_1(Z_{a_k})\right| \geq \frac{|E_Z|}{|V_Z|} \geq \frac{3N^m|U_Z|}{N^m(N-d)} = \frac{3|U_Z|}{N-d}.$$

Thus by induction the total number of functions that appear in the sets at depth $d+1$ is at least

$$\frac{3^d \cdot |U_S|}{N(N-1)\cdots(N-d)} = \frac{3^d \cdot |U_S| \cdot (N-d-1)!}{N!},$$

where the size of U_S is at least $|S|/N^{m+1} \geq N!/N$. Now we are ready to lower bound the number of nodes at depth $d+1$. Note that the number of permutations with k values fixed is $(N-k)!$, and hence a node at depth $d+1$ has at most $(N-d-1)!$ functions in its set. The number of nodes at depth $d+1$ is at least the total number of functions at depth $d+1$ divided by the upper bound on the number of functions in one node, that is

$$\frac{3^d \cdot |U_S| \cdot (N-d-1)!}{N!} / (N-d-1)! \geq \frac{3^d}{N}.$$

For $d = N^\alpha + 1$ we get the desired lower bound $\frac{3^{N^\alpha}}{N} = 2^{\Omega(N^\alpha)}$ on the number of leaves. $\square$

B Protocol balancing

In this section we show that any formula balancing technique that preserves monotonicity can be also used for communication protocols. As De Morgan's formulas balancing methods are well studied, it is tempting to apply it to arbitrary communication protocols as a black-box. Let P be an arbitrary communication problem. We start by showing that every communication protocol Π for P can be viewed as a communication protocol solving *the monotone Karchmer–Wigderson game* for some monotone function f_Π defined by Π, so it can be syntactically transformed into a monotone formula ϕ_Π computing f_Π. Due to Karchmer-Wigderson theorem, any *monotone* formula ψ for f_Π can be syntactically transformed into a protocol Π_ψ solving P and having the same underlying tree. Thus we can convert a protocol for P into a monotone formula, balance it using a technique preserving monotonicity, and then convert it back into a new (balanced) protocol for the original problem P.

Definition 23. *The monotone Karchmer–Wigderson game (monotone KW game)* for monotone Boolean function $f : \{0,1\}^n \to \{0,1\}$ is the following communication problem: Alice gets an input $x \in \{0,1\}^n$ such that $f(x) = 0$, and Bob gets as input $y \in \{0,1\}^n$ such that $f(y) = 1$. Their goal is to find a coordinate $i \in [n]$ such that $x_i < y_i$. The monotone KW game corresponds to a communication problem for *the monotone Karchmer–Wigderson relation for* f:

$$\mathrm{mKW}_f = \{(x, y, i) \mid x, y \in \{0,1\}^n, i \in [n], f(x) = 0, f(y) = 1, x_i < y_i\}.$$

The following transformation of an arbitrary communication problem into a monotone KW relation is folklore [18, 5]. Let $P \subset X \times Y \times Z$ be any communication problem, and let Π be a communication protocol solving P with s leaves $l_1, \ldots, l_s$. For every $x \in X$, let $a(x) \in \{0,1\}^s$ be such that $a(x)_i = 0 \iff \exists y \in Y : (x, y) \in R_i$, where $R_i \subset X \times Y$ is the combinatorial rectangle of inputs corresponding to the leaf l_i. Similarly, for every $y \in Y$, let $b(y) \in \{0,1\}^s$ such that $b(y)_i = 1 \iff \exists x \in X : (x, y) \in R_i$.

Lemma 24 (Folklore)**.** *For every pair of inputs $(x, y) \in X \times Y$ the protocol Π terminates in a leaf l_i if and only if $a(x)_i < b(y)_i$ and $a(x)_j \geq b(y)_j$ for all $j \neq i$.*

Proof. Every $(x, y) \in X \times Y$ belongs to exactly one leaf rectangle of the protocol Π. Transcript $\Pi(x, y)$ terminates in a leaf l_i if and only if $(x, y) \in R_i$. By definition of a and b and since R_i is a combinatorial rectangle, $a(x)_i = 0$ and $b(y)_i = 1$ is equivalent to $(x, y) \in R_i$. For all $j \neq i$, $(x, y) \notin R_j$, and hence $a(x)_j \geq b(y)_j$. ☐

Now consider a De Morgan formula $\phi_\Pi(a_1, \dots, a_s)$ that is syntactically constructed from Π as in Karchmer–Wigderson theorem. Let $f_\Pi : \{0,1\}^s \to \{0,1\}$ be the function computed by ϕ_Π. Function f_Π has the following properties:

- $\forall x \in X,\ f_\Pi(a(x)) = 0$,
- $\forall y \in Y,\ f_\Pi(b(y)) = 1$.

Moreover, by Lemma 24 for any $x \in X$ and $y \in Y$ there is always unique $i \in [s]$ such that $a(x)_i < b(y)_i$, hence the output of any protocol for mKW_{f_Π} on $(a(x), b(y))$ coincides with the output of the protocol Π on (x, y).

Let $\psi(a_1, \dots, a_s)$ be a monotone formula for f_Π. Consider a communication protocol for mKW_{f_Π} obtained from ψ via Karchmer–Wigderson theorem. Let a and b be the inputs of the players following this protocol. Suppose that the players reached a leaf labelled with some i. The monotonicity of ψ guarantees that in this case $a_i < b_i$.

Consider the following protocol Π' for the original communication problem P. Given $(x, y) \in X \times Y$, Alice and Bob simulate the protocol Π_ψ for mKW_f on $(a(x), b(y))$. Let i be the output of Π_ψ on $(a(x), b(y))$. Alice and Bob outputs the label of the leaf l_i of Π.

Lemma 25. *Π' is a correct protocol for P.*

Proof. By Lemma 24, for every $(x, y) \in X \times Y$ there is always a unique index i such that $a(x)_i < b(y)_i$. At the same time, any protocol solving mKW_f must output i such that $a(x)_i < b(y)_i$. So, for all $(x, y) \in X \times Y$ the outputs of Π and Π' coincide. ☐

Now we are ready to prove the main theorem of this section.

Theorem 26. *For every communication problem P with a protocol of size L*

$$\mathrm{CC}(P) \leq 1.73 \log_2 L.$$

Proof. We start with a protocol Π for P with L leaves, transform it to a formula ϕ_Π of the same size, balance it using the formula balancing technique by Khrapchenko [15, 11], get some formula ψ, and finally construct a protocol Π' of depth at most $1.73 \log_2 L$ based on ψ. By Lemma 25 the protocol Π' is a correct protocol for communication problem P. ☐

Now we can use this theorem to prove Lemma 20.

Lemma 20. *For all $n, m \in \mathbb{N}$, there exists $g : \{0,1\}^n \to \{0,1\}^n$ such that any communication protocol Π for $\mathrm{Id}_n \boxplus_m g$,*

$$\log_2 \mathrm{L}(\Pi) \geq \frac{(2 - 2^{-m+1})n}{1.73} - O(\log n).$$

Proof. Apply Theorem 26 to the statement of Theorem 9. ☐

C Restrictions for generalized Karchmer–Wigderson games

In this section we show that we can adapt random restriction technique for communication protocols for generalized Karchmer–Wigderson games. In the seminal paper [7], Håstad analyzes the expected size of a formula after it has been hit with a random restriction. A *restriction* for a formula on n variables is an element of $\{0, 1, *\}^n$. For $p \in [0, 1]$ a random restriction ρ from R_p is chosen by that we set randomly and independently each variable to $*$ with probability p and 0, 1 with equal probabilities $\frac{1-p}{2}$. The interpretation of giving a value $*$ to a variable is that it remains a variable, while in the other cases the given constant is substituted as the value of the variable. The Main Shrinkage Theorem [7, Theorem 7.1] bounds the expected size of the resulting formula.

Theorem 27 (Theorem 7.1 in [7])**.** *Let ϕ be a formula of size L and ρ a random restriction in R_p. Then the expected size of $\phi\restriction_\rho$ is bounded by*

$$O\left(p^2\big(1 + (\log(\min(1/p, L)))^{3/2}\big)L + p\sqrt{L}\right).$$

We want to argue that exactly the same reasoning can be applied to general Karchmer–Wigderson games, and hence we get the following theorem.

Theorem 28. *Let Π be a protocol for generalized Karchmer–Wigderson game of size L and ρ a random restriction in R_p. Then expected size of $\Pi\restriction_\rho$ is bounded by*

$$O\left(p^2\big(1 + (\log(\min(1/p, L)))^{3/2}\big)L + p\sqrt{L}\right).$$

If we were talking about regular Karchmer–Wigderson games then we would be able to say that this theorem is an immediate corollary of Theorem 27 due to Karchmer–Wigderson correspondence between protocols and formulas. For generalized Karchmer–Wigderson games the situation is a little bit trickier: we still can syntactically translate a protocol into a formula, but it is unclear how the resulting formula is related to the (multioutput) function in the protocol. E.g., if we construct a formula in this way for a naive protocol solving generalized Karchmer–Wigderson game for Id_n, then it will be a formula for a constant function.

Remark. A generalized Karchmer–Wigderson game for a function f is a communication problem with *promise* — players are promised that $f(x) \neq f(y)$. It is possibility that there is a leaf in a protocol for KW_f with label i such that for some pair of inputs in this leaf $x_i = 0$ and $y_i = 1$ and for other pair of inputs the situation is opposite, so $x_i = 1$ and $y_i = 0$. That can not happen in non-promise communication problems due to the fact that all inputs corresponding to a node of a protocol form a combinatorial rectangle. Every protocol for KW_f can be modified such that every leaf with label i contains input pairs of only one of these types, and the size of the protocol increases no more than twice. Therefore, we assume that all protocols in this section have this property.

First of all we need to define how restrictions affect communication protocols for generalized Karchmer–Wigderson games. Let $f : \{0, 1\}^n \to \{0, 1\}^r$ be a non-constant function and Π be a protocol for KW_f. The protocol Π is defined on all pair of inputs in $X = \big\{(x, y) \mid x, y \in \{0, 1\}^n, x \neq y\big\}$. When a protocol gets hit with a restriction ρ the set of possible input pairs gets narrowed to

$$X\restriction_\rho = \big\{(x, y) \mid x, y \in \{0, 1\}^n, x \neq y, \forall i : \rho(x_i) \neq * \implies x_i = y_i = \rho(x_i)\big\}.$$

After that some of the nodes of Π become unreachable and can be eliminated. I.e., if $\rho(x_i) \neq *$ for some i then all the leaves labeled with i become unreachable and can be eliminated. In [7], Håstad considers the following list of simplifications.

- If one input to a $\vee$-gate ($\wedge$-gate) is given the value 0 (value 1) we erase this input and let the other input of this gate take the place of the output of the gate.
- If one input to a $\vee$-gate ($\wedge$-gate) is given the value 1 (value 0) we replace the gate by the constant 1 (constant 0).
- If one input of a $\vee$-gate ($\wedge$-gate) is reduced to the single literal $x_i/\bar{x}_i$ then $x_i = 0/x_i = 1$ ($x_i = 1/x_i = 0$) is substituted in the formula giving the other input to this gate. If possible we do further simplifications in this subformula.

All these simplifications of De Morgan formula can be reformulated in terms of the corresponding communication protocol for Karchmer–Wigderson game. We want to say that exactly the same can be done for communication protocols for generalized Karchmer–Wigderson games as they are syntactically indistinguishable (it is important here that every leaf of a protocol correspond to a literal). Thus, we conclude that Theorem 28 holds.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il