Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 116 (2020)

Toward better depth lower bounds: the XOR-KRW conjecture

Ivan Mihajlin* Alexander Smal†

May 19, 2021

Abstract

In this paper, we propose a new conjecture, the XOR-KRW conjecture, which is a relaxation of the Karchmer-Raz-Wigderson conjecture [KRW95]. This relaxation is still strong enough to imply $\mathbf{P} \not\subseteq \mathbf{NC}^1$ if proven. We also present a weaker version of this conjecture that might be used for breaking n^3 lower bound for De Morgan formulas. Our study of this conjecture allows us to partially answer an open question stated in [GMWW17] regarding the composition of the universal relation with a function. To be more precise, we prove that there exists a function g such that the composition of the universal relation with g is significantly harder than just a universal relation. The fact that we can only prove the existence of g is an inherent feature of our approach.

The paper's main technical contribution is a new approach to lower bounds for multiplexer-type relations based on the non-deterministic hardness of non-equality and a new method of converting lower bounds for multiplexer-type relations into lower bounds against some function. In order to do this, we develop techniques to lower bound communication complexity in half-duplex and partially half-duplex communication models.

1 Introduction

1.1 Background

Proving lower bounds on the Boolean formula complexity is one of the classical problems of computational complexity theory. For over 40 years, the researchers had been developing the methods for proving lower bounds — starting with the works of Subbotovskaya [Sub61] and Khrapchenko [Khr71] all the way to the celebrated work of Håstad [Hås98]. As a result, the researchers managed to achieve a cubic lower bound on the formula complexity of an explicit Boolean function (Andreev's function). This lower bound has been unbeaten for over 20 years (up to lower order terms, see. [Tal14] for more information).

Karchmer, Raz, and Wigderson [KRW95] suggested an approach for proving superpolynomial formula size lower bound for Boolean functions from class $\mathbf{P}$. The suggested approach is to prove lower bounds on the formula depth of *the block-composition* of two arbitrary 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* $f \diamond g : (\{0,1\}^n)^m \to \{0,1\}$ is defined by

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

*St. Petersburg Department of Steklov Mathematical Institute of RAS, ivmihajlin@gmail.com

†St. Petersburg Department of Steklov Mathematical Institute of RAS, smal@pdmi.ras.ru

ISSN 1433-8092

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

Let $\mathrm{D}(f)$ denotes 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 the formula for g. Karchmer, Raz, and Wigderson [KRW95] 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 polynomial-time computable function that does not have De Morgan formula of polynomial size, and hence $\mathbf{P} \not\subseteq \mathbf{NC}^1$. 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:

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

It is not hard to see that $h \in \mathbf{P}$. To show that $h \notin \mathbf{NC}^1$, 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, the function $\tilde{f} \diamond \cdots \diamond \tilde{f}$ has depth complexity roughly $\log n \cdot (\log n/\log\log n) = \omega(\log n)$, and hence $\tilde{f} \diamond \cdots \diamond \tilde{f} \notin \mathbf{NC}^1$. Any formula for h must compute $\tilde{f} \diamond \cdots \diamond \tilde{f}$ if we hard-wire $f = \tilde{f}$ in it, so $h \notin \mathbf{NC}^1$. 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 [RR97] (the function h is very special, so the argument does not satisfy "largeness" property). It 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 $\epsilon > 0$.

The seminal work of Karchmer and Wigderson [KW88] 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 depth formula 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 $\mathrm{CC}(R)$ denotes deterministic communication complexity of a relation R. For convenience, we also define *a block-composition for KW relations*, so that the following equality holds: $\mathrm{KW}_{f \diamond g} = \mathrm{KW}_f \diamond \mathrm{KW}_g$. 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*

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

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 the monotone counterparts of classes $\mathbf{NC}^1$ and $\mathbf{NC}^2$ [KW88]. Therefore, there is a 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 [EIRS01, HW90, GMWW17, DM18, KM18, dRMN$^+$20] several steps were taken towards proving the KRW conjecture. In the first two works [EIRS01, HW90] the authors proved the similar bound for the block-composition of two *universal relations*.

Definition 5. *The universal relation* of length n,

$$\mathrm{U}_n = \{(x, y, i) \mid x, y \in \{0,1\}^n, i \in [n], x_i \neq y_i\} \cup \{(x, x, \perp) \mid x \in \{0,1\}^n\}.$$

A communication problem for the universal relation is a generalization of the Karchmer-Wigderson games: Alice and Bob are given n-bit distinct strings and their goal is to find a coordinate $i \in [n]$ such that $x_i \neq y_i$. In contrast to KW games, in this game Alice and Bob can be given the same input string — in that case, they have to output a special symbol $\perp$ to indicate that the promise is broken. Intuitively, the universal relation is a more complex communication problem than KW game because the players do not have proof that their inputs are different. For any non-constant $f : \{0,1\}^n \to \{0,1\}$, there is a natural reduction from KW_f to U_n: given inputs (x, y) for KW_f the players follow a protocol for U_n, the protocol outputs some i such that $x_i \neq y_i$, the players output i as it is a correct output for KW_f. The block-composition of the universal relations generalizes the block-composition of KW games in the same manner. A similar reduction uses a protocol for the block-composition of the universal relations to solve the block-composition KW games. Thus, proving lower bounds for the universal relations seems to be a natural first step.

In the subsequent works [GMWW17, KM18], the authors proved a lower bound on the block-composition of the Karchmer-Wigderson relation for an arbitrary function and the universal relation. This result is presented in terms of the number of leaves rather than formula depth. In [DM18], 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 [Hås98] using an entirely different approach). Their result gives an alternative proof of the cubic lower bound for Andreev's function [Hås98]. In the most recent paper [dRMN$^+$20] of the series, the authors extended the range of inner functions that can be handled in the monotone version of the KRW conjecture to all functions whose depth complexity can be lower bounded via query-to-communication lifting theorem. They also introduce an intermediate semi-monotone setting where only inner function is monotone and show a lower bound on the composition of the (non-monotone) universal relation with every monotone inner function for which a lower bound can be proved using a lifting theorem.

In the last section of [EIRS01], the authors introduced *the same function multiplexer communication game*, that is very similar to the Karchmer-Wigderson game for *the multiplexer function.*

Definition 6. *The multiplexer function* of size n is a function $\mathsf{M}_n : \{0,1\}^{2^n} \times \{0,1\}^n \to \{0,1\}$ with two arguments, such that $\mathsf{M}_n(f,x) = f_x$. It is convenient to interpret the string f as a truthtable of some function $f : \{0,1\}^n \to \{0,1\}$, so we can say that $\mathsf{M}_n(f,x) = f(x)$.

In the KW game for M_n, Alice gets a function $f : \{0,1\}^n \to \{0,1\}$ and $x \in \{0,1\}^n$, such that $f(x) = 0$, Bob gets a function $g : \{0,1\}^n \to \{0,1\}$ and $y \in \{0,1\}^n$, such that $g(y) = 1$. Their goal is to find a coordinate $i \in [2^n + n]$ such that $(f,x)_i \neq (g,y)_i$. The authors of [EIRS01] suggest to consider a version of this game where players are given the same function, i.e., $f = g$, so they only need to find the differing coordinate between x and y.

Definition 7. In *the same function multiplexer communication game (the multiplexer game)* MUX_n, Alice gets a function $f : \{0,1\}^n \to \{0,1\}$ and $x \in \{0,1\}^n$ such that $f(x) = 0$, Bob gets the same function $g : \{0,1\}^n \to \{0,1\}$ and $y \in \{0,1\}^n$ such that $g(y) = 1$. Their goal is to find a coordinate $i \in [n]$ such that $x_i \neq y_i$, or output $\perp$ if $f \neq g$ (if $x \neq y$ and $f \neq g$ then both outputs are possible).

The same function multiplexer communication game can be considered as a generalization of the Karchmer-Wigderson games for Boolean functions on n bits. Indeed, solving the KW game for any $g : \{0,1\}^n \to \{0,1\}$ can be reduced to the same function multiplexer game: Alice and Bob are given g and the corresponding x and y. Given that we already have a lower bound on $f \diamond \mathrm{U}_n$ [GMWW17, KM18], it looks natural to study the block-composition of the KW game for an arbitrary function and the same function multiplexer game. The detailed explanation how a lower bound on the block-composition of the KW game for an arbitrary function and the same function multiplexer might be used to separate $\mathbf{P}$ and $\mathbf{NC}^1$, see [Mei20] for details (to the best of our knowledge, this result was independently proved by Russell Impagliazzo).

Remark 8. The KW game for M_n can also be considered as a generalization of KW games using the same reduction. On the other hand, it is unclear whether lower bounds on the block-composition with it implies any new results. Moreover, the following lower bound applies. Let $\mathrm{L}(f)$ denotes the minimal size of De Morgan formula computing f.

Theorem 9. *For any $m, n \in \mathbb{N}$ with $n \geq 6 \log m$, and any non-constant function $f : \{0,1\}^m \to \{0,1\}$,*

$$\mathrm{CC}(\mathrm{KW}_{f \diamond \mathsf{M}_n}) \geq \log L(f) + n - O(\log^* n).$$

The proof is given in Appendix B.

1.2 The XOR-KRW conjecture

As an alternative to the block-composition, we define a new composition operation.

Definition 10. For any $n, m, k \in \mathbb{N}$ with $k \mid n$, and functions $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^k \to \{0,1\}^k$ *the XOR-composition* $f \boxplus_m g : (\{0,1\}^n)^m \to \{0,1\}$ is defined by

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

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

This composition becomes a stronger version of the block composition if we consider case of $n = m = k$. In this case, both compositions are mapping an $n \times n$ matrix into a vector and then applying a function to it. But in the XOR-composition every bit of the vector depends on the entire matrix rather than just one row. However we will focus on the case of constant m as we believe it might be sufficient for our goals.

We suggest the following generalization of the KRW conjecture.

Conjecture 11 (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 $g : \{0,1\}^k \to \{0,1\}^k$,*

$$\mathrm{D}(f \boxplus_m g) \geq \mathrm{D}(f) + \epsilon k.$$

Using the ideas from [KRW95] one can show that XOR-KRW implies $\mathbf{P} \neq \mathbf{NC}^1$.

Theorem 12. *If Conjecture 11 is true then $\mathbf{P} \neq \mathbf{NC}^1$.*

Proof. Suppose Conjecture 11 is true. Let f be any non-constant function from $\{0,1\}^{\log n}$ to $\{0,1\}$, and let $m \in \mathbb{N}$ be provided by Conjecture 11. For every $t \in \mathbb{N}$, consider a function h_t defined by:

$$h_t(x, g_1, g_2, \ldots g_t) = (f \boxplus_m g_1 \boxplus_m g_2 \boxplus_m \cdots \boxplus_m g_t)(x),$$

where $x \in \{0,1\}^{m^t \log n}$ and $g_i : \{0,1\}^{\log n} \to \{0,1\}^{\log n}$ for all $i \in [t]$. Conjecture 11 implies that there exist $m \in \mathbb{N}$ and $g_1, \ldots, g_t : \{0,1\}^{\log n} \to \{0,1\}^{\log n}$, such that $\mathrm{D}(f \boxplus_m g_1 \boxplus_m g_2 \boxplus_m \cdots \boxplus_m g_t) = \mathrm{D}(h_t) \geq \epsilon t \log n - O(t)$. For $t = \log n$ that gives us

$$\mathrm{D}(h_{\log n}) \geq \epsilon \log^2 n - O(\log n).$$

Now lets estimate the size of the input to $h_{\log n}$. Each g_i requires $n \log n$ bits of description, x requires $m^{\log n} \log n = n^{\log m} \log n = n^{O(1)}$. So, the size of the input to $h_{\log n}$ is $N = n^{O(1)}$ bits, and $\mathrm{D}(h_{\log n}) \geq \epsilon \log^2 n - O(\log n) = \Omega(\log^2 N)$. Thus, $h_{\log n} \notin \mathbf{NC}^1$. On the other hand, we can compute $h_{\log n}$ in a natural way in $\mathbf{P}$. $\square$

The idea behind the XOR-KRW conjecture is influenced by the constructions used in the areas of pseudorandomness and cryptography, where bit-wise xor is used to achieve better results. The proof of hardness of the composition of the universal relations is based on the idea that any protocol that makes progress solving the top relation of the composition is leaking very little information about the actual inputs of the composition. We hope that the additional entanglement provided by taking entry-wise xor of multiple copies of a gadget function g will make it possible to use the same kind of argument about the composition of functions.

In this paper we will focus on specific case of $k = n$. In this case, $f \boxplus_m g$ has the same number of inputs as f. This is not the regime we need for the KRW conjecture in order to separate $\mathbf{P}$ and $\mathbf{NC}^1$, as the proof of the Theorem 12 uses KRW for the case of $k \ll n$. But let us scale our ambitions down a bit. One of the current major challenges of circuit complexity is to beat the $\Omega(n^3)$ lower bound for a specific formula. As we already have mentioned, this bound was proved by Håstad in [Hås98] and was not improved rather than by lower terms since then. If we only aim to prove a supercubic lower bound for a specific formula then we can only focus on the case $k = n$. For $k = n$, the definition of the XOR-composition a bit simpler.

Definition 13 (A special case of Definition 10 for $k = n$)**.** For $n, m \in \mathbb{N}$ and functions $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}^n$ *the XOR-composition* $f \boxplus_m g : (\{0,1\}^n)^m \to \{0,1\}$ is defined by

$$(f \boxplus_m g)(x_1, \ldots, x_m) = f\left(g(x_1) \oplus \cdots \oplus g(x_m)\right),$$

where $x_i \in \{0,1\}^n$ for all $i \in [m]$.

This definition allows us to formulate a weak version of the XOR-KRW conjecture.

Conjecture 14 (The weak XOR-KRW conjecture)**.** *There exists $m \in \mathbb{N}$ and $\epsilon > 0$, such that for all $n \in \mathbb{N}$, for any non-constant functions $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}^n$:*

$$\mathrm{D}(f \boxplus_m g) \geq \mathrm{D}(f) + \epsilon n.$$

We also introduce a version of this conjecture for a formula size rather than depth. Proving that this conjecture is true would allow us to beat $\Omega(n^3)$ formula size lower bound.

Conjecture 15 (The weak XOR-KRW conjecture for formula size)**.** *There exists $m \in \mathbb{N}$ and $\epsilon > 0$, such that for all $n \in \mathbb{N}$, for any non-constant function $f : \{0,1\}^n \to \{0,1\}$ there exists a non-constant function $g : \{0,1\}^n \to \{0,1\}^n$:*

$$\mathrm{L}(f \boxplus_m g) \geq 2^{\epsilon n} \cdot \mathrm{L}(f).$$

The weak XOR-KRW conjecture implies the existence of a function $h = f \boxplus_m g$ for some $f : \{0,1\}^{\log n} \to \{0,1\}$, $g : \{0,1\}^{\log n} \to \{0,1\}^{\log n}$ and $m \in \mathbb{N}$, such that $\mathrm{CC}(\mathrm{KW}_h) \geq (1+\epsilon)\log n$. In order to prove a cubic lower bound for the Andreev's function one needs to hardwire a hard function into it's description. We define a modified Andreev's function that takes the XOR-composition of functions instead. Note that there are $n^{\log n+1}$ pairs of functions $f : \{0,1\}^{\log n} \to \{0,1\}$ and $g : \{0,1\}^{\log n} \to \{0,1\}^{\log n}$. That means that one can encode h with $\theta(n \log n)$ bit.

Definition 16. For $n \in \mathbb{N}$ that is a power of two, any $m \in \mathbb{N}$, and any functions $f : \{0,1\}^{\log n} \to \{0,1\}$ and $g : \{0,1\}^{\log n} \to \{0,1\}^{\log n}$ *the XOR-composed Andreev's function* $\mathrm{Andr}_{\boxplus m}$ is defined by

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

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

The input size of $\mathrm{Andr}_{\boxplus m}$ is $\Theta(n \log n)$. It is also important that there is a natural polynomial time algorithm for $\mathrm{Andr}_{\boxplus m}$.

Theorem 17. *Conjecture 15 implies that* $\mathrm{L}(\mathrm{Andr}_{\boxplus m}) = \Omega(n^{3+\epsilon})$ *for some $m \in \mathbb{N}$.*

The proof of this theorem is identical to the original proof of Håstad with only difference that we can now hardwire functions f and g for some hard f and g provided by the conjecture.

As the main result of this paper we show that some form of XOR-KRW conjecture holds for XOR-composition of the universal relation and the KW game for some hard function. It would be interesting to see if our techniques could be extended to handle the case of $k < n$. It feels that this setting is significantly more sensitive and would require more intricate proof. In this paper, we focused on the regime of $k = n$ since this is the regime that is useful for super-cubic formula lower bounds, but the regime of smaller k's would be useful for other applications.

1.3 Techniques and Results

The paper's main technical contribution is a new approach to lower bounds for multiplexer-type relations based on the non-deterministic hardness of non-equality and a new method of converting lower bounds for multiplexer-type relations into lower bounds against some function. We define two communication problems based on the XOR-composition and prove lower bounds on it: a

XOR-composition of the universal relation with the KW game for some function g, we denote it $\mathrm{U}_n \boxplus \mathrm{KW}_g$, and the XOR-composition of the universal relation with the multiplexer relation, we denote it $\mathrm{U}_n \boxplus \mathrm{MUX}_n$. Both communication problems are based on the XOR-composition for $m = 2$. Our proofs also allow to get a lower bound for the standard block composition of the universal relation and a function (see Appendix A).

Further in this section we discuss a special case of Definition 10 for $m = 2$, which is sufficient for our purposes. Then we will discuss the problem $\mathrm{U}_n \boxplus \mathrm{KW}_g$, which is a relaxed version of the weak KRW-conjecture, and describe our main result, which is a lower bound for this problem. Next, we discuss an even more relaxed version of the problem $\mathrm{U}_n \boxplus \mathrm{MUX}_n$, and describe our second result, which is a lower bound to that problem. Finally, we describe how the second result is proved, and how we use it to derive the first result.

Definition 18 (Special case of Definition 13 for $m = 2$)**.** For functions $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}^n$ *the XOR-composition* $f \boxplus g$ is defined by

$$(f \boxplus g)(x, y) = f(g(x) \oplus g(y)),$$

where $x, y \in \{0,1\}^n$.

In the definitions of the problems below, we are going to use a communication problem that is a generalization of the Karchmer-Wigderson game for non-Boolean functions. So, it is convenient to extend the definition of the KW game to handle the case of multioutput functions.

Definition 19. *The Karchmer-Wigderson game* for function $g : \{0,1\}^n \to \{0,1\}^k$ is the following communication problem: Alice gets an input $x \in \{0,1\}^n$, Bob gets as input $y \in \{0,1\}^n$. Their goal is to find a coordinate $i \in [n]$ such that $x_i \neq y_i$. If $g(x) = g(y)$ then the players are allowed to output $\perp$.

Recall that our ultimate goal is to prove a lower bound for $f \boxplus g$. As an intermediate problem, we consider a version of this game f replaced with the universal relation. In a communication game for $\mathrm{KW}_{f \boxplus g}$, Alice is given $x_a, y_a \in \{0,1\}^n$, such that $(f \boxplus g)(x_a, y_a) = 0$, and Bob is given $x_b, y_b \in \{0,1\}^n$, such that $(f \boxplus g)(x_b, y_b) = 1$. Their goal is to find $i \in [2n]$ such that $(x_a \circ y_a)_i \neq (x_b \circ y_b)_i$. We now replace f with U_n, so the players only know that $g(x_a) \oplus g(y_a) \neq g(x_b) \oplus g(y_b)$.

Definition 20. Let $g : \{0,1\}^n \to \{0,1\}^n$. A communication game $\mathrm{U}_n \boxplus \mathrm{KW}_g$ is the XOR-composition of U_n and KW_g in the following way: Alice is given $x_a, y_a \in \{0,1\}^n$ and Bob is given $x_b, y_b \in \{0,1\}^n$. Their goal is to find $i \in [2n]$ such that $(x_a \circ y_a)_i \neq (x_b \circ y_b)_i$. If $g(x_a) \oplus g(y_a) = g(x_b) \oplus g(y_b)$ they can output $\perp$.

The trivial upper bound for $\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}_g)$ is $\mathrm{CC}(\mathrm{KW}_g) + n + O(\log n) \leq 2n + O(\log n)$: Alice sends x_a to Bob, and Bob compares it with x_b. If he finds a difference then he sends the answer to Alice using $O(\log n)$ bits of communication. Otherwise, they simulate the shortest protocol for KW_g on y_a and y_b that outputs some index j. If $(y_a)_j \neq (y_b)_j$ then they output $n + j$, otherwise they output $\perp$. We are going to prove that there exists a function $g : \{0,1\}^n \to \{0,1\}^n$ such that $\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}_g) \geq 1.5n - O(\log n)$.

Theorem 21. *For all $n \in \mathbb{N}$, there exists $g : \{0,1\}^n \to \{0,1\}^n$ such that*

$$\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}_g) \geq 1.5n - O(\log n).$$

This theorem partially answer an open question from [GMWW17] showing a lower bound for the XOR-composition of the universal relation with a function. The answer is partial because the original open question was to prove a composition result for $\mathrm{U} \diamond \mathrm{KW}_g$ for every function g, and we prove that there exists some hard function g for which a composition result holds. We also only focus on the case where both U and g have the same input length. A corresponding result for the block-composition follows from our proof. See Appendix A for details.

In order to prove the result on $\mathrm{U}_n \boxplus \mathrm{KW}_g$, we will consider a similar communication problem where the function g is given to the players as a part of the input rather than being hardwired into definition of the problem.

Definition 22. In a *communication problem* $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ Alice is given $x_a, y_a \in \{0,1\}^n$ and $g_a : \{0,1\}^n \to \{0,1\}^n$, Bob is given $x_b, y_b \in \{0,1\}^n$ and $g_b : \{0,1\}^n \to \{0,1\}^n$. Their goal is to find $i \in [2n]$ such that $(x_a \circ y_a)_i \neq (x_b \circ y_b)_i$. If $g_a(x_a) \oplus g_a(y_a) = g_b(x_b) \oplus g_b(y_b)$ or $g_a \neq g_b$ they can output $\perp$.

In some sense, the communication problem $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ contains an instance of $\mathrm{U}_n \boxplus \mathrm{KW}_g$ for every g as a special case where Alice and Bob receive g as a part of the input. So, on the one hand, it might be easier to prove a lower bound for it as it is a more complex problem. On the other hand, it seems that there is a natural way of arguing that a lower bound on $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ implies a lower bound on $\mathrm{U}_n \boxplus \mathrm{KW}_g$ for some g: if the problem is hard in common, then it has to be hard in some of the special cases.

The trivial upper bound for $\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{MUX}_n)$ is $2n + O(\log n)$: Alice sends x_a and y_a to Bob, he compares it with x_b and y_b, and then he either finds a difference or realizes that they are allowed to output $\perp$. At the end, Bob sends the answer to Alice using $O(\log n)$ bits of communication. We prove the following lower bound using a reductions from non-deterministic communication complexity.

Theorem 23. *For all* $n \in \mathbb{N}$, $\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{MUX}_n) \geq 1.5n - o(n)$.

After we prove this lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$, we will translate it to a lower bound on $\mathrm{U}_n \boxplus \mathrm{KW}_g$ for some g. The problem $\mathrm{U}_n \boxplus \mathrm{KW}_g$ is a special case of $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ for fixed g. The intuition suggests that if $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ is hard then there should be some function g such that $\mathrm{U}_n \boxplus \mathrm{KW}_g$ is hard. Thus, to get a lower bound for $\mathrm{U}_n \boxplus \mathrm{KW}_g$ for some g from a lower bound on $\mathrm{U}_n \boxplus \mathrm{MUX}_n$, we need to show that $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ is at most as hard as $\mathrm{U}_n \boxplus \mathrm{KW}_g$ for the "hardest" function that we can feed to the players, and hence we can hard-wire this "hardest" function in $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ to get $\mathrm{U}_n \boxplus \mathrm{KW}_g$. Let's forget about the outer U_n for a bit, and consider MUX_n. It seems almost obvious that the complexity of MUX_n is equal to the complexity of the hardest function: given some function g in the MUX_n game the players can use the optimal protocol for KW_g, hence the complexity of MUX_n is upper bounded by the complexity of the hardest KW_g. The same idea should work for the composed problems like $\mathrm{U}_n \boxplus \mathrm{MUX}_n$. However, this argument is incorrect. In the argument we assume that the players choose a protocol depending on the function g they have got as a part of the input. This is not possible in the classical model of communication complexity. Suppose that in the best protocol for KW_{g_1} Alice sends the first message, while in the best protocol for KW_{g_2} for $g_2 \neq g_2$ the first message is sent by Bob. Then it is not clear who sends first in the protocol for MUX_n. There is a natural workaround — we can consider only alternating protocols where Alice sends every odd message and Bob sends every even message [Mei20]. The drawback of this approach is that all the lower bounds in this setting have to be multiplied by $1/2$ when translated to the unrestricted case, that might make them useless for proving non-trivial bounds. This obstacle motivated the study of half-duplex communications models [HIMS18b, DIS+21]. In half-duplex communication models, every player can send messages in every round, but if both players send simultaneously, then their messages get lost. Thus, if we use half-duplex communication model instead of the classical one, then the described problem will not arise, and we can show that the complexity of $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ is at most the complexity of $\mathrm{U}_n \boxplus \mathrm{KW}_g$ for some function g. Using a technique that employs half-duplex communication, we translate the lower bound of Theorem 23 to $\mathrm{U}_n \boxplus \mathrm{KW}_g$.

1.4 Organization of this paper

In Section 2, we review the required preliminaries. In Section 3, we prove a lower bound for the XOR-composition of the universal relation with the multiplexer relation using a reduction from non-deterministic communication complexity (Theorem 23). In Section 4, we prove a lower bound for the XOR-composition of the universal relation with the KW game for some function using the same ideas together with the results from half-duplex communication complexity (Theorem 21). Section 5 contains a conclusion and open problems. In Appendix A, we show the block-composition analogue of Theorem 21. In Appendix B, we prove Theorem 9.

2 Preliminaries

2.1 Notation

Let us mention the notation used in this paper. We use $[k]$ as a shortcut for $\{1, \dots, k\}$, $\mathbb{B}$ as a shortcut for $\{0, 1\}$ and $\circ$ to denote concatenation of binary strings. Working with binary strings we use $\oplus$ for entry-wise xor: $\forall u, v \in \mathbb{B}^k: \ (v \oplus u)_i = v_i \oplus u_i$. For a set of tuples S we use $\pi_i(S)$ to denote the projection of S on the ith coordinate: $\pi_i(S) = \{e_i \mid (e_1, e_2, \dots, e_i, \dots) \in S\}$.

2.2 Communication complexity

We expect that the reader is familiar with the standard definitions of communication complexity that can be found in [KN97]. It will be important to understand how the nodes of communication protocol relate to combinatorial rectangles of the input matrix. Throughout the paper whenever we discuss rectangles we always mean the rectangles of the input matrix of the communication problem under consideration. If some rectangle has equal sides, i.e., it is equal to $A \times A$ for some set A, then we call it *a square*.

We are going to use the following simple theorem that is a generalization of the well-known lower bound for the equality function. For any non-empty finite set S, *the equality on* S is a function $\mathrm{EQ}_S : S \times S \to \mathbb{B}$, such that for all $a, b \in S$, $\mathrm{EQ}_S(a, b) = 1 \iff a = b$.

Theorem 24. *For any non-empty finite set S, $\mathrm{CC}(\mathrm{EQ}_S) \geq \log |S|$.*

Proof. For any $a, b \in S$, $a \neq b$, a communication transcript on input (a, a) must be different from a transcript on input (b, b), otherwise the same transcript would correspond to (a, b) and (b, a). Thus, the length of the longest transcript is at least $\log |S|$. ☐

For convenience, we are going to use some basic results from non-deterministic communication complexity. Let X and Y be non-empty finite sets.

Definition 25. We say that a function $f : X \times Y \to \mathbb{B}$ has *non-deterministic communication protocol* of complexity d if there are two functions $A : X \times \mathbb{B}^d \to \mathbb{B}$ and $B : Y \times \mathbb{B}^d \to \mathbb{B}$ such that

- $\forall (x, y) \in f^{-1}(1)\ \exists w \in \mathbb{B}^d : A(x, w) = B(y, w) = 1$,
- $\forall (x, y) \in f^{-1}(0)\ \forall w \in \mathbb{B}^d : A(x, w) \neq 1 \vee B(y, w) \neq 1$.

The non-deterministic communication complexity of f, denoted $\mathrm{NCC}(f)$, is the minimal complexity of a non-deterministic communication protocol for f.

In contrast to deterministic case, the definition of non-deterministic complexity is asymmetric and hence the complexity of a function and its negation might be different. We will use the following lower bound for the negation of the equality function. For any non-empty finite set S *the non-equality on* S is a function $\mathrm{NEQ}_S : S \times S \to \mathbb{B}$, such that

$$\mathrm{NEQ}_S(a, b) = 1 - \mathrm{EQ}_S(a, b).$$

Theorem 26. *For any non-empty finite set* S*,* $\mathrm{NCC}(\mathrm{NEQ}_S) \geq \log\log|S|$.

Proof. Assume, for the sake of contradiction, that for some S, $\mathrm{NCC}(\mathrm{NEQ}_S) = d \leq \log\log|S| - 1$. Then the following deterministic protocol solves EQ_S: Alice sends $A(x, w)$ for all possible $w \in \mathbb{B}^d$, Bob replies with 1 if and only if there is some $w \in \mathbb{B}^d : A(x, w) = B(x, w) = 1$. The complexity of this protocol is

$$2^d + 1 \leq 2^{\log\log|S|-1} + 1 = \frac{1}{2}\log|S| + 1 < \log|S|$$

that contradicts Theorem 24. □

Notable property of non-deterministic communication complexity is that it does not involve any communication at all. For our purposes it will be easier for us to think about the following alternative definition of non-deterministic communication, which is implicitly mentioned in the classical book by Nisan and Kushilevich [KN97].

Definition 27. We say that a function $f : X \times Y \to \mathbb{B}$ has *privately non-deterministic communication protocol* of complexity d if there is a function $\hat{f} : (X \times \mathbb{B}^*) \times (Y \times \mathbb{B}^*) \to \mathbb{B}$ of (deterministic) communication complexity at most d such that

- $\forall (x, y) \in f^{-1}(1)\ \exists w_x, w_y \in \mathbb{B}^* : \hat{f}((x, w_x), (y, w_y)) = 1$,
- $\forall (x, y) \in f^{-1}(0)\ \forall w_x, w_y \in \mathbb{B}^* : \hat{f}((x, w_x), (y, w_y)) = 0$.

The privately non-deterministic communication complexity of f, denoted $\mathrm{NCC}'(f)$, is the minimal depth of a privately non-deterministic communication protocol for f.

This alternative definition of non-deterministic communication uses private witnesses instead of a public one, and hence the players need to communicate. Let us prove the equivalence of these definitions.

Theorem 28. *For any function* $f : X \times Y \to \mathbb{B}$*,*

$$\mathrm{NCC}(f) + 2 \geq \mathrm{NCC}'(f) \geq \mathrm{NCC}(f).$$

Proof. To prove the first inequality, we suppose that there is a non-deterministic protocol of complexity d for f defined by functions A and B. Lets show that there is a privately non-deterministic protocol for f of complexity $d+2$. We define a function $\hat{f}: (X \times \mathbb{B}^*) \times (Y \times \mathbb{B}^*) \to \mathbb{B}$ such that

$$\hat{f}((x, w_x), (y, w_y)) = 1 \iff |w_x| = |w_y| = d \wedge A(x, w_x) = B(y, w_y) = 1 \wedge w_x = w_y.$$

This function has a deterministic protocol with $d+2$ bits of communication: given some x Alice privately guesses $w_x \in \mathbb{B}^d$ and sends $w_x \circ A(x, w_x)$ to Bob, Bob privately guesses $w_y \in \mathbb{B}^d$ and replies with 1 if and only if $A(x, w_x) = B(y, w_y) = 1$ and $w_x = w_y$, otherwise he replies with 0.

Now we show the second inequality by constructing a non-deterministic protocol of complexity d given a privately non-deterministic protocol of complexity d. Let $\hat{f}$ defines the privately non-deterministic protocol for f, and let Π is a (deterministic) protocol for $\hat{f}$ of depth d. In the non-deterministic protocol for f Alice and Bob interpret the public non-deterministic witness w as a transcript of Π on $((x, w_x), (y, w_y))$ for some (unknown) w_x and w_y. We define a function $A(x, w)$ such that $A(x, w) = 1$ if and only if there exists $w_x \in \mathbb{B}^*$ such that w is a valid transcript for (x, w_x) leading to output 1. Similarly, we define function $B(y, w)$ such that $B(y, w) = 1$ if and only if there exists $w_y \in \mathbb{B}^*$ such that w is a valid transcript for (y, w_y) leading to output 1. The resulting non-deterministic protocol for f defined by A and B has complexity d. ☐

Corollary 29. *For any non-empty finite set S,* $\mathrm{NCC}'(\mathrm{NEQ}_S) \geq \log\log |S|$.

2.3 Half-duplex communication complexity

The essential property of the classical model of communication complexity proposed by Yao is that in every round of communication one player sends some bit and the other one receives it. In [HIMS18b], the authors suggest a generalization of the classical communication model, *the half-duplex model*, where the players are allowed to speak simultaneously. Lets assume that the players have some synchronising mechanism, e.g., synchronised clock, that allows then understand when each round begins. Every round each player chooses one of three actions: send 0, send 1, or receive. There are three different types of rounds.

- If one player sends some bit and the other one receives then communication works like in the classical case, we call such rounds *normal* or *classical*.
- If both players send bits during the round then these bits get lost (the same happens if two persons try to speak via a "walkie-talkie" simultaneously), these rounds are called *wasted*.
- If both players receive, these rounds are called *silent*.

In [HIMS18b], the authors consider three variations of this model based on what happens in silent rounds. We are going to focus on one of the models — *half-duplex communication with adversary*, where in silent round both players receive *some* bits. In order to solve a communication problem in half-duplex communication model with adversary the players have to devise a protocol that is correct for any bits that were received in silent rounds (the protocol must give a correct answer even if these bits were chosen by an adversary).

In the classical case, a protocol is a binary rooted tree that describes the communication of players on all possible inputs: every internal node corresponds to a state of communication and defines which of the players sends in this round. Unlike the classical case in half-duplex communication player does not always know what the other's player action was — the information about it can be “lost”, i.e., in wasted rounds a player do not know what the other player’s action was. It means that a player might not know what node of the protocol corresponds to the current state of communication. The protocol for half-duplex communication can be described by a pair of rooted trees of arity 4 that describe how Alice and Bob communicate on all possible inputs and for any bits they receive in silent rounds. The arity 4 stands for four possible events: send 0, send 1, receive 0, and receive 1. However, in this paper, it will be convenient for us to talk about the half-duplex protocol being a single tree that describes all the actions of players from the point of view of an external observer.

We can also think about half-duplex communication in a following way. In the classical communication protocol player’s action (send or receive) is always defined by the previous communication. In half-duplex communication player’s action can also depend on the input. We will also consider an intermediate model where player’s action depends on the previous communication and a part of the input. We call such a model *partially half-duplex communication model*. 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 protocols but with a restriction: if $f = g$ then the communication must have no non-classical rounds.

Let P be a communication problem with classical communication complexity k. It is not hard to see that half-duplex communication complexity is bounded between $k/2$ and k — classical protocol can be used in the half-duplex model and every half-duplex protocol can be simulated by a classical protocol of double depth where Alice sends only in even rounds and Bob sends only in odd rounds. In [HIMS18b, DIS+21], a series of non-trivial bounds were proved for various functions and KW relations.

We use CC^{hd} to denote the half-duplex communication complexity a communication problem with adversary.

Theorem 30 ([HIMS18b])**.** *For any non-empty finite set S, $\mathrm{CC}^{hd}(\mathrm{EQ}_S) \geq \log|S|/\log 2.5$.*

The main motivation to study half-duplex communication comes from the following lemma.

Lemma 31. *For all $n \in \mathbb{N}$, there exist a function $f : \mathbb{B}^n \to \mathbb{B}$ such that*

$$\mathrm{CC}(\mathrm{KW}_f) \geq \mathrm{CC}^{hd}(\mathrm{MUX}_n) - O(\log n).$$

The statement of this lemma seems almost trivial since it is easy to prove that there exists a function f such that $\mathrm{CC}(\mathrm{KW}_f) \geq n - O(\log n)$, and at the same time $\mathrm{CC}^{hd}(\mathrm{MUX}_n) \leq n + O(\log n)$. Nevertheless, we are going to prove it as a warm-up toward the proof of the main result to demonstrate how the half-duplex complexity comes into play. In the proof, Alice and Bob use the shortest protocols for given functions, and hence the lower bound on MUX_n would imply the existence of a hard function. Later when we will consider a multiplexer as a part of a XOR-composition with the universal relation, we will still be able to use the same argument to show the existence of a hard function.

Proof. Suppose that $\mathrm{CC}(\mathrm{KW}_f) \leq d$ for all $f : \mathbb{B}^n \to \mathbb{B}$. Consider the following half-duplex protocol for MUX_n. For every $f : \mathbb{B}^n \to \mathbb{B}$ let Π_f be the shortest (classical) protocol for KW_f. Alice, who is given f and x, follows the protocol Π_f using x as her input. Meanwhile Bob, who is given g and y, follows the protocol Π_g using y as his input. If f is different from g they might use different protocols, which is fine because we are in the half-duplex communication model.

When Alice reaches some leaf of Π_f she starts listening until the end of round d. Bob does the same. After d rounds of communication Alice has a candidate i for $x_i \neq y_i$, which is a valid output if $f = g$. Bob has a candidate j for $x_j \neq y_j$, that is equal to i if $f = g$. Now Alice and Bob just need to check that indeed $x_i \neq y_j$ and $i = j$, which can be done in $O(\log n)$. They output i if both conditions are true and $\perp$ otherwise. The total number of rounds of this half-duplex protocol for MUX_n is $d + O(\log n)$. □

This lemma shows that if we had a good understanding of half-duplex complexity we could translate lower bounds for multiplexer into the existence of a hard function. Unfortunately we will need to use a couple more tricks. Let CC^{phd} denotes partially half-duplex communication complexity of a communication problem with adversary.

Lemma 32. *For all $n \in \mathbb{N}$, there exists a function $f : \mathbb{B}^n \to \mathbb{B}$ such that*

$$\mathrm{CC}(\mathrm{KW}_f) \geq \mathrm{CC}^{phd}(\mathrm{MUX}_n) - O(\log n).$$

Proof. The proof follows from proof of Lemma 31 by observing that the protocol for MUX_n in there is partially half-duplex: if $f = g$ the the players in fact follow the same classical protocol for KW_f. □

Now we are going to demonstrate how to prove lower bounds for partially half-duplex protocols.

Lemma 33. *For all $n \in \mathbb{N}$, $\mathrm{CC}^{phd}(\mathrm{MUX}_n) \geq n - O(\log n)$.*

Proof. Let NEQ_{2^n} be a shortcut for non-equality on $\mathbb{B}^{2^n}$. We will show that $\mathrm{CC}^{phd}(\mathrm{MUX}_n) = d$ implies $\mathrm{NCC}(\mathrm{NEQ}_{2^n}) \leq d + O(\log n)$. Let Π be a partially half-duplex protocol for MUX_n. The main idea is that in partially half-duplex protocols for MUX_n any non-classical round indicates that the given functions are different. The non-deterministic protocol for NEQ_{2^n} goes as follows: the players guess a number $t \leq d$, a bit string $T \in \mathbb{B}^t$, and two bits $b_1, b_2 \in \mathbb{B}$. The players interpret T as a transcript of the first t rounds of Π such that it has only classical rounds (so, the communication can be described by t bits). Then they check that this transcript leads to a leaf marked with $\perp$ or to a non-classical round. To be more more precise, suppose Alice and Bob are given $f \in \mathbb{B}^{2^n}$ and $g \in \mathbb{B}^{2^n}$, respectively, as inputs for NEQ_{2^n}. The players guess a quadruple (t, T, b_1, b_2) as described. They have to check that

1. there exist $x \in f^{-1}(0)$ and $y \in g^{-1}(1)$ such that T is a valid transcript of the first t rounds of the protocol for MUX_n on input $((f, x), (g, y))$ assuming that all rounds are classical,
2. if $b_1 = 0$ then T is a transcript that ends up at a leaf labeled with $\perp$,
3. if $b_1 = 1$ and $b_2 = 0$ then both players were supposed to receive in round $t + 1$,
4. if $b_1 = 1$ and $b_2 = 1$ then both players were supposed to send in round $t + 1$.

Alice verifies that there exists x such that $f(x) = 0$ and T correctly describes first t rounds of communication on input (f, x). In addition, Alice checks the second condition and partially checks the last two conditions (i.e., if the third condition applies then Alice checks that she was supposed to receive in round $t+1$, and if the fourth condition applies then she checks that she was supposed to send). Bob does the symmetric thing for y such that $g(y) = 1$. If there exist x and y that pass all the checks then the protocol for MUX_n on $((f, x), (g, y))$ either returns $\perp$ or contains a non-classical round. In both cases this is sufficient proof that $f \neq g$. Moreover, such a witness exists if and only if $f \neq g$. The size of the witness is $d + \log d + 2 = d + O(\log n)$.

The described protocol can be used to non-deterministically solve non-equality on binary strings of length 2^n. Theorem 26 implies $\mathrm{NCC}(\mathrm{NEQ}_{2^n}) \geq n$, so we can conclude that $d \geq n - O(\log n)$. $\square$

The proof of this Lemma illustrates the important idea of reducing an instance of NEQ to the problem under consideration. Further in the paper, we will repeatedly use similar reductions.

3 Lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$

Let $\mathcal{P}$ be a set of all permutations of $\mathbb{B}^n$, and $N = 2^n$. Consider the following domain

$$\mathcal{X} = \mathcal{P} \times \mathbb{B}^n \times \mathbb{B}^n.$$

We are going to prove the following lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ on the rectangle $\mathcal{R} = \mathcal{X} \times \mathcal{X}$

$$\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{MUX}_n) \geq \mathrm{CC}_{\mathcal{R}}(\mathrm{U}_n \boxplus \mathrm{MUX}_n) \geq 1.5n - O(\log n),$$

and hence get the desired lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$.

Theorem 23. *For all $n \in \mathbb{N}$, $\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{MUX}_n) \geq 1.5n - o(n)$.*

To simplify our life a bit more we will stop applying g to one of the arguments inside $\mathrm{U}_n \boxplus \mathrm{MUX}_n$. Consider the following communication problem (where $g(x) \oplus g(y)$ is replaced with $x \oplus g(y)$).

Definition 34. In a *communication problem* $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ Alice is given $x_a, y_a \in \mathbb{B}^n$ and $g_a : \mathbb{B}^n \to \mathbb{B}^n$, Bob is given $x_b, y_b \in \mathbb{B}^n$ and $g_b : \mathbb{B}^n \to \mathbb{B}^n$. Their goal is to find $i \in [2n]$ such that $(x_a \circ y_a)_i \neq (x_b \circ y_b)_i$. If $x_a \oplus g_a(y_a) = x_b \oplus g_b(y_b)$ or $g_a \neq g_b$ they can output $\perp$.

If we can prove a lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ for it will also imply a lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$. The same argument works for classical communication, for half-duplex communication and for partially half-duplex communication.

Lemma 35. *For all $n \in \mathbb{N}$,*

$$\mathrm{CC}^*(\mathrm{U}_n \boxplus \mathrm{MUX}_n) \geq \mathrm{CC}^*(\mathrm{U}_n \boxplus \mathrm{MUX}'_n) - O(1),$$

where CC^* is one of CC, CC^{hd}, or CC^{phd}.

Proof. Suppose that $\mathrm{CC}^*(\mathrm{U}_n \boxplus \mathrm{MUX}_n) \leq h(n)$. Consider the following protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$. Alice is given x_a, y_a and g_a. Alice defines $x'_a = 0 \circ x_a$, $y'_a = 1 \circ y_a$, and

$$g'_a(b \circ z) = \begin{cases} 0 \circ z, & b = 0, \\ 0 \circ g_a(z), & b = 1. \end{cases}$$

Bob is given x_b, y_b and g_b. He defines x'_b, y'_b and g'_b in the same manner. Now the players can simulate the best protocol for $\mathrm{U}_{n+1} \circ \mathrm{MUX}_{n+1}$ of complexity at most $h(n+1) \leq h(n) + O(1)$ (this inequality is due to the linear upper bound on the complexity of $\mathrm{U}_n \boxplus \mathrm{MUX}_n$). Hence, $\mathrm{CC}^*(\mathrm{U}_n \boxplus \mathrm{MUX}'_n) \leq h(n) + O(1)$. $\square$

The proof consists of two stages. At the first stage we go down the protocol tree and find a node at depth almost n (more precisely at depth $n-3$) such that its rectangle contains many inputs that could be given to both to Alice and to Bob. Then we show that solving the problem on any large square requires depth about $\frac{n}{2}$. For the first stage we will use the following general lemma.

Lemma 36. *Let P be a communication problem such that on a square $S \times S$ every monochromatic rectangle $A \times B$ has $|A \cap B| \leq \frac{|S|}{2^r}$ for some $r \geq 1$. Then for every $d \leq r$, every protocol that solves P on $S \times S$ has a node at depth d with rectangle $A \times B$ such that $|A \cap B| \geq \frac{|S|}{2^d}$.*

Proof. Proof by induction: the base case $d = 0$ is obvious. Now suppose that there exists a node at depth $d-1$ with a rectangle $A' \times B'$ such that $|A' \cap B'| \geq \frac{|S|}{2^{d-1}}$. As $d-1 < r$ we know that $A' \times B'$ is not monochromatic, and hence this node is not a leaf. W.l.o.g, assume that this node corresponds to Alice speaking. Let $A_0 \times B'$ and $A_1 \times B'$ be the children's rectangles, where $A' = A_0 \cup A_1$ and $A_0 \cap A_1 = \emptyset$. So, for some $i \in \{0, 1\}$ we have $|A_i \cap B'| \geq \frac{1}{2}|A' \cap B'| \geq \frac{|S|}{2^d}$. Which concludes the proof. □

We derive the following lemma from Lemma 36.

Lemma 37. *For all natural $d \leq n$, any protocol tree that solves $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $\mathcal{R}$ has a node at depth d with a corresponding rectangle $A \times B$ such that $|A \cap B| \geq |\mathcal{X}|/2^d = N^2 \cdot |\mathcal{P}|/2^d$.*

Proof. Every monochromatic rectangle $A \times B$ of $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ is labeled with either an index or $\perp$. In the first case, $|A \cap B| = 0$. In the second case, for any $a = (g_a, x_a, y_a) \in A$ and $b = (g_b, x_b, y_b) \in B$ we have $g_a \neq g_b$ or $x_a \oplus g_a(y_a) = x_b \oplus g_b(y_b)$. We can subdivide all the elements of $C = A \cap B$ into 2^n disjoint groups $C = \bigcup_{z \in \mathbb{B}^n} C_z$, such that $(g, x, y) \in C_z$ if and only if $x \oplus g(y) = z$. For every two distinct $z_1, z_2 \in \mathbb{B}^n$ and inputs $(g_1, x_1, y_1) \in C_{z_1}$, $(g_2, x_2, y_2) \in C_{z_2}$, the permutations g_1 and g_2 are different (otherwise, $\perp$ would not be the correct output on this pair of inputs). Therefore, every permutation $g \in \mathcal{P}$ appear in at most one group. For fixed $g \in \mathcal{P}$ and $z \in \mathbb{B}^n$, there are only 2^n pairs $(x, y) : x \oplus g(y) = z$. That gives an upper bound on the number of elements in C, $|C| \leq 2^n \cdot |\mathcal{P}| = |\mathcal{X}|/2^n$. Application of Lemma 36 for $d \leq n$ concludes the proof. □

For the second lemma it is convenient to define the following combinatorial object that helps to understand the structure of a subset of inputs.

Definition 38. For a subset of inputs $S \subseteq \mathcal{X}$ we define *a domain graph* to be a bipartite graph $G_S = (U_S, V_S, E_S)$, such that $U_S \subseteq \mathcal{P}$, $V_S \subseteq \mathbb{B}^n \times \mathbb{B}^n$, and $(g, (x, y)) \in E_S \iff (g, x, y) \in S$.

The statement of the next lemma seems to be very technical. The high-level idea is the following. We consider a large enough subset of inputs $S \subseteq \mathcal{X}$ with two additional properties saying that every function in S is defined on sufficiently many inputs and that for fixed $g \in \mathcal{P}$ and $y \in \mathbb{B}^n$ there are only a few $x \in \mathbb{B}^n$ such that $(g, x, y) \in S$. The first property is easy to achieve and the second comes from the proof of Theorem 23. The lemma shows that from such S we can extract a large set of functions H that will allow us reduce solving non-deterministic communication problem NEQ_H to solving (deterministic) communication problem $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S \times S$. So, we will be able to translate a lower bound of $\log\log|H|$ on the non-deterministic complexity of NEQ_H to a lower bound on deterministic complexity of $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S \times S$.

Lemma 39. *Let $S \subseteq \mathcal{X}$ be a subset of inputs such that $|S| \geq N \cdot N!$, and let $G_S = (U_S, V_S, E_S)$ be a domain graph of S. If $\min_{g \in U_S}\{\deg_{G_S}(g)\} \geq 4N$ and*

$$\forall g \in \mathcal{P},\ \forall y \in \mathbb{B}^n,\ \left|\{x \mid (g,(x,y)) \in E_S\}\right| \leq \sqrt{N}, \tag{1}$$

then there is a set $H \subseteq U_S$ of size $2^{\Omega(\sqrt{N})}$ such that for all distinct $g_1, g_2 \in H$, there exist (x,y): $(g_1,x,y),(g_2,x,y) \in S$, and $g_1(y) \neq g_2(y)$.

Before we prove this lemma, lets look how it is used in the proof of Theorem 23.

Proof of Theorem 23. We start with applying Lemma 37 for $d = n-3$ to find a rectangle $A \times B$ such that $|A \cap B| \geq 8NN!$. Let $S = A \cap B$ and $G_S = (U_S, V_S, E_S)$ be a domain graph of S. Average degree of the vertices in U_S is at least $8NN!/N! = 8N$. To increase the minimum degree we throw out all the vertices of low degree. Let $S' = S \setminus \{(g,x,y) \mid \deg_{G_S}(g) < 4N\}$. The size of $|S'| > |S| - 4N \cdot |\mathcal{P}| = 4NN!$. Let $G_{S'} = (U_{S'}, V_{S'}, E_{S'})$ be a domain graph of S'.

If there is $g \in \mathcal{P}$ and $y \in \mathbb{B}^n$ such that $\left|\{x \mid (g,(x,y)) \in E_{S'}\}\right| > \sqrt{N}$ then the protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S' \times S'$ can be used to solve the equality problem on a set $W_{g,y} = \{x \mid (g,(x,y)) \in E_{S'}\}$. Given inputs $x_a, x_b \in W_{g,y}$, Alice and Bob simulate the protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S' \times S'$ for inputs (g, x_a, y) and (g, x_b, y). If the protocol outputs $\perp$ then the players output 1, otherwise they output 0. For for inputs (g, x_a, y) and (g, x_b, y), the protocol outputs $\perp$ if and only if $x_a = x_b$, so this reduction gives a correct protocol for $\mathrm{EQ}_{W_{g,y}}$ of the same depth. By Theorem 24 any protocol for $\mathrm{EQ}_{W_{g,y}}$ has depth at least $\log|W_{g,y}| \geq \log(\sqrt{N}) = n/2$. By the reduction, the same lower bound applies for the protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S' \times S'$.

Otherwise we apply Lemma 39 to construct a set H of size $2^{\Omega(\sqrt{N})}$. We are going to show that the protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S' \times S'$ can be used to non-deterministically solve NEQ_H. Suppose that Alice and Bob are given $g_1 \in H$ and $g_2 \in H$ respectively, and they want to non-deterministically verify that $g_1 \neq g_2$ using a privately non-deterministic protocol. Alice privately guesses (x_a, y_a) such that $(g_1, x_a, y_a) \in S'$ and $k \in [n]$, Bob privately guesses (x_b, y_b) such that $(g_2, x_b, y_b) \in S'$. At first, the players verify that $x_a \oplus g_a(y_a) \neq x_b \oplus g_b(x_b)$: Alice sends k together with the k-th bit of $x_a \oplus g_a(y_a)$ and Bob compares it with the k-th bit of $x_b \oplus g_b(y_b)$. If the bits are equal then they reject (i.e., the function defining the privately non-deterministic protocol on these inputs equals 0). Otherwise, the players run the protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S' \times S'$. If the protocol outputs $\perp$ then the private guesses give a valid proof of $g_1 \neq g_2$. Otherwise, if the protocol outputs some $i \in [2n]$ such that $(x_a, y_a)_i \neq (x_b, y_b)_i$ then the players reject. By Lemma 39, such private guesses exist for all distinct $g_1, g_2 \in H$. On the other hand, the statement of the problem $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ guarantees that if $x_a \oplus g_a(y_a) \neq x_b \oplus g_b(x_b)$ then the protocol can output $\perp$ only if $g_1 \neq g_2$. Thus, the depth of the protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S' \times S'$ is at least

$$\mathrm{NCC}'(\mathrm{NEQ}_H) - O(\log n) = \log\log|H| - O(\log n) \geq n/2 - O(\log n).$$

Finally, we use Lemma 35 to translate the lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ to $\mathrm{U}_n \boxplus \mathrm{MUX}_n$.

□

Now it is time to prove Lemma 39.

Proof of Lemma 39. 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 $(x_v, y_v) \in V_S$,
- for every leaf ℓ labeled with F_ℓ and every it's ancestor labeled with (x, y) there exists $a \in \mathbb{B}^n$ such that $\forall g \in F_\ell$, $g(y) = a$ and $(g, x, y) \in S$.
- for every two leaves labeled with F_1 and F_2, and their lowest common ancestor labeled with (x, y): $F_1 \cap F_2 = \emptyset$ and for all $g_1 \in F_1$, $g_2 \in F_2$, such that $g_1(y) \neq g_2(y)$,
- the number of leaves is a least $\frac{3^{\sqrt{N}}}{N}$.

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 $g_1, g_2 \in H$, $g_1 \neq g_2$, there exist (x, y), the label of the least common ancestor of corresponding leaves, such that $(g_1, x, y), (g_2, x, y) \in S$, and $g_1(y) \neq g_2(y)$.

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 $\min_{g \in U_Z}\{\deg_{G_Z}(g)\} \geq 2N$ then the rooted tree $T(Z)$ consists of a root node labelled with (x_Z, y_Z), where (x_Z, y_Z) is a vertex of maximal degree in V_Z, and a set of subtrees — for every $a \in \mathbb{B}^n$ such that $\exists g \in U_Z : (g, x_Z, y_Z) \in Z, g(y_Z) = a$ there is a subtree $T(Z_a)$ attached to the root node, where

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

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 $\sqrt{N} + 1$. Let z be some node of $T(S)$ at depth $d \leq \sqrt{N}$ labeled with (x_Z, y_Z) corresponding 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 $4N - d\sqrt{N} \geq 3N$. At the same time $|V_Z| \leq N(N - d)$. Let $T(Z_{a_1}), \dots, T(Z_{a_k})$ — 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 $Z_{a_1}, \dots, Z_{a_k}$ is exactly the number of functions in Z defined on (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,

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

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 $|S|/N^2 \geq N!/N$. 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 $d = \sqrt{N} + 1$ we get the desired lower bound $\frac{3^{\sqrt{N}}}{N} = 2^{\Omega(\sqrt{N})}$ on the number of leaves. $\square$

4 Lower bound for $\mathrm{U}_n \boxplus \mathrm{KW}_g$

Our final goal is to show hardness of $\mathrm{U}_n \boxplus g$ for some function $g : \mathbb{B}^n \to \mathbb{B}^n$. Showing the lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ was the first step in this direction. As we discussed it earlier, it might be tempting to try to show that that hardness of multiplexer implies existence of a hard function. Unfortunately, the question whether that is true has remained open for decades. To get around this issue we will gradually extend the lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ using results from half-duplex communication complexity.

We start with extending the lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ to the half-duplex model.

Theorem 40. *For all $n \in \mathbb{N}$,*

$$\mathrm{CC}^{hd}(\mathrm{U}_n \boxplus \mathrm{MUX}_n) \geq \left(\frac{1}{\log \frac{5}{2}} + \frac{1}{4}\right) n - O(1) \geq 1.006n - O(1).$$

The proof of this theorem mimics the proof for the classical case (Theorem 23). During the first stage, given a protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ we will find a large enough square $S \times S$, such that it is significantly easier to solve $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on this square. Then we will show that on every big square the problem is still hard. Finally, we apply Lemma 35 to get a result for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$. The following lemma lower bounds the size of a square for the first stage.

Lemma 41. *Let Π be a half-duplex protocol of length d that solves a communication problem on a rectangle $U \times U$. For every $t \leq d$ there exist a subset $S \subset U$ of size at least $(\frac{2}{5})^t \cdot |U|$, and a half-duplex protocol Π' of length $d - t$ that gives the same output as Π for all inputs from $S \times S$.*

Proof. In [HIMS18a, Theorem 22], it is shown for $t = 1$. The general case follows by induction. □

Now we are ready to prove Theorem 40.

Proof of Theorem 40. Suppose $\mathrm{CC}^{hd}(\mathrm{U}_n \boxplus \mathrm{MUX}'_n) = d$ and let $t = \frac{n-3}{\log 2.5}$. According to Lemma 41 there is a subset $S \subset \mathcal{X}$ of size

$$|S| \geq \left(\frac{2}{5}\right)^t \cdot |\mathcal{X}| = \frac{8}{N} \cdot N^2 N! = 8NN!,$$

and a half-duplex protocol length $d - \frac{n-3}{\log 2.5}$ that can solve $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S \times S$. Any half-duplex protocol can be transformed into a classical one while at most doubling the length [HIMS18b]. Then there is a length $2(d - \frac{n-3}{\log 2.5})$ classical protocol that solves $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S \times S$.

We apply the same argument as in the proof of Theorem 23 where we used Lemma 39 to solve NEQ_H using privately non-deterministic protocol, and we get

$$2\left(d - \frac{n-3}{\log 2.5}\right) \geq \frac{n}{2}.$$

Which gives us the following lower bound

$$d \geq \left(\frac{1}{\log 2.5} + \frac{1}{4}\right) n - O(1) > 1.006n - O(1).$$

Finally, we use Lemma 35 to translate this lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ to $\mathrm{U}_n \boxplus \mathrm{MUX}_n$. □

Out next step is to relate the complexities of problems $\mathrm{U}_n \boxplus \mathrm{KW}_g$ and $\mathrm{U}_n \boxplus \mathrm{MUX}_n$.

Lemma 42. *There exists $g : \mathbb{B}^n \to \mathbb{B}^n$ such that*

$$\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}_g) \geq \mathrm{CC}^{hd}(\mathrm{U}_n \boxplus \mathrm{MUX}_n) - O(\log n).$$

The proof is almost identical to the proof of Lemma 31. Note that, in contrast to Lemma 31, the statement of this Lemma does not seem to be trivial.

Proof. Suppose that $\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}_g) \leq d$ for all $g : \mathbb{B}^n \to \mathbb{B}^n$. Consider the following half-duplex protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$. For every $g : \mathbb{B}^n \to \mathbb{B}^n$ let Π_g be the shortest (classical) protocol for $\mathrm{U}_n \boxplus \mathrm{KW}_g$. Alice, who is given x_a, y_a and g_a, follows protocol Π_{g_a} on input (x_a, y_a). Meanwhile Bob, who is given x_b, y_b and g_b, follows protocol Π_{g_b} on input (x_b, y_b). If g_a is different from g_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_{g_a} she starts listening until the end of round d. Bob does the same. After d rounds of communication Alice has a candidate i for $(x_a \circ y_a)_i \neq (x_b \circ y_b)_i$, which is a valid output if $g_a = g_b$. Bob has a candidate j for $(x_a \circ y_a)_j \neq (x_b \circ y_b)_j$, that is equal to i if $g_a = g_b$. Now Alice and Bob need to check that indeed $(x_a \circ y_a)_i \neq (x_b \circ y_b)_j$ and $i = j$, which can be done in $O(\log n)$. They output i if both conditions are true and $\perp$ otherwise. The total number of rounds of this half-duplex protocol for $\mathrm{U}_n \boxplus \mathrm{KW}_g$ is $d + O(\log n)$. $\square$

Immediately we get the following theorem.

Theorem 43. *There exists $g : \mathbb{B}^n \to \mathbb{B}^n$ such that*

$$\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}_g) \geq 1.006n.$$

To improve this bound we will have to look deeper into the protocol structure and use the fact that it is partially half-duplex.

Definition 44. A half-duplex protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ 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 listen simultaneously if $g_a = g_b$.

We are going to need the following analogue of Lemma 42.

Lemma 45. *There exists $g : \mathbb{B}^n \to \mathbb{B}^n$ such that*

$$\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}_g) \geq \mathrm{CC}^{phd}(\mathrm{U}_n \boxplus \mathrm{MUX}_n) - O(\log n).$$

Proof. Note that the protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ in the proof of Lemma 42 is partially half-duplex (i.e., it has only classical rounds unless $g_a \neq g_b$). The rest of the proof is identical to the proof of Lemma 42. $\square$

Next Lemma proves a lower bound on the partially half-duplex complexity of $\mathrm{U}_n \boxplus \mathrm{MUX}_n$.

Lemma 46. *Any partially half-duplex protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ has depth at least $\frac{3}{2}n - O(\log n)$.*

Together with Lemma 42, this lemma immediately implies our main result that the XOR-KRW holds for a composition of the universal relation with the KW-game for some function.

Theorem 21. *For all $n \in \mathbb{N}$, there exists $g : \mathbb{B}^n \to \mathbb{B}^n$ such that*

$$\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}_g) \geq 1.5n - O(\log n).$$

Once again we are going to split the proof of Lemma 46 in two parts. In the first part, instead of finding one large subrectangle we will find a collection of subrectangles. 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 47. *For any partially half-duplex protocol Π for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$, there exists a subset of inputs $S \subset \mathcal{X}$, $|S| \geq 8NN!$, and a string $T \in \mathbb{B}^{n-3}$, such that if Alice and Bob are given the same input from S then the transcript of the first $n-3$ rounds is equal to T.*

Proof. Let $D = \{((g,x,y),(g,x,y)) \mid (g,x,y) \in \mathcal{X}\}$ be a subset of inputs where Alice's and Bob'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 $n-3$ rounds of communication. There are at most 2^{n-3} different transcripts of length $n-3$, so there is a transcript T that corresponds to at least $|D|/2^{n-3} = 8NN!$ inputs from D. Let S be the set of all these inputs. $\square$

The difference from what we have seen before is 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 $n-3$ 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.

Now we will prove Lemma 46 by showing that if $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ has a short protocol then we can use it to solve either equality or non-equality more efficiently than it is possible using a dichotomy similar to one from the proof of Theorem 23.

Proof of Lemma 46. Suppose that Π is a partially half-duplex protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ of depth d. Let S be the set provided by Lemma 47. Let $S' = S \setminus \{(g,x,y) \mid \deg_{G_S}(g) < 4N\}$, so $|S'| > 4NN!$. 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 $4N$.

Suppose that there is $g \in \mathcal{P}$ and $y \in \mathbb{B}^n$ such that $\left|\{x \mid (g,(x,y)) \in E_{S'}\}\right| > \sqrt{N}$. Let $S_{g,y} = \{(g,x,y) \mid (g,(x,y)) \in E_{S'}\}$. We can extract from Π a classical protocol of depth at most $d-n-3$ that solves $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S_{g,y} \times S_{g,y}$. This follows from the fact that Π s partially half-duplex, so it has only classical rounds for inputs from $S_{g,y} \times S_{g,y}$. To solve $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ on $S_{g,y} \times S_{g,y}$ the players would have to solve the equality problem for $W_{g,y} = \{x \mid (g,(x,y)) \in E_{S'}\}$

that requires at least $\log|W_{g,u}| \geq \log(\sqrt{N}) = n/2$. The reduction is the same as in the proof of Theorem 23. Thus, we have $d \geq 1.5n - 3$.

Otherwise we apply Lemma 39 to construct a set H of size at least $2^{\Omega(2^{n/2})}$. Then the protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ 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 $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ is similar to the one we have seen in the proof of Theorem 23 with just a few twists.

Let's first see what are the necessary and sufficient conditions for $g_a, g_b \in H$ to be not equal. Let $R_{g_a,g_b} = \{((g_a, x_a, y_a), (g_b, x_b, y_b)) \in S' \times S' \mid x_a \oplus g_a(y_a) \neq x_b \oplus g_b(y_b)\}$.

- On elements of $D = \{((g, x, y), (g, x, y)) \mid (g, x, y) \in S'\}$ that contain g_a and g_b, the protocol Π performs differently during the first $n-3$ rounds. The partial transcript T of the first $n-3$ rounds of Π on elements of D is fixed by Lemma 47, 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 $g_a \neq g_b$ — for every fixed $g_a = g_b$ 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_{g_a,g_b}. If $g_a = g_b$ then Π can only perform classical rounds by the definition of partially half-duplex communication.

- Π performs classically on some input from R_{g_a,g_b} and returns $\perp$.

We can argue that one of this conditions is satisfied iff $g_a \neq g_b$. Indeed, suppose that $g_a \neq g_b$. If the first or the second condition is satisfied we are done, so let's assume that it is not. The first $n-3$ rounds of Π on inputs from R_{g_a,g_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 x, y, such that (g_a, x, y) and (g_b, x, y) belong to S', and also $x \oplus g_a(y) \neq x \oplus g_b(y)$. By the definition of $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ the protocol Π has to output $\perp$, and hence satisfy the third condition.

Now suppose that $g_a = g_b$. 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 definition of the $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$.

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 $n-3$ rounds. Verification requires only $\log n$ bits of communication.

- For the second condition the players guess a number $t \in [d-n+3]$, a string $s \in \mathbb{B}^t$, a number $k \in [n]$, and bits b, p. Then they verify that there exist pairs (x_a, y_a) and (x_b, y_b) such that:
  - $p = (x_a \oplus g_a(y_a))_k \neq (x_b \oplus g_b(y_b))_k = 1 - p$,
  - both players are consisted with s being an extension of the partial transcript T on inputs $((g_a, x_a, y_a), (g_b, x_b, y_b))$, 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 $b = 1$) or both receive (in case $b = 0$).

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

- For the third condition the players guess a string $s \in \mathbb{B}^{d-n+3}$, a number $i \in [n]$, and a bit p. Then they verify that there exist pairs (x_a, y_a) and (x_b, y_b) such that:
  - $p = (x_a \oplus g_a(y_a))_k \neq (x_b \oplus g_b(y_b))_k = 1 - p$,
  - both players are consisted with s being an extension of the partial transcript T on inputs $((g_a, x_a, y_a), (g_b, x_b, y_b))$, 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 marked labeled $\perp$.

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

This reduction shows that NEQ_H can be non-deterministically solved with a protocol of size $d - n + O(\log n)$. Thus, the depth of the protocol for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ is at least

$$n + \mathrm{NCC}(\mathrm{NEQ}_H) - O(\log n) \geq n + \log\log|H| - O(\log n)$$
$$\geq n + \log\sqrt{N} - O(\log\log(N)) = 1.5n - O(\log n).$$

Finally, we use Lemma 35 to translate this lower bound for $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ to $\mathrm{U}_n \boxplus \mathrm{MUX}_n$. □

5 Conclusion

In this paper we presented a lower bound for $\mathrm{U}_n \boxplus \mathrm{KW}_g$ for some function g. Our result complements the result from [GMWW17] where a lower bound for $\mathrm{KW}_g \diamond \mathrm{U}_n$ was shown. It remains to understand if the techniques from these two papers can be forced to work in harmony. We are very optimistic about it: the structure of our proof reminds of the first results regarding $\mathrm{U}_m \diamond \mathrm{U}_n$ from [EIRS01]: we maintain the symmetry for as long as possible and then show that some of the hardness still remains in the problem. The proof from [GMWW17] shows how to substitute the symmetry with some hardness measure and hopefully the same magic can be applied to this instance.

5.1 Open questions

1. Is there a generic ways to convert lower bounds for classical communication into half-duplex and partially half-duplex?

2. Is there another proof of the results from this paper, that doesn't rely on non-classical models?

3. Prove lower bound of $2n - o(n)$ for $\mathrm{U}_n \boxplus \mathrm{MUX}_n$ in classical, partially half-duplex or half-duplex model.

4. Prove that for some $f, g : \mathbb{B}^n \to \mathbb{B}^n$, $\mathrm{CC}(\mathrm{KW}_{f \boxplus g}) \geq (1 + \epsilon)n$.

Acknowledgement

We would like to thank the anonymous reviewers who have done a tremendous job carefully reading our paper and whose detailed comments helped us significantly improve the text of the paper and make it more readable.

A Lower bound for a block-composition of a universal relation and a function

Definition 48. Let $g : \{0,1\}^m \to \{0,1\}$ be a Boolean function. *The block-composition of a universal relation with a function* $\mathrm{U} \diamond g$ is the following relation:

$$\mathrm{U}_n \diamond g_m = \{(A, B, (i,j)) \mid A[i,j] \neq B[i,j]\} \cup \{(A, B, \perp) \mid \forall i \in [n] : g(A[i]) = g(B[i])\},$$

where $A, B \in \{0,1\}^{n \times m}$.

Theorem 49. *There exists* $f : \{0,1\}^n \to \{0,1\}$*, such that:* $\mathrm{CC}(\mathrm{U}_n \diamond f_n) \geq 1.5n - O(\log n)$*.*

In order to prove this, we need to argue that the result in Theorem 21 also holds for the following version of $\mathrm{U}_n \boxplus \mathrm{KW}_g$.

Definition 50. Let $g : \mathbb{B}^n \to \mathbb{B}^n$. In a communication game $\mathrm{U}_n \boxplus \mathrm{KW}'_g$: Alice is given $x_a, y_a \in \mathbb{B}^n$ and Bob is given $x_b, y_b \in \mathbb{B}_n$. Their goal is to find $i \in [2n]$ such that $(x_a \circ y_a)_i \neq (x_b \circ y_b)_i$. If $x_a \oplus g(y_a) = x_b \oplus g(y_b)$ they can output $\perp$.

This problem relates to $\mathrm{U}_n \boxplus \mathrm{KW}_g$ as $\mathrm{U}_n \boxplus \mathrm{MUX}'_n$ relates to $\mathrm{U}_n \boxplus \mathrm{MUX}_n$. If fact, if we do not use Lemma 35 in the proof of Theorem 21 then we prove the following lower bound.

Theorem 51. *For all* $n \in \mathbb{N}$*, there exists* $g : \mathbb{B}^n \to \mathbb{B}^n$ *such that*

$$\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}'_g) \geq 1.5n - O(\log n).$$

Now we are ready to prove the lower bound for the block-composition.

Proof of Theorem 49. We prove this Theorem by a reduction from $\mathrm{U}_n \boxplus \mathrm{KW}'_g$. Let $g : \{0,1\}^n \to \{0,1\}^n$ be such that

$$\mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}'_g) \geq 1.5n - O(\log n).$$

Let $f : \{0,1\}^{n+\log n+1} \to \{0,1\}$ be a function that treats it's input x as a n-bit string x', a number $i_x \in [n]$ and a bit b_x. In these terms

$$f(x) = b_x \oplus g(x')[i_x].$$

Given x_a, y_a Alice constructs a matrix A as follows: in the i-th row she puts y_a as the first n bits, then she puts i in binary as the next $\log n$ bits and she adds $x_a[i]$ as the last bit. Then she adds $\log n + 1$ rows with zeroes. As a result she gets a matrix $A \in \{0,1\}^{l \times l}$ for $l = n + \log n + 1$. Bob does the symmetric thing and gets a matrix B. Now it is not hard to see that for every $i \in [n]$, $(x_a \oplus g(y_a))[i] = f(A[i])$. Thus, if we have solved $\mathrm{U}_l \diamond f_l$ on (A, B) and the result was $\perp$ then $\perp$ is the correct answer for $\mathrm{U}_n \boxplus \mathrm{KW}'_g$. Now suppose that $A[i,j] \neq B[i,j]$. If $i = n + \log n + 1$ then $x_a[j] \neq x_b[j]$. If $i \leq n$ then $y_a[i] \neq y_b[i]$. That gives us

$$\mathrm{CC}(\mathrm{U}_l \diamond f_l) \geq \mathrm{CC}(\mathrm{U}_n \boxplus \mathrm{KW}'_g) \geq 1.5n - O(\log n),$$

and hence

$$\mathrm{CC}(\mathrm{U}_n \diamond f_n) \geq 1.5n - O(\log n).$$

□

B Proof of Theorem 9

Theorem 9. *For any $m, n \in \mathbb{N}$ with $n \geq 6 \log m$, and any non-constant function $f : \{0,1\}^m \to \{0,1\}$,*

$$\mathrm{CC}(\mathrm{KW}_{f \diamond \mathsf{M}_n}) \geq \log L(f) + n - O(\log^* n).$$

Proof. First of all, we show that for any non-constant function $f : \mathbb{B}^m \to \mathbb{B}$,

$$\mathrm{CC}(\mathrm{KW}_{f \diamond \mathsf{M}_n}) \geq \mathrm{CC}(\mathrm{KW}_f \diamond \mathrm{U}_n) - O(\log n)$$

by reducing $\mathrm{KW}_f \diamond \mathrm{U}_n$ to $\mathrm{KW}_{f \diamond \mathsf{M}_n}$, and then we apply the lower bound on $\mathrm{CC}(\mathrm{KW}_f \diamond \mathrm{U}_n)$ proved in [GMWW17, KM18].

Consider a communication game $\mathrm{KW}_f \diamond \mathrm{U}_n$: Alice and Bob are given (x, X) and (y, Y) respectively, where $x \in f^{-1}(0)$, $y \in f^{-1}(1)$, $X, Y \in \mathbb{B}^{m \times n}$, and they want to find a position where X and Y differ. The following construction describes a reduction from this game to $\mathrm{KW}_{f \diamond \mathsf{M}_n}$. Given x and X Alice defines functions $s_1, \ldots, s_n$:

$$s_i(r) = \begin{cases} x[i], & r = X_i \\ 0, & \text{otherwise,} \end{cases}$$

where X_i is the i-th row of X. Given y and Y Bob defines functions $t_1, \ldots, t_n$ in the same way. The reduction guarantees that

$$(f \diamond \mathsf{M}_n)(s_1, X_1, \ldots, s_m, X_m) = 0 \quad \text{and} \quad (f \diamond \mathsf{M}_n)(t_1, Y_1, \ldots, t_m, Y_m) = 1,$$

and hence the players can simulate the KW game for $f \diamond \mathsf{M}_n$ on these inputs. There are two possible outcomes of such a game: Alice and Bob find a difference between either some rows X_i and Y_i or some functions s_i and t_i.

In the first case, they are done — the players have found a difference between X and Y. In the second case, Alice and Bob find a position where two functions s_i and t_i differ for some $i \in [m]$, i.e., at the end of the protocol they both know some r such that $s_i(r) \neq t_i(r)$. Then either $r = X_i$ or $r = Y_i$. Using two extra bits of communication Alice and Bob can find out which of these two cases applies. If $r = X_i \neq Y_i$ then Bob can find a position where $r = X_i$ and Y_i differ, and send it to Alice using $\log n$ bits. The other case is symmetric.

The reduction shows that

$$\mathrm{CC}(\mathrm{KW}_f \diamond \mathrm{U}_n) \leq \mathrm{CC}(\mathrm{KW}_{f \diamond \mathsf{M}_n}) + O(\log n).$$

To complete the proof we use the following bound from [KM18]:

$$\mathrm{CC}(\mathrm{KW}_f \diamond \mathrm{U}_n) \geq \log \mathrm{L}(f) + n - O(\log^* n). \qquad \square$$

References

[DIS+21] Yuriy Dementiev, Artur Ignatiev, Vyacheslav Sidelnik, Alexander Smal, and Mikhail Ushakov. New bounds on the half-duplex communication complexity. In *SOFSEM 2021: Theory and Practice of Computer Science - 47th International Conference on Current Trends in Theory and Practice of Computer Science, SOFSEM 2021, Bolzano-Bozen, Italy, January 25-29, 2021, Proceedings*, volume 12607 of *Lecture Notes in Computer Science*, pages 233–248. Springer, 2021.

[DM18] Irit Dinur and Or Meir. Toward the KRW composition conjecture: Cubic formula lower bounds via communication complexity. *Comput. Complex.*, 27(3):375–462, 2018.

[dRMN+20] Susanna F. de Rezende, Or Meir, Jakob Nordström, Toniann Pitassi, and Robert Robere. KRW composition theorems via lifting. In *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*, pages 43–49. IEEE, 2020.

[EIRS01] Jeff Edmonds, Russell Impagliazzo, Steven Rudich, and Jirí Sgall. Communication complexity towards lower bounds on circuit depth. *Comput. Complex.*, 10(3):210–246, 2001.

[GMWW17] 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.

[Hås98] Johan Håstad. The shrinkage exponent of de morgan formulas is 2. *SIAM J. Comput.*, 27(1):48–64, 1998.

[HIMS18a] Kenneth Hoover, Russell Impagliazzo, Ivan Mihajlin, and Alexander Smal. Half-duplex communication complexity. *Electronic Colloquium on Computational Complexity (ECCC)*, 25:89, 2018.

[HIMS18b] Kenneth Hoover, Russell Impagliazzo, Ivan Mihajlin, and Alexander V. Smal. Half-duplex communication complexity. In Wen-Lian Hsu, Der-Tsai Lee, and Chung-Shou Liao, editors, *29th International Symposium on Algorithms and Computation, ISAAC 2018, December 16-19, 2018, Jiaoxi, Yilan, Taiwan*, volume 123 of *LIPIcs*, pages 10:1–10:12. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.

[HW90] Johan Håstad and Avi Wigderson. Composition of the universal relation. In Jin-Yi Cai, editor, *Advances In Computational Complexity Theory, Proceedings of a DIMACS Workshop, New Jersey, USA, December 3-7, 1990*, volume 13 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 119–134. DIMACS/AMS, 1990.

[Khr71] 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.

[KM18] Sajin Koroth and Or Meir. Improved Composition Theorems for Functions and Relations. In Eric Blais, Klaus Jansen, José D. P. Rolim, and David Steurer, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2018)*, volume 116 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 48:1–48:18, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

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

[KRW95] 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.

[KW88] Mauricio Karchmer and Avi Wigderson. Monotone circuits for connectivity require super-logarithmic depth. In Janos Simon, editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 539–550. ACM, 1988.

[Mei20] Or Meir. Toward better depth lower bounds: Two results on the multiplexor relation. *Comput. Complex.*, 29(1):4, 2020.

[RR97] Alexander A. Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24–35, 1997.

[Sub61] 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.

[Tal14] Avishay Tal. Shrinkage of de morgan formulae by spectral techniques. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, pages 551–560. IEEE Computer Society, 2014.

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il