Electronic Colloquium on Computational Complexity, Report No. 120 (2019)

Toward Better Depth Lower Bounds: Two Results on the Multiplexor Relation

Or Meir*

September 11, 2019

Abstract

One of the major open problems in complexity theory is proving super-logarithmic lower bounds on the depth of circuits (i.e., $\mathbf{P} \not\subseteq \mathbf{NC}^1$). Karchmer, Raz, and Wigderson [KRW95] suggested to approach this problem by proving that depth complexity behaves "as expected" with respect to the composition of functions $f \diamond g$. They showed that the validity of this conjecture would imply that $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

As a way to realize this program, Edmonds et. al. [EIRS01] suggested to study the "multiplexor relation" MUX, which is a simplification of functions. In this note, we present two results regarding this relation:

- The multiplexor relation is "complete" for the approach of [KRW95] in the following sense: if we could prove (a variant of) their conjecture for the composition $f \diamond MUX$ for every function f, then this would imply $\mathbf{P} \not\subseteq \mathbf{NC}^1$.
- A simpler proof of a lower bound for the multiplexor relation due to [EIRS01]. Our proof has the additional benefit of fitting better with the machinery used in previous works on the subject.

1 Introduction

A major frontier of the research on circuit complexity is proving super-logarithmic lower bounds on the depth complexity of an explicit function, i.e., proving that $\mathbf{P} \not\subseteq \mathbf{NC}^1$. Karchmer, Raz, and Wigderson [KRW95] proposed to approach this problem by studying the (block-)composition of boolean functions, defined as follows: if $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ are boolean functions, then their composition $f \diamond g$ takes inputs in $(\{0,1\}^n)^m$ and is defined by

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

Let us denote by $\mathsf{D}(f)$ the minimal depth of a circuit that computes f with fan-in 2. It is easy to see that $\mathsf{D}(f \diamond g) \leq \mathsf{D}(f) + \mathsf{D}(g)$. Karchmer, Raz, and Wigderson [KRW95] conjectured that this upper bound is roughly optimal:

Conjecture 1.1 (The KRW conjecture)**.** *Let $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ be non-constant functions. Then*

$$\mathsf{D}(f \diamond g) \approx \mathsf{D}(f) + \mathsf{D}(g). \tag{1}$$

*Department of Computer Science, University of Haifa, Haifa 3498838, Israel. ormeir@cs.haifa.ac.il. Partially supported by the Israel Science Foundation (grant No. 1445/16).

ISSN 1433-8092

[KRW95] observed that this conjecture, if proved, would imply that $\mathbf{P} \not\subseteq \mathbf{NC}^1$. To see why, consider the function $F : \{0,1\}^{2^N} \to \{0,1\}$, which takes as input the truth table of a function $f : \{0,1\}^{\log N} \to \{0,1\}$ and a string $\overline{x} \in \{0,1\}^N$, and computes

$$F(f, \overline{x}) = (\underbrace{f \diamond \ldots \diamond f}_{\frac{\log N}{\log \log N} \text{ times}})(\overline{x}). \tag{2}$$

It can be verified that $\overline{x}$ is indeed a valid input for the function $f \diamond \ldots \diamond f$. We claim that F has depth complexity $\approx \frac{\log^2 N}{\log \log N}$: to see it, observe that we can fix f to be a (non-explicit) function with maximal depth complexity of $\approx \log N$, and then the KRW conjecture implies that

$$\mathsf{D}(F) = \mathsf{D}(f \diamond \ldots \diamond f) \approx \frac{\log N}{\log \log N} \cdot \mathsf{D}(f) \approx \frac{\log^2 N}{\log \log N}.$$

In this note, we present two results toward realizing this approach. Below, we explain the relevant background, and then describe our contribution in more detail.

Karchmer-Wigderson relations. [KRW95] suggested to study their conjecture using the framework of Karchmer-Wigderson relations [KW90]. Given a function $f : \{0,1\}^n \to \{0,1\}$, the *Karchmer-Wigderson relation* KW_f (or "KW relation" for short) is the following communication problem: Alice gets an input $x \in f^{-1}(1)$, and Bob gets as input $y \in f^{-1}(0)$. The goal of Alice and Bob is to find a coordinate $i \in [n]$ such that $x_i \neq y_i$. Karchmer and Wigderson [KW90] observed that the communication complexity of KW_f is exactly equal to $\mathsf{D}(f)$. This observation allows us to study questions about depth complexity from the perspective of communication complexity.

Previous work on the KRW conjecture. As a first step toward resolving their conjecture, [KRW95] suggested to prove it for the universal relation U, which is a simplification of KW relations. This challenge was met by Edmonds et. al. [EIRS01], who proved the KRW conjecture for the composition $U \diamond U$, and an alternative proof was given later[1] by Håstad and Wigderson [HW93].

More recently, Gavinsky et. al. [GMWW17] proved a version of the KRW conjecture for compositions of the form $f \diamond U$, where f can be any non-constant function, and this result was improved quantitatively by Koroth and Meir [KM18]. In addition, the work of Håstad on the shrinkage exponent [Hås98] implicitly proved the KRW conjecture for compositions of the form $f \diamond \bigoplus$, where $\bigoplus$ is the parity function and f is any non-constant function. Dinur and Meir [DM18] gave an alternative proof of the latter result using the framework of KW relations, thus being more in line with the works of [KRW95, EIRS01, GMWW17, KM18].

A major difficulty in proving the KRW conjecture is that it requires us to prove a lower bound for arbitrary choices of f and g. The previous works seem to suggest that the crux of the difficulty lies in dealing with an arbitrary choice of the function g (since the previous works can already handle an arbitrary choice of f). In this paper, we discuss a way to bypass the need to deal with an arbitrary choice of g. To this end, we first discuss the multiplexor relation of [EIRS01].

The multiplexor relation. Instead of proving the full KRW conjecture, one could prove[2] that $\mathbf{P} \not\subseteq \mathbf{NC}^1$ by proving a depth lower bound directly on the function F of Equation (2). Proving a

[1] [HW93] appears to be earlier than [KRW95] and [EIRS01] in the citations because we cite the journal version of those works. The conference versions of [KRW95] and [EIRS01] appeared in 1991.

[2] This approach was suggested by [EIRS01] and independently by Karchmer (see [HW93]).

lower bound on F might be easier, since now the function f becomes part of the input, and thus we can choose f in any way that serves our argument.

Motivated by this consideration, [EIRS01] defined the "multiplexor relation", which is a KW relation in which the function f is part of the input. Formally, the multiplexor relation MUX_n is the following communication problem: Alice gets a function $f : \{0,1\}^n \to \{0,1\}$ and an input $x \in f^{-1}(1)$. Bob gets *the same function* f and an input $y \in f^{-1}(0)$. Their goal is to find a coordinate $i \in [n]$ such that $x_i \neq y_i$.

The communication complexity of MUX_n is known to be at most $n+2$ by a protocol of [TZ97]. It is easy to prove a corresponding lower bound of $n - \log\log n + \Theta(1)$ using a counting argument. However, such an argument does not fit well with the framework of KW relations. Thus, [EIRS01] gave an alternative proof of a lower bound of $\Omega(n)$, based on an adversary argument. Our second main contribution is a simpler version of that argument.

Our contribution. In this work, we study a composition of the form $f \diamond MUX$, where f is an arbitrary function. We propose a version of the KRW conjecture for this composition, and show[3] that this conjecture implies that $\mathbf{P} \not\subseteq \mathbf{NC}^1$. In a sense, this shows that the MUX relation is "complete" for the KRW conjecture. In particular, it provides a way to bypass the need to deal with an arbitrary choice of g. In light of the previous works on the KRW conjecture, dealing with the composition $f \diamond MUX$ might be within reach. We believe that proving the conjecture on $f \diamond MUX$ is a good direction for separating $\mathbf{P}$ from $\mathbf{NC}$, and we discuss it in Section 2.

Our second contribution is a simpler version of the lower bound on MUX of [EIRS01]. In particular, our adversary argument should be easier to combine with the techniques used in previous works on the KRW conjecture. Thus, this argument might be useful for proving the conjecture on $f \diamond MUX$. We present this result in Section 3.

Preliminaries. For $n \in \mathbb{N}$, we denote $[n] \stackrel{\text{def}}{=} \{1, \ldots n\}$. We use the standard definitions of communication complexity — see the book of Kushilevitz and Nisan [KN97] for more details. Given Given a communication problem P, we denote the *deterministic* communication complexity of P by $\mathsf{C}(P)$.

2 The composition $f \diamond MUX$

In this section, we define the composition $f \diamond MUX$ and discuss its applications to separating $\mathbf{NC}^1$ from $\mathbf{P}$. As a warm-up for the definition of $f \diamond MUX$, it is useful to recall how the KW relation of the composed function $f \diamond g$ looks like. Let $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ be boolean functions. In the KW relation $KW_{f \diamond g}$, Alice gets strings $x_1, \ldots, x_m \in \{0,1\}^n$ and Bob gets strings $y_1, \ldots, y_m \in \{0,1\}^n$. We define strings $a, b \in \{0,1\}^m$ as follows:

$$a \stackrel{\text{def}}{=} (g(x_1), \ldots, g(x_m)), \;\; b \stackrel{\text{def}}{=} (g(y_1), \ldots, g(y_m)).$$

Those strings satisfy $a \in f^{-1}(1)$ and $b \in f^{-1}(0)$, and the goal of the players is to find $i \in [m]$ and $j \in [n]$ such that $(x_i)_j \neq (y_i)_j$. Observe that this relation has an obvious protocol: The players first solve KW_f on a and b, thus obtaining a coordinate $i \in [m]$ such that $a_i \neq b_i$ (note that a and b are indeed legal inputs for KW_f). Then, Alice and Bob solve KW_g on x_i and y_i, thus obtaining a coordinate $j \in [n]$ where $(x_i)_j \neq (y_i)_j$ (note that x_i and y_i are indeed legal inputs

[3] We need to make a small change in the KRW conjecture for this implication to hold. This change was suggested by Avishay Tal.

for KW_g, since $a_i \neq b_i$ implies $g(x_i) \neq g(y_i)$). The communication complexity of this protocol is $\mathsf{C}(KW_f) + \mathsf{C}(KW_g)$, and the KRW conjecture can be viewed as saying that this obvious protocol is roughly optimal.

The composition $f \diamond MUX$ is defined similarly, with the following modification: whenever the players received an input of KW_g in $KW_{f \diamond g}$, they will receive an input of MUX in $f \diamond MUX$.

Definition 2.1. Let $f : \{0,1\}^m \to \{0,1\}$ be a boolean function, and let $n \in \mathbb{N}$. The relation $f \diamond MUX_n$ is the following communication problem. Alice gets strings $x_1, \ldots, x_m \in \{0,1\}^n$ and functions $g_1, \ldots, g_m : \{0,1\}^n \to \{0,1\}$. Bob gets strings $y_1, \ldots, y_m \in \{0,1\}^n$ and *the same functions* $g_1, \ldots, g_m : \{0,1\}^n \to \{0,1\}$ *as Alice*. We define strings $a, b \in \{0,1\}^m$ as follows:

$$a \stackrel{\text{def}}{=} (g_1(x_1), \ldots, g_m(x_m)), \;\; b \stackrel{\text{def}}{=} (g_1(y_1), \ldots, g_m(y_m)).$$

Those strings must satisfy $a \in f^{-1}(1)$ and $b \in f^{-1}(0)$, and the goal of the players is to find $i \in [m]$ and $j \in [n]$ such that $(x_i)_j \neq (y_i)_j$.

It is not hard to see that the same obvious protocol from before works for $f \diamond MUX$ as well, and therefore

$$\mathsf{C}(f \diamond MUX_n) \leq \mathsf{C}(KW_f) + n + 2.$$

It is therefore natural to conjecture that this obvious protocol is roughly optimal.

Conjecture 2.2 (The KRW conjecture for $f \diamond MUX$)**.** *For every non-constant function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$, it holds that $\mathsf{C}(f \diamond MUX_n) \geq \mathsf{C}(KW_f) + n - O(\log \log n)$.*

For the purpose of separating $\mathbf{NC}^1$ and $\mathbf{P}$, it suffices to consider the following weaker version of the (see discussion below).

Conjecture 2.3 (Weak conjecture for $f \diamond MUX$)**.** *For every function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$, it holds that $\mathsf{C}(f \diamond MUX_n) \geq \mathsf{C}(KW_f) + \omega(\log n)$.*

We believe that Conjecture 2.3 implies that $\mathbf{P} \not\subseteq \mathbf{NC}^1$. Unfortunately, we do not know how to prove that implication. However, it turns out that a close variant of Conjecture 2.3 does imply that $\mathbf{P} \not\subseteq \mathbf{NC}^1$. In order to state this variant, we use the following notion of "alternating protocols": those are protocols in which each player sends exactly one bit in each of her turns (i.e., Alice sends one bit, then Bob sends one bit, then Alice sends one bit, etc.). Such protocols have been considered in the past in the interactive coding literature (see, e.g., [KR13]).

Definition 2.4. We say that a communication protocol is *alternating* if in every transcript, the bits at odd positions are transmitted by Alice, and the bits at even positions are transmitted by Bob. Given a communication problem P, its *alternating communication complexity* $\mathsf{C}_{\mathrm{ALT}}(P)$ is the minimal communication complexity of a deterministic alternating protocol that solves P.

We now state a variant of Conjecture 2.3 for alternating communication complexity, which does imply that $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

Conjecture 2.5 (Alternating conjecture for $f \diamond MUX$)**.** *For every non-constant function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$, it holds that $\mathsf{C}_{\mathrm{ALT}}(f \diamond MUX) \geq \mathsf{C}_{\mathrm{ALT}}(KW_f) + \omega(\log n)$.*

Theorem 2.6. *If Conjecture 2.5 holds then $\mathbf{P} \not\subseteq \mathbf{NC}^1$.*

In the rest of this section we prove Theorem 2.6. As a warm-up, we first describe in Section 2.1 a natural (yet flawed) argument for showing that the original Conjecture 2.3 implies $\mathbf{P} \not\subseteq \mathbf{NC}^1$. We then discuss a subtle issue in that argument, and explain how to resolve this issue for Conjecture 2.5 in Section 2.2.

Discussion. We believe that attacking Conjecture 2.5 is a viable approach for separating $\mathbf{P}$ from $\mathbf{NC}^1$. To justify this belief, let us consider first Conjecture 2.3: As explained in the introduction, we already have similar results for compositions $f \diamond g$ where f is an arbitrary function and g is a specific function. The proofs of those results usually rely on knowing what g is, and in particular, the lower bound for $KW_{f \diamond g}$ usually builds on a proof of a lower bound for KW_g. This makes it difficult to extend the previous results to work for an arbitrary choice of g. On the other hand, MUX is a specific communication problem for which we have a proof of a lower bound, and therefore it is conceivable that we could extend the previous results to $f \diamond MUX$. This leads us to hope that Conjecture 2.3 might be within reach.

Of course, as discussed above, what we need is a proof of Conjecture 2.5 rather than Conjecture 2.3. However, all the previous results on the KRW conjecture can be adapted to work for alternating communication complexity rather easily. Thus, we believe that a proof of Conjecture 2.3 would likely yield a proof of Conjecture 2.5 as well.

2.1 On proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$ from Conjecture 2.3

We present the flawed argument for showing that Conjecture 2.3 implies that $\mathbf{P} \not\subseteq \mathbf{NC}^1$. This argument works by first "proving" that Conjecture 2.3 implies a certain weaker version of the KRW conjecture, and then observing that the latter version implies $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

We first state the weaker version of the KRW conjecture, which differs from the original in two ways: The first difference is that we replace the inner function g with multiple inner functions $g_1, \ldots, g_m$. The second (and more important) difference is that rather than requiring the lower bound to hold for *every* choice of $g_1, \ldots, g_m$, we only require it to hold for *some* choice of those functions.

Notation 2.7. Let $f : \{0,1\}^m \to \{0,1\}$ and $g_1, \ldots, g_m : \{0,1\}^n \to \{0,1\}$ be boolean functions. Then the function $f \circ (g_1, \ldots, g_m) : (\{0,1\}^n)^m \to \{0,1\}$ is the function that takes as inputs m strings $x_1, \ldots, x_m$ and outputs

$$f \circ (g_1, \ldots, g_m)(x_1, \ldots, x_m) = f\left(g_1(x_1), \ldots, g_m(x_m)\right)$$

Conjecture 2.8 (Weak version of the KRW conjecture)**.** *For every non-constant function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$ there exist functions $g_1, \ldots, g_m : \{0,1\}^n \to \{0,1\}$ such that*

$$\mathsf{D}\left(f \circ (g_1, \ldots, g_m)\right) \geq \mathsf{D}(f) + \omega(\log n).$$

Proposition 2.9. *If Conjecture 2.8 holds then $\mathbf{P} \not\subseteq \mathbf{NC}^1$.*

The proof of the last proposition is a simple variant of the argument of [KRW95] and other folklore arguments, and we defer it to Section 2.3 below. Observe that Conjecture 2.8 indeed follows from the KRW conjecture, by choosing $g_1 = \ldots = g_m$ to be some maximally-hard function whose existence can be proved by a counting argument. We are now ready to "prove" that Conjecture 2.3 implies $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

Conjecture 2.10. *If Conjecture 2.3 holds then $\mathbf{P} \not\subseteq \mathbf{NC}^1$.*

"Proof" of Conjecture 2.10. It suffices to show that Conjecture 2.3 implies Conjecture 2.8. Suppose that Conjecture 2.8 is false, that is, there exists a non-constant function $f : \{0,1\}^m$ such that for all functions $g_1, \ldots, g_m$ it holds that

$$\mathsf{D}\left(f \circ (g_1, \ldots, g_m)\right) \leq \mathsf{D}(f) + O(\log n).$$

We show that f is a counter-example for Conjecture 2.3, that is, we prove that $\mathsf{C}(f \diamond MUX) \leq \mathsf{C}(KW_f) + O(\log n)$.

Recall that in the communication problem $f \diamond MUX$, Alice and Bob get strings $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ respectively, and they both get functions $g_1, \ldots, g_m$ such that

$$f(g_1(x_1), \ldots, g_m(x_m)) = 0$$
$$f(g_1(y_1), \ldots, g_m(y_m)) = 1.$$

Their goal is to find $i \in [m]$ and $j \in [n]$ such that $(x_i)_j \neq (y_i)_j$. Now, observe that for every fixed choice of $g_1, \ldots, g_m$, this problem is exactly the KW relation of $f \circ (g_1, \ldots, g_m)$, and therefore its communication complexity is at most

$$\mathsf{D}(f) + O(\log n) \leq \mathsf{C}(KW_f) + O(\log n)$$

by our assumption. Thus, the following protocol solves $f \diamond MUX$ using at most $\mathsf{C}(KW_f) + O(\log n)$ bits: given their inputs, the players invoke the optimal protocol for $KW_{f \circ (g_1, \ldots, g_m)}$ on the strings $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$, thus finding a solution for $f \diamond MUX$. This protocol shows that $\mathsf{C}(f \diamond MUX) \leq \mathsf{C}(KW_f) + O(\log n)$, as required. ■

The flaw in the above "proof". Unfortunately, the protocol for $f \diamond MUX$ in the above argument is not well-defined. The standard definition of a protocol (e.g., [KN97]) requires that, at any given point during the execution of the protocol, an external observer is able to tell whose turn is it to speak. In other words, given a partial transcript of the protocol, we should be able to tell who sends the next bit, without looking at the inputs of the players. However, this is not the case in the above protocol.

In order to tell who sends the next bit in the above protocol, we have to know the functions $g_1, \ldots, g_m$. For example, it could be the case that for some choices of $g_1, \ldots, g_m$, Alice sends the first bit, while for other choices Bob sends the first bit. The reason is that the question who sends the first bit depends on the optimal protocol for $KW_{f \circ (g_1, \ldots, g_m)}$, which in turn depends on the choice of $g_1, \ldots, g_m$. However, the functions $g_1, \ldots, g_m$ are part of the inputs of the players, and are not known to an external observer. Thus, the above protocol for $f \diamond MUX$ is not well-defined.

This subtle issue was studied in a more general context in the work of [HIMS18], and was pointed out to us by Russel Impaglizazzo and Ivan Mihajlin.

2.2 Proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$ using alternating protocols

As discussed above, the issue in proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$ from Conjecture 2.3 stems from the fact that optimal protocols for $KW_{f \circ (g_1, \ldots, g_m)}$ may have different speaking orders, depending on the choice of $g_1, \ldots, g_m$. Avishay Tal observed that this issue can be bypassed if we restrict ourselves to protocols with a fixed order of speaking. For simplicity, we can restrict ourselves to alternating protocols. The foregoing argument now goes through without additional difficulty. Below we provide the formal details. We start by defining an "alternating analogue" of depth complexity.

Definition 2.11. We say that a circuit is alternating if all its gates in the odd layers are OR gates, and all its gates in the even layers are even. Here, we define the output gate to be the first layer, the gates that feed into the output gate to be the second layer, etc. Given a boolean function $h : \{0,1\}^k \to \{0,1\}$, we define its *alternating depth complexity* $\mathsf{D}_{\mathrm{ALT}}(h)$ to be the minimal depth of an alternating circuit with fan-in 2 that computes h.

It is easy to see that every circuit can be turned into an alternating circuit by at most doubling its depth complexity, so for every $h : \{0,1\}^k \to \{0,1\}$ it holds that

$$\mathsf{D}(h) \leq \mathsf{D}_{\mathrm{ALT}}(h) \leq 2 \cdot \mathsf{D}(h). \tag{3}$$

It is also not hard to verify that the Karchmer-Wigderson framework [KW90] implies that $\mathsf{D}_{\mathrm{ALT}}(h) = \mathsf{C}_{\mathrm{ALT}}(KW_h)$ for every function h. We now have the following "alternating analogue" of Conjecture 2.8 and Proposition 2.9.

Conjecture 2.12 (Weak version of the KRW conjecture)**.** *For every non-constant function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$ there exist functions $g_1, \ldots, g_m : \{0,1\}^n \to \{0,1\}$ such that*

$$\mathsf{D}_{\mathrm{ALT}}\left(f \circ (g_1, \ldots, g_m)\right) \geq \mathsf{D}_{\mathrm{ALT}}(f) + \omega(\log n).$$

Proposition 2.13. *If Conjecture 2.12 holds then $\mathbf{P} \not\subseteq \mathbf{NC}^1$.*

The proof of the last proposition is similar to that of Proposition 2.9. By repeating exactly the same argument, we get a function $F : \{0,1\}^N \to \{0,1\}$ in $\mathbf{P}$ such that $\mathsf{D}_{\mathrm{ALT}}(F) = \omega(\log N)$. By Equation (3), it follows that $\mathsf{D}(F) = \omega(\log N)$, as required. We conclude with proving Theorem 2.6 using exactly the same argument as before, which now goes through.

Conjecture 2.5. *For every non-constant function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$, it holds that $\mathsf{C}_{\mathrm{ALT}}(f \diamond MUX_n) \geq \mathsf{C}_{\mathrm{ALT}}(KW_f) + \omega(\log n)$.*

Theorem 2.6. *If Conjecture 2.5 holds then $\mathbf{P} \not\subseteq \mathbf{NC}^1$.*

Proof. It suffices to prove that Conjecture 2.5 implies Conjecture 2.12. Suppose that Conjecture 2.12 is false, that is, there exists a non-constant function $f : \{0,1\}^m$ such that for all functions $g_1, \ldots, g_m$ it holds that

$$\mathsf{D}_{\mathrm{ALT}}\left(f \circ (g_1, \ldots, g_m)\right) \leq \mathsf{D}_{\mathrm{ALT}}(f) + O(\log n).$$

We show that f is a counter-example for Conjecture 2.3, that is, we prove that $\mathsf{C}_{\mathrm{ALT}}(f \diamond MUX) \leq \mathsf{C}_{\mathrm{ALT}}(KW_f) + O(\log n)$.

Consider the following protocol for $f \diamond MUX$: given their inputs $g_1, \ldots, g_m$, $x_1, \ldots, x_m$, and $y_1, \ldots, y_m$, the players invoke the optimal alternating protocol for $KW_{f \circ (g_1, \ldots, g_m)}$ on $x_1, \ldots, x_m$, and $y_1, \ldots, y_m$, thus obtaining a solution for $f \diamond MUX$. Clearly, this protocol is an alternating protocol, since all the optimal protocols it invokes are alternating. In particular, this protocol is well-defined, since the speaking order of the players does not depend on the choice of $g_1, \ldots, g_m$. The complexity of this protocol is the maximal complexity of an optimal alternating protocol for $KW_{f \circ (g_1, \ldots, g_m)}$, and by our assumption this complexity is at most

$$\begin{aligned} \mathsf{C}_{\mathrm{ALT}}(KW_{f \circ (g_1, \ldots, g_m)}) &= \mathsf{D}_{\mathrm{ALT}}\left(f \circ (g_1, \ldots, g_m)\right) \\ &\leq \mathsf{D}_{\mathrm{ALT}}(f) + O(\log n) \\ &\leq \mathsf{C}_{\mathrm{ALT}}(f) + O(\log n). \end{aligned}$$

It follows that $\mathsf{C}_{\mathrm{ALT}}(f \diamond MUX) = \mathsf{C}_{\mathrm{ALT}}(KW_f) + O(\log n)$, as required. ■

2.3 Proof of Proposition 2.9

In this section, we prove that Conjecture 2.8, restated next, implies that $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

Conjecture 2.8. *For every non-constant function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$ there exist functions $g_1, \ldots, g_m : \{0,1\}^n \to \{0,1\}$ such that*

$$\mathsf{D}\left(f \circ (g_1, \ldots, g_m)\right) \geq \mathsf{D}(f) + \omega(\log n).$$

Suppose that Conjecture 2.8 holds. Then, there exists a function $\alpha : \mathbb{N} \to \mathbb{N}$ such that $\alpha(n) = \omega(\log n)$ such that for every non-constant function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$ there exist functions $g_1, \ldots, g_m : \{0,1\}^n \to \{0,1\}$ satisfying

$$\mathsf{D}\left(f \circ (g_1, \ldots, g_m)\right) \geq \mathsf{D}(f) + \alpha(n).$$

We prove that this assumption implies super-logarithmic lower bounds on the depth complexity of the "iterated multiplexor function" of [EIRS01] (a.k.a. the "tree-evaluation function"). We start by providing the definition of this function.

Definition 2.14. Let $d, n \in \mathbb{N}$, and let $T_{n,d}$ be the perfect n-ary tree of height d. The *iterated multiplexor function with d levels*, denoted $IMUX_{n,d}$, takes as input a labeling of the nodes of $T_{n,d}$, such that every leaf ℓ is labeled with a bit $x_\ell \in \{0,1\}$, and every internal node v is labeled with a function $h_v : \{0,1\}^n \to \{0,1\}$. Given such a labeling, we assign to every node a binary value in $T_{n,d}$ recursively: the value of leaf ℓ is just its label x_ℓ, and the value of an internal node v is the output of h_v when invoked on the n values of v's children. The output of $IMUX_{h,d}$ is the value of the root of $T_{n,d}$.

It is not hard to see that the input of $IMUX_{n,d}$ is of length $N \stackrel{\text{def}}{=} n^d + \frac{n^d - 1}{n-1} \cdot 2^n = \Theta(n^{d-1} \cdot 2^n)$. Below, we will prove that $\mathsf{D}(IMUX_{n,d}) \geq (d-1) \cdot \alpha(n)$. This will imply the desired lower bound, since by setting $d - 1 = \frac{n}{\log n}$, we will obtain that the input length of $IMUX_{n,d}$ is $N = \Theta(2^{2n})$ and that

$$\mathsf{D}(IMUX_{n,d}) \geq \frac{n}{\log n} \cdot \alpha(n) = \omega(n) = \omega(\log N).$$

Hence, for this setting of d we will get that $IMUX_{n,d}$ is a function in $\mathbf{P}$ with super-logarithmic depth complexity, thus establishing that $\mathbf{P} \not\subseteq \mathbf{NC}^1$. It remains to prove that $\mathsf{D}(IMUX_{n,d}) \geq (d-1) \cdot \alpha(n)$. In fact, we show the following stronger result, which will conclude the proof.

Proposition 2.15. *For every $n, d \in \mathbb{N}$, there exists a labeling of the internal nodes of $T_{n,d}$ such that even if we hard-wire this labeling, the depth complexity of $IMUX_{n,d}$ is at least $(d-1) \cdot \alpha(n)$.*

Proof. Fix $n \in \mathbb{N}$. We prove the proposition by induction on d. For the base case of $d = 1$ there is nothing to prove. Suppose that the proposition holds for some $d \geq 1$, that is, that there exists a labeling L_d of the internal nodes of $T_{n,d}$ as in the proposition. We prove that the proposition holds for $d + 1$ by constructing an appropriate labeling L_{d+1} for $T_{n,d+1}$.

Let F_d denote the function obtained from $IMUX_{n,d}$ by hard-wiring the labeling L_d, so $\mathsf{D}(F_d) \geq (d-1) \cdot \alpha(n)$. Observe that the input length of F is $m \stackrel{\text{def}}{=} n^d$ (since this is the number of leaves of $T_{n,d}$). By Conjecture 2.8, there exists functions $g_1, \ldots, g_m : \{0,1\}^n \to \{0,1\}$ such that

$$\mathsf{D}\left(F_d \circ (g_1, \ldots, g_m)\right) \geq \mathsf{D}(F_d) + \alpha(n) \geq d \cdot \alpha(n).$$

Next, we construct the desired labeling L_{d+1} of the internal nodes of $T_{n,d+1}$ as follows: the internal nodes of depth at most $d - 1$ are labeled as in L_d, and the $m = n^d$ modes of depth d are labeled with the functions $g_1, \ldots, g_m$. Let F_{d+1} be the function obtained from $IMUX_{n,d}$ by hard-wiring the labeling L_{d+1}. Now, observe that the function F_{d+1} is exactly the function $F_d \circ (g_1, \ldots, g_m)$, and therefore $\mathsf{D}(F_{d+1}) \geq d \cdot \alpha(n)$, as required. ■

3 Simpler lower bound for MUX

Motivation. As discussed in the introduction, [EIRS01] proved a lower bound of $\Omega(n)$ on the communication complexity of MUX_n. While it is easy to prove such a lower bound using a counting argument, the importance of the proof of [EIRS01] is that it was based on an adversary argument. They hoped that such an argument would combine better with other arguments in the literature on the KRW conjecture. In this section, we provide a simpler version of their proof. Our proof also has an added benefit, to be discussed next.

Recall that an adversary argument works by taking a protocol Π that is "too efficient", and constructing a transcript of Π that makes an error. Usually, such a transcript is constructed in iterations, where in each iteration the adversary chooses the next message to be transmitted. In many proofs of this kind, the adversary simply chooses the message that reveals the smallest amount of information (i.e., the one which is most likely to be transmitted, under some suitably chosen distribution). On the other hand, the adversary of [EIRS01] chooses the next message using a rather sophisticated strategy. This means that the adversary does not necessarily choose the message that reveals the smallest amount of information, and in fact may choose a message that leaks a large amount of information.

This property of the adversary of [EIRS01] makes it difficult to combine with other lower bounds in the literature on the KRW conjecture. In particular, several of those lower bounds rely on constructing adversaries that only reveal a small amount on information, and this property cannot be guaranteed for the adversary of [EIRS01]. A nice feature of our proof is that we give a more "traditional" adversary, which always chooses the message that reveals the smallest amount of information. We thus hope that our proof could be used in combination with the previous works to prove a lower bound on $f \diamond MUX$.

The adversary. We prove that $\mathsf{C}(MUX_n) \geq \frac{n-1}{7}$. Assume for the sake of contradiction there exists a protocol Π that solves MUX_n by transmitting less than $(n-1)/7$ bits. We design an adversary that constructs an erroneous transcript of Π. Our adversary, like the adversary of [EIRS01], constructs the transcript bit-by-bit, while preserving a certain invariant, to be discussed next.

Let us denote by π the partial transcript that was constructed so far. Given a string $v \in \{0,1\}^n$ and a function $f : \{0,1\}^n \to \{0,1\}$, we say the pair (v, f) is *consistent* if it satisfies the following conditions:

- If $f(v) = 1$, then the pair (v, f) can be given as input to Alice (i.e., the transcript π is consistent with Alice having the input (v, f)).
- If $f(v) = 0$, then the pair (v, f) can be given as input to Bob.

Let us denote the length of π by c. The invariant we preserve is that there exist a set $V \subseteq \{0,1\}^n$ of size at least $2^{n-7\cdot c}$ and a set F of functions from $\{0,1\}^n$ to $\{0,1\}$ that satisfy the following properties:

1. All the pairs in $V \times F$ are consistent.
2. The functions in F, when restricted to V, consist of all functions from V to $\{0,1\}$.

It is obvious that when the transcript π is empty, the invariant holds: we can choose $V = \{0,1\}^n$ and F to be the set of all functions. The crux of the argument of [EIRS01] is to show that as long as the protocol has not stopped, the transcript π can be extended by one bit while preserving the above invariant.

Let us first explain why this is sufficient in order to prove the lower bound. Given the protocol Π, the adversary will construct a transcript π by starting from the empty transcript and extending it bit-by-bit until the protocol halts. Let π_{full} be the full transcript that is obtained when the protocol halts, and let $i \in [n]$ be the output of π_{full}, so the input strings of Alice and Bob should differ on the coordinate i. By assumption, the length of π is at most $(n-1)/7$ bits, and by the invariant, there exist sets V, F that satisfy the above properties such that $|V| \geq 4$. In particular, the set V contains two distinct strings x, y such that $x_i = y_i$. Moreover, by the invariant, the set F contains a function $f : \{0,1\}^n \to \{0,1\}$ such that $f(x) = 1$ and $f(y) = 0$, and such that the pairs (x, f) and (y, f) are consistent. This means that we can give (x, f) and (y, f) as inputs to Alice and Bob. However, this means that π_{full} is incorrect, since it claims that $x_i \neq y_i$.

In the rest of this section, we explain how a transcript π can be extended by one bit while preserving the invariant. Fix a transcript π, and let V, F be the corresponding sets that exist by the invariant. Without loss of generality, assume that it is Alice's turn to speak at π. We also assume without loss of generality that the every function $f \in F$ has a different restriction to V, so $|F| = 2^{|V|}$ (if there are multiple functions in F with the same restriction to V, we keep only one of them). We show that there exists a message bit $\sigma \in \{0,1\}$ for Alice and sets $V' \subseteq V, F' \subseteq F$ such that the transcript $\pi \circ \sigma$ satisfies the invariant with V', F'.

Extending the transcript. The main difficulty in constructing σ, V', F' is to guarantee the first property of the invariant (i.e., that all the pairs in $V' \times F'$ are consistent) while also ensuring that V' and F' are sufficiently large. Once this is achieved, the second property of the invariant is obtained by a direct application of the Sauer-Shelah lemma (stated below). As discussed above, the adversary of [EIRS01] obtained the first property of the invariant by a careful choice of the bit σ.

Our adversary, on the other hand simply chooses σ to be "the most likely bit": Let σ be the bit that Alice transmits on most pairs $(v, f) \in V \times F$ such that $f(v) = 1$ (breaking ties arbitrarily). Let $W \subseteq V \times F$ be the set of pairs (v, f) that are consistent with σ in the following sense: either $f(v) = 1$ and Alice transmits σ when given input (v, f), or $f(v) = 0$. Observe that $|W| \geq \frac{3}{4} \cdot |V \times F|$ (since exactly half of the pairs $(v, f) \in V \times F$ satisfy $f(v) = 1$).

Next, we show that W can be modified to preserve the first property of the invariant. Clearly, all the inputs in W are consistent, but in order to satisfy the invariant, W needs to be a transformed into combinatorial rectangle. To this end, we show that there exist sufficiently large sets $V_0 \subseteq V$ and $F_0 \subseteq F$ such that $V_0 \times F_0 \subseteq W$. Our main observation is that this can be obtained by a direct application of the Kövári-Sós-Turán theorem, stated below.

Theorem 3.1 (The Kövári-Sós-Turán theorem [KST54])**.** *Let G be a bipartite graph with m vertices on the left and n vertices on the right, such that the average degree on the left side is at least d. Then, for every $t \in \mathbb{N}$, the graph G contains a bi-clique with t vertices on the right and*

$$\left(\frac{d-t}{n-t}\right)^t \cdot m$$

vertices on the left.

Since the Kövári-Sós-Turán theorem is central to our argument, we provide its proof in the appendix. Now, consider the graph bipartite graph G whose left and right sets are F and V respectively, and whose edges are determined by W. The average left degree of G is

$$\frac{|W|}{|F|} \geq \frac{\frac{3}{4} \cdot |V \times F|}{|F|} = \frac{3}{4} \cdot |V| .$$

Thus, by Kövári-Sós-Turán theorem, the graph G contains a bi-clique with $t \stackrel{\text{def}}{=} \frac{1}{8} \cdot |V|$ vertices on the right and at least

$$\left(\frac{\frac{3}{4} \cdot |V| - t}{|V| - t}\right)^t \cdot |F| \geq \left(\frac{5}{7}\right)^t \cdot |F|$$

vertices on the right. In other words, there exist sets $V_0 \subseteq V$ and $F_0 \subseteq F$ such that $V_0 \times F_0 \subseteq W$, $|V_0| = \frac{1}{8} \cdot |V|$, and $|F_0| \geq \left(\frac{5}{7}\right)^{|V_0|} \cdot |F|$. Thus, the set $V_0 \times F_0$ satisfies the first property of the invariant. In order to obtain the second property of the invariant, we use the Sauer-Shelah lemma, stated next.

Theorem 3.2 (The Sauer-Shelah lemma [Sau72, She72])**.** *Let $S \subseteq \{0,1\}^N$ be such that $|S| \geq \sum_{j=0}^{d} \binom{N}{j}$. Then, there exists a set $K \subseteq [N]$ of d coordinates such that the projection of S to K consists of all strings in $\{0,1\}^K$.*

Let us denote by $F_0|_{V_0}$ the set of functions obtained by projecting the the functions in F_0 to V_0. Observe that

$$\begin{aligned} |F_0|_{V_0}| &\geq \frac{|F_0|}{2^{|V|-|V_0|}} \geq \frac{\left(\frac{5}{7}\right)^{|V_0|} \cdot |F|}{2^{|V|-|V_0|}} = \left(\frac{5}{7}\right)^{|V_0|} \cdot \frac{2^{|V|}}{2^{|V|-|V_0|}} \\ &= \left(\frac{5}{7}\right)^{|V_0|} \cdot 2^{|V_0|} \geq 2^{\frac{1}{2} \cdot |V_0|} \end{aligned}$$

By applying the Sauer-Shelah lemma[4] to $F_0|_{V_0}$, and noting that $2^{\frac{1}{2}N} \geq \sum_{j=0}^{\frac{N}{10}} \binom{N}{j}$, we obtain a set $V' \subseteq V_0$ of size at least $\frac{1}{10} \cdot |V_0|$ such that $F_0|_{V'}$ consists of all functions from V' to $\{0,1\}$. Finally, we set $F' = F_0$ and observe that V' and F' satisfy the desired invariant since

$$\left|V'\right| \geq \frac{1}{10} \cdot |V_0| \geq \frac{1}{80} \cdot |V| \geq 2^{-7} \cdot |V| \geq 2^{n-7(c+1)}.$$

This concludes the proof.

Acknowledgement. We thank Russel Impagliazzo and Ivan Mihajlin for many valuable discussions and ideas on the multiplexor relation, and in particular for pointing out the issue in the simple "proof" of Conjecture 2.10 to us (see Section 2.1). We are also grateful to Avishay Tal for valuable ideas and in particular for his permission to include his observation in this paper (see Section 2.2). The aforementioned discussions took place at the Simons Institute for the Theory of Computing, as part of the program on Lower Bounds in Computational Complexity.

A Proof of the Kövári-Sós-Turán theorem

In this appendix we prove the Kövári-Sós-Turán theorem, restated next.

Theorem 3.1. *Let G be a bipartite graph with m vertices on the left and n vertices on the right, such that the average degree on the left side is at least d. Then, for every $t \in \mathbb{N}$, the graph G contains a bi-clique with t vertices on the right and*

$$\left(\frac{d-t}{n-t}\right)^t \cdot m$$

vertices on the left.

[4]Here, we view $F_0|_{V_0}$ as a subset of $\{0,1\}^{|V_0|}$.

Proof. We may assume without loss of generality that $t < d$, since otherwise there is nothing to prove. We prove the theorem by induction on t. We assume that the theorem holds for t, and prove it for $t+1$.

Let $G = (L \cup R, E)$ be a bipartite graph, let $m \stackrel{\text{def}}{=} |L|$, and let $n \stackrel{\text{def}}{=} |R|$. Assume that the average left degree (i.e., the average degree of the vertices in L) at least d . In other words, the number of edges is at least $d \cdot m$, and therefore the average right degree is at least $\frac{d}{n} \cdot m$. Hence, there exists a vertex v on the right which has at least $\frac{d}{n} \cdot m$ neighbors.

Let us denote by L' the set of neighbors of v, and let $R' \stackrel{\text{def}}{=} R - \{v\}$. Now, let G' be the induced sub-graph on $L' \cup R'$. Observe that the average left degree of G' is at least $d-1$, since every vertex in L' has all the neighbors it had in G except v. Thus, by the induction assumption, G' contains a bi-clique with t vertices on the right and

$$\left(\frac{d-1-t}{n-1-t}\right)^t \cdot \left|L'\right| \geq \left(\frac{d-1-t}{n-1-t}\right)^t \cdot \frac{d}{n} \cdot m \geq \left(\frac{d-(t+1)}{n-(t+1)}\right)^{t+1} \cdot m.$$

vertices on the left. We now obtain the desired bi-clique in G by adding v to the bi-clique of G'. ■

References

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

[EIRS01] Jeff Edmonds, Russell Impagliazzo, Steven Rudich, and Jiri Sgall. Communication complexity towards lower bounds on circuit depth. *Computational Complexity*, 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.

[HIMS18] Kenneth Hoover, Russell Impagliazzo, Ivan Mihajlin, and Alexander V. Smal. Half-duplex communication complexity. In *29th International Symposium on Algorithms and Computation, ISAAC 2018, December 16-19, 2018, Jiaoxi, Yilan, Taiwan*, pages 10:1–10:12, 2018.

[HW93] Johan Håstad and Avi Wigderson. Composition of the universal relation. In *Advances in computational complexity theory, AMS-DIMACS*, 1993.

[KM18] Sajin Koroth and Or Meir. Improved composition theorems for functions and relations. In *RANDOM*, 2018.

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

[KR13] Gillat Kol and Ran Raz. Interactive channel capacity. In *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 715–724, 2013.

[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.

[KST54] Tamás Kővári, Vera T. Sós, and Pál Turán. On a problem of k. zarankiewicz. *Colloquium Mathematicae*, 3:50–57, 1954.

[KW90] Mauricio Karchmer and Avi Wigderson. Monotone circuits for connectivity require super-logarithmic depth. *SIAM J. Discrete Math.*, 3(2):255–265, 1990.

[Sau72] Norbert Sauer. On the density of families of sets. *J. Comb. Theory, Ser. A*, 13(1):145–147, 1972.

[She72] Saharon Shelah. "a combinatorial problem; stability and order for models and theories in infinitary languages. *Pacific Journal of Mathematics*, 41:247–261, 1972.

[TZ97] Gábor Tardos and Uri Zwick. The communication complexity of the universal relation. In *Proceedings of the Twelfth Annual IEEE Conference on Computational Complexity, Ulm, Germany, June 24-27, 1997*, pages 247–259, 1997.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il