Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 120 (2019)

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

Or Meir[*]

May 5, 2020

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 (Computational Complexity 5(3/4), 1995) 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. (Computational Complexity 10(3), 2001) suggested to study the "multiplexor relation" MUX. In this paper, we present two results regarding this relation:

- The multiplexor relation is "complete" for the approach of Karchmer et. al. 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 Edmonds et. al. 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 with fan-in 2 that computes f. 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

Karchmer et. al. [KRW95] observed that this conjecture, if proved, would imply that $\mathbf{P} \not\subseteq \mathbf{NC}^1$. To see why, consider the function $F : \{0,1\}^{2N} \to \{0,1\}$, 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

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

Note that $\overline{x}$ is indeed a valid input for the function $f \diamond \ldots \diamond f$ (since its length is $(\log N)^{\frac{\log N}{\log\log N}} = N$). We claim that the conjecture implies 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 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 paper, 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. Karchmer et. al. [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, Karchmer et. al. [KRW95] suggested to prove it for the universal relation[1] 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[2] $U \diamond U$, and an alternative proof was given later[3] 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[4] with the works of [KRW95, EIRS01, HW93, GMWW17, KM18].

[1] The universal relation is the following communication problem: Alice and Bob get two *distinct* strings x, y, and their goal is to find a coordinate on which they disagree. This relation is a simplification of KW relations, since it removes the function f from the problem.

[2] This composition is not a composition of functions. Rather, it is a communication problem that mimics the KW relation $KW_{f \diamond g}$.

[3] The work [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.

[4] The proof of Håstad [Hås98] works by studying de-Morgan formulas and how they shrink under random restrictions, rather than by analyzing communication protocols. The proof of Dinur and Meir [DM18] gives an adversary argument that analyzes communication protocols, and in this sense it follows the other works on the KRW conjecture.

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

The multiplexor relation. Instead of proving the full KRW conjecture, one could prove[5] that $\mathbf{P} \not\subseteq \mathbf{NC}^1$ by proving a depth lower bound directly on the function F of Equation (2). Proving a 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, Edmonds et. al. [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 $x_i \neq y_i$. Edmonds et. al. viewed the multiplexor relation as a "single level" version of the function F of Equation (2) (which consists of $\frac{\log N}{\log\log N}$ levels), and thus hoped that the study of MUX would shed light on F. One could also hope to make progress toward proving lower bounds on F by first proving a lower bound on the "single level" version (i.e., MUX), then proving lower bounds on the "two level" version ($MUX \diamond MUX$), and continuing gradually until we get to $\frac{\log N}{\log\log N}$ levels (which is F).

The communication complexity of MUX_n is known to be at most $n+2$ by a protocol of [TZ97] (improving over the trivial upper bound of $n + \log(n)$). It is easy to prove a corresponding lower bound of $n - \log\log n + \Theta(1)$: to see it, note that if we fix f to be a (non-explicit) function with maximal depth complexity, then MUX_n becomes KW_f, and therefore the communication complexity of MUX_n becomes $\mathsf{D}(f) \geq n - \log\log n + \Theta(1)$. However, such an argument does not fit well with the framework of KW relations, since the existence of the function with maximal depth complexity is proved by counting circuits rather than by arguing about communication. Thus, Edmonds et. al. [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[6] $f \diamond MUX$, where f is an arbitrary function. We propose a version[7] of the KRW conjecture for this specific composition (see Conjecture 2.5), and prove 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 $\mathbf{NC}^1$, and we discuss it in Section 2. We also suggest some concrete open problems for this direction in Section 4.

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

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

[6] Again, this composition is not a composition of functions. Rather, it is a communication problem that mimics the KW relation $KW_{f \diamond g}$.

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

works on the KRW conjecture.[8] Thus, this argument might be useful for proving the conjecture regarding $f \diamond MUX$. We present this result in Section 3.

Preliminaries. For $n \in \mathbb{N}$, we denote $[n] \overset{\text{def}}{=} \{1, \dots n\}$. We use the standard definitions of communication complexity — see the book of Kushilevitz and Nisan [KN97] for more details. 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 $x_1, \dots, x_m \in \{0,1\}^n$ and Bob gets strings $y_1, \dots, y_m \in \{0,1\}^n$. We define strings $a, b \in \{0,1\}^m$ as follows:

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

Those strings are guaranteed to 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 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: Note that in $KW_{f \diamond g}$, whenever $a_i \neq b_i$, the i-th inputs x_i, y_i are an instance of KW_g. In $f \diamond MUX$, whenever $a_i \neq b_i$, the i-th inputs are an instance of 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 $x_1, \dots, x_m \in \{0,1\}^n$ and functions $g_1, \dots, g_m : \{0,1\}^n \to \{0,1\}$. Bob gets strings $y_1, \dots, y_m \in \{0,1\}^n$ and *the same functions* $g_1, \dots, g_m : \{0,1\}^n \to \{0,1\}$ *as Alice.* We define strings $a, b \in \{0,1\}^m$ as follows:

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

Those strings are guaranteed to 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 $f \diamond MUX$, 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.

[8] The key point is that the adversary of [EIRS01] chooses the messages of the protocol in a rather delicate way, while our adversary always chooses the next message to be the most popular message. See discussion in the beginning of Section 3 for more details.

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* $\mathsf{C}(f \diamond MUX_n) \geq \mathsf{C}(KW_f) + n - O(\log \log n)$*.*

Actually, for the purpose of separating $\mathbf{NC}^1$ and $\mathbf{P}$, it suffices to consider the following weaker version of Conjecture 2.2 (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 their 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* $\mathsf{C}_{\text{ALT}}(P)$ is the minimal communication complexity of a deterministic alternating protocol that solves P.

Observe that every protocol can be turned into an alternating protocol by at most doubling its communication complexity, so for every $h : \{0,1\}^k \to \{0,1\}$ it holds that

$$\mathsf{C}(KW_h) \leq \mathsf{C}_{\text{ALT}}(KW_h) \leq 2 \cdot \mathsf{C}(KW_h). \tag{3}$$

Thus, in order to prove that $\mathbf{P} \not\subseteq \mathbf{NC}^1$, it suffices to prove a lower bound of $\omega(\log n)$ on the alternating communication complexity of some Karchmer-Wigderson relation. We now state a variant[9] 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* $\mathsf{C}_{\text{ALT}}(f \diamond MUX) \geq \mathsf{C}_{\text{ALT}}(KW_f) + \omega(\log n)$*.*

Our first main result is the follows.

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

[9] Note that Conjecture 2.5 does not follow from Conjecture 2.3 via Equation (3): the reason is that we cannot afford to lose a factor of 2 in those conjectures.

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. In particular, this hope motivates revisiting the lower bound for MUX, which is done in Section 3.

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*

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

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 Appendix A. Observe that Conjecture 2.8 indeed follows from the KRW conjecture (Conjecture 1.1), by choosing $g_1 = \ldots = g_m$ to be some 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

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

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 the same functions $g_1, \ldots, g_m$ such that

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

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 $KW_{f \circ (g_1, \ldots, g_m)}$, and therefore its communication complexity is at most $\mathsf{C}(KW_f) + O(\log n)$ 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 does not satisfy the standard definition of a protocol (see, e.g., [KN97]). The standard definition 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 for $f \diamond MUX$, we have to know the functions $g_1, \ldots, g_m$. The reason is that the question who sends the next bit in the protocol for $f \diamond MUX$ depends on the protocol for $KW_{f \circ (g_1, \ldots, g_m)}$, which in turn depends on $g_1, \ldots, g_m$. However, in the protocol for $f \diamond MUX$, 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 $f \diamond MUX$ does not satisfy the aforementioned requirement of the standard definition.

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

Remark 2.11. It is tempting to ask whether one can change the standard definition of a protocol in a way that would make the foregoing proof go through. A natural approach would be to relax the definition such that only the players would be required to know who sends the next bit (rather than an external observer). Note that the above protocol for $f \diamond MUX$ satisfies this requirement, since the players do know $g_1, \ldots, g_m$.

While such a definition makes sense, this model of communication is significantly more complicated than the standard model. In particular, it is not hard to see that such protocols do not necessarily satisfy the "rectangle property" of standard protocols, which says that the set of inputs that are consistent with a transcript forms a combinatorial rectangle. Since this property is at the core of almost all lower bound proofs in communication complexity, it would probably be more difficult to prove lower bounds for this model, and therefore we choose not to work with it.

A different approach was taken in the work of Hoover et. al. [HIMS18], who defined a model of communication in which even the players do not know whose turn it is to speak. This model, too, seems to be more difficult to analyze than the standard model. Hence, we chose not to work with that model as well. In short, it appears that the model of alternating protocols is the simplest known model that allows the foregoing proof to go through.

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 with the following "alternating analogues" of Conjecture 2.8 and Proposition 2.9.

Conjecture 2.12 (Weak alternating 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*

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

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

The proof of the last proposition is identical to that of Proposition 2.9, except that we replace C with $\mathsf{C}_{\mathrm{ALT}}$. We conclude with proving Theorem 2.6 using exactly the same argument as before, which now goes through.

Conjecture 2.5 (restated). *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 (restated). *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

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

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

3 Simpler lower bound for MUX

Recall that 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 $x_i \neq y_i$. In this section, we prove that $\mathsf{C}(MUX_n) = \Omega(n)$.

3.1 Motivation

As discussed in the introduction, Edmonds et. al. [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. After the next message is chosen, all the inputs that are inconsistent[10] with that message are discarded. Finally, when the protocol ends, the adversary finds inputs that survived the process and on which the output of the protocol is incorrect. If the adversary can do so, then it shows that the protocol Π is erroneous.

In many proofs of this kind, the adversary follows a certain template in each iteration. Specifically, in each iteration adversary performs the following two steps (without loss of generality assume that it is Alice's turn to speak):

- First, the adversary chooses the next message of Alice to be the message that is supported by the largest number of remaining inputs.
- Then, the adversary discards some of Alice's and Bob's inputs (including inputs that are consistent with the chosen message).

Intuitively, in the first step the adversary chooses the message that reveals the smallest amount of information on the inputs of the players. Then, in the second step, the adversary gets rid of all the "easy inputs", i.e., the inputs on which solving the problem has become easy by the message that was chosen.

The adversary of [EIRS01] does not follow this scheme. While that adversary does discard "easy inputs" in each iteration, it chooses the next message using a rather sophisticated strategy. In particular, it does not necessarily choose the message that reveals the smallest amount of information on the inputs, 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 on the remaining inputs, 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 follows the foregoing template. We thus hope that our proof could be used in combination with the previous works to prove a lower bound on $f \diamond MUX$.

3.2 The proof

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 (with π)* if it satisfies the following conditions:

- If $f(v) = 1$, then the transcript π is consistent with Alice having the input (v, f).
- If $f(v) = 0$, then the transcript π is consistent with Bob having the input (v, f).

[10] i.e., the inputs on which the player would have sent a different message.

The invariant. Let us denote the length of π by c. The invariant that the adversary preserves 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 with π.

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 $(n-2)/7$ bits, and by the invariant, there exist sets V and F that satisfy the above properties such that $|V| \geq 4$. In particular, the set V contains two distinct strings x and 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 with π. 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 and 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 $V' \subseteq V$ and $F' \subseteq F$ such that the transcript $\pi \circ \sigma$ satisfies the invariant with V' and 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 with $\pi \circ \sigma$) 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 $\pi \circ \sigma$. Observe that for every $(v, f) \in W$, it holds that either $f(v) = 1$ and Alice transmits σ when given input (v, f), or $f(v) = 0$. Hence, it holds 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, as in the template of Section 3.1, the adversary discards some of the inputs in W so it preserves the invariant. We start by showing that there exist sufficiently large sets $V_0 \subseteq V$ and $F_0 \subseteq F$ such that $V_0 \times F_0 \subseteq W$ (and so every $(v, f) \in V_0 \times F_0$ is consistent with $\pi \circ \sigma$). Our main observation is that this can be obtained by a direct application of the Kővári-Sós-Turán theorem, stated below.

Theorem 3.1 (The Kővári-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 Kővári-Sós-Turán theorem is central to our argument, we provide its proof in Appendix B. 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 the Kővári-Sós-Turán theorem, the graph G contains a bi-clique with $t \overset{\text{def}}{=} \frac{1}{8} \cdot |V|$ vertices on the right and at least

$$\left(\frac{\frac{3}{4} \cdot |V| - t}{|V| - t}\right)^t \cdot |F| = \left(\frac{\frac{3}{4} \cdot |V| - \frac{1}{8} \cdot |V|}{|V| - \frac{1}{8} \cdot |V|}\right)^t \cdot |F| = \left(\frac{5}{7}\right)^t \cdot |F|$$

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 $|F_0| \geq \left(\frac{5}{7}\right)^{|V_0|} \cdot |F|$. We now use the Sauer-Shelah lemma, stated next, in order to obtain the second property of the invariant.

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

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

By applying the Sauer-Shelah lemma[11] to $F_0|_{V_0}$, and noting that $2^{\frac{1}{2} \cdot |V_0|} \geq \sum_{j=0}^{\frac{|V_0|}{10}} \binom{|V_0|}{j}$, 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

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

This concludes the proof. Observe that our adversary indeed obeys the template described in Section 3.1: in each iteration, it first chooses the most likely message, and then discards inputs of Alice and Bob to preserve the invariant.

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

4 Open problems

Proving the KRW conjecture for $f \diamond MUX$, even in its weak version (Conjecture 2.3) seems to be beyond reach at the moment. However, there are simpler variants of the conjecture that might be more feasible. For start, one could consider the composition $U \diamond MUX$ of the universal relation with the multiplexor relation. This composition is defined similarly to $f \diamond MUX$, but instead of promising the players that $a \in f^{-1}(1)$ and $b \in f^{-1}(0)$ for some function f, we only promise that $a \neq b$. Since the complexity of the universal relation over m bits is known to be $m + \Theta(1)$ [TZ97], the natural analogue of Conjecture 2.3 in this case would be that

$$\mathsf{C}(U \diamond MUX) \geq m + \omega(\log n).$$

Can we prove such a bound? Such a proof would constitute an important step toward proving Conjecture 2.3. A nice feature of this question is that the composition $U \diamond MUX$ is a very clean communication problem, which does not involve an unknown function f.

Another interesting question is to consider the monotone setting: Karchmer-Wigderson relations have an analogue for monotone depth complexity: Given a monotone function f, the monotone KW relation mKW_f is defined similarly to KW_f, but this time the players are required to find a coordinate i where $x_i > y_i$ (rather than $x_i \neq y_i$). Karchmer and Wigderson [KW90] showed that $\mathsf{C}(mKW_f)$ is equal exactly to the monotone depth complexity of f. Monotone depth complexity and monotone KW relations are much better understood than their non-monotone counterparts, and in particular, the monotone version of $\mathbf{P} \not\subseteq \mathbf{NC}^1$ has been proved long ago [KW90].

It is therefore natural to ask whether we can prove a monotone analogue of Conjecture 2.3. We define the monotone version of the composition $f \diamond MUX$ similarly to $f \diamond MUX$, but we require the function f and the functions[12] $g_1, \ldots, g_m$ to be monotone, and we require the players to find an entry (i, j) where $(x_i)_j > (y_i)_j$ (rather than $(x_i)_j \neq (y_i)_j$). Can we prove a lower bound of $\mathsf{C}(mKW_f) + \omega(\log n)$ for this composition?

We note that proving either of the conjectures discussed above would not imply new circuit lower bounds. This might mean that those conjectures are more feasible than Conjecture 2.3.

Acknowledgments

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. Finally, we thank Oded Goldreich for many comments and suggestions that improved the presentation of this paper.

A Proof of Proposition 2.9

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

Conjecture 2.8 (restated). *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*

$$\mathsf{C}\left(KW_{f \circ (g_1, \ldots, g_m)}\right) \geq \mathsf{C}(KW_f) + \omega(\log n). \tag{4}$$

[12] Recall that $g_1, \ldots, g_m$ are the functions that are given as input to both players in $f \diamond MUX$.

Suppose that Conjecture 2.8 holds. In particular, let $\alpha : \mathbb{N} \to \mathbb{N}$ be the function such that $\alpha(n) = \omega(\log n)$ and such that Equation (4) holds with

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

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 A.1. 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 applied to the n values of v's children. Hence, the input of of $IMUX_{h,d}$ is the labeling of the nodes, and its output is the value of the root of $T_{n,d}$.

Note that the input of $IMUX_{n,d}$ is of length $N \overset{\text{def}}{=} n^d + \frac{n^d-1}{n-1} \cdot 2^n = \Theta(n^{d-1} \cdot 2^n)$. Below, we will prove that $\mathsf{C}(KW_{IMUX_{n,d}}) \geq (d-1) \cdot \alpha(n)$. 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

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

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 $\mathsf{C}(KW_{IMUX_{n,d}}) \geq (d-1) \cdot \alpha(n)$.

In fact, we prove a stronger result. Given a labeling L of the internal nodes of $T_{n,d}$, we denote by $IMUX_{n,d}[L]$ the function that is obtained from $IMUX_{n,d}$ by hard-wiring L as an input. In the rest of this appendix we prove the following proposition, which will conclude the proof.

Proposition A.2. *Assuming Conjecture 2.8, the following holds. For every $n, d \in \mathbb{N}$, there exists a labeling L of the internal nodes of $T_{n,d}$ such that $\mathsf{C}(KW_{IMUX_{n,d}[L]}) \geq (d-1) \cdot \alpha(n)$.*

Proof. Fix $n \in \mathbb{N}$. We prove the proposition by induction on d. The base case of $d = 1$ holds vacuously. Suppose that the proposition holds for some $d \geq 1$; that is, that there exists a labeling L_d of the internal nodes of $T_{n,d}$ such that $\mathsf{C}(KW_{IMUX_{n,d}[L_d]}) \geq (d-1) \cdot \alpha(n)$. We prove that the proposition holds for $d+1$ by constructing an appropriate labeling L_{d+1} for $T_{n,d+1}$.

Observe that the input length of $IMUX_{n,d}[L_d]$ is $m \overset{\text{def}}{=} n^d$ (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

$$\mathsf{C}\left(KW_{IMUX_{n,d}[L_d] \circ (g_1,\ldots,g_m)}\right) \geq \mathsf{C}(KW_{F_d}) + \alpha(n) \geq d \cdot \alpha(n).$$

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 $m = n^d$ nodes of depth d are labeled with the functions $g_1, \ldots, g_m$. Now, observe that the function $IMUX_{n,d+1}[L_{d+1}]$ is exactly the function

$$IMUX_{n,d}[L_d] \circ (g_1, \ldots, g_m),$$

and therefore $\mathsf{C}(KW_{IMUX_{n,d+1}[L_{d+1}]}) \geq d \cdot \alpha(n)$, as required. ■

B Proof of the Kővári-Sós-Turán theorem

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

Theorem 3.1 (restated). *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.

We use the following standard extension of the binomial coefficients to the real numbers: for every $x \in \mathbb{R}$ and $k \in \mathbb{N}$, let

$$\binom{x}{k} \stackrel{\text{def}}{=} \begin{cases} \frac{x\cdot(x-1)\cdots[x-(k-1)]}{k!} & \text{if } x \geq k-1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We may assume without loss of generality that $t < d$, since otherwise the theorem holds vacuously. We construct a bi-clique in G using the probabilistic method: let T be a uniformly distributed set of t vertices on the right, and let S be the set of vertices on the left that are connected to all the vertices in T. We prove that $\mathbb{E}\left[|S|\right] \geq \left(\frac{d-t}{n-t}\right)^t \cdot m$, and this will establish the theorem.

We identify the vertices on the left with $[m]$, and denote the degree of the vertex i by d_i. The vertex i belongs to S if T happens to be one of the $\binom{d_i}{t}$ subsets of the neighbors of i, and therefore

$$\Pr\left[i \in S\right] = \frac{\binom{d_i}{t}}{\binom{n}{t}}.$$

This implies that

$$\mathbb{E}\left[|S|\right] = \sum_{i=1}^{m} \frac{\binom{d_i}{t}}{\binom{n}{t}} = \left(\frac{1}{m} \cdot \sum_{i=1}^{m} \binom{d_i}{t}\right) \cdot \frac{1}{\binom{n}{t}} \cdot m.$$

Now, the binomial coefficient $\binom{x}{k}$ is a convex function of x, and hence by Jensen's inequality it follows that

$$\begin{aligned} \mathbb{E}\left[|S|\right] &\geq \binom{\frac{1}{m}\sum_{i=1}^{m} d_i}{t} \cdot \frac{1}{\binom{n}{t}} \cdot m \\ &= \frac{\binom{d}{t}}{\binom{n}{t}} \cdot m && \text{(By the definition of } d\text{)} \\ &= \frac{d\cdot(d-1)\cdots[d-(t+1)]}{n\cdot(n-1)\cdots[n-(t+1)]} \cdot m \\ &\geq \left(\frac{d-t}{n-t}\right)^t \cdot m, \end{aligned}$$

as required. ■

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