KRW Composition Theorems via Lifting

Susanna F. de Rezende*, Or Meir†, Jakob Nordström‡, Toniann Pitassi§ and Robert Robere¶
*Institute of Mathematics of the Czech Academy of Sciences
†Department of Computer Science, University of Haifa, Israel
‡University of Copenhagen and Lund University
§Department of Computer Science, University of Toronto, Canada
and Institute of Advanced Study, Princeton, USA.
¶McGill University, Canada

2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS) | 978-1-7281-9621-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/FOCS46700.2020.00013

***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 [13] 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 $\mathbf{P} \not\subseteq \mathbf{NC}^1$.**

Several works have made progress toward resolving this conjecture by proving special cases. In particular, these works proved the KRW conjecture for every outer function f, but only for few inner functions g. Thus, it is an important challenge to prove the KRW conjecture for a wider range of inner functions.

In this work, we extend significantly the range of inner functions that can be handled. First, we consider the *monotone* version of the KRW conjecture. We prove it for every monotone inner function g whose depth complexity can be lower bounded via a query-to-communication lifting theorem. This allows us to handle several new and well-studied functions such as the s-t-connectivity, clique, and generation functions.

In order to carry this progress back to the *non-monotone* setting, we introduce a new notion of *semi-monotone* composition, which combines the non-monotone complexity of the outer function f with the monotone complexity of the inner function g. In this setting, we prove the KRW conjecture for a similar selection of inner functions g, but only for a specific choice of the outer function f.

***Keywords*-KRW; Lifting; Simulation; Karchmer-Wigderson relations; KW relations; circuit complexity; circuit lower bounds; formula complexity; formula lower bounds; depth complexity; depth lower bounds; communication complexity;**

I. 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 $\mathbf{P} \not\subseteq \mathbf{NC}^1$. This question is an important milestone toward proving lower bounds on general circuits, and also captures the natural question of whether there are tractable computational tasks that cannot be parallelized. The state of the art is the work of Håstad [10], which proved a lower bound of $(3 - o(1)) \cdot \log n$, following a long line of work [24], [15], [1], [19], [12]. This lower bound has not been improved for more than two decades except for the lower order terms [25], and it is an important problem to break this barrier.

Karchmer, Raz, and Wigderson [13] 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

$$f \diamond g(x_1, \ldots, x_m) = f\left(g(x_1), \ldots, g(x_m)\right). \tag{1}$$

Let us denote by $\mathsf{D}(f)$ the minimal depth of a circuit with fan-in 2 that computes f. The circuit that computes $f \diamond g$ using Equation (1) has depth $\mathsf{D}(f) + \mathsf{D}(g)$. Karchmer et al. [13] conjectured that this upper bound is roughly optimal:

Conjecture I.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*

$$\mathsf{D}(f \diamond g) \approx \mathsf{D}(f) + \mathsf{D}(g). \tag{2}$$

Karchmer et al. observed that their conjecture, if proved, would imply that $\mathbf{P} \not\subseteq \mathbf{NC}^1$. They also successfully used this approach to give an alternative proof for $\mathbf{P} \not\subseteq \mathbf{NC}^1$ in the monotone setting. The meaning of "approximate equality" in Equation (2) is intentionally left vague, since there are many variants that would imply the separation.

While we are still far from resolving the KRW conjecture, several works [13], [6], [11], [10], [7], [5], [16] have made progress toward it by proving special cases. The state of the art is that the KRW conjecture is known to hold for every outer function f, but only when combined with two specific choices of the inner function g: the parity function, and the universal relation. There are no results proving the KRW conjecture for a broader family of inner functions.

In this work, we prove the KRW conjecture for a rich family of inner functions g, namely, those functions whose depth complexity can be lower bounded using *lifting theorems*. This includes functions that are considerably more interesting than previous composition theorems could handle. We prove these results in the *monotone* setting, and in a new setting which we call the *semi-monotone* setting. Below, we discuss the background to this work and present our results.

2575-8454/20/$31.00 ©2020 IEEE
DOI 10.1109/FOCS46700.2020.00013

Karchmer-Wigderson relations: It is useful to study the KRW conjecture through the lens of communication complexity, and in particular, using the framework of *Karchmer-Wigderson relations*. Let us denote the (deterministic) communication complexity of a problem R by $\mathsf{CC}(R)$. The *Karchmer-Wigderson relation* of a function $f : \{0,1\}^n \to \{0,1\}$, denoted KW_f, is the communication problem in which the inputs of Alice and Bob are $x \in f^{-1}(1)$ and $y \in f^{-1}(0)$ respectively, and their goal is to find a coordinate i such that $x_i \neq y_i$. Karchmer and Wigderson [14] observed that $\mathsf{D}(f) = \mathsf{CC}(KW_f)$. This connection between functions and communication problems allows us to study the depth complexity of functions using techniques from communication complexity.

The KRW conjecture from the KW perspective: Let $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ be non-constant functions. It will be useful to denote the KW relation $KW_{f \diamond g}$ of the composed function by $KW_f \diamond KW_g$. In this relation, Alice and Bob get $X \in (f \diamond g)^{-1}(1)$ and $Y \in (f \diamond g)^{-1}(0)$, viewed as $m \times n$ matrices, and their goal is to find an entry (i,j) such that $X_{i,j} \neq Y_{i,j}$. The KRW conjecture can be restated as:

$$\mathsf{CC}(KW_f \diamond KW_g) \approx \mathsf{CC}(KW_f) + \mathsf{CC}(KW_g).$$

It is worth noting the obvious protocol for solving $KW_f \diamond KW_g$: Let a, b be the column vectors that are obtained from applying g to the rows of X, Y, and observe that they constitute an instance of KW_f. The players begin by solving KW_f on a and b, thus obtaining a coordinate $i \in [m]$ such that $a_i \neq b_i$. Then, they solve KW_g on the rows X_i, Y_i, which constitute an instance of KW_g, thus obtaining a coordinate $j \in [n]$ where $X_{i,j} \neq Y_{i,j}$. The communication complexity of this protocol is $\mathsf{CC}(KW_f)+\mathsf{CC}(KW_g)$, and the KRW conjecture says that this obvious protocol is roughly optimal.

Previous work on the KRW conjecture: The KRW conjecture has been studied extensively, and a long line of papers have made progress on important restricted cases. These papers can be broadly divided into two categories.

The first category involves proving the KRW conjecture for a simplified communication problem. Specifically, Karchmer et al. [13] proposed a simplification of KW relations called the *universal relation* (denoted U_n) which is the following communication problem: Alice and Bob get two *distinct* strings $x, y \in \{0,1\}^n$, and their goal is to find a coordinate on which they disagree. The universal relation is harder to solve than KW relations, since the inputs of Alice and Bob are not assumed to come from the preimage of some function f, and so the protocol cannot take advantage of any properties of f. Just as the universal relation is a simplified version of KW relations, one can define simplified versions of $KW_f \diamond KW_g$, such as the composition $U_m \diamond U_n$ of two universal relations and the composition $KW_f \diamond U_n$ of a KW relation and a function. Several works have studied this type of compositions [13], [6], [11], [7], [16], and the state of the art is that the KRW conjecture holds for $KW_f \diamond U_n$ for every non-constant function $f : \{0,1\}^m \to \{0,1\}$ [7], [16].

The second category where important progress was made is for $KW_f \diamond KW_{\bigoplus}$ where f can be any non-constant function and $\bigoplus$ is the parity function. The KRW conjecture for this case has been proved implicitly by Håstad [10], and an alternative proof was recently given by Dinur and Meir [5].

The papers discussed so far are able to handle an arbitrary choice of the outer relation KW_f, but only very specific choices of the inner relation KW_g. This seems to suggest that the crux of the difficulty in proving the KRW conjecture lies in having to deal with an arbitrary choice of KW_g. In order to bypass this difficulty, Meir [18] recently observed that in order to prove that $\mathbf{P} \not\subseteq \mathbf{NC}^1$, it suffices to prove a version of the KRW conjecture in which KW_g is replaced with a specific communication problem, namely, the *multiplexor relation MUX* of [6]. Specifically, he defined a composition of the form $KW_f \diamond MUX$, and showed that if a variant of the KRW conjecture for $KW_f \diamond MUX$ holds for every non-constant outer function f, then $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

Motivation: Following the above discussion, our goal is to "replace" the relations U_n and $KW_{\bigoplus}$ in the known results with *MUX*. Unfortunately, this seems to be very difficult — in particular, the relation *MUX* seems to be significantly more complicated than U_n and $KW_{\bigoplus}$.

In order to make progress, we propose that a good intermediate goal would be to try to prove the KRW conjecture for the composition $KW_f \diamond KW_g$ *for inner functions* g *that are as complex and expressive as possible*. Ideally, by extending the range of inner functions g that we can handle, we will develop stronger techniques, which would eventually allow us to prove the conjecture for $KW_f \diamond MUX$.

An additional motivation for proving the KRW conjecture for harder inner functions is that it may allow us to improve the state of the art lower bounds on depth complexity. The best known lower bound of $(3-o(1)) \cdot \log n$ [1], [19], [12], [10] was achieved by implicitly proving the KRW conjecture for $KW_f \diamond KW_{\bigoplus}$, and it may be improved by proving the KRW conjecture for new inner functions.

The question is, which inner functions g would be good candidates for such a program? Ideally, a good candidate for g would be such that the KW relation KW_g is more interesting than U_n and $KW_{\bigoplus}$, but less complicated than *MUX*. Unfortunately, there are not too many examples for such relations: in fact, the relations U_n, $KW_{\bigoplus}$, and *MUX* are more or less the only relations that are well-understood. Thus, we have a shortage of good candidates g for this program.

As a way out of this shortage, we propose to consider *monotone depth complexity* in the study of inner functions. Given a *monotone* function f, the *monotone depth complexity of* f, denoted $\mathsf{mD}(f)$, is the minimal depth of a *monotone* circuit that computes f. The *monotone KW relation* of a

monotone function f, denoted mKW_f, is defined similarly to KW_f, but this time the goal of Alice and Bob is to find a coordinate i such that $x_i > y_i$ (rather than $x_i \neq y_i$). Karchmer and Wigderson [14] observed that $\mathsf{mD}(f) = \mathsf{CC}(mKW_f)$.

Fortunately, there are many monotone KW relations that are well-understood, and which are significantly more interesting than U_n and $KW_{\bigoplus}$. We would like to study compositions in which these monotone KW relations serve as the "inner part", in the hope that such study would lead us to discover new techniques.

A. Our results

1) The monotone composition theorem: Motivated by considerations discussed above, our first result concerns the *monotone KRW conjecture*. This conjecture says that for every two non-constant monotone functions f, g it holds that

$$\mathsf{CC}(mKW_f \diamond mKW_g) \approx \mathsf{CC}(mKW_f) + \mathsf{CC}(mKW_g)$$

(where $mKW_f \diamond mKW_g \stackrel{\text{def}}{=} mKW_{f \diamond g}$). This conjecture was studied in the original paper of Karchmer et al. [13], who proved it for the case where both f and g are the set-cover function, and used the latter result to prove that $\mathbf{P} \not\subseteq \mathbf{NC}^1$ in the monotone setting. However, this conjecture received far less attention than the non-monotone conjecture, perhaps because the monotone analogue of $\mathbf{P} \not\subseteq \mathbf{NC}^1$ has been known to hold for a long time, and monotone depth complexity is considered to be very well understood in general.

Nevertheless, we believe that this conjecture is interesting for several reasons: First, it is a very natural question in its own right. Second, if we cannot prove the KRW conjecture in the monotone setting, what hope do we have to prove it in the non-monotone setting, which is far less understood? Finally, proving the monotone KRW conjecture might prove useful for tackling other important questions on monotone depth complexity, such as proving lower bounds on slice functions (which in particular would imply non-monotone lower bounds).

Our first main result is a proof of the monotone KRW conjecture for every non-constant monotone function f, and for a wide range of monotone functions g. Specifically, our result holds for every function g whose monotone depth complexity can be lower bounded using a "lifting theorem": A *lifted search problem* $S \diamond \mathrm{gd}$ is obtained by composing a search problem S with an appropriate "gadget" function gd. A *lifting theorem* is a theorem that translates a lower bound for S in a weak model of computation to a lower bound for $S \diamond \mathrm{gd}$ in a strong model.

Here, the relevant weak model of computation is query complexity. Informally, the *query complexity* of a search problem S, denoted $\mathsf{Q}(S)$, is the number of queries one should make to the input in order to find a solution. Fix a gadget $\mathrm{gd} : \{0,1\}^t \times \{0,1\}^t \to \{0,1\}$ of input length t. A few lifting theorems [20], [3], [27], [2] establish that if the gadget gd satisfies certain conditions, then $\mathsf{CC}(S \diamond \mathrm{gd}) = \Omega(\mathsf{Q}(S) \cdot t)$. In this work, we use a lifting theorem of Chattopadhyay et al. [2], which holds for every gadget gd that has sufficiently low discrepancy and sufficiently large input length (see the full version of this work for the formal statement).

Our result says that the monotone KRW conjecture holds whenever the lower bound on mKW_g can be proved using the theorem of [2]. More specifically, there should exist a reduction to mKW_g from a lifted search problem $S \diamond \mathrm{gd}$ that satisfies the conditions of [2]. This is a much wider family of inner functions than what previous composition theorems could handle (i.e., universal relation and parity), though we are now working in the monotone rather than the non-monotone setting. Informally, the composition theorem can be stated as follows (see the full version of this work for the formal statement):

Theorem I.2 (monotone composition theorem, informal)**.** *Let $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ be non-constant monotone functions. If there is a lifted search problem $S \diamond \mathrm{gd}$ that reduces to mKW_g and satisfies the conditions of the theorem of [2], then*

$$\mathsf{CC}(mKW_f \diamond mKW_g) \geq \mathsf{CC}(mKW_f) + \Omega(\mathsf{Q}(S) \cdot t).$$

In particular, if $\mathsf{CC}(mKW_g) = \tilde{O}(\mathsf{Q}(S) \cdot t)$, then

$$\mathsf{CC}(mKW_f \diamond mKW_g) \geq \mathsf{CC}(mKW_f) + \tilde{\Omega}(\mathsf{CC}(mKW_g)). \quad (3)$$

We would like to note that the theorem is applicable to many interesting inner functions, including the classical s-t-connectivity function [14], [9], clique function [8], [21], and generation function [20] (see the full version of this work for details). Moreover, we would like to mention that the bound of Equation (3) is good enough for the purposes of the KRW conjecture.

We would also like to stress that while the statement of our monotone composition theorem refers to the lifting theorem of [2], we believe it can be adapted to work with similar lifting theorems such as the ones of [20], [3], [27] (in other words, the specific choice of the lifting theorem is not particularly crucial). Finally, it should be mentioned that the formal statement of the monotone composition theorem actually refers to formula complexity rather than depth complexity.

In order to prove Theorem I.2, we introduce a generalization of the lifting theorem of [2], which may be of independent interest. Roughly, our generalization shows a lower bound for the lifted problem $S \diamond \mathrm{gd}$ even when restricted to a subset of its inputs, as long as this subset satisfies a certain condition. See Section I-B1 for further discussion.

2) The semi-monotone composition theorem: Recall that our end goal is to gain insight into the *non-monotone* setting. To this end, we define a new form of composition,

called *semi-monotone composition*, which composes a *non-monotone* outer KW relation with a *monotone* inner KW relation. The purpose of this new composition is to enjoy the best of both worlds: On the one hand, this notion allows us to use candidates for the inner function g that come from the monotone setting. On the other hand, we believe that this notion is much closer to the non-monotone setting. Thus, by studying semi-monotone composition we can tackle issues that come up in the non-monotone setting but not in the monotone setting.

In order to gain intuition for the definition of this composition, consider the obvious protocol for the non-monotone composition $KW_f \diamond KW_g$. Recall that the inputs to this protocol are matrices $X, Y \in \{0,1\}^{m \times n}$, and that we denote by a, b the column vectors that are obtained by applying g to the rows of those matrices. Observe that there are two key properties of $KW_f \diamond KW_g$ that allow the obvious protocol to work:

- The players can find a row $i \in [m]$ such that $a_i \neq b_i$ by solving KW_f on a, b.
- For every $i \in [m]$ such that $a_i \neq b_i$, the players can find a solution for $KW_f \diamond KW_g$ by solving mKW_g on the rows X_i, Y_i.

Note that, while the obvious protocol always finds a solution in a row i where $a_i \neq b_i$, the rows where $a_i = b_i$ might contain solutions as well.

We define the semi-monotone composition of KW_f and mKW_g as a communication problem that is identical to $KW_f \diamond KW_g$, except that in the second property above, the non-monotone relation KW_g is replaced with the monotone relation mKW_g. Formally, we define semi-monotone composition as follows.

Definition I.3 (Semi-monotone composition)**.** Let $f : \{0,1\}^m \to \{0,1\}$ be a non-constant (possibly non-monotone) function, and let $g : \{0,1\}^n \to \{0,1\}$ be a non-constant monotone function. The *semi-monotone composition* $KW_f \diamond mKW_g$ is the following communication problem. Alice and Bob get as inputs $m \times n$ binary matrices X and Y respectively. Let $a, b \in \{0,1\}^m$ denote the column vectors that are obtained by applying g to each row of X and Y respectively. Then, $f(a) = 1$ and $f(b) = 0$, and the goal of the players is to find an entry (i, j) that satisfies one of the following three options:

- $a_i > b_i$ and $X_{i,j} > Y_{i,j}$.
- $a_i < b_i$ and $X_{i,j} < Y_{i,j}$.
- $a_i = b_i$ and $X_{i,j} \neq Y_{i,j}$.

Note that this communication problem has the desired structure: Indeed, it is not hard to see that when $a_i \neq b_i$, finding a solution in the i-th row is equivalent to solving mKW_g on X_i, Y_i. It is also not hard to show that $\mathsf{CC}(KW_f \diamond mKW_g) \leq \mathsf{CC}(KW_f) + \mathsf{CC}(mKW_g)$ bits, by using an appropriate variant of the obvious protocol of $KW_f \diamond KW_g$.

Therefore, a natural "semi-monotone variant" of the KRW conjecture would be the following.

Conjecture I.4 (Semi-monotone KRW conjecture)**.** *For every non-constant function $f : \{0,1\}^m \to \{0,1\}$ and non-constant monotone function $g : \{0,1\}^n \to \{0,1\}$,*

$$\mathsf{CC}(KW_f \diamond mKW_g) \gtrapprox \mathsf{CC}(KW_f) + \mathsf{CC}(mKW_g).$$

Our result: Ideally, we would have liked to prove Conjecture I.4 for every outer function f and for a wide range of inner functions g. Unfortunately, we are only able to prove it for the case where the outer relation KW_f is replaced with the (non-monotone) universal relation, i.e., the composition $U_m \diamond mKW_g$. This composition is defined similarly to Definition I.3, with the following difference: instead of promising that $f(a) = 1$ and $f(b) = 0$, we only promise that $a \neq b$. The natural conjecture in this case would be that

$$\mathsf{CC}(U_m \diamond mKW_g) \gtrapprox \mathsf{CC}(U_m) + \mathsf{CC}(mKW_g) \geq m + \mathsf{CC}(mKW_g), \tag{4}$$

where the second inequality holds since $\mathsf{CC}(U_m) = m + \Theta(1)$ (see [13], [26]). Our semi-monotone composition theorem proves such a result for every monotone inner function g for which a lower bound on $\mathsf{CC}(mKW_g)$ can be proved using a lifting theorem of [4].

Before describing our result, we briefly describe the lifting theorem of [4]. Given an unsatisfiable CNF formula ϕ, its *associated search problem* S_ϕ is the following task: given an assignment z to ϕ, find a clause of ϕ that is violated by z. The *Nullstellensatz degree* of ϕ, denoted $NS_{\mathbb{F}}(\phi)$, is a complexity measure that reflects how hard it is prove that ϕ is unsatisfiable in the Nullstellensatz proof system over a field $\mathbb{F}$. Fix a gadget $\mathrm{gd} : \{0,1\}^t \times \{0,1\}^t \to \{0,1\}$ of input length t. The lifting theorem of [4] says that $\mathsf{CC}(S_\phi \diamond \mathrm{gd}) \geq \Omega(NS_{\mathbb{F}_2}(\phi) \cdot t)$ provided that the gadget gd has sufficiently large rank.

Our result says that Equation (4) holds whenever there is a reduction from such a lifted problem $S_\phi \diamond \mathrm{gd}$ to mKW_g. We require the gadget gd to be the equality function eq, and require the reduction to be *injective* (see the full version of this work for the definition of injective reduction). Informally, our semi-monotone composition theorem can be stated as follows (see the full version of this work for the formal statement):

Theorem I.5 (semi-monotone composition theorem, informal)**.** *Let $g : \{0,1\}^n$ be a non-constant monotone function, and let* eq *be the equality function on strings of length t. Suppose there exists a lifted search problem $S_\phi \diamond \mathrm{eq}$ that reduces to mKW_g via an injective reduction and satisfies the conditions of the theorem of [4]. Then*

$$\mathsf{CC}(U_m \diamond mKW_g) \geq m + \Omega(NS_{\mathbb{F}_2}(\phi) \cdot t).$$

In particular, if $\mathsf{CC}(mKW_g) = \tilde{O}(NS_{\mathbb{F}_2}(\phi) \cdot t)$*, then*

$$\mathsf{CC}(U_m \diamond mKW_g) \geq m + \tilde{\Omega}(\mathsf{CC}(mKW_g)).$$

As in the case of the monotone composition theorem, the semi-monotone theorem is applicable to many interesting inner functions, including the classical s-t-connectivity, clique, and generation functions mentioned above (see the full version of this work for details), and the bound that it gives is good enough for the purposes of the KRW conjecture.

Comparison to monotone composition: Recall that our goal in defining semi-monotone composition is to captures issues that arise in the non-monotone setting but are not captured by the monotone setting. We claim that our definition succeeds in this task for at least one significant issue, to be discussed next.

Recall that the KRW conjecture says that the obvious protocol for $KW_f \diamond KW_g$ is essentially optimal. Intuitively, this should be the case since it seems that the best strategy for the players is to work on a row where $a_i \neq b_i$, and to do it, they must first find such a row. While it seems reasonable that the best strategy is to work on a row where $a_i \neq b_i$, it is not clear how to prove it: indeed, this is a central challenge in the proofs of known composition theorems (though not the only challenge).

On the other hand, Karchmer et al. [13] observed that in the monotone setting, the players can be forced to solve the problem on a row where $a_i > b_i$. This means that in the monotone setting, we can easily bypass a central challenge of the non-monotone case. An important feature of semi-monotone composition is that the observation of [13] fails for this composition. Hence, we believe that the semi-monotone setting is much closer to the non-monotone KRW conjecture than the monotone setting.

B. Our techniques

1) The monotone composition theorem: We use the high level proof strategy that was introduced by [6], and further developed in [5], [17], [16]. The main technical lemma is a structure theorem, formalizing that any correct protocol must first solve mKW_f, and then solve mKW_g. A bit more formally, we show that for any partial transcript π_1 of Π, if mKW_f has not yet been solved at π_1, then Π must send $\approx \mathsf{CC}(mKW_g)$ additional bits before it can find a solution for $mKW_f \diamond mKW_g$.

To accomplish this, at π_1, we partition the rows of X, Y into two types: (1) "revealed" rows where π_1 reveals a lot of information, and (2) "unrevealed" rows, where π_1 reveals only a small amount of information. We then show that the revealed rows can be forced to be useless (that is, we can ensure that there is no solution (i, j) where i is a revealed row). It follows that in order for the protocol to finish after π_1, it has to solve mKW_g on one of the unrevealed rows.

The remaining step is therefore to show that in order to solve mKW_g on one of the unrevealed rows, the protocol must transmit $\approx \mathsf{CC}(mKW_g)$ additional bits. While this claim sounds intuitive, proving it is non-trivial since some (small amount of) information has been learned about each unrevealed row, and this revealed information can be highly dependent. Moreover, the protocol is allowed to choose on which unrevealed row it solves mKW_g, and this could in principle make the task significantly easier. In previous works, these issues are dealt with in a way that is tailored to the particular choice of g. Specifically, one takes a known lower bound proof for KW_g, and shows that it still goes through even after accounting for the aforementioned complications.

In our case, we do not know the particular choice of g, but we do know that the lower bound for mKW_g is proved using the lifting theorem of [2]. Hence, our goal is show that this lower bound proof still goes through. To this end, we prove a generalization of this lifting theorem which may be of independent interest. Informally, our generalization shows that $S \diamond \mathrm{gd}$ remains hard even if we restrict it to a subset $\mathcal{X} \times \mathcal{Y}$ of its inputs, as long as the coordinates remain *unpredictable*. Since this is the case for the unrevealed rows, we get the lower bound that we desire.

The notion of unpredictability required by our lifting theorem is based on *average degree* as defined by [6], [20]: given a set of strings $\mathcal{W} \in \Lambda^\ell$ and a subset of coordinates $I \subseteq [\ell]$, the *average degree* $\mathrm{AvgDeg}_I(\mathcal{W})$ is the average number of ways to complete a string in $\mathcal{W}|_{[\ell]-I}$ to a string in $\mathcal{W}$. Informally, our generalized lifting theorem says the following (see the full version of this work for the formal statement):

Theorem I.6 (informal)**.** *Let* $S \diamond \mathrm{gd}$ *be a lifted search problem that satisfies the conditions of of [2]. Let* $\mathcal{X} \times \mathcal{Y}$ *be a subset of the inputs of* $S \diamond \mathrm{gd}$ *such that* $\mathrm{AvgDeg}_I(\mathcal{X})$ *and* $\mathrm{AvgDeg}_I(\mathcal{Y})$ *are sufficiently large for every set of coordinates* I*. Then, the communication complexity of solving* $S \diamond \mathrm{gd}$ *on the inputs in* $\mathcal{X} \times \mathcal{Y}$ *is at least* $\Omega(\mathsf{Q}(S) \cdot t)$*.*

Our proof of the generalized lifting theorem mostly follows the proof of [2], except for one significant issue: The original proof of [2] uses a potential argument to bound the communication complexity, where the potential function is the min-entropy deficiency with respect to the uniform distribution *over all the inputs*. In our proof, on the other hand, the potential function measures the deficiency with respect to the uniform distribution *over the restricted set of inputs*. The latter distribution is less structured, and hence the potential argument requires a more refined analysis.

2) The semi-monotone composition theorem: We prove the lower bound on $U_m \diamond mKW_g$ using the Razborov rank method [22]. Basically, in order to use this method to prove a lower bound on a communication problem $S \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$, one needs to construct a matrix A of order $|\mathcal{X}| \times |\mathcal{Y}|$

such that A has high rank, but its restriction to every S-monochromatic rectangle has low rank. Roughly, the lifting theorem of [4] gives such a matrix A for mKW_g, and we use this matrix to construct a corresponding matrix M for $U_m \diamond \mathit{mKW}_g$.

The matrix M for $U_m \diamond \mathit{mKW}_g$ is constructed as follows. The rows and columns of M are indexed by matrices X and Y respectively. We view the matrix M as a block matrix that consists of $2^m \cdot 2^m$ blocks — a block for each value of a and b. For every a, b such that $a = b$, the corresponding block is the all-zeros matrix. For every other choice of a, b, the corresponding block is formed by taking the Kronecker product, for every $i \in [m]$, of either A (if $a_i \neq b_i$) or the identity matrix I (if $a_i = b_i$).

The matrix M is constructed in this way in order to guarantee that all its restrictions to monochromatic rectangles have low rank. On the one hand, having the matrix A in rows i where $a_i \neq b_i$ guarantees that monochromatic rectangles that solve mKW_g on such rows X_i, Y_i have low rank. On the other hand, having the identity matrix I in rows i where $a_i = b_i$ guarantees that monochromatic rectangles that find different entries $X_{i,j} \neq Y_{i,j}$ are all-zeros rectangles.

An important part of the proof is the observation that the when the theorem of [4] is applied with the equality gadget over $\mathbb{F}_2$ (as we do), it gives a matrix A that satisfies $A^2 = I$. This property creates a connection between A and I that allows us to analyze the rank of M and of its sub-matrices using Gaussian elimination.

II. Open questions

An obvious question that arises from this work is whether we can strengthen our semi-monotone composition theorem (Theorem I.5) to work for every non-constant outer function f. As a starting point, can we prove such a semi-monotone composition theorem that holds when the inner function g is the s-t-connectivity function? We note that proving such a result would likely require new ideas, since our techniques seem to be insufficient:

- On the one hand, we cannot prove such a result along the lines of our monotone composition theorem, since in the semi-monotone setting we cannot assume that the protocol outputs an entry (i, j) for which $a_i \neq b_i$ (as in the observation of [13] in the monotone case).
- On the other hand, we cannot prove such a result along the lines of our semi-monotone composition theorem, since the Razborov rank measure cannot prove interesting lower bounds for non-monotone KW relations [23]. In particular, we would not be able to analyze the complexity of a non-monotone outer relation KW_f using this technique.

Another interesting question is whether we can strengthen our monotone composition theorem (Theorem I.2) even further: Although this theorem holds for many choices of the inner functions g, there are still a few "classical" functions that it does not cover — most notably the matching function [21]. Can we prove a monotone composition theorem where f can be any non-constant monotone function, and g is the matching function?

Finally, recall that in the long run, our goal is to prove the KRW conjecture for the composition $\mathit{KW}_f \diamond \mathit{MUX}$ (for every f), since this would imply that $\mathbf{P} \not\subseteq \mathbf{NC}^1$. To this end, it seems reasonable to try to prove first the monotone and semi-monotone versions of this conjecture. The monotone version might be within reach (see [18] for the statement of this conjecture). Can we prove it?

Acknowledgment

This work was partly carried out while the authors were visiting the Simons Institute for the Theory of Computing in association with the DIMACS/Simons Collaboration on Lower Bounds in Computational Complexity, which is conducted with support from the National Science Foundation.

Susanna F. de Rezende is supported by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2013) ERC grant agreement no. 279611, as well as by the Knut and Alice Wallenberg grants KAW 2016.0066 and KAW 2018.0371. Or Meir is supported by the Israel Science Foundation (grant No. 1445/16). Jakob Nordström is supported by the Swedish Research Council grant 2016-00782, the Knut and Alice Wallenberg grant KAW 2016.006, and the Independent Research Fund Denmark grant 9040-00389B. Toniann Pitassi is supported by NSERC and by NSF CCF grant 1900460. This research was performed while Robert Robere was a postdoctoral researcher at DIMACS and the Institute for Advanced Study. Robert Robere was supported by NSERC, the Charles Simonyi Endowment, and indirectly supported by the National Science Foundation Grant No. CCF-1900460. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] A. E. Andreev, "On a method for obtaining more than quadratic effective lower bounds for the complexity of π-schemes," *Moscow University Mathematics Bulletin*, vol. 42, no. 1, pp. 24–29, 1987.

[2] A. Chattopadhyay, Y. Filmus, S. Koroth, O. Meir, and T. Pitassi, "Query-to-communication lifting using low-discrepancy gadgets," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 26, p. 103, 2019.

[3] A. Chattopadhyay, M. Koucký, B. Loff, and S. Mukhopadhyay, "Simulation theorems via pseudo-random properties," *Computational Complexity*, vol. 28, pp. 617–659, Dec. 2019.

[4] S. F. de Rezende, O. Meir, J. Nordström, T. Pitassi, R. Robere, and M. Vinyals, "Lifting with simple gadgets and applications to circuit and proof complexity," in *Proceedings of the 61st Annual IEEE Symposium on Foundations of Computer Science (FOCS '20)*, Nov. 2020, also available as ECCC TR19-186.

[5] I. Dinur and O. Meir, "Toward the KRW composition conjecture: Cubic formula lower bounds via communication complexity," *Computational Complexity*, vol. 27, no. 3, pp. 375–462, 2018.

[6] J. Edmonds, R. Impagliazzo, S. Rudich, and J. Sgall, "Communication complexity towards lower bounds on circuit depth," *Computational Complexity*, vol. 10, no. 3, pp. 210–246, 2001.

[7] D. Gavinsky, O. Meir, O. Weinstein, and A. Wigderson, "Toward better formula lower bounds: The composition of a function and a universal relation," *SIAM J. Comput.*, vol. 46, no. 1, pp. 114–131, 2017.

[8] M. Goldmann and J. Håstad, "A simple lower bound for monotone clique using a communication game," *Inf. Process. Lett.*, vol. 41, no. 4, pp. 221–226, 1992.

[9] M. Grigni and M. Sipser, "Monotone separation of Logspace from NC," in *Structure in Complexity Theory Conference*, 1991, pp. 294–298.

[10] J. Håstad, "The shrinkage exponent of De Morgan formulas is 2," *SIAM J. Comput.*, vol. 27, no. 1, pp. 48–64, 1998.

[11] J. Håstad and A. Wigderson, "Composition of the universal relation," in *Advances in computational complexity theory, AMS-DIMACS*, 1993.

[12] R. Impagliazzo and N. Nisan, "The effect of random restrictions on formula size," *Random Struct. Algorithms*, vol. 4, no. 2, pp. 121–134, 1993.

[13] M. Karchmer, R. Raz, and A. Wigderson, "Super-logarithmic depth lower bounds via the direct sum in communication complexity," *Computational Complexity*, vol. 5, no. 3/4, pp. 191–204, 1995.

[14] M. Karchmer and A. Wigderson, "Monotone circuits for connectivity require super-logarithmic depth," *SIAM J. Discrete Math.*, vol. 3, no. 2, pp. 255–265, 1990.

[15] V. M. Khrapchenko, "A method of obtaining lower bounds for the complexity of π-schemes," *Mathematical Notes Academy of Sciences USSR*, vol. 10, pp. 474–479, 1972.

[16] S. Koroth and O. Meir, "Improved composition theorems for functions and relations," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM '18)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), vol. 116, Aug. 2018, pp. 48:1–48:18.

[17] O. Meir, "On derandomized composition of boolean functions," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 24, p. 146, 2017.

[18] ——, "Toward better depth lower bounds: Two results on the multiplexor relation," *Computational Complexity*, vol. 29, no. 1, p. 4, 2020, available on ECCC as TR19-120.

[19] M. Paterson and U. Zwick, "Shrinkage of De Morgan formulae under restriction," *Random Struct. Algorithms*, vol. 4, no. 2, pp. 135–150, 1993.

[20] R. Raz and P. McKenzie, "Separation of the monotone NC hierarchy," *Combinatorica*, vol. 19, no. 3, pp. 403–435, 1999.

[21] R. Raz and A. Wigderson, "Monotone circuits for matching require linear depth," *J. ACM*, vol. 39, no. 3, pp. 736–744, 1992.

[22] A. A. Razborov, "Applications of matrix methods to the theory of lower bounds in computational complexity," *Combinatorica*, vol. 10, no. 1, pp. 81–93, 1990.

[23] ——, "On submodular complexity measures," in *Proceedings of the London Mathematical Society Symposium on Boolean Function Complexity*. New York, NY, USA: Cambridge University Press, 1992, pp. 76–83.

[24] B. A. Subbotovskaya, "Realizations of linear functions by formulas using +,.,-," *Soviet Mathematics Doklady*, vol. 2, pp. 110–112, 1961.

[25] A. Tal, "Shrinkage of De Morgan formulae by spectral techniques," in *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science (FOCS '14)*, 2014, pp. 551–560.

[26] G. Tardos and U. Zwick, "The communication complexity of the universal relation," in *Proceedings of the Twelfth Annual IEEE Conference on Computational Complexity*, 1997, pp. 247–259.

[27] X. Wu, P. Yao, and H. S. Yuen, "Raz-McKenzie simulation with the inner product gadget," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 24, p. 10, 2017.