Super-cubic lower bound for generalized Karchmer–Wigderson games

Artur Ignatiev, Ivan Mihajlin, Alexander Smal

December 21, 2022

ISAAC 2022

Introduction

Motivation

We want to prove:

$$P \neq NC^1$$

Motivation

We want to prove:

$$P \neq NC^1$$

.

By proving the KRW conjecture.

Motivation

We want to prove:

$$P \neq NC^1$$

By proving the KRW conjecture.

(no connection to Korean Wons)

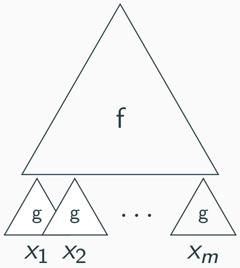
Karchmer–Raz–Wigderson conjecture

Block-composition

For $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$, *the block-composition* $f \diamond g : (\{0,1\}^n)^m \to \{0,1\}$ is defined by

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

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



The KRW conjecture

For any non-constant $f, g : \{0,1\}^m \to \{0,1\}$

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

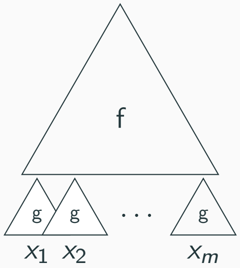
where $D(f)$ is the De Morgan formula complexity of f.

Block-composition

For $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$, *the block-composition* $f \diamond g : (\{0,1\}^n)^m \to \{0,1\}$ is defined by

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

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



The KRW conjecture

For any non-constant $f, g : \{0,1\}^m \to \{0,1\}$

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

where $D(f)$ is the De Morgan formula complexity of f.

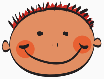
KRW conjecture implies $\mathrm{P} \not\subseteq \mathrm{NC}^1$**.**

Communication complexity

Introduced by Andrew Yao in 1979.

Alice

Bob



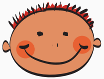
Communication complexity

Introduced by Andrew Yao in 1979.

Alice

$x \in \{0,1\}^n$

Bob



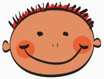
$y \in \{0,1\}^n$

Communication complexity

Introduced by Andrew Yao in 1979.

Alice

Bob



$x \in \{0,1\}^n$

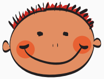
$y \in \{0,1\}^n$

Alice and Bob want to find z: $(x, y, z) \in R$.

Communication complexity

Introduced by Andrew Yao in 1979.

Alice $\xrightarrow{\quad b_1 \quad}$ Bob

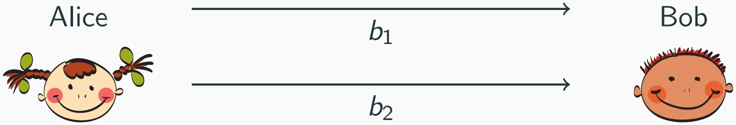


$x \in \{0,1\}^n$ $y \in \{0,1\}^n$

Alice and Bob want to find z: $(x, y, z) \in R$.

Communication complexity

Introduced by Andrew Yao in 1979.



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

Alice and Bob want to find z: $(x, y, z) \in R$.

Communication complexity

Introduced by Andrew Yao in 1979.

Alice

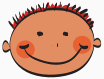
$x \in \{0,1\}^n$

$\xrightarrow{\quad b_1 \quad}$

$\xrightarrow{\quad b_2 \quad}$

$\xleftarrow{\quad b_3 \quad}$

Bob

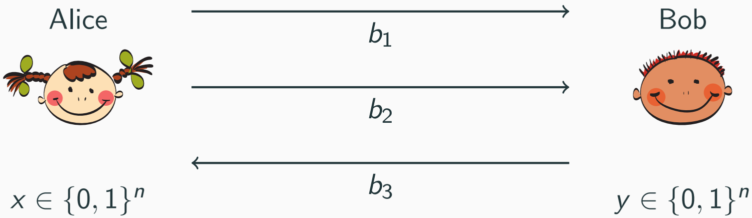


$y \in \{0,1\}^n$

Alice and Bob want to find z: $(x, y, z) \in R$.

Communication complexity

Introduced by Andrew Yao in 1979.



Alice and Bob want to find z: $(x, y, z) \in R$.

Communication complexity of relation R is a minimal number of messages that is enough to find z for any x and y, denoted $\mathrm{CC}(R)$.

Karchmer–Wigderson games

The Karchmer–Wigderson game for $f : \{0,1\}^n \to \{0,1\}$:

- Alice gets $x \in \{0,1\}^n$ such that $f(x) = 0$.
- Bob gets $y \in \{0,1\}^n$ such that $f(y) = 1$.
- Their goal is to find $i \in [n]$ such that $x_i \neq y_i$.

The Karchmer–Wigderson relation for f:

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

Karchmer–Wigderson games

The Karchmer–Wigderson game for $f : \{0,1\}^n \to \{0,1\}$:

- Alice gets $x \in \{0,1\}^n$ such that $f(x) = 0$.
- Bob gets $y \in \{0,1\}^n$ such that $f(y) = 1$.
- Their goal is to find $i \in [n]$ such that $x_i \neq y_i$.

The Karchmer–Wigderson relation for f:

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

Theorem (Karchmer, Wigderson)

For any non-constant $f : \{0,1\}^n \to \{0,1\}$,

$$\mathrm{CC}(\mathrm{KW}_f) = \mathrm{D}(f).$$

KRW conjecture (communication complexity formulation)

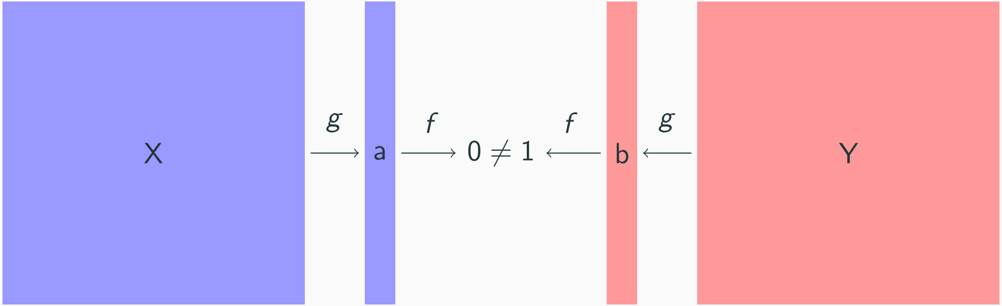
Let $f, g : \{0,1\}^m \to \{0,1\}$ be non-constant functions. Then

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

KRW conjecture (communication complexity formulation)

Let $f, g : \{0,1\}^m \to \{0,1\}$ be non-constant functions. Then

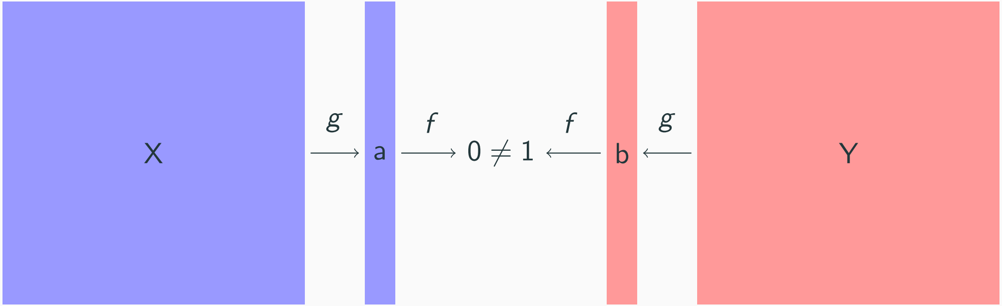
$$\mathrm{CC}(\mathrm{KW}_{f \diamond g}) \approx \mathrm{CC}(\mathrm{KW}_f) + \mathrm{CC}(\mathrm{KW}_g).$$



KRW conjecture (communication complexity formulation)

Let $f, g : \{0,1\}^m \to \{0,1\}$ be non-constant functions. Then

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

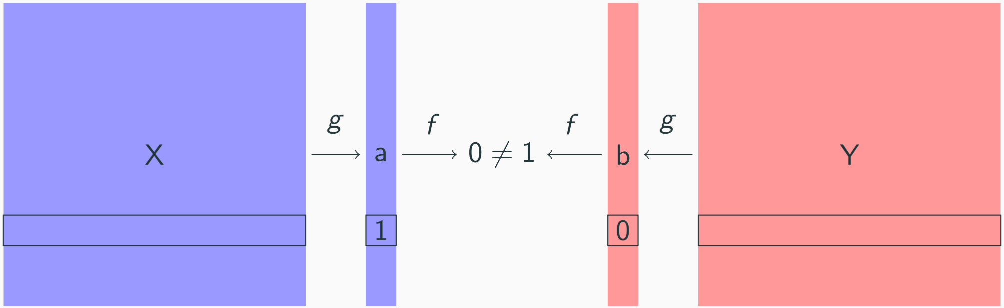


Solve KW_f on (a, b) first, then solve KW_g on (X_i, Y_i).

KRW conjecture (communication complexity formulation)

Let $f, g : \{0,1\}^m \to \{0,1\}$ be non-constant functions. Then

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

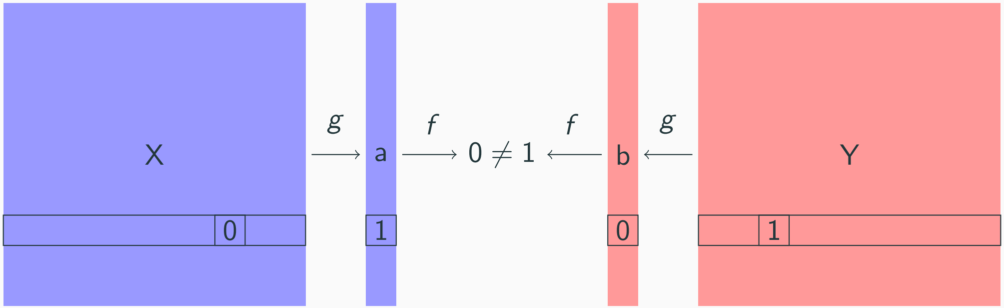


Solve KW_f on (a, b) first, then solve KW_g on (X_i, Y_i).

KRW conjecture (communication complexity formulation)

Let $f, g : \{0,1\}^m \to \{0,1\}$ be non-constant functions. Then

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



Solve KW_f on (a, b) first, then solve KW_g on (X_i, Y_i).

Universal relation

The universal relation of length n,

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

Universal relation

The universal relation of length n,

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

Known results:

- [Edmonds, Impagliazzo, Rudich, Sgall, 01] and [Håstad, Wigderson, 98]:

$$\mathrm{CC}(\mathrm{U}_n \diamond \mathrm{U}_n) = 2n - o(n).$$

- [Gavinsky, Meir, Weinstein, Wigderson, 16], improved by [Meir, Koroth, 19]:

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

- [Mihajlin, S. 21]:

$$\exists g \colon \{0,1\}^n \to \{0,1\} : \quad \mathrm{CC}(\mathrm{U}_n \diamond g) \geq 1.5n - o(n).$$
$$\exists g \colon \{0,1\}^n \to \{0,1\}^n : \ \mathrm{CC}(\mathrm{Id}_n \boxplus_2 g) \geq 1.5n - o(n).$$

Our results

XOR-composition

For $n, m \in \mathbb{N}$, and functions $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}^n$ *the XOR-composition* $f \boxplus_m g : \{0,1\}^{nm} \to \{0,1\}$ is defined by

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

where $x_i \in \{0,1\}^n$ and $\oplus$ denotes bit-wise XOR.

Theorem 1

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

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

Generalized Karchmer–Wigderson games

Definition

The generalized Karchmer–Wigderson game for $f : \{0,1\}^n \to \{0,1\}^\ell$:

- Alice gets $x \in \{0,1\}^n$, Bob gets $y \in \{0,1\}^n$.
- They are promised that $f(x) \neq f(y)$.
- Their goal is to find $i \in [n]$ such that $x_i \neq y_i$.

Theorem 2

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

Techniques

Proof of Theorem 1

Theorem 1

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

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

Proof by induction on the number of inner functions:

- Consider $\mathrm{Id}_n \boxplus (g_1, \ldots, g_m)$ instead of $\mathrm{Id}_n \boxplus g$.
- Assume a lower bound for $\mathrm{CC}_{S \times S}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m))$.
- Prove a lower bound for $\mathrm{CC}^{phd}_{S \times S}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{MUX}))$.
- Extract a hard function g_{m+1} such that a lower bound holds for $\mathrm{CC}_{S \times S}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, g_{m+1}))$.

Multiplexer relation

- Alice gets $g : \{0,1\}^n \to \{0,1\}^n$ and $x \in \{0,1\}^n$.
- Bob gets **the same** g and $y \in \{0,1\}^n$.
- They are promised that $g(x) \neq g(y)$.
- Goal: find $i \in [n]$ such that $x_i \neq y_i$.

Multiplexer relation

- Alice gets $g : \{0,1\}^n \to \{0,1\}^n$ and $x \in \{0,1\}^n$.
- Bob gets **the same** g and $y \in \{0,1\}^n$.
- They are promised that $g(x) \neq g(y)$.
- Goal: find $i \in [n]$ such that $x_i \neq y_i$.

How we use it?

Multiplexer relation

- Alice gets $g : \{0,1\}^n \to \{0,1\}^n$ and $x \in \{0,1\}^n$.
- Bob gets **the same** g and $y \in \{0,1\}^n$.
- They are promised that $g(x) \neq g(y)$.
- Goal: find $i \in [n]$ such that $x_i \neq y_i$.

How we use it?

- Assume that we have a lower bound for $\mathrm{CC}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{MUX}))$.

Multiplexer relation

- Alice gets $g : \{0,1\}^n \to \{0,1\}^n$ and $x \in \{0,1\}^n$.
- Bob gets **the same** g and $y \in \{0,1\}^n$.
- They are promised that $g(x) \neq g(y)$.
- Goal: find $i \in [n]$ such that $x_i \neq y_i$.

How we use it?

- Assume that we have a lower bound for $\mathrm{CC}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{MUX}))$.
- There exists the "hardest" g_{m+1} such that the same lower bound holds for $\mathrm{CC}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, g_{m+1})$.

Multiplexer relation

- Alice gets $g : \{0,1\}^n \to \{0,1\}^n$ and $x \in \{0,1\}^n$.
- Bob gets **the same** g and $y \in \{0,1\}^n$.
- They are promised that $g(x) \neq g(y)$.
- Goal: find $i \in [n]$ such that $x_i \neq y_i$.

How we use it?

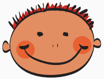
- Assume that we have a lower bound for $\mathrm{CC}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, \mathrm{MUX}))$.
- There exists the "hardest" g_{m+1} such that the same lower bound holds for $\mathrm{CC}(\mathrm{Id}_n \boxplus (g_1, \ldots, g_m, g_{m+1}))$.
- To make this plan works we need to allow players to choose a protocol *after* they see their inputs.

Half-duplex communication model

Players talk over half-duplex channel ("wakie-talkie") [HIMS18]

Alice

Bob



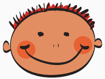
Half-duplex communication model

Players talk over half-duplex channel ("wakie-talkie") [HIMS18]

Alice

$x \in \{0,1\}^n$

Bob



$y \in \{0,1\}^n$

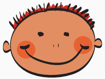
Half-duplex communication model

Players talk over half-duplex channel (“wakie-talkie”) [HIMS18]

Alice

$x \in \{0,1\}^n$

Bob



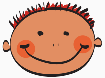
$y \in \{0,1\}^n$

Alice and Bob want to find z: $(x, y, z) \in R$.

Half-duplex communication model

Players talk over half-duplex channel ("wakie-talkie") [HIMS18]

Alice $\xrightarrow{b_1}$ Bob



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

Alice and Bob want to find z: $(x, y, z) \in R$.

Half-duplex communication model

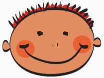
Players talk over half-duplex channel ("wakie-talkie") [HIMS18]

Alice

$\xrightarrow{\quad b_1 \quad}$

$\xleftarrow{\quad b_2 \quad}$

Bob

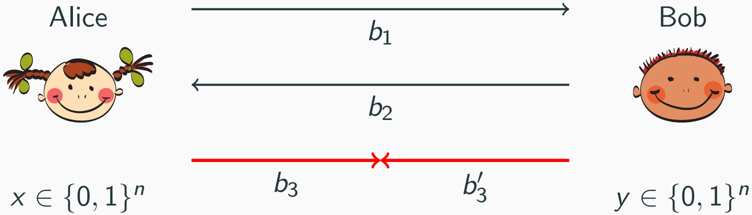


$x \in \{0,1\}^n$ $\qquad$ $y \in \{0,1\}^n$

Alice and Bob want to find z: $(x, y, z) \in R$.

Half-duplex communication model

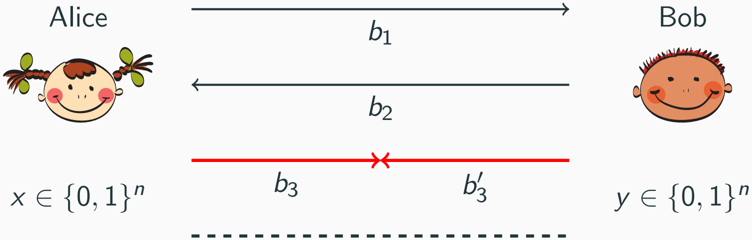
Players talk over half-duplex channel ("wakie-talkie") [HIMS18]



Alice and Bob want to find z: $(x, y, z) \in R$.

Half-duplex communication model

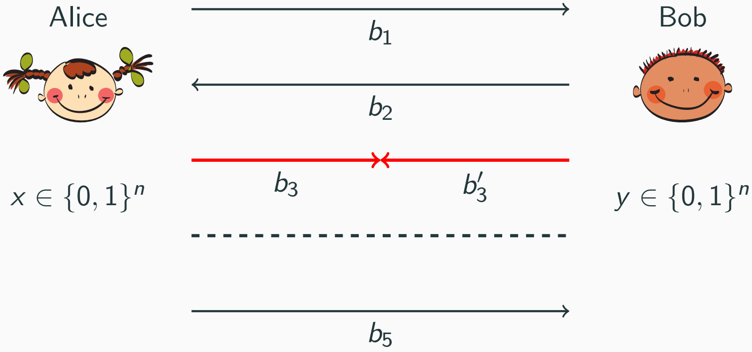
Players talk over half-duplex channel (“wakie-talkie”) [HIMS18]



Alice and Bob want to find z: $(x, y, z) \in R$.

Half-duplex communication model

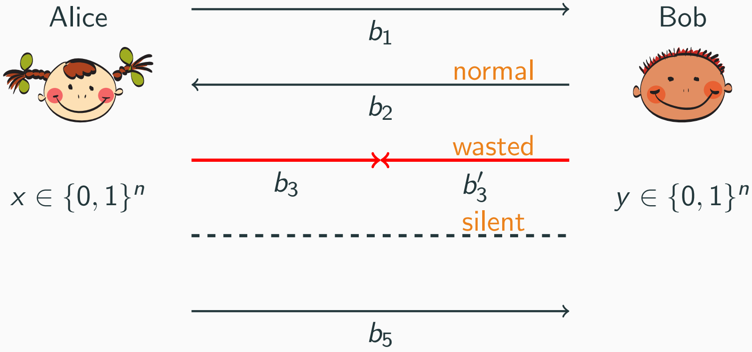
Players talk over half-duplex channel ("wakie-talkie") [HIMS18]



Alice and Bob want to find z: $(x, y, z) \in R$.

Half-duplex communication model

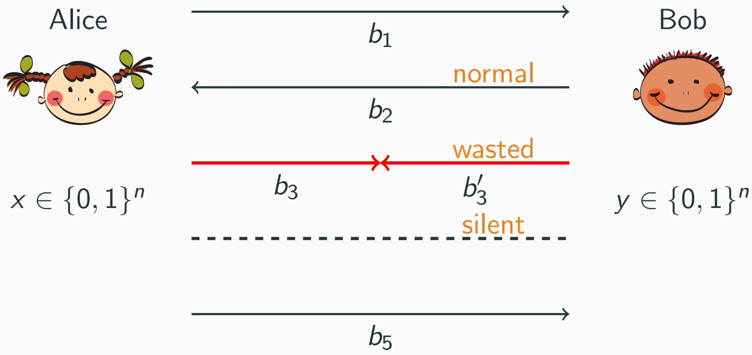
Players talk over half-duplex channel (“wakie-talkie”) [HIMS18]



Alice and Bob want to find z: $(x, y, z) \in R$.

Half-duplex communication model

Players talk over half-duplex channel ("wakie-talkie") [HIMS18]



Alice and Bob want to find z: $(x, y, z) \in R$.

Half-duplex communication complexity $\mathrm{CC}^{hd}(R)$ = required number of rounds.

Toy problem

Lemma

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

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

Toy problem

Lemma

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

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

Proof.

- Suppose that $\mathrm{CC}(\mathrm{KW}_f) \leq d$ for all $f : \{0,1\}^n \to \{0,1\}$.
- The following protocol solves MUX_n:
  - Alice follows the optimal protocol for f on x.
  - Bob follows the optimal protocol for f on y.
- Hence, $\mathrm{CC}^{hd}(\mathrm{MUX}_n) < d$.

□

Toy problem

Lemma

For all $n \in \mathbb{N}$, there exists $f : \{0,1\}^n \to \{0,1\}^n$ such that

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

Proof.

- Suppose that $\mathrm{CC}(\mathrm{KW}_f) \leq d$ for all $f : \{0,1\}^n \to \{0,1\}$.
- The following protocol solves MUX_n:
  - Alice follows the optimal protocol for f on x.
  - Bob follows the optimal protocol for f on y.
- Hence, $\mathrm{CC}^{hd}(\mathrm{MUX}_n) < d$.

□

Why this protocol does not work with classical model?

Proof of Theorem 2

Theorem 2

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

Proof of Theorem 2

Theorem 2

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

The proof follows the ideas of Håstad's $\tilde{\Omega}(n^3)$ De Morgan formula lower bound.

Proof of Theorem 2

Theorem 2

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

The proof follows the ideas of Håstad's $\tilde{\Omega}(n^3)$ De Morgan formula lower bound.

- Lower bound on *the XOR-composed Andreev's function* $\mathrm{Andr}_{n,m}$ is defined by

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

Proof of Theorem 2

Theorem 2

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

The proof follows the ideas of Håstad's $\tilde{\Omega}(n^3)$ De Morgan formula lower bound.

- Lower bound on *the XOR-composed Andreev's function* $\mathrm{Andr}_{n,m}$ is defined by

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

- Apply random restriction that kills many variables.

Proof of Theorem 2

Theorem 2

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

The proof follows the ideas of Håstad's $\tilde{\Omega}(n^3)$ De Morgan formula lower bound.

- Lower bound on *the XOR-composed Andreev's function* $\mathrm{Andr}_{n,m}$ is defined by

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

- Apply random restriction that kills many variables.
- Show that the protocol shrinks significantly.

Proof of Theorem 2

Theorem 2

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

The proof follows the ideas of Håstad's $\tilde{\Omega}(n^3)$ De Morgan formula lower bound.

- Lower bound on *the XOR-composed Andreev's function* $\mathrm{Andr}_{n,m}$ is defined by

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

- Apply random restriction that kills many variables.
- Show that the protocol shrinks significantly.
- Show that w.h.p. every internal $\oplus(x_i)$ have at least one variable that survived.

Proof of Theorem 2

Theorem 2

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

The proof follows the ideas of Håstad's $\tilde{\Omega}(n^3)$ De Morgan formula lower bound.

- Lower bound on *the XOR-composed Andreev's function* $\mathrm{Andr}_{n,m}$ is defined by

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

- Apply random restriction that kills many variables.
- Show that the protocol shrinks significantly.
- Show that w.h.p. every internal $\oplus(x_i)$ have at least one variable that survived.
- Apply Theorem 1.

Theorem 2: necessary ingredients

- Generalize random restriction technique for communication protocols.
  - See at the corresponding De Morgan formula.
- Shrinkage theorem for protocols.
  - Håstad's Shrinkage Theorem can be used for protocols.
- Convert depth lower bound into size lower bound.
  - Use Hrapchenko's balancing theorem.

Open questions

1. Show a better lower bound for block-composition of a universal relation and some function.
2. Non-trivial lower bounds for generalized Karchmer–Wigderson games for functions from $\{0,1\}^n \to \{0,1\}^m$ for $m = \alpha \log n$ for large enough α.
3. Show n^4 lower bound for generalized Karchmer–Wigderson games for function from $\{0,1\}^n \to \{0,1\}^{\log n}$ (avoid balancing?).
4. Are there interesting upper and lower bounds for generalized Karchmer–Wigderson outside of the scope of KRW conjecture?

Thank You!