The KRW conjecture

Ivan Mihajlin

May 28, 2021

Motivation

It would be amazing if any function computable in time $n^{O(1)}$ can be computed in time $O(\log n)$ on a parallel computer!

Motivation

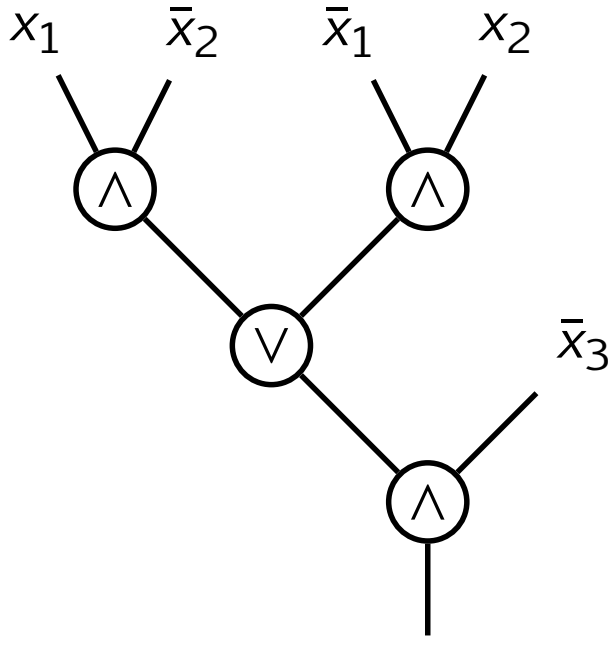
It would be amazing if any function computable in time $n^{O(1)}$ can be computed in time $O(\log n)$ on a parallel computer!

We want to prove that that it is not possible, in other words that:

$$\mathrm{P} \neq \mathrm{NC}^1$$

.

Formula



$$((x_1 \wedge \bar{x}_2) \vee (\bar{x}_1 \wedge x_2)) \wedge x_3$$

Formulas

It's hard to prove lower bounds against algorithms, so we will focus on formulas.

Formulas

It's hard to prove lower bounds against algorithms, so we will focus on formulas.

Definition

For $f : \{0,1\}^n \to \{0,1\}$: $D(f)$ is the minimal depth of a formula that computes f.

Formulas

It's hard to prove lower bounds against algorithms, so we will focus on formulas.

Definition

For $f : \{0,1\}^n \to \{0,1\}$: $D(f)$ is the minimal depth of a formula that computes f.

To prove $\mathrm{P} \neq \mathrm{NC}^1$ we need to show that for some $f \in \mathrm{P}$:

$$D(f) = \omega(\log n).$$

The KRW conjecture

Definition

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

Conjecture (The KRW conjecture)

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

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

Theorem

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

Karchmer-Wigderson games

Definition

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:

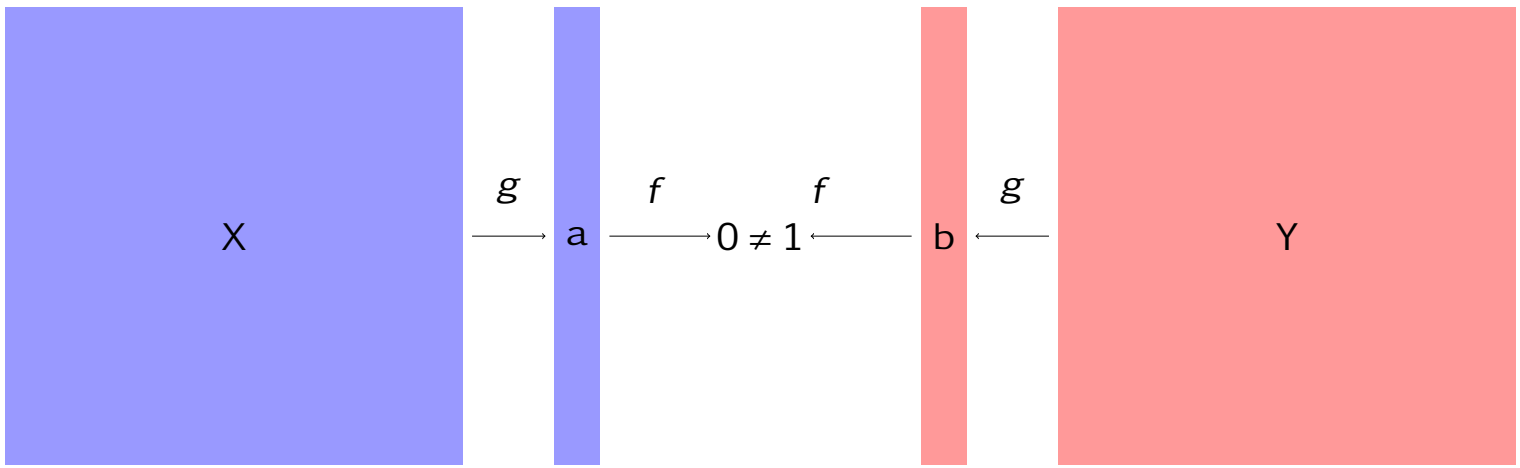
$$\mathrm{KW}_f = \{(x, y, i) \mid x, y \in \{0,1\}^n, i \in [n], f(x) = 0, f(y) = 1, x_i \neq y_i\}.$$

Conjecture (The KRW conjecture (reformulation))

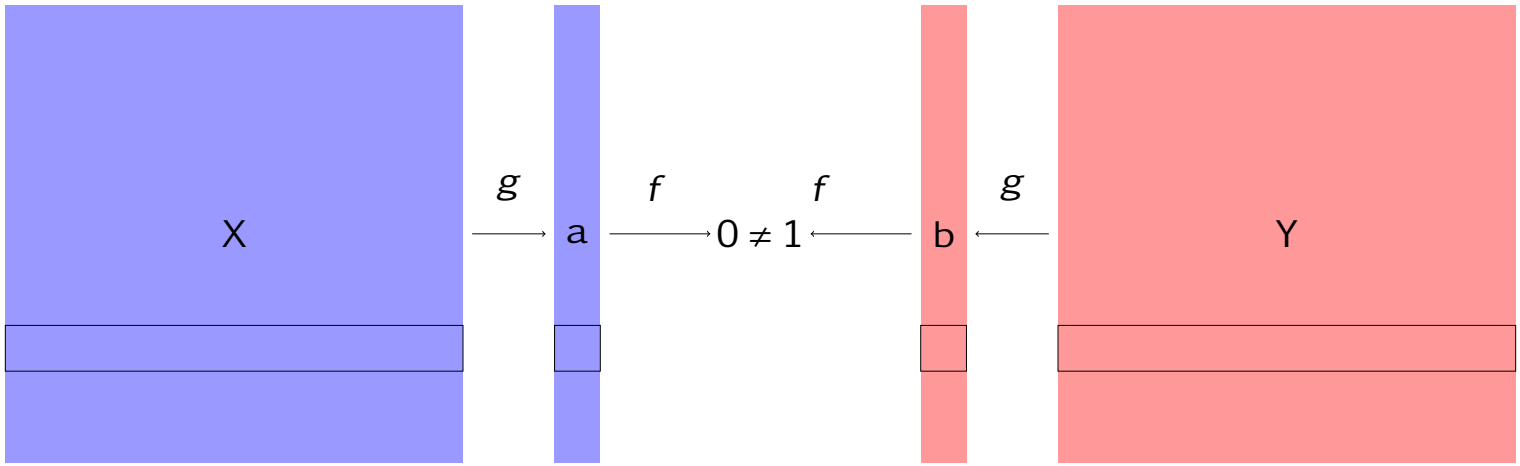
Let $f, g : \{0,1\}^m \to \{0,1\}$ *be non-constant functions. Then*

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

Composition of KW games



Composition of KW games



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

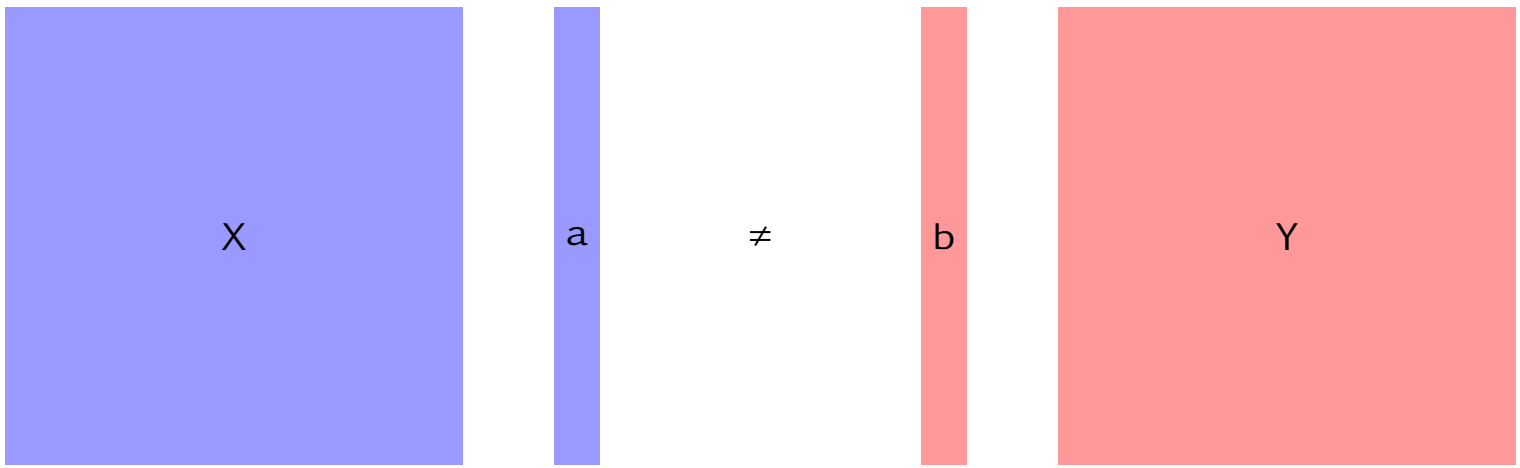
The universal relation of length n,

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

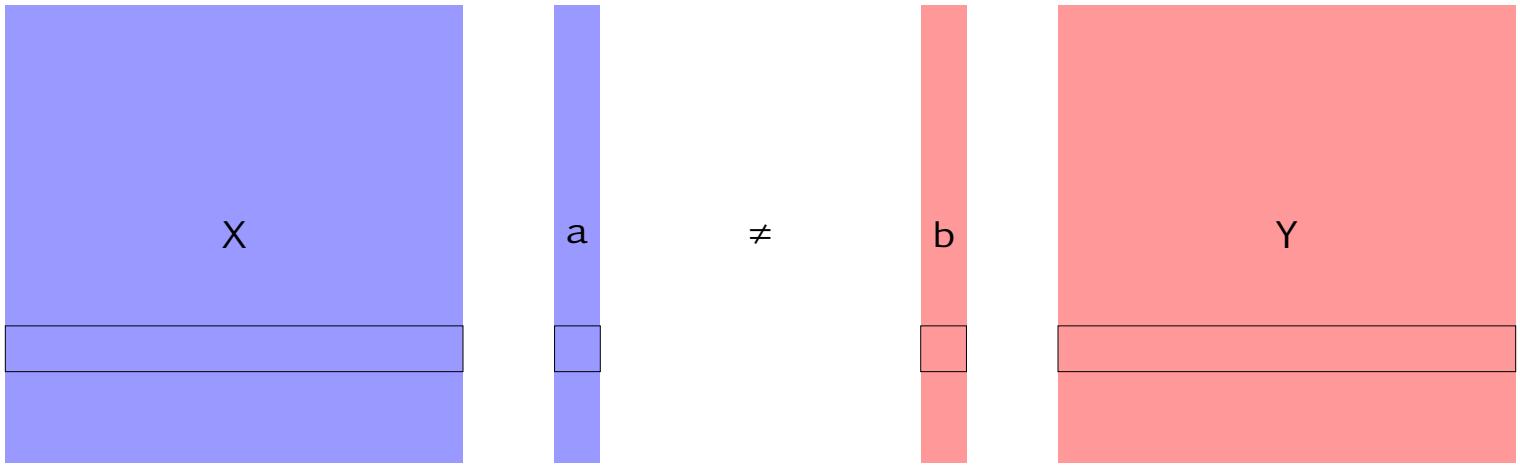
The composition of universal relations

$$\mathrm{U}_m \diamond \mathrm{U}_n = \Big\{\big((a, X), (b, Y), (i, j)\big) \mid a, b \in \{0,1\}^m, X, Y \in \{0,1\}^{m \times n},$$
$$i \in [m], j \in [n], a \neq b, \forall k \in [m] : a_k \neq b_k \implies X_k \neq Y_k\Big\}.$$

Composition of universal relations



Composition of universal relations



Use that $a_i \neq b_i$ implies that $X_i \neq Y_i$.
Solve U on (a, b) first, then solve U on rows (X_i, 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]:

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

- [Mihajlin, Smal 21]]:

$$\exists g : \ \mathrm{CC}(\mathrm{U}_n \diamond g) \geq 1.5n - o(n).$$

Maintaining symmetry

The first lower bound for $\mathrm{U}_n \diamond \mathrm{U}_n$ was proven by maintaining symmetry.

Maintaining symmetry

The first lower bound for $\mathrm{U}_n \diamond \mathrm{U}_n$ was proven by maintaining symmetry.

- Go down the protocol by the path that preserve as many inputs that could be given to both players as possible.

Maintaining symmetry

The first lower bound for $\mathrm{U}_n \diamond \mathrm{U}_n$ was proven by maintaining symmetry.

- Go down the protocol by the path that preserve as many inputs that could be given to both players as possible.
- Show that after $n - o(n)$ bits of communication there is still a row in A and B such that players don't know much about.

Maintaining symmetry

The first lower bound for $\mathrm{U}_n \diamond \mathrm{U}_n$ was proven by maintaining symmetry.

- Go down the protocol by the path that preserve as many inputs that could be given to both players as possible.
- Show that after $n - o(n)$ bits of communication there is still a row in A and B such that players don't know much about.
- Force players to find difference in that row.

Maintaining symmetry

The first lower bound for $\mathrm{U}_n \diamond \mathrm{U}_n$ was proven by maintaining symmetry.

- Go down the protocol by the path that preserve as many inputs that could be given to both players as possible.
- Show that after $n - o(n)$ bits of communication there is still a row in A and B such that players don't know much about.
- Force players to find difference in that row.
- Show that it would take $n - o(n)$ bits of communication.

Measure argument

The first lower bound for $f \diamond \mathrm{U}_n$ was proven by finding a good measure.

Measure argument

The first lower bound for $f \diamond \mathrm{U}_n$ was proven by finding a good measure.

- Find a measure μ of a rectangle $A \times B$ such that after every round of communication it does not reduce too much.

Measure argument

The first lower bound for $f \diamond \mathrm{U}_n$ was proven by finding a good measure.

- Find a measure μ of a rectangle $A \times B$ such that after every round of communication it does not reduce too much.
- Show a lower bound on μ at the start of the protocol.

Measure argument

The first lower bound for $f \diamond \mathrm{U}_n$ was proven by finding a good measure.

- Find a measure μ of a rectangle $A \times B$ such that after every round of communication it does not reduce too much.
- Show a lower bound on μ at the start of the protocol.
- Show an upper bound on μ at the end of the protocol.

Reasons to be optimistic

The lower bound for $\mathrm{U}_n \diamond g$ was proven by the symmetry argument!

Reasons to be optimistic

The lower bound for $\mathrm{U}_n \diamond g$ was proven by the symmetry argument!

We hope that one can find a good measure to swap U_n for a function f.

Multiplexer relation

Definition

The same function multiplexer communication game MUX_n:

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

Definition

The non-promise version MUX'_n:

- Alice gets $f : \{0,1\}^n \to \{0,1\}$ and $x \in \{0,1\}^n$: $g(x) = 0$,
- Bob gets $g : \{0,1\}^n \to \{0,1\}$ and $y \in \{0,1\}^n$: $g(y) = 1$,
- Goal: find $i \in [n]$ such that $x_i \neq y_i$, or output $\perp$ if $f \neq g$.

Half-duplex communication complexity: definitions

- Alice and Bob communication over half-duplex channel.
- Every round each player chooses one of three actions: send 0, send 1, or receive. Three types of rounds:
  - **classical**: one sends, one receives
  - **wasted**: both sends
  - **silent**: both receives
- Protocol is a pair of rooted trees of arity 4 (send 0, send 1, receive 0, and receive 1).
- For all $f\{0,1\}^n \to \{0,1\}$,

$$\mathrm{CC}(f) \geq \mathrm{CC}^{hd}(f) \geq \mathrm{CC}(f)/2.$$

- $\mathrm{CC}^{hd}(\mathrm{EQ}_n) \geq n/\log 2.5$.

Half-duplex communication complexity: facts

Theorem

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

Lemma

For all $n \in \mathbb{N}$, there exist a function $f : \{0,1\}^n \to \{0,1\}$ 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 shortest protocol for f on x.
  - Bob follows the shortest protocol for g on y.
  - They check that the answer is correct using $O(\log n)$ bits.

Idea for the proof of $f \diamond g$

- Consider composition of multiplexor relations.

Idea for the proof of $f \diamond g$

- Consider composition of multiplexor relations.
- Find a good measure μ.

Idea for the proof of $f \diamond g$

- Consider composition of multiplexor relations.
- Find a good measure μ.
- Show that this measure does not reduce too much after one round of a half-duplex protocol.

Idea for the proof of $f \diamond g$

- Consider composition of multiplexor relations.
- Find a good measure μ.
- Show that this measure does not reduce too much after one round of a half-duplex protocol.
- Show lower bound on this measure at the start and upper bound at the end of the protocol.

Idea for the proof of $f \diamond g$

- Consider composition of multiplexor relations.
- Find a good measure μ.
- Show that this measure does not reduce too much after one round of a half-duplex protocol.
- Show lower bound on this measure at the start and upper bound at the end of the protocol.
- Use it to prove lower bound and then use this lower bound to show existence of hard functions.

Idea for the proof of $f \diamond g$

- Consider composition of multiplexor relations.
- Find a good measure μ.
- Show that this measure does not reduce too much after one round of a half-duplex protocol.
- Show lower bound on this measure at the start and upper bound at the end of the protocol.
- Use it to prove lower bound and then use this lower bound to show existence of hard functions.
- Show That $\mathrm{P} \neq \mathrm{NC}^1$.