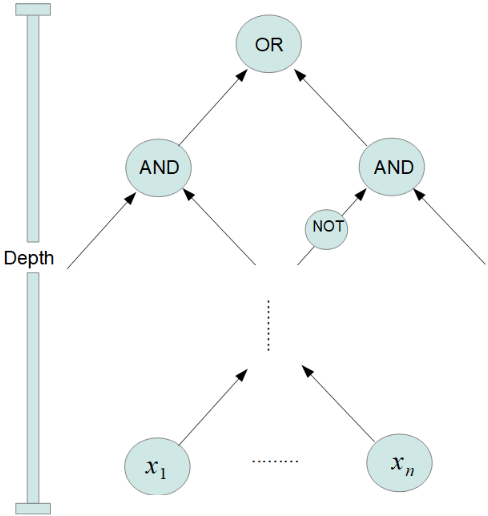
A KRW-like theorem for Strong Composition

Or Meir

Outline

Outline

Circuit depth



Fan-in 2: Every gate has at most 2 incoming wires.

Depth complexity

- Let $f : \{0,1\}^n \to \{0,1\}$.
- Depth complexity $\mathsf{D}(f)$: depth of a shallowest circuit for f.

Depth complexity

- Let $f : \{0,1\}^n \to \{0,1\}$.
- Depth complexity $\mathsf{D}(f)$: depth of a shallowest circuit for f.
- Major frontier: Explicit $f \in \mathbf{P}$ with $\mathsf{D}(f) = \omega(\log n)$.
- a.k.a. $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

Depth complexity

- Let $f : \{0,1\}^n \to \{0,1\}$.
- Depth complexity $\mathsf{D}(f)$: depth of a shallowest circuit for f.
- Major frontier: Explicit $f \in \mathbf{P}$ with $\mathsf{D}(f) = \omega(\log n)$.
- a.k.a. $\mathbf{P} \not\subseteq \mathbf{NC}^1$.
- State of the art: $D(f) \geq (3 - o(1)) \cdot \log n$ [H93, T14].

Composition

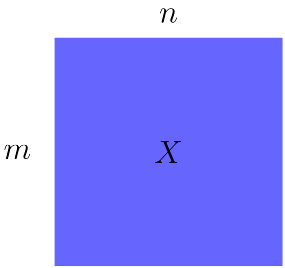
- [KRW91]: We need to understand composition.

Composition

- [KRW91]: We need to understand composition.
- Let $f : \{0,1\}^m \to \{0,1\}$, $g : \{0,1\}^n \to \{0,1\}$.

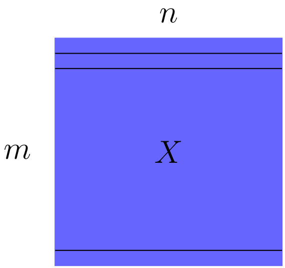
Composition

- [KRW91]: We need to understand composition.
- Let $f : \{0,1\}^m \to \{0,1\}$, $g : \{0,1\}^n \to \{0,1\}$.
- The composition $f \diamond g : \{0,1\}^{m \times n} \to \{0,1\}$ is



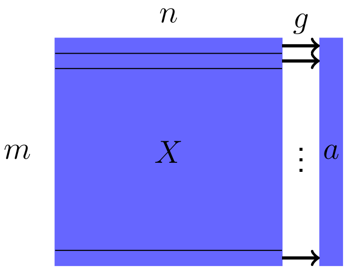
Composition

- [KRW91]: We need to understand composition.
- Let $f : \{0,1\}^m \to \{0,1\}$, $g : \{0,1\}^n \to \{0,1\}$.
- The composition $f \diamond g : \{0,1\}^{m \times n} \to \{0,1\}$ is



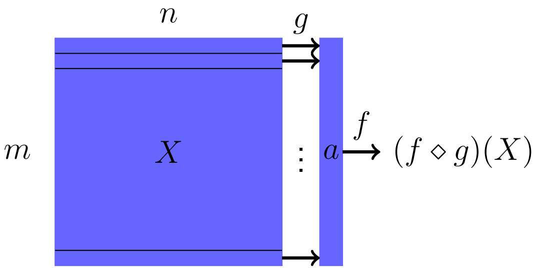
Composition

- [KRW91]: We need to understand composition.
- Let $f : \{0,1\}^m \to \{0,1\}$, $g : \{0,1\}^n \to \{0,1\}$.
- The composition $f \diamond g : \{0,1\}^{m \times n} \to \{0,1\}$ is

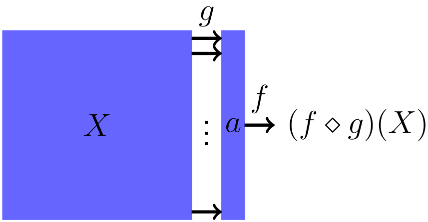


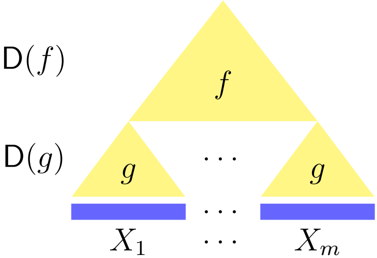
Composition

- [KRW91]: We need to understand composition.
- Let $f : \{0,1\}^m \to \{0,1\}$, $g : \{0,1\}^n \to \{0,1\}$.
- The composition $f \diamond g : \{0,1\}^{m \times n} \to \{0,1\}$ is



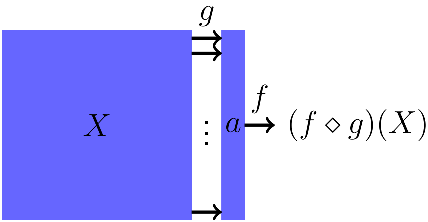
The KRW conjecture

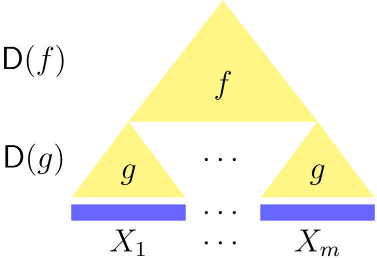




- Clearly, $\mathsf{D}(f \diamond g) \leq \mathsf{D}(f) + \mathsf{D}(g)$.

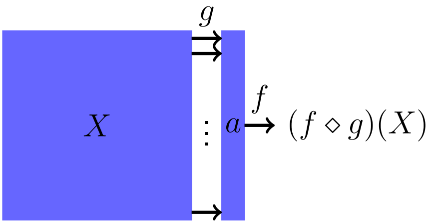
The KRW conjecture

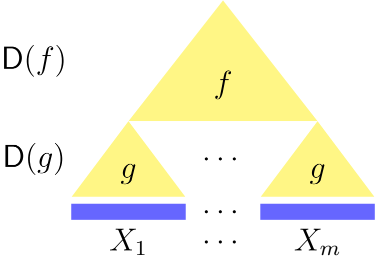




- Clearly, $\mathsf{D}(f \diamond g) \leq \mathsf{D}(f) + \mathsf{D}(g)$.
- KRW conjecture: $\forall f, g:\ \mathsf{D}(f \diamond g) \approx \mathsf{D}(f) + \mathsf{D}(g)$.

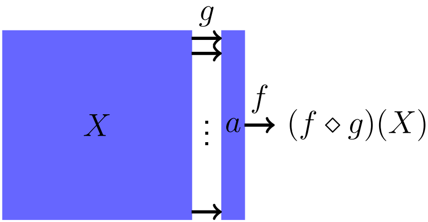
The KRW conjecture

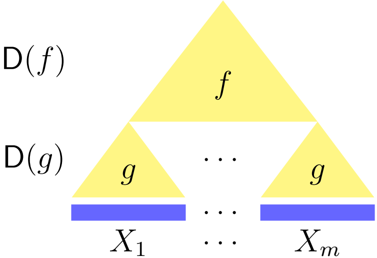




- Clearly, $\mathsf{D}(f \diamond g) \leq \mathsf{D}(f) + \mathsf{D}(g)$.
- KRW conjecture: $\forall f, g: \ \mathsf{D}(f \diamond g) \approx \mathsf{D}(f) + \mathsf{D}(g)$.
- Theorem [KRW91]: the conjecture implies that $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

The KRW conjecture





- Clearly, $\mathsf{D}(f \diamond g) \leq \mathsf{D}(f) + \mathsf{D}(g)$.
- KRW conjecture: $\forall f, g: \ \mathsf{D}(f \diamond g) \approx \mathsf{D}(f) + \mathsf{D}(g)$.
- Theorem [KRW91]: the conjecture implies that $\mathbf{P} \not\subseteq \mathbf{NC}^1$.
- Special cases: [EIRS91, H93, HW93, GMWW14, DM16, KM18, dRMNPR20, FMT21].

The weak KRW conjecture

- KRW conjecture: $\forall f \; \forall g : \; \mathsf{D}(f \diamond g) \approx \mathsf{D}(f) + \mathsf{D}(g)$.

The weak KRW conjecture

- KRW conjecture: $\forall f \; \forall g : \; \mathsf{D}(f \diamond g) \approx \mathsf{D}(f) + \mathsf{D}(g)$.
- Sufficient for $\mathbf{P} \not\subseteq \mathbf{NC}^1$ (folklore): $\forall f \; \exists$ hard g.

The weak KRW conjecture

- KRW conjecture: $\forall f\ \forall g:\ \mathsf{D}(f \diamond g) \approx \mathsf{D}(f) + \mathsf{D}(g)$.
- Sufficient for $\mathbf{P} \not\subseteq \mathbf{NC}^1$ (folklore): $\forall f\ \exists$ hard g.

Weak KRW conjecture

For every f and $n \in \mathbb{N}$, there exists $g : \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathsf{D}(f \diamond g) \geq \mathsf{D}(f) + \omega(\log n).$$

The weak KRW conjecture

- KRW conjecture: $\forall f\ \forall g:\ \mathsf{D}(f \diamond g) \approx \mathsf{D}(f) + \mathsf{D}(g)$.
- Sufficient for $\mathbf{P} \not\subseteq \mathbf{NC}^1$ (folklore): $\forall f\ \exists$ hard g.

Weak KRW conjecture

For every f and $n \in \mathbb{N}$, there exists $g : \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathsf{D}(f \diamond g) \geq \mathsf{D}(f) + \omega(\log n).$$

- [MS21]: proved such a result for $U \diamond g$.
  - $U =$ the universal relation.

Karchmer-Wigderson relations

- Relate $\mathsf{D}(f)$ to complexity of a communication problem KW_f.

Karchmer-Wigderson relations

- Relate $\mathsf{D}(f)$ to complexity of a communication problem KW_f.
- The KW relation KW_f is defined as follows:
  - Alice gets $x \in f^{-1}(1)$.
  - Bob gets $y \in f^{-1}(0)$.
  - Clearly, $x \neq y$, so $\exists i$ s.t. $x_i \neq y_i$.
  - Want to find such i.

Karchmer-Wigderson relations

- Relate $\mathsf{D}(f)$ to complexity of a communication problem KW_f.
- The KW relation KW_f is defined as follows:
  - Alice gets $x \in f^{-1}(1)$.
  - Bob gets $y \in f^{-1}(0)$.
  - Clearly, $x \neq y$, so $\exists i$ s.t. $x_i \neq y_i$.
  - Want to find such i.
- Theorem [KW88]: $\mathsf{D}(f) = \mathsf{CC}(\mathit{KW}_f)$.

Karchmer-Wigderson relations

- Relate $\mathsf{D}(f)$ to complexity of a communication problem KW_f.
- The KW relation KW_f is defined as follows:
  - Alice gets $x \in f^{-1}(1)$.
  - Bob gets $y \in f^{-1}(0)$.
  - Clearly, $x \neq y$, so $\exists i$ s.t. $x_i \neq y_i$.
  - Want to find such i.
- Theorem [KW88]: $\mathsf{D}(f) = \mathsf{CC}(KW_f)$.
- KRW conjecture: $\mathsf{CC}(KW_{f \diamond g}) \approx \mathsf{CC}(KW_f) + \mathsf{CC}(KW_g)$

The KW relation $KW_{f \diamond g}$

The KW relation $KW_{f \diamond g}$

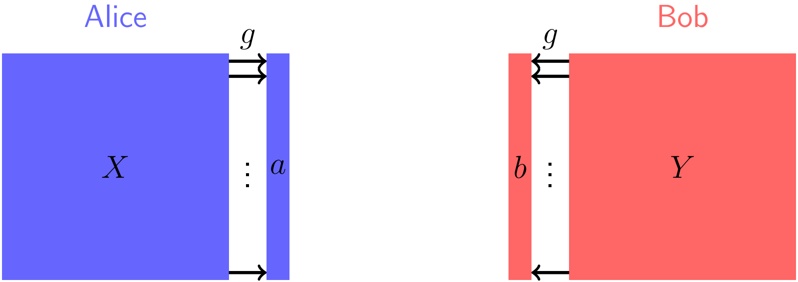
- Recall: $f \diamond g$ maps $\{0,1\}^{m \times n}$ to $\{0,1\}$.

The KW relation $KW_{f \diamond g}$

- Recall: $f \diamond g$ maps $\{0,1\}^{m \times n}$ to $\{0,1\}$.
- Goal: Find (i,j) such that $X_{i,j} \neq Y_{i,j}$.

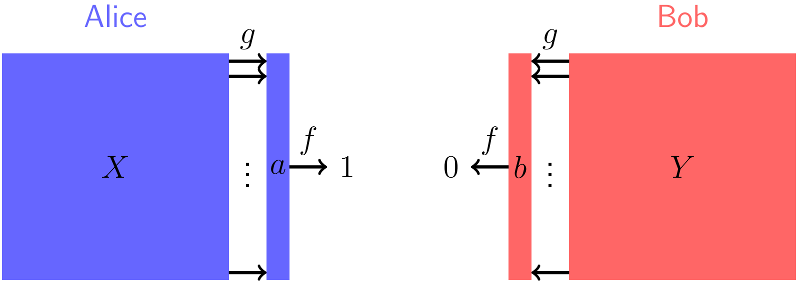
The KW relation $KW_{f \diamond g}$

- Recall: $f \diamond g$ maps $\{0,1\}^{m \times n}$ to $\{0,1\}$.
- Goal: Find (i,j) such that $X_{i,j} \neq Y_{i,j}$.



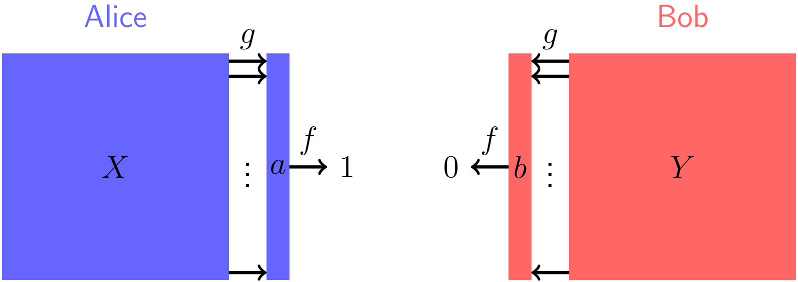
The KW relation $KW_{f \diamond g}$

- Recall: $f \diamond g$ maps $\{0,1\}^{m \times n}$ to $\{0,1\}$.
- Goal: Find (i,j) such that $X_{i,j} \neq Y_{i,j}$.



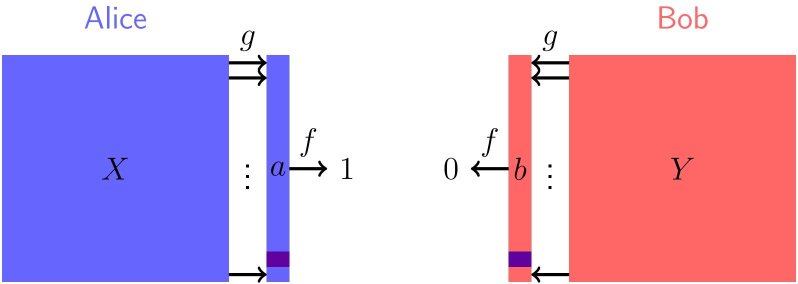
The KW relation $KW_{f \diamond g}$

- Recall: $f \diamond g$ maps $\{0,1\}^{m \times n}$ to $\{0,1\}$.
- Goal: Find (i,j) such that $X_{i,j} \neq Y_{i,j}$.
- Claim: $\mathsf{CC}(KW_{f \diamond g}) \leq \mathsf{CC}(KW_f) + \mathsf{CC}(KW_g)$.



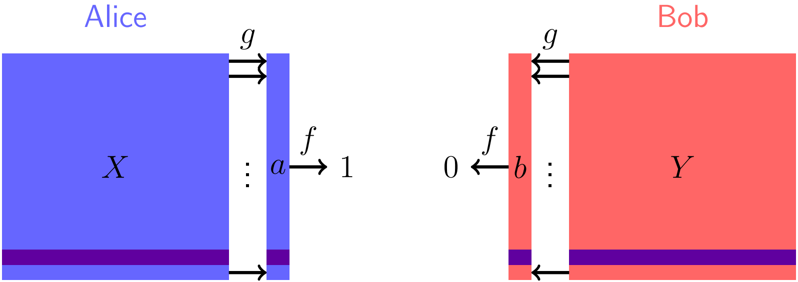
The KW relation $KW_{f \diamond g}$

- Recall: $f \diamond g$ maps $\{0,1\}^{m \times n}$ to $\{0,1\}$.
- Goal: Find (i,j) such that $X_{i,j} \neq Y_{i,j}$.
- Claim: $\mathsf{CC}(KW_{f \diamond g}) \leq \mathsf{CC}(KW_f) + \mathsf{CC}(KW_g)$.



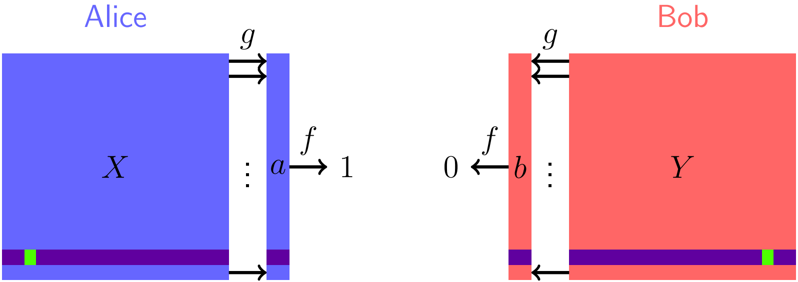
The KW relation $KW_{f \diamond g}$

- Recall: $f \diamond g$ maps $\{0,1\}^{m \times n}$ to $\{0,1\}$.
- Goal: Find (i,j) such that $X_{i,j} \neq Y_{i,j}$.
- Claim: $\mathsf{CC}(KW_{f \diamond g}) \leq \mathsf{CC}(KW_f) + \mathsf{CC}(KW_g)$.



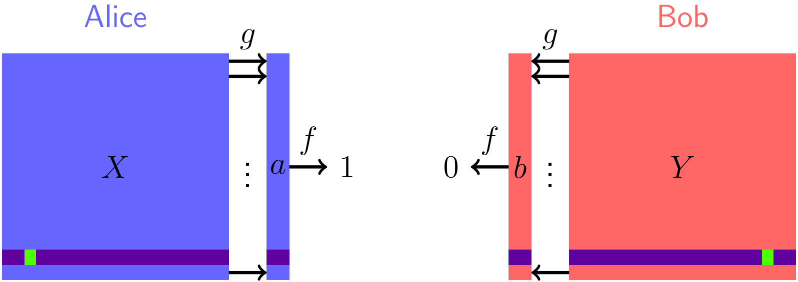
The KW relation $KW_{f \diamond g}$

- Recall: $f \diamond g$ maps $\{0,1\}^{m \times n}$ to $\{0,1\}$.
- Goal: Find (i,j) such that $X_{i,j} \neq Y_{i,j}$.
- Claim: $\mathsf{CC}(KW_{f \diamond g}) \leq \mathsf{CC}(KW_f) + \mathsf{CC}(KW_g)$.



The KW relation $KW_{f \diamond g}$

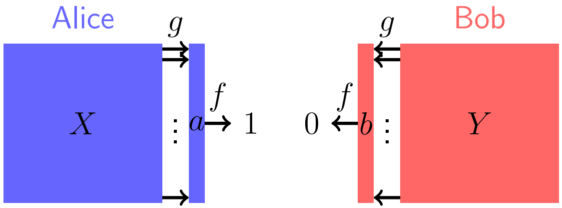
- Recall: $f \diamond g$ maps $\{0,1\}^{m \times n}$ to $\{0,1\}$.
- Goal: Find (i,j) such that $X_{i,j} \neq Y_{i,j}$.
- Claim: $\mathsf{CC}(KW_{f \diamond g}) \leq \mathsf{CC}(KW_f) + \mathsf{CC}(KW_g)$.



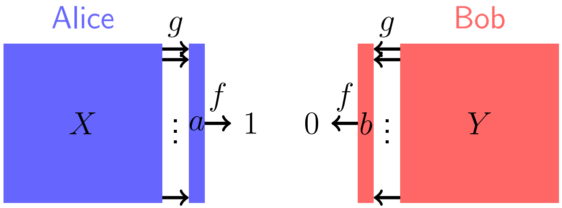
- KRW conjecture: the obvious protocol is essentially optimal.

Outline

Why should the obvious protocol be optimal?

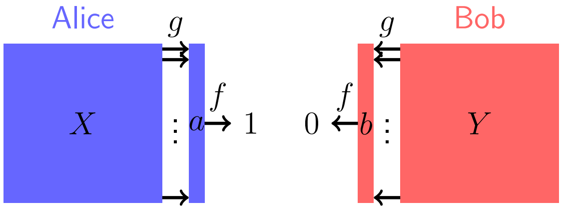


Why should the obvious protocol be optimal?



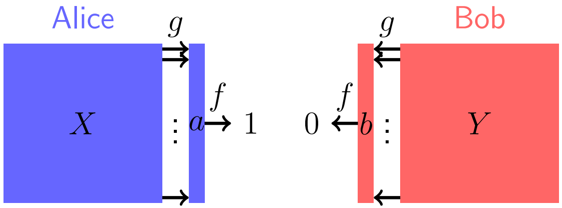
- The players should look for (i, j) in a row where $a_i \neq b_i$.

Why should the obvious protocol be optimal?



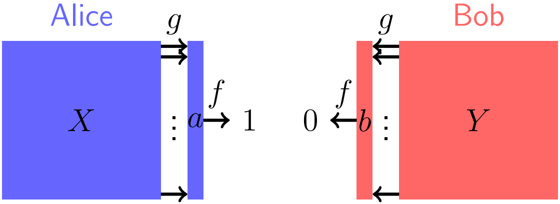
- The players should look for (i, j) in a row where $a_i \neq b_i$.
    - In other rows, a solution might not even exist.

Why should the obvious protocol be optimal?



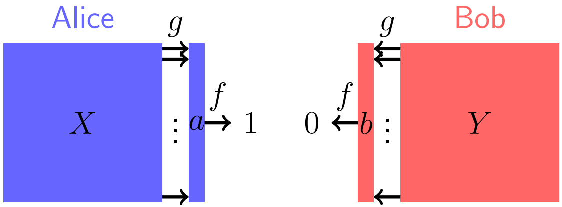
- The players should look for (i, j) in a row where $a_i \neq b_i$.
  - In other rows, a solution might not even exist.
- To do this, they must find a row i such that $a_i \neq b_i$.

Why should the obvious protocol be optimal?



- The players should look for (i, j) in a row where $a_i \neq b_i$.
  - In other rows, a solution might not even exist.
- To do this, they must find a row i such that $a_i \neq b_i$.
- To find such a row, they must solve KW_f.

Why should the obvious protocol be optimal?



- The players should look for (i, j) in a row where $a_i \neq b_i$.
  - In other rows, a solution might not even exist.
- To do this, they must find a row i such that $a_i \neq b_i$.
- To find such a row, they must solve KW_f.
- To find (i, j) in such a row, they must solve KW_g.

Obstacles

This intuition is very appealing...

Obstacles

This intuition is very appealing... but there are two obstacles in turning it into a proof:

Obstacles

This intuition is very appealing... but there are two obstacles in turning it into a proof:

1. We assumed that players find (i, j) s.t. $a_i \neq b_i$.

Obstacles

This intuition is very appealing... but there are two obstacles in turning it into a proof:

1. We assumed that players find (i, j) s.t. $a_i \neq b_i$.
   - but we need to prove it...

Obstacles

This intuition is very appealing... but there are two obstacles in turning it into a proof:

1. We assumed that players find (i, j) s.t. $a_i \neq b_i$.
   - but we need to prove it...
2. Even if players must solve both KW_f and KW_g,

Obstacles

This intuition is very appealing... but there are two obstacles in turning it into a proof:

1. We assumed that players find (i, j) s.t. $a_i \neq b_i$.
   - but we need to prove it...
2. Even if players must solve both KW_f and KW_g,
   - still does not imply they communicate $\mathsf{CC}(KW_f) + \mathsf{CC}(KW_g)$ bits.

Obstacles

This intuition is very appealing... but there are two obstacles in turning it into a proof:

1. We assumed that players find (i, j) s.t. $a_i \neq b_i$.
   - but we need to prove it...
2. Even if players must solve both KW_f and KW_g,
   - still does not imply they communicate $\mathsf{CC}(KW_f) + \mathsf{CC}(KW_g)$ bits.
   - This is the direct-sum problem.

Obstacles

This intuition is very appealing... but there are two obstacles in turning it into a proof:

1. We assumed that players find (i, j) s.t. $a_i \neq b_i$.
   - but we need to prove it...
2. Even if players must solve both KW_f and KW_g,
   - still does not imply they communicate $\mathsf{CC}(KW_f) + \mathsf{CC}(KW_g)$ bits.
   - This is the direct-sum problem.

In this work, we focus on the direct-sum problem.

Strong composition

- The strong composition $KW_f \circledast KW_g$:

Strong composition

- The strong composition $KW_f \circledast KW_g$:
  - defined like $KW_{f \diamond g}$, but

Strong composition

- The strong composition $KW_f \circledast KW_g$:
  - defined like $KW_{f \diamond g}$, but
  - the solution (i, j) must be in a row where $a_i \neq b_i$.

Strong composition

- The strong composition $KW_f \circledast KW_g$:
  - defined like $KW_{f \diamond g}$, but
  - the solution (i, j) must be in a row where $a_i \neq b_i$.
- Challenge (folklore): Prove KRW conjecture for $KW_f \circledast KW_g$.

Strong composition

- The strong composition $KW_f \circledast KW_g$:
  - defined like $KW_{f \diamond g}$, but
  - the solution (i, j) must be in a row where $a_i \neq b_i$.
- Challenge (folklore): Prove KRW conjecture for $KW_f \circledast KW_g$.
  - Necessary for proving original KRW conjecture.

Strong composition

- The strong composition $KW_f \circledast KW_g$:
  - defined like $KW_{f \diamond g}$, but
  - the solution (i, j) must be in a row where $a_i \neq b_i$.
- Challenge (folklore): Prove KRW conjecture for $KW_f \circledast KW_g$.
  - Necessary for proving original KRW conjecture.
  - Focus on the direct-sum problem.

Our result

A “weak KRW” theorem ($\forall f\ \exists$ hard g) for strong composition.

Our result

A "weak KRW" theorem ($\forall f\ \exists$ hard g) for strong composition.

Theorem (informal)

For every $f : \{0,1\}^m \to \{0,1\}$ and every $n \in \mathbb{N}$,
there exists $g : \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathsf{CC}(KW_f \circledast KW_g) > \mathsf{CC}(KW_f) + n - 0.96 \cdot m - O\left(\log(m \cdot n)\right).$$

Our result

A "weak KRW" theorem ($\forall f$ $\exists$ hard g) for strong composition.

Theorem (informal)

For every $f : \{0,1\}^m \to \{0,1\}$ and every $n \in \mathbb{N}$,
there exists $g : \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathsf{CC}(KW_f \circledast KW_g) > \mathsf{CC}(KW_f) + n - 0.96 \cdot m - O(\log(m \cdot n)) .$$

If proved for $KW_{f \diamond g}$ instead of $KW_f \circledast KW_g$:

- an explicit function with depth complexity $\geq 3.04 \cdot \log n$.

Our result

A "weak KRW" theorem ($\forall f\ \exists$ hard g) for strong composition.

Theorem (informal)

For every $f : \{0,1\}^m \to \{0,1\}$ and every $n \in \mathbb{N}$, there exists $g : \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathsf{CC}(\mathit{KW}_f \circledast \mathit{KW}_g) > \mathsf{CC}(\mathit{KW}_f) + n - 0.96 \cdot m - O\left(\log(m \cdot n)\right).$$

If proved for $\mathit{KW}_{f \diamond g}$ instead of $\mathit{KW}_f \circledast \mathit{KW}_g$:

- an explicit function with depth complexity $\geq 3.04 \cdot \log n$.
- First improvement in depth lower bounds since [H93]!

Our result

A "weak KRW" theorem ($\forall f\ \exists$ hard g) for strong composition.

Theorem (informal)

For every $f : \{0,1\}^m \to \{0,1\}$ and every $n \in \mathbb{N}$,
there exists $g : \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathsf{CC}(\mathit{KW}_f \circledast \mathit{KW}_g) > \mathsf{CC}(\mathit{KW}_f) + n - 0.96 \cdot m - O(\log(m \cdot n)).$$

If proved for $\mathit{KW}_{f \diamond g}$ instead of $\mathit{KW}_f \circledast \mathit{KW}_g$:

- an explicit function with depth complexity $\geq 3.04 \cdot \log n$.
- First improvement in depth lower bounds since [H93]!
- Insufficient for proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$ due to $-0.96 \cdot m$.

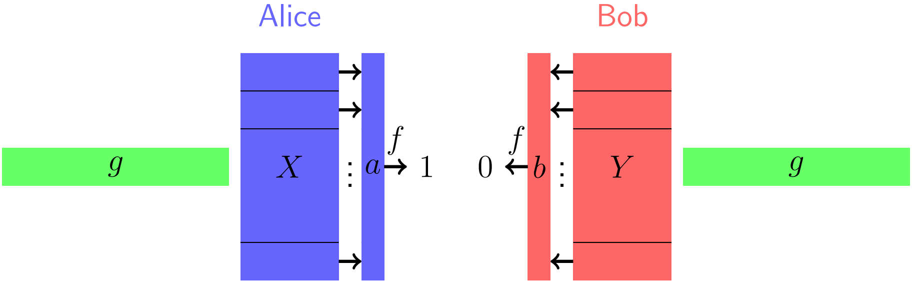
Outline

Multiplexor composition

- Fix a function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$.
- Goal: $\exists\ g : \{0,1\}^n \to \{0,1\}$ s.t. $\mathsf{CC}(\mathit{KW}_f \circledast \mathit{KW}_g)$ is large.

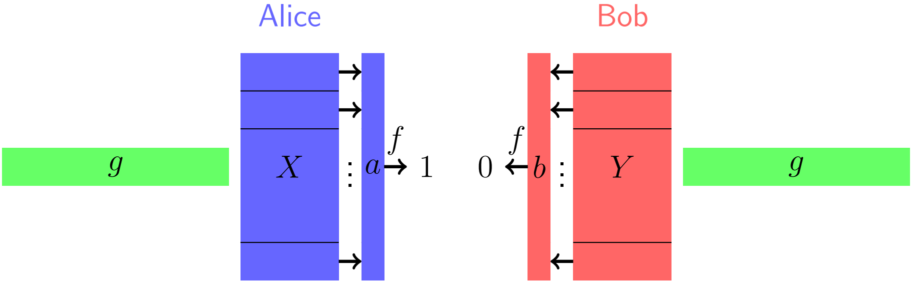
Multiplexor composition

- Fix a function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$.
- Goal: $\exists\, g : \{0,1\}^n \to \{0,1\}$ s.t. $\mathsf{CC}(\mathit{KW}_f \circledast \mathit{KW}_g)$ is large.
- Define the composition $\mathit{KW}_f \circledast \mathit{MUX}_n$:



Multiplexor composition

- Fix a function $f : \{0,1\}^m \to \{0,1\}$ and $n \in \mathbb{N}$.
- Goal: $\exists\, g : \{0,1\}^n \to \{0,1\}$ s.t. $\mathsf{CC}(KW_f \circledast KW_g)$ is large.
- Define the composition $KW_f \circledast MUX_n$:



- Suffices [MS21]*: $\mathsf{CC}(KW_f \circledast MUX_n) > \mathsf{CC}(KW_f) + n -$ loss.

Proof strategy [EIRS91]

- We wish to show that the following protocol is optimal:

Proof strategy [EIRS91]

- We wish to show that the following protocol is optimal:
  - First solve KW_f on a and b.

Proof strategy [EIRS91]

- We wish to show that the following protocol is optimal:
  - First solve KW_f on a and b.
  - Then solve KW_g on X_i and Y_i.

Proof strategy [EIRS91]

- We wish to show that the following protocol is optimal:
  - First solve KW_f on a and b.
  - Then solve KW_g on X_i and Y_i.
- Challenge: Cannot solve KW_f and KW_g together faster than solving each of them separately.

Proof strategy [EIRS91]

- We wish to show that the following protocol is optimal:
  - First solve KW_f on a and b.
  - Then solve KW_g on X_i and Y_i.
- Challenge: Cannot solve KW_f and KW_g together faster than solving each of them separately.
- Intuition: Alice and Bob must finish solving KW_f before starting to solve KW_g.

Proof strategy [EIRS91]

- We wish to show that the following protocol is optimal:
  - First solve KW_f on a and b.
  - Then solve KW_g on X_i and Y_i.
- Challenge: Cannot solve KW_f and KW_g together faster than solving each of them separately.
- Intuition: Alice and Bob must finish solving KW_f before starting to solve KW_g.
- Fix a protocol Π for $KW_f \circledast MUX_n$.

Proof strategy [EIRS91]

- We wish to show that the following protocol is optimal:
  - First solve KW_f on a and b.
  - Then solve KW_g on X_i and Y_i.
- Challenge: Cannot solve KW_f and KW_g together faster than solving each of them separately.
- Intuition: Alice and Bob must finish solving KW_f before starting to solve KW_g.
- Fix a protocol Π for $KW_f \circledast MUX_n$.
- Roughly, we prove that:
  - as long as Π does not finish solving KW_f,
  - it cannot make progress on KW_g.

Proof strategy [EIRS91]

Structure theorem (informal)

Let π_1 be a partial transcript s.t.

- π_1 is still far from solving KW_f, and
- π_1 reveals little information about the inputs.

Then, after reaching π_1, the players must still communicate $\approx n$ more bits.

Proof strategy [EIRS91]

Structure theorem (informal)

Let π_1 be a partial transcript s.t.

- π_1 is still far from solving KW_f, and
- π_1 reveals little information about the inputs.

Then, after reaching π_1, the players must still communicate $\approx n$ more bits.

- It is not hard to show that there exists such π_1 of length $\mathsf{CC}(\mathit{KW}_f) - \mathsf{loss}$.

Proof strategy [EIRS91]

Structure theorem (informal)

Let π_1 be a partial transcript s.t.

- π_1 is still far from solving KW_f, and
- π_1 reveals little information about the inputs.

Then, after reaching π_1, the players must still communicate $\approx n$ more bits.

- It is not hard to show that there exists such π_1 of length $\mathsf{CC}(KW_f) - \mathsf{loss}$.
- By applying the theorem, we get a lower bound of

$$\approx \mathsf{CC}(KW_f) + n - \mathsf{loss}.$$

Outline

Intersecting functions

- Fix a partial transcript π_1.
- Goal: players must communicate $\approx n$ more bits.

Intersecting functions

- Fix a partial transcript π_1.
- Goal: players must communicate $\approx n$ more bits.

Notation

For every function $g : \{0,1\}^n \to \{0,1\}$ denote:

$$\mathcal{X}(g) = \{X : \text{the input } (g, X) \text{ is legal for Alice given } \pi_1\}$$
$$\mathcal{Y}(g) = \text{Same for } Y \text{ and Bob.}$$

Intersecting functions

- Fix a partial transcript π_1.
- Goal: players must communicate $\approx n$ more bits.

Notation

For every function $g : \{0,1\}^n \to \{0,1\}$ denote:

$$\mathcal{X}(g) = \{X : \text{the input } (g, X) \text{ is legal for Alice given } \pi_1\}$$
$$\mathcal{Y}(g) = \text{Same for } Y \text{ and Bob.}$$

Definition

We say that $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ intersect iff

- either $\mathcal{X}(g_1) \cap \mathcal{Y}(g_2) \neq \emptyset$ or $\mathcal{X}(g_2) \cap \mathcal{Y}(g_1) \neq \emptyset$.

Intersecting functions

- Goal: players must communicate $\approx n$ more bits.

Definition

We say that $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ intersect iff

- either $\mathcal{X}(g_1) \cap \mathcal{Y}(g_2) \neq \emptyset$ or $\mathcal{X}(g_2) \cap \mathcal{Y}(g_1) \neq \emptyset$.

Intersecting functions

- Goal: players must communicate $\approx n$ more bits.

Definition

We say that $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ intersect iff

- either $\mathcal{X}(g_1) \cap \mathcal{Y}(g_2) \neq \emptyset$ or $\mathcal{X}(g_2) \cap \mathcal{Y}(g_1) \neq \emptyset$.

Lemma (implicit in [MS21])

If $\exists$ a set $\mathcal{V}$ of functions s.t. $\forall$ distinct $g_1, g_2 \in \mathcal{V}$ intersect, then the players must send $\gtrapprox \log\log|\mathcal{V}|$ more bits after reaching π_1.

Intersecting functions

- Goal: players must communicate $\approx n$ more bits.

Definition

We say that $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ intersect iff

- either $\mathcal{X}(g_1) \cap \mathcal{Y}(g_2) \neq \emptyset$ or $\mathcal{X}(g_2) \cap \mathcal{Y}(g_1) \neq \emptyset$.

Lemma (implicit in [MS21])

If $\exists$ a set $\mathcal{V}$ of functions s.t. $\forall$ distinct $g_1, g_2 \in \mathcal{V}$ intersect, then the players must send $\gtrapprox \log\log|\mathcal{V}|$ more bits after reaching π_1.

- Holds even for standard composition.

Intersecting functions

- Goal: players must communicate $\approx n$ more bits.

Definition

We say that $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ intersect iff

- either $\mathcal{X}(g_1) \cap \mathcal{Y}(g_2) \neq \emptyset$ or $\mathcal{X}(g_2) \cap \mathcal{Y}(g_1) \neq \emptyset$.

Lemma (implicit in [MS21])

If $\exists$ a set $\mathcal{V}$ of functions s.t. $\forall$ distinct $g_1, g_2 \in \mathcal{V}$ intersect, then the players must send $\gtrapprox \log\log|\mathcal{V}|$ more bits after reaching π_1.

- Holds even for standard composition.
- To use lemma, need to construct $\mathcal{V}$ s.t. $|\mathcal{V}| \approx 2^{2^n}$.

Intersecting functions

- Goal: players must communicate $\approx n$ more bits.

Definition

We say that $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ intersect iff

- either $\mathcal{X}(g_1) \cap \mathcal{Y}(g_2) \neq \emptyset$ or $\mathcal{X}(g_2) \cap \mathcal{Y}(g_1) \neq \emptyset$.

Lemma (implicit in [MS21])

If $\exists$ a set $\mathcal{V}$ of functions s.t. $\forall$ distinct $g_1, g_2 \in \mathcal{V}$ intersect, then the players must send $\gtrapprox \log \log |\mathcal{V}|$ more bits after reaching π_1.

- Holds even for standard composition.
- To use lemma, need to construct $\mathcal{V}$ s.t. $|\mathcal{V}| \approx 2^{2^n}$.
- Difficulty: need that every two functions in $\mathcal{V}$ intersect.

A graph-theoretic perspective

Definition

The characteristic graph $\mathcal{G}_{\pi_1}$ satisfies:

- The vertices are all functions $g : \{0,1\}^n \to \{0,1\}$.
- There is an edge betwen g_1 and g_2 iff they intersect.

A graph-theoretic perspective

Definition

The characteristic graph $\mathcal{G}_{\pi_1}$ satisfies:

- The vertices are all functions $g : \{0,1\}^n \to \{0,1\}$.
- There is an edge betwen g_1 and g_2 iff they intersect.

Lemma of [MS21]

The players must send $\gtrapprox \log\log\omega(\mathcal{G}_{\pi_1})$ more bits.
($\omega(\mathcal{G}_{\pi_1})$ — maximum size of a clique in $\mathcal{G}_{\pi_1}$).

A graph-theoretic perspective

Definition

The characteristic graph $\mathcal{G}_{\pi_1}$ satisfies:

- The vertices are all functions $g : \{0, 1\}^n \to \{0, 1\}$.
- There is an edge betwen g_1 and g_2 iff they intersect.

Lemma of [MS21]

The players must send $\gtrapprox \log \log \omega(\mathcal{G}_{\pi_1})$ more bits.
($\omega(\mathcal{G}_{\pi_1})$ — maximum size of a clique in $\mathcal{G}_{\pi_1}$).

Lemma (this work)

The players must send $\gtrapprox \log \log \chi(\mathcal{G}_{\pi_1})$ more bits
($\chi(\mathcal{G}_{\pi_1})$ — minimum number of colors required to color $\mathcal{G}_{\pi_1}$).

Back to strong composition

Back to strong composition

- Recall: In strong composition, players have to look for a solution in rows where $a_i \neq b_i$.

Back to strong composition

- Recall: In strong composition, players have to look for a solution in rows where $a_i \neq b_i$.
- The same results hold, but we need to change the notion of intersecting functions to focus on rows where $a_i \neq b_i$.

Back to strong composition

- Recall: In strong composition, players have to look for a solution in rows where $a_i \neq b_i$.
- The same results hold, but we need to change the notion of intersecting functions to focus on rows where $a_i \neq b_i$.

Definition

We say that $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ weakly intersect iff

Back to strong composition

- Recall: In strong composition, players have to look for a solution in rows where $a_i \neq b_i$.
- The same results hold, but we need to change the notion of intersecting functions to focus on rows where $a_i \neq b_i$.

Definition

We say that $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ weakly intersect iff

- there exist matrices $X \in \mathcal{X}(g_1)$ and $Y \in \mathcal{Y}(g_2)$ s.t.
  - $X_i = Y_i$ for every $i \in [m]$ for which $a_i \neq b_i$
  - (where $a = g_1(X)$ and $b = g_2(Y)$),

Back to strong composition

- Recall: In strong composition, players have to look for a solution in rows where $a_i \neq b_i$.
- The same results hold, but we need to change the notion of intersecting functions to focus on rows where $a_i \neq b_i$.

Definition

We say that $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ weakly intersect iff

- there exist matrices $X \in \mathcal{X}(g_1)$ and $Y \in \mathcal{Y}(g_2)$ s.t.
  - $X_i = Y_i$ for every $i \in [m]$ for which $a_i \neq b_i$
  - (where $a = g_1(X)$ and $b = g_2(Y)$),
- or vice versa.

Outline

Proving weak intersection

- How can we prove that two functions weakly intersect?

Proving weak intersection

- How can we prove that two functions weakly intersect?
- Need to prove: there exist $X \in \mathcal{X}(g_1)$ and $Y \in \mathcal{Y}(g_2)$ that are equal on the rows where $a_i \neq b_i$.

Proving weak intersection

- How can we prove that two functions weakly intersect?
- Need to prove: there exist $X \in \mathcal{X}(g_1)$ and $Y \in \mathcal{Y}(g_2)$ that are equal on the rows where $a_i \neq b_i$.
- Due to the assumptions on π_1:

Proving weak intersection

- How can we prove that two functions weakly intersect?
- Need to prove: there exist $X \in \mathcal{X}(g_1)$ and $Y \in \mathcal{Y}(g_2)$ that are equal on the rows where $a_i \neq b_i$.
- Due to the assumptions on π_1:
  - The sets $\mathcal{X}(g_1)$ and $\mathcal{Y}(g_2)$ are large (density $\geq 2^{-\varepsilon \cdot m}$)

Proving weak intersection

- How can we prove that two functions weakly intersect?
- Need to prove: there exist $X \in \mathcal{X}(g_1)$ and $Y \in \mathcal{Y}(g_2)$ that are equal on the rows where $a_i \neq b_i$.
- Due to the assumptions on π_1:
  - The sets $\mathcal{X}(g_1)$ and $\mathcal{Y}(g_2)$ are large (density $\geq 2^{-\varepsilon \cdot m}$) (since π_1 does not reveal much information on the inputs).

Proving weak intersection

- How can we prove that two functions weakly intersect?
- Need to prove: there exist $X \in \mathcal{X}(g_1)$ and $Y \in \mathcal{Y}(g_2)$ that are equal on the rows where $a_i \neq b_i$.
- Due to the assumptions on π_1:
  - The sets $\mathcal{X}(g_1)$ and $\mathcal{Y}(g_2)$ are large (density $\geq 2^{-\varepsilon \cdot m}$) (since π_1 does not reveal much information on the inputs).
  - It holds that $a_i \neq b_i$ for at most $\alpha \cdot m$ rows

Proving weak intersection

- How can we prove that two functions weakly intersect?
- Need to prove: there exist $X \in \mathcal{X}(g_1)$ and $Y \in \mathcal{Y}(g_2)$ that are equal on the rows where $a_i \neq b_i$.
- Due to the assumptions on π_1:
  - The sets $\mathcal{X}(g_1)$ and $\mathcal{Y}(g_2)$ are large (density $\geq 2^{-\varepsilon \cdot m}$) (since π_1 does not reveal much information on the inputs).
  - It holds that $a_i \neq b_i$ for at most $\alpha \cdot m$ rows (since π_1 is far from solving KW_f).

Proving weak intersection

- How can we prove that two functions weakly intersect?
- Need to prove: there exist $X \in \mathcal{X}(g_1)$ and $Y \in \mathcal{Y}(g_2)$ that are equal on the rows where $a_i \neq b_i$.
- Due to the assumptions on π_1:
  - The sets $\mathcal{X}(g_1)$ and $\mathcal{Y}(g_2)$ are large (density $\geq 2^{-\varepsilon \cdot m}$) (since π_1 does not reveal much information on the inputs).
  - It holds that $a_i \neq b_i$ for at most $\alpha \cdot m$ rows (since π_1 is far from solving KW_f).
- Warm-up: prove that there exist $X \in \mathcal{X}(g_1)$ and $Y \in \mathcal{Y}(g_2)$ that are equal on $\geq \alpha \cdot m$ rows.

A simpler combinatorial question

- Let Σ be a finite alphabet.
- Let $\mathcal{X}, \mathcal{Y} \subseteq \Sigma^m$ be sets of strings of density $\geq 2^{-\varepsilon \cdot m}$ (for some $\varepsilon > 0$).

A simpler combinatorial question

- Let Σ be a finite alphabet.
- Let $\mathcal{X}, \mathcal{Y} \subseteq \Sigma^m$ be sets of strings of density $\geq 2^{-\varepsilon \cdot m}$ (for some $\varepsilon > 0$).

Toy problem

Prove that there exist strings $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ that agree on at least $\alpha \cdot m$ coordinates (for some α that depends only on ε).

A simpler combinatorial question

- Let Σ be a finite alphabet.
- Let $\mathcal{X}, \mathcal{Y} \subseteq \Sigma^m$ be sets of strings of density $\geq 2^{-\varepsilon \cdot m}$ (for some $\varepsilon > 0$).

Toy problem

Prove that there exist strings $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ that agree on at least $\alpha \cdot m$ coordinates (for some α that depends only on ε).

- In other words: there exists $I \subseteq [m]$ of size $\geq \alpha \cdot m$ s.t. $\mathcal{X}|_I \cap \mathcal{Y}|_I \neq \emptyset$.

A simpler combinatorial question

- Let Σ be a finite alphabet.
- Let $\mathcal{X}, \mathcal{Y} \subseteq \Sigma^m$ be sets of strings of density $\geq 2^{-\varepsilon \cdot m}$ (for some $\varepsilon > 0$).

Toy problem

Prove that there exist strings $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ that agree on at least $\alpha \cdot m$ coordinates (for some α that depends only on ε).

- In other words: there exists $I \subseteq [m]$ of size $\geq \alpha \cdot m$ s.t. $\mathcal{X}|_I \cap \mathcal{Y}|_I \neq \emptyset$.
- Idea: choose I such that $\mathcal{X}|_I$ and $\mathcal{Y}|_I$ are "prefix-thick sets".

Prefix-thick sets

Definition

We say that $\mathcal{X} \subseteq \Sigma^m$ is prefix thick iff for every prefix w of $\mathcal{X}$ of length $< m$, there exist more than $\frac{|\Sigma|}{2}$ symbols σ such that $w \circ \sigma$ is a prefix of $\mathcal{X}$.

Prefix-thick sets

Definition

We say that $\mathcal{X} \subseteq \Sigma^m$ is prefix thick iff for every prefix w of $\mathcal{X}$ of length $< m$, there exist more than $\frac{|\Sigma|}{2}$ symbols σ such that $w \circ \sigma$ is a prefix of $\mathcal{X}$.

Observation

If $\mathcal{X}$ and $\mathcal{Y}$ are prefix-thick subsets of Σ^m, then $\mathcal{X} \cap \mathcal{Y} \neq \emptyset$.

Prefix-thick sets

Definition

We say that $\mathcal{X}$ is prefix thick iff for every prefix w of length $< m$, there exist more than $\frac{|\Sigma|}{2}$ symbols σ such that $w \circ \sigma$ is a prefix.

Prefix-thick sets

Definition

We say that $\mathcal{X}$ is prefix thick iff for every prefix w of length $< m$, there exist more than $\frac{|\Sigma|}{2}$ symbols σ such that $w \circ \sigma$ is a prefix.

Lemma (this work)

Let $\mathcal{X} \subseteq \Sigma^m$ be a set of some density δ. Then, $\mathcal{X}|_I$ is prefix thick for at least δ fraction of the sets $I \subseteq [m]$.

Prefix-thick sets

Definition

We say that $\mathcal{X}$ is prefix thick iff for every prefix w of length $< m$, there exist more than $\frac{|\Sigma|}{2}$ symbols σ such that $w \circ \sigma$ is a prefix.

Lemma (this work)

Let $\mathcal{X} \subseteq \Sigma^m$ be a set of some density δ. Then, $\mathcal{X}|_I$ is prefix thick for at least δ fraction of the sets $I \subseteq [m]$.

- Proof: Easy corollary of a result of [ST14] about discrete dynamical systems.

Prefix-thick sets

Definition

We say that $\mathcal{X}$ is prefix thick iff for every prefix w of length $< m$, there exist more than $\frac{|\Sigma|}{2}$ symbols σ such that $w \circ \sigma$ is a prefix.

Lemma (this work)

Let $\mathcal{X} \subseteq \Sigma^m$ be a set of some density δ. Then, $\mathcal{X}|_I$ is prefix thick for at least δ fraction of the sets $I \subseteq [m]$.

- Proof: Easy corollary of a result of [ST14] about discrete dynamical systems.
- Can be viewed as a generalization of the Sauer-Shelah lemma to large alphabets.

Putting everything together

- Using the last lemma, we can find a set I s.t. $\mathcal{X}(g_1)|_I$ and $\mathcal{Y}(g_2)|_I$ are prefix thick.

Putting everything together

- Using the last lemma, we can find a set I s.t. $\mathcal{X}(g_1)|_I$ and $\mathcal{Y}(g_2)|_I$ are prefix thick.
- Together with additional ideas, we can prove that many pairs of functions weakly intersect.

Putting everything together

- Using the last lemma, we can find a set I s.t. $\mathcal{X}(g_1)|_I$ and $\mathcal{Y}(g_2)|_I$ are prefix thick.
- Together with additional ideas, we can prove that many pairs of functions weakly intersect.
- In other words, we can prove the existence of many edges in the characteristic $\mathcal{G}_{\pi_1}$.

Putting everything together

- Using the last lemma, we can find a set I s.t. $\mathcal{X}(g_1)|_I$ and $\mathcal{Y}(g_2)|_I$ are prefix thick.
- Together with additional ideas, we can prove that many pairs of functions weakly intersect.
- In other words, we can prove the existence of many edges in the characteristic $\mathcal{G}_{\pi_1}$.
- This allows us to prove a lower bound on the chromatic number of $\mathcal{G}_{\pi_1}$...

Putting everything together

- Using the last lemma, we can find a set I s.t. $\mathcal{X}(g_1)|_I$ and $\mathcal{Y}(g_2)|_I$ are prefix thick.
- Together with additional ideas, we can prove that many pairs of functions weakly intersect.
- In other words, we can prove the existence of many edges in the characteristic $\mathcal{G}_{\pi_1}$.
- This allows us to prove a lower bound on the chromatic number of $\mathcal{G}_{\pi_1}$...
- and hence get the desired lower bound on communication complexity.

Summary

- The KRW conjecture is a promising approach for proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

Summary

- The KRW conjecture is a promising approach for proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$.
- Even a weak version suffices ($\forall f$ $\exists$ hard g).

Summary

- The KRW conjecture is a promising approach for proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$.
- Even a weak version suffices ($\forall f\ \exists$ hard g).
- Strong composition: focus on the direct-sum obstacle.

Summary

- The KRW conjecture is a promising approach for proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$.
- Even a weak version suffices ($\forall f$ $\exists$ hard g).
- Strong composition: focus on the direct-sum obstacle.
- Our result: a version of the weak conjecture for strong composition.

Summary

- The KRW conjecture is a promising approach for proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$.
- Even a weak version suffices ($\forall f$ $\exists$ hard g).
- Strong composition: focus on the direct-sum obstacle.
- Our result: a version of the weak conjecture for strong composition.
- Open problems:

Summary

- The KRW conjecture is a promising approach for proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$.
- Even a weak version suffices ($\forall f$ $\exists$ hard g).
- Strong composition: focus on the direct-sum obstacle.
- Our result: a version of the weak conjecture for strong composition.
- Open problems:
    - Get rid of the $-0.96 \cdot m$ loss.

Summary

- The KRW conjecture is a promising approach for proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$.
- Even a weak version suffices ($\forall f\ \exists$ hard g).
- Strong composition: focus on the direct-sum obstacle.
- Our result: a version of the weak conjecture for strong composition.
- Open problems:
  - Get rid of the $-0.96 \cdot m$ loss.
  - Lower bound for formula complexity.

Summary

- The KRW conjecture is a promising approach for proving $\mathbf{P} \not\subseteq \mathbf{NC}^1$.
- Even a weak version suffices ($\forall f\ \exists$ hard g).
- Strong composition: focus on the direct-sum obstacle.
- Our result: a version of the weak conjecture for strong composition.
- Open problems:
  - Get rid of the $-0.96 \cdot m$ loss.
  - Lower bound for formula complexity.

Thank you!