Improved Composition Theorems for Functions and Relations

Sajin Koroth

University of Haifa

joint work with

Or Meir

University of Haifa

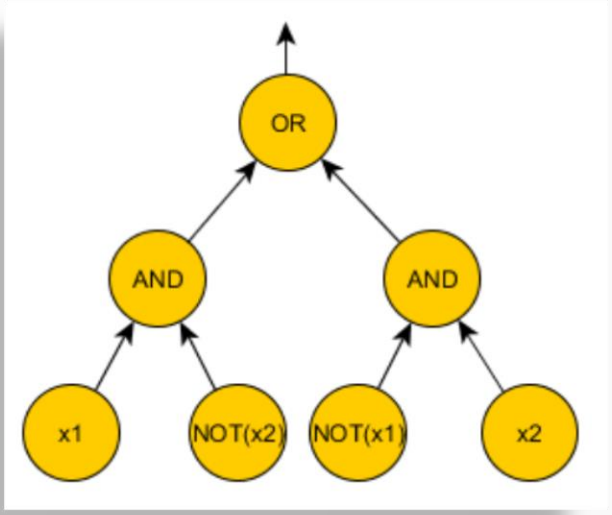
אוניברסיטת חיפה
University of Haifa

Outline

- Background
- Our results
- Proof Overview
- Highlight of the key ideas of our improvement
- 5 minutes break 
- Technical details of the key ideas in our improvement

Background

- **P vs NP**
- Attack via **Boolean Circuits**
- **Size** : The **number of internal gates** in the circuit
- **Depth :** The **length of the longest path from root to a leaf**
- **Size ~ Time in T.M.**
- **Depth ~ Parallel Time, Space in T.M.**
- **Fan in :** number of inputs to a gate, fixed to **2**



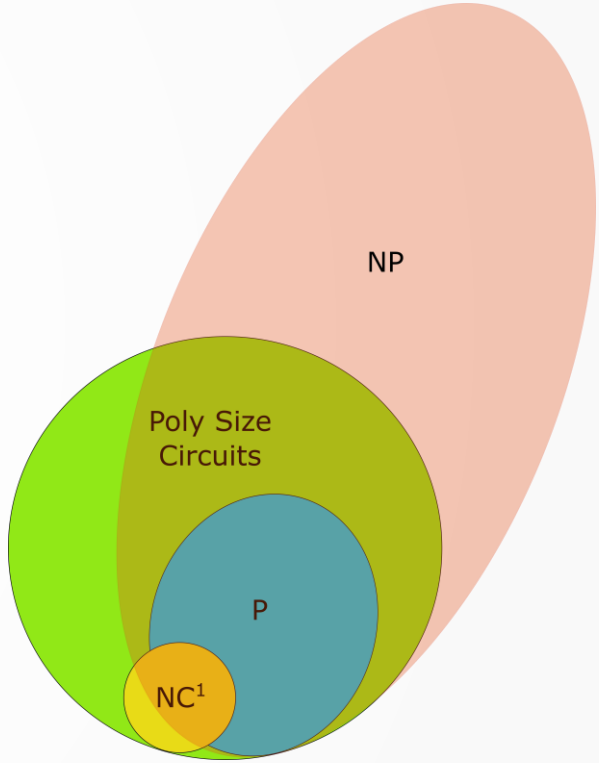
Circuit computing Parity on 2 bits

P vs NP through circuits

- P has **Poly Size** circuits
- NP is **believed not to** have Poly Size circuits
- Unfortunately the best known for NP : $(5 - o(1))n$
- Natural Strategy : super poly lower bounds for **weaker** class of circuits
- Making circuit class weaker : restrict **depth**

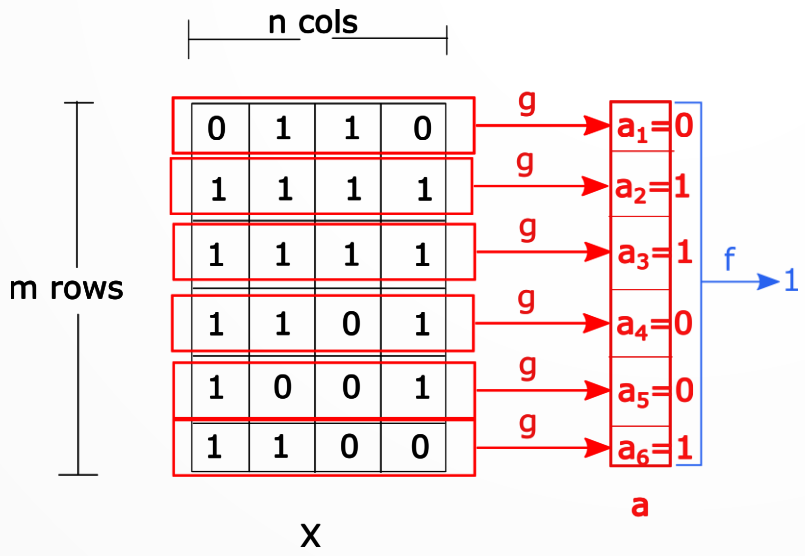
NP vs NC^1 and P vs NC^1

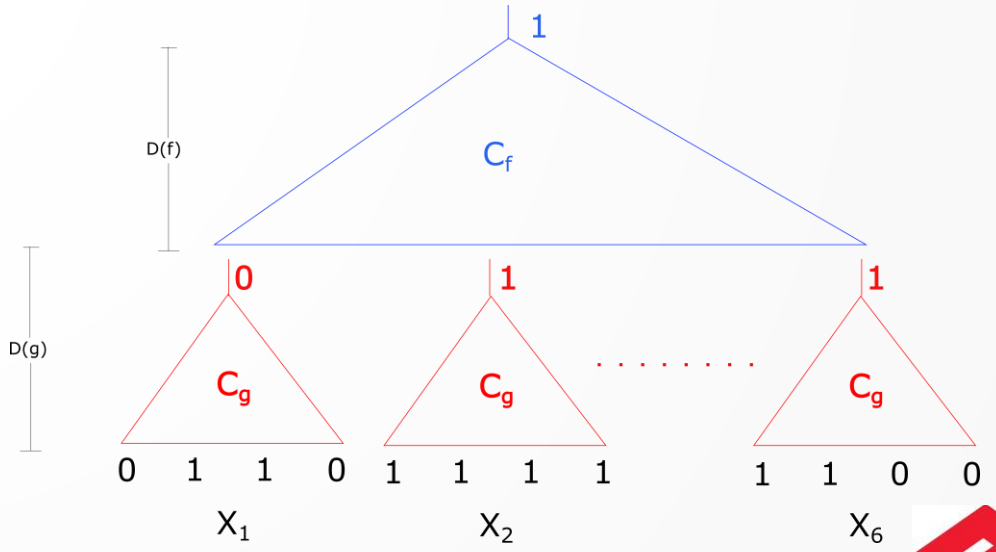
- NC^1 : poly size, $\boldsymbol{O}(\log \boldsymbol{n})$ **depth**, fan-in 2
- NC^1 : efficient parallel algorithms
- Weaker goal : Prove that NP does not have NC^1 circuits
- **Belief** : there are functions in P which does **not** have efficient parallel algorithms
- **Goal : explicit** function f in P with $D(f) = \omega(\log n)$
- $D(f)$ is the **minimum depth** of any circuit computing f



Compositions and P vs NC^1

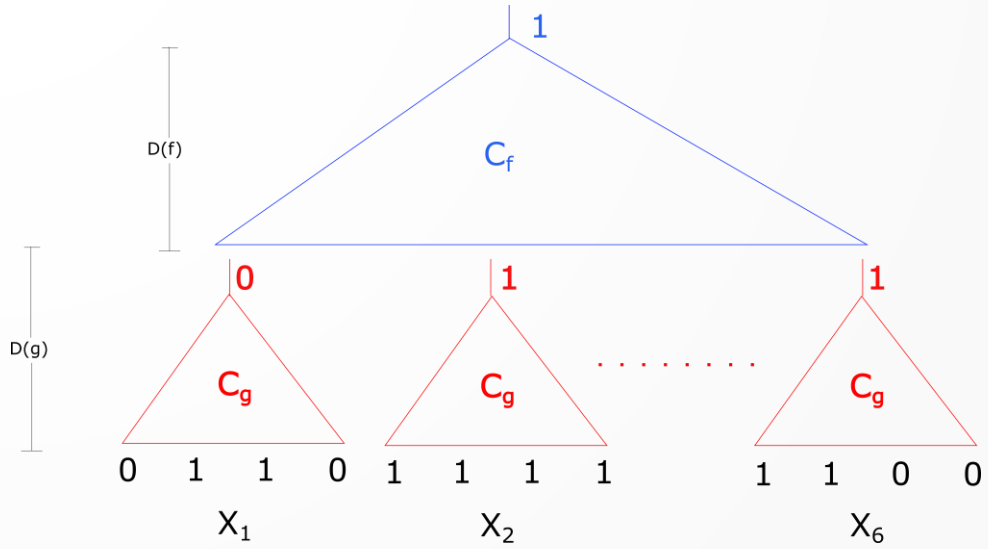
- Karchmer Raz and Wigderson '91 : **study composition** of functions **to study depth**
- Given two arbitrary functions $f:\{0,1\}^m \to \{0,1\}$ and $g:\{0,1\}^n \to \{0,1\}$ define their composition $f \diamond g$ as a function on mn bits





KRW Conjecture

- KRW'91 : Given two arbitrary functions $f: \{0,1\}^m \to \{0,1\}$ and $g: \{0,1\}^n \to \{0,1\}$
- The composition $f \diamond g$ as the function on mn bits as before
- **Fact :** $\boldsymbol{D(f \diamond g) \leq D(f) + D(g)}$
- **KRW Conjecture :** $\boldsymbol{D(f \diamond g) \approx D(f) + D(g)}$
- **If KRW Conjecture is true** then there is a function f in P such that $D(f) = \omega(\log\ n)$
- Implies $\boldsymbol{P \neq NC^1}$



Karchmer Wigderson Relations

- Let $f: \{0,1\}^m \to \{0,1\}$ be an arbitrary Boolean function

$x \in f^{-1}(0)$

$y \in f^{-1}(1)$

- **Goal** : Find an index $i \in [m]$ for which $x_i \neq y_i$
- **Objective** : Minimize the total number of bits spoken

Communication Complexity

- Alice **can't** see Bob's input
- Bob **can't** see Alice's input
- **Can** : agree on a **protocol** and **send messages to each other**
- Cost of a protocol on (x,y) : The total number of bits spoken
- Cost of a protocol : worst case over all possible (x,y)
- For this talk : **players have no randomness**
- **Communication complexity of R, CC(R) :** Minimum cost of a protocol solving R

$x \in f^{-1}(0)$

$y \in f^{-1}(1)$

Circuit complexity to communication

- KW'90 : $CC(KW_f) = D(f)$

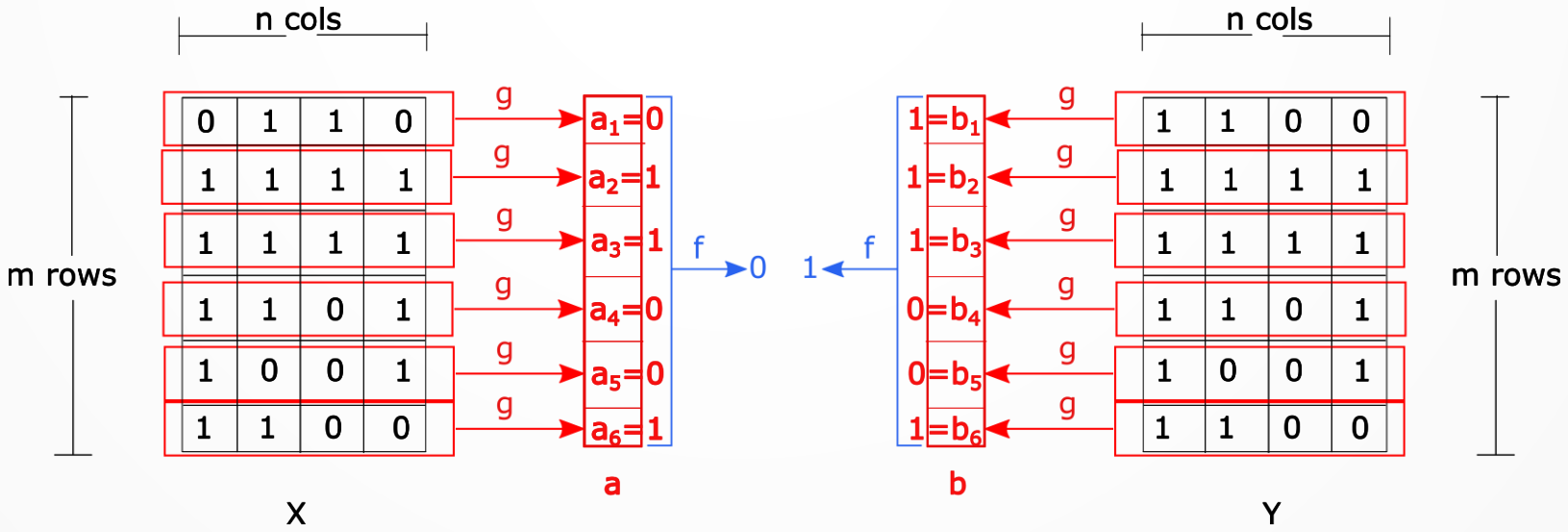
$x \in f^{-1}(0)$

Goal : find $i, x_i \neq y_i$

$y \in f^{-1}(1)$

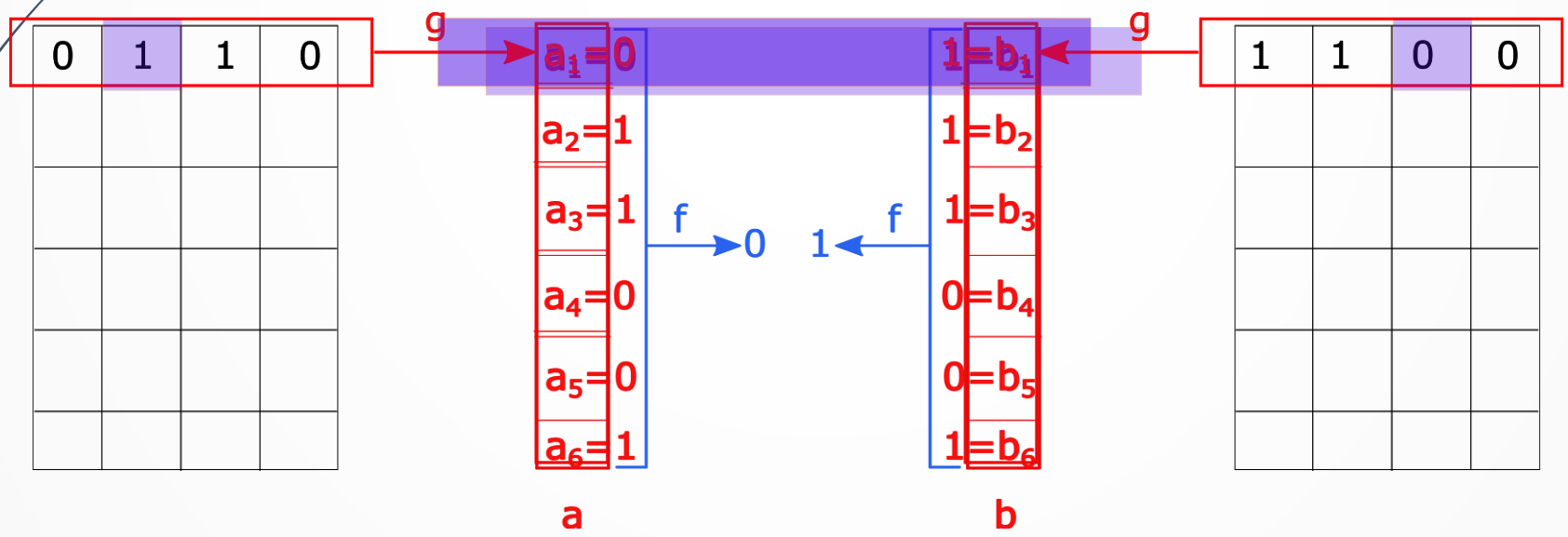
KRW conjecture (communication version)

- Karchmer Wigderson relation of f, $KW_f = \{(i, x, y) \mid x_i \neq y_i, f(x) = 0, f(y) = 1\}$
- KW'90 : $CC(KW_f) = D(f)$
- Restating KRW conjecture : $CC(KW_{f \diamond g}) \approx CC(KW_f) + CC(KW_g)$
- What does the KW relation corresponding to $f \diamond g$ look like



$KW_{f \diamond g}$: an easy upper bound

- Solve KW_f first finding $a_i \neq b_i$
- Solve KW_g on the resulting rows X_i, Y_i
- $CC(KW_{fog}) \leq CC(KW_f) + CC(KW_g)$



Simplifying functions – Universal relation

- KRW conjecture implies $\boldsymbol{P \neq NC^1}$ and this is a **very hard problem**
- **KRW** suggested a simplification : universal relation
- Known : $CC(U_n) = n$

$x \in f^{-1}(0)$

Remove f

Goal : find $i, x_i \neq y_i$

Promise : $x \neq y$

$y \in f^{-1}(1)$

Composition of Universal Relations

- Similar to $f \diamond g$, but drop f, drop g
- KRW Conjecture adapted to Universal relations (suggested by KRW'95) : $\boldsymbol{CC(U_m \diamond U_n) \approx CC(U_m) + CC(U_n)}$

n cols

Promise 1 : $a \neq b$

n cols

m rows

0	1	1	0
1	1	1	1
1	1	1	1
1	1	0	1
1	0	0	1
1	1	0	0

X

0
1
1
0
0
1

a

1
1
1
0
0
1

b

1	1	0	0
1	1	1	1
1	1	1	1
1	1	0	1
1	0	0	1
1	1	0	0

Y

m rows

Promise 2 : $a_i \neq b_i$ implies $X_i \neq Y_i$

Known results

- First progress: result by Edmonds, Impagliazzo, Rudich and Sgall (EIRS)
- EIRS'91: $CC(U_m \diamond U_n) \geq m + n - O(\sqrt{m})$
- The result is for $m = n$, but can be generalized in a straightforward manner
- Håstad and Wigderson '90: Alternate proof. Almost tight for $m = n$, weak for $m \neq n$
- HW'90 : $CC(U_m \diamond U_n) \geq 2n - o(1)$

Composition of functions with universal relation : $f \diamond U_n$

- Gavinsky, Meir, Weinstein and Wigderson (GMWW'14) defined $f \diamond U_n$ for any function $f: \{0,1\}^m \to \{0,1\}$
- GMWW'14 : suggested studying $f \diamond U_n$ as a next step between $U_m \diamond U_n$ and $f \diamond g$
- GMWW'14 : $CC(f \diamond U_n) \geq \log L(f) + n - O(\frac{m}{n} \log m)$
- This talk : $\log L(f) = D(f)$ (this is not true in reality, but we can handle this)

Our Results

- $CC(f \diamond U_n) \geq \log L(f) + n - O(\log m)$
- $CC(U_m \diamond U_n) \geq m + n - O(\log m)$

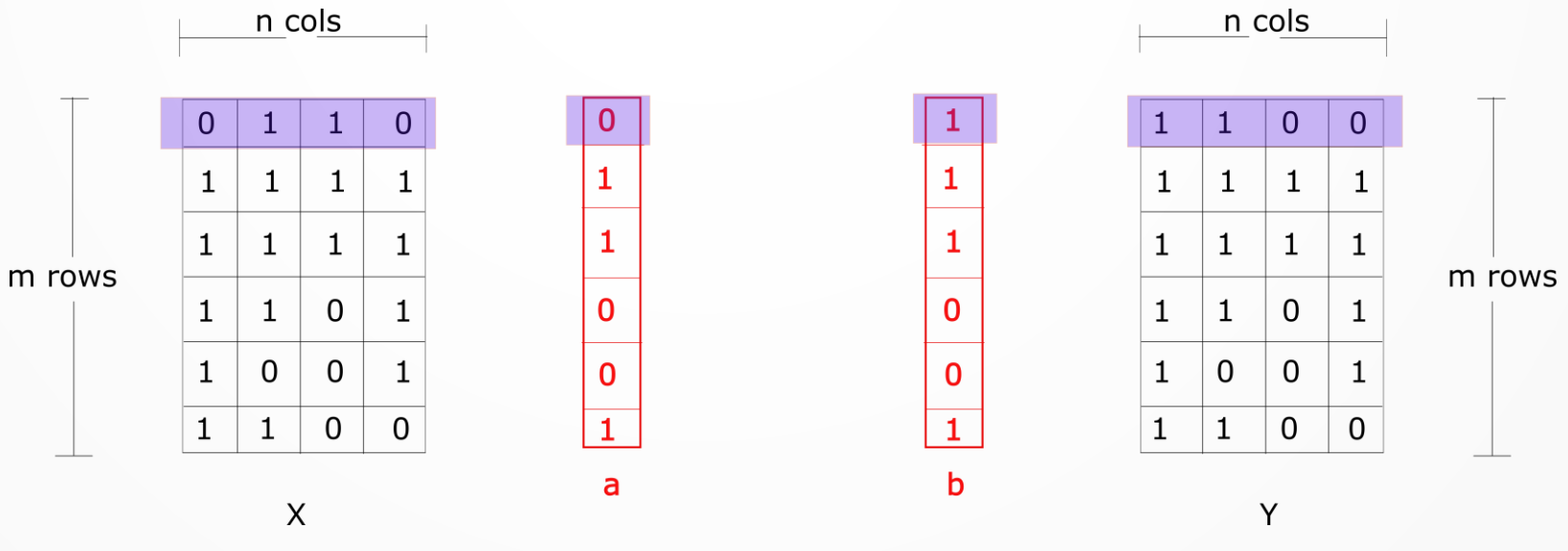
Relation	Known Lower bounds	Trivial Upper Bounds	Our Results
$U_m \diamond U_n$	$m + n - O(\sqrt{m})$ EIRS'91	$m + n$	$m + n - O(\log m)$
$f \diamond g$	$\log L(f) + n - O\left(1 + \frac{m}{n}\right) \log m$ GMWW'14	$\log L(f) + n$	$\log L(f) + n - O(\log m)$

Motivation

- The results are interesting in itself
- To get $P \neq NC^1$ from the KRW conjecture :
  - Prove the conjecture $f \diamond g$ for **arbitrary f**, **random g**
  - Close to $f \diamond U_n$
  - **But :** need $m = \frac{2^n}{\log n}$
  - **The losses in all** earlier bounds **are significant** even when $m = \omega(n^2)$
  - **Avoiding $m = \omega(n^2)$** : Prove the conjecture $f \diamond g$ for **random f**, **arbitrary g**
  - **Problem :** Close to $U_m \diamond g$, and we don't know any lower bounds!

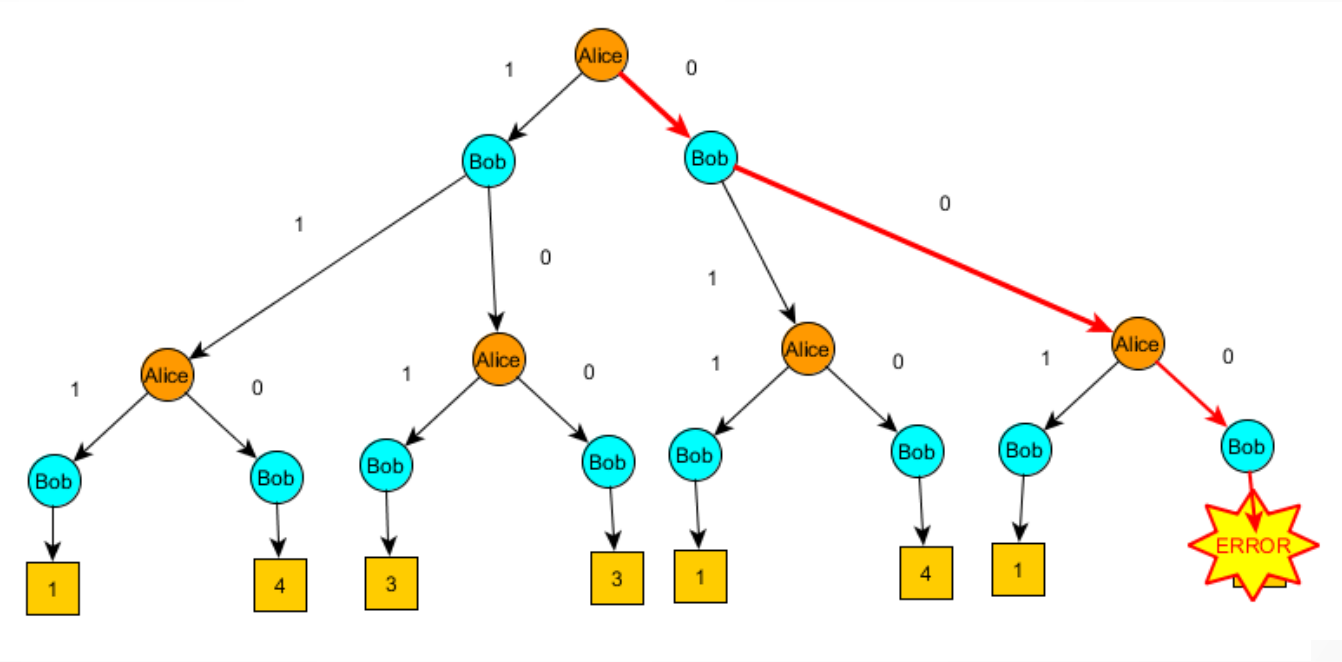
Basic intuition

- We will show the proof for $U_m \diamond U_n$
- Players **have to** solve U_n on at least one row. Say row i.
- They need the promise: $X_i \neq Y_i$
- For this promise : they need to solve U_m, i.e., know for sure $a_i \neq b_i$
- Hence : $CC(U_m \diamond U_n) \approx CC(U_m) + CC(U_n) \approx m + n$
- **Notation** : **matrix part**, **vector part** of players input



Adversarial Argument

Maintains a path
and a set of inputs



Deterministic protocol

High Level Idea

- Divide communication **into two stages**
- **First stage** : where players must solve U_m
- Defined to be **first $m - \alpha$ bits** (α : slack term)
- **Second Stage** : rest of the communication
- **Lower bound :**
  - Adversary constructs a **good first stage transcript**
  - **On this** transcript, players must speak $\approx n$ **bits in the second stage**

An easy case

- Recall : Input to $U_m \diamond U_n$: $((X, a), (Y, b))$. **Matrix part : X, Y, vector part : a, b**
- **Suppose** the players **don't speak about matrix part in the first stage**
- They haven't solved U_m yet
- No matter which **row** they find where $a_i \neq b_i$, **they know nothing about the row**
- Hence **second stage : at least $\approx n$ bits** $(CC(U_n))$

Another easy case

- Recall : Input to $U_m \diamond U_n$: $((X, a), (Y, b))$. **Matrix part : X, Y, vector part : a, b**
- **Suppose** the players **don't speak about vector part in the first stage**
- They haven't solved U_m **at all**
- #rows for which the players have learned at least **1 bit** of information < $m - \alpha$
- **Make these rows useless. Set $a_i = b_i$ for such rows**
- Complexity of U_m after fixing $a_i = b_i$: $m - (m - \alpha)$
- If $\alpha > 1$, at least one index which is not fixed
- Hence **second stage : at least $\approx n - 1$ bits** $(CC(U_n))$

Challenging case

- Recall : Input to $U_m \diamond U_n$: $((X, a), (Y, b))$. **Matrix part : X, Y, vector part : a, b**
- The players **do speak about matrix part in the first stage**
- They haven't solved U_m yet.
- They don't know any row where $X_i \neq Y_i$ is guaranteed
- **Goal :** communication in the first stage about matrix part is wasted on rows $X_i = Y_i$
- **Strategy :**
  - Adversary fixes a good transcript of the first stage
  - **Classify rows** into : **revealed** and **unrevealed**
  - **Revealed : players spoke more than τ bits about the row**.
  - **Unrevealed row** : players **have to speak $\approx n - \tau$ bits** in the second stage
  - For **every revealed row** : **fix $a_i = b_i$**

Fixing Revealed Rows

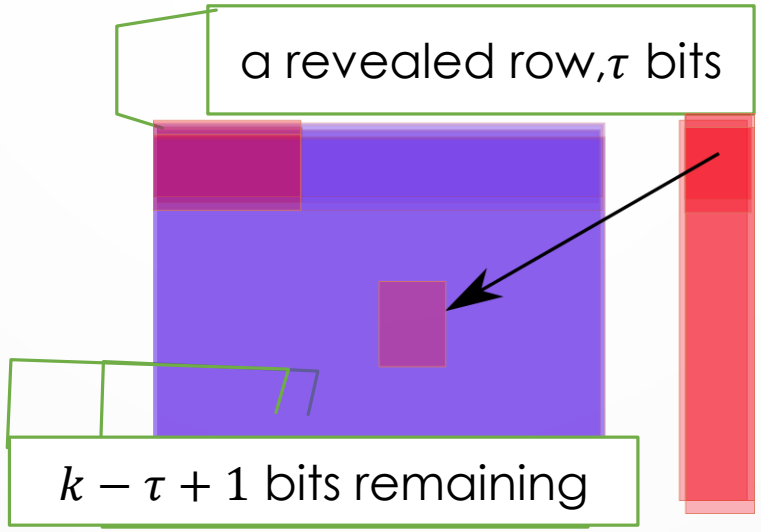
- For the strategy to work : need to fix $a_i = b_i$ for every revealed row
- Suppose : players spoke k bits about the matrix part
- Number of revealed rows : k/τ (by an averaging argument)
- **Constraint due to fixing :** #(revealed rows) < β (β : bits remaining to solve U_m)
- Lower bound : $\approx m - \alpha + n - \tau$ subject to $\frac{k}{\tau} < \beta$
- EIRS :
  - $k \leq m - \alpha$
  - $\tau = \sqrt{m}, \alpha = \sqrt{m}$
  - $\frac{k}{\tau} < \sqrt{m}, \ \beta > \alpha$
  - Lower bound : $\approx m - \sqrt{m} + n - \sqrt{m}$

Our analysis

- Suppose : players spoke k bits about the matrix part
- Constraint due to fixing : #(revealed rows) < β (β : bits remaining to solve U_m)
- **Main Idea : first stage ≥ communication (matrix part) + communication (vector part)**
- Hence $\beta \geq \alpha + k$ (#bits(vector part) <= $m - \alpha - k$)
- Lower bound : $\approx m - \alpha + n - \tau$ subject to $\frac{k}{\tau} < \beta$
  - Set $\tau > 1$
  - $\frac{k}{\tau} < k + \alpha.$
  - Hence $\frac{k}{\tau} < \beta$ is satisfied

A complication

- **first stage : communication (matrix part), k bits + communication (vector part), $m - \alpha - k$ bits**
- Fixing a bit $a_i = b_i$, could reveal a bit of information about the matrices
- Unrevealed row at the end of fixing : $\tau + k/\tau$ **bits**
- **Solution :** An **Iterative** Adversary



Iterative Adversary

- After fixing i revealed rows, #bits known about the remaining rows : $\boldsymbol{k} - (\boldsymbol{\tau}$

Thank you

- **Questions ?**
- Technical details of the key ideas after the break!