The KRW conjecture Results and Open problems

Or Meir





### Proof strategy



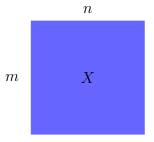
- Let  $f: \{0,1\}^n \to \{0,1\}$ .
- The depth complexity D(f) is the depth of the shallowest circuit for f.
- Captures the complexity of parallel computation.

- Let  $f: \{0,1\}^n \to \{0,1\}$ .
- The depth complexity D(f) is the depth of the shallowest circuit for f.
- Captures the complexity of parallel computation.
- We only consider circuits with fan-in 2.

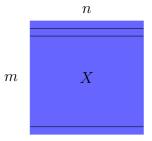
- Let  $f: \{0,1\}^n \to \{0,1\}$ .
- The depth complexity D(f) is the depth of the shallowest circuit for f.
- Captures the complexity of parallel computation.
- We only consider circuits with fan-in 2.
- Major frontier: Explicit f with  $D(f) = \omega(\log n)$ .
- a.k.a.  $\mathbf{P} \neq \mathbf{NC}^1$ .

• [Karchmer-Raz-Wigderson-91]: We need to understand composition.

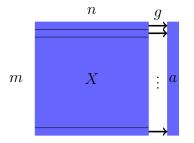
- [Karchmer-Raz-Wigderson-91]: We need to understand composition.
- Let  $f: \{0,1\}^m \to \{0,1\}, g: \{0,1\}^n \to \{0,1\}.$
- The composition  $f \diamond g : \{0,1\}^{m \times n} \to \{0,1\}$  is



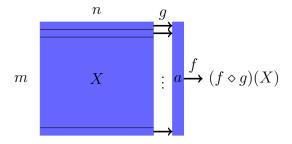
- [Karchmer-Raz-Wigderson-91]: We need to understand composition.
- Let  $f: \{0,1\}^m \to \{0,1\}, g: \{0,1\}^n \to \{0,1\}.$
- The composition  $f \diamond g : \{0,1\}^{m \times n} \to \{0,1\}$  is



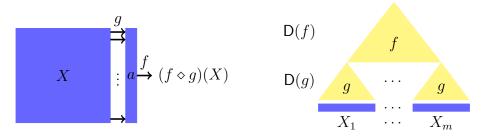
- [Karchmer-Raz-Wigderson-91]: We need to understand composition.
- Let  $f: \{0,1\}^m \to \{0,1\}, g: \{0,1\}^n \to \{0,1\}.$
- The composition  $f\diamond g: \{0,1\}^{m\times n} \to \{0,1\}$  is



- [Karchmer-Raz-Wigderson-91]: 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

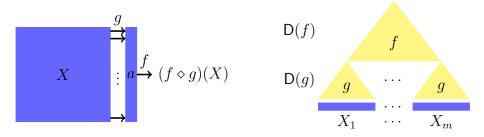


# The KRW conjecture



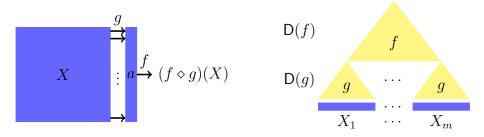
### • Clearly, $D(f \diamond g) \leq D(f) + D(g)$ .

# The KRW conjecture



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

# The KRW conjecture



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

• Theorem [KRW91]: the conjecture implies that  $P \neq NC^1$ .

# Outline

### 1 Introduction



Proof strategy



• Relate D(f) to complexity of a communication problem  $KW_f$ .

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

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

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

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

- Can we use KW games to attack the KRW conjecture?
- What does  $KW_{f\diamond g}$  look like?
- Recall:  $f \diamond g$  maps  $\{0,1\}^{m \times n}$  to  $\{0,1\}$ .

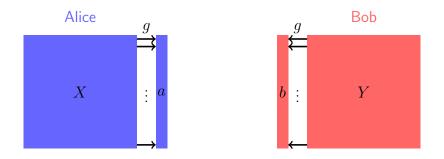
#### Alice



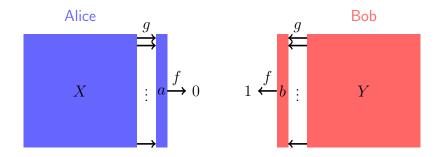
#### Bob



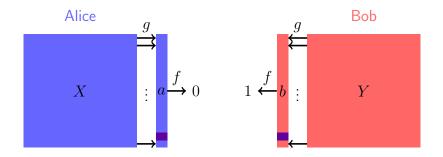
- Can we use KW games to attack the KRW conjecture?
- What does  $KW_{f \diamond g}$  look like?
- Recall:  $f \diamond g$  maps  $\{0, 1\}^{m \times n}$  to  $\{0, 1\}$ .



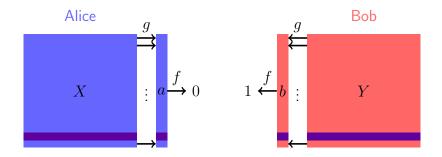
- Can we use KW games to attack the KRW conjecture?
- What does  $KW_{f \diamond g}$  look like?
- Recall:  $f \diamond g$  maps  $\{0, 1\}^{m \times n}$  to  $\{0, 1\}$ .



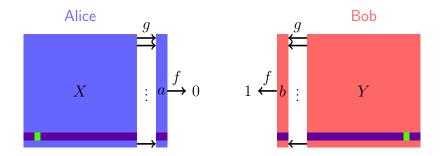
- Can we use KW games to attack the KRW conjecture?
- What does  $KW_{f \diamond g}$  look like?
- Recall:  $f \diamond g$  maps  $\{0, 1\}^{m \times n}$  to  $\{0, 1\}$ .



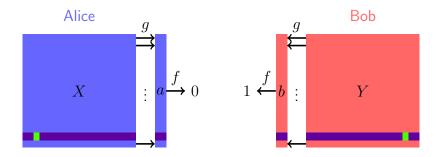
- Can we use KW games to attack the KRW conjecture?
- What does  $KW_{f \diamond g}$  look like?
- Recall:  $f \diamond g$  maps  $\{0, 1\}^{m \times n}$  to  $\{0, 1\}$ .



- Can we use KW games to attack the KRW conjecture?
- What does  $KW_{f \diamond g}$  look like?
- Recall:  $f \diamond g$  maps  $\{0, 1\}^{m \times n}$  to  $\{0, 1\}$ .



- Can we use KW games to attack the KRW conjecture?
- What does  $KW_{f \diamond g}$  look like?
- Recall:  $f \diamond g$  maps  $\{0, 1\}^{m \times n}$  to  $\{0, 1\}$ .



- Hence,  $C(KW_{f \diamond g}) \leq C(KW_f) + C(KW_g)$ .
- KRW conjecture: the obvious protocol is essentially optimal.

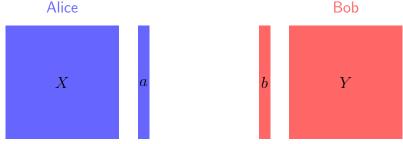
- The KRW conjecture is hard.
- [KRW91] suggested a starting point.

- The KRW conjecture is hard.
- [KRW91] suggested a starting point.
- The universal relation  $U_n$  is:
  - Alice gets  $x \in \{0,1\}^n$ .
  - Bob gets  $y \in \{0, 1\}^n$ .
  - $x \neq y$ .
  - Wish to find i s.t.  $x_i \neq y_i$ .

- The KRW conjecture is hard.
- [KRW91] suggested a starting point.
- The universal relation  $U_n$  is:
  - Alice gets  $x \in \{0,1\}^n$ .
  - Bob gets  $y \in \{0, 1\}^n$ .
  - $x \neq y$ .
  - Wish to find i s.t.  $x_i \neq y_i$ .
- Easy to prove:  $C(U_n) \ge n$ .

- The KRW conjecture is hard.
- [KRW91] suggested a starting point.
- The universal relation  $U_n$  is:
  - Alice gets  $x \in \{0,1\}^n$ .
  - Bob gets  $y \in \{0,1\}^n$ .
  - $x \neq y$ .
  - Wish to find i s.t.  $x_i \neq y_i$ .
- Easy to prove:  $C(U_n) \ge n$ .
- [KRW91] suggested to study  $U_m \diamond U_n$ .

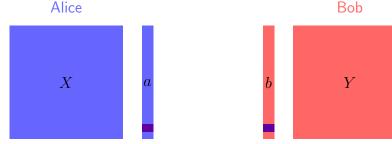
• [KRW91] suggested to study the composition  $U_m \diamond U_n$ .



Bob

- $a \neq b$ .
- If  $a_i \neq b_i$  then  $X_i \neq Y_i$ .

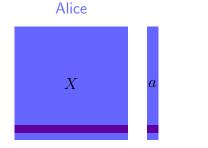
• [KRW91] suggested to study the composition  $U_m \diamond U_n$ .



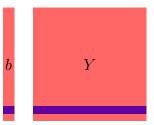
Bob

- $a \neq b$ .
- If  $a_i \neq b_i$  then  $X_i \neq Y_i$ .

• [KRW91] suggested to study the composition  $U_m \diamond U_n$ .

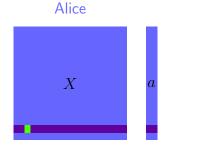


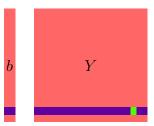




- $a \neq b$ .
- If  $a_i \neq b_i$  then  $X_i \neq Y_i$ .

• [KRW91] suggested to study the composition  $U_m \diamond U_n$ .



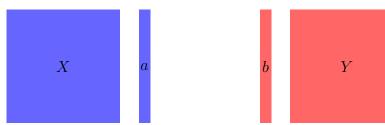


### Bob

- $a \neq b$ .
- If  $a_i \neq b_i$  then  $X_i \neq Y_i$ .

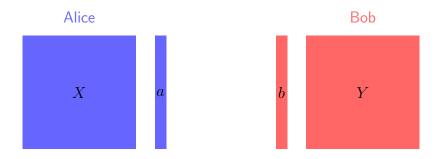
• Goal:  $C(U_m \diamond U_n) = C(U_m) + C(U_n) \ge m + n.$ 

### Alice



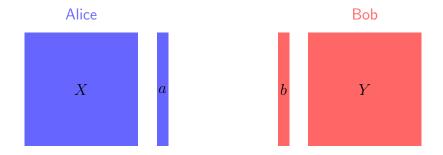
Bob

- Goal:  $C(U_m \diamond U_n) = C(U_m) + C(U_n) \ge m + n.$
- Challenge was met by [Edmonds-Impagliazzo-Rudich-S'gall-91].



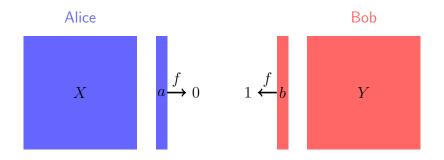
#### The composition of the universal relation

- Goal:  $C(U_m \diamond U_n) = C(U_m) + C(U_n) \ge m + n.$
- Challenge was met by [Edmonds-Impagliazzo-Rudich-S'gall-91].
- Alternative proof obtained by [Håstad-Wigderson-93].



# Composing a function and the universal relation

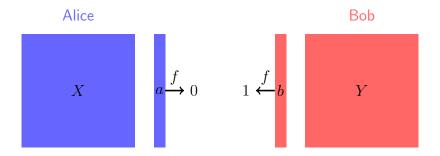
 An analog of KRW conjecture for KW<sub>f</sub> ◊ U<sub>n</sub> for any f. [Gavinsky-M-Weinstein-Wigderson-14]



- If  $a_i \neq b_i$  then  $X_j \neq Y_j$ .
- The obvious protocol works.

# Composing a function and the universal relation

- An analog of KRW conjecture for KW<sub>f</sub> ◊ U<sub>n</sub> for any f. [Gavinsky-M-Weinstein-Wigderson-14]
- Quantative improvement by [Koroth-M-18].



- If  $a_i \neq b_i$  then  $X_j \neq Y_j$ .
- The obvious protocol works.

#### Composing any function and parity

• [Dinur-M-16]: (Re-)proved KRW conjecture for  $f \diamond \bigoplus_n$ 

#### Composing any function and parity

- [Dinur-M-16]: (Re-)proved KRW conjecture for  $f \diamond \bigoplus_n$
- Actually, this case was already implicit in [Håstad 98].

#### Composing any function and parity

- [Dinur-M-16]: (Re-)proved KRW conjecture for  $f \diamond \bigoplus_n$
- Actually, this case was already implicit in [Håstad 98].
- However, our proof was very different, and more in line with the other works on the KRW conjecture.

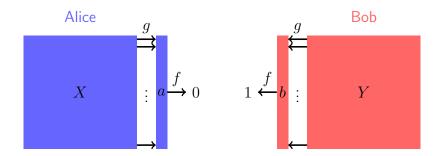
### Outline

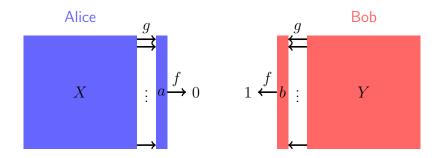
#### Introduction



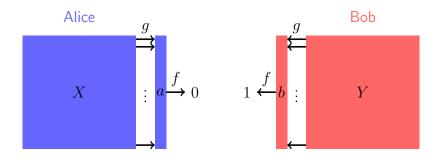




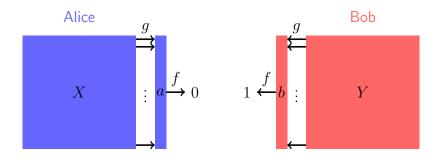




• The players must solve  $KW_q$  on some row.



- The players must solve  $KW_q$  on some row.
- To do this, they must find a row i such that g(X<sub>i</sub>) ≠ g(Y<sub>i</sub>) (i.e. a<sub>i</sub> ≠ b<sub>i</sub>).



- The players must solve  $KW_q$  on some row.
- To do this, they must find a row i such that g(X<sub>i</sub>) ≠ g(Y<sub>i</sub>) (i.e. a<sub>i</sub> ≠ b<sub>i</sub>).
- To find such a row, they must solve  $KW_f$ .

• Implement the foregoing intuition using an adversary argument.

- Implement the foregoing intuition using an adversary argument.
- Measure the progress that Alice and Bob make toward solving  $KW_q$  on each row.

- Implement the foregoing intuition using an adversary argument.
- Measure the progress that Alice and Bob make toward solving  $KW_q$  on each row.
- Whenever they make too much progress on a row:
  - the adversary "kills" the row by forcing  $a_i = b_i$ ,
  - thereby preventing the players from solving  $KW_g$  on that row.

- Implement the foregoing intuition using an adversary argument.
- Measure the progress that Alice and Bob make toward solving  $KW_q$  on each row.
- Whenever they make too much progress on a row:
  - the adversary "kills" the row by forcing  $a_i = b_i$ ,
  - thereby preventing the players from solving  $KW_g$  on that row.
- Adversary can do this until players solve  $KW_f$ .

- Implement the foregoing intuition using an adversary argument.
- Measure the progress that Alice and Bob make toward solving  $KW_g$  on each row.
- Whenever they make too much progress on a row:
  - the adversary "kills" the row by forcing  $a_i = b_i$ ,
  - thereby preventing the players from solving  $KW_g$  on that row.
- Adversary can do this until players solve  $KW_f$ .
- Therefore, the players must first solve  $KW_f$  and then solve  $KW_g$ .

• How do we measure the progress the players make on each row?

- How do we measure the progress the players make on each row?
- Possible solution:

- How do we measure the progress the players make on each row?
- Possible solution:
  - Suppose the lower bound for  $KW_g$  itself is proved using an adversary argument.

- How do we measure the progress the players make on each row?
- Possible solution:
  - Suppose the lower bound for  $KW_g$  itself is proved using an adversary argument.
  - Suppose there is a nice measure for the progress of this adversary argument.
    - (say, the amount of information transmitted by the players)

- How do we measure the progress the players make on each row?
- Possible solution:
  - Suppose the lower bound for  $KW_g$  itself is proved using an adversary argument.
  - Suppose there is a nice measure for the progress of this adversary argument.
    - (say, the amount of information transmitted by the players)
  - Then we can use this measure in the composition adversary argument.

- How do we measure the progress the players make on each row?
- Possible solution:
  - Suppose the lower bound for  $KW_g$  itself is proved using an adversary argument.
  - Suppose there is a nice measure for the progress of this adversary argument.
    - (say, the amount of information transmitted by the players)
  - Then we can use this measure in the composition adversary argument.
- This is how the proofs for universal relation and parity work.

- How do we measure the progress the players make on each row?
- Possible solution:
  - Suppose the lower bound for  $KW_g$  itself is proved using an adversary argument.
  - Suppose there is a nice measure for the progress of this adversary argument.
    - (say, the amount of information transmitted by the players)
  - Then we can use this measure in the composition adversary argument.
- This is how the proofs for universal relation and parity work.
- Call the adversary of  $KW_g$  an "information-theoretic adversary".

### Outline

#### Introduction

- 2 Known results
- 3 Proof strategy



• KRW conjecture: need  $f \diamond g$  for arbitrary f, g.

- KRW conjecture: need  $f \diamond g$  for arbitrary f, g.
- Can deal with arbitrary f.
- Arbitrary g seems much harder.

- KRW conjecture: need  $f \diamond g$  for arbitrary f, g.
- Can deal with arbitrary f.
- Arbitrary g seems much harder.
- Arbitrary g may not have an information-theoretic adversary.

- KRW conjecture: need  $f \diamond g$  for arbitrary f, g.
- Can deal with arbitrary f.
- Arbitrary g seems much harder.
- Arbitrary g may not have an information-theoretic adversary.
- Maybe we do not need to deal with an arbitrary g to prove lower bounds?

- KRW conjecture: need  $f \diamond g$  for arbitrary f, g.
- Can deal with arbitrary f.
- Arbitrary g seems much harder.
- Arbitrary g may not have an information-theoretic adversary.
- Maybe we do not need to deal with an arbitrary g to prove lower bounds?
- Maybe we can find a "complete" relation R, such that it suffices to prove the KRW conjecture for  $KW_f \diamond R$ ?

- KRW conjecture: need  $f \diamond g$  for arbitrary f, g.
- Can deal with arbitrary f.
- Arbitrary g seems much harder.
- Arbitrary g may not have an information-theoretic adversary.
- Maybe we do not need to deal with an arbitrary g to prove lower bounds?
- Maybe we can find a "complete" relation *R*, such that it suffices to prove the KRW conjecture for *KW<sub>f</sub>* ◊ *R*?
- We have a candidate: the multiplexor relation.

# The multiplexor relation [EIRS91]

• The function g becomes part of the input.

# The multiplexor relation [EIRS91]

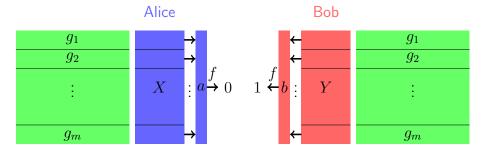
- The function g becomes part of the input.
- Alice gets a function  $g: \{0,1\}^n \to \{0,1\}$  and  $x \in g^{-1}(0)$ .
- Bob gets the same function g and  $y \in g^{-1}(1)$ .
- Want to find  $i \in [n]$  such that  $x_i \neq y_i$ .

- The function g becomes part of the input.
- Alice gets a function  $g: \{0,1\}^n \to \{0,1\}$  and  $x \in g^{-1}(0)$ .
- Bob gets the same function g and  $y \in g^{-1}(1)$ .
- Want to find  $i \in [n]$  such that  $x_i \neq y_i$ .
- Like KW relation of the address function, but with promise.

- The function g becomes part of the input.
- Alice gets a function  $g: \{0,1\}^n \to \{0,1\}$  and  $x \in g^{-1}(0)$ .
- Bob gets the same function g and  $y \in g^{-1}(1)$ .
- Want to find  $i \in [n]$  such that  $x_i \neq y_i$ .
- Like KW relation of the address function, but with promise.
- Easy to prove:  $C(MUX_n) = \Omega(n)$ .

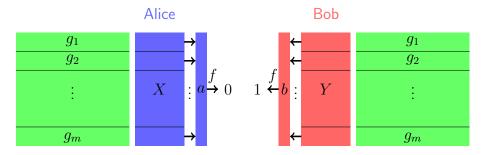
#### Multiplexor composition

• Given f, define the composition  $KW_f \diamond MUX_n$ :



#### Multiplexor composition

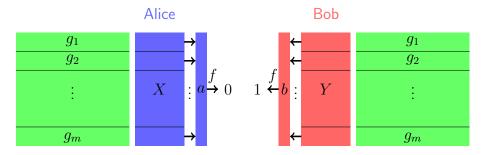
• Given f, define the composition  $KW_f \diamond MUX_n$ :



• Conjecture 1:  $C(KW_f \diamond MUX_n) \gtrsim C(KW_f) + \Omega(n)$ .

### Multiplexor composition

• Given f, define the composition  $KW_f \diamond MUX_n$ :



• Conjecture 1:  $C(KW_f \diamond MUX_n) \gtrsim C(KW_f) + \Omega(n)$ .

• Conjecture 2: Conjecture 1 implies that  $\mathbf{P} \neq \mathbf{NC}^1$ .

• [EIRS91]: The *MUX* relation has an information-theortetic adversary.

# Possible Approach to $\ \mathbf{P} eq \mathbf{N} \mathbf{C}^1$

- [EIRS91]: The *MUX* relation has an information-theortetic adversary.
- Plan:

- [EIRS91]: The *MUX* relation has an information-theortetic adversary.
- Plan:
  - Use that adversary in our strategy.

- [EIRS91]: The *MUX* relation has an information-theortetic adversary.
- Plan:
  - Use that adversary in our strategy.
  - Prove KRW conjecture for  $KW_f \diamond MUX$ .

- [EIRS91]: The *MUX* relation has an information-theortetic adversary.
- Plan:
  - Use that adversary in our strategy.
  - Prove KRW conjecture for  $KW_f \diamond MUX$ .
  - Separate **P** from **NC**<sup>1</sup>.

- [EIRS91]: The *MUX* relation has an information-theortetic adversary.
- Plan:
  - Use that adversary in our strategy.
  - Prove KRW conjecture for  $KW_f \diamond MUX$ .
  - Separate **P** from **NC**<sup>1</sup>.
- Unfortunately, the adversary of *MUX* is very complicated.
- Very hard to incorporate in our proof strategy.

# Possible Approach to $~~{f P} eq{f NC}^1$

• We need to extend our techniques to handle more sophisticated adversaries.

- We need to extend our techniques to handle more sophisticated adversaries.
- Suggestion: Implement our strategy with adversaries that are:

- We need to extend our techniques to handle more sophisticated adversaries.
- Suggestion: Implement our strategy with adversaries that are:
  - simpler than the one of MUX,

- We need to extend our techniques to handle more sophisticated adversaries.
- Suggestion: Implement our strategy with adversaries that are:
  - simpler than the one of MUX,
  - and more interesting than those of  $U_n$  and  $\bigoplus_n$ .

- We need to extend our techniques to handle more sophisticated adversaries.
- Suggestion: Implement our strategy with adversaries that are:
  - simpler than the one of MUX,
  - and more interesting than those of  $U_n$  and  $\bigoplus_n$ .
- There are several nice communication problems with such adversaries.
- Let's try to prove composition results for them.

- Here are some candidates:
  - $\bullet~$  The Grigni-Sipser  ${\rm FORK}$  relation.

- The Grigni-Sipser FORK relation.
- The monotone *st*CONN relation.

- The Grigni-Sipser FORK relation.
- The monotone *st*CONN relation.
- $\bullet\,$  The monotone  $\mathrm{CLIQUE}$  relation.

- The Grigni-Sipser FORK relation.
- The monotone *st*CONN relation.
- The monotone CLIQUE relation.
- All these problems have a simple information-theoretic adversary.

- The Grigni-Sipser FORK relation.
- The monotone *st*CONN relation.
- The monotone CLIQUE relation.
- All these problems have a simple information-theoretic adversary.
- Can we prove the KRW conjecture for *KW<sub>f</sub>* ◊ FORK, *KW<sub>f</sub>* ◊ *st*CONN or *KW<sub>f</sub>* ◊ CLIQUE?

- The Grigni-Sipser FORK relation.
- The monotone *st*CONN relation.
- The monotone CLIQUE relation.
- All these problems have a simple information-theoretic adversary.
- Can we prove the KRW conjecture for *KW<sub>f</sub>* ◊ FORK, *KW<sub>f</sub>* ◊ *st*CONN or *KW<sub>f</sub>* ◊ CLIQUE?
- How about  $U \diamond FORK$ ,  $U \diamond stCONN$  or  $U \diamond CLIQUE$ ?

- The Grigni-Sipser FORK relation.
- The monotone *st*CONN relation.
- The monotone CLIQUE relation.
- All these problems have a simple information-theoretic adversary.
- Can we prove the KRW conjecture for *KW<sub>f</sub>* ◊ FORK, *KW<sub>f</sub>* ◊ *st*CONN or *KW<sub>f</sub>* ◊ CLIQUE?
- How about  $U \diamond FORK$ ,  $U \diamond stCONN$  or  $U \diamond CLIQUE$ ?
- Those are clean and (hopefuly) tractable open questions.



 The KRW conjecture is a promising approach for proving P ≠ NC<sup>1</sup>.

### Summary

- The KRW conjecture is a promising approach for proving P ≠ NC<sup>1</sup>.
- We know how to prove it when the inner function is
  - the universal relation,
  - the parity function.

- The KRW conjecture is a promising approach for proving  $\mathbf{P} \neq \mathbf{NC}^1$ .
- We know how to prove it when the inner function is
  - the universal relation,
  - the parity function.
- Possible approach to  $\mathbf{P} \neq \mathbf{NC}^1$ :
  - Prove the KRW conjecture when the inner function is the multiplexor relation.

- The KRW conjecture is a promising approach for proving  $\mathbf{P} \neq \mathbf{NC}^1$ .
- We know how to prove it when the inner function is
  - the universal relation,
  - the parity function.
- Possible approach to  $\mathbf{P} \neq \mathbf{NC}^1$ :
  - Prove the KRW conjecture when the inner function is the multiplexor relation.
- Open problems: Prove the KRW conjecture when the inner function is
  - $\bullet$  the  $\ensuremath{\mathbf{FORK}}$  relation.
  - the monotone  $st\mathrm{CONN}$  relation,
  - $\bullet\,$  or the monotone  $\mathrm{CLIQUE}$  relation.

# Thank you!