Zero-Information Protocols and Unambiguity in Arthur–Merlin Communication

Mika Göös   Toniann Pitassi   Thomas Watson

University of Toronto

Communication complexity?

[Yao, STOC'79]

Alice **Bob**

Communication complexity?

[Yao, STOC'79]

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

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

Compute: $f\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

Models of communication

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

Models of communication

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

P

Models of communication

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

BPP

Models of communication

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

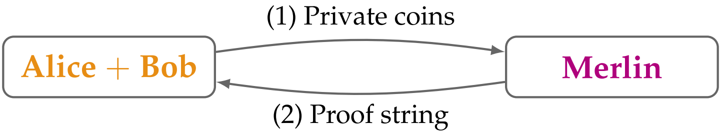
NP

Models of communication

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

AM

AM communication



Completeness (1-inputs):

W.h.p. $\exists$ proof that both parties accept

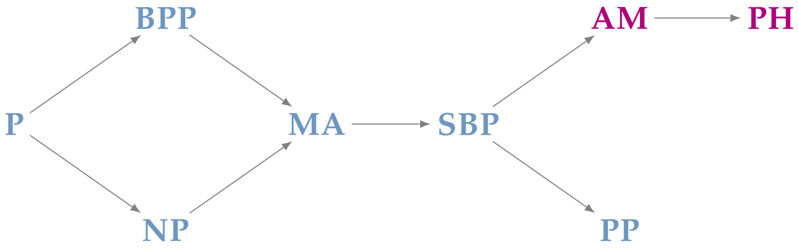
Soundness (0-inputs):

W.h.p. $\neg\exists$ proof that both parties accept

Communication complexity:

Length of proof string
$=$ log of the number of proof rectangles

AM in context



Long-standing open problems:

- Explicit lower bounds for **AM**
- Rigidity lower bounds (related to **PH**)

This work:

Information complexity $+$ **AM communication**

Information complexity

Transcript of protocol leaks information about input

[CSWY01, BYJKS04, JKS03, CKS03, Gro09, Jay09, DKS12, BM13, BGPW13, BEO+13, . . .]

This work:

Information complexity $+$ **AM communication**

Information complexity

Transcript of protocol leaks information about input

UAM: ***Unambiguous* AM**

At most one accepting proof on any 1-input

$\Longrightarrow$ "transcript" := Merlin's unique proof
(only defined for 1-inputs)

This work:

Information complexity $+$ **AM communication**

Information complexity

Transcript of protocol leaks information about input

UAM: *Unambiguous* **AM**

At most one accepting proof on any 1-input

$\implies$ "transcript" $:=$ Merlin's unique proof
(only defined for 1-inputs)

ZAM: *Zero-information* protocols

Transcript independent of input—info approach fails!

Example

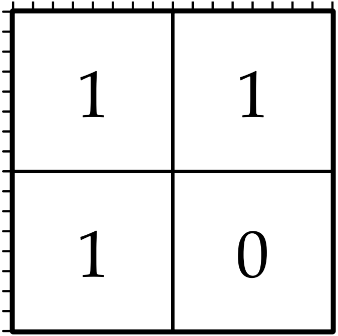
Zero-information (ZAM) protocol for NAND

1	1
1	0

Communication matrix for
NAND: $\{0,1\}^2 \to \{0,1\}$

Example

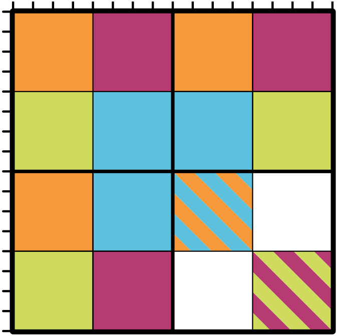
Zero-information (ZAM) protocol for NAND



Augment inputs with private randomness

Example

Zero-information (ZAM) protocol for NAND



Merlin's proof is uniform in {■, ■, ■, ■}
Independent of the 1-input!

Implication:

ZAM protocol for every function!

Proof

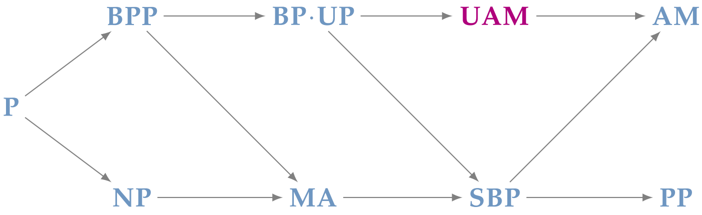
1. $\mathbf{ZAM}(\mathrm{NAND}) \leq O(1)$
2. $\mathrm{Disj}_n := \mathrm{AND}_n \circ \mathrm{NAND}^n$
   $\implies \quad \mathbf{ZAM}(\mathrm{Disj}_n) \leq O(n)$
3. $\forall f: \quad f \leq \mathrm{Disj}_{2^n}$
   $\implies \quad \mathbf{ZAM}(f) \leq O(2^n)$

Results

$$\begin{tikzcd}
 & \mathbf{BPP} \arrow[r] \arrow[ddr] & \mathbf{BP\cdot UP} \arrow[r] \arrow[ddr] & \mathbf{UAM} \arrow[r] & \mathbf{AM} \\
\mathbf{P} \arrow[ur] \arrow[dr] & & & & \\
 & \mathbf{NP} \arrow[r] & \mathbf{MA} \arrow[r] & \mathbf{SBP} \arrow[r] \arrow[uur] & \mathbf{PP}
\end{tikzcd}$$

Theorem 1: $\forall f: \quad \mathbf{ZAM}(f) \leq 2^n$

Results



Theorem 1: $\forall f: \quad \mathbf{ZAM}(f) \leq \text{BranchingProgramSize}(f)$

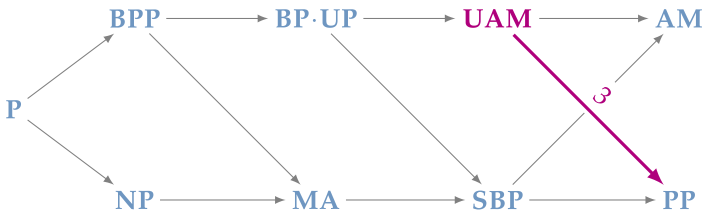
Results

$$\begin{tikzcd}
 & \mathbf{BPP} \arrow[r] \arrow[ddr] & \mathbf{BP\cdot UP} \arrow[r] \arrow[ddr] & \mathbf{UAM} \arrow[r] & \mathbf{AM} \\
\mathbf{P} \arrow[ur] \arrow[dr] & & & & \\
 & \mathbf{NP} \arrow[r] & \mathbf{MA} \arrow[r] & \mathbf{SBP} \arrow[r] \arrow[uur] & \mathbf{PP}
\end{tikzcd}$$

Theorem 1: $\forall f: \quad \mathbf{ZAM}(f) \leq \text{BranchingProgramSize}(f)$

Theorem 2: $\forall f: \quad \mathbf{ZAM}(f) \geq \mathbf{coNP}(f)$

Results

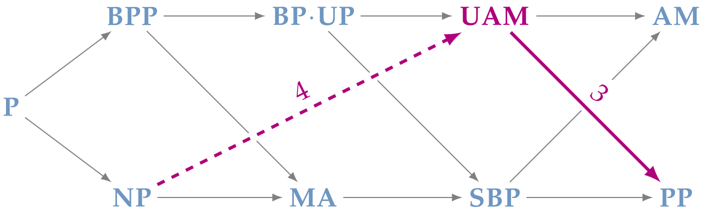


Theorem 1: $\forall f: \quad \mathbf{ZAM}(f) \leq \text{BranchingProgramSize}(f)$

Theorem 2: $\forall f: \quad \mathbf{ZAM}(f) \geq \mathbf{coNP}(f)$

Theorem 3: $\forall f: \quad \mathbf{UAM}(f) \geq \mathbf{PP}(f) \qquad = \Theta(\text{discrepancy})$

Results



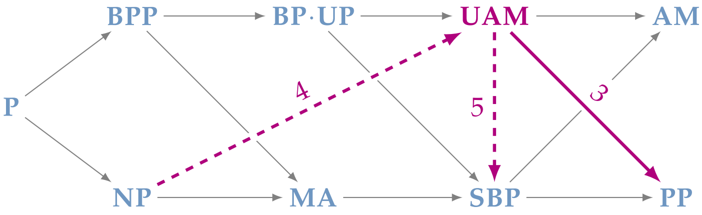
Theorem 1: $\forall f: \quad \mathbf{ZAM}(f) \leq \text{BranchingProgramSize}(f)$

Theorem 2: $\forall f: \quad \mathbf{ZAM}(f) \geq \mathbf{coNP}(f)$

Theorem 3: $\forall f: \quad \mathbf{UAM}(f) \geq \mathbf{PP}(f) \qquad = \Theta(\text{discrepancy})$

Theorem 4: $\mathbf{UAM}(\text{set-intersection}) \geq \Omega(n)$

Results



Theorem 1: $\forall f: \quad \mathbf{ZAM}(f) \leq \text{BranchingProgramSize}(f)$

Theorem 2: $\forall f: \quad \mathbf{ZAM}(f) \geq \mathbf{coNP}(f)$

Theorem 3: $\forall f: \quad \mathbf{UAM}(f) \geq \mathbf{PP}(f) \qquad = \Theta(\text{discrepancy})$

Theorem 4: $\mathbf{UAM}(\text{set-intersection}) \geq \Omega(n)$

Theorem 5:* $\exists f: \quad \mathbf{UAM}(f) \ll \mathbf{SBP}(f) \qquad = \Theta(\text{corruption})$

Proof idea for $\mathbf{ZAM}(f) \leq \text{BranchingProgramSize}(f)$

1. Reduce f to problem of form $\det(M_f) \neq 0$ [Valiant]

$$\begin{array}{r l} \text{Alice} \left\{ \begin{array}{c} \\ \\ \\ \end{array} \right. & \\ \text{Bob} \left\{ \begin{array}{c} \\ \\ \\ \end{array} \right. & \end{array} \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 3 \\ 4 & 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 3 & 1 & 0 & 1 \\ 1 & 1 & 3 & 0 & 1 & 2 \\ 0 & 0 & 1 & 4 & 4 & 1 \\ 2 & 0 & 1 & 1 & 0 & 3 \end{bmatrix}$$

Proof idea for $\mathbf{ZAM}(f) \leq \text{BranchingProgramSize}(f)$

1. Reduce f to problem of form $\det(M_f) \neq 0$ [Valiant]
2. **ZAM** protocol for $\det(M_f) \neq 0$:
   - Alice+Bob pick random vector

$$\begin{array}{cc} \begin{array}{c} \text{Alice}\left\{\begin{array}{c} \\ \\ \\ \end{array}\right. \\ \text{Bob}\left\{\begin{array}{c} \\ \\ \\ \end{array}\right. \end{array} & \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 3 \\ 4 & 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 3 & 1 & 0 & 1 \\ 1 & 1 & 3 & 0 & 1 & 2 \\ 0 & 0 & 1 & 4 & 4 & 1 \\ 2 & 0 & 1 & 1 & 0 & 3 \end{bmatrix} \qquad \begin{bmatrix} 3 \\ 3 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \end{array}$$

Proof idea for $\mathbf{ZAM}(f) \leq \text{BranchingProgramSize}(f)$

1. Reduce f to problem of form $\det(M_f) \neq 0$ [Valiant]
2. **ZAM** protocol for $\det(M_f) \neq 0$:
   - Alice+Bob pick random vector
   - Merlin sends a preimage
   - Alice+Bob check that preimage maps to vector

$$\begin{array}{c} \text{Alice}\left\{\begin{array}{c}\\ \\ \\ \end{array}\right. \\ \text{Bob}\left\{\begin{array}{c}\\ \\ \\ \end{array}\right. \end{array} \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 3 \\ 4 & 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 3 & 1 & 0 & 1 \\ 1 & 1 & 3 & 0 & 1 & 2 \\ 0 & 0 & 1 & 4 & 4 & 1 \\ 2 & 0 & 1 & 1 & 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 4 \\ 3 \\ 4 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Summary

This work:

- We introduced restricted models **ZAM** and **UAM** that capture some of the difficulty of **AM**

Open problems:

- Most annoying: Prove

$$\mathbf{ZAM}(\text{set-disjointness}) \geq \Omega(n)$$

- Close the gap:

$$\forall f : \mathbf{ZAM}(f) \leq 2^n \quad \text{vs.} \quad \exists f : \mathbf{ZAM}(f) \geq n$$

Questions?