One-way multi-party communication lower bound for pointer jumping with applications

Emanuele Viola & Avi Wigderson

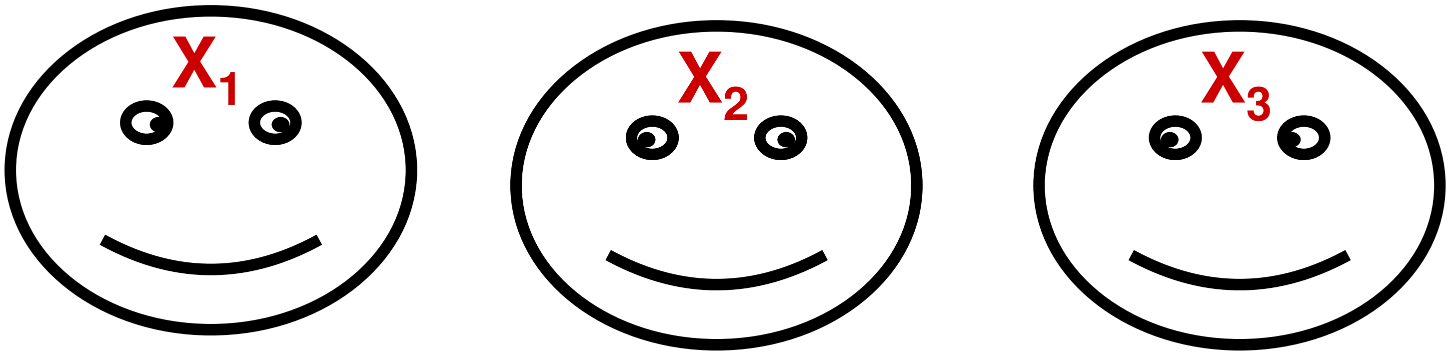
Columbia University
work done while at IAS

IAS

October 2007

Multiparty protocols

[Yao, Chandra Furst Lipton ‘83]



- k parties wish to compute $f : X_1 \times X_2 \ldots \times X_k \to \{0,1\}$
  Party i knows all inputs except x_i (on forehead)
  Cost of protocol = communication c

- Applications to many areas of computer science
  – Circuit/proof complexity, PRGs, TM’s, branching programs…

- Context: no lower bound known for $k \geq \log n$ parties

Rounds

[Papadimitriou Sipser '82]

- Parties only exchange **r** messages (any order, length $\leq$c)

- Question: More rounds more power?

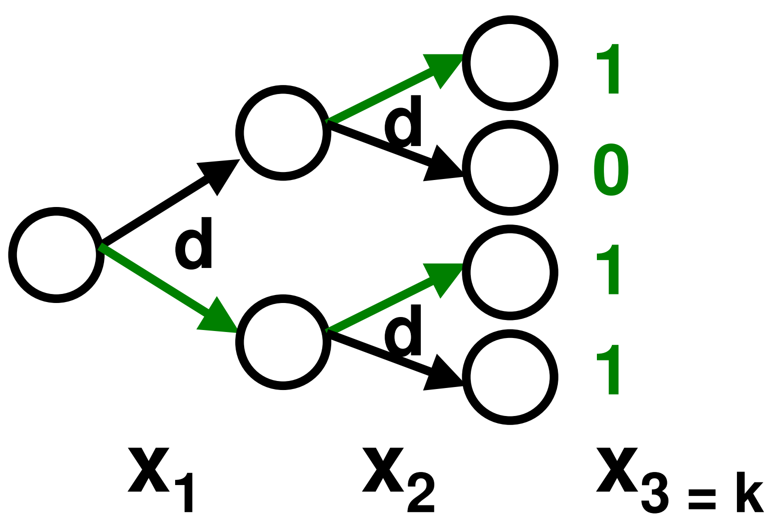
- Theorem[Duris Galil Schnitger, …, Nisan Wigderson]
  Hierarchy for k = 2 parties. $\exists\, f : X_1 \times X_2 \to \{0,1\}$:
  communication $c = n^{\Omega(1)}$ for 2-party **r**-round
  communication $c = O(\log n)$ for 2-party (**r+1**)-round

- Theorem[This work]
  Hierarchy for any k parties. $\exists\, f : X_1 \times \ldots \times X_k \to \{0,1\}$:
  communication $c = n^{\Omega(1)}$ for k-party **r**-round
  communication $c = O(\log n)$ for k-party (**2 r**)-round

One-way model and PJ

- Results on rounds $\Leftarrow$ new bound in one-way model:
  Parties speak once, in turn: 1,2,…,k

- Pointer jumping function $PJ_k : X_1 \times \ldots \times X_k = \{0,1\}^n \to \{0,1\}$
  d-regular tree of depth k-1
  Input = pointers node $\to$ child, leaf $\to$ 0 or 1
  Output = bit reached following path from root

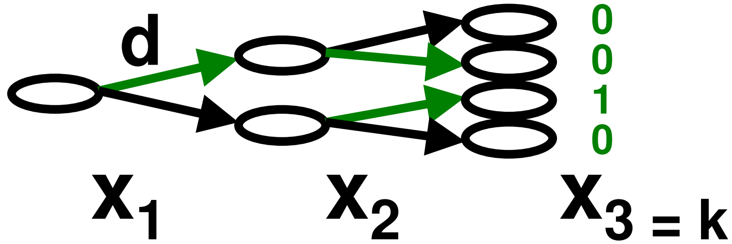


$d = n^{1/(k-1)}$

- Party i knows all pointers except those on i-th level (x_i)

Previous results on PJ

- $PJ_k : X_1 \times \ldots \times X_k = \{0,1\}^n \to \{0,1\}$



$d = n^{1/(k-1)}$

Trivial upper bound: Communication $c \leq$ degree d

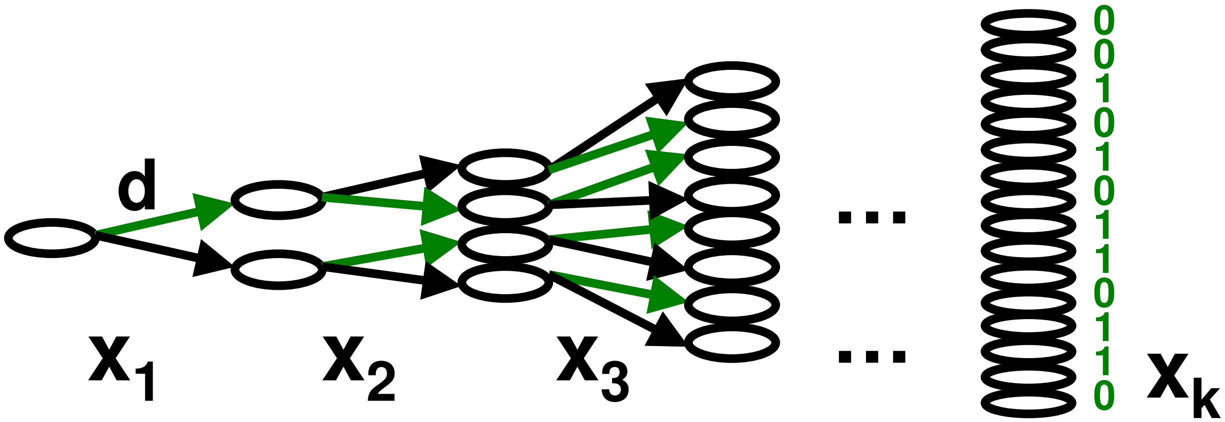
- Theorem[Wigderson]:
Communication $c \geq \Omega(d) = \Omega(n^{0.5})$ for $k = 3$ parties

- Theorem[Damm Jukna Sgall '96, Chakrabarti '07]
Lower bounds for $k > 3$ parties in restricted models

- Nothing was known for $k = 4$ parties in one-way model

Our main theorem

- PJ_k :



$d = n^{1/(k-1)}$

- Theorem[This work]
  One-way communication of k-party
  $PJ_k : \{0,1\}^n \to \{0,1\}$ is $c \geq d / k^k = n^{1/(k-1)} / k^k$

- Tight for fixed k: Trivial upper bound $c \leq$ degree d
- Non-trivial up to $k = \log^{1/3} n$ (by definition $k \leq \log n$)
- Distributional result $\Rightarrow$ bounds randomized protocols

Consequences of our main theorem

- General model with bounded rounds

1) Round hierarchy ∀ k parties (already mentioned)
2) Separating nondeterminism from determinism ∀ k

- One-way model

1) Separation of different orders for parties
2) Lower bound for disjointess; extend simultaneous bound in [Beame Pitassi Segerlind Wigderson]

- Streaming algorithms

Lower bound even with access to many orderings

Outline

- Main result and consequences
- Proof of lower bound

Main theorem

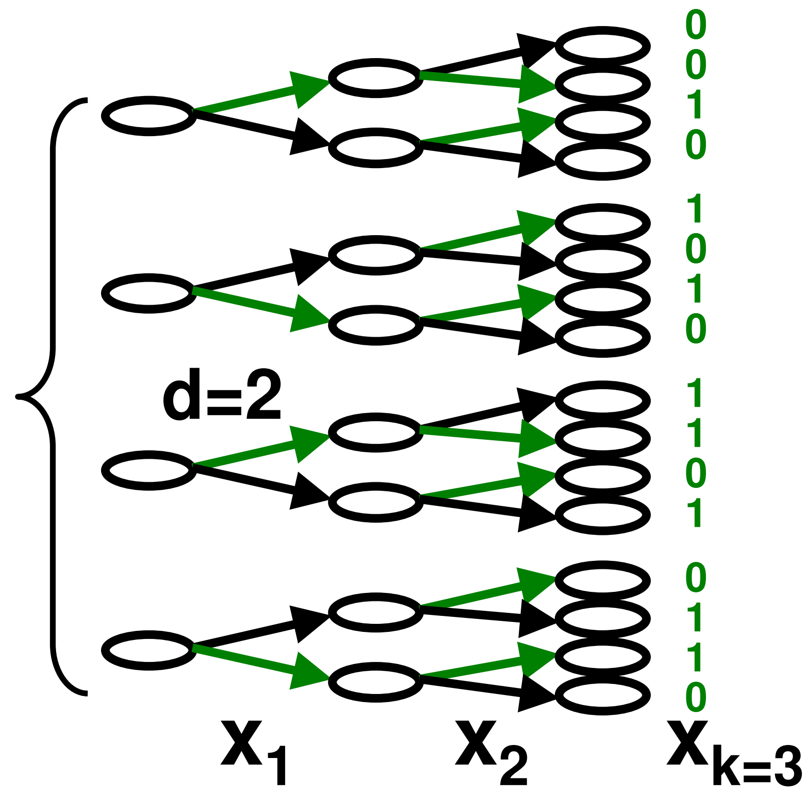
- Want: $\forall$ k parties there is no protocol Π:

$$\boxed{\Pr_x[\Pi(x) = PJ_k(x)] = 1 \text{ with } c \leq o(d)}$$

- m-bit extension of PJ_k

  $PJ_k^m : X_1 \times \ldots \times X_k \to \{0,1\}^m$

Example **m=4**



- Will prove: $\forall$ k parties there is no protocol Π:

$$\boxed{\Pr_x[\Pi(x) = PJ_k^m(x)] \geq \exp(-o(m)) \text{ with } c \leq o(m \cdot d)}$$

Proof

- Th.: $\forall$ k parties there is no protocol Π:

$$\boxed{\Pr_x[\Pi(x) = PJ_k^m(x)] \geq \exp(-o(m)) \text{ with } c \leq o(m \cdot d)}$$

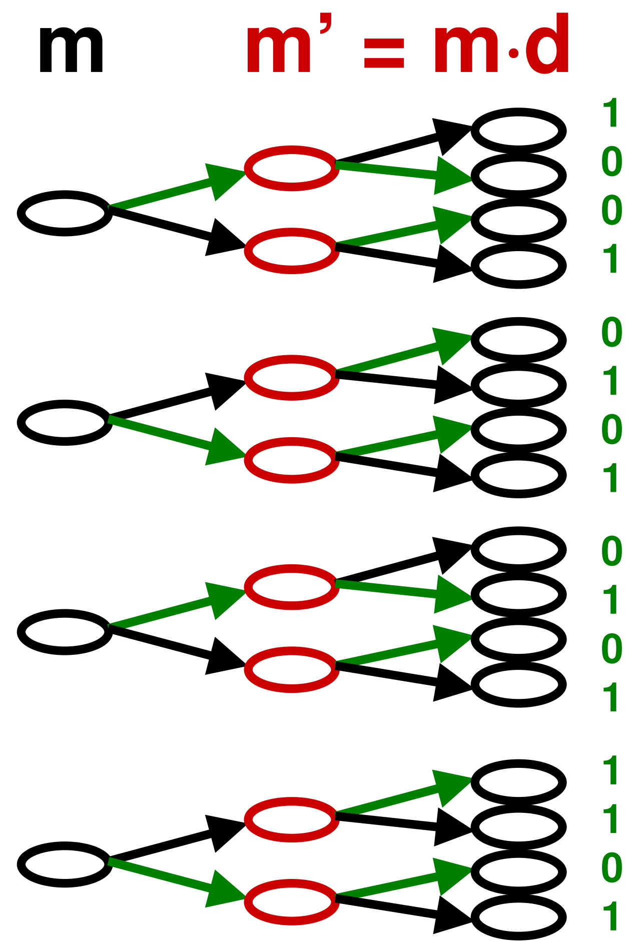
- Proof by induction on k = parties

  Assume for contradiction

$$\boxed{\begin{array}{l}\Pr_x[\Pi(x) = PJ_k^m(x)] \geq \exp(-o(m)) \\ \text{with } c \leq o(m \cdot d)\end{array}}$$

$$\Downarrow$$

$$\boxed{\begin{array}{l}\Pr_x[\Pi'(x) = PJ_{k-1}^{m'}(x)] \geq \exp(-o(m')) \\ \text{with } c' \leq o(m' \cdot d), \;\; m' = m \cdot d\end{array}}$$



Proof of inductive step

- Assume for contradiction

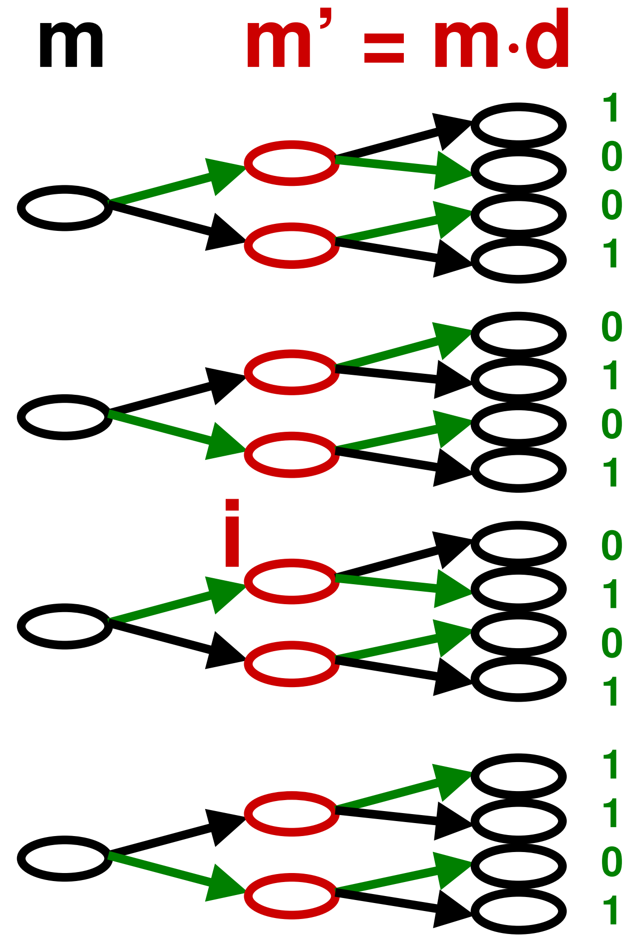
$$\boxed{\Pr_x[\Pi(x) = PJ_k^m(x)] \geq \exp(-o(m)) \text{ with } c \leq o(m \cdot d)}$$

- Definition of Π'

Input $y = x_2 x_3 \ldots x_k$

Choose $x_1^1, x_1^2, \ldots, x_1^d \in^R X_1$

Run Π d times on $x_1^1 y, \ldots, x_1^d y$



i-th output bit:

If some x_1^h hits **i**, use output of Π

If not, output random bit

[Ben-Aroya, Regev, de Wolf; '07]

Analysis

- Assume for contradiction

$\boxed{Pr_x[\Pi(x) = PJ_k^m(x)] \geq \exp(-o(m)) \text{ with } c \leq o(m \cdot d)}$

- Definition of Π'

Input $y = x_2 x_3 \dots x_k$

Choose $x_1^1, x_1^2, \dots, x_1^d \in^R X_1$

Run Π d times on $x_1^1 y, \dots, x_1^d y$

Analysis

$c' = d \cdot c = o(m' \cdot d)$ √

$Pr[\text{all d runs correct}] \geq \exp(-o(m))^d = \exp(-o(m'))$ √

i-th output bit:

If some x_1^h hits **i**, use output of Π

If not, output random bit

Analysis

W.h.p. hit $(1-o(1)) \cdot m'$ **i**'s. Success $= \exp(-o(m'))$ √

Conclusion

- First one-way communication lower bound for pointer jumping with $k \geq 4$ parties

  Theorem[This work]
  One-way comm. of PJ_k is $c \geq d / k^k = n^{1/(k-1)} / k^k$

- Applications
  general bounded-rounds model, e.g. round hierarchy
  one-way model, e.g. disjointness

- Proof: compute $PJ_k \Rightarrow$ compute many copies of PJ_{k-1}

- Open problem: bound for $k \geq \log n$ on general graph?