

The Maximum Communication Complexity of Multi-Party Pointer Jumping

Joshua Brody

DARTMOUTH COLLEGE
HANOVER, NH USA

24th CCC, 2009, Paris

Talk Outline

- Multi-Party Communication Games
- The Multi-Party Pointer Jumping Problem
- Results
- Proof of Main Theorem
- Conclusions

Multi-party Communication Games



Multi-Party Communication Games

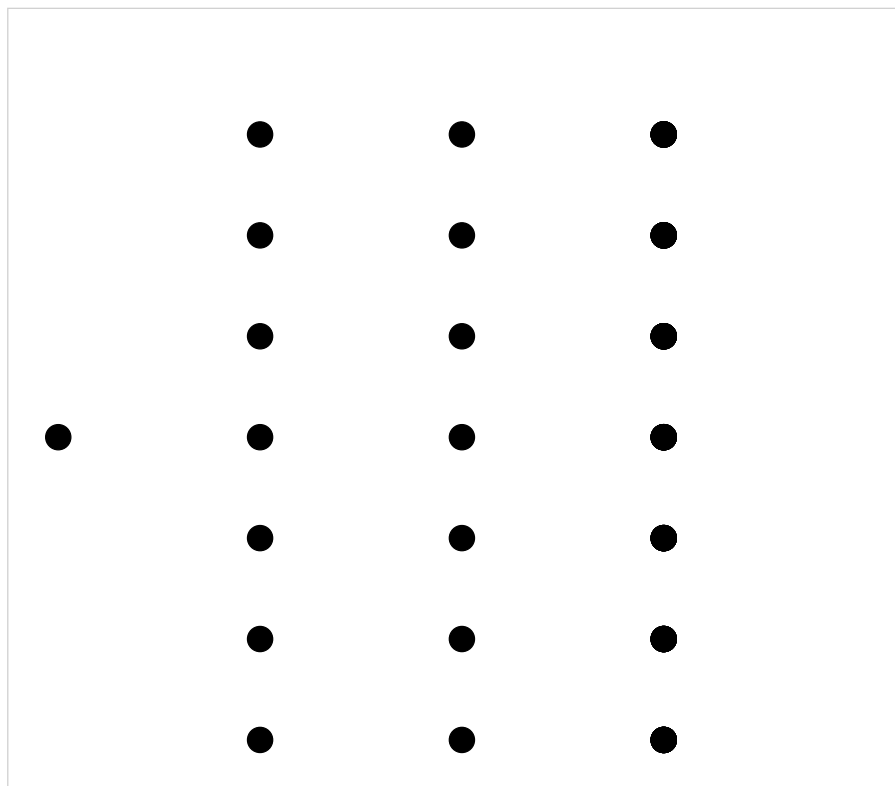
Input $x = (x_1, \dots, x_k)$ is split between k players.

Goal: minimize communication needed to compute $f(x)$.

Our model of communication:

- Player i sees every input except x_i (NOF model).
- One-way communication: each player speaks once and in order.
- Blackboard communication: all players see every message sent.

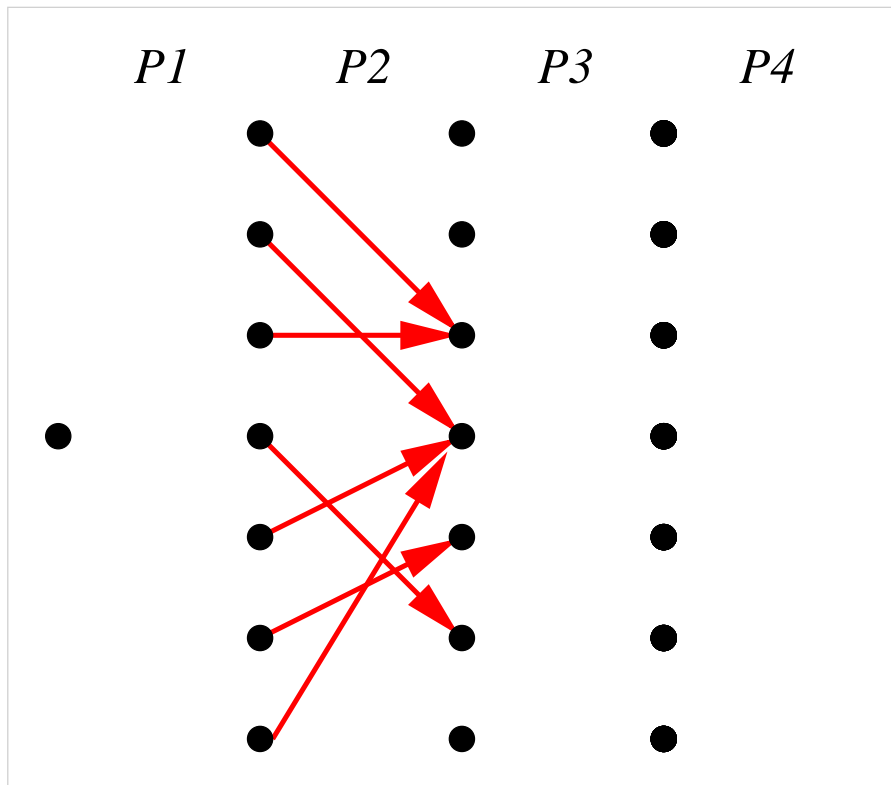
Pointer Jumping



Vertices:

- $k - 1$ layers, plus start vertex
- layers have n vertices

Pointer Jumping



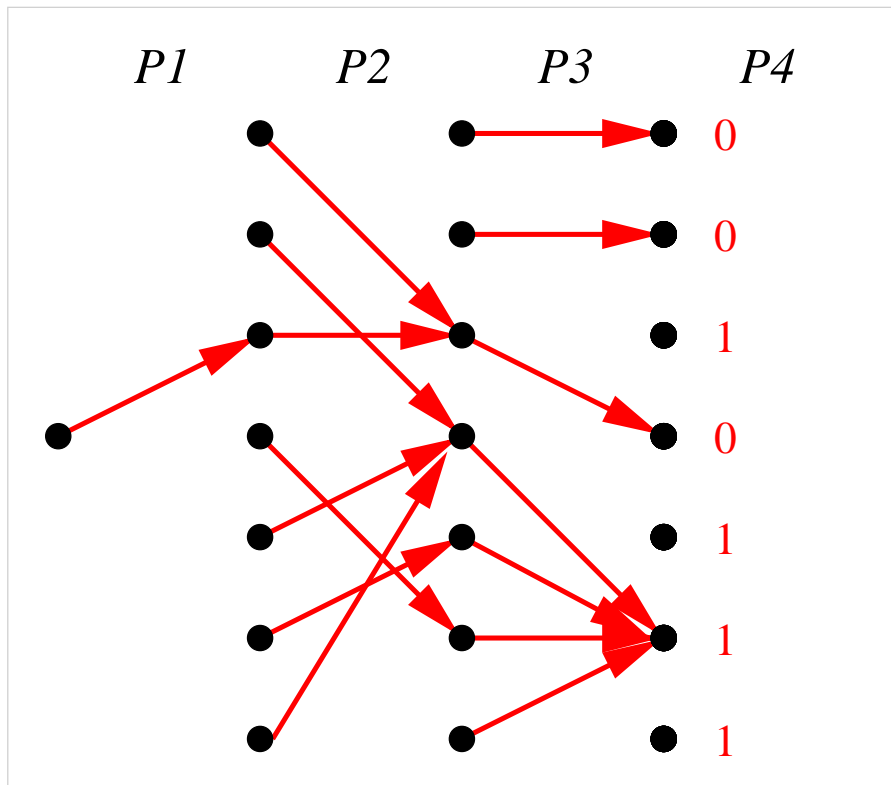
Vertices:

- $k - 1$ layers, plus start vertex
- layers have n vertices

Input:

- $k - 1$ layers of pointers
- n bit string

Pointer Jumping



Vertices:

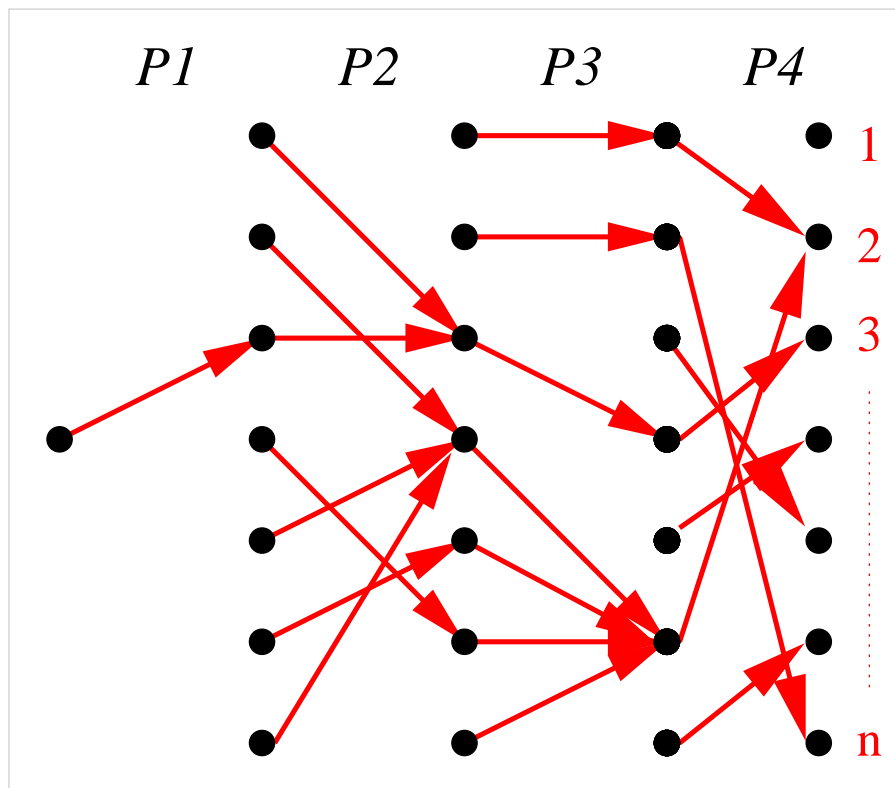
- $k - 1$ layers, plus start vertex
- layers have n vertices

Input:

- $k - 1$ layers of pointers
- n bit string

Compute $MPJ_k =$ bit reached by following pointers from start vertex.

Pointer Jumping: non-Boolean version



Vertices:

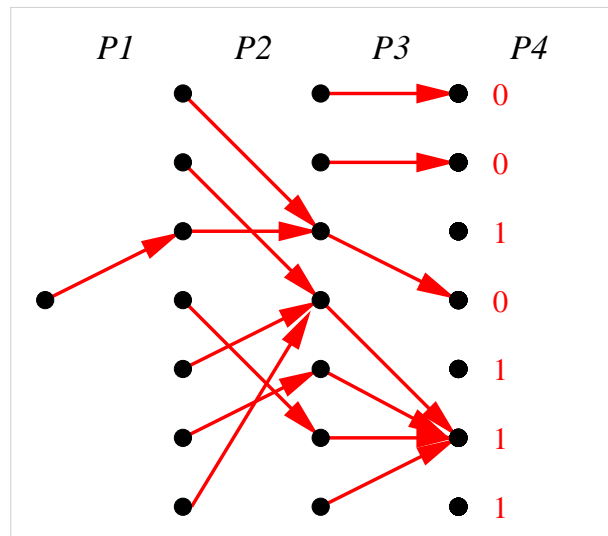
- k layers, plus start vertex
- layers have n vertices

Input:

- k layers of pointers

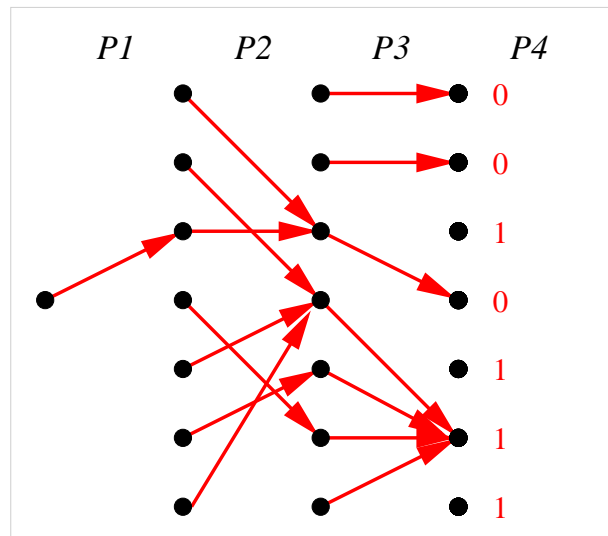
Compute $\widehat{MPJ}_k = \underline{\text{vertex}}$ reached by following pointers from start vertex.

Pointer Jumping: Trivial Bounds



- One-way: any order except $P1, P2, \dots, Pk$: $O(\log n)$
- One way: in the order $P1, P2, \dots, Pk$: $O(n)$

Pointer Jumping: Trivial Bounds



- One-way: any order except $P1, P2, \dots, Pk$: $O(\log n)$
- One way: in the order $P1, P2, \dots, Pk$: $O(n)$
 - Problem seems hard. Maybe $n^{\Omega(1)}$ lower bound?

Motivation

ACC^0 complexity class: AC^0 plus MOD_m gates.

- No function $f \notin \text{ACC}^0$ is known.
- If $f : \{0, 1\}^n \rightarrow \{0, 1\}$ and $f \in \text{ACC}^0$, then f has deterministic NOF protocol with $\text{poly}(\log n)$ communication, for $k = \text{poly}(\log n)$ players.

[Yao'90], [Håstad-Goldmann'91], [Beigel-Tarui'94]

More Motivation

ACC^0 complexity class: AC^0 plus MOD_m gates.

- No function $f \notin \text{ACC}^0$ is known.
- If $f : \{0, 1\}^n \rightarrow \{0, 1\}$ and $f \in \text{ACC}^0$, then f has deterministic NOF protocol with $\text{poly}(\log n)$ communication, for $k = \text{poly}(\log n)$ players.

[Yao'90], [Håstad-Goldmann'91], [Beigel-Tarui'94]

Recently pointer jumping has been used to prove lower bounds in:

- threshold circuits [Razborov-Wigderson'93]
- proof size [Beame-Pitassi-Segerlind'05]
- matroid intersection queries [Harvey'08]
- randomly-ordered data streams [Chakrabarti-Cormode-McGregor'08]

Previous Result Highlights

Far from proving $\text{MPJ}_{\text{poly}(\log n)} \notin \text{ACC}^0$

- $\Omega(n^{1/2})$ for MPJ_3 [Wigderson'97]
- $\Omega(n^{1/(k-1)}/k^k)$ for MPJ_k [Viola-Wigderson'07]
- $O\left(n \log^{(k-1)} n\right)$ for $\widehat{\text{MPJ}}_k$ [Damm-Jukna-Sgall'96]
- $O\left(n \sqrt{\frac{\log \log n}{\log n}}\right)$ for MPJ_3 [B.-Chakrabarti'08]

Restricted Protocols

Partial progress: protocols with more restricted forms of information sharing

- **Myopic protocols:** P_j only sees layers $1, \dots, (j - 1)$ as well as layer $(j + 1)$ of graph. (i.e., limited visibility of layers ahead)

[Gronemeier'06]

- **Conservative protocols:** P_j sees layers $(j + 1), \dots, k$ of graph, plus composition of layers $1, \dots, (j - 1)$. Doesn't see individual layers $1, \dots, (j - 1)$ themselves. (i.e., limited visibility of layers behind)

[Damm-Jukna-Sgall'96]

Restricted Protocols

Partial progress: protocols with more restricted forms of information sharing

- **Myopic protocols:** P_j only sees layers $1, \dots, (j - 1)$ as well as layer $(j + 1)$ of graph. (i.e., limited visibility of layers ahead)

[Gronemeier'06]

- **Conservative protocols:** P_j sees layers $(j + 1), \dots, k$ of graph, plus composition of layers $1, \dots, (j - 1)$. Doesn't see individual layers $1, \dots, (j - 1)$ themselves. (i.e., limited visibility of layers behind)

[Damm-Jukna-Sgall'96]

Note: The DJS protocol for $\widehat{\text{MPJ}}_k$ is both **myopic** and **conservative**!

Restricted Protocols

Partial progress: protocols with more restricted forms of information sharing

- **Myopic protocols:** P_j only sees layers $1, \dots, (j - 1)$ as well as layer $(j + 1)$ of graph. (i.e., limited visibility of layers ahead)

[Gronemeier'06]

- **Conservative protocols:** P_j sees layers $(j + 1), \dots, k$ of graph, plus composition of layers $1, \dots, (j - 1)$. Doesn't see individual layers $1, \dots, (j - 1)$ themselves. (i.e., limited visibility of layers behind)

[Damm-Jukna-Sgall'96]

Note: The DJS protocol for $\widehat{\text{MPJ}}_k$ is both **myopic** and **conservative**!

[Chakrabarti'07] gave randomized lower bounds for restricted protocols:

- **myopic:** $\Omega(n/k)$ bits.
- **conservative:** $\Omega(n/k^2)$ bits.

Restricted Protocols

Partial progress: protocols with more restricted forms of information sharing

- **Myopic protocols:** P_j only sees layers $1, \dots, (j - 1)$ as well as layer $(j + 1)$ of graph. (i.e., limited visibility of layers ahead)

[Gronemeier'06]

- **Conservative protocols:** P_j sees layers $(j + 1), \dots, k$ of graph, plus composition of layers $1, \dots, (j - 1)$. Doesn't see individual layers $1, \dots, (j - 1)$ themselves. (i.e., limited visibility of layers behind)

[Damm-Jukna-Sgall'96]

Note: The DJS protocol for $\widehat{\text{MPJ}}_k$ is both **myopic** and **conservative**!

[Chakrabarti'07] gave randomized lower bounds for restricted protocols:

- **myopic:** $\Omega(n/k)$ bits.
- **conservative:** $\Omega(n/k^2)$ bits.

For the rest of this talk: all protocols are **myopic**.

Our Results

Question: Can there be any nontrivial **myopic** protocol for MPJ_k ?

Our Results

Question: Can there be any nontrivial **myopic** protocol for MPJ_k ?

No, but in an interesting way...

Our Results

Question: Can there be any nontrivial **myopic** protocol for MPJ_k ?

No, but in an interesting way...

Theorem: In any myopic protocol for MPJ_k , some player must send at least $n/2$ bits.

Our Results

Question: Can there be any nontrivial **myopic** protocol for MPJ_k ?

No, but in an interesting way...

Theorem: In any myopic protocol for MPJ_k , some player must send at least $n/2$ bits.

Definitions:

- $\text{cost}(\mathcal{P}) :=$ cost of **largest message** of \mathcal{P} .
- $\text{tcost}(\mathcal{P}) :=$ total cost of \mathcal{P} .
- δn -bit protocol: $\text{cost}(\mathcal{P}) = \delta n$.

Detailed Results

Main Theorem: There exists a decreasing function $\phi : \mathbb{N} \rightarrow \mathbb{R}$ with $\lim_{k \rightarrow \infty} \phi(k) = \frac{1}{2}$ such that

1. Any deterministic protocol for MPJ_k costs at least $\phi(k)n$ bits.

Detailed Results

Main Theorem: There exists a decreasing function $\phi : \mathbb{N} \rightarrow \mathbb{R}$ with $\lim_{k \rightarrow \infty} \phi(k) = \frac{1}{2}$ such that

1. Any deterministic protocol for MPJ_k costs at least $\phi(k)n$ bits.
2. There exists a protocol \mathcal{P} for MPJ_k with $\text{cost}(\mathcal{P}) = \phi(k)n + o(n)$.

Detailed Results

Main Theorem: There exists a decreasing function $\phi : \mathbb{N} \rightarrow \mathbb{R}$ with $\lim_{k \rightarrow \infty} \phi(k) = \frac{1}{2}$ such that

1. Any deterministic protocol for MPJ_k costs at least $\phi(k)n$ bits.
2. There exists a protocol \mathcal{P} for MPJ_k with $\text{cost}(\mathcal{P}) = \phi(k)n + o(n)$.

Corollary: Any deterministic protocol for MPJ_k has total cost at least n .

Theorem: If \mathcal{P} is a deterministic protocol for $\widehat{\text{MPJ}}_k$ then

$$\text{cost}(\mathcal{P}) \geq n \left(\log^{(k-1)} n \right) (1 - o(1)).$$

Theorem: Any randomized protocol for MPJ_k has

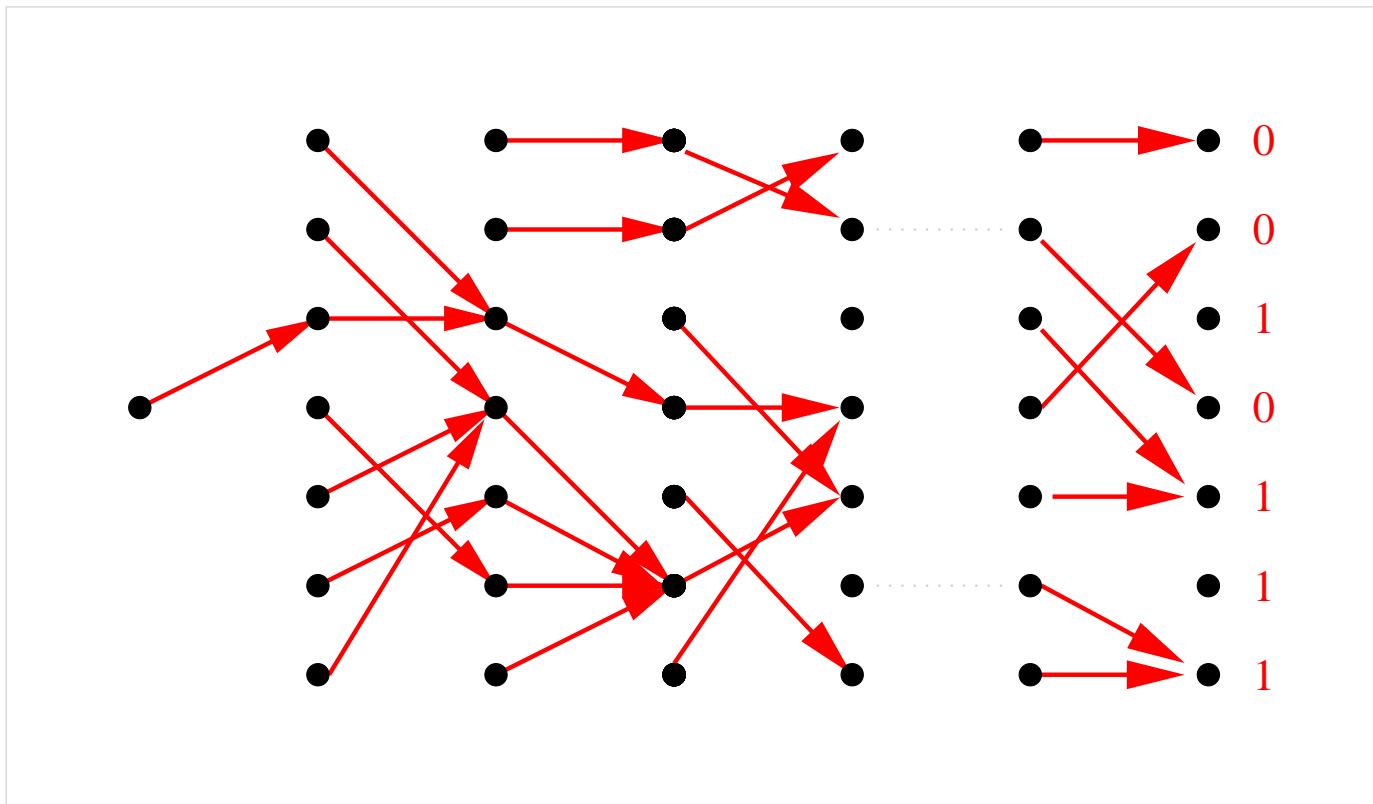
$$\text{cost}(\mathcal{P}) = \Omega \left(\frac{n}{k \log n} \right).$$

Talk Outline

- Multi-Party Communication Games
- The Multi-Party Pointer Jumping Problem
- Results
- Proof of Main Theorem
- Conclusions

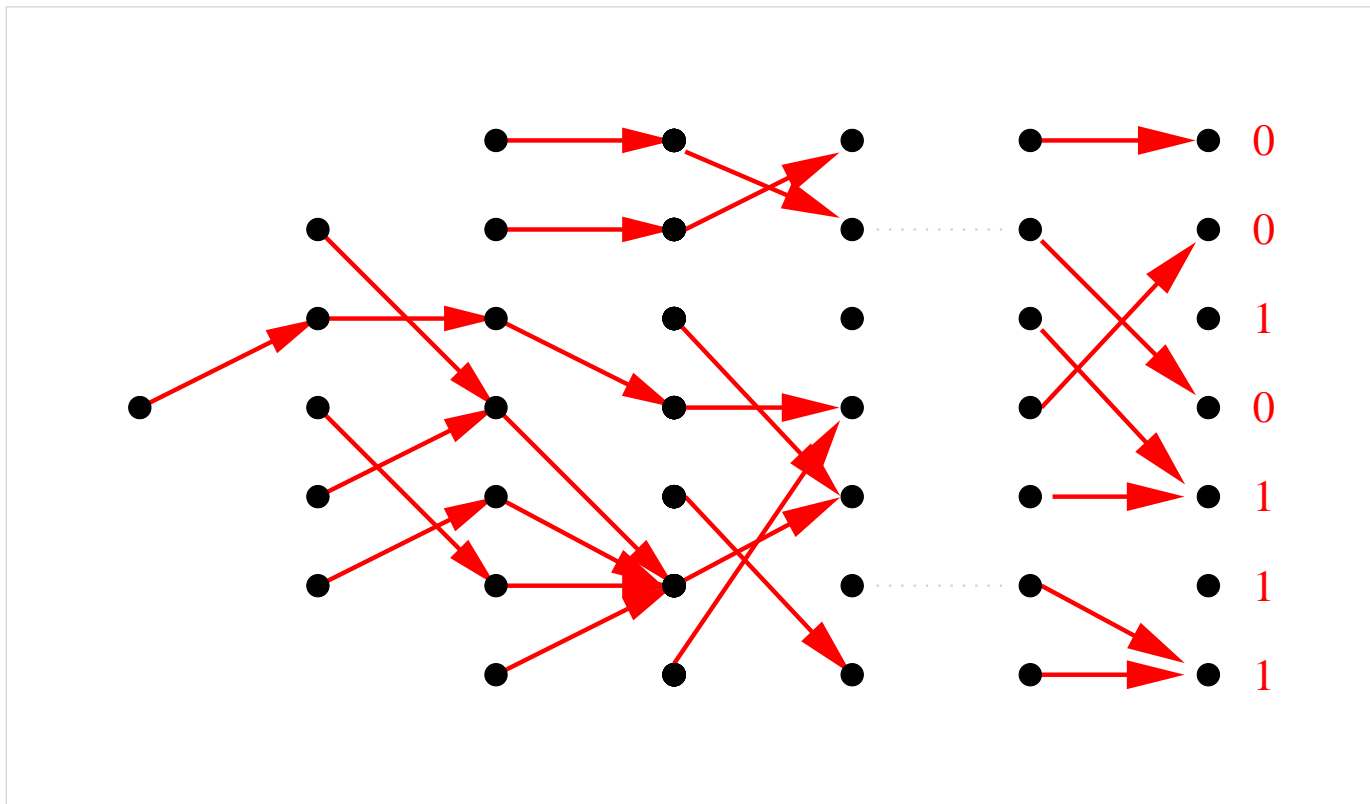
Generalized Pointer Jumping

$MPJ_{m,k}$: just like MPJ_k , except $m \leq n$ vertices in first layer.



Generalized Pointer Jumping

$MPJ_{m,k}$: just like MPJ_k , except $m \leq n$ vertices in first layer.



Round Elimination Lemma

Base Case Lemma: Any protocol \mathcal{P} for $\text{MPJ}_{m,2}$ has $\text{cost}(\mathcal{P}) \geq m$ (INDEX)

Round Elimination Lemma: Let $k \geq 3$. If there is a δn -bit protocol \mathcal{P} for $\text{MPJ}_{m,k}$, then there is a δn -bit protocol \mathcal{Q} for $\text{MPJ}_{m',k-1}$ with $m' = n \cdot 2^{-\delta n/m}$.

Round Elimination Lemma

Base Case Lemma: Any protocol \mathcal{P} for $\text{MPJ}_{m,2}$ has $\text{cost}(\mathcal{P}) \geq m$ (INDEX)

Round Elimination Lemma: Let $k \geq 3$. If there is a δn -bit protocol \mathcal{P} for $\text{MPJ}_{m,k}$, then there is a δn -bit protocol \mathcal{Q} for $\text{MPJ}_{m',k-1}$ with $m' = n \cdot 2^{-\delta n/m}$.

Message Sets:

- P1's input: $f_2 \in [n]^{[m]}$
- $M := M_{\mathbf{m}} = \{f_2 : \text{P1 sends } \mathbf{m} \text{ on input } f_2\}$.
- Fix \mathbf{m} to maximize $|M|$; then $|M| \geq \frac{n^m}{2^{\delta n}}$.

Definition: For $\mathcal{F} \subseteq [n]^{[m]}$, $\text{Range}(i, \mathcal{F}) := \{f_2(i) : f_2 \in \mathcal{F}\}$

Round Elimination Lemma

Base Case Lemma: Any protocol \mathcal{P} for $\text{MPJ}_{m,2}$ has $\text{cost}(\mathcal{P}) \geq m$ (INDEX)

Round Elimination Lemma: Let $k \geq 3$. If there is a δn -bit protocol \mathcal{P} for $\text{MPJ}_{m,k}$, then there is a δn -bit protocol \mathcal{Q} for $\text{MPJ}_{m',k-1}$ with $m' = n \cdot 2^{-\delta n/m}$.

Message Sets:

- P1's input: $f_2 \in [n]^{[m]}$
- $M := M_{\mathbf{m}} = \{f_2 : \text{P1 sends } \mathbf{m} \text{ on input } f_2\}$.
- Fix \mathbf{m} to maximize $|M|$; then $|M| \geq \frac{n^m}{2^{\delta n}}$.

Definition: For $\mathcal{F} \subseteq [n]^{[m]}$, $\text{Range}(i, \mathcal{F}) := \{f_2(i) : f_2 \in \mathcal{F}\}$

Range Lemma: If $|\mathcal{F}| \geq (m')^m$, then $\exists i$ with $|\text{Range}(i, \mathcal{F})| \geq m'$

Proof of Round Elimination Lemma

Base Case Lemma: Any protocol \mathcal{P} for $\text{MPJ}_{m,2}$ has $\text{cost}(\mathcal{P}) \geq m$ (INDEX)

Round Elimination Lemma: Let $k \geq 3$. If there is a δn -bit protocol \mathcal{P} for $\text{MPJ}_{m,k}$, then there is a δn -bit protocol \mathcal{Q} for $\text{MPJ}_{m',k-1}$ with $m' = n \cdot 2^{-\delta n/m}$.

Proof:

Proof of Round Elimination Lemma

Base Case Lemma: Any protocol \mathcal{P} for $\text{MPJ}_{m,2}$ has $\text{cost}(\mathcal{P}) \geq m$ (INDEX)

Round Elimination Lemma: Let $k \geq 3$. If there is a δn -bit protocol \mathcal{P} for $\text{MPJ}_{m,k}$, then there is a δn -bit protocol \mathcal{Q} for $\text{MPJ}_{m',k-1}$ with $m' = n \cdot 2^{-\delta n/m}$.

Proof:

- Fix M . Note: $|M| \geq \frac{n^m}{2^{\delta n}} = 2^{m \log n - \delta n} = (m')^m$.
- By Range Lemma, $\exists i \in [m]$ s.t. $|\text{Range}(i, M)| \geq m'$. Fix i .
- For each $j \in [m']$, fix $g_j \in M$ s.t. $g_j(i) = j$.
- Protocol \mathcal{Q} : on input $(j, f_3, \dots, f_{k-1}, x)$, players simulate \mathcal{P} on input $(i, g_j, f_3, \dots, f_{k-1}, x)$.

Analysis

Define

- $a_0 := 0, a_\ell := \delta 2^{a_\ell - 1}$
- $m_\ell := n 2^{-a_\ell}$

$$a_0 = 0$$

Definition: Let $\phi(k) :=$ least δ such that $a_{k-1} \geq 1$

Analysis

Define

- $a_0 := 0, a_\ell := \delta 2^{a_\ell - 1}$
- $m_\ell := n 2^{-a_\ell}$

$$a_1 = \delta$$

Definition: Let $\phi(k) :=$ least δ such that $a_{k-1} \geq 1$

Analysis

Define

- $a_0 := 0, a_\ell := \delta 2^{a_\ell - 1}$
- $m_\ell := n 2^{-a_\ell}$

$$a_2 = \delta 2^\delta$$

Definition: Let $\phi(k) :=$ least δ such that $a_{k-1} \geq 1$

Analysis

Define

- $a_0 := 0, a_\ell := \delta 2^{a_\ell - 1}$
- $m_\ell := n 2^{-a_\ell}$

$$a_3 = \delta 2^{\delta 2^\delta}$$

Definition: Let $\phi(k) :=$ least δ such that $a_{k-1} \geq 1$

Analysis

Define

- $a_0 := 0, a_\ell := \delta 2^{a_{\ell-1}}$
- $m_\ell := n 2^{-a_\ell}$

$$a_4 = \delta 2^{\delta 2^{\delta 2^\delta}}$$

Definition: Let $\phi(k) :=$ least δ such that $a_{k-1} \geq 1$

Analysis

Define

- $a_0 := 0, a_\ell := \delta 2^{a_{\ell-1}}$
- $m_\ell := n 2^{-a_\ell}$

$$a_\ell = \delta 2^{\delta 2^{\delta 2^{\delta 2^{\dots}}}}$$

Definition: Let $\phi(k) :=$ least δ such that $a_{k-1} \geq 1$

Analysis

Define

- $a_0 := 0, a_\ell := \delta 2^{a_\ell - 1}$
- $m_\ell := n 2^{-a_\ell}$

$$a_\ell = \delta 2^{\delta 2^{\delta 2^{\delta 2^{\dots}}}}$$

Definition: Let $\phi(k) :=$ least δ such that $a_{k-1} \geq 1$

Claim: $\lim_{k \rightarrow \infty} \phi(k) = 1/2$ (Induction)

Round elimination ($m = m_\ell$):

$$m' = n 2^{-\frac{\delta n}{m_\ell}} = n 2^{-\delta n / n 2^{-a_\ell}} = n 2^{-\delta 2^{a_\ell}} = n 2^{-a_{\ell+1}} = m_{\ell+1}$$

Proof of Main Theorem

Theorem: Any myopic protocol \mathcal{P} for $\text{MPJ}_k = \text{MPJ}_{n,k}$ has

$$\text{cost}(\mathcal{P}) \geq n\phi(k).$$

Proof:

Proof of Main Theorem

Theorem: Any myopic protocol \mathcal{P} for $\text{MPJ}_k = \text{MPJ}_{n,k}$ has

$$\text{cost}(\mathcal{P}) \geq n\phi(k).$$

Proof:

δn -bit protocol for $\text{MPJ}_{m_0,k} \Rightarrow$

$\dots k - 2$ round eliminations $\dots \Rightarrow$

δn -bit protocol for $\text{MPJ}_{m_{k-2},2} \Rightarrow$

$\delta n \geq n2^{-a_{k-2}} = m_{k-2}$ (Base Case Lemma) \Rightarrow

$a_{k-1} = \delta 2^{a_{k-2}} \geq 1 \Rightarrow$

$\delta \geq \phi(k)$ (by def. of $\phi(k)$)

A Sketch of Matching Upper Bound

Idea: Cover $[n]^{[m]}$ with sets $S_1, \dots, S_t \subseteq [n]^{[m]}$ s.t.

$$|\text{Range}(i, S)| = m' \text{ for all } i, S.$$

Packing lower bound: $t \geq 2^{\delta n}$.

Claim: $t \leq 2^{\delta n + o(n)}$. (Prob. Method)

Protocol:

- P1 sends $S \ni f_2$. (cost = $\delta n + o(n)$)
- Players $2, \dots, k$ see i , set $[m'] := \text{Range}(i, S)$.
- Players $2, \dots, k$ run $\text{MPJ}_{m', k-1}$ protocol on $(f_2(i), f_3, \dots, x)$.

Randomizing the Lower Bound

Round Elimination Lemma: Let $k \geq 3$. If there is a δn -bit, ε -error protocol \mathcal{P} for $\text{MPJ}_{m,k}$, then there is a δn -bit, ε' -error protocol \mathcal{Q} for $\text{MPJ}_{m',k-1}$ with $m' = n \cdot 2^{-2\delta n/m}$ and $\varepsilon' = 2n\varepsilon$.

Conclusions/Open Problems

Conclusions

- Still far from proving $MPJ_k \notin ACC^0$
- Characterized maximum communication complexity of myopic protocols up to $1 + o(1)$ factors.
- Technique applies to MPJ_k and \widehat{MPJ}_k and does randomize.
- Technique seems promising for other problems (e.g. Gap Hamming) - there's still juice to squeeze here!

Open Problems

1. Settle $D(MPJ_k)$
2. Possible first step: improve bound on MPJ_3
3. Relax protocol restrictions: 2-myopic, ...

Thanks!

Questions? Comments? Post-Doc/Job offers?
Contact jbrody@cs.dartmouth.edu