Some Lower Bounds in Dynamic Networks with Oblivious Adversaries

Irvan Jahja Haifeng Yu
National University of Singapore

Yuda Zhao
Grab

Background on Dynamic Networks

- Flourishing topic
  - Augustine et al. PODC 13', Censor-Hillel et al. PODC '16, Chen et al. JACM '14, Cornejo et al. PODC '12, Dutta et al. SODA '13, Ghaffari et al. PODC '13, Kuhn et al. PODC '10, STOC '10, PODC '11, etc.
- n fixed nodes
- Nodes proceeds in synchronous rounds
- Each round, adversary choose an arbitrary connected topology

Some Fundamental Problems in Dynamic Networks

- (Binary) Consensus
  - Each node starts with 0 or 1
  - Need to output a common value
- Leader Election
  - Need to output on a common node
- Aggregations problems: (Binary) Sum, Max
- Confirmed Flooding
  - v needs to flood a $O(\log n)$ sized token
  - Output when tokens has been received by all

Our Central Question

- Time complexity: number of rounds until all nodes output
  - (Dynamic) diameter d = minimum rounds to propagate message from one node to all others by flooding
    - Not known by protocol
  - $tc(d, n)$ = time complexity if ran over network with n nodes, d diameter
- Diameter crucially affects time complexity
  - $tc(d,n) = \Omega(d)$

Ignoring $\text{polylog}(n)$ terms, is $tc(d, n)$ independent of the network size n?

Known Results

Ignoring $\text{polylog}(n)$ terms, is $tc(d, n)$ independent of the network size n?

	Answer	
Static network	**Yes**	$tc(d, n) = O(d)$
Dynamic network, unlimited message size	**Yes**	$tc(d, n) = O(d)$ [Kuhn et al. PODC '11]
Dynamic network, $O(\log n)$ message size	**No**	$tc(d, n) = \Omega(d + \text{poly}(n))$ [Yu et al. SPAA '16]

Oblivious and Adaptive Adversaries

- Lower bound in [Yu et al. SPAA ‘16] critically relies on a powerful adaptive adversary.
  - Sees all coin flip outcomes up to and including current round when deciding topology.
- Proof breaks under oblivious adversary.
  - Decides topology in the start.
- Different adversaries often requires different approaches

Topic	Adaptive	Oblivious
Information dissemination	[Dutta et al. SODA ‘13]	[Augustine et al. DISC ‘16]
Dynamic MIS	[Konig et al. OPODIS13]	[Censor-Hillel et al. PODC16]
Broadcasting	[Kuhn et al. PODC ‘10]	[Ghaffari et al. PODC ‘13]

Our Contributions

Ignoring $\text{polylog}(n)$ terms, is $\text{tc}(d, n)$ independent of the network size n?

Static network	**Yes**	$\text{tc}(d, m) = O(d)$
Dynamic network unlimited message size	**Yes**	$\text{tc}(d, m) = O(d)$ [Kuhn et al. PODC '11]
Dynamic network $O(\log n)$ message Adaptive adversary	**No**	$\text{tc}(d, n) = \Omega(d + \text{poly}(n))$ [Yu et al. SPAA '16]
Dynamic network $O(\log n)$ message size Oblivious adversary	???	

Our Contributions

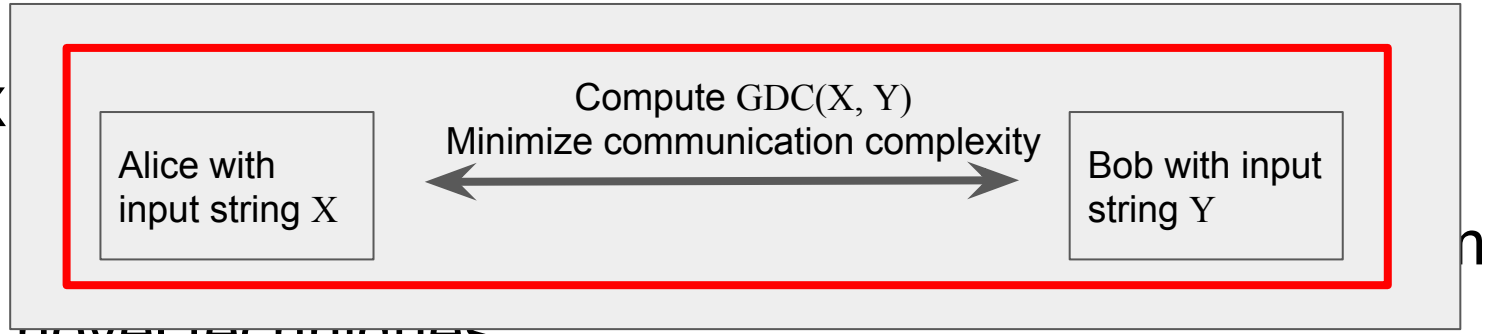
- **Even for constant diameter networks, protocols for Consensus, Leader Election, Aggregations (Sum, Max), and Confirmed Flooding will need poly(n) rounds**
- We use Consensus as an example for the rest of the discussion.

Adaptive adversary		
Dynamic network O(log n) message size Oblivious adversary	**No**	tc(d, n) = Ω(d + poly(n))

Existing Framework

- Builds upon the framework in [Yu et al. SPAA '16], two major novel techniques.
- Lower bound via reduction from two-party communication complexity (cc) problem: *Gap Disjointness with Cycle Promise* (GDC)
- Alice and Bob simulate:
  - An adversary (i.e., dynamic network)
  - Execution of an oracle Consensus protocol over the adversary.
- Lower bound on cc of GDC $\rightarrow$ Lower bound on $\mathrm{tc}(\mathrm{d},\mathrm{m})$

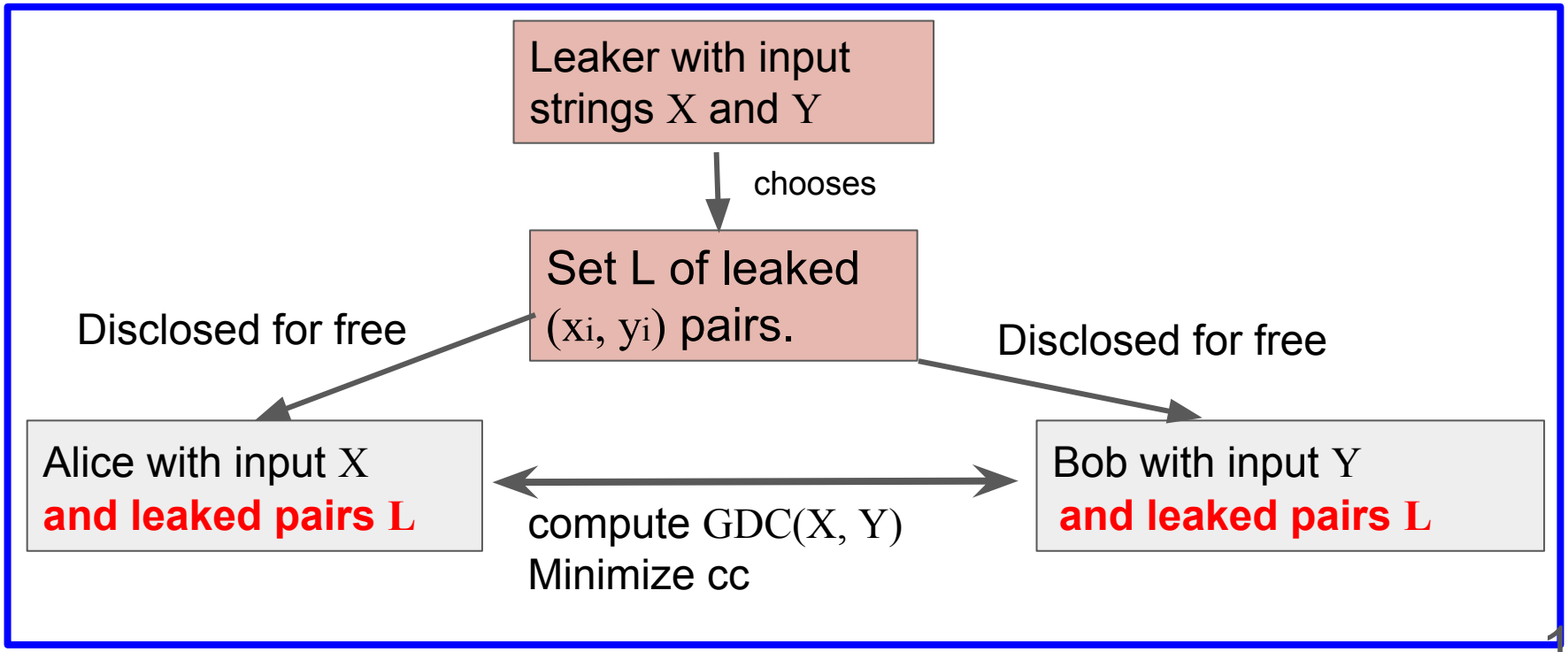
Ex



- major novel techniques:
- Lower bound via reduction from two-party communication complexity (cc) problem: *Gap Disjointness with Cycle Promise* (GDC)
- Alice and Bob simulate:
  - An adversary (i.e., dynamic network)
  - Execution of an oracle Consensus protocol over the adversary.
- Lower bound on cc of GDC → Lower bound on $tc(d,m)$

Needs to be oblivious

First Novel Technique: Communication Complexity with Leaker



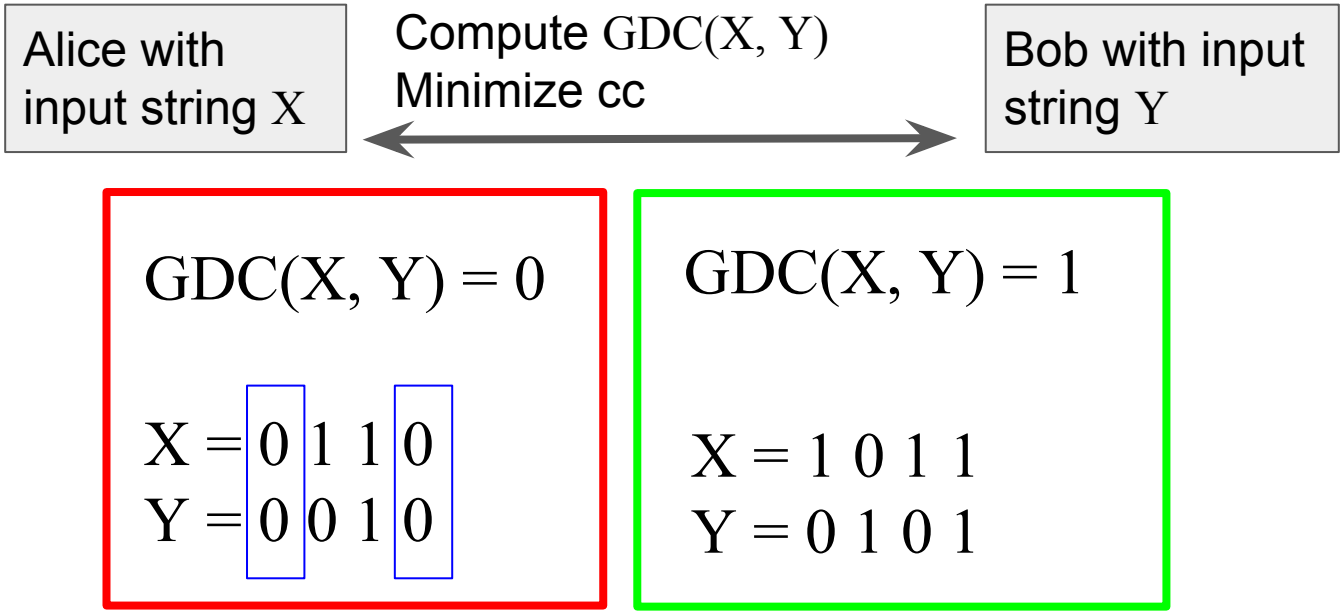
Second Novel Technique:
Sanitized Adaptive Adversary

- Alice and Bob simulate an adversary
  - The adversary is still adaptive
  - The adversary is a special case of adaptive adversary: Sanitized adaptive adversary
- We prove sanitized adaptive adversary has equivalent power as oblivious adversary

Roadmap

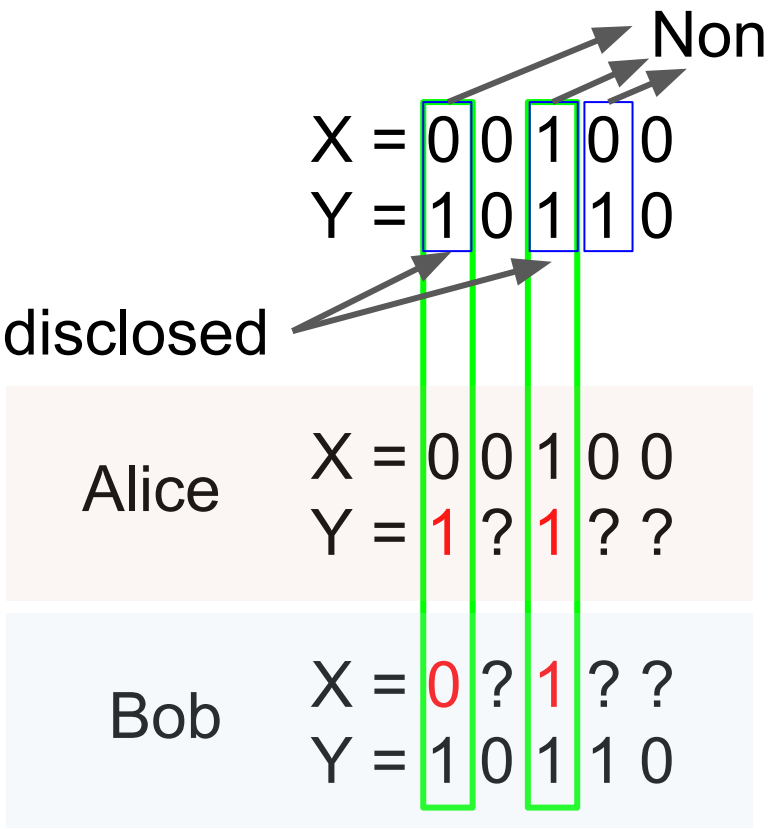
- Summary of Contributions and Approach ✓
- ➡ Novel Technique #1: Communication Complexity with Leaker
- Novel Technique #2: Sanitized Adaptive Adversary
- Putting It All Together

Novel Technique #1: GDC with Leaker



GDC with parameter g: if $(0, 0)$ exists, at least g such pairs exists.

Novel Technique #1: GDC with Leaker



Leaker discloses each non (0, 0) pair with half probability

Novel Technique #1: GDC with Leaker

- Leaker affects cc?
- For some problems, having a leaker reduces cc from polynomial to 0.
- We prove a lower bound on GDC with Leaker
  - We reduce from GDC with leaker into GDC without leaker
  - The leaker behavior is simulated in the reduction
  - Details in the paper

Novel Technique #2: Sanitized Adaptive Adversary

- In the existing framework [Yu et al. SPAA '16], Alice and Bob simulated an adaptive adversary α
  - α makes adaptive decisions
- In this work, Alice and Bob simulate a sanitized adaptive adversary β based on α. For each decision of α:
  - With half probability, β does exactly what α do
  - With half probability, β does opposite what α do

Novel Technique #2:
The Power of Sanitized Adaptive Adversary β

- β is still adaptive
- β is not more powerful than oblivious adversary
  - $tc(d, n)$ under β must be less than or equal to $tc(d, n)$ under some oblivious adversary

Putting It All Together

- Previous reduction [Yu et al. SPAA ‘16]: Alice and Bob simulates adaptive adversary
  - Makes adaptive decisions to remove certain edges in some rounds
- In this work, Alice and Bob makes guesses for each adaptive decision that α makes

Making Guesses

- If guess is correct, proceed as before
- If guess is wrong
  - Simulation can’t continue as previously
  - The pairs disclosed by the leaker allow the simulation to continue
  - The adversary simulated still adaptive, but it becomes a sanitized adaptive adversary
- Details are in the paper

Conclusion

For Consensus, Leader Election, Sum, Max, Confirmed Flooding:

> Ignoring $\text{polylog}(n)$ terms, is $\text{tc}(d, n)$ independent of the network size n? **No**

- Even for constant diameter graphs, solving these problems requires $\mathbf{poly(n)}$ rounds
- We used two major techniques to obtain this result:
  - Communication complexity with leaker
  - Sanitized adaptive adversary