Communication Complexity of Set-disjointness for All Probabilities

Mika Göös & Thomas Watson

University of Toronto

Communication complexity?

[Yao, STOC'79]

Alice **Bob**

Communication complexity?

[Yao, STOC'79]

Alice $x \subseteq [n]$

Bob $y \subseteq [n]$

Set-disjointness: $x \cap y = \emptyset$?

Communication complexity?

[Yao, STOC'79]

Alice

$x \subseteq [n]$

Bob

$y \subseteq [n]$

Set-disjointness: $x \cap y = \emptyset$?

[Kalyanasundaram–Schnitger'92], [Razborov'92], [Bar-Yossef et al.'04] ...

Main result

Bounded-error model:

- ***yes***-inputs accepted with prob. $\geq 99\%$
- ***no***-inputs accepted with prob. $\leq 1\%$

Main result

Our focus: Arbitrary probabilities $\alpha(n) > \beta(n)$:

- ***yes***-inputs accepted with prob. $\geq \alpha$
- ***no***-inputs accepted with prob. $\leq \beta$

Main result

Our focus: Arbitrary probabilities $\alpha(n) > \beta(n)$:

- ***yes***-inputs accepted with prob. $\geq \alpha$
- ***no***-inputs accepted with prob. $\leq \beta$
- Public vs. private coins

Tight bound: $\Theta(n \cdot (1 - \beta/\alpha))$

Simplifies: [Braun et al., FOCS'12]: EFs for max-clique
[Braverman–Moitra, STOC'13]: $\alpha = 1/2 + \epsilon, \beta = 1/2 - \epsilon$

Main result

Our focus: Arbitrary probabilities $\alpha(n) > \beta(n)$:

- ***yes***-inputs accepted with prob. $\geq \alpha$
- ***no***-inputs accepted with prob. $\leq \beta$
- Public vs. private coins

Tight bound: $\Theta(n \cdot (1 - \beta/\alpha))$

Simplifies: [Braun et al., FOCS'12]: EFs for max-clique
[Braverman–Moitra, STOC'13]: $\alpha = 1/2 + \epsilon, \beta = 1/2 - \epsilon$

Key insight: Suffices to understand case $\beta = \alpha/2$

SBP: Case $\beta = \alpha/2$

cf. [Böhler et al.'06]

SBP: Small bounded-error computations

- ***yes***-inputs accepted with prob. $\geq \alpha$
- ***no***-inputs accepted with prob. $\leq \alpha/2$

SBP: Small bounded-error computations

- ***yes***-inputs accepted with prob. $\geq \alpha$
- ***no***-inputs accepted with prob. $\leq \alpha/2$

New: $$\mathbf{SBP}(f) = \min_{\alpha(n)>0} \mathsf{R}^{\mathsf{pub}}_{\alpha,\alpha/2}(f) + \log(1/\alpha)$$

SBP: Case $\beta = \alpha/2$

cf. [Böhler et al.'06]

SBP: Small bounded-error computations

- ***yes***-inputs accepted with prob. $\geq \alpha$
- ***no***-inputs accepted with prob. $\leq \alpha/2$

New: $$\mathbf{SBP}(f) = \min_{\alpha(n)>0} \mathsf{R}^{\mathsf{pub}}_{\alpha,\alpha/2}(f) + \log(1/\alpha)$$

Compare: $$\mathbf{PP}(f) = \min_{\epsilon(n)>0} \mathsf{R}^{\mathsf{pub}}_{1/2+\epsilon,1/2-\epsilon}(f) + \log(1/\epsilon)$$

SBP: Case $\beta = \alpha/2$ cf. [Böhler et al.'06]

SBP: Small bounded-error computations

- ***yes***-inputs accepted with prob. $\geq \alpha$
- ***no***-inputs accepted with prob. $\leq \alpha/2$

New:

$$\mathbf{SBP}(f) = \min_{\alpha(n)>0} \mathsf{R}^{\mathsf{pub}}_{\alpha,\alpha/2}(f) + \log(1/\alpha)$$

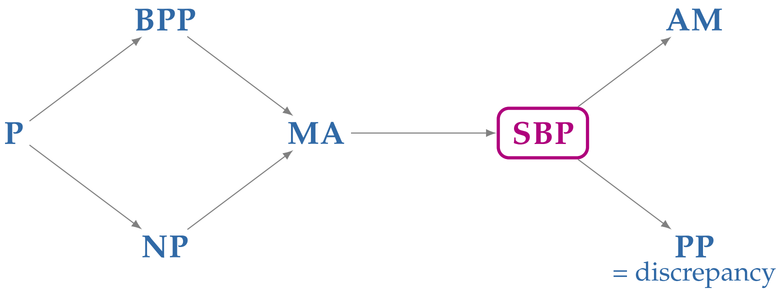
$$\mathbf{USBP}(f) = \min_{\alpha(n)>0} \mathsf{R}^{\mathsf{priv}}_{\alpha,\alpha/2}(f)$$

Compare:

$$\mathbf{PP}(f) = \min_{\epsilon(n)>0} \mathsf{R}^{\mathsf{pub}}_{1/2+\epsilon,1/2-\epsilon}(f) + \log(1/\epsilon)$$

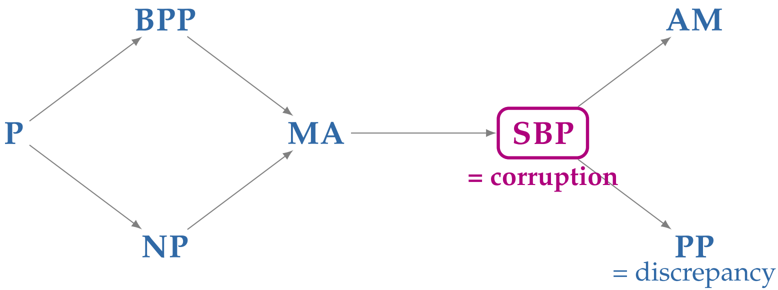
$$\mathbf{UPP}(f) = \min_{\epsilon(n)>0} \mathsf{R}^{\mathsf{priv}}_{1/2+\epsilon,1/2-\epsilon}(f)$$

SBP in context



[Klauck'07]: $\mathbf{PP} = \text{Disc}$
[Klauck'03]: $\mathbf{MA} \subseteq \text{Corr} \subseteq \mathbf{AM}$

SBP in context



[Klauck'07]: $\mathbf{PP} = \text{Disc}$

[Klauck'03]: $\mathbf{MA} \subseteq \text{Corr} \subseteq \mathbf{AM}$

Results for **SBP** and **USBP**

Theorem: $\mathbf{SBP}(f) = \Theta(\mathrm{Corr}(f))$

Results for **SBP** and **USBP**

Theorem: $\mathbf{SBP}(f) = \Theta(\mathrm{Corr}(f))$

Corruption bound:

- Let μ_{yes} and μ_{no} be supported on $f^{-1}(1)$ and $f^{-1}(0)$
- Rectangle R is *1-biased* iff $\mu_{\mathsf{yes}}(R) \geq 2 \cdot \mu_{\mathsf{no}}(R)$
- $\mathrm{Corr}(f, \mu_{\mathsf{yes}}, \mu_{\mathsf{no}}) = \max \Delta$ such that all 1-biased R have size $\mu_{\mathsf{yes}}(R) \leq 2^{-\Delta}$

Results for SBP and USBP

Theorem: $\mathbf{SBP}(f) = \Theta(\mathrm{Corr}(f))$

Corruption bound:

- Let μ_{yes} and μ_{no} be supported on $f^{-1}(1)$ and $f^{-1}(0)$
- Rectangle R is *1-biased* iff $\mu_{\mathsf{yes}}(R) \geq 2 \cdot \mu_{\mathsf{no}}(R)$
- $\mathrm{Corr}(f, \mu_{\mathsf{yes}}, \mu_{\mathsf{no}}) = \max \Delta$ such that all 1-biased R have size $\mu_{\mathsf{yes}}(R) \leq 2^{-\Delta}$
- $\mathrm{Corr}(f) = \max_{\mu_{\mathsf{yes}}, \mu_{\mathsf{no}}} \mathrm{Corr}(f, \mu_{\mathsf{yes}}, \mu_{\mathsf{no}})$

Results for **SBP** and **USBP**

Theorem: $\mathbf{SBP}(f) = \Theta(\mathrm{Corr}(f))$

Corollary: $\mathbf{SBP}(\mathrm{Disj}) = \Omega(n)$ [Razborov'92]

Results for **SBP** and **USBP**

Theorem: $\mathbf{SBP}(f) = \Theta(\mathrm{Corr}(f))$

Corollary: $\mathbf{SBP}(\mathrm{Disj}) = \Omega(n)$ [Razborov'92]

Theorem: $\mathbf{USBP}(\mathrm{Disj}) = \Omega(n)$

Simple proof of main theorem

Proof of $\Omega(n \cdot (1 - \beta/\alpha))$

1. Start with (α, β)-protocol Π
2. **And**-amplify into (α^k, β^k)-protocol Π^k
3. Then Π^k is an **SBP** protocol for $k = (1 - \beta/\alpha)^{-1}$
4. Hence $|\Pi^k| \geq \Omega(n)$
5. Hence $|\Pi| \geq \Omega(n/k) = \Omega(n \cdot (1 - \beta/\alpha))$

Simple proof of main theorem

Proof of $\Omega(n \cdot (1 - \beta/\alpha))$

1. Start with (α, β)-protocol Π
2. **And**-amplify into (α^k, β^k)-protocol Π^k
3. Then Π^k is an **SBP** protocol for $k = (1 - \beta/\alpha)^{-1}$
4. Hence $|\Pi^k| \geq \Omega(n)$
5. Hence $|\Pi| \geq \Omega(n/k) = \Omega(n \cdot (1 - \beta/\alpha))$

Note: And-amplification for nonnegative rank

1. Start with nonnegative matrix M
2. Raise entries to power k
3. Basic fact: $\mathrm{rank}_+(M^{(k)}) \leq \mathrm{rank}_+(M)^k$

Proof ideas (for experts)

Theorem: $\mathbf{SBP}(f) = \Theta(\mathrm{Corr}(f))$

- Analogous to [Klauck'07]
- Uses minimax

Proof ideas (for experts)

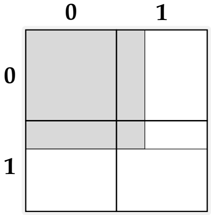
Theorem: $\mathbf{USBP}(\mathrm{Disj}) = \Omega(n)$

- Information complexity framework [Bar-Yossef et al.'04]
- **New challenge:** Transcript useless $1 - \alpha$ of the time
  Solution: Study transcripts conditioned on acceptance
- Cannot prove $\Omega(1)$ info lower bound for 2-bit NAND function!

Proof ideas (for experts)

Theorem: $\mathbf{USBP}(\mathrm{Disj}) = \Omega(n)$

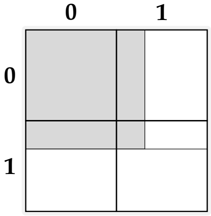
- Information complexity framework [Bar-Yossef et al.'04]
- **New challenge:** Transcript useless $1-\alpha$ of the time
  Solution: Study transcripts conditioned on acceptance
- Cannot prove $\Omega(1)$ info lower bound for 2-bit NAND function!



Proof ideas (for experts)

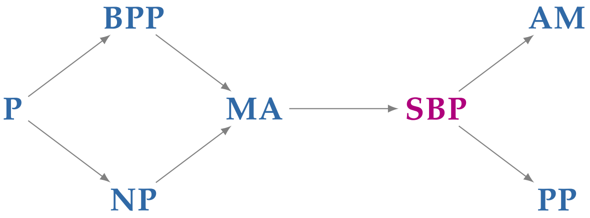
Theorem: $\mathbf{USBP}(\mathrm{Disj}) = \Omega(n)$

- Information complexity framework [Bar-Yossef et al.'04]
- **New challenge:** Transcript useless $1 - \alpha$ of the time
  Solution: Study transcripts conditioned on acceptance
- Cannot prove $\Omega(1)$ info lower bound for 2-bit NAND function!
  Solution: Use a different gadget



	1	2
0	1	1
1	0	1
2	1	0

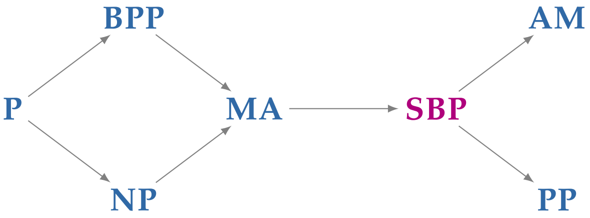
Summary



Future work:

- WIP: Separating **MA** and **SBP** ?
- No ideas: Separating **SBP** and **USBP** ?
- Long standing: Lower bounds for **AM** ?

Summary



Future work:

- WIP: Separating **MA** and **SBP** ?
- No ideas: Separating **SBP** and **USBP** ?
- Long standing: Lower bounds for **AM** ?

Cheers!