Strong XOR Lemma for Communication with Bounded Rounds

Huacheng Yu

Princeton University

n-fold XOR function

For function $f : \mathcal{Z} \to \{0,1\}$, its n-fold XOR $f^{\oplus n} : \mathcal{Z}^n \to \{0,1\}$ is:

$$f^{\oplus n}(Z_1, \ldots, Z_n) = f(Z_1) \oplus \cdots \oplus f(Z_n)$$

n-fold XOR function

For function $f : \mathcal{Z} \to \{0,1\}$, its n-fold XOR $f^{\oplus n} : \mathcal{Z}^n \to \{0,1\}$ is:

$$f^{\oplus n}(Z_1, \dots, Z_n) = f(Z_1) \oplus \cdots \oplus f(Z_n)$$

This talk: "CC of f" vs "CC of $f^{\oplus n}$"

Naive algorithm for $f^{\oplus n}$

Suppose f can be computed using resource C w.p. $2/3$

Compute n copies independently and output their XOR

Naive algorithm for $f^{\oplus n}$

Suppose f can be computed using resource C w.p. $2/3$

Compute n copies independently and output their XOR

Use $n \cdot C$ resource in total, and succeed w.p. $1/2 + \exp(-\Theta(n))$

Naive algorithm for $f^{\oplus n}$

Suppose f can be computed using resource C w.p. $2/3$

Compute n copies independently and output their XOR

Use $n \cdot C$ resource in total, and succeed w.p. $1/2 + \exp(-\Theta(n))$

If this is the best possible, then

- moderately hard Boolean-valued $f \implies$ very hard Boolean-valued $f^{\oplus n}$

Strong XOR lemma

A strong XOR lemma (for a model of computation and a class of functions):
"$f^{\oplus n}$ cannot be computed much better than solving all instances independently"

Strong XOR lemma

A strong XOR lemma (for a model of computation and a class of functions):
"$f^{\oplus n}$ cannot be computed much better than solving all instances independently"

Previous XOR lemmas:

- query complexity [Dru'12, BKLS'20]
- w/o n times more resource: circuit complexity [Yao'82], streaming alg [AN'21]
- w/o exponentially small adv: information complexity [BBCR'10]

Strong XOR lemma

A strong XOR lemma (for a model of computation and a class of functions):
"$f^{\oplus n}$ cannot be computed much better than solving all instances independently"

Previous XOR lemmas:

- query complexity [Dru'12, BKLS'20]
- w/o n times more resource: circuit complexity [Yao'82], streaming alg [AN'21]
- w/o exponentially small adv: information complexity [BBCR'10]
- communication complexity & functions with small discrepancy [Shaltiel'03]
- ...

Main result

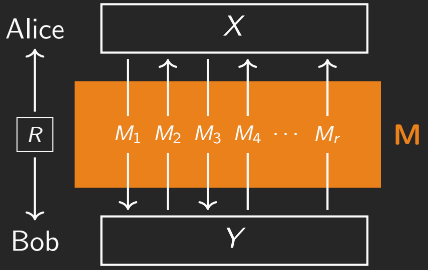
A strong XOR lemma for bounded-round communication...

Main result

A strong XOR lemma for bounded-round communication...

r-round communication for $f(X, Y)$:

- input pair (X, Y), public random bits R
- Alice speaks in odd rounds, Bob speaks in even rounds
- **M** determines the output

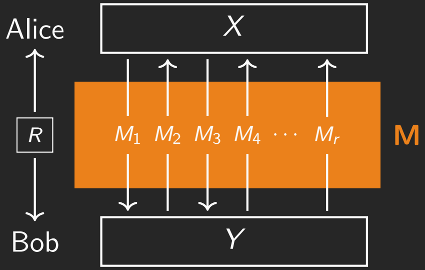


Main result

A strong XOR lemma for bounded-round communication...

r-round communication for $f(X, Y)$:

- input pair (X, Y), public random bits R
- Alice speaks in odd rounds, Bob speaks in even rounds
- **M** determines the output
- cost: $\max \sum_{i=1}^{r} |M_i|$



Main result

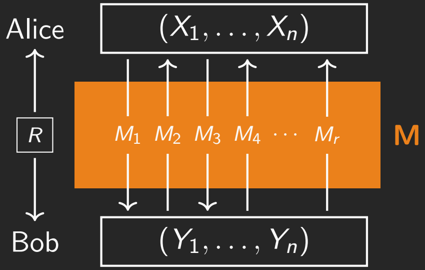
A strong XOR lemma for bounded-round communication...

r-round communication for $f(X, Y)$:

- input pair (X, Y), public random bits R
- Alice speaks in odd rounds, Bob speaks in even rounds
- **M** determines the output
- cost: $\max \sum_{i=1}^{r} |M_i|$

n-fold XOR function:

$$f^{\oplus n}(X_1, \ldots, X_n, Y_1, \ldots, Y_n) \\ = f(X_1, Y_1) \oplus \cdots \oplus f(X_n, Y_n)$$



A strong XOR lemma for bounded-round communication

Let $\mathbf{R}_q^{(r)}(f)$ be the min communication cost to compute f in r rounds with prob q.

Theorem

For any f and r, we must have

$$\mathbf{R}^{(r)}_{1/2+2^{-n}}(f^{\oplus n}) \geq n \cdot \left(r^{-O(r)} \cdot \mathbf{R}^{(r)}_{2/3}(f) - 1\right).$$

A strong XOR lemma for bounded-round communication

Let $\mathbf{R}_q^{(r)}(f)$ be the min communication cost to compute f in r rounds with prob q.

Theorem

For any f and r, we must have

$$\mathbf{R}^{(r)}_{1/2+2^{-n}}(f^{\oplus n}) \geq n \cdot \left(r^{-O(r)} \cdot \mathbf{R}^{(r)}_{2/3}(f) - 1\right).$$

Remarks:

- for constant r: $\mathbf{R}^{(r)}_{1/2+2^{-n}}(f^{\oplus n}) \geq \Omega(n \cdot (\mathbf{R}^{(r)}_{2/3}(f) - O(1)))$

A strong XOR lemma for bounded-round communication

Let $\mathbf{R}_q^{(r)}(f)$ be the min communication cost to compute f in r rounds with prob q.

Theorem

For any f and r, we must have

$$\mathbf{R}^{(r)}_{1/2+2^{-n}}(f^{\oplus n}) \geq n \cdot \left(r^{-O(r)} \cdot \mathbf{R}^{(r)}_{2/3}(f) - 1 \right).$$

Remarks:

- for constant r: $\mathbf{R}^{(r)}_{1/2+2^{-n}}(f^{\oplus n}) \geq \Omega(n \cdot (\mathbf{R}^{(r)}_{2/3}(f) - O(1)))$
- "$-O(1)$" is needed: $f(X_i, Y_i) = X_{i,1} \oplus Y_{i,1}$ (XOR of 1st bit)

A strong XOR lemma for bounded-round communication

Let $\mathbf{R}_q^{(r)}(f)$ be the min communication cost to compute f in r rounds with prob q.

Theorem

For any f and r, we must have

$$\mathbf{R}^{(r)}_{1/2+2^{-n}}(f^{\oplus n}) \geq n \cdot \left(r^{-O(r)} \cdot \mathbf{R}^{(r)}_{2/3}(f) - 1\right).$$

[BBCR'10]: XOR lemma for info complexity
(with const adv instead of 2^{-n})

A strong XOR lemma for bounded-round communication

Let $\mathbf{R}_q^{(r)}(f)$ be the min communication cost to compute f in r rounds with prob q.

Theorem

For any f and r, we must have

$$\mathbf{R}^{(r)}_{1/2+2^{-n}}(f^{\oplus n}) \geq n \cdot \left(r^{-O(r)} \cdot \mathbf{R}^{(r)}_{2/3}(f) - 1\right).$$

[BBCR'10]: XOR lemma for info complexity
(with const adv instead of 2^{-n})

[BR'11]: for const r, information $\Longrightarrow$ communication

A strong XOR lemma for bounded-round communication

Let $\mathbf{R}_q^{(r)}(f)$ be the min communication cost to compute f in r rounds with prob q.

Theorem

For any f and r, we must have

$$\mathbf{R}^{(r)}_{1/2+2^{-n}}(f^{\oplus n}) \geq n \cdot \left(r^{-O(r)} \cdot \mathbf{R}^{(r)}_{2/3}(f) - 1 \right).$$

[BBCR'10]: XOR lemma for info complexity
(with const adv instead of 2^{-n})

[BR'11]: for const r, information $\Longrightarrow$ communication

Imply: for const r, $\mathbf{R}^{(r)}_{2/3}(f^{\oplus n}) \geq \Omega(n \cdot (\mathbf{R}^{(r)}_{2/3}(f) - O(1)))$

A strong XOR lemma for bounded-round communication

Let $\mathbf{R}_q^{(r)}(f)$ be the min communication cost to compute f in r rounds with prob q.

Theorem

For any f and r, we must have

$$\mathbf{R}^{(r)}_{1/2+2^{-n}}(f^{\oplus n}) \geq n \cdot \left(r^{-O(r)} \cdot \mathbf{R}^{(r)}_{2/3}(f) - 1\right).$$

[BBCR'10]: XOR lemma for info complexity $\Longleftarrow$ starting point of our proof
(with const adv instead of 2^{-n})

[BR'11]: for const r, information $\Longrightarrow$ communication

Imply: for const r, $\mathbf{R}^{(r)}_{2/3}(f^{\oplus n}) \geq \Omega(n \cdot (\mathbf{R}^{(r)}_{2/3}(f) - O(1)))$

Distributional strong XOR lemma

We also prove a strong XOR lemma w.r.t. a fixed input distribution μ:

Theorem

If every r-round C-bit comm. protocol computes f under input dist. μ w.p. at most

$$1/2 + \alpha/2,$$

then every r-round $o(r^{-1}nC)$-bit protocol computes $f^{\oplus n}$ under μ^n w.p. at most

$$1/2 + \alpha^{\Omega(n)}/2,$$

where $\alpha < r^{-\omega(r)}$ and $C > \omega(\log(1/\alpha))$.

Distributional strong XOR lemma

We also prove a strong XOR lemma w.r.t. a fixed input distribution μ:

Theorem

If every r-round C-bit comm. protocol computes f under input dist. μ w.p. at most

$$1/2 + \alpha/2,$$

then every r-round $o(r^{-1}nC)$-bit protocol computes $f^{\oplus n}$ under μ^n w.p. at most

$$1/2 + \alpha^{\Omega(n)}/2,$$

where $\alpha < r^{-\omega(r)}$ and $C > \omega(\log(1/\alpha))$.

distributional strong XOR lemma + Yao's minimax + repetition $\Longrightarrow$ main theorem

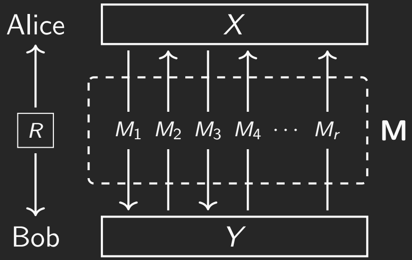
Outline

Rest of the talk, focus on distributional strong XOR lemma:

- alternative view of the XOR lemma for information complexity [BBCR'10]
- obtaining exponentially small advantage

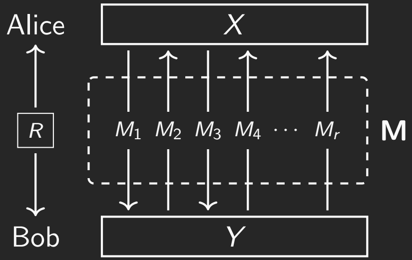
Information complexity

input distribution μ + protocol defines a joint distribution π over $(X, Y, R, \mathbf{M})$...



Information complexity

input distribution μ + protocol defines a joint distribution π over $(X, Y, R, \mathbf{M})$...

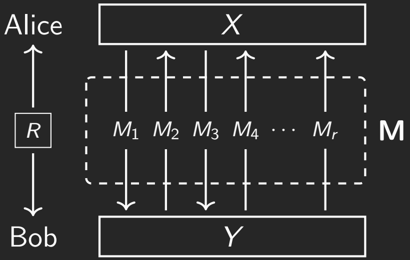


(internal) information cost of π: $I(X; \mathbf{M} \mid Y, R) + I(Y; \mathbf{M} \mid X, R)$

- 1st term: "amt of info $\mathbf{M}$ reveals about X conditioned on everything Bob knows"

Information complexity

input distribution μ + protocol defines a joint distribution π over $(X, Y, R, \mathbf{M})$...



(internal) information cost of π: $I(X; \mathbf{M} \mid Y, R) + I(Y; \mathbf{M} \mid X, R)$

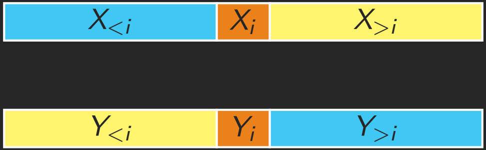
- 1st term: "amt of info $\mathbf{M}$ reveals about X conditioned on everything Bob knows"

information complexity of f under μ: min information cost to compute f

XOR lemma for information complexity [BBCR'10]

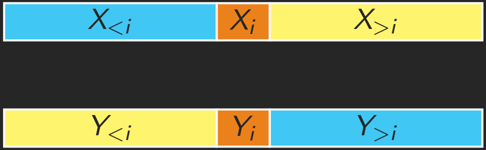
[BBCR'10]: if info complexity of $f^{\oplus n}$ under μ^n is $\leq I$,
then info complexity of f under μ is $\leq I/n + O(1)$

(assuming success probability 1 for now)



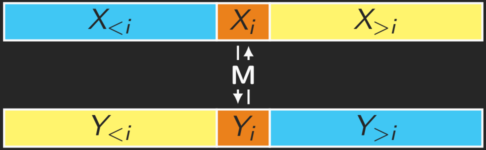
fix π for $f^{\oplus n}$ with info cost I; Protocol τ for $f(x, y)$:

1. sample $i \in [n]$; set $X_i = x$, $Y_i = y$



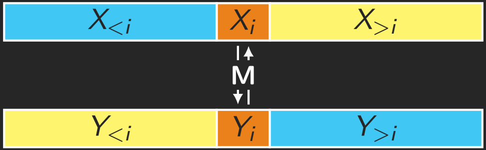
fix π for $f^{\oplus n}$ with info cost I; Protocol τ for $f(x, y)$:

1. sample $i \in [n]$; set $X_i = x$, $Y_i = y$
2. **publicly** sample $X_{>i}$ and $Y_{<i}$
3. Alice **privately** samples $X_{<i}$ cond. on $Y_{<i}$; Bob **priv.** samples $Y_{>i}$ cond. on $X_{>i}$



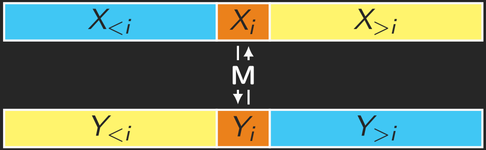
fix π for $f^{\oplus n}$ with info cost I; Protocol τ for $f(x, y)$:

1. sample $i \in [n]$; set $X_i = x$, $Y_i = y$
2. **publicly** sample $X_{>i}$ and $Y_{<i}$
3. Alice **privately** samples $X_{<i}$ cond. on $Y_{<i}$; Bob **priv.** samples $Y_{>i}$ cond. on $X_{>i}$
4. Alice and Bob run π;



fix π for $f^{\oplus n}$ with info cost I; Protocol τ for $f(x, y)$:

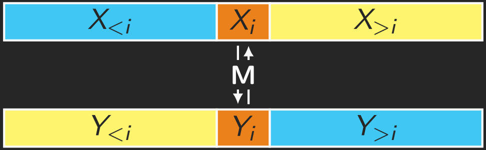
1. sample $i \in [n]$; set $X_i = x$, $Y_i = y$
2. **publicly** sample $X_{>i}$ and $Y_{<i}$
3. Alice **privately** samples $X_{<i}$ cond. on $Y_{<i}$; Bob **priv.** samples $Y_{>i}$ cond. on $X_{>i}$
4. Alice and Bob run π; Alice sends $f^{\oplus i-1}(X_{<i}, Y_{<i})$; Bob sends $f^{\oplus n-i}(X_{>i}, Y_{>i})$



fix π for $f^{\oplus n}$ with info cost I; Protocol τ for $f(x, y)$:

1. sample $i \in [n]$; set $X_i = x$, $Y_i = y$
2. **publicly** sample $X_{>i}$ and $Y_{<i}$
3. Alice **privately** samples $X_{<i}$ cond. on $Y_{<i}$; Bob **priv.** samples $Y_{>i}$ cond. on $X_{>i}$
4. Alice and Bob run π; Alice sends $f^{\oplus i-1}(X_{<i}, Y_{<i})$; Bob sends $f^{\oplus n-i}(X_{>i}, Y_{>i})$

τ computes $f(x, y)$: $f(X_i, Y_i) = f^{\oplus n}(X, Y) \oplus f^{\oplus i-1}(X_{<i}, Y_{<i}) \oplus f^{\oplus n-i}(X_{>i}, Y_{>i})$.

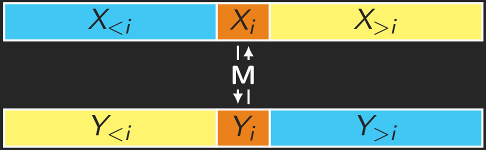


fix π for $f^{\oplus n}$ with info cost I; Protocol τ for $f(x, y)$:

1. sample $i \in [n]$; set $X_i = x$, $Y_i = y$
2. **publicly** sample $X_{>i}$ and $Y_{<i}$
3. Alice **privately** samples $X_{<i}$ cond. on $Y_{<i}$; Bob **priv.** samples $Y_{>i}$ cond. on $X_{>i}$
4. Alice and Bob run π; Alice sends $f^{\oplus i-1}(X_{<i}, Y_{<i})$; Bob sends $f^{\oplus n-i}(X_{>i}, Y_{>i})$

τ computes $f(x, y) : f(X_i, Y_i) = f^{\oplus n}(X, Y) \oplus f^{\oplus i-1}(X_{<i}, Y_{<i}) \oplus f^{\oplus n-i}(X_{>i}, Y_{>i})$.

info cost (1st term): $\mathbb{E}_{i \in [n]}\left[I(X_i; \mathbf{M} \mid X_{>i}, Y, R)\right] + O(1)$

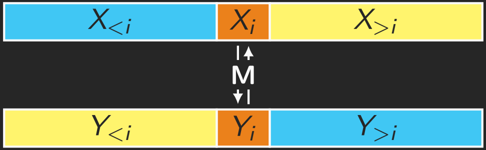


fix π for $f^{\oplus n}$ with info cost I; Protocol τ for $f(x, y)$:

1. sample $i \in [n]$; set $X_i = x$, $Y_i = y$
2. **publicly** sample $X_{>i}$ and $Y_{<i}$
3. Alice **privately** samples $X_{<i}$ cond. on $Y_{<i}$; Bob **priv.** samples $Y_{>i}$ cond. on $X_{>i}$
4. Alice and Bob run π; Alice sends $f^{\oplus i-1}(X_{<i}, Y_{<i})$; Bob sends $f^{\oplus n-i}(X_{>i}, Y_{>i})$

τ computes $f(x, y) : f(X_i, Y_i) = f^{\oplus n}(X, Y) \oplus f^{\oplus i-1}(X_{<i}, Y_{<i}) \oplus f^{\oplus n-i}(X_{>i}, Y_{>i})$.

info cost (1st term): $\mathbb{E}_{i \in [n]} [I(X_i; \mathbf{M} \mid X_{>i}, Y, R)] + O(1) = \frac{1}{n} I(X; \mathbf{M} \mid Y, R) + O(1)$



fix π for $f^{\oplus n}$ with info cost I; Protocol τ for $f(x,y)$:

1. sample $i \in [n]$; set $X_i = x$, $Y_i = y$
2. **publicly** sample $X_{>i}$ and $Y_{<i}$
3. Alice **privately** samples $X_{<i}$ cond. on $Y_{<i}$; Bob **priv.** samples $Y_{>i}$ cond. on $X_{>i}$
4. Alice and Bob run π; Alice sends $f^{\oplus i-1}(X_{<i}, Y_{<i})$; Bob sends $f^{\oplus n-i}(X_{>i}, Y_{>i})$

τ computes $f(x,y) : f(X_i, Y_i) = f^{\oplus n}(X,Y) \oplus f^{\oplus i-1}(X_{<i}, Y_{<i}) \oplus f^{\oplus n-i}(X_{>i}, Y_{>i})$.

info cost (1st term): $\mathbb{E}_{i\in[n]}\left[I(X_i; \mathbf{M} \mid X_{>i}, Y, R)\right] + O(1) = \frac{1}{n} I(X; \mathbf{M} \mid Y, R) + O(1)$

sum up both terms: τ computes f with info cost $I/n + O(1)$

XOR lemma for information complexity [BBCR'10]

[BBCR'10]: <u>if</u> info complexity of $f^{\oplus n}$ under μ^n is $\leq I$,
<u>then</u> info complexity of f under μ is $\leq I/n + O(1)$

XOR lemma for information complexity [BBCR'10]

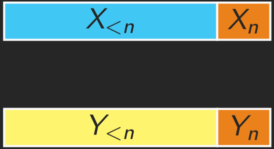
[BBCR'10]: <u>if</u> info complexity of $f^{\oplus n}$ under μ^n is $\leq I$,
<u>then</u> info complexity of f under μ is $\leq I/n + O(1)$

an alternative view of their proof:

- fix π for $f^{\oplus n}$ with info cost I
- "decompose" π into π_n for f and info cost I_1 and
  $\pi_{<n}$ for $f^{\oplus n-1}$ with info cost I_2

  such that $I_1 + I_2 = I + O(1)$

Decomposition of π

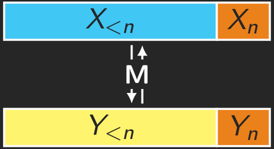


Input: 1 pair

Protocol π_n:

- view input as X_n and Y_n
- publicly sample $Y_{<n}$
- Alice priv. samples $X_{<n}$ cond. on $Y_{<n}$

Decomposition of π

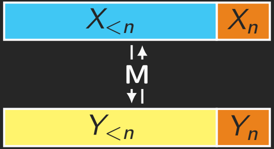


Input: 1 pair

Protocol π_n:

- view input as X_n and Y_n
- publicly sample $Y_{<n}$
- Alice priv. samples $X_{<n}$ cond. on $Y_{<n}$
- run π and A. sends $f^{\oplus n-1}(X_{<n}, Y_{<n})$

Decomposition of π



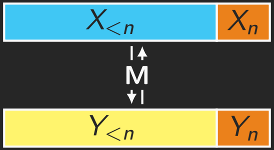
Input: 1 pair

Protocol π_n:

- view input as X_n and Y_n
- publicly sample $Y_{<n}$
- Alice priv. samples $X_{<n}$ cond. on $Y_{<n}$
- run π and A. sends $f^{\oplus n-1}(X_{<n}, Y_{<n})$

Cost: $I(X_n; \mathbf{M} \mid Y, R) + 1$ (1st term)

Decomposition of π

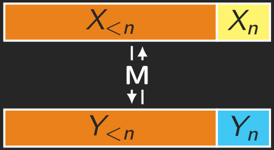


Input: 1 pair

Protocol π_n:

- view input as X_n and Y_n
- publicly sample $Y_{<n}$
- Alice priv. samples $X_{<n}$ cond. on $Y_{<n}$
- run π and A. sends $f^{\oplus n-1}(X_{<n}, Y_{<n})$

Cost: $I(X_n; \mathbf{M} \mid Y, R) + 1$ (1st term)

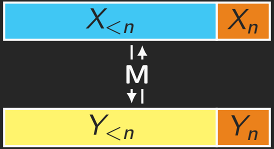


Input: $n-1$ pairs

Protocol $\pi_{<n}$:

- view input as $X_{<n}$ and $Y_{<n}$
- publicly sample X_n
- Bob privately samples Y_n cond. on X_n
- run π and Bob sends $f(X_n, Y_n)$

Decomposition of π

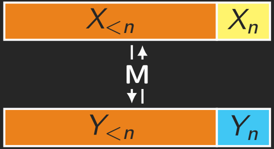


Input: 1 pair

Protocol π_n:

- view input as X_n and Y_n
- publicly sample $Y_{<n}$
- Alice priv. samples $X_{<n}$ cond. on $Y_{<n}$
- run π and A. sends $f^{\oplus n-1}(X_{<n}, Y_{<n})$

Cost: $I(X_n; \mathbf{M} \mid Y, R) + 1$ (1st term)



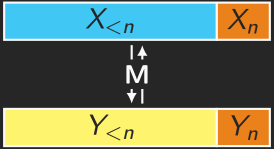
Input: $n-1$ pairs

Protocol $\pi_{<n}$:

- view input as $X_{<n}$ and $Y_{<n}$
- publicly sample X_n
- Bob privately samples Y_n cond. on X_n
- run π and Bob sends $f(X_n, Y_n)$

Cost: $I(X_{<n}; \mathbf{M} \mid X_n, Y, R)$ (1st term)

Decomposition of π

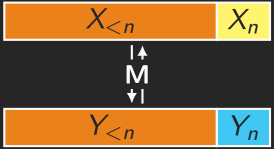


Input: 1 pair

Protocol π_n:

- view input as X_n and Y_n
- publicly sample $Y_{<n}$
- Alice priv. samples $X_{<n}$ cond. on $Y_{<n}$
- run π and A. sends $f^{\oplus n-1}(X_{<n}, Y_{<n})$

Cost: $I(X_n; \mathbf{M} \mid Y, R) + 1$ (1st term)



Input: $n-1$ pairs

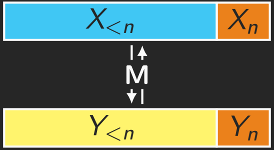
Protocol $\pi_{<n}$:

- view input as $X_{<n}$ and $Y_{<n}$
- publicly sample X_n
- Bob privately samples Y_n cond. on X_n
- run π and Bob sends $f(X_n, Y_n)$

Cost: $I(X_{<n}; \mathbf{M} \mid X_n, Y, R)$ (1st term)

1st terms in costs sum up to $I(X; \mathbf{M} \mid Y, R) + 1$ by chain rule

Decomposition of π

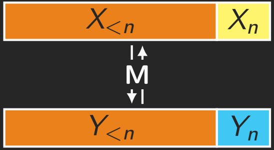


Input: 1 pair

Protocol π_n:

- view input as X_n and Y_n
- publicly sample $Y_{<n}$
- Alice priv. samples $X_{<n}$ cond. on $Y_{<n}$
- run π and A. sends $f^{\oplus n-1}(X_{<n}, Y_{<n})$

Cost: $I(X_n; \mathbf{M} \mid Y, R) + 1$ (1st term)



Input: $n-1$ pairs

Protocol $\pi_{<n}$:

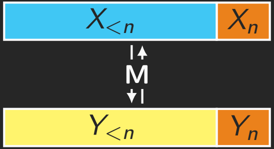
- view input as $X_{<n}$ and $Y_{<n}$
- publicly sample X_n
- Bob privately samples Y_n cond. on X_n
- run π and Bob sends $f(X_n, Y_n)$

Cost: $I(X_{<n}; \mathbf{M} \mid X_n, Y, R)$ (1st term)

1st terms in costs sum up to $I(X; \mathbf{M} \mid Y, R) + 1$ by chain rule

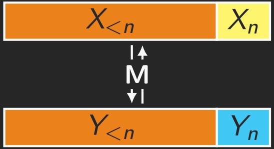
2nd term is similar; info costs of $\pi_{<n}$ and π_n sum up to $I + O(1)$

Decomposition of π



Input: 1 pair

Protocol π_n



Input: $n-1$ pairs

Protocol $\pi_{<n}$

iteratively decomposing $\pi_{<n}$ gives n protocols for f

- i-th last: the original protocol when it embeds input into (X_i, Y_i)

Another view of decomposition of π

for the same underlying distribution of $(X, Y, R, \mathbf{M})$, we view different parts of it as inputs, public randomness, transcript (private randomness not important)

- π: inputs (X, Y), public randomness R, transcript $\mathbf{M}$
- π_n: inputs (X_n, Y_n), public rand. $(R, Y_{<n})$, transcript $(\mathbf{M}, f^{\oplus n-1}(X_{<n}, Y_{<n}))$
- $\pi_{<n}$: inputs $(X_{<n}, Y_{<n})$, public randomness (R, X_n), transcript $(\mathbf{M}, f(X_n, Y_n))$

Exponentially small advantage

given a protocol computing $f^{\oplus n}$ w.p. $2/3$ under μ^n with cost $o(nC)$

then there is a protocol computing f w.p. $2/3$ under μ with cost $\leq C$

Exponentially small advantage

To prove strong XOR lemma, need to show:

given a protocol computing $f^{\oplus n}$ w.p. $1/2 + \alpha^{o(n)}/2$ under μ^n with cost $o(nC)$

then there is a protocol computing f w.p. $1/2 + \alpha/2$ under μ with cost $\leq C$

Exponentially small advantage

To prove strong XOR lemma, need to show:

given a protocol computing $f^{\oplus n}$ w.p. $1/2+\alpha^{o(n)}/2$ under μ^n with cost $o(nC)$

then there is a protocol computing f w.p. $1/2+\alpha/2$ under μ with cost $\leq C$

Main challenge: design a decomposition that increases the advantage

Benefit of the alternative view

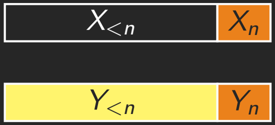
let $\mathrm{adv}(f \mid \mathbf{W}) := |2\Pr[f = 1 \mid \mathbf{W}] - 1| \in [0, 1]$ be the advantage for f cond. on $\mathbf{W}$

- given $\mathbf{W}$, one can predict f w.p. $1/2 + \mathrm{adv}(f \mid \mathbf{W})/2$
- $\mathrm{adv}(b_1 \oplus b_2) = \mathrm{adv}(b_1) \cdot \mathrm{adv}(b_2)$

let $\mathrm{adv}(f \mid \mathbf{W}) := |2\Pr[f = 1 \mid \mathbf{W}] - 1| \in [0, 1]$ be the advantage for f cond. on $\mathbf{W}$

- given $\mathbf{W}$, one can predict f w.p. $1/2 + \mathrm{adv}(f \mid \mathbf{W})/2$
- $\mathrm{adv}(b_1 \oplus b_2) = \mathrm{adv}(b_1) \cdot \mathrm{adv}(b_2)$

End of π_n, Alice knows $(X_n, Y_{<n}, R, \mathbf{M})$



: input, : public

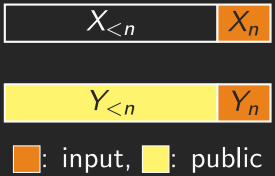
$\mathrm{adv}(f(X_n, Y_n) \mid X_n, Y_{<n}, R, \mathbf{M})$

Benefit of the alternative view

let $\operatorname{adv}(f \mid \mathbf{W}) := |2\Pr[f = 1 \mid \mathbf{W}] - 1| \in [0, 1]$ be the advantage for f cond. on $\mathbf{W}$

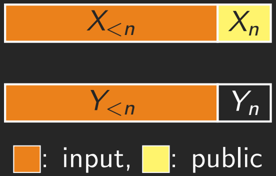
- given $\mathbf{W}$, one can predict f w.p. $1/2 + \operatorname{adv}(f \mid \mathbf{W})/2$
- $\operatorname{adv}(b_1 \oplus b_2) = \operatorname{adv}(b_1) \cdot \operatorname{adv}(b_2)$

End of π_n, Alice knows $(X_n, Y_{<n}, R, \mathbf{M})$



$\operatorname{adv}(f(X_n, Y_n) \mid X_n, Y_{<n}, R, \mathbf{M})$

End of $\pi_{<n}$, Bob knows $(X_n, Y_{<n}, R, \mathbf{M})$



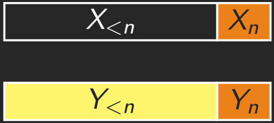
$\operatorname{adv}(f^{\oplus n-1}(X_{<n}, Y_{<n}) \mid X_n, Y_{<n}, R, \mathbf{M})$

Benefit of the alternative view

let $\mathrm{adv}(f \mid \mathbf{W}) := |2\Pr[f = 1 \mid \mathbf{W}] - 1| \in [0,1]$ be the advantage for f cond. on $\mathbf{W}$

- given $\mathbf{W}$, one can predict f w.p. $1/2 + \mathrm{adv}(f \mid \mathbf{W})/2$
- $\mathrm{adv}(b_1 \oplus b_2) = \mathrm{adv}(b_1) \cdot \mathrm{adv}(b_2)$

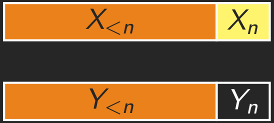
End of π_n, Alice knows $(X_n, Y_{<n}, R, \mathbf{M})$



■: input, ■: public

$\mathrm{adv}(f(X_n, Y_n) \mid X_n, Y_{<n}, R, \mathbf{M})$

End of $\pi_{<n}$, Bob knows $(X_n, Y_{<n}, R, \mathbf{M})$

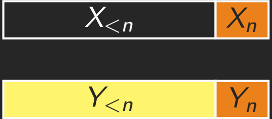


■: input, ■: public

$\mathrm{adv}(f^{\oplus n-1}(X_{<n}, Y_{<n}) \mid X_n, Y_{<n}, R, \mathbf{M})$

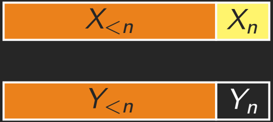
Key obs: $f(X_n, Y_n)$ and $f^{\oplus n-1}(X_{<n}, Y_{<n})$ are independent cond. on $(X_n, Y_{<n}, R, \mathbf{M})$

Benefit of the alternative view



: input, : public

$\mathrm{adv}(f(X_n, Y_n) \mid X_n, Y_{<n}, R, \mathbf{M})$

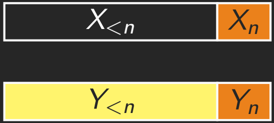


: input, : public

$\mathrm{adv}(f^{\oplus n-1}(X_{<n}, Y_{<n}) \mid X_n, Y_{<n}, R, \mathbf{M})$

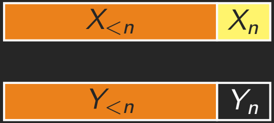
Key obs: $f(X_n, Y_n)$ and $f^{\oplus n-1}(X_{<n}, Y_{<n})$ are independent cond. on $(X_n, Y_{<n}, R, \mathbf{M})$

Benefit of the alternative view



: input, : public

$\mathrm{adv}(f(X_n, Y_n) \mid X_n, Y_{<n}, R, \mathbf{M})$



: input, : public

$\mathrm{adv}(f^{\oplus n-1}(X_{<n}, Y_{<n}) \mid X_n, Y_{<n}, R, \mathbf{M})$

Key obs: $f(X_n, Y_n)$ and $f^{\oplus n-1}(X_{<n}, Y_{<n})$ are independent cond. on $(X_n, Y_{<n}, R, \mathbf{M})$

Since $f^{\oplus n}(X, Y) = f^{\oplus n-1}(X_{<n}, Y_{<n}) \oplus f(X_n, Y_n)$,

$$\mathrm{adv}(f(X_n, Y_n) \mid X_n, Y_{<n}, R, \mathbf{M}) \cdot \mathrm{adv}(f^{\oplus n-1}(X_{<n}, Y_{<n}) \mid X_n, Y_{<n}, R, \mathbf{M})$$
$$= \mathrm{adv}(f^{\oplus n}(X, Y) \mid X_n, Y_{<n}, R, \mathbf{M})$$

Pointwise equality for advantage

let $\mathrm{adv}(f \mid \mathbf{W}) := |2\Pr[f = 1 \mid \mathbf{W}] - 1| \in [0,1]$ be the advantage for f cond. on $\mathbf{W}$

$$\begin{aligned}
&\mathrm{adv}(f(X_n, Y_n) \mid X_n, Y_{<n}, R, \mathbf{M}) \cdot \mathrm{adv}(f^{\oplus n-1}(X_{<n}, Y_{<n}) \mid X_n, Y_{<n}, R, \mathbf{M}) \\
&\quad = \mathrm{adv}(f^{\oplus n}(X, Y) \mid X_n, Y_{<n}, R, \mathbf{M})
\end{aligned}$$

Pointwise equality for advantage

let $\mathrm{adv}(f \mid \mathbf{W}) := |2\Pr[f = 1 \mid \mathbf{W}] - 1| \in [0,1]$ be the advantage for f cond. on $\mathbf{W}$

$$\begin{aligned} &\mathrm{adv}(f(X_n, Y_n) \mid X_n, Y_{<n}, R, \mathbf{M}) \cdot \mathrm{adv}(f^{\oplus n-1}(X_{<n}, Y_{<n}) \mid X_n, Y_{<n}, R, \mathbf{M}) \\ &\quad = \mathrm{adv}(f^{\oplus n}(X, Y) \mid X_n, Y_{<n}, R, \mathbf{M}) \end{aligned}$$

Relate adv of π_n and adv of $\pi_{<n}$ to adv of π

Pointwise equality for advantage

let $\mathrm{adv}(f \mid \mathbf{W}) := |2\Pr[f = 1 \mid \mathbf{W}] - 1| \in [0, 1]$ be the advantage for f cond. on $\mathbf{W}$

$$\begin{aligned}\mathrm{adv}(f(X_n, Y_n) \mid X_n, Y_{<n}, R, \mathbf{M}) \cdot \mathrm{adv}(f^{\oplus n-1}(X_{<n}, Y_{<n}) \mid X_n, Y_{<n}, R, \mathbf{M}) \\ = \mathrm{adv}(f^{\oplus n}(X, Y) \mid X_n, Y_{<n}, R, \mathbf{M})\end{aligned}$$

Relate adv of π_n and adv of $\pi_{<n}$ to adv of π

If π_n does not have "high success prob", then adv of $\pi_{<n}$ is larger than adv of π by a factor

Pointwise equality for advantage

let $\mathrm{adv}(f \mid \mathbf{W}) := |2\Pr[f = 1 \mid \mathbf{W}] - 1| \in [0, 1]$ be the advantage for f cond. on $\mathbf{W}$

$$\begin{aligned} &\mathrm{adv}(f(X_n, Y_n) \mid X_n, Y_{<n}, R, \mathbf{M}) \cdot \mathrm{adv}(f^{\oplus n-1}(X_{<n}, Y_{<n}) \mid X_n, Y_{<n}, R, \mathbf{M}) \\ &\quad = \mathrm{adv}(f^{\oplus n}(X, Y) \mid X_n, Y_{<n}, R, \mathbf{M}) \end{aligned}$$

Relate adv of π_n and adv of $\pi_{<n}$ to adv of π

If π_n does not have "high success prob", then adv of $\pi_{<n}$ is larger than adv of π by a factor

- decomposition increases the advantage

High-level proof strategy

Proof strategy:

1. given π for $f^{\oplus n}$, decompose into π_n for f and $\pi_{<n}$ for $f^{\oplus n-1}$
2. prove:
    2.1 if π_n has “high cost”: $\pi_{<n}$ has much “lower cost” than π
    2.2 if π_n has “low succ prob”: $\pi_{<n}$ has much “higher adv” than π

High-level proof strategy

Proof strategy:

1. given π for $f^{\oplus n}$, decompose into π_n for f and $\pi_{<n}$ for $f^{\oplus n-1}$
2. prove:
   2.1 if π_n has "high cost": $\pi_{<n}$ has much "lower cost" than π
   2.2 if π_n has "low succ prob": $\pi_{<n}$ has much "higher adv" than π

   o.w. π_n is good

High-level proof strategy

Proof strategy:

1. given π for $f^{\oplus n}$, decompose into π_n for f and $\pi_{<n}$ for $f^{\oplus n-1}$
2. prove:
   2.1 if π_n has "high cost": $\pi_{<n}$ has much "lower cost" than π
   2.2 if π_n has "low succ prob": $\pi_{<n}$ has much "higher adv" than π

   o.w. π_n is good
3. if π has "low cost" and non-trivial adv: iterative decomposition gives a good protocol for f

"Exponential version" of info cost

Strong XOR lemma is false for info complexity

- compute $f^{\oplus n}$ exactly w.p. $1/n$; output random bit w.p. $1 - 1/n$

“Exponential version” of info cost

Strong XOR lemma is false for info complexity

- compute $f^{\oplus n}$ exactly w.p. $1/n$; output random bit w.p. $1 - 1/n$

Information cost is an average measure: it lower-bounds the expected communication

- (1st term) $I_\pi(X; \mathbf{M} \mid Y, R) = \mathbb{E}\left[\log\left(\frac{\pi(X|\mathbf{M}, Y, R)}{\pi(X|Y, R)}\right)\right]$

“Exponential version” of info cost

Strong XOR lemma is false for info complexity

- compute $f^{\oplus n}$ exactly w.p. $1/n$; output random bit w.p. $1 - 1/n$

Information cost is an average measure: it lower-bounds the expected communication

- (1st term) $I_\pi(X; \mathbf{M} \mid Y, R) = \mathbb{E}\left[\log\left(\frac{\pi(X|\mathbf{M},Y,R)}{\pi(X|Y,R)}\right)\right]$

We work with the “exponential version” χ^2-cost:

$$\mathbb{E}\left[\frac{\pi(X \mid \mathbf{M}, Y, R)}{\pi(X \mid Y, R)}\right]$$

“Exponential version” of info cost

Strong XOR lemma is false for info complexity

- compute $f^{\oplus n}$ exactly w.p. $1/n$; output random bit w.p. $1 - 1/n$

Information cost is an average measure: it lower-bounds the expected communication

- (1st term) $I_\pi(X; \mathbf{M} \mid Y, R) = \mathbb{E}\left[\log\left(\frac{\pi(X|\mathbf{M},Y,R)}{\pi(X|Y,R)}\right)\right]$

We work with the “exponential version” χ^2-cost:

$$\mathbb{E}\left[\frac{\pi(X \mid \mathbf{M}, Y, R)}{\pi(X \mid Y, R)}\right]$$

- instead of proving info cost $\leq I$, we prove χ^2-cost $\leq 2^{O(I)}$:
  provide strong concentration on $\log\left(\frac{\pi(X|\mathbf{M},Y,R)}{\pi(X|Y,R)}\right)$

“Exponential version” of info cost

Strong XOR lemma is false for info complexity

- compute $f^{\oplus n}$ exactly w.p. $1/n$; output random bit w.p. $1-1/n$

Information cost is an average measure: it lower-bounds the expected communication

- (1st term) $I_\pi(X;\mathbf{M}\mid Y,R) = \mathbb{E}\left[\log\left(\frac{\pi(X|\mathbf{M},Y,R)}{\pi(X|Y,R)}\right)\right]$

We work with the “exponential version” χ^2-cost:

$$\mathbb{E}\left[\frac{\pi(X\mid\mathbf{M},Y,R)}{\pi(X\mid Y,R)}\right]$$

- instead of proving info cost $\leq I$, we prove χ^2-cost $\leq 2^{O(I)}$: provide strong concentration on $\log\left(\frac{\pi(X|\mathbf{M},Y,R)}{\pi(X|Y,R)}\right)$
- a pointwise version of chain-rule holds

Open problems

Given a protocol π computing $f^{\oplus n}$ with const prob

- obtain a protocol computing f w.p. $1 - O(1/n)$?

Open problems

Given a protocol π computing $f^{\oplus n}$ with const prob

- obtain a protocol computing f w.p. $1 - O(1/n)$?

General communication without round restrictions?

Open problems

Given a protocol π computing $f^{\oplus n}$ with const prob

- obtain a protocol computing f w.p. $1 - O(1/n)$?

General communication without round restrictions?

More applications of χ^2-costs

- strong concentration on $\log\left(\frac{\pi(X|\mathbf{M},Y,R)}{\pi(X|Y,R)}\right) \implies$ small overhead when doing information-compression

Open problems

Given a protocol π computing $f^{\oplus n}$ with const prob

- obtain a protocol computing f w.p. $1 - O(1/n)$?

General communication without round restrictions?

More applications of χ^2-costs

- strong concentration on $\log\left(\frac{\pi(X|\mathbf{M},Y,R)}{\pi(X|Y,R)}\right) \implies$ small overhead when doing information-compression

Understand the relation between χ^2-costs and communication?

Open problems

Given a protocol π computing $f^{\oplus n}$ with const prob

- obtain a protocol computing f w.p. $1 - O(1/n)$?

General communication without round restrictions?

More applications of χ^2-costs

- strong concentration on $\log\left(\frac{\pi(X|\mathbf{M},Y,R)}{\pi(X|Y,R)}\right) \implies$ small overhead when doing information-compression

Understand the relation between χ^2-costs and communication?

Thank you for listening!