A Lifting Theorem with Applications to Symmetric Functions

Nikhil Mande

TIFR, Mumbai

Joint work with Arkadev Chattopadhyay (TIFR)

Outline of talk

Definition and examples

Definition and examples

- A function $f : \{-1,1\}^n \to \{-1,1\}$ is said to be *symmetric* if its value only depends on the Hamming weight of the input.

Definition and examples

- A function $f : \{-1,1\}^n \to \{-1,1\}$ is said to be *symmetric* if its value only depends on the Hamming weight of the input.
- i.e. $f(x) = f(\sigma(x))$ for all $\sigma \in S_n$.

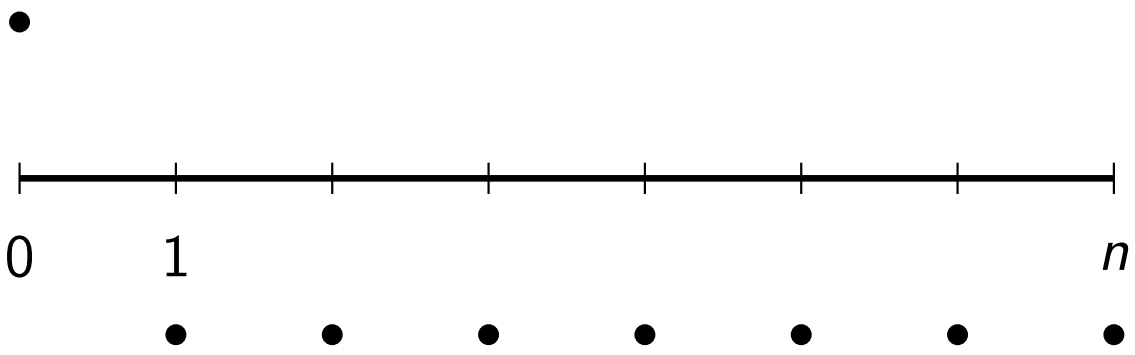
Definition and examples

- A function $f : \{-1,1\}^n \to \{-1,1\}$ is said to be *symmetric* if its value only depends on the Hamming weight of the input.
- i.e. $f(x) = f(\sigma(x))$ for all $\sigma \in S_n$.
- Induces the spectrum (predicate) $D_f : \{0\} \cup [n] \to \{-1,1\}$.

Definition and examples

- A function $f : \{-1,1\}^n \to \{-1,1\}$ is said to be *symmetric* if its value only depends on the Hamming weight of the input.
- i.e. $f(x) = f(\sigma(x))$ for all $\sigma \in S_n$.
- Induces the spectrum (predicate) $D_f : \{0\} \cup [n] \to \{-1,1\}$.

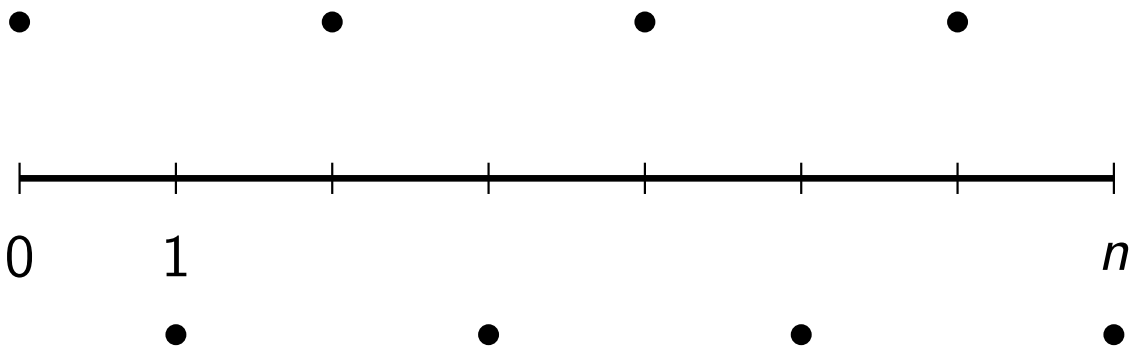
- Example: Or.



Definition and examples

- A function $f : \{-1,1\}^n \to \{-1,1\}$ is said to be *symmetric* if its value only depends on the Hamming weight of the input.
- i.e. $f(x) = f(\sigma(x))$ for all $\sigma \in S_n$.
- Induces the spectrum (predicate) $D_f : \{0\} \cup [n] \to \{-1,1\}$.

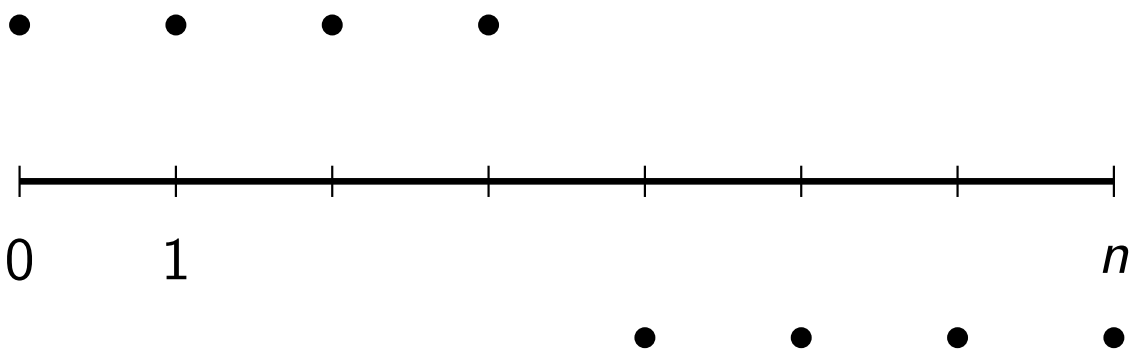
- Example: Parity.



Definition and examples

- A function $f : \{-1,1\}^n \to \{-1,1\}$ is said to be *symmetric* if its value only depends on the Hamming weight of the input.
- i.e. $f(x) = f(\sigma(x))$ for all $\sigma \in S_n$.
- Induces the spectrum (predicate) $D_f : \{0\} \cup [n] \to \{-1,1\}$.

- Example: Majority.



Sign degree (monomial complexity)

Sign degree (monomial complexity)

Definition (Sign degree (monomial complexity))

$\deg_{\pm}(f)$ $(\mathrm{mon}_{\pm}(f))$ = min degree (number of monomials) required by a real polynomial p such that $p(x)f(x) > 0$ for all $x \in \{-1,1\}^n$.

Sign degree (monomial complexity)

Definition (Sign degree (monomial complexity))

$\deg_{\pm}(f)$ $(\mathrm{mon}_{\pm}(f))$ = min degree (number of monomials) required by a real polynomial p such that $p(x)f(x) > 0$ for all $x \in \{-1,1\}^n$.

- The sign degree of a symmetric function equals $|i \in \{0\} \cup [n-1] : D_f(i) \neq D_f(i+1)|$.

Sign degree (monomial complexity)

Definition (Sign degree (monomial complexity))

$\deg_{\pm}(f)$ ($\mathrm{mon}_{\pm}(f)$) = min degree (number of monomials) required by a real polynomial p such that $p(x)f(x) > 0$ for all $x \in \{-1,1\}^n$.

- The sign degree of a symmetric function equals $|i \in \{0\} \cup [n-1] : D_f(i) \neq D_f(i+1)|$.
- Example: $\deg_{\pm}(\text{Parity}) = n$, $\deg_{\pm}(\text{Majority}) = 1$.

Approximate degree (weight)

Approximate degree (weight)

Definition (Weight of a polynomial)

Let $p : \{-1,1\}^n \to \mathbb{R}$ be given uniquely by $p = \sum_{S \subseteq [n]} \hat{p}(S) x_S$. Define $\mathrm{wt}(p) = \sum_{S \subseteq [n]} |\hat{p}(S)|$.

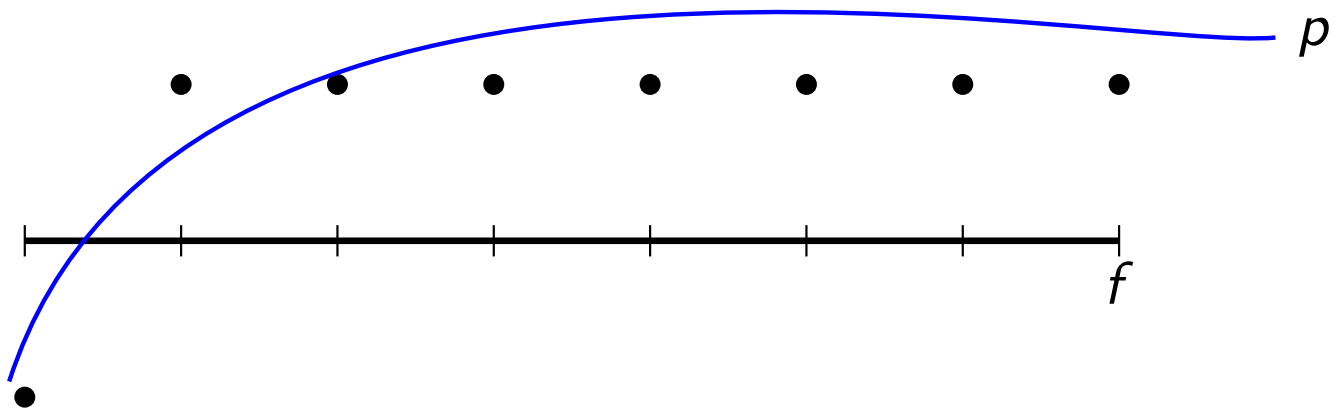
Approximate degree (weight)

Definition (Weight of a polynomial)

Let $p : \{-1,1\}^n \to \mathbb{R}$ be given uniquely by $p = \sum_{S \subseteq [n]} \hat{p}(S) x_S$. Define $\mathrm{wt}(p) = \sum_{S \subseteq [n]} |\hat{p}(S)|$.

Definition (Approximate degree (weight))

$\deg_{1/3}(f)$ ($\mathrm{wt}_{1/3}(f)$) = min degree (weight) required by a real polynomial p such that $|p(x) - f(x)| \leq 1/3$ for all $x \in \{-1,1\}^n$.



Measures of symmetric functions

Measures of symmetric functions

Definition (Odd-even degree)

$$\deg_{oe}(f) = |i \in \{0, 1, \ldots, n-2\} : D_f(i) \neq D_f(i+2)|.$$

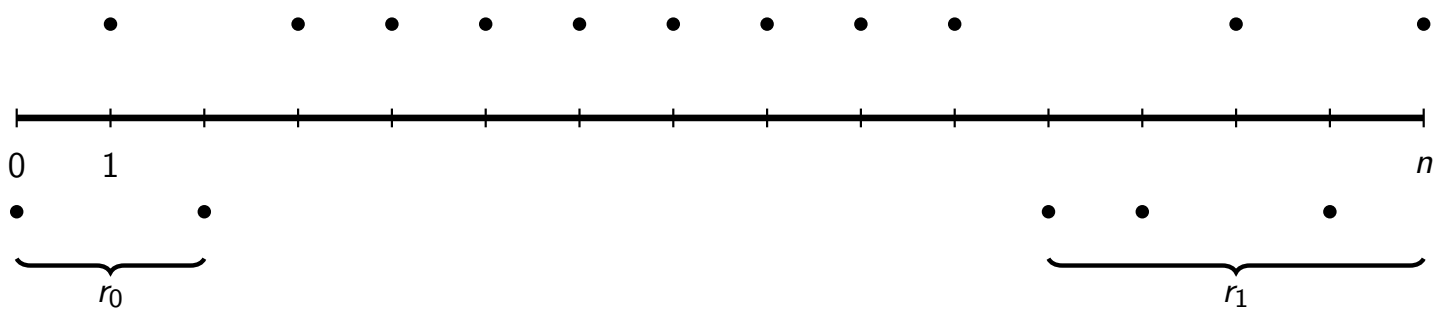
Measures of symmetric functions

Definition (Odd-even degree)

$$\deg_{oe}(f) = |i \in \{0, 1, \ldots, n-2\} : D_f(i) \neq D_f(i+2)|.$$

Definition

Let $F : \{-1,1\}^n \to \{-1,1\}$ be a symmetric function. Define r_0, r_1 to be the min integers such that $r_0, r_1 \leq n/2$ and $D_F(i) = D_F(i+2)$ for all $i \in [r_0, n - r_1)$. Define $r(F) = \max\{r_0, r_1\}$.



Known results for symmetric functions

Known results for symmetric functions

Theorem ([Paturi'92])

For any symmetric function $f : \{-1,1\}^n \to \{-1,1\}$, *define the quantity* $\Gamma(f) = \min_{0 \le k \le n-1} \{|2k - n + 1| : D_f(k) \neq D_f(k+1)\}$. *Then*

$$\deg_{1/3}(f) = \Theta\left(\sqrt{n(n - \Gamma(f))}\right).$$

Known results for symmetric functions

Theorem ([Paturi'92])

For any symmetric function $f : \{-1,1\}^n \to \{-1,1\}$, *define the quantity* $\Gamma(f) = \min_{0 \le k \le n-1} \{|2k - n + 1| : D_f(k) \neq D_f(k+1)\}$. *Then*

$$\deg_{1/3}(f) = \Theta\left(\sqrt{n(n - \Gamma(f))}\right).$$

Theorem ([AFH'12])

For any symmetric function $f : \{-1,1\}^n \to \{-1,1\}$,

$$\log(wt(f)) = \Theta\left(r(f) \log\left(\frac{n}{r(f)}\right)\right).$$

This work

Theorem (Main conjecture in [AFH'12])

Let $F : \{-1,1\}^{4n} \to \{-1,1\}$ *be any symmetric function. Then*

$$\log(wt_{1/3}(F)) = \Omega(r(F)).$$

This work

Theorem (Main conjecture in [AFH'12])

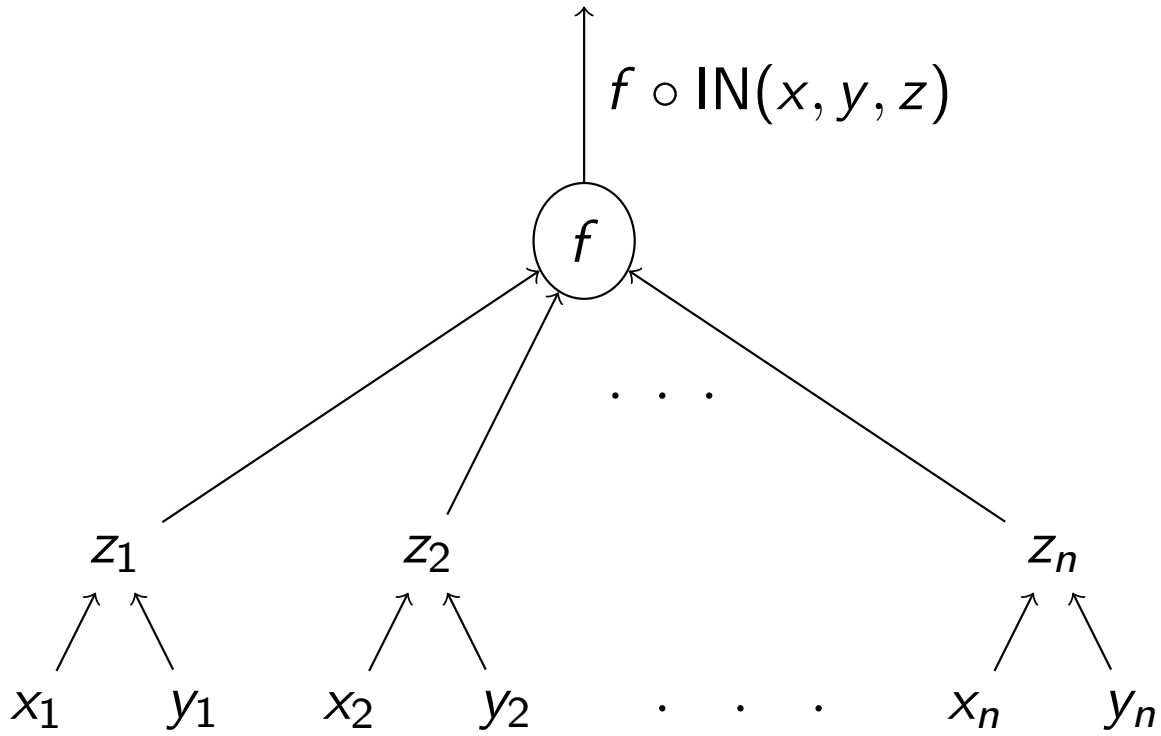
Let $F : \{-1,1\}^{4n} \to \{-1,1\}$ *be any symmetric function. Then*

$$\log(wt_{1/3}(F)) = \Omega(r(F)).$$

(Also proved subsequently by [AFK'17], using different techniques).

The gadget: Indexing

The gadget: Indexing



z_i 'selects' one of x_i and y_i as ith input to f.

Lifting theorem

Lifting theorem

$$\deg_{1/3} \geq d \longrightarrow \mathrm{wt}_{1/3} \geq 2^{\Omega(d)}$$

no degree d approximation to error $1 - 1/2^d$ $\longrightarrow$ 'polynomial margin' of f at most $1/2^{\Omega(d)}$

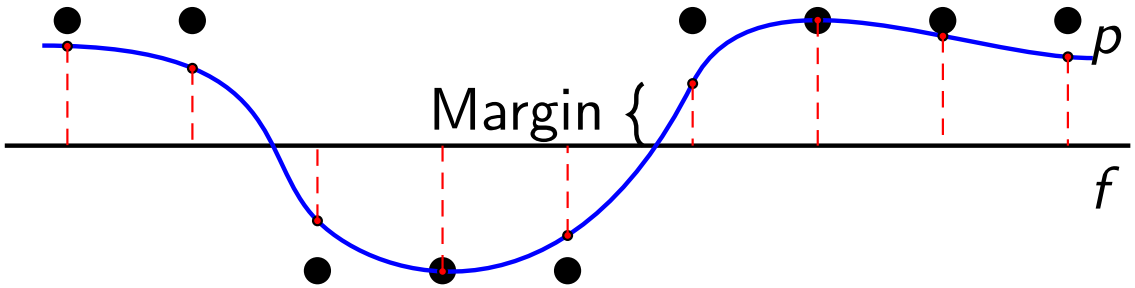
$$\deg_{\pm} \geq d \xrightarrow{\text{[KP'97]}} \mathrm{mon}_{\pm} \geq 2^d$$

Lifting theorem

$$\deg_{1/3} \geq d \longrightarrow \mathrm{wt}_{1/3} \geq 2^{\Omega(d)}$$

no degree d approximation to error $1 - 1/2^d$ $\longrightarrow$ 'polynomial margin' of f at most $1/2^{\Omega(d)}$

$$\deg_{\pm} \geq d \xrightarrow{\text{[KP'97]}} \mathrm{mon}_{\pm} \geq 2^d$$



Monomial projection

Monomial projection

Definition (Monomial projection)

We call a function $g : \{-1,1\}^m \to \{-1,1\}$ a *monomial projection* of a function $f : \{-1,1\}^n \to \{-1,1\}$ if $g(x_1,\ldots,x_m) = f(M_1,\ldots,M_n)$, where each M_i is a monomial in the variables $x_1,\ldots,x_m$.

Monomial projection

Definition (Monomial projection)

We call a function $g : \{-1,1\}^m \to \{-1,1\}$ a *monomial projection* of a function $f : \{-1,1\}^n \to \{-1,1\}$ if $g(x_1,\ldots,x_m) = f(M_1,\ldots,M_n)$, where each M_i is a monomial in the variables $x_1,\ldots,x_m$.

Observation (Projections preserve monomial/weight properties)

For any functions $f : \{-1,1\}^n \to \{-1,1\}$ and $g : \{-1,1\}^m \to \{-1,1\}$ such that g is a monomial projection of f,

$$\mathrm{mon}_{\pm}(g) \leq \mathrm{mon}_{\pm}(f), \qquad \mathrm{wt}(g) \leq \mathrm{wt}(f),$$
$$\mathrm{wt}_{1/3}(g) \leq \mathrm{wt}_{1/3}(f), \qquad m(f) \leq m(g).$$

Projections of symmetric functions

Projections of symmetric functions

Lemma (Projection Lemma)

Given predicate $D_F : [4n] \to \{-1, 1\}$, *consider the predicate* $D_f(b) = D_F(2b + n)$ *for all* $b \in \{0, 1, \ldots, n\}$. *Then* $f \circ \mathsf{IN}$ *is a monomial projection of* F.

Projections of symmetric functions

Lemma (Projection Lemma)

Given predicate $D_F : [4n] \to \{-1, 1\}$, consider the predicate $D_f(b) = D_F(2b + n)$ for all $b \in \{0, 1, \ldots, n\}$. Then $f \circ \mathsf{IN}$ is a monomial projection of F.

Proof idea: Define $g : \{-1, 1\}^{3n} \to \{-1, 1\}$ as follows.

$$g(x_1, \ldots x_n, y_1, \ldots, y_n, z_1, \ldots, z_n) = F(x_1, \ldots, x_n, y_1, \ldots, y_n, -x_1 z_1, \ldots, -x_n z_n, y_1 z_1, \ldots, y_n z_n).$$

Projections of symmetric functions

Lemma (Projection Lemma)

Given predicate $D_F : [4n] \to \{-1, 1\}$, consider the predicate $D_f(b) = D_F(2b + n)$ for all $b \in \{0, 1, \ldots, n\}$. Then $f \circ \mathsf{IN}$ is a monomial projection of F.

Proof idea: Define $g : \{-1, 1\}^{3n} \to \{-1, 1\}$ as follows.

$$g(x_1, \ldots x_n, y_1, \ldots, y_n, z_1, \ldots, z_n) = F(x_1, \ldots, x_n, y_1, \ldots, y_n, -x_1 z_1, \ldots, -x_n z_n, y_1 z_1, \ldots, y_n z_n).$$

Clearly, g is a monomial projection of F.

Projections of symmetric functions

Lemma (Projection Lemma)

Given predicate $D_F : [4n] \to \{-1, 1\}$, consider the predicate $D_f(b) = D_F(2b + n)$ for all $b \in \{0, 1, \ldots, n\}$. Then $f \circ \mathsf{IN}$ is a monomial projection of F.

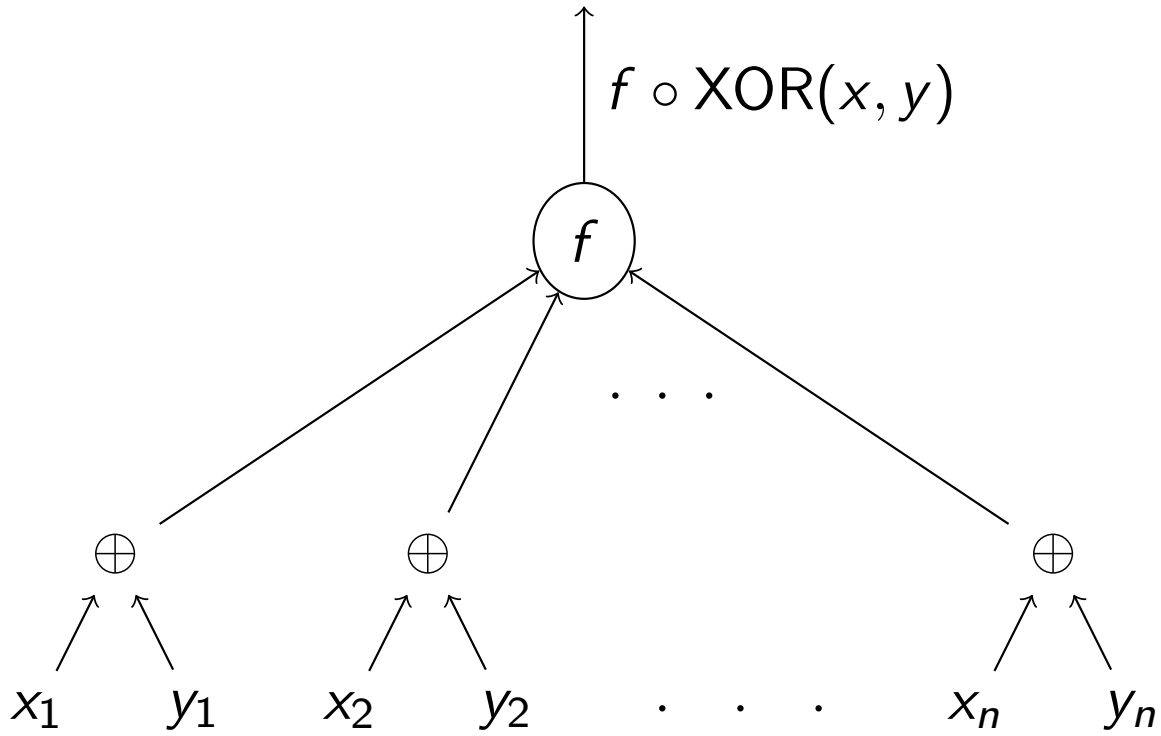
Proof idea: Define $g : \{-1, 1\}^{3n} \to \{-1, 1\}$ as follows.

$$g(x_1, \ldots x_n, y_1, \ldots, y_n, z_1, \ldots, z_n) = F(x_1, \ldots, x_n, y_1, \ldots, y_n, -x_1 z_1, \ldots, -x_n z_n, y_1 z_1, \ldots, y_n z_n).$$

Clearly, g is a monomial projection of F. Can show that $g = f \circ \mathsf{IN}$.

XOR functions

XOR functions



Widely studied class of functions under various models of communication.

Communication complexity: model of interest

Communication complexity: model of interest

$$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

Alice
$X \in \{0,1\}^n$
R_A

Bob
$Y \in \{0,1\}^n$
R_B

Figure : A protocol Π

Communication complexity: model of interest

$$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

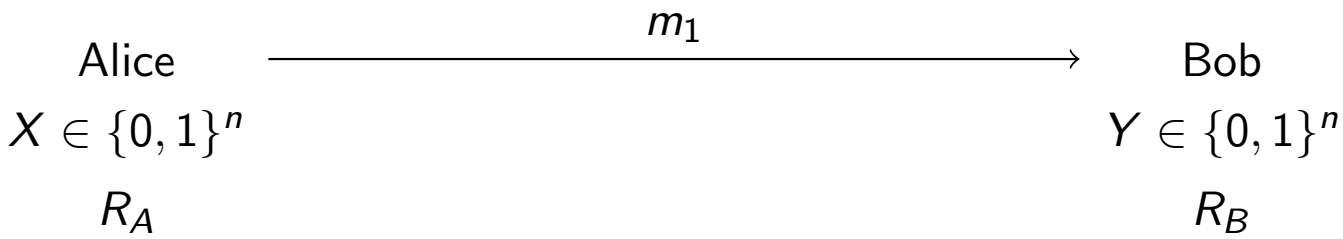


Figure : A protocol Π

Communication complexity: model of interest

$$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

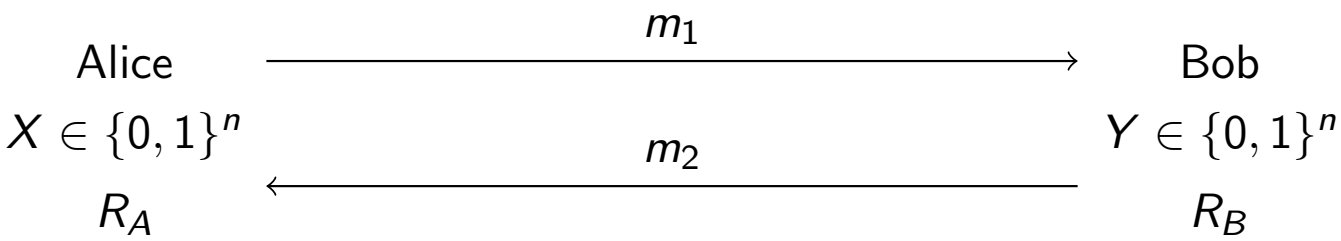


Figure : A protocol Π

Communication complexity: model of interest

$$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

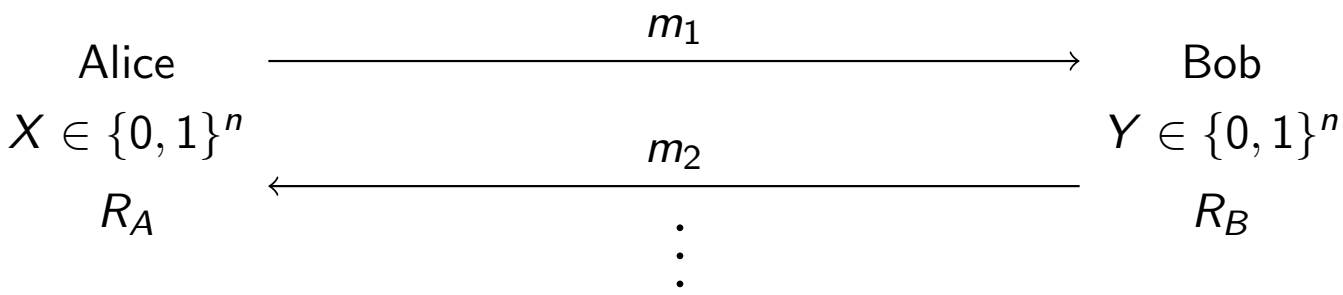


Figure : A protocol Π

Communication complexity: model of interest

$$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

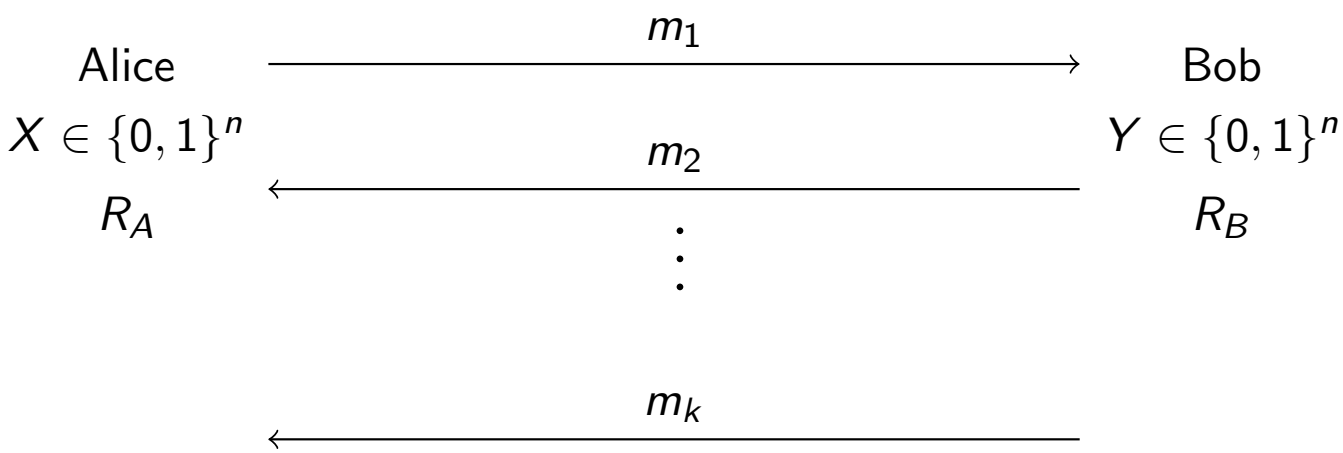


Figure : A protocol Π

Communication complexity: model of interest

$$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

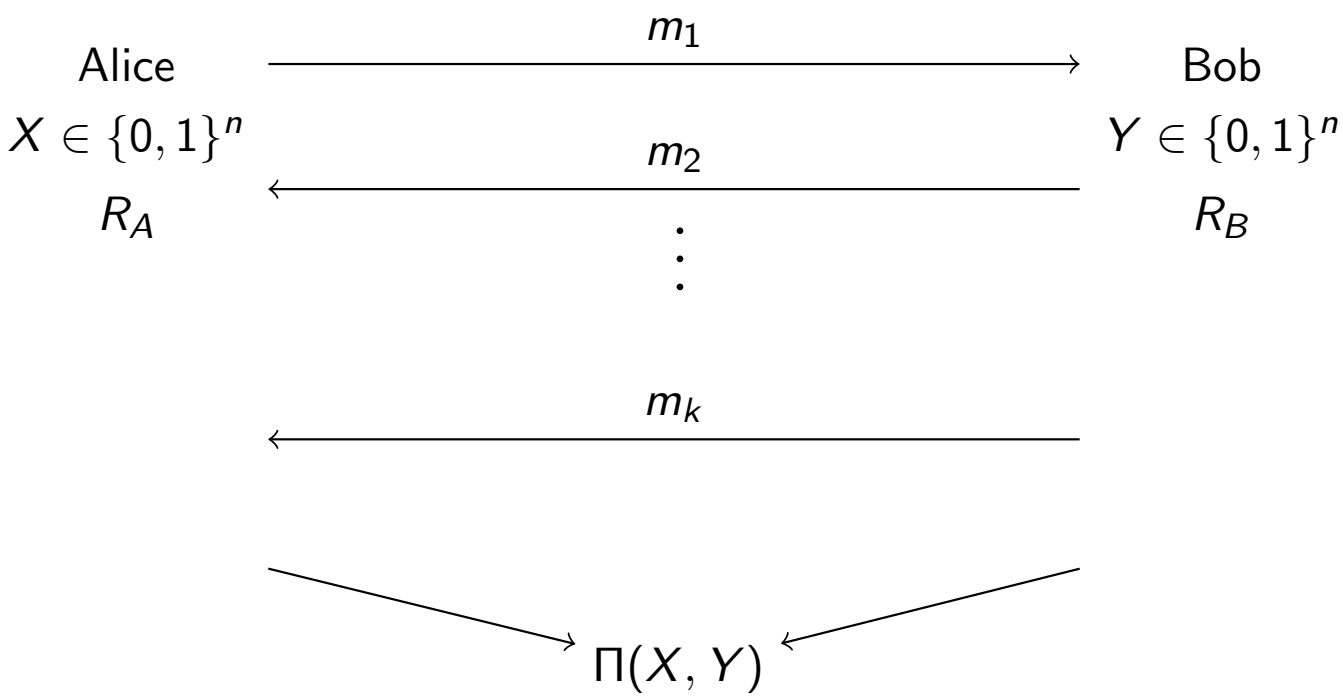


Figure : A protocol Π

Cost

Cost

- A protocol has ϵ advantage if $\forall X, Y \ \Pr[\Pi(X, Y) = F(X, Y)] \geq \frac{1}{2} + \epsilon$.

Cost

- A protocol has ϵ advantage if $\forall X, Y \ \Pr[\Pi(X, Y) = F(X, Y)] \geq \frac{1}{2} + \epsilon$.
- $R_\epsilon(F)$ is the number of bits communicated in the worst case the cheapest ϵ advantageous protocol.

Cost

- A protocol has ϵ advantage if $\forall X, Y \ \Pr[\Pi(X, Y) = F(X, Y)] \geq \frac{1}{2} + \epsilon$.
- $R_\epsilon(F)$ is the number of bits communicated in the worst case the cheapest ϵ advantageous protocol.
- $\mathrm{PP}(F) = \inf_{\epsilon > 0} \left(R_\epsilon(F) + \log(1/\epsilon) \right)$.

PP complexity of symmetric XOR functions

PP complexity of symmetric XOR functions

Lifting theorem + projection lemma + margin-discrepancy equivalence (extended version of this paper) yields:

PP complexity of symmetric XOR functions

Lifting theorem + projection lemma + margin-discrepancy equivalence (extended version of this paper) yields:

Theorem (Weak form of conjecture in [SZ'09])

For symmetric f,

$$\mathrm{PP}(f \circ \mathrm{XOR}) \approx \deg_{oe}(f).$$

PP complexity of symmetric XOR functions

Lifting theorem + projection lemma + margin-discrepancy equivalence (extended version of this paper) yields:

Theorem (Weak form of conjecture in [SZ'09])

For symmetric f,

$$\mathrm{PP}(f \circ \mathrm{XOR}) \approx \deg_{oe}(f).$$

(Stronger form proved independently by [HQ'17] and [AFK'17], using different techniques).

What I didn't cover

What I didn't cover

- Characterization of PTF sparsity of symmetric functions.

What I didn't cover

- Characterization of PTF sparsity of symmetric functions.
- $\mathrm{mon}_{1/3}(f) = \Theta^*(r(f))$ for symmetric f.

What I didn't cover

- Characterization of PTF sparsity of symmetric functions.
- $\mathrm{mon}_{1/3}(f) = \Theta^*(r(f))$ for symmetric f.
- Quantum?

What I didn't cover

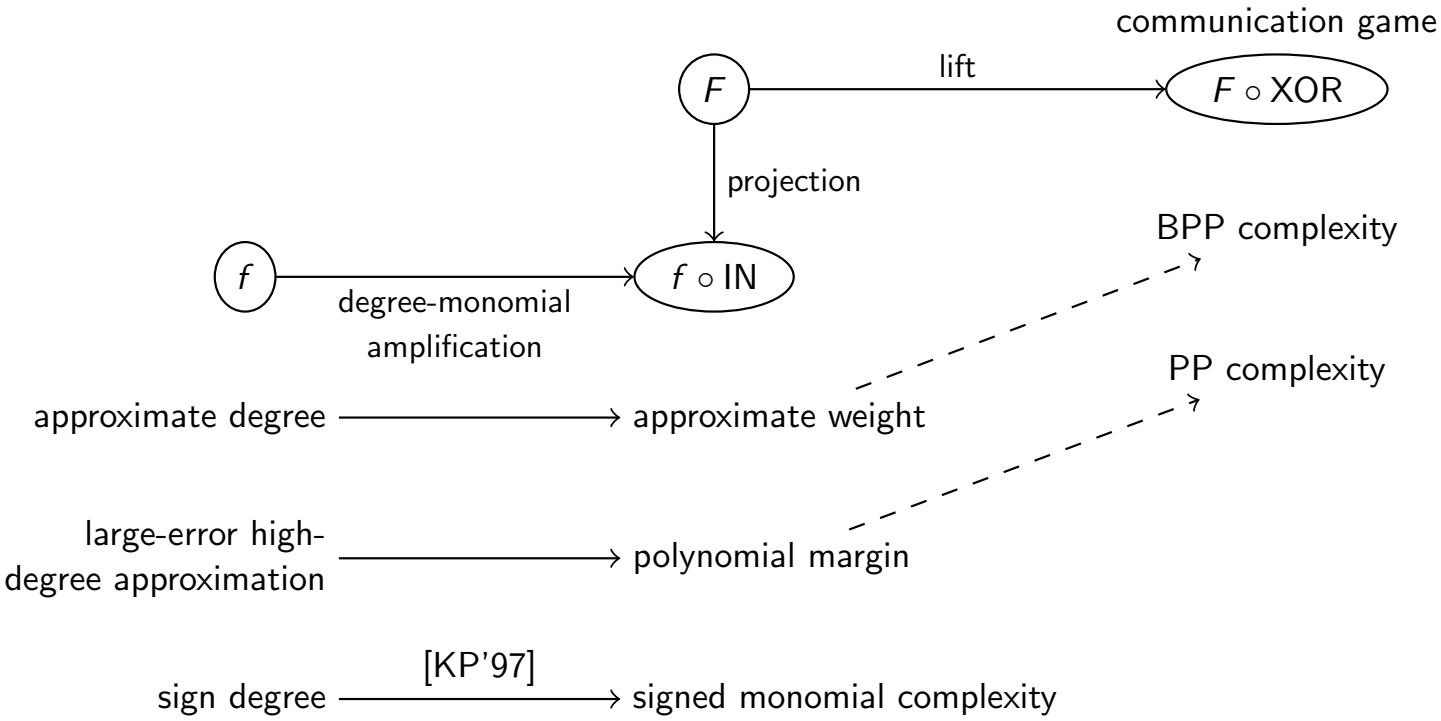
- Characterization of PTF sparsity of symmetric functions.
- $\mathrm{mon}_{1/3}(f) = \Theta^*(r(f))$ for symmetric f.
- Quantum?
- $\mathrm{BPP}(f \circ \mathrm{XOR}) \geq \mathrm{wt}_{1/3}(f)$ for symmetric f (Reproof of result from [SZ'09]).

What I didn't cover

- Characterization of PTF sparsity of symmetric functions.
- $\mathrm{mon}_{1/3}(f) = \Theta^*(r(f))$ for symmetric f.
- Quantum?
- $\mathrm{BPP}(f \circ \mathrm{XOR}) \geq \mathrm{wt}_{1/3}(f)$ for symmetric f (Reproof of result from [SZ'09]).
- Resolution of approximate log rank conjecture for symmetric XOR functions (check!).

Summary

Summary


communication game
lift
F
$F \circ \mathrm{XOR}$
projection
BPP complexity
f
$f \circ \mathrm{IN}$
degree-monomial amplification
PP complexity
approximate degree
approximate weight
large-error high-degree approximation
polynomial margin
[KP'97]
sign degree
signed monomial complexity

Thank You!