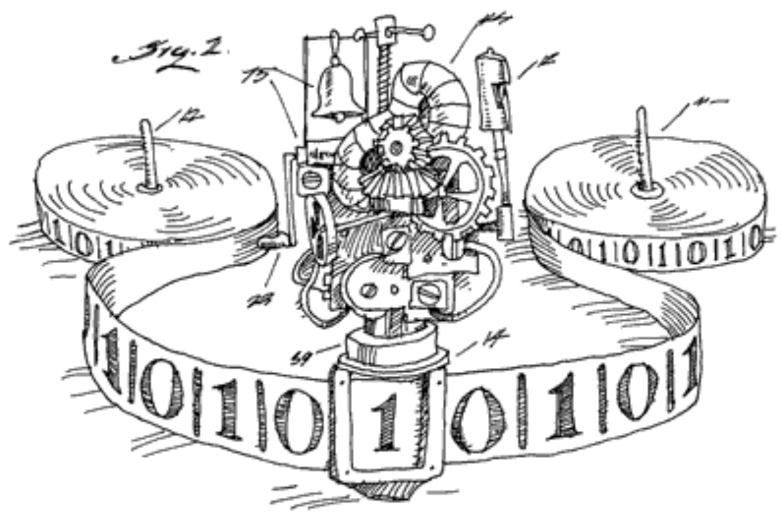
SHANNON MEETS TURING

Pei Wu

April. 2023

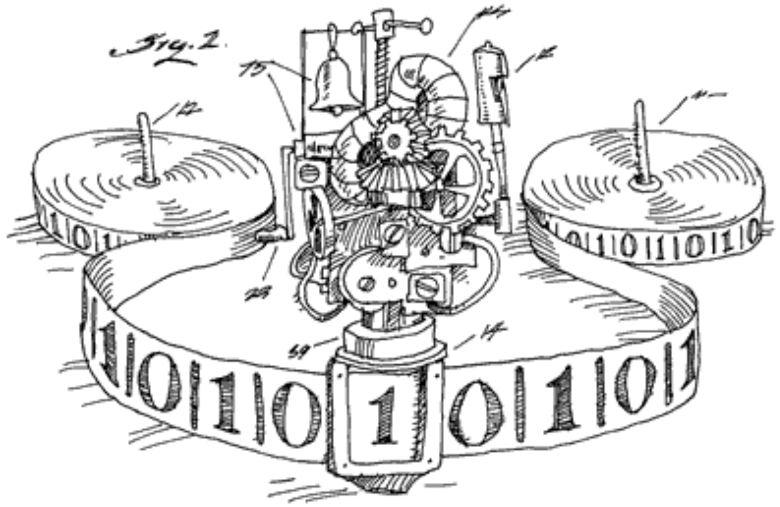
Theory of Computation

A. Turing



Theory of Computation

A. Turing

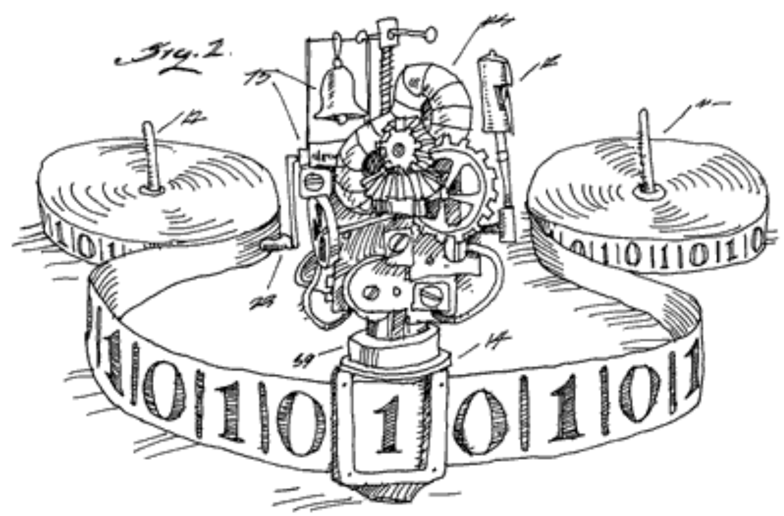


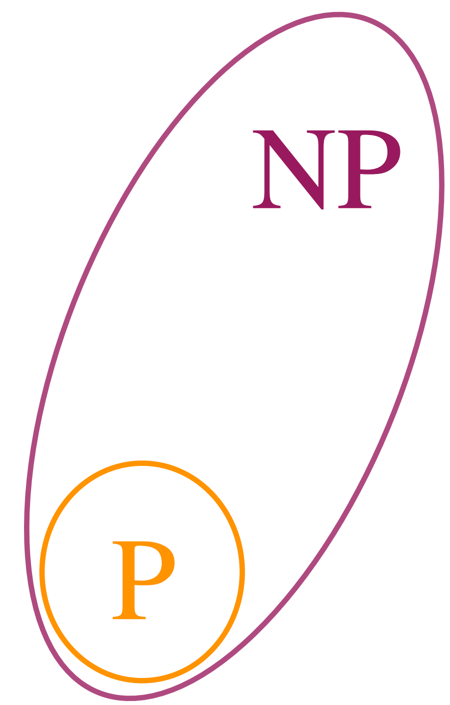
deterministic polynomial-time

non-determinism

Theory of Computation

A. Turing



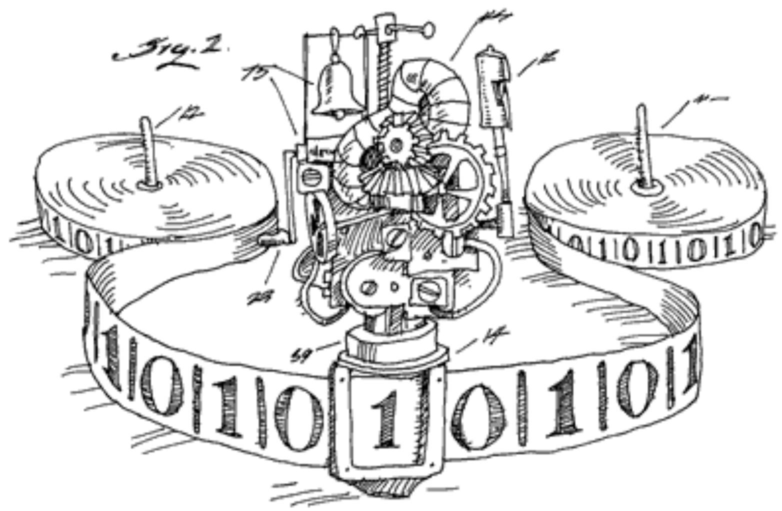


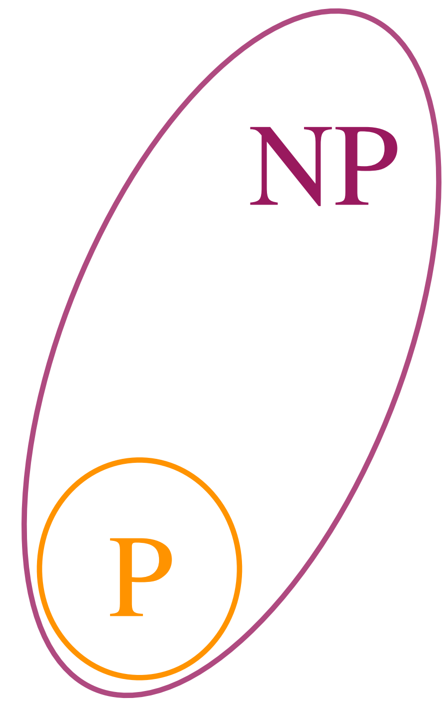
deterministic polynomial-time

non-determinism

Theory of Computation

A. Turing





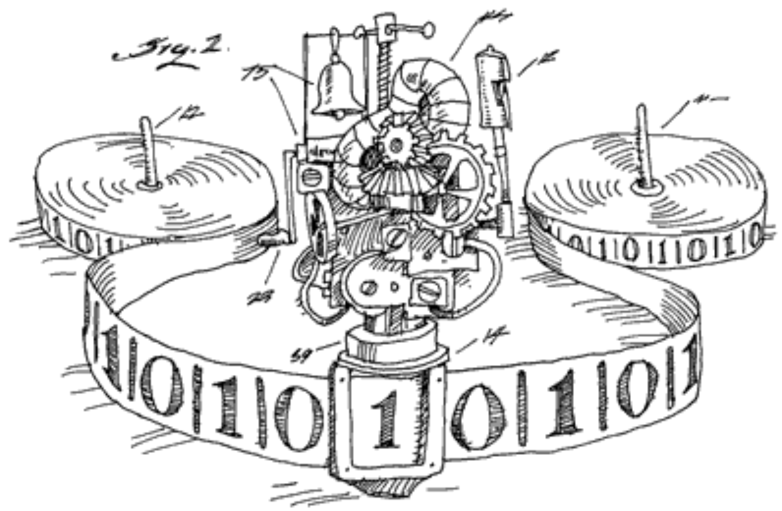
deterministic polynomial-time

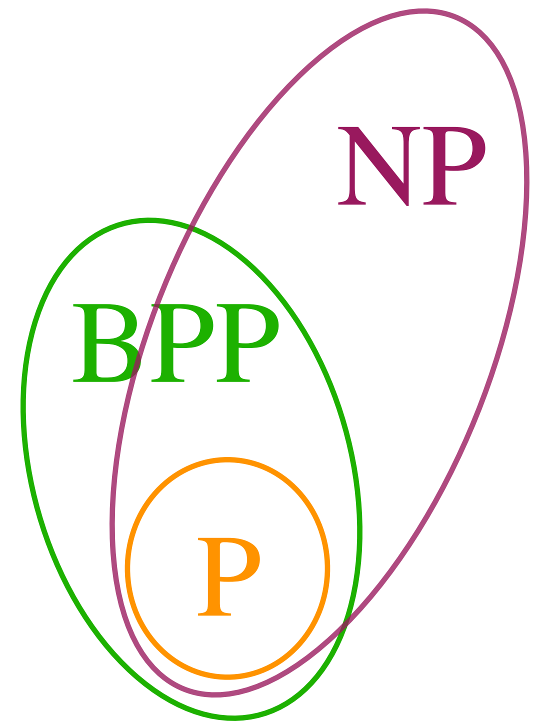
non-determinism

randomness

Theory of Computation

A. Turing





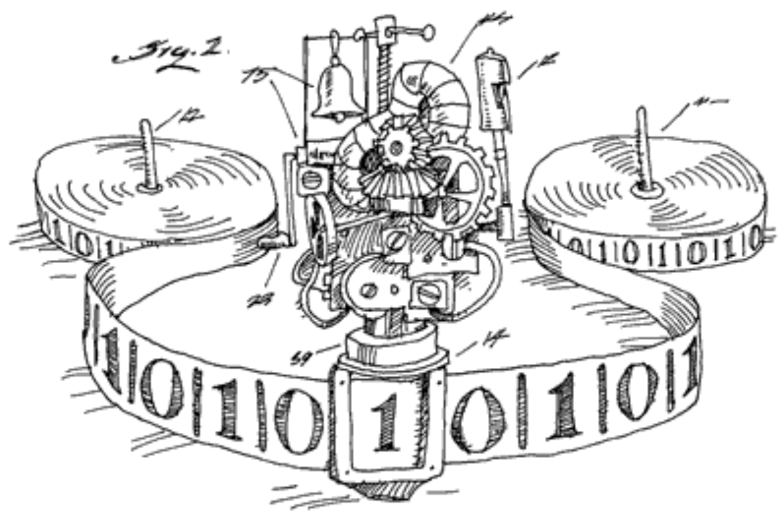
deterministic polynomial-time

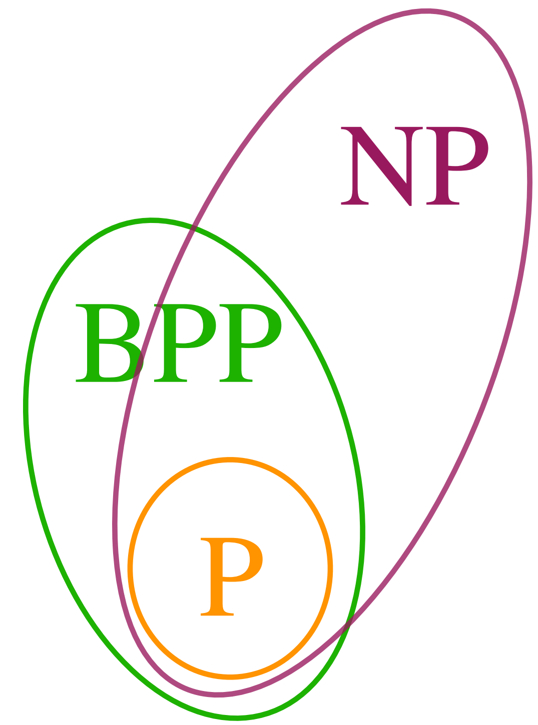
non-determinism

randomness

Theory of Computation

A. Turing





deterministic polynomial-time

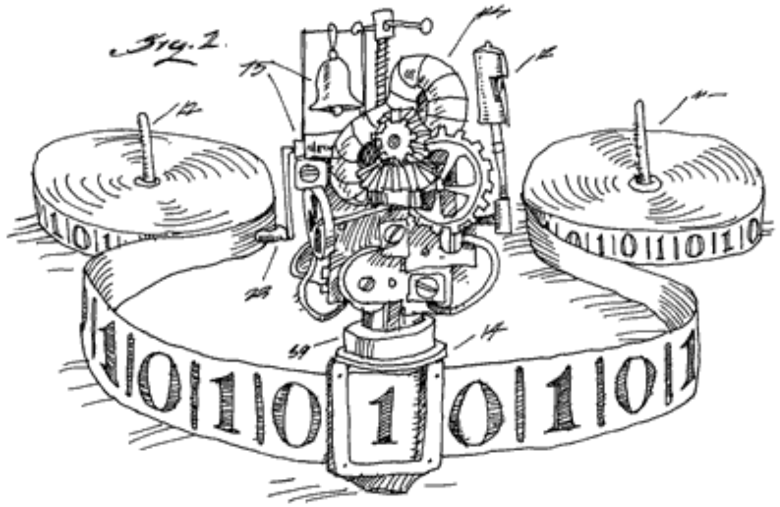
non-determinism

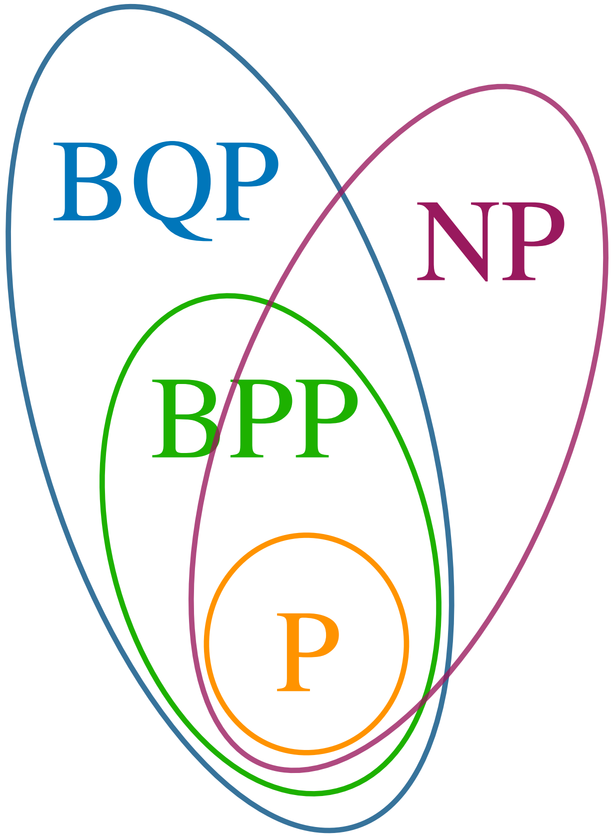
randomness

quantum

Theory of Computation

A. Turing





deterministic polynomial-time

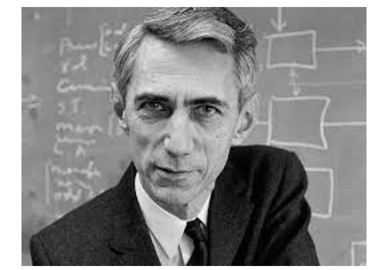
non-determinism

randomness

quantum

Theory of Communication (one-way)

Reprinted with corrections from *The Bell System Technical Journal,*
Vol. 27, pp. 379–423, 623–656, July, October, 1948.



A Mathematical Theory of Communication

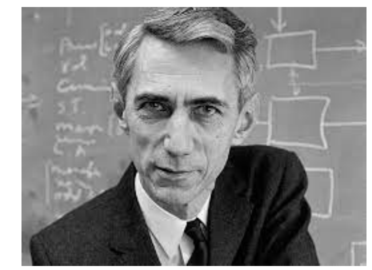
By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A

Theory of Communication (one-way)

Reprinted with corrections from *The Bell System Technical Journal,*
Vol. 27, pp. 379–423, 623–656, July, October, 1948.



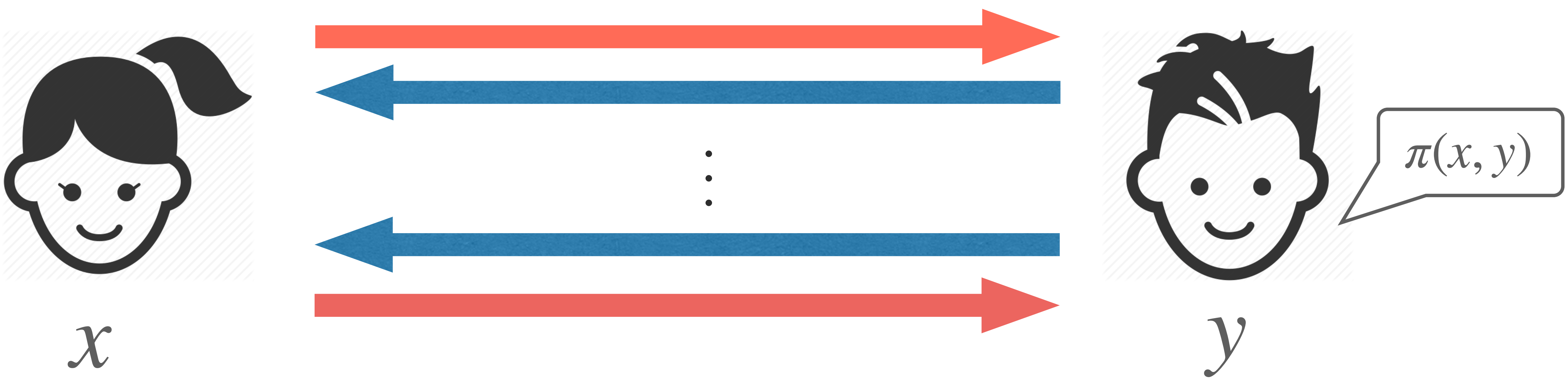
A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A

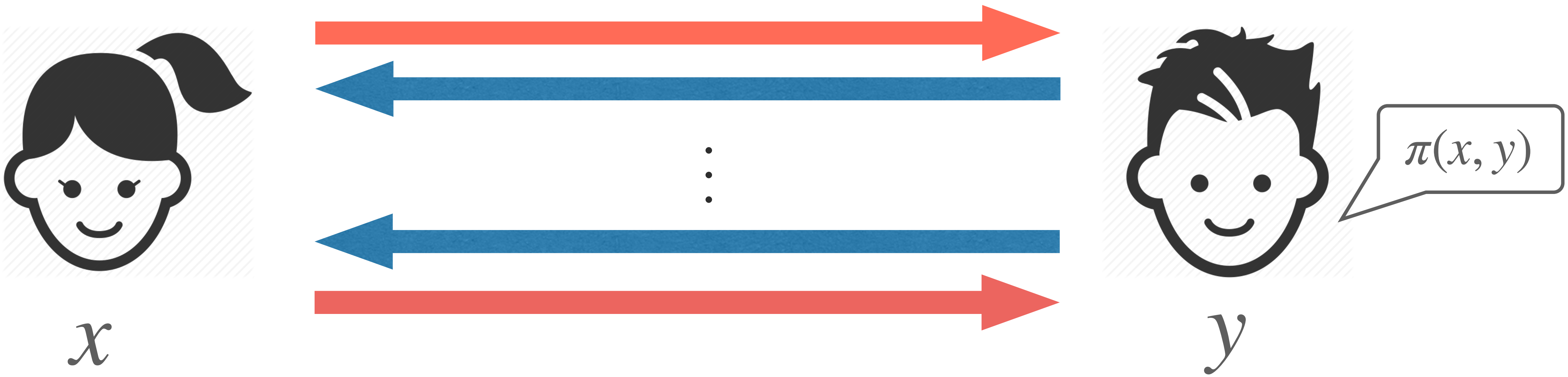
Theory of Communication (interactive)



Theory of Communication (interactive)

A. Yao '79

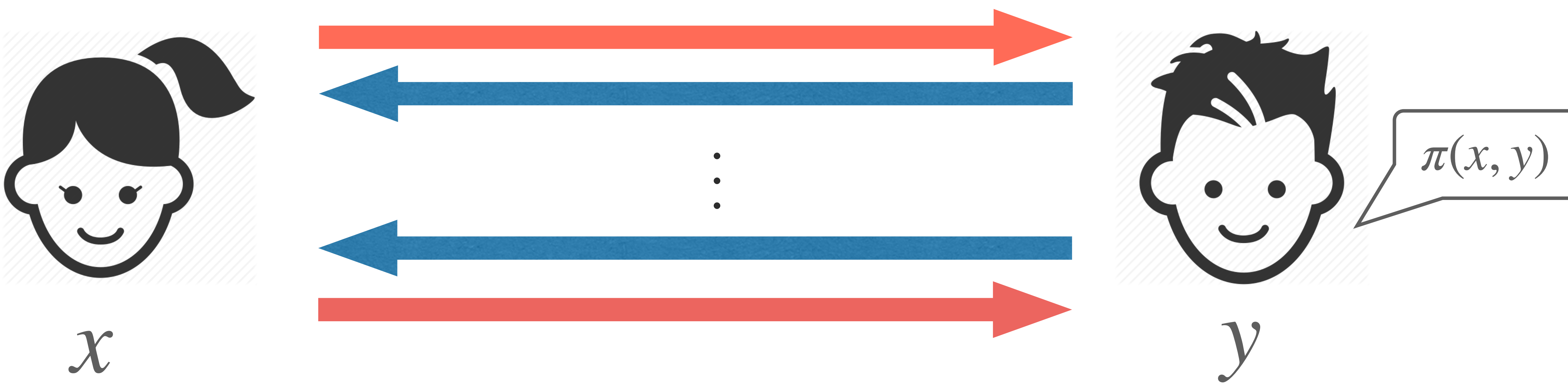
$f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$



Theory of Communication (interactive)

A. Yao '79

$f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$



A trivial, $O(n)$-communication solution

Theory of Communication (interactive)

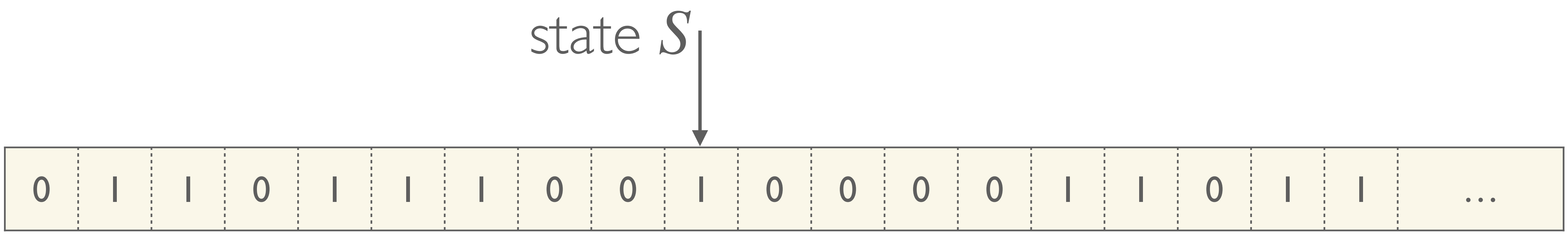
Theory of Communication (interactive)

Central in cs:

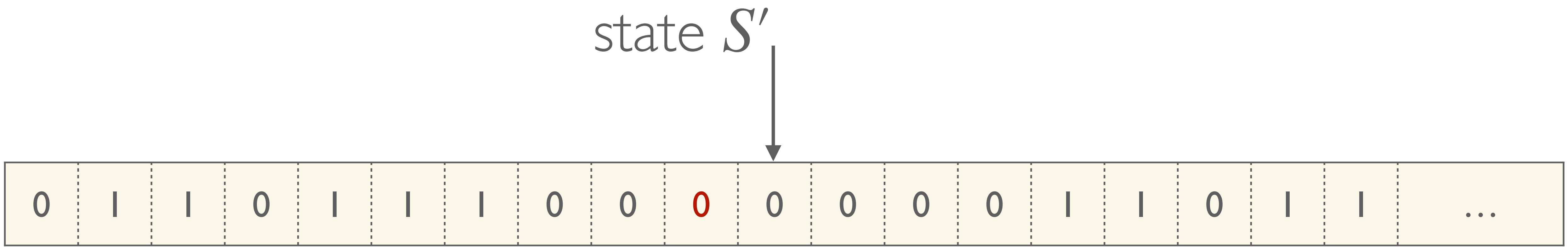
circuits complexity,
streaming algorithm,
learning theory,
differential privacy,
computational economics

…

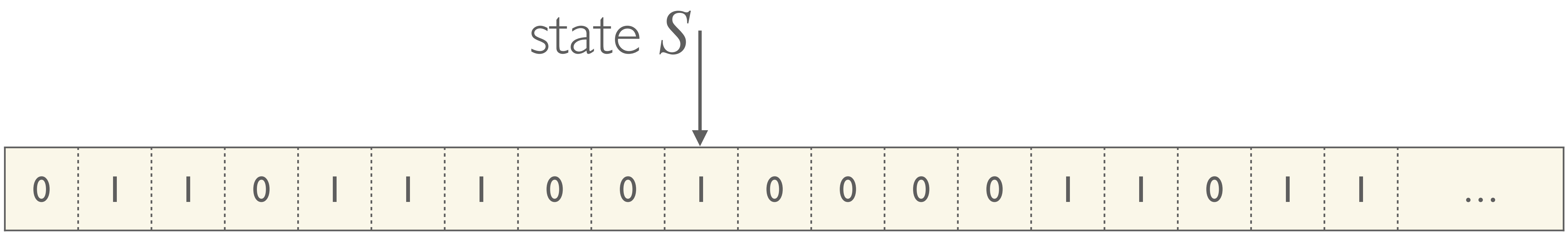
An example



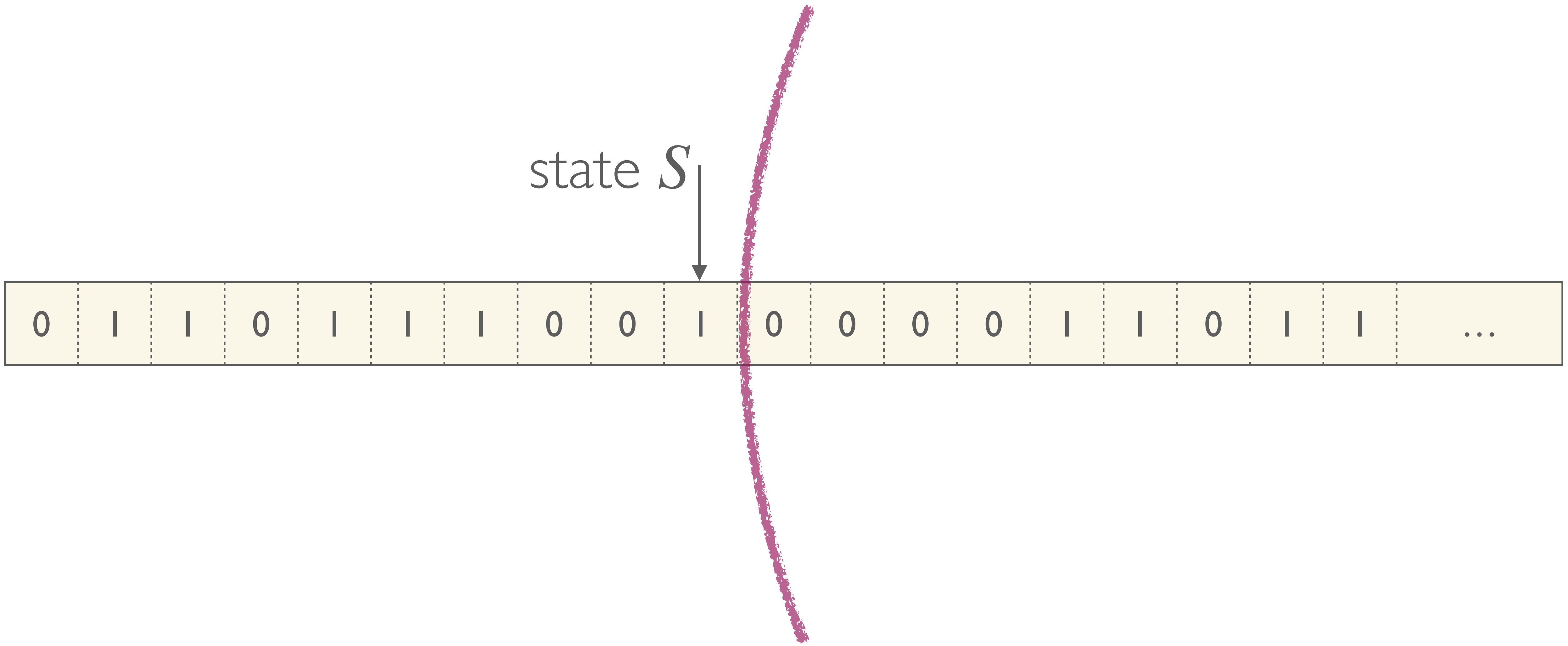
An example



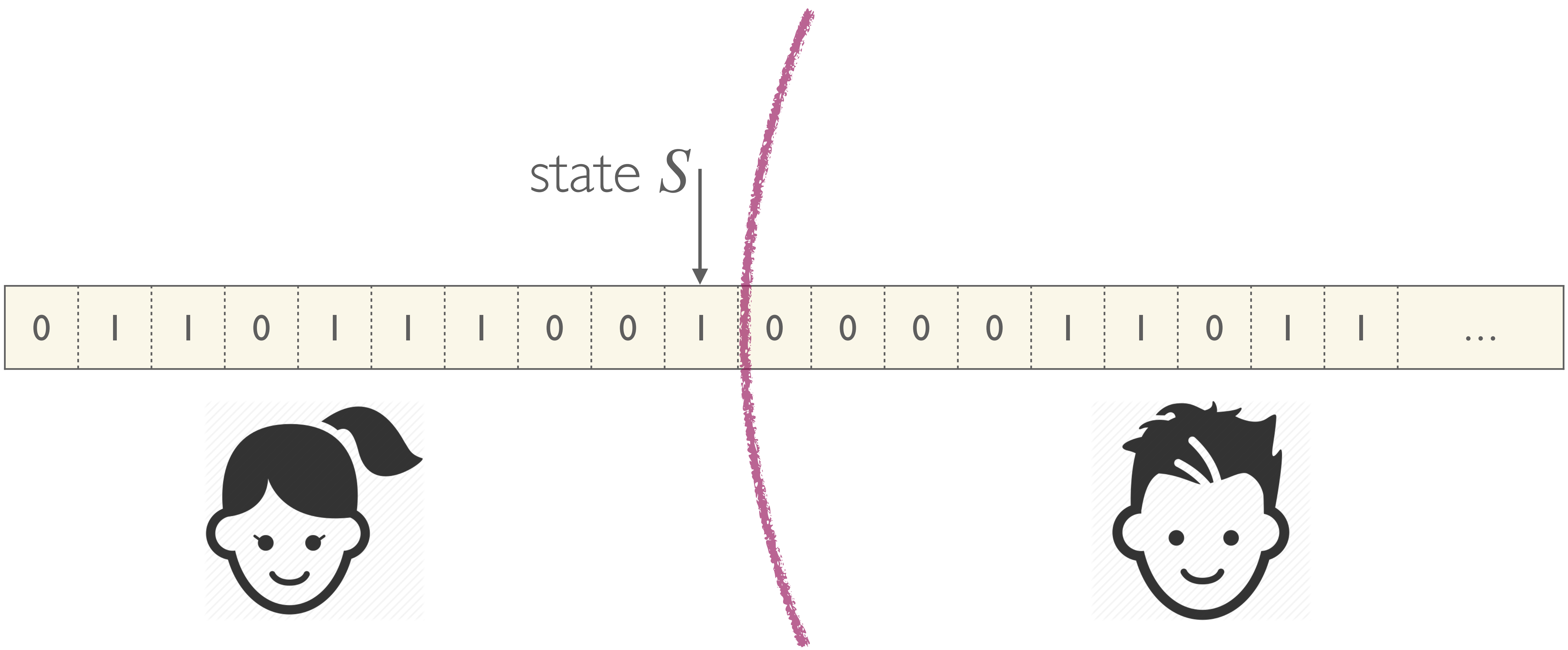
An example



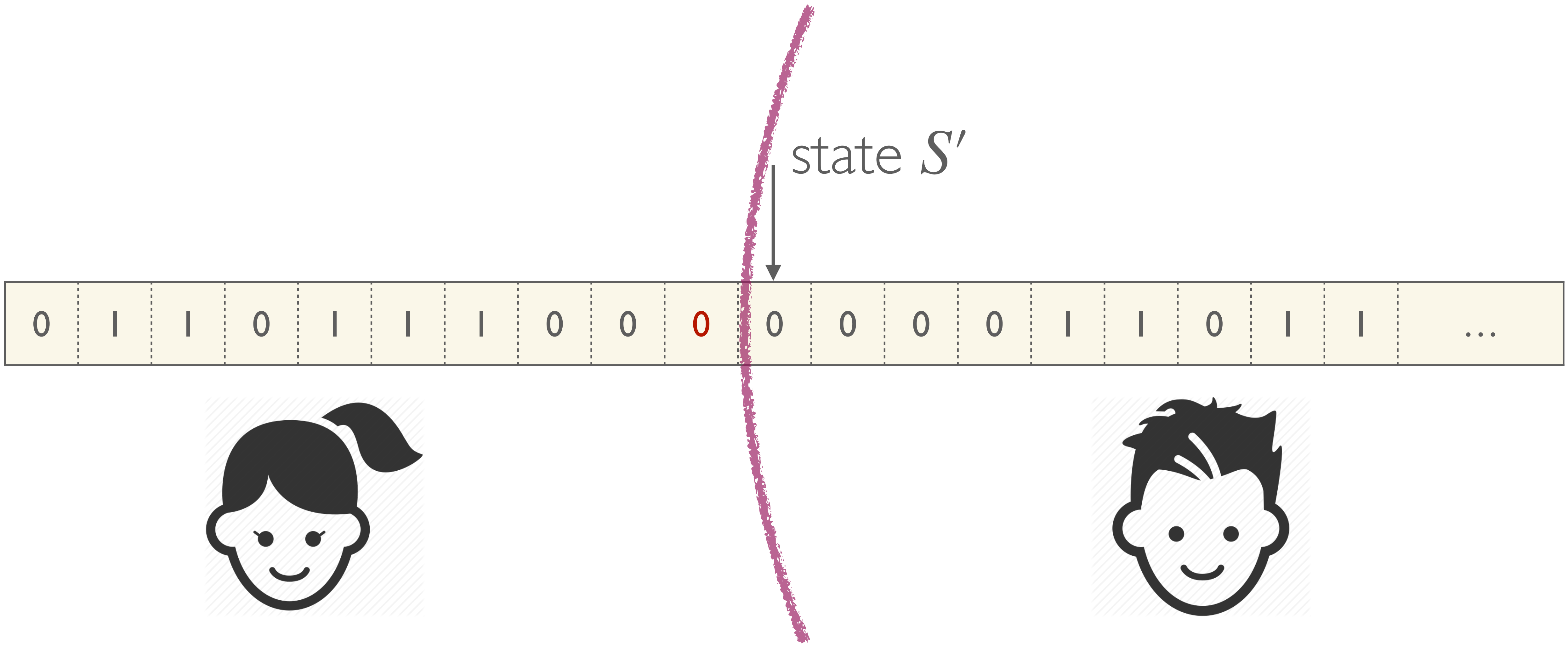
An example



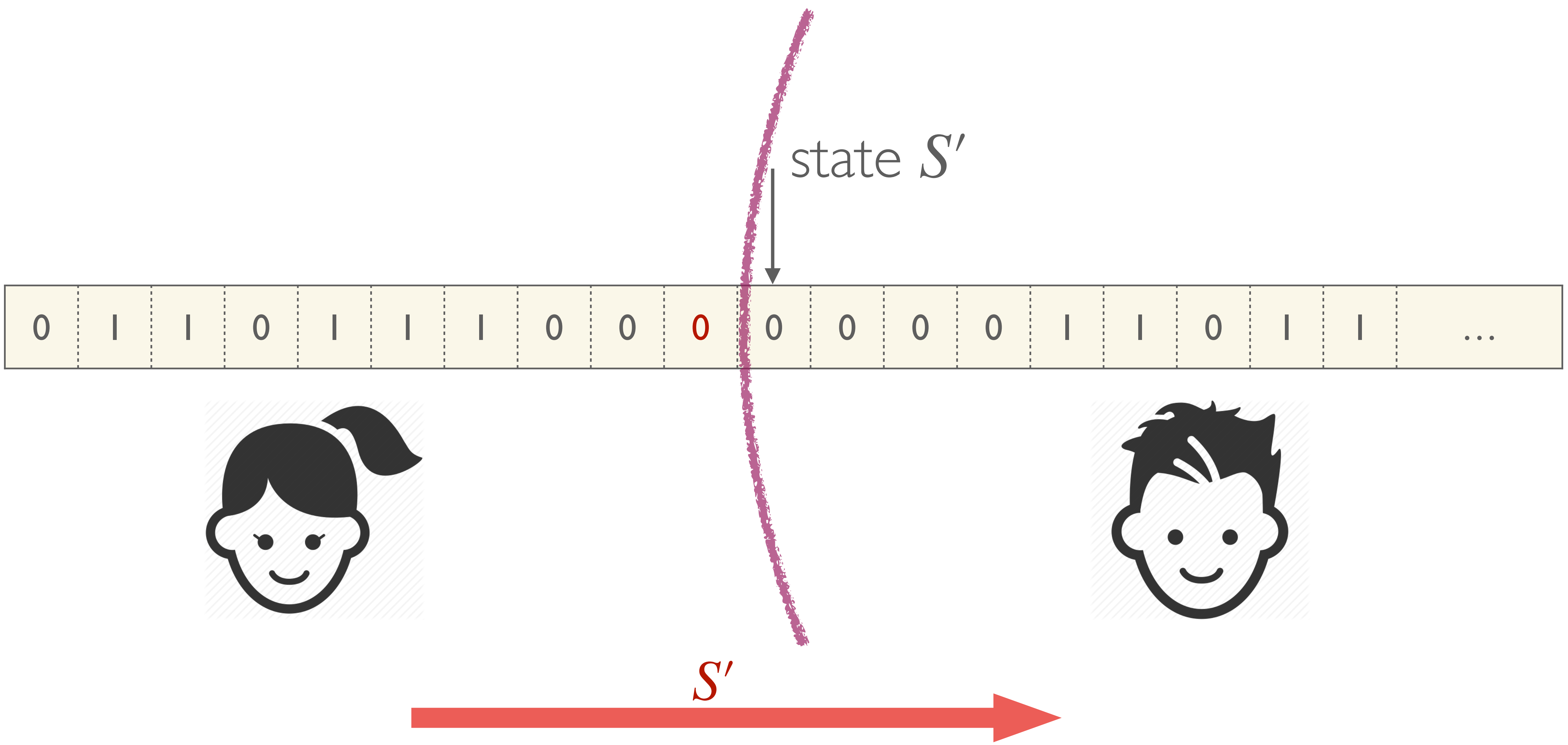
An example



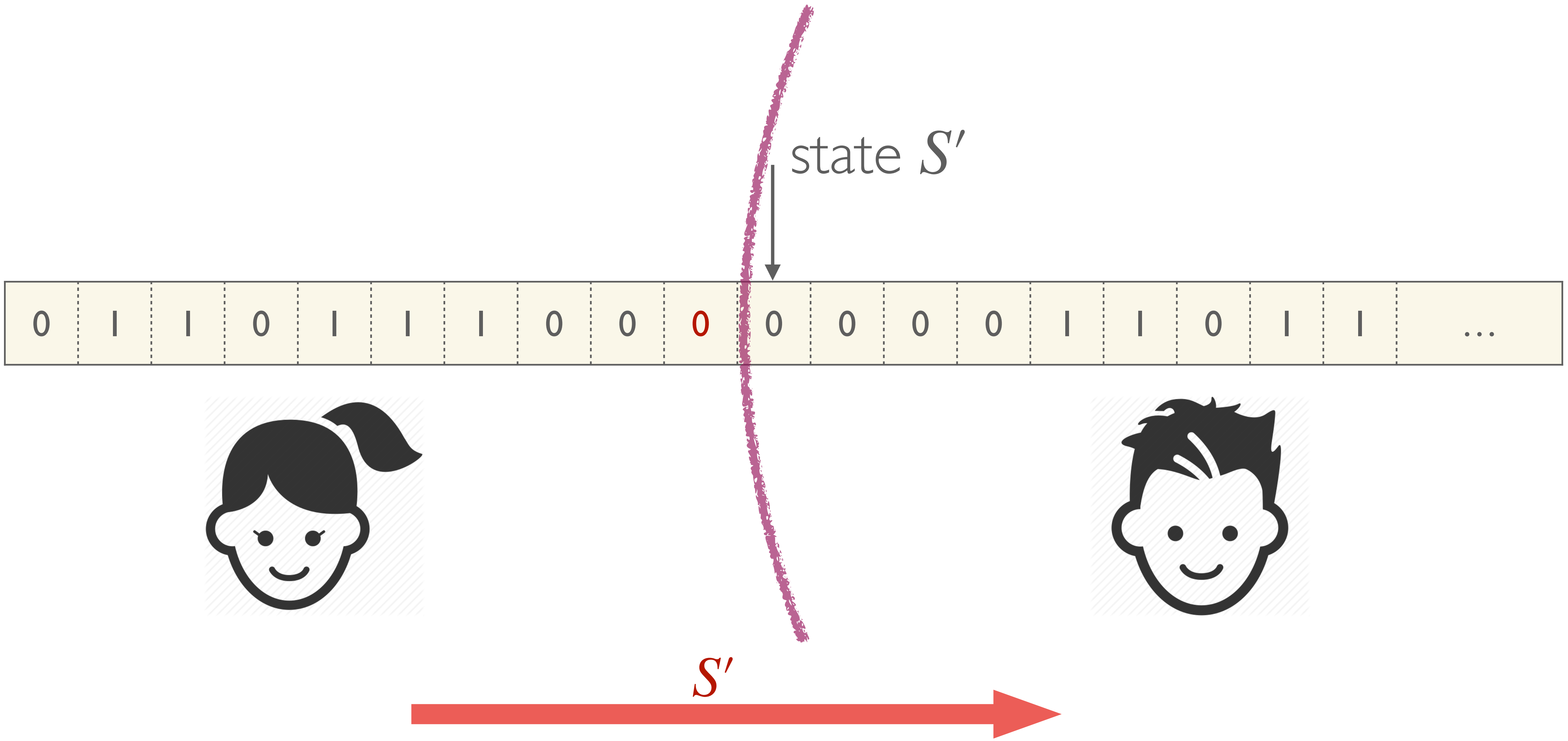
An example



An example



An example



communication ≈ running time

Communication Complexity

[Babai-Frankl-Simon '86]

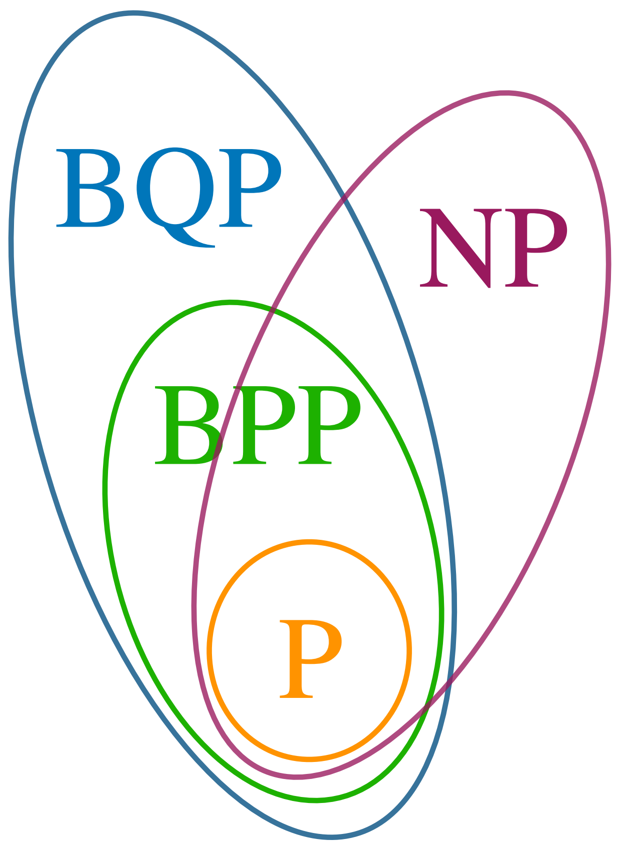
P: deterministic communication

NP: non-deterministic communication

BPP: randomized communication
(bounded-error)

BQP: quantum communication

PP: randomized communication
(unbounded-error)



Communication Complexity

[Babai-Frankl-Simon '86]

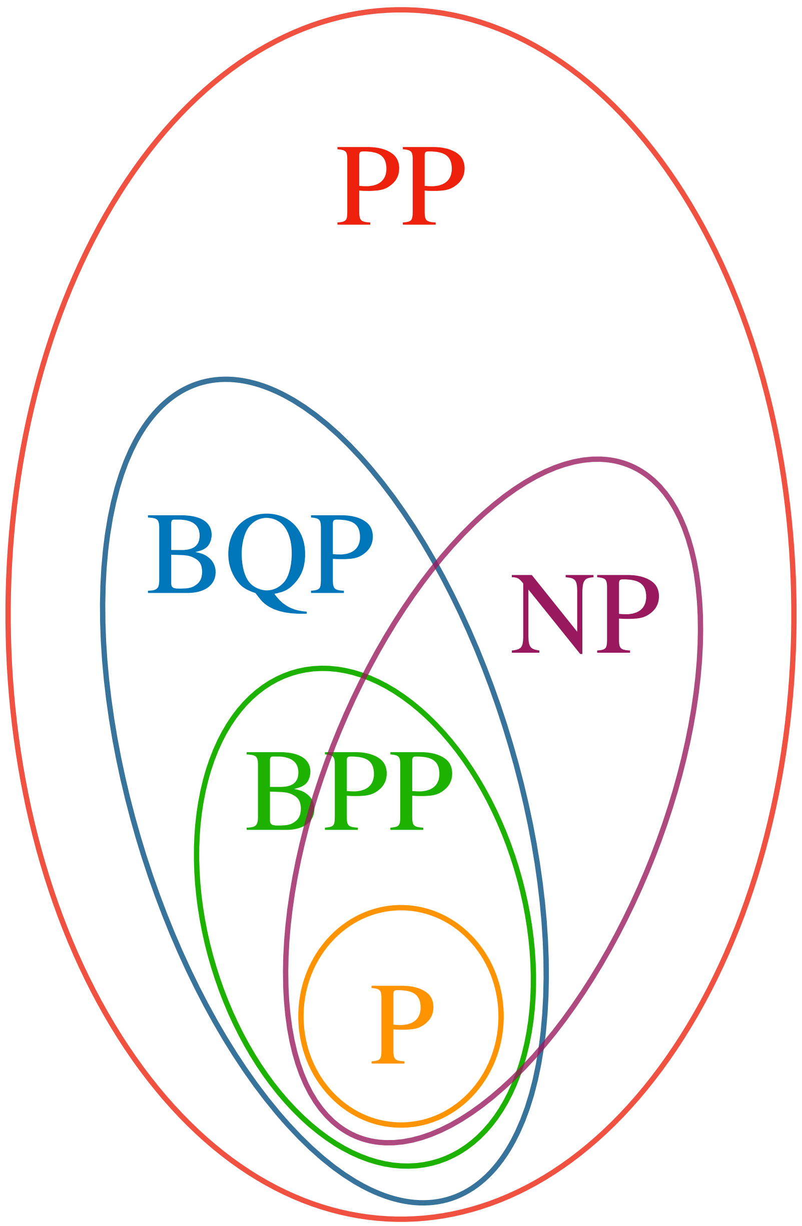
P: deterministic communication

NP: non-deterministic communication

BPP: randomized communication
(bounded-error)

BQP: quantum communication

PP: randomized communication
(unbounded-error)



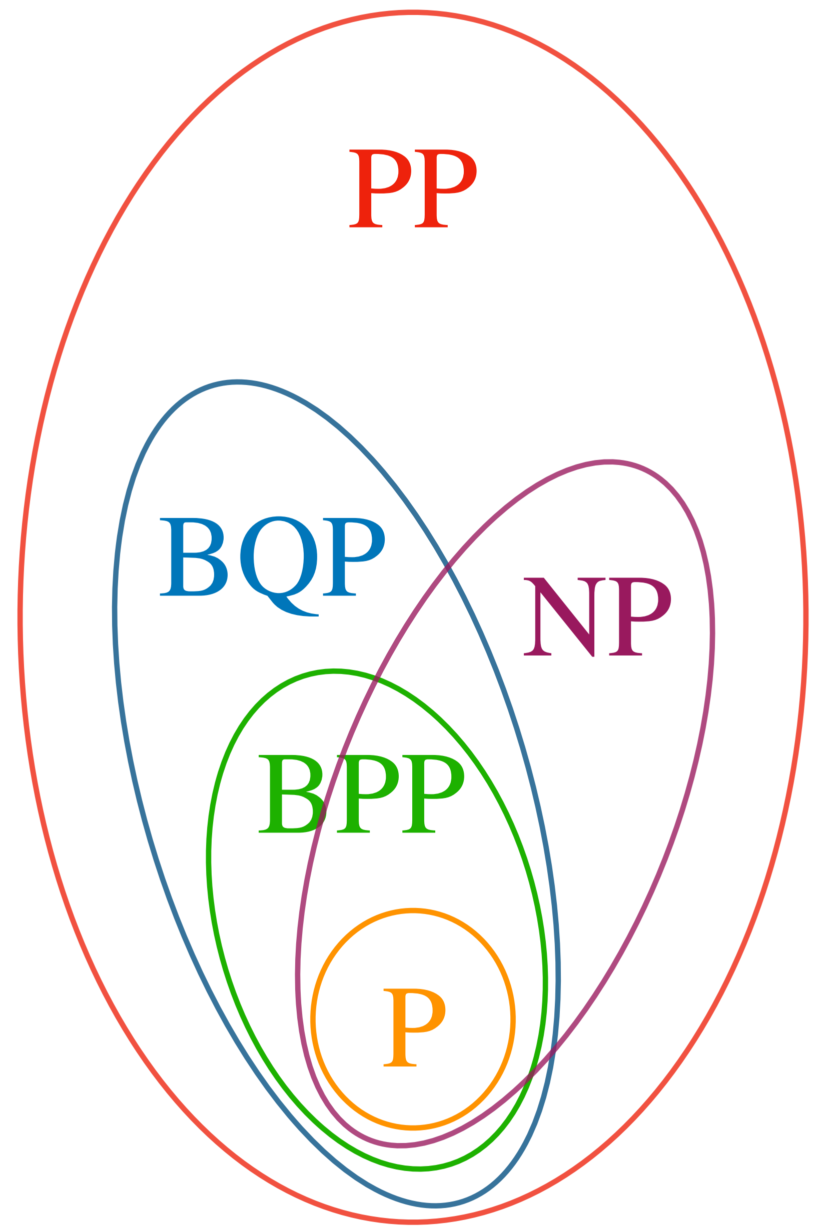
Communication Complexity

[Babai-Frankl-Simon '86]

P: deterministic communication

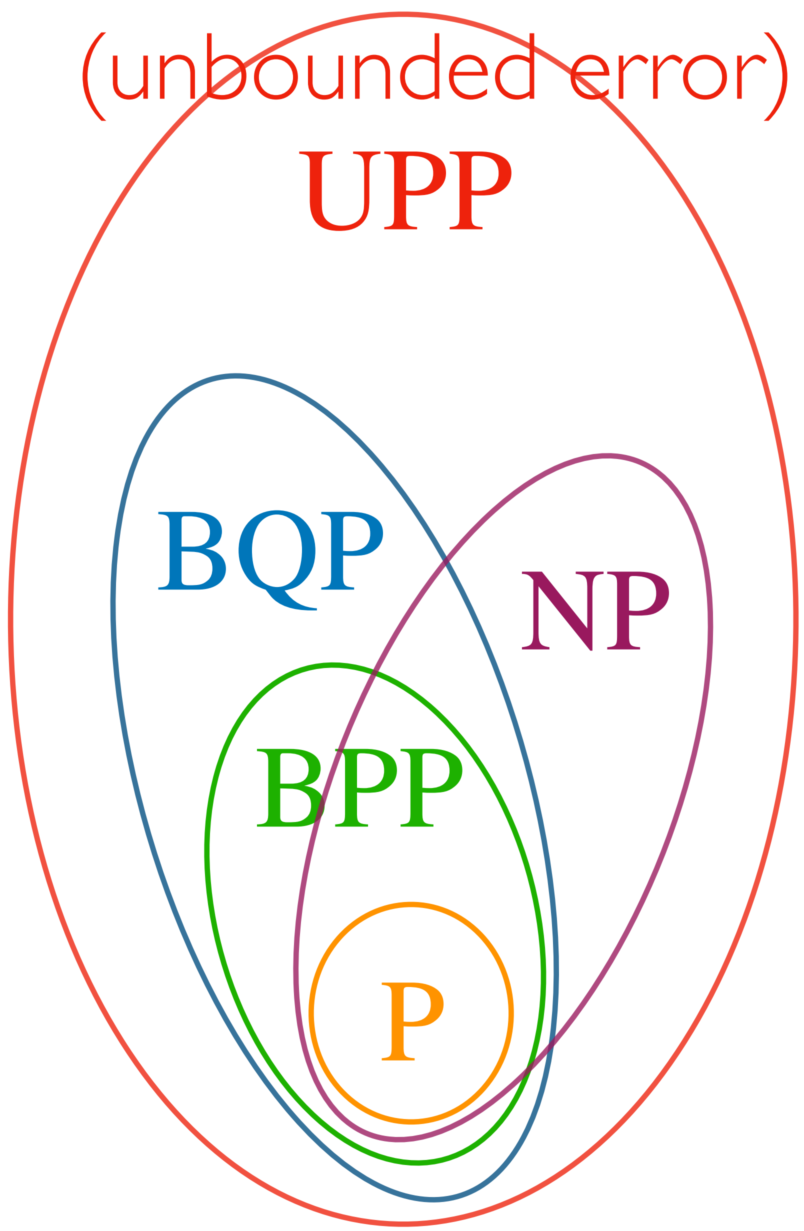
NP: non-deterministic communication

- BPP: randomized communication (bounded-error)
- BQP: quantum communication
- PP: randomized communication (unbounded-error)



Unbounded-error communication

[Babai-Frankl-Simon '86]



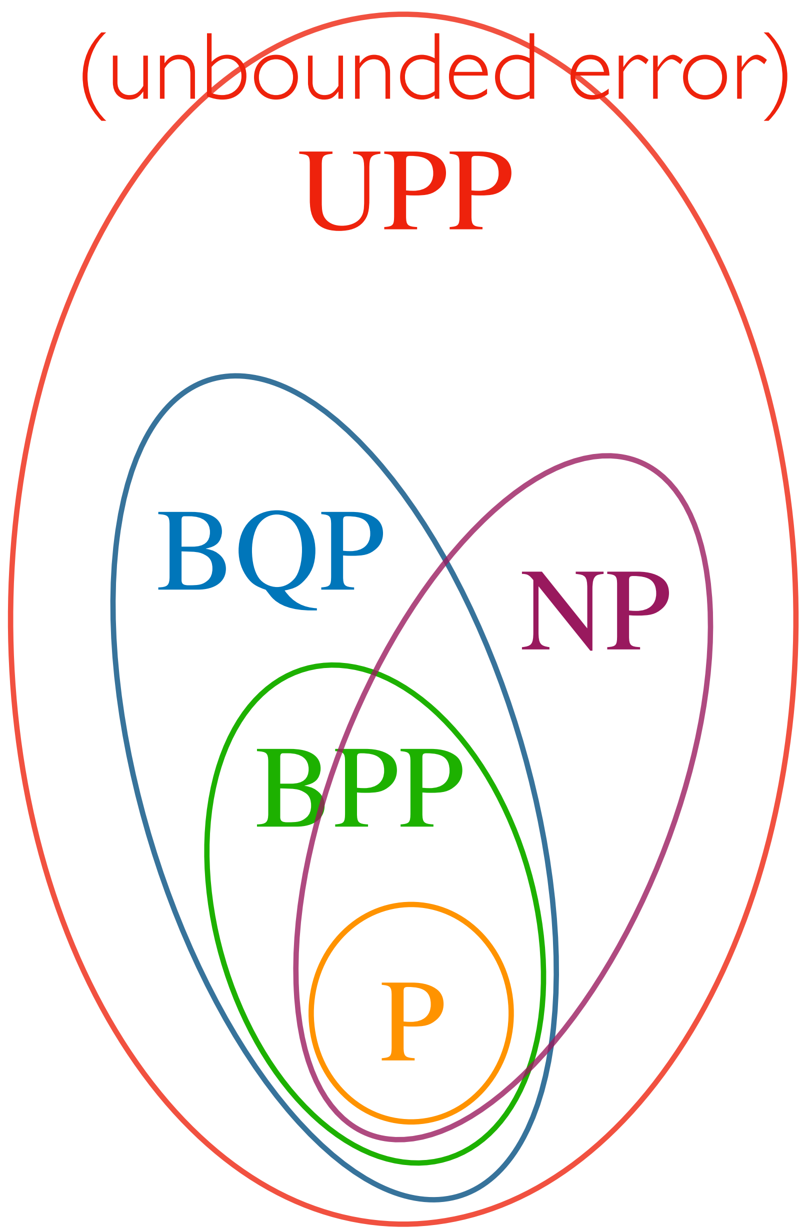
- UPP research frontier

- In communication world,

$$\mathrm{P} \subsetneq \mathrm{BPP} \subseteq \mathrm{BQP} \subsetneq \mathrm{UPP},$$
$$\mathrm{P} \subsetneq \mathrm{NP} \subsetneq \mathrm{UPP}\,.$$

Unbounded-error communication

[Babai-Frankl-Simon '86]



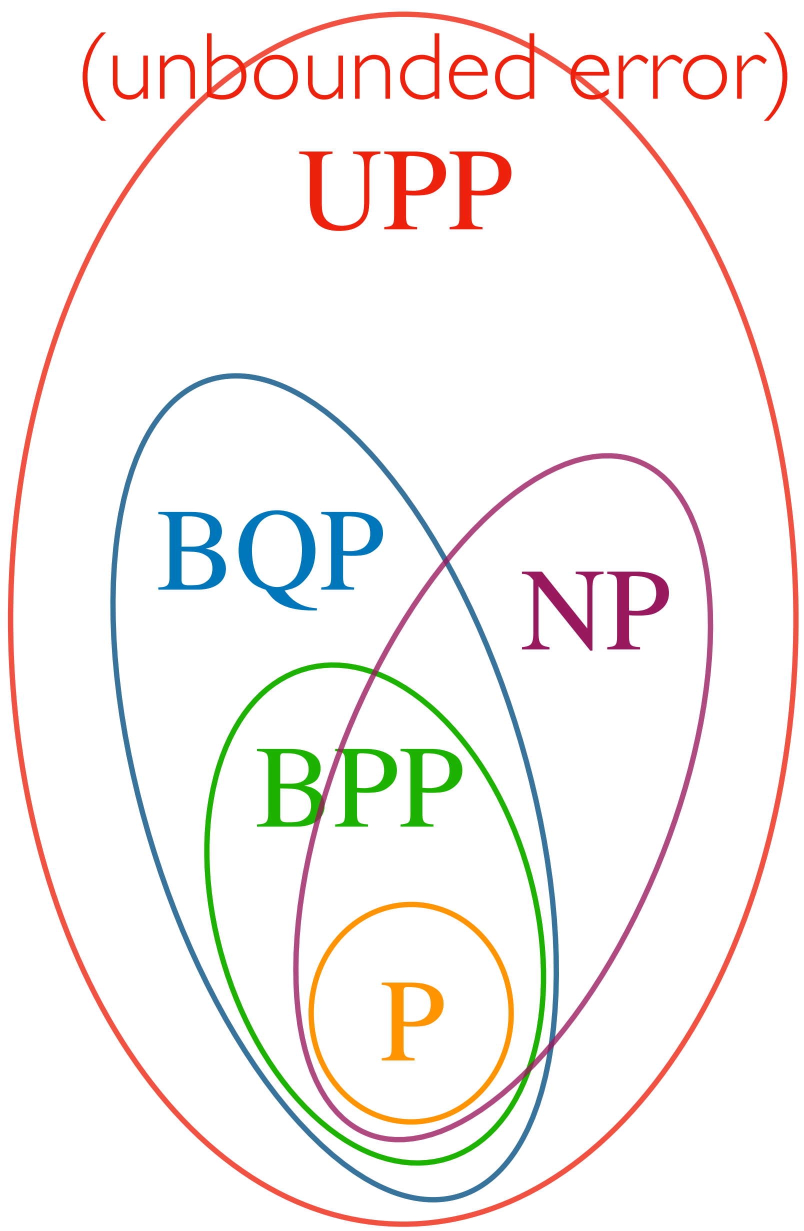
- UPP research frontier

- In communication world,

$$P \subsetneq BPP \subseteq BQP \subsetneq UPP,$$
$$P \subsetneq NP \subsetneq UPP\,.$$

Unbounded-error communication

[Babai-Frankl-Simon '86]



- UPP research frontier

  Result 1: $AC^0 \notin UPP$

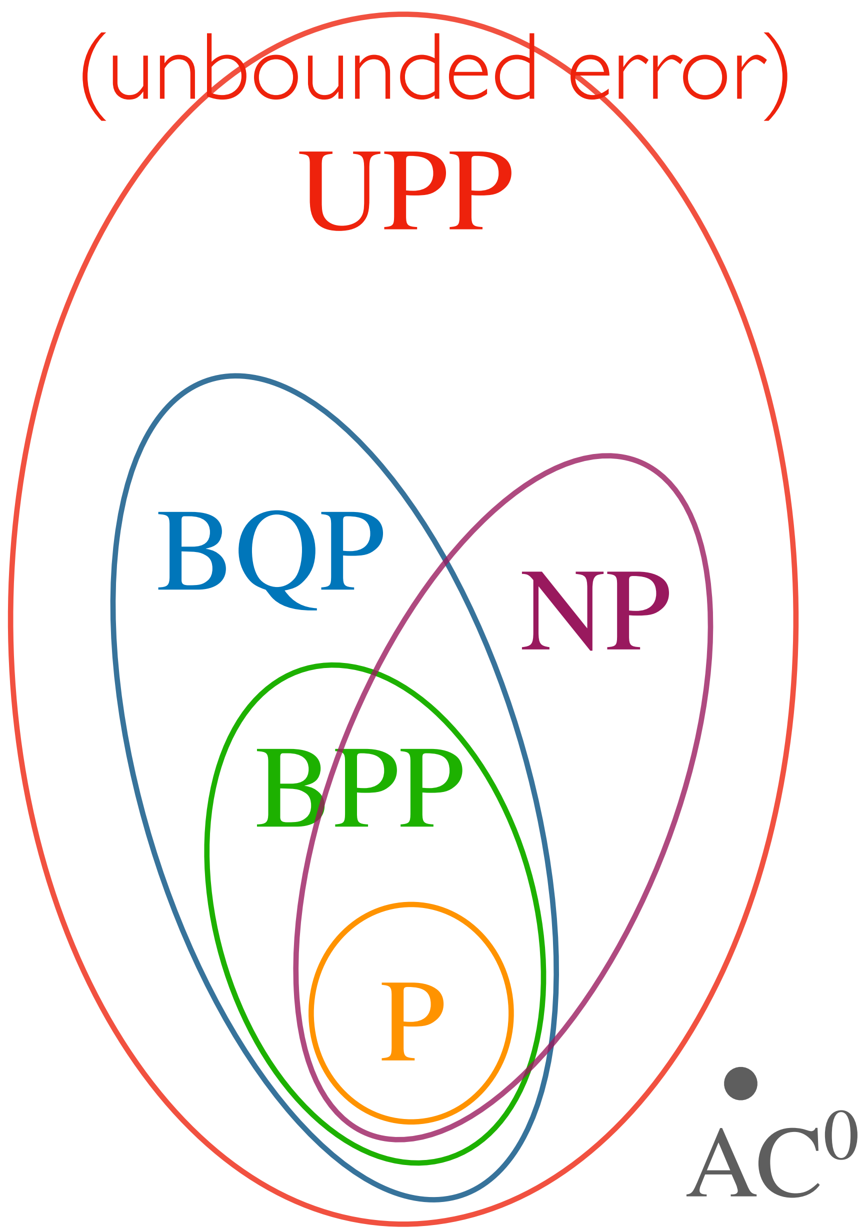
- In communication world,

  $P \subsetneq BPP \subseteq BQP \subsetneq UPP$,

  $P \subsetneq NP \subsetneq UPP$.

Unbounded-error communication

[Babai-Frankl-Simon '86]



- UPP research frontier

  Result 1: $AC^0 \not\in UPP$

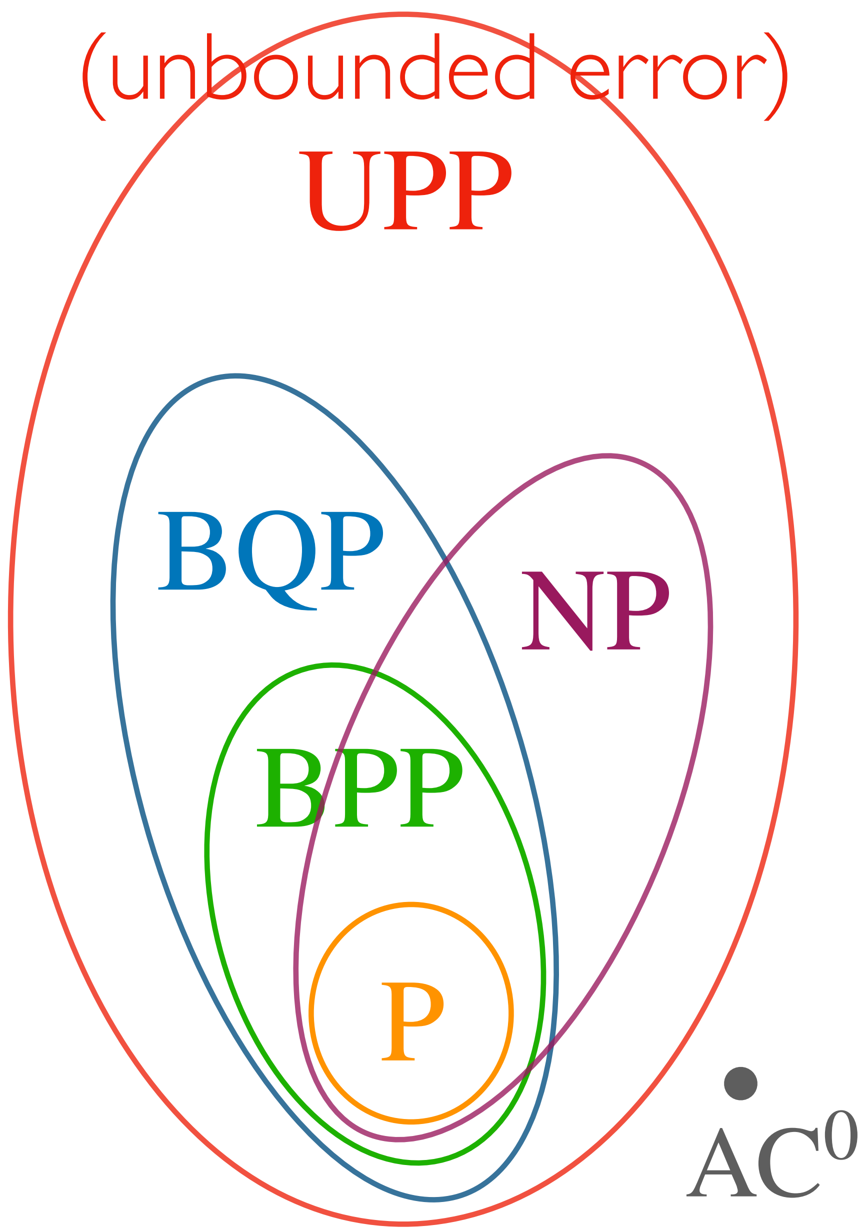
- In communication world,

  $P \subsetneq BPP \subseteq BQP \subsetneq UPP$,

  $P \subsetneq NP \subsetneq UPP$.

Unbounded-error communication

[Babai-Frankl-Simon '86]



- UPP research frontier

  Result 1: $\mathrm{AC}^0 \notin \mathrm{UPP}$

- In communication world,

  $\mathrm{P} \subsetneq \mathrm{BPP} \subseteq \mathrm{BQP} \subsetneq \mathrm{UPP}$,

  $\mathrm{P} \subsetneq \mathrm{NP} \subsetneq \mathrm{UPP}$.

  Result 2: quantum advantage in communication world

Roadmap

- UPP Unbounded-error comm.
- BQP vs. BPP communication

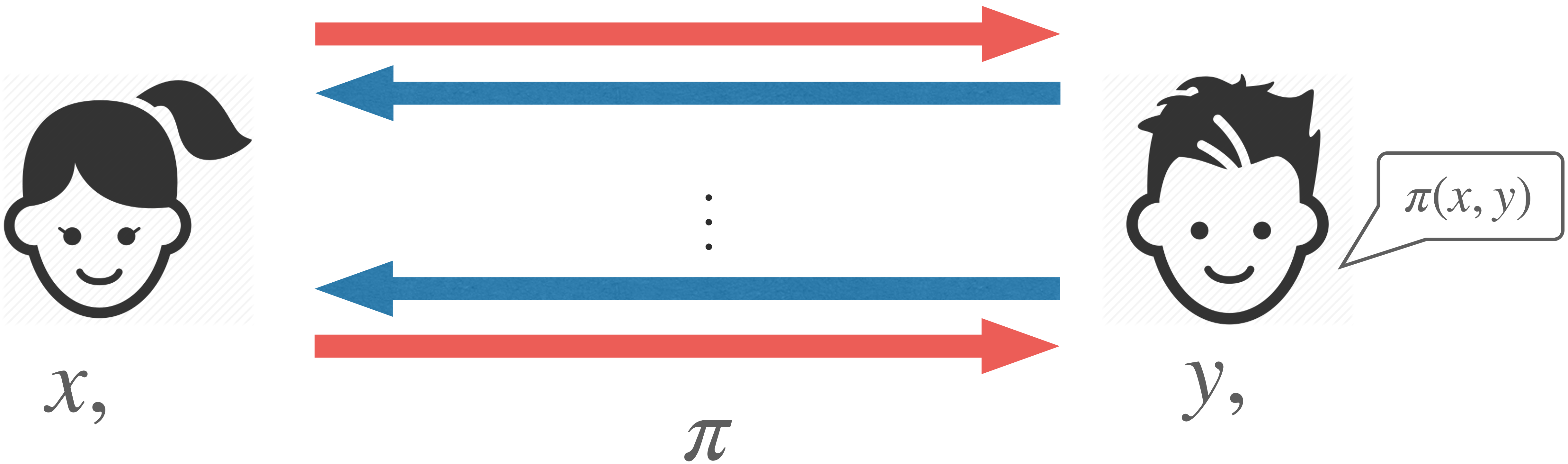
Roadmap

- UPP Unbounded-error comm.
- BQP vs. BPP communication

Unbounded-error communication

[Babai-Frankl-Simon '86]

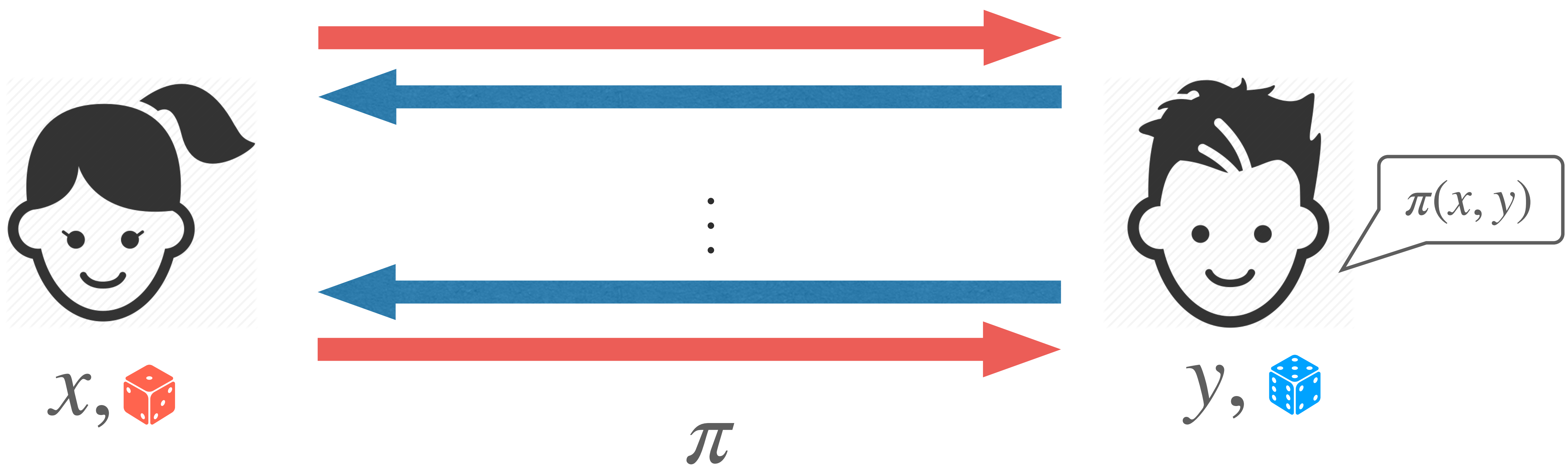
$f : X \times Y \to \{0,1\}$



Unbounded-error communication

[Babai-Frankl-Simon '86]

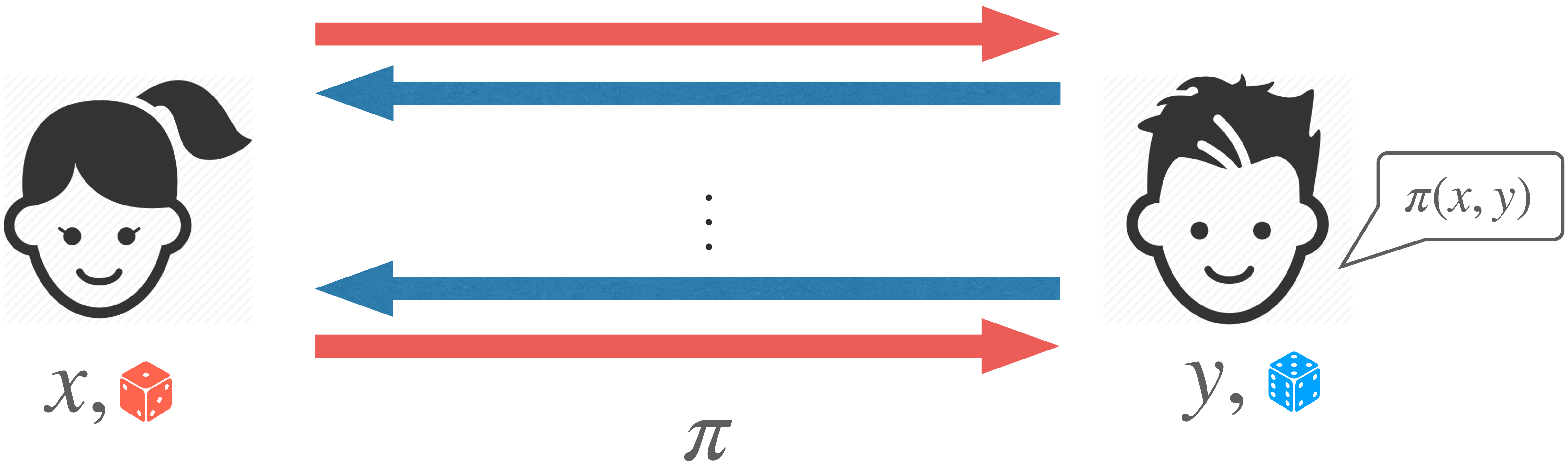
$f : X \times Y \to \{0,1\}$



Unbounded-error communication

[Babai-Frankl-Simon '86]

$f : X \times Y \to \{0,1\}$

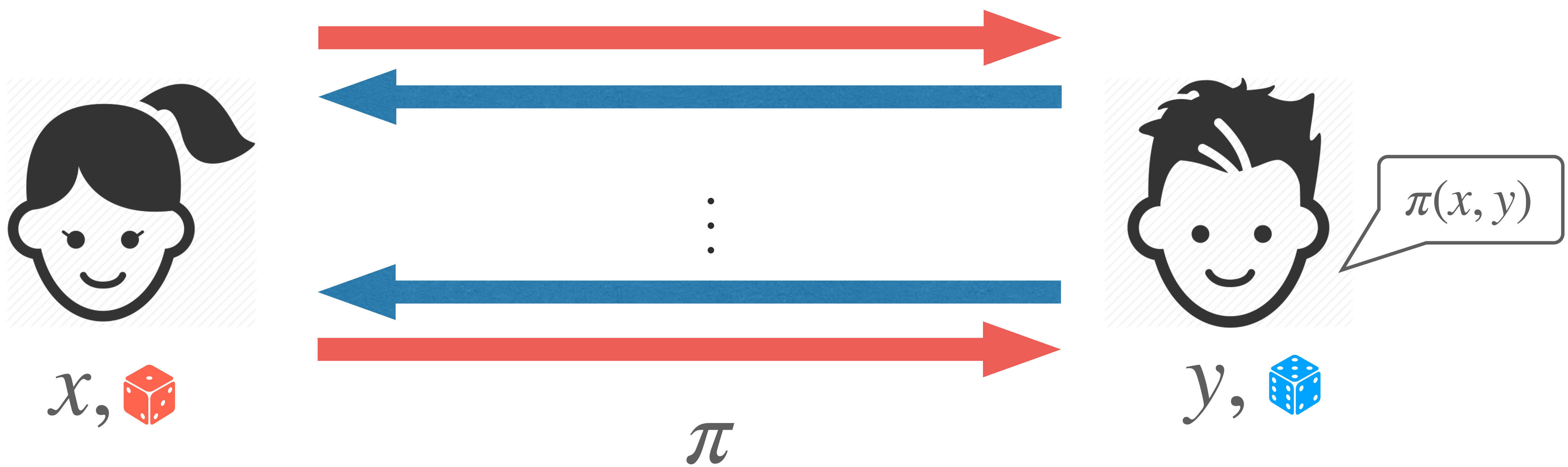


Correctness: $\Pr[\pi(x,y) = f(x,y)] > \dfrac{1}{2}, \ \forall x, y\,.$

Unbounded-error communication

[Babai-Frankl-Simon '86]

$f : X \times Y \to \{0,1\}$



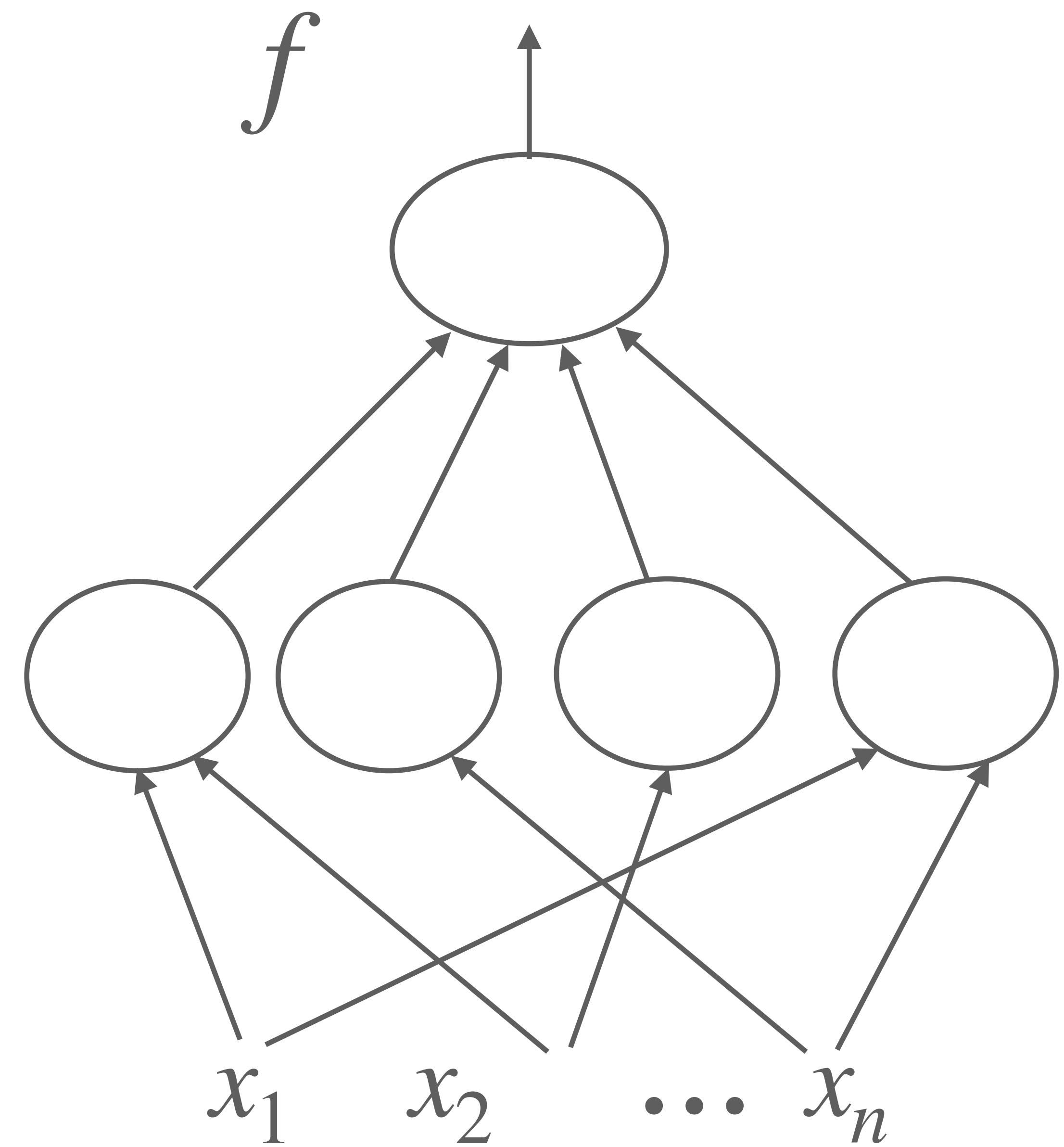
Correctness: $\Pr[\pi(x, y) = f(x, y)] > \frac{1}{2}, \forall x, y$.

Barely larger than guess

Unbounded-error communication

$f:\{0,1\}^n \to \{0,1\}$

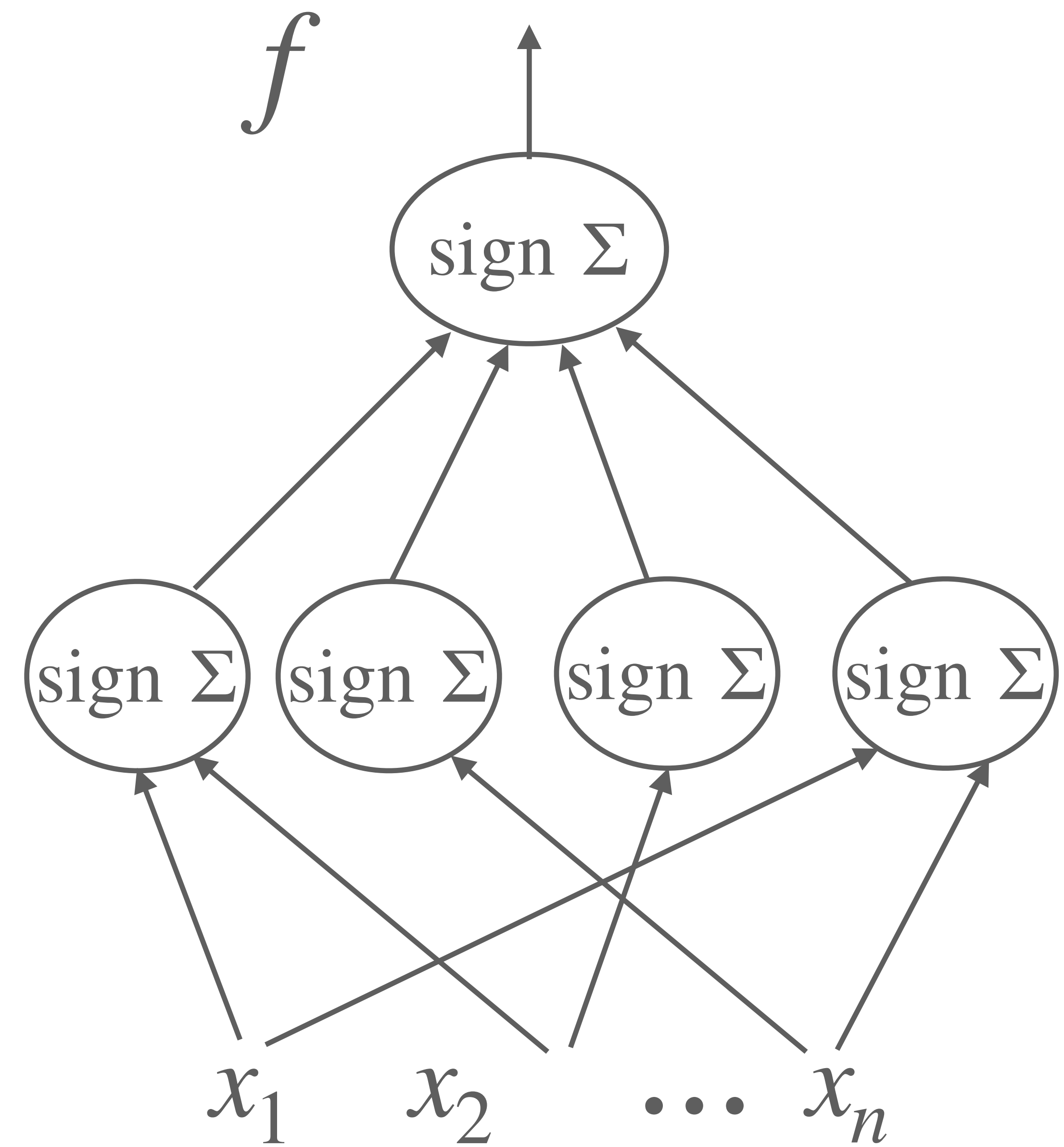
A simple neural network



Unbounded-error communication

$f : \{0,1\}^n \to \{0,1\}$

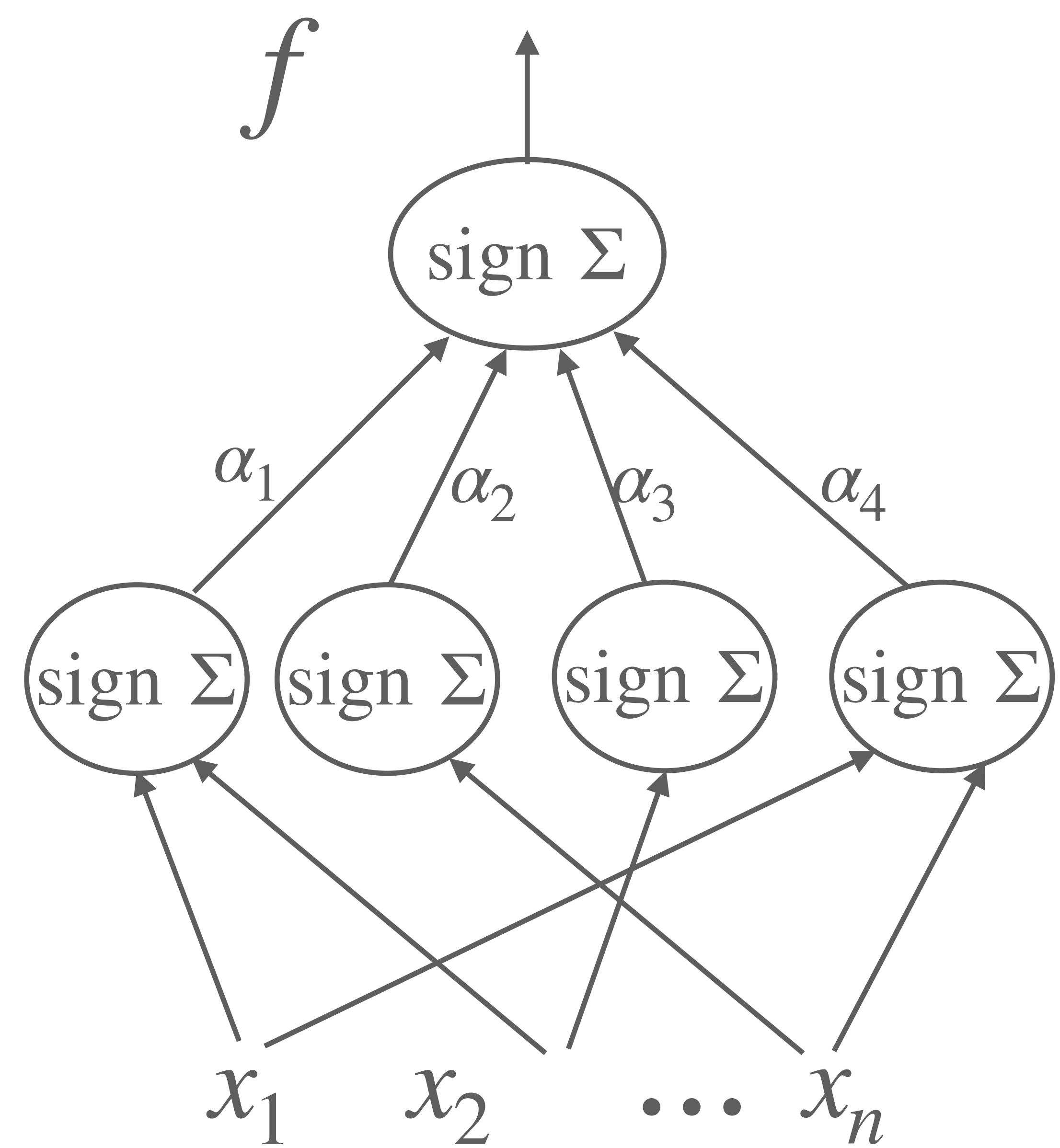
A simple neural network



Unbounded-error communication

$f : \{0,1\}^n \to \{0,1\}$

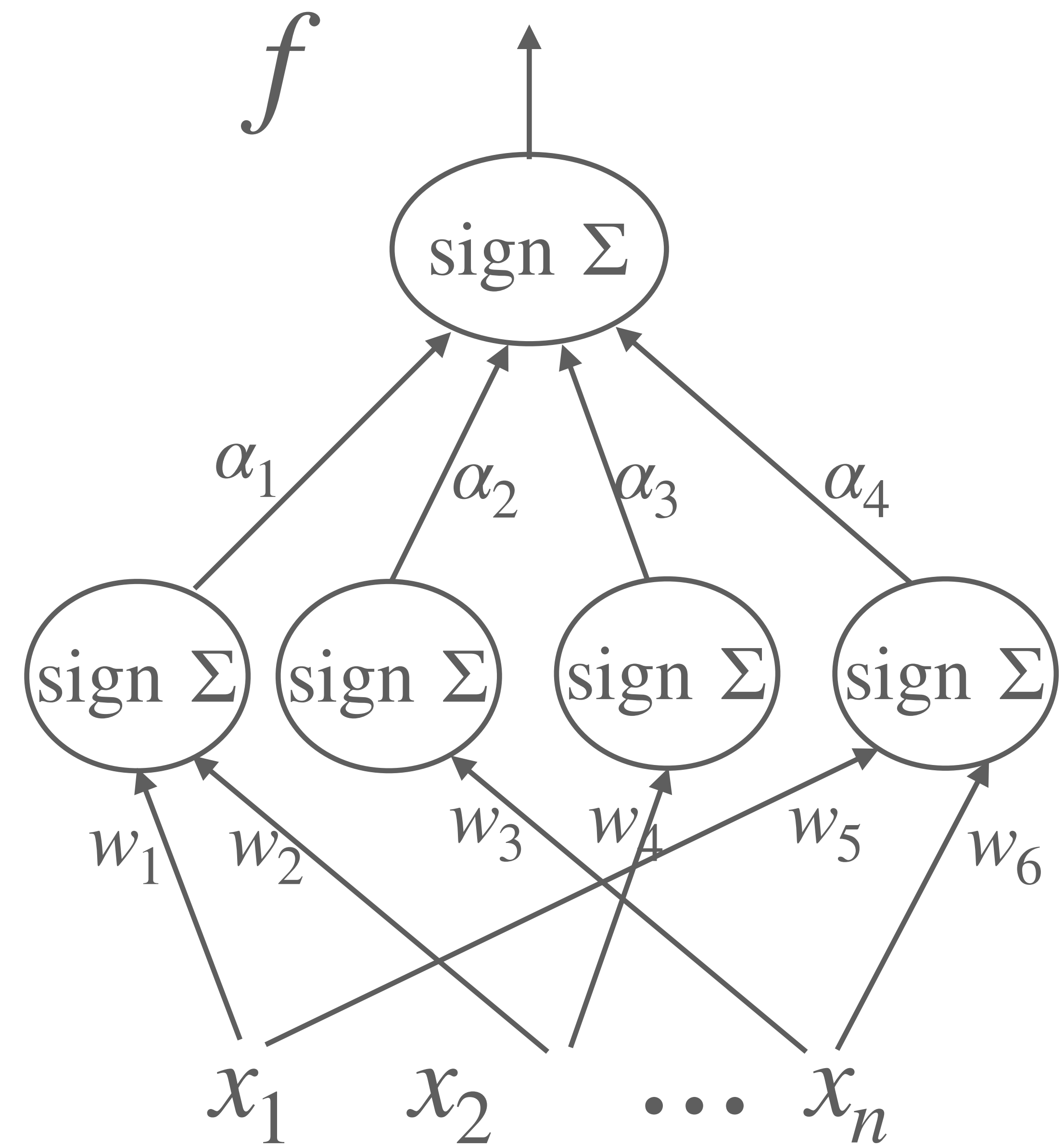
A simple neural network



Unbounded-error communication

$f : \{0,1\}^n \to \{0,1\}$

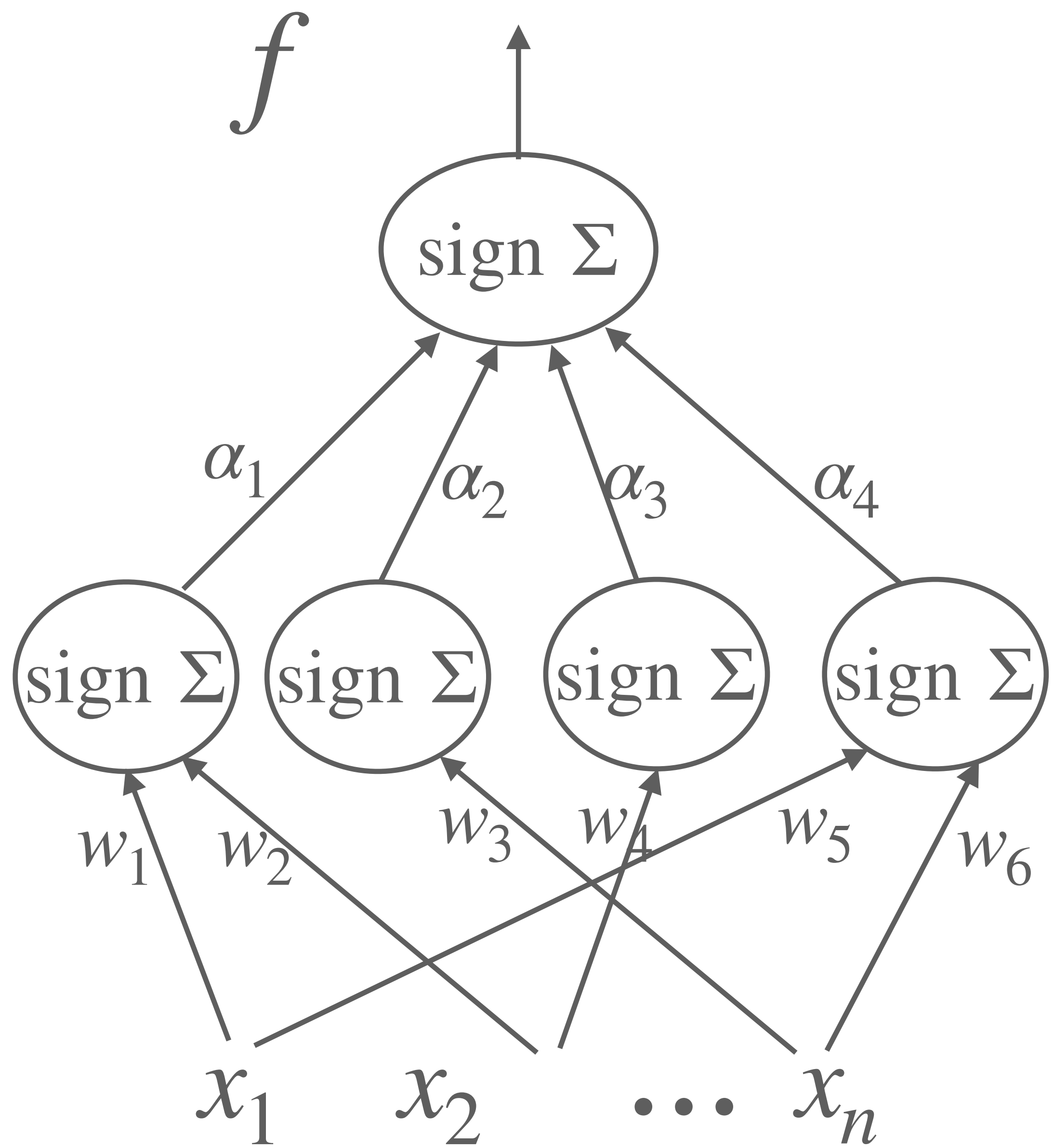
A simple neural network



Unbounded-error communication

$f : \{0,1\}^n \to \{0,1\}$

A simple neural network



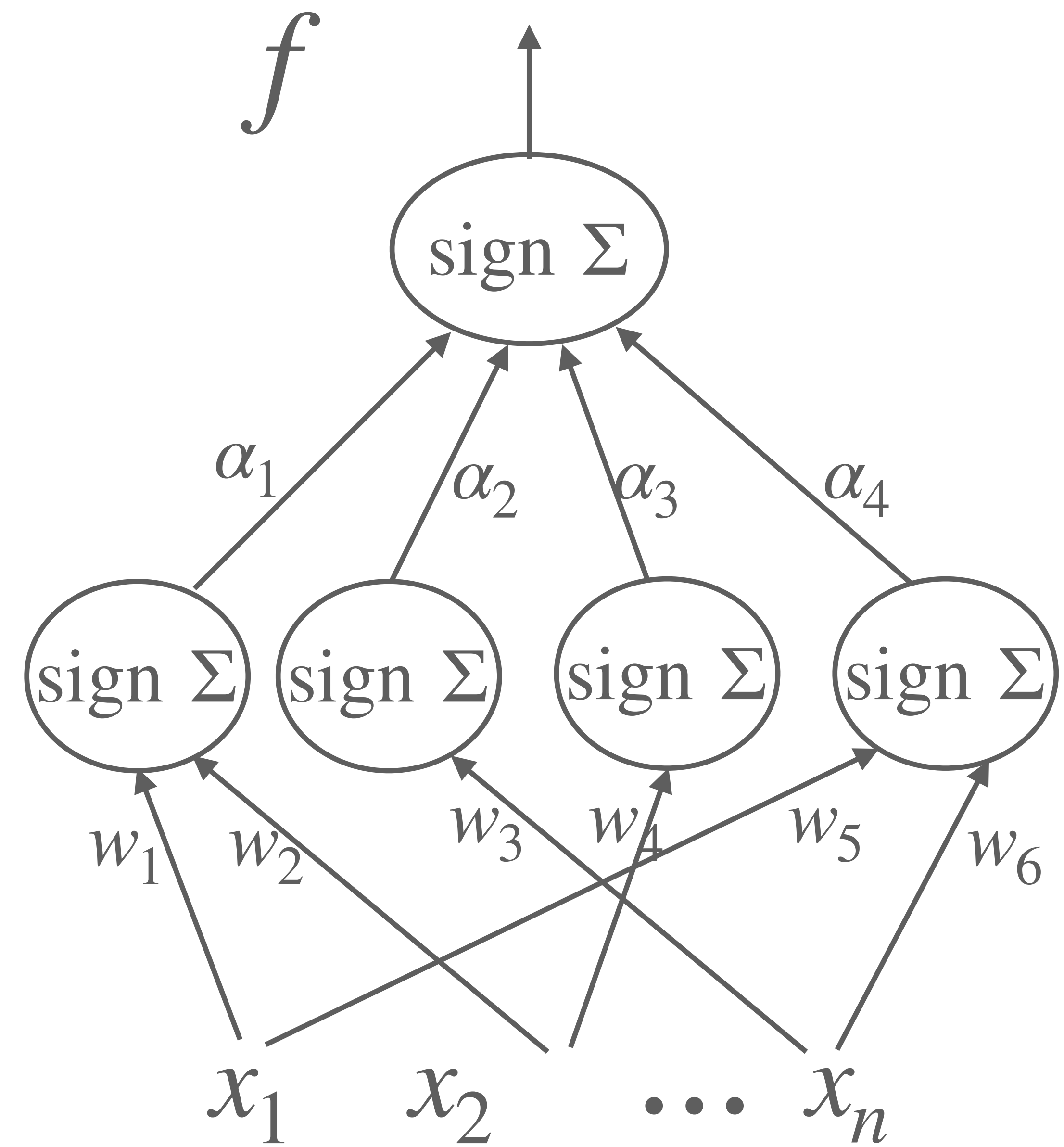
Unbounded-error communication

$f : \{0,1\}^n \to \{0,1\}$

$x_1 \ldots x_{n/2}$

$x_{n/2+1} \cdots x_n$

A simple neural network



Unbounded-error communication

$f : \{0,1\}^n \to \{0,1\}$

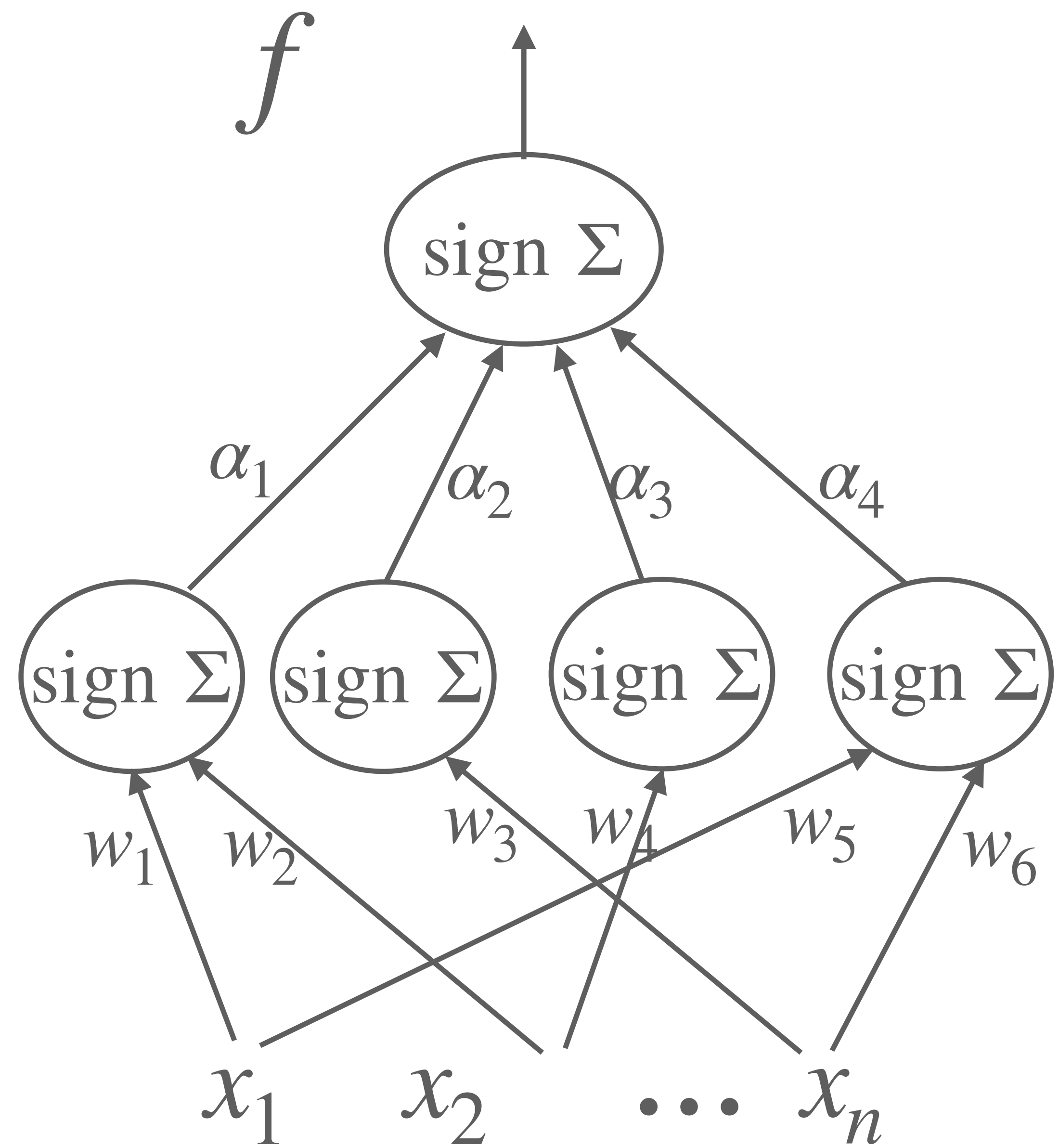
$x_1 \ldots x_{n/2}$

$x_{n/2+1} \cdots x_n$

Theorem * (Forster et al. '01).

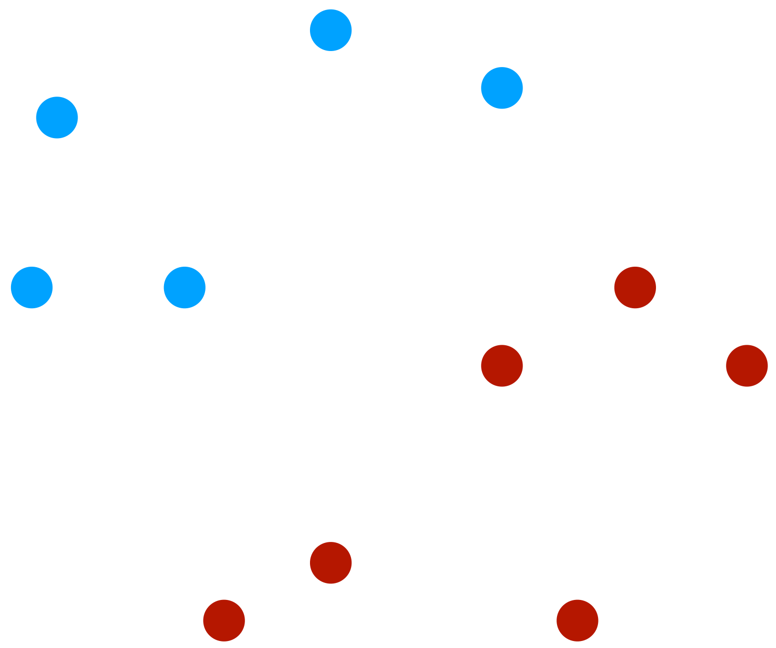
$\mathrm{size}(f) \gtrsim 2^{\Omega(U(f))}$.

A simple neural network



Unbounded-error communication

Learn halfspaces

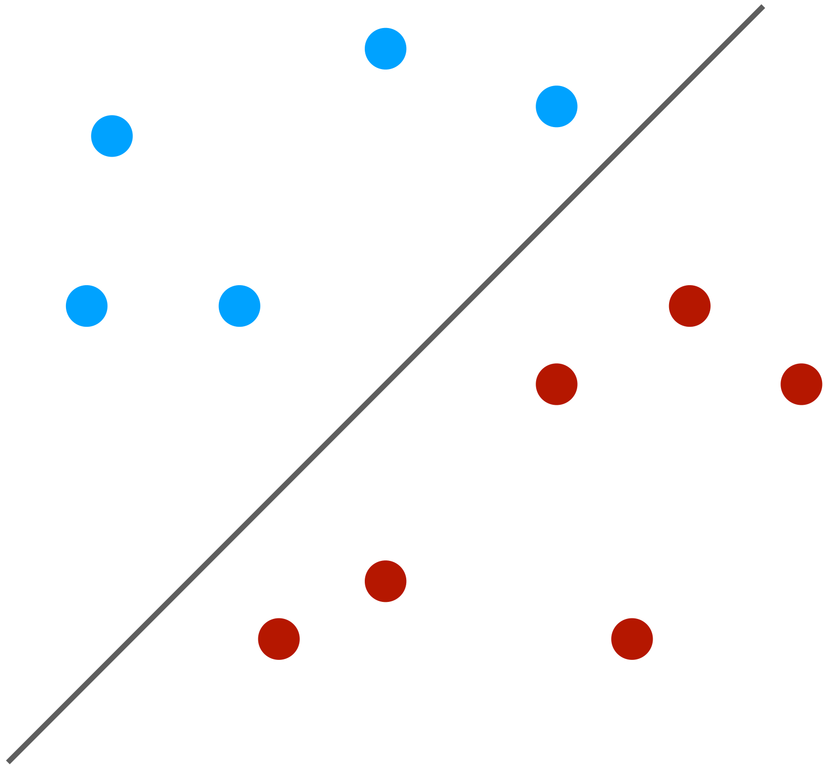


$$a_1x_1 + a_2x_2 + a_3x_3 + a_0 \geq 0$$

learn the coefficients a

Unbounded-error communication

Learn halfspaces

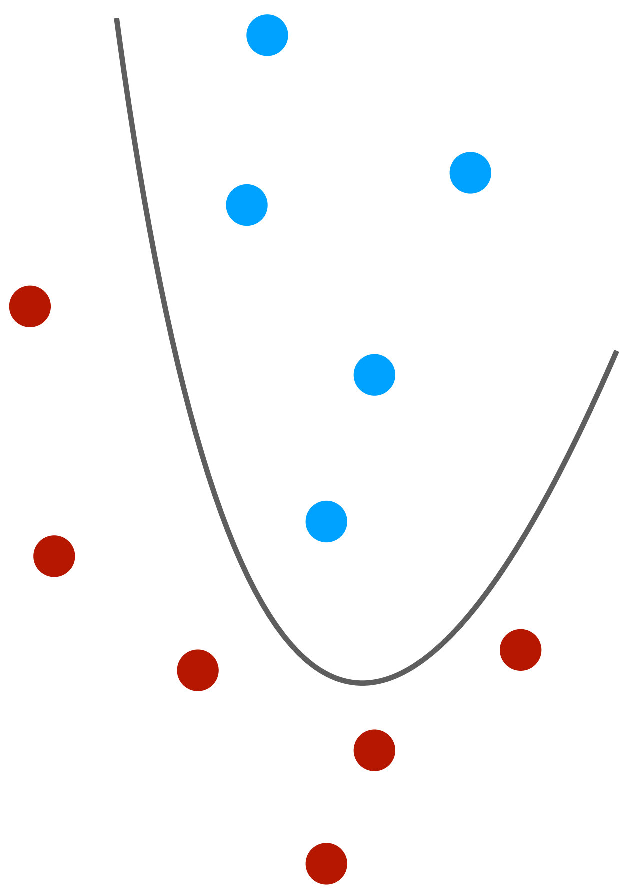


$$a_1x_1 + a_2x_2 + a_3x_3 + a_0 \geq 0$$

learn the coefficients a

Unbounded-error communication

Learn low degree polynomials

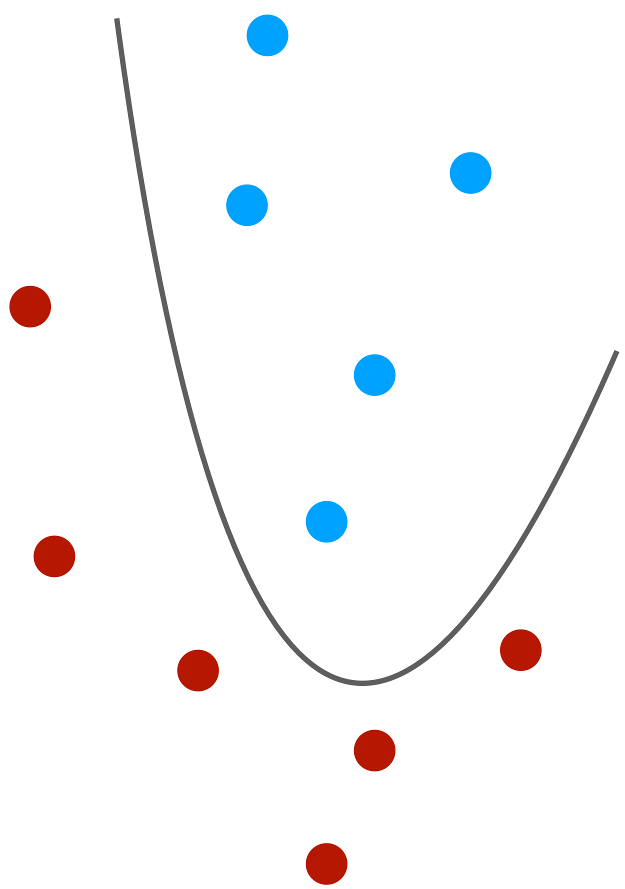


$$a_1x_1 + a_2x_2 + a_3x_3 + a_{12} \cdot x_1x_2 + \\ a_{13} \cdot x_1x_3 + a_{23} \cdot x_2x_3 \geq 0$$

learn the coefficients a

Unbounded-error communication

Learn low degree polynomials

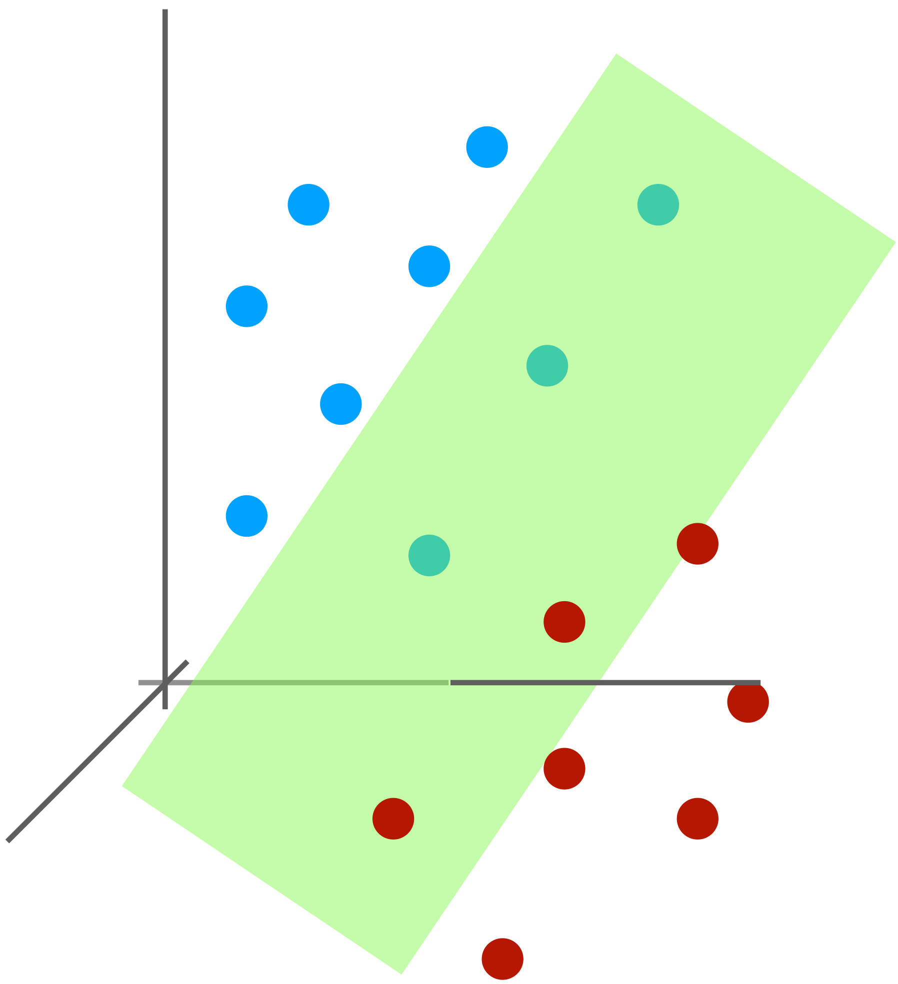


$$a_1x_1 + a_2x_2 + a_3x_3 + a_{12} \cdot \overset{y_{12}}{\cancel{x_1x_2}} +$$
$$a_{13} \cdot \underset{y_{13}}{\cancel{x_1x_3}} + a_{23} \cdot \underset{y_{23}}{\cancel{x_2x_3}} \geq 0$$

learn the coefficients a

Unbounded-error communication

Learn low degree polynomials

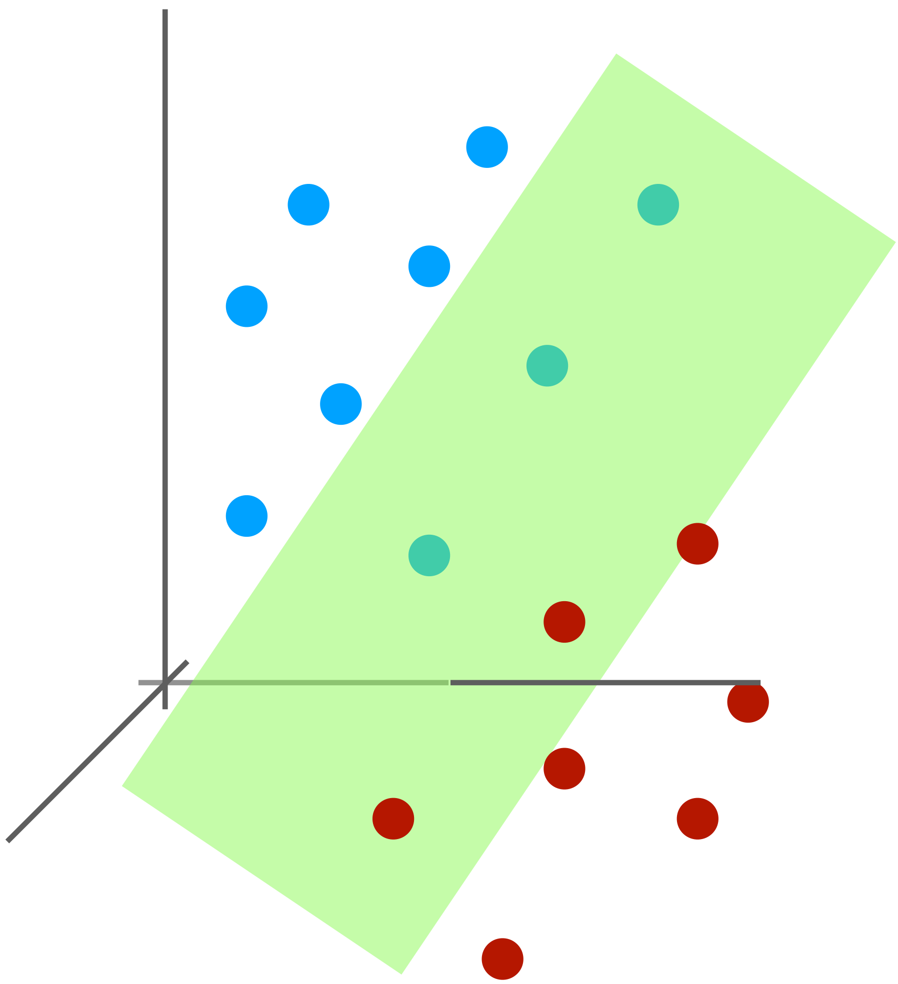


$$a_1x_1 + a_2x_2 + a_3x_3 + a_{12}\cdot \overset{y_{12}}{\cancel{x_1x_2}} +$$
$$a_{13}\cdot \underset{y_{13}}{\cancel{x_1x_3}} + a_{23}\cdot \underset{y_{23}}{\cancel{x_2x_3}} \geq 0$$

learn the coefficients a

Unbounded-error communication

Learn low degree polynomials



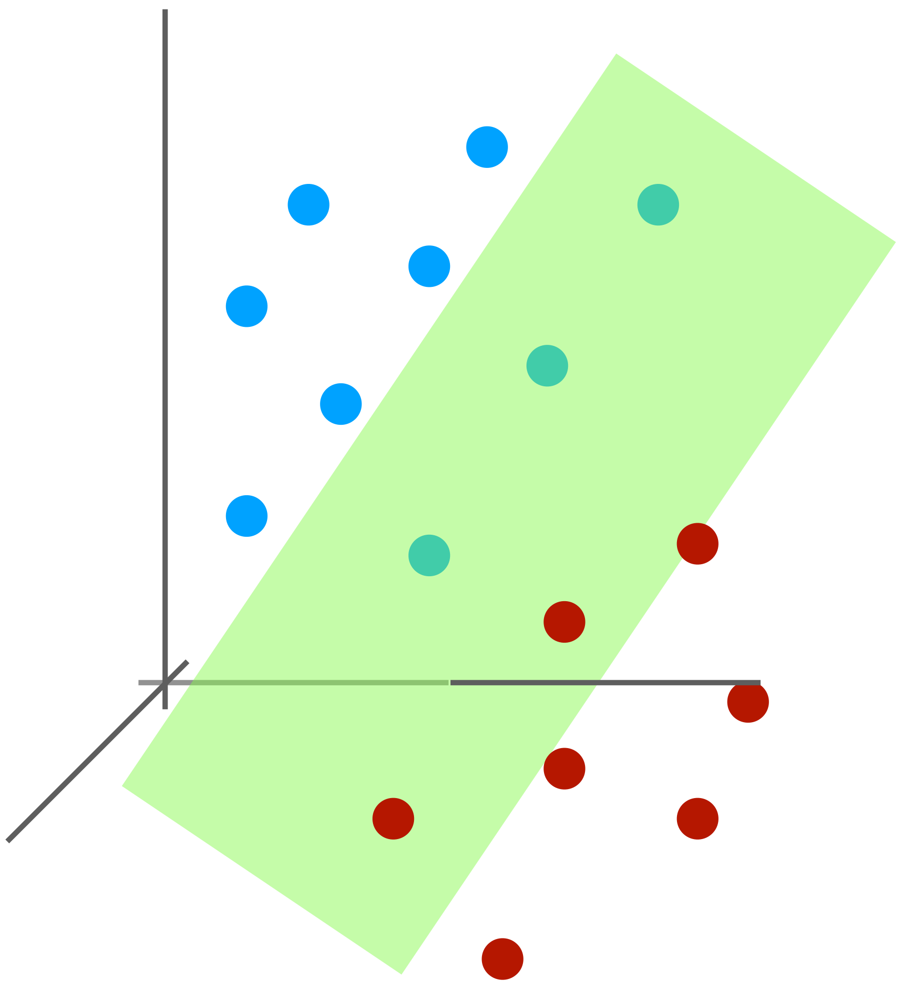
$$a_1x_1 + a_2x_2 + a_3x_3 + a_{12}\cdot \overset{y_{12}}{\cancel{x_1x_2}} +$$
$$a_{13}\cdot \underset{y_{13}}{\cancel{x_1x_3}} + a_{23}\cdot \underset{y_{23}}{\cancel{x_2x_3}} \geq 0$$

Def. $f : \{0,1\}^n \to \{0, 1\}$,
$\deg_{\pm}(f)$: min degree of a separating curve

learn the coefficients a

Unbounded-error communication

Embedding into spaces with larger dimension



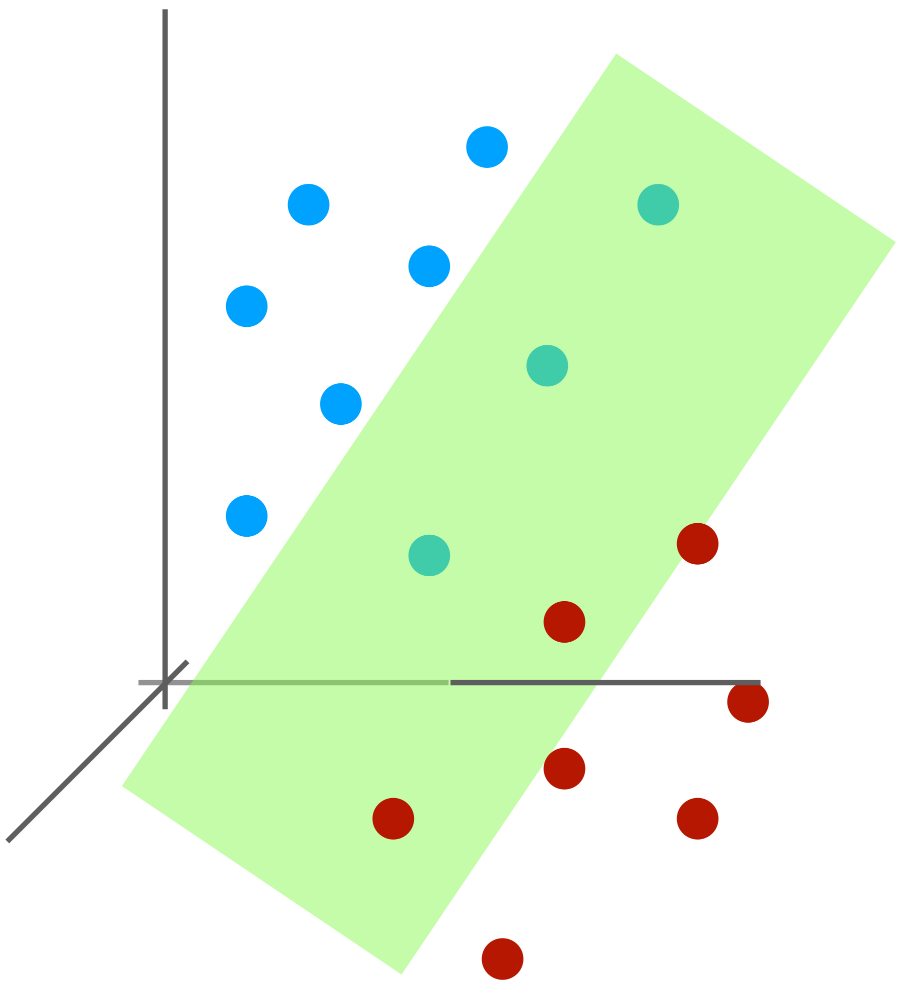
Dimension complexity

$\mathscr{C}$ concept class,

$\mathbf{dc}(\mathscr{C})$ minimum dimension for such embedding

Unbounded-error communication

Embedding into spaces with
larger dimension

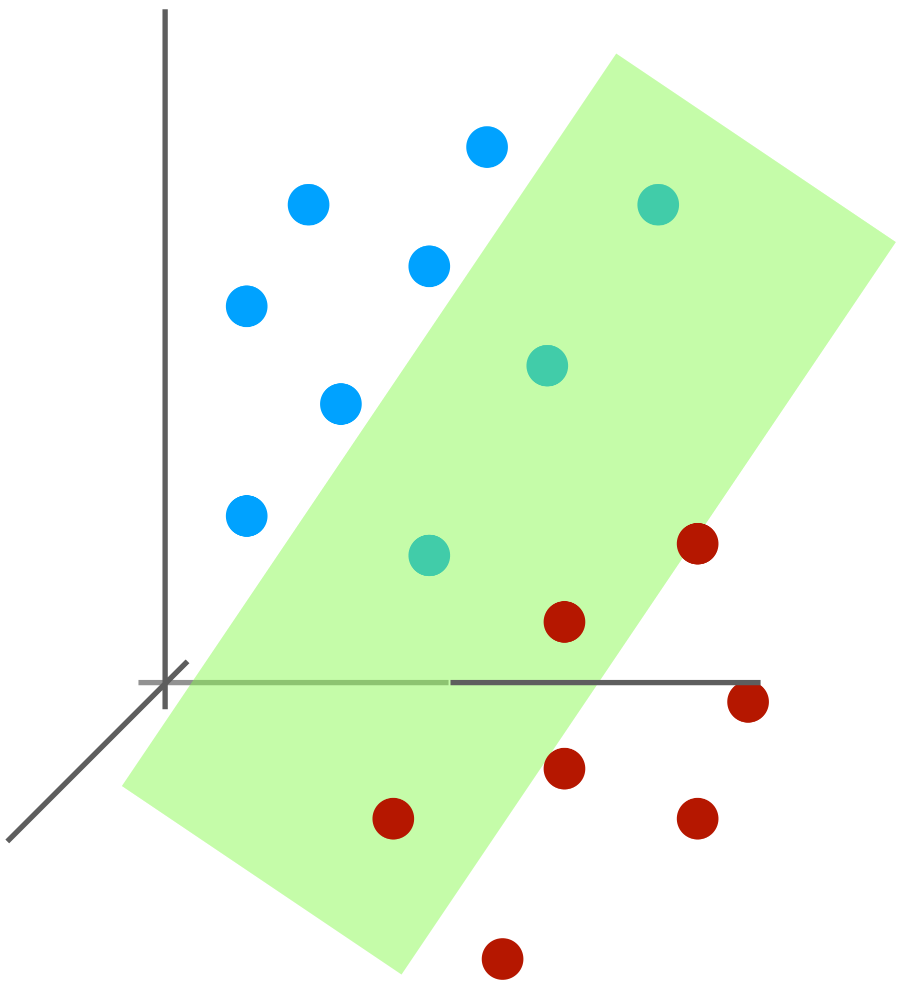


Dimension complexity
$\mathscr{C}$ concept class,
$\mathbf{dc}(\mathscr{C})$ minimum dimension
for such embedding

Surprisingly powerful!
Captures many results in PAC
learning model.

Unbounded-error communication

Embedding into spaces with larger dimension



Dimension complexity
$\mathscr{C}$ concept class,
$\mathbf{dc}(\mathscr{C})$ minimum dimension for such embedding

Fact (folklore).
$\mathrm{dc}(\mathscr{C}) = 2^{\Theta(U(M_{\mathscr{C}}))}$,
where $M_{\mathscr{C}}(f, x) = f(x)$.

$f \in \mathscr{C}$

x

goal: output f(x)

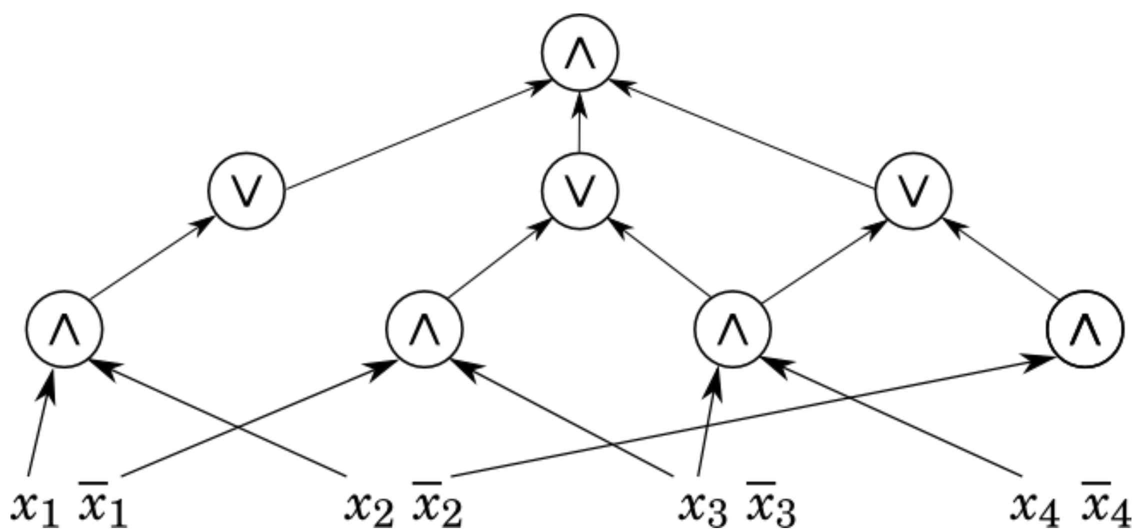
Unbounded-error communication

Theorem (Sherstov-W. 19)
$\mathrm{U}(\mathrm{AC}^0) \geq \Omega(n^{1-\epsilon})$.

Unbounded-error communication

Theorem (Sherstov-W. 19)

$\mathrm{U}(\mathrm{AC}^0) \geq \Omega(n^{1-\epsilon})$.

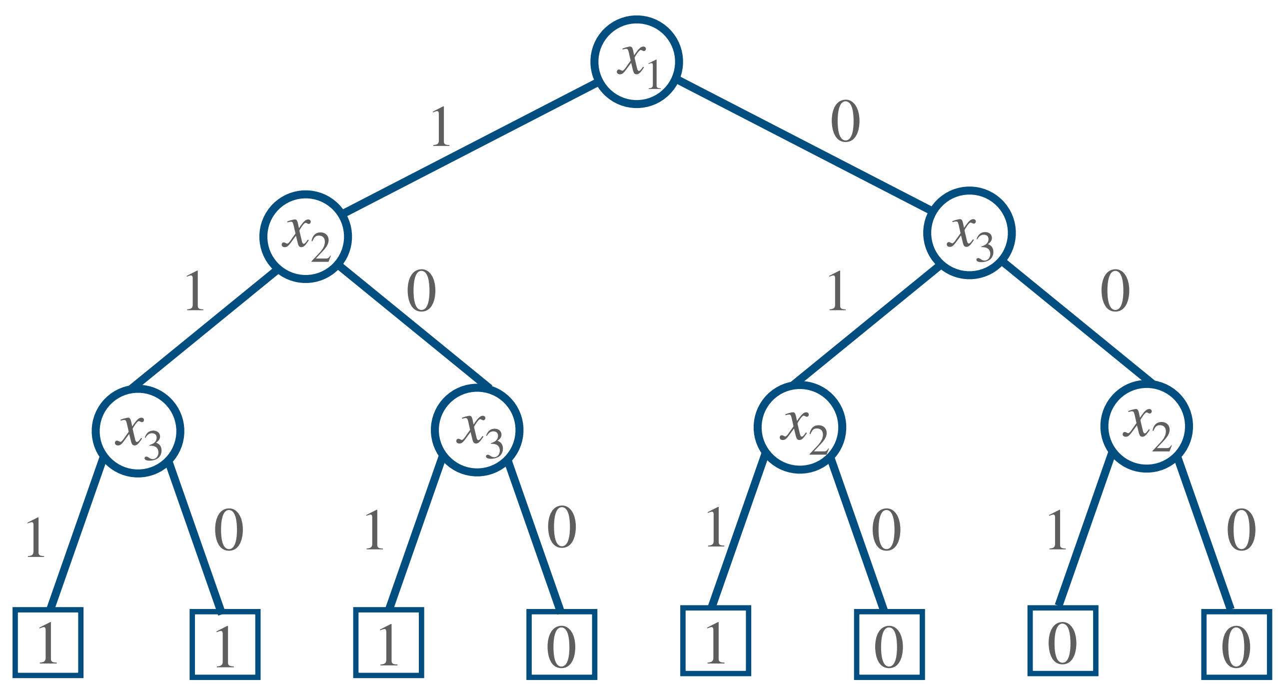


AC^0: constant depth, polynomial #gates ($\wedge$, $\vee$, $\neg$)

Unbounded-error communication

Theorem (Sherstov-W. 19)

$\mathrm{U}(\mathrm{AC}^0) \geq \Omega(n^{1-\epsilon})\,.$

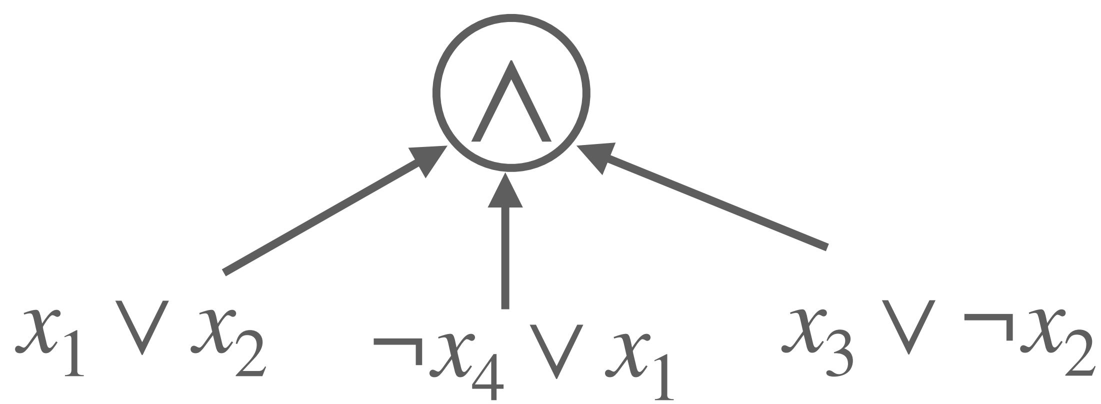


a decision tree

Unbounded-error communication

Theorem (Sherstov-W. 19)

$\mathrm{U}(\mathrm{AC}^0) \geq \Omega(n^{1-\epsilon})$.

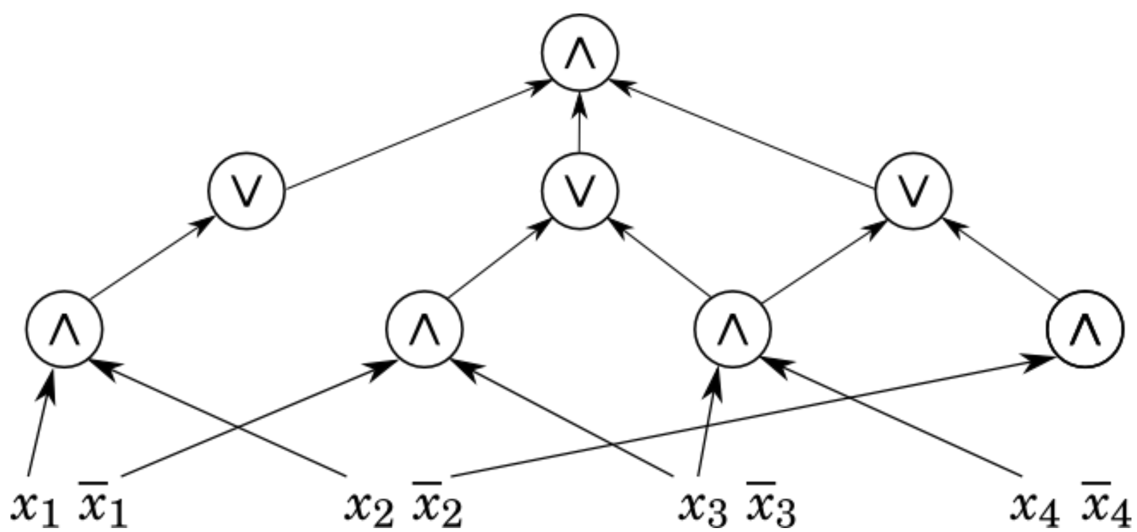


a CNF

Unbounded-error communication

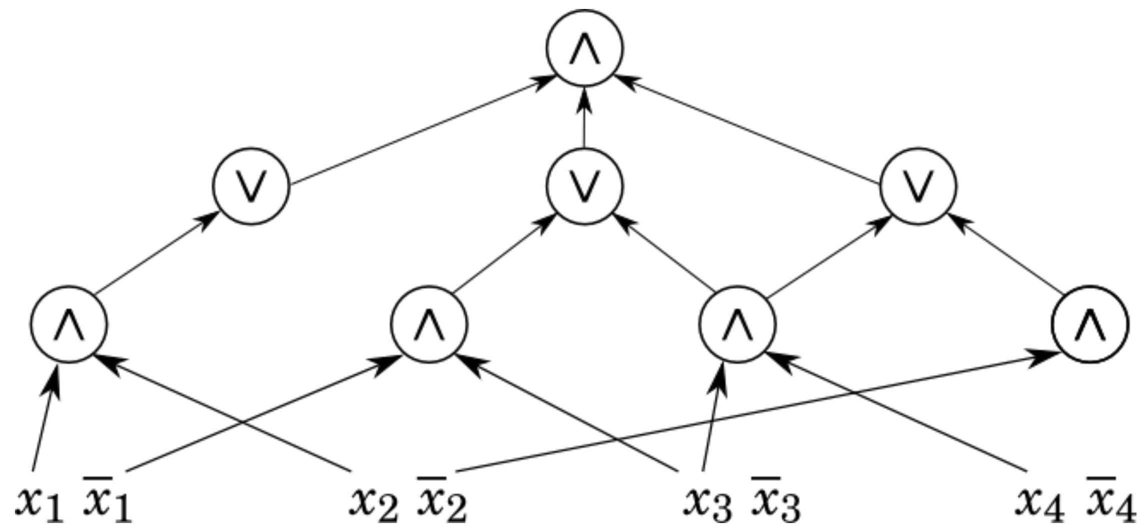
Theorem (Sherstov-W. 19)

$\mathrm{U}(\mathrm{AC}^0) \geq \Omega(n^{1-\epsilon})$.



AC^0: constant depth, polynomial #gates ($\wedge$, $\vee$, $\neg$)

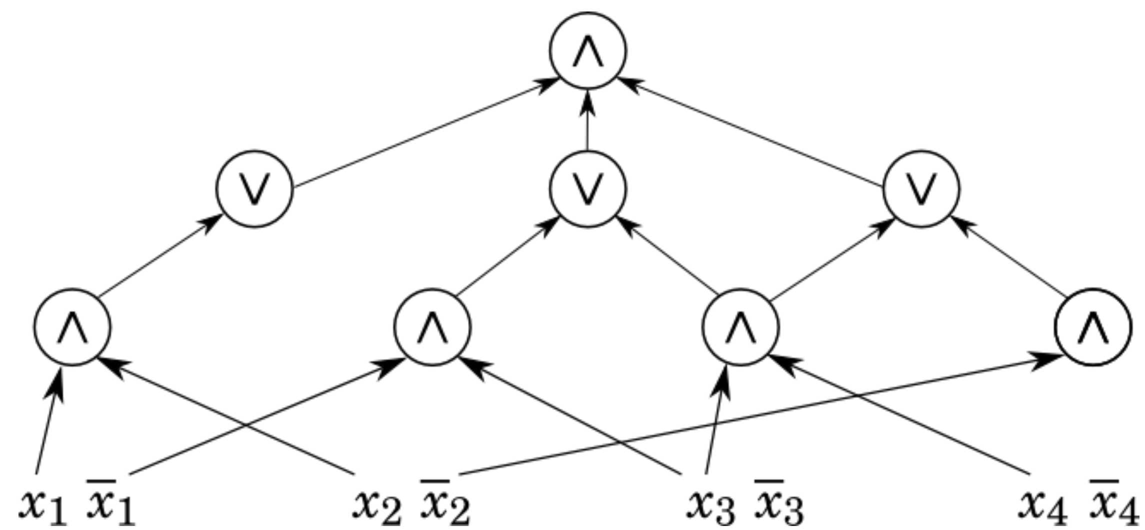
Constant depth circuits (AC^0)



Circuits lower bound "P vs NP"

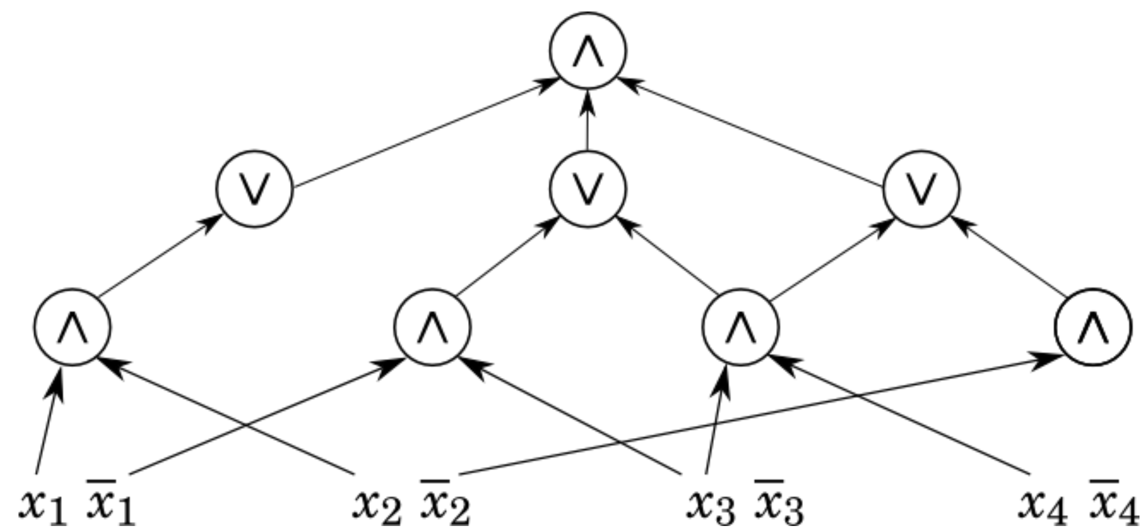
[FSS84, Ajt83, Yao85, Has86, Aar10, RS10, LV11, BIL12, IMP12, Has14, AA15, LRR17, Ros18, Vio18]

Constant depth circuits (AC^0)



Circuits lower bound "P vs NP"	[FSS84, Ajt83, Yao85, Has86, Aar10, RS10, LV11, BIL12, IMP12, Has14, AA15, LRR17, Ros18, Vio18]
"P vs BPP"	[LN90, Nis91, Baz07, Raz08, Bra09, ETT10, GMR13, TX13, Tal14, CSV15, HS16, Tal17, ST18, DHH18, Lyu22]

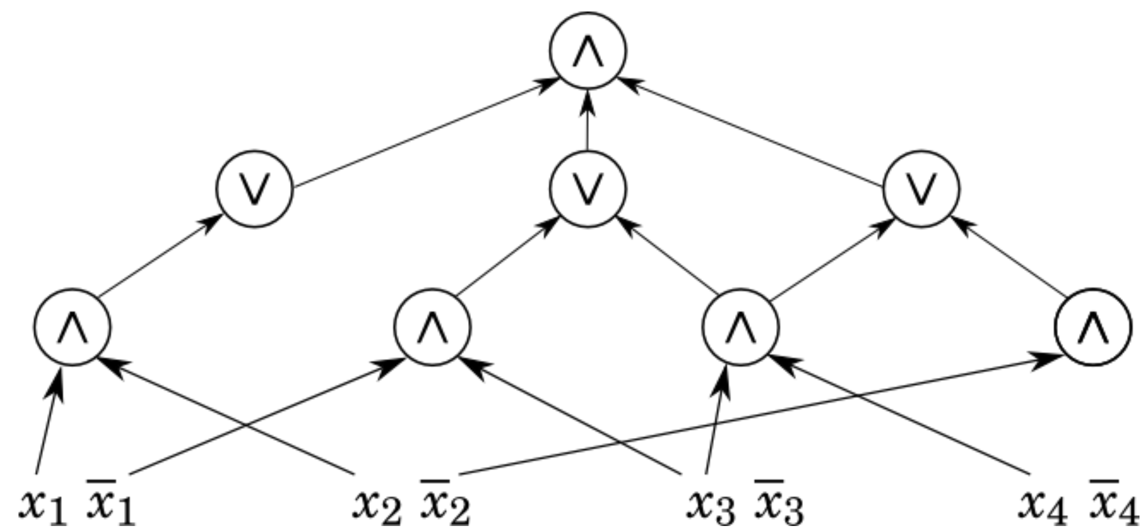
Constant depth circuits (AC^0)



Quantum advantage

[AS04, Amb07, ACR+10, BM10, Rei10, Bel12, BS13, RT19]

Constant depth circuits (AC^0)



Quantum advantage	[AS04, Amb07, ACR+10, BM10, Rei10, Bel12, BS13, RT19]
Learning	[LMN93, Jac02, BES03, OS03, KOS04, KS04, LMSS07, AMY16, DRG17, AGS20]

……

Threshold degree of AC^0

Theorem (Sherstov-W. 19).
$\deg_{\pm}(\mathrm{AC}^0) = \Omega(n^{1-\epsilon})$.

Threshold degree of AC^0

Theorem (Sherstov-W. 19).
$\deg_{\pm}(\mathrm{AC}^0) = \Omega(n^{1-\epsilon})$.

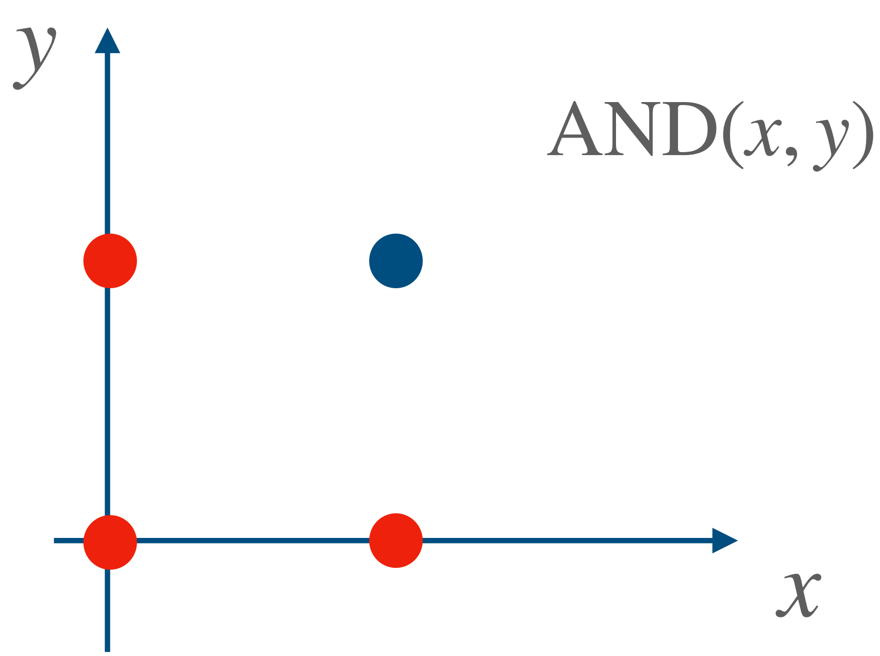
Definition.
$\deg_{\pm}(f) = \min\{\deg p : p(x) \cdot (-1)^{f(x)} > 0, \ \forall x \in X\}$.

Threshold degree of AC^0

Definition.
$\deg_{\pm}(f) = \min\{\deg p : p(x) \cdot (-1)^{f(x)} > 0,\ \forall x \in X\}$.

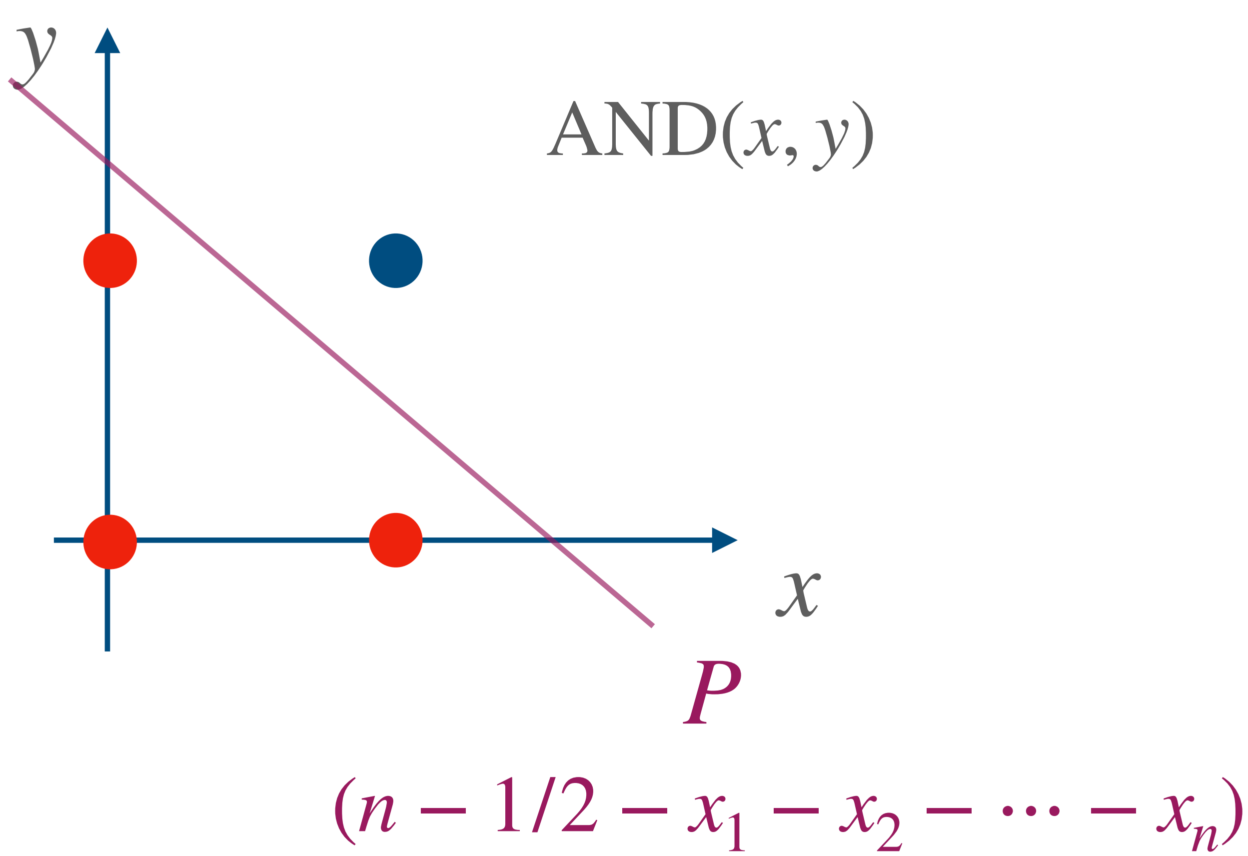
Threshold degree of AC^0

Definition.
$\deg_{\pm}(f) = \min\{\deg p : p(x) \cdot (-1)^{f(x)} > 0,\ \forall x \in X\}$.



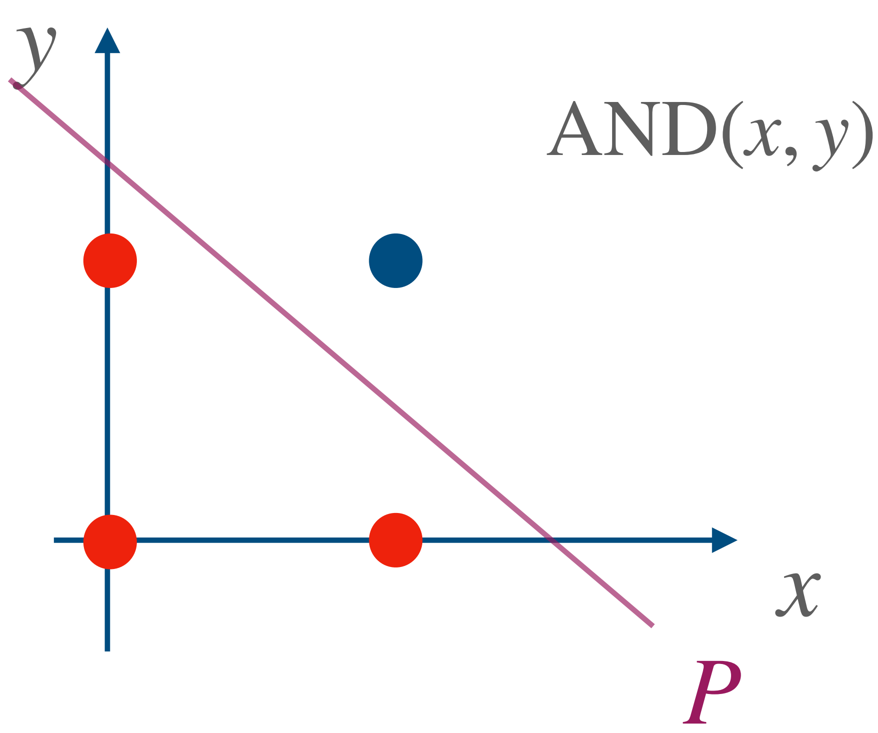
Threshold degree of AC^0

Definition.
$\deg_{\pm}(f) = \min\{\deg p : p(x) \cdot (-1)^{f(x)} > 0, \ \forall x \in X\}$.



Threshold degree of AC^0

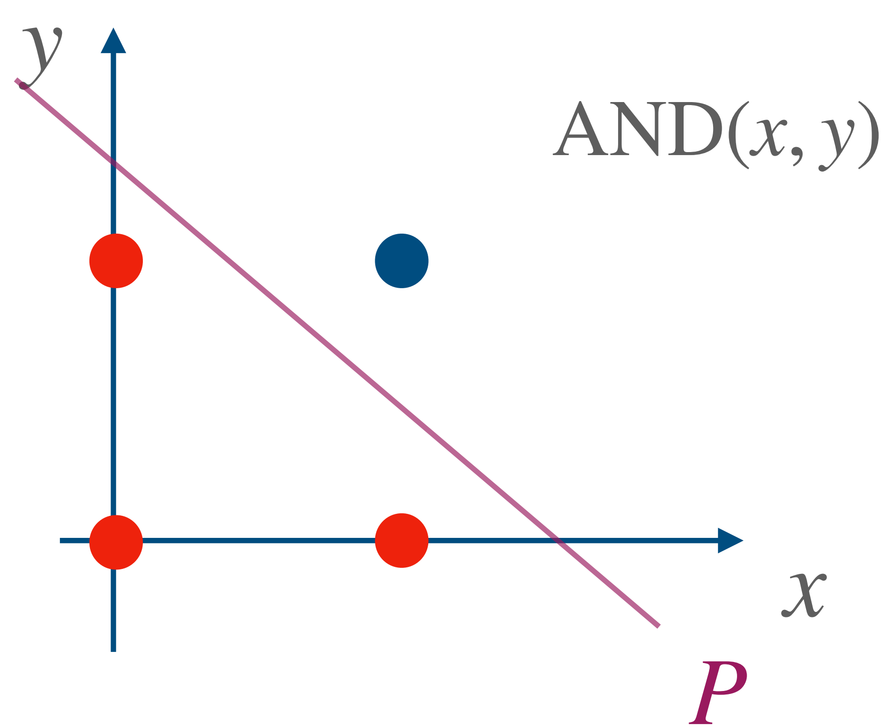
Definition.
$\deg_{\pm}(f) = \min\{\deg p : p(x) \cdot (-1)^{f(x)} > 0,\ \forall x \in X\}$.



$(-1)^{\mathrm{AND}(x)} \cdot (n - 1/2 - x_1 - x_2 - \cdots - x_n) > 0$

Threshold degree of AC^0

Definition.
$\deg_\pm(f) = \min\{\deg p : p(x)\cdot(-1)^{f(x)} > 0,\ \forall x \in X\}$.

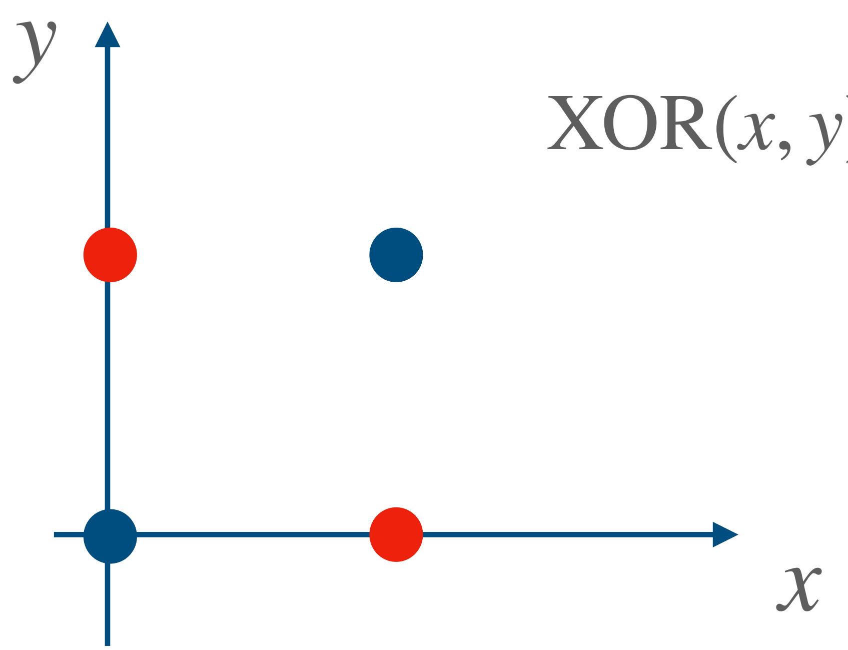


$(-1)^{\mathrm{AND}(x)} \cdot (n - 1/2 - x_1 - x_2 - \cdots - x_n) > 0$

$\deg_\pm(\mathrm{AND}(x)) = 1.$

Threshold degree of AC^0

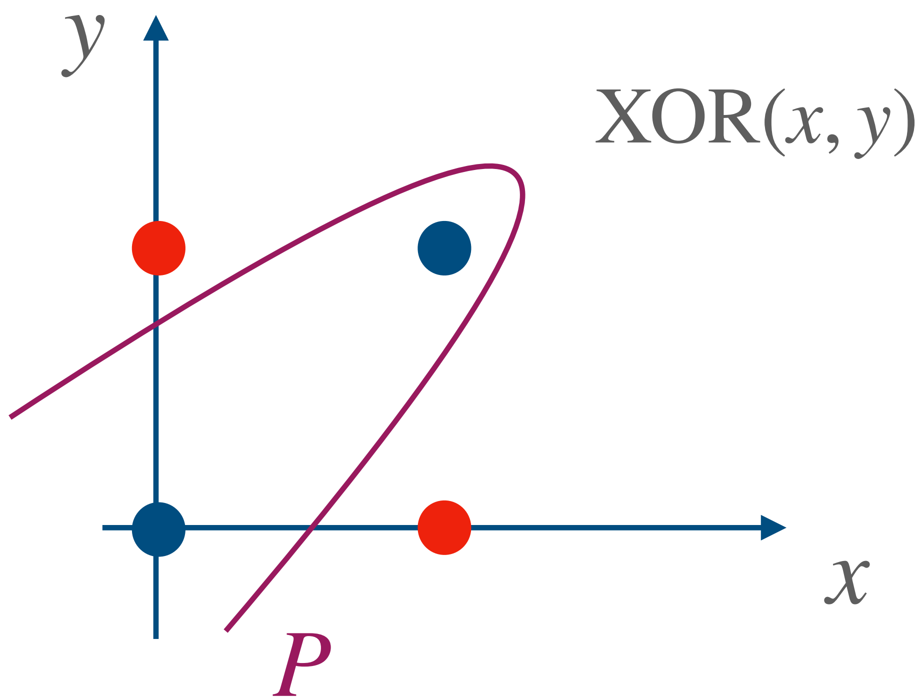
Definition.
$\deg_{\pm}(f) = \min\{\deg p : p(x) \cdot (-1)^{f(x)} > 0,\ \forall x \in X\}$.



$\mathrm{XOR}(x, y)$

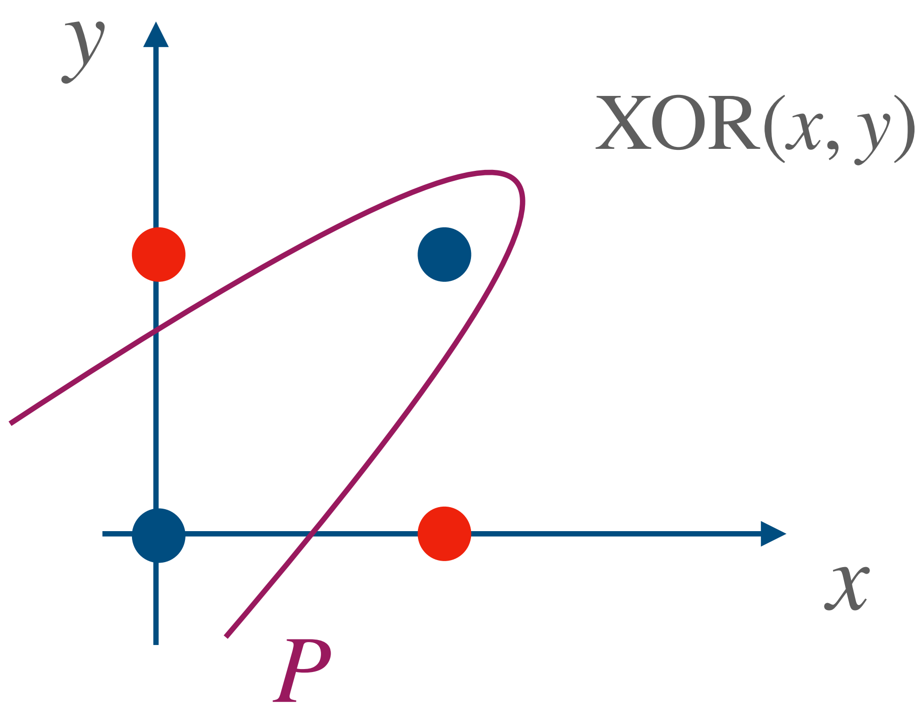
Threshold degree of AC^0

Definition.
$\deg_{\pm}(f) = \min\{\deg p : p(x) \cdot (-1)^{f(x)} > 0,\ \forall x \in X\}$.



Threshold degree of AC^0

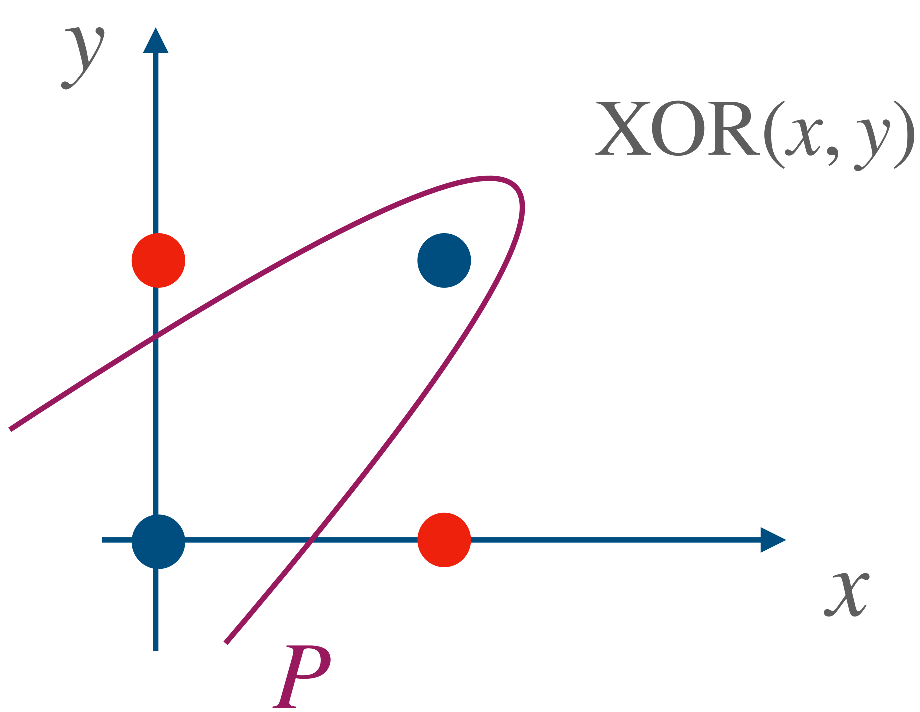
Definition.
$\deg_{\pm}(f) = \min\{\deg p : p(x) \cdot (-1)^{f(x)} > 0,\ \forall x \in X\}$.



$\deg_{\pm}(\mathrm{XOR}(x)) = n$.

Threshold degree of AC^0

Definition.
$\deg_{\pm}(f) = \min\{\deg p : p(x) \cdot (-1)^{f(x)} > 0,\ \forall x \in X\}$.

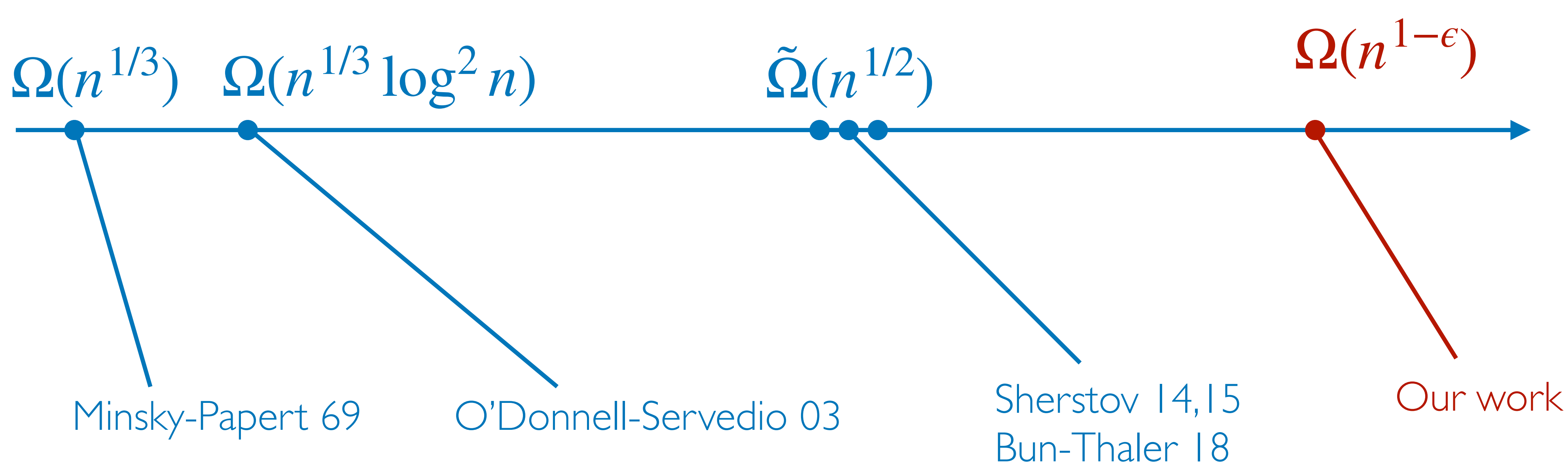


Prob. Minsky-Papert 69
Max threshold degree of AC^0?

$\deg_{\pm}(\mathrm{XOR}(x)) = n$.

Threshold degree of AC^0

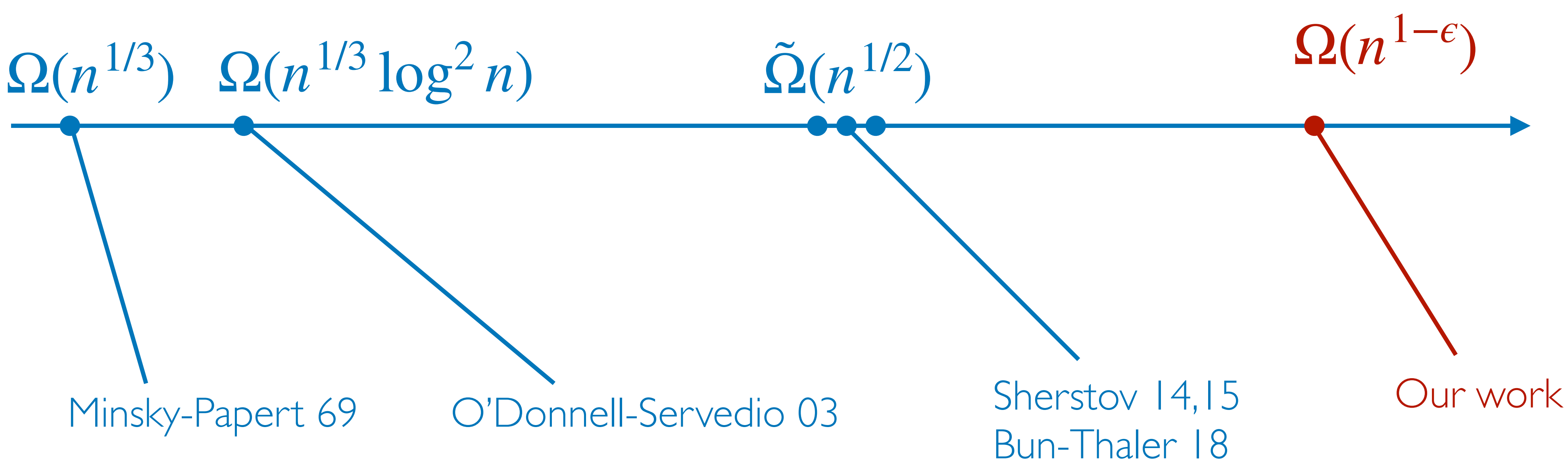
Theorem (Sherstov-W. 19).
$\deg_{\pm}(\mathrm{AC}^0) = \Omega(n^{1-\epsilon})$.



Threshold degree of AC^0

Theorem (Sherstov-W. 19).
$\deg_{\pm}(\mathrm{AC}^0) = \Omega(n^{1-\epsilon})$.

Trivial bound:
$\deg_{\pm}(f) \leq n$.



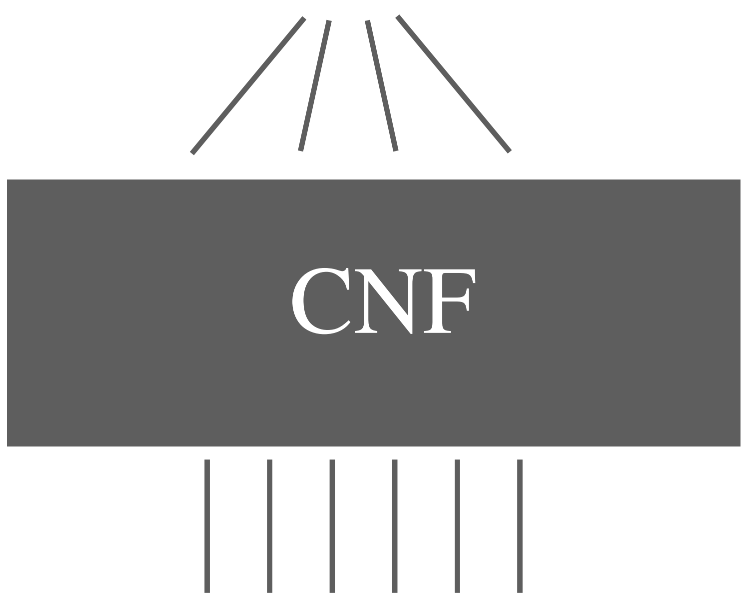
Proof Sketch: Hardness amplification

Given $f : \{0,1\}^n \to \{0,1\}, \qquad \deg_{\pm}(f) = n^{1-\epsilon}$

Proof Sketch: Hardness amplification

Given $f : \{0,1\}^n \to \{0,1\}, \qquad \deg_{\pm}(f) = n^{1-\epsilon}$

Then $F = \quad f$

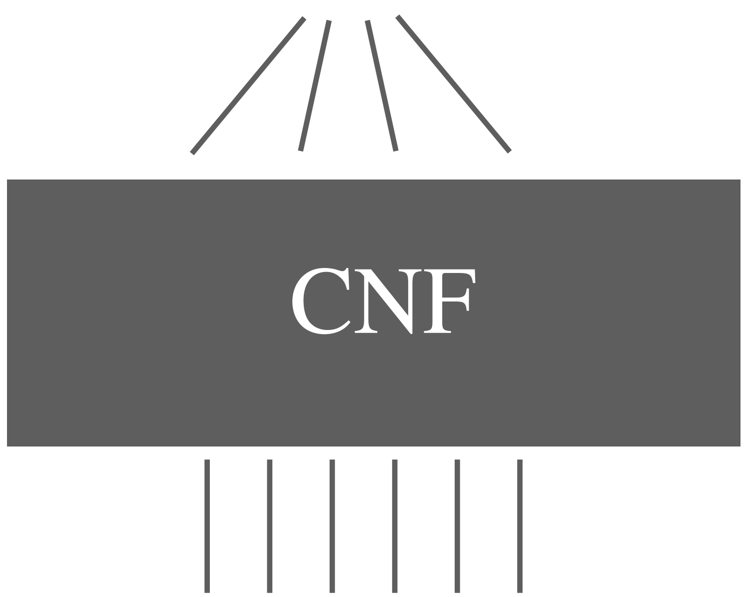


$y \in \{0,1\}^N$

Proof Sketch: Hardness amplification

Given $f : \{0,1\}^n \to \{0,1\}$, $\qquad \deg_\pm(f) = n^{1-\epsilon}$

Then $F = \quad f$



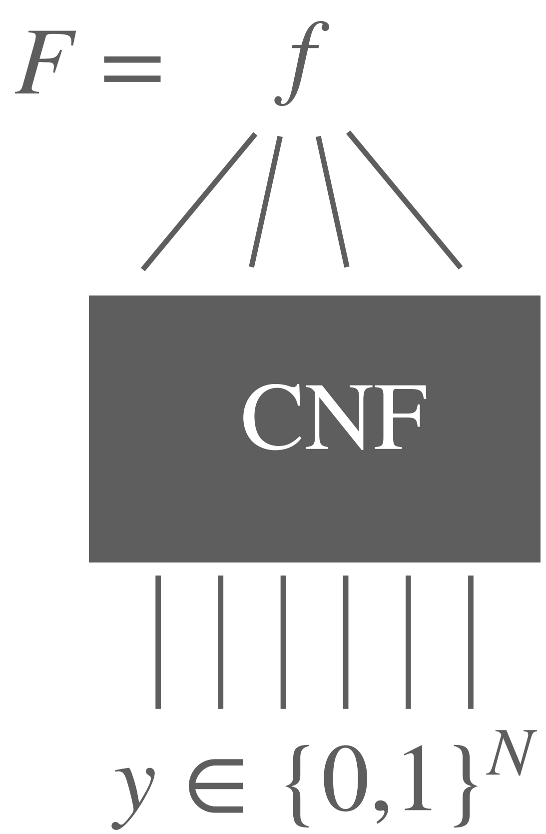
$y \in \{0,1\}^N$

$$\deg_\pm(f \circ \mathrm{CNF}_m) \geq n^{1-\epsilon} \cdot m$$

Proof Sketch: Compression

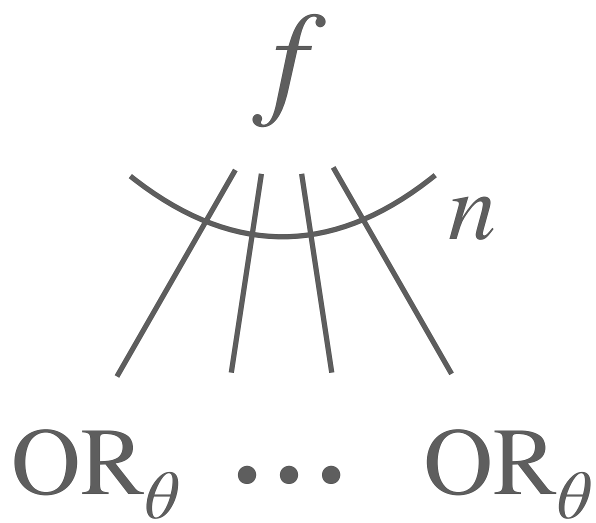
Given $f : \{0,1\}^n \to \{0,1\},$ $\qquad \deg_{\pm}(f) = n^{1-\epsilon}$

Then



$\deg_{\pm}(f \circ \mathrm{CNF}_m) \geq n^{1-\epsilon} \cdot m$

Compression: input transformation

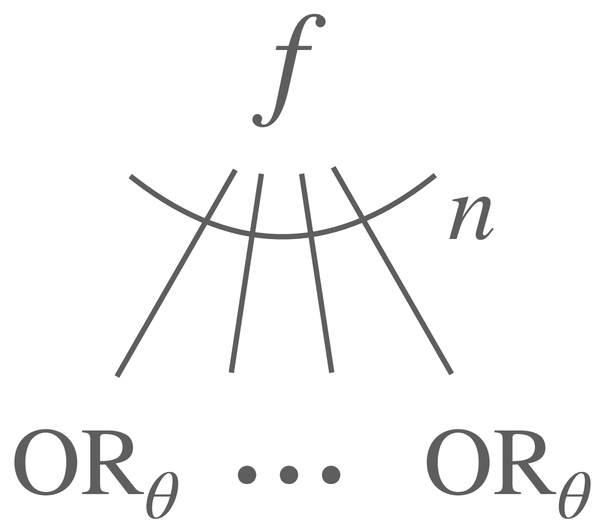


$\boldsymbol{\theta}$

0	1	1	0	0	1	1
0	0	1	1	0	1	0
1	0	1	0	1	0	1
0	1	0	1	1	0	0
0	0	1	0	0	1	1
1	1	0	0	0	1	0
1	1	0	1	1	0	0
0	0	1	1	0	0	1

$\boldsymbol{n}$

Compression: input transformation

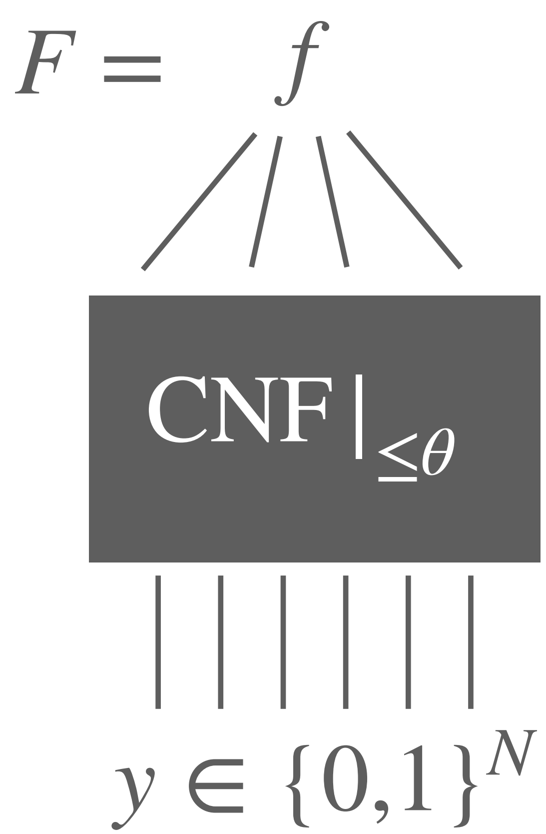


$$\theta \; \underset{\Large n}{\begin{bmatrix} 0&1&1&0&0&1&1\\ 0&0&1&1&0&1&0\\ 1&0&1&0&1&0&1\\ 0&1&0&1&1&0&0\\ 0&0&1&0&0&1&1\\ 1&1&0&0&0&1&0\\ 1&1&0&1&1&0&0\\ 0&0&1&1&0&0&1 \end{bmatrix}} \xrightarrow[\{0,1\}^{\theta\times n}|_{\leq\theta}]{\textit{Restrict}} \begin{bmatrix} 0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&1&0&0&0&0&0\\ 1&0&0&0&0&0&0\\ 0&0&0&0&1&0&0 \end{bmatrix}$$

Proof Sketch: Compression

Given $f : \{0,1\}^n \to \{0,1\},$ $\deg_\pm(f) = n^{1-\epsilon}$

Then



$(f \circ \mathrm{CNF_m})|_{\leq\theta}$

$\deg_\pm(\cancel{f \circ \mathrm{CNF}_m}) \geq n^{1-\epsilon} \cdot m$

More tools from duality.

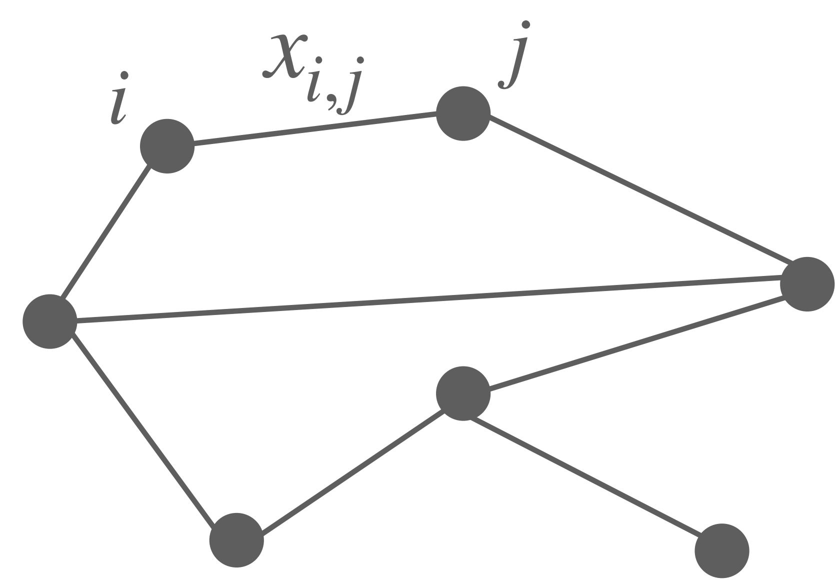
Open problems

Problem:
$\deg_{\pm}(\mathrm{AC}^0) \geq \Omega(n)$?
$\mathrm{U}(\mathrm{AC}^0) \geq \Omega(n)$?

Problem:
$\widetilde{\deg}(\mathrm{AC}^0) \geq \Omega(n)$?

Problem:
Understand depth-2 circuits,
$\widetilde{\deg}(\textit{triangle}) = ?$

Triangle detection problem: Is there a triangle in the graph?



Open problems

Problem:

$\deg_{\pm}(\mathrm{AC}^0) \geq \Omega(n)?$

$\mathrm{U}(\mathrm{AC}^0) \geq \Omega(n)?$

Problem:

$\widetilde{\deg}(\mathrm{AC}^0) \geq \Omega(n)?$

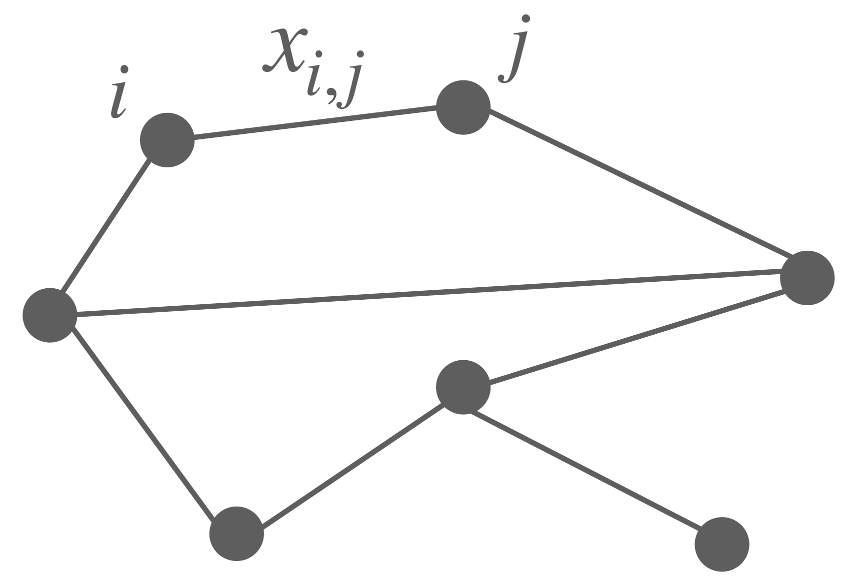
Problem:

Understand depth-2 circuits,

$\widetilde{\deg}(\textit{triangle}) = ?$

Significant in quantum computing

Triangle detection problem: Is there a triangle in the graph?



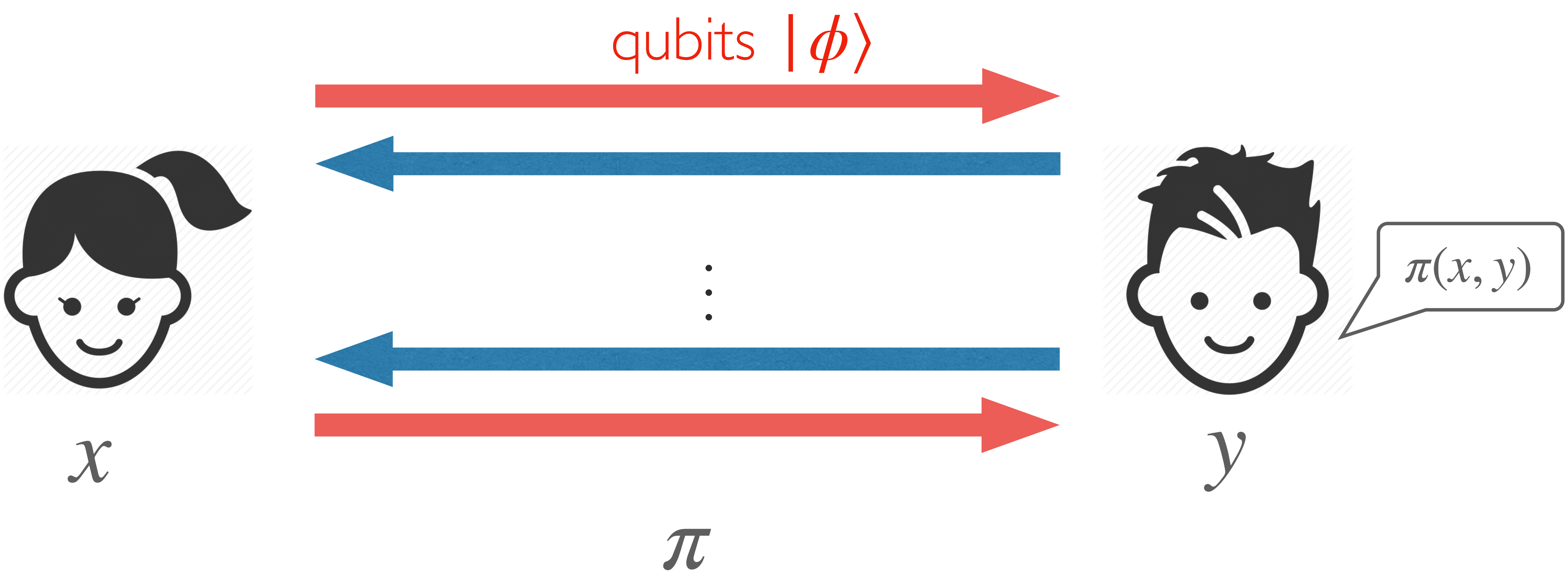
Roadmap

- UPP Unbounded-error comm.
- BQP vs. BPP communication

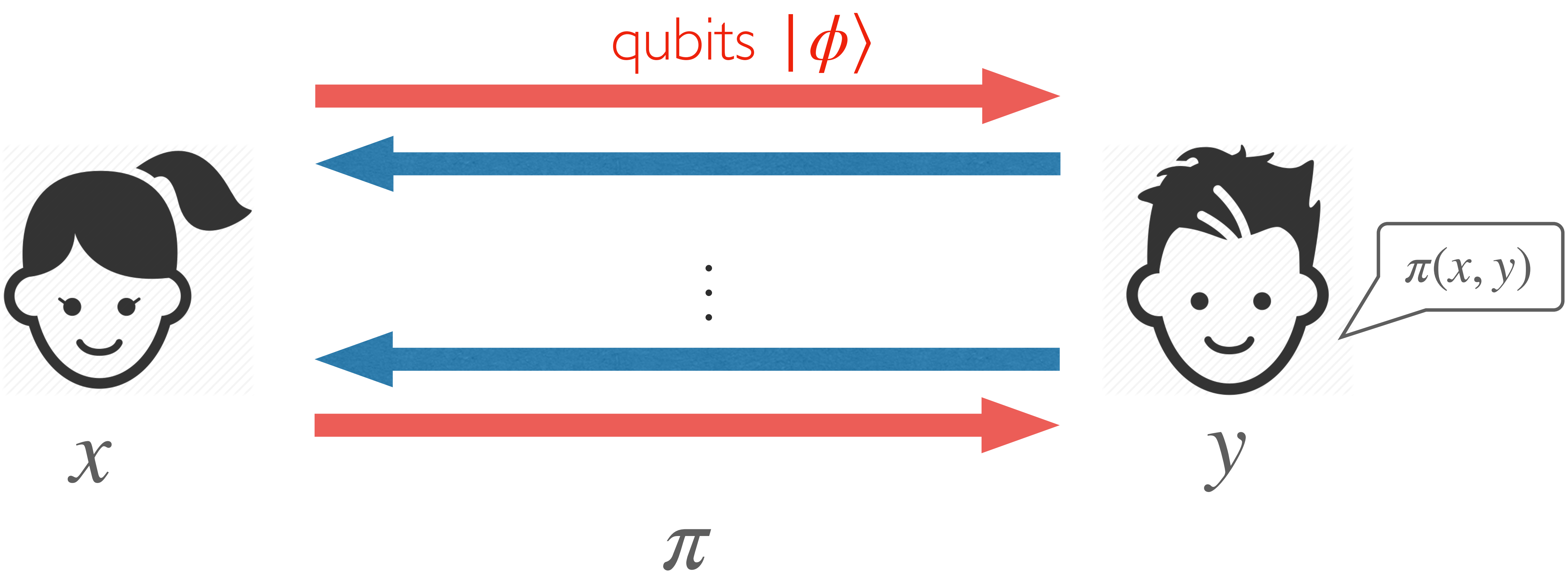
Communication complexity (Quantum)

"Quantum advantage?"

Communication complexity (Quantum)



Communication complexity (Quantum)



Correctness: $\Pr[\pi(x, y) = f(x, y)] \geq \frac{2}{3}, \forall x, y$.

What's the largest separation?

Partial functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1,\text{undef}\}$,

	Classical	Quantum
Buhrman et al. '98	$\mathrm{D}(f) = \Omega(n)$	$O(\log n)$

What's the largest separation?

Partial functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1,\text{undef}\}$,

	Classical	Quantum
Buhrman et al. '98	$\mathrm{D}(f) = \Omega(n)$	$O(\log n)$
Raz '99	$\mathrm{R}(f) = \tilde{\Omega}(n^{1/4})$	$O(\log n)$
Klartag-Regev '10	$\mathrm{R}(f) = \tilde{\Omega}(n^{1/3})$	$O(\log n)$
Aaronson-Ambainis '15	$\mathrm{R}(f) = \tilde{\Omega}(n^{1/2})$	$O(\log n)$
Tal '19	$\mathrm{R}(f) = \Omega(n^{2/3-\epsilon})$	$O(\log n)$

What's the largest separation?

Partial functions $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1,\text{undef}\}$,

	Classical	Quantum
Buhrman et al. '98	$D(f) = \Omega(n)$	$O(\log n)$
Raz '99	$R(f) = \tilde{\Omega}(n^{1/4})$	$O(\log n)$
Klartag-Regev '10	$R(f) = \tilde{\Omega}(n^{1/3})$	$O(\log n)$
Aaronson-Ambainis '15	$R(f) = \tilde{\Omega}(n^{1/2})$	$O(\log n)$
Tal '19	$R(f) = \Omega(n^{2/3-\epsilon})$	$O(\log n)$
SSW., '20	$R(f) = \Omega(n^{1-\epsilon})$	$O(\log n)$

What's the largest separation?

Partial functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1,\text{undef}\}$,

	Classical	Quantum
Buhrman et al. '98	$\mathrm{D}(f) = \Omega(n)$	$O(\log n)$
Raz '99	$\mathrm{R}(f) = \tilde{\Omega}(n^{1/4})$	$O(\log n)$
Klartag-Regev '10	$\mathrm{R}(f) = \tilde{\Omega}(n^{1/3})$	$O(\log n)$
Aaronson-Ambainis '15	$\mathrm{R}(f) = \tilde{\Omega}(n^{1/2})$	$O(\log n)$
Tal '19	$\mathrm{R}(f) = \Omega(n^{2/3-\epsilon})$	$O(\log n)$
SSW., '20	$\mathrm{R}(f) = \Omega(n^{1-\epsilon})$	$O(\log n)$

near-optimal

What's the largest separation?

Total functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,

	Classical vs. Quantum
Buhrman et al., '98, Razborov, '02	$R(f) \geq \Omega(Q(f)^2)$
Aaronson et al., '15	$R(f) \geq \tilde{\Omega}(Q(f)^{5/2})$
Tal, '19	$R(f) \geq \Omega(Q(f)^{8/3-o(1)})$
SSW., '20	$R(f) \geq \Omega(Q(f)^{3-o(1)})$

What's the largest separation?

Total functions $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,

	Classical vs. Quantum
Buhrman et al., '98, Razborov, '02	$R(f) \geq \Omega(Q(f)^2)$
Aaronson et al., '15	$R(f) \geq \tilde{\Omega}(Q(f)^{5/2})$
Tal, '19	$R(f) \geq \Omega(Q(f)^{8/3-o(1)})$
SSW., '20	$R(f) \geq \Omega(Q(f)^{3-o(1)})$

Lifting

In short,

f, hard for query model

$\big\downarrow$ lift

[Raz-McKenzie., '99]

[Goos et al., '15]

[Chattopattyay et al., '19]

F, hard for communication model

Query complexity

a huge unstructured database

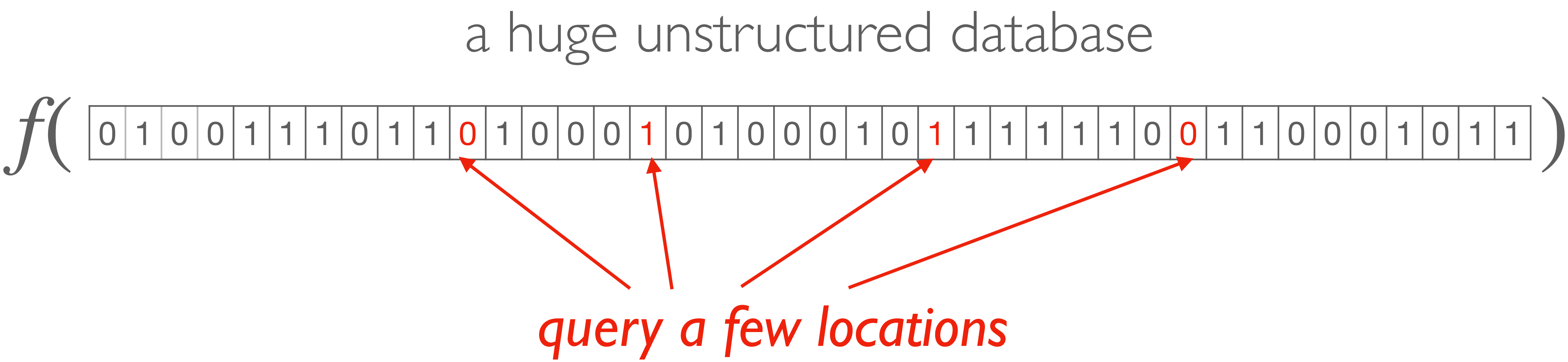
0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	1	1	1	1	1	0	0	1	1	0	0	0	1	0	1	1

Query complexity

a huge unstructured database

$$f\left(\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}\hline 0&1&0&0&1&1&1&0&1&1&0&1&0&0&0&1&0&1&0&0&0&1&0&1&1&1&1&1&1&0&0&1&1&0&0&0&1&0&1&1\\\hline\end{array}\right)$$

Query complexity



Query complexity

a huge unstructured database

$f($ 0 1 0 0 1 1 1 0 1 1 0 1 0 0 0 1 0 1 0 0 0 1 0 1 1 1 1 1 1 0 0 1 1 0 0 0 1 0 1 1 $)$

query a few locations

query complexity = min queries

Quantum query complexity

State any unit vector in a fixed Euclidean space

Query $$|\phi\rangle = \sum_{i,w} a_{i,w} |i\rangle |w\rangle$$

Quantum query complexity

State any unit vector in a fixed Euclidean space

Query $$|\phi\rangle = \sum_{i,w} a_{i,w} |i\rangle |w\rangle$$

query
index

Quantum query complexity

State any unit vector in a fixed Euclidean space

workspace

Query $$|\phi\rangle = \sum_{i,w} a_{i,w} |i\rangle |w\rangle$$

query
index

Quantum query complexity

State any unit vector in a fixed Euclidean space

Query

workspace

$$|\phi\rangle = \sum_{i,w} a_{i,w} |i\rangle |w\rangle$$

query index

$$\downarrow$$

$$|\phi'\rangle = \sum_{i,w} a_{i,w} (-1)^{x_i} |i\rangle |w\rangle$$

Quantum query complexity

State any unit vector in a fixed Euclidean space

workspace

Query $$|\phi\rangle = \sum_{i,w} a_{i,w} |i\rangle |w\rangle$$

query index

$$\downarrow$$

$$|\phi'\rangle = \sum_{i,w} a_{i,w} (-1)^{x_i} |i\rangle |w\rangle$$

can access all x_i in a single query!

Quantum speedups

Query model captures nearly all quantum breakthroughs:

Deutsch-Jozsa's algorithm

Bernstein-Vazirani's algorithm

Simon's algorithm

Shor's factoring algorithm

Grover's search

……

Largest possible separation?

Partial functions

	Randomized	Quantum
Simon '97	$\Omega(\sqrt{n})$	$O(\log n)$
Aaronson-Ambainis '15	$\tilde{\Omega}(\sqrt{n})$	1
AA '15, BGGS '21	$O_k(n^{1-\frac{1}{k}})$	$k/2$
Tal '19	$\tilde{\Omega}(n^{\frac{2k-2}{3k-1}})$	$k/2$
Our result	$\tilde{\Omega}(n^{1-\frac{1}{k}})$	$k/2$

Largest possible separation?

Partial functions

	Randomized	Quantum
Simon '97	$\Omega(\sqrt{n})$	$O(\log n)$
Aaronson-Ambainis '15	$\tilde{\Omega}(\sqrt{n})$	1
AA '15, BGGS '21	$O_k(n^{1-\frac{1}{k}})$	$k/2$
Tal '19	$\tilde{\Omega}(n^{\frac{2k-2}{3k-1}})$	$k/2$
Our result	$\tilde{\Omega}(n^{1-\frac{1}{k}})$	$k/2$

Optimal

Largest possible separation?

Total functions

	Randomized vs. Quantum
Grover '69, BBBV '97	$R(f) = \Omega(Q(f)^2)$
Beals et al. '01	$R(f) = O(Q(f)^6)$
Aaronson et al. '16	$R(f) \geq \tilde{\Omega}(Q(f)^{2.5})$
Tal '19	$R(f) \geq Q(f)^{\frac{8}{3}-o(1)}$
Aaronson et al. '20	$R(f) = O(Q(f)^4)$
Our result	$R(f) \geq Q(f)^{3-o(1)}$

Largest possible separation?

Total functions

	Randomized vs. Quantum
Grover '69, BBBV '97	$R(f) = \Omega(Q(f)^2)$
Beals et al. '01	$R(f) = O(Q(f)^6)$
Aaronson et al. '16	$R(f) \geq \tilde{\Omega}(Q(f)^{2.5})$
Tal '19	$R(f) \geq Q(f)^{\frac{8}{3}-o(1)}$
Aaronson et al. '20	$R(f) = O(Q(f)^4)$
Our result	$R(f) \geq Q(f)^{3-o(1)}$

Largest possible separation?

Total functions

	Randomized vs. Quantum
Grover '69, BBBV '97	$R(f) = \Omega(Q(f)^2)$
Beals et al. '01	$R(f) = O(Q(f)^6)$
Aaronson et al. '16	$R(f) \geq \tilde{\Omega}(Q(f)^{2.5})$
Tal '19	$R(f) \geq Q(f)^{\frac{8}{3}-o(1)}$
Aaronson et al. '20	$R(f) = O(Q(f)^4)$
Our result	$R(f) \geq Q(f)^{3-o(1)}$

Fourier weight of decision trees

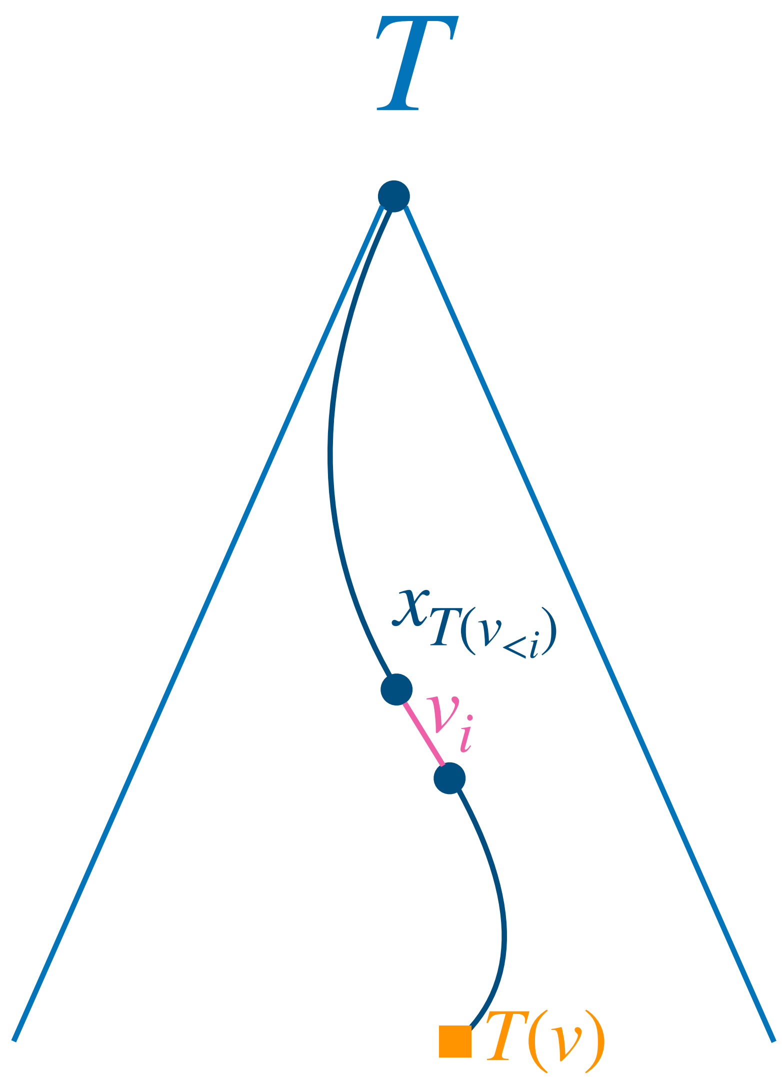
Theorem. (Sherstov-Storochenko-W.)

For any decision tree $T : \{-1,1\}^n \to \{0,1\}$ of depth d,

$$\sum_{\substack{S \subseteq \{1,2,\ldots,n\}: \\ |S| = \ell}} |\hat{T}(S)| \leq c^{\ell} \sqrt{\binom{d}{\ell}(1+\log n)^{\ell-1}}\,.$$

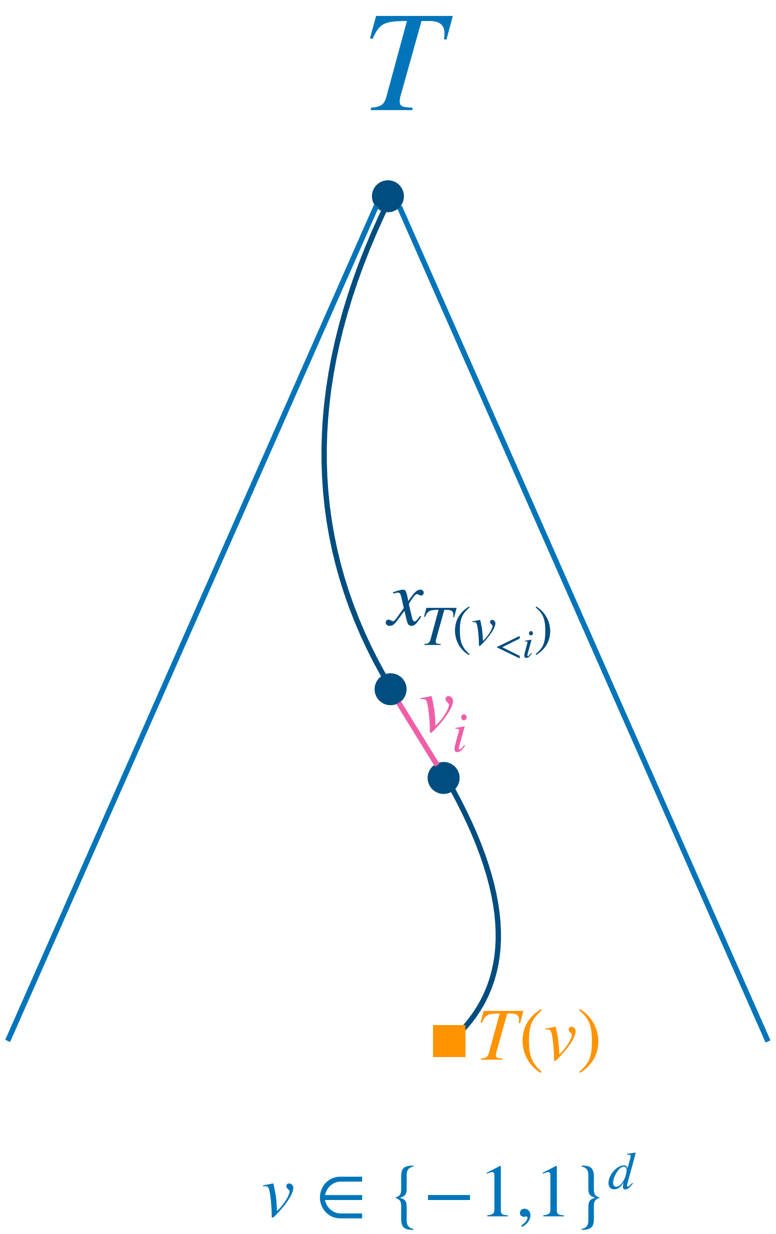
Our approach

Our approach



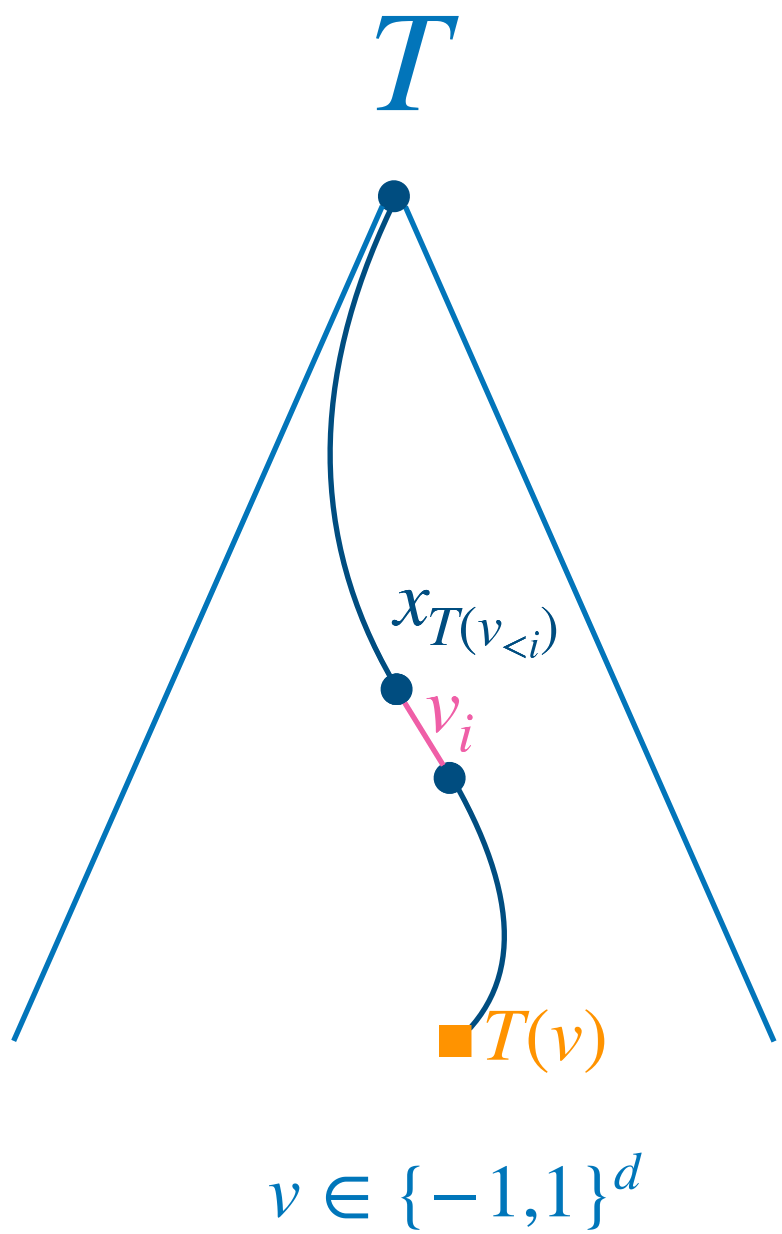
$v \in \{-1,1\}^d$

Our approach



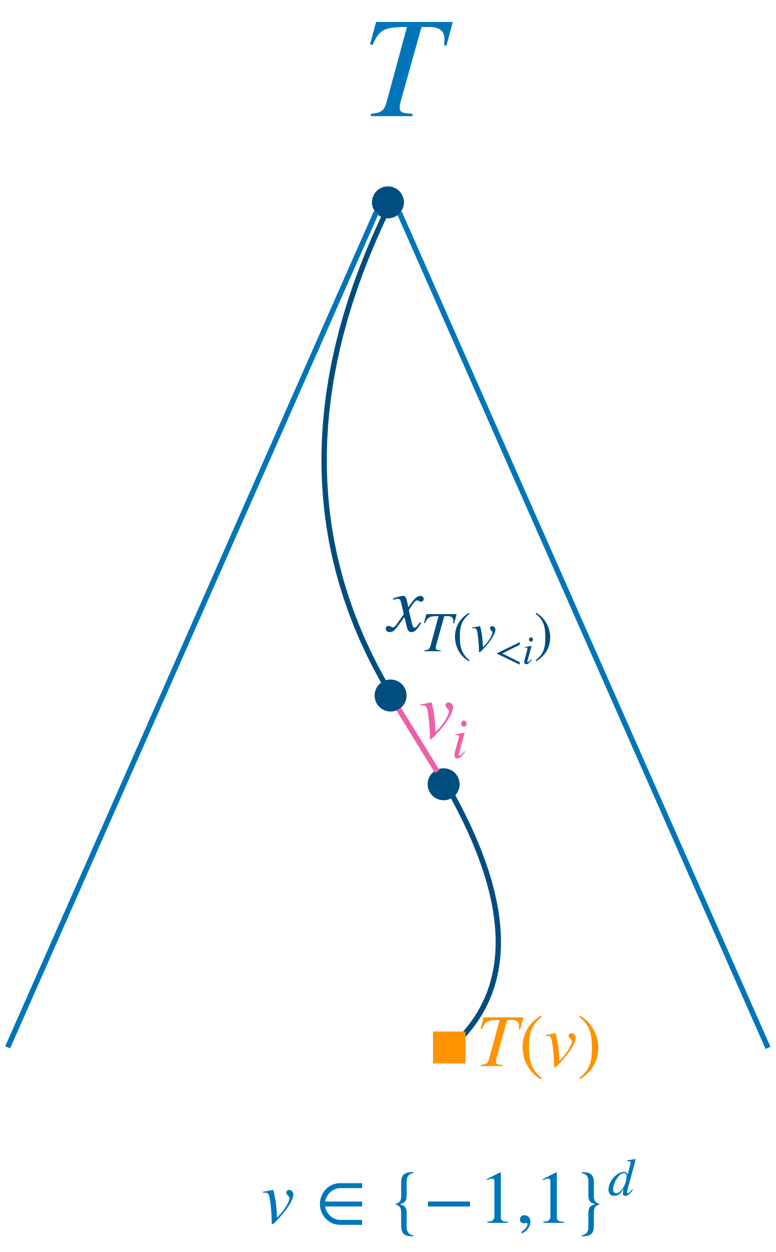
$$T(v)\prod_{i=1}^{d}\frac{1+v_i x_{T(v_{<i})}}{2}$$

Our approach



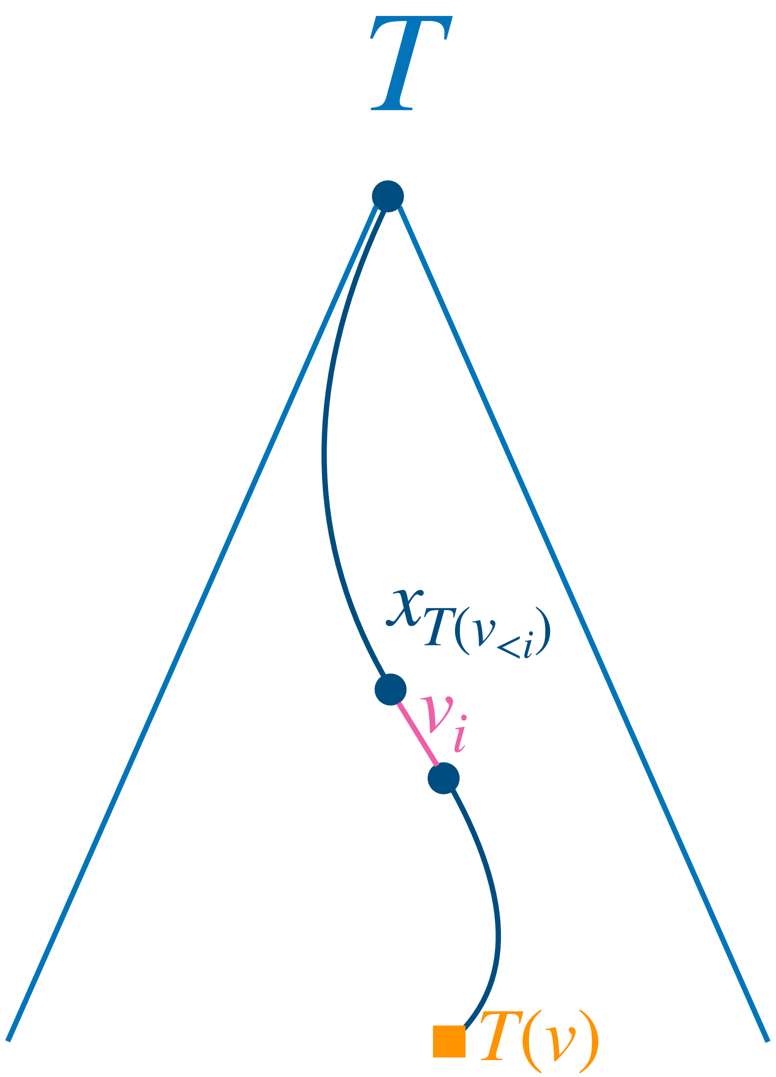
$$T = \sum_{v \in \{-1,1\}^d} T(v) \prod_{i=1}^{d} \frac{1 + v_i x_{T(v_{<i})}}{2}$$

Our approach



$$T = \sum_{v \in \{-1,1\}^d} T(v) \prod_{i=1}^{d} \frac{1 + v_i x_{T(v_{<i})}}{2}$$
$$= \sum_{v \in \{-1,1\}^d} T(v) 2^{-d} \sum_{S \subseteq \{1,\ldots,d\}} \prod_{i \in S} v_i x_{T(v_{<i})}$$

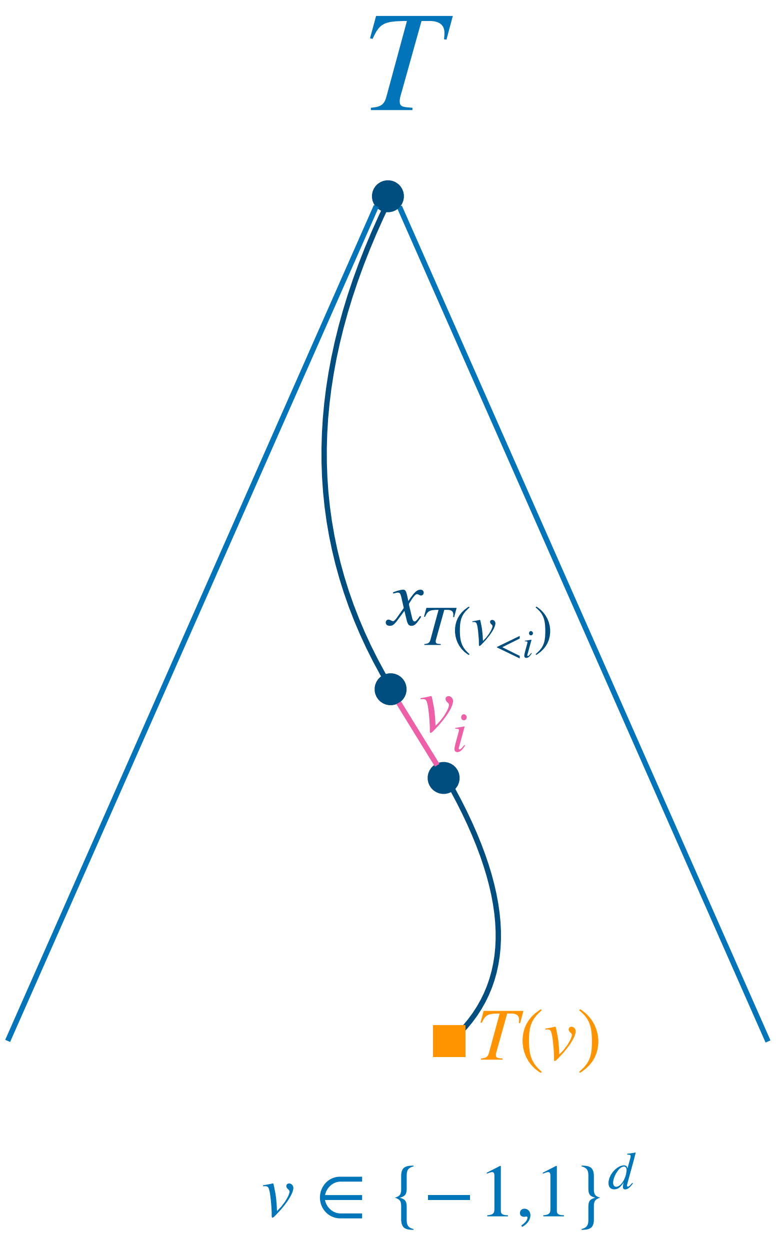
Our approach



$v \in \{-1,1\}^d$

$$
\begin{aligned}
T &= \sum_{v\in\{-1,1\}^d} T(v)\prod_{i=1}^{d}\frac{1+v_i x_{T(v_{<i})}}{2} \\
&= \sum_{v\in\{-1,1\}^d} T(v)2^{-d} \sum_{S\subseteq\{1,\ldots,d\}} \prod_{i\in S} v_i x_{T(v_{<i})} \\
&= \sum_{S\subseteq\{1,\ldots,d\}} \sum_{v\in\{-1,1\}^d} T(v)2^{-d}\prod_{i\in S} v_i x_{T(v_{<i})}\,.
\end{aligned}
$$

Our approach



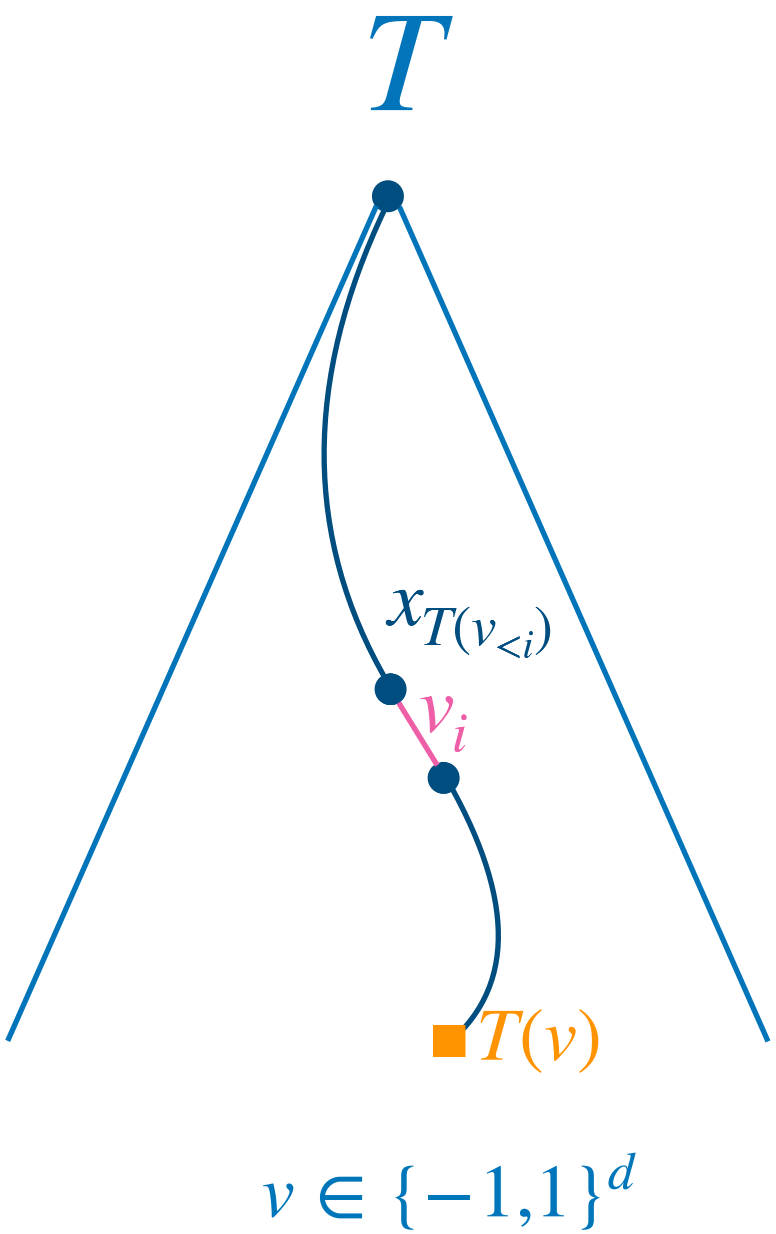
$$T = \sum_{v\in\{-1,1\}^d} T(v)\prod_{i=1}^{d}\frac{1+v_i x_{T(v_{<i})}}{2}$$

$$= \sum_{v\in\{-1,1\}^d} T(v)2^{-d} \sum_{S\subseteq\{1,\ldots,d\}} \prod_{i\in S} v_i x_{T(v_{<i})}$$

$$= \sum_{S\subseteq\{1,\ldots,d\}} \sum_{v\in\{-1,1\}^d} T(v)2^{-d}\prod_{i\in S} v_i x_{T(v_{<i})} \,.$$

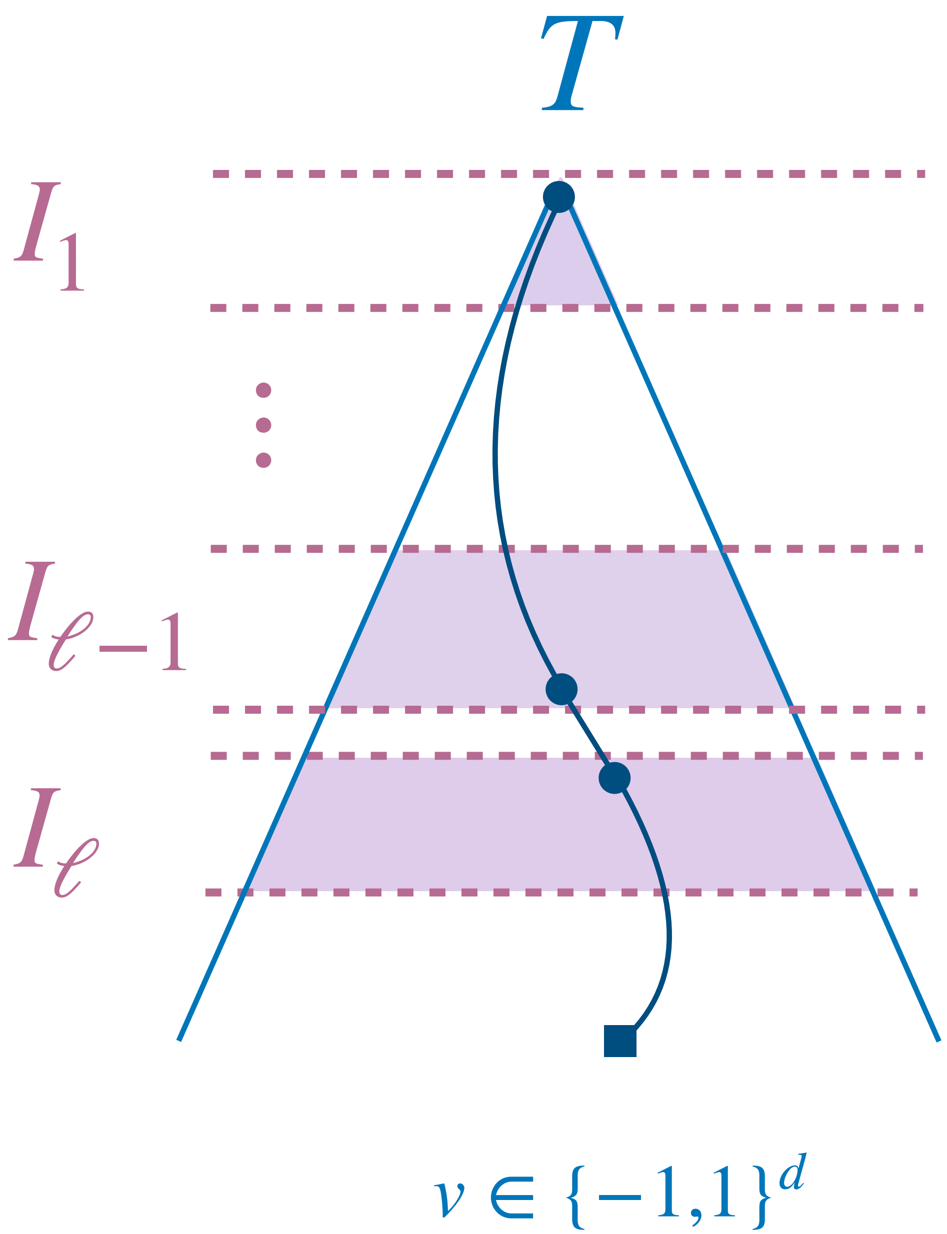
$$L_\ell T = \sum_{S\in\mathscr{P}_{d,\ell}} \sum_{v\in\{-1,1\}^d} T(v)2^{-d}\prod_{i\in S} v_i x_{T(v_{<i})} \,.$$

Our approach



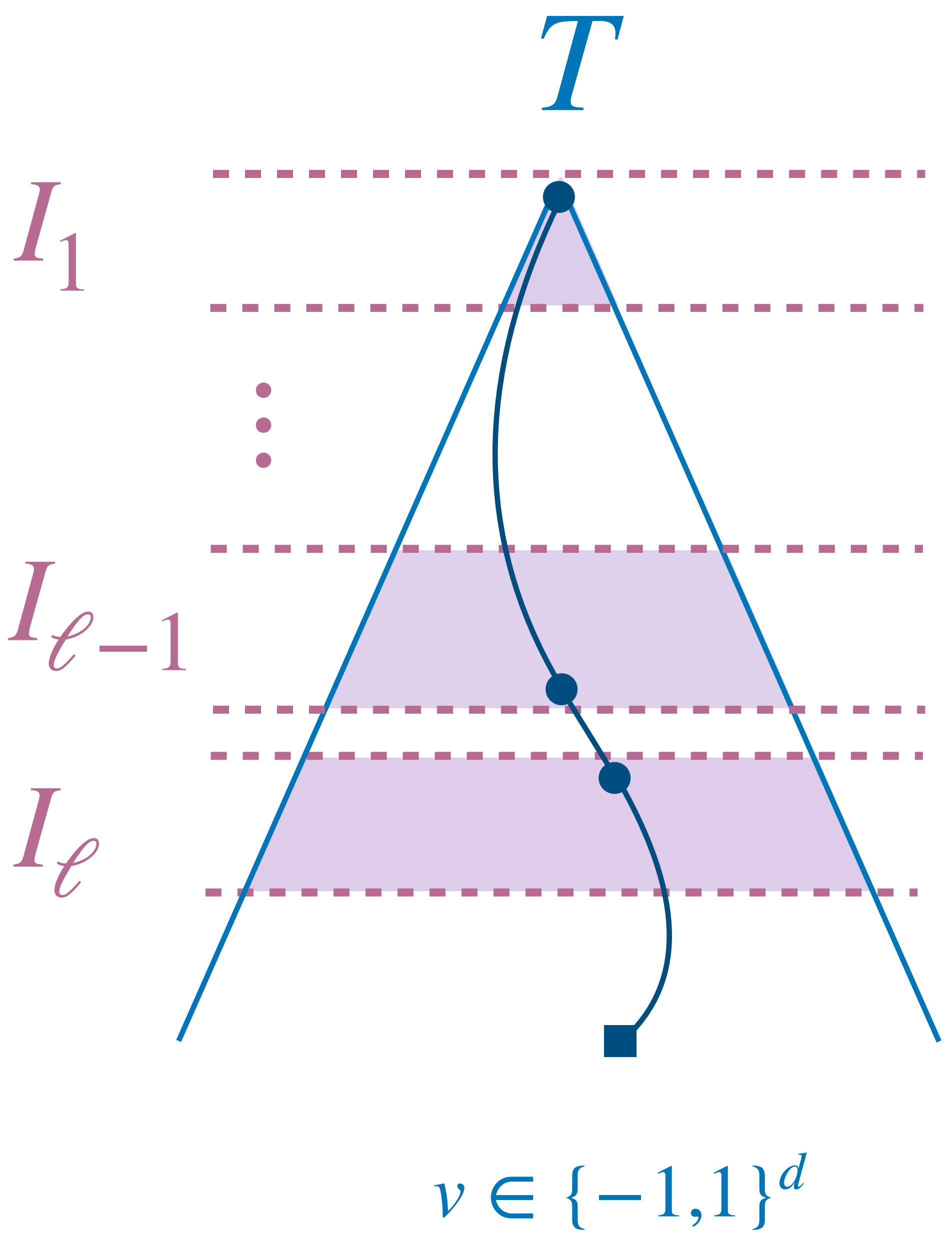
$$L_\ell T = \sum_{S \in \mathscr{P}_{d,\ell}} \sum_{v \in \{-1,1\}^d} T(v) 2^{-d} \prod_{i \in S} v_i x_{T(v_{<i})} .$$

Our approach



$$L_\ell T = \sum_{S \in \mathscr{P}_{d,\ell}} \sum_{v \in \{-1,1\}^d} T(v) 2^{-d} \prod_{i \in S} v_i x_{T(v_{<i})} \,.$$

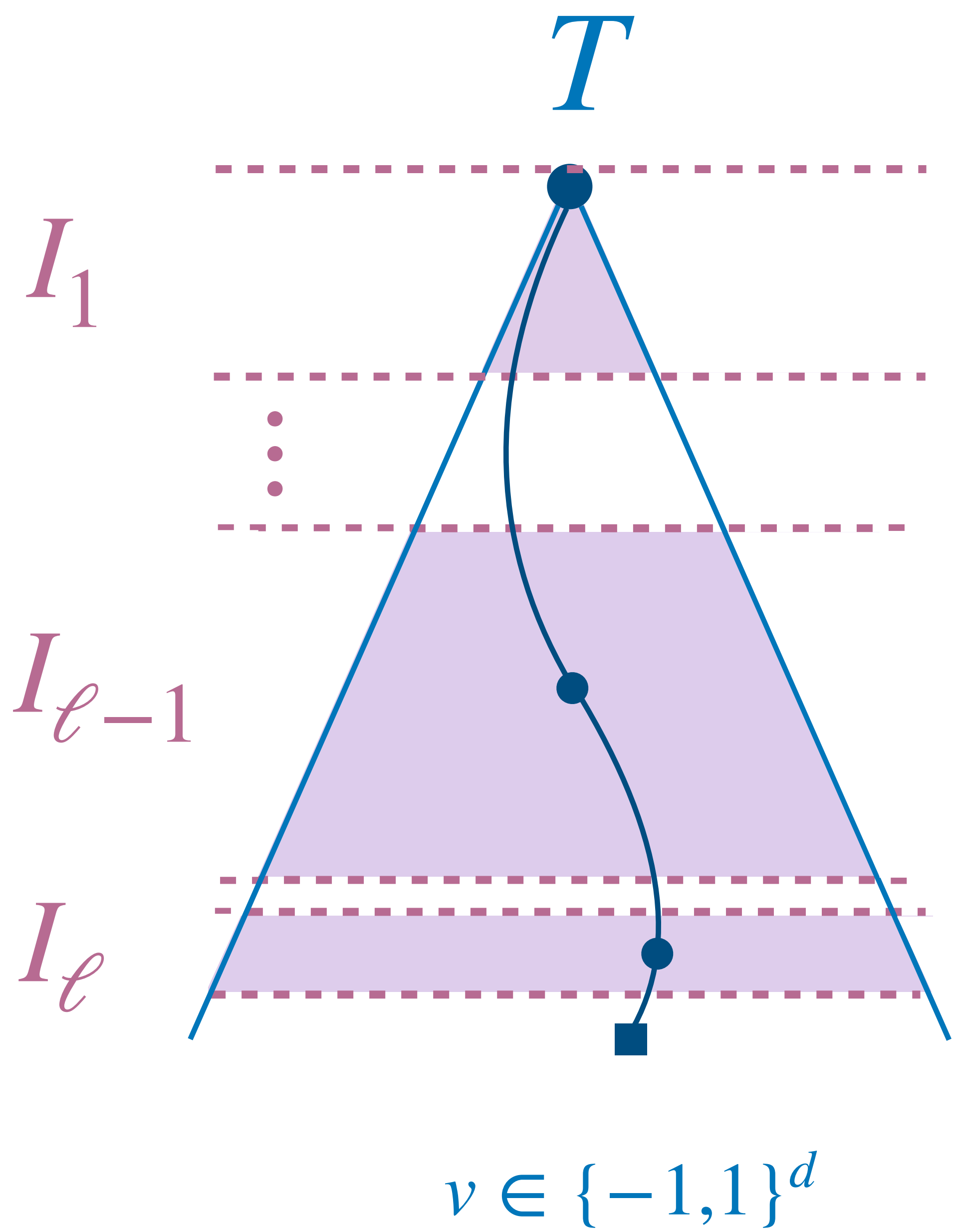
Our approach



$$L_\ell T = \sum_{S \in \mathscr{P}_{d,\ell}} \sum_{v \in \{-1,1\}^d} T(v) 2^{-d} \prod_{i \in S} v_i x_{T(v_{<i})} .$$

$$T|_{I_1 * I_2 * \ldots * I_\ell} = \sum_{\substack{S \subseteq \{1,\ldots,d\}: \\ |S \cap I_i| = 1}} \sum_{v \in \{-1,1\}^d} T(v) 2^{-d} \prod_{i \in S} v_i x_{T(v_{<i})} .$$

Our approach

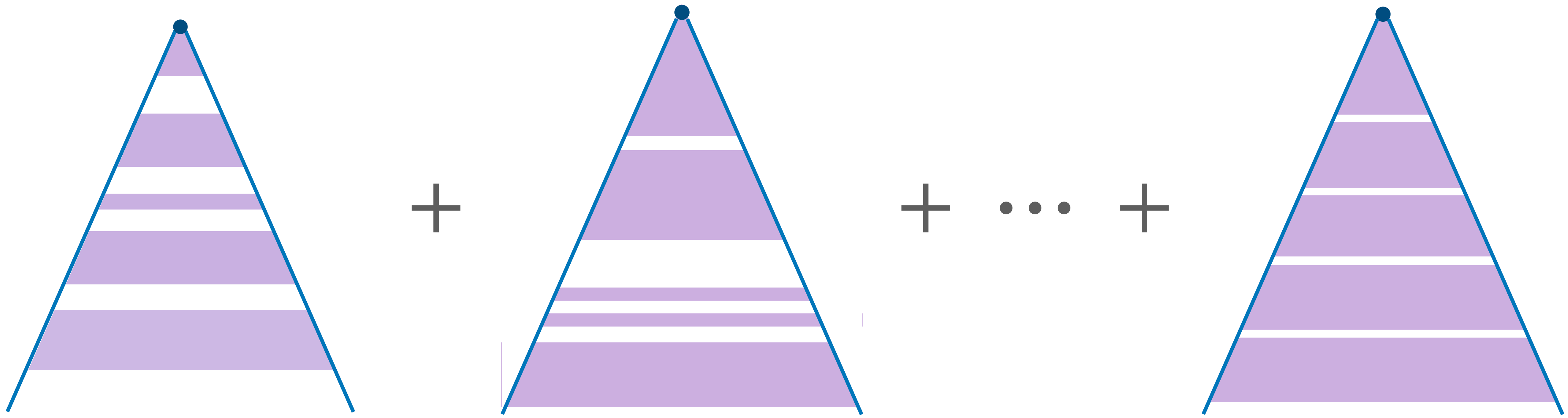


$$L_\ell T = \sum_{S \in \mathscr{P}_{d,\ell}} \sum_{v \in \{-1,1\}^d} T(v) 2^{-d} \prod_{i \in S} v_i x_{T(v_{<i})}.$$

$$T|_{I_1 * I_2 * \ldots * I_\ell} = \sum_{\substack{S \subseteq \{1,\ldots,d\}: \\ |S \cap I_i| = 1}} \sum_{v \in \{-1,1\}^d} T(v) 2^{-d} \prod_{i \in S} v_i x_{T(v_{<i})}.$$

Fourier weight of decision trees

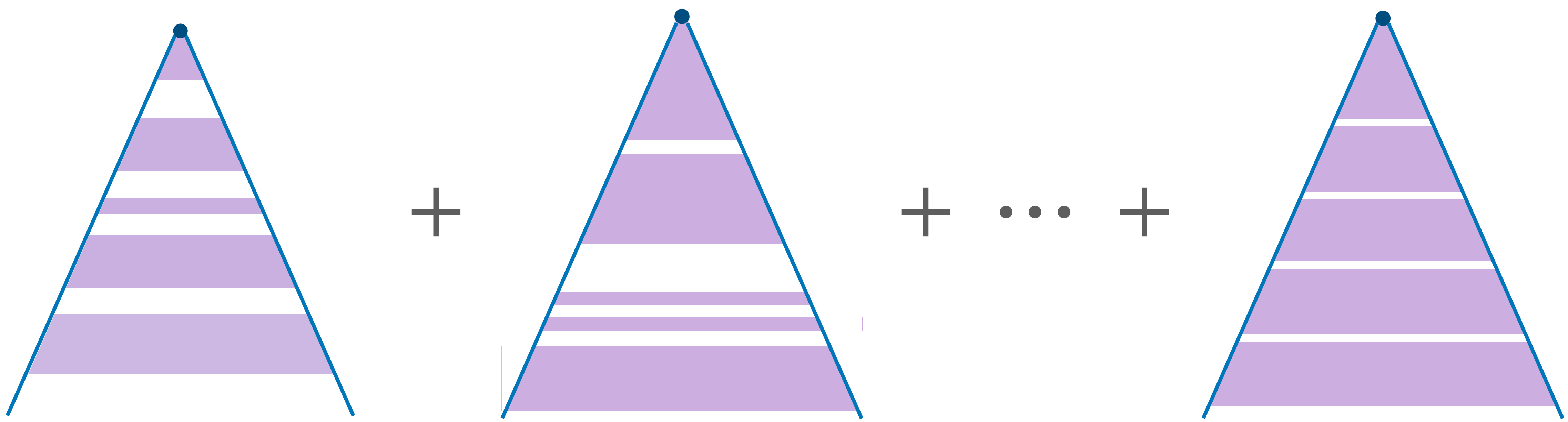
$L_\ell T =$



$$T|_{\mathscr{E}_1} + T|_{\mathscr{E}_2} + \cdots + T|_{\mathscr{E}_m}$$

Fourier weight of decision trees

$L_\ell T =$



$$T|_{\mathscr{E}_1} + T|_{\mathscr{E}_2} + \cdots + T|_{\mathscr{E}_m}$$

$$\| L_\ell T \| \leq \sum \| T|_{\mathscr{E}_i} \| .$$ (Triangle-inequality)

Some more problems

Problem 1. In the query world, for total function, $R(f)$ v.s. $Q(f)$

Problem 2. In the query worlk, for total function, $R(f)$ v.s. <u>exact</u> quantum algorithm (think about Monte Carlo)

Problem 3. <u>Unified</u> theory for partial and total functions.

Grand Challenges

Grand Challenges

1. Quantum v.s. Classical Communication
2. Quantum Proof System

Grand Challenges

1. Quantum v.s. Classical Communication
2. Quantum Proof System

Thank you!