AN OPTIMAL SEPARATION OF RANDOMIZED AND QUANTUM QUERY COMPLEXITY

Alexander Sherstov, Andrey Storozhenko, and Pei Wu

UCLA

STOC 2021

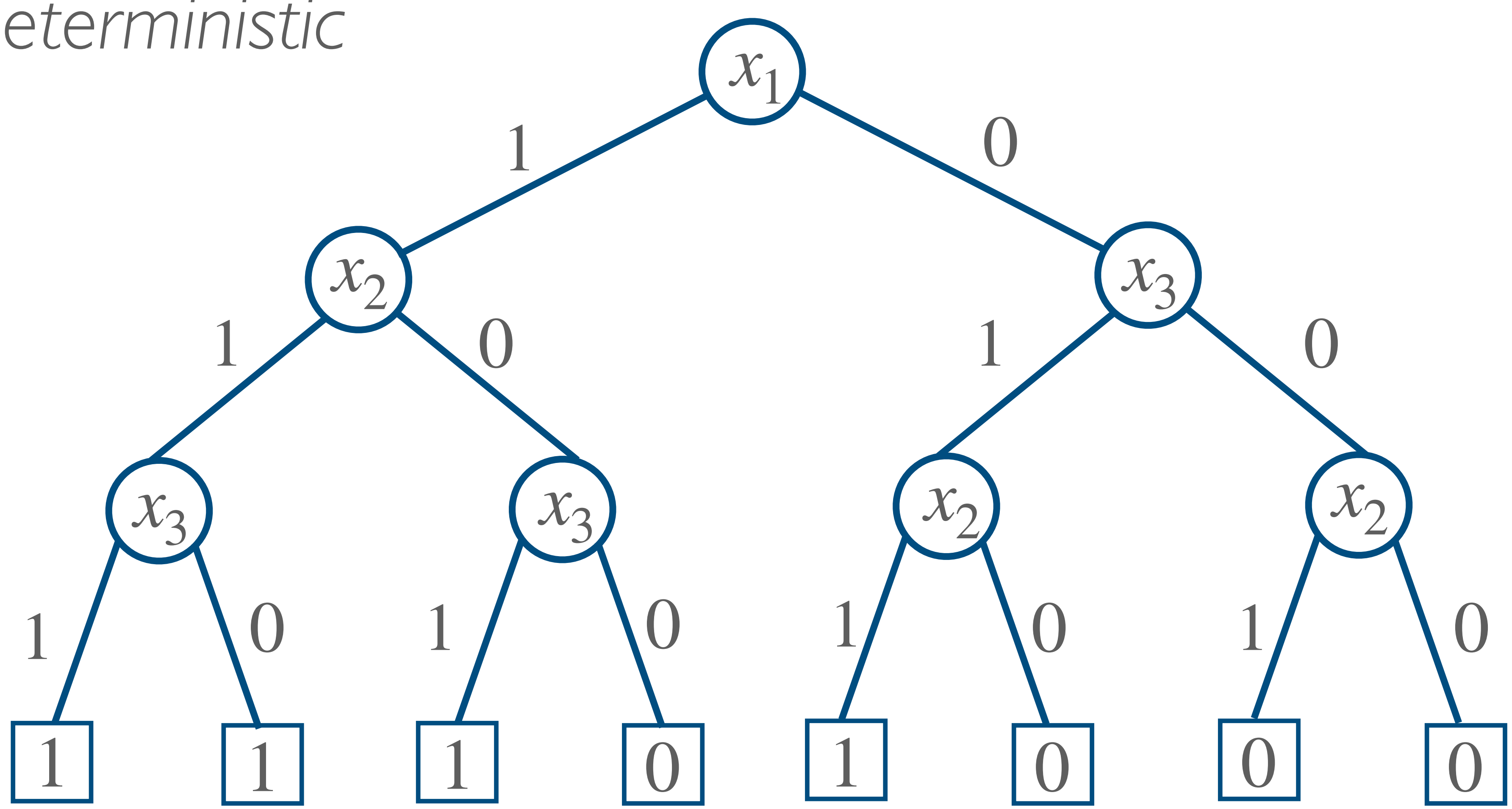
Central open problem

How much faster can quantum computers be than classical?

Most research focuses on the query model.

Query complexity

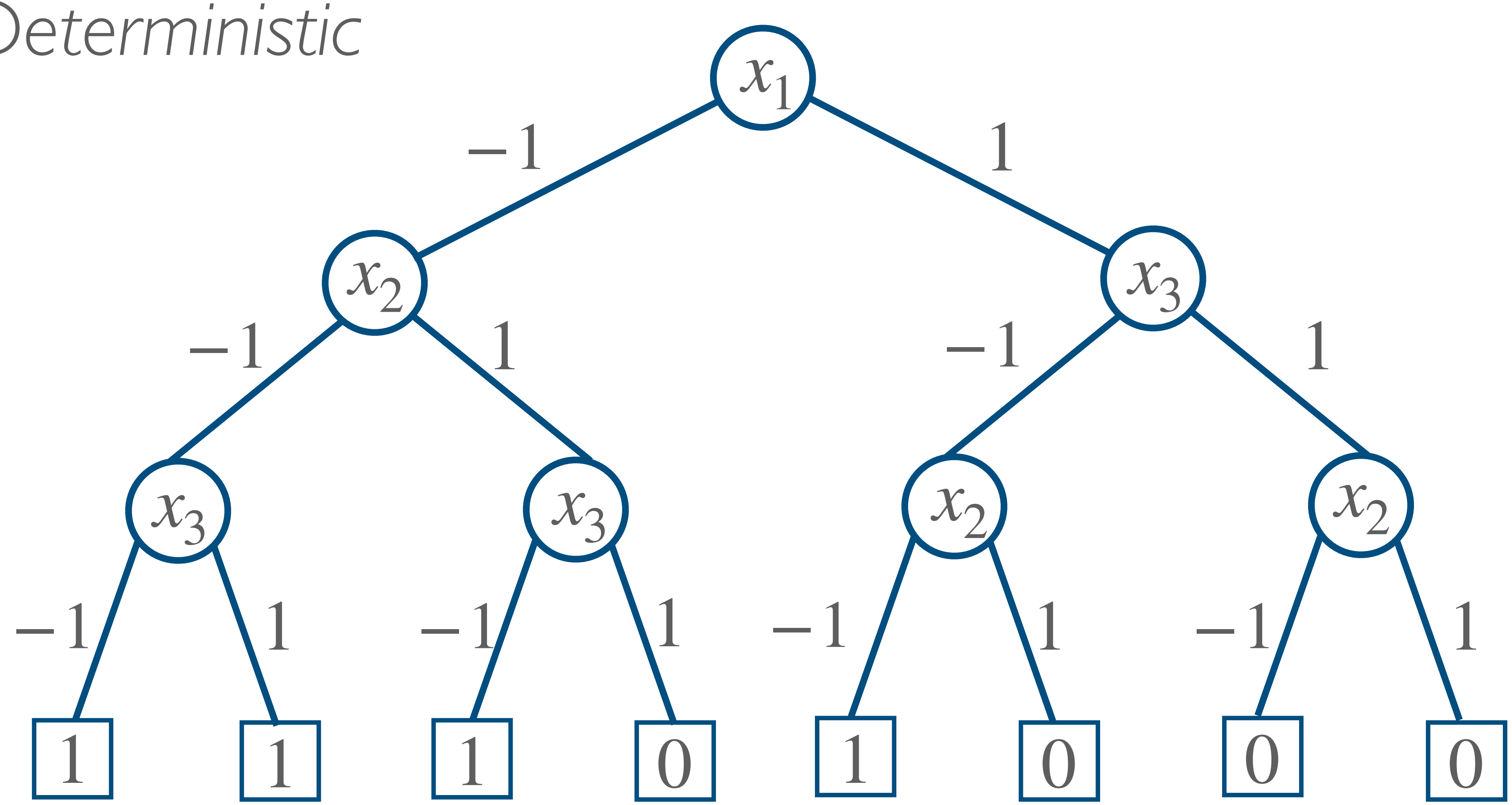
Deterministic



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

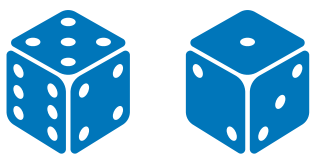
Query complexity

Deterministic

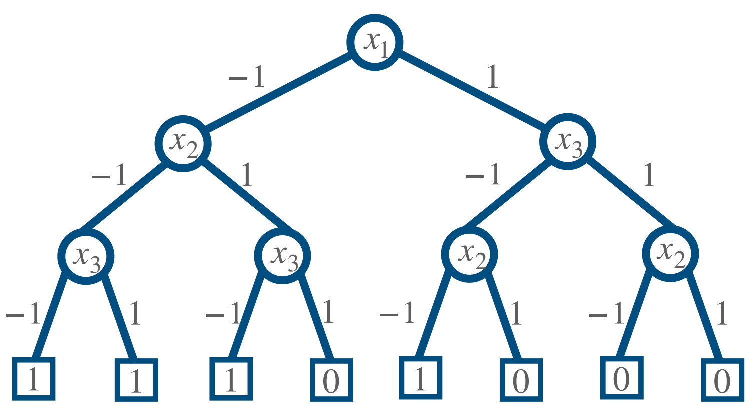


$$T : \{-1,1\}^n \to \{0,1\}$$

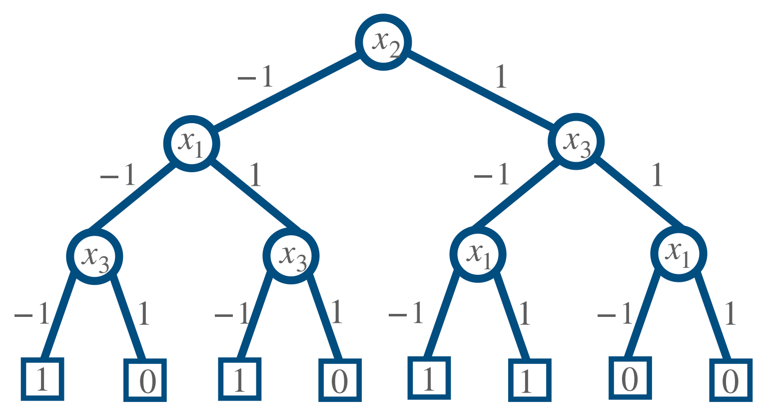
Query complexity



Randomized



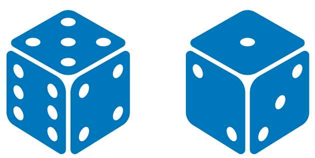
T_1



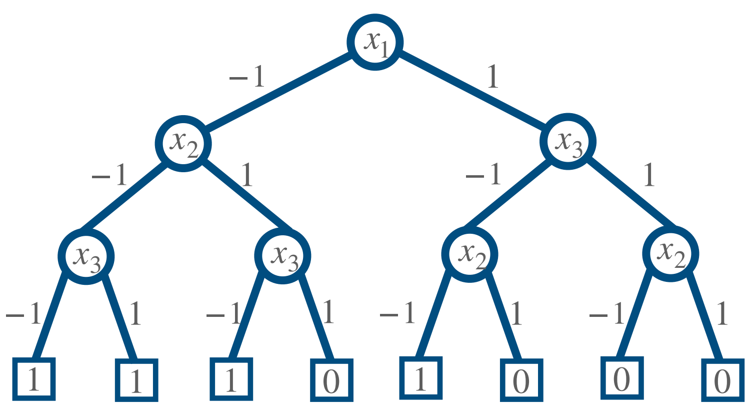
T_2

$\cdots$

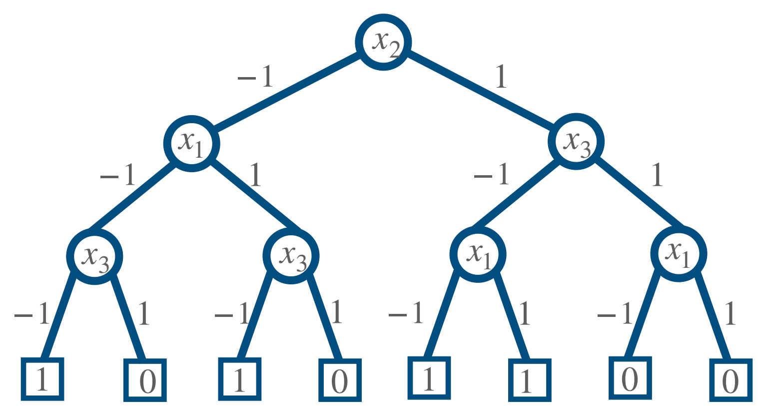
Query complexity



Randomized



T_1



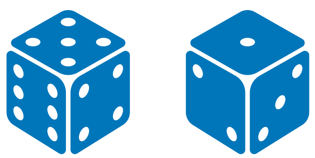
T_2

$\cdots$

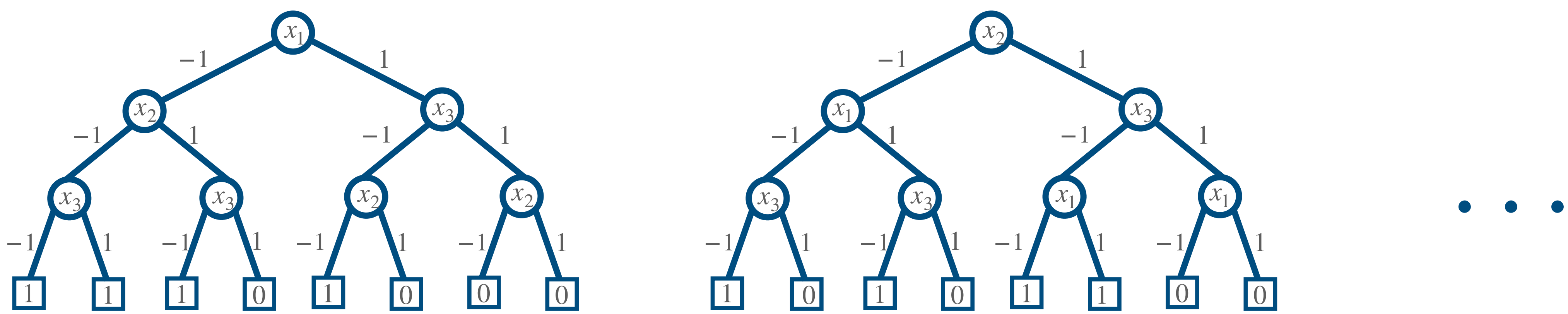
T computes $f : \{-1,1\}^n \to \{0,1\}$ with error ϵ if

$$\mathbf{P}_r[T_r(x) \neq f(x)] \leq \epsilon, \qquad \forall x \in \{-1,1\}^n.$$

Query complexity



Randomized

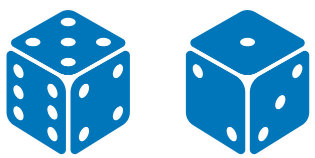


T_1 T_2

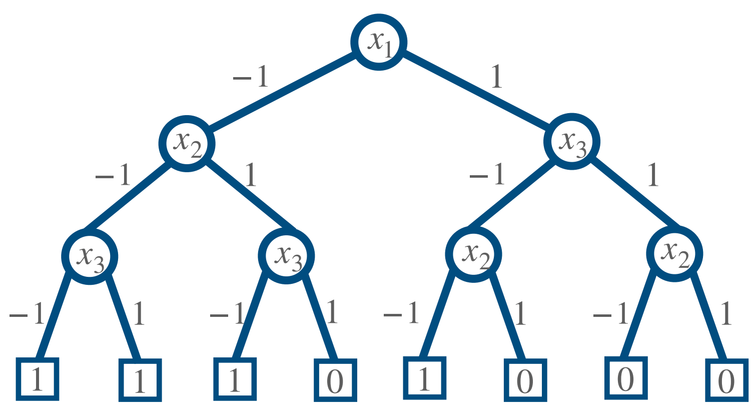
T computes $f : \{-1,1\}^n \to \{0,1,*\}$ with error ϵ if

$$\mathbf{P}_r[T_r(x) \neq f(x)] \leq \epsilon, \qquad \forall x \in f^{-1}(0) \cup f^{-1}(1)\,.$$

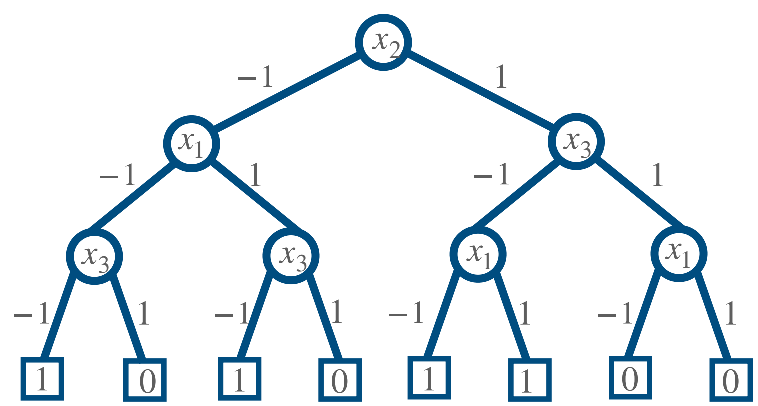
Query complexity



Randomized



T_1



T_2

$\cdots$

$R_\epsilon(f) =$ minimum depth of a randomized decision tree for f with error ϵ.

Quantum query complexity

Quantum query

workspace

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

query
index

$$\downarrow$$

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

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

……

Quantum speedups

Reference	Randomized	Quantum
Simon 97	$\Omega(\sqrt{n})$	$O(\log n)$

Largest possible separation?

[Buhrman et al. 02, Aaronson-Ambainis 15]

Reference	Randomized	Quantum
Simon 97	$\Omega(\sqrt{n})$	$O(\log n)$

~~$R(f) = \Omega(n), Q(f) = O(1)$~~

Impossible!

Largest possible separation?

[Buhrman et al. 02, Aaronson-Ambainis 15]

Reference	Randomized	Quantum	
Simon 97	$\Omega(\sqrt{n})$	$O(\log n)$	
Aaronson-Ambainis 15	$\tilde{\Omega}(\sqrt{n})$	1	"forrelation"
Aaronson-Ambainis 15	$O_k(n^{1-\frac{1}{k}})$	$k/2$	simulation
Tal 19	$\tilde{\Omega}(n^{\frac{2k-2}{3k-1}})$	$k/2$	"rorrelation"

Largest possible separation?

[Buhrman et al. 02, Aaronson-Ambainis 15]

Reference	Randomized	Quantum	
Simon 97	$\Omega(\sqrt{n})$	$O(\log n)$	
Aaronson-Ambainis 15	$\tilde{\Omega}(\sqrt{n})$	1	"forrelation"
Aaronson-Ambainis 15	$O_k(n^{1-\frac{1}{k}})$	$k/2$	simulation
Tal 19	$\tilde{\Omega}(n^{\frac{2k-2}{3k-1}})$	$k/2$	"rorrelation"
Our work	$\tilde{\Omega}(n^{1-\frac{1}{k}})$	$k/2$	"rorrelation"

Optimal

Our results

Theorem.

Let k be any positive integer, $k \leq \dfrac{1}{3} \log n$. Then there is $f_k : \{-1,1\}^n \to \{0,1,*\}$ such that

$$Q_{\frac{1}{2}-\frac{1}{2^{k+4}}}(f_k) \leq \left\lceil \frac{k}{2} \right\rceil,$$

$$R_{\frac{1}{2^{k+1}}}(f_k) \geq \Omega\left(\frac{n^{1-\frac{1}{k}}}{(\log n)^{2-\frac{1}{k}}}\right).$$

$$Q_{1/3}(f_k) = O\left(k4^k\right),$$

$$R_{1/3}(f_k) = \Omega\left(\frac{n^{1-\frac{1}{k}}}{k(\log n)^{2-\frac{1}{k}}}\right).$$

Our results

Corollary 1.

For any $\epsilon > 0$, there is $f: \{-1,1\}^n \to \{0,1,*\}$ with

$$Q_{1/3}(f) = O(1),$$
$$R_{1/3}(f) = \Omega(n^{1-\epsilon}).$$

Take $k = 1 + \lceil 1/\epsilon \rceil$

Corollary 2.

For any monotone $\alpha: \mathbb{N} \to \mathbb{N}$, there is $f: \{-1,1\}^n \to \{0,1,*\}$ with

$$Q_{1/3}(f) \leq \alpha(n),$$
$$R_{1/3}(f) = n^{1-o(1)}.$$

Take $k = k(n)$ an arbitrarily slow-growing function, e.g. $k = \log\log\log n$.

Our results: total functions

Reference	Randomized vs. Quantum
Grover 69, BBBV 97	$R(f) = \Omega(Q(f)^2)$
Beals et al. 01	$R(f) = O(Q(f)^6)$

“cheatsheet”

“cheatsheet”

“cheatsheet”

Our results: communication

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

Reference	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	$R(f) = \Omega(n^{2/3-\epsilon})$	$O(\log n)$
Our work	$R(f) = \Omega(n^{1-\epsilon})$	$O(\log n)$

near-optimal

lifting from query model

Our results: communication

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

Reference	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	$R(f) \geq \Omega(Q(f)^{8/3-o(1)})$
Our work	$R(f) \geq \Omega(Q(f)^{3-o(1)})$

Our results: Fourier weight

Theorem

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

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

- Essentially optimal
- Settles conjecture by Tal (2019)
- Previous bounds trivial already at $\ell \ge \sqrt{d}$

Independent work by Bansal & Sinha

Bansal–Sinha	**Our work**
stochastic calculus	Fourier analysis
• advanced machinery	• elementary
• no Fourier weight bound	• optimal Fourier weight of decision trees
explicit	existential

The problem: rorrelation

Rorrelation

Parameters:

$U \in \mathbb{R}^{n \times n}$, orthogonal matrix

Rorrelation of k vectors:

$$x_1, x_2, \ldots, x_k \in \{-1,1\}^n$$

$$\phi_{n,k,U}(x_1, x_2, \ldots, x_k) = \frac{1}{n}\mathbf{1}^T D_{x_1} U D_{x_2} U \cdots U D_{x_k} \mathbf{1}$$

The correlation problem:

$$f_{n,k,U}(x_1, x_2, \ldots, x_k) = \begin{cases} 1 & \phi_{n,k,U} > 2^{-k}, \\ 0 & |\phi_{n,k,U}| \le 2^{-k-1}, \\ * & \text{otherwise}. \end{cases}$$

Rorrelation: quantum algorithms

$$\phi_{n,k,U}(x_1, x_2, \ldots, x_k) = \frac{1}{n}\mathbf{1}^T D_{x_1} U D_{x_2} U \cdots U D_{x_k} \mathbf{1}$$

$$f_{n,k,U}(x_1, x_2, \ldots, x_k) = \begin{cases} 1 & \phi_{n,k,U} > 2^{-k}, \\ 0 & |\phi_{n,k,U}| \leq 2^{-k-1}, \\ * & \text{otherwise}. \end{cases}$$

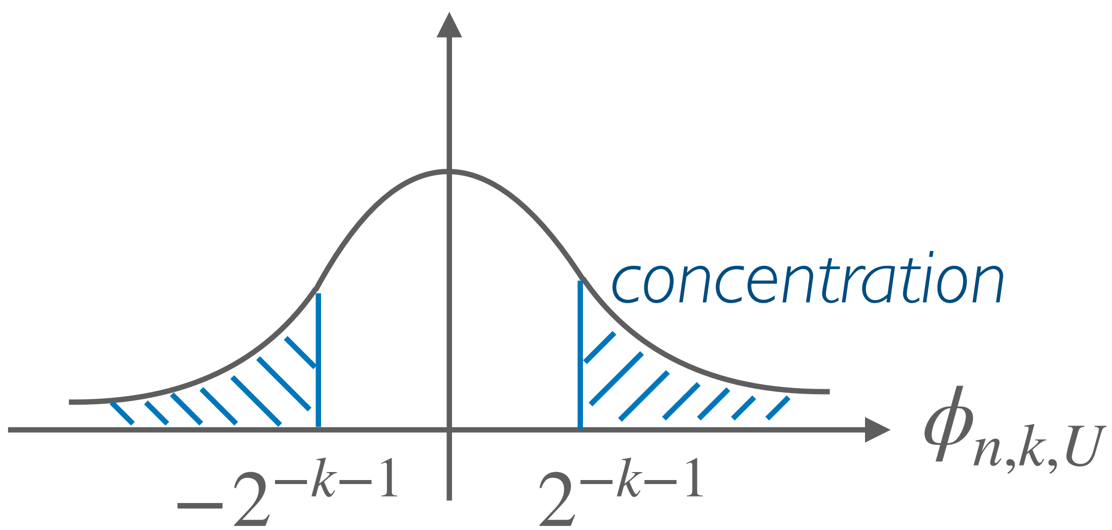
Theorem (Aaronson-Ambainis, Tal).
There is a quantum algorithm using $\lceil k/2 \rceil$ queries that accepts x with probability

$$\frac{\phi_{n,k,U}(x) + 1}{2}.$$

Rorrelation: classical lower bound

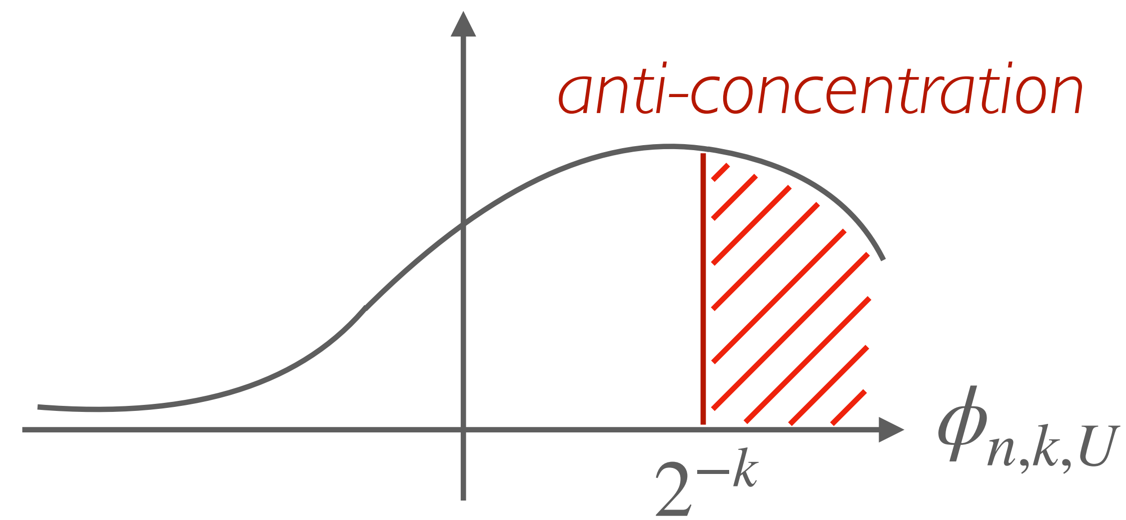
—the "indistinguishability" argument

$\mathscr{U}_{n,k}$ = uniform distribution



$\mathbf{P}_{\mathscr{U}_{n,k}}[\phi > 2^{-k-1}] < 2^{-k-1}$

$\mathscr{D}_{n,k,U}$ = correlated distribution

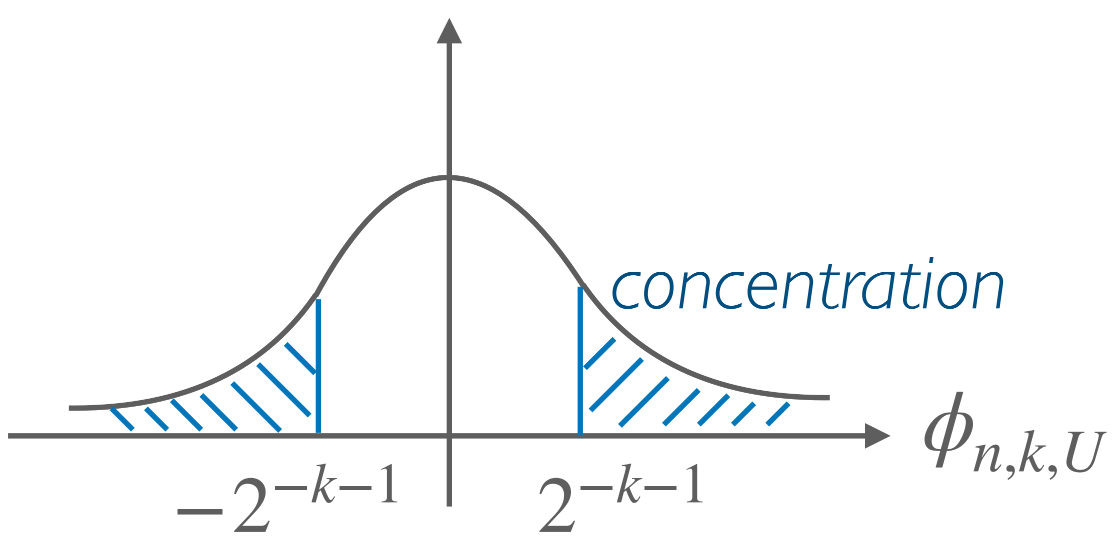


$\mathbf{P}_{\mathscr{D}_{n,k,U}}[\phi \geq 2^{-k}] \geq 2^{-k}$

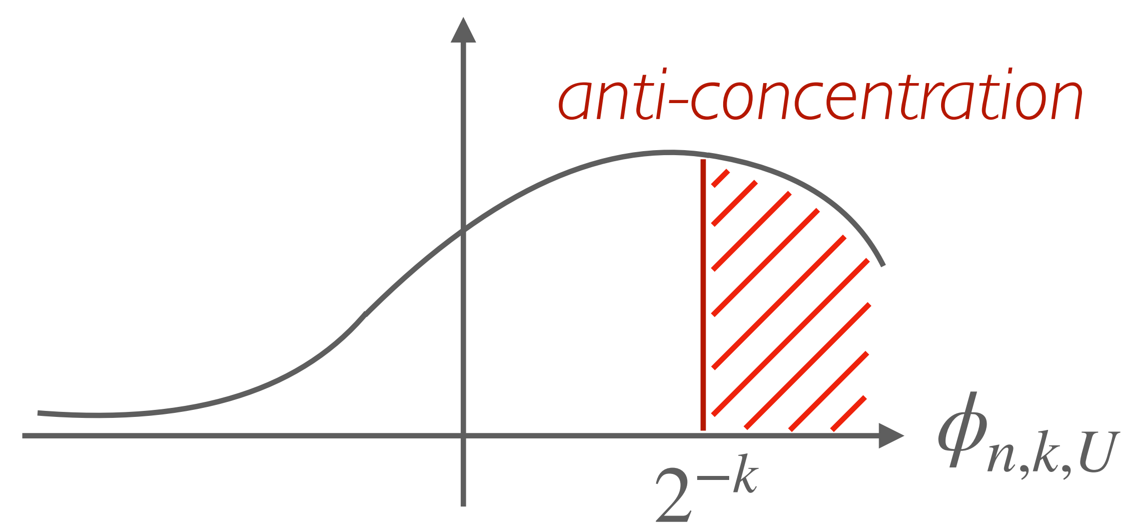
Rorrelation: classical lower bound

—the "indistinguishability" argument

$\mathscr{U}_{n,k}$ = uniform distribution



$\mathscr{D}_{n,k,U}$ = correlated distribution



Thus, for any randomized query algorithm g of error ϵ,

$$\mathbf{E}_{\mathscr{D}_{n,k,U}} g(x) \; - \; \mathbf{E}_{\mathscr{U}_{n,k}} g(x) \; \geq 2^{-k-1} - 2\epsilon \, .$$

Rorrelation: classical lower bound

—the "indistinguishability" argument

$$\mathbf{E}_{\mathscr{D}_{n,k,U}} g(x) - \mathbf{E}_{\mathscr{U}_{n,k}} g(x)$$

[al]

$$\leq O\left(\frac{\ell \log n}{n}\right)^{\frac{\ell}{2}\frac{k-1}{k}}$$

We prove: $\leq c^{\ell}\sqrt{\binom{d}{\ell}(\ln en)^{\ell-1}}$

Therefore,

$R_{2^{-O(k)}}(f_k) = \tilde{\Omega}(n^{1-\frac{1}{k}})$. ∎

Fourier weight of decision trees

Fourier weight of decision trees

Main Theorem.

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

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

Fourier weight of decision trees

Main Theorem.

Fix any decision tree $T : \{-1,1\}^n \to \{-1,0,1\}$ of depth d, and $\mathbf{P}[T(x) \neq 0] = p$. Then

$$|||\, L_\ell T \,||| \leq c^\ell \sqrt{\binom{d}{\ell}} \Lambda_{n^2,\ell}(p),$$

Fourier weight of decision trees

Main Theorem.

Fix any decision tree $T : \{-1,1\}^n \to \{-1,0,1\}$ of depth d, and $\mathrm{dns}(T) = p$. Then

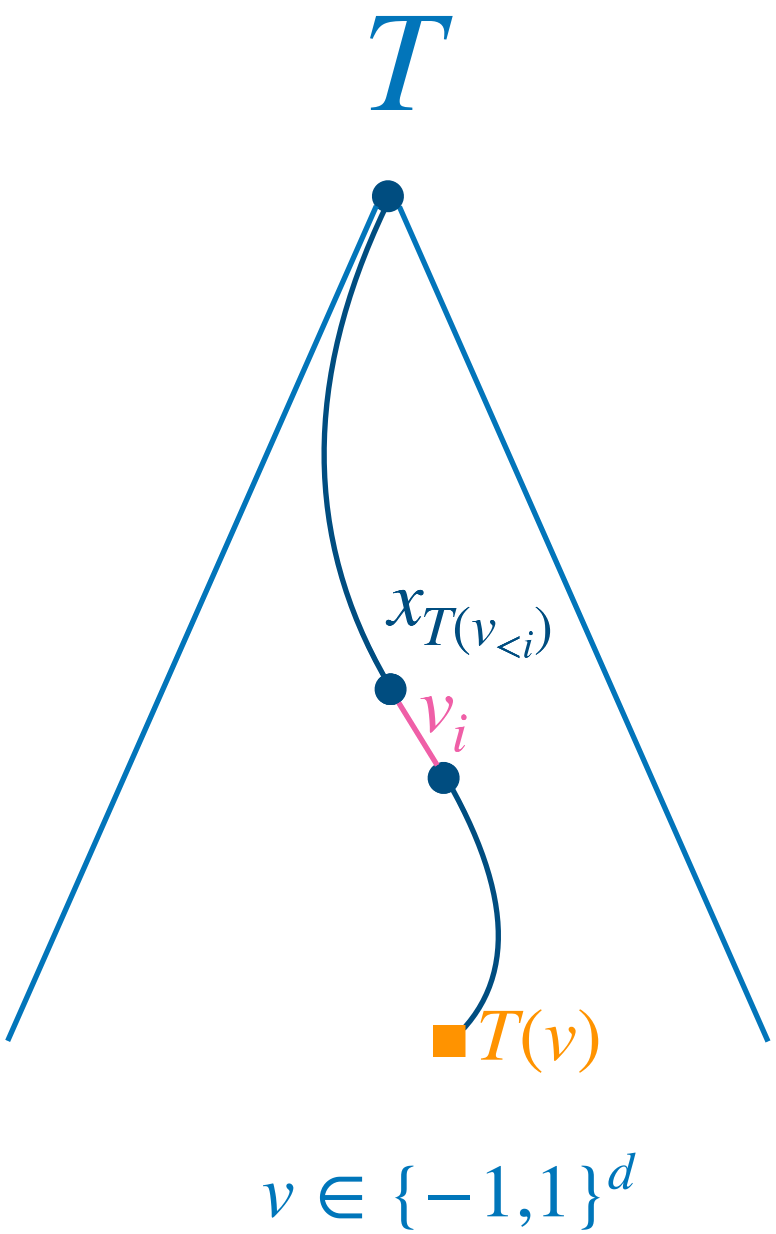
$$\| L_\ell T \| \le c^\ell \sqrt{\binom{d}{\ell}} \Lambda_{n^2,\ell}(p), \le \sqrt{(\ln(en^2))^{\ell-1}}$$

$$\Lambda_{m,\ell} = \begin{cases} 0, & \textit{if } p = 0, \\ p\sqrt{\left(\frac{1}{\ell}\ln\frac{e^\ell m^{\ell-1}}{p}\right)^\ell}, & \textit{if } 0 < p \le 1/m, \\ p\sqrt{\left(\ln\frac{e}{p}\right)(\ln em)^{\ell-1}}, & \textit{if } 1/m \le p \le 1. \end{cases}$$

increasing, concave

Our approach

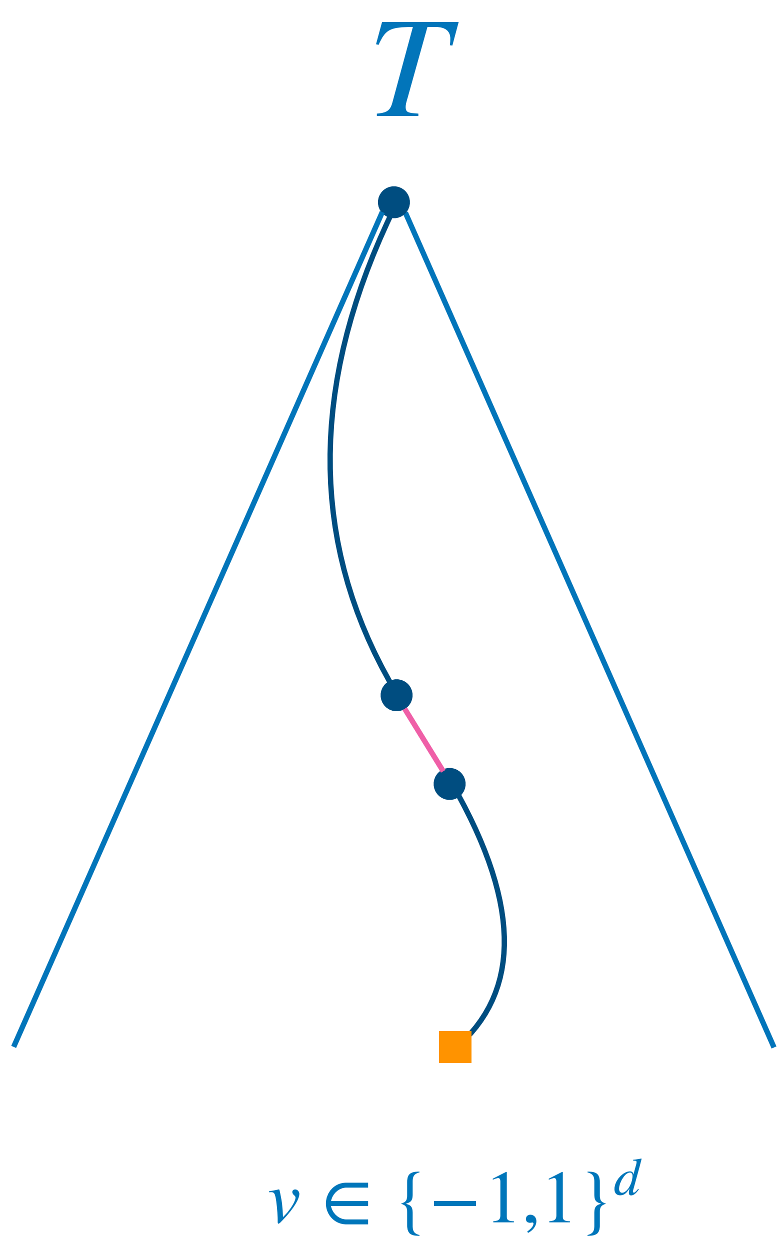
Our approach



Function computed by T

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

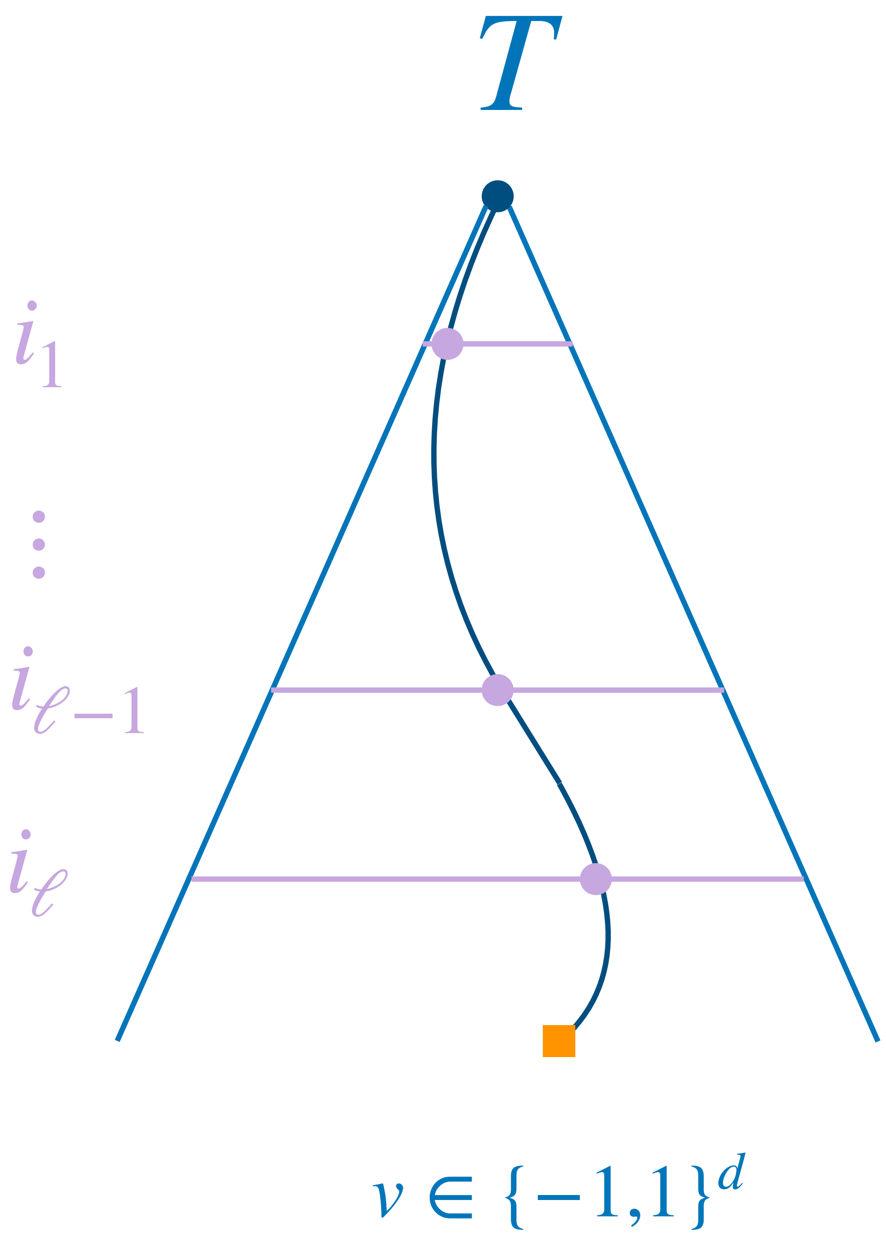
Our approach



Level-ℓ Fourier spectrum of T

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

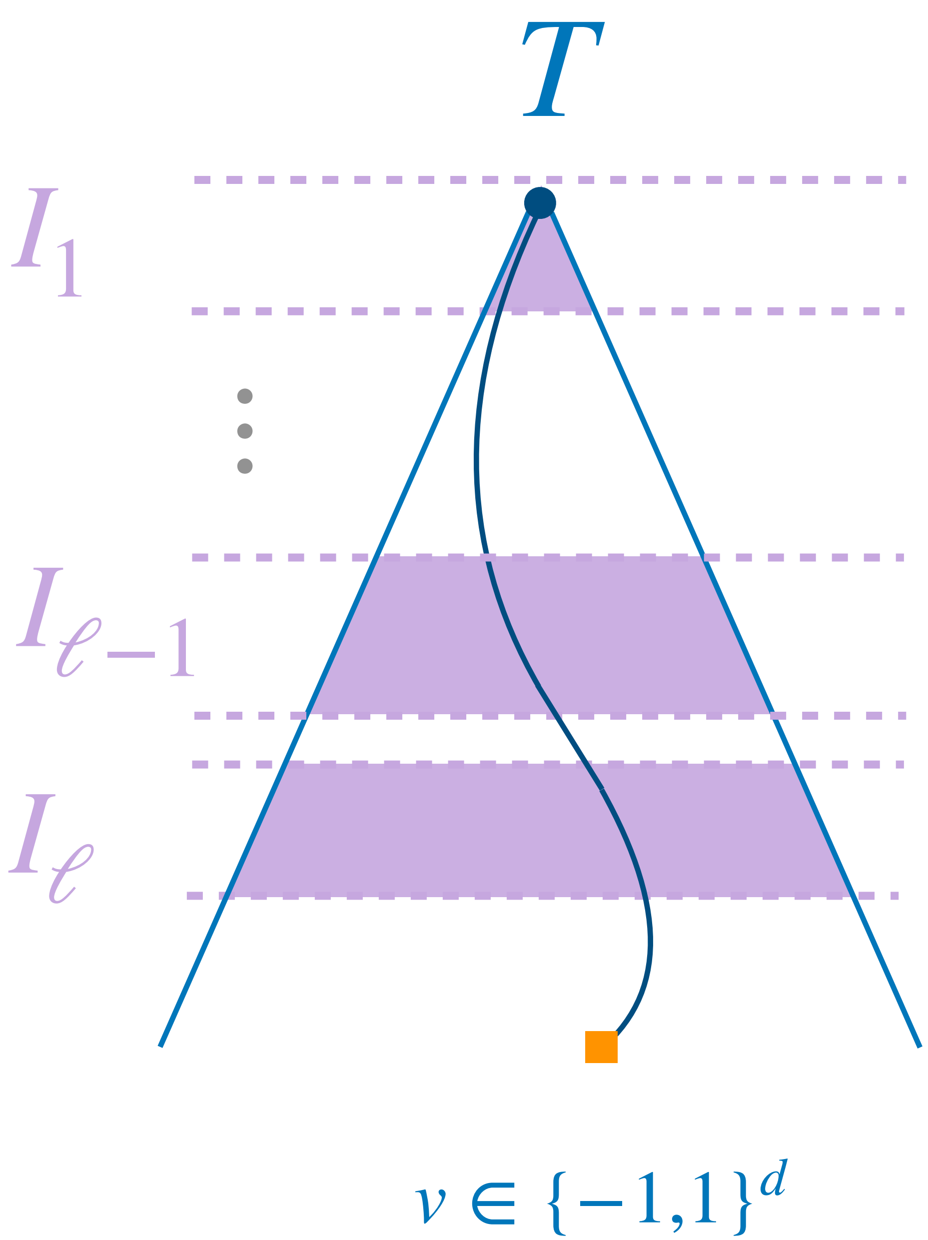
Our approach



Level-ℓ Fourier spectrum of T

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

Our approach



Level-ℓ Fourier spectrum of T

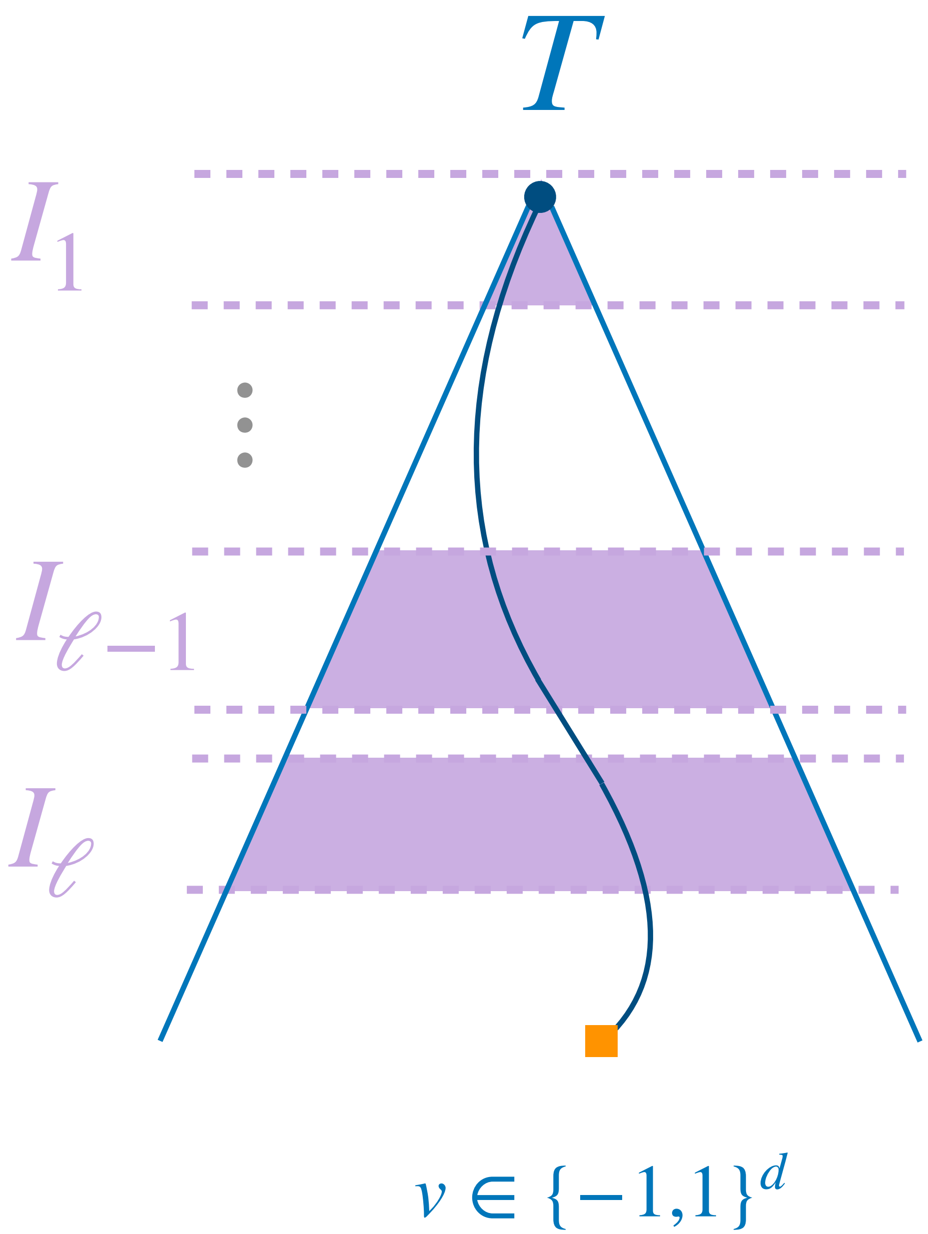
$$L_\ell T = \sum_{S \in \mathscr{P}_{d,\ell}} \sum_{v \in \{-1,1\}^d} T(v) 2^{-d} \prod_{i \in S} v_i x_{T(v_{<i})} .$$

**Key definition:*

Elementary family (simplified)

$$I_1 * I_2 * \cdots * I_\ell = \{\{i_1, i_2, \ldots, i_\ell\} : i_j \in I_j\} .$$

Our approach



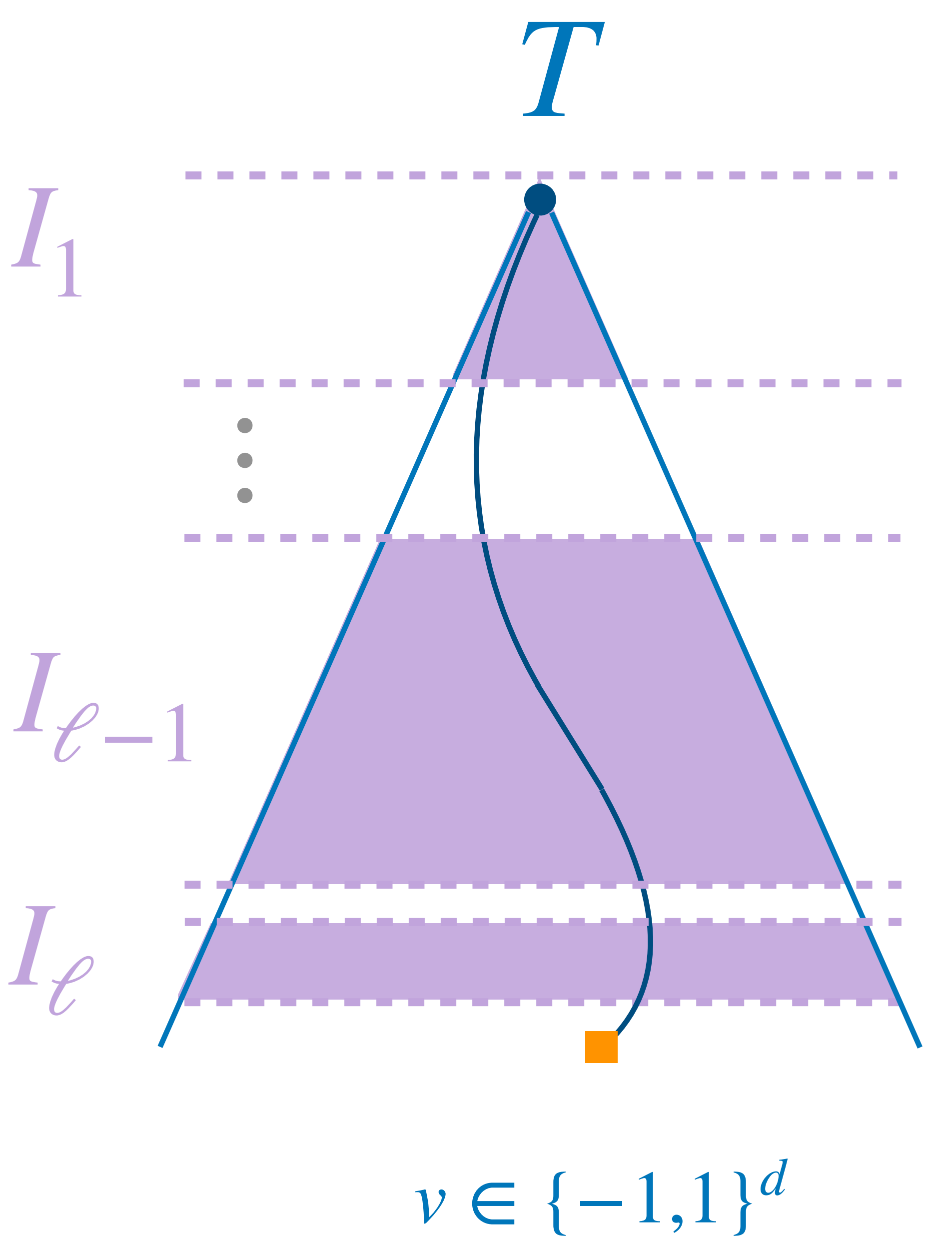
Level-ℓ Fourier spectrum of T

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

Level-ℓ Fourier spectrum restrict to $I_1 * I_2 * \cdots * I_\ell$

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

Our approach



Level-ℓ Fourier spectrum of T

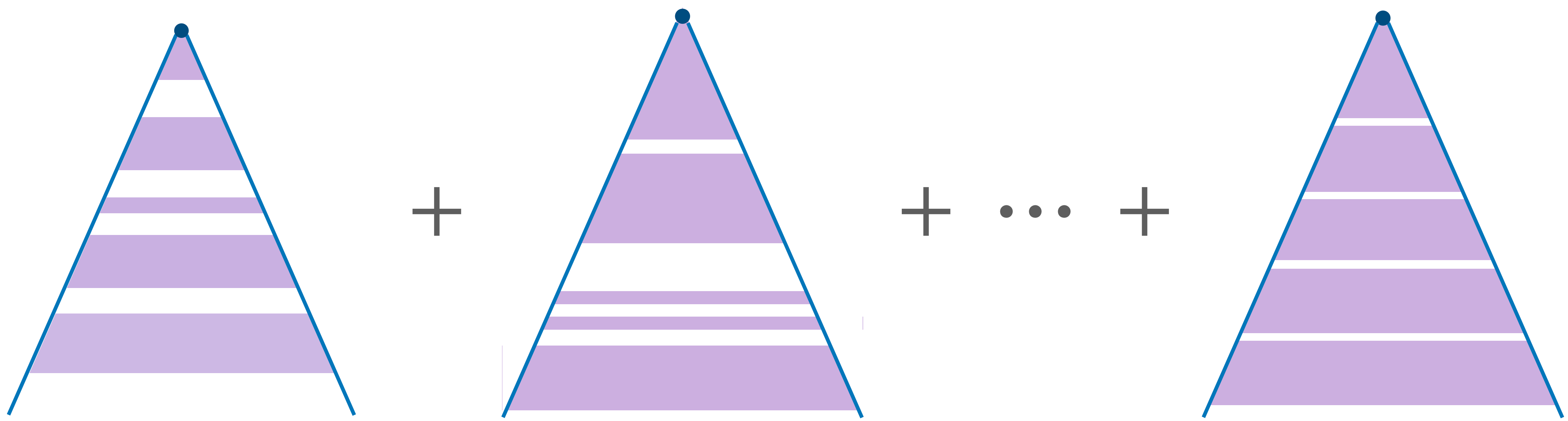
$$L_\ell T = \sum_{S \in \mathscr{P}_{d,\ell}} \sum_{v \in \{-1,1\}^d} T(v) 2^{-d} \prod_{i \in S} v_i x_{T(v_{<i})} .$$

Level-ℓ Fourier spectrum restrict to $I_1 * I_2 * \cdots * I_\ell$

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

Our key idea

$L_\ell T =$



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

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

Our proof

$$\left\| L_\ell T \right\| \le \sum_i \left\| T|_{\mathscr{E}_i} \right\| .$$

Theorem 1.

For some absolute constant c, and any elementary family $\mathscr{E} = I_1 * I_2 * \cdots * I_\ell$,

$$\left\| T|_{\mathscr{E}} \right\| \le c^\ell \sqrt{|\mathscr{E}|}\, \Lambda_{n^2,\ell}(\mathrm{dns}(T)) .$$

Theorem 2. ⚠ **not exactly**

$\mathscr{P}_{d,\ell}$ can be partitioned into elementary families $\mathscr{E}_1, \mathscr{E}_2, \ldots, \mathscr{E}_m$ s.t. for some const C,

$$\sum_{i=1}^{m} \sqrt{|\mathscr{E}_i|} \le C^\ell \sqrt{\binom{d}{\ell}} .$$

$$\left\| L_\ell T \right\| \le (cC)^\ell \sqrt{\binom{d}{\ell}} \times \Lambda_{n^2,\ell}(\mathrm{dns}(T))$$

Open problems

Problem 1

In query model, for any total function f, is

$R(f) \leq O(Q(f)^3)$?

Problem 2

In communication model, is there absolute constant C, such that, for any total function f,

$R^{\mathrm{cc}}(f) \leq O(Q^{\mathrm{cc}}(f)^C)$?

Thank you!