Quantum and Classical Strong Direct Product Theorems and Optimal Time-Space Tradeoffs

Robert Špalek

joint work with Ronald de Wolf

and Hartmut Klauck

UNIVERSITY OF CALGARY

Computing Many Copies of a Function

- Suppose the complexity of f is well understood,
  e.g. we need $T(f)$ resources to compute f with small error
- Specify "compute" and "resources"
  (circuit size, queries, communication, …)
- Fundamental question:

  how hard is it to compute k independent instances $f(x^1),\ldots,f(x^k)$?

Direct Product Theorems

- Relation between total resources T and overall success probability σ?
- Intuition: constant error on each instance $\Rightarrow$ exponentially small σ
- *Weak* direct product theorem:

$$T \leq \alpha T(f) \Rightarrow \sigma \leq 2^{-\gamma k}$$

- *Strong* direct product theorem:

$$T \leq \alpha k T(f) \Rightarrow \sigma \leq 2^{-\gamma k}$$

Our Results

Strong direct product theorems for:

1. Classical query complexity of OR
2. *Quantum query complexity of OR*
3. Quantum communication complexity of Disj

Time-space tradeoffs for:

1. *Quantum sorting*
2. Classical and quantum Boolean matrix products

Communication-space tradeoffs for quantum matrix products

DPT 1: Classical Query Complexity

- Task: compute $\mathrm{OR}_n^{(k)}$ using T queries

$$x = \underbrace{\boxed{\;x^1\;}}_{n \text{ bits}}\underbrace{\boxed{\;x^2\;}}_{n \text{ bits}}\cdots\cdots\underbrace{\boxed{\;x^k\;}}_{n \text{ bits}}$$

- Strong direct product theorem:

  Every classical algorithm with $T \leq \alpha k n$ queries has worst-case success probability $\sigma \leq 2^{-\gamma k}$

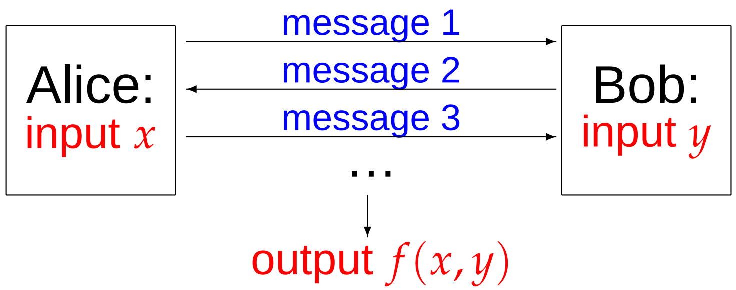
$$T \leq \alpha k n \;\Rightarrow\; \sigma \leq 2^{-\gamma k}$$

DPT 2: Quantum Query Complexity

- [Grover, 1996]
  OR_n with $\sigma \approx 1$ in $\Theta(\sqrt{n})$ queries
- [Buhrman, Newman, Röhrig & de Wolf, 2003]
  $\mathrm{OR}_n^{(k)}$ with $\sigma \approx 1$ in $O(k\sqrt{n})$ queries, i.e. no log-factor needed!
- Direct product theorem:

$$\#\text{queries } T \leq \alpha k\sqrt{n} \;\Rightarrow\; \text{success } \sigma \leq 2^{-\gamma k}$$

DPT 3: Quantum Communication Complexity



- Disjointness problem: “distributed NOR”

  Alice has n-bit input x, Bob has n-bit y
  Question: $x \cap y = \emptyset$ or not?

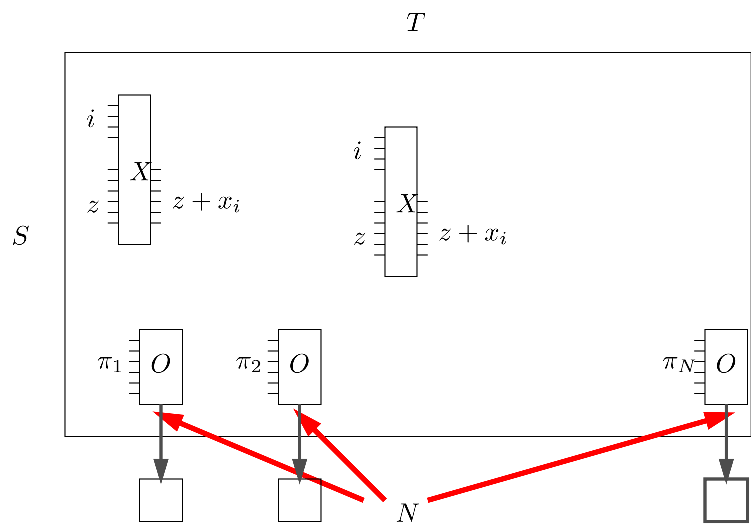
- Classical: $\Theta(n)$ bits of communication
  Quantum: $\Theta(\sqrt{n})$ qubits [BCW, AA, Razborov]

- We prove a DPT: communication $C \leq \alpha k \sqrt{n}$ qubits $\Rightarrow \sigma \leq 2^{-\gamma k}$

Time-space tradeoffs

Tradeoff: Sorting by a Quantum Circuit

- Input: $x_1, \ldots, x_N$ accessed by input gates X
- Output: Indices π of x sorted *large to small*, sent to output gates O

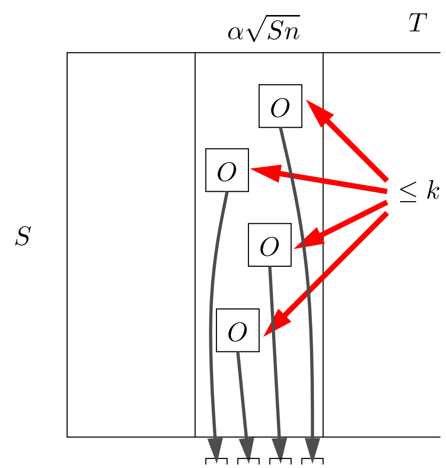


$$S \ll N \log N$$

- [Klauck, 2003] $T^2 S = O(N^3 \log^3 N)$
- [our paper] $T^2 S = \Omega(N^3)$

Slicing the Sorting Circuit

- Slice the circuit into $\frac{T}{\alpha\sqrt{SN}}$ slices, each containing $\alpha\sqrt{SN}$ queries.
- Let each slice contain $\leq k$ output gates.



- We show that $k = O(S)$ due to the DPT.
- $N \leq$ # slices $\cdot\, k = O\left(\frac{T\sqrt{S}}{\alpha\sqrt{N}}\right)$, hence $T^2 S = \Omega(N^3)$.

Each Slice Has Only Few Output Gates: $k = O(S)$

If $k < S$, then certainly $k = O(S)$, so assume $k \geq S$.

- Within slice, the circuit outputs $\pi_{a+1}, \ldots, \pi_{a+k}$ with probability $\geq 2/3$.
  - Plug $x = (2^a, \quad z_1, z_2, \ldots, z_{N/2}, \quad 0^{N/2-a})$ for given $z \in \{0,1\}^{N/2}$.
  - $|z| \geq k \iff \forall \ell = 1, \ldots, k: \ x_{\pi_{a+\ell}} = 1$.
  - Bounded-error sorting can compute Threshold$_k$ with one-sided error.
- Replace S-qubit starting state by completely mixed state; *overlap* with correct state is 2^{-S} $\Rightarrow$ circuit for Threshold$_k$ with probability $\sigma \geq \frac{2}{3} \cdot 2^{-S}$.
- However #queries $T = \alpha\sqrt{SN} \leq \alpha\sqrt{kN}$, hence by DPT $\sigma \leq 2^{-\gamma k}$.

Conclude that $k = O(S)$.

Tradeoff: Boolean Matrix Products

- Input: vector b
- Output: Boolean product $c = Ab$ for a fixed matrix A

$$c_i = \bigvee_{\ell=1}^{N} A_{i,\ell} \wedge b_\ell$$

- [Abrahamson, 1990] Classically, $TS = \Omega(N^{3/2})$
- [our paper] $\left.\begin{array}{ll}\text{Classically,} & TS = \Omega(N^2) \\ \text{Quantumly,} & T^2S = \Omega(N^3)\end{array}\right\}$ both tight

Communication-Space Tradeoffs

- Input: Alice has A and Bob has b.
- Output: *Boolean* product $c = Ab$.

- [Beame, Tompa & Yan, 1994] Tight bounds for $\mathrm{GF}(2)$ products.
- [our paper] Quantumly, *Boolean* products $C^2 S = \Omega(N^3)$ (tight up to polylog factors).

Proof of quantum DPT

DPT Sounds Plausible, but not Always True

- [Shaltiel, 2001] Uniform input distribution and

$$f(x_1, \ldots, x_n) = x_1 \vee (x_2 \oplus \cdots \oplus x_n)$$

With $\frac{2}{3}n$ queries, success probability is $3/4$: $\mathrm{Succ}_{\frac{2}{3}n}(f) = 3/4$.

- But on average, $\approx k/2$ instances can be solved with only 1 query. The saved queries can be used to answer the other $\approx k/2$ instances:

$$\mathrm{Succ}_{\frac{2}{3}kn}(f^{(k)}) = 1 - 2^{-\Omega(k)} \gg (3/4)^k.$$

- DPT plausible for "hard on average" f

The Polynomial Method

[Beals, Buhrman, Cleve, Mosca & de Wolf, 1998]

- Final state of T-query algorithm on input $x \in \{0,1\}^N$

$$\sum_z \alpha_z(x)|z\rangle$$

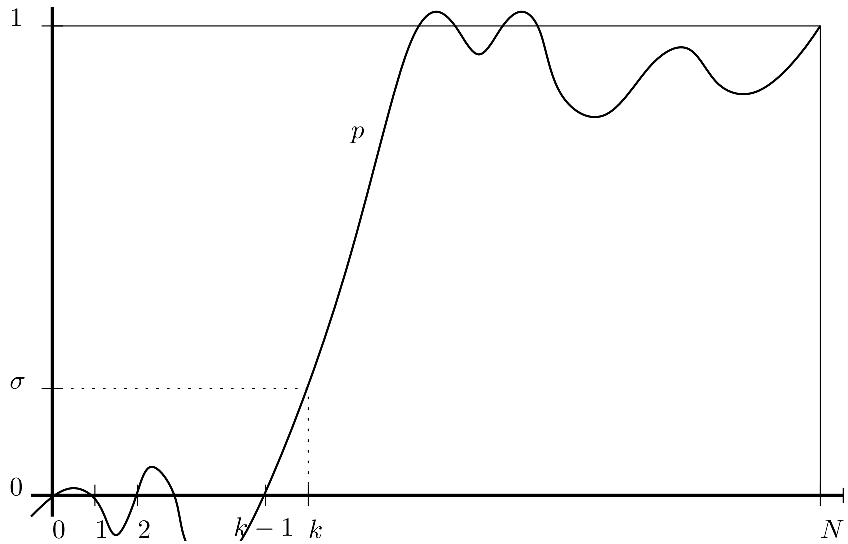
- $\alpha_z(x)$ is degree-T polynomial $\Rightarrow$

  acceptance prob is degree-$2T$ polynomial

- *Query lower bounds from polynomial degree lower bounds*

Lower Bound for k-Threshold (lite)

- Consider degree-d polynomial p ($N = kn$)

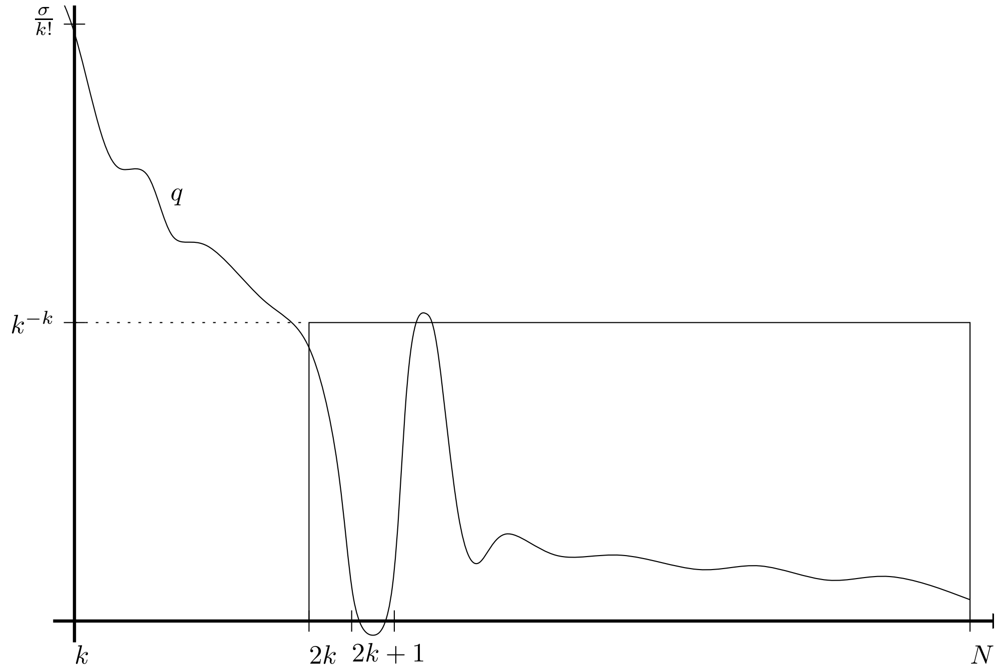


$$p(x) \begin{cases} = 0; & x = 0, \ldots, k-1 \\ \in [0,1]; & x = k, \ldots, N \end{cases}$$

How big can $\sigma = p(k)$ be?

- [Aaronson, 2004] $d \le \alpha\sqrt{kn} \Rightarrow \sigma \le 2^{-\gamma k}$
- [our paper] $d \le \alpha k \sqrt{n} \Rightarrow \sigma \le 2^{-\gamma k}$

Lower Bound for k-Threshold (cont)



- *Factor* p as

$$p(x) = q(x) \prod_{j=0}^{k-1} (x - j)$$

- $q(k) = \dfrac{\sigma}{k!}$

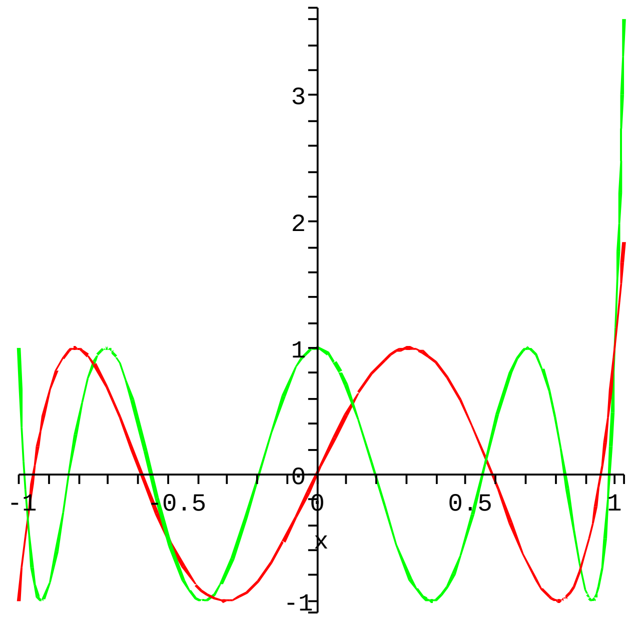
$|q(i)| \le k^{-k}$ for integers $i \in \{2k, \dots, N\}$

- [Coppersmith & Rivlin, 1992]

$|q(x)| \le k^{-k} e^{d^2/N}$ for all real $x \in [2k, N]$

Lower Bound for k-Threshold (cont)

- Rescale q to $[-1,1] \times [-1,1]$,
  upper bound it by degree-d
  Чебышев *(Chebyshev)* polynomial T_d:



- $T_d(1+\mu) \leq e^{2d\sqrt{2\mu+\mu^2}}$
- Combining everything gives ($d = \alpha k \sqrt{n}$)

$$\sigma \leq e^{(\alpha^2+4\alpha-1)k}$$

  Choose α sufficiently small

- We have proven degree $d \leq \alpha k \sqrt{n} \Rightarrow$ success $\sigma \leq 2^{-\gamma k}$

Reduction: Quantum DPT for OR (lite)

- *k-threshold*: for kn-bit input, decide whether $|x| \geq k$
  - [BBCMW98] Acceptance probability of a T-query algorithm is a degree-$2T$ polynomial
  - key lemma $\Longrightarrow$ *one-sided* error algorithms with $\alpha k\sqrt{n}$ queries have σ exponentially small
- *k independent search problems*
  - can solve $k/2$-threshold with good probability using k-search
  - apply random permutation of input bits
- *k independent OR problems*
  - can solve k-search by binary search using k-OR
  - verify the 1 at the end to make it one-sided

$\Longrightarrow$ lower bound for k-OR

DPT for Search

$$x = \overbrace{\underbrace{\boxed{x^1}}_{n \text{ bits}}\ \underbrace{\boxed{x^2}}_{n \text{ bits}} \cdots\cdots \underbrace{\boxed{x^k}}_{n \text{ bits}}}^{N=kn \text{ bits}}$$

Suppose we have algorithm A for Search$^{(k)}$,
with $T = \alpha k \sqrt{n}$ queries and success prob σ.

Use A to solve $k/2$-threshold:

1. Randomly permute $x \in \{0,1\}^N$.
   With prob $\geq 2^{-k/2}$: all $k/2$ ones in separate blocks
2. Run A, check its k outputs, return 1 iff $\geq k/2$ ones found

This solves $k/2$-threshold with prob $\geq \sigma 2^{-k/2}$

$$\Rightarrow \sigma \leq 2^{-\gamma k} \text{ for small } \alpha$$

DPT for OR

Suppose we have algorithm A for $\mathrm{OR}_n^{(k)}$,
with $T = \alpha k\sqrt{n}$ queries and success prob σ.

Use A to solve Search$^{(k)}$:

1. Do $s = 2\log(1/\alpha)$ rounds of binary search on the k blocks using A
2. Run *exact* Grover on each $\frac{n}{2^s}$ block
3. For each block, return 1 if found a one

This uses $\underbrace{sT}_{\text{step 1}} + \underbrace{k\sqrt{n/2^s}}_{\text{step 2}} \approx 2\alpha\log(1/\alpha)k\sqrt{n}$ queries,
and has success probability $\geq \sigma^s$

$$\Rightarrow \sigma \leq 2^{-\gamma k} \text{ for small } \alpha$$

Summary

- *Strong direct product theorem:*
  resources for $f^{(k)} \ll k *$ resources for f
  $\Rightarrow$ success probability $\sigma \leq 2^{-\gamma k}$.

- We prove this for $f =$OR in 3 settings:
  1. Classical query complexity
  2. Quantum query complexity
  3. Quantum communication complexity

- Implies strong *time-space tradeoffs* (sorting, Boolean matrix products) and *communication-space tradeoffs* (Boolean matrix products)