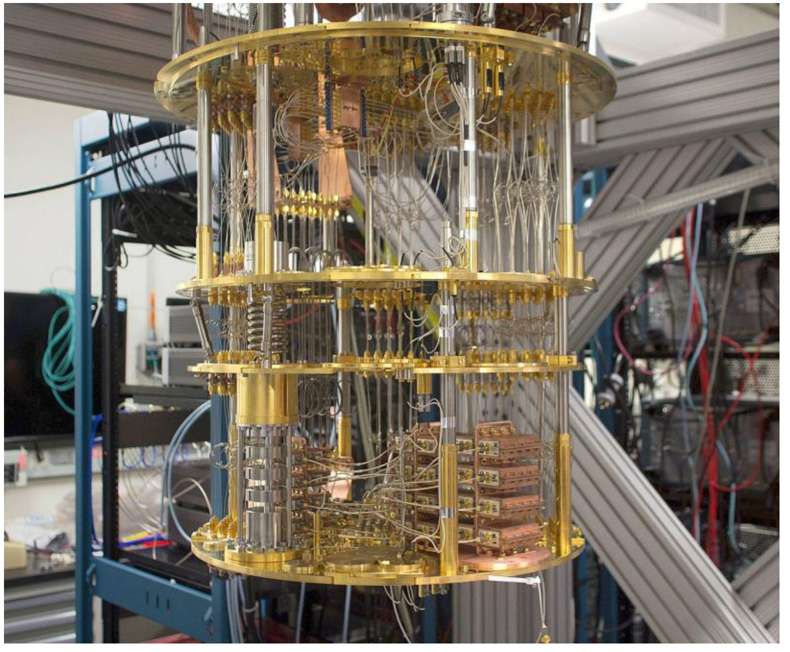
Classical Lower Bounds from Quantum Upper Bounds

Shalev Ben-David, Adam Bouland,
Ankit Garg, Robin Kothari

MIT
Microsoft Research
Berkeley UNIVERSITY OF CALIFORNIA
JOINT CENTER FOR QUANTUM INFORMATION AND COMPUTER SCIENCE

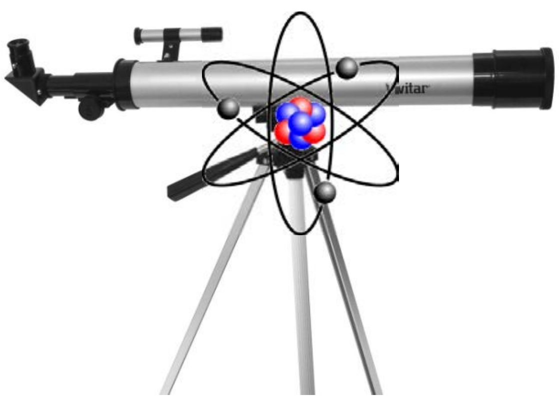
What is quantum information good for?

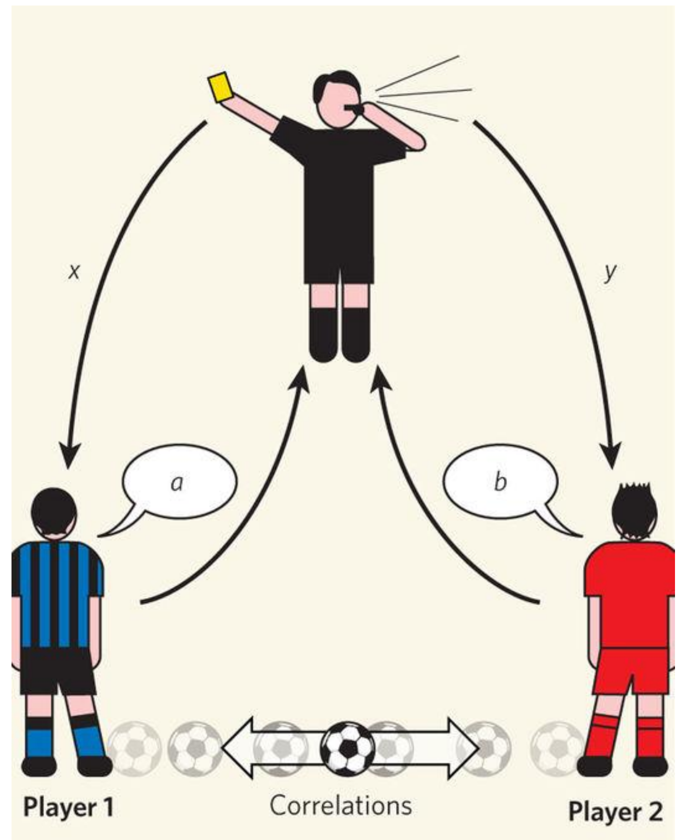
- Building/understanding quantum computers



What is quantum information good for?

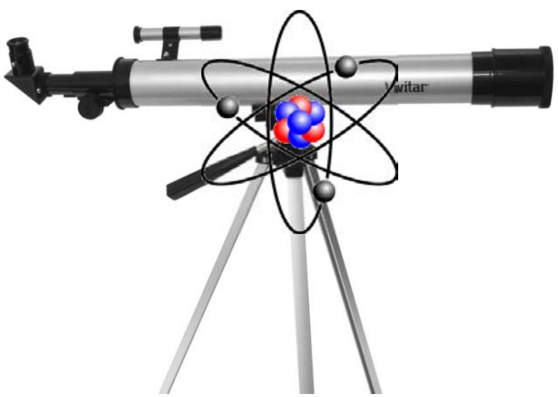
- Understanding quantum mechanics

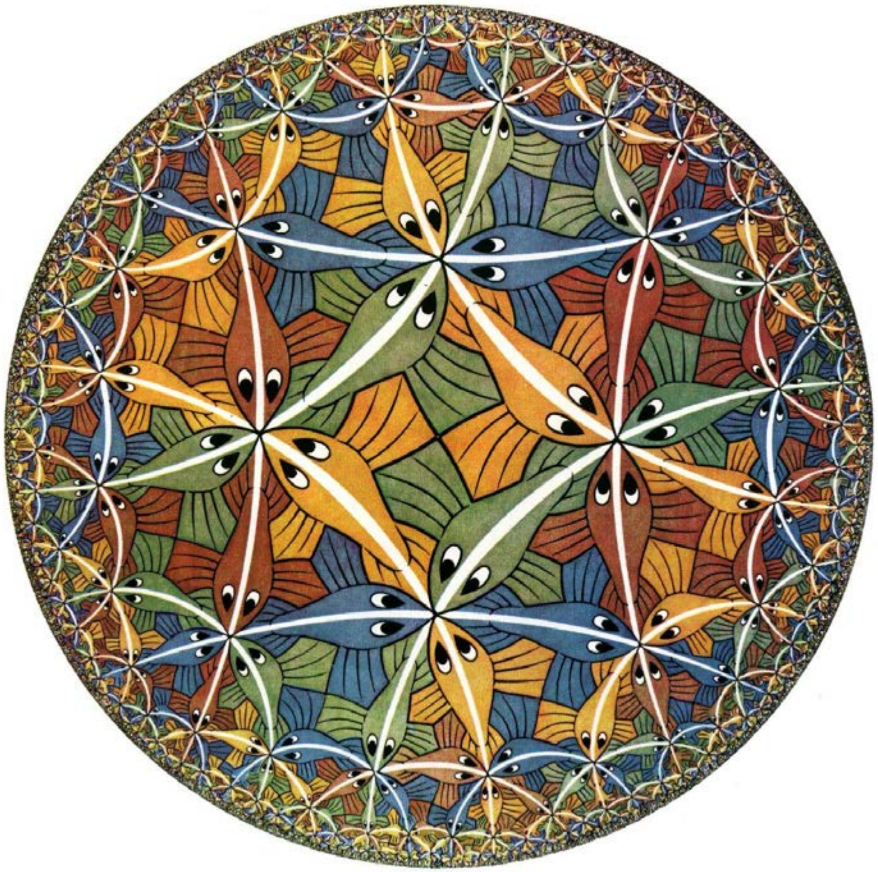




What is quantum information good for?

- Understanding quantum gravity

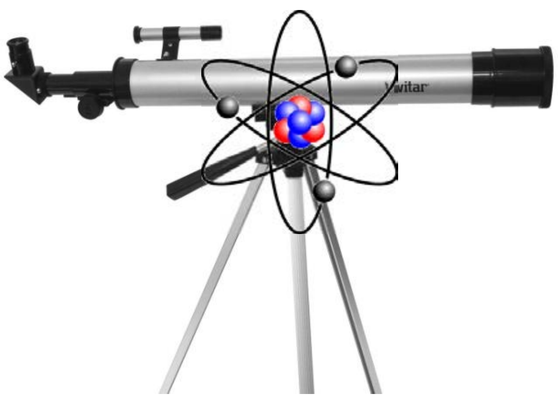


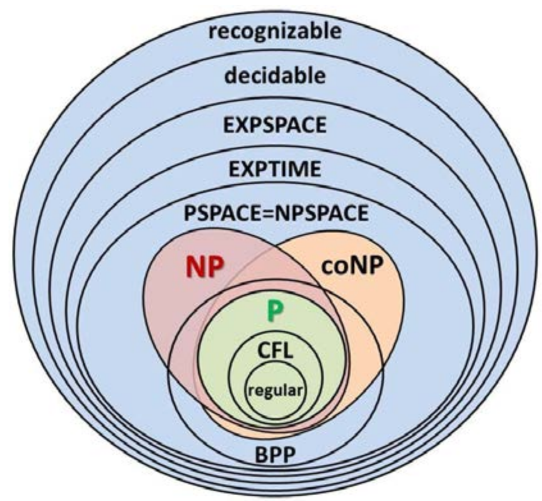


What is quantum information good for?

- Learning about the nature of computation

Oftentimes one can prove statements about classical computer science using quantum ideas and techniques: The Quantum Method





What is quantum information good for?

- Learning about the nature of computation

Oftentimes one can prove statements about classical computer science using quantum ideas and techniques: The Quantum Method

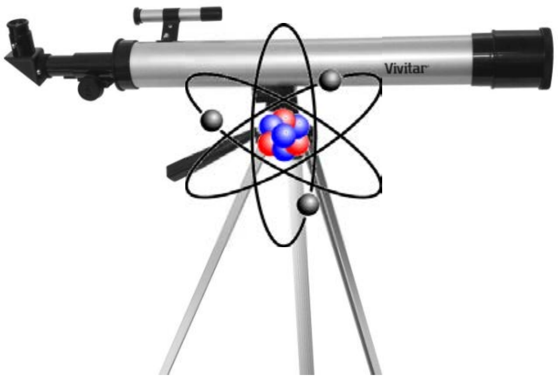
THEORY OF COMPUTING LIBRARY
GRADUATE SURVEYS 2 (2011), pp. 1–54
www.theoryofcomputing.org

Quantum Proofs for Classical Theorems

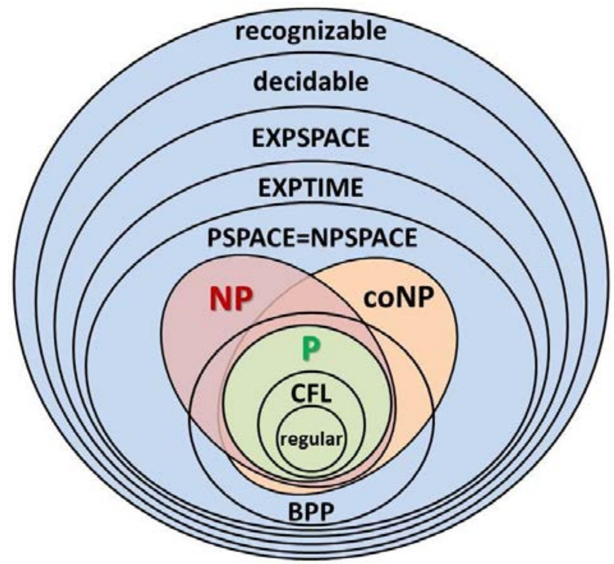
Andrew Drucker* Ronald de Wolf†

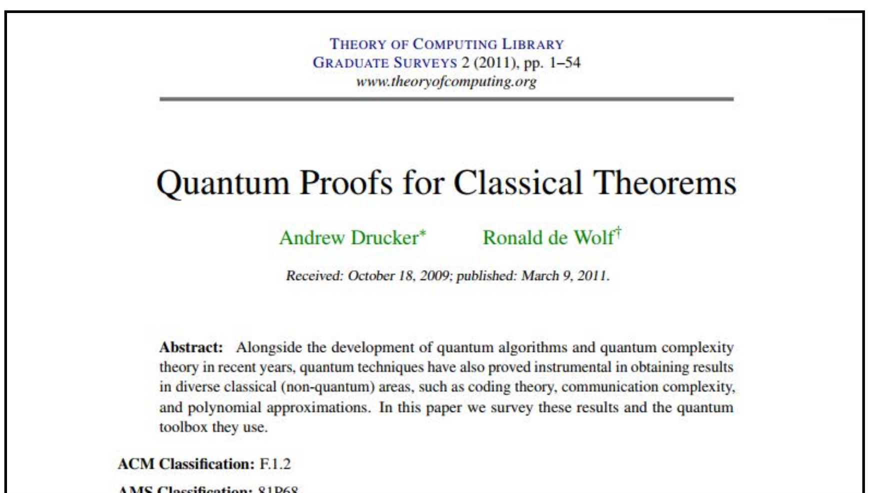
Received: October 18, 2009; published: March 9, 2011.

Our Results



Approximate degree & communication complexity





THEORY OF COMPUTING LIBRARY
GRADUATE SURVEYS 2 (2011), pp. 1–54
www.theoryofcomputing.org

Quantum Proofs for Classical Theorems

Andrew Drucker* Ronald de Wolf†

Received: October 18, 2009; published: March 9, 2011.

Abstract: Alongside the development of quantum algorithms and quantum complexity theory in recent years, quantum techniques have also proved instrumental in obtaining results in diverse classical (non-quantum) areas, such as coding theory, communication complexity, and polynomial approximations. In this paper we survey these results and the quantum toolbox they use.

ACM Classification: F.1.2

AMS Classification: 81P68

Our Results

Main Result:

A lower bound on the "approximate degree" of certain compositions of functions, and related quantities in communication complexity

Proof uses a **quantum algorithm** of Belovs, and there is **no known classical proof** of these results

Wait, what??

"Ironic Complexity"

Often one can use fast algorithms (upper bounds) to prove lower bounds

> **Non-Uniform ACC Circuit Lower Bounds**
>
> Ryan Williams*
> IBM Almaden Research Center
>
> November 23, 2010
>
> **Abstract**
>
> The class ACC consists of circuit families with constant depth over unbounded fan-in AND, OR, NOT, and MOD_m gates, where $m > 1$ is an arbitrary constant. We prove:
>
> - $\mathsf{NTIME}[2^n]$ does not have non-uniform ACC circuits of polynomial size. The size lower bound can be slightly strengthened to quasi-polynomials and other less natural functions.
> - E^{NP}, the class of languages recognized in $2^{O(n)}$ time with an NP oracle, doesn't have non-uniform ACC circuits of $2^{n^{o(1)}}$ size. The lower bound gives an exponential size-depth tradeoff: for every d

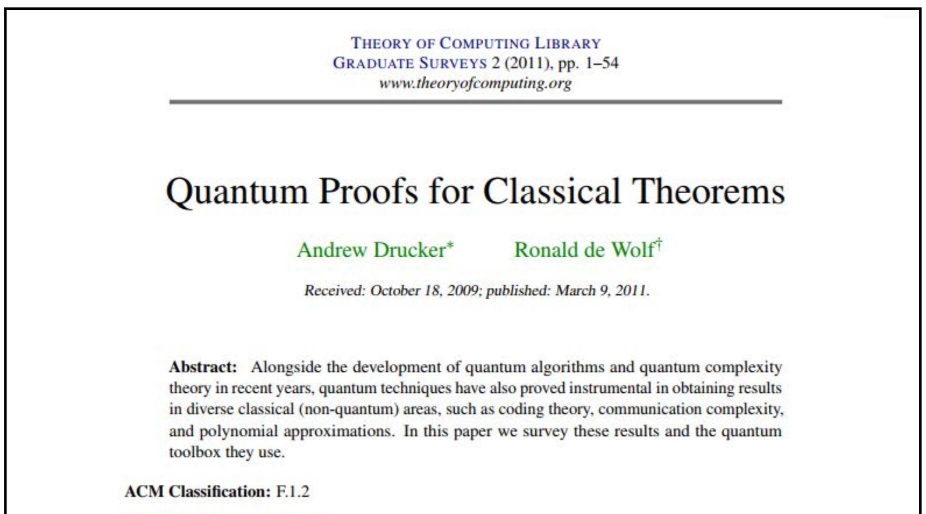
Also Hoza '17, Cleve et al '13

Our Results

"Quantum Method" + "Ironic Complexity"

Using quantum methods to prove classical theorems

Using fast algorithms to prove lower bounds


THEORY OF COMPUTING LIBRARY
GRADUATE SURVEYS 2 (2011), pp. 1–54
www.theoryofcomputing.org

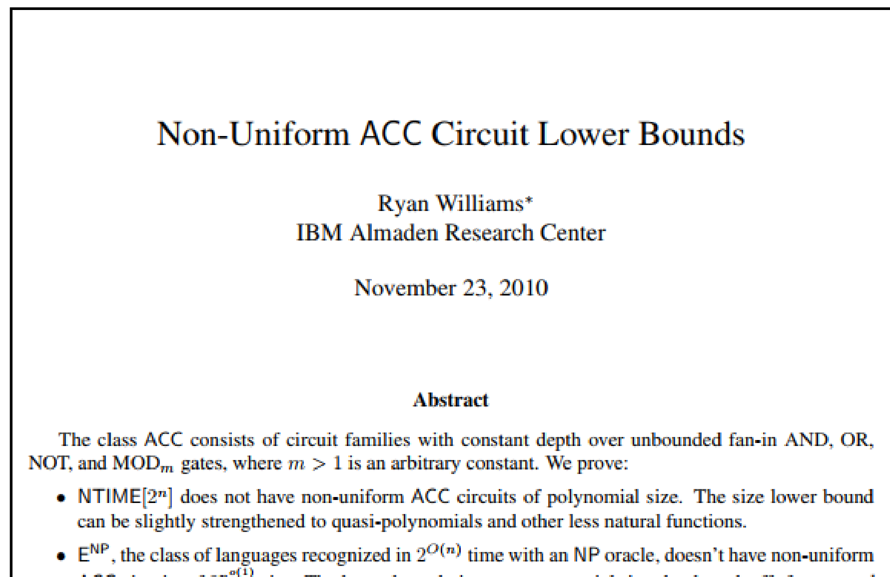
Quantum Proofs for Classical Theorems

Andrew Drucker* Ronald de Wolf†

Received: October 18, 2009; published: March 9, 2011.

Abstract: Alongside the development of quantum algorithms and quantum complexity theory in recent years, quantum techniques have also proved instrumental in obtaining results in diverse classical (non-quantum) areas, such as coding theory, communication complexity, and polynomial approximations. In this paper we survey these results and the quantum toolbox they use.

ACM Classification: F.1.2



Non-Uniform ACC Circuit Lower Bounds

Ryan Williams*
IBM Almaden Research Center

November 23, 2010

Abstract

The class ACC consists of circuit families with constant depth over unbounded fan-in AND, OR, NOT, and MOD_m gates, where $m > 1$ is an arbitrary constant. We prove:

- $\text{NTIME}[2^n]$ does not have non-uniform ACC circuits of polynomial size. The size lower bound can be slightly strengthened to quasi-polynomials and other less natural functions.
- E^{NP}, the class of languages recognized in $2^{O(n)}$ time with an NP oracle, doesn't have non-uniform ACC circuits of $2^{n^{o(1)}}$ size. The lower bound gives an exponential size-depth tradeoff: for every d

Background

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

Approximate degree is a classical measure of the "complexity" of f (denoted $\widetilde{\deg}(f)$)
[Minsky Papert '69, Nisan Szegedy '94]

Background

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

$\widetilde{\deg}(f)$ is the minimum degree of a polynomial p in variables $x_1 \ldots x_m$ such that for all x in $\{0,1\}^m$

$$|f(x) - p(x)| \leq 1/3$$

Lower bounds quantum query complexity

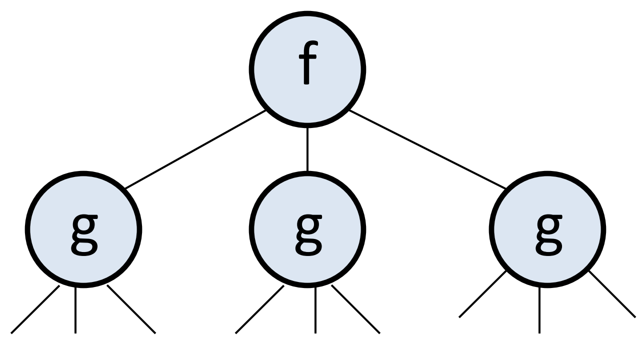
(Beals et al.)

Background

Fundamental Problem: How does $\widetilde{\deg}(f)$ behave under composition?

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

$f \circ g : \{0,1\}^{nm} \to \{0,1\} = f(g,g,g,\ldots g)$



What is $\widetilde{\deg}(f \circ g)$?

Background

What is $\widetilde{\deg}(f \circ g)$?

Prior work: deg(f ◦g) = O(deg(f) deg(g))
[Sherstov ’12, improving Buhrman et al. ‘07]

Proof: compose the polynomials**!

Leaves open: is $\widetilde{\deg}(f \circ g) = \Omega(\widetilde{\deg}(f)\, \widetilde{\deg}(g))$?

Difficult to prove this! Only known for specific f,g

Our results

For all functions f,

$$\widetilde{\deg}(\mathsf{OR}_n \circ f) = \Omega(\sqrt{n}\ \widetilde{\deg}(f))$$

Prior Results

What is the deg($OR_n \circ AND_n$)?

Bound	Citation
$O(n)$	Høyer, Mosca and de Wolf [HMdW03]
$\Omega\left(\sqrt{n}\right)$	Nisan and Szegedy [NS94]
$\Omega\left(\sqrt{n \log n}\right)$	Shi [Shi02]
$\Omega\left(n^{0.66\ldots}\right)$	Ambainis [Amb05]
$\Omega\left(n^{0.75}\right)$	Sherstov [She09]
$\Omega(n)$	Sherstov [She13a] and Bun and Thaler [BT13]

Took 20 years to resolve just AND-OR tree!

Our results

For all functions f,

$$\widetilde{\deg}(\mathsf{OR}_n \circ f) = \Omega(\sqrt{n}\ \widetilde{\deg}(f))$$

(

vs. prior was only known

$$\widetilde{\deg}(\mathsf{OR}_n \circ \mathsf{AND}_m) = \Omega(\sqrt{nm})$$

)

Generalizes existing results of AND-OR tree towards a general composition theorem,

with completely different proof technique

Our Results

Unbalanced case:

$$\widetilde{\deg}\Big(\mathsf{OR}_n \circ (f_1, f_2, \ldots, f_n)\Big)^2 = \Theta\Big(\sum_i \widetilde{\deg}(f_i)^2\Big)$$

-> tightly characterizes unbalanced AND-OR trees of any constant depth

[See also Ambainis'06]

Our Results

We tightly characterize OR composition for deg

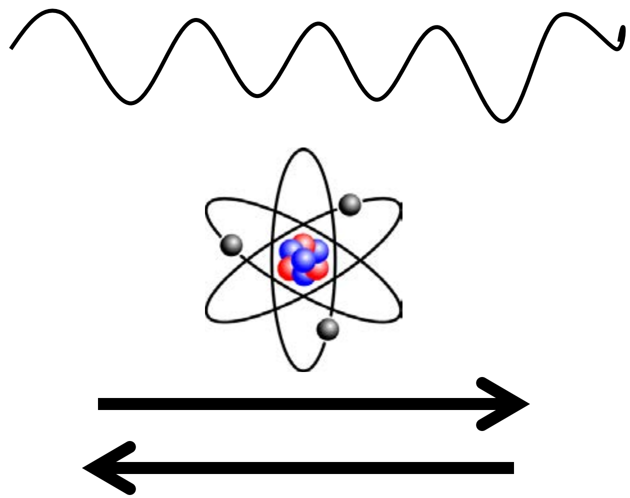
$$\widetilde{\deg}(\mathrm{OR}_n \circ f) = \Omega(\sqrt{n}\ \widetilde{\deg}(f))$$

Also extend our results to quantum communication complexity

Our Results: Extensions

Quantum communication complexity:

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



$x \in \mathcal{X}$ $y \in \mathcal{Y}$

Quantum communication

Unlimited preshared entanglement

Q*(F)

Our Results: Extensions

How much communication is required to compute Q*($\mathrm{OR}_n \circ F$)?

We have for all F:

$$Q^* \left(\mathrm{OR}_n \circ F\right) = \Omega\left(\frac{\sqrt{n}\log\widetilde{\gamma}_2(F)}{\operatorname{polylog} n}\right)$$

If F has an all zero row or column,

$$Q^* \left(\mathrm{OR}_n \circ F\right) = \Omega(\sqrt{n}\log\widetilde{\gamma}_2(F))$$

Our Results: Extensions

How powerful are these new communication results?

We can reprove many (hard) quantum communication lower bounds

Our Results: Extensions

Reprove powerful old results:

1. DISJOINTNESS= $\bigvee_{i=1}^{n}(x_i \wedge y_i)$

   Q*(DISJOINTNESS)= $\Omega(n^{1/2})$

Reproves [Razbarov'03]

2. In fact it even requires $\Omega(n^{1/2}/\log n)$ in "quantum information complexity"

Reproves [Braverman et al. '15] up to log

Our Results

Summary:

We’ve characterized how approximate degree & quantum communication quantities

compose under OR composition

(up to log factors)

This surpasses previous results, and can even be used to reprove many known lower bounds

Our Techniques

All proofs have a common technique:

Use a clever algorithm of Belovs for a seemingly unrelated problem called “Combinatorial Group Testing”

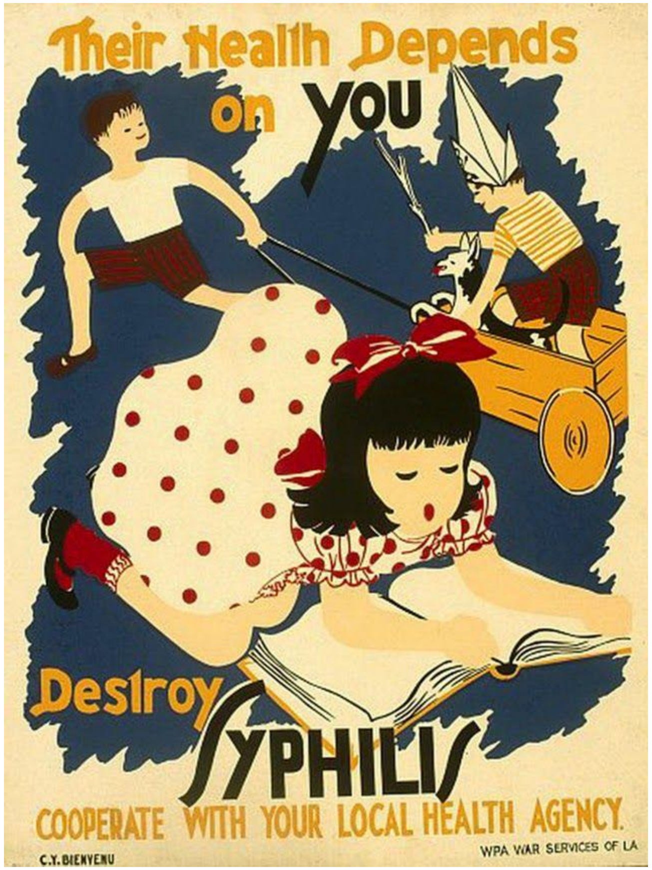
Combinatorial Group Testing

Origins: WWII testing for Syphilis

Goal: Given blood samples from n people, determine which have disease

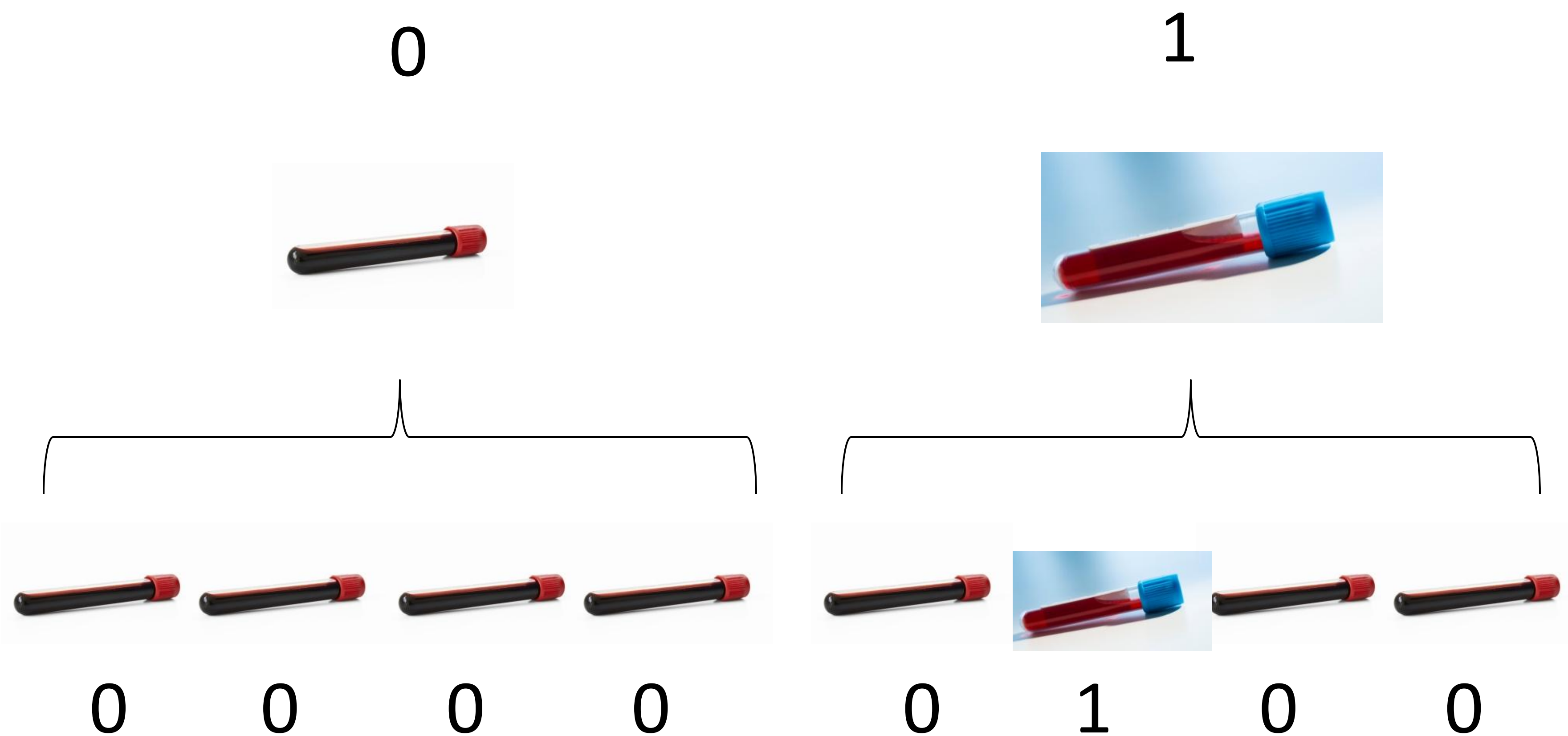
Blood test detected antigen, want to minimize # tests

Note: If you mix multiple samples, you can tell if at least one of the samples has the antigen



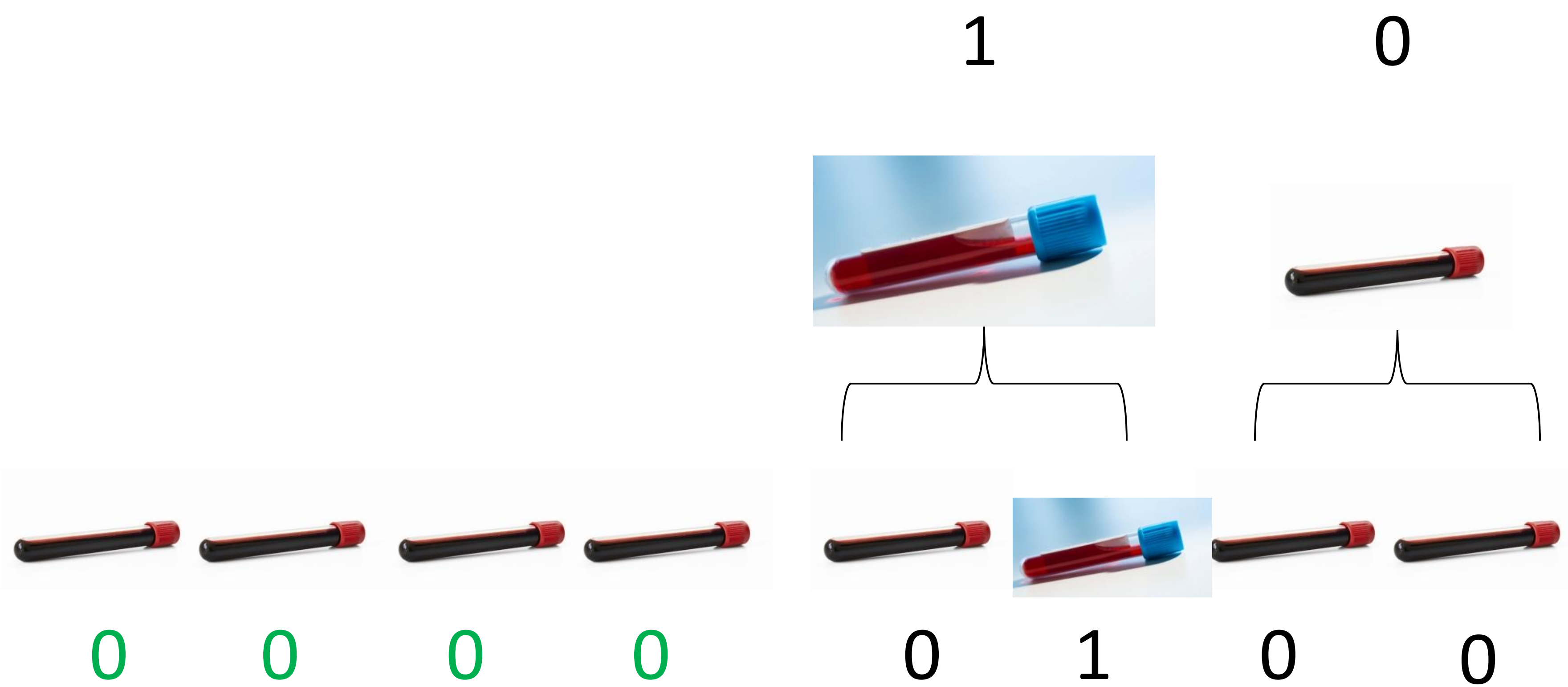
Combinatorial Group Testing

If few have the disease, can use fewer than n tests



Combinatorial Group Testing

If few have the disease, can use fewer than n tests



Combinatorial Group Testing

If you know only 1 person has disease, can get away with only O(log n) tests instead of n

If k have disease, need O(k log n) tests

0 0 0 0 0 1 0 0

Combinatorial Group Testing

For worst-case inputs still need Ω(n) tests:

Reduces to search if all but one have disease

Every subset tests positive, except singleton set with the non-sick person

1

1 1 1 1 1 0 1 1

Combinatorial Group Testing

Formalization: Hidden string x in $\{0,1\}^n$

Goal: Learn x

Queries: Given a subset S of $\{0,1\}^n$, can learn

$$x_S = \bigvee_{i \in S} x_i \quad .$$

Classical complexity: $\Theta(n)$ for worst case x

(but $O(k \log n)$ for k-sparse x)

Combinatorial Group Testing

What if we could make the OR subset queries to hidden string x in superposition?

Classical: $\Theta(n)$ for generic strings x

Belovs '13: $\Theta(n^{1/2})$ for generic strings x

(also prior work by Ambainis-Montanaro '12)

Combinatorial Group Testing

What if we could make the OR subset queries to hidden string x in superposition?

Classical: Θ(n) for generic string

Belovs '

generic

Belovs' proof: Adversary magic

that we allow A of size less than k. In this section, we prove the following result:

Theorem 3. *The quantum query complexity of the combinatorial group testing problem is* $\Theta(\sqrt{k})$.

The lower bound can be proved by a reduction from the unordered search, refer to [4] for more detail. Here we prove the upper bound. We do so by constructing a feasible solution to (3). This is done in two steps: First, we define rank-1 matrices $Y_S(p)$, and then build the matrices X_S from them.

Let P be the binomial probability distribution on $[n]$ with probability p. Recall that it is a probability distribution on the subsets of $[n]$, where each element of $[n]$ is included into the subset independently with probability p. By $P(S)$, we denote the probability of sampling S from P: $P(S) = p^{|S|}(1-p)^{n-|S|}$. Finally, let $\triangle$ denote the symmetric difference of sets.

We define $Y(p) = (Y_S(p))_{S\subseteq[n]}$ by

$$Y_S(p) = \frac{P(S)}{2p}\,\psi\psi^* \succeq 0,$$

where

$$\psi[A] = \frac{1}{(1-p)^{|A|/2}} \times \begin{cases} \sqrt[4]{kp/(1-p)}, & \text{if } |A\cap S| = 0; \\ \sqrt[4]{(1-p)/(kp)}, & \text{if } |A\cap S| = 1; \\ 0, & \text{otherwise;} \end{cases}$$

for all $A \in \mathcal{C}$. In this notation,

$$\begin{aligned}\sum_{S\subseteq[n]} Y_S(p)[A,A] &= \frac{1}{2p\,(1-p)^{|A|}}\left(\Pr_{S\sim P}\big[|S\cap A| = 0\big]\sqrt{\frac{kp}{1-p}} + \Pr_{S\sim P}\big[|S\cap A| = 1\big]\sqrt{\frac{1-p}{kp}}\right) \\ &= \frac{1}{2p\,(1-p)^{|A|}}\left((1-p)^{|A|}\sqrt{\frac{kp}{1-p}} + |A|p\,(1-p)^{|A|-1}\sqrt{\frac{1-p}{kp}}\right) \le \sqrt{\frac{k}{p\,(1-p)}}\,.\end{aligned}$$

Now we fix two distinct elements A, B of $\mathcal{C}$. An element A is used in Y_S only if $|S \cap A| \le 1$. Thus, we are only interested in $S \subseteq [n]$ such that $|A\cap S| + |B\cap S| = 1$. Thus,

$$\begin{aligned}\sum_{S:\, f_A(S)\ne f_B(S)} Y_S(p)[A,B] &= \frac{\Pr_{S\sim P}\big[|A\cap S| + |B\cap S| = 1\big]}{2p\,(1-p)^{(|A|+|B|)/2}} \\ &= \frac{|A\triangle B|\,p\,(1-p)^{|A\cup B|-1}}{2p\,(1-p)^{(|A|+|B|)/2}} = \frac{|A\triangle B|}{2}(1-p)^{\frac{|A\triangle B|}{2}-1}\,.\end{aligned}$$

Now, for each $S \subseteq [n]$, let

$$X_S = \int_0^1 Y_S(p)\,\mathrm{d}p\,.$$

First, each X_S is positive semi-definite, because positive semi-definite matrices form a convex cone. Next, for any $A \in \mathcal{C}$:

$$\sum_{S\subseteq[n]} X_S[A,A] \le \sqrt{k}\int_0^1 \frac{\mathrm{d}p}{\sqrt{p\,(1-p)}} = \pi\sqrt{k}\,.$$

And finally, for all $A \ne B$ in $\mathcal{C}$:

$$\sum_{S:\, f_A(S)\ne f_B(S)} X_S[A,B] = \frac{|A\triangle B|}{2}\int_0^1 (1-p)^{\frac{|A\triangle B|}{2}-1}\,\mathrm{d}p = 1.$$

6

Combinatorial Group Testing

What if we could make the OR subset queries to hidden string x in superposition?

Classical: Θ(n) for generic string

Belovs '

generic

Belovs' proof: Adversary magic

that we allow A of size less than k. In this section, we prove the following result:

Theorem 3. *The quantum query complexity of the combinatorial group testing problem is* $\Theta(\sqrt{k})$.

The lower bound can be proved by a reduction from the unordered search, refer to [4] for more detail. Here we prove the upper bound. We do so by constructing a feasible solution to (3). This is done in two steps: First, we define rank-1 matrices $Y_S(p)$, and then build the matrices X_S from them.

Let P be the binomial probability distribution on $[n]$ with probability p. Recall that it is a probability distribution on the subsets of $[n]$, where each element of $[n]$ is included into the subset independently with probability p. By $P(S)$, we denote the probability of sampling S from P: $P(S) = p^{|S|}(1-p)^{n-|S|}$. Finally, let Δ denote the symmetric difference of sets.

We define $Y(p) = (Y_S(p))_{S\subseteq[n]}$ by

$$Y_S(p) = \frac{P(S)}{2p}\,\psi\psi^* \succeq 0,$$

where

$$\psi[A] = \frac{1}{(1-p)^{|A|/2}} \times \begin{cases} \sqrt[4]{kp/(1-p)}, & \text{if } |A\cap S| = 0; \\ \sqrt[4]{(1-p)/(kp)}, & \text{if } |A\cap S| = 1; \\ 0, & \text{otherwise;} \end{cases}$$

for all $A \in \mathcal{C}$. In this notation,

$$\begin{aligned} \sum_{S\subseteq[n]} Y_S(p)[A,A] &= \frac{1}{2p\,(1-p)^{|A|}}\left(\Pr_{S\sim P}\big[|S\cap A| = 0\big]\sqrt{\frac{kp}{1-p}} + \Pr_{S\sim P}\big[|S\cap A| = 1\big]\sqrt{\frac{1-p}{kp}}\right) \\ &= \frac{1}{2p\,(1-p)^{|A|}}\left((1-p)^{|A|}\sqrt{\frac{kp}{1-p}} + |A|p\,(1-p)^{|A|-1}\sqrt{\frac{1-p}{kp}}\right) \le \sqrt{\frac{k}{p\,(1-p)}}\,. \end{aligned}$$

Now we fix two distinct elements A, B of $\mathcal{C}$. An element A is used in Y_S only if $|S\cap A| \le 1$. Thus, we are only interested in $S \subseteq [n]$ such that $|A\cap S| + |B\cap S| = 1$. Thus,

$$\begin{aligned} \sum_{S:\, f_A(S)\ne f_B(S)} Y_S(p)[A,B] &= \frac{\Pr_{S\sim P}\big[|A\cap S| + |B\cap S| = 1\big]}{2p\,(1-p)^{(|A|+|B|)/2}} \\ &= \frac{|A\,\Delta\,B|\,p\,(1-p)^{|A\cup B|-1}}{2p\,(1-p)^{(|A|+|B|)/2}} = \frac{|A\,\Delta\,B|}{2}(1-p)^{\frac{|A\Delta B|}{2}-1}\,. \end{aligned}$$

Now, for each $S \subseteq [n]$, let

$$X_S = \int_0^1 Y_S(p)\,\mathrm{d}p\,.$$

First, each X_S is positive semi-definite, because positive semi-definite matrices form a convex cone. Next, for any $A \in \mathcal{C}$:

$$\sum_{S\subseteq[n]} X_S[A,A] \le \sqrt{k}\int_0^1 \frac{\mathrm{d}p}{\sqrt{p\,(1-p)}} = \pi\sqrt{k}\,.$$

And finally, for all $A \ne B$ in $\mathcal{C}$:

$$\sum_{S:\, f_A(S)\ne f_B(S)} X_S[A,B] = \frac{|A\,\Delta\,B|}{2}\int_0^1 (1-p)^{\frac{|A\Delta B|}{2}-1}\,\mathrm{d}p = 1.$$

6

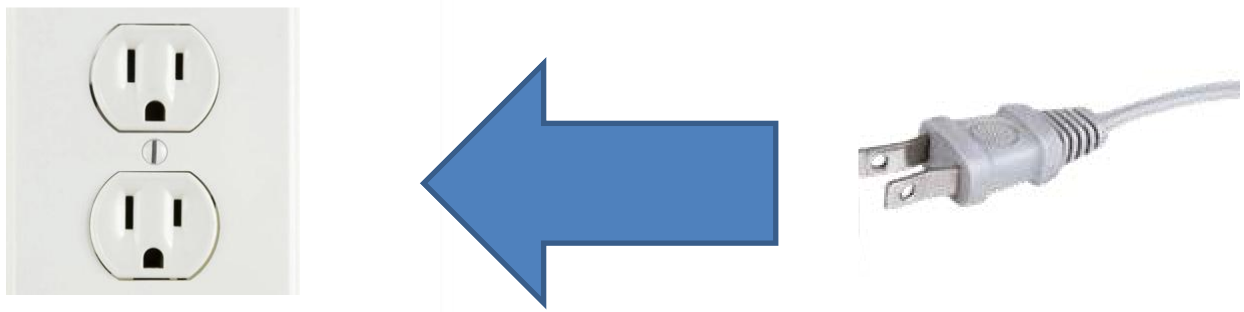
Proof of Main Result

Goal: lower bound $\widetilde{\deg}(\mathrm{OR}_n \circ f)$

Suppose $\widetilde{\deg}(\mathrm{OR}_n \circ f)$ =T, where T too small, and let p be corresponding polynomial

Basic idea: Compose p with Belovs' algorithm to get a ``too good to be true" polynomial for a harder problem

Proof of Main Result



Belovs polynomial q
Input: ORs of subsets
Cost $n^{1/2}$

p for $\widetilde{\deg}(\mathrm{OR}_n \circ f)$
Cost T

Proof of Main Result

Get a polynomial of degree $Tn^{1/2}$ which computes string of f's and hence XOR_n f

BUT $T\, n^{1/2} >= \deg(XOR_n\ f) >= \Omega(n \deg(f))$ [Sherstov '12]

Proof of Main Result

$$T = \widetilde{\deg}(\mathrm{OR}_n \circ f) = \Omega(n^{1/2} \deg(f))$$

Get … which

com … XOR_n f

BUT $T\, n^{1/2} >= \deg(XOR_n\ f) >= \Omega(n \deg(f))$

[Sherstov '12]

Proof of Main Result

Summary: If there were a better polynomial for

$$\widetilde{\deg}(\mathrm{OR}_n \circ f)$$

Then combining it with Belov's algorithm, would get a too-good-to-be-true polynomial for

$$\widetilde{\deg}(\mathrm{XOR}_n \circ f)$$

Which we know must be very high

Proof of Main Result

Belovs

p for $\widetilde{\deg}(\mathrm{OR}_n \circ f)$

Proof of Main Result

Belovs

p for $\widetilde{\deg}(\mathrm{OR}_n \circ f)$

Robustification: making polynomials robust to receiving "approximately boolean" inputs

[Sherstov '13]

Proof of Main Result

Communication results: pass too-good to be true approx rank decomp of OR_nF through the Belovs polynomial using Hadamard product …. make too-good-to-be-true approx rank decomposition of XOR_n

Where can I read about this!?

Cornell University Library

We gratefully acknowledge support from
the Simons Foundation
and member institutions

arXiv.org > search

Search or Article ID | All papers

(Help | Advanced search)

Search arXiv.org

Search gave no matches

No matches were found for your search: all:(kothari AND (garg AND (bouland AND (ben AND david))))

Please try again.

Author/title/abstract search

Select subject areas to restrict search (default is to search all subject areas)

☐ Computer Science ☐ Economics ☐ Electrical Engineering and Systems Science ☐ Mathematics

☐ Physics [archive: All ▾] ☐ Quantitative Biology ☐ Quantitative Finance ☐ Statistics

Select years to search (default is to search all years)

☐ Past year or the year ____ or the years from ____ to ____

Forthcoming Generalization

For all symmetric s,

$$\widetilde{\deg}(s \circ f) = \ \Omega(\widetilde{\deg}(f)\,\widetilde{\deg}(s)/\log(n))$$

Requires opening black boxes of Belovs algorithm and Sherstov robustification

Open Problems

- Is $\widetilde{\deg}(f \circ g) = \Omega(\widetilde{\deg}(f)\,\widetilde{\deg}(g))$?

- Can one construct a dual witness for our bound on $\widetilde{\deg}(\mathsf{OR} \circ f)$?

- Can we use f-queries instead of OR-queries to learn x efficiently, following Belovs?

Thanks for your attention!

Questions?