Sculpting Quantum Speedups

SCOTT AARONSON SHALEV BEN-DAVID

Query Complexity

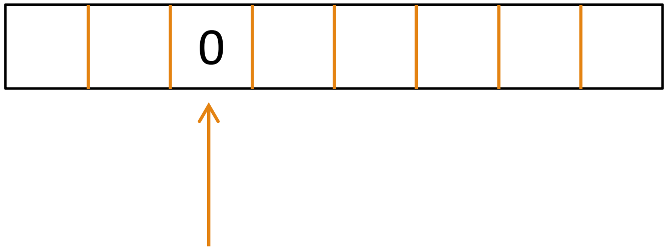
There is a known function $f:\{0,1\}^n \to \{0,1\}$

Given oracle access to a string x in $\{0,1\}^n$, compute f(x)

Cost: number of queries to the bits of x

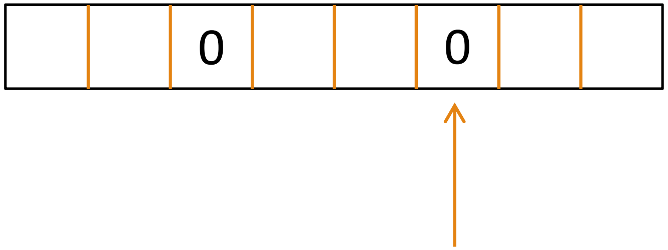
Query Complexity

- f = OR



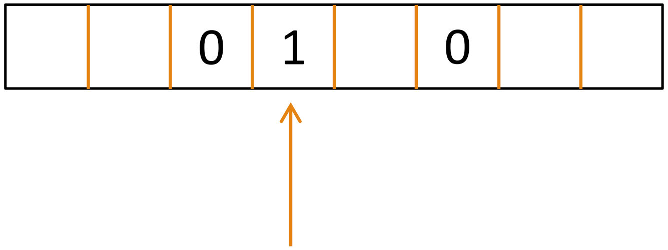
Query Complexity

- f = OR



Query Complexity

- f = OR



Query Complexity

The complexity of f is the worst-case number of queries for the best algorithm

- D(f) = deterministic algorithms
- $R_0(f)$ = zero-error randomized algorithms (Las Vegas)
- R(f) = bounded-error randomized algorithms (Monte Carlo)
- Q(f) = bounded-error quantum algorithms

- $Q(f) \leq R(f) \leq R_0(f) \leq D(f)$

Previously, on *QUANTUM QUERY COMPLEXITY*

Beals, Buhrman, Cleve, Mosca, de Wolf ('98):

- All these query measures are polynomially related for total functions

Ambainis, Balodis, Belovs, Lee, Santha, Smotrovs (2015):

- Some surprising polynomial separations for total functions

Aaronson, B., Kothari (2015):

- Even more quibbling over polynomial factors

Real complexity theorists don't care about polynomial factors

Can we get exponential speedups?

Beals, Buhrman, Cleve, Mosca, de Wolf ('98):

- Not for total functions

Simon ('94), Shor ('94):

- Exponential quantum speedups are possible if there is a promise on the input
- Example promise: the input string is periodic

When are exponential quantum speedups possible?

Again:

- for total functions, exponential speedups are not possible
- If there is a promise, exponential speedups are possible

But when? What kinds of functions? What kinds of promises?

Given a total function f, is there a promise such that there is an exponential quantum speedup when f is restricted to the promise?

Sculpting problem

Sculpting Question

Given a total function f, is there a promise such that there is an exponential quantum speedup when f is restricted to it?

In other words: there is probably no quantum speedup for 3-SAT. But is there a set of instances of 3-SAT that are particularly quantum-friendly?

Want to say: " There is an exponential quantum speedup for 3-SAT* "

*If we restrict the instances to a sufficiently artificial set

We give a characterization of when such speedups are possible

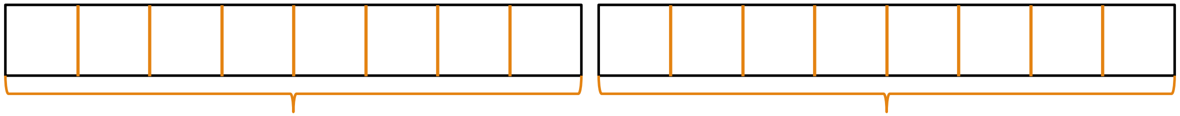
Example: OR

Can we restrict OR to a promise such that on inputs from that promise, there is an exponential quantum speedup?

Aaronson '04: No. Quadratic speedup on all promises

Example: parity

Can we restrict parity to a promise such that on inputs from that promise, there is an exponential quantum speedup?



Simon's problem

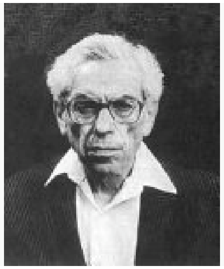
Promise: input here makes the total parity equal to the value of Simon's problem

H Index

Used to measure research output

Maximum number k such that you have at least k publications with at least k citations each

H Index variant: maximum number k such that you have at least 2^k publications with at least k citations each



Paul Erdős

Follow

Mathematics

number theory, combinatorics, probability, set theory, mathematical analysis

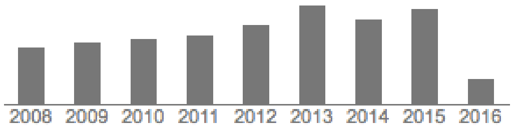
No verified email - Homepage

Title 1–20	Cited by	Year
On random graphs I. P ERDdS, A R&WI Publ. Math. Debrecen 6, 290-297	11979 *	1959
On the evolution of random graphs P Erdos, A Rényi Bull. Inst. Internat. Statist 38 (4), 343-347	~~7475~~	1961
On random graphs P Erdős, A Rényi Publicationes Mathematicae Debrecen 6, 290-297	~~6819~~ *	1959
A combinatorial problem in geometry P Erdös, G Szekeres Compositio Mathematica 2, 463-470	1209	1935

Google Scholar

Get my own profile

Citation indices	All	Since 2011
Citations	[illegible]	21453
h-index	108	59
i10-index	[illegible]	328



Co-authors View all...

Ralph Faudree

András Sárközy

Janos Pach

Laszlo Lovasz

∧

OR_n

Publications (inputs)	(value)	Citations (certificates)
00…0000	0	n
00…0001	1	1
00…0010	1	1
00…0011	1	1
00…0100	1	1
00…0101	1	1
00…0110	1	1
…	…	…
11…1111	1	1

2^n

Most cited (certificate complexity)	n
h-index	1

$\oplus$ PARITY_n

Publications (inputs)	(value)	Citations (certificates)
00…0000	0	n
00…0001	1	n
00…0010	1	n
00…0011	0	n
00…0100	1	n
00…0101	0	n
00…0110	0	n
…	…	…
11…1111	?	n

2^n

Most cited (certificate complexity)	n
h-index	n

Characterization Result

$H(C_f)$ is the H-index of the vector of certificate sizes for f

"Sculpting is possible iff $H(C_f)$ is large"

$$\forall_f\ \exists_P\ \ R(f|_P) = \Omega\left(\frac{H(C_f)^{1/6}}{\log^3 n}\right), \quad Q(f|_P) = O(\log^2 H(C_f))$$

$$\forall_f\ \forall_P\ \ R(f|_P) = O(Q(f|_P)^2 H(C_f)^2)$$

Other sculpting results

D vs. R_0: same $H(C_f)$ characterization (somewhat better bounds)

R_0 vs. R: it is ***always*** possible to sculpt

Intuition: OR function

- Is there a promise we can place on OR to get an R_0 speedup vs. D?
- Is there a promise we can place on OR to get an R speedup vs. R_0?

Why Certificates?

Actually, the sculpting construction uses $H(bs_f)$ instead of $H(C_f)$

The two are quadratically related

Intuitively, these measure whether the function is difficult in only one spot (like OR), or everywhere (like parity)

Proof sketch: sculpting impossibility

Want to show $R(f|_P)=O(Q(f|_P)^2H(C_f)^2)$

"If there are few large certificates, R and Q are quadratically related"

Step 1: use the standard $D \leq C^2$ algorithm to kill small certificates

we have few 1-inputs left

Step 2: show that $R \leq Q^2$ on any function with few 1-inputs

Side Result

$$Q(f) = \Omega\left(\frac{\sqrt{D(f)}}{\log|Dom(f)|}\right)$$

Example: OR

Proof idea: generalize RC≤QC^2, and show C=RC when the domain is small

Proof sketch: sculpting existence

Given f, want P such that

$$R(f|_P) \geq \text{poly}(H(C_f)), \quad Q(f|_P) \leq \text{polylog } H(C_f)$$

"If there are many hard inputs, there is a promise P with exponential quantum speedup for $f|_P$"

Step 1: replace $H(C_f)$ with $H(bs_f)$

Step 2: Sauer's lemma

Step 3: reduce to communication

Step 2: Sauer's lemma

For any $S \subseteq \{0,1\}^n$, there is a set of bits of size ~ log |S|/log n with all possible actions

001000
101111
110001
101110
101010

Step 2: Sauer's lemma

Hard inputs look like:

x	s(x)

The x part can be any string

Since there are many hard inputs, the x part is large

We define a promise problem on the x part that has a quantum speedup

What if the s(x) part lets the classical algorithm cheat?

Is it possible for s(x) to contain the answers to all possible problems that give a quantum speedup?

Step 3: reducing to communication

Hard inputs look like:

x	s(x)

Take a communication task that can be solved quantumly but not randomly (Klartag and Regev 2011)

Give x to Bob

Give a different string y to Alice so that (x,y) satisfies the promise

Consider strategies in which Alice sends Bob randomized queries to x or s(x) (log n bits each)

This strategy must fail for some y; this y defines the desired function

Sculpting in the Turing machine model

In the Turing machine model, we say a language is sculptable if it can be restricted to a promise problem inside promiseBQP but outside promiseBPP

To be sculptable, a language must be outside BPP

Paddable languages

A language is paddable if it's possible to add irrelevant junk to its strings

Formally: L is paddable if there exists poly-time invertible f(x,y) such that

x in L iff f(x,y) in L

Example: 3-SAT

If promiseBQP is hard on average for P/poly, every paddable language outside BPP is sculptable

Idea: use the promise to ecode the hard problem in promiseBQP inside the padding

Sculpting all languages?

A language is called BPP-immune if no infinite subset of it is in BPP

A language is called BPP-bi-immune if it is BPP-immune and its complement is also BPP-immune

Theorem: if there is a BPP-bi-immune language in BQP, then all languages outside BPP can be sculpted

Idea: If H is BPP-bi-immune and we want to sculpt L, consider the intersection of L with H and with the complement of H

Conclusions

A full characterization of sculpting: which problems can be restricted to a promise that gives rise to an exponential quantum speedup

“Quantum computers give an exponential speedup for *some* 3-SAT instances”

✓ **Complexity Theorist Approved**

Most Boolean functions are sculptable

“Quantum speedups are not about the function, they are about the promise”

Next question: which *promises* give rise to exponential speedups?


THE END