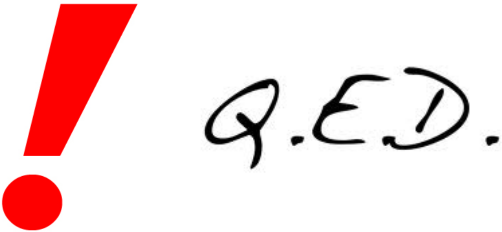
Quantum Proofs for Classical Theorems

Andrew Drucker

Feb. 22, 2011

- Based on a survey co-written with Ronald de Wolf (CWI, Netherlands).

Surprising proof methods



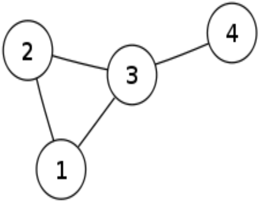
- Often “import” unexpected objects or concepts.

Surprising proof methods

- Celebrated example: *the probabilistic method* (Erdős et al.)

Example: maximum edge cut

- Given: an undirected graph $G = (V, E)$.



Claim

There exists a partition $V = (A, B)$ *such that*

$$|E(A, B)| \geq |E|/2 \ .$$

Example: maximum edge cut

Claim

There exists a partition $V = (A, B)$ *such that*

$$|E(A, B)| \geq |E|/2 \ .$$

Proof: Send each vertex to A or B *randomly*!
Each $e \in E$ lands in $E(A, B)$ with probability $1/2$, so

$$\mathbb{E}[|E(A, B)|] = |E|/2 \ .$$

$\square$

An objection

- Do we really need randomness here?
- "Just" a counting argument.

However...

- Language of probability theory brings *intuitions and tools*:
- Concentration of measure; martingales; Lovasz local lemma; ...

A 'quantum method'?

- Past 10+ years: quantum concepts and tools used as a proof-tool for *classical* math and CS.
- Used either directly, or as inspiration.
  [DdW] surveys many examples. (No quantum background needed!)

A ‘quantum method’?

- Aren’t quantum arguments ‘just’ linear algebra (+ matrix analysis, etc.)?
- Yes, *but*...
- Quantum concepts and intuitions seem to help!

A ‘quantum method’?

- Area is still young...
- In most cases, alternate ‘classical proofs’ are available.
- Room for growth and new ideas!

What is quantum?

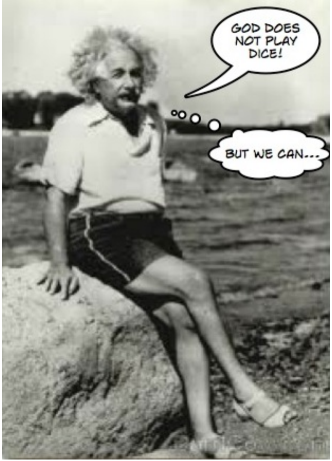
- Our perspective: QM is a *framework* for describing systems and changes they undergo.
- A *strange, distinctive* framework... that's the point!
- Not a full physical theory!

What is quantum?

- Similar situation in classical theoretical CS—bits, logic, TMs, etc.:
- Studied *independently* of its physical realization.
- Most of the quantum systems we'll describe cannot yet be realized!

What is quantum?

- Can use quantum proof tools, even if QM turns out to be wrong!



Quantum basics

- A **quantum state** (for us) is just a *unit vector*

$$|\psi\rangle \in \mathbb{C}^d$$

- (we only use *pure*, finite-dimensional states)
- "m-qubit state": $d = 2^m$, basis vectors $|x\rangle$, $x \in \{0,1\}^m$:

$$|\psi\rangle = \sum_x \alpha_x |x\rangle$$

Quantum basics

- Product states:

$$|\alpha\rangle \in \mathbb{C}^{d}, |\beta\rangle \in \mathbb{C}^{d'} \quad \Rightarrow \quad |\alpha\rangle|\beta\rangle \in \mathbb{C}^{d \cdot d'} \ :$$
$$(|\alpha\rangle|\beta\rangle)_{i,j} = \alpha_i \beta_j$$

- "independent subsystems"

(Discrete-time) quantum evolution

Two things we can do with a quantum state:

- Transform it “unitarily”
- Measure it

Unitary transformations

$$|\psi\rangle \longmapsto U|\psi\rangle \ ,$$

where $U \in \mathbb{C}^{d \times d}$ is **unitary** (norm-preserving)

Measurements

- **Projective measurement** M defined by *orthogonal projectors* $P_1, \ldots, P_k \in \mathbb{C}^{d \times d}$, with

$$\sum_i P_i = I_{d \times d}$$

- Applied to $|\psi\rangle$: observe outcome $i \in [k]$ with probability $p_i = ||P_i|\psi\rangle||^2$.
- $|||\psi\rangle|| = 1$, so probs. sum to 1
- After outcome i, state "collapses" to $\frac{P_i|\psi\rangle}{||P_i|\psi\rangle||}$.

First quantum insight

- Quantum states can't store too much *accessible* information.

Theorem (Holevo, CDNT—informal)

Suppose Alice wants to send Bob n bits of information. Then the two parties must exchange $\Omega(n)$ qubits of communication.

- (even with prior entanglement)

Application: Communication Complexity of Inner Product

Alice: x **Bob:** y $(|x| = |y| = n)$

Want to compute:

$$IP(x, y) = x \cdot y \mod 2$$

- Known that $\Omega(n)$ (qu)bits of communication are necessary
- (even with prior entanglement)

Application: Communication Complexity of Inner Product

- Result is nontrivial even for *classical* randomized case ("discrepancy method").
- Quantum techniques give a novel, elegant proof. **[Cleve, van Dam, Nielsen, Tapp]**

Proof idea

- Say $\mathcal{P}$ is a c-bit classical protocol computing IP (*exactly*, for simplicity). WTS $c = \Omega(n)$.
- **First step:** Convert $\mathcal{P}$ to a **clean** *quantum* protocol
- *Clean protocol:* of form

$$|x\rangle|y\rangle \quad \longmapsto^{\mathcal{P}} \quad |x\rangle(-1)^{x\cdot y}|y\rangle$$

Proof idea

- *Clean protocol:* of form

$$|x\rangle|y\rangle \quad \longmapsto^{\mathcal{P}} \quad |x\rangle(-1)^{x\cdot y}|y\rangle$$

- Here's how:

$$|x\rangle|y\rangle \longmapsto^{\mathcal{P}} |\Phi_{x,y}\rangle$$

$$\longmapsto^{(Bob)} (-1)^{x\cdot y}|\Phi_{x,y}\rangle$$

$$\longmapsto^{\mathcal{P}^{-1}} (-1)^{x\cdot y}|x\rangle|y\rangle$$

Proof idea

- $\mathcal{P}$ communicates c bits $\implies$ $\mathcal{P}'$ communicates $2c$ qubits.

Proof idea

- **Second step:** Run clean protocol *in superposition* over all y:
- Start state: $|x\rangle\left(\frac{1}{\sqrt{2^n}}\sum_y |y\rangle\right)$
  $\longmapsto^{\mathcal{P}'} |x\rangle\left(\frac{1}{\sqrt{2^n}}\sum_y (-1)^{x\cdot y}|y\rangle\right)$

Proof idea

- **Third step:** Bob performs *Hadamard transformation*:

$$|x\rangle \left(\frac{1}{\sqrt{2^n}} \sum_y (-1)^{x \cdot y} |y\rangle \right) \longmapsto^{H^{\otimes n}} |x\rangle|x\rangle$$

- **SO:** Alice transmits x to Bob in $2c$ qubits!
- Holevo $\implies 2c = \Omega(n)$.

Application: Coding theory lower bounds

- *Locally decodable codes:*

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

- Want to recover any desired bit x_i, using $q \ll n$ queries to $C(x)$ (nonadaptive)
- Tolerate a .01 fraction of errors in transmitted codeword $\tilde{C}(x)$....
- Still succeed with $2/3$ probability (for any i)
- How large must codelength m be?

Application: Coding theory lower bounds

- **Open:** Achieve $m = \mathrm{poly}(n)$ for some constant $q = O(1)$?
- $q = 3$: $m = 2^{n^{o(1)}}$ is possible **[Yekhanin, Efremenko]**
- **[Kerenedis, de Wolf]**: if $q = 2$, need $m = 2^{\Omega(n)}$
- Proof in **[KdW]** is quantum
- Later classical proof **[Ben-Aroya, Regev, de Wolf]**; modeled on quantum

Application: Coding theory lower bounds

- **Proof idea:** Convert C into *quantum encoding*:

$$x \longmapsto |\phi_x\rangle := \sum_{j=1}^{m} (-1)^{C(x)_j} |j\rangle$$

- Only $\log m$ qubits!
- **[KdW]**: If $q = 2$, $\{|\phi_x\rangle\}$ is a **quantum random access code (QRAC)** for n bits
- (can recover desired x_i with prob. $\frac{1}{2} + \Omega(1)$ over random x)
- Variant of Holevo's theorem for QRACs **[Nayak]** implies $\log m = \Omega(n)$.

Second quantum insight

- Quantum algorithms useful to *construct polynomials*.

Quantum query algorithms

Unknown input $y \in \{0,1\}^n$; want to compute some function $f(y)$.

$$\text{basis state: } \underbrace{|i,b\rangle}_{i\in[n],b\in\{0,1\}}^{\text{index register}} \quad \underbrace{|z\rangle}_{\text{aux. register}}$$

- **Query step:** $|\psi\rangle \longmapsto O_y|\psi\rangle$

$$|i,b\rangle|z\rangle \overset{O_y}{\longmapsto} |i, b\oplus y_i\rangle|z\rangle$$

- (Indirect access to input y)

Quantum query algorithms

- **Unitary step:** $|\psi\rangle \to U|\psi\rangle$
- (Independent of y)

Quantum query algorithms

T**-query quantum algorithm:**

$$|\psi_0\rangle \longmapsto U_T O_y U_{T-1} O_y \ldots U_1 O_y U_0 |\psi_0\rangle$$

- Final measurement step, yields a value $v \in \mathbb{R}$

The polynomial connection

T-query quantum algorithm $\mathcal{A}$:

$$|\psi_0\rangle \longmapsto U_T O_y U_{T-1} O_y \dots U_1 O_y U_0 |\psi_0\rangle$$

Theorem (BBCMdW)

For any $v \in \mathbb{R}$, the quantity

$$p_v(y) = \Pr_{\mathcal{A}}[\mathcal{A}(y) \textit{ outputs } v]$$

is a degree-$2T$ multilinear polynomial in $y_1, \dots, y_n$.

The polynomial connection

Theorem (BBCMdW)

For any $v \in \mathbb{R}$, *the quantity*

$$p_v(y) = \Pr_{\mathcal{A}}[\mathcal{A}(y) \textit{ outputs } v]$$

is a degree-$2T$ *multilinear polynomial in* $y_1, \ldots, y_n$.

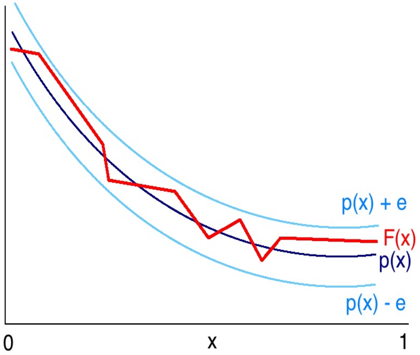
- Often used to prove *lower bounds* on the quantum query complexity of specific functions, via lower bounds on polynomial degree...
- But here we use it to build explicit polynomials.

Application: uniform approximation

Theorem (Weierstrass, 1885)

Say $F : [0,1] \to \mathbb{R}$ is continuous. Given $\varepsilon > 0$, there exists a polynomial $p(x)$ such that

$$\sup_{x \in [0,1]} |p(x) - F(x)| \leq \varepsilon \ .$$



Application: uniform approximation

Theorem (Weierstrass, 1885)

Say $F : [0, 1] \to \mathbb{R}$ is continuous. Given $\varepsilon > 0$, there exists a polynomial $p(x)$ such that

$$\sup_{x \in [0,1]} |p(x) - F(x)| \leq \varepsilon \ .$$

- Fix F; suppose we require $\deg(p) \leq n$. How low can ε be?

Bernstein's proof

- Bernstein, $\sim$1910: proof of W.'s Theorem by "probabilistic method"!
- Gives bounds on error of degree-n polynomial approximations.

Bernstein's proof

- Fix F, n, and $x \in [0, 1]$.
- **Experiment** $\mathcal{A}(x)$:

-Flip n coins $c_1, \ldots, c_n$ with bias x;

-Let $k =$ number of 1s seen; **-Output** $F\left(\frac{k}{n}\right)$.

- **Idea:** $\frac{k}{n} \approx x \pm \frac{1}{\sqrt{n}}$, so

$$\mathbb{E}_{c_1,\ldots,c_n}[\mathcal{A}(x)] \approx F(x \pm 1/\sqrt{n}) \ .$$

Bernstein's proof

- $\sup_{x \in [0,1]} |\mathbb{E}[\mathcal{A}(x)] - F(x)| \leq$

  $O($max fluctuation of F on any interval of length $1/\sqrt{n})$)

- $\to 0$ as $n \to \infty$
- **Observation:** $\mathbb{E}[\mathcal{A}(x)]$ is a *degree-n polynomial* in x!
- Because, e.g., $\Pr[(c_1, \ldots, c_n) = \text{all-zero}] = (1 - x)^n$

Jackson's theorem

- Jackson, also $\sim$1910: proof of Weierstrass's Theorem by trigonometric tools
- Better error bounds for fixed n:

Theorem (Jackson)

If $F : [0,1] \to \mathbb{R}$ is continuous, there exists a degree-n polynomial J_n such that

$$\sup_{x \in [0,1]} |J_n(x) - F(x)| \leq$$

$$O(\textit{max fluctuation of } F \textit{ on any interval of length } 1/n)$$

Jackson's theorem—the quantum way

- **[D., de Wolf]**: Prove Jackson's Theorem, using Bernstein's elegant technique.
- **Idea:** Replace the classical algorithm $\mathcal{A}$ with a quantum algorithm!

Quantum estimation

Claim

There is a quantum algorithm **QEst**$(c_1, \ldots, c_N)$*, which:*

- *makes* $\sqrt{N}$ *quantum queries to* $(c_1, \ldots, c_N)$*;*
- *outputs an estimate* $\tilde{x}$ *satisfying*

$$\mathbb{E}\left[\left|\tilde{x} - \frac{c_1 + \ldots + c_N}{N}\right|\right] = O\left(\frac{1}{\sqrt{N}}\right).$$

- Proof idea: Apply a known quantum estimation algorithm **[Brassard, Høyer, Mosca, Tapp]** 3 times; take the median value.

Jackson's theorem—the quantum way

- Fix F, n, and $x \in [0, 1]$.
- **Experiment** $\mathcal{A}'(x)$:

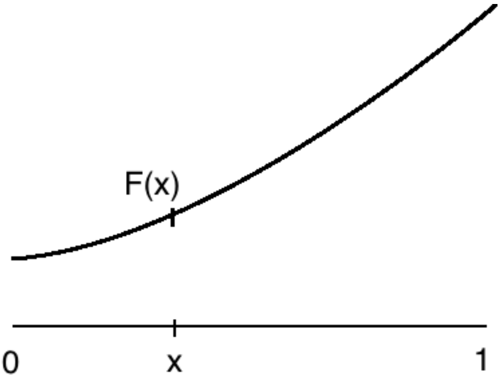
-Flip $N = n^2$ coins $c_1, \ldots, c_N$ with bias x;

-Let $\tilde{x} = \mathbf{QEst}(\overline{c})$;

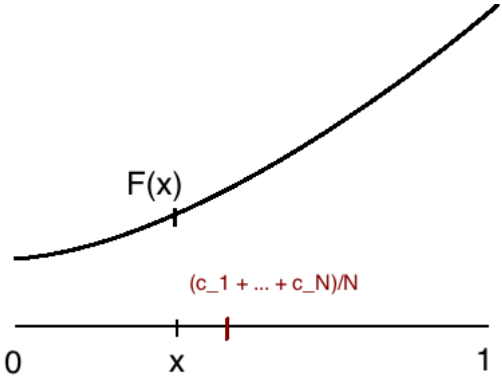
-**Output** $F(\tilde{x})$.

- Let $J_n(x) = \mathbb{E}[\mathcal{A}'(x)] = \mathbb{E}[F(\tilde{x})]$.

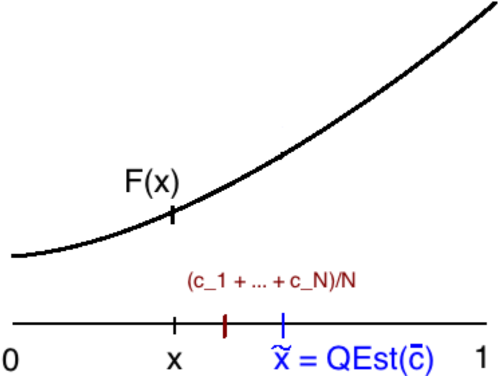
Jackson's theorem—the quantum way



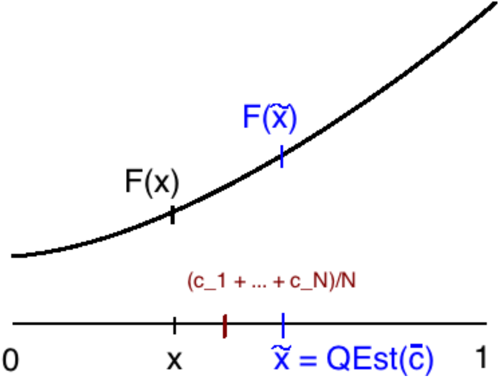
Jackson's theorem—the quantum way



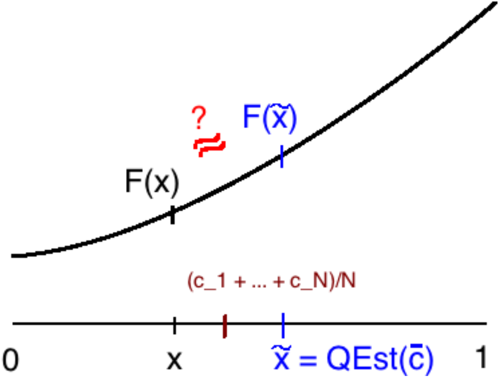
Jackson's theorem—the quantum way



Jackson's theorem—the quantum way



Jackson's theorem—the quantum way



Jackson's theorem—the quantum way

Recall $N = n^2$.

Analysis idea:

$$\frac{c_1 + \ldots + c_N}{N} \approx x \;\pm\; \frac{1}{n} \qquad \text{(by Chernoff bounds);}$$

$$\tilde{x} \approx \frac{c_1 + \ldots + c_N}{N} \;\pm\; \frac{1}{n} \qquad \text{(by properties of } \mathbf{QEst}(\overline{c})\text{);}$$

So:

$$J_n(x) = \mathbb{E}[F(\tilde{x})] \approx F(x \pm 1/n \pm 1/n) \;,$$

$$\text{i.e., } |J_n(x) - F(x)| \leq$$

$$O(\text{max fluctuation of } F \text{ on an interval of length } 1/n) \;.$$

Jackson's theorem—the quantum way

- So, J_n is the desired approximation to F.
- **Claim:** it's a polynomial in x of degree $2n$.
- Easy proof, using **[BBCMdW]**:

$$J_n(x) = \mathbb{E}[F(\tilde{x})] = \mathbb{E}_{\overline{c}}[\mathbb{E}[F(\tilde{x})|\overline{c}]]$$

$$= \mathbb{E}[(\text{degree-}2n \text{ poly in } c_1, \ldots, c_n)] \quad (\text{by } \textbf{[BBCMdW]})$$

$$= (\text{degree-}2n \text{ poly in } x)$$

Application: robust polynomials

- **Noisy queries:** each query gives wrong answer with some small probability $\varepsilon_i \leq 1/4$.
- (Models use of probabilistic subroutines)

Application: robust polynomials

Classical query algorithms: Require $\Omega(n \log n)$ noisy queries to compute $y_1 \oplus \ldots \oplus y_n$. **[Feige, Raghavan, Peleg, Upfal]**

Theorem (Buhrman, Newman, Röhrig, de Wolf)

Any *Boolean function can be computed with bounded error using* $O(n)$ *noisy quantum queries.*

Proof Idea: Maintain guesses of $y_1, \ldots, y_n$;
repeatedly use variant of Grover search to reduce number of errors.

Application: robust polynomials

- Using their result, **[BNRdW]** give a new kind of polynomial approximations of Boolean functions.

Application: robust polynomials

- Let $p : \mathbb{R}^n \to \mathbb{R}$ be a polynomial, f a Boolean function. p **robustly approximates** f if for all $y \in \{0,1\}^n$, and all $z \in [0,1]^n$,

$$||z - y||_\infty \le 1/4 \quad \Rightarrow \quad |p(z) - f(y)| \le 1/4 \ .$$

Theorem (BNRdW)

For any Boolean function f, there is a polynomial p of degree $O(n)$ that robustly approximates f.

Third quantum insight

Quantum mechanics is *inspiring*.

Third quantum insight

- **[Aharonov, Regev]**: Classical proof systems for approximate shortest vector problem, inspired by their earlier quantum proof systems.
- **[Aaronson]**: New lower bounds on classical query complexity of “local search”, inspired by Ambainis’ quantum adversary method.

What's next?

- More classical applications of quantum proof tools? Seems likely.
- One avenue: compare quantum proofs with "linear algebra method" in combinatorics **[Babai, Frankl]**
- Looking forward to more surprising proofs!

What's next?

Thanks!