

Quantum Property Testing

Hein Röhrig (CWI)

Joint work with Harry Buhrman (CWI & UvA),
Lance Fortnow (NEC), and Ilan Newman (Haifa)

Quantum Property Tester

algorithm	classical	quantum
object		
classical		X
quantum		

- input n bits/values $x = x_1x_2 \dots x_n, x \in X$
- property $P \subseteq X$
- quantum tester circuit
complexity: count # oracle query gates O_x
- if x has property, $x \in P$, tester accepts
- if x is ϵ -far from every $x' \in P$, tester rejects w.h.p.

Analyzing Large Data Sets

Large Data

- e.g. genome data, WWW
- difficult to store
- cannot look at entire input

What can be done in sub-linear (constant) time?

- random access
- allow randomization
- allow error

Classical Property Tester

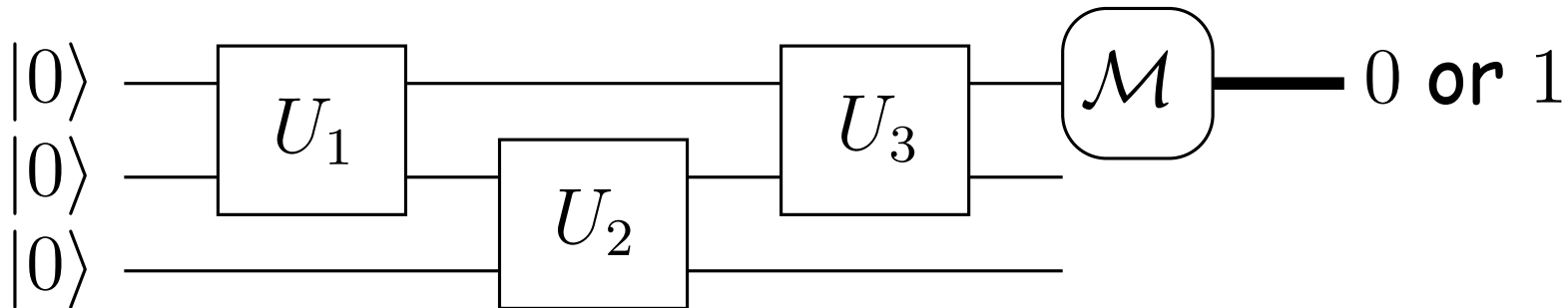
[Rubinfeld Sudan] and [Goldreich Goldwasser Ron]

- input n bits/values $x = x_1x_2 \dots x_n, x \in X$
- property $P \subseteq X$
- randomized **tester** algorithm for P
complexity: count **# queries** $x_i = ?$
- if x has property, $x \in P$, tester **accepts**
- if x is **ϵ -far** from every $x' \in P$, tester **rejects** w.h.p.
 ϵ -far: Hamming distance $\geq \epsilon n$

Classically Testable Properties

- Linearity test ($f(x) + f(y) = f(x + y) \forall x, y$) [Blum Luby Rubinfeld Bellare Coppersmith Hastad Kiwi Sudan]
- Graph Properties—colorability, not containing a forbidden subgraph, connectivity, acyclicity, rapidly mixing, max cut, ... [Frieze Kannan Goldreich Ron Alon Fischer Krivelevich Szegedy Parnas Ron Bender Ron Fischer Alon]...
- Monotonicity [Goldreich Goldwasser Lehman Ron Dodis Raskhodnikova Samorodnitsky Fischer Newman Rubinfeld]
- Set properties—equality, distinctness, ... [Ergun Kannan Kumar Rubinfeld Viswanathan]
- Geometric properties—metrics, clustering, convex hulls,... [Parnas Ron Alon Dar Czumaj Sohler]
- Membership in low-complexity languages—regular languages, constant-width branching programs, context-free languages [Alon Krivelevich Newman Szegedy Parnas Ron Rubinfeld]

Quantum Circuits



- **State:** k qubits are vector

$$|\psi\rangle = \sum_{j \in \{0,1\}^k} \alpha_j |j\rangle$$

with $\alpha_j \in \mathbb{C}$ and $\sum_{j \in \{0,1\}^k} |\alpha_j|^2 = 1$

- **Gate:** unitary operator U (length-preserving matrix)
- **Output:** measurement \mathcal{M} ; for final state $\sum_{j \in \{0,1\}^k} \beta_j |j\rangle$

$$\Pr[\text{output } 1] = \sum_{j \in 1\{0,1\}^{k-1}} |\beta_j|^2$$

Quantum Black-Box Algorithms

Gates:

- computational gates, e.g.,

$$\text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- queries to oracle for $x \in \{0, 1\}^n$

quantum memory

$$O_x : |j, b\rangle \mapsto |j, b \oplus x_j\rangle \quad (j \in \{0, 1\}^{\log n}, b \in \{0, 1\})$$

Task:

- given $f : \{0, 1\}^n \rightarrow \{0, 1\}$
- Q circuit for computing $f(x)$ w.h.p. from input $|0\rangle$
- complexity = # gates O_x

Quantum Property Tester

algorithm	classical	quantum
object		
classical		X
quantum		

- input n bits/values $x = x_1x_2 \dots x_n, x \in X$
- property $P \subseteq X$
- quantum tester circuit
complexity: count # oracle query gates O_x
- if x has property, $x \in P$, tester accepts
- if x is ϵ -far from every $x' \in P$, tester rejects w.h.p.

Hadamard Codewords

Inner Product mod 2: for $y, j \in \{0, 1\}^{\log n}$:

$$y \cdot j := \sum_{\ell=1}^{\log n} y_{\ell} j_{\ell} \pmod{2}$$

Hadamard code of $y \in \{0, 1\}^{\log n}$:

$$h(y) := x_0 \dots x_{n-1} \text{ with } x_j = y \cdot j$$

Hadamard Codewords

Inner Product mod 2: for $y, j \in \{0, 1\}^{\log n}$:

$$y \cdot j := \sum_{\ell=1}^{\log n} y_{\ell} j_{\ell} \pmod{2}$$

Hadamard code of $y \in \{0, 1\}^{\log n}$:

$$h(y) := x_0 \dots x_{n-1} \text{ with } x_j = y \cdot j$$

\exists quantum black-box algorithm to find y with **one** application of $O_{h(y)}$ [Bernstein Vazirani]

Classically: need **$\log n$** queries to oracle for $h(y)$ (information theory)

Hadamard Codewords

Inner Product mod 2: for $y, j \in \{0, 1\}^{\log n}$:

$$y \cdot j := \sum_{\ell=1}^{\log n} y_{\ell} j_{\ell} \pmod{2}$$

Hadamard code of $y \in \{0, 1\}^{\log n}$:

$$h(y) := x_0 \dots x_{n-1} \text{ with } x_j = y \cdot j$$

\exists quantum black-box algorithm to find y with **one** application of $O_{h(y)}$ [Bernstein Vazirani]

Classically: need **$\log n$** queries to oracle for $h(y)$ (information theory)

Candidate property: is x a (**any**) Hadamard codeword?

Testing Hadamard Codewords

Candidate Property $P = h(\{0, 1\}^n)$, i.e., all Hadamard codewords

Quantum Tester for input $x \in \{0, 1\}^n$

- apply [BV] algorithm to obtain y
- for $O(1/\epsilon)$ many j s: check $h(y)_j = y \cdot j$

Testing Hadamard Codewords

Candidate Property $P = h(\{0, 1\}^n)$, i.e., all Hadamard codewords

Quantum Tester for input $x \in \{0, 1\}^n$

- apply [BV] algorithm to obtain y
- for $O(1/\epsilon)$ many j s: check $h(y)_j = y \cdot j$

Catch: Classical Tester

- for $O(1/\epsilon)$ many pairs j, j' : query $x_j, x_{j'}$, and $x_{j \oplus j'}$.
- reject if $x_j \oplus x_{j'} \neq x_{j \oplus j'}$.
- accept

Observation: classically cannot extract y . Therefore property $P_A = h(A)$ of Hadamard codewords from a set $A \subseteq \{0, 1\}^{\log n}$.

Classical Lower Bound

Property $P_A = h(A)$ Hadamard codewords of random set

$$A \subseteq \{0, 1\}^{\log n}$$

- consider **deterministic** algorithms and prob. distribution **on inputs** (for Yao principle)
- for any **fixed** deterministic algorithm \mathcal{T} :

$$\Pr_A[\mathcal{T} \text{ correct on large fraction of } A] \leq 2^{-n/\text{const}}$$

(using expectation & Chernoff bound)

- **number** of (adaptive) deterministic **q -query** algorithms $\leq (2n)^{2^q}$
- \Rightarrow if $q = o(\log n)$, for most A **all** det. q -query alg. have large error
- **Yao principle**: for most A , **all** q -query rand. alg. have large error

Exponential Separation

Simon's problem: find $s \neq 0^m$ given $x : \{0, 1\}^m \rightarrow \{0, 1\}^m$ with

$$\forall j, j' \quad x(j) = x(j') \text{ iff } j' = j \oplus s \quad (\text{in } \mathbb{Z}_2^m)$$

Classically, need $2^{\Omega(m)}$ queries (\approx birthday paradox).

Quantumly, m queries suffice [Simon] and [Brassard Høyer].

Derived property: for $x : \{0, 1\}^{\log n} \rightarrow \{0, 1\}$,

$$P := \{x : \exists s \neq 0^{\log n} \text{ s.t. } \forall j \in \{0, 1\}^{\log n} \quad x(j) = x(j \oplus s)\}$$

We show (in paper)

- $\exists O(\log n \log \log n)$ -query quantum tester for P
- a classical tester must make $\Omega(\sqrt{n})$ queries

Limits to Quantum Property Testing

- **Polynomial method:** q -query quantum black-box algorithm $Q(x)$ with oracle $x \in \{0, 1\}^n$ induces degree- $2q$ multilinear polynomial $p(x)$ s.t.

$$\forall x \in \{0, 1\}^n \quad p(x) = \Pr[Q(x) \text{ accepts}]$$

[Beals Buhrman Cleve Mosca de Wolf]

- \exists d -wise independent pseudo-random number generators with range size $(\log n)^{O(d)}$ [Alon Babai Itai]
- $P := \text{range}$
- select x at random; given quantum algorithm, difference $E[p(x)] - E[p(x)|x \in P] \neq 0$ must be due to monomials of degree $> d$

Quantum Property Testing

Trivial extension of Q black-box decision problems? **No:**

- not the case **classically**
- not obvious: what is P (if any!) tested by given q algorithm
- for separation, need new classical lower bounds

Interesting? **Yes:**

- **characterize** power of quantum computing
- “in P or ϵ -far” weak general promise — **but still exponential separation!**

Conclusion

This work:

- Motivate & define **quantum** property testing
- Complexity separations: give properties s.t.

quantum	classical	
$O(1)$	$\Omega(\log n)$	(random Hadamard codewords)
$O(\log n)$	$n^{\Omega(1)}$	(Simon)
$n^{\Omega(1)}$		(pseudo-random numbers)

n = number of values in input

Open problems:

- gap $O(1)$ versus $\Omega(n)$ possible?
- applications? non-approximability, ...
- characterization of quantum testing by polynomials/group theory?