# Efficient Quantum Algorithms for (Gapped) Group Testing and Junta Testing

Andris Ambainis (University of Latvia)

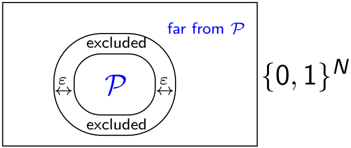
Joint with Alexander Belov (CWI),

Oded Regev (NYU), Ronald de Wolf (CWI)

QIP'16

# Property testing

- Property testing: assume object
  (1) has the property $\mathcal{P}$, or
  (2) is far from the property:
  needs many changes to get $\mathcal{P}$




- Possible to test a property by accesssing a small fraction of data.
- Useful for large data.

# Example: testing sortedness

- Input: list of numbers $A_1, \ldots, A_n$.
- Test if
  - List is sorted: $A_1 \leq A_2 \leq \ldots \leq A_n$ or
  - List is far from sorted: at least $\epsilon n$ numbers must be removed to make it sorted.
- [EKKRV00]: test for sortedness with $O(\log n/\epsilon)$ queries to $A_i$.

# Example: Blum-Luby-Rubinfeld [BLR90] linearity test

- Def: $f : \{0,1\}^n \to \{0,1\}$ is linear if $f(x \oplus y) = f(x) \oplus f(y)$ for all $x, y \in \{0,1\}^n$
- Distinguishing if a function is truly linear or not requires $2^n$ queries
- Property testing: BLR test uses only 3 queries:
  choose $x, y \in \{0,1\}^n$ uniformly at random; query $f(x)$, $f(y)$ and $f(x \oplus y)$; accept if $f(x) \oplus f(y) = f(x \oplus y)$
- if $f$ is linear: test accepts with probability 1
  if $f$ is $\varepsilon$-far from linear: test accepts with probability $\leq 1 - \varepsilon$
- Can repeat this $O(1/\varepsilon)$ times to reduce $1 - \varepsilon$ to 0.001

# Property testing in the quantum world

- Quantum information expands this area: the tester can be a quantum algorithm!
- Lots of interesting work in recent years of relevance to crypto and experiments (also on quantum properties). See survey by Ashley Montanaro and Ronald de Wolf.

# Some quantum speed-ups for classical properties

- $\mathcal{P} = N$-vertex bounded-degree bipartite graphs [ACL'11]
  Classical: $N^{1/2}$ queries,
  Quantum: $\widetilde{O}(N^{1/3})$ queries (using element distinctness)

- "Forrelation": $\mathcal{P} = \{(f, g) : g \approx \widehat{f}\}$ [AA'14]
  Classical: $N^{1/2}$ queries,
  Quantum: 1 query

# Our main result: junta testing

- $f : \{0,1\}^n \to \{0,1\}$ is a $k$-junta if it only depends on $k$ of the $n$ input bits

- How many queries to $f$ do we need to distinguish $k$-juntas from functions that are $\varepsilon$-far from any $k$-junta?
- Classically: $O(k \log k)$ suffice (Blais'09); $\Omega(k)$ needed
- [Atıcı-Servedio'07]: $O(k)$ quantum queries, Fourier sampling
- We give a new quantum tester:
  using $O(\sqrt{k} \log k)$ queries, running time $\widetilde{O}(n\sqrt{k})$

# Main Ingredient: Combinatorial group "testing"

- $n$ soldiers hand in blood samples, up to $k$ soldiers are sick.
  How do you identify the sick ones with few blood tests?

  Answer: combine parts of blood samples of first $n/2$ soldiers, testing this tells you if there is a sick soldier among those $n/2$; recurse to find one sick soldier with $\log n$ tests.
  $k \log n$ blood tests suffice to find set $A$ of all $k$ sick soldiers

# Gapped group testing

- Formally: given $f_A : \{0,1\}^n \to \{0,1\}$,
  there is unknown $k$-set $A \subseteq [n]$ s.t. $f_A(S) = 1$ iff $S \cap A$
  Query $f_A(S)$ = blood test for mix of blood from soldiers in $S$
- *Gapped* group testing: distinguish $|A| \leq k$ from $|A| \geq k + d$
  - Classical complexity: $(k/d)^2$ queries
  - Quantum complexity: $(k/d)^{1/2}$ by adversary bound
- Note: 4th power quantum speed-up! (more than Grover)

# Our quantum junta tester (sketch)

- Input $f : \{0,1\}^n \to \{0,1\}$ either depends on $k$ variables, or is $\varepsilon$-far from any $k$-junta
- Lemma (roughly): in the latter case, there exists a $d \geq 1$ such that there are $k+d$ variables each with $\varepsilon/d$ "influence"
- The quantum tester: apply the quantum algorithm for group testing, combined with a procedure that checks whether any of the variables in a given subset has influence $> \varepsilon/d$
  Cost: $\sqrt{\frac{k}{d}}\sqrt{\frac{d}{\varepsilon}} = O(\sqrt{k/\varepsilon})$ queries to $f$
- (since we don't know $d$ we need to try several guesses; $d > k$ is dealt with separately)

Zooming in:
some glimpses of the proofs

# Adversary bound

- The main method for quantum query lower bounds.
- Considers weighted sum of inner products $\langle \psi_x | \psi_y \rangle$ where $|\psi_x\rangle$ is algorithm's state on the input $x$.
- $Adv^{+}(f)$ - the best lower bound from this method (with the best choice of weights).
- Finding the best lower bound $=$ a semidefinite program.
- [Reichardt, 2009-2011]: dual SDP $=$ finding the best quantum algorithm.
- Universal method for designing quantum algorithms.

# Adversary bound

- Computational problem $f(x)$, $x = (x_1, \ldots, x_n)$.
- For each variable $x_i$, we can choose a matrix $X_i \succeq 0$ indexed by inputs $x, y$.
- Goal: minimize
$$\max_x \sum_i X_i[x, x]$$
subject to
$$\sum_{i: x_i \neq y_i} X_i[x, y] = 1$$
for all $x, y : f(x) \neq f(y)$.
- Minimum $= Adv^{\pm}$.

# Adversary bound for gapped group testing

$\mathcal{X} = \{A \subseteq [n] : |A| = k\}$
$\mathcal{Y} = \{B \subseteq [n] : |B| = k + d\}$

SDP which characterizes quantum query complexity:

$$\begin{aligned} \min \max_{A \in \mathcal{X} \cup \mathcal{Y}} & \sum\nolimits_{S \subseteq [n]} X_S[A, A] \\ \text{s.t.} & \sum_{S:\, A \cap S = \emptyset \text{ xor } B \cap S = \emptyset} X_S[A, B] = 1 \quad \forall A \in \mathcal{X}, B \in \mathcal{Y}; \\ & X_S \succeq 0 \qquad \forall S \subseteq [n] \end{aligned}$$

We give feasible solution $X_S = \phi_S \phi_S^*$,
with $\phi_S$ a vector depending on real parameters $\alpha_1, \ldots, \alpha_{n-k-d+1}$,
with objective value $W = O(\sqrt{k/d})$

$\Rightarrow$ *existence* of a query-optimal algorithm

# From adversary bound to algorithm

- Transformation $U = R_\Lambda O_f$ where $O_f, R_\Lambda$ - two reflections.
- $O_f$ - query, $R_\Lambda$ defined by the solution of the adversary SDP.
- If $f=1$, $|\psi_{start}\rangle \approx |\psi\rangle$ , $R_\Lambda O_f|\psi\rangle = |\psi\rangle$.
- If $f=0$, the fraction of $|\psi_{start}\rangle$ consisting of $|\psi\rangle$, $R_\Lambda O_f|\psi\rangle = \lambda|\psi\rangle$, $|\lambda - 1| \leq \frac{1}{W}$ is small.
- Eigenvalue estimation distinguishes the two cases, in $O(W)$ steps.

# Time-efficient implementation

- Need: reflection through $\Lambda := \mathrm{span}\{\psi_A : A \in \mathcal{X}\}$,

$$\psi_A = |0\rangle + \gamma \sum_{s=1}^{n-k-d+1} \alpha_s \sum_{S\subseteq[n]:\ |S|=s,\ S\cap A=\emptyset} |S\rangle$$

- $\Lambda$ - symmetric w.r.t. permuting elements of $\{1, 2, \ldots, n\}$.
- Schur-Weyl transform: expresses state in the Fourier basis, with basis states corresponding to representations of $S_n$.
- $\Lambda$ has simple form in Fourier basis.

# Time-efficient implementation

- Cost: $O(\sqrt{k/d})$ executions of $U = O_f R_\Lambda$
- How many elementary gates needed to implement $R_\Lambda$?
- Implementing $R_\Lambda$:
  1. Use QFT (Schur-Weyl) to change to Fourier basis
  2. Reflect in Fourier basis
  3. Undo step 1
- [Bacon-Chuang-Harrow, 06]: Schur-Weyl transform with $\widetilde{O}(n)$ gates.
- Time complexity becomes $\widetilde{O}(n\sqrt{k/d})$ for group testing, and $\widetilde{O}(n\sqrt{k/\varepsilon})$ for junta testing

# Lower bounds

- Image testing: given black-box access to $g : [n] \to [m]$, test if
  - $|Image(g)| \leq l$;
  - $g$ is $\epsilon$-far from any $h : |Image(h)| \leq l$;
- Junta testing $\Rightarrow$ Image testing;
- Image testing requires $\Omega(l^{1/3})$ queries (collision lower bound).
- Does it require $\Omega(\sqrt{l})$ queries?
- Example: distinguish whether $g$ is
  - a 2-1 function ($|Image(g)| = n/2$);
  - 3-1 on half of domain and 1-1 on half of domain ($|Image(g)| = 2n/3$).

# Summary & some questions

- We gave $\tilde{O}(\sqrt{k})$-query quantum algorithm for testing whether $f$ is $k$-junta or far from all $k$-juntas
- With time-efficient implementation
- Based on an optimal algorithm for gapped group testing

Questions:

1. Is there a better algorithm for junta testing?
   Best known lower bound is $\Omega(k^{1/3})$ (from collision problem)
2. Testing if $f : \{0,1\}^n \to \{0,1\}$ is monotone?
   Best classical upper bound is $\widetilde{O}(\sqrt{n})$, lower bound $\Omega(n^{1/4})$.
   Quantum upper bound $\widetilde{O}(n^{1/4})$ (Belovs-Blais).
3. More quantum testers for graph properties?