How do I get that $a^{p+1}=0$? Bruh. $\sum a_j =: a$.

08/26/19

Property Testing

Def ε-tester accept $x \in \mathcal{P}$ (property) w/ $\Pr \geq \frac{2}{3}$ (completeness) and reject ε-far w/ $\Pr \geq \frac{2}{3}$ (soundness)

$j \in \{0,1\}^n$ function $f: \{0,1\}^n \to \{0,1\}$ is identified as a string $x \in \{0,1\}^N$, $N = 2^n$ $\quad x_j := f(j)$

(powerset of sets that get mapped to 0)

Algorithm	G	f:	H
Deutsch-Jozsa	$\mathbb{Z}_2$	$\{0,1\}^n \to \mathbb{Z}_2$	e or $\mathbb{Z}_2$
Bernstein-Vazirani	$\mathbb{Z}_2^n$	(not coset separating)	$\mathbb{Z}_2$
Simon	$\mathbb{Z}_2^n$	$\{0,1\}^n \to \mathbb{Z}_2^n$	$\mathbb{Z}_2$
Shor	$\mathbb{Z},+$	$\mathbb{Z}_2^n$	$\{0,r,2r,\ldots\}$, $r \in G$

① Amplitude amplification Q algo. output z s.t. $f(z)=1$ w/ Pr. p $\Rightarrow$ Find z w/ $\mathcal{O}(1/\sqrt{p})$ queries w/ success $\Pr \geq 2/3$.

② Bernstein-Vazirani

They define Hadamard encoding

$$h: \{0,1\}^n \to \{0,1\}^N \quad \text{Normally written as } f: \{0,1\}^n \to \{0,1\}$$

group element s $\quad$ function

$$[h(s)](y) = s \cdot y \mod 2$$

Functions are not coset-separating. Two Hadamard codewords are at distance 1/2 because of mod 2

$$d(x,y) = \frac{|\{j \mid x_j \neq y_j\}|}{N}$$

Quantum

Given $A \subset \{0,1\}^n$, test property $\mathcal{P} = \{$funcs $x \in \{0,1\}^N$ s.t. $x = h(s)$ for some $s \in A\}$

Run BV $\to$ $s \in A \to$ test $s \cdot y$ reject ε-far w/ prob. $\varepsilon \to$ AA to get $\boxed{\mathcal{O}(1/\sqrt{\varepsilon}) \text{ queries}}$

$\quad\to$ $s \notin A$ reject

Classical $\boxed{\text{No test w/ } \frac{\log N}{2} \text{ or fewer queries}}$

If $\mathcal{P}$ can be $\frac{1}{2}$-tested w/ T queries, there is a decision tree that accepts x correctly w/ 2/3 Pr. Is there such a tree? How many? Well, every Hadamard codeword is $\frac{1}{2}$-away from each other, so such a tree accepts w/ prob. $\frac{1}{2}$. To accept w/ Pr $\frac{2}{3}$ need Pr $2^{-\Omega(N)}$ by Chernoff bound.

Binary output value for each 2^T leaves

choose $A \in \{0,1\}^N$ to query

But there are at most $2^{2^T} N^{2^T-1}$ trees of depth T.

at each 2^{T-1} node

$$2^{-\Omega(N)} 2^{2^T} N^{2^T-1} \sim \frac{2^{n2^T-1}}{2^{2^n-2^T}}$$

small for $T = n/2$

③ Fourier sampling test of k-junta

variable $s_1 = 1000\cdots$
$s_2 = 0100\cdots$
$s_3 = 0010\cdots$
$s_4 = 0001\cdots$

Use BV but now not "Hadamard codeword" (which depends only on the "variable" s) but a function $f(s) \Rightarrow$ Support of $\tilde{f}(s)$ is $\le k$ if k-junta. We start by setting $W = \phi$ and keep adding s that we find from AA (w/ Pr $\ge \epsilon$, Fourier sampling outputs $s \notin W$) w/ $\boxed{O(k/\sqrt{\epsilon})}$ queries in total we find if f is not k-junta.

Ambainis et al. $O\left(\sqrt{\frac{k}{\epsilon}}\right)$

Classical – Upper bound $O(k \log k + k/\epsilon)$
– Lower bound $\Omega(k)$

④ Simon

In the original Simon's problem, we have a coset-separating func. $f: \{0,1\}^n \to \{0,1\}^n$ (The image needs to be at least $\{0,1\}^{n-1}$ b/c f must take different values on different 2^{n-1} cosets)

Not phase-query

$$\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle|0\rangle^{\otimes n} \mapsto \frac{1}{\sqrt{N}} \sum_x |x\rangle|f(x)\rangle \xrightarrow{\text{measure}} \frac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}}$$

$$\xrightarrow{\text{FT}} \frac{1}{\sqrt{2N}} \sum_z \underbrace{\left[(-1)^{x \cdot z} + (-1)^{(x \oplus s)\cdot z}\right]}_{\text{No destructive interference iff } s \cdot z = 0} |z\rangle$$

$\Theta(n)$ queries $\Rightarrow$ learn $n-1$ L.I. $z \Rightarrow$ Gaussian elimination to find s s.t. $\begin{pmatrix} z_1 \\ \vdots \\ z_{n-1} \end{pmatrix} \cdot s = 0$

↘ w/ high prob. $\to$ Deterministic algo. by Brassard and Høyer

Simon property

$\mathcal{P}_{\text{Simon}}$ = set of coset-functions $f(j) = f(k)$ if $j = k \oplus s$
but diff. cosets can have same value

Quantum: Run Simon $n-1$ time $= \boxed{O(\log N)}$ queries. to learn s. Then test a few $(j, j\oplus s)$ pairs and reject if they are not equal (w/ Pr say, $\frac{N}{4}$ for $\epsilon = \frac{1}{4}$)

Classical: Suppose there is a randomized algorithm that distinguish uniform distribution over $\mathcal{P}_{\text{Simon}}$ and $\mathcal{P}_{\frac{1}{4}\text{-Simon}}$ w/ Pr $\ge 2/3$.

They show that

$$\begin{array}{ccc} & \text{dist. } \mathcal{P}_{\frac{1}{4}\text{-Simon}} & \\ O(T^2/N) \swarrow\!\!\nearrow & & \nwarrow\!\!\searrow o(1) \\ \text{dist. } \mathcal{P}_{\text{Simon}} & \longleftrightarrow & \text{Uniform} \end{array}$$

Advantage $O\left(\frac{T^2}{N}\right) + o(1)$ over random guessing

Figure out # of queries required to have success Pr $\ge 2/3$.

B/c functions are not coset-separating, only diff. values of observed $f(j)$ can successfully distinguish $\mathcal{P}_{\text{Simon}}$ and Uniform. "Good" seq.

Pr(good seq.) is $O(T^2/N)$
$\ge$ success prob. $2/3$
$\Rightarrow \boxed{T = \Omega(\sqrt{N})}$

⑤ Shor Test a function in $[m]^N$ (take values in $[m]$)

if it has period $\underbrace{q \le p}\le r \le \sqrt{\frac{N}{2}}$

Quantum $\Theta(1)$

Classical $q = \frac{r}{2}$, $\Omega\left(\sqrt{r/\log r}\,\log N\right)$

$r = \sqrt{N} \Rightarrow \Omega(N^{1/4}/\log N)$

⑥ Grover

Can estimate frequency of inputs $\{j \mid x_j \in S\}$, $S \subset [m]$ with precision $C\left(\frac{\sqrt{p}}{T} + \frac{1}{T^2}\right)$ where T is # of queries.

Quantum Given two distributions on $[m]$ (given as frequency on $[m]^N$) Q ϵ-tester uses $\boxed{\Theta\left(\frac{\sqrt{m}}{\epsilon^8}\right)}$ queries

Bravyi ϵ-additive estimate TVD uses $\Theta\left(\frac{\sqrt{m}}{\epsilon^8}\right)$ queries

Montanaro $\Theta\left(\sqrt{m}/(\epsilon^{3/2}\log \epsilon^{-1})\right)$

Classical

- Upper $\Theta\left(\left(\frac{m}{\epsilon}\right)^{2/3}\log m\right)$
- Lower $\Omega(m^{2/3})$

$\Theta(m^{2/3}/\epsilon^{4/3})$

⑦ Element distinctness

Polynomial method

Acceptance prob. of a T-query quantum algorithm on N-bit input is a polynomial of deg. $\leq 2T$ on N variables.

$x_j \in \{0,1\}$ $\quad (-1)^{x_j} = 1 - 2x_j$

Thm $\mathcal{P} \subset \{0,1\}^N$, $|\mathcal{P}_{close}| < 2^{N-1}$

$\mathcal{D}$ be a distribution on $\{0,1\}^N$ s.t. $p_z = 0$ for $z \notin \mathcal{P}$

$\mathcal{U}$ uniform over $\{0,1\}^N$

$\mathbb{E}_{\mathcal{D}}[z_{i_1} \cdots z_{i_\ell}] = 2^{-\ell}$ $\quad \forall \ell \leq k$ indices

Every quantum ϵ-tester must make at least $\frac{k+1}{2}$ queries

■ Assume $\exists$ algorithm w/ success $Pr \geq 2/3$ $\forall z \in \mathcal{P}_{close}$

$\mathbb{E}_{z \sim \mathcal{D}}[p(z)] \geq \frac{2}{3}$

$\underbrace{\geq \tfrac{2}{3} \geq \tfrac{2}{3} \cdots \geq \tfrac{2}{3}}_{\mathcal{P}} \; 0 \; 0 \cdots 0$

$\mathbb{E}_{z \sim \mathcal{U}}[p(z)] \leq \frac{|\mathcal{P}_{close}|}{2^N} \cancel{1} + \frac{1}{3}\left(1 - \frac{|\mathcal{P}_{close}|}{2^N}\right) < \frac{2}{3}$

Upper bound of acceptance of prob. is 1 ($\frac{2}{3}$ is just lower bound)

$|\mathcal{P}_{close}| < 2^{N-1}$

Write $p(z) = \sum_{\deg \ell \leq k} \alpha$ monomials$[z_{i_1} \cdots z_{i_\ell}]$

By linearity of expectation and the assumption that expectations on $z_{i_1} \cdots z_{i_\ell}$ are indistinguishable from uniform on $\ell \leq k$ bits, we have that

$$\mathbb{E}_{z \sim \mathcal{D}}[p(z)] = \mathbb{E}_{z \sim \mathcal{U}}[p(z)]$$

$\Rightarrow$ Both $\mathbb{E}[p(z)] \geq \frac{2}{3}$ and $< \frac{2}{3}$. Contradiction. □

Communication complexity

Classical - communication lower bound $\Rightarrow$ tester lower bound w/ const. overhead

Ex k-linear tester $\leftrightarrow$ disjointness tester

k-linear functions are linear and depend on k input bits ("exactly k-junta")

Test if weight-$k/2$ strings x, y are disjoint = testing that $x \oplus y$ is k-linear

$|x \oplus y| = |x| + |y| - 2|x \cap y|$

Shared randomness $\Rightarrow$ 1 query = 2 bit of communication

$A \underset{i \cdot y}{\overset{i \cdot x}{\rightleftarrows}} B$

Communication lower bound: $\Omega(k)$; one-way $\Omega(k \log k)$ $\Rightarrow$ Non-adaptive k-linear tester

Overhead for quantum is linear in n b/c you can query superpositions

$\sum_{i \in \{0,1\}^n} |i\rangle$ $\quad$ n terms

Lower bound $\Omega(1)$ for k-linear tester is achieved by BV.

09/07/19 Why can't Bouland prove average-case hardness from approx. sampling from Stockmeyer?

Understand worst-to-average-case reduction

Conjecture 6 implies QS

p. 18 "