Preemptive Make-up class Next week - will send e-mail

9/11/07

$\boxed{\text{Ph 452}}$ Lecture 7

IQI Quick Review

Query complexity problems — see lecture notes.

Simon's Problem:

$n \in \mathbb{N}$, $N = 2^n$, $\Sigma = \mathbb{B}^n$ (alphabet size grows with problem!)

$g : X \to Y$, $Y = \mathbb{B}$ (Boolean fn.)

$X \subsetneq \Sigma^N$ (partial fn)

$$X = \{ x = \underbrace{(x_0, \ldots, x_{N-1})}_{\substack{\in \Sigma^N \\ (N \text{ letters})}}, x_i \in \Sigma \mid x_i = x_j \text{ iff } i = j \oplus s \}$$

$$g(x) = \begin{cases} 0 & s = 0^n \\ 1 & s \neq 0^n \end{cases}$$

X_i has a <u>period</u> of s if we think of each $X_i \in (\mathbb{Z}_2)^n$ instead of $\mathbb{Z}_{2^n}$:

Example: $n = 3$, $N = 8$ $\Sigma = \{0, \ldots, 7\}$, $s = 3 = 011_2$

$x_{000} = x_{011}$ x has abbacddc pattern

$x_{001} = x_{010}$

$x_{100} = x_{111}$ $X = \{ 01100110, 01101001, 01101221, 01102112, \ldots$

$x_{101} = x_{110}$ $\ldots, 76677667 \}$

$s = 0^n$: g is a 1 to 1 function

$s \neq 0^n$: g is a 2 to 1 function w/ period s

$\boxed{\text{Ph 45a}}$ Lecture 7

Worst case? $N/2+1$ queries suffice to reveal $2\text{-}1$ or $1\text{-}1$. (Like Deutsch-Jozsa)

Qm: $N^{1/3}$
2002: Shi

Can do with fewer!

"B/c Simon's problem has more structure"

$s = \{0, \dots, N-1\}$, revealed by x_i, x_j s.t. $x_i = x_j$

ways $i = j \oplus s$: k s.t. $\binom{k}{2} \geq N$

$k \sim \sqrt{N}$

Example: $n=3$, $N=8$

$x_{000}, x_{001}, x_{010}, x_{100}, x_{111}$

$x_{000} = x_{001}$? $\Leftrightarrow s = 001$?
$x_{000} = x_{010}$? $\Leftrightarrow s = 010$?
$x_{001} = x_{010}$? $\Leftrightarrow s = 011$?
$x_{000} = x_{100}$? $\Leftrightarrow s = 100$?
$x_{001} = x_{100}$? $\Leftrightarrow s = 101$?
$x_{010} = x_{100}$? $\Leftrightarrow s = 110$?
$x_{000} = x_{111}$? $\Leftrightarrow s = 111$?

Choose i's so that $i \neq$ XOR of any 2 previous i's.

$\frac{k(k-1)}{2} \geq N$: $k^2 - k - 2N \geq 0$ $\quad k \geq \frac{1}{2} \pm \frac{1}{2}\sqrt{1+4\cdot 2N}$

$N=8$

$\frac{1}{2}\sqrt{65} + \frac{1}{2}$
$= \frac{8+2}{2} + \varepsilon$
$= 4.5 + \varepsilon = 5$

$$\boxed{D(g) = \left\lceil \frac{1}{2}\sqrt{8N+1} + \frac{1}{2} \right\rceil}$$

Simon's Algorithm: Quantum query complexity of

$$\boxed{Q_2(g) = \Theta(\log N)}$$

"This of course leads to 3 questions:

1) What does Big-O mean?
2) What is a quantum query?
3) What does Q_2 mean?

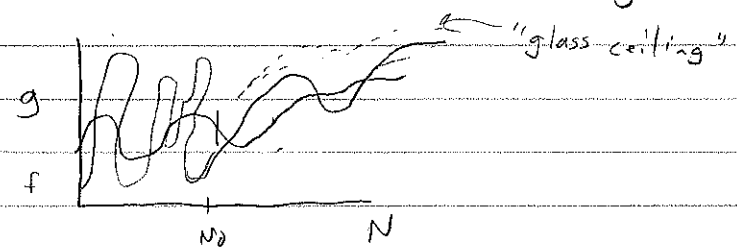
Ph 452 Lecture 7

Big-O notation:

$$f(N) = O(g(N)) \iff$$

$$(\exists N_0 > 0)(\exists k > 0)(\forall N > N_0)\ [f(N) \le k\, g(N)]$$

"f grows no faster than a constant multiple of g for large N"



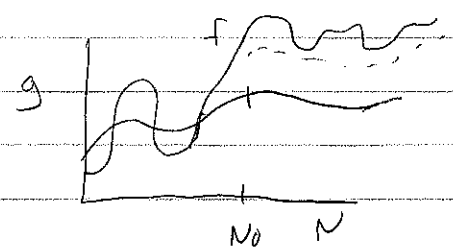
"g is an upper bound for f"

Big-Ω notation

$$f(N) = \Omega(g(N)) \iff$$

$$(\exists N_0 > 0)(\exists k > 0)(\forall N > N_0)\ [f(N) \ge k\, g(N)]$$

"f grows at least as fast as a constant multiple of g for large N"



Big-Θ notation

$$f(N) = \Theta(g(N)) \iff f(N) = O(g(N)) \text{ and } f(N) = \Omega(g(N))$$

$c = \max(c_0, c_2)$

"f is within a constant multiple of g for large N"

Ph 432 Lecture 7

What is a quantum query?

Querying is physical! Input x stored somewhere — not by some "oracle."

"The bits & bytes of the universe aren't held by angels — there held in the physical quantities around us. And by physical, I mean objects which can be measured experimentally to yield outcomes."

Irreversible: $i \to x_i$

Reversible: $(i, j) \to (i, i \oplus x_i)$

Quantum: $|i, j\rangle \to |i, i \oplus x_j\rangle$

What is an algorithm?

(a) A procedure for solving a computational problem.

(b) A consistent uniform circuit family.

alg = consistent unif. family
efficient alg $\Leftrightarrow$ $|C_k| = \mathrm{poly}(k)$ and uniform

Family: set of acyclic circuits $\{C_1, C_2, \ldots\}$

Consistent: $C_n(\vec{\rho}_m \otimes \vec{0}^{\otimes n-m}) = C_m \vec{\rho}_m \otimes \vec{0}^{n-m}$

Issue: computability vs. complexity on uniformity criterion

Uniform: Each $C_k = C(k)$ is itself ~~constructable by an algorithm~~ (has a "finite description")

Query complexity: min # queries in an algorithm evaluating g on worst-case x

Ph 452 Lecture 7

How does an algorithm evaluate a function?

Exactly: Measurement of output (Bayes / Born) yields $g(x)$ with certainty.

"Las Vegas" With Zero Error: Measurement of output yields "inconclusive" w/prob $\leq 1/2$ — otherwise yields $g(x)$ with certainty.

"Santa Ana?" With 1-sided Error: Measurement of output yields $g(x)$ with certainty if $g(x)=1$. It yields $g(x)$ w/prob $\geq 2/3$ if $g(x)=0$.

"Monte Carlo" With 2-sided, or "bounded" error: Measurement of output yields $g(x)$ w/prob $\geq 2/3$.

Types of (reversible) query algorithms:

Deterministic: Gates are permutations

Randomized: Gates are stochastic

Quantum: Gates are unitary

Has nothing to do w/ inputs or outputs!

Notation:

$D(g)$ - Deterministic
$R_0(g)$ - Zero-err, randomized
$R_1(g)$ - 1-sided - " "
$R_2(g)$ - 2 - " " "
$Q_E(g)$ Quantum exact
Got this far Q_0, Q_1, Q_2 similar to R_0, R_1, R_2.