Lecture 7

Q2) Quick Review

Query complexity problems — see lecture notes.

Simon's Problem:

\[ n \in \mathbb{N}, \quad N = 2^n, \quad \Sigma = \mathbb{B}^n \quad (\text{alphabet size grows with problem}) \]

\[ g : X \to Y, \quad Y = \mathbb{B} \quad (\text{Boolean fn.}) \]

\[ X \subseteq \Sigma^N \quad (\text{partial fn.}) \]

\[ X = \{ x = (x_0, \ldots, x_{n-1}) \mid x_i \in \Sigma, \quad x_i = x_j \text{ if } i \equiv j \pmod{s} \} \]

\[ g(x) = \begin{cases} 0 & s = 0^n \\ 1 & s \not= 0^n \end{cases} \]

\[ X_i \text{ has a period of } s \text{ if we think of each } X_i \in (\mathbb{Z}_2)^n \]

Instead of \( \mathbb{Z}_2^n \):

Example: \( n = 3, \quad N = 8, \quad \Sigma = \{0, \ldots, 7\}, \quad s = 3 \)

\[ X_{00} = X_{011}, \quad \text{X has abba cddc pattern} \]

\[ X_{01} = X_{010} \]

\[ X_{10} = X_{111}, \quad X = \{01100110, 01101001, 01101241, 01102112, \ldots \} \]

\[ X_{11} = X_{110}, \quad \ldots, \quad 7667276673 \]

\( s = 0^n \); \( g \) is a total function

\( s \not= 0^n \); \( g \) is a total function w/ period \( s \)
What case? \( N/2 + 1 \) superimposed suffice to reveal \( \pm 1 \) or \( 1 - 1 \). (Like Deutsch-Jozsa)

Can do with fewer.

\[ s = 00, \ldots, N-13, \text{ revealed by } x_i, x_j \text{ s.t. } x_i = x_j \]

\# ways \( i \neq j \): \( k \) s.t. \( \binom{k}{2} \geq N \)

\[ k = \sqrt{N} \]

Example: \( n=3, N=8 \)

\[ x_{000}, x_{001}, x_{010}, x_{100}, x_{111} \]

\( x_{000} = x_{001} ? \) \( \Leftrightarrow s = 001 ? \) Choose \( i,j \) s.t.
\( x_{000} = x_{010} ? \) \( \Leftrightarrow s = 010 ? \) i \# any of any 2 prevent i's
\( x_{001} = x_{010} ? \) \( \Leftrightarrow s = 011 ? \)
\( x_{001} = x_{011} ? \) \( \Leftrightarrow s = 100 ? \)
\( x_{001} = x_{010} ? \) \( \Leftrightarrow s = 101 ? \)
\( x_{001} = x_{011} ? \) \( \Leftrightarrow s = 110 ? \)
\( x_{001} = x_{100} ? \) \( \Leftrightarrow s = 111 ? \)

\[ (k-2) \geq N \Rightarrow k^2 - k - 2N^2 \geq 0 \Rightarrow k \geq \frac{1}{2} \pm \frac{1}{2} \sqrt{1 + 4 \cdot 2N} \]

\[ D(g) = \left\lceil \frac{1}{2} \sqrt{(N+1)} \right\rceil + \frac{1}{2} \]

Simon's Algorithm: Quantum query complexity of

\[ Q_2(g) = O(\log N) \]

This of course leads to 3 questions:

1. What does Big-O mean?
2. What is a quantum query?
3. What does O mean?
Big-O notation:

\[ f(N) = O(g(N)) \iff (\exists N_0) (\exists k > 0) (\forall N > N_0) \left[ f(N) \leq k g(N) \right] \]

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

\[ g \]
\[ f \]
\[ N_0 \]
\[ N \]

Big-Ω notation:

\[ f(N) = \Omega(g(N)) \iff (\exists N_0) (\exists k > 0) (\forall N > N_0) \left[ f(N) \geq k g(N) \right] \]

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

\[ g \]
\[ f \]
\[ N_0 \]
\[ N \]

Big-Θ notation:

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

"f is within a constant multiple of g for large N"
Ph.452 Lecture 7

What is a quantum query?

Querying is physical, input X stored somewhere—not by some "oracle."

"The bits & bytes of the universe are held by angels—those held in the physical quantities around us. And by physical, I mean objects which can be measured experimentally to yield outcomes."

Irreversible: \( i \rightarrow x_j \)

Reversible: \( (i, j) \rightarrow (i, j \otimes x_j) \)

Quantum: \( |i, j \rangle \rightarrow |i, j \otimes x_j \rangle \)

What is an algorithm?

- A procedure for solving a computational problem,

- A consistent uniform circuit family

\[ \text{Family: set of circuits } C_1, C_2, \ldots, C_n \]

Consistent:

\[ C_n (\rho_m \otimes \tilde{\rho}^{n-m}) = C_m \rho_m \otimes \tilde{\rho}^{n-m} \]

Uniform: Each \( C_k = C(x) \) is itself constructable by an algorithm (has a "finite description")

Query complexity: \( \min \) # queries in an algorithm evaluating \( g \) on worst x
Lecture 7

How does an algorithm evaluate a function?

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

"Los Angeles": With zero error: Measurement of output yields "inconclusive" with prob $1/2$ - otherwise yields $g(x)$ with certainty.

"Sada Ana?": With 1-sided error: Measurement of output yields $g(x)$ with certainty: if $g(x) = 1$, it yields $g(x)$ with prob $> 1/3$ if $g(x) = 0$.

"Modo loco": With 2-sided, or "bounded" error: Measurement of output yields $g(x)$ with prob $> 1/3$.

Types of (reversible) query algorithms:

- Deterministic: Gates are permutations
- Randomized: Gates are stochastic
- Quantum: Gates are unitary

Notation:

- $D(g)$ - Deterministic
- $R_0(g)$ - Zero-cir, randomized
- $R_1(g)$ - 1-sided
- $R_2(g)$ - 2-sided
- $QF(g)$ - Quantum exact

Gotthiser $O_0, O_1, O_2$ similar $K_0, K_1, K_2$. 