## CSE439 Fall 2025 Weeks 7 and 8: Deutsch-Jozsa and Simon's Problems

These lectures begin a "vibe shift" from pictorial to formulaic. Note that the pictorial way of tracing the matrix calculations---via Feynman paths---scales exponentially with the number $n$ of qubits. Not only that, it also forks exponentially with the number of Hadamard gates (or square-root-of-NOT or other nondeterministic gates). *Formulas*, however, can scale linearly or at worst polynomially in $n$.

These chapters also lead into the two major applications where **quantum advantage** is strongly believed: Shor's and Grover's algorithms (to come in chapters 11--13). On the way are the Deutsch-Jozsa Problem---where it is unresolved whether the classical criticism of the original Deutsch's Problem fully applies---and Simon's Problem, where an exponential lower bound on the expected time for any classically randomized algorithm has been proven under reasonable stipulations.

### Deutsch-Jozsa Extension (Ch. 9)

Getting back to Deutsch's Problem, Richard Jozsa added that if you only care about distinguishing ***constant*** functions $f : \{0,1\}^n \rightarrow \{0,1\}$ from ***balanced*** ones, then you can make the classical algorithms require $2^{n-1} + 1$ queries, while the quantum ones can still do it on one query to a completely separable superposed state. This is a conditional problem, called a **promise problem**, in that it only applies when $f$ is in one of those two cases. If $f$ is neither balanced nor constant, then "all bets are off"---any answer is fine, even $|\ \overline{}\backslash\_(ツ)\_/\overline{}\ \rangle$.

The maze diagrams would get exponentially big, but we can track the computations via linear algebra. It is like Deutsch's setup except with $\mathbf{H}^{\otimes n}$ in place of the first $\mathbf{H}$, input $|0^n 1\rangle$ in place of $|01\rangle$, and targets (ignoring the $\sqrt{2}$ normalizers):

- constant $\mapsto |0^n\rangle\big(|0\rangle + |1\rangle\big)$ (instead of $\big(|00\rangle + |01\rangle\big)$, so that $0^n$ is certainly measured.
- balanced $\mapsto |?\,\rangle$ (instead of $\big(|10\rangle + |11\rangle\big)$, such that $0^n$ is certainly *not* measured.

The key observation is that for any $f$, any argument $x \in \{0,1\}^n$, and $b \in \{0,1\}$, the amplitude in the component $xb$ of the final quantum state $\phi$ is

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{t \in \{0,1\}^n} (-1)^{x \bullet t} (-1)^{f(t) \oplus b}.$$

Here $x \bullet t$ means taking the dot-products $x_i \cdot t_i$ (which is the same as $x_i \wedge t_i$) and adding them up modulo $2$ (which is the same as XOR-ing them). Well, when $x = 0^n$ this is always just zero, so the first term is $(-1)^0$ and just drops out, leaving

$$\phi\left(0^n b\right) \;=\; \frac{1}{\sqrt{2^{n+1}}}(-1)^b \sum_{t \in \{0,1\}^n} (-1)^{f(t)}.$$

Note that the $(-1)^b$ term is independent of the sum over $t$, so it comes out of the sum---and this is why we get two equal possibilities in the original Deutsch's algorithm as well. Ths final point is that:

- When $f$ is ***constant***, these terms are all the same, so they ***amplify***---giving $\frac{1}{\sqrt{2}}$ for the constant-false function and $\frac{-1}{\sqrt{2}}$ for constant-true. Both of these amplitudes square to $\frac{1}{2}$ and so together soak up all the output probability, so that $0^n$ is measured with certainty.
- When $f$ is ***balanced***, the big sum has an equal number of $+1$ and $-1$ terms, so they all ***interfere*** and *cancel*. Hence $0^n$ will certainly not be measured.

Added: A *randomized* classical algorithm can efficiently tell with high probability whether $f$ is constant by querying some random strings. If it ever gets different answers $f(y) \;\neq\; f(y')$ then definitely $f$ is not constant. (So, under the condition of the "promised problem," it must be balanced.) If it always gets the same answer, then since any balanced function gives 50-50 probability on random strings, it can quickly figure that $f$ is constant. But it is still the case that a deterministic algorithm needs exponentially many queries and hence exponential time.

**At this point, coverage transits to handwritten notes on the blackboard and/or projector:**
https://cse.buffalo.edu/~regan/cse439/CSE439week8notes.pdf
Note also that week 7 generally includes the First prelim Exam, while one lecture of week 8 is erased by the short Fall Break. So they are really "one week of lectures."