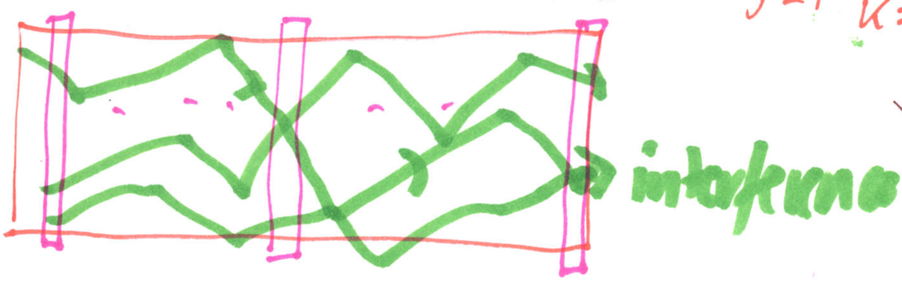
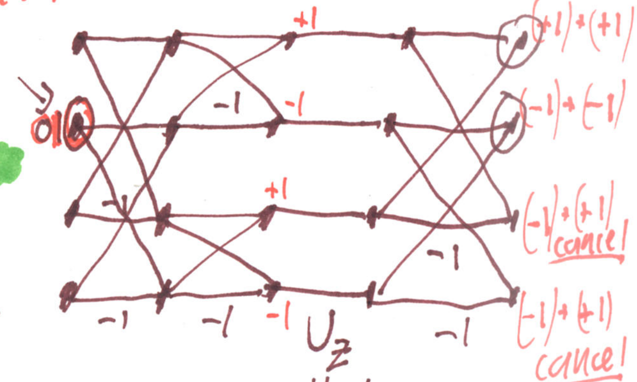
CSE 596 Lecture Fri Dec 7 Fall 2018

$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ "Schrödinger Style": Matrix Computation

Feynman-Style: Huge sum of scalar products

$N \times N = 2^n \times 2^n$ $\quad A \cdot B \cdot C[i,\ell] = \sum_{j=1}^{N} \sum_{k=1}^{N} A[i,j]B[j,k]C[k,\ell]$.





[The lecture went on to trace maze diagrams like the above from the text ch. 8 showing how cancellations owing to <u>interference</u> can be <u>targeted</u> to pile up the nonzero amplitude on to other nodes designated for acceptance. Depending on U_Z & U_F <u>vs.</u> U_{Id} & U_{NOT}, the amplitude piles up on the upper two nodes (qubit 1 = 0) vs. the lower two nodes. Getting such a "switcheroo" to reflect desired accept/reject criteria is the essence of designing quantum algorithms for decision problems. For functions $f(x) = y$ the simplistic goal is to pile up $(1-\varepsilon)$ amplitude on the outcome y, but what more often concretely happens is <u>sampling</u> from a distribution in which multiple outputs are possible.]

<u>Ch. 9</u> extends Deutsch's task from 1+1 qubits to $n+1$ qubits. Now it takes $2^{n-1}+1$ evaluations to conclusively tell whether $f(x_1, \ldots, x_n)$ is constant <u>versus</u> its being balanced (<u>presuming</u> it is one or the other) in a classical setting. But, a quantum setting starting with $H^{\otimes(n+1)}$ applied to $|0^n 1\rangle$. The final "1" picks up a minus sign that spurs cancellations. The effects are similar. <u>Points:</u>

- The "quantum advantage" is exponential in n (though the criterion is contrived).
- "Maze diagrams" don't <u>scale</u>, but the <u>linear</u> <u>algebra</u> calculations remain tractable.

Added: That was as far as I got (orally) in the lecture. The intended endpoint was Ch 10: Simon's Algorithm in which the two situations being distinguished are f is 1-to-1 vs. f is rectilinearly 2-to-1:

There is a "hidden vector" $s \in \{0,1\}^n$ such that for all vectors $y, z \in \{0,1\}^n$:

$$f(y) = f(z) \iff y = z \oplus s$$

bitwise XOR

If $s = 0^n$ then the RHS is $y = z$ so it says $f(y) = f(z) \iff y = z$ so f permutes $\{0,1\}^n$. Else f defines a "cleft" in $\{0,1\}^n$ in the following sense: $\{0,1\}^n = A \cup B$ such that $B = \{v \oplus s : v \in A\} =_{def} A \oplus s$ and f behaves identically (and injectively) on A vis-à-vis B. How quickly can we tell whether a given f has such a cleft?

Theorem:

- A classical randomized algorithm — with f given (previously known) only as a "black box" to get values $f(y)$ given binary y — needs exponential time to tell with high probability.

- Whereas a quantum algorithm can compute n equations defining s in expected time $O(n)$ iterations $\times$ $O(n)$ work per iteration. [D. Simon 1992]

This does not imply BQP $\neq$ BPP because of the black-box condition on how f is accessed — which even allows f to be non-computable! But it is the main proven result of that character. And it inspired Peter Shor to replace the initial $H^{\otimes n}$ Hadamard transform by the n-qubit Quantum Fourier Transform to see what happens... leading to Shor's quantum factoring algorithm [1993-94]. Taken together, can this "Quantum Advantage for Hidden Subgroups" phenomenon be understood further?