Quantum Information: lecture 3

- quantum key distribution — Preskill 4.2.2 or 4.5 (update)
- quantum algorithms — Preskill 6.3
- quantum error correction — Preskill 7.1

quantum key distribution

- there exists an unbreakable code: “one-time pad” — add a random bit string (shared key) to the message
- unpractical: the shared key can only be used once, and a new key must be exchanged securely (what if the key is intercepted and copied during transmission?)
- quantum key distribution relies on entanglement and the no-cloning theorem to ensure private exchange

Alice and Bob share a batch of entangled qubits $|\uparrow\rangle_A|\uparrow\rangle_B - |\downarrow\rangle_A|\downarrow\rangle_B$ and each measures $\hat{n}\cdot\sigma$ for randomly chosen orientations differing by 45°, as in the Bell test; violation of the Bell inequality guarantees that the entanglement has not been broken by an eavesdropper; the measurement outcomes for identical basis choices are perfectly correlated and establish a shared random key.

quantum algorithms (1)

Deutsch (1985) presented the first problem that can be solved more efficiently on a quantum computer:
the function $f : \{0, 1\} \mapsto \{0, 1\}$ is expensive to evaluate, find out if $f(0) = f(1)$ or $f(0) \neq f(1)$ in as few function calls as possible; classically, two calls are needed; a quantum computer needs only one single call.

Incorporate the function in the unitary two-qubit operation $U : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$;

apply U to the quantum superposition $(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$, which is transformed into $\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right](|0\rangle - |1\rangle)$ with a *single* call to f; then perform a Hadamard operation on the first qubit and measure it: the outcome is 0 if $f(0) = f(1)$ and 1 if $f(0) \neq f(1)$.

quantum parallelism effectively evaluates both $f(0)$ and $f(1)$ in a single function call

Deutsch-Josza: generalization to N qubits, with exponential speedup

quantum algorithms (2)

Shor's algorithm (1994) factors large numbers with exponential speedup on a quantum computer; the key ingredient is the period-finding subroutine (Simon's algorithm):

$f : \{0,1\}^N \to \{0,1\}^N$ has period a: $f(x) = f(y)$ if and only if $y = x \oplus a$; the problem is to find a; classically of order 2^N function calls are needed; a quantum computer finds a in order N calls.

use two registers of N qubits each, in a state represented by the binary number x ranging from 0 to $2^N - 1$; incorporate f in the unitary operator $U : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$; apply U to the superposition $\left(\sum_x |x\rangle\right)|0\rangle \mapsto \sum_x |x\rangle|f(x)\rangle$; measure the second register and find $f(X)$, resulting in the state $(|X\rangle + |X \oplus a\rangle)|f(X)\rangle$; perform a Hadamard on each qubit in the first register and measure; the outcome y satisfies $y \odot a \equiv y_1 a_1 \oplus y_2 a_2 \cdots \oplus y_N a_N = 0$; repeat N times and find a from the N linear equations.

Hadamard $|x\rangle \mapsto \prod_i \left(|0\rangle + (-1)^{x_i}|1\rangle\right) = \sum_y (-1)^{x \odot y}|y\rangle$

hence $|x \oplus a\rangle \to \sum_y (-1)^{(x\oplus a)\odot y}|y\rangle$ and $\left(|x\rangle + |x \oplus a\rangle\right) \mapsto \sum_{y \odot a = 0} |y\rangle$

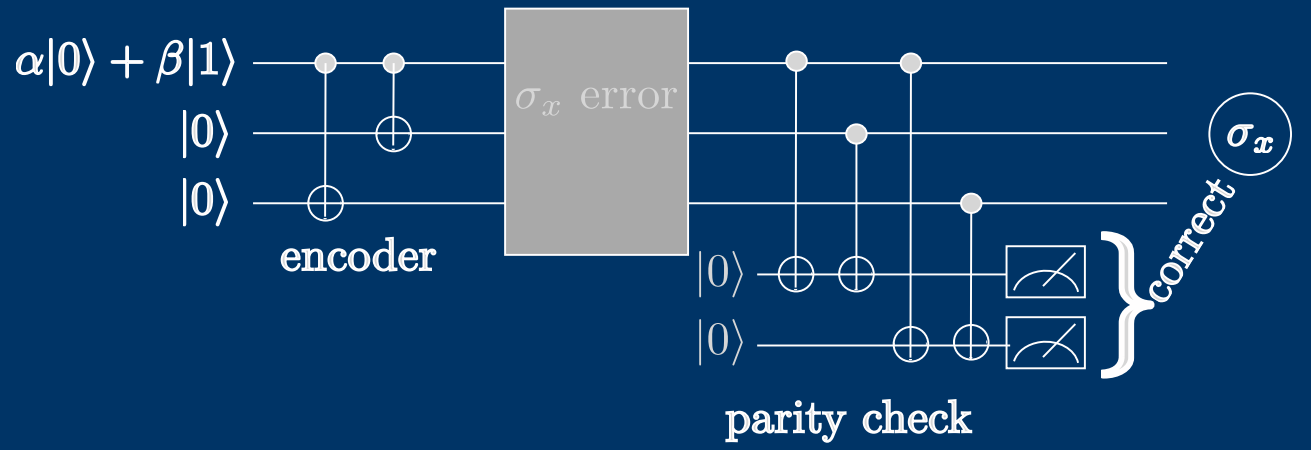
quantum error correction

If you cannot measure qubits without destroying them,
how to correct errors? *encode one qubit into three*

original: $\alpha|000\rangle + \beta|111\rangle$

damaged: $\alpha|010\rangle + \beta|101\rangle$

parity check tells you which spin has flipped, without knowing α
(so without measuring the qubit)



a three-qubit code can correct one σ_x error; a nine-qubit code can correct one error from an arbitrary Pauli matrix.