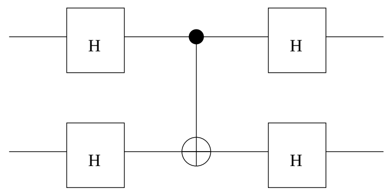
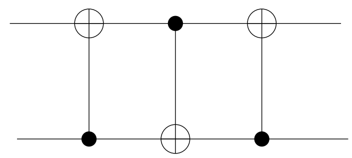
Homework 1

Out: August 27, 2007 **In:** September 10, 2007

1. **(Simple quantum circuits.)** In this exercise we warm up with some simple quantum circuits.

   (a) What do the following quantum circuits do?

   (b) Let X, Y, Z be the single qubit Pauli matrices, H be the single qubit Hadamard matrix and P be the single qubit phase gate. Observe that $HZH = X$ and $P^\dagger Y P = X$ (these identities will be important for error correction later on). Using these identities, implement controlled-Y and controlled-Z in terms of CNOT and single qubit gates.

2. **(Exponential of a matrix.)** Let A be an $n \times n$ complex matrix. Recall the definition of $e^A := \mathbb{1} + \frac{A}{1!} + \frac{A^2}{2!} + \cdots$ and the spectral norm $\|A\| := \max_{v:\|v\|=1} \|Av\|$.

   (a) Show that the Cauchy tail $\frac{A^n}{n!} + \cdots + \frac{A^m}{m!}$, $m > n$, m, n integers approaches the zero matrix as $n \to \infty$. One way to show this will be to first show that $\|B\| \to 0$ implies $B \to 0$ in the Frobenius distance for a matrix B, then show that the spectral norm of the Cauchy tail approaches zero. Use the fact that over complex numbers Cauchy convergence implies convergence to conclude that the series for e^A converges for any matrix A.

   (b) Prove the following third-order Trotter formula: If $\|A\| + \|B\| \le \delta \le 1$, then

   $$\|e^{A+B} - e^{B/2} e^A e^{B/2}\| \le 3\delta^3.$$

   You may use the inequalities $e^x - 1 - x - \frac{x^2}{2} \le \frac{x^3}{3}$, $e^x - 1 - x \le x^2$ and $e^x - 1 \le 2x$ for $0 \le x \le 1$ if you wish.

   (c) If we use the third-order Trotter formula for the universality construction, what size of a circuit will we get if we want to approximate a $2^n \times 2^n$ unitary U to within a spectral distance of ϵ?

3. **(Schrödinger equation and unitary evolution.)** Schrödinger equation describes the dynamics of an isolated quantum system in terms of a time-evolving Hermitian matrix called the *Hamiltonian*. For simplicity, assume that our quantum system has a finite dimensional Hilbert space. If $|\psi(t)\rangle$, $H(t)$ are the state vector and Hamiltonian of the system at time t, then Schrödinger equation says that

   $$\frac{d}{dt}|\psi(t)\rangle = -iH(t)|\psi(t)\rangle.$$

(a) Show that the time evolution is linear, that is, there is a time-evolving matrix $M(t)$ such that $|\psi(t)\rangle = M(t)|\psi(0)\rangle$. You may want to use the existence and uniqueness theorem for ordinary first order differential equations.

(b) A naive guess for $M(t)$ would be $M(t) = \exp(-i\int_0^t H(x)dx)$. Argue that this is wrong in general.

(c) Show that, nevertheless, $M(t)$ is a unitary matrix. One way to show this is to prove that for any two initial state vectors $|\psi(0)\rangle$, $|\phi(0)\rangle$, $\langle\psi(t)|\phi(t)\rangle = \langle\psi(0)|\phi(0)\rangle$ as can be seen by differentiating the left hand side with respect to t.

(d) Show that if the time evolution operator $M(t)$ of a quantum system is unitary, then its state vector must satisfy the Schrödinger equation for some Hamiltonian $H(t)$.

4. **(Goldreich-Levin problem.)** Let $a \in \{0,1\}^n$. Suppose we have a unitary oracle O_a on $n+1$ qubits behaving as follows:

$$|x\rangle|b\rangle \mapsto |x\rangle|b \oplus a \cdot x\rangle,$$

where $x \in \{0,1\}^n$, $b \in \{0,1\}$. Intuitively, only the oracle knows a and he reveals information about a in the above fashion. Oracles like these are an important theoretical tool in cryptography. The naive classical algorithm discovers a by querying O_a with the n standard basis vectors $|i\rangle$, $i = 1,\ldots,n$. It turns out that any classical algorithm requires $\Omega(n)$ queries to O_a in order to learn a with high probability. Show that there is a quantum algorithm that learns a exactly, making only one query to O_a.

5. **(Universal classical reversible computation.)** In this exercise, we shall see why single and two bit classical reversible gates cannot implement all functions $x \mapsto f(x)$, even with work bits and allowing garbage. We shall need the concept of an *affine function* on the vector space $\mathbb{F}_2^n$, where $\mathbb{F}_2$ is the field of integers modulo 2. An affine function is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ of the form $y \mapsto Ay + b$, where A is an $n \times n$ matrix over $\mathbb{F}_2$ and b, y are $n \times 1$ vectors over $\mathbb{F}_2$.

(a) Show that one and two-bit classical reversible gates are invertible affine functions on $\mathbb{F}_1$ and $\mathbb{F}_2$ respectively.

(b) Show that a circuit on n bits built out of one and two-bit classical reversible gates implements an invertible affine function on $\mathbb{F}_2^n$.

(c) Show that, in fact, all invertible affine functions on $\mathbb{F}_2^n$ can be implemented by circuits built out of NOT and CNOT gates.

(d) Show that the Toffoli gate cannot be realised by a circuit composed of one and two-bit classical reversible gates, even with work bits and allowing garbage.