MASSACHUSETTS INSTITUE OF TECHNOLOGY

Media Laboratory

MAS.961 Quantum Information Science September 11, 2001

Problem Set #1

(due in class, 27-Sep-01)

Instructions: You will be graded only on the *problems* (middle section, below). The *exercises* are for your own enlightenment and practice. Project *questions* need not be handed in; they are candidate questions which you may work on for your final project paper, due at the end of the semester.
Homework Policy: You are welcome to work with anyone else on the problem set, but please give them credit (i.e., list who you worked with on which problems). Cite any sources you use, but please don't look up the answer.

Lecture Topics (9/11, 9/13, 9/18, 9/20): Quantum circuits, QFT algorithms, quantum simulation

Recommended Reading: Nielsen and Chuang, Chapters 3-5

Exercises:

E1: (**Universal gate sets**) The Hadamard, phase, CNOT, and $\pi/8$ gates form a universal gate set. However, one of these gates is unnecessary. Which one, and why?

E2: (**Pauli operators and Bloch Sphere**) Compute the eigenvectors of the Pauli matrices, and find the points on the Bloch sphere which correspond to the normalized eigenvectors of the different Pauli matrices.

E3: Express the Hadamard gate H as a product of R_x and R_z rotations and $e^{i\phi}$ for some ϕ.

E4: An arbitrary single qubit unitary operator can be written in the form

$$U = \exp(i\alpha)R_{\hat{n}}(\theta) \tag{1}$$

for some real numbers α and θ, and a real three-dimensional unit vector $\hat{n}$.

1. Prove this fact.
2. Find values for α, θ, and $\hat{n}$ giving the Hadamard gate H.
3. Find values for α, θ, and $\hat{n}$ giving the phase gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \tag{2}$$

E5: (CNOT **action on density matrices**) The CNOT gate is a simple permutation whose action on a density matrix ρ is to rearrange the elements in the matrix. Write out this action explicitly in the computational basis.

E6: Find a circuit containing $O(n^2)$ Toffoli, CNOT and single qubit gates which implements a $C^n(X)$ gate (for $n > 3$), using no work qubits.

E7: Suppose ρ is the density matrix describing a two qubit system. Suppose we perform a projective measurement in the computational basis of the second qubit. Let $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ be the projectors onto the $|0\rangle$ and $|1\rangle$ states of the second qubit, respectively. Let ρ' be the density matrix which would be assigned to the system after the measurement by an observer who did not learn the measurement result. Show that

$$\rho' = P_0 \rho P_0 + P_1 \rho P_1 \,. \tag{3}$$

Also show that the reduced density matrix for the first qubit is not affected by the measurement, that is, $\mathrm{tr}_2(\rho) = \mathrm{tr}_2(\rho')$.

<u>**Problems:**</u>

P1: (**Composition of single qubit operations**) The Bloch representation gives a nice way to visualize the effect of composing two rotations.

(a) Prove that if a rotation through an angle β_1 about the axis $\hat{n}_1$ is followed by a rotation through an angle β_2 about an axis $\hat{n}_2$, then the overall rotation is through an angle β_{12} about an axis $\hat{n}_{12}$ given by

$$c_{12} = c_1 c_2 - s_1 s_2 \, \hat{n}_1 \cdot \hat{n}_2 \tag{4}$$

$$s_{12} \hat{n}_{12} = s_1 c_2 \hat{n}_1 + c_1 s_2 \hat{n}_2 - s_1 s_2 \, \hat{n}_2 \times \hat{n}_1 \,, \tag{5}$$

where $c_i = \cos(\beta_i/2)$, $s_i = \sin(\beta_i/2)$, $c_{12} = \cos(\beta_{12}/2)$, and $s_{12} = \sin(\beta_{12}/2)$.

(b) Show that if $\beta_1 = \beta_2$ and $\hat{n}_1 = \hat{z}$ these equations simplify to

$$c_{12} = c^2 - s^2 \, \hat{z} \cdot \hat{n}_2 \tag{6}$$

$$s_{12} \hat{n}_{12} = sc(\hat{z} + \hat{n}_2) - s^2 \, \hat{n}_2 \times \hat{z} \,, \tag{7}$$

where $c = c_1$ and $s = s_1$.

P2: (**Encoded universality**) In a particular physical system, the allowed interactions between fundamental units may not allow universal computation on those units. Nevertheless, it may still be possible to do universal computation on an *encoded subspace.* Consider a system of qubits that can be made to interact via the Hamiltonian $H_{jk} = J_{jk}(t) E_{jk}$, where $E_{jk} = \vec{\sigma}_j \cdot \vec{\sigma}_k$ and $J_{jk}(t)$ is a coupling that can be adjusted as a function of time. E_{jk} is known as the *exchange interaction.* Since the exchange interaction couples qubits, it cannot be used to perform single-qubit gates on the raw qubits.

(a) Consider a set of three qubits with pairwise exchange couplings. For convenience, we define the following operators:

$$H_0 = -\frac{1}{3}(E_{12} + E_{23} + E_{31}) \tag{8}$$

$$H_1 = \frac{1}{4\sqrt{3}}(E_{23} - E_{31}) \tag{9}$$

$$H_2 = i[H_1, H_3] \tag{10}$$

$$H_3 = \frac{1}{12}(E_{23} + E_{31} - 2E_{12})\,. \tag{11}$$

Calculate the commutators $[H_\alpha, H_\beta]$ for all α, β and summarize them concisely. Where have you seen these commutators before?

(b) Now define logical qubits as follows:

$$|0_L\rangle = \frac{1}{\sqrt{2}}(|010\rangle - |100\rangle) \tag{12}$$

$$|1_L\rangle = \frac{1}{\sqrt{6}}(2|001\rangle - |010\rangle - |100\rangle)\,. \tag{13}$$

Show that these states are eigenstates of the operator

$$S^2 = \frac{1}{4}(\vec{\sigma}_1 + \vec{\sigma}_2 + \vec{\sigma}_3) \cdot (\vec{\sigma}_1 + \vec{\sigma}_2 + \vec{\sigma}_3) \tag{14}$$

with eigenvalue $\frac{1}{2}(\frac{1}{2}+1)$. This means that these are states of total spin 1/2.

(c) Calculate the action of H_α on these logical qubits. What can you conclude about single-qubit rotations of the logical qubits?

(d) (Optional) Consider a pair of logical qubits. Show that some sequence of exchange interactions can be used to implement a nontrivial two-qubit gate.

P3: (**Quantum circuit for Hamming weight**) Construct a quantum circuit that performs the following unitary transformation:

$$|z\rangle|0\rangle \to |z\rangle|w(z)\rangle\,,$$

where $w(z)$ denotes the Hamming weight of z (the number of ones in its binary representation).

P4: (**Alternate universality construction**) Suppose U is a unitary matrix on n qubits. Define $H \equiv i\ln(U)$. Show that

(a) H is Hermitian, with eigenvalues in the range 0 to 2π.

(b) H can be written

$$H = \sum_g h_g g\,, \tag{15}$$

where h_g are real numbers and the sum is over all n-fold tensor products g of the Pauli matrices $\{I, X, Y, Z\}$.

(c) Let $\Delta = 1/k$, for some positive integer k. Explain how the unitary operation $\exp(-ih_g g\Delta)$ may be implemented using $O(n)$ one and two qubit operations.

(d) Show that

$$\exp(-iH\Delta) = \prod_g \exp(-ih_g g\Delta) + O(4^n\Delta^2)\,, \tag{16}$$

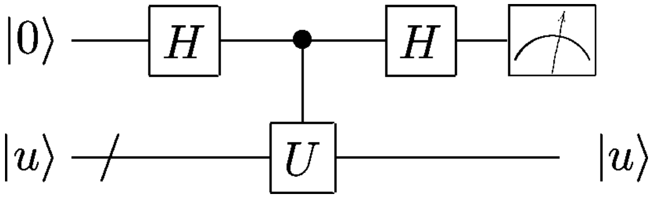
where the product is taken with respect to any fixed ordering of the n-fold tensor products of Pauli matrices, g.

(e) Show that

$$U = \left[\prod_g \exp(-ih_g g\Delta)\right]^k + O(4^n\Delta). \tag{17}$$

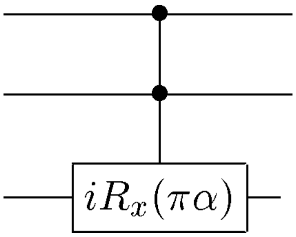
(f) Explain how to approximate U to within a distance $\epsilon > 0$ using $O(n16^n/\epsilon)$ one and two qubit unitary operations.

P5: (**Kitaev's algorithm**) Consider the quantum circuit



where $|u\rangle$ is an eigenstate of U with eigenvalue $e^{2\pi i\phi}$. Show that the top qubit is measured to be 0 with probability $p \equiv \cos^2(\pi\phi)$. Since the state $|u\rangle$ is unaffected by the circuit it may be reused; if U can be replaced by U^k, where k is an arbitrary integer under your control, show that by repeating this circuit and increasing k appropriately, you can efficiently obtain as many bits of p as desired, and thus, of ϕ. This is an alternative to the phase estimation algorithm.

P6: Show that the three qubit gate G defined by the circuit:



is universal for quantum computation whenever α is irrational. This gate is known as the Deutsch gate.

Project Questions:

Q1: (**Quantum compiling**) Write a classical computer program that takes as input a $2^n \times 2^n$ unitary matrix U and a desired precision ϵ and outputs a circuit that implements U to within precision ϵ. The circuit should use only Hadamard, $\pi/8$, phase, and controlled-NOT gates. The output could be in the form of a postscript file containing a picture of the circuit.

Resources: Nielsen and Chuang, Aram Harrow's thesis.

Q2: (**1.**) **Improving upon Solovay-Kitaev** The Solovay-Kitaev theorem gives an algorithm for approximating any unitary gate $U \in SU(N)$ out of a fixed set of base gates to a precision ϵ, using $\log^c(1/\epsilon)$ gates and with a running time polynomial in $\log(1/\epsilon)$. In Kitaev's paper, $c = 3$ and in Appendix C of Nielsen and Chuang, $c = \log 5/\log(3/2)$. Your challenge, should you choose to accept it, is to improve on c with a polytime algorithm, or even to come up with a novel polytime algorithm that has a comparable value of c.

Resources: Kitaev's paper "Quantum computations: algorithms and error correction," in Russ. Math. Surv. v.52, p.1191, 1997; Aram Harrow's thesis.

Q3: (**Nonabelian Fourier transform**) Find an algorithm for implementing the quantum Fourier transform over some particular nonabelian groups other than the symmetric group.

Resources: Beals, STOC 97.

Q4: (**2.**) **Finite-order Universal Gates** One of the homework problems asks you to prove that the $C^2R_x(\pi\alpha)$ gate is universal for all irrational α. However, the requirement that α be irrational is slightly stronger than necessary. Obviously $\alpha = 1$ is completely uninteresting by itself, and $\alpha = \frac{1}{2}$ is just a classical C^2NOT, but it is unknown which rational values of α lead to computationally universal gates. Certainly in $SU(2)$, the $T = e^{i\frac{\pi}{8}Z}$ and H gates are both finite order (8 and 2, respectively), but together are computationally universal, and TH is infinite order. (The *order* of a group element g is the smallest positive integer r such that $g^r = 1$. If $\alpha = p/q$ for $p, q \in \mathbf{Z}$, then $R_x(\pi\alpha)$ has order q, but if α is irrational then $R_x(\pi\alpha)$ has infinite order.) All these observations suggest a series of open problems.

(a) For which values of α is the gate $C^2R_x(\pi\alpha)$ *not* computationally universal?

(b) For which values of α is the set of gates $\{R_x(\pi\alpha), R_y(\pi\alpha), R_z(\pi\alpha)\}$ universal for a single qubit?

(c) Does there exist $\mathcal{G}$, a subgroup of $SU(2)$, such that $\mathcal{G}$ is dense and every element in $\mathcal{G}$ has finite order.?

(d) How about for $SU(N)$?

Q5: (**3.**) **Compiling with universal families of Hamiltonians** Although many families of Hamiltonians are known to be universal on encoded subsets, such as the example given in the homework of the exchange Hamiltonian acting on adjacent qubits, coming up with efficient methods of implementing basic gates with them is usually non-trivial. The general statement of the problem is as follows. Find an efficient algorithm that given Hamiltonians $H_1, \cdots, H_k$ acting on a d-dimensional Hilbert space, and $U \in SU(d)$, will express U as a product of a short sequence of terms of the form e^{-iH_jt}. Here, "efficient" means polynomial in k and d and "short" means that the sequence is not much longer than the optimal $O(d^2)$ construction, but given the difficulty of the problem, relaxing either of these terms for a novel algorithm is reasonable. There are many interesting variants of this problem, as well. One might also seek to minimize the total time that the Hamiltonians are applied, or (nearly equivalently) one might be able to apply any linear combination of the possible Hamiltonians. Another is to have the Hilbert space that we're compiling in be only an encoded subspace of a larger Hilbert space. A practical example of this is trying to construct a CNOT on encoded qubits by using the exchange operation.