1 Classical Computers

1 Give a reversible circuit to add two single-bit numbers x and y, giving the output as a two-bit number.

2 List all possible single-bit functions of a two-bit input x (so $f(x_1x_0)$ is 0 or 1 for each input). Give reversible circuit representations using the universal gate set $\{NOT, CNOT, CCNOT\}$ for all such functions with $f(00) = 0$. State a simple modification of these circuits to produce circuits for all such functions with $f(00) = 1$. Given that $\{NOT, CNOT\}$ is not a universal gate set, is it possible to construct all the functions without using CCNOT?

3 Give definitions of the complexity classes P, NP, PSPACE and EXP, and prove the inclusions $P \subseteq NP \subseteq PSPACE \subseteq EXP$.

2 Quantum Computers

4 Show that

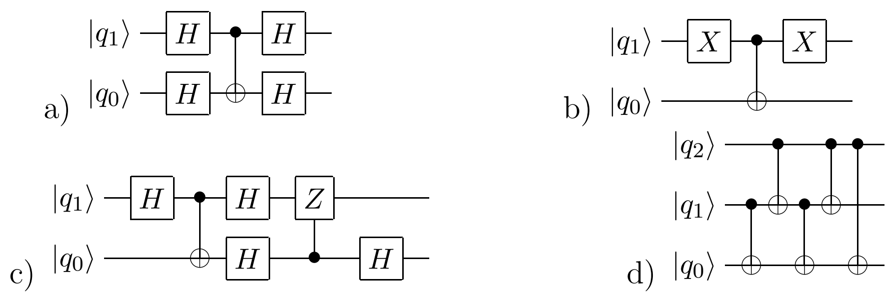
$$R_{\hat{n}}(\theta) = \cos(\theta/2)I - i\sin(\theta/2)(n_xX + n_yY + n_zZ),$$

where $\hat{n} = (n_x, n_y, n_z)$ is a unit vector in $\mathbb{R}^3$, is a unitary operator. Show that if a single qubit has the state

$$\hat{\rho} = \frac{1}{2}(I + \mathbf{r}\cdot\boldsymbol{\sigma}) = \frac{1}{2}(I + xX + yY + zZ),$$

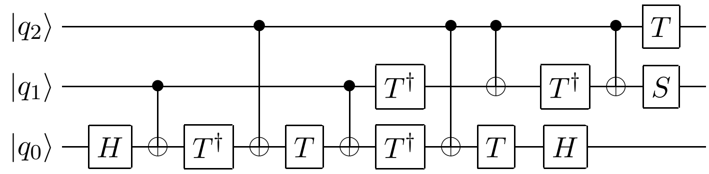
where $\mathbf{r} = (x, y, z)$ is a unit vector (that is, this is a pure state), then the effect of the unitary operator $R_{\hat{n}}(\theta)$ is to rotate $\mathbf{r}$ about the axis $\hat{n}$ in the Bloch sphere by an angle θ.

5 Compute the action of the circuits below on states in the computational basis. Give simpler equivalent circuits where possible.



6 Show that $S = \frac{1}{2}(1 + X_iX_j + Y_iY_j + Z_iZ_j)$ defines a swap operator, interchanging the state of qubits i and j.

7 By considering the action on computational basis states, show that the circuit given in lectures (and reproduced below) does implement the Toffoli gate (CCNOT).



8 Consider a two-qubit system. Construct a circuit to realise the operation $U = \begin{pmatrix} T & 0 \\ 0 & X \end{pmatrix}$, where T, X are the standard 2×2 matrices.

9 Consider a two-qubit system. Construct a circuit to realise the operation $U = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

10 Consider a two-qubit system. We wish to construct a circuit to realise the operation

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \end{pmatrix}$$

(a) First decompose this operator in terms of unitary operators U_1, U_2, U_3 which each act non-trivially on a two-dimensional subspace of the Hilbert space, $U = U_1 U_2 U_3$.

(b) Use CNOTs to convert the operators which do not act on a subspace corresponding to a single qubit into ones that do.

(c) Draw the resulting quantum circuit.

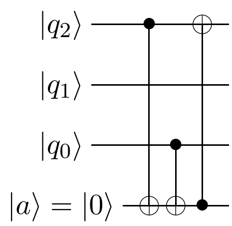
11 Defining the error $E(U, V) \equiv \max_\psi ||(U - V)|\psi\rangle||$, show that $E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\beta)) = \frac{1}{\sqrt{2}}|1 - e^{i(\alpha - \beta)}|$.

12 Delayed measurement: In the discussion of quantum teleportation, observers were often required to perform operations which depended on the result of a measurement. In a quantum circuit, we would represent such actions by performing a measurement on one qubit and then acting with a unitary on another if the result of the measurement was 1.

Show that such an operation can always be replaced by a controlled-unitary gate, with the measurement postponed to the end of the computation.

3 Error-correcting codes

13 Suppose three qubits were initially in some state $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$ in the usual code subspace for single qubit bit-flip error correction, and have subsequently become entangled with an environment, such that the joint state is $|e_1\rangle \otimes |\psi\rangle + |e_2\rangle \otimes X_2|\psi\rangle$. Show that the circuit below will return the qubits to their original state, transferring the entanglement with the environment to the ancillary qubit $|a\rangle$.



14 Construct a 3-qubit code subspace protecting against single phase errors, that is against the random action of Z on any single qubit, by showing that the error syndromes X_0X_1 and X_0X_2 will diagnose single phase errors, and finding their $+1$, $+1$ eigenspace.

15 In classical codes, greater redundancy reduces the risk of errors; if we have five bits for each logical bit, we are protected against two single bit errors. Consider the 5 qubit code $|\bar{0}\rangle = |00000\rangle$, $|\bar{1}\rangle = |11111\rangle$. Does this protect against any two single bit flip errors? Justify your answer.

16 Suppose we have a state $|\psi\rangle$ which was encoded using the Steane code, and we want to check whether a Y_2 error has acted on it. Identify an appropriate error syndrome to diagnose this error, and draw a quantum circuit to measure this syndrome.

17 How many distinct subspaces do we need to encode a single logical qubit to allow for recovery from independent single qubit errors acting on up to two qubits in an n-qubit system? What is the smallest number of qubits where such an encoding could exist?

18 Demonstrate that if we have two logical qubits encoded using the Steane code, $\overline{CNOT} = \prod_{i=1}^{7} CNOT_{ii}$ implements the CNOT operation on the logical qubits, where CNOT_{ii} is the CNOT operation between the ith physical qubit of the first codeword and the ith physical qubit of the second codeword.

Hint: This can be solved elegantly using the representation of the logical $|\bar{0}\rangle$ and $|\bar{1}\rangle$ in terms of the M_a.

19 We wish to construct a 5 qubit error correcting code.

(a) Show that

$$M_0 = Z_1X_2X_3Z_4, \quad M_1 = Z_0Z_2X_3X_4, \quad M_2 = X_0Z_1Z_3X_4, \quad M_3 = X_0X_1Z_2Z_4$$

are a good set of error syndromes, by showing that they all commute, and that the possible errors will map the $(+1, +1, +1, +1)$ eigenspace to distinct orthogonal subspaces.

(b) Find a basis for the $(+1, +1, +1, +1)$ eigenspace.

(c) Show that for an appropriate choice of encoding, $\bar{Z} = Z_0Z_1Z_2Z_3Z_4$ acts as Pauli Z on the logical qubit, and $\bar{X} = X_0X_1X_2X_3X_4$ acts as Pauli X on the logical qubit.

4 Quantum Algorithms

20 A general state of an n-qubit system can be written as

$$|\psi\rangle = \sum_{y=0}^{2^n-1} \psi(y)|y\rangle.$$

Find the condition on $\psi(y)$ for this to be a product state, so that

$$|\psi\rangle = \prod_{i=0}^{n} [a(i)|0\rangle + b(i)|1\rangle]$$

for some functions a, b.

21 Consider the Bernstein-Vazirani problem: Given a unitary operator U_f acting on n input bits x and one output bit m such that

$$U_f|x\rangle|m\rangle = |x\rangle|m \oplus f(x)\rangle,$$

where $f(x) = a \cdot x$, we want to find the value of a. Here $a \cdot x$ is the bitwise multiplication introduced in lectures, with $x \cdot y = x_{n-1}y_{n-1} \oplus \ldots \oplus x_0 y_0$, where $\oplus$ denotes addition mod 2 (or equivalently XOR when acting on single bit values).

(a) Describe how to construct a quantum circuit realising U_f for specific values of n and a. Illustrate this explicitly for $n = 5$ and $a = (10010)_2$.

(b) Using this quantum circuit and the result of question 5 a), or otherwise, show that

$$H^{\otimes(n+1)} U_f H^{\otimes(n+1)} |0\rangle_n |1\rangle_1 = |a\rangle_n |1\rangle_1.$$

Hence, using this quantum operation, we can learn the value of a with a single application of U_f.

22 Determine the action of U_{FT}^2. Hence show that $U_{FT}^4 = I$.

23 Give the inverse for U_{FT}, and give the explicit quantum circuit for the inverse for three qubits.

24 Consider the Quantum Fourier Transform, defined as the linear operator U_{FT} on an n qubit Hilbert space whose action on basis states $|x\rangle$, $x = 0, \ldots 2^n - 1$ is

$$U_{FT}|x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i xy/N} |y\rangle \ ,$$

where $N = 2^n$.

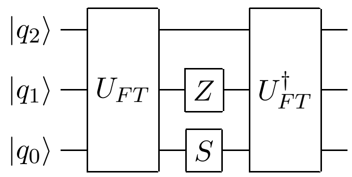
(a) Show that we can rewrite the transform as a product of states for the individual qubits,

$$U_{FT}|x\rangle = \frac{1}{2^{n/2}} \otimes_{l=0}^{n-1} [|0\rangle + \alpha_l |1\rangle],$$

where you should give a formula for the phases α_l.

(b) Show directly (that is, without assuming the unitarity of U_{FT}) that for $x \neq z$, $U_{FT}|x\rangle$ is orthogonal to $U_{FT}|z\rangle$.

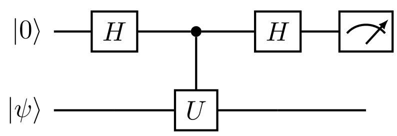
(c) Consider a 3-qubit system, and consider the unitary transform $U_{FT}^\dagger S_0 Z_1 U_{FT}$, represented by the quantum circuit below.



Show that this circuit implements the operation $x \to x + 2 \bmod 8$.

25 Suppose we have a unitary operator U on a one-qubit Hilbert space, with an eigenvector $|\psi\rangle$ such that $U|\psi\rangle = e^{2\pi i\varphi}|\psi\rangle$, and we want to find the phase φ.

(a) Show that if the qubit q_0 is initially set to 0, the measurement



produces a result 0 with probability $p = \cos^2(\pi\varphi)$.

(b) Find the probability for a 0 result when U is replaced by U^k. Hence give a procedure for estimating φ.

26 Find the period of the function $f(a) = y^a \bmod N$ for $N = 713$, for some y of your choosing (if the period is odd, choose again). Use the result to find a prime factor of N.

27 The diffusion operator is defined by

$$D = 2|\psi\rangle\langle\psi| - I,$$

where $|\psi\rangle = \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}|y\rangle$ is the uniform superposition of all the computational basis states.

(a) Show that D is a unitary operator.

(b) Show that the action of this operator on an arbitrary state $|\chi\rangle = \sum_x \chi_x|x\rangle$ is

$$D|\chi\rangle = \sum_x (2\bar{\chi} - \chi_x)|x\rangle,$$

where $\bar{\chi} = \frac{1}{2^n}\sum_x \chi_x$ is the average value of the coefficients. It is for this reason that D is also referred to as inversion about the mean.

(c) Construct a quantum circuit to realise this operator.

28 Suppose we have a quantum circuit implementing a unitary operator U such that $U|0\rangle = |\psi\rangle$. Using this, give a circuit implementing the operator

$$U_\psi = I - 2|\psi\rangle\langle\psi|.$$

29 Consider a function $f(x)$, where x is a 3-bit number, which has two values a_1, a_2 such that $f(a_1) = f(a_2) = 1$, and $f(x) = 0$ for all other values.

(a) The state

$$|\psi\rangle = H^{\otimes 3}|0\rangle = \frac{1}{\sqrt{8}} \sum_{i=0}^{7} |i\rangle$$

can be decomposed into a component $|\psi\rangle_a$ in the subspace $\mathcal{H}_a$ spanned by $|a_1\rangle$, $|a_2\rangle$, and a component $|\psi\rangle_\perp$ in the orthogonal subspace $\mathcal{H}_\perp$. Give explicit expressions for the unit normalised vectors

$$|a\rangle = \frac{|\psi\rangle_a}{\||\psi\rangle_a\|}, \quad |\perp\rangle = \frac{|\psi\rangle_\perp}{\||\psi\rangle_\perp\|}.$$

(b) Given a unitary U_f such that

$$U_f|x\rangle \otimes |m\rangle = |x\rangle \otimes |m \oplus f(x)\rangle,$$

where $|m\rangle$ is the state of a single ancillary qubit, construct an operation V which reflects vectors in the Hilbert space about the subspace $\mathcal{H}_\perp$. That is, if $|\chi\rangle = |\chi\rangle_a + |\chi\rangle_\perp$ with $|\chi\rangle_a \in \mathcal{H}_a$ and $|\chi\rangle_\perp \in \mathcal{H}_\perp$,

$$V|\chi\rangle = -|\chi\rangle_a + |\chi\rangle_\perp.$$

(c) Show that if we have a vector in the two-dimensional subspace spanned by $|a\rangle$ and $|\perp\rangle$, applying V and

$$D = 2|\psi\rangle\langle\psi| - I$$

rotates the state in this subspace, and find the rotation angle.

(d) Give an algorithm to use this rotation to find one of the special values a_1, a_2.

30 Generalise the Grover search algorithm to the case where the function $f(x)$ has more than one value where $f(x) = 1$; that is, to find one of a number of special items. If x has n digits and there are r special values, how many times should we apply the Grover iteration? How many searches will it typically take to find all the special values? [You can give estimations with the assumptions $N = 2^n \gg r \geq 1$.]