TA session – Day 2

1 More basics about circuits

Exercise 1. Show that the circuit in Fig. 1 implements quantum teleportation of a single qubit state $|\psi\rangle$ from qubit 1 to qubit 3. In other words, verify that the output state on the right hand side is equal to the input $|\psi\rangle$.

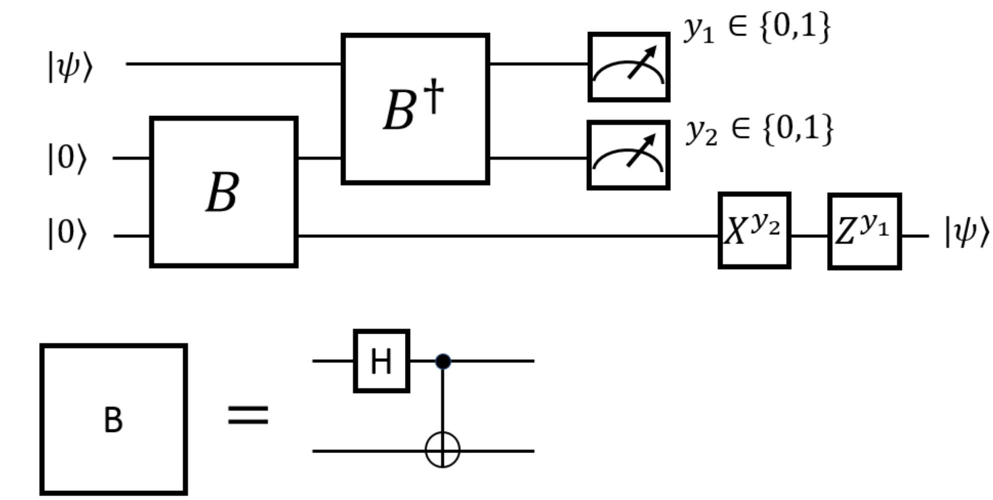

Figure 1: Teleportation

Exercise 2 (Clean computation)**.** Prove that if a function $f : \{0,1\}^n \longmapsto \{0,1\}$ can be computed using a classical circuit with m elementary gates, then the unitary corresponding to the *clean* computation of f,

$$(x, b) \longmapsto (x, b \bigoplus f(x))$$

for $x \in \{0,1\}^n, b \in \{0,1\}$, can be generated by a quantum circuit which uses only $O(m)$ elementary gates.

Exercise 3 (Pauli basis and Quantum One-Time Pad)**.** Show that the 2^{2n} tensor products of the Pauli σ_X and σ_Z matrices form an orthonormal basis for the complex vector space of $2^n \times 2^n$ matrices, equipped with the trace inner product. By expanding an arbitrary n-qubit density matrix ρ in this basis, deduce that

$$\frac{1}{2^{2n}} \sum_{k=(a,b)} E_k(\rho) \;=\; \frac{1}{2^n}\,\mathrm{Id}\,,$$

where $E_{(a,b)}(\rho) = (X^a Z^b)\rho(X^a Z^b)^\dagger$.

Exercise 4 (Gate application using magic states)**.** Define the single-qubit state

$$|\pi/4\rangle = T|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\pi/4}}{\sqrt{2}}|1\rangle \ . \tag{1}$$

Verify that the circuit indicated in Figure 2 has the claimed effect, for any single-qubit state $|\psi\rangle$ provided as the second input. (Recall P is the phase gate, such that $T^2 = P$ and $P^2 = Z$.) Next, suppose that instead of

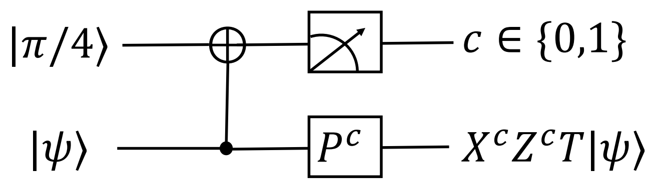

Figure 2: Teleporting into a T gate.

being applied directly to the state $|\psi\rangle$, the circuit is applied to an encrypted version of $|\psi\rangle$, $\sigma_X^a \sigma_Z^b |\psi\rangle$. Show that the outcome of the circuit is then $P^a \sigma_X^{a'} \sigma_Z^{a'} T|\psi\rangle$, for some bits a' and b' depending on a, b and c.
[Note: this circuit is used in many protocols for delegation. The circuit can be applied directly by the server on authenticated qubits, provided the authentication code allows for transversal computation of Clifford gates. A classical interaction is required to allow the server to apply the right P gate correction, as it depends on the verifier's private one-time pad keys.]

2 Hamiltonians, QMA and phase estimation

Exercise 5. Show that the state $|\text{🐱}\rangle = (|0\rangle^{\otimes n} + |1\rangle^{\otimes n})/\sqrt{2}$ cannot be the *unique* ground-state of any local Hamiltonian. (Hint: local measurements can't detect global sign-flips.)

Exercise 6 (Measuring the energy of a local Hamiltonian)**.** Suppose H_0 is a local Hamiltonian such that (for convenience) $0 \le H_0 \le I$. Suppose we are given one of its eigenstates $|\psi\rangle$. That is, $H_0|\psi\rangle = E|\psi\rangle$ for some unknown $E \in [0, 1]$. Show how to use the circuit shown in Fig. 3 to compute an estimate of $\cos^2(Et/2)$ which lies within a given additive error ϵ with high probability. The middle gate is a controlled

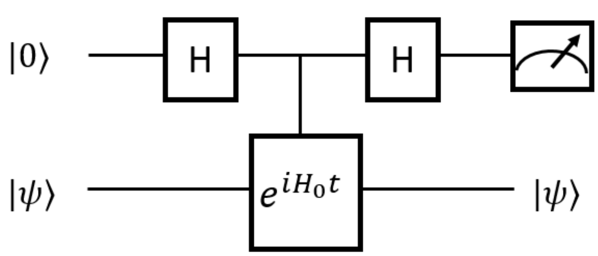

Figure 3: Circuit used to measure energy.

Hamiltonian evolution which can be implemented using the known efficient algorithms for Hamiltonian simulation which we discussed in class.

Exercise 7. (QMA amplification) In the lecture about QMA, it was mentioned that if the gap between completeness c and soundness s is at least $|c-s| \geq 1/\operatorname{poly}(n)$ then it can be amplified efficiently so that $c > 1 - 1/\exp(n)$, $s < 1/\exp(n)$. Prove this claim.

Exercise 8 (Measuring a local Hamiltonian)**.** Recall that any Hermitian matrix can be written as a sum

$$H = \sum_j \lambda_j |\alpha_j\rangle\langle\alpha_j|.$$

Consider such a matrix acting on qubits $1 \ldots k$, and suppose that λ_j are all between 0 and 1. Let T be a unitary matrix satisfying:

$$T|\alpha_j\rangle|0\rangle = |\alpha_j\rangle(\sqrt{\lambda_j}|0\rangle + \sqrt{1-\lambda_j}|1\rangle)$$

(Note that you can complete T to act on the rest of the space so that it is unitary). Show that measuring the last qubit of $T(|\psi\rangle \otimes |0\rangle)$ gives outcome 0 with probability

$$Pr(0) = \langle\psi|H|\psi\rangle.$$