M526/P623 Quantum Computation Ninnat Dangniam

Homework Assignment 2

45 points DUE: 23 Dec 2024

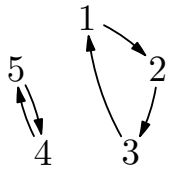
1. Reversible computation from Toffoli gates (20 points).

The goal of the first parts of this exercise is to show that Toffoli gates suffice to simulate any circuit *without* relying on the universality of AND and NOT, but directly using the fact that any reversible circuit is a permutation of bitstrings. Since we can employ the uncomputation trick to compute any irreversible function by a reversible circuit, it suffices to focus on constructing reversible circuits from Toffoli gates.

The *permutation group* S_N (also called the *symmetric group*) on N objects is a group with $N!$ elements, each of which rearranges N ordered objects into a different order (except the identity permutation). We can express an element $\sigma \in S_N$ in several ways. In the two-line notation,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

means a permutation composed of two disjoint cycles: $1 \to 2 \to 3 \to 1$ and $4 \to 5 \to 4$. A better notation would be



or more compactly: (123)(45). In general, $(a_1 a_2 \cdots a_l)$ is a cycle of length l. Cycles of length 2 are given a special name, *transpositions*. It is a fact that every permutation can be expressed as, not only a product of disjoint cycles, but also a product of transpositions. In other words, transpositions generate the group S_N.

In the lectures, we argued that $\Lambda^3(X)$ can't be created from $\Lambda^2(X)$ without using an ancilla qubit because $\Lambda^3(X)$ is an odd permutation of 4-bit strings, whereas $\Lambda^2(X)$ is an even permutation on 4-bit strings. So let us first formalize the concept of the parity of a permutation.

(a) Consider the action of S_N on the polynomial

$$\Delta = \prod_{1 \le j < k \le N} (x_k - x_j)$$

of N unknowns $x_1, \ldots x_N$ by permuting the subscripts:

$$f_\sigma(\Delta) = \prod_{1 \le j < k \le N} (x_{\sigma(k)} - x_{\sigma(j)}).$$

For example, for $N = 4$, the polynomial would be

$$\Delta = (x_2 - x_1)(x_3 - x_1)(x_4 - x_1)(x_3 - x_2)(x_4 - x_2)(x_4 - x_3).$$

f_σ acting on Δ always returns Δ up to a sign:

$$f_\sigma(\Delta) = (-1)^p \Delta. \tag{1}$$

p, being even or odd, is the *parity* of the permutation.

Show that $f_\sigma \circ f_\rho = f_{\sigma\rho}$ for all $\sigma, \rho \in S_N$. Also show that if σ is a transposition, then $f_\sigma(\Delta) = -\Delta$. Then conclude that parity is well defined. That is, a given permutation is either even or odd, but not both.

(b) If we think of a permutation as an N-by-N matrix acting on a vector of indices $1 \le j \le N$, what would be the matrix function that corresponds to the parity?

Now let us specialize the discussion to our scenario. Any reversible circuit is a permutation of bistrings. For example, the Toffoli gate on 3-bit strings is an odd permutation (110 111). In particular, it is an example of a transposition that changes the Hamming weight of the bitstrings by 1. For any given transposition, we say that it is a *Hamming-weight-s* transposition if it exchanges bitstrings whose Hamming weights differ by s.

(c) Show that any Hamming-weight-s transposition can be written as a product of Hamming-weight-1 transpositions.

(d) Given a Hamming-weight-1 transposition, write down a circuit composed of TOFFOLI and NOT that produces the transposition.

For the rest of this exercise, we will think about the space cost, i.e. the number of ancilla qubits, of constructing multiply-controlled gates from Toffoli gates.

(e) Use $n-3$ ancilla qubits, all set to 0 at the beginning and return to the value 0 at the end, to construct $\Lambda^{n-1}(X)$ from $O(n)$ $\Lambda^2(X)$ gates.

(f) Use $n-3$ ancilla qubits, which can be set to any value at the beginning and return to that value at the end, to construct $\Lambda^{n-1}(X)$ from $O(n)$ $\Lambda^2(X)$ gates.

(g) Construct $\Lambda^{n-1}(X)$ from $\Lambda^2(X)$ using only one ancilla qubit. How many $\Lambda^2(X)$ did you use?

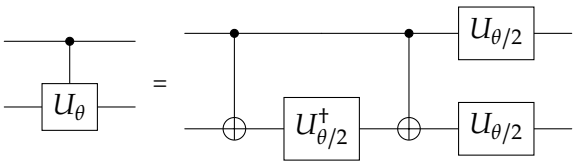
---

2. Controlled unitaries from CNOT and single-qubit gates (10 points).

Define

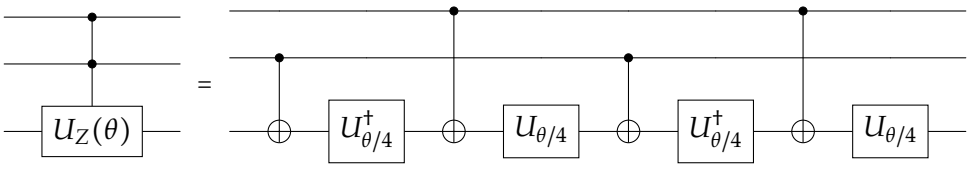
$$U_Z(\theta) \equiv e^{-iZ\theta/2}, \qquad\qquad U_\theta \equiv e^{i\theta/2} U_z(\theta) \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

(a) Using the identity, $U_z(\theta) = X U_z^\dagger(\theta) X$, show the following circuit identity:



Specialize this circuit to controlled-Z and controlled-S gates.

(b) Using the same approach as in **(a)**, show the following circuit identity:

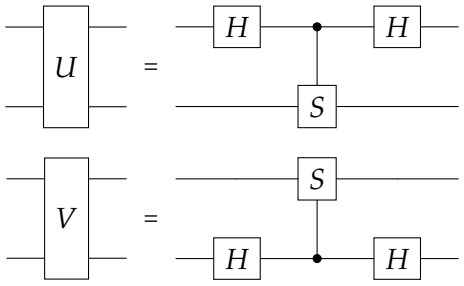


Generalize the circuit identity to construct $\Lambda^2(U_\theta)$, and then specializing to $\Lambda^2(Z)$ and construct a circuit for the Toffili gate.

---

3. $\{H, \Lambda(S)\}$ **is universal (10 points).**

(a) Consider the two-qubit unitaries U and V defined by the following circuits.



Show that both U and V act trivially on the states $|00\rangle$ and $(|01\rangle + |10\rangle + |11\rangle)/\sqrt{3}$.

(b) Thus, U and V act nontrivially only in the two-dimensional subspace spanned by the vectors $(|01\rangle - |10\rangle)/\sqrt{2}$ and $(|01\rangle + |10\rangle - 2|11\rangle)/\sqrt{6}$. Write down the matrix forms for U and V in this basis.

(c) Show that U and V can be written in the form

$$e^{i\pi/4}\left(\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}\,\hat{\mathbf{n}}\cdot\sigma\right).$$

What is the unit vector $\hat{\mathbf{n}}$ for each unitary?

(d) Construct the transformation $V^{-1}U$. (Note that V^{-1} can be constructed from H and $\Lambda(S)$.) Show that it produces a rotation with half-angle $\theta/2$ in the two-dimensional subspace spanned by the basis in **(b)**, where $\cos(\theta/2) = 1/4$.

As it turns out, the angle θ is not a rational multiple of π. Equivalently, $e^{i\theta/2}$ is not a root of unity; there is no finite integral power n such that $(e^{i\theta/2})^n = 1$. It follows that powers of $V^{-1}U$ are dense in a U(1) subgroup of SU(4). Similar reasoning shows that UV^{-1} is dense in another U(1) subgroup about a different axis. Products of elements of these two noncommuting U(1) are dense in the SU(2) subgroup that contains both U and V.

Going further, conjugating $V^{-1}U$ and UV^{-1} by $\Lambda(S)$, and taking products of these unitaries produce a dense subset in another SU(2), acting on the span of $(|01\rangle - |10\rangle)\sqrt{2}$ and $(|01\rangle + |10\rangle - 2i|11\rangle)/\sqrt{6}$. Together, these two SU(2) produce the whole SU(3) subgroup that acts on the three-dimensional space orthogonal to $|00\rangle$. Conjugating this SU(3) by $H^{\otimes 2}$ we obtain another SU(3)

acting on the three-dimensional space orthogonal to $|{+}{+}\rangle$. The only subgroup of SU(4) that contains both of these SU(3) subgroups is SU(4) itself. Thus, H and $\Lambda(S)$ suffice to approximate any two-qubit gate to any accuracy.

---

4. Encoded universality (5 points).

The Toffoli gate $\Lambda^2(X)$ is universal for reversible classical computation. What must be added to realize the full power of quantum computing? It turns out that just H and $\Lambda^2(X)$ suffice to efficiently simulate any quantum computation. Note however that this doesn't imply that H and $\Lambda^2(X)$ can generate an arbitrary unitary operation since H and $\Lambda^2(X)$ contain only real entries. What happens is that an n-qubit system is isomorphic to an $(n+1)$-*rebit* system (a 2^{n+1}-dimensional real vector space). Here is how to realize this isomorphism:

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} c_x |x\rangle \longleftrightarrow |\tilde{\psi}\rangle = \sum_{x\in\{0,1\}^n} (\mathrm{Re}(c_x)|x\rangle|0\rangle + \mathrm{Im}(c_x)|x\rangle|1\rangle).$$

Denote the real encoding of a unitary transformation U by $\widetilde{U}$, with the action

$$\begin{aligned}\widetilde{U} : |x\rangle|0\rangle &\mapsto \mathrm{Re}(U)|x\rangle|0\rangle + \mathrm{Im}(U)|x\rangle|1\rangle \\ |x\rangle|1\rangle &\mapsto -\mathrm{Im}(U)|x\rangle|0\rangle + \mathrm{Re}(U)|x\rangle|1\rangle\end{aligned}$$

Construct the real gate $\Lambda^2(XZ)$ from H and TOFFOLI, and verify that $\widetilde{\Lambda(S)} = \Lambda^2(XZ)$. This together with the result of **Problem 3** imply that H and $\Lambda^2(X)$ suffice to simulate any unitary operations.

Thus, we see that the Toffoli gate doesn't need much help to unleash the power of quantum computing. In fact, the Hadamard gate can be replaced by any single-qubit gate that doesn't preserve the computational basis.

Reversible classical computation + Change of basis = Quantum computation