M526/P623 Quantum Computation *Lecturer: Ninnat Dangniam*

Homework Assignment 3

DUE: 13 Jan 2025 35 points

For the first two problems, you may use the result of Exercise 4.15 of Nielsen and Chuang. In particular, if a Z rotation U_κ by an angle κ is followed by a rotation $U_\kappa(\hat{\mathbf{n}})$ by the same angle but about a different axis $\hat{\mathbf{n}}$, then the overall rotation is by an angle κ' about an axis $\hat{\mathbf{n}}'$ given by

$$\begin{aligned}\cos\bigl(\kappa'/2\bigr) &= \cos^2(\kappa/2) - \sin^2(\kappa/2)\,\hat{\mathbf{z}}\cdot\hat{\mathbf{n}},\\ \sin\bigl(\kappa'/2\bigr)\hat{\mathbf{n}}' &= \sin(\kappa/2)\cos(\kappa/2)(\hat{\mathbf{z}}+\hat{\mathbf{n}}) - \sin^2(\kappa/2)\,\hat{\mathbf{n}}\times\hat{\mathbf{z}}.\end{aligned}$$

1. Two-qubit entangling gates (10 points).

We say that a two-qubit unitary quantum gate is *local* if it is a tensor product of single-qubit gates, and that the two-qubit gates U and V are *locally equivalent* if one can be transformed to the other by local gates:

$$V = (A\otimes B)U(C\otimes D).$$

It turns out that every two-qubit gate is locally equivalent to a gate of the form

$$V(\theta_x,\theta_y,\theta_z) = \exp\bigl[i(\theta_x X\otimes X + \theta_y Y\otimes Y + \theta_z Z\otimes Z)\bigr],$$

where $-\pi/4 < \theta_x \le \theta_y \le \theta_z \le \pi/4$.

(a) Show that up to an overall phase, $V(\pi/4,\pi/4,\pi/4)$ is the SWAP gate.

(b) Show that $V(0,0,\pi/4)$ is locally equivalent to the CNOT gate. Generalize the result to show that $V(0,0,\theta)$ is locally equivalent to the controlled rotation $\Lambda[e^{-2i\theta(\hat{\mathbf{n}}\cdot\sigma)}]$ by an angle 4θ about an arbitrary axis of rotation.

(c) Show that

$$\begin{aligned}(\mathbb{1}\otimes X)V(\theta_x,\theta_y,\theta_z)(\mathbb{1}\otimes X)V(\theta_x,\theta_y,\theta_z) &= V(2\theta_x,0,0),\\ (\mathbb{1}\otimes Y)V(\theta_x,\theta_y,\theta_z)(\mathbb{1}\otimes Y)V(\theta_x,\theta_y,\theta_z) &= V(0,2\theta_y,0),\\ (\mathbb{1}\otimes Z)V(\theta_x,\theta_y,\theta_z)(\mathbb{1}\otimes Z)V(\theta_x,\theta_y,\theta_z) &= V(0,0,2\theta_z).\end{aligned}$$

(d) Consider a two-qubit gate U locally equivalent to $V(\theta_x,\theta_y,\theta_z)$. Assume that U does not belong to the following special cases:

1. $\theta_x = \theta_y = \theta_z = 0$ (i.e., U is local),
2. $\theta_x = \theta_y = \theta_z = \pi/4$ (i.e., U is locally equivalent to SWAP).

Show that a CNOT gate can be implemented using U gates and single-qubit gates. (**Hint:** Use the result of Exercise 4.15 of Nielsen and Chuang.)

2. Solovay-Kitaev theorem for SU(2) (10 points).

Denote by $D(U,V) = \|U - V\|_{\text{op}}$ the distance between operators U and V, where $\|A\|_{\text{op}}$ is the operator norm of A. For convenience, let us also define the group commutator $[[V,W]] \equiv VWV^{-1}W^{-1}$. We have seen that errors of composing unitary operations add linearly in general; if $D(U,\widetilde{U}) = D(V,\widetilde{V}) = \epsilon$, then $D(UV,\widetilde{U}\widetilde{V}) \leq 2\epsilon$. But if the unitaries being composed have structure, we may have error cancellation and get a better-than-expected error. This is the crux of the Solovay-Kitaev theorem.

(a) Show that if V and W are unitary operators with $D(\mathbb{1},V), D(\mathbb{1},W) \leq \epsilon$, then $D(\mathbb{1},[[V,W]]) \leq 2\epsilon^2$. This means that, given the ability to construct a unitary near the identity with accuracy ϵ, we can always construct another unitary near the identity with an improved accuracy $2\epsilon^2$.

For the rest of the problem, we specialize to the qubit case. Let $U = e^{-i\theta\hat{\mathbf{n}}\cdot\sigma/2} \in \mathrm{SU}(2)$. For a Hermitian operator A with eigenvalues $\{a\}$, we saw in the lectures that

$$D(\mathbb{1},e^{iA}) = \max_{\{a\}} 2\sin\left(\frac{|a|}{2}\right).$$

This translates to $D(\mathbb{1},U) \leq 2\sin(\theta/4) = \theta/2 + O(\theta^3)$. Our goal is to find V and W such that $U = [[V,W]]$ and such that $D(\mathbb{1},V), D(\mathbb{1},W) \leq C\sqrt{\theta}$ for some constant C.

(b) Suppose that V is a rotation by ϕ about the Z axis, and W is a rotation by the same angle ϕ about the Y axis. Show that the group commutator $[[V,W]]$ is a rotation by an angle θ satisfying

$$\sin(\theta/2) = 2\sin^2(\phi/2)\sqrt{1-\sin^4(\phi/2)}.$$

(**Hint:** You may use the result of Exercise 4.15 of Nielsen and Chuang.)

(c) Using the result of **(b)**, devise a strategy to find V and W such that $U = [[V,W]]$ and such that $D(\mathbb{1},V), D(\mathbb{1},W) \approx \sqrt{\theta/2}$.

---

3. Phase kickback with qudits (5 points): Moore and Mertens 15.31 (p.896).

4. Fast Fourier transform (10 points).

The Quantum Fourier transform (QFT) on n qubits is a unitary operator defined in the standard (position) basis $\{|j\rangle, j = 0,\ldots,N-1\}$ by

$$F|j\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle,$$

where $N = 2^n$. Since j and k are n-bit numbers, i.e.,

$$j = j_1\ldots j_n.0 = \sum_{l=1}^{n} j_l 2^{n-l}, \qquad k = k_1\ldots k_n.0 = \sum_{l=1}^{n} k_l 2^{n-l},$$

we can write the Fourier coefficients as

$$e^{2\pi ijk/N} = \prod_{l=1}^{n} e^{2\pi ik_l j/2^l} = \prod_{l=1}^{n} e^{2\pi ik_l 0.j_{n-l+1}\cdots j_n}. \tag{1}$$

This allows us to put the QFT in the form

$$F|j\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} |k_l\rangle\, e^{2\pi i k_l 0.j_{n-l+1}\cdots j_n} = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i 0.j_{n-l+1}\cdots j_n} |1\rangle\right),$$

which is suitable for translation into an efficient quantum circuit that performs the QFT in $O(n^2)$ elementary gates.

Applying the QFT to a state $|\psi\rangle = \sum_j x_j |j\rangle$ changes the amplitudes in the standard basis according to

$$y_j = \langle j|F|\psi\rangle = \sum_{k=0}^{N-1} \langle j|F|k\rangle\, x_k = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} x_k.$$

This transformation is called the discrete Fourier transform (DFT). Of course, the QFT doesn't compute the DFT, i.e., compute the output amplitudes y_k; it just transforms amplitudes according to the DFT.

To compute the DFT involves taking the matrix product of a $N \times N$ matrix and a N-dimensional input vector. A naïve approach to this matrix multiplication requires evaluating $O(N^2)$ products. **Use the identity (1) above to devise an algorithm for computing the DFT using only $O(nN)$ elementary multiplications.** This algorithm, indispensable for practical applications of Fourier transform, is called the fast Fourier transform(FFT). (The discovery of FFT is generally credited to the work of James Cooley and John Tukey published in 1965, but the idea of FFT can be traced back to an 1805 unpublished work by Gauss.)