Worksheet 6: Universality and Quantum Circuits II

Quantum Computation and Error Correction

Suggested time: 150 minutes — Reading: Nielsen & Chuang §4.2–4.5

Teaching assistant: Sarthak Girdhar (sarthak.sarthak@unibas.ch)

To be discussed on **October 27, 2026**.

Conventions. As in Worksheet 5: qubits are numbered from 0, $|ab\rangle$ means qubit 0 is in state a, and $P_0 = |0\rangle\langle 0| = \frac{1}{2}(\mathbb{I} + Z)$, $P_1 = |1\rangle\langle 1| = \frac{1}{2}(\mathbb{I} - Z)$. A circuit "first G_1, then G_2" is the matrix $G_2 G_1$.

The gate toolkit.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = T^2, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \qquad |\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}.$$

Rotations. For a unit vector $\hat{n}$ and $\hat{n} \cdot \vec{\sigma} = n_x X + n_y Y + n_z Z$,

$$R_{\hat{n}}(\theta) = \exp\Big(-\tfrac{i\theta}{2}\, \hat{n} \cdot \vec{\sigma} \Big), \qquad R_x(\theta) = e^{-i\theta X/2}, \quad R_y(\theta) = e^{-i\theta Y/2}, \quad R_z(\theta) = e^{-i\theta Z/2}.$$

This is the convention of Nielsen & Chuang and of Qiskit's `rx`, `ry`, `rz`. Beware: some notes use the opposite sign in the exponent.

Two-qubit and three-qubit gates. $\texttt{cx}(a, b) = P_0 \otimes \mathbb{I} + P_1 \otimes X$ (control a, target b); `cz` likewise with Z; controlled-U is $P_0 \otimes \mathbb{I} + P_1 \otimes U$; $\texttt{ccx}(a, b, c)$ is the Toffoli gate, which flips qubit c iff qubits a and b are both 1; `ccz` multiplies by -1 iff all three qubits are 1.

Timing guide: Part A ≈ 50 min Part B ≈ 55 min Part C ≈ 45 min.

Part A — Single-qubit gates and rotations

1. Rotations of a single qubit.

(a) Using $(\hat{n} \cdot \vec{\sigma})^2 = \mathbb{I}$ and the power series of the exponential, show that

$$R_{\hat{n}}(\theta) = \cos\tfrac{\theta}{2}\, \mathbb{I} - i \sin\tfrac{\theta}{2}\, \hat{n} \cdot \vec{\sigma}.$$

(b) Write $R_z(\theta)$ as a diagonal matrix. Hence show that, up to a global phase factor, $Z = R_z(\pi)$, $S = R_z(\pi/2)$ and $T = R_z(\pi/4)$, and give the phase factor in each case.

(c) Write $R_y(\pi/2)$ as a matrix and show that $H = R_y(\pi/2)\, Z$ exactly. Conclude that $H = e^{i\pi/2} R_y(\pi/2) R_z(\pi)$.

(d) Why do we regard $e^{i\alpha}U$ and U as *the same gate*? Give the one-line argument in terms of measurement probabilities. (We will see in Q4(c) that this is no longer true when the gate is *controlled*.)

2. The Z–Y–Z decomposition.

The claim: every single-qubit gate can be written as

$$U = e^{i\alpha}\, R_z(\beta)\, R_y(\gamma)\, R_z(\delta)$$

for some real $\alpha, \beta, \gamma, \delta$. This is the whole "single-qubit" part of universality: three rotations about two fixed axes are enough.

(a) Multiply out and show that

$$R_z(\beta)R_y(\gamma)R_z(\delta) = \begin{pmatrix} e^{-i(\beta+\delta)/2}\cos\frac{\gamma}{2} & -e^{-i(\beta-\delta)/2}\sin\frac{\gamma}{2} \\ e^{i(\beta-\delta)/2}\sin\frac{\gamma}{2} & e^{i(\beta+\delta)/2}\cos\frac{\gamma}{2} \end{pmatrix}.$$

(b) Let $U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ be any 2×2 unitary. Using only that its columns are orthonormal, show that $(c, d) = e^{i\varphi}(-\bar{b}, \bar{a})$ for some real φ, and hence that

$$U = e^{i\alpha}\begin{pmatrix} a' & -\bar{b}' \\ b' & \bar{a}' \end{pmatrix} \qquad \text{with } |a'|^2 + |b'|^2 = 1.$$

(c) Compare (a) and (b): explain how to read off γ from $|a'|$, and β and δ from the phases of a' and b'. This proves the claim.

(d) Find $(\alpha, \beta, \gamma, \delta)$ for $U = H$. *Hint: Q1(c) has already done the work.*

3. A discrete gate set: H and T. A real device cannot implement $R_y(\gamma)$ for a continuum of angles γ with perfect precision, and fault-tolerant schemes work with a *finite* set of gates. The standard choice is the Clifford gates (H, S, `cx`) plus T.

(a) Compute $TXT^\dagger$ and show it equals $(X + Y)/\sqrt{2}$. In Worksheet 5 a Clifford gate was defined as one that maps every Pauli to a Pauli (up to sign). Conclude that T is *not* a Clifford gate.

(b) Show that $HTH = e^{i\pi/8}R_x(\pi/4)$. *Hint: $HZH = X$, and H can be moved inside the exponential.*

(c) Hence $THTH = e^{i\pi/4}R_z(\pi/4)R_x(\pi/4)$. A product of two rotations is again a rotation, $R_{\hat{m}}(\theta)$ about some axis $\hat{m}$. Using $\operatorname{tr} R_{\hat{m}}(\theta) = 2\cos\frac{\theta}{2}$ and the fact that X, Z and ZX are all traceless, show that the angle satisfies

$$\cos\tfrac{\theta}{2} = \cos^2\tfrac{\pi}{8}.$$

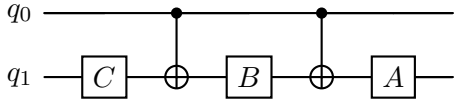
(d) It can be shown that this θ is an irrational multiple of π (take this on trust). Explain why this means the powers $(THTH)^k$, $k = 1, 2, 3, \ldots$, come arbitrarily close to $R_{\hat{m}}(\phi)$ for *every* angle ϕ. *Hint: think of $k\theta$ modulo 2π as points on a circle.*

(e) Sketch (no calculation) why rotations about $\hat{m}$ together with rotations about a second, non-parallel axis let you approximate *every* single-qubit gate. Which result of Q2 is being used?

Part B — Controlled gates

4. Building controlled-U from `cx` and single-qubit gates.

(a) Suppose A, B, C are single-qubit gates with $ABC = \mathbb{I}$ and $AXBXC = U$. Show that the circuit



implements controlled-U with qubit 0 as control. *Hint: write the circuit as $(\mathbb{I}\otimes A)$ `cx` $(\mathbb{I}\otimes B)$ `cx` $(\mathbb{I}\otimes C)$ and act on $|0\rangle\otimes|\psi\rangle$ and $|1\rangle\otimes|\psi\rangle$ separately.*

(b) Verify that $XR_z(\theta)X = R_z(-\theta)$ and $XR_y(\theta)X = R_y(-\theta)$. Use the first to show that $A = R_z(\beta/2)$, $B = R_z(-\beta/2)$, $C = \mathbb{I}$ gives controlled-$R_z(\beta)$.

(c) **The phase matters for controlled U.** Show that controlled-$(e^{i\alpha}U)$ is *not* the same as controlled-U: it equals controlled-U followed by the single-qubit gate $\mathrm{diag}(1, e^{i\alpha})$ on the *control*. Express $\mathrm{diag}(1, e^{i\alpha})$ as a rotation times a phase. So a "global" phase is invisible on its own but perfectly measurable once the gate is controlled.

(d) For a general $U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$ take

$$A = R_z(\beta)R_y(\gamma/2), \qquad B = R_y(-\gamma/2)R_z\big(-\tfrac{\delta+\beta}{2}\big), \qquad C = R_z\big(\tfrac{\delta-\beta}{2}\big).$$

Check $ABC = \mathbb{I}$ and $AXBXC = R_z(\beta)R_y(\gamma)R_z(\delta)$. Together with (c): *any* controlled-U costs at most two `cx` gates plus single-qubit gates.

5. The Toffoli gate needs T. Every gate on Worksheet 5 was a Clifford. The Toffoli gate $\texttt{ccx}(0,1,2)$ is the first one you have met that is not, and it is the gate that makes classical reversible logic (Worksheet 1) available inside a quantum circuit.

(a) Let $X_0 = X \otimes \mathbb{I} \otimes \mathbb{I}$. Show that $\texttt{ccx}\, X_0\, \texttt{ccx} = X_0\, \texttt{cx}(1,2)$. Since $\texttt{cx}(1,2)$ is not a product of Paulis, the Toffoli is not a Clifford gate.

(b) Show that $\texttt{ccx}(0,1,2) = (\mathbb{I}\otimes\mathbb{I}\otimes H)\,\texttt{ccz}\,(\mathbb{I}\otimes\mathbb{I}\otimes H)$, exactly as `cx` and `cz` were related in Worksheet 5.

(c) On a basis state $|abc\rangle$, `ccz` gives the phase $(-1)^{abc} = e^{i\pi abc}$. Writing Z_j for Z on qubit j, show that on every basis state $\frac{1}{2}(\mathbb{I} - Z_j)$ acts as the bit j, and hence that

$$\texttt{ccz} = \exp\Big[\tfrac{i\pi}{8}\,(\mathbb{I}-Z_0)(\mathbb{I}-Z_1)(\mathbb{I}-Z_2)\Big] = \exp\Big[\tfrac{i\pi}{8}\big(\mathbb{I}-Z_0-Z_1-Z_2+Z_0Z_1+Z_0Z_2+Z_1Z_2-Z_0Z_1Z_2\big)\Big].$$

(d) All the operators in the exponent commute, so the exponential factorises into seven factors of the form $e^{\pm i\pi Z_j/8}$, $e^{\pm i\pi Z_iZ_j/8}$ and $e^{-i\pi Z_0Z_1Z_2/8}$, times a global phase. Show that $e^{-i\pi Z_j/8} = e^{-i\pi/8}\,T_j$, and use the Worksheet 5 result $\texttt{cx}(i,j)\,Z_j\,\texttt{cx}(i,j) = Z_iZ_j$ to show that

$$\texttt{cx}(i,j)\,e^{i\phi Z_j}\,\texttt{cx}(i,j) = e^{i\phi Z_iZ_j} \qquad \text{and} \qquad \texttt{cx}(0,2)\texttt{cx}(1,2)\,e^{i\phi Z_2}\,\texttt{cx}(1,2)\texttt{cx}(0,2) = e^{i\phi Z_0Z_1Z_2}.$$

Hint: $\texttt{cx}\,f(M)\,\texttt{cx} = f(\texttt{cx}\,M\,\texttt{cx})$ *for any power series* f*, because* $\texttt{cx}^2 = \mathbb{I}$.

(e) Assemble a circuit for `ccz`, and hence for the Toffoli, using only `cx`, H, T and $T^\dagger$. How many T or $T^\dagger$ gates does it use? (This "T-count" is what makes the Toffoli expensive in fault-tolerant schemes, where T is by far the costliest gate.)

Part C — What "universal" does and does not mean

6. Finite gate sets, counting, and the inadequacy of Clifford gates.

(a) A gate set $\mathcal{G}$ is finite. Explain why the set of all circuits built from $\mathcal{G}$ is *countable*, while the set of single-qubit gates is not. Conclude that no finite gate set can produce every single-qubit gate *exactly*. "Universal" for a finite set can thus only mean "to any desired accuracy".

(b) Show that if two Clifford gates U and V give the same result when they act on X and Z as $AXA^\dagger$ and $AZA^\dagger$, $A \in \{U, V\}$ respectively, then U and V differ only by a phase, i.e., they are the *same* gates. *Hint: every* 2×2 *matrix is a combination of* $\mathbb{I}$, X, Y, Z, *and* $Y = iXZ$.

(c) The above result means that the action of a Clifford gate on any two of the three Pauli matrices fixes the gate. Just based on this information and the definition of a Clifford gate, count the maximum number of Clifford gates possible.

(d) All single-qubit Clifford gates can be generated by a circuit containing only H and S gates (take this on trust). Why does this show that the Clifford gates are not universal, even in the approximate sense of (a)? *Hint: go back to Q3.*

Remark: for many qubits the Clifford group is still finite and nonuniversal. In fact, a quantum circuit consisting of merely Clifford gates can be simulated efficiently on a classical computer. This is the Gottesman–Knill theorem. Adding the single non-Clifford gate T turns the set into a universal one.

7. Errors add up. A universal gate set only approximates the gates of an ideal circuit. Define the error of approximating U by V as $E(U,V) = \max_{|\psi\rangle} \left\| (U-V)\,|\psi\rangle \right\|$ over normalised states.

(a) Show that $E(U_2U_1, V_2V_1) \le E(U_2,V_2) + E(U_1,V_1)$ for unitaries U_i, V_i. *Hint:* $U_2U_1 - V_2V_1 = (U_2-V_2)U_1 + V_2(U_1-V_1)$*, and unitaries preserve norms.*

(b) An ideal circuit has N gates and you need total error at most ε. To what accuracy must each gate be approximated?

(c) The Solovay–Kitaev theorem says that any gate can be approximated to accuracy δ using $O(\log^c(1/\delta))$ physical gates from a universal set, where c is a constant of order 2. Combine with (b): how does the total number of gates grow with N and ε? Why is this the result that makes finite gate sets *practical*, and not just universal in principle?

8. On a computer (optional). In Qiskit, build your `ccz` circuit from Q5(e) and check it against a `ccz` gate with `Operator(qc1).equiv(Operator(qc2))`. Then transpile a circuit containing a single `ccx` gate with

```
transpile(qc, basis_gates=['h','t','tdg','cx'])
```

and count the T and $T^\dagger$ gates Qiskit uses.