University of Oslo

FYS3415/FYS4415 — Quantum computing and quantum information

Problem set 6

This problem set will be discussed on **Mar. 4**.

Problem 1: Measurement in the Circuit Model

a) Measurement commutes with controls. Consider a qubit q_1 that is the control of a controlled-U gate, with target q_2. All measurements are in the computational basis.

i) The following two procedures act on an arbitrary two-qubit state $|\Psi\rangle$:



Show that the two procedures produce the same measurement probabilities and the same post-measurement state for each outcome. Deduce that *measurement commutes with controls*: it does not matter whether the control qubit is measured before or after the controlled operation.

ii) Now suppose the circuit also contains an unconditional single-qubit gate V on q_1 *between* the controlled-U and the measurement. Compare the two procedures:

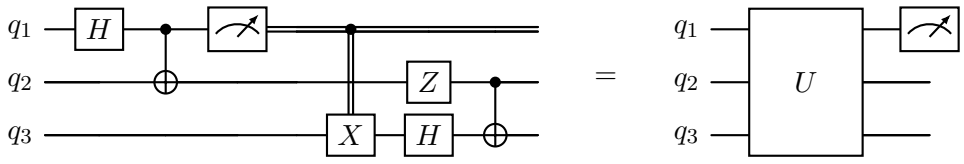


Does the equivalence from (i) still hold? Work out both procedures and compare the measurement probabilities and post-measurement states.

Hint[1].

b) The principle of deferred measurement states that intermediate measurements can always be moved to the end of a quantum circuit.

Consider the following equivalence, where an intermediate measurement and classical control are replaced by a single three-qubit unitary block U followed by a deferred measurement:



i) Find U. Draw the explicit quantum circuit inside the block U.

ii) Explain why this equivalence holds. What specific rules or previous results guarantee this?

[1] Write $|\Psi\rangle = |0\rangle\,|\phi_0\rangle + |1\rangle\,|\phi_1\rangle$ and work out each procedure separately.

c) The Principle of Implicit Measurement states that any unterminated quantum wires at the end of a circuit can be assumed to be measured (and their results discarded) without affecting the state of the remaining qubits.

In problem 4 last week, you calculated Bob's reduced density matrix in two different scenarios:

- Scenario 1 (Unterminated wires): Alice does nothing to her qubits. You calculated Bob's state by taking the partial trace over Alice's system before she measures: $\rho^B_{\text{pre}} = \text{Tr}_A(|\Psi_2\rangle\langle\Psi_2|)$.
- Scenario 2 (Measure and discard): Alice measures her qubits, obtaining outcome m with probability $p(m)$, but Bob never receives the classical result. You calculated Bob's averaged state before he received Alice's outcomes as: $\rho^B_{\text{after}} = \sum_m p(m)\rho^B_m$.

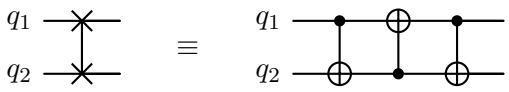
You proved that $\rho^B_{\text{pre}} = \rho^B_{\text{after}} = \mathbb{1}/2$. Furthermore, in the general proof of no-signaling, you proved that $\text{Tr}_A(\rho^{AB}) = \sum_m p(m)\rho^B_m$ holds for *any* bipartite state and any measurement. Explain in 2–3 sentences how this specific mathematical identity, $\text{Tr}_A(\rho^{AB}) = \sum_m p(m)\rho^B_m$, perfectly justifies the principle of implicit measurement.

Problem 2: Circuit decomposition and gate construction

In this problem you will practice a key circuit-design technique — decomposing a gate into simpler pieces and upgrading each piece to its controlled version — and connect the result to the universality of quantum computation.

a) Gate decompositions and controlled gates.

i) Show that the SWAP gate can be decomposed into three alternating CNOTs:

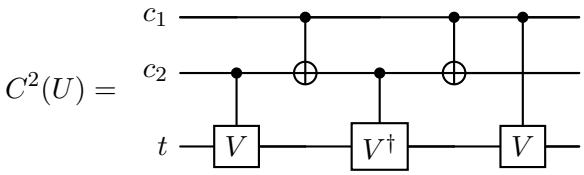


Verify this by computing the action on $|a\rangle\,|b\rangle$ for arbitrary computational basis states $a, b \in \{0, 1\}$.

ii) Apply the "decompose then control" strategy to build a controlled-Z (CZ) gate: First, verify the identity $Z = HXH$. Next, upgrade all three gates in this decomposition to their controlled versions (yielding controlled-H, CNOT, and controlled-H). Finally, argue why the controls on the outer H gates can be safely removed, giving a circuit for CZ using only one CNOT and two unconditional H gates.

b) Fredkin gate construction Recall that the Fredkin (controlled-SWAP) gate swaps two target qubits if and only if a control qubit is $|1\rangle$.

The following circuit implements a doubly-controlled-U gate ($C^2(U)$) using a gate V with $V^2 = U$:

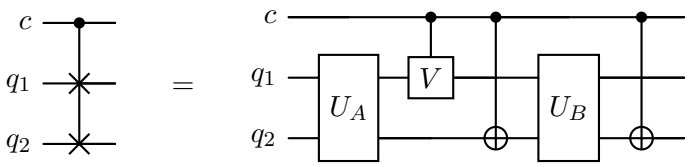


i) Give a quantum circuit which uses three Toffoli gates to construct the Fredkin gate.

ii) Show that the first and last Toffoli gates can be downgraded to plain CNOT gates.

iii) Now replace the middle Toffoli gate with the $C^2(U)$ circuit above to obtain a Fredkin gate construction using only 7 two-qubit gates. Draw the circuit diagram.

iv) Using explicit commutation arguments, show how to reduce the sequence to only five two-qubit gates:



(The symbol left of the equals sign denotes a controlled-SWAP, i.e. Fredkin gate.) What operations do the U_A and U_B gates contain?

Problem 3: Irrational Rotations and Approximate Universality

Allowing arbitrary single-qubit gates (a continuous set) together with CNOT gives an exact universal set of gates for quantum computation. We can also consider an approximate universal gate set, when it is possible to implement gates arbitrarily close to any desired unitary using some gate set. A useful way to show approximate universality for single-qubit gates is to find a rotation about some axis by an angle θ which is an *irrational* multiple of 2π. Then the angles $(k\theta) \bmod 2\pi$ obtained by repeating the rotation become dense in $[0, 2\pi)$, giving arbitrarily fine rotation angles about that axis. Together with the ability to rotate about a second, non-parallel axis, this leads to a dense set of single-qubit gates.

In this problem, we will show that the discrete gate set $\{H, T\}$ achieves this. Recall the general rotation operator $U_{\hat{n}}(\alpha) = \cos(\alpha/2)I - i\sin(\alpha/2)(\hat{n}\cdot\vec{\sigma})$. More precisely,

$$e^{-i\pi/8}T = U_z(\pi/4) = \cos\left(\frac{\pi}{8}\right)I - i\sin\left(\frac{\pi}{8}\right)Z.$$

a) Changing the axis of rotation. Show that wrapping the T-gate in Hadamard gates creates an identical rotation, but around the x-axis. That is, show that up to global phase:

$$HTH \sim U_x(\pi/4)$$

b) The combined rotation. Now consider the unitary operation U created by applying T followed by HTH:

$$U = (HTH)\,T \sim U_x(\pi/4)\,U_z(\pi/4).$$

Expand this matrix product into the form

$$cI - i\left(v_xX + v_yY + v_zZ\right).$$

Hint[2].

[2] Use the Pauli matrix multiplication rules, specifically $XZ = -iY$.

c) The irrational angle. The last expression is an element of SU(2), so it must be equivalent to some single rotation

$$U_{\hat{n}}(\theta) = \cos(\theta/2)I - i\sin(\theta/2)(\hat{n}\cdot\vec{\sigma})$$

around a new axis $\hat{n}$.

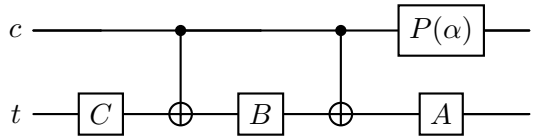
i) By comparing your result from part (b) with the general formula for $U_{\hat{n}}(\theta)$, find an expression for $\cos(\theta/2)$.

ii) Find an expression for the value of $\cos(\theta/2)$. Use a computer algebra system to determine whether θ is a rational or irrational multiple of 2π. Use the result to explain why this implies that $\{H, T\}$ is an approximately universal single-qubit gate set.

d) From Single-Qubit to Multi-Qubit Universality. To achieve universal quantum computation, we must extend our single-qubit control to multiple qubits using an entangling gate. A crucial step is showing that we can construct a *controlled-U* gate for *any* single-qubit unitary U using only CNOTs and single-qubit gates.

Any single-qubit unitary can be factored as $U = e^{i\alpha}AXBXC$, where A, B, and C are single-qubit unitaries satisfying $ABC = I$, X is the Pauli-X gate, and $e^{i\alpha}$ is a global phase.

Consider the following circuit, where $P(\alpha) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{smallmatrix}\right)$ is a phase gate:



i) Verify that this circuit correctly implements a controlled-U gate by tracing the evolution of the target qubit when the control is $|0\rangle$ and when it is $|1\rangle$.

ii) A fundamental result in quantum circuit theory establishes that any n-qubit unitary operation can be decomposed into a sequence of single-qubit gates and two-qubit controlled-U gates. In 2–3 sentences, explain how combining this exact decomposition, the circuit above, and the properties of the $\{H, T\}$ gate set from the previous steps shows that $\{H, T, \text{CNOT}\}$ is universal for quantum computation in the *approximate* sense.