C S 358H: Intro to Quantum Information Science

Sayam Sethi

October 2024

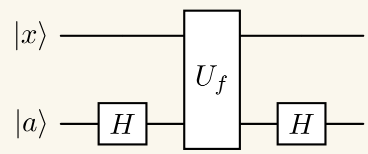
Contents

1 Oracle Queries

Question 1.1

Question. *Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, recall that an "XOR query" maps basis states of the form $|x\rangle|a\rangle$ to $|x\rangle|a \oplus f(x)\rangle$, while a "phase query" maps basis states of the form $|x\rangle|a\rangle$ to $(-1)^{a\cdot f(x)}|x\rangle|a\rangle$, where $x \in \{0,1\}^n$ and $a \in \{0,1\}$. Show that given a phase query we can simulate an XOR query and vice versa.*

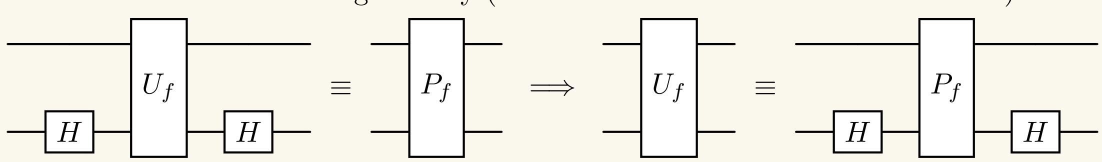
Proof. We define the "XOR oracle" as U_f and the "phase oracle" as P_f. Now consider the following circuit:



Now, consider the state of the qubits after the above operations on the two basis states for $|a\rangle$, right before the final Hadamard gate,

$$|x,a\rangle \mapsto \frac{|x,f(x)\rangle + (-1)^a |x,\overline{f(x)}\rangle}{\sqrt{2}} = (-1)^{a\cdot f(x)}\left(\frac{|x,0\rangle + (-1)^a|x,1\rangle}{\sqrt{2}}\right) \tag{1}$$

In the second step above, we get a global phase of -1 when $a \neq 0$ and $f(x) = 1$, which can be combined as $a \cdot f(x)$. Now, when we apply the Hadamard gate on the ancilla qubit, we get the state $(-1)^{a\cdot f(x)}|x,a\rangle$, which is exactly the output of the phase oracle. Thus, we have shown that we can simulate P_f using U_f.
We can now write the following identity (since the result holds for all basis states):



Therefore, to obtain U_f from P_f, we can simply add H gates before and after P_f on the ancilla qubits which will cancel out the Hadamards on the LHS of the idenitity, giving us the result we want.

$\square$

2 Quantum Mechanics Interpretations

Question 2.1

Question. *Which of the following views about quantum mechanics necessarily lead to experimental predictions that are* different *from the predictions of conventional QM? Make two distinct lists: one list of the views that do, and one list of the views that don't. (Note: For this question, we're only interested in clear-cut predictions about the observed behaviors of "dumb physical systems" like masses or entangled particles, not about the experiences of conscious observers like Wigner's friend. Beyond that, though, we don't care how easy or hard the prediction is to test in practice.)*

(A) The Many-Worlds Interpretation

(B) The Copenhagen Interpretation

(C) GRW (Ghirardi-Rimini-Weber) dynamical collapse

(D) Penrose's gravity-induced quantum state collapse

(E) Local hidden variables

(F) Nonlocal hidden variables (including Bohmian mechanics)

Solution.

- **Views that lead to different predictions:**
  1. GRW (Ghirardi-Rimini-Weber) dynamical collapse – an experiment on a system larger than a probability p of collapse for each individual particle, then this theory will have a different outcome on that system from conventional QM (we have been able to construct dobule slit experiments on larger and larger particles, like the buckyball)
  2. Penrose's gravity-induced quantum state collapse – similar to GRW, an experiment for a large enough system, separated by a large enough distance, will have a different outcome than conventional QM (and experiments have been heading in this direction with long-distance teleportation that has been shown)
  3. Local hidden variables – this has been proven false by experiments that disobey the Bell inequality
- **Views that don't lead to different predictions:**
  1. The Many-Worlds Interpretation – this agrees with predictions of conventional QM, albeit not at a philosophical level
  2. The Copenhagen Interpretation – this agrees with predictions of conventional QM since it just says that it is a result of calculations
  3. Nonlocal hidden variables (including Bohmian mechanics) – this agrees with predictions of conventional QM, but requires someone to "monitor" all particles with faster-than-light communication

□

3 Quantum computation with real amplitudes

'Real quantum mechanics' is a hypothetical theory that's identical to standard quantum mechanics, except that the amplitudes always need to be real—and instead of unitary matrices, we're restricted to applying real orthogonal matrices.

Question 3.1

Question. *Prove that any standard quantum circuit acting on n qubits can be perfectly simulated by a real quantum circuit acting on $n+1$ qubits — and moreover, by a circuit containing exactly as many gates as the original circuit (although the gates might act on slightly more qubits than the gates of the original circuit). Your proof should give a mapping from complex-valued states to real-valued states and from unitary matrices to real orthogonal matrices.*
Hint: Observe that, with $n+1$ qubits rather than n, you have 2^{n+1} amplitudes rather than just 2^n.

Proof. Consider the following mapping for a n qubit state with complex amplitudes to a $n+1$ qubit state with real amplitudes:

$$\mathbf{M} : \left(|\psi\rangle = \sum_{b \in \{0,1\}^n} (\alpha_b + i\beta_b) |b\rangle \right) \mapsto \left(|\psi'\rangle = \sum_{b \in \{0,1\}^n} \alpha_b |b0\rangle + \beta_b |b1\rangle \right) \tag{2}$$

Notice that the state $|\psi'\rangle$ is still normalized and since we start with real α_b, β_b for all b, all amplitudes in $|\psi'\rangle$ are real. We can now give a mapping for any unitary whose actions are defined on the computational states as:

$$U|x\rangle = \sum_{b \in \{0,1\}^n} (\alpha_b + i\beta_b) |b\rangle \mapsto \begin{cases} U'|x0\rangle = \mathbf{M}(U|x\rangle) & = \sum_{b \in \{0,1\}^n} (\alpha_b |b0\rangle + \beta_b |b1\rangle) \\ U'|x1\rangle = \mathbf{M}(i \cdot U|x\rangle) & = \sum_{b \in \{0,1\}^n} (-\beta_b |b0\rangle + \alpha_b |b1\rangle) \end{cases} \tag{3}$$

□

Clearly, we have defined the unitary on all basis states for $n+1$ qubits and it is easy to see that the values in U' are real. Since the columns in U are orthogonal to each other, it implies that the columns in U' will also be orthogonal to each other. The orthogonality for the basis states which have the same last bit follows from the fact that $\mathsf{Re}(\langle Ux|Uy\rangle) = 0$ and for the basis states that differ in the last bit follows from the fact that $\mathsf{Im}(\langle Ux|Uy\rangle) = 0$. This in turn follows from the fact that all columns in U are orthogonal and hence both real and imaginary parts of the inner products should be equal to 0.
Therefore, we have given an orthogonal transformation on the basis states for $n+1$ qubits. Using this we can also construct a suitable $2^{n+1} \times 2^{n+1}$ orthogonal matrix from the $2^n \times 2^n$ matrix U. Hence, proved.

Question 3.2

Question. *To illustrate your construction, show how the phase gate gets converted into a purely real gate in your simulation.*

Solution. We can transform the phase gate as:

$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \mapsto P' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{4}$$

□

Question 3.3

Question. *Conclude the proof that complex amplitudes are never actually needed for quantum computing speedups — positive and negative real amplitudes suffice — by explaining how measurements are performed.*

Solution. To measure a qubit in the system with real amplitudues on the $n+1$ qubit state such that the output probabilities are the same as for the system with complex amplitudes on the n qubit state, we can simply measure the first n qubits and report the output as the bitstring obtained on the first n qubits. If we want to measure in a different basis, we apply U' on the $n+1$ qubit system (where U' is the transformed unitary of U as defined in Question 3.1, and U is the change of basis unitary) and then perform a measurement on the computational basis by measuring the first n qubits.

Note that in the above method of measurements, the probability of measuring a bitstring $|b\rangle$ is the same in both formalisations: $\alpha_b^2 + \beta_b^2$ □

4 Universal gate sets

Identify the following gate sets as either universal or not universal *in the sense — specifically — of able to approximate any target unitary to any desired precision.* If it is not, argue why (if it is, you do not have to give an argument).
Recall: $S = \left[\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right]$.

Question 4.1

Question. $\{$*All single qubit gates, CNOT*$\}$

Proof. **Universal**: This is a universal gate set since we can approximate any n qubit unitary using an arbitrary single qubit unitary combined with CNOT gates. □

Question 4.2

Question. $\{$*Toffoli, Hadamard*$\}$

Proof. **Not Universal**: This cannot be a universal gate since we cannot obtain complex amplitudes using just Toffoli and Hadamard gates, therefore, we cannot approximate an arbitrary unitary. Although this is computationally universal (i.e., we can simulate any quantum computation with atmost a polynomial overhead). □

Question 4.3

Question. $\{$*Toffoli*, $S\}$

Proof. **Not Universal**: This cannot be universal since we cannot generate superposition just by using Toffoli and S gates, even though we can generate complex amplitudes on basis states using this gate set. □

Question 4.4

Question. $\{$*Toffoli*, S, *Hadamard*$\}$

Proof. **Universal**: This is a universal gate set for a system with at least 3 qubits. We will be unable to approximate any unitary on 2 qubits without having to use more than 2 qubits. □

Question 4.5

Question. $\{$*Hadamard*, S, *Controlled* $Z\}$

Proof. **Not Universal**: This gate set generates the Clifford group since we can obtain a CNOT gate using the idenitity proven in Homework 3. Additionally, we have no non-Clifford gate in the gate set, therefore, we cannot approximate any unitary that is not in the Clifford group. □

Question 4.6

Question. $\{$*Controlled Hadamard, Controlled* S*, NOT*$\}$

Proof. **Universal**: This gate set is universal since the first two gates are in the $C^{(3)}$ Clifford hierarchy and we can generate the Clifford group using the set. Therefore, combined with the Clifford group and a gate from C^3, we can approximate any unitary. $\square$