Frontiers of Quantum Complexity and Cryptography Spring 2022

Lecture 6 – Unitary Synthesis

Lecturer: Henry Yuen *Scribes: Julia Martin*

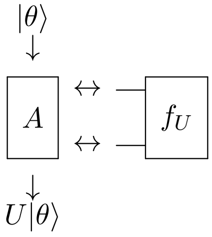
1 Unitary Synthesis Problem (USP)

We now turn to a different, but related, problem. Here, the goal is to synthesize not just a single state but an entire *unitary transformation*. Consider an n-qubit unitary U. From an analogous counting argument, in the worst case the unitary U might be exponentially complex, meaning that the smallest quantum circuit (consisting of one- and two-qubit gates) that implements the unitary operation U requires $2^{\Omega(n)}$ elementary operations to perform.

Similarly to the State Synthesis Problem, the Unitary Synthesis Problem asks whether it is possible to reduce the complexity of implementing a quantum unitary to the complexity of computing a classical boolean function. More precisely:

Unitary Synthesis Problem. Is there a quantum query algorithm A, a polynomial $p(n)$, and an encoding scheme that maps n-qubit unitaries U to boolean functions $f_U : \{0,1\}^{p(n)} \to \{0,1\}$ such that, given an input state $|\theta\rangle$, the algorithm A makes *poly*(n) queries to f_U, uses *poly*(n) qubits of space, and outputs a good approximation of $U|\theta\rangle$?

Diagrammatically, the task looks like the following:



What makes the Unitary Synthesis Problem (abbreviated USP) different from the State Synthesis Problem is that there is an additional input to the algorithm A, which is an unknown state $|\theta\rangle$. The algorithm A knows nothing about it, but yet it wants to be able to apply the unitary U to it, and it is only allowed to make a small number of queries to a *classical boolean function* to get information about U.

What do we know about USP? Not very much, actually. For all we know, there might be an efficient solution to USP just like with SSP. However, this seems like a hard problem; some researchers conjecture that any solution to USP requires exponentially many queries to the classical oracle f_U.

If we drop the polynomial space requirement on the algorithm A, then just like with SSP, there exists an easy 1-query algorithm (based on the Bernstein-Vazirani trick) that uses exponentially many qubits of space. But if we restrict to polynomial space, then it's not clear what is possible. A nontrivial upper bound based on Grover search was discovered by Rosenthal in [**?**].

Given that SSP has an efficient solution, the USP is a nice way of investigating the differences between the complexity of quantum states and quantum unitaries.

From one point of view, it may be puzzling that there would be a meaningful difference between the complexity of quantum states and quantum unitaries. For example, a $2n$-qubit state $|\psi\rangle$ has roughly the same number of free parameters as an n-qubit unitary U (one is a vector of length 2^{2n} and the other is a matrix of size $2^n \times 2^n$).

Reducing Unitary Synthesis to State Synthesis. Is it possible to relate these two problems? In other words, can we solve the Unitary Synthesis Problem by converting it to a related State Synthesis Problem (for which we have an efficient solution to)? More specifically, it would be really interesting if we could do the following. Rather than directly encoding a unitary U into a classical function f_U, we first try to come up with a way to encode a unitary U into a *program state* $|\psi_U\rangle$, with the property that there is an efficient quantum algorithm A such that for all input states $|\theta\rangle$

$$A|\psi_U\rangle \otimes |\theta\rangle \approx U|\theta\rangle \otimes |junk\rangle \ .$$

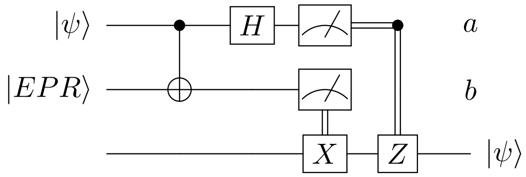
In other words, the algorithm A does not query a classical oracle anymore, but instead uses the state $|\psi_U\rangle$ to obtain the relevant information about implementing the unitary U.

If we can do this efficiently for all unitaries U (meaning that $|\psi_U\rangle$ doesn't require too many qubits), then we can then solve USP by solving the State Synthesis problem for $|\psi_U\rangle$.

1.1 Gate Teleportation

We now explore an approach to program states that sounds promising, but as we will see, does not quite solve the problem. This approach is based on the concept of *gate teleportation.* We first review "standard" quantum teleportation.

Recall the quantum teleportation circuit. Here the first wire carries a qubit state $|\psi\rangle$, and the second and third wire carry the entangled pair $|EPR\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$.



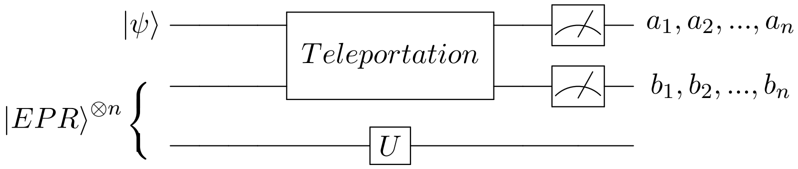
Once the two measurements are performed to obtain bits $a, b \in \{0, 1\}$ (known as *correction keys* or *teleportation keys*), the state of the third wire is the original qubit state $|\psi\rangle$, but masked by the correction operators:

$$X^b Z^a |\psi\rangle \ .$$

We can undo the corresponding correction operators to get $|\psi\rangle$. No matter what $|\psi\rangle$ is, all possible a, b combinations occur with equal probability. In other words, the correction keys are uniformly distributed.

This teleportation circuit can be generalized to more qubits; simply repeat the circuit n times to teleport n qubits. This results in $2n$ correction bits $(a_1, \ldots, a_n, b_1, \ldots, b_n)$.

So how can we use this to apply arbitrary unitary U to $|\psi\rangle$? Say that $|\psi\rangle$ is an n-qubit state, and that we also have n EPR pairs, denoted by $|EPR\rangle^{\otimes n}$. We can imagine first applying U to the second half of those n EPR pairs, and then performing the teleportation circuit as before.



Suppose for a second that all of the correction keys were zero: $a_1 = \cdots = a_n = b_1 = \cdots = b_n = 0$. Then the resulting state on the third wire would be $U|\psi\rangle$; in essence we have teleported the state $|\psi\rangle$ "through" the unitary U. What a nifty way of applying the unitary U! The problem, though, is that this scenario occurs with vanishingly small probability: 4^{-n}. In general, if any correction key were nonzero, then the resulting state on the third wire would be some complicated mess of the form

$$U(X^{b_1}Z^{a_1} \otimes \cdots \otimes X^{b_n}Z^{b_n})|\psi\rangle \ .$$

In other words, the corrections are "getting in the way" of the unitary U.

If it weren't for this issue, then the state $(I \otimes U)|EPR\rangle^{\otimes n}$ would be a very good candidate for a program state.

In the next lecture, we will show how we can efficiently encode unitaries into states, for special types of unitaries.