Hidden Subgroups and Quantum Computation

Lecture 04

Dheeran E. Wiggins

Summer 2025
Illinois Mathematics and Science Academy

July 11, 2025

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Overview

Today we will describe what a quantum circuit is, using the mathematical language we have built thus far.

Then, we can discuss some preliminaries on the HSP.

Suppose our quantum processing unit (QPU) has n qubits. Recall that by the multiple systems axiom, this means our state space $\mathcal{H}$ for the QPU is isomorphic to the n-fold tensor product

$$\mathcal{H} \simeq \mathbb{C}^2 \underbrace{\otimes \cdots \otimes}_{n \text{ times}} \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes n}$$

of dimension 2^n.

Then, the states of our system should be given by the density operators on $\mathcal{H}$.

That is, we care about the operators

$$\mathcal{D}(\mathcal{H}) = \{\rho \in \mathbb{M}_{2^n}(\mathbb{C}) : \mathrm{tr}(\rho) = 1 \text{ and } \rho \geq 0\},$$

where $\rho \geq 0$ means $\langle\varphi|\rho|\varphi\rangle \geq 0$ for all $|\varphi\rangle \in \mathcal{H}$.

Furthermore, the system evolution axiom tells us that if $\rho_t \in \mathcal{D}(\mathcal{H})$ is the state of our system at time t, then closed evolution in the times $t \in [t_1, t_2]$, the state of our system follows

$$\rho_{t_2} = U \rho_{t_1} U^\dagger.$$

Remember, we require $U \in \mathbb{M}_{2^n}(\mathbb{C})$ to be unitary:

$$U U^\dagger = U^\dagger U = I_{2^n}.$$

Note that one sort of density operator is a pure state, i.e., one of the form

$$\rho = |\varphi\rangle\langle\varphi|\,, \quad |\varphi\rangle \in \mathcal{H} \text{ of unit length.}$$

It is thus often easier to consider states as just normalized vectors $|\varphi\rangle$ in $\mathcal{H}$, where now closed evolution is of the form

$$|\varphi_{t_2}\rangle = U\,|\varphi_{t_1}\rangle\,,$$

since taking outer products gives back our original $U(-)U^\dagger$ form for pure states:

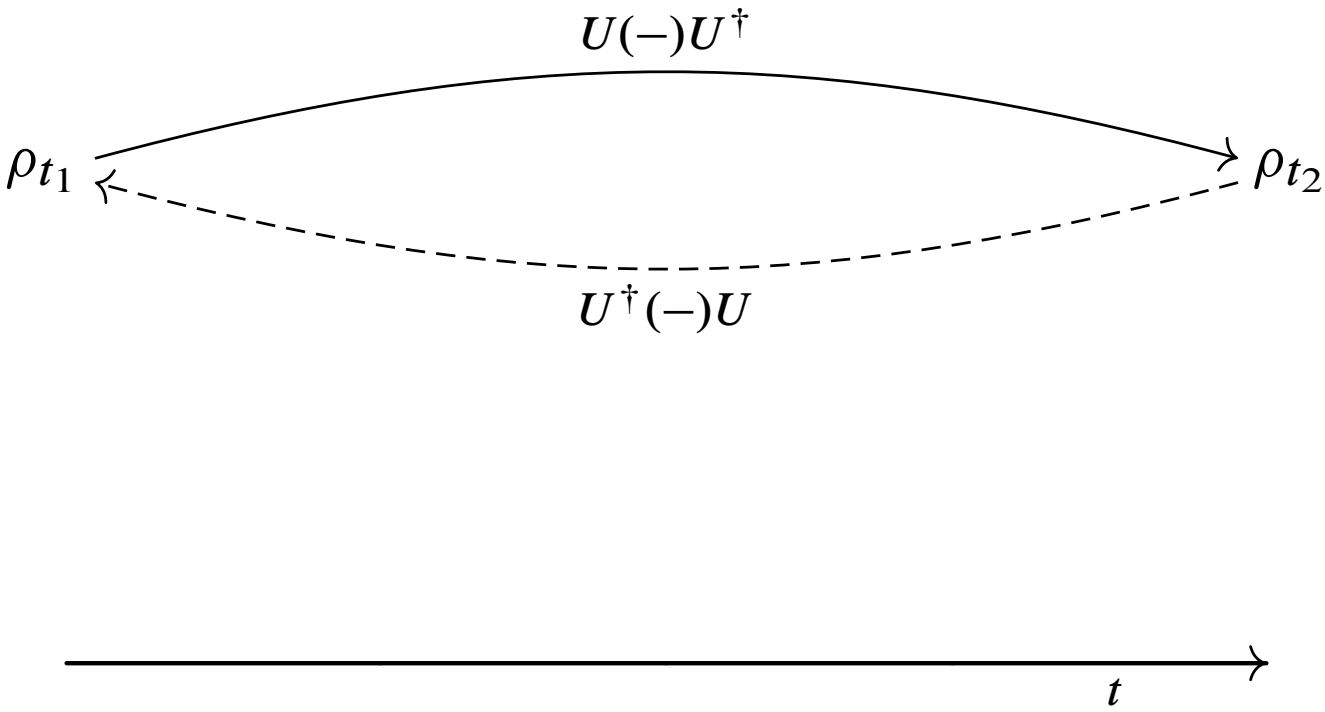
$$|\varphi_{t_2}\rangle\langle\varphi_{t_2}| = U\,|\varphi_{t_1}\rangle\,(U\,|\varphi_{t_1}\rangle)^\dagger = U\,|\varphi_{t_1}\rangle\langle\varphi_{t_1}|\,U^\dagger.$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Observe that

$$U^\dagger \rho_{t_2} U = U^\dagger U \rho_{t_1} U^\dagger U = \rho_{t_1},$$

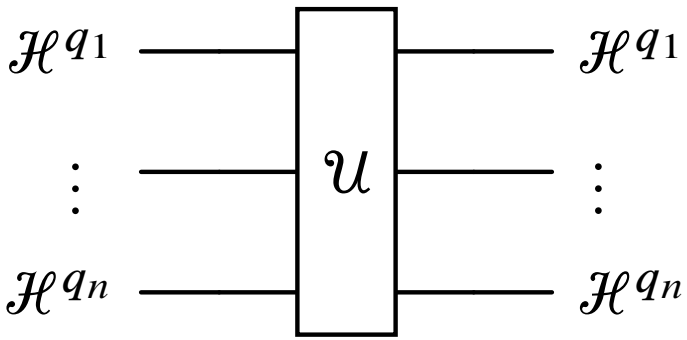
so quantum computation is reversible.


$U(-)U^\dagger$
ρ_{t_1}
ρ_{t_2}
$U^\dagger(-)U$
t

We call a unitary U acting on $s \leq n$ qubits $q_1, \ldots, q_s$ in the space $(\mathbb{C}^2)^{\otimes n}$ a quantum gate.

Quantum gates are the analogues of classical gates (e.g., AND, XOR, NOT) in the classical circuit diagrams you have seen.

A quantum circuit should be something which looks like



ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

We can interpret each wire as a part of the tensor product, where $\mathcal{H}^{q_j} \simeq \mathbb{C}^2$ for all $1 \leq j \leq n$ and $\mathcal{H} \simeq \bigotimes_{j=1}^{n} \mathcal{H}^{q_j}$.

Moving to the right along a wire represents moving forward in time, though we usually work under the assumption that our quantum gates U in $\mathcal{U}$ work instantaneously.

Assigned reading: §2.2 of Lomont's review for a slightly more rigorous treatment of quantum circuits.

`https://arxiv.org/pdf/quant-ph/0411037`.

Then, take a look at §3.1.

We now take a look at the statement of the HSP.

For a group element $j \in G$ and subgroup $H \leq G$, the (left) coset jH is the subset

$$jH = \{jh : h \in H\} \subseteq G.$$

When H is normal in G, these cosets were precisely the elements of our quotient group G/H.

Let $(G, \cdot)$ be a group, S be an arbitrary set, and $H \leq G$ be a subgroup. Then, a function

$$f : G \to S$$

separates H-cosets if for all elements $j, k \in G$,

$$f(j) = f(k) \quad \text{if and only if} \quad jH = kH.$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

The hidden subgroup problem (HSP) is as follows:

Let $(G, \cdot)$ be a group; let $S = \{s_1, \ldots, s_n\}$ be a finite set. If $f : G \to S$ separates H-cosets for some subgroup $H \leq G$, then use the value of f on some elements of G to determine a set $X \subseteq G$ such that $\langle X \rangle = H$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Next time we will discuss

(i) the quantum Fourier transform F_n on $\mathbb{Z}/n$.

(ii) the cyclic HSP algorithm.

Then, we will move on to the more general abelian HSP algorithm and applications to Simon's and Shor's algorithms.