Density Operators and Partial Trace

Raul-Martin Rebane

March 21, 2020

The definitions of density operators, quantum state probability distributions etc can be found in prof. Unruh's lecture notes and you should have that open in parallel.

NB *If you found this document helpful, please mention that in your homework submission as feedback for me.*

1 Motivation

In this part of the course we introduce a new way to describe quantum states and operations. Until now we have described our quantum states as vectors with norm 1, and our operations as unitary matrices. However this has some limitations - for example what is the state if I was to measure $|+\rangle$, and then do a Hadamard gate? The answer is $|+\rangle$ or $|-\rangle$ depending on the result of my measurement. This creates a kind of branching in the state of our program, and with many sequential branchings, it can be cumbersome to track the state of our program. We would potentially have to reason like "If the result of my first measurement is A and the result of my second measurement is B ... then I am in state $|\Psi\rangle$.

Now we look at a different method of describing our quantum state called Density Operators which have several advantages. For one they allow us to view our wires as distributions of states, solving the problem above. Later in the course we will see how they also allow us to define a measure of distinguishability between two states - to bound the probability with which a distinguisher could tell apart two different states.

2 Warmup: Quantum State Probability Distributions

First, we can solve the above problem of being able to speak about our quantum states as distributions. In the above scenario we would say that we start with the

distribution

$$E_1 = \{|+\rangle @ 1\}$$

and after measuring our distribution is

$$E_2 = \{|0\rangle @ \frac{1}{2},\ |1\rangle @ \frac{1}{2}\}$$

Note that this explicitly says that our wire has the state $|0\rangle$ with $\frac{1}{2}$ probability and the same for $|1\rangle$. This is **not** a superposition of states. This is a distribution of states. And using our predefined rules, we can also apply unitaries to it.

$$E_3 = HE_2 = \{H|0\rangle @ \frac{1}{2},\ H|1\rangle @ \frac{1}{2}\} = \{|+\rangle @ \frac{1}{2},\ |-\rangle @ \frac{1}{2}\}$$

Notice how if we were to measure this in the computational basis, we could describe the post-measurement state of our system as just

$$E_4 = \{|0\rangle @ \frac{1}{2}, |1\rangle @ \frac{1}{2}\}$$

As the path at which we arrive to one of these outcomes does not matter in terms of describing the quantum state on the wire.

In this course we will often use the terms "pure state" and "mixed state". A pure state is described with $E_p = \{|\Psi\rangle @ 1\}$ for some $|\Psi\rangle$ and a mixed state refers to a distribution of more than one states (e.g E_2).

3 Density Operators

Density operators are similar to quantum state probability distributions, as they allow us to define a distribution using only a single matrix. The density operator for a pure state $|\Psi\rangle$ is just $|\Psi\rangle\langle\Psi|$. Remember that $\langle\Psi|$ is $(|\Psi\rangle)^\dagger$, the conjugate transpose of $|\Psi\rangle$. For a mixed state like E_4 above, we take the sum of all the pure state density matrices, and scale them with their respective probabilities.

$$\rho_{E_4} = \frac{1}{2} \cdot |0\rangle\langle 0| + \frac{1}{2} \cdot |1\rangle\langle 1| = \frac{1}{2} I$$

Note that our density matrices can also have off-diagonal elements. For example for the state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ the corresponding density matrix is

$$\begin{aligned}
\rho &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle))^\dagger = \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)(\frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)) = \\
&= \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)
\end{aligned}$$

Generally we don't compute out the actual value of the density matrix, and often leave it as a general formula. For that reason it is important to be comfortable using different properties of linear algebra. Luckily we won't need all that many and they are fairly intuitive.

Useful properties:

- $(A \otimes B)(C \otimes D) = (AC) \otimes (BC)$
- $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$
- $(A + B)^\dagger = A^\dagger + B^\dagger$
- $(AB)^\dagger = B^\dagger A^\dagger$
- $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
- $A \otimes (B + C) = A \otimes B + A \otimes C$
- $(B + C) \otimes A = B \otimes A + C \otimes A$

If you're ever confused by a step in a computation, then unless specified otherwise it is most likely one of these properties being applied.

4 Partial Trace

The partial trace corresponds to "throwing away" a part of the system and restricting our view to the rest. This can also be viewed as measuring and forgetting part of the system. The result of the trace represents all of the information that can be extracted from the initial state ρ given only the subsystem that you haven't "thrown away".

Suppose we have a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ which consists of a separate "A" and "B" subsystems. Then given a density operator $\rho = \sigma \otimes \tau$ where σ corresponds to the $\mathcal{H}_A$ part and τ to the $\mathcal{H}_B$, we say that tracing away the "A" part corresponds to $tr_A\ \sigma \otimes \tau = (tr\ \sigma) \cdot \tau$ and tracing away the "B" part is $tr_B\ \sigma \otimes \tau = \sigma \cdot tr\ \tau$.

It is important to note that by tr_X we denote "tracing away subsystem X" and by just tr we signify the trace of a matrix: $tr\ A = \sum_i A_{ii}$.

As an example, let's try to trace away the second qubit of the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We found its density matrix earlier.

$$\rho = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$$

Unfortunately this is not in a nice $\sigma \otimes \tau$ form. Luckily the trace operator is linear, meaning $tr_A(u + v) = tr_A\ u + tr_A\ v$. And the summands we have are very easily expressible via tensors.

Remember that by $|00\rangle$ we really mean $|0\rangle \otimes |0\rangle$. Thus $|00\rangle\langle 00|$ is $(|0\rangle \otimes |0\rangle)(\langle 0| \otimes \langle 0|) = |0\rangle\langle 0| \otimes |0\rangle\langle 0|$. We can apply this to each summand separately to get our density operator in a nicer form.

$$\rho = \frac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|)$$

And now we can apply the trace operation on it.

$$tr_B\rho = \frac{1}{2}(|0\rangle\langle 0| \cdot tr\ |0\rangle\langle 0| + |0\rangle\langle 1| \cdot tr\ |0\rangle\langle 1| + |1\rangle\langle 0| \cdot tr\ |1\rangle\langle 0| + |1\rangle\langle 1| \cdot tr\ |1\rangle\langle 1|)$$

Now notice that for two **basis** vectors i, j the matrix $|i\rangle\langle j|$ is going to have only one non-zero entry on row i and column j. This means that its trace (as in the sum of elements on diagonal) $tr\ |i\rangle\langle j|$ will be 0 when $i \neq j$ and 1 when $i = j$. This allows us to easily find traces of elements like $tr\ |0\rangle\langle 1|$.

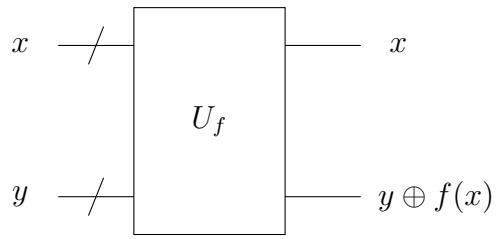
$$tr_B\ \rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}I$$

This is the exact same as the density operator for the ensemble E_2 which we got by measuring $|+\rangle$ in the computational basis. So while we started in an EPR pair, by tracing out one of the qubits we have effectively measured (and forgotten the result) of the one that's left.

5 Example: Constructing unitary boolean functions

5.1 The ideal construction

For an example of a more "general" density matrix, let's describe the density operator after evaluating U_f in superposition. Recall that $U_f|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$. Consider the following system consisting of a n-qubit "input" register and a m-qubit "output" register.



The state in the start of our system is some unknown $|\Psi\rangle$. We can express it as $|\Phi\rangle = \sum_{xy} \alpha_{xy}|x, y\rangle$ for our basis vectors (we may not know what the individual α but they exist). And then after applying U_f we have $|\Psi\rangle = \sum_{xy} \alpha_{xy}|x, y \oplus f(x)\rangle$. Now to compute the corresponding density matrix we get

$$\rho = |\Psi\rangle\langle\Psi| = (\sum_{xy} \alpha_{xy}|x, y \oplus f(x)\rangle)(\sum_{\tilde{x}\tilde{y}} \alpha_{\tilde{x}\tilde{y}}|\tilde{x}, \tilde{y} \oplus f(\tilde{x})\rangle)^\dagger$$

Currently the reason the second sum has j rather than $\tilde{x}$ and $\tilde{y}$ is not currently significant, but it soon will be. Because now we can apply $(A + B)^\dagger = A^\dagger + B^\dagger$.

$$\rho = (\sum_{i} \alpha_i|i, f(i)\rangle)(\sum_{j} \alpha_j^*\langle j, f(j)|)$$

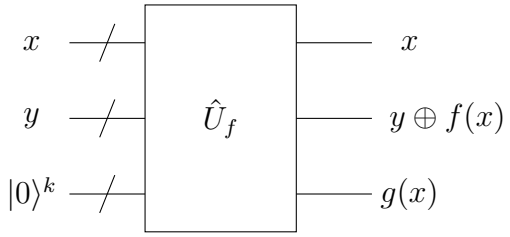
And now we have a product between two big sums, which is just a big sum of pairwise product, same as if you had $(a+b+c)(a+b+c) = aa+ab+ac+bb+bc+cb+cc$ which is why we need the $\tilde{x}$ and $\tilde{y}$ because for each xy (like a above) we are multiplying it all other elements from the second sum (conjugate transpose) (giving $aa + ab + ac$). And thus we reach

$$\rho_{ideal} = \sum_{xy\tilde{x}\tilde{y}} \alpha_{xy}\alpha^*_{\tilde{x}\tilde{y}}|x, y \oplus f(x)\rangle\langle\tilde{x}, \tilde{y} \oplus f(\tilde{x})|$$

5.2 What happens without properly cleaning up

In our lab we found a way to evaluate arbitrary boolean functions. Any boolean circuit can be implemented using only $\wedge$ and $\neg$ and these we can implement using the Toffoli gate, the NOT-gate and some extra buffer qubits.

However this leaves some intermediate values in the buffer qubits, which may depend on our input. So what we have is a $\hat{U}_f|x, y, 0\rangle \to |x, y \oplus f(x), g(x)\rangle$. The function g represents the leftover values that may depend on x.



What happens if we were to simply throw away these buffer qubits that we don't need anymore? Since we can take partial traces, we can answer this question. We can take the density operator almost identically to what we did in section 5.1.

$$\rho = \sum_{xy\tilde{x}\tilde{y}} \alpha_{xy}\alpha^*_{\tilde{x}\tilde{y}}|x, y \oplus f(x), g(x)\rangle\langle\tilde{x}, \tilde{y} \oplus f(\tilde{x}), g(\tilde{x})|$$

Now let's start tracing out our buffer subsystem (let's call it C, with k qubits). The computation works similarly to the example in section 4 by first expressing the summands as tensors.

$$\rho = \sum_{xy\tilde{x}\tilde{y}} \alpha_{xy}\alpha^*_{\tilde{x}\tilde{y}}|x, y \oplus f(x)\rangle\langle\tilde{x}, \tilde{y} \oplus f(\tilde{x})| \otimes |g(x)\rangle\langle g(\tilde{x})|$$

And now the trace result will depend on the function g. Let's view a drastic case where the g is an injective function, meaning that the output is unique for each input. For simplicity let's say $g(x) = x$. We can simplify our density matrix by evaluating g.

$$\rho = \sum_{xy\tilde{x}\tilde{y}} \alpha_{xy}\alpha^*_{\tilde{x}\tilde{y}}|x, y \oplus f(x)\rangle\langle\tilde{x}, \tilde{y} \oplus f(\tilde{x})| \otimes |x\rangle\langle\tilde{x}|$$

Then similarly as before, since these are basis vectors we can say that $|i\rangle\langle j|$ has trace 0 when $i \neq j$ and 1 when $i = j$. Meaning the only summands left are the ones where $x = \tilde{x}$ and $y = \tilde{y}$. And since $\alpha_{xy}\alpha^*_{\tilde{x}\tilde{y}} = |\alpha_{xy}|^2$ we have our final density matrix.

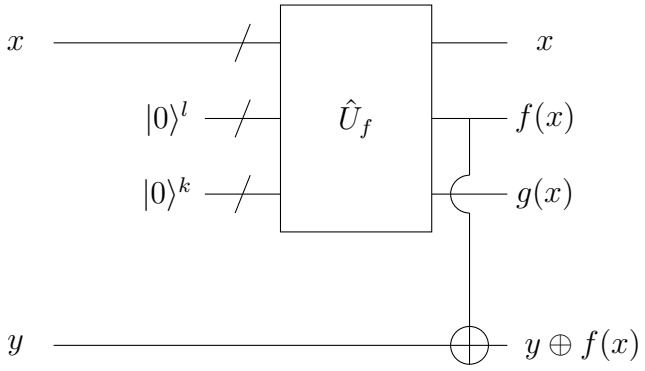
$$tr_C(\rho) = \sum_{xy} |\alpha_{xy}|^2|x, y \oplus f(x)\rangle\langle x, y \oplus f(x)|$$

And this is completely different from the ρ_{ideal} we got at the end of the section 5.1! This is a purely diagonal matrix - it doesn't contain non-diagonal entries. This means that this is no longer a superposition.

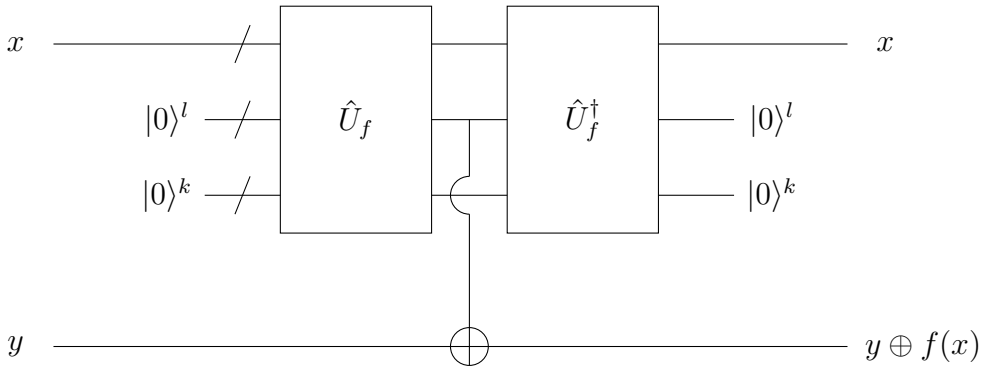
We have shown this for $g(x) = x$. But this also holds for all injective g function. In our argumentation it was important whether or not $x = \tilde{x}$ in $|x\rangle\langle\tilde{x}|$. In the case of some unknown (but injective) g, what will matter is if $g(x) = g(\tilde{x})$ in $|g(x)\rangle\langle g(\tilde{x})|$. And from injectivity we know that this is true only if $x = \tilde{x}$.

6 Cleaning up properly

So from the previous section we know that we can't just throw away our buffer qubits. However we can use our $\hat{U}_f$ by first applying it to a buffer register, not the "y" register, and then CNOT'ing the result over to the register containing "y".

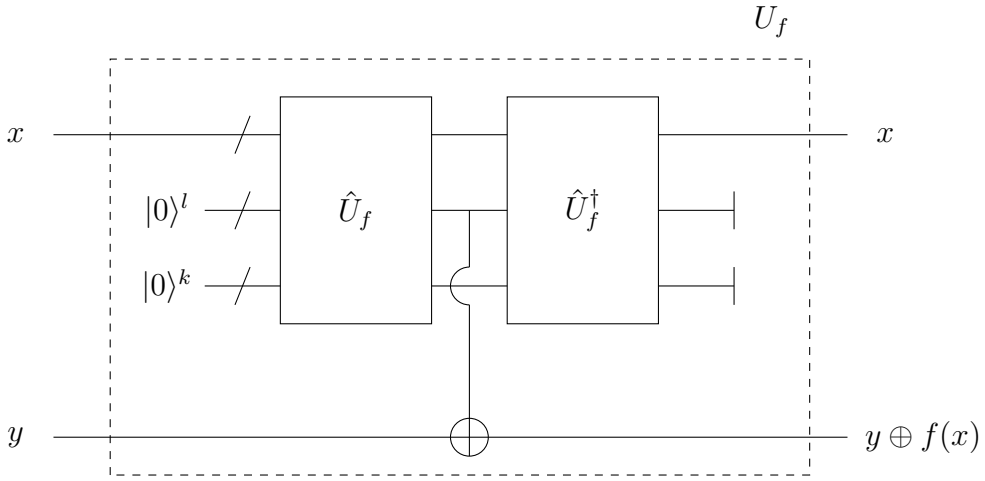


And then we can run the inverse of $\hat{U}_f$ on the first three registers. We know that this exists - it's $\hat{U}_f^\dagger$. And this clearly reverts the first three registers' values to what they were before.



And now since the buffer qubits are reset to zeroes again (and are independent of the input register), they are now safe to trace away. To see that this is true, you can try to do the above tracing we did in section 6, and use $g(x) = c$ for some arbitrary constant. Every summand will have $|c\rangle\langle c|$ which has trace 1, and you will get ρ_{ideal} from section 5.1.

And thus finally, if we add in and then trace away the buffer qubits, we have our ideal unitary implementation from section 5.1.


U_f
x
$|0\rangle^l$
$|0\rangle^k$
$\hat{U}_f$
$\hat{U}_f^\dagger$
x
y
$y \oplus f(x)$