Institut für Theoretische Physik
der Universität zu Köln

Rochus Klesse
Laurens Ligthart , Felipe Montealegre-Mora

Quantum Information Theory – Sheet 2

Wintersemester 2021/22

Webpage: *http://www.thp.uni-koeln.de/∼rk/qit_22.html/*

Submission of solutions as pdf-file until Thursday, May 5, 12 pm, to
ligthart.exams[at]gmail.com
Joint solutions of teams with up to three members are allowed, welcomed, and highly recommended!

4. Purifications (solution) *6 points*

We start from the Schmidt decomposition of the states

$$|\Psi_1\rangle = \sum_i \lambda_i \, |a_i\rangle \, |b_i\rangle \,,$$
$$|\Psi_2\rangle = \sum_i \lambda'_i \, \big|a'_i\big\rangle \, \big|b'_i\big\rangle \,,$$

where $\{|a_i\rangle\}$, $\{|a'_i\rangle$ are orthonormal sets of states in A, and similarly $\{|b_i\rangle\}$, $\{|b'_i\rangle$ are orthonormal sets in B. We assume that the Schmidt spetrum is non-degenerate (i.e., $\lambda_i \neq \lambda_{i'}$ for $i \neq i'$). Taking the partial trace,

$$\rho_A = \mathrm{tr}_B \, |\Psi_1\rangle\langle\Psi_1| = \sum_i \lambda_i \, |a_i\rangle\langle a_i| = \mathrm{tr}_B \, |\Psi_2\rangle\langle\Psi_2| = \sum_i \lambda'_i \, \big|a'_i\big\rangle\big\langle a'_i\big| \,.$$

Because ρ_A has a non-degenerate spectrum, this equation gives the unique diagonalization of that matrix. In particular, $\lambda_i = \lambda'_i$ and $|a_i\rangle\langle a_i| = |a'_i\rangle\langle a'_i|$ (and thus $|a'_i\rangle = e^{i\alpha_i} \, |a_i\rangle$). Let $|c_i\rangle := e^{i\alpha_i} \, |b'_i\rangle$— notice that the set $\{|c_i\rangle\}$ is also orthonormal in B. Then,

$$|\Psi_1\rangle = \sum_i \lambda_i \, |a_i\rangle \, |b_i\rangle \,,$$
$$|\Psi_2\rangle = \sum_i \lambda_i \, |a_i\rangle \, |c_i\rangle \,.$$

Finally, complete the sets $\{|b_i\rangle\}$ and $\{|c_i\rangle\}$ to two orthonormal bases of B. Then the linear map U_B on B defined by the relations $U_B \, |c_i\rangle = |b_i\rangle$ is unitary:

$$\langle c_i| \, U_B^\dagger U_B \, |c_j\rangle = \delta_{ij} \implies U_B^\dagger U_B = \mathbf{1}.$$

Finally, by construction $\Psi_1 = (\mathbf{1} \otimes U_B)\Psi_2$.

5. Measurements on the other systems don't matter (solution) *6 points*

Following the hint: we may expand O_{AB} as a sum of product operators

$$O_{AB} = \sum_i O_A^{(i)} \otimes O_B^{(i)}.$$

Then

$$\begin{aligned}\mathrm{tr}_B(\mathbf{1}_A \otimes B)O_{AB} &= \sum_i \mathrm{tr}_B\left((\mathbf{1}_A \otimes B)(O_A^{(i)} \otimes O_B^{(i)})\right)\\ &= \sum_i O_A^{(i)}\,\mathrm{tr}\left(BO_B^{(i)}\right)\\ &= \sum_i O_A^{(i)}\,\mathrm{tr}\left(O_B^{(i)}B\right)\\ &= \sum_i \mathrm{tr}_B\left((O_A^{(i)} \otimes O_B^{(i)})(\mathbf{1}_A \otimes B)\right)\\ &= \mathrm{tr}_B\, O_{AB}(\mathbf{1}_A \otimes B)\end{aligned}$$

It follows from this that

$$\begin{aligned}\mathrm{tr}_B\,\rho'_{AB} &= \sum_l \mathrm{tr}_B(\mathbf{1}_A \otimes M_l)\rho_{AB}(\mathbf{1}_A \otimes M_l^\dagger)\\ &= \sum_l \mathrm{tr}_B\,\rho_{AB}(\mathbf{1}_A \otimes M_l^\dagger M_l)\\ &= \mathrm{tr}_B\,\rho_{AB},\end{aligned}$$

where the last equality follows from

$$\sum_l M_l^\dagger M_l = \mathbf{1}_B.$$

6. Equivalent circuits (solution)

6 points

Equivalence of the controlled Z: one may directly verify that they act in the same way on the computational basis,

$$|00\rangle \mapsto |00\rangle\,, \quad |01\rangle \mapsto |01\rangle\,, \quad |10\rangle \mapsto |10\rangle\,, \quad |11\rangle \mapsto -|11\rangle\,.$$

On the CNOT circuits: Recall that $H^2 = \mathbf{1}$. We will show the equivalent statement

$$(H \otimes H)CNOT_{21} = CNOT_{12}(H \otimes H).$$

Consider any computational basis element $|a, b\rangle$. Then, a short calculation shows that

$$(H \otimes H)\,|a, b\rangle = \frac{1}{2}\sum_{a',b'}(-1)^{a'a+b'b}\left|a', b'\right\rangle,$$

and

$$CNOT_{12}\,|a, b\rangle = |a, a + b \mod 2\rangle\,, \quad CNOT_{21}\,|a, b\rangle = |a + b \mod 2, b\rangle\,.$$

Throughout the rest of the proof we simply write $a + b$ to denote $a + b \mod 2$.
This way, on the one hand,

$$\begin{aligned}(H \otimes H)CNOT_{21}\,|a, b\rangle &= (H \otimes H)\,|a + b, b\rangle\\ &= \frac{1}{2}\sum_{a',b'}(-1)^{a'(a+b)+b'b}\left|a', b'\right\rangle.\end{aligned}$$

On the other hand,

$$CNOT_{12}(H\otimes H)\left|a,b\right\rangle = \frac{1}{2}\sum_{a',b'}(-1)^{a'a+b'b}CNOT_{12}\left|a',b'\right\rangle \tag{1}$$

$$= \frac{1}{2}\sum_{a',b'}(-1)^{a'a+b'b}\left|a',a'+b'\right\rangle . \tag{2}$$

Relabelling the variables in the last sum: $c' := a'$ and $d' := a' + b'$, so $b' = d' + a'$, we obtain

$$\frac{1}{2}\sum_{c',d'}(-1)^{c'a+(d'+c')b}\left|c',d'\right\rangle = \frac{1}{2}\sum_{c',d'}(-1)^{c'(a+b)+d'b}\left|c',d'\right\rangle \tag{3}$$

we see that (2) and (3) are the same state. Since this holds for arbitrary a, b, this implies the two unitary operators are equal.

7. Classical and quantum CCNOT (solution) *2+2+2+0=6 points*

a) Using the hint: it is sufficient to show how to implement the NAND and BRANCH gates using CCNOTs. Consider a CCNOT controlling on the first two bits and acting on the third one:

$$CCNOT(a,b,c) = \begin{cases}(a,b,c), & \text{if } a \text{ or } b \neq 1,\\ (a,b,c+1), & \text{if } a,b=1,\end{cases}$$

where, as before $c+1 := c+1 \mod 2$. We may rewrite this action as $CCNOT(a,b,c) = (a,b,c+ab)$. Then, $CCNOT(a,b,1) = (a,b,1+AND(a,b)) = (a,b,NAND(a,b))$, thus the outcome of the NAND gate is obtained in the third bit. Similarly, $CCNOT(a,1,0) = (a,1,AND(a,1)) = (a,1,a)$, so the first and third bits contain the output of $BRANCH(a)$.

b) Acting on a computational basis state $|a,b,c\rangle$ with the circuit on the right,

$$\begin{aligned}CV_{13}CX_{12}CV_{23}^{\dagger}CX_{12}CV_{23}\left|a,b,c\right\rangle &= CV_{13}CX_{12}CV_{23}^{\dagger}CX_{12}\left|a\right\rangle\left|b\right\rangle\left(V^b\left|c\right\rangle\right)\\ &= CV_{13}CX_{12}CV_{23}^{\dagger}\left|a\right\rangle\left|a+b\right\rangle\left(V^b\left|c\right\rangle\right)\\ &= CV_{13}CX_{12}\left|a\right\rangle\left|a+b\right\rangle\left((V^{\dagger})^{a+b}V^b\left|c\right\rangle\right)\\ &= CV_{13}\left|a\right\rangle\left|b\right\rangle\left((V^{\dagger})^{a+b}V^b\left|c\right\rangle\right)\\ &= \left|a\right\rangle\left|b\right\rangle\left(V^a(V^{\dagger})^{a+b}V^b\left|c\right\rangle\right),\end{aligned}$$

where, remember, I've used the short notation $a+b := a+b \mod 2 \in \{0,1\}$. If a or $b \neq 1$, then the factors of V and $V^{\dagger}$ cancel out in the equation above: for example if $a=0$ and $b=1$, it holds that $V^a(V^{\dagger})^{a+b}V^b = V^0(V^{\dagger})^1V^1 = V^{\dagger}V = \mathbf{1}$. This holds similarly for the other cases. If $a,b=1$, then $a+b=0$ so that $(V^{\dagger})^{a+b} = (V^{\dagger})^0 = \mathbf{1}$. Thus, in this case the factors on the third qubit combine to

$$V^a(V^{\dagger})^{a+b}V^b = V\mathbf{1}V = V^2 = U.$$

In summary, we have that, denoting by $\mathcal{C}$ the circuit on the right-hand side of the claimed equation,

$$\begin{aligned}\mathcal{C}\left|a,b,c\right\rangle &= \begin{cases}\left|a,b,c\right\rangle & \text{if } a \text{ or } b \neq 1,\\ (\mathbf{1}\otimes\mathbf{1}\otimes U)\left|1,1,c\right\rangle\end{cases}\\ &= CU\left|a,b,c\right\rangle ,\end{aligned}$$

for all a,b,c. Thus the two operators are equal.

c) It is sufficient to find a V such that $V^2 = X$ and substitute it in the circuit above. We may express the matrix $X = |+\rangle\langle+| - |-\rangle\langle-|$ in its diagonalized form. Then, the matrix $V = |+\rangle\langle+| + i\,|-\rangle\langle-|$ satisfies $V^2 = X$.

d) By c), using two-qubit quantum gates we may implement the CCNOT gate. Moreover, by a), any classical circuit (decomposed into NAND and BRANCH gates) may be performed using CCNOT gates and using a number of additional bits which is at most twice the (NAND,BRANCH)-circuit length. This implies that any finite (NAND,BRANCH)-circuit may be substituted by an equivalent finite CCNOT-circuit.
Encoding bitstrings $(a, b, c, \dots)$ as their corresponding computational basis element $|a, b, c, \dots\rangle$ on the quantum computer, we may perform the classical circuit on the quantum computer. The outcome of the quantum circuit will be the encoding of the outcome of the classical circuit. Finally, measuring the computational basis at the end of the circuit will deterministically (i.e., with probability = 1) produce the outcome of the classical circuit (this follows because the outcome of a quantum circuit that only uses CCNOT gates is a computational basis state).

8. Circuit for an ideal measurement (solution) *6 points*

At the different stages of the circuit, the state of the system is:

$$\begin{aligned}
|\psi_1\rangle &:= (H\,|0\rangle)\,|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|\psi\rangle \\
|\psi_2\rangle &:= \frac{1}{\sqrt{2}}(|0\rangle\,|\psi\rangle + |1\rangle\,U\,|\psi\rangle \\
|\psi_3\rangle &:= \frac{1}{2}(|0\rangle\,|\psi\rangle + |1\rangle\,|\psi\rangle + |0\rangle\,U\,|\psi\rangle - |1\rangle\,U\,|\psi\rangle) \\
&= \frac{1}{2}(|0\rangle\,(\mathbf{1}+U)\,|\psi\rangle + |1\rangle\,(\mathbf{1}-U)\,|\psi\rangle),
\end{aligned}$$

here, $|\psi_3\rangle$ is the state right before the measurement. Upon measuring the computational basis on the first qubit, the following happens: if the outcome is "0," then the post-measurement state is

$$|\phi_+\rangle := c_+(\mathbf{1}+U)\,|\psi\rangle\,,$$

where $c_+ \in \mathbb{R}_+$ is a normalization constant. If, instead, the outcome is "1," the post-measurement state is

$$|\phi_-\rangle := c_-(\mathbf{1}-U)\,|\psi\rangle\,.$$

Finally $U\,|\phi_\pm\rangle = c_\pm(U \pm U^2)\,|\psi\rangle = c_\pm(U \pm \mathbf{1})\,|\psi\rangle = \pm\,|\phi_\pm\rangle$.
Added notes: we may diagonalize the operator U. By doing so, it becomes clear that $\frac{1}{2}(\mathbf{1}+U)$ projects onto the "+" eigenspace of U, and similarly $\frac{1}{2}(\mathbf{1}-U)$ onto the "-" eigenspace. This provides an alternative proof of the last statement.
Finally, let's look at the probability of each outcome:

$$\begin{aligned}
p_0 &= \mathrm{tr}((|0\rangle\langle 0| \otimes \mathbf{1})(|\psi_3\rangle\langle\psi_3|)) = \langle\psi|\,\frac{1}{2}(\mathbf{1}+U)\,|\psi\rangle\,, \\
p_1 &= \mathrm{tr}((|1\rangle\langle 1| \otimes \mathbf{1})(|\psi_3\rangle\langle\psi_3|)) = \langle\psi|\,\frac{1}{2}(\mathbf{1}-U)\,|\psi\rangle\,.
\end{aligned}$$

We can see that what the circuit is doing is *literally* measuring U on the state $|\psi\rangle$. Indeed, the probabilities of each outcome are given by the Born-rule probabilities obtained by measuring U, and the post-measurement state is given exactly as if we would have measured U directly on $|\psi\rangle$. If it barks like a U measurement, and looks like a U measurement, and wags its tail like a U measurement, it *is* a U measurement.