Quantum Cryptography (spring 2020) Dominique Unruh

Exercise Sheet 5

Out: 2020-04-05 Due: 2020-04-15

Problem 1: Purification

Compute purifications of the following density operators:

$$\rho_1 := \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \qquad \rho_2 := \tfrac{1}{2}|00\rangle\langle 00| + \tfrac{1}{2}|11\rangle\langle 11|, \qquad \rho_3 := \begin{pmatrix}\frac{1}{2} & \frac{1}{4}\\ \frac{1}{4} & \frac{1}{2}\end{pmatrix}.$$

Hint: Eigenvectors of ρ_3 are $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.

Problem 2: Deutsch-Jozsa Algorithm

Assume that $f : \{0,1\}^n \to \{0,1\}$ is a function that satisfies one of the following two properties:

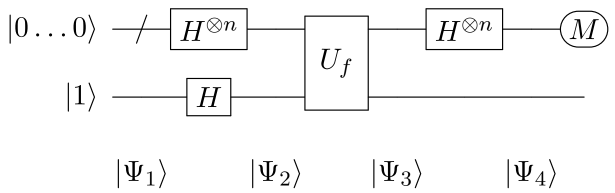
- f is constant (i.e., $f(x) = f(y)$ for all $x, y \in \{0,1\}^n$), or
- f is balanced (i.e., $|\{x : f(x) = 0\}| = |\{x : f(x) = 1\}| = 2^{n-1}$).

That is, we have the promise that f is constant or balanced, but we do not know which of the two holds.

Let U_f be the unitary transformation on $\mathbb{C}^{2^{n+1}}$ defined by

$$U_f|x, y\rangle = |x, y \oplus f(x)\rangle \qquad (x \in \{0,1\}^n, y \in \{0,1\}).$$

Consider the following circuit:



where M is a complete measurement in the computational basis.

The $|\Psi_i\rangle$ denote the intermediate states after the individual steps of the algorithm. E.g., $|\Psi_1\rangle = |0\dots01\rangle$.

(a) What is $|\Psi_2\rangle$?

(b) Show that

$$|\Psi_3\rangle = \sum_{x\in\{0,1\}^n} 2^{-n/2-1/2}|x, f(x)\rangle - 2^{-n/2-1/2}|x, \overline{f(x)}\rangle.$$

(Here $\overline{f(x)} := 1 - f(x)$.)

(c) Show that

$$|\Psi_3\rangle = \Big(2^{-n/2} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle\Big) \otimes |-\rangle$$

Here $|-\rangle$ is short for $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.

(d) Show that $H^{\otimes n}|x\rangle = 2^{-n/2} \sum_{z\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle$ where $x \cdot z := \sum_{i=1}^n x_i z_i$.

(e) What is $|\Psi_4\rangle$?

(f) Show that the probability P of measuring $0\dots0$ in the measurement is $\big(2^{-n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\big)^2$.

(g) Compute the probability P of measuring $0\dots0$ in the case that f is constant.

(h) Compute the probability P of measuring $0\dots0$ in the case that f is balanced.

Problem 3: Quantum Operations (Bonus Problem)

Describe the partial trace as a quantum operation. More exactly, let $\mathcal{H}_A = \mathbb{C}^n$, $\mathcal{H}_B = \mathbb{C}^m$. Find operators $E_k : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A$ such that these define a quantum operation $\mathcal{E} = \{E_k\}_k$ with the property that $\mathcal{E}(\rho) = \operatorname{tr}_B \rho$ for all ρ. Show that $\mathcal{E}$ is indeed a quantum operation (i.e., that the E_k are valid operators for defining a quantum operation).

Hint: For density operators ρ we have $\operatorname{tr}\rho = \sum_k \langle k|\rho|k\rangle$. Note that here $\langle k|$ is a linear operator from $\mathcal{H}_B$ to $\mathbb{C}$. And $I \otimes \langle k|$ is a linear operator from $\mathcal{H}_A \otimes \mathcal{H}_B$ to $\mathcal{H}_A \otimes \mathbb{C} = \mathcal{H}_A$. Note that it is sufficient to check that $\mathcal{E}(\rho) = \operatorname{tr}_B \rho$ for $\rho = \sigma \otimes \tau$, the rest follows by linearity.