Lehr- und Forschungsgebiet
Mathematische Grundlagen der Informatik
RWTH Aachen
Prof. Dr. E. Grädel, D. Fischer, T. Ganzow,
B. Puchala

WS 09/10

Complexity Theory and Quantum Computing — Assignment 9

Due: Monday, January 11, 12:00

Exercise 1

We consider the Hilbert spaces $H_{2^n} = H_2 \otimes \ldots \otimes H_2$ (n times) with the standard computational basis $(|0\ldots0\rangle, \ldots, |1\ldots1\rangle)$.

(a) Which of the following vectors in H_2 are possible states of a qubit?
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{\sqrt{3}}{2}|1\rangle - \frac{1}{2}|0\rangle$, $0.7|0\rangle + 0.3|1\rangle$, $0.8|0\rangle + 0.6|1\rangle$, $\cos\vartheta|0\rangle + i\sin\vartheta|0\rangle$, $\cos^2\vartheta|0\rangle - \sin^2\vartheta|1\rangle$.

(b) For each valid state among the above vectors, give the probabilities of observing $|0\rangle$ and $|1\rangle$ when the state is measured. What are the probabilities of the two outcomes when the state is measured in the basis $(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$ instead of the standard computational basis?

(c) A two-qubit system is in the state $\frac{1}{\sqrt{30}}(|00\rangle + 2i|01\rangle - 3|10\rangle - 4i|11\rangle)$ and the first qubit is measured. What is the probability that the outcome of the measurement is $|1\rangle$? What is the state of the system after the measurement if the outcome actually is $|1\rangle$? What is the probability that a subsequent measurement of the second qubit will observe a $|0\rangle$?

(d) Consider the EPR-pair $|\vartheta\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Assume a two-qubit system is in the state $|\vartheta\rangle$ and the first qubit is measured and observed to be $|\sigma\rangle$ with $\sigma \in \{0, 1\}$. What are the probabilities, that a subsequent measurement of the second qubit will observe $|\sigma\rangle$ and $|1-\sigma\rangle$, respectively? What if we measure the second qubit first?

Exercise 2

(a) Show that the following measurements of a two-qubit quantum register yield the same probability distribution over outcomes.

  (1) Measure the register.
  (2) Measure the first qubit, then measure the second qubit.
  (3) Measure the second qubit, then measure the first qubit.

(b) Assume that $|\vartheta\rangle$ is an entangled state of a two-qubit register and the first qubit of the register is measured with outcome $|\sigma\rangle$. Prove or disprove that the probability that a subsequent measurement of the second qubit of the register yields $|1-\sigma\rangle$ is 0.

Exercise 3

(a) Express the state $|\varphi\rangle \otimes |\varphi\rangle$ where $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the Bell basis:

$$\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\right).$$

(b) Design a matrix that maps, for any $i \in \{1, 2, 3, 4\}$, the i-th Bell basis vector in H_4 to the i-th standard basis vector.

(c) For each one of the following operations: NOT, cNOT, and ccNOT (Toffoli) (see Exercise 4), write down the 8×8 matrix that describes the mapping induced by applying this operation to the first qubits of a three-qubit register.

Exercise 4

We consider *reversible Boolean functions*, i.e., permutations $f : \{0,1\}^n \to \{0,1\}^n$. Obviously, Boolean functions like AND are not reversible, i.e., you cannot deduce the input values from the output. However, each non-reversible Boolean function can be realised by reversible ones using additional inputs (set to zero or one) and ouputs (that may be discarded), also called *source* and *sink* bits, respectively.

The so-called *Toffoli gate* with three inputs and outputs represents the reversible function $f(x_1, x_2, x_3) = (x_1, x_2, (x_1 \wedge x_2) \oplus x_3)$.

Realise the following functions using only Toffoli gates (first determine the number of necessary additional bits):

- AND;
- cNOT, where $\text{cNOT}(x_1, x_2) = (x_1, x_1 \oplus x_2)$;
- COPY (or FAN-OUT), where $\text{COPY}(x_1) = (x_1, x_1)$.