INF587 Exercise sheet 1

Recall that (Hadamard basis)

$$|+\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad |-\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Exercise 1. *Determine whether the following states are qubits or not:*

- $\frac{1}{3}|0\rangle - \frac{2}{3}|1\rangle$.
- $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|+\rangle$.
- $\frac{1}{2}|0\rangle + (1 - \frac{1}{\sqrt{2}})|+\rangle + \frac{1}{2}|1\rangle$.

Exercise 2.

1. *Compute the scalar product between* $|+1\rangle$, $|10\rangle$ *and* $|11\rangle$.
2. *Let* $(|e_0\rangle, |e_1\rangle)$ *be an orthonormal basis of* $\mathbb{C}^2$. *Show that* $(|e_{i_1}\rangle \cdots |e_{i_n}\rangle)$ *for* $i_1, \dots, i_n \in \{0,1\}^n$ *is an orthonormal basis of* $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} = \mathbb{C}^{2^n}$.
3. *Do we have* $|00\rangle + |10\rangle = (|0\rangle + |1\rangle) \otimes |0\rangle$*?*
4. $(\star)$ *Show that is does not exist* $|\psi_1\rangle$ *and* $|\psi_2\rangle$ *such that*

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\psi_1\rangle \otimes |\psi_2\rangle.$$

   In other words, show that the EPR[1]*-pair* $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *is entangled.*

5. *Do there exist two qubits* $|\psi_1\rangle$ *and* $|\psi_2\rangle$ *such that*

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = |\psi_1\rangle \otimes |\psi_2\rangle.$$

Exercise 3 (No cloning theorem)**.** *Our goal is to prove the no cloning theorem:*

[1]EPR stands for Einstein, Podolsky and Rosen

Theorem. *There is no unitary* $\mathbf{U}$ *on* 2 *qubits that on input* $|\psi\rangle|0\rangle$ *outputs* $|\psi\rangle|\psi\rangle$ *for all qubits* $|\psi\rangle$.

Prove this theorem. To do this, assume that such a unitary $\mathbf{U}$ *exists and obtain a contradiction, for example by computing* $\mathbf{U}|\psi\rangle|0\rangle$ *for* $|\psi\rangle$ *in the computational and in the Hadamard basis,* i.e. $(|+\rangle, |-\rangle)$.

Exercise 4.

1. *Give a qubit such that measuring it in the computational basis simulates a Bernoulli distribution of parameter* p*, namely the outcome is* $|1\rangle$ *with probability* p *and* $|0\rangle$ *with probability* $1-p$.
2. *Let* $(X,Y) \in \{0,1\}$ *be the following dependent Bernoulli random variables*

$$\mathbb{P}(X=1)=p, \quad \mathbb{P}(Y=1 \mid X=1)=p_1 \quad \textit{and} \quad \mathbb{P}(Y=1 \mid X=0)=p_0$$

   Give a two-qubit state such that measuring the first qubit and then the second one it in the computational basis simulates the distribution of (X,Y)*. In other words, the probability to measure* $|bb'\rangle$ *is equal to* $\mathbb{P}((X,Y)=(b,b'))$.

Exercise 5. *Determine whether the following matrices are unitary matrices:*

- $\mathbf{M}_1 \overset{def}{=} |0\rangle\langle 0| + |+\rangle\langle 1|$.
- $\mathbf{M}_2 \overset{def}{=} \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\right)$.
- $\mathbf{M}_3 \overset{def}{=} |+\rangle\langle -| + |-\rangle\langle +|$

Exercise 6. *Show that unitaries cannot "delete" information: there is no* 1*-quibit unitary* $\mathbf{U}$ *that maps* $|\psi\rangle \mapsto |0\rangle$ *for every* 1*-qubit state* $|\psi\rangle$.

Exercise 7. *Let* $f:\{0,1\}\to\{0,1\}$ *be some function. Suppose that you have access to the following quantum gate (why is it a quantum gate?)*

$$\mathbf{U}_f : |x,y\rangle \mapsto |x\rangle|y\oplus f(x)\rangle.$$ [2]

[2] $0\oplus 0 = 1\oplus 1 = 0$ and $1\oplus 0 = 0\oplus 1 = 1$.

1. *How to build the following state ("quantum parallelism") starting from* $|00\rangle$

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

2. *By using the Hadamard gate* $\mathbf{H}$ *and* $\mathbf{U}_f$ *show how to implement*

$$|0,1\rangle \mapsto \frac{1}{2} \sum_{x \in \{0,1\}} (-1)^{f(x)} |x\rangle \otimes (|0\rangle - |1\rangle) .$$

Exercise 8 (The Deutsch-Josza algorithm)**.**

1. *Let* $\mathbf{H}$ *be the quantum Hadamard gate over qubits. Let* $\mathbf{H}^{\otimes n} \stackrel{def}{=} \underbrace{\mathbf{H} \otimes \cdots \otimes \mathbf{H}}_{n \text{ times}}$.

   Show that
$$\forall \mathbf{x} \in \{0,1\}^n, \ \mathbf{H}^{\otimes n} |\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y} \in \{0,1\}^n} (-1)^{\mathbf{x} \cdot \mathbf{y}} |\mathbf{y}\rangle$$

   where $\mathbf{x} \cdot \mathbf{y} \stackrel{def}{=} \sum_{i=1}^{n} x_i y_i$ *(it denotes the standard inner product over* $\{0,1\}^n$*).*

2. *Let* $f : \{0,1\}^n \to \{0,1\}$ *be a function that is either constant or balanced. Suppose that we have access to*

$$\mathbf{U}_f : |\mathbf{x}\rangle |y\rangle \mapsto |\mathbf{x}\rangle |y \oplus f(\mathbf{x})\rangle .$$

   Give the quantum algorithm starting with the $(n+1)$*-quibit* $|0\rangle^{\otimes n} |1\rangle$ *making only one query to* $\mathbf{U}_f$ *and some calls to* $\mathbf{H}^{\otimes n}$ *which decides with certainty if* f *is balanced or not.*

Hint: *use the previous exercise and the Deutsch-Josza algorithm that we have seen during the course.*

Exercise 9. *Let* $\theta \in [0, 2\pi)$, $\mathbf{U}_\theta \stackrel{def}{=} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, $|\psi\rangle \stackrel{def}{=} \mathbf{U}_\theta |0\rangle$ *and* $|\psi^\perp\rangle \stackrel{def}{=} \mathbf{U}_\theta |1\rangle$*. Recall that* $\mathbf{X} = |1\rangle\langle 0| + |0\rangle\langle 1|$ *and* $\mathbf{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$.

1. *Show that* $\mathbf{ZX} |\psi^\perp\rangle = |\psi\rangle$.

2. *Show that* $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *can also be written as* $\frac{1}{\sqrt{2}}\left(|\psi\rangle|\psi\rangle + \left|\psi^\perp\right\rangle\left|\psi^\perp\right\rangle\right)$.

3. *Suppose Alice and Bob start with an* EPR-*pair. Alice applies* $\mathbf{U}_\theta^{-1}$ *to her qubit and then measures it in the computational basis. What state does Bob have if her outcome was* 0*, and what state does he has if her outcome was* 1*?*

4. *Suppose Alice knows the number* θ *but Bob does not. Give a protocol that uses one* EPR-*pair and one classical bit of communication where Bob ends up with the qubit* $|\psi\rangle$.

Exercise 10 (Encoding Integers versus qubits and qudits)**.** *A bit is defined as* $b \in \{0, 1\}$ *and it verifies the following bit operations*

$$0 \oplus 0 = 1 \oplus 1 \quad \textit{and} \quad 0 \oplus 1 = 1 \oplus 0 = 1$$

Given an integer $x \in \mathbb{N}$*, its binary decomposition is* $(b_0, \ldots, b_{M-1}) \in \{0, 1\}^M$ *where*

$$x = \sum_{i=0}^{M-1} b_i \, 2^i$$

In a classical computer, integers are described with their binary decomposition. A classical computer is allowed to perform bit summation. For instance given $1, 5 \in \{0, \ldots, 7\}$,

$$1 \equiv (1, 0, 0, 0) \quad \textit{and} \quad 5 \equiv (1, 0, 1, 0) \longrightarrow (1, 0, 0, 0) \oplus (1, 0, 1, 0) = (1, 1, 1, 0)$$

A classical computer is also allowed to perform bit summation "by keeping the carry". For instance given $1, 5 \in \{0, \ldots, 7\}$,

$$1 \equiv (1, 0, 0, 0) \quad \textit{and} \quad 5 \equiv (1, 0, 1, 0) \longrightarrow (1, 0, 0, 0) + (1, 0, 1, 0) = (0, 1, 1, 0) \equiv 6$$

1. *Given two integers* $x, y \in \{0, \ldots, 2^\ell - 1\}$ *a computer computes their bit summation by keeping the carry, which mathematical operation is it performing?*

2. *Suppose now that you want to perform addition modulo* 3 *with a classical computer. First how do you encode* $t \in \{0, 1, 2\}$*? Which operations do you use to perform addition modulo* 3*?*

3. *It may happen that we consider in quantum computation Hilbert spaces* $\mathbb{C}^q$. *Vectors of norm* 1 *in* $\mathbb{C}^q$ *are called qudits (when* $q = 2$ *it corresponds to qubits). How do we write qudits when* $q = 2^\ell$*?*

4. *How do you write qudits when* q *is not a power of* 2 *with qubits (think classically)? How would you perform the addition modulo* q *quantumly?*