Solutions to the exam in MAT3420, Spring 2020

Problem 1.

Which of the following are possible states of qubits?

a) $\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle$,

b) $\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$,

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

Solution.
An expression $\alpha|0\rangle+\beta|1\rangle$ defines a state, that is, a unit vector, if and only if $|\alpha|^2+|\beta|^2 = 1$. Therefore

a) NO, b) YES, c) YES.

Problem 2.

Suppose we have m input/output qubits and n ancilla qubits. Consider a quantum circuit consisting of one unitary gate U operating on n ancilla qubits. Prove that we won't see any effect of U.

Solution. A (pure) state of the entire system is represented by a unit vector of the form

$$\sum_{x=0}^{2^m-1} |x\rangle \otimes v_x,$$

where v_x are vectors in the state space of the ancilla qubits, with $\sum_x \|v_x\|^2 = 1$. Our circuit transforms this into

$$\sum_x |x\rangle \otimes Uv_x.$$

The probability of the outcome x is therefore $\|Uv_x\|^2 = \|v_x\|^2$, which is independent of U.

Problem 3.

One of the classical subroutines of Shor's factoring algorithm computes the modular inverse of a number. Explain this classical algorithm and consider the following example: find the modular inverse of 16 modulo 21, that is, find a number n such that $16n = 1 \mod 21$.

Solution. The algorithm was explained in the last lecture. In this case it runs as follows:

1) Divide 21 by 16 with remainder: $21 = 1 \cdot 16 + 5$.

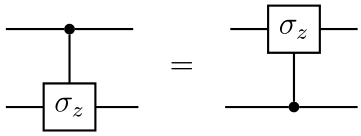
2) Divide 16 by 5 with remainder: $16 = 3 \cdot 5 + 1$. Then rewrite this back in terms of 21 and 16: $16 = 3 \cdot (21 - 1 \cdot 16) + 1$. In other words,

$$4 \cdot 16 - 3 \cdot 21 = 1.$$

As the remainder is already 1, the algorithm stops at this step: the inverse of 16 modulo 21 is 4.

Problem 4.

Prove the following equality of quantum circuits:

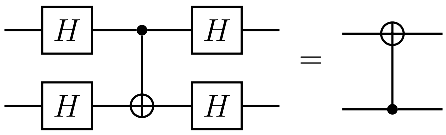


where σ_z is the Pauli matrix (also denoted by Z).

Solution. This can be checked directly on the four input states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. In a bit more concise form, one can also observe that the left hand side maps $|xy\rangle = |x\rangle \otimes |y\rangle$ into $|x\rangle \otimes (-1)^{xy}|y\rangle = (-1)^{xy}|xy\rangle$, and the right hand side maps $|xy\rangle = |x\rangle \otimes |y\rangle$ into $(-1)^{xy}|x\rangle \otimes |y\rangle = (-1)^{xy}|xy\rangle$.

Problem 5.

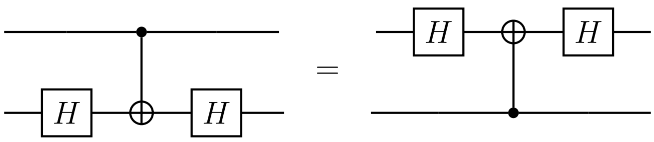
Prove the following equality of quantum circuits:



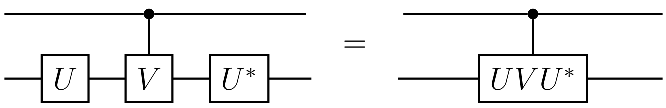
Solution. One possibility is again just to check this directly on the four input states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. But it is also possible to deduce this from the previous problem as follows.

We can apply $H^{-1} = H$ to the first qubit before and after running these circuits. In other words, an equivalent identity is

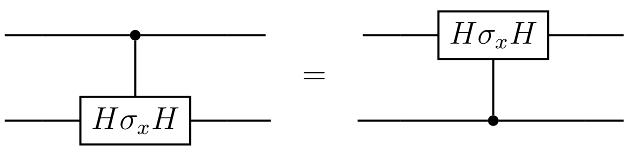
(1)



Next, observe that for any unitary gates U and V we have



It follows that (1) is equivalent to



But $H\sigma_x H = \sigma_z$, so this is exactly the identity from the previous problem.

Problem 6.

Assume we have two quantum circuits U and U' with m input/output qubits and n ancilla qubits, both computing a function f, but U does this without leaving garbage in the ancilla qubits, while U' possibly not. In other words, we have

$$U(|x\rangle \otimes |0\rangle) = |f(x)\rangle \otimes |0\rangle, \qquad U'(|x\rangle \otimes |0\rangle) = |f(x)\rangle \otimes |g(x)\rangle$$

for some function g. What are necessary and sufficient conditions on g for not seeing any difference between U and U' for any (mixed) input state?

Solution. The formulation was unfortunate. The way the problem is formulated, g does not need any special properties. Indeed, implicitly we assume that f is bijective, and therefore by applying the circuits to a state $\sum_x \alpha_x|x\rangle \otimes |0\rangle$ we get

$$U(\sum_x \alpha_x|x\rangle \otimes |0\rangle) = \sum_x \alpha_x|f(x)\rangle \otimes |0\rangle, \quad U'(\sum_x \alpha_x|x\rangle \otimes |0\rangle) = \sum_x \alpha_x|f(x)\rangle \otimes |g(x)\rangle,$$

and in both cases the probability of the outcome $|f(x)\rangle$ for the output qubits is $|\alpha_x|^2$.

Problem 7.

Consider two quantum systems A and B with (finite dimensional) state spaces H_A and H_B. Let $\xi \in H_A \otimes H_B$ be a pure state (unit vector) of the composite system. It can be shown that there exist an orthonormal system of vectors $e_1, \dots, e_n$ in H_A, an orthonormal system of vectors $f_1, \dots, f_n \in H_B$, and numbers $\lambda_k > 0$ such that

$$\xi = \sum_{k=1}^{n} \lambda_k e_k \otimes f_k.$$

This is called a *Schmidt decomposition* of ξ. (See [Chuang–Nielsen], p. 109, for a proof, but it is not needed to solving this problem.) Can you find n without knowing the decomposition? Show that the number n depends only on ξ. It is called the *Schmidt number* of ξ and can be considered as a measure of entanglement of ξ.

Solution. The number n can be expressed as the rank of an operator, or in other words, as the dimension of a vector space, in a number of related ways. For example, as follows.

For every $u \in H_B$ we can define a linear map $\ell_u\colon H_A \otimes H_B \to H_A$ by $\ell_u(v \otimes w) = (w, u)v$. Then, on the one hand, the set of vectors $\ell_u(\xi)$ for all $u \in H_B$ is exactly the linear span of $e_1, \dots, e_n$, so it is a vector space of dimension n. On the other hand, this set depends on ξ itself and not on anything else.