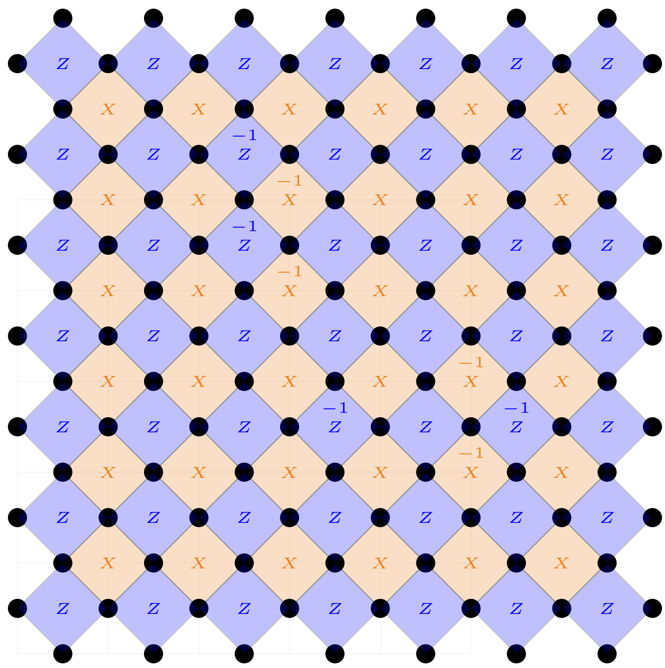
Quantum algorithms 2023/2024: Final exam

Benoît Vermersch (benoit.vermersch@lpmmc.cnrs.fr) - 2023 Dec 18th, 10:30-12:30 (2 hours)

- Documents allowed: Slides of the lectures, documents of the exercices, hand-written notes
- You can only use your laptop to look at the documents from Moodle.
- You can also use printed versions of these documents.
- The use of smartphones or tablets is not allowed.

1 Surface code decoding

1. We recall the definition of the single qubit Pauli Y operator, $Y = iXZ$. Show that $YXY = -X$, and $YZY = -Z$, and explain how the surface code detects single qubit Y errors.
2. With very brief justifications, give a possible list of errors explaining the following measurements of plaquette operators. As in the lecture, the presence of a -1 inside the plaquette means the measured value is -1. Otherwise, the measured value is 1.



2 Warm-ups for Simon's problem

2.1 XOR operations

Note: The following results will be useful for the rest of the exam.

1. Recall the truth table of the XOR operation $A \oplus B$ on two bits A, B.
2. It can be proven easily that the XOR operation is associative, i.e $(A \oplus B) \oplus C = A \oplus (B \oplus C)$. Using this property, show that $B = A \oplus (A \oplus B)$.

2.2 Hadamard gate

Note: The following results will be useful for the rest of the exam.

1. Show that $H^{\otimes n} |0^{\otimes n}\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$, where $\sum_x$ is the sum over all possible 2^n bitstrings $x = (x_1, \dots, x_n)$.
2. Show that $H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_w (-1)^{x.w} |w\rangle$, with $x.w = \sum_i x_i w_i \text{ mod}(2)$. *In the second part of the exam, we will use the fact that $x.w$ can be rewritten as $x.w = x_1 w_1 \oplus x_2 w_2 \oplus \cdots \oplus x_n w_n$ (I am not asking you to prove this).*

3 Simon's problem

We consider a function $f = \{0,1\}^n \to \{0,1\}^n$ mapping a bitstring $x = (x_1, \dots, x_n)$ of length n to another bitstring $f(x)$, which is also of length n. We assume that this function satisfies the property

$$f(x) = f(y) \text{ if and only if } (y = x \text{ or } y = x \oplus s), \tag{1}$$

where $\oplus$ denotes here the 'bitwise' XOR function, i.e., $x \oplus s = (x_1 \oplus s_1, \dots, x_n \oplus s_n)$, and $s \neq (0, \dots, 0)$. Our goal is to find the bitstring s. Note: the following two subsections can be treated independently.

3.1 Classical algorithm

1. Simon's problem is a hard problem for a classical computer, i.e., requires typically expononentially many queries to the oracle function $f(x)$. In order to prove this statement, first show that one can only obtain s by finding two different bitstrings x and y such that $f(x) = f(y)$.
2. Explain without further calculations why one typically needs to evaluate f exponentially many times to find two such bitstrings x and y.

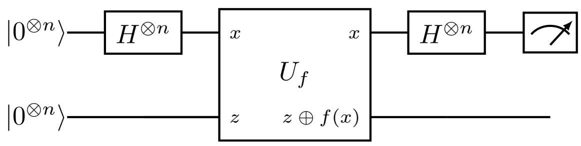
3.2 Quantum algorithm for Simon's problem

Given the function f, we first introduce a quantum oracle U_f. It acts on two n-qubit registers as follows

$$U_f |x, z\rangle = |x, z \oplus f(x)\rangle \,. \tag{2}$$

where x and z are two n-qubits states, and $\oplus$ is again the bitwise XOR operation.

1. The quantum circuit we consider is given by



   Write the wavefunction after the first n Hadamard gates.

2. Write the wavefunction of the circuit after the oracle U_f
3. Write the wavefunction of the circuit after the last n Hadamards (just before the measurement)
4. Show that the probability to measure a bitstring w at the end of the circuit reads

$$P(w) = \frac{1}{4^n} \sum_x (1 + (-1)^{x.w + (x \oplus s).w}) \tag{3}$$

   Note: we recall that the probability to measure w can be expressed as $P(w) = \langle \psi | \left(|w\rangle \langle w| \otimes 1_n \right) |\psi\rangle$, where $|\psi\rangle$ is the state of the quantum system, and 1_n is the identity operator on n qubits.

5. Using the relation, (known as distributivity of XOR and AND operations)

$$(x \oplus s).w = (x.w) \oplus (s.w) \tag{4}$$

   Simplify the expression of the probability $P(w)$ for the two cases (i) $s.w = 0$ and (ii) $s.w = 1$. Show that this means the measurement provides meaningful information about s.

6. We perform M measurements, leading to M measured bitstrings $w^{(t)}$, $t = 1, \dots, M$. Represent this data as a linear system of equations over s. Explain without further calculations that s can be obtained from this system of equations when M is of order n.