Quantum algorithms 2023/2024: Final exam

Benoît Vermersch (benoit.vermersch@lpmmc.cnrs.fr) - 2023 Jan 9th, 10:15-12:15 (2 hours)

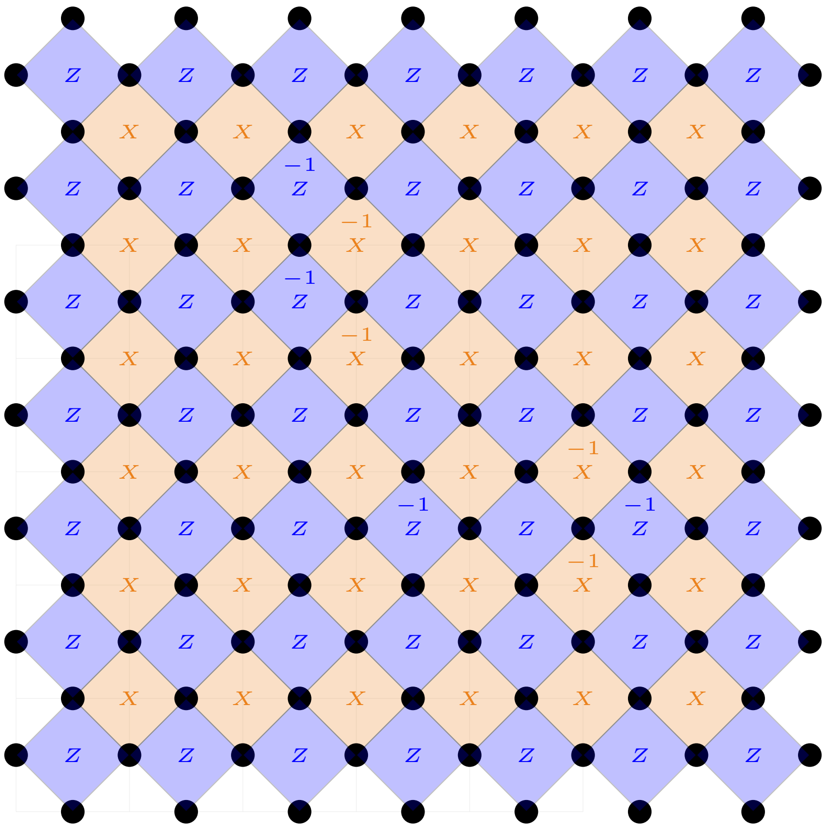
- Documents allowed: Slides of the lectures, documents of the exercices, hand-written notes
- You can only use your laptop to look at the documents from Moodle.
- You can also use printed versions of these documents.
- The use of smartphones or tablets is not allowed.

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.

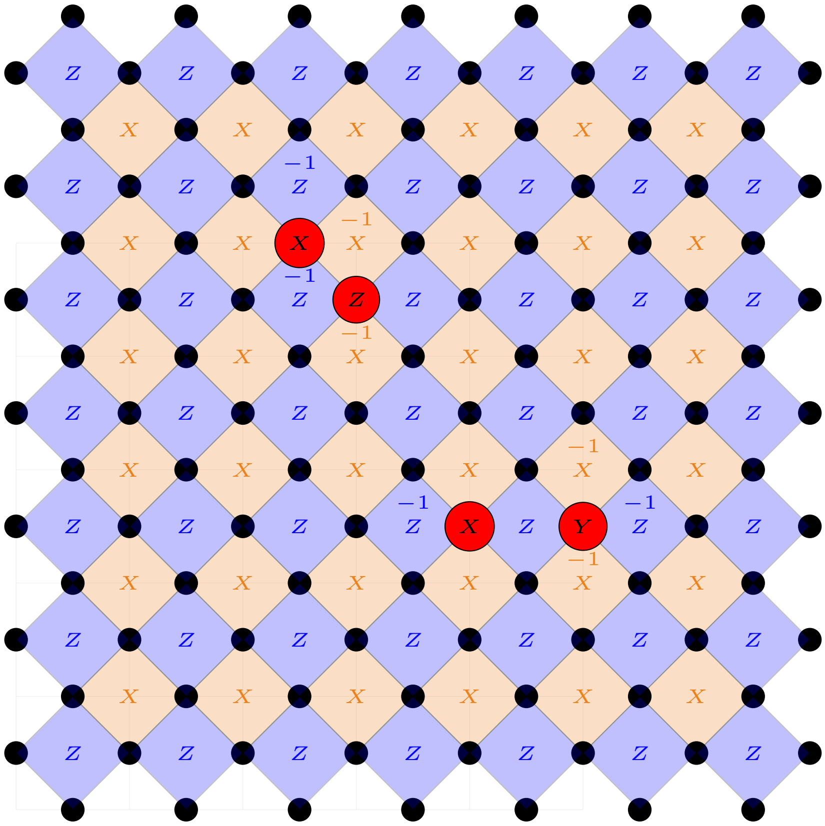
   Solution: *$YXY = i^2XZX^2Z = -XZ^2 = -X$, $YZY = i^2XZ^2XZ = -Z$. Therefore, single qubit Y errors will flip the expectation value of both corresponding X and Z plaquette operators.*

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.



Solution: *The top-left pattern of errors can be easily explained via an X error between the two faulty Z plaquettes, and a Z error between the two faulty X plaquettes.*

To explain the faulty X plaquettes in the bottom right, we need to consider at the intersection either a Z or a Y error. This turns out to be a Y error to explain the right faulty Z plaquette, and we have also an X error on the other side.



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.

   Solution:

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

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 $B = A \oplus (A \oplus B)$.

   Solution: *Therefore* $A \oplus (A \oplus B) = (A \oplus A) \oplus B = 0 \oplus B = B$

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 $x = (x_1, \ldots, x_n)$.

   Solution:

$$H^{\otimes n} |0^{\otimes n}\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \ldots \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2^n}} \sum_{x_1,\ldots,x_n} (|x_1\rangle \ldots |x_n\rangle) = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \qquad (1)$$

2. Show that $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_w (-1)^{x.w}|w\rangle$, with $x.w = \sum_i x_i w_i \bmod(2)$. *In the second part of the exam, we will use the fact that $x.w$ can be rewritten as $x.w = x_1w_1 \oplus x_2w_2 \oplus \cdots \oplus x_nw_n$ (I am not asking you to prove this).*

   Solution:
   $$H^{\otimes n}|x\rangle = H|x_1\rangle \dots H|x_n\rangle \tag{2}$$
   We know that $H|x_i\rangle = (|0\rangle + |1\rangle)\sqrt{2}$ if $x_i = 0$, $H|x_i\rangle = (|0\rangle - |1\rangle)\sqrt{2}$ if $x_i = 1$. Therefore, for any x_i,
   $$H|x_i\rangle = \frac{|0\rangle + (-1)^{x_i}|1\rangle}{\sqrt{2}} = \frac{\sum_{w_i=0}^{1}(-1)^{x_iw_i}|w_i\rangle}{\sqrt{2}} \tag{3}$$
   and we obtain
   $$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{w_1}(-1)^{x_1w_1}|w_1\rangle\right)\dots\left(\sum_{w_n}(-1)^{x_nw_n}|w_n\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_w(-1)^{x.w}|w\rangle \tag{4}$$
   with $x.w = \sum_i x_iw_i \bmod(2)$.

   Note: The fact that $\sum_i x_iw_i \bmod(2) = x_1w_1 \oplus \cdots \oplus x_nw_n$ can be proven by recurrence.

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

$$f(x) = f(y) \text{ if and only if } (x = y \text{ or } y = x \oplus s), \tag{5}$$

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

3.1 Classical algorithm

1. Simon's problem is 'hard' 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 obtain s by finding two different bitstrings x and y such that $f(x) = f(y)$.

   Solution: *The only thing we can do in a classical algorithm is to evaluate f sequentially. When we observe different outputs $f(x) \neq f(y)$, we cannot say anything about s. When we observe a doublon $f(x) = f(y)$, we can learn s. This is because in this case, we know that $y = x \oplus s$, and we can compute*
   $$x \oplus y = (x_1 \oplus y_1, \dots, x_n \oplus y_n) = (x_1 \oplus (x_1 \oplus s_1), \dots, x_n \oplus (x_n \oplus s_n)) = (s_1, \dots, s_n) = s \tag{6}$$
   i.e we can learn s from the knowledge of x and y.

2. Explain without further calculations why one typically needs to evaluate f exponentially many times to find two such bitstrings x and y.

   Solution: *We need two finds two doublons in a an exponentially large dataset (2^n bistrings). This is clearly exponentially hard. Note: The typical number of required queries to obtain a doublon with order 1 probability is $\sqrt{2^n}$, as known from the 'birthday paradox' paradigm.*

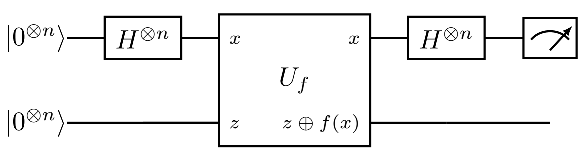
3.2 Quantum algorithm for Simon's problem

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

$$U_f|x, z\rangle = |x, z \oplus f(x)\rangle\,. \tag{7}$$

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.

Solution:

$$|\psi\rangle = H^{\otimes n} |0^{\otimes n}\rangle |0^{\otimes n}\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x, 0^{\otimes n}\rangle \tag{8}$$

2. Write the wavefunction of the circuit after the oracle U_f

   Solution:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} U_f \sum_x |x, 0^{\otimes n}\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x, 0^{\otimes n} \oplus f(x)\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x, f(x)\rangle \tag{9}$$

3. Write the wavefunction of the circuit after the last n Hadamards (just before the measurement)

   Solution:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x H^{\otimes n} |x, f(x)\rangle = \frac{1}{2^n} \sum_{x,w} (-1)^{x.w} |w, f(x)\rangle \tag{10}$$

4. Show that the probability to measure a bitstring w at the end of the circuit reads

$$P(w) = \frac{1}{4^n} \sum_x (1 + (-1)^{x.w + (x \oplus s).w)}) \tag{11}$$

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

   Solution:

$$P(w) = \langle\psi|(|w\rangle \langle w| \otimes \mathbf{1})|\psi\rangle = \frac{1}{4^n} \sum_{x,y} (-1)^{x.w+y.w} \langle f(x)|f(y)\rangle \tag{12}$$

   Now we use that $f(x) = f(y)$ iff $y = x$ or $y = x \oplus s$.

$$P(w) = \langle\psi|(|w\rangle \langle w| \otimes \mathbf{1})|\psi\rangle = \frac{1}{4^n} \sum_x (1 + (-1)^{x.w+(x\oplus s).w)}) \tag{13}$$

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

$$(x \oplus s).w = (x.w) \oplus (s.w) \tag{14}$$

   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.

   Solution:

$$P(w) = \frac{1}{4^n} \sum_x (1 + (-1)^{x.w+(x.w)\oplus(s.w)}) \tag{15}$$

   If $s.w = 1$, $x.w + (x.w) \oplus (s.w) = 1$, therefore $P(w) = 0$. Instead, if $s.w = 0$, $x.w + (x.w) \oplus (s.w) = 0 \bmod(2)$, and therefore

$$P(w) = \frac{1}{4^n} \sum_x 2 = \frac{1}{2^{n-1}} \tag{16}$$

   There the bitstrings w that we measure are such $s.w = 0$. This is a linear relation that we can try to invert to find s.

   Note the above property can be proven as follows:

$$(x \oplus s).w = (x_1 \oplus s_1)w_1 \oplus \cdots = (x_1 w_1 \oplus s_1 w_1) \oplus \cdots = x.w \oplus s.w \tag{17}$$

6. We perform M measurements, leading to M measured bitstrings $w^{(t)}$, $t = 1, \ldots, M$. 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.

   Solution: *We have*

$$s.w^{(1)} = s_1 w_1^{(1)} \oplus s_2 w_2^{(1)} \oplus \ldots = 0 \tag{18}$$

$$s.w^{(2)} = s_1 w_1^{(2)} \oplus s_2 w_2^{(2)} \oplus \ldots = 0 \tag{19}$$

$$\ldots \tag{20}$$

$$s.w^{(M)} = s_1 w_1^{(M)} \oplus s_2 w_2^{(M)} \oplus \ldots = 0 \tag{21}$$

   When $M > n$, we have obtained from random sampling over 2^{n-1} choices of w, M such equations. Thus, there is a high probability that we have obtained at least n linearly independent equations. As the unknown variable s is a vector of n entries, we can then solve the system efficiently on a classical computer, using for instance Gaussian elimination.