Quantum Algorithms 2021/2022: Exercices 2

Benoît Vermersch (benoit.vermersch@lpmmc.cnrs.fr) -October 11, 2021

1 Grover's algorithm

The goal is to demonstrate the performance of a Grover's algorithm by calculating the wavefunction $|\psi_t\rangle$ representing the circuit after t iterations. Notation $N = 2^n$ the number of entries of the function f, w is the single solution, i.e. $f(x) = 1$, iff $x = w$.

1. $U_w = 1 - 2|w\rangle\langle w|$ and $U_\psi = 2|\psi\rangle\langle\psi| - 1$

2. $$|\psi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}(|0\rangle + |1\rangle)^{\otimes n} = \frac{1}{\sqrt{N}}\sum_i |i\rangle \tag{1}$$

3. With
$$\alpha = \frac{1}{\sqrt{N-1}}\sum_{i\neq w}|i\rangle\,, \tag{2}$$
we can write
$$|\psi\rangle = \frac{1}{\sqrt{N}}(|w\rangle + \sqrt{N-1}\,|\alpha\rangle) = \sin(\theta/2)|w\rangle + \cos(\theta/2)|\alpha\rangle\,, \tag{3}$$
with $\sin(\theta/2) = 1/\sqrt{N}$. Therefore,
$$|\psi\rangle_1 \;=\; U_\psi\left(\cos(\theta/2)|\alpha\rangle - \sin(\theta/2)|w\rangle\right). \tag{4}$$
$$\begin{aligned} U_\psi|\alpha\rangle &= 2|\psi\rangle\langle\psi|\alpha\rangle - |\alpha\rangle = \left(2\cos(\theta/2)^2 - 1\right)|\alpha\rangle + 2\sin(\theta/2)\cos(\theta/2)|w\rangle \\ &= \cos(\theta)|\alpha\rangle + \sin(\theta)|w\rangle \qquad (5) \\ U_\psi|w\rangle &= 2|\psi\rangle\langle\psi|w\rangle - |w\rangle = \left(2\sin(\theta/2)^2 - 1\right)|w\rangle \\ &+ 2\sin(\theta/2)\cos(\theta/2)|\alpha\rangle \\ &= -\cos(\theta)|w\rangle + \sin(\theta)|\alpha\rangle \qquad (6) \end{aligned}$$
This leads to
$$\begin{aligned} |\psi\rangle_1 &= (\cos(\theta/2)\sin(\theta) + \sin(\theta/2)\cos(\theta))|w\rangle + (\cos(\theta/2)\cos(\theta) - \sin(\theta/2)\sin(\theta))|\alpha\rangle \\ &= \sin(3\theta/2)|w\rangle + \cos(3\theta/2)|\alpha\rangle \qquad (7) \end{aligned}$$

4. Assume
$$|\psi\rangle_{t-1} \;=\; \sin((2(t-1)+1)\theta/2)|w\rangle + \cos((2(t-1)+1)\theta/2)|\alpha\rangle \tag{8}$$
we get
$$|\psi\rangle_t \;=\; U_\psi\left(\cos((2(t-1)+1)\theta/2)|\alpha\rangle - \sin((2(t-1)+1)\theta/2)|w\rangle\right). \tag{9}$$
This leads to
$$\begin{aligned} |\psi\rangle_t &= (\cos((2(t-1)+1/2)\sin(\theta) + \sin((2(t-1)+1/2)\cos(\theta))|w\rangle \\ &+ (\cos((2(t-1)+1/2)\cos(\theta) - \sin((2(t-1)+1/2)\sin(\theta))|\alpha\rangle \\ &= \sin((2t+1)\theta/2)|w\rangle + \cos((2t+1)\theta/2)|\alpha\rangle \qquad (10) \end{aligned}$$

5. The probability to measure the right state w is
$$P_t(w) = |\langle w|\psi\rangle_t|^2 == \sin^2((2(t-1)+1)\theta/2) \tag{11}$$
The probability is maximal for $2(t-1)+1 = \pi/\theta \approx \pi\sqrt{N}$, which shows the quadratic scaling of the Grover algorithm.

2 Implementation of Grover's diffuser operator

Our goal is to design a quantum circuit for $U_\psi = 2\left|\psi\right\rangle\left\langle\psi\right| - 1$.

1. $U_1 = H^{\otimes n}$
2. $U_1^2 = (H^{\otimes n})(H^{\otimes n} = (H^2)^{\otimes n} = 1$.
3. $U_\psi = 2U_1\left|0\right\rangle^{\otimes n}\left\langle 0\right|^{\otimes n} U_1 - U_1^2 = U_1(2\left|0\right\rangle^{\otimes n}\left\langle 0\right|^{\otimes n} - 1)U_1$
4. $U_2 = 2\left|0\right\rangle^{\otimes n}\left\langle 0\right|^{\otimes n} - 1 = X^{\otimes n}(2\left|1\right\rangle^{\otimes n}\left\langle 1\right|^{\otimes n} - 1)X^{\otimes n}$.

$$\begin{aligned} U_3 &= 1 - 2\left|1\right\rangle^{\otimes n}\left\langle 1\right|^{\otimes n} = 1 - \left|1\right\rangle^{\otimes n-1}\left\langle 1\right|^{\otimes n-1}(1_n - Z_n) \\ &= (1 - \left|1\right\rangle^{\otimes n-1}\left\langle 1\right|^{\otimes n-1})1_n + \left|1\right\rangle^{\otimes n-1}\left\langle 1\right|^{\otimes n-1} Z_n \end{aligned} \tag{12}$$

is the N qubit controlled Z gate (I get a minus sign iff all qubits are 1).

5. $Z = HXH$.

$$\begin{aligned} U_3 &= (1 - \left|1\right\rangle^{\otimes n-1}\left\langle 1\right|^{\otimes n-1})H_n H_n + \left|1\right\rangle^{\otimes n-1}\left\langle 1\right|^{\otimes n-1} H_n X_n H_n \\ &= H_n[(1 - \left|1\right\rangle^{\otimes n-1}\left\langle 1\right|^{\otimes n-1})1 + \left|1\right\rangle^{\otimes n-1}\left\langle 1\right|^{\otimes n-1} X]H_n. \end{aligned} \tag{13}$$

The gate in the middle is the $n-$qubit Toffoli gate T_n.

6.

$$U_\psi = H^{\otimes n} U_2 H^{\otimes n} = -H^{\otimes n} X^{\otimes n} U_3 X^{\otimes n} H^{\otimes n} = -H^{\otimes n} X^{\otimes n} H_n T_n H_n X^{\otimes n} H^{\otimes n} \tag{14}$$

3 Implementation of the quantum Fourier transform

Ref: Nielsen and Chuang. The quantum Fourier transform realizes the transformation

$$U\left|j\right\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N}\left|k\right\rangle, \tag{15}$$

with $j, k = 0, \ldots, N-1$. Our goal is to implement this transformation for $N = 2^n$, using 2 coupled circuits of n qubits.

1. Binary representation $j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$
2. We use the notation $0.j_l \ldots j_n = j_l/2 + \ldots j_n/2^{n-l+1}$.

$$\begin{aligned} U\left|j\right\rangle &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N}\left|k\right\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{k_1,\ldots,k_n}^{N-1} e^{2\pi i j(k_1 2^{n-1} + \cdots + k_n 2^0)/2^n}\left|k_1, \ldots, k_n\right\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{k_1,\ldots,k_n} \bigotimes_l \left(e^{2\pi i j k_l 2^{-l}}\left|k_l\right\rangle\right) \\ &= \frac{1}{2^{n/2}} \bigotimes_l \left[\sum_{k_l} e^{2\pi i j k_l 2^{-l}}\left|k_l\right\rangle\right] \\ &= \frac{1}{2^{n/2}} \bigotimes_l \left[\left|0\right\rangle + e^{2\pi i j 2^{-l}}\left|1\right\rangle\right] \\ &= \frac{1}{2^{n/2}}(\left|0\right\rangle + e^{2i\pi j/2}\left|1\right\rangle)(\left|0\right\rangle + e^{2i\pi(j/4)}\left|1\right\rangle)\ldots(\left|0\right\rangle + e^{2i\pi(j/2^n)}\left|1\right\rangle) \\ &= \frac{1}{2^{n/2}}(\left|0\right\rangle + e^{2i\pi j_n/2}\left|1\right\rangle)(\left|0\right\rangle + e^{2i\pi(j_{n-1}/2 + j_n/4)}\left|1\right\rangle)\ldots(\left|0\right\rangle + e^{2i\pi(j_1/2 + \cdots + j_n/2^n}\left|1\right\rangle) \\ &= \frac{1}{2^{n/2}}(\left|0\right\rangle + e^{2i\pi 0.j_n}\left|1\right\rangle)(\left|0\right\rangle + e^{2i\pi 0.j_{n-1}j_n}\left|1\right\rangle)\ldots(\left|0\right\rangle + e^{2i\pi 0.j_1\cdots j_n}\left|1\right\rangle) \end{aligned} \tag{16}$$

3. We have

$$R_2 = \begin{bmatrix} 1 & 0 \\ 0 & e^{2i\pi/2^2} \end{bmatrix}. \tag{17}$$

$$\begin{aligned} C[R_2]H_1 |j\rangle &= \frac{1}{\sqrt{2}} C[R_2] \left(|0\rangle + e^{2i\pi 0.j_1} |1\rangle\right) |j_2 \dots j_n\rangle \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2i\pi 0.j_1} e^{2i\pi j_2/2^2} |1\rangle\right) |j_2 \dots j_n\rangle \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2i\pi 0.j_1 j_2} |1\rangle\right) |j_2 \dots j_n\rangle \end{aligned} \tag{18}$$

After the first R_n rotations

$$C[R_n] \dots C[R_2]H_1 |j\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2i\pi 0.j_1 j_2 \dots j_n} |1\rangle\right) |j_2 \dots j_n\rangle \tag{19}$$

4. After the Hadamard on the second qubit, we obtain

$$\frac{1}{2} \left(|0\rangle + e^{2i\pi 0.j_1 j_2 \dots j_n} |1\rangle\right) \left(|0\rangle + e^{2i\pi 0.j_2} |1\rangle\right) |j_3 \dots j_n\rangle \tag{20}$$

After the controlled R_k rotations on the second qubit, we obtain

$$\frac{1}{2} \left(|0\rangle + e^{2i\pi 0.j_1 j_2 \dots j_n} |1\rangle\right) \left(|0\rangle + e^{2i\pi 0.j_2 \dots j_n} |1\rangle\right) |j_3 \dots j_n\rangle \tag{21}$$

At the end of the circuit

$$\frac{1}{2^{n/2}} \left(|0\rangle + e^{2i\pi 0.j_1 j_2 \dots j_n} |1\rangle\right) \left(|0\rangle + e^{2i\pi 0.j_2 \dots j_n} |1\rangle\right) \dots \left(|0\rangle + e^{2i\pi 0.j_n} |1\rangle\right) \tag{22}$$

Up to a swap transformation, this is the desired transformation.

4 Factorizing 21 with Shor's algorithm

We take $N = 21$.

1. **Classical part** Assume we randonly pick $a = 2$. Show that the function $f(x) = a^x \mod(N)$ is 6 periodic. $2^6 = 64 = 1 + 21 \times 3 = 1 \mod(N)$. $f(x+6) = a^{x+6} \mod(N) = a^x(1 + N \times 3) \mod(N) = a^x \mod(N) = f(x)$.

2. Find two non-trivial divisors of N. We have: N divides $a^6 - 1$. Therefore, with $b = a^3 = 8$, N divides $b^2 - 1$. According to the result presented in Lecture 2, $\gcd(N, b \pm 1) = 7, 3$ are non-trivial divisors of N.

3. **Quantum subroutine** The quantum subroutine of Shor's algorithm consists in finding the period $r = 6$ of $f(x)$. How many qubits do we need to implement this algorithms? $N^2 = 441$, we thus need 2 registers of $q = 9$ qubits.

4. Write the state of the system after modular exponentiation.

$$\psi = \frac{1}{\sqrt{Q}} \sum_x |x\rangle \otimes |f(x)\rangle, \tag{23}$$

with $Q = 2^q = 512$.

5. Write the state after inverse quantum Fourier transform and the probability $P(y)$ to observe the bitstring y after measuring the first q qubits.

$$|\psi\rangle = \frac{1}{Q} \sum_x (\sum_y e^{2i\pi xy/Q} |y\rangle) \otimes |f(x)\rangle \tag{24}$$

$$|\psi\rangle = \frac{1}{Q} \sum_y \left(|y\rangle \otimes \sum_x e^{2i\pi xy/Q} |f(x)\rangle \right) \tag{25}$$

$$\begin{aligned} P(y) &= \sum_{y'} | \langle y, y'| \, |\psi\rangle |^2 = \frac{1}{Q^2} \sum_{x_1, x_2} e^{2i\pi(x_2 - x_1)y/Q} \langle f(x_1)| \sum_{y'} |y'\rangle \langle y'| \, |f(x_2)\rangle \\ &= \frac{1}{Q^2} \sum_{x_1, x_2} e^{2i\pi(x_2 - x_1)y/Q} \langle f(x_1)| \, |f(x_2)\rangle \end{aligned}$$

6. Plot the function $P(y)$ and give the table of the three most likely measured bitstrings.

7. The continued fraction algorithm gives us the closest fraction p/r to the measured y/Q rational, with a maximum $r_{\max}$ tunable value for r. For Python, this is implemented as fractions.Fraction(float).limit_denominator(rmax). Give the attributed value for each most likely bitstring r. Comment. For $y = 85$, we search for a fraction such that $85/512 = 0.166 \approx 1/6$. We end up with $b = \sqrt{2^6} = 8$. For $y = 171$, $r = 3 \to$ fail, or $r = 6$, $\to$ success. For $y = 512$, we attibute $r = 2$ from $1/2$ (instead of 6 from $3/6$, which results in a fail.

8. Repeat the same exercise with $a = 13$. The function is $r = 2$ periodic. We find $b = 13$, and $7, 3$ as non-trivial divisors. In this case, the success probability is $1/2$, obtained when measuring $y = Q/2$.