Quantum Algorithms 2021/2022: Exercices 2

Benoît Vermersch (benoit.vermersch@lpmmc.cnrs.fr) -October 4, 2021

1 Grover's algorithm

The goal is to demonstrate the performance of Grover's algorithm by calculating the wavefunction $|\psi_t\rangle$ representing the circuit after t iterations.

1. Represent the circuit of Grover's algorithm. Write down the expression of the oracle U_w and the diffuser U_ψ.
2. Write down explicitely the expression of $|\psi\rangle$, the state of the circuit before the first application of the oracle.
3. Write down the expression of $|\psi_1\rangle = U_\psi U_w |\psi\rangle$, the state of the circuit after the first iteration. Hint: It will be convenient to decompose $|\psi\rangle$ in terms of $|w\rangle$ and $\alpha = 1/\sqrt{N-1}\sum_{i\neq w}|i\rangle$, and introduce θ, such that $\sin(\theta/2) = 1/\sqrt{N}$.
4. Generalize to t iterations and express the probabilities associated with the final measurement.
5. Show that the required number of iterations to measure the solution w with probability of order 1 scales with the square root of the number of solution N.

2 Implementation of Grover's diffuser operator

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

1. Write down a circuit U_1 that prepares $|\psi\rangle$ from $|0\rangle^{\otimes n}$
2. Evaluate U_1^2.
3. We aim at implementing U_ψ as $U_\psi = U_1 U_2 U_1$. Write down the circuit corresponding to U_2.
4. Prove that U_2 can be written as $U_2 = -X^{\otimes n} U_3 X^{\otimes n}$, with U_3 a N-qubit controlled Z gate
5. Write U_3 in terms of the Toffoli gate.
6. Write down the full circuit for $-U_\psi$. Comment on the role of the minus sign.

Quantum Algorithms 2021/2022: Exercices 2

Benoît Vermersch (benoit.vermersch@lpmmc.cnrs.fr) -October 4, 2021

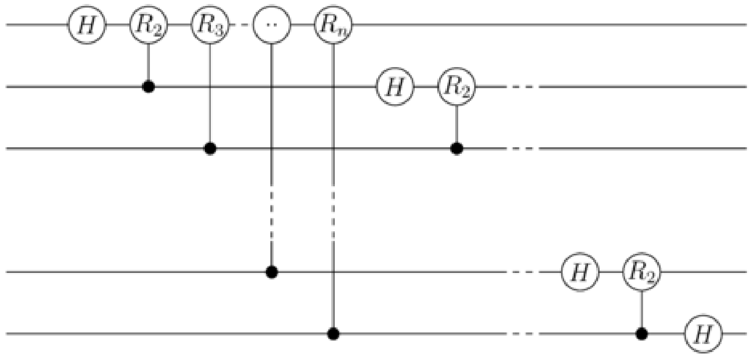
3 Implementation of the quantum Fourier transform

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

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

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

1. Write any integer j in terms of a binary representation $j = j_1 \dots j_n$. In our quantum circuit, j_l will represent the state of qubit l.
2. We use the notation $0.j_l \dots j_n = j_l/2 + \dots j_n/2^{n-l+1}$. Show that
$$U|j\rangle = \frac{1}{2^{n/2}}(|0\rangle + e^{2i\pi 0.j_n}|1\rangle)(|0\rangle + e^{2i\pi 0.j_{n-1}j_n}|1\rangle)\dots(|0\rangle + e^{2i\pi 0.j_1\dots j_n}|1\rangle) \tag{2}$$
3. We show the circuit of the quantum Fourier transform.



The single qubit gate R_k is defined as
$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2i\pi/2^k} \end{bmatrix}. \tag{3}$$
How is a basis $|j\rangle$ transformed after the first controlled R_2 rotation? After the first R_n rotation?
4. Write down the state at the end of the circuit. Conclusion.

4 Factorizing 21 with Shor's algorithm

We take $N = 21$.

1. **Classical part** Assume we randomly pick $a = 2$. Show that the function $f(x) = a^x \bmod(N)$ is 6 periodic.
2. Find two non-trivial divisors of N.
3. **The 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 algorithm?
4. Write the state of the system after modular exponentiation.
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.
6. Plot the function $P(y)$ and extract the three most likely measured bitstrings.
7. The continued fraction algorithm is a classical algorithm that gives the closest fraction p/r from the measured y/Q rational, with a maximum $r_{\max}$ value for r. In Python, this is implemented as fractions.Fraction(float).limit_denominator(rmax).

   Give the attributed value for each most likely bitstring r. Comment.
8. Repeat the same exercice, aiming at factorizing 35.