Introduction to quantum computing

Lecture 2: Quantum algorithms

Benoît Vermersch

March 28, 2024

LPMMC Grenoble

Outline

Our first quantum algorithm: Deutsch's algorithm

Quadratic speedup: Grover's algorithm

- Implementation details

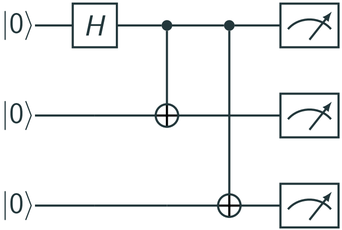
Other important quantum algorithms

What is an error in quantum computing?

Outline

Reminder: Structure of a quantum circuit

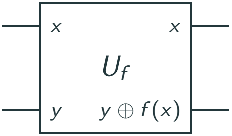
Quantum circuit: single qubit/two-qubit gates and measurements:



Algorithm: a quantum circuit to retrieve the solution of a problem in the measurement data with high probability.

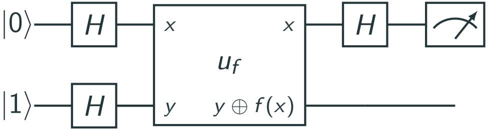
Deutsch's algorithm

- Problem: Given a single bit Boolean function $f(x)$, is f constant i.e $f(0) = f(1)$, or balanced, i.e $f(0) \neq f(1)$?
- We need to introduce an object called an *Oracle*, aka quantum black box.
- An oracle evaluates the classical function f on quantum states



- Complexity will refer here to the number of oracles evaluation.
- Note: a quantum algorithm will be of practical use if the oracle can be implemented easily

Deutsch's algorithm



One measurement gives me the solution, I would need two function evaluations in the classical case: quantum speedup

Deutsch's algorithm

After the first Hadamards

$$|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

After the oracle

$$|\psi\rangle' = \frac{1}{2}\left(|0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle\right)$$

If $f(0) = f(1)$, let $0 \oplus f(0) = 0 \oplus f(1) = a$, $1 \oplus f(0) = 1 \oplus f(1) = b = 1 - a$

$$|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|a\rangle - |b\rangle)$$

After the last Hadamard,

$$|\psi\rangle \quad = \quad \frac{1}{\sqrt{2}}\,|0\rangle\,(|a\rangle - |b\rangle)$$

I measure $|0\rangle$ with probability 1

Deutsch's algorithm

If $f(0) \neq f(1)$, let $0 \oplus f(0) = 1 \oplus f(1) = a$, $1 \oplus f(0) = 0 \oplus f(1) = b$

$$|\psi\rangle = \frac{1}{2}(|0\rangle - |1\rangle)(|a\rangle - |b\rangle)$$

After the last Hadamard,

$$|\psi\rangle \quad = \quad \frac{1}{\sqrt{2}} |1\rangle \left(|a\rangle - |b\rangle\right)$$

I measure $|1\rangle$ with probability 1

Further reading

Some related algorithm using oracles:

- Deutsch Joza algorithm: generalization of Deutsch's algorithm to multiple qubits: oracle separation between **P** and **EQP** (exact quantum polynomial)
- Bernstein Vazirani and Simon's algorithm: Prove an oracle separation between **BPP** (bounded error classical polynomial) and **BQP** (bounded-error quantum polynomial).

Outline

Our first quantum algorithm: Deutsch's algorithm

Quadratic speedup: Grover's algorithm

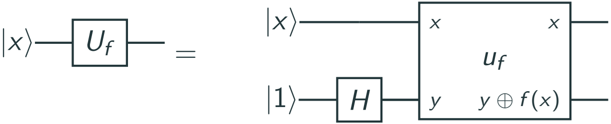
- Implementation details

Other important quantum algorithms

What is an error in quantum computing?

Grover's algorithm

- Unstructured search problem: Given a $n-$bit Boolean function $f(x)$, such that there exists a unique w such that $f(w) = 1$, find w.
- Application: Subroutine in various classical algorithms (example minimization problem, or machine learning)
- Input: A n-bit phase oracle



For any input x, we can mark to the solution

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle$$

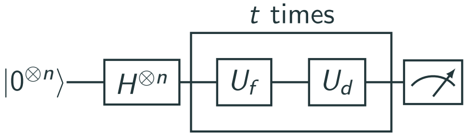
The ancilla qubit has been 'uncomputed'.

Grover's algorithm

- Classical algorithm: $O(2^n)$ evaluations (Just test in a loop...)
- Grover's quantum algorithm $O(\sqrt{2^n})$ oracle evaluations: quadratic speedup
- Possible applications: solving NP-complete problems that allow for oracle implementations (eg the 3-SAT problem), brute-force attacks on cryptographic keys ...

Grover's algorithm

So simple...



- with the diffuser $U_d = 2\,|\psi\rangle\,\langle\psi| - 1$, with $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle$ the superposition on all $N = 2^n$ bitstrings $x = x_1, \ldots, x_n$.

Grover's algorithm

After the first Hadamards ($N = 2^n$), the state is

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}(|0\rangle + |1\rangle)^{\otimes n} = \frac{1}{\sqrt{N}}\sum_x |x\rangle = |\psi\rangle$$

Introducing, $|\alpha\rangle = \frac{1}{\sqrt{N-1}}\sum_{x\neq w}|x\rangle$, we can write

$$|\psi\rangle = \sin(\theta/2)|w\rangle + \cos(\theta/2)|\alpha\rangle\,,$$

with $\sin(\theta/2) = 1/\sqrt{N}$.

Combined application of oracle and diffuser will lead to a rotation of the state $|\psi\rangle$ towards the solution.

$$U_f|\psi\rangle = -\sin(\theta/2)|w\rangle + \cos(\theta/2)|\alpha\rangle\,,$$

Grover's algorithm

$$
\begin{aligned}
U_d \left|\alpha\right\rangle &= \cos(\theta)\left|\alpha\right\rangle + \sin(\theta)\left|w\right\rangle \\
U_d \left|w\right\rangle &= -\cos(\theta)\left|w\right\rangle + \sin(\theta)\left|\alpha\right\rangle
\end{aligned}
$$

After one iteration,

$$
\left|\psi_1\right\rangle = U_d U_f \left|\psi\right\rangle = \sin(3\theta/2)\left|w\right\rangle + \cos(3\theta/2)\left|\alpha\right\rangle
$$

After t iterations,

$$
\left|\psi_t\right\rangle = \sin((2t+1)\theta/2)\left|w\right\rangle + \cos((2t+1)\theta/2)\left|\alpha\right\rangle
$$

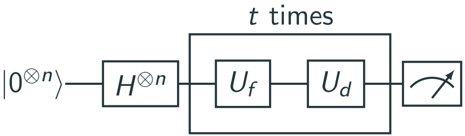
Grover's algorithm: time complexity

- Success probability

$$p_t \quad = \quad |\langle w|\psi_t\rangle|^2 = \sin((2t+1)\theta/2)^2,$$

  which becomes of order one for $\theta t = \mathcal{O}(1)$.
- Remember that $\sin(\theta/2) = 1/\sqrt{N} = 1/\sqrt{2^n}$, thus $\theta \approx 2/\sqrt{2^n}$, we obtain t should be of the order of $\sqrt{2^n}$.

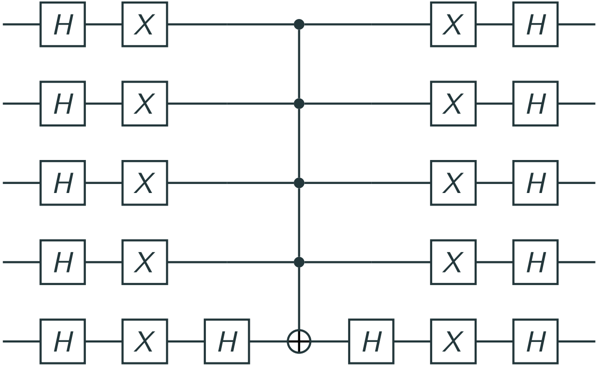
Implementation details



- Implentation of the oracle U_f depending on the function f: Careful Boolean logic to 'mark' solution without knowing the solution, eg test Boolean assertions using $CNOT$s and ancillas.

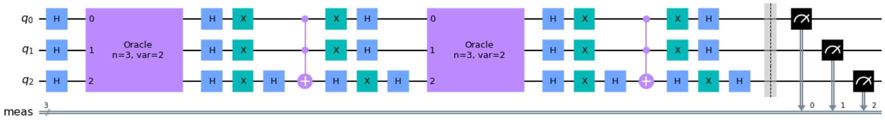
Implementation details

- Implementation of the diffuser $U_d = 2\left|\psi\right\rangle\left\langle\psi\right| - 1$: This can be done with a few gates, including a N-qubit Toffoli gate

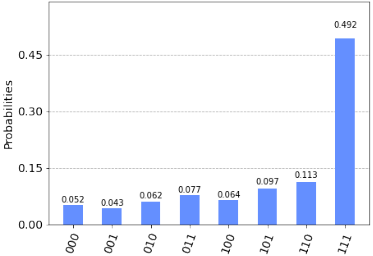


- In practice, the Toffoli gate must be decomposed in elementary CNOT gates, in an optimal way that is platform dependent

Illustration with an IBM quantum computer (c.f., Quantum Practical 2)



- The measurement gives you the solution (if errors are not too large)

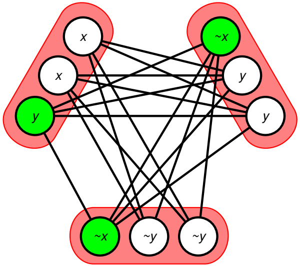


- Take-Home Message: The required number of oracle evaluations $\sim \sqrt{N}$ is smaller than the number of entries N of the database!

Grover's algorithm: final remarks

- The quadratic speedup $\sqrt{N = 2^n}$ of Grover's algorithm is optimal for any quantum algorithm for unstructured search (see eg Preskill).
- This is sad news!!!: With an exponential speedup, some NP-complete problems could have been solved in polynomial time in the size n, thus *any* NP problem could have been solved in polynomial time. . . .

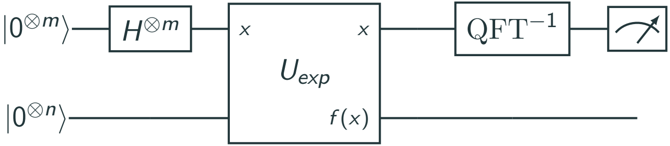
1. Consider a NP-complete problem of size n represented by a Boolean function f (eg 3-sat)
2. Implement the corresponding Grover oracle with n qubits
3. Run Grover's algorithm



Outline

Shor's algorithm

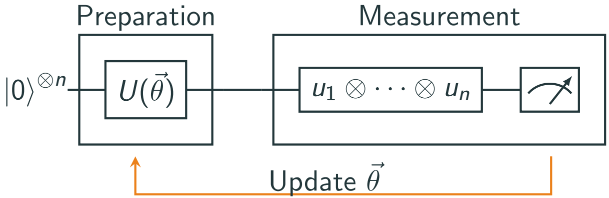
- Perhaps the most famous quantum algorithm
- Exponential speedup over the best known factorization algorithm
- Relies on order finding: find the period r of the function $f(x) = a^x \bmod(N)$.



- Performance limited by the first step of modular exponentiation, $\sim \mathcal{O}(N^3)$ in some schemes.
- Similar circuit for Quantum Phase Estimation algorithm

Quantum Optimization

- Encodes a classical optimization problem in a Hamiltonian operator $H(x)$
- Minimizes H using quantum annealing, or variational algorithms.



- Very attractive for quantum problems H: condensed matter, quantum chemistry
- Absolute limitations: Active field of research.

State of the art

Quantum algorithms: A survey of applications and end-to-end complexities

Alexander M. Dalzell, Sam McArdle, Mario Berta, Przemyslaw Bienias, Chi-Fang Chen, András Gilyén, Connor T. Hann, Michael J. Kastoryano, Emil T. Khabiboulline, Aleksander Kubica, Grant Salton, Samson Wang, Fernando G. S. L. Brandão

arxiv.org/abs/2310.03011

Outline

Our first quantum algorithm: Deutsch's algorithm

Quadratic speedup: Grover's algorithm

Implementation details

Other important quantum algorithms

What is an error in quantum computing?

An error in a quantum computer?

- Example: Spontaneous emission with an atomic qubit $|\psi\rangle = |1\rangle$

$$|1\rangle \to \sqrt{1-p}\,|1\rangle\,|0\rangle_{\text{photon}} + \sqrt{p}\,|0\rangle\,|1\rangle_{\text{photon}} \tag{1}$$

- Spontaneous emission process corresponds to a 'bitflip error' $|\psi\rangle \to X\,|\psi\rangle$

$$|\psi\rangle \to |\psi\rangle\,|E\rangle_I + X\,|\psi\rangle\,|E\rangle_X \tag{2}$$

An error in a quantum computer?

- For a general qubit state $|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle)$, a decoherence process can always be interpretated as a sum of 'Pauli Errors':

$$|\psi\rangle \rightarrow |\psi\rangle |E\rangle_I + X|\psi\rangle |E\rangle_X + Y|\psi\rangle |E\rangle_Y + Z|\psi\rangle |E\rangle_Z \qquad (3)$$

- Quantum error correction: How to detect an error without destroying the quantum superposition?

The bit flip code

- Our first code: The bit flip code

$$|\psi\rangle = \alpha |0\rangle_L + \beta |1\rangle_L \tag{4}$$

with a logical qubit that is made of three physical qubits

$$|0\rangle_L = |000\rangle \quad |1\rangle_L = |111\rangle \tag{5}$$

- The code aims at tracking and correcting X errors occurring on one of the three physical qubits

$$|\psi\rangle \rightarrow |\psi\rangle |E\rangle_I + \sum_{i=1,2,3} X_i |\psi\rangle |E\rangle_{X_i} \rightarrow_{\text{QEC}} \quad |\psi\rangle \tag{6}$$

The bit flip code

- There are two mesurements to be made $\langle Z_1 Z_2 \rangle$, $\langle Z_2 Z_3 \rangle$, giving rise to unique error syndromes, independently of the qubit superposition state.

Error	State	$\langle Z_1 Z_2 \rangle$, $\langle Z_2 Z_3 \rangle$
none	$\alpha \|000\rangle + \beta \|111\rangle$	1,1
X_1	$\alpha \|100\rangle + \beta \|011\rangle$	-1,1
X_2	$\alpha \|010\rangle + \beta \|101\rangle$	-1,-1
X_3	$\alpha \|001\rangle + \beta \|110\rangle$	1,-1

- Code distance: Number of errors that map one logical state to the other. Here it's $d = 3$. For a general d, we can correct t errors if $d \geq 2t + 1$.
- How to measure and correct errors?

The bit flip code: Collective measurements

- We require a collective measurement of $\langle Z_1 Z_2 \rangle$ with two measurement outcomes (eigenvalues) $\epsilon = \pm 1$:

$$Z_1 Z_2 = \underbrace{|00\rangle\langle 00| + |11\rangle\langle 11|}_{P_1} - \underbrace{(|01\rangle\langle 01| + |10\rangle\langle 10|)}_{P_{-1}}$$

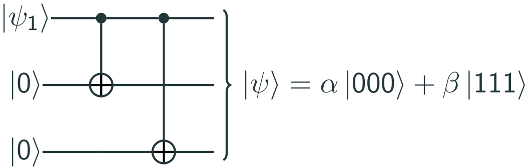
- A measurement on $|\psi'\rangle$ gives a mesurement outcome ϵ and a projection

$$|\psi'\rangle \to P_\epsilon |\psi'\rangle \text{ with probability } \langle \psi | P_\epsilon | \psi \rangle$$

- If $|\psi'\rangle$ is proportional to $|\psi\rangle, X_1|\psi\rangle, X_2|\psi\rangle$, we obtain a deterministic measurement $\epsilon = 1$, or $\epsilon = -1$, and the state is unchanged.
- For a quantum superposition of errors, the outcome is probabilitic, but the post-measured state is compatible with such outcome.

The bit flip code: Implementation aspects

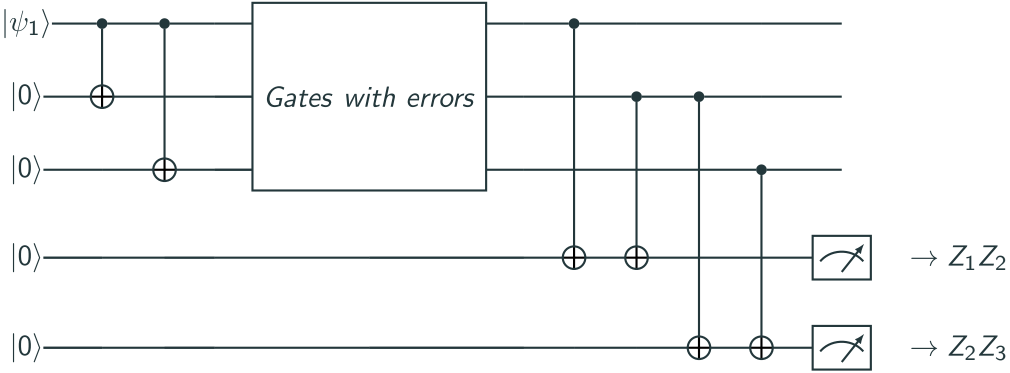
- Step 1: Encoding from a physical qubit state $|\psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$:



- Side remark: This is very different from quantum cloning $|\psi\rangle \to |\psi\rangle^{\otimes 3}$, which can be proven to be strictly impossible.

The bit flip code: Implementation aspects

- Step 2: Error syndromes and recoveries: One requires ancilla qubits (see also Exercices 4)



- The logical gates $X_L = |0\rangle_L \langle 1| + h.c = X_1 X_2 X_3$, $Z_L = |0\rangle_L \langle 0| - |1\rangle_L \langle 1| = Z_1$,

The bit flip code: Limitations

- The bit flip code fails for two and three qubit bit flip errors with probability

$$p_L = 3p^2(1-p) + p^3 \tag{7}$$

  with p the single qubit error
- Notion of threshold: Quantum error correction is only useful when the logical qubit lifetime is larger than the physical qubit lifetime, i.e when $p_L \leq p$, this means when $p \leq 1/2$.
- What about combined presence of X, Y, Z errors?

Steane code

- One logical qubit made of seven physical qubits.
- The error syndromes are defined as the set $S = \{Z_4Z_5Z_6Z_7, Z_2Z_3Z_6Z_7, Z_1Z_3Z_5Z_7, X_4X_5X_6X_7, X_2X_3X_6X_7, X_1X_3X_5X_7\}$.
- These operators commute, i.e errors can be measured successively
- The 'code world' (distance $d = 3$)

$$\begin{aligned} |0\rangle_L &= 1/\sqrt{8}\,(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle) \\ |1\rangle_L &= X_1X_2X_3\,|0\rangle_L \end{aligned} \tag{8}$$

- The code is 'stabilized' by S: For any $|\psi\rangle = \alpha\,|0\rangle_L + \beta\,|1\rangle_L$, for any $g \in S$, $g\,|\psi\rangle = |\psi\rangle$.
- The logical gates are $X_L = \prod_i X_i$, $Z_L = \prod_i Z_i$

Steane code

- The Steane code is an example of *stabilizer codes*, whose error syndromes are elements of a commuting Pauli subgroup.
- For the purpose of this lecture, we will simply check that the syndromes do the job.
- General rules:
  - If Z_i is present in an error syndrome g, it will detect X_i errors (because $X_i Z_i X_i = -Z_i$, and operators acting on different sites i, j commute.)
  - Similarly, Z_i errors are detected by X_i operators .
  - $Y = iXZ$, therefore a Y error is a Z error followed by an X error.

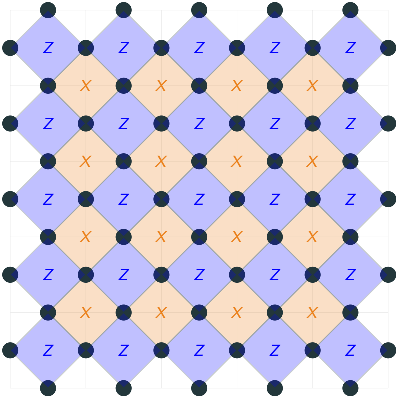
Steane code

Error	$Z_4 Z_5 Z_6 Z_7$	$Z_2 Z_3 Z_6 Z_7$	$Z_1 Z_3 Z_5 Z_7$	$X_4 X_5 X_6 X_7$	$X_2 X_3 X_6 X_7$	$X_1 X_3 X_5 X_7$
none	1	1	1	1	1	1
X_1	1	1	-1	1	1	1
X_2	1	-1	1	1	1	1
X_3	1	-1	-1	1	1	1
X_4	-1	1	-1	1	1	1
X_5	-1	1	-1	1	1	1
X_6	-1	-1	1	1	1	1
X_7	-1	-1	-1	1	1	1
Z_1	1	1	1	1	1	-1
$\vdots$						
Y_1	1	1	-1	1	1	-1
$\vdots$						

Steane code: Conclusion

- The Steane corrects any single qubit errors.
- As the bitflip code, it does not corrected double errors (ex: X_1X_2).
- A first option to achieve Fault tolerance (reaching arbitrary precision in presence of a finite error probability): Concatenated Steane Codes.
- Another approach: Surface codes.

Surface code



- Kitaev, Bravyi (1997), following works on 'Toric codes'.
- The physical qubits sit on a 2D lattice.
- The stabilizer operators, i.e the measurements to be made for error detection, are

$$Z_{i_1} Z_{i_2} Z_{i_3} Z_{i_4} \text{ on plaquettes}$$
$$X_{j_1} X_{j_2} X_{j_3} X_{j_4} \text{ on vertices}$$

- Code world is 'stabilized' by all such operators $g\,|\psi\rangle = |\psi\rangle$

Quantum error correction in 2024

Rydberg atom qubits (Harvard, M. Lukin group)