ACCQ 206 - Simon's algorithm, Quantum Fourier transform and Shor's algorithm

Alex Bredariol Grilo
Alex.Bredariol-Grilo@lip6.fr

Quantum operations

Evolution of quantum states is described by unitary operators

- $UU^\dagger = U^\dagger U = I$
  - For every quantum state $|\psi\rangle$, $U|\psi\rangle$ is also a quantum state
  - Reversible: no information loss
- Equivalent models of quantum computation:
  - Quantum Turing Machines
  - Quantum circuits
  - Adiabatic quantum computation
  - Measurement-based quantum computation
  - ...

Universal gateset

Definition

ε-approximation An n-qubit unitary U ε-approximates an n-qubit unitary U' if

$$\max_{|\psi\rangle \in \mathbb{C}^{2^n}} ||U|\psi\rangle - U'|\psi\rangle|| \leq \varepsilon.$$

Definition

Universal gateset A gateset $\mathcal{G}$ is universal if for every unitary U, there exists a unitary U' composed by gates in $\mathcal{G}$ such that U' ε-approximates U.

Lemma

The following gatesets are universal:

- $\{1\text{-qubit gates}, CNOT\}$
- $\{CNOT, H, T\}$
- $\{H, CCNOT\}$ *(for unitaries with real entries)*

Quantum circuits

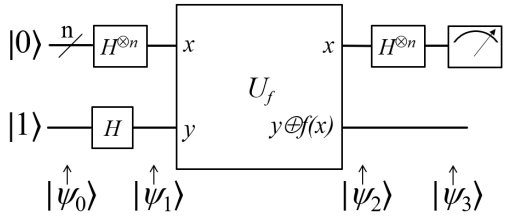
Deutsch-Josza algorithm (1992)

Problem

Given oracle access to $f : \{0,1\}^n \to \{0,1\}$ with the promise that:

- f is constant
- f is balanced

Find out which is the case.



Quantum parallelism: $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\,|f(x)\rangle$

Simon's algorithm (1994)

Problem

Given oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$ such that:

$$\exists s \neq 0^n \text{ such that } f(x) = f(y) \text{ iff } y \in \{x, s \oplus y\}.$$

Find s.

Simon's algorithm

Problem

Given oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$ such that:

$$\exists s \neq 0^n \text{ such that } f(x) = f(y) \text{ iff } y \in \{x, s \oplus y\}.$$

Find s.

Randomized algorithms:

Simon's algorithm

Lemma

With a single quantum query, we can compute a random $d \in \{0,1\}^n$ such that

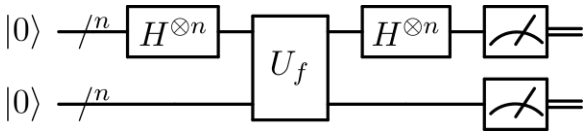
$$d \cdot s = 0.$$

Theorem

There is a quantum algorithm that retrieves s with high probability with $O(n)$ queries.

Proof

Simon's algorithm - sampling d s.t. $d \cdot s = 0$



Analysis

Simon's algorithm

Analysis (cont.)

Simon's algorithm - recap

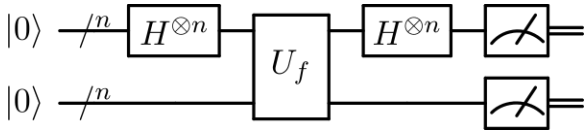
Problem

Given oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$ such that:

$$\exists s \neq 0^n \text{ such that } f(x) = f(y) \text{ iff } y \in \{x, s \oplus y\}.$$

Find s.

The following circuit samples random d such that



Sampling it $O(n)$ times, with high probability we have n linearly independent d_i's and we can solve the following linear system of equations to compute s

$$\forall 1 \leq i \leq n, d_i \cdot s = 0.$$

Simon's algorithm - applications

Kaplan, Leurent, Leverrier and Naya-Plasencia. Breaking Symmetric Cryptosystems using Quantum Period Finding. CRYPTO 2016

Authentication schemes that are secure classically are broken in the quantum query model using Simon's algorithm.

Mahadev. Classical Verification of Quantum Computations. FOCS 2018

Breakthrough result on delegation of quantum computation by classical clients, it uses a variant of Simon's algorithm to make the server perform an unknown measurement.

Factoring

Problem

For a composite number N, find a non-trivial factor of N.

Classical algorithms:

Shor's algorithm (1994) - overview

Periodic functions

Definition

A function $f : \mathbb{F} \to \mathbb{F}$ is periodic if $\exists\ r$ such that $f(a) = f(b)$ iff $b = a + kr$.

Example

For every a, N, $f_a(x) = a^x \pmod{N}$ is periodic.

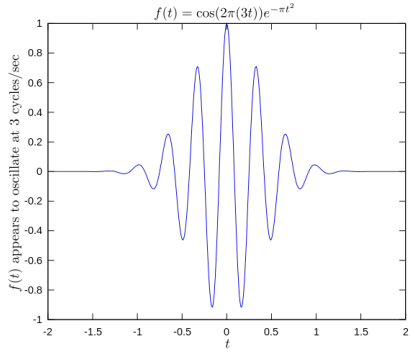
Shor's algorithm - from period finding to factoring

Algorithm 1: Factoring from period finding

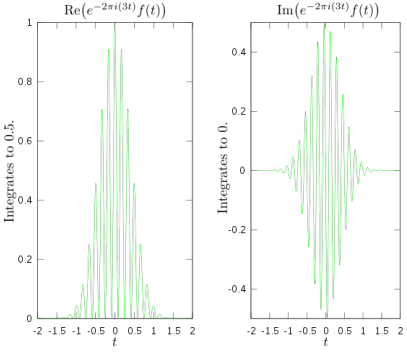
Pick an unif. random $a \in \{2, ..., N\}$;
if $gcd(x, N) > 1$ **then**
  return $gcd(a, N)$;
end
Find the period r of $f_a(x) = a^x \pmod N$;
if r *is odd* or $a^{r/2} = \pm 1 \pmod N$ **then**
  return $\perp$;
else
  return $\max\left(gcd(N, a^{\frac{r}{2}} + 1), gcd(N, a^{\frac{r}{2}} - 1)\right)$;
end

Fourier Transform

Original signal



Fourier transform



$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi} dx$$

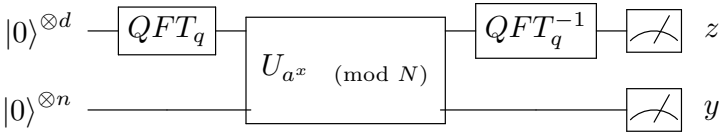
Discrete Fourier Transform

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \dots & 1 & \dots & 1 \\ 1 & \omega & \dots & \omega^{j-1} & \dots & \omega^{N-1} \\ & & & \dots & & \\ 1 & \omega^{i-1} & \dots & \omega^{(i-1)(j-1)} & \dots & \omega^{i(N-1)} \\ & & & \dots & & \\ 1 & \omega^{N-1} & \dots & \omega^{(N-1)(j-1)} & \dots & \omega^{(N-1)^2} \end{pmatrix}$$

Quantum Fourier Transform

Shor's algorithm - quantum algorithm for period finding

Pick $q = 2^d$ such that $N^2 < q < 2N^2$.



+ classical post-processing

Factoring in quantum polynomial time

Unstructured search

Computational problem

Let us assume that a function $f : \{0,1\}^n \to \{0,1\}$ has the following property:

$$\exists \text{ a unique } x^* \text{ such that } f(x^*) = 1.$$

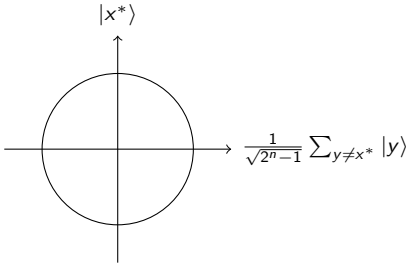
Find x^*.

Classical algorithms:

Grover search - amplitude amplification

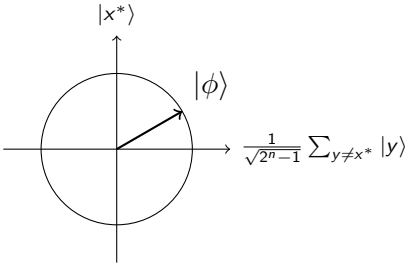
Grover search - amplitude amplification

Phase inversion



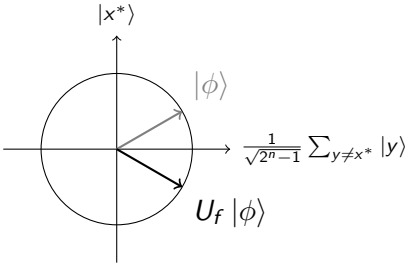
Grover search - amplitude amplification

Phase inversion



Grover search - amplitude amplification

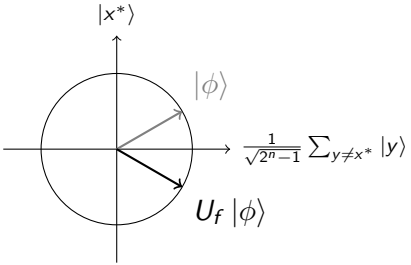
Phase inversion



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

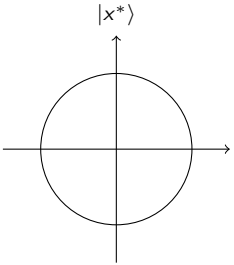
Grover search - amplitude amplification

Phase inversion



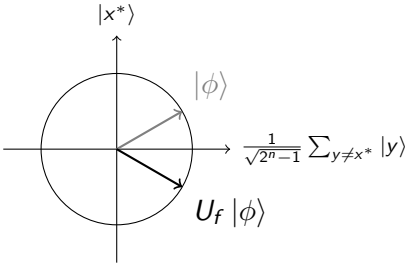
$U_f |i\rangle = (-1)^{f(i)} |i\rangle$

Inversion about the mean



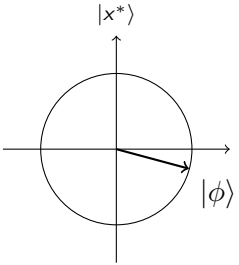
Grover search - amplitude amplification

Phase inversion



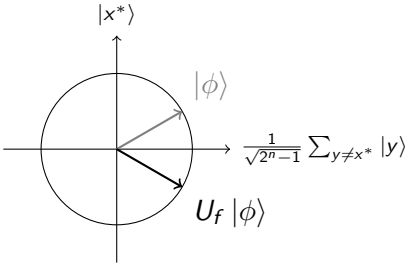
$U_f |i\rangle = (-1)^{f(i)} |i\rangle$

Inversion about the mean



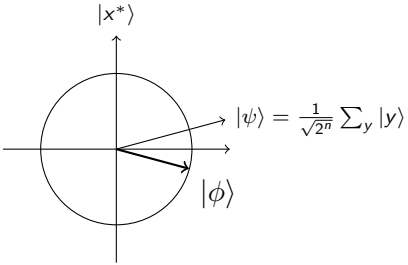
Grover search - amplitude amplification

Phase inversion



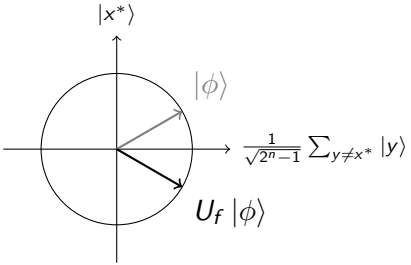
$U_f |i\rangle = (-1)^{f(i)} |i\rangle$

Inversion about the mean



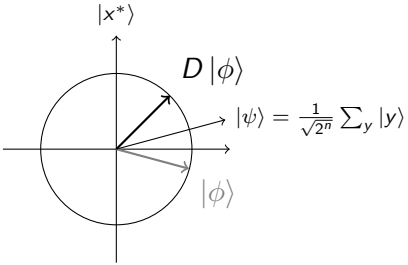
Grover search - amplitude amplification

Phase inversion



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

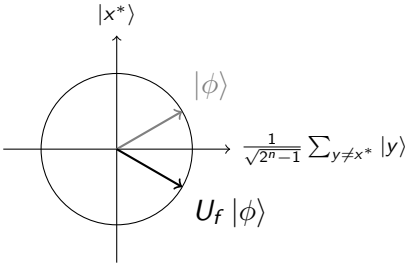
Inversion about the mean



$D |i\rangle = H^{\otimes n}(I - 2 |0\rangle\langle 0|)H^{\otimes n} |i\rangle$

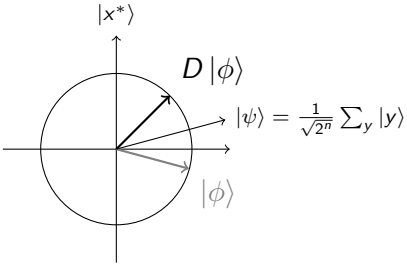
Grover search - amplitude amplification

Phase inversion



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

Inversion about the mean



$D|i\rangle = H^{\otimes n}(I - 2|0\rangle\langle 0|)H^{\otimes n}|i\rangle$

Grover's algorithm

Start from $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$ and repeat these two procedures $\sqrt{2^n}$ times.

Grover search and amplitude amplification

- The algorithm can be generalized for different settings: more than one marked element, amplification of success probability, quantum rewinding in quantum cryptographic protocols
- Quadratic speedup over classical algorithm
- Not so drastic, but it solves a generic problem
- It can be reframed into different frameworks: quantum walks, block encoding and Hamiltonian simulations, ...

Recent (somewhat) advances in quantum algorithms

- Quantum linear algebra
  - Linear system of equations
  - Semi-definite programming
  - Applications to Quantum Machine Learning: faster recommendation systems, ...
- Quantum learning theory
  - Learning theory: ML from the perspective of complexity theory
  - Exponential separation between some quantum and classical models
  - Connections to cryptography and circuit lower bounds
- Quantum chemistry
  - Using quantum computers to simulate quantum systems
- NISQ: Near-term intermediate scale quantum computers
  - What can we do with current Google, IBM, D-Wave devices?