Quantum algorithms for groups

Katalin Friedl
&
Ivanyos Gábor
MTA SZTAKI (Budapest)

Quantum computation – the beginning

Moore's Law (G. Moore, co-founder of Intel, 1965):

transistor density doubles every couple of years

$\Rightarrow$ transistor $\approx$ atom by the year 2020

$\Rightarrow$ laws of quantum physics might be in effect

$\Rightarrow$ basic rules of computation may change

$\Rightarrow$ quantum computer

simulation of quantum physical systems:
not efficient by classical machines

$\Rightarrow$ quantum computers would be more powerful
(good in simulating quantum systems)

Benioff, Feynman, $\approx$ 1980

Physical realization

several attempts
- nuclear magnetic resonance
- ion traps
- photon polarization, etc

huge machine — tiny computational power

Theoretical model

- new complexity classes
- algorithms from new point of view

Main features:

- randomization
- high parallelism

in an $\mathcal{UNUSUAL}$ way

Bits

Classical bit

$$b \in \{0, 1\}$$

Random bit

$$r = \begin{cases} 0 & \text{with prob. } p \\ 1 & \text{with prob. } 1 - p \end{cases}$$

$\Rightarrow$ distribution $d = (p, q) \in \mathbb{R}^2_+$, $\|d\|_1 = 1$

Quantum bit = *qubit*

$$q \in \mathbb{C}^2, \ \|q\|_2 = 1$$

Fix an orthonormal basis v_0, v_1 of $\mathbb{C}^2$

$$q = \alpha v_0 + \beta v_1,$$
$$\alpha, \beta \in \mathbb{C},$$
$$|\alpha|^2 + |\beta|^2 = 1$$

Dictionary

Dirac's notation is preferred
(thanks to physicists)

linear combination	–	superposition
coefficient α	–	amplitude α
column vector w	–	"ket" vector $\|w\rangle$
row vector w^t	–	"bra" vector $\langle w\|$
inner product $w^t z$	–	$\langle w\|z\rangle \quad \in \mathbb{C}$
basis vectors v_0, v_1	–	$\|0\rangle$, $\|1\rangle$
$v_{b_1 b_2 \ldots b_n}$	–	$\|b_1 b_2 \ldots b_n\rangle$
$v_{0\ldots0}, v_{0\ldots01}, v_{0\ldots10}, \ldots$	–	$\|0\rangle, \|1\rangle, \|2\rangle, \ldots$

Possible steps

Computational step on a qubit $|\psi\rangle$

apply some linear transformation T on $|\psi\rangle$

condition:
has to produce a qubit: $\| T|\psi\rangle \|_2 = 1$

$\Rightarrow T^*T = Id$ (*unitary transformation*)
($T^* = \overline{T}^t$ conjugate transpose of T)

Measurement or *observation:*

checking a value can modify it
(by laws of physics)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \overset{\text{Meas.}}{\longrightarrow} \begin{cases} |0\rangle & \text{Pr} = |\alpha|^2 \\ |1\rangle & \text{Pr} = |\beta|^2 \end{cases}$$

Example

Hadamard transformation:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\Rightarrow \qquad H^* = H,\ H^*H = Id$$

$$|0\rangle \overset{H}{\to} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{\text{Meas.}} \begin{cases} |0\rangle & \text{Pr} = 1/2 \\ |1\rangle & \text{Pr} = 1/2 \end{cases}$$

$$\overset{H}{\to} \quad \xrightarrow{\text{Meas.}} \begin{cases} |0\rangle & \quad \text{Pr} = 1/2 \\ |1\rangle & \quad \text{Pr} = 1/2 \end{cases}$$

$$|0\rangle \overset{H}{\to} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \overset{H}{\to} |0\rangle \xrightarrow{\text{Meas.}} |0\rangle$$

n-qubit register

space: $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$

base:
$$\begin{array}{c}
|0\rangle \otimes \ldots \otimes |0\rangle \otimes |0\rangle, \\
|0\rangle \otimes \ldots \otimes |0\rangle \otimes |1\rangle, \\
|0\rangle \otimes \ldots \otimes |1\rangle \otimes |0\rangle, \\
\vdots \\
|1\rangle \otimes \ldots \otimes |1\rangle \otimes |1\rangle.
\end{array}$$

$$\downarrow$$

$$|0\ldots00\rangle, \quad |0\ldots01\rangle, \quad |0\ldots10\rangle, \quad \ldots \quad |1\ldots11\rangle$$

$$\downarrow$$

$$|0\rangle, \quad |1\rangle, \quad |2\rangle, \quad \ldots \quad |2^n-1\rangle$$

n-qubit register:

$$|\psi\rangle \in \mathbb{C}^{2^n}, \quad \| \, |\psi\rangle \, \|_2 = 1$$

$$|\psi\rangle = \sum_{b_i \in \{0,1\}} \alpha_{b_1 b_2 \ldots b_n} |b_1 b_2 \ldots b_n\rangle$$

$$\sum |\alpha_{b_1 b_2 \ldots b_n}|^2 = 1$$

Steps

- local unitary transformations on $\mathbb{C}^{2^n}$

  local $\approx$ built from $poly(n)$ constant dimensional transformations (by tensor product)

- measurements
  $|\psi\rangle \longrightarrow |b_1 b_2 \ldots b_n\rangle$ with prob. $|\alpha_{b_1 b_2 \ldots b_n}|^2$

  (in general: projections to an orthogonal decomposition of the space)

No-cloning theorem

There is no unitary transformation U, s.t. for every qubit $|\psi\rangle$

$$|\psi\rangle \otimes |0\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle.$$

Classical copying:

$$\begin{array}{rcl} |\psi\rangle \otimes |0\rangle & = & (\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \\ & & \downarrow \\ & & \alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |1\rangle \quad \neq |\psi\rangle \otimes |\psi\rangle \end{array}$$

Example

Given $f : \{0, \ldots, N-1\} \to \{0, 1\}$, $N = 2^n$

Decide if f is constant
or f is balanced: $|f^{-1}(0)| = N/2$

Classical: $N/2 + 1$ queries necessary
when f is given by black box

$$x \longrightarrow \boxed{f} \longrightarrow f(x)$$

Quantum: 1 query is sufficient
with a "quantum box"

Quantum box 1.

$$\sum_{k,b} \alpha_{k,b} |k\rangle \otimes |b\rangle \longrightarrow \quad f \quad \longrightarrow \sum_{k,b} \alpha_{k,b} |k\rangle \otimes |b + f(k)\rangle$$

Quantum box 2.

$$\sum_{k} \alpha_{k} |k\rangle \longrightarrow \quad f \quad \longrightarrow \sum_{k} (-1)^{f(k)} \alpha_{k} |k\rangle$$

Quantum box 2 from 1 :

$$\sum_{k} \alpha_{k} |k\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \longrightarrow \quad f \quad \longrightarrow$$

$$\sum_{k} \alpha_{k} |k\rangle \otimes \frac{|f(k)\rangle - |1 + f(k)\rangle}{\sqrt{2}} \xrightarrow{H}$$

$$\sum_{k} \alpha_{k} |k\rangle \otimes (-1)^{f(k)} |1\rangle$$

Algorithm

$$|0^n\rangle \xrightarrow{H^{\otimes n}} \quad f \quad \xrightarrow{H^{\otimes n}} \text{ Meas.} \longrightarrow$$

Step 1. $\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle$

Step 2. $f \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (-1)^{f(k)} |k\rangle$

quantum parallelism

Step 3. $\xrightarrow{H^{\otimes n}} |\psi\rangle$

interference

$\psi = \alpha|0\rangle + \dots$ where

$$\alpha = \frac{1}{N} \sum_{k=0}^{N-1} (-1)^{f(k)}$$

$$= \begin{cases} \pm 1 & \text{if } f \text{ is constant} \\ 0 & \text{if } f \text{ is balanced} \end{cases}$$

Computational power

- classical Turing machine can be simulated by quantum Turing machine

  quantum computational steps =
  unitary transformations
  $\Rightarrow$ invertible

  classical computation
  can be made invertible
  (reversible computation)

  can be described by "local"
  unitary transformations

- quantum Turing machine can be simulated by classical Turing machine

Difference in efficiency ?

- Search in an unordered list Grover'96
  classical (randomized): $\Theta(n)$
  quantum (randomized): $\Theta(\sqrt{n})$

- Search in an ordered list Ambainis'99
  classical and quantum: $\Theta(\log n)$

- Factoring integers Shor'94
  quantum (randomized) poly time

  generalizes to "hidden subgroup problem"
  important tool: Fourier transform on groups