Hidden Symmetry Detection on a Quantum Computer

Ralf Schützhold &
William G. Unruh

- Introduction
- Motivation
- Hidden Symmetry Detection
- Simon-type Symmetry
- Shor-type Symmetry
- Summary and Outlook

Introduction

$$\exists\, U \;:\; \forall\, x \;:\; f(x) = f(U[x])$$

Hidden sub-group problem

- Shor $f(x+p) = f(x)$
- Simon $f(x \oplus p) = f(x)$
- Bernstein-Vazirani $f(x) = a \cdot x$
- Deutsch-Jozsa $f(x) = f(x')$?
- Deutsch $f(0) = f(1)$?

With $\oplus$ bit-wise addition modulo two $1001 \oplus 1100 = 0101$

$$x \cdot y = x_1 \oplus y_1 \oplus \cdots \oplus x_n \oplus y_n = \sum_{l=1}^{n} x_l y_l \bmod 2$$

Scalar product modulo two

$\Rightarrow$ **exponential speed-up**

Shor's period-finding $\Rightarrow$ factoring, etc.

Further Algorithms?

Restrictions:

- neither acquisition of information
  e.g., quantum imaging and pattern recognition
- nor transport of information
  e.g., cryptography and super-dense coding
- classical problems
  i.e., no quantum simulation

$\Rightarrow$ just information processing

Formulation: given $f : x \rightarrow f(x)$, find out property

Exponential speed-up $\Rightarrow$

- polynomial representation of function f $(PSPACE)$
- exponential number of arguments/elements x

Hidden sub-group problem

$$f\left(U[x]\right) = f(x)$$

Abelian $(\oplus, +)$ and non-Abelian (e.g., permutations)?

Motivation

Which other problems admit an exponential speed-up?

Warning! **Warning!**

The following arguments are

- intuitive as well as
- suggestive but
- neither conclusive
- nor rigorous.

Warning! **Warning!**

Relevance of Elements

$$|\Psi_{\rm out}\rangle = \mathcal{U}_m \mathcal{U}_f \mathcal{U}_{m-1} \cdots \mathcal{U}_1 \mathcal{U}_f \mathcal{U}_0 |0\rangle$$

Most general sequential quantum algorithm

I.e., neither quantum adiabatic evolution ($\Rightarrow$ ground state)

nor simulated (quantum) annealing, etc.

Polynomial $\mathcal{U}_j$ and

$$\mathcal{U}_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

With possible extension $\mathcal{U}_f \rightarrow \mathcal{U}_f \otimes \mathbf{1}$

$$\mathcal{U}_f = (\mathcal{P}_{\rm rel} + \mathcal{P}_{\rm irr}) \mathcal{U}_f (\mathcal{P}_{\rm rel} + \mathcal{P}_{\rm irr})$$

Assumption: $\mathcal{U}_j$ do not favor $\mathcal{P}_{\rm rel}\mathfrak{H}$

$\Rightarrow$ no exponentially small number of relevant elements

Example: period-finding (all elements equally relevant)

Counter-example: chess, traveling salesman problem

Still polynomial speed-up possible

E.g., Grover: $\sqrt{N}$ vs. N , bilinear structure (norm)

Excess Information

Unitary gates $\Rightarrow$ reversible computation

Erasing of information only by measurement (e.g., phase)

Example: period-finding, state after measurement

$$|\Psi\rangle = \frac{1}{\sqrt{L}} \sum_{l=0}^{L-1} |x_0 + lp\rangle$$

$\Rightarrow x_0$ ($\rightarrow$ phase) and p ($\rightarrow$ wave-number)

Notion of "classical information of quantum state"

Information required for reproducing the quantum state $|\Psi\rangle$ from $|0\rangle$ in the computational basis via elementary operations

No unitarily invariant information measure!

Counter-example: average invertability check $\langle \dim(f^{-1}) \rangle$

$$|\Psi_y\rangle = \frac{1}{\sqrt{L}} \sum^{(L)} |x \,:\, f(x) = y\rangle$$

Apparently too much excess information to get rid of

Hidden Symmetry Detection

Hidden sub-group $\Leftrightarrow U$

$$f\left(U[x]\right) = f(x)$$

Symmetry ensures conditions for exponential speed-up

- all elements are equally relevant
- not too much excess information

Other symmetries achieving the same goal?

$$V\left\{f(x), f\left(U[x]\right)\right\} = 0$$

Hidden symmetry $\Leftrightarrow U, V$ as generalization

Quantum algorithm for finding U (and V)?

Superposition principle ("quantum parallelism")

$\Rightarrow$ linear representation (Abelian/non-Abelian?)

Simon $U[x] = x \oplus p$ and Shor $U[x] = x + p$

Generalization of Simon's Algorithm

$$f(x) \oplus f(x \oplus p) \oplus q = 0 \;\leftrightarrow\; f(x \oplus p) = f(x) \oplus q$$

With $0 \leq x, f(x), p, q < N = 2^n$

Usual trick ("quantum parallelism")

$$\begin{aligned} |\Psi\rangle &= \mathcal{U}_f \left(\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|0\rangle \right) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|f(x)\rangle \\ &= \sum_{x_0}^{(N/2)} \frac{|x_0\rangle\,|f(x_0)\rangle + |x_0 \oplus p\rangle\,|f(x_0) \oplus q\rangle}{\sqrt{N}} \end{aligned}$$

Multiple application of Hadamard gate

$$\mathcal{H}^{(2n)}\,|\Psi\rangle = \frac{2}{\sqrt{N^3}} \sum_{x_0}^{(N/2)} \sum_{R \cdot Y = 0}^{(N^2/2)} (-1)^{X \cdot Y}\,|Y\rangle$$

With $|X\rangle = |x_0\rangle \otimes |f(x_0)\rangle$ and $|R\rangle = |p\rangle \otimes |q\rangle$

$$R \cdot Y = \sum_{l=0}^{2n} R_l Y_l \bmod 2 = \sum_{l=0}^{n} (p_l Y_l + q_l Y_{n+l}) \bmod 2$$

For $|X\rangle = |x_0\rangle \otimes |f(x_0)\rangle$ pseudo-randomly distributed

$\mathcal{O}(2n)$ measurements of Y yield $|R\rangle = |p\rangle \otimes |q\rangle$

Generalization of Shor's Algorithm

$$f(x+p) = f(x) + q$$

With $0 \leq x, f(x) < N = 2^n$ and $N^{\delta>0} \ll q \ll p \ll N^{\varepsilon<1}$

$$\begin{aligned} |\Psi\rangle &= \mathcal{U}_f \left(\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|0\rangle \right) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|f(x)\rangle \\ &\approx \sum_{x_0=0}^{p-1} \sum_{l=0}^{[N/p]} \frac{|x_0 + lp\rangle\,|f(x_0) + lq\rangle}{\sqrt{N}} \end{aligned}$$

Double quantum Fourier transform

$$\begin{aligned} \mathcal{QFT}^{(2)}\,|\Psi\rangle \approx & \sum_{k_x=0}^{N-1} \sum_{k_y=0}^{N-1} \sum_{x_0=0}^{p-1} \frac{e^{2\pi i (x_0 k_x + f(x_0) k_y)/N}}{\sqrt{N^3}} \times \\ & \sum_{l=0}^{[N/p]} \exp\left\{ 2\pi i \, \frac{p k_x + q k_y}{N} \, l \right\} |k_x\rangle\,|k_y\rangle \end{aligned}$$

Constructive interference

$$\frac{p k_x + q k_y}{N} \in \mathbb{N} \pm \mathcal{O}\left(\frac{p}{N}\right)$$

No structure (e.g., additional periodicity) in $f(x_0)$

$\Rightarrow$ k_x and k_y separately pseudo-random

Continued Fraction Algorithm

$$\frac{pk_x + qk_y}{N} \in \mathbb{N} \pm \mathcal{O}\left(\frac{p}{N}\right)$$

With $p, q \ll k_x, k_y, N$

$$p\,\frac{a}{b} + q\,\frac{c}{d} \in \mathbb{N}$$

With $a, b, c, d \ll k_x, k_y, N$, but possibly $a, b, c, d \gg p, q$

$$pa + q\,\frac{bc}{d} \bmod b = 0$$

Obviously $qbc/d \in \mathbb{N} \Rightarrow$ determine q with several runs

$$p = -a^{-1} q\,\frac{bc}{d} \bmod b$$

Euklid's algorithm (polynomial)

$\Rightarrow$ **exponential speed-up**

Another example

$$f(x + p) = f(x) + pq \bmod N$$

With both, p and q unknown

$$g(x) = f(x) - qx \bmod N \;\rightsquigarrow\; g(x + p) = g(x)$$

Discussion

- generalization of hidden sub-group problem
- also NP-problem
- inverse problem (input+output$\rightarrow$parameter)
- Simon: $U \leftrightarrow p$ and $V \leftrightarrow q$ unknown

  Shor: $U \leftrightarrow p$ unknown and $V \leftrightarrow q$ known

  (For known p problem is much easier.)

Outlook

- most general (explicit) two-point symmetry

$$V\{f(x), f(U[x, f(x)])\} = 0$$

- $(m+1)$-point symmetries

$$V\{f(x), f(U_1[x]), \ldots, f(U_m[x])\} = 0$$

- further groups (Abelian/non-Abelian)
- gauge symmetries
- applications

Summary

The detection of hidden (two-point) symmetries

$$V\{f(x), f(U[x])\} = 0$$

can also admit an exponential speed-up:

- Simon-type symmetry $f(x \oplus p) = f(x) \oplus q$
- Shor-type symmetry $f(x + p) = f(x) + q$

Preprint: `quant-ph/0304090`

Acknowledgments

- valuable conversations with R. Laflamme and R. Cleve
- Alexander von Humboldt foundation
- Canadian Institute for Advanced Research
- Natural Science and Engineering Research Council of Canada