Problems Solved by Quantum Fourier Transform Efficiently

2019.10.25

BOBO

4th undergraduate, UTokyo

Structure of Today’s Topics

On Non-Abelian Groups

Finding hidden normal subgroups of
- solvable groups
- permutation groups

finding hidden subgroups
- of groups with small commutator subgroup
- of groups admitting an elementary Abelian normal 2-subgroup of small index

Dihedral Hidden Subgroup Problem

Graph Isomorphism

On Abelian Groups

HSP

Order Finding Problem, $(Z_n, +)$
Periodicity Finding Problem, $(\{0,1\}^n, \oplus)$
Discrete Logarithm Problem, $(Z_n \times Z_n, +)$
$\vdots$

Classification of Hidden Subgroup Problems

Structure of Today's Topics

On Non-Abelian Groups

Efficiently solved by QFT

On Abelian Groups

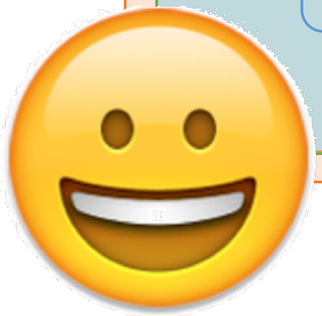
HSP $\left\{ \begin{array}{c} \text{Order Finding Problem, } (Z_n, +) \\ \text{Periodicity Finding Problem, } (\{0,1\}^n, \oplus) \\ \text{Discrete Logarithm Problem, } (Z_n \times Z_n, +) \\ \vdots \end{array} \right\}$

Finding hidden normal subgroups of
- solvable groups
- permutation groups

finding hidden subgroups
- of groups with small commutator subgroup
- of groups admitting an elementary Abelian normal 2-subgroup of small index

Dihedral Hidden Subgroup Problem

Graph Isomorphism



Classification of Hidden Subgroup Problems

Structure of Today's Topics

On Non-Abelian Groups

Efficiently solved by QFT

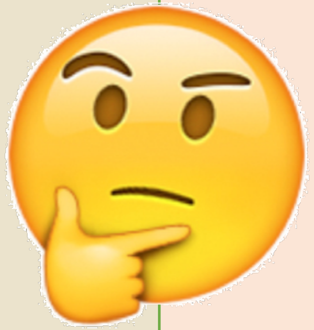
On Abelian Groups

HSP $\left\{ \begin{array}{c} \text{Order Finding Problem, } (Z_n, +) \\ \text{Periodicity Finding Problem, } (\{0,1\}^n, \oplus) \\ \text{Discrete Logarithm Problem, } (Z_n \times Z_n, +) \\ \vdots \end{array} \right\}$

Finding hidden normal subgroups of
- solvable groups
- permutation groups

finding hidden subgroups
- of groups with small commutator subgroup
- of groups admitting an elementary Abelian normal 2-subgroup of small index

Dihedral Hidden Subgroup Problem



Graph Isomorphism

Classification of Hidden Subgroup Problems

Outline of Today’s Topics

- Examples of efficient algorithms using Quantum Fourier Transform
- Efficiency of QFT solving Hidden Subgroup Problems (HSP) over General Abelian Groups
- QFT over non-Abelian Groups
- Recent results

Order Finding Problem

- Definition of the Problem
  - INPUT : N, y coprime to N
  - OUTPUT : order r of y mod N (the min-number r satisfying $y^r \equiv 1 \bmod N$)
- Formalization
  - Z_n : group of integer mod n
  - $f : Z_Q \to Z_N$, Q is arbitrary large number
    $x \mapsto y^x \bmod N$
  - If r is the order of y mod N, for $x + r \le q$, $f(x+r) = f(x)$

$$U_f : |x_1\rangle|x_2\rangle \mapsto |x_1\rangle|x_2 + y^{x_1}\, mod\ N\rangle$$
for $x_1 \in Z_q,\ x_2 \in Z_N$

- Example
  - The order of $y = 4$ mod $N = 11$ is $r = 5$

$4^1 = 4 \bmod 11$
$4^2 = 16 = 5 \bmod 11$
$4^3 = 64 = 9 \bmod 11$
$4^4 = 256 = 3 \bmod 11$
$4^5 = 1024 = 1 \bmod 11$

Order Finding Problem
--- Shor's Algorithm (Shor 1994)

- Step 1
  - $|0^q\rangle|0^N\rangle \xrightarrow{(H^{\otimes q})\otimes I} \left(H^{\otimes q}|0^q\rangle\right)|0^N\rangle = \frac{1}{\sqrt{2^q}}\sum_{x=0}^{2^q-1}|x\rangle\,|0^N\rangle$
- Step 2
  - $\xrightarrow{U_f}$ $U_f\left(\frac{1}{\sqrt{2^q}}\sum_{x=0}^{2^q-1}|x\rangle\,|0^N\rangle\right) = \frac{1}{\sqrt{2^q}}\sum_{x=0}^{2^q-1}|x\rangle\,|y^x\rangle$
- Step 3
  - $\xrightarrow{measurement}$ $\frac{1}{\sqrt{A+1}}\sum_{\lambda=0}^{A}|x_0+\lambda r\rangle\,|y^{x_0}\rangle$
- Step 4
  - $\xrightarrow{DFT_q}$ $\sum_{k\in Z_r} e^{i\phi_k(x_0)}\left|\frac{k2^q}{r}\right\rangle|y^{x_0}\rangle$
- Step 5
  - $\xrightarrow{measurement}$ $\frac{k2^q}{r}$
  - using continued fractions to get the value of order r

Assumption: $\mathrm{Q} = 2^q$
for general $\mathrm{Q} \in \mathbb{N}$, it is also efficient,
with the probablistic algorithm by Kitaev

measure register 2, and we
assume that getting y^{x_0}

Fourier Transform
$|k\rangle \mapsto \frac{1}{\sqrt{2^q}}\sum_{x=0}^{2^q-1} e^{i2\pi x\frac{k}{2^q}}|x\rangle$, for $|k\rangle \in Z_{2^q}$

Period Finding Problem on Boolean Function

- Definition of the Problem
  - INPUT : two-to-one function $f: \{0,1\}^n \to \{0,1\}^n$ with unknown periodicity $\xi \in \{0,1\}^n$, satisfying $f(x) = f(y) \Leftrightarrow y = x \oplus \xi$
  - OUTPUT : periodicity $\xi \in \{0,1\}^n$

$U_f : |x_1\rangle|x_2\rangle \mapsto |x_1\rangle|x_2 \oplus f(x_1)\rangle$
for $x_1, x_2 \in \{0,1\}^n$

- Example (Deutsch)
  - In the case of $n = 1$, the problem is to check $\xi = 0 \; or \; 1$.
  - $|+\rangle|-\rangle \xrightarrow{U_f} (-1)^{f(0)} \frac{1}{2} (|0\rangle + (-1)^{f(0)\oplus f(1)}) |-\rangle$

$$\xrightarrow{H} \frac{1}{2}\left(\left(1 + (-1)^{f(0)\oplus f(1)}\right)|0\rangle + \left(1 - (-1)^{f(0)\oplus f(1)}\right)|1\rangle\right)$$

If $\xi = 0$, then f is balanced
If $\xi = 1$, then f is constant

Period Finding Problem on Boolean Function --- Simon's Algorithm (Simon 1994)

- Step 1
  - $|0^n\rangle|0^n\rangle \xrightarrow{(H^{\otimes n})\otimes I} \left(H^{\otimes n}|0^n\rangle\right)|0^n\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{n-1}|x\rangle\,|0^n\rangle$
- Step 2
  - $\xrightarrow{U_f}$ $U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{q-1}|x\rangle\,|0^n\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{n-1}|x\rangle\,|f(x)\rangle$
- Step 3
  - $\xrightarrow{measurement} \frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus \xi\rangle)$
- Step 4
  - $\xrightarrow{H^{\otimes n}}$ $\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x_0\cdot y}|y\rangle + \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{(x_0\oplus\xi)\cdot y}|y\rangle = \pm\frac{1}{\sqrt{2^n}}\sum_{y:\,y\cdot\xi=0}|y\rangle$
- Step 5
  - $\xrightarrow{measurement} y$, satisfying $y \cdot \xi = 0$
  - Solve the linear system $y_k \cdot \xi = 0$, $(k = 1, \cdots, n)$ and get the period ξ

$x \cdot y = (x_1 y_1) \oplus \cdots \oplus (x_n y_n) \in \{0,1\}$

measure register 2, and we assume that getting y $(= x_0 \oplus \xi)$

$H^{\otimes n}$ corresponds to the Fourier Transform in Shor's algorithm
Actually, $H^{\otimes n}$ *is* a Fourier Transform

Generalization

- Having similar argument on the general Abelian groups.
  - Show (quantum) Fourier transform is available on Abelian groups
  - Show quantum Fourier transform is efficient on Abelian groups

Hidden Subgroup Problem on Abelian Groups

G : (finite) Abelian group
$\{|g\rangle \mid g \in G\}$: orthonormal basis of $\mathcal{H}$

$\exists$unitary shifting actions
$h : |g\rangle \mapsto |hg\rangle, \qquad h, g \in G$

- Definition of HSP
  - INPUT : function $f : G \to X$
  - OUTPUT : a stabilizer $K = \{k \in G \mid \forall g \in G. f(kg) = f(g)\}$
- Aim : To find the stabilizer K in $O(\mathrm{poly}(\log|G|))$ time
- Step 1, 2, 3
  - Prepare the superposition, apply function f, and read the second register
  - $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle \xrightarrow{measure} \left(\frac{1}{\sqrt{|K|}} \sum_{k \in K} |g_0 k\rangle\right) |f(g_0)\rangle$

$$\sum_{k \in K} |g_0 k\rangle = g_0 \left(\sum_{k \in K} |k\rangle\right)$$

Choosing one of the cosets of G by K
[quantum coset state]

- Step 4, 5
  - The label g_0 contains no information about K
  - →*Apply QFT defined at the next slides, in order to obtain one of the elements of K*

Construction of QFT over Abelian Groups

- Aim : Define shift invariant orthonormal basis $\{|\chi_i\rangle \mid i = 1, \cdots, |G|\}$ for Fourier transform (FT)
- Prop. : $\exists\ state\ |\chi_i\rangle. \forall g \in G. g|\chi_i\rangle = e^{\phi_i(g)}|\chi_i\rangle$
- Specific construction
  - Consider any homomorphism $\chi : G \to \mathbb{C}^{\times}$
  - $|\chi_i\rangle \coloneqq \frac{1}{\sqrt{|G|}} \sum_{g \in G} \overline{\chi_i(g)} |g\rangle$
    - $\forall g \in G.\ g|\chi_i\rangle = \chi_i(g)|\chi_i\rangle$
  - Representation of FT by matrix :

$$(FT)_{ij} = \frac{1}{\sqrt{|G|}} \chi_i(g_j)$$

    - This unitary transform maps elements of $\{|\chi_i\rangle\}$ to the representations with $\{|g_i\rangle\}$ in terms of Fourier transform on finite group
- $\rightarrow$ Back to Step 4, 5
  - Apply FT to output state at Step 3, then do measurement on register 1

G is a unitary Abelian group by Def.

Useful properties of χ

- $\forall g \in G.\ \chi(g)$ is a $|G|^{th}$ root of 1
- $\frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \delta_{ij}$ (orthonormality)
- There exists exactly $|G|$ different homomorphisms

Construction of QFT over Abelian Groups

- In Shor's algorithm : for $G = Z_Q$

$$[FT]_{km} = \frac{1}{\sqrt{Q}}\chi_k(m) = \frac{1}{\sqrt{Q}}\chi_k(1)^m = \frac{1}{\sqrt{Q}}e^{i2\pi\frac{km}{Q}}$$

- In Simon's algorithm : for $G = \{0,1\}^n$

$$[FT]_{ij} = \frac{1}{\sqrt{2^n}}\chi_{x_i}(y_j) = \frac{1}{\sqrt{2^n}}(-1)^{x_i \cdot y_j}, \qquad x_i, y_j \in \{0,1\}^n$$

$FT = H^{\otimes n}$ in this case

$$\frac{1}{\sqrt{4}}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{pmatrix} = \frac{1}{\sqrt{4}}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}, \omega = e^{i2\pi\frac{1}{4}}$$

Efficiency of QFT over Abelian Groups

- Is the efficiency of QFT unique to quantum system? --- …Yes (?)
- Superposition + nonlocality of synthetic quantum system
  - $w = Mv$
  - $M = S^{(1)} \otimes \cdots \otimes S^{(n)}$
  - $w_{j_1 \cdots j_n} = \sum_{B^n} S^{(1)}_{j_1 i_1} \cdots S^{(n)}_{j_n i_n} v_{i_1 \cdots i_n}$
- The violation of Bell inequalities (and its proof) relies on the superposition and nonlocality of synthetic quantum system
  - → Does QFT process also use the state of which the correlation violates Bell inequalities? --- …Yes (?)
- Operator which can be decomposed into tensor product of some small fractions, is executed exponentially faster than classical algorithm …(?)

Brief Summary for HSP and QFT on Abelian Group

- Not only Order finding Problem, other problems with remarkable fast algorithm (e.g. DLP), are also the case of HSP on Abelian group!

- It is efficient to solve Hidden Subgroup Problem over Abelian Group, by using Quantum Fourier Transform

Name	G	X	K	Function
Deutsch	$\{0,1\}, \oplus$	$\{0,1\}$	$\{0\}$ or $\{0,1\}$	$K=\{0,1\}: \begin{cases} f(x)=0 \\ f(x)=1 \end{cases}$ $K=\{0\}: \begin{cases} f(x)=x \\ f(x)=1-x \end{cases}$
Simon	$\{0,1\}^n, \oplus$	any finite set	$\{0,s\}$ $s \in \{0,1\}^n$	$f(x \oplus s) = f(x)$
Period-finding	$\mathbf{Z}$, +	any finite set	$\{0,r,2r,\ldots\}$ $r \in G$	$f(x+r) = f(x)$
Order-finding	$\mathbf{Z}$, +	$\{a^j\}$ $j \in Z_r$ $a^r = 1$	$\{0,r,2r,\ldots\}$ $r \in G$	$f(x) = a^x$ $f(x+r) = f(x)$
Discrete logarithm	$\mathbf{Z}_r \times \mathbf{Z}_r$ + (mod r)	$\{a^j\}$ $j \in Z_r$ $a^r = 1$	$(\ell, -\ell s)$ $\ell, s \in \mathbf{Z}_r$	$f(x_1,x_2) = a^{kx_1+x_2}$ $f(x_1+\ell, x_2-\ell s) = f(x_1,x_2)$
Order of a permutation	$\mathbf{Z}_{2^m} \times \mathbf{Z}_{2^n}$ + (mod 2^m)	$\mathbf{Z}_{2^n}$	$\{0,r,2r,\ldots\}$ $r \in X$	$f(x,y) = \pi^x(y)$ $f(x+r,y) = f(x,y)$ π = permutation on X
Hidden linear function	$\mathbf{Z} \times \mathbf{Z}$, +	$\mathbf{Z}_N$	$(\ell, -\ell s)$ $\ell, s \in X$	$f(x_1,x_2) =$ $\pi(sx_1 + x_2 \bmod N)$ π = permutation on X
Abelian stabilizer	(H, X) H = any Abelian group	any finite set	$\{s \in H \mid f(s,x) = x, \forall x \in X\}$	$f(gh,x) = f(g, f(h,x))$ $f(gs,x) = f(g,x)$

Reference : Michael A. Nielsen & Isaac L. Chuang ,
Quantum Computation and Quantum Information, page 241, Figure 5.5

QFT over Non-Abelian Groups

- If a group is not Abelian…
  - $\rightarrow$ There does not necessarily exist shift invariant basis
  - $\rightarrow$ Cannot apply QFT directly

- Some special cases focusing on structures of group theory are efficiently computable by QFT

Results on QFT over Non-Abelian Groups

- Graph Isomorphism
  - entangled quantum measurements on at least $\Omega(n \log n)$ coset states are necessary to get useful information for the case of graph isomorphism
- Dihedral Hidden Subgroup Problem (DHSP)
  - Greg Kuperberg has shown a $2^{O(\sqrt{\log N})}$ time algorithm in 2005
- the normal HSP in solvable and permutation groups
  - the efficient quantum solution for without any assumption on the computability of noncommutative Fourier transforms is shown by G ́abor Ivanyos, Fr ́ed ́eric Magniez, and Miklos Santha in 2006
- the shifted Legendre symbol problem
  - Wim Van Dam, Sean Hallgren, and Lawrence Ip gave an efficient algorithm
- the hidden subgroup approach is also guaranteed to always fail for the arbitrarily large classes of graph isomorphism problems

  → the hidden subgroup approach is essentially a dead …REALLY!?

References

- Textbooks
  - Chung, I. L., and M. A. Nielsen. "Quantum Computing and Quantum Information." (2000).
- Papers
  - Jozsa, Richard. "Quantum algorithms and the Fourier transform." *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 454.1969 (1998): 323-337.
  - Jozsa, Richard. "Entanglement and quantum computation." *arXiv preprint quant-ph/9707034* (1997).
  - Ivanyos, Gábor, Frédéric Magniez, and Miklos Santha. "Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem." *International Journal of Foundations of Computer Science* 14.05 (2003): 723-739.
  - Hallgren, Sean, et al. "Limitations of quantum coset states for graph isomorphism." *Journal of the ACM (JACM)* 57.6 (2010): 34.
  - Kuperberg, Greg. "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem." *SIAM Journal on Computing* 35.1 (2005): 170-188.
  - Hallgren, Sean, Alexander Russell, and Amnon Ta-Shma. "The hidden subgroup problem and quantum computation using group representations." *SIAM Journal on Computing* 32.4 (2003): 916-934.
  - Hallgren, Sean, et al. "Limitations of quantum coset states for graph isomorphism." *Journal of the ACM (JACM)* 57.6 (2010): 34.
  - Van Dam, Wim, Sean Hallgren, and Lawrence Ip. "Quantum algorithms for some hidden shift problems." *SIAM Journal on Computing* 36.3 (2006): 763-778.
  - Shehab, Omar, and Samuel J. Lomonaco Jr. "Quantum Fourier Sampling is Guaranteed to Fail to Compute Automorphism Groups of Easy Graphs." *arXiv preprint arXiv:1705.00760* (2017).
- Online Pages
  - https://quantumalgorithmzoo.org/