Weak Fourier-Schur Sampling, the Hidden Subgroup Problem & the Quantum Collision Problem

Pawel M. Wocjan

School of Electrical Engineering and Computer Science

University of Central Florida

Orlando

wocjan@cs.ucf.edu

Joint work

- Andrew Childs (Caltech)
- Aram Harrow (University of Bristol)

Hidden Subgroup Problem

- let G be a finite group and S some finite set
- let $f : G \to S$ be a black-box function
- we have the promise that f hides a subgroup $H \leq G$, that is, $f(g) = f(g')$ iff $gH = g'H$
- the task is to determine the unknown subgroup H (say, in terms of a generating set) as quickly as possible
- an algorithm is considered to be efficient if it runs in time poly(log($|G|$)

Motivation - Integer Factorization

- integer factorization can be reduced (probabilistically) to determining the order of an element a modulo n
- this can be viewed as a HSP over $G := \mathbb{Z}$
- let $S := \mathbb{Z}_n$ and define f by setting $f(x) = a^x$
- the HSP is $r\mathbb{Z}$, where r is the order of a, that is, the smallest positive integer such that $a^r = 1$

Motivation - Graph Auto/Isomorphism

- graph automorphism (and also graph isomorphism) can be reduced to HSP over the symmetric group S_n
- let $G := S_n$, S be the set of adjacency matrices of graphs on n vertices, and A be some adjacency matrix
- define f by setting $f(\pi) = P_\pi A P_\pi^{-1}$, where P_π is the permutation matrix of size $n \times n$ corresponding to π
- the HSP is the automorphism group of the graph defined by A

Classical vs. Quantum Algorithms for HSP

- classical query complexity $\Theta(|G|)$
- quantum query complexity $O(\mathrm{poly}(\log(|G|))$
- quantum time complexity $O(\mathrm{poly}(\log(|G|))$ for
  - abelian groups
  - Heisenberg groups
  - extraspecial groups
  - and some more (good news: the list has been growing steadily)
- big challenges:
  - symmetric groups $\Longrightarrow$ graph auto/isomorphism
  - dihedral groups $\Longrightarrow$ shortest lattice vector problem

Standard Approach to HSP

- evaluate f in superposition

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle$$

- measure second register; assume s is observed; then we obtain the coset state

$$|gH\rangle := \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$$

in the first register, where g is such that $f(g) = s$; the element g is completely at random

HSP as Quantum State Identification

- using mixed states, this is described by

$$\rho_H = \frac{1}{|G|} \sum_{g \in G} |gH\rangle\langle gH|$$

- the HSP consists in distinguishing the states ρ_H for the possible $H \leq G$

Symmetry of Coset States

- the coset state ρ_H can be expressed as

$$\rho_H = \frac{1}{|G|} \sum_{g \in G} L(g)|H\rangle\langle H|L(g)^\dagger$$

  where $L(g)|h\rangle = |gh\rangle$ is the left regular representation of G

- this symmetry can be exploited with the help of Fourier decomposition

Fourier Decomposition

- the group algebra $\mathbb{C}G$ decomposes as

$$\mathbb{C}G \overset{G\times G}{\cong} \bigoplus_{\sigma\in\hat{G}} \mathcal{V}_\sigma \otimes \mathcal{V}_\sigma^*$$

where $\hat{G}$ denotes a complete set of irreducible representations of G, and $\mathcal{V}_\sigma$ and $\mathcal{V}_\sigma^*$ are the row and column subspaces acted upon by σ

Block Structure in the Fourier Basis

- ρ_H is invariant under the left multiplication of G
- the Fourier decomposition shows that

$$\rho_H \cong \frac{1}{|G|} \bigoplus_{\sigma \in \hat{G}} I_{\dim \mathcal{V}_\sigma} \otimes \rho_{H,\sigma}$$

- this means that ρ_H is block diagonal in the Fourier basis:
  - with blocks labeled by the irreps $\sigma \in \hat{G}$
  - for each σ, there is a $\dim \mathcal{V}_\sigma \times \dim \mathcal{V}_\sigma$ block $\rho_{H,\sigma}$ that appears $\dim \mathcal{V}_\sigma$ times (or in word, that it is maximally mixed in the row space)

Weak Fourier Sampling

- information gain vs. disturbance: measurements extract information about the quantum state, but at the same disturb/destroy it
- without loss of information, we can
  - measure the irrep name σ and
  - discard the information about which σ-isotopic block occurred
- the process of measuring the irrep name σ is referred to as weak Fourier sampling
- weak Fourier sampling alone produces insufficient information about H for most nonabelian groups

Strong Fourier Sampling

- therefore, a refined measurement must be performed inside the resulting subspace
- this is referred to as strong Fourier sampling
- many possibilities; especially if the irrep has large dimension

k copies $\rho_H^{\otimes k}$

- just one ρ_H is not sufficient to determine H
- $\Rightarrow$ we must repeat the sampling procedure to obtain statistics
- however, repeating strong Fourier sampling a polynomial number of times is not sufficient
- $\Rightarrow$ to solve the HSP in general, we must perform a joint measurement on $k = \mathrm{poly}(\log(|G|))$ copies of $\rho_H^{\otimes k}$
- in fact, for some groups such as the symmetric group must be entangled across $\Omega(\log(|G|)$ copies
- $\Rightarrow$ the difficulty of the general HSP may be attributed at least in part to that fact that highly entangled measurements are required

Motivation for Schur sampling

there is another measurement that can also be performed without loss of information

$$\rho_H \otimes \rho_H \otimes \cdots \otimes \rho_H$$

we consider the permutation symmetry, that is, that the state $\rho_H^{\otimes k}$ is invariant under permuting the tensor components

Schur Duality

- the decomposition of $(\mathbb{C}G)^{\otimes k}$ afforded by *Schur duality* decomposes k copies of a d-dimensional space as

$$(\mathbb{C}^d)^{\otimes k} \overset{\mathcal{S}_k \times \mathcal{U}_d}{\cong} \bigoplus_{\lambda \vdash k} \mathcal{P}_\lambda \otimes \mathcal{Q}_\lambda^d$$

- the symmetric group $\mathcal{S}_k$ acts to permute the k registers
- the unitary group $\mathcal{U}_d$ acts identically on each register
- the subspaces $\mathcal{P}_\lambda$ and $\mathcal{Q}_\lambda^d$ correspond to irreps of $\mathcal{S}_k$ and $\mathcal{U}_d$, respectively
- the irreps are labeled by partitions $\lambda \vdash k$), that is, $\lambda = (\lambda_1, \lambda_2, \ldots)$ where $\lambda_1 \geq \lambda_2 \geq \ldots$ and $\sum_j \lambda_j = k$

Form in Schur basis

- $\rho_H^{\otimes k}$ is invariant under the action of $\mathcal{S}_k \Rightarrow$ the Schur decomposition shows that it is block diagonal
- for each λ, there is a $\dim \mathcal{Q}_\lambda^{|G|} \times \dim \mathcal{Q}_\lambda^{|G|}$ block that appears $\dim \mathcal{P}_\lambda$ times; or in other words, the state is maximally mixed in the permutation space
- no information is lost if we measure the partition λ and discard the permutation register
- by analogy to weak Fourier sampling, we refer to this as *weak Schur sampling*.
- this is a natural measurement to consider (no loss of information and entangling measurement)

Weak Schur Sampling

- the distribution under weak Schur sampling is given by

$$\Pr(\lambda|\gamma) = \mathrm{tr}(\Pi_\lambda \gamma)$$

  - Π_λ is the projector onto the λ-subspace

$$\Pi_\lambda := \frac{\dim \mathcal{P}_\lambda}{k!} \sum_{\pi \in \mathcal{S}_k} \chi_\lambda(\pi)\, P(\pi)$$

  - χ_λ is the character of the irrep of $\mathcal{S}_k$ labeled by λ, and
  - P is the (reducible) representation of $\mathcal{S}_k$ that acts to permute the k registers:
    $P(\pi)|i_1\rangle \ldots |i_k\rangle = |i_{\pi^{-1}(1)}\rangle \ldots |i_{\pi^{-1}(k)}\rangle$

Invariance of the Schur Distribution

- the distribution of λ according to weak Schur sampling is invariant under the actions of the permutation and unitary groups:

$$\Pr(\lambda|\gamma) = \Pr(\lambda|P(\pi)U^{\otimes k}\,\gamma\,U^{\dagger\otimes k}P(\pi)^{\dagger})$$

  for all $U \in \mathcal{U}_d$ and all $\pi \in \mathcal{S}_k$

- in particular, the invariance under $U^{\otimes k}$ implies that for $\gamma = \rho_H^{\otimes k}$, the distribution according to weak Schur sampling depends only on the spectrum of ρ

Failure of Weak Schur Sampling

- the state ρ_H is proportional to a projector of rank $|G|/|H|$
- suppose we could distinguish between ρ_H for $H = \{1\}$ and some particular H of order $|H| \geq 2$
- $\Rightarrow$ we could distinguish between
  - k copies of the maximally mixed state $I_{|G|}/|G|$
  - k copies of the state $J_{|G|/|H|}/(|G|/|H|)$
- $\Rightarrow$ we could distinguish 1-to-1 functions from $|H|$-to-1 functions using k queries of the function
- $\Rightarrow$ this would violate the quantum lower bound for the $|H|$-collision problem stating that $k = \Omega(\sqrt[3]{|G|/|H|})$ copies are required
- however, $O(\sqrt[3]{|G|/|H|})$ copies are not sufficient

Quantum Collision Sampling Problem

Theorem: Given $\rho^{\otimes k}$, distinguishing between

- $\rho = I/d$ and
- $\rho^2 = \rho/\frac{d}{r}$, that is, ρ is proportional to a projector of rank d/r

is possible with success probability $1 - \exp(-\Theta(kr/d))/2$.
In particular, constant advantage is possible iff $k = \Omega(d/r)$.

In addition to providing the first results on estimation of the spectrum of a quantum state in the regime where $k \ll d^2$, this gives tight estimates of the effectiveness of weak Schur sampling

Proof Idea

- the proof relies on a very careful analysis of the *Schur distribution*, $\mathrm{Schur}(k,d)$, with

$$\Pr(\lambda) = \frac{\dim \mathcal{P}_\lambda \dim \mathcal{Q}_\lambda^d}{d^k} = \frac{(\dim \mathcal{P}_\lambda)^2}{k!} \prod_{(i,j)\in\lambda} \left(1 + \frac{j-i}{d}\right)$$

- we make use of known results on the typical shape of partitions under the Plancherel distributions
- we derive matching lower and upper bounds on the total variation distance of $\mathrm{Schur}(k,d)$ and $\mathrm{Schur}(k,d/r)$

Failure of Weak Schur Sampling

Corollary: Applying weak Schur sampling to $\rho_H^{\otimes k}$ (where ρ_H is defined in, one can distinguish the case $|H| \geq r$ from the case $H = \{1\}$ with constant advantage iff $k = \Omega(|G|/r)$.

Weak Fourier-Schur Sampling

- it is possible to combine Fourier and Schur sampling
- carry out weak Fourier sampling k times; since the order in which the irreps are obtained does not carry any information, we just consider the type $\underline{\sigma} := (\sigma_1, \sigma_2, \ldots, \sigma_k) \in \hat{G}^k$
- this weak Fourier-type sampling leads to a permutation-symmetric state $\rho_{H,\underline{\sigma}}$
- apply weak Schur sampling to $\rho_{H,\underline{\sigma}}$

it turns out that the distributions of $\underline{\sigma}$ and λ are uncorrelated provided that $\underline{\sigma}$ is multiplicity free; this is extremely unlikely for many groups

Failure of Weak Fourier-Schur Sampling

Theorem: The probability that weak Fourier-Schur sampling applied to $\rho_H^{\otimes k}$ provides a result that depends on $|H|$ is at most $k^2 d_{\max}^2 |H|/|G|$, where $d_{\max}$ is the largest dimension of an irrep of G.

Corollary (Weak Fourier-Schur sampling on $\mathcal{D}_N$ and $\mathcal{S}_n$):

- Weak Fourier-Schur sampling on the dihedral group $\mathcal{D}_N$ cannot distinguish the trivial subgroup from a hidden reflection with constant advantage (i.e., success probability $\frac{1}{2} + \Omega(1)$) unless $k = \Omega(\sqrt{N})$.
- weak Fourier-Schur sampling on the symmetric group $\mathcal{S}_n$ or on the wreath product $\mathcal{S}_n \wr \mathbb{Z}_2$ cannot distinguish the trivial subgroup from an order 2 subgroup with constant advantage unless $k = \exp(\Omega(\sqrt{n}))$