On the transportation problem and related questions

+ some computational algebra problems for quantum computing

Gábor Ivanyos
Institute for Computer Science and Control
Eötvös Loránd Research Network

Workshop on Quantum Algorithms in Number Theory
Fields Institute, April 19 - 21, 2022

The transportation problem

G (in this talk finite) group with

permutation action on a set Ω

Given $\omega_1, \omega_2 \in \Omega$, find

$$G_{\omega_1 \to \omega_2} = \{x \in G : x\omega_1 = \omega_2\}$$

empty or a coset of the stabilizer $G_{\omega_1} = G_{\omega_1 \to \omega_1}$

For $\omega_1 \neq \omega_2$, often just one element of $G_{\omega_1 \to \omega_2}$ is sufficient

Examples

Discrete log: $G = \mathbb{Z}_N^*$, $\Omega = \{a^x : x \in G\}$ $a^N = 1$, $\quad x \cdot a = a^x$
Graph isomorphism: $G = S_n$,
$\Omega = \{E : E$ is the edge set of a graph on n vertices$\}$,
$\{u, v\} \in \pi \cdot E$ if $\{\pi^{-1}(u), \pi^{-1}(v)\} \in E$

Toy reductions

Transportation $\prec$ Stabilizer:

$$\Gamma = \Omega \times \Omega,\ K = G \wr \mathbb{Z}_2 = (G \times G) \rtimes \mathbb{Z}_2$$

$$K_{(\omega_1,\omega_2)} \setminus G \times G$$

Stabilizer $\prec$ Hidden Subgroup: $f : x \mapsto x\omega$

level sets: left cosets of G_ω

For abelian G, further $\prec$ Stabilizer/HSP in $G \rtimes \mathbb{Z}_2$

Regular Transportation (case $G_{\omega_i} = 1$) $\prec$ Shift of injective functions

$$f_i(x) = x\omega_i$$

Abelian transportation/shift

Often better to consider transportation as a two-part problem:

Find the stabilizer H in G
Solve the "regular" transportation problem over G/H
No need to replace G with a more complicated group
A similar decomposition "works" in the noncommutative case
up to problems in G

The best/most important abelian algorithms:

Stabilizer: Shor-Kitaev 1994-95: poly($|G|$)
Regular Transportation: Kuperberg 2003, 2011; Regev 2004
exp($O(\sqrt{|G|})$)
in $\mathbb{Z}_p^n$, $p = O(1)$ prime: Friedl, I., Magniez, Santha, Sen 2003
poly(n)

From HSP/Shift to Stabilizer/Transportation

"function graph" $|f\rangle = \frac{1}{\sqrt{|G|}} \sum_{z \in G} |z\rangle |f(z)\rangle$

G permutes function graphs: $|xf\rangle = \frac{1}{\sqrt{|G|}} \sum_{z \in G} |z\rangle |f(xz)\rangle$

to compute: $|xf\rangle = \frac{1}{\sqrt{|G|}} \sum_{z \in G} \left|x^{-1}z\right\rangle |f(z)\rangle$

If the level sets of f are the left cosets of H then

the states $|xf\rangle$ are pairwise orthogonal/identical

"quantum version" of the Stabilizer problem:

Ω is an orthonormal system in a Hilbert space
action of G on Ω by oracle
input: by oracle or as a stream of copies of $|\omega\rangle$ (or $|\omega_1, \omega_2\rangle$)

$\approx$ the same problems

quantum versions of HSP and Stabilizer are equivalent

by the reductions, can use the term Stabilizer or the term HSP for all of these problems

Discrete log as an abelian HSP

does not follow the $\wr/\rtimes$ approach

group $G = \mathbb{Z}_N \times \mathbb{Z}_N$, (not $\mathbb{Z}_N^* \times \mathbb{Z}_N^*$!)

$$f(x, y) = (a^x)(b^y)^{-1}$$

First steps in typical HSP algorithms

H = hidden subgroup

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle|0\rangle$$
$$\downarrow$$
$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle|f(x)\rangle$$
$$\downarrow \text{ measure } f(x) \qquad \text{(not necessary, simplifies presentation)}$$
$$\frac{1}{\sqrt{|H|}} \sum_{x \in H} |ax\rangle$$

"random" level set (= coset) superposition

First steps II.

$\frac{1}{\sqrt{|H|}} \sum_{x \in H} |ax\rangle$ "random" coset superposition

without measurement: mixture of the coset superpositions

(name: subgroup state)

Most HSP algorithms work with a stream of subgroup states as input

$\sim$ a generalization of Stabilizer:

input: stream

$|\omega_1\rangle, |\omega_2\rangle, |\omega_3\rangle \ldots$ with $G_{\omega_i} = H$

Query complexity even of this is poly

(Ettinger, Hoyer,Knill 2004)

Orbit superposition

$$|G\omega\rangle = \frac{1}{\sqrt{|G|}} \sum_{x\in G} |x\omega\rangle = \frac{1}{\sqrt{|G\omega|}} \sum_{\omega'\in G\omega} |\omega'\rangle$$

Why is it useful:

$K \lhd G$, G/K acts on $\{|K\omega\rangle : |\omega\rangle \in \Omega\}$

recursion to G/K computes $G_{K\omega_1 \to K\omega_2}$

Inside this, finding $G_{\omega_1\to\omega_2} \prec$ finding $K_{\omega_1\to\omega_2'}$

Orbit superposition and transportation I

Friedl, I, Magniez, Santha, Sen 2003, 2014

What we would like:

$$|G\omega\rangle = \frac{1}{\sqrt{|G\omega|}} \sum_{\omega' \in G\omega} |\omega'\rangle$$

What we can compute:

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle|x\omega\rangle = \frac{1}{\sqrt{|G\omega|}} \sum_{\omega' \in G\omega} |G_{\omega \to \omega'}\rangle|\omega'\rangle$$

$|\omega'\rangle$ is entangled with $|G_{\omega \to \omega'}\rangle$

Need to "reverse-compute" $|G_{\omega \to \omega'}\rangle$:

inverse of solving the transportation problem

Orbit superposition and transportation II.

Issue: to compute $|G_{\omega\to\omega'}\rangle$, need many copies of $|\omega\rangle$ and $|\omega'\rangle$
Workaround: action on $\Omega^{(r)} = \{|\omega\rangle^{\otimes r} : |\omega\rangle \in \Omega\}$
(r sufficiently large)

Assume G solvable. $G \rhd G' \rhd G'' \rhd \ldots \rhd 1$
length $O(\log\log|G|)$ (Glasby 1989)
Recursion along this, using the Shor-Kitaev HSP, and Kuperberg's shift algorithms in the abelian factors $\longrightarrow$ time

$$\exp(O(\sqrt{\log|G|}\log\log|G|)).$$

Orbit superposition and transportation III.

Friedl, I, Magniez, Santha, Sen 2003

For $O(1)$-step solvable groups G of exponent $O(1)$,

a poly time shift algorithm in factors $\mathbb{Z}_p^n$

(for $p = O(1)$, prime)

$\downarrow$

poly time Stabilizer in G

Remark: the orbit superposition approach does not work

with subgroup states as input!

Abelian shift/transportation

From now on, omit normalizing factors and use measurements

Interesting case: A regularly acts on Ω, $\omega_2 = s\omega_1$, find s.
On $A \times \{0,1\}$, $\quad |f(x,t)\rangle = |x\omega_{2-t}\rangle$.

Level set superpositions:

$$|x\rangle|0\rangle + |x+s\rangle|1\rangle$$

Apply Fourier transform of A, measure character, obtain

$$|0\rangle + \chi(s)|1\rangle$$

Shift in $A = \mathbb{Z}_p^n$

Friedl, I, Magniez, Santha, Sen 2003

Measure $|0\rangle + \chi(s)|1\rangle$ in the (Hadamard) basis $(|0\rangle + |1\rangle, |0\rangle - |1\rangle)$.

If we get $|0\rangle - |1\rangle$, then $\chi(s) \neq 1$.

Use $A \cong A^*$: $\chi(x) = \omega^{(u,x)}$ for some $u \in \mathbb{Z}_p^n$ $\quad (\omega = \sqrt[p]{1})$

Get (essentially) uniformly random u with $(u, s) \neq 0$

$(u, s)^{p-1} - 1$ polynomial in u

$O(p\binom{n+p-2}{p-1})$ "random" zeros determine the coeffs $\rightarrow s$.

Problem: Hyperplane cover

Decision version of finding s

search reducible to $O(n(p+1))$ instances

Problem: given hyperplanes in $\mathbb{Z}_p^n$, do they cover the space?

NP-complete

Average case relaxation: what is the smallest $M = M(p, n)$ s.t.

M random hyperplanes cover $\mathbb{Z}_p^n$ in a way

provable in time poly(n, M)

$O(np \log p)$ sufficient to cover with good probability

Open: Are $(np)^{O(1)}$ sufficient to efficiently provably cover?

Multiple shift in $\mathbb{Z}_p^n$

Assume that the level sets of f on $\mathbb{Z}_p^n \times M$ are

$$\{u + t \cdot s : t \in M\} \qquad M \subseteq \{0, \ldots, p\}$$

Childs, van Dam 2007:

poly time for $n = 1$, $M = \{0, \ldots, k\}$ $p = k^{O(1)}$

I, Prakash, Santha 2018; Chen, Liu, Zhandry 2021

generalizations of Friedl et al 2003 work in poly time

when $p - |M| = O(1)$.

Open question: for $k = p/O(1)$, large n?

Stabilizer/HSP in nilpotent groups

$[G, [G, [\dots, G]]] = 1$ (c brackets), $c =$nilpotency class

For constant class, the interesting case

G p-group of exponent p, $|H| = p$ (p prime)

$$\text{Example: } G = \left\{ \begin{pmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{pmatrix} \right\} \; ([G, [G, G]] = 1, \text{ class } 2)$$

Manipulating representations in class 2

$G' = [G, G] \leq Z(G)$, exponent p

I, Sanselme, Santha 2007-8

Idea comes from Clifford theory of representations

Also has an "elementary" version

G has automorphisms σ_k $(k = 1, \ldots, p-1)$

σ_k raises to the kth power modulo G'

to the k^2th power in G'

can be used to change reps

while HG' remains the same

The elementary approach

Goal: from $|cH\rangle$, would like to make $|cG'H\rangle$

from several states $|c_iG'H\rangle$, compute $G'H$

using the abelian HSP algorithm

find H in $G'H$

$$|G'\rangle|cH\rangle = \sum_{z\in G'}\sum_{y\in H}|z\rangle|cy\rangle$$

$\downarrow$ (multiplication)

$$\sum_{z\in G'}\sum_{y\in H}|z\rangle|czy\rangle$$

$\downarrow$ (Fourier of G', measure character)

$$\sum_{z\in G'}\sum_{y\in H}\chi(z)|czy\rangle$$

would like $\chi(z) = 1$ for all $z \in G'$

Canceling out

$\sum_{z\in G'}\sum_{y\in H}\chi(z)|czy\rangle$
is an eigenstate for multiplication by $a\in G'$:

$$\sum_{z\in G'}\sum_{y\in H}\chi(z)|aczy\rangle = \chi^{-1}(a)\sum_{z\in G'}\sum_{y\in H}\chi(z)|czy\rangle$$

Make several copies:

$$\bigotimes_{i=1}^m \sum_{z_i\in G'}\sum_{y_i\in H}\chi_i(z_i)|c_iz_iy_i\rangle =: |\Psi\rangle$$

Choose appropriate $k_1,\ldots,k_m$,
define action of G on $|\Psi\rangle$:

$$|x\cdot\Psi\rangle := \bigotimes_{i=1}^m \sum_{z_i\in G'}\sum_{y_i\in H}\chi_i(z_i)|c_iz_iy_i\sigma_{k_i}(x)\rangle$$

Canceling out II.

$$|x \cdot \Psi\rangle = \bigotimes_{i=1}^{m} \sum_{z_i \in G'} \sum_{y_i \in H} \chi_i(z_i) |c_i z_i y_i \sigma_{k_i}(x)\rangle$$

For $a \in G'$

$$|a \cdot \Psi\rangle = \prod \chi_i^{-k_i^2}(a) |\Psi\rangle$$

If $\prod \chi_i^{k_i^2} = 1$ then

$$|a \cdot \Psi\rangle = \Psi$$

Also, for $x \notin G'H$

$$|x \cdot \Psi\rangle \perp |\Psi\rangle.$$

Equations for canceling out

Condition $\prod \chi_i^{k_i^2} = 1$ in G':

$n = \mathrm{rk} G'$ homogeneous linear equations in k_i^2

These + n homogeneous linear eqs in k_i also ensure

$$|x\Psi\rangle = |\Psi\rangle \text{ for } x \in G'H$$

If not all k_i are zero

$$|x\Psi\rangle \perp |\Psi\rangle \text{ for } x \notin G'H$$

For $m = O(n^3)$ we can find a nontrivial solution in poly time

(Chevalley-Warning: existence for $m > 3n$)

HSP in $\mathbb{Z}_p^n \rtimes \mathbb{Z}_p$

Decker, Hoyer, I., Santha 2014; I., Santha 2015

$V = \mathbb{Z}_p^n$, $G = V \rtimes \mathbb{Z}_p$

fix $y \in G \setminus V$, conjugation on V by y:

$I + N$, $N^d = 0$ $\quad$ (d=nilp. class of G, $d \leq p$)

$H = \langle vy \rangle$ $(v \in V)$

$(vy)^t = v(t)y^t \qquad v(t) \in \mathbb{F}[t]^n$, degree d

HSP in $\mathbb{Z}_p^n \rtimes \mathbb{Z}_p$ II.

$\sum_t |w + v(t)\rangle|t\rangle$ coset superposition

$\downarrow$ Fourier of V, measure character

$\sum_t \chi(w + v(t))|t\rangle$

$\chi(w + v(t)) = \omega^{(u, w+v(t))}$ for some $u \in V$

repeat m times, add $|Z_p\rangle = \sum_t |t\rangle$ in a new register

$$\sum_{t_1,\ldots,t_m,t} \omega^{(\sum_i u_i, w_i + v(t_i))}|t_1, \ldots, t_m\rangle|t\rangle$$

$\downarrow$ find δ_i (not all zero) s.t. $\sum \delta_i^d u_i = 0$, subtract $\delta_i t$ from t_i

$$\sum_t \sum_{t_1,\ldots,t_m} \omega^{(\sum_i u_i, w_i + v(t_i + \delta_i t))}|t_1, \ldots, t_m\rangle|t\rangle$$

$(\sum_i u_i, w_i + v(t_i + \delta_i t))$ will have degree $d - 1$ in t

measure $t_1, \ldots, t_m$

HSP in $\mathbb{Z}_p^n \rtimes \mathbb{Z}_p$ III.

collect m' copies, let the degree $d-1$-parts cancel out each other,

... repeat until we get

$$\sum_t \omega^{\ell(t)}|t\rangle$$

with *linear* $\ell(t)$

Fourier gives the degree 1 coefficient of $\ell(t)$

This coefficient is a "random" linear combination of the coefficients of $v(t)$

Obtained a linear equation for those

Collect such equations until $v(t)$ gets determined

Equations for canceling out

$x_1^d v_1 + \ldots + x_m^d v_m = 0 \qquad (v_1, \ldots, v_m \in \mathbb{Z}_p^n \text{ random})$

need a nontrivial solution $\quad (d|p-1$ can be assumed$)$

Chevalley-Warning: existence for $m > dn$

"Polynomial-time effective version":

For how large m can be found in time poly$(nm \log p)$?

I., Santha 2015: poly time algorithm for $m = d^{\Omega(d^2 \log d)}(n+1)^{\Omega(d \log d)}$

Open: Is there something closer to dn?

In the special case $d = p - 1$?

("poly-time effective Davenport-constant"?)

Main problems

Hyperplane cover:

$H_1, \ldots, H_m$ random hyperplanes in $\mathbb{Z}_p^n$

How large sample size m needed to find efficiently an evidence witnessing that $\mathbb{Z}_p^n$ is covered

would like $m = (n+p)^{O(1)}$ but have $(n+p)^{O(p)}$

Systems of diagonal equations/an effective Chevalley-Warning-type problem:

$x_1^d v_1 \ldots, x_m^d v_m = 0$ ($v_i \in \mathbb{F}_p^n$ random)

How large should m be to efficiently find a nontrivial solution?

existence for $m > nd$ (Chevalley-Warning)

would like $m = (nd)^{O(1)}$ but have $m = (nd)^{O(d^2 \log d)}$

Imran, I. (ongoing): slight improvement for certain d

can the "average-case" situation be exploited?

Special case $d = p - 1$: zero sum subset (Alt. proof: Olson)