The Hidden Subgroup Problem for Universal Algebras

Matthew Moore*, Taylor Walenczyk

The University of Kansas
Department of Electrical Engineering and Computer Science

July 8 – 11, 2020
1 Quantum Computation

2 Hidden Subgroups, Hidden Kernels

3 The Hidden Kernel Problem for Post’s Lattice
Compared to classical computers, quantum computers are
- based on a different model of computation,
- very hard/maybe impossible to build,
- very hard to program and reason about.

Classical computers are
- based on well-studied model of computation,
- cheap/easy to build,
- “easy” to program and reason about,
- fast (approx. exponential growth in speed).

Why bother?
Physical constraints: we will probably never have

- clock speeds faster than the electron transition frequency ($\approx 10^{15}$ Hz),
- components smaller than the diameter of a hydrogen atom ($\approx 10^{-8}$ cm).

**Classical computers will always struggle with exponential complexity.**

**Idea:** exploit natural phenomena to aid in computation.

- Quantum phenomena are hard to exploit...

How about using classical phenomena? Maybe use an analog co-processor?

- Classical phenomena can be simulated in polynomial time and space.
- Speedup will be at most polynomial.
- Classical physics is too “easy” to be useful.
Consider a quantum system of $n$ particles with spins 0 or 1.

- Each particle is modelled by vector space $\mathcal{B} = \mathbb{C}\text{-span}\{|0\rangle, |1\rangle\}$.
- Total system is modelled by $2^n$-dimensional vector space,
  \[\mathcal{B}^\otimes n = \mathbb{C}\text{-span}\{ |s_1 \cdots s_k\rangle \mid s_i \in \{0, 1\} \}.\]
- Possible states of the system are norm 1 vectors,
  \[\sum_{s_1,\ldots,s_n \in \{0,1\}} \lambda_{s_1\ldots s_n} |s_1 \cdots s_n\rangle = |\alpha\rangle.\]
- Probability of observing $|t_1 \cdots t_n\rangle$ when $|\alpha\rangle$ is measured $= |\lambda_{t_1\ldots t_n}|^2$.
- Evolution over time is determined by action of $2^n \times 2^n$ unitary matrices.

Quantum systems represent exponentially difficult computational problems, in contrast to “easy” classical systems.
Hidden Subgroups, Hidden Kernels
Let $G$ be a group, $X$ a set, and $f : G \rightarrow X$ a function.

$f$ hides a subgroup $D \leq G$ if $f$ is constant precisely on $D$-cosets.

\[ f(a) = f(b) \quad \iff \quad aD = bD \]

The Hidden Subgroup Problem (HSP)

Input: $G$, $f : G \rightarrow X$ hiding some subgroup as a blackbox

Output: the subgroup $D$ that $f$ hides (as generators)

Considerations

- Input size is $\lg(|G|)$.
- $D$ must be specified with $\text{poly}(\lg(|G|))$ information.
- Clearly in $O(|G|) = O(2^{\lg(|G|)})$.
- Two kinds of complexity: circuit size, evaluations of $f$. 
The Hidden Subgroup Problem (HSP)

Input: \( G, f : G \to X \) hiding some subgroup (as a blackbox):
\[
[f(a) = f(b) \iff aD = bD]
\]

Output: the subgroup \( D \) that \( f \) hides (as generators)

Many famous problems are special cases of the HSP.

<table>
<thead>
<tr>
<th>Problem</th>
<th>( G )</th>
<th>Classical</th>
<th>Quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simon’s problem</td>
<td>( \mathbb{Z}_2^n )</td>
<td>( \Omega(2^n) )</td>
<td>( \mathcal{O}(n^2) )</td>
</tr>
<tr>
<td>Factoring</td>
<td>( \mathbb{Z} )</td>
<td>( \mathcal{O}(2^K \lg(n)^{1/3} \lg \lg(n)^{2/3}) )</td>
<td>( \mathcal{O}(n^3) )</td>
</tr>
<tr>
<td>Discrete log</td>
<td>( \mathbb{Z} \times \mathbb{Z} )</td>
<td>( \mathcal{O}(2^K \lg(n)^{1/3} \lg \lg(n)^{2/3}) )</td>
<td>( \mathcal{O}(n^3) )</td>
</tr>
<tr>
<td>Graph isomorphism</td>
<td>( S_n )</td>
<td>( \mathcal{O}(2^{\lg(n)^K}) )</td>
<td></td>
</tr>
<tr>
<td>Shortest vector</td>
<td>( D_n )</td>
<td>( \mathcal{O}(2^{Kn}) )</td>
<td>sub-exp</td>
</tr>
</tbody>
</table>

Polynomial-time quantum algorithms are known for

- abelian groups (Simon, Shor, Kitaev, et al),
- an irregular constellation of other groups.
Questions

- What makes abelian groups special?
- Can “hiding” a subgroup be made more natural?

Algebras

- An algebra is a set $A$ together with operations $f_i : A^{n_i} \to A$ for $i \in I$. Written $\mathbb{A} = \langle A; \{f_i\}_{i \in I} \rangle$.

- Subalgebras don’t form a meaningful partition of $A$, it’s not clear how to define “hiding” a subalgebra.

- A congruence of $\mathbb{A}$ is a compatible equivalence relation. Equivalently, a congruence is the kernel of a homomorphism $\varphi : \mathbb{A} \to \mathbb{B}$.

- How does $f : A \to X$ hide a congruence $\theta$ of $\mathbb{A}$?
Hidden Kernel Problem (v1)

Input: $A, f: A \to X$ hiding some congruence (as a blackbox)
Output: the congruence $\theta$ of $A$ that $f$ hides (as generators)

For $f: A \to X$, we say that $f$ hides congruence $\theta$ of $A$ if

$$f(a) = f(b) \iff a \theta b.$$

This allows us to impose algebraic structure on $X$: $A/\theta$.

$f$ is actually a homomorphism with kernel $\theta$!

Hidden Kernel Problem

Input: algebras $A, B$, homomorphism $\varphi: A \to B$ (as a blackbox)
Output: generators of $\ker(\varphi)$
The Hidden Kernel Problem for Post’s Lattice
Hidden Kernel Problem

Input: homomorphism
\[ \varphi : A \rightarrow B \]
Output: \( \ker(\varphi) \) (generators)

Simon’s algorithm solves this for \( A = (\mathbb{Z}_2)^n \).

How about if \( A = B^n \), where \( B \) is a 2-element algebra?

How many such \( B \) are there?
Theorem

There exists / doesn’t exist a poly-time quantum solution for HKP($\mathbb{B}^n$), where

<table>
<thead>
<tr>
<th>$\mathbb{B}$</th>
<th>$\text{Ops on } {0, 1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{A}P_0$</td>
<td>$x + y$ (<em>known</em>)</td>
</tr>
<tr>
<td>$\mathcal{MPT}_0^\infty$</td>
<td>$x \land (y \lor z)$</td>
</tr>
<tr>
<td>$\mathcal{MPT}_1^\infty$</td>
<td>$x \lor (y \land z)$</td>
</tr>
<tr>
<td>$\mathcal{A}P$</td>
<td>$x + y + z$</td>
</tr>
<tr>
<td>$\mathcal{D}M$</td>
<td>$\text{maj}(x, y, z)$</td>
</tr>
<tr>
<td>$\land$</td>
<td>$x \land y, 0, 1$</td>
</tr>
<tr>
<td>$\lor$</td>
<td>$x \lor y, 0, 1$</td>
</tr>
<tr>
<td>$\forall$</td>
<td>$\neg x, 0$</td>
</tr>
</tbody>
</table>

Observations

- *exists* is inherited up,
- *doesn’t exist* is inherited down.
Theorem

There **exists** / **doesn’t exist** a poly-time **classical** solution for $HKP(B^n)$, where

<table>
<thead>
<tr>
<th>$B$</th>
<th>$Ops$ on ${0, 1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{MPT}_0^\infty$</td>
<td>$x \land (y \lor z)$</td>
</tr>
<tr>
<td>$\mathcal{MPT}_1^\infty$</td>
<td>$x \lor (y \land z)$</td>
</tr>
<tr>
<td>$DM$</td>
<td>$\text{maj}(x, y, z)$</td>
</tr>
<tr>
<td>$A$</td>
<td>$x \leftrightarrow y, 0$</td>
</tr>
<tr>
<td>$\land$</td>
<td>$x \land y, 0, 1$</td>
</tr>
<tr>
<td>$\lor$</td>
<td>$x \lor y, 0, 1$</td>
</tr>
<tr>
<td>$U$</td>
<td>$\neg x, 0$</td>
</tr>
</tbody>
</table>

Observations

- **exists** is inherited up,
- **doesn’t exist** is inherited down.
Quantum

Classical

$\mathcal{AP}_0 \approx \mathbb{Z}_2$

$\mathcal{MPT}_0^\infty$

$\lor$

$\land$

$\mathcal{DM}$

$\mathcal{AP}$

$\mathcal{MPT}_1^\infty$

$\mathcal{U}$

$\lor$

$\land$
The Hidden Subgroup Problem for Universal Algebras

**Theorem**

Let $\mathbb{B}$ be a 2-element algebra and consider $HKP(\mathbb{B}^n)$.

- If $\mathcal{MPT}_0^\infty$, $\mathcal{MPT}_1^\infty$, or $\mathcal{DM}$ is contained in $\mathbb{B}$ then classical and quantum poly-time solutions exist.

- If $\mathcal{AP} \preceq \mathbb{B} \preceq \mathcal{A}$ then a quantum poly-time solution exists while no classical poly-time one does.

- If $\mathbb{B}$ is contained in $\wedge$, $\vee$, or $\mathcal{U}$, then no poly-time quantum or classical solutions exist.

Thank you for your attention.