The Hidden Subgroup Problem for Universal Algebras

Matthew Moore

The University of Kansas
Department of Electrical Engineering and Computer Science

October 17, 2019

Quantum Computation

Compared to classical computers, quantum computers are

- based on a different model of computation,
- very hard/maybe impossible to build at scale,
- 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).

Even in the distant future, classical computers will continue to struggle with problems of 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 $\mathfrak{B} = \mathbb{C}\text{-span}\{|0\rangle, |1\rangle\}$.
- Total system is modelled by 2^n-dimensional vector space,

$$\mathfrak{B}^{\otimes n} = \mathbb{C}\text{-span}\left\{ |s_1 \cdots s_n\rangle \mid s_i \in \{0,1\} \right\}.$$

- Possible states of the system are norm 1 vectors,

$$\sum_{s_1,\dots,s_n \in \{0,1\}} \lambda_{s_1 \cdots s_n} |s_1 \cdots s_n\rangle = |\alpha\rangle .$$

- Probability of observing $|t_1 \cdots t_n\rangle$ when $|\alpha\rangle$ is measured $= |\lambda_{t_1 \cdots t_n}|^2$.
- Evolution over time is determined by action of $2^n \times 2^n$ unitary matrices.

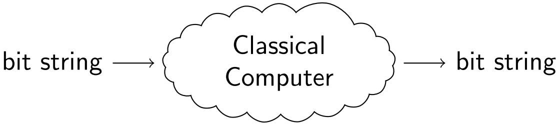
Quantum systems represent exponentially difficult computational problems, in contrast to "easy" classical systems.

Qubits

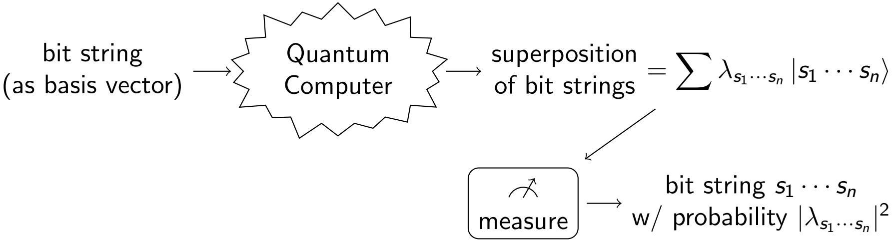
- Qubits are what a quantum computer operates on.
- single qubit $\approx$ basis vector of $\mathfrak{B} := \mathbb{C}\text{-span}\{|0\rangle, |1\rangle\} \approx |s\rangle$, $s \in \{0,1\}$
- multiple qubits $\approx$ basis vectors of $\mathfrak{B}^{\otimes n} \approx |s_1 \cdots s_n\rangle$ for $s_i \in \{0,1\}$
- quantum state $\approx$ norm 1 element of $\mathfrak{B}^{\otimes n} \approx |\alpha\rangle = \sum \lambda_{s_1 \cdots s_n} |s_1 \cdots s_n\rangle$
- probability of observing state $|s_1 \cdots s_n\rangle \approx |\lambda_{s_1 \cdots s_n}|^2 \approx |\langle \alpha \mid s_1 \cdots s_n \rangle|^2$
- evolution of $|\alpha\rangle$ over time $\approx U|\alpha\rangle$, U a unitary matrix

Conventions

- $|s\rangle$ is a vertical vector, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- $\langle s| := |s\rangle^*$ (conjugate transpose) is a horizontal vector
- $\langle s| \, |t\rangle =: \langle s \mid t \rangle$ is the inner product
- $|s\rangle \otimes |t\rangle =: |st\rangle$ or $|s, t\rangle$
- U unitary $\Leftrightarrow$ U preserves inner product $\Leftrightarrow$ $U^{-1} = U^*$

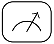


- deterministic: equal inputs give equal outputs
- need not be reversible
- represented by a boolean circuit (for fixed length input)



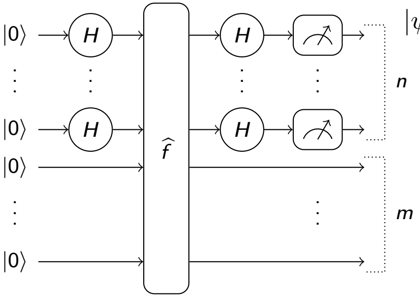
- probabilistic, likely need to run multiple times
- must be reversible (before measurement)
- represented by a quantum circuit (for fixed length input)

A quantum circuit consists of

- gates (unitary transformations), H , σ_x , . . .
- measurement operations. 

Every unitary transf. can be built using gates from the standard gate set.

Circuits are specified graphically or given inline.

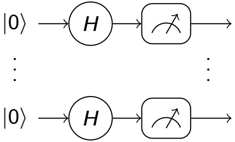


$$|\psi\rangle = (H^{\otimes n} \otimes I_m)\ \widehat{f}\ (H^{\otimes n} \otimes I_m)\ (|0^n\rangle \otimes |0^m\rangle)$$

The complexity of a circuit is the number of gates.

Measurement of a subset of qubits is the partial trace of the density matrix, $\mathrm{Tr}_n(|\psi\rangle\langle\psi|)$.

The H gate is the Hadamard operator, $H\,|q\rangle = \frac{1}{\sqrt{2}}\Big(\,|0\rangle + (-1)^q\,|1\rangle\,\Big)$.



Pre-measurement outcome:

$$\big(H\,|0\rangle\,\big)^{\otimes n} = \left(\frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\right)^{\otimes n}$$
$$= \frac{1}{2^{n/2}} \sum_{x_1,\dots x_n \in \{0,1\}} |x_1 \cdots x_n\rangle\,.$$

This is the uniform distribution!

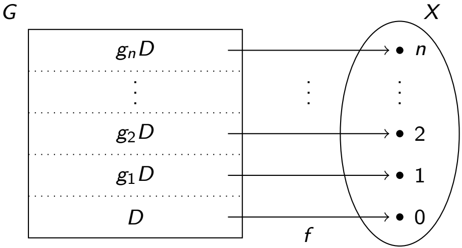
The circuit generates perfect n-bit random numbers.

Hidden Subgroups, Hidden Kernels

Let $\mathbb{G}$ be a group, X a set, and $f : G \to X$ a function.

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

$$f(a) = f(b) \iff aD = bD$$



The Hidden Subgroup Problem (HSP)

`Input:` $\mathbb{G}$, $f : G \to X$ hiding some subgroup **as a blackbox**

`Output:` the subgroup $\mathbb{D}$ that f hides (as generators)

Considerations

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

The Hidden Subgroup Problem (HSP)

`Input:` $\mathbb{G}$, $f : G \to X$ hiding some subgroup (as a blackbox):
$\left[f(a) = f(b) \Leftrightarrow aD = bD\right]$

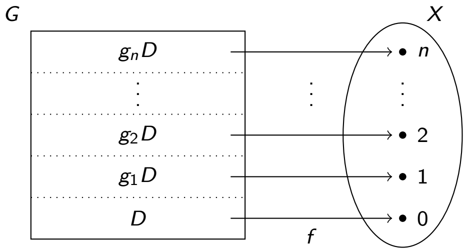
`Output:` the subgroup $\mathbb{D}$ that f hides (as generators)

Many famous problems are special cases of the HSP.

Problem	$\mathbb{G}$	Classical	Quantum
Simon's problem	$\mathbb{Z}_2^n$	$\Omega(2^n)$	$\mathcal{O}(n^2)$
Factoring	$\mathbb{Z}$	$\mathcal{O}(2^{K \lg(n)^{1/3} \lg\lg(n)^{2/3}})$	$\mathcal{O}(n^3)$
Discrete log	$\mathbb{Z} \times \mathbb{Z}$	$\mathcal{O}(2^{K \lg(n)^{1/3} \lg\lg(n)^{2/3}})$	$\mathcal{O}(n^3)$
Shortest vector	$\mathbb{D}_n$	$\mathcal{O}(2^{Kn})$	$\approx \mathcal{O}(8^{\sqrt{n}})$
Graph isomorphism	$\mathbb{S}_n$	$\mathcal{O}(2^{\lg(n)^K})$	

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 θ of $\mathbb{A}$?

Hidden Kernel Problem (v1)

`Input`: $\mathbb{A}$, $f : A \to X$ hiding some congruence (as a blackbox)

`Output`: the congruence θ of $\mathbb{A}$ that f hides (as generators)

For $f : A \to X$, we say that f hides congruence θ of $\mathbb{A}$ if

$$f(a) = f(b) \qquad \Longleftrightarrow \qquad a \;\theta\; b.$$

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

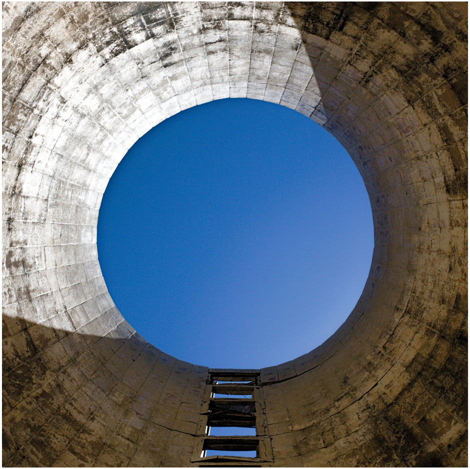
f is actually a homomorphism with kernel θ!

Hidden Kernel Problem

`Input`: algebras $\mathbb{A}$, $\mathbb{B}$, homomorphism $\varphi : \mathbb{A} \to \mathbb{B}$ (as a blackbox)

`Output`: generators of $\ker(\varphi)$

The Hidden Kernel Problem for Post's Lattice



Hidden Kernel Problem

`Input`: homomorphism

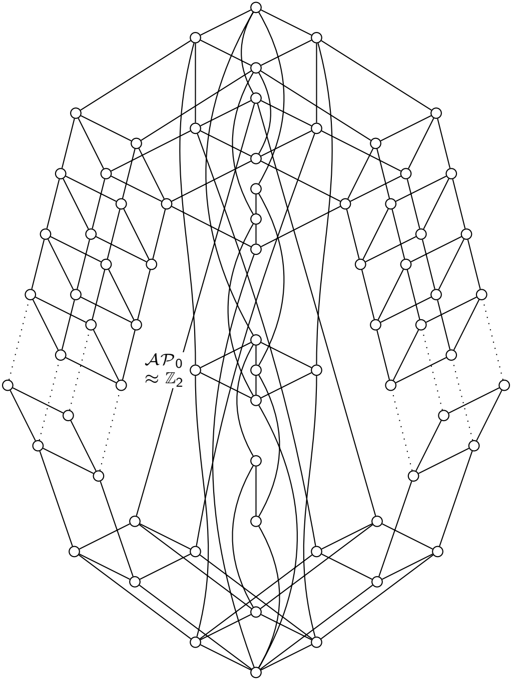
$\varphi : \mathbb{A} \to \mathbb{B}$

`Output`: $\ker(\varphi)$ (generators)

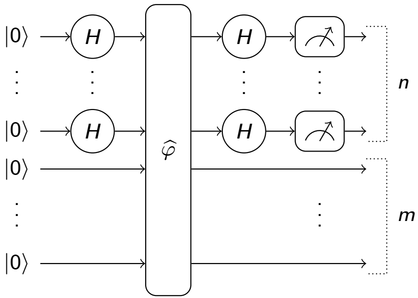
Simon's algorithm solves this for $\mathbb{A} = (\mathbb{Z}_2)^n$.

How about if $\mathbb{A} = \mathbb{B}^n$, where $\mathbb{B}$ is a 2-element algebra?

How many such $\mathbb{B}$ are there?



Define quantum circuit $\mathcal{S}$ =



Consider an instance of the HKP:

- $\mathbb{B}$ a 2-element algebra,
- $\mathbb{A} = \mathbb{B}^n$, $\mathbb{D} = \mathbb{B}^m$,
- homomorphism $\varphi : \mathbb{A} \to \mathbb{D}$.

The $\widehat{\varphi}$ gate

- Define $\varphi_\oplus : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ by $\varphi_\oplus(x, y) = (x, y + f(x))$.
- Define unitary transformation $\widehat{\varphi}$ by $\widehat{\varphi}\,|x, y\rangle = |x, y + \varphi(x)\rangle$.

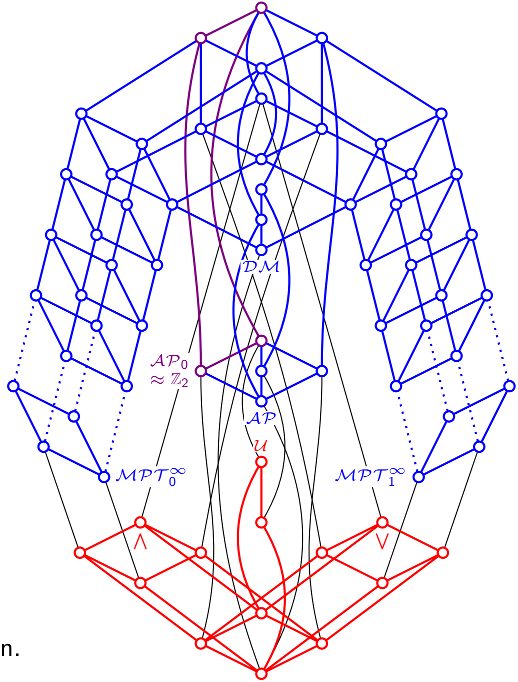
What does it mean for $\mathcal{S}$ to solve this problem?

- Output is probabilistic.
- Must run $\mathcal{S}$ multiple times, collecting the output.
- Overall complexity is (size of $\mathcal{S}$)·(number of runs).

Theorem

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

$\mathbb{B}$	*Ops on* $\{0,1\}$
$\mathcal{AP}_0$	$x + y$ (**known**)
$\mathcal{MPT}_0^\infty$	$x \wedge (y \vee z)$
$\mathcal{MPT}_1^\infty$	$x \vee (y \wedge z)$
$\mathcal{AP}$	$x + y + z$
$\mathcal{DM}$	$\mathrm{maj}(x, y, z)$
$\bigwedge$	$x \wedge y$, 0, 1
$\bigvee$	$x \vee y$, 0, 1
$\mathcal{U}$	$\neg x$, 0



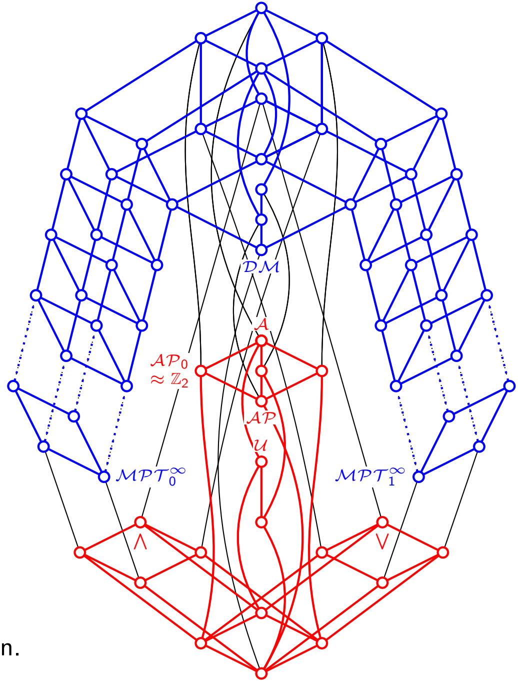
Observations

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

Theorem

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

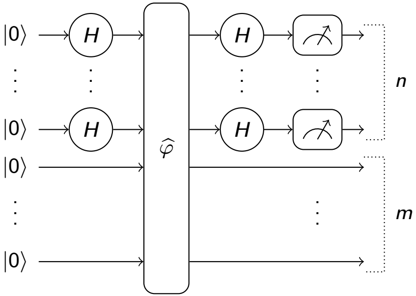
$\mathbb{B}$	*Ops on* $\{0,1\}$
$\mathcal{MPT}_0^\infty$	$x \wedge (y \vee z)$
$\mathcal{MPT}_1^\infty$	$x \vee (y \wedge z)$
$\mathcal{DM}$	$\mathrm{maj}(x,y,z)$
$\mathcal{A}$	$x \leftrightarrow y$, 0
$\bigwedge$	$x \wedge y$, 0, 1
$\bigvee$	$x \vee y$, 0, 1



Observations

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

How does $\mathcal{S}$ work?



$$(H^{\otimes n} \otimes I_m)\ \widehat{\varphi} \left[\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0^m\rangle \right]$$

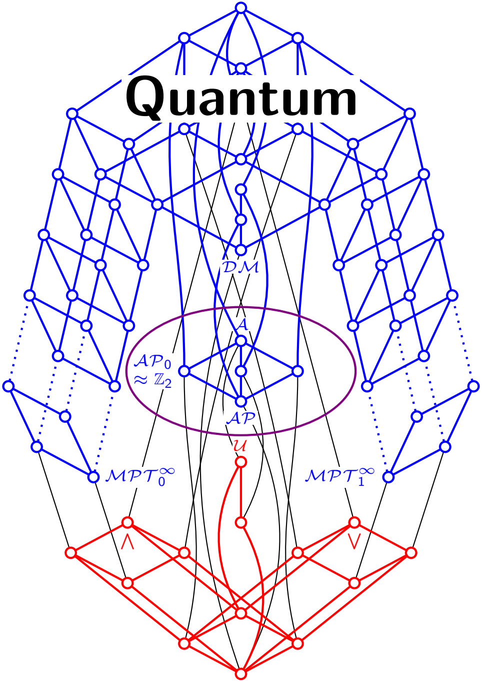
$$= \frac{1}{2^{n/2}} (H^{\otimes n} \otimes I_m) \sum_{x \in \{0,1\}^n} |x\rangle \otimes |\varphi(x)\rangle$$

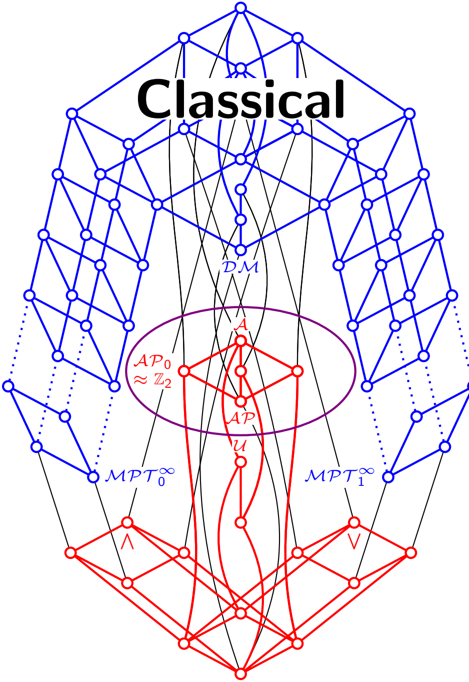
$$= \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} H^{\otimes n} |x\rangle \otimes |\varphi(x)\rangle$$

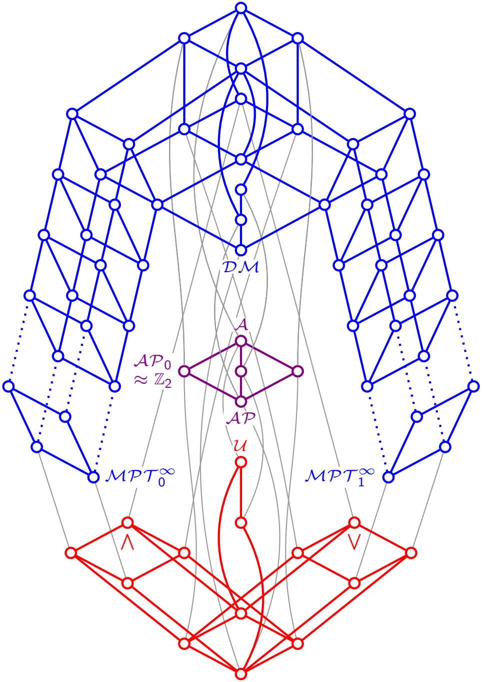
$$= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \otimes |\varphi(x)\rangle$$

Notes

- $H|q\rangle = \frac{1}{\sqrt{2}} \Big(|0\rangle + (-1)^q |1\rangle \Big) = \frac{1}{\sqrt{2}} \sum_{p \in \{0,1\}} (-1)^{pq} |p\rangle$
- $H^{-1} = H^* = H$
- $\varphi : \{0,1\}^n \to \{0,1\}^m$ defines gate $\widehat{\varphi}$, $\quad \widehat{\varphi}|x, y\rangle = |x, y + \varphi(x)\rangle$


Quantum
$\mathcal{DM}$
$\mathcal{A}$
$\mathcal{AP}_0$
$\approx \mathbb{Z}_2$
$\mathcal{AP}$
$\mathcal{U}$
$\mathcal{MPT}_0^\infty$
$\mathcal{MPT}_1^\infty$
$\wedge$
$\vee$


Classical
$\mathcal{DM}$
$\mathcal{A}$
$\mathcal{AP}_0$
$\approx \mathbb{Z}_2$
$\mathcal{AP}$
$\mathcal{U}$
$\mathcal{MPT}_0^\infty$
$\mathcal{MPT}_1^\infty$
$\wedge$
$\vee$



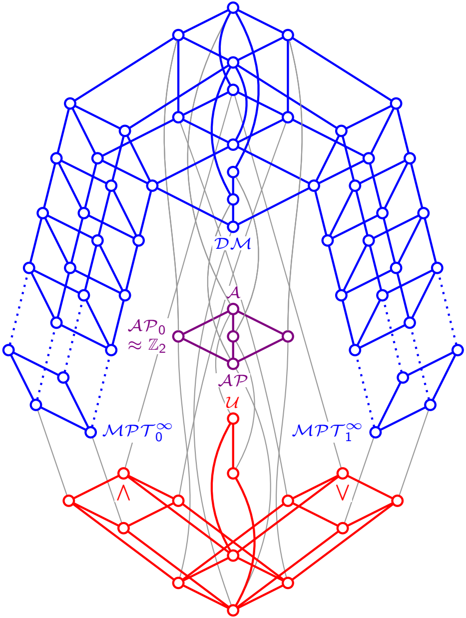
$\mathcal{DM}$
$\mathcal{A}$
$\mathcal{AP}_0$
$\approx \mathbb{Z}_2$
$\mathcal{AP}$
$\mathcal{U}$
$\mathcal{MPT}_0^\infty$
$\mathcal{MPT}_1^\infty$
$\wedge$
$\vee$

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 $\bigwedge$, $\bigvee$, or $\mathcal{U}$, then no poly-time quantum or classical solutions exist.*



Thank you for your attention.