The Hidden Subgroup Problem for Universal Algebras

Matthew Moore
The University of Kansas
matthew.moore@ku.edu

Taylor Walenczyk
The University of Kansas
tawalenczyk@ku.edu

Abstract

The Hidden Subgroup Problem (HSP) is a computational problem which includes as special cases integer factorization, the discrete logarithm problem, graph isomorphism, and the shortest vector problem. The celebrated polynomial-time quantum algorithms for factorization and the discrete logarithm are restricted versions of a generic polynomial-time quantum solution to the HSP for *abelian* groups, but despite focused research no polynomial-time solution for general groups has yet been found. We propose a generalization of the HSP to include *arbitrary* algebraic structures and analyze this new problem on powers of 2-element algebras. We prove a complete classification of every such power as quantum tractable (i.e. polynomial-time), classically tractable, quantum intractable, or classically intractable. In particular, we identify a class of algebras for which the generalized HSP exhibits super-polynomial speedup on a quantum computer compared to a classical one.

CCS Concepts: • **Theory of computation → Quantum query complexity**; **Finite Model Theory**; *Quantum complexity theory*; *Problems, reductions and completeness.*

Keywords: quantum computation, hidden subgroup problem, hidden kernel problem, universal algebra, clone theory

ACM Reference Format:
Matthew Moore and Taylor Walenczyk. 2020. The Hidden Subgroup Problem for Universal Algebras. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS '20), July 8–11, 2020, Saarbrücken, Germany*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3373718.3394764

1 Introduction

Quantum algorithms enable new methods of computation through the exploitation of the natural phenomena associated with quantum systems. Sometimes, this makes possible efficient (i.e. polynomial-time) solutions to computational problems for which no efficient classical algorithm exists. While there is no proof that quantum computation is super-polynomially faster than classical methods, there is a growing body of evidence in support of such a claim.

Perhaps the most famous quantum algorithm exhibiting super-polynomial speedup over classical ones is Shor's algorithm for integer factorization [18]. Other examples include Shor's solution to the discrete logarithm problem [18], Simon's algorithm [19], the unit and class group algorithms [6], and Pell's equation and the principal ideal algorithm [6] (see [15] for more details). Surprisingly, these superficially diverse problems are all special cases of a unifying problem called the *Hidden Subgroup Problem*.

Given a group $\mathbb{G}$, a set X, and a function $f : G \to X$, the function f *hides* a subgroup $\mathbb{D} \leq \mathbb{G}$ if $f(g) = f(h)$ if and only if $gD = hD$ (i.e. f is constant exactly on the cosets of $\mathbb{D}$ in $\mathbb{G}$). We follow the convention in Universal Algebra of distinguishing between an algebraic structure (e.g. a group) and its underlying set, using $\mathbb{G}$ for the former and G for the latter.

Hidden Subgroup Problem (HSP)

`Input:`	group $\mathbb{G}$,
	function $f : G \to X$ hiding some subgroup
`Task:`	determine the subgroup $\mathbb{D} \leq \mathbb{G}$ that f hides

The group $\mathbb{G}$ may be specified either by providing a multiplication table or by fixing a family $(\mathbb{G}_n)_{n\in\mathbb{N}}$ of groups (e.g. the symmetric groups $\mathbb{S}_n$) and providing an index n. Formally, these two kinds of specification will determine different input sizes to the problem. In any case, however, we *always* consider the input size to be $\lg |G|$. The function f is given as an oracle (i.e. a black-box function). Typically, $\mathbb{D}$ is 'determined' by generators, but any other scheme which uniquely identifies $\mathbb{D}$ amongst all other subgroups is permitted.

When $\mathbb{G}$ is *abelian*, HSP($\mathbb{G}$) includes all of the problems in the previous paragraph, and a general solution in this setting is due to Kitaev [11], though it includes many of the aforementioned previously known algorithms. The case for non-abelian $\mathbb{G}$ has proven to be more challenging.

The HSP for *non-abelian* $\mathbb{G}$ has been solved in some quite specific cases [1, 3, 5, 7–9, 14, 17], but it remains open in general. The HSP for the symmetric groups and the dihedral groups correspond to the *graph isomorphism* and *shortest*

LICS '20, July 8–11, 2020, Saarbrücken, Germany

ACM ISBN 978-1-4503-7104-9/20/07…$15.00
https://doi.org/10.1145/3373718.3394764

vector problems, respectively, and so these cases are of particular interest. Despite focused research over the years, no general polynomial-time quantum algorithm has been found.

We propose a generalization of the Hidden Subgroup Problem to arbitrary algebraic structures called *universal algebras*, and call the generalized problem the *Hidden Kernel Problem (HKP)*. Perhaps the simplest non-trivial instance of the HSP is when $\mathbb{G} = \mathbb{Z}_2^n$, and this is known as Simon's Problem. Along the same lines, we consider the Hidden Kernel Problem for powers of 2-element structures, and give a complete classification of which structures admit a polynomial-time quantum solution, a polynomial-time classical solution, no polynomial-time classical solution, and no polynomial-time quantum solution. In particular, we fully classify all powers of 2-element universal algebras for which a quantum algorithm achieves super-polynomial speedup when compared to a classical algorithm.

We begin with some necessary background in Universal Algebra and Clone theory, as well as a brief discussion of Quantum Computation in Section 2. In Section 3 we develop and state the Hidden Kernel Problem and outline the plan of attack for analyzing the HKP on powers of 2-element universal algebras (of which there are infinitely many). We determine which of these algebras admit polynomial-time quantum and classical solutions to their HKP in Section 4, and in Section 5 we determine which have an exponential lower-bound for classical or quantum solutions. Taken together, these results provide a complete classification of the quantum as well as classical computational complexity of the HKP on powers of 2-element universal algebras. Section 6 concludes with an overview of the results as well as a discussion of some open questions about the Hidden Kernel Problem.

2 Background

Universal Algebra seeks to include and extend classical algebraic results (for instance, from group theory and ring theory). In bringing together diverse areas of research, Universal Algebra provides a common scaffolding upon which to build general techniques. "What looks messy and complicated in a particular framework may turn out to be simple and obvious in the proper general one," as Smith [20] describes it.

The subsections below give a brief overview of the topics needed for the later sections, and though self-contained, they are necessarily brief. The interested reader is encouraged to consult [13] and [21], which are both good references for the algebraic topics. The section concludes with a short overview of Quantum Computation, for which [15] is a more extensive reference.

2.1 Universal Algebra

Given a set A, an *operation* on A is a function $f : A^n \to A$, where $n \in \mathbb{N}$ is the arity of f. The set A together with some operations $(f_i)_{i\in I}$ is a *universal algebra*, commonly denoted $\mathbb{A}$. We specify the set and the operations by writing

$$\mathbb{A} = \langle A\ ;\ (f_i)_{i\in I}\rangle \qquad \text{or} \qquad \mathbb{A} = \langle A\ ;\ f_1, \ldots, f_k\rangle\,,$$

depending on whether I is finite. A non-empty subset $B \subseteq A$ which is closed under all operations f_i of $\mathbb{A}$ is called a *subalgebra*, written $\mathbb{B} \leq \mathbb{A}$. If $C \subseteq A$ is non-empty, then we define the *subalgebra generated by* C to be the smallest subalgebra containing C, written $\mathrm{Sg}(C)$. These general definitions of algebras and subalgebras include most of the classical algebraic structures (groups, rings, boolean algebras, etc.) and allow for the unification of a host of results.

The appropriate generalization of a normal subgroup for a universal algebra is a *congruence*. Precisely, a congruence θ of an algebra $\mathbb{A}$ is a binary equivalence relation on the set A which is compatible with the operations of $\mathbb{A}$, meaning

$$a_1\ \theta\ b_1, \ldots, a_k\ \theta\ b_k \quad \Rightarrow \quad f(a_1, \ldots, a_k)\ \theta\ f(b_1, \ldots, b_k)$$

for all operations f of $\mathbb{A}$ (infix notation is used here for binary relations). As with subalgebras, given a set $D \subseteq A^2$, we define the *congruence generated by* D to be the smallest congruence containing D, written $\mathrm{Cg}(D)$. Similar to normal subgroups, the quotient structure $\mathbb{A}/\theta$ is well-defined, and general versions of the classic isomorphism theorems for groups and rings hold true in this context.

Two algebras $\mathbb{A}$ and $\mathbb{B}$ are said to be *similar* if there is a bijective correspondence between the k-ary operations of $\mathbb{A}$ and $\mathbb{B}$ for each k. In this case, $f^{\mathbb{A}}$ is written for the operation of $\mathbb{A}$ corresponding to the operation $f^{\mathbb{B}}$ of $\mathbb{B}$. When there is no chance for confusion, however, these superscripts are omitted and we simply use the same symbol f for both $f^{\mathbb{A}}$ and $f^{\mathbb{B}}$. A *homomorphism* between similar structures $\mathbb{A}$ and $\mathbb{B}$ is a function $\varphi : A \to B$ such that for each k-ary operation $f^{\mathbb{A}}$ of $\mathbb{A}$ and all $a_1, \ldots, a_k \in A$,

$$\varphi\big(f^{\mathbb{A}}(a_1, \ldots, a_k)\big) = f^{\mathbb{B}}\big(\varphi(a_1), \ldots, \varphi(a_k)\big)$$

(i.e. φ is compatible with the operations of $\mathbb{A}$ and $\mathbb{B}$). This is indicated by writing $\varphi : \mathbb{A} \to \mathbb{B}$. Similar to groups and rings, congruences are precisely the *kernels* of homomorphisms

$$\ker(\varphi) = \big\{(a, b) \in A^2 \mid \varphi(a) = \varphi(b)\big\},$$

but in contrast to groups the kernel is a binary relation.

Every algebra $\mathbb{A}$ has at least two (possibly non-distinct) congruences — the trivial congruence $\mathbf{0}$ and the universal congruence $\mathbf{1}$,

$$\mathbf{0} = \big\{(a, a) \in A^2 \mid a \in A\big\} \qquad \text{and}$$
$$\mathbf{1} = A^2 = \big\{(a, b) \in A^2 \mid a, b \in A\big\},$$

As with groups, if these are the only congruences of $\mathbb{A}$, then we call $\mathbb{A}$ *simple*.

The set of congruences of $\mathbb{A}$ is denoted $\mathrm{Con}(\mathbb{A})$, and can be ordered by inclusion, in which case $\mathbf{1}$ and $\mathbf{0}$ are the maximal and minimal elements, respectively. More than this, $\mathrm{Con}(\mathbb{A})$ has the structure of a lattice, where the operations of $\wedge$ and $\vee$ are defined

$$\theta \wedge \psi \coloneqq \theta \cap \psi \qquad \text{and} \qquad \theta \vee \psi \coloneqq \mathrm{Cg}\left(\theta \cup \psi\right)$$

for $\theta, \psi \in \mathrm{Con}(\mathbb{A})$. Perhaps surprisingly, different kinds of lattice-theoretic structure in $\mathrm{Con}(\mathbb{A})$ are in correspondence with algebraic structure in $\mathbb{A}$, and this correspondence is a central area of study in the field. Of particular interest for us is when $\mathrm{Con}(\mathbb{A})$ is a *distributive lattice*, meaning

$$\alpha \wedge \left(\beta \vee \gamma\right) = \left(\alpha \wedge \beta\right) \vee \left(\alpha \wedge \gamma\right)$$

for all $\alpha, \beta, \gamma \in \mathrm{Con}(\mathbb{A})$. In this case, we say that $\mathbb{A}$ is *congruence distributive*.

2.2 Clones

Given a set F of operations on a common domain A, new operations may be produced by composing operations. Formally, if $f \in F$ is n-ary and $g_i \in F$ is k_i-ary for $i \in [n]$, then

$$h(x_{11}, \ldots, x_{nk_n}) \coloneqq f\big(g_1(x_{11}, \ldots, x_{1k_i}), \ldots, g_n(x_{n1}, \ldots, x_{nk_n})\big)$$

is a $(\sum k_i)$-ary operation of A.

New operations of A may also be produced by variable manipulations. Given n-ary operation $f \in F$ and any function $\sigma : [n] \to [m]$,

$$h(x_1, \ldots, x_m) \coloneqq f\big(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\big)$$

is an m-ary operation of A. Less formally, given n-ary $f \in F$ we may define operations of equal arity by permuting variables, operations of smaller arity by identifying variables, and operations of larger arity by introducing extraneous variables.

A *clone* over a domain A is a set of operations of A which is closed under composition and variable manipulations (as detailed above). The *clone generated by* a set of operations F, written $\mathrm{Clo}(F)$ is the smallest clone containing F. Likewise, the *clone of term operations* of the algebra $\mathbb{A}$, written $\mathrm{Clo}(\mathbb{A})$, is the clone generated by the operations of $\mathbb{A}$.

Given a fixed domain A, the set of clones over A can be ordered by inclusion. As with the set of congruences of an algebra, the set of clones over A forms a lattice with operations $\wedge$ and $\vee$ defined

$$\mathcal{A} \wedge \mathcal{B} \coloneqq \mathcal{A} \cap \mathcal{B} \qquad \text{and} \qquad \mathcal{A} \vee \mathcal{B} \coloneqq \mathrm{Clo}\left(\mathcal{A} \cup \mathcal{B}\right)$$

for clones $\mathcal{A}$ and $\mathcal{B}$ over the domain A. We extend the ordering on clones to algebras $\mathbb{B}$ and $\mathbb{D}$ over the common domain A by writing $\mathbb{B} \preceq \mathbb{D}$ if and only if $\mathrm{Clo}(\mathbb{B}) \subseteq \mathrm{Clo}(\mathbb{D})$. If C is a clone over the domain A, then we will slightly abuse this notation by writing $C \preceq \mathbb{B}$ if $C \subseteq \mathrm{Clo}(\mathbb{B})$, and similarly for $\mathbb{B} \preceq C$.

2.3 Quantum Computation

Qubits are the information-theoretic foundation of quantum computation. A qubit can have a *pure* state of either 0 or 1, but may also be in a *superposition* of 0 and 1 states. Formally, this is represented by a 2-dimensional normed complex vector space (i.e. a Hilbert space),

$$\mathfrak{B} \coloneqq \mathbb{C}\text{-span}\left\{\, |0\rangle, |1\rangle \,\right\}.$$

We adopt the notation of Dirac [4] where $|\alpha\rangle$ denotes a column vector and $\langle\alpha| \coloneqq |\alpha\rangle^\dagger$ denotes a row vector ("$\dagger$" represents the Hermitian adjoint).

A system of k qubits is represented by the tensor power of $\mathfrak{B}$, written $\mathfrak{B}^{\otimes k} \coloneqq \mathfrak{B} \otimes \cdots \otimes \mathfrak{B}$. This vector space has dimension 2^k with basis $\left\{\, |x_1\rangle \otimes \cdots \otimes |x_k\rangle \mid x_i \in \{0,1\} \right\}$. Using the notation $|x_1 x_2\rangle \coloneqq |x_1\rangle \otimes |x_1\rangle$ gives us

$$\mathfrak{B}^{\otimes k} = \mathbb{C}\text{-span}\left\{\, |x_1 \cdots x_k\rangle \mid x_i \in \{0,1\} \right\}.$$

A *quantum state* is a vector in $\mathfrak{B}^{\otimes k}$,

$$|\alpha\rangle = \sum_{x_i \in \{0,1\}} \lambda_{x_1 \cdots x_k} |x_1 \cdots x_k\rangle \quad \text{such that} \quad \|\alpha\| = 1.$$

The condition that $\|\alpha\| = 1$ is equivalent to $\sum |\lambda_{x_1 \cdots x_k}|^2 = 1$, and so $\left(|\lambda_{x_1 \cdots x_k}|^2\right)_{x_i \in \{0,1\}}$ is regarded as a *probability distribution*: when the quantum state $|\alpha\rangle$ is measured, the pure state $|y_1 \cdots y_k\rangle$ will be observed with probability $|\lambda_{y_1 \cdots y_k}|^2$.

The evolution over time of a quantum state $|\alpha\rangle$ is represented by the action of a unitary operator U on $|\alpha\rangle$. A given unitary operator can be approximated using products and tensor products of operators from the *standard quantum gate set*. A *quantum circuit* for the operator U is this decomposition, typically given as a diagram. Figure 2 is an example of such a diagram and Definition 3.2 is the inline form of the same circuit.

One particular quantum gate which we will make use of is the Hadamard gate H, defined by its action on the basis vectors of $\mathfrak{B}$ by

$$H|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big), \qquad H|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big).$$

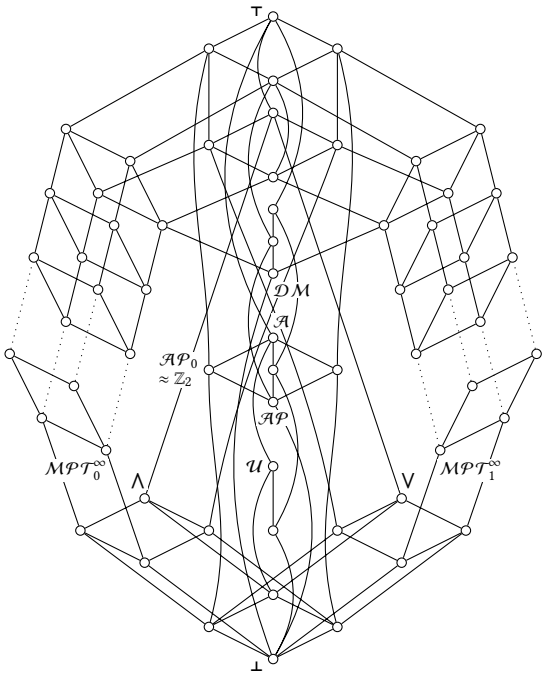
A convenient formula for the action of $H^{\otimes n}$ on an arbitrary n-qubit state is

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

where $a \cdot x$ is the dot product of a and x modulo 2 (regarded as $\mathbb{Z}_2$-vectors).

3 The Hidden Kernel Problem

As described in the introduction, given a group $\mathbb{G}$, the function $f : G \to X$ *hides* a subgroup $\mathbb{D} \leq \mathbb{G}$ if $f(g) = f(h)$ if and only if $gD = hD$.



Clone	Generating Operations
$\bot$	$\emptyset$
$\bigwedge$	$x \wedge y$, 0, 1
$\bigvee$	$x \vee y$, 0, 1
$\mathcal{U}$	$\neg x$, 0
$\mathcal{MPT}_0^\infty$	$x \vee (y \wedge z)$
$\mathcal{MPT}_1^\infty$	$x \wedge (y \vee z)$
$\mathcal{AP}$	$x + y + z$
$\mathcal{AP}_0$	$x + y$
$\mathcal{A}$	$x \leftrightarrow y$, 0
$\mathcal{DM}$	$\mathrm{maj}(x, y, z)$
$\top$	$x \vee y, \neg x$

Figure 1. Diagram of Post's Lattice, the lattice of all clones on a 2-element domain (i.e. boolean clones). Clones which will be relevant later have been labelled, and operations generating each of them are given in the table to the right. Simon's Problem corresponds to the HKP on the operational clone of the group $\mathbb{Z}_2$, namely $\mathcal{AP}_0$.

Hidden Subgroup Problem (HSP)

Input:	group $\mathbb{G}$,
	oracle $f : G \to X$ hiding some subgroup
Task:	determine the subgroup $\mathbb{D} \leq \mathbb{G}$ that f hides

A quantum polynomial-time solution to the HSP for *abelian* $\mathbb{G}$ is known [11], and this case contains many famous quantum algorithms exhibiting super-polynomial speedup over classical solutions. The HSP for *non-abelian* $\mathbb{G}$ has been solved in some quite specific cases and restrictive settings, but it remains open in general. In spite of focused research, no general polynomial-time quantum algorithm for the HSP has been found.

That the HSP has been efficiently solved for a large class of groups (abelian ones) and an irregular constellation of groups otherwise suggests two possibilities.

1. There is no quantum polynomial-time solution to the general HSP. It is suspected that quantum algorithms cannot solve NP-complete problems in polynomial time, and it may be the case that the general HSP is NP-complete.
2. There is a quantum polynomial-time solution, but it requires a deeper insight into the problem than has been obtained over the past 30 years.

In either of these cases, large additional classes of structures for which the HSP has an efficient solution would be incredibly valuable. To this end, we propose a generalization of the HSP to universal algebraic structures. Such a generalization will extend the domain of the problem to classes of structures with additional gradations of complexity, with the expectation that these these gradations will be reflected in the complexity of the generalized problem.

3.1 The Hidden Kernel Problem

The Hidden Subgroup Problem can be framed as a problem about the *quotient structure* induced by the hidden subgroup $\mathbb{D}$, namely G/D (the set of cosets of $\mathbb{D}$ in $\mathbb{G}$). In this formulation, we are given $\mathbb{G}$ and a *bijective* function $f : G/D \to X$ as an oracle, and tasked with computing $\mathbb{D} \leq \mathbb{G}$. The set G/D does *not* have group structure itself unless $\mathbb{D}$ is a normal subgroup. The progress which has been made on the general HSP begins with a deep analysis of what limited structure G/D *does* have for certain classes of groups.

For abelian groups, every subgroup is normal, so the structure of G/D is quite uniform. Restricting attention to only the *normal* subgroups yields the *Hidden Normal Subgroup Problem*. It is this problem which we generalize to obtain the *Hidden Kernel Problem*.

Let $\mathbb{A}$ be an algebra and θ a congruence of $\mathbb{A}$. Following the definition of a hidden subgroup, the function $f : A \to X$ *hides* the congruence θ if $f(a) = f(b)$ precisely when $a\ \theta\ b$.

The Hidden Kernel Problem (preliminary version)

Input:	algebra $\mathbb{A}$, oracle $f : A \to X$ hiding some congruence
Task:	determine the congruence θ of $\mathbb{A}$ that f hides

It is not hard to show that a function $f : \mathbb{A} \to X$ hides a congruence θ if and only if f is a homomorphism with $\theta = \ker(f)$. This observation leads to the general statement of the Hidden Kernel Problem.

The Hidden Kernel Problem (HKP)

Input:	similar algebras $\mathbb{A}$ and $\mathbb{B}$, homomorphism $\varphi : \mathbb{A} \to \mathbb{B}$ (as an oracle)
Task:	determine the congruence $\ker(\varphi)$

This generalization includes and extends the Hidden Normal Subgroup Problem, and abstracts away the somewhat unnatural notion of "hiding".

3.2 Simon's Problem and Post's Lattice

Perhaps the simplest instance of the Hidden Subgroup Problem is when the group is an elementary abelian 2-group, $\mathbb{G} = \mathbb{Z}_2^n$. This instance of the HSP is known as *Simon's Problem* [19], and historically is one of the first examples of super-polynomial speedup when using a quantum algorithm.

We will consider a universal algebraic version of Simon's Problem — The Hidden Kernel Problem on $\mathbb{A} = \mathbb{B}^n$, where $\mathbb{B}$ is a 2-element algebra. There are infinitely many such $\mathbb{B}$, and *a priori* there seems to be neither a natural starting point nor a systematic way in which to proceed. One crucial observation is the following.

Observation 3.1. Let $\mathbb{B}$ and $\mathbb{D}$ be universal algebras such that $B = D$ and $\mathrm{Clo}(\mathbb{B}) \subseteq \mathrm{Clo}(\mathbb{D})$. Each specific instance of $\mathrm{HKP}(\mathbb{D}^n)$ is a specific instance of $\mathrm{HKP}(\mathbb{B}^n)$. A solution to all instances of $\mathrm{HKP}(\mathbb{B}^n)$ yields a solution to all instances of $\mathrm{HKP}(\mathbb{D}^n)$.

This observation follows from the fact that every homomorphism of $\mathbb{D}^n$ is also a homomorphism of $\mathbb{B}^n$ when $\mathrm{Clo}(\mathbb{B}) \subseteq \mathrm{Clo}(\mathbb{D})$ ($\Leftrightarrow \mathbb{B} \preceq \mathbb{D}$). The observation implies that $\mathrm{HKP}(\mathbb{B}^n)$ is equivalent to $\mathrm{HKP}(\mathbb{D}^n)$ whenever $\mathrm{Clo}(\mathbb{B}) = \mathrm{Clo}(\mathbb{D})$. Instead of considering all possible 2-element algebras $\mathbb{B}$, we therefore consider only those algebras with distinct clones of term operations.

The task of describing all clones of operations on a 2-element domain (also known as boolean clones), was famously undertaken in 1941 by Emil Post [16]. Ordered by inclusion, the set of all boolean clones is known as *Post's Lattice*, and has a particularly regular structure (see Figure 1). The operations given in Figure 1 are in terms of the familiar boolean operations, with the possible exception of the *majority* function, defined

$$\mathrm{maj}(x, y, z) \coloneqq (x \wedge y) \vee (x \wedge z) \vee (y \wedge z).$$

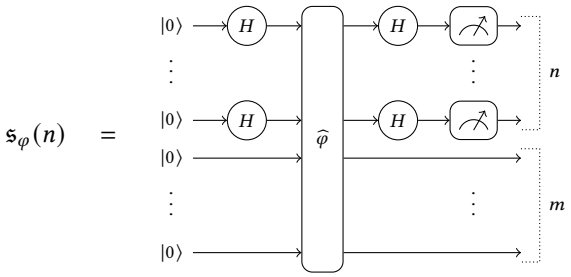


Figure 2. The circuit $\mathfrak{s}_\varphi(n)$ of Definition 3.2.

An important property of this operation is that

$$x = \mathrm{maj}(y, x, x) = \mathrm{maj}(x, y, x) = \mathrm{maj}(x, x, y).$$

We end this subsection by defining the quantum circuit which will yield a polynomial-time quantum solution to $\mathrm{HKP}(\mathbb{B}^n)$ for many of the algebras we consider. This circuit is essentially the same as Simon's original circuit [19].

Definition 3.2. Let $\varphi : \{0,1\}^n \to \{0,1\}^m$, and define the 2^{n+m}-dimensional unitary transformation $\widehat{\varphi}$ by its action on basis vectors,

$$\widehat{\varphi}\big(\,|x\rangle \otimes |y\rangle\,\big) \coloneqq |x\rangle \otimes |y + \varphi(x)\rangle\,,$$

where $x \in \{0,1\}^n$, $y \in \{0,1\}^m$, and "+" is componentwise addition modulo 2. The quantum circuit $\mathfrak{s}_\varphi(n)$ is the circuit

$$\mathfrak{s}_\varphi(n) \coloneqq \left(H^{\otimes n} \otimes I_m\right) \widehat{\varphi} \left(H^{\otimes n} \otimes I_m\right)$$

of size $n + m$, where measurement is performed on the first n qubits. The circuit $\mathfrak{s}_\varphi(n)$ is given graphically in Figure 2. Note that we can always take $m \leq n$, so the circuit is of size $\Theta(n)$.

4 The HKP and Post's Lattice: Algorithms

In this section we present positive results for solving the Hidden Kernel Problem for Post's Lattice in polynomial time using classical and quantum algorithms. The main quantum result is Theorem 4.1 and the main classical result is Corollary 4.2, stated below.

Theorem 4.1. *Let $\mathbb{B}$ be a 2-element algebra such that one of*

1. $\mathcal{MPT}_0^\infty \preceq \mathbb{B}$,
2. $\mathcal{MPT}_1^\infty \preceq \mathbb{B}$, *or*
3. $\mathcal{AP} \preceq \mathbb{B}$

holds and let $\mathbb{A} = \mathbb{B}^n$. The quantum circuit $\mathfrak{s}_\varphi(n)$ of Definition 3.2 solves $\mathrm{HKP}(\mathbb{A})$ with probability $1 - 1/\tau$ in $\Theta(n + \lg(\tau))$ iterations.

Corollary 4.2. *Let $\mathbb{B}$ be a 2-element algebra such that one of*

1. $\mathcal{MPT}_0^\infty \preceq \mathbb{B}$,
2. $\mathcal{MPT}_1^\infty \preceq \mathbb{B}$, *or*
3. $\mathcal{DM} \preceq \mathbb{B}$

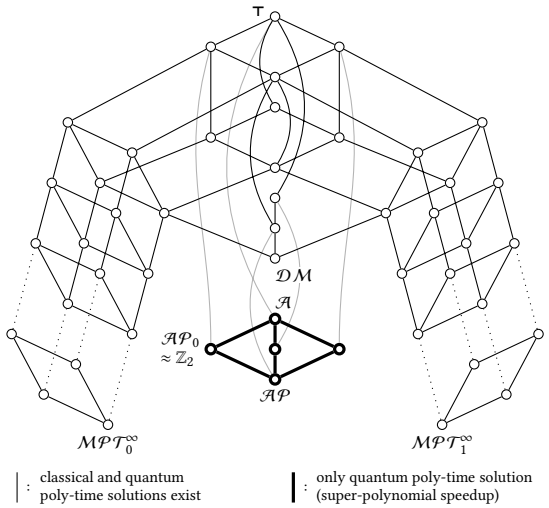


Figure 3. The fragment of Post's Lattice for which the HKP is solvable in polynomial-time using a quantum algorithm (whole diagram). Bold lines indicate clones exhibiting a super-polynomial speedup with a quantum algorithm (i.e. no classical polynomial-time algorithm exists, see Theorem 5.1), while plain lines indicate clones for which a classical polynomial-time algorithm exists.

holds and let $\mathbb{A} = \mathbb{B}^n$. *Then* $\mathrm{HKP}(\mathbb{A})$ *is solvable classically in* $O(n)$ *time.*

The best way to summarize these two results is in terms of Post's Lattice, see Figure 3. In particular, powers of algebras whose clones are contained in the interval between $\mathcal{AP}$ and $\mathcal{A}$ have HKP solvable in polynomial-time using a quantum algorithm, but not a classical one (see Theorem 5.1). Combined with the results of the next section, this provides a complete quantum and classical classification of the algorithmic complexity of the HKP for powers of 2-element algebras.

The remainder of the section is devoted to proving Theorem 4.1 and Corollary 4.2. We proceed by proving a series of lemmas, beginning first with two lemmas leading up to the famous result of Simon [19], which we phrase and prove in terms of the Hidden Kernel Problem.

Lemma 4.3. *Let* $\mathbb{D} \leq \left(\mathbb{Z}_2^n\right)^2$. *For all* $g \in \left(\mathbb{Z}_2^n\right)^2$,

$$\sum_{d \in D} (-1)^{g \cdot d} = \begin{cases} |D| & \text{if } g \cdot d = 0 \text{ for all } d \in D, \\ 0 & \text{otherwise,} \end{cases}$$

where $g \cdot d$ *is the dot product modulo 2 of* g *and* d *(regarded as* $\mathbb{Z}_2$*-vectors).*

Proof. Define sets

$$D_0 = \left\{d \in D \mid g \cdot d = 0\right\} \quad \text{and} \quad D_1 = \left\{d \in D \mid g \cdot d = 1\right\}.$$

Observe that these sets are disjoint and $D = D_0 \cup D_1$, so they partition D. Thus,

$$\sum_{d \in D} (-1)^{g \cdot d} = |D_0| - |D_1|.$$

It is not hard to see that D_0 is a subgroup of $\mathbb{D}$. If $D_1 = \emptyset$, then the summation is equal to $|D|$ and $g \cdot d = 0$ for all $d \in D$. Let us assume therefore that $D_1 \neq \emptyset$ and let $d \in D_1$. It follows that $d + D_0 \subseteq D_1$ and $d + D_1 \subseteq D_0$. Hence $D_1 = d + D_0$ and so D_1 is a coset of D_0. Therefore $|D_1| = |D_0|$ and the summation equals 0. □

Lemma 4.4. *Let* θ *be a congruence of* $\mathbb{Z}_2^n$ *and let* $X \subseteq \theta$. *The set* X *generates* θ *with probability* $1 - 1/\tau$, *where* $|X| \in \Theta(n + \lg(\tau))$. *Specifically, if* $|X| = 2n$ *then the probability of generation is* $1 - 2^{-n}$.

Proof. Let ψ be an arbitrary congruence of $\mathbb{Z}_2^n$. We have $g \;\psi\; h$ if and only if $(g+h) \;\psi\; 0$, so the congruence class of ψ containing $0 \in \mathbb{Z}_2^n$ uniquely characterizes ψ. Call this congruence class H_ψ,

$$H_\psi = \left\{g \in \mathbb{Z}_2^n \mid g \;\psi\; 0\right\}.$$

It's not hard to see that H_ψ is a subgroup of $\mathbb{Z}_2^n$. In this manner subgroups (normal subgroups, in general) correspond to congruences.

Let $X_0 = \{x + y \mid (x, y) \in X\}$ and note that X_0 is contained in the congruence class of 0 in θ. From the paragraph above, we have $\mathrm{Cg}(X) \neq \theta$ if and only if $\mathrm{Sg}(X_0) \neq \mathbb{H}_\theta$. The set X_0 fails to generate $\mathbb{H}_\theta$ if and only if X_0 is contained in some maximal subgroup $\mathbb{M}$ of $\mathbb{H}_\theta$. Since $\mathbb{H}_\theta$ is abelian and a subgroup of $\mathbb{Z}_2^n$, these are all of size $|H_\theta|/2$. Thus,

$$\begin{aligned} \mathrm{P}\left(\mathrm{Cg}(X) \neq \theta\right) &= \mathrm{P}\left(\mathrm{Sg}(X_0) \neq \mathbb{H}_\theta\right) \\ &= \mathrm{P}\left(\exists \text{ maximal } \mathbb{M} \leq \mathbb{H}_\theta \text{ with } X_0 \subseteq M\right) \\ &\leq \sum_{\text{maximal } \mathbb{M} \leq \mathbb{H}_\theta} \mathrm{P}\left(X_0 \subseteq M\right) \\ &= \sum_{\text{maximal } \mathbb{M} \leq \mathbb{H}_\theta} \prod_{g \in X_0} \mathrm{P}\left(g \in M\right) \\ &= \sum_{\text{maximal } \mathbb{M} \leq \mathbb{H}_\theta} \prod_{g \in X_0} \frac{1}{2} = \frac{L}{2^{|X_0|}}, \end{aligned}$$

where L is the number of maximal subgroups of $\mathbb{H}_\theta$. We now endeavor to calculate L.

Since $\mathbb{Z}_2^n$ is an elementary abelian 2-group, $\mathbb{H}_\theta$ is as well. It follows that $\mathbb{H}_\theta$ can be regarded as a $\mathbb{Z}_2$-vector space. Maximal subgroups correspond to maximal subspaces, and each maximal subspace can be uniquely characterized as the orthogonal complement of a 1-dimensional subspace. The number of 1-dimensional subspaces is $|H_\theta| - 1$, and so is at most $2^n - 1$. Combining everything, we have

$$\mathrm{P}\left(\mathrm{Cg}(X) \neq \theta\right) \leq \frac{L}{2^{|X_0|}} \leq \frac{2^n - 1}{2^{|X_0|}}.$$

It follows that X generates θ with probability $1 - 1/\tau$, where $|X| \in \Theta(n + \lg(\tau))$, as claimed. □

Theorem 4.5 (Simon [19]). *Let $\mathbb{A} = \mathbb{Z}_2^n$. The quantum circuit $\mathfrak{s}_\varphi(n)$ of Definition 3.2 solves* HKP($\mathbb{A}$) *with probability $1 - 1/\tau$ using $\Theta(n + \lg(\tau))$ iterations.*

Proof. Instead of calculating the pre-measurement output (call it $|\psi\rangle$), it will be more convenient for us to calculate the density matrix of the pre-measurement output, $\rho = |\psi\rangle\langle\psi|$, and take the partial trace.

The circuit operates on two registers, initially set to $|\psi_0\rangle = |0^n\rangle \otimes |0^m\rangle$. This state has density matrix $\rho_0 = |\psi_0\rangle\langle\psi_0|$. After the first set of Hadamard gates, the density matrix is

$$\begin{aligned}\rho_1 &\coloneqq (H^{\otimes n} \otimes I)\rho_0(H^{\otimes n} \otimes I)\\ &= \left(H^{\otimes n}|0^n\rangle \otimes |0^m\rangle\right)\left(\langle 0^n| H^{\otimes n} \otimes \langle 0^m|\right)\\ &= \left(\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n} |x\rangle \otimes |0^m\rangle\right)\left(\frac{1}{2^{n/2}}\sum_{y\in\{0,1\}^n} \langle y| \otimes \langle 0^m|\right)\\ &= \frac{1}{2^n}\sum_{x,y\in\{0,1\}^n} |x\rangle\langle y| \otimes |0^m\rangle\langle 0^m|.\end{aligned}$$

We now describe the $\widehat{\varphi}$ gate. A homomorphism $\varphi : \mathbb{A} \to \mathbb{B}$ is given as input as an oracle from which we may make queries. As a function, φ can be regarded as mapping bit strings from $\{0,1\}^n$ to $\{0,1\}^m$. Define the function $\widehat{\varphi}$ by

$$\begin{aligned}\widehat{\varphi} : \{0,1\}^{n+m} &\to \{0,1\}^{n+m},\\ (a,b) &\mapsto (a, \varphi(a) + b).\end{aligned}$$

Observe that $\widehat{\varphi}$ is invertible and that the original value of $\varphi(a)$ can be recovered — $\widehat{\varphi}(a,0) = (a,\varphi(a))$. The function $\widehat{\varphi}$ can be regarded as a permutation of basis vectors of the space $\mathfrak{B}^{\otimes(n+m)}$, and thus can be extended to a unitary transformation $\widehat{\varphi}$ on the space.

Continuing with the evaluation of the circuit, after applying the $\widehat{\varphi}$ gate the density matrix is

$$\begin{aligned}\rho_2 &\coloneqq \widehat{\varphi}\rho_1\widehat{\varphi}^\dagger = \frac{1}{2^n}\sum_{x,y\in\{0,1\}^n} \left(\widehat{\varphi}|x\rangle \otimes |0^m\rangle\right)\left(\widehat{\varphi}|y\rangle \otimes |0^m\rangle\right)^\dagger\\ &= \frac{1}{2^n}\sum_{x,y\in\{0,1\}^n} \left(|x\rangle \otimes |\varphi(x)\rangle\right)\left(|y\rangle \otimes |\varphi(y)\rangle\right)^\dagger\\ &= \frac{1}{2^n}\sum_{x,y\in\{0,1\}^n} |x\rangle\langle y| \otimes |\varphi(x)\rangle\langle\varphi(y)|.\end{aligned}$$

Applying the last set of Hadamard gates yields the final pre-measurement density matrix,

$$\begin{aligned}\rho &\coloneqq \frac{1}{2^n}\sum_{x,y\in\{0,1\}^n} H^{\otimes n}|x\rangle\langle y| H^{\otimes n} \otimes |\varphi(x)\rangle\langle\varphi(y)|\\ &= \frac{1}{2^{2n}}\sum_{\substack{a,b\in\{0,1\}^n,\\ x,y\in\{0,1\}^n}} (-1)^{a\cdot x + b\cdot y}|a\rangle\langle b| \otimes |\varphi(x)\rangle\langle\varphi(y)|.\end{aligned}$$

The density matrix for the first register is given by taking the partial trace of ρ over the second register. Doing this, we have

$$\mathrm{Tr}_2(\rho) = \frac{1}{2^{2n}}\sum_{\substack{a,b\in\{0,1\}^n,\\ x,y\in\{0,1\}^n}} (-1)^{a\cdot x + b\cdot y}|a\rangle\langle b|\ \mathrm{Tr}\left(|\varphi(x)\rangle\langle\varphi(y)|\right).$$

It isn't hard to see that $\mathrm{Tr}(|\varphi(x)\rangle\langle\varphi(y)|) = 1$ if $\varphi(x) = \varphi(y)$ (i.e. if $(x,y) \in \ker(\varphi)$) and is 0 otherwise. Thus,

$$\mathrm{Tr}_2(\rho) = \frac{1}{2^{2n}}\sum_{a,b\in\{0,1\}^n}\ \sum_{(x,y)\in\ker(\varphi)} (-1)^{a\cdot x + b\cdot y}|a\rangle\langle b|.$$

The congruence $\ker(\varphi)$ is a subgroup of $(\mathbb{Z}_2^n)^2$ and we have $a\cdot x + b\cdot y = (a,b)\cdot(x,y)$. Lemma 4.3 thus applies to the inner summation. Applying it yields

$$\mathrm{Tr}_2(\rho) = \frac{|\ker(\varphi)|}{2^{2n}}\sum_{(a,b)\in\ker(\varphi)^\perp} |a\rangle\langle b|,$$

where

$$\ker(\varphi)^\perp = \left\{(a,b) \mid (a,b)\cdot(x,y) = 0 \text{ for all } (x,y) \in \ker(\varphi)\right\}.$$

The congruence $\ker(\varphi)$ is a $\mathbb{Z}_2$-subspace of $\mathbb{A}^2$, and this is its orthogonal complement. It follows that $\ker(\varphi)^\perp$ is also a congruence of $\mathbb{A}$ and $|\ker(\varphi)||\ker(\varphi)^\perp| = |A|^2 = 2^{2n}$. Thus

$$\mathrm{Tr}_2(\rho) = \frac{1}{|\ker(\varphi)^\perp|}\sum_{(a,b)\in\ker(\varphi)^\perp} |a\rangle\langle b|.$$

This corresponds to a uniform distribution over elements in $\ker(\varphi)^\perp$. By Lemma 4.4, iterating this procedure $\Theta(n + \lg(\tau))$ times will produce a generating set for $\ker(\varphi)^\perp$ with probability $1 - 1/\tau$.

As $\ker(\varphi) = \left(\ker(\varphi)^\perp\right)^\perp$, we have succeeded in calculating $\ker(\varphi)$ with probability $1 - 1/\tau$ using $\Theta(n + \lg(\tau))$ iterations of a circuit of size $\Theta(n)$. □

At this point, we have established a quantum polynomial-time algorithm for the HKP for powers of algebras above the clone $\mathcal{AP}_0$ in Post's Lattice. Aside from the group $\mathbb{Z}_2$, this includes only 3 other structures (see Figure 3). The next lemma and theorem greatly expand this list by deducing a classical algorithm for powers of certain congruence distributive algebras which includes the infinite "wings" of Post's Lattice.

Lemma 4.6. *Let $\mathbb{B}_1, \ldots, \mathbb{B}_n$ be similar algebras which are simple and let $\mathbb{A} = \prod_{i=1}^n \mathbb{B}_i$ be congruence distributive. Every congruence of $\mathbb{A}$ is the kernel of a projection homomorphism $\mathrm{proj}_I : \mathbb{A} \to \prod_{i\in I}\mathbb{B}_i$ for some $I \subseteq [n]$.*

Proof. For each $i \in [n]$ define $\eta_i = \ker(\mathrm{proj}_i)$. Let θ be a congruence of $\mathbb{A}$. Each algebra $\mathbb{B}_i$ is simple, so each congruence η_i is maximal in $\mathrm{Con}(\mathbb{A})$. It follows that

$$\theta \vee \eta_i = \begin{cases}\eta_i & \text{if } \theta \le \eta_i,\\ \mathbf{1} & \text{otherwise.}\end{cases}$$

Using congruence distributivity, we now have

$$\theta = \theta \vee \mathbf{0} = \theta \vee \bigwedge_{i\in[n]} \eta_i = \bigwedge_{i\in[n]} (\theta \vee \eta_i) = \bigwedge_{i\in I} \eta_i = \ker(\mathrm{proj}_I),$$

where $I = \{i \mid \theta \leq \eta_i\}$. □

Theorem 4.7. *Let $\mathbb{B}_1, \ldots, \mathbb{B}_n$ be similar algebras which are simple and let $\mathbb{A} = \prod_{i=1}^{n} \mathbb{B}_i$ be congruence distributive. There is a classical $O(n)$ algorithm solving* HKP($\mathbb{A}$).

Proof. Let $\varphi : \mathbb{A} \to \mathbb{D}$ be a homomorphism. Lemma 4.6 implies that $\ker(\varphi) = \ker(\mathrm{proj}_I)$ for some $I \subseteq [n]$. Thus, specifying I uniquely determines $\ker(\varphi)$. Without loss of generality, we may assume that $|B_i| \geq 2$ since we can eliminate any $\mathbb{B}_i$ of size 1 in the product and produce an algebra isomorphic to $\mathbb{A}$. For each i, fix distinct elements $a_i, b_i \in B_i$. We have that

$$i \notin I \qquad \Leftrightarrow \qquad \varphi(a_1, \ldots, a_n) = \varphi(a_1, \ldots, b_i, \ldots, a_n),$$

where the inputs to φ differ only at position i. Starting at coordinate $i = 1$ and proceeding to coordinate $i = n$, we evaluate both sides of the equality, recording when it holds and when it fails. The set of i for which the equality fails is I. This is an $O(n)$ procedure. □

We are now ready to prove Corollary 4.2, which we began the section with.

Corollary 4.2 (redux)**.** *Let $\mathbb{B}$ be a 2-element algebra such that one of*

1. $\mathcal{MPT}_0^\infty \preceq \mathbb{B}$,
2. $\mathcal{MPT}_1^\infty \preceq \mathbb{B}$, *or*
3. $\mathcal{DM} \preceq \mathbb{B}$

holds and let $\mathbb{A} = \mathbb{B}^n$. Then HKP($\mathbb{A}$) *is solvable classically in $O(n)$ time.*

Proof. By Theorem 4.7, it is sufficient to show that $\mathbb{A}$ is congruence distributive. The primary tool that we use is the existence of Jónsson term operations [10], which is equivalent to $\mathbb{A}$ being congruence distributive. Briefly, these are a collection of 3-ary term operations of $\mathbb{A}$, $J_1, \ldots, J_{2m+1}$, satisfying the universally quantified identities

$$\begin{aligned}
&J_1(x,x,y) = x, && J_{2m+1}(x,y,y) = y,\\
&J_i(x,y,x) = x, && \text{for } i \in [2m+1],\\
&J_{2i+1}(x,y,y) = J_{2i+2}(x,y,y) && \text{for } i \in [m-1],\\
&J_{2i}(x,x,y) = J_{2i+1}(x,x,y) && \text{for } i \in [m].
\end{aligned}$$

We are now ready to proceed with the proof.

Suppose that $\mathcal{DM} \preceq \mathbb{B}$ and let $\mathbb{A} = \mathbb{B}^n$. The clone $\mathcal{DM}$ has $\mathrm{maj}(x,y,z)$ as a generating operation (see the discussion at the end of Section 3 and Figure 1), and so this is also an operation of $\mathbb{B}$ and hence of $\mathbb{A}$ (where it is extended from $\mathbb{B}$ componentwise). Simply taking $J_1(x,y,z) \coloneqq \mathrm{maj}(x,y,z)$ and verifying that this choice satisfies the Jónsson identities is sufficient to prove that $\mathbb{A}$ is congruence distributive.

The arguments for $\mathcal{MPT}_0^\infty$ and $\mathcal{MPT}_1^\infty$ are quite similar, so we will present only the $\mathcal{MPT}_0^\infty \preceq \mathbb{B}$ case. Suppose that $\mathcal{MPT}_0^\infty \preceq \mathbb{B}$ and let $\mathbb{A} = \mathbb{B}^n$. Recall that $\mathcal{MPT}_0^\infty$ has $x \wedge (y \vee z)$ as a generating operation, and so this is an operation of $\mathbb{A}$. Observe that $x \wedge y = x \wedge (y \vee y)$, so $\mathbb{A}$ also has $x \wedge y$ as an operation. Define term operations of $\mathbb{A}$,

$$\begin{aligned}
&J_1(x,y,z) \coloneqq x \wedge (y \vee z), \qquad && J_2(x,y,z) \coloneqq x \wedge z,\\
&J_3(x,y,z) \coloneqq z \wedge (x \vee y).
\end{aligned}$$

It is an easy exercise to show that these terms satisfy the identities above and are hence Jónsson terms. It follows that $\mathbb{A}$ is congruence distributive. □

Returning again to the fragment of Post's Lattice in Figure 3, we are left to analyze the central diamond of clones between $\mathcal{AP}$ and $\mathcal{A}$. The next lemma allows us to apply Theorem 4.5 to these clones.

Lemma 4.8. *Let $\mathbb{B}$ be a 2-element algebra such that $\mathcal{AP} = \mathbb{B}$ and let $\mathbb{A} = \mathbb{B}^n$. If θ is a congruence of $\mathbb{A}$ then θ is also a congruence of the group $\mathbb{Z}_2^n$.*

Proof. The clone $\mathcal{AP}$ has ternary addition, $x + y + z$, as its generating operation (see Figure 1). In order to show that θ is a congruence of $\mathbb{Z}_2^n$, it is sufficient to show that the set θ is closed under binary addition. Let $(a, a'), (b, b') \in \theta$. We have

$$a + b = (a + b + 0)\ \theta\ (a' + b' + 0) = a' + b',$$

and hence $(a + a', b + b') \in \theta$, as desired. □

We are now ready to prove Theorem 4.1, which we started the section with. The proof splits into two portions, depending on whether the algebra in question has clone contained in one of the infinite "wings" or whether it is above the bottom of the central diamond.

Theorem 4.1 (redux)**.** *Let $\mathbb{B}$ be a 2-element algebra such that one of*

1. $\mathcal{MPT}_0^\infty \preceq \mathbb{B}$,
2. $\mathcal{MPT}_1^\infty \preceq \mathbb{B}$, *or*
3. $\mathcal{AP} \preceq \mathbb{B}$

holds and let $\mathbb{A} = \mathbb{B}^n$. The quantum circuit $\mathfrak{s}_\varphi(n)$ of Definition 3.2 solves HKP($\mathbb{A}$) *with probability $1 - 1/\tau$ in $\Theta(n + \lg(\tau))$ iterations.*

Proof. Consider an instance of the HKP($\mathbb{A}$) with homomorphism $\varphi : \mathbb{A} \to \mathbb{X}$. If $\mathcal{MPT}_0^\infty \preceq \mathbb{B}$ or $\mathcal{MPT}_1^\infty \preceq \mathbb{B}$, then $\mathbb{B}$ is congruence distributive. By Lemma 4.6, $\ker(\varphi)$ is therefore the kernel of a projection. All such kernels are also congruences of $\mathbb{Z}_2^n$. If, on the other hand, $\mathcal{AP} \preceq \mathbb{B}$, then by Lemma 4.8 and Observation 3.1, we have that the congruence $\ker(\varphi)$ of $\mathbb{A}$ is also a congruence of the group $\mathbb{Z}_2^n$.

Theorem 4.5 therefore applies in all cases, so $\ker(\varphi)$ can be calculated with probability $1 - 1/\tau$ in $\Theta(n + \lg(\tau))$ iterations of the circuit. □

5 The HKP and Post's Lattice: Hardness

The previous section presented quantum and classical algorithms for the HKP on the infinite upper portion of Post's Lattice. In this section, we establish quantum and classical hardness results for the remaining clones. The main classical result is Theorem 5.1 and the main quantum result is Theorem 5.2, stated below.

Theorem 5.1. *Let $\mathbb{B}$ be a 2-element algebra such that one of*

1. $\mathbb{B} \leq \bigwedge$,
2. $\mathbb{B} \leq \bigvee$, *or*
3. $\mathbb{B} \leq \mathcal{A}$

holds, and let $\mathbb{A} = \mathbb{B}^n$. Any classical algorithm which solves $\mathrm{HKP}(\mathbb{A})$ *must make $\Omega(2^{n/2})$ queries to the oracle.*

Theorem 5.2. *Let $\mathbb{B}$ be a 2-element algebra such that one of*

1. $\mathbb{B} \leq \bigwedge$,
2. $\mathbb{B} \leq \bigvee$, *or*
3. $\mathbb{B} \leq \mathcal{U}$

holds, and let $\mathbb{A} = \mathbb{B}^n$. Any quantum algorithm which solves $\mathrm{HKP}(\mathbb{A})$ *must make $\Omega((1+\varepsilon)^n)$ queries to the oracle for $0 < \varepsilon < 1$.*

The best way to summarize these two results is in terms of Post's Lattice, see Figure 4. In particular, powers of algebras whose clones are contained in the interval between $\mathcal{AP}$ and $\mathcal{A}$ have HKP which exhibits super-polynomial speedup using a quantum algorithm. Clones which are below $\mathcal{U}$, $\bigwedge$, or $\bigvee$ have HKP for which no polynomial-time quantum algorithm exists. Combined with the results of the previous section, this provides a complete quantum and classical classification of the complexity of the HKP for powers of 2-element algebras.

The remainder of the section is devoted to proving Theorems 5.1 and 5.2. The proof technique relies on various counting arguments and a close analysis of congruence generation in different algebras. The primary tool we use is a result due to Maltsev [12], commonly called a "Maltsev chain".

Definition 5.3. Let $\mathbb{A}$ be an algebra and $X \subseteq A^2$. If $\alpha, \beta \in A$ are such that there exists an m-ary term operation t and pairs $(a_1, b_1), \ldots, (a_m, b_m) \in X \cup \mathbf{0}$ with

$$\{\alpha, \beta\} = \{t(a_1, \ldots, a_m), t(b_1, \ldots, b_m)\}$$

then we will write $\alpha \rightsquigarrow \beta$. A *Maltsev chain* between α and β is a sequence $\lambda_0, \ldots, \lambda_n \in A$ such that

$$\alpha = \lambda_0 \rightsquigarrow \lambda_1 \rightsquigarrow \cdots \rightsquigarrow \lambda_n = \beta,$$

written $\alpha \rightsquigarrow^n \beta$.

Proposition 5.4 (Maltsev [12])**.** *Let $\mathbb{A}$ be an algebra, $X \subseteq A^2$, and $\theta = \mathrm{Cg}(X)$. Then $(\alpha, \beta) \in \theta$ if and only if $\alpha \rightsquigarrow^n \beta$ for some n.*

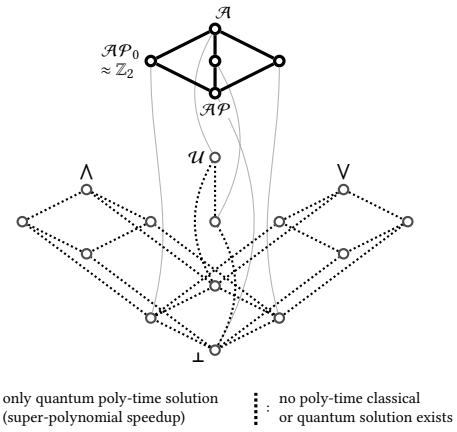


Figure 4. The fragment of Post's Lattice for which no classical polynomial-time algorithm for the HKP exists (whole diagram). Dotted lines indicate clones for which no polynomial-time quantum algorithm exists, while bold lines indicate clones for which no polynomial-time classical algorithm exists, but a polynomial-time quantum algorithm does exist (i.e. those clones which exhibit super-polynomial speedup).

We begin by proving that if $\mathbb{B} \leq \bigwedge$ or $\mathbb{B} \leq \bigvee$, then exponentially-many queries to the oracle are necessary to solve the HKP for powers of $\mathbb{B}$ for both classical and quantum algorithms. This proves items 1 and 2 of Theorems 5.1 and 5.2. The proof of this is contained in the following lemma, combined with Observation 3.1.

Lemma 5.5. *Let $\mathbb{B}$ be a 2-element algebra such that* $\mathrm{Clo}(\mathbb{B}) = \bigwedge$ *or* $\mathrm{Clo}(\mathbb{B}) = \bigvee$ *and let $\mathbb{A} = \mathbb{B}^n$. Any algorithm (classical or quantum) solving* $\mathrm{HKP}(\mathbb{A})$ *must make $\Omega((1+\varepsilon)^n)$ queries to the oracle for $0 < \varepsilon < 1$.*

Proof. We will present the argument for $\mathrm{Clo}(\mathbb{B}) = \bigwedge$. The argument for $\mathrm{Clo}(\mathbb{B}) = \bigvee$ is analogous. The clone $\bigwedge$ has $x \wedge y$ amongst its generating operations (see Figure 1). The set $\{0, 1\}$ has a natural order (namely $0 \leq 1$), and this can be extended to an ordering on $\{0, 1\}^n$. The operation of $\wedge$ is compatible with this order: $x \wedge y = x$ if and only if $x \leq y$.

Define a set of $\leq$-incomparable elements of $\{0, 1\}^n$,

$$M = \{a \in A \mid \text{exactly } \lfloor n/2 \rfloor \text{ coordinates of } a \text{ are } 0\}$$

and choose arbitrary $Z \subseteq M$. Let θ_Z be the smallest congruence of $\mathbb{A}$ with Z^2 contained in a single equivalence class — that is, $\theta_Z := \mathrm{Cg}(Z^2)$. We will carefully analyze the generation of θ_Z via a series of claims.

Claim. *Let $X \subseteq A^2$ and $\theta = \mathrm{Cg}(X)$. If $\alpha\ \theta\ \beta$ and $\alpha \neq \beta$ then there is $(a, b) \in X$ with $\alpha \leq a$ or $\alpha \leq b$.*

Proof of claim. By Proposition 5.4, there is an m-ary term operation t and pairs $(a_1, b_1), \ldots, (a_m, b_m) \in X \cup \mathbf{0}$ such that $\alpha \in \{t(a_1, \ldots, a_m), t(b_1, \ldots, b_m)\}$. Each term operation of $\mathbb{B}$ (and hence $\mathbb{A}$) can be written

$$t(x_1, \ldots, x_m) = x_{i_1} \wedge \cdots \wedge x_{i_k}$$

where $\{i_1, \ldots, i_k\} \subseteq [m]$. The claim follows. ∘

Claim. *If $z \in Z$ and $\gamma > z$ then $(z, \gamma) \notin \theta_Z$.*

Proof of claim. Suppose towards a contradiction that $z\ \theta_Z\ \gamma$. By the first claim, there must be some $z' \in Z$ such that $\gamma \leq z'$. This implies that $z < z'$, but since $Z \subseteq M$ and M consists of $\leq$-incomparable elements, this is impossible. ∘

Claim. *If $X \subseteq A^2$ is such that $\theta_Z = \mathrm{Cg}(X)$, then $|Z| \leq |X|$.*

Proof of claim. By the first claim, for each $z \in Z$ there is some $(a_z, b_z) \in X$ with (without loss of generality) $z \leq a_z$. We argue that each a_z is distinct and thus $|Z| \leq |X|$.

Suppose that there are distinct $z, z' \in Z$ such that $a_z = a_{z'}$. Summarizing our assumptions,

$$(a_z, b_z) \in X \subseteq \mathrm{Cg}(X) = \theta_Z = \mathrm{Cg}(Z^2).$$

Applying the first claim with Z in place of X yields some $u \in Z$ such that $b_z \leq u$. Since $(a_z, b_z), (z, u) \in \theta_Z$, we have

$$z = \big(a_z \wedge z\big)\ \theta_Z\ \big(b_z \wedge u\big) = b_z$$

and hence $a_z\ \theta_Z\ z$. The second claim together with $z \leq a_z$ now yields a contradiction unless $z = a_z$. The same argument for z' then gives us $z = a_z = a_{z'} = z'$, contradicting z and z' being distinct and finishing the proof of the claim. ∘

From the claim above, determining the congruence θ_Z requires specifying at least $|Z|$-many elements. Using Stirling's approximation, we have

$$|M| = \binom{n}{n/2} = \frac{n!}{\big((n/2)!\big)^2} \approx \frac{\sqrt{n}(n/e)^n}{\big(\sqrt{n}(n/(2e))^{n/2}\big)^2} = \frac{2^n}{\sqrt{n}},$$

where the "$\approx$" symbol means that both sides have the same Θ-complexity class. There are thus exponentially-many subsets Z with $|Z| \in \Omega((1+\varepsilon)^n)$ for $0 < \varepsilon < 1$. Any algorithm (quantum or classical) for solving $\mathrm{HKP}(\mathbb{A})$ must distinguish between these subsets, and by the previous claim this requires specifying at least $|Z|$-many elements. □

In order to complete the proof of Theorem 5.1, which we opened the section with, we need only prove item 3: for all $\mathbb{B} \leq \mathcal{A}$, the HKP for powers of $\mathbb{B}$ *classically* requires exponentially-many oracle queries. The proof of this is contained in the following lemma, combined with Observation 3.1.

Lemma 5.6. *Let $\mathbb{B}$ be a 2-element algebra with $\mathrm{Clo}(\mathbb{B}) = \mathcal{A}$ and let $\mathbb{A} = \mathbb{B}^n$. Any classical (resp. probabilistic) algorithm solving $\mathrm{HKP}(\mathbb{A})$ must make $\Omega(2^n)$ (resp. $\Omega(2^{n/2})$) queries to the oracle.*

Proof. The clone $\mathcal{A}$ has the operation $x \leftrightarrow y$ as a generating operation (see Figure 1). Choose a random $z \in A \setminus \{0^n\}$ and define θ_z to be the congruence generated by relating 0^n and z,

$$\theta_z \coloneqq \mathrm{Cg}(0^n, z).$$

Observe that modulo-2 addition is definable in $\mathcal{A}$ (and hence $\mathbb{B}$ and $\mathbb{A}$) by

$$x + y \coloneqq x \leftrightarrow (0 \leftrightarrow y).$$

Claim. *The congruence θ_z has equivalence classes $x/\theta_z \coloneqq \{x, x+z\}$.*

Proof of claim. Take ψ to be the equivalence relation with the claimed equivalence classes. To prove that ψ is a congruence we need only show that if $a\ \psi\ a'$ and $b\ \psi\ b'$ then

$$(a \leftrightarrow b)\ \psi\ (a' \leftrightarrow b').$$

By the definition of ψ, we have that $a' = a + \varepsilon z$ and $b' = b + \tau z$ for some $\varepsilon, \tau \in \{0, 1\}$. The operation $\leftrightarrow$ is commutative and associative, so using "+" as defined before the claim, we have

$$\begin{aligned}(w + x) \leftrightarrow y &= w \leftrightarrow 0 \leftrightarrow x \leftrightarrow y \\ &= w \leftrightarrow 0 \leftrightarrow y \leftrightarrow x = (w + y) \leftrightarrow x.\end{aligned}$$

Thus $(w + x) \leftrightarrow y = (w + y) \leftrightarrow x$. Using this identity twice,

$$\begin{aligned}a' \leftrightarrow b' &= (a + \varepsilon z) \leftrightarrow (b + \tau z) \\ &= \big(a \leftrightarrow (b + \tau z)\big) + \varepsilon z = (a \leftrightarrow b) + (\varepsilon + \tau) z.\end{aligned}$$

Addition is defined modulo 2, so $\varepsilon + \tau \in \{0, 1\}$ and we have $(a \leftrightarrow a)\ \psi\ (a' \leftrightarrow b')$, as desired. The congruence θ_z is minimal and contains ψ, so $\theta_z = \psi$. ∘

We will now show that it is exponentially hard for a classical algorithm to distinguish between θ_z and the identity congruence $\mathbf{0}$ for randomly chosen z. Let φ be the homomorphism

$$\begin{aligned}\varphi : \mathbb{A} &\to \mathbb{A}/\theta_z, \\ a &\mapsto a/\theta_z,\end{aligned}$$

so that $\ker(\varphi) = \theta_z$.

Suppose that we have a classical procedure for solving $\mathrm{HKP}(\mathbb{A})$, and that this procedure evaluates φ on a subset $E = \{e_1, \ldots, e_\ell\} \subseteq A$. We are able to distinguish θ_z from $\mathbf{0}$ if and only if $|\varphi(E)| < |E|$. By the claim above, for distinct $e_i, e_j \in E$, we have that $\varphi(e_i) = \varphi(e_j)$ if and only if $e_i = e_j + z$. The element z was chosen randomly, so the probability of this occurring is $1/(|\mathbb{A}| - 1)$. It follows that for fixed j, the probability that $e_i = e_j + z$ for some $i < j$ is

$$\mathrm{P}\left(\exists i < j\ \big[e_i = e_j + z\big]\right) = \frac{j-1}{|\mathbb{A}| - 1}.$$

Therefore the probability that for some distinct $e_i, e_j \in E$ we have $e_i = e_j + z$ (equivalently, $|\varphi(E)| < |E|$) is

$$\begin{aligned}\mathrm{P}\left(|\varphi(E)| < |E|\right) &= \mathrm{P}\left(\exists i, j\ \big[e_i = e_j + z\big]\right) \\ &= \sum_{j=1}^{|E|} \mathrm{P}\left(\exists i < j\ \big[e_i = e_j + z\big]\right) = \sum_{j=1}^{|E|} \frac{j-1}{|\mathbb{A}| - 1} \\ &= \frac{|E|(|E| - 1)}{2(|\mathbb{A}| - 1)}.\end{aligned}$$

Thus, the only way for a classical algorithm to correctly distinguish θ_z from $\mathbf{0}$ with probability at least $1/2$ is by making

$|E| \in \Omega(|\mathbb{A}|^{1/2}) = \Omega(2^{n/2})$ evaluations of φ. To be correct with probability 1 requires $|E| \in \Omega(2^n)$ evaluations. □

We now complete the proof of Theorem 5.2 from the start of the section. It remains to prove the last item of that theorem, that for all $\mathbb{B} \preceq \mathcal{U}$, the HKP for powers of $\mathbb{B}$ requires exponentially-many oracle queries for a *quantum* algorithm. Observation 3.1 together with the next lemma establish this.

Lemma 5.7. *Let $\mathbb{B}$ be a 2-element algebra with $\mathrm{Clo}(\mathbb{B}) = \mathcal{U}$ and let $\mathbb{A} = \mathbb{B}^n$. Any algorithm (classical or quantum) solving $\mathrm{HKP}(\mathbb{A})$ must make $\Omega(2^n)$ queries to the oracle.*

Proof. The clone $\mathcal{U}$ has $\neg x$ amongst its generating operations (see Figure 1). Partition A into four disjoint sets of equal size, A_0, B_0, A_1, B_1, such that

$$A_1 = \neg A_0 = \{\neg a \mid a \in A_0\}, \qquad B_1 = \neg B_0 = \{\neg b \mid b \in B_0\}.$$

Enumerate the elements of A_0 and B_0 as $a_1, \ldots, a_{2^{n-2}}$ and $b_1, \ldots, b_{2^{n-2}}$ respectively. Define $C = \{(a_i, b_i) \mid i \in [2^{n-2}]\}$. Finally, for each subset $Y \subseteq C$ let $\theta_Y = \mathrm{Cg}(Y)$.

We will show that all the θ_Y are distinct and that specifying θ_Y by generators requires finding a set of size $|Y|$. There are $\Omega(2^n)$-many distinct Y of size $\Omega(2^n)$, so this is sufficient to prove the lemma.

Claim. *Suppose that $Y = \{(a_i, b_i) \mid i \in I\} \subseteq C$ for some $I \subseteq [2^{n-2}]$. Then*

$$\theta_Y = \mathbf{0} \cup Y \cup Y^\partial \cup (\neg Y) \cup (\neg Y)^\partial$$

where $\neg Y \coloneqq \{(\neg a_i, \neg b_i) \mid i \in I\}$ and $Z^\partial \coloneqq \{(y, x) \mid (x, y) \in Z\}$ for $Z \subseteq A^2$.

Proof of claim. Let $\psi = \mathbf{0} \cup Y \cup Y^\partial \cup (\neg Y) \cup (\neg Y)^\partial$. The congruence θ_Y is the least congruence containing Y, so $\psi \subseteq \theta_Y$. In order to show that $\psi = \theta_Y$, it is therefore enough to show that ψ is closed under the operation of $\neg$. This is clear from the construction of ψ. ○

By the above claim, each distinct $Y \subseteq C$ determines a distinct θ_Y, and specifying θ_Y requires producing a subset of size $|Y|$. Since there are $\Omega(2^n)$-many distinct Y of size $\Omega(2^n)$, the conclusion of the lemma follows. □

6 Conclusion

Combining Theorem 4.1, Corollary 4.2, Theorem 5.1, and Theorem 5.2 provides a complete classification of the quantum and classical algorithmic complexity of $\mathrm{HKP}(\mathbb{B}^n)$, where $\mathbb{B}$ is a 2-element algebra. This classification is summarized in the theorem below and in Figure 5.

Theorem 6.1. *Let $\mathbb{B}$ be a 2-element algebra.*

1. *If $\mathcal{MPT}_0^\infty \preceq \mathbb{B}$, $\mathcal{MPT}_1^\infty \preceq \mathbb{B}$, or $\mathcal{DM} \preceq \mathbb{B}$, then there exist both classical and quantum polynomial-time algorithms for $\mathrm{HKP}(\mathbb{B}^n)$.*
2. *If $\mathcal{AP} \preceq \mathbb{B} \preceq \mathcal{A}$, then a quantum polynomial-time algorithm solving $\mathrm{HKP}(\mathbb{B}^n)$ exists. Furthermore, no classical polynomial-time algorithm for $\mathrm{HKP}(\mathbb{B}^n)$ exists.*

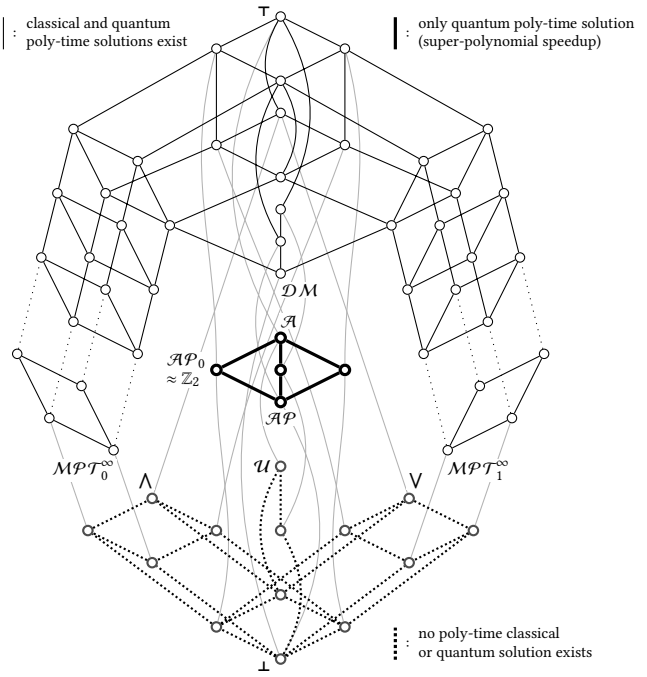


Figure 5. Diagram of Post's Lattice. The HKP for powers of clones in bold have a efficient quantum solution, but no efficient classical solution (i.e. they exhibit super-polynomial speedup). Powers of clones in plain lines have polynomial-time classical and quantum solutions to their HKPs, while powers of clones indicated with dotted lines have neither classical nor quantum polynomial-time solutions to their respective HKPs. The clone of the group $\mathbb{Z}_2$ is indicated.

3. *If $\mathbb{B} \preceq \bigwedge$, $\mathbb{B} \preceq \bigvee$, or $\mathbb{B} \preceq \mathcal{U}$ then no quantum or classical polynomial-time algorithm for $\mathrm{HKP}(\mathbb{B}^n)$ exists.*

This classification can be seen as a broad extension of the results of Simon [19], which are included in item 2 of the theorem when $\mathbb{B} = \mathbb{Z}_2$.

There are many open questions surrounding the Hidden Kernel Problem, a few of which we detail below. Theorems 6.1 and 5.1 state that both classically and using a quantum algorithm, $\mathrm{HKP}(\mathbb{A})$ is either in P or EXP when $\mathbb{A}$ is the power of a 2-element algebra.

Question. For *arbitrary* fixed finite algebras $\mathbb{A}$, precisely which complexity classes (quantum or classical) are parameterized by $\mathrm{HKP}(\mathbb{A})$?

Turning this problem around, we can instead ask for algebraic properties which enforce the existence of an efficient quantum solution to $\mathrm{HKP}(\mathbb{A}^n)$.

Question. Consider $\mathrm{HKP}(\mathbb{A}^n)$, where $\mathbb{A}$ is an arbitrary finite algebra. What structural conditions on $\mathbb{A}$ ensure that $\mathrm{HKP}(\mathbb{A}^n)$ always admits a polynomial-time quantum solution?

In an algebra $\mathbb{A}$, the term operation $t(x_1, \ldots, x_n)$ is said to be a *cube term* if for every $i \in [n]$ there is a choice of $u_1, \ldots, u_n \in \{x, y\}$ with $u_i = y$ such that the equation $t(u_1, \ldots, u_n) = x$ holds in $\mathbb{A}$. The clone $\mathcal{AP}$ has a cube term given by $x + y + z$ and $\mathcal{DM}$ has a cube term given by $\mathrm{maj}(x, y, z)$. More generally, every group has a cube term given by $xy^{-1}z$.

The study of cube terms originated with algebraic approach to the *Constraint Satisfaction Problem (CSP)* in [2], and the existence of a cube term for $\mathbb{A}$ is associated with some quite strong regularity conditions on the structure of powers of $\mathbb{A}$.

If $\mathbb{A}$ has a cube term, then subalgebras of $\mathbb{A}^n$ have a generating set which is bounded by a polynomial in n. This applies in particular to congruences of $\mathbb{A}^n$. It follows that if $\mathbb{A}$ has a cube term, then counting arguments similar to those in the proofs of Lemmas 5.5 and 5.7 will not be sufficient to rule out the existence of a quantum algorithm. This leads us to conjecture the following.

Conjecture. *If $\mathbb{A}$ has a cube term, then* $\mathrm{HKP}(\mathbb{A}^n)$ *has an efficient quantum solution.*

As mentioned above, every group has a cube term. An efficient quantum solution to the above conjecture would therefore restrict to an efficient quantum solution to the hidden normal subgroup problem.

References

[1] Dave Bacon, Andrew M Childs, and Wim van Dam. 2005. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05)*. IEEE, 469–478.

[2] Joel Berman, Paweł Idziak, Petar Marković, Ralph McKenzie, Matthew Valeriote, and Ross Willard. 2010. Varieties with few subalgebras of powers. *Trans. Amer. Math. Soc.* 362, 3 (2010), 1445–1473. https://doi.org/10.1090/S0002-9947-09-04874-0

[3] Aaron Denney, Cristopher Moore, and Alexander Russell. 2010. Finding conjugate stabilizer subgroups in PSL (2; q) and related groups. *Quantum Information & Computation* 10, 3 (2010), 282–291.

[4] Paul Adrien Maurice Dirac. 1939. A new notation for quantum mechanics. In *Mathematical Proceedings of the Cambridge Philosophical Society*, Vol. 35. Cambridge University Press, 416–418.

[5] Dmitry Gavinsky. 2004. Quantum solution to the hidden subgroup problem for poly-near-Hamiltonian groups. *Quantum Information & Computation* 4, 3 (2004), 229–235.

[6] Sean Hallgren. 2007. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *Journal of the ACM (JACM)* 54, 1 (2007), 4.

[7] Gábor Ivanyos, Frédéric Magniez, and Miklos Santha. 2003. 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.

[8] Gábor Ivanyos, Luc Sanselme, and Miklos Santha. 2007. An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups. In *Annual Symposium on Theoretical Aspects of Computer Science*. Springer, 586–597.

[9] Gábor Ivanyos, Luc Sanselme, and Miklos Santha. 2008. An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. In *Latin American Symposium on Theoretical Informatics*. Springer, 759–771.

[10] Bjarni Jónsson. 1967. Algebras whose congruence lattices are distributive. *Math. Scand.* 21 (1967), 110–121 (1968). https://doi.org/10.7146/math.scand.a-10850

[11] Alexei Kitaev. 1996. Quantum measurements and the Abelian stabilizer problem. In *Electronic Colloq. on Computational Complexity*.

[12] A. I. Mal'cev. 1954. On the general theory of algebraic systems. *Mat. Sb. N.S.* 35(77) (1954), 3–20.

[13] Ralph N. McKenzie, George F. McNulty, and Walter F. Taylor. 1987. *Algebras, lattices, varieties. Vol. I.* Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA. xvi+361 pages.

[14] Cristopher Moore, Daniel Rockmore, Alexander Russell, and Leonard J Schulman. 2004. The power of basis selection in Fourier sampling: Hidden subgroup problems in affine groups. In *Proceedings of the fifteenth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics, 1113–1122.

[15] Michael A Nielsen and Isaac L Chuang. 2000. Quantum computation and quantum information.

[16] Emil L. Post. 1941. *The Two-Valued Iterative Systems of Mathematical Logic*. Princeton University Press, Princeton, N. J. viii+122 pages.

[17] Martin Roetteler and Thomas Beth. 1998. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. *arXiv preprint quant-ph/9812070* (1998).

[18] Peter W Shor. 1994. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 124–134.

[19] Daniel R Simon. 1997. On the power of quantum computation. *SIAM journal on computing* 26, 5 (1997), 1474–1483.

[20] Jonathan D. H. Smith. 1976. *Mal'cev varieties*. Springer-Verlag, Berlin-New York. viii+158 pages.

[21] Walter Taylor. 1993. Abstract clone theory. In *Algebras and orders (Montreal, PQ, 1991)*. NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., Vol. 389. Kluwer Acad. Publ., Dordrecht, 507–530.