Check for updates

ACM DIGITAL LIBRARY | Association for Computing Machinery | acm open

Latest updates: https://dl.acm.org/doi/10.1145/2869073

PDF Download
2869073.pdf
03 February 2026
Total Citations: 6
Total Downloads: 487

Published: 04 May 2016
Accepted: 01 December 2015
Revised: 01 September 2015
Received: 01 December 2011

Citation in BibTeX format

RESEARCH-ARTICLE

Computational Complexity of Quantum Satisfiability

CHRISTIAN HERRMANN, Technical University of Darmstadt, Darmstadt, Hessen, Germany

MARTIN ZIEGLER, Korea Advanced Institute of Science and Technology, Daejeon, South Korea

Open Access Support provided by:

Technical University of Darmstadt

Korea Advanced Institute of Science and Technology

Computational Complexity of Quantum Satisfiability

CHRISTIAN HERRMANN and MARTIN ZIEGLER, TU Darmstadt and KAIST

We connect both discrete and algebraic complexity theory with the satisfiability problem in certain non-Boolean lattices.

Specifically, quantum logic was introduced in 1936 by Garrett Birkhoff and John von Neumann as a framework for capturing the logical peculiarities of quantum observables: in the 1D case it coincides with Boolean propositional logic but, starting with dimension two, violates the distributive law.

We introduce the weak and strong satisfiability problem for quantum logic propositional formulae. It turns out that in dimension two, both are also $\mathcal{NP}$–complete.

For higher-dimensional spaces $\mathbb{R}^d$ and $\mathbb{C}^d$ with $d \geq 3$ fixed, on the other hand, we show both problems to be complete for the nondeterministic Blum-Shub-Smale (BSS) model of real computation. This provides a unified view on both Turing and real BSS complexity theory, and extends the (still relatively scarce) list of problems established $\mathcal{NP}_{\mathbb{R}}$–complete with one, perhaps, closest in spirit to the classical Cook-Levin Theorem. More precisely, strong satisfiability of $\bigwedge\bigvee\bigwedge$–terms is complete, while that of $\bigwedge\bigvee$–terms (i.e., those in conjunctive form) can be decided in polynomial time in dimensions $d \geq 2$.

The decidability of the infinite-dimensional case being still open, we proceed to investigate the case of indefinite finite dimensions. Here, weak satisfiability still belongs to $\mathcal{NP}_{\mathbb{R}}$ and strong satisfiability is still hard; the latter, in fact, turns out as polynomial-time equivalent to the feasibility of noncommutative integer polynomial equations over matrix rings.

Categories and Subject Descriptors: F.4.1 [**Mathematical Logic and Formal Languages**]: Computational Logic; F.1.3 [**Computation by Abstract Devices**]: Complexity Measures and Classes

General Terms: Theory

Additional Key Words and Phrases: Quantum logic, existential theory of the reals, Blum-Shub-Smale model, computational complexity, satisfiability

ACM Reference Format:
Christian Herrmann and Martin Ziegler. 2016. Computational complexity of quantum satisfiability. J. ACM 63, 2, Article 19 (May 2016), 31 pages.
DOI: http://dx.doi.org/10.1145/2869073

1. INTRODUCTION

Quantum physics is famous for its seemingly paradoxical (yet very real) effects. Shaping them into a mathematically sound physical theory was a big achievement of the last century [Neumann 1955]. There, physical *observables* correspond to linear self-adjoint operators on some Hilbert space $\mathcal{H}$; and *properties* (i.e., observables attaining

This work was started under support of the *German Research Foundation* DFG with grant Zi 1009/2-1 and completed under grant Zi 1009/4-1. The authors thank Arno Pauly, Micheale Susan Roddy, Marina Semenova, Peter Scheiblechner, and Karl Svozil for helpful discussions. Further gratitude is due to anonymous referees for helpful suggestions on improvement from the earlier version [Herrmann and Ziegler 2011].
Authors' addresses: C. Herrmann, Dept. of Mathematics, TU Darmstadt, Schlossgartenstrasse 7, 64289 Darmstadt, Germany; email: herrmann@mathematik.tu-darmstadt.de; M. Ziegler, School of Computing, KAIST, Daehak-ro 291, 34141 Daejeon, Rep. of Korea; email: m@zie.de.
Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, to redistribute to lists, or to use any component of this work in other works requires prior specific permission and/or a fee. Permissions may be requested from Publications Dept., ACM, Inc., 2 Penn Plaza, Suite 701, New York, NY 10121-0701 USA, fax +1 (212) 869-0481, or permissions@acm.org.
© 2016 ACM 0004-5411/2016/05-ART19 $15.00
DOI: http://dx.doi.org/10.1145/2869073

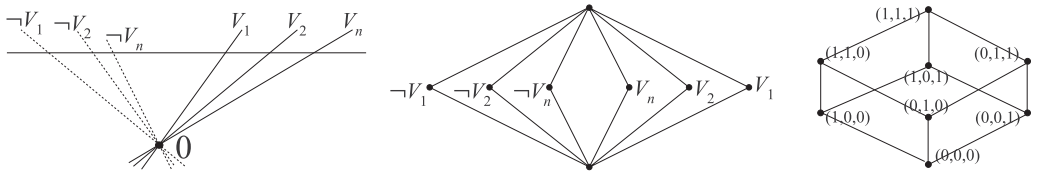

Fig. 1. Prototype $\mathcal{MO}_n$ of a non-distributive modular ortholattice—left: as sublattice of $\mathrm{L}(\mathbb{R}^2)$, mid: its Hasse diagram, right: Hasse diagram of the Boolean ortholattice $\{0,1\}^3$.

only (eigen)values 0 or 1) to projection operators—which, in turn, can be identified with closed subspaces of $\mathcal{H}$. Their logical features (reflecting non-commutativity of operators) have been captured [Mackey 1963; Piron 1964; Beltrametti et al. 1984] as abstract properties of the *ortholattice* $\mathrm{L}(\mathcal{H})$ of closed subspaces of $\mathcal{H}$, equipped with the connectives *meet*, *complement*, and *join*:

$$\wedge\colon \mathrm{L}(\mathcal{H}) \times \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}),\ (U,V) \mapsto U \cap V$$
$$\neg\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}),\ U \mapsto U^{\perp} = \{\vec{x} \in \mathcal{H} \mid \forall \vec{u} \in U.\ \langle \vec{x} \mid \vec{u} \rangle = 0\},$$
$$\vee\colon \mathrm{L}(\mathcal{H}) \times \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}),\ (U,V) \mapsto (U \cup V)^{\perp\perp}$$

and, in addition, with the constants $\mathbf{0} := \{\vec{0}\} \in \mathrm{L}(\mathcal{H})$ and $\mathbf{1} := \mathcal{H} \in \mathrm{L}(\mathcal{H})$. Subset containment $\subseteq$ as a partial order on $\mathrm{L}(\mathcal{H})$ recovers $\vee$ as least upper bound and $\wedge$ as greatest lower bound.

While the above refers to infinite dimensional spaces, primarily, newer developments, like categorical quantum mechanics [Abramsky and Coecke 2004], focus on finite dimensional spaces [Harding 2009] and find their companions in quantum information and computation [Coecke et al. 2000]. In fact, the $\mathrm{L}(\mathcal{H})$ with $\dim(\mathcal{H}) < \infty$ had been the subject of the seminal work [Birkhoff and Von Neumann 1936] on quantum logic, a point of view revived by Dunn et al. [2005]. Of course, by choice of an orthonormal basis, these $\mathcal{H}$ may be identified with the vector spaces $\mathbb{C}^d$ endowed with the canonical scalar product $\langle \vec{x} \mid \vec{y} \rangle = \sum_{i=1}^{d} x_i^{\dagger} y_i$, where $\mathbb{C}$ is the field of complex numbers and $x^{\dagger}$ is the conjugate of x.

Slightly more generally, we consider the quantum logics $\mathrm{L}(\mathbb{F}^d)$ of all linear subspaces of spaces $\mathbb{F}^d$ with inherited scalar product, where $\mathbb{F}$ denotes a subfield of $\mathbb{C}$ closed under conjugation. This includes the fields $\mathbb{R}$ of reals, $\mathbb{A}$ of algebraic numbers, and $\mathbb{Q}$ of rationals[1]. Let $\dim(U)$ denote the dimension of $U \in \mathrm{L}(\mathbb{F}^d)$. Observe that, due to the finite dimension, $U = U^{\perp\perp}$ and $U \vee V = U + V$ for all $U, V \in \mathrm{L}(\mathbb{F}^d)$. Our main concern will be to algorithmically recover the ring $\mathbb{F}$ from the orthologic L; formally: to establish an interpretation [Tarski 1953, Section I.4], [Hodges 1993, Section 5.3] aka semantic embedding [Burris and Sankappanavar 1981, Section V.5] aka transduction [Grohe 2012, Section 2.4]: a generalization, well known in Logic, of the notion of a reduction that respects not (just propositional) truth but values (in structures) (see Section 2 below).

Example 1.1. *In case $d = 1$, $\mathrm{L}(\mathbb{F}^d) = \{\mathbf{0}, \mathbf{1}\}$ coincides with the set of Boolean truth values. However, starting with dimension 2, the distributive law "$X \vee (Y \wedge Z) = (X \wedge Y) \vee (X \wedge Z)$" generally fails: consider, e.g., $X := \{(t,t) : t \in \mathbb{F}\} \in \mathrm{L}(\mathbb{F}^d)$, $Y := \{(t,0) : t \in \mathbb{F}\} \in \mathrm{L}(\mathbb{F}^d)$, $Z := \{(0,t) : t \in \mathbb{F}\} \in \mathrm{L}(\mathbb{F}^d)$. This is generally seen as one cause underlying the counter-intuitive effects of quantum physics. The lack of distributivity boils down to a (combinatorial) structure $\mathcal{MO}_n$; compare to Figure 1. Observe that $\mathcal{MO}_1 \cong \{\mathbf{0}, \mathbf{1}\}^2$ and that $\mathcal{MO}_n$ embeds into $\mathrm{L}(\mathbb{F}^2)$ for any field $\mathbb{F} \subseteq \mathbb{C}$.*

[1]The standard basis of $\mathbb{F}^d$ is orthonormal, yet most linear subspaces of $\mathbb{Q}^d$ fail to admit any orthonormal basis.

Except for distributivity, the operations $\vee, \wedge, \neg$ on $\mathrm{L}(\mathbb{F}^d)$ satisfy most axioms of Boolean algebra: commutativity, associativity, idempotency $x \wedge (x \vee y) = x = x \vee (x \wedge y)$, and identities $\mathbf{0} \wedge x = \mathbf{0}$, $\mathbf{1} \wedge x = x$, as well as the de Morgan rules, double negation $\neg\neg x = x$, and complementation $x \vee \neg x = \mathbf{1}$ and $x \wedge \neg x = \mathbf{0}$. An abstract structure complying with these laws is denoted by an ortholattice. In particular, on such, one has a partial order defined by $a \geq c$ iff $a = a \vee c$, equivalently $c = a \wedge c$; it follows $x \wedge y = \inf\{x, y\}$, $x \vee y = \sup\{x, y\}$. Both $\mathrm{L}(\mathbb{F}^d)$ and $\mathcal{MO}_m$ still satisfy a weakening of distributivity called the modular law:

$$a \geq c \quad \Rightarrow \quad a \wedge (b \vee c) = (a \wedge b) \vee c. \tag{1}$$

In view of this, we will refer to them as *Modular Ortholattices (MOLs)* (but beware of entering into an axiomatic theory). The study of these as 'domains of propositions' might be termed *modular quantum logic*, intermediate between Boolean and *orthomodular* quantum logic.

1.1. Models of Computation: Quantum Computers and Blum-Shub-Smale Machines

We suppose familiarity with the standard Turing complexity classes of binary decision problems $A \subseteq \{0, 1\}^*$, such as $\mathcal{P}, \mathcal{NP}$, PSPACE, and the notion of (many-one) polynomial-time reduction. By the Cook-Levin Theorem, any $A \in \mathcal{NP}$ reduces to the Boolean satisfiability problem SAT, that is the question of whether a given (suitably encoded) term t over $\vee, \wedge, \neg$ and variables $X_1, \ldots, X_n$ admits an assignment $x_1, \ldots, x_n \in \{\mathbf{0}, \mathbf{1}\}^n$ making $t(x_1, \ldots, x_n)$ evaluate to $\mathbf{1}$.

Quantum computers have been suggested as an alternative (and perhaps more powerful) model of computation. They exploit linearity of quantum mechanics, namely, that its evolution extends from pure states to superpositions. Therefore, a physical system realizing some "computation" on (say, polynomially many) so-called "qubits" also works on linear combinations thereof—simultaneously: quantum parallelism. The difficulty in exploiting this capability algorithmically consists in preparing the superposition and in extracting the output from the resulting state. Quantum logic, on the other hand, as describing operations on observables rather than states, has also been proposed as an approach to computational purposes [Pykacz 2000; Bub 2007; Pavičić 2007] and to computational concepts [Dunn et al. 2005; Ying 2005].

In algebraic complexity, the BSS machine (equivalent to the *real-RAM*) is a common model [Blum et al. 1998] of uniform computation [Bürgisser 2000]. It captures arithmetic on numbers as entities with unit cost per operation; more precisely, its $\mathbb{R}$–version can read, store, operate, compare, and output a constant number of reals in each step.

Definition 1.2. Consider a commutative ring R. A (deterministic) BSS machine $\mathcal{M}$ over R contains a finite number of constants $c \in R$, a register array, and three index registers. It receives as input some finite tuple $\bar{x} \in R^n$ together with its length $n =: |\bar{x}| \in \mathbb{N}$. $\mathcal{M}$ can then apply arithmetic operations $+, -, \times$ (and partial $\div$ in case R is a field, but *no* conjugation $z \mapsto \bar{z}$, even in the complex case[2]) to these x_j, to its pre-stored constants, or to some array elements accessed via index registers, and store the result. It may furthermore branch, based on the test for equality $=, \neq$ (in the case of a ring *equipped* with an order also for $<, \leq, >, \geq$) of two array elements. Each operation/branching is counted for as one step. On a fixed input $\bar{x} \in R^n$, $\mathcal{M}$ may accept, reject, or loop indefinitely. It runs in *polynomial time* if there is a polynomial

[2]This is the standard conception [Blum et al. 1998, Section 2.1], noting that, otherwise, $\mathbb{C}$ would become computationally isomorphic to $\mathbb{R}^2$ and violate the natural differences between algebraic and semi-algebraic geometry [Blum et al. 1998, Section 2.3].

$p(n)$ bounding, in terms of the input length n only, the number of steps $\mathcal{M}$ performs beforeccepting or rejecting.

Compare Blum et al. [1998, Definition 3.1] and compare also, e.g., Poizat [1995, §4.A] or Tucker and Zucker [2001, §3]. Note that operations and comparisons are presumed exact. (As with nondeterministic Turing machines, the importance of BSS machines does not hinge on them being realistic or practical.)

Example 1.3. Gaussian Elimination *for $n \times n$–matrices over a fixed field $\mathbb{F}$ is a typical algorithm for BSS machines over $\mathbb{F}$ with polynomial running time $\mathcal{O}(n^3)$. Here, exact comparisons are employed during pivot search.*

Furthermore, this model commonly underlies algorithms devised, among others, in polynomial system solving [Cox et al. 2007] and in computational geometry [De Berg et al. 2000].

BSS machines over the field $\mathbb{Z}_2 = \{0, 1\}$ can be seen equivalent to Turing machines. Definition 1.2 thus extends the traditional, discrete theory of computation, and has led to a rich, structural-complexity theory [Meer et al. 1997]. In particular, *nondeterministic* BSS machines over R may make and verify guesses from R. Doing so in polynomial time gives rise to the complexity class $\mathcal{NP}_R$, thus, naturally extending the classical question "$\mathcal{P} = \mathcal{NP}$?" to this setting—which has turned out as equally inaccessible [Fournier and Koiran 1998, 2000]. As a matter of fact, both "$\mathcal{P}$ versus $\mathcal{NP}$" *and* "$\mathcal{P}_{\mathbb{C}}$ versus $\mathcal{NP}_{\mathbb{C}}$" are propagated as *Third Problem for the Next Century* [Smale 1998].

Example 1.4. *Fix a commutative*[3] *ring R. The following problem* $\mathrm{FEAS}_{R,R}$ *can be decided by a nondeterministic polynomial-time BSS machine over R, i.e., belongs to $\mathcal{NP}_R$:*

Given ($n \in \mathbb{N}$ and the list of monomials and coefficients of each of) finitely many polynomials $p_1, \ldots, p_k \in R[X_1, \ldots, X_n]$, do they admit a common root in R, i.e., some $\bar{x} \in R^n$, such that $p_1(\bar{x}) = \cdots = p_k(\bar{x}) = 0$?

Indeed, such a machine may simply "guess" an assignment $x_1, \ldots, x_n \in R$ and "verify" it by evaluating the polynomials—clearly possible in a number of steps polynomial in (and noting that n is bounded by) the length of (the descriptions of) the polynomials. $\mathrm{FEAS}_{\mathbb{C},\mathbb{C}}$ is classically characterized by the famous Hilbert's Nullstellensatz in algebraic geometry.

Generalizing the Cook-Levin Theorem, the problem $\mathrm{FEAS}_{R,R}$ has been established BSS-complete for $\mathcal{NP}_R$: for any fixed $\mathbb{L} \in \mathcal{NP}_R$ and machine $\mathcal{M}$ witnessing this, there is a deterministic BSS machine over R which, given $\bar{x} \in R^n$, within time polynomial in $|\bar{x}| = n$, will output an instance of $\mathrm{FEAS}_{R,R}$ that is feasible iff $\bar{x} \in \mathbb{L}$ holds; cmp. [Blum et al. 1989, Main Theorem], [Cucker 1993, Theorem 3.1], and [Blum et al. 1998, Section 5.4]. From these proofs we record the following:

Observation 1.5. *Finite Boolean combinations of rational in-/equalities over a field can be expressed as (the feasibility of a system of) polynomial equations:*

(*a*) $p(\bar{x}) = 0 \ \vee \ q(\bar{x}) = 0 \quad \Leftrightarrow \quad (p^{\times} q)(\bar{x}) = 0$
(*b*) $p(\bar{x}) \neq 0 \quad \Leftrightarrow \quad \exists y : y \cdot p(\bar{x}) - 1 = 0$
(*c*) $p_1(\bar{x})/q_1(\bar{x}) = p_2(\bar{x})/q_2(\bar{x}) \quad \Leftrightarrow \quad (p_1 \cdot q_2 - p_2 \cdot q_1)(\bar{x}) = 0.$
(*d*) Over any subfield of $\mathbb{C}$, it holds $p(\bar{x}) = 0 \ \wedge \ q(\bar{x}) = 0 \quad \Leftrightarrow \quad (p \cdot p^{\dagger} + q \cdot q^{\dagger})(\bar{x}) = 0.$

Note that, other than a BSS machine, even a nondeterministic Turing machine cannot, in general, guess assignments over R in case the ring is infinite; in fact, $\mathrm{FEAS}_{\mathbb{Z},\mathbb{Z}}$ is

[3]Section 4.1 will naturally arrive at considering also noncommutative rings.

undecidable according to Matijasevič [1970]; cmp. Fact 1.11(d), below. Similarly to the *Church-Turing Hypothesis*, this raises the question of how, for various R, the BSS model over R compares to the Turing model. Of course the latter is not fitted to process inputs containing arbitrary, say, real numbers:

EXAMPLE 1.6.

(*a*) *The decision problem* $\{\langle z, \mathrm{bin}(n)\rangle \mid z \in \mathbb{C}, n \in \mathbb{N}, z^n = 1\}$ *for complex roots of unity belongs to* $\mathcal{P}_{\mathbb{C}}$*, but its instances cannot naturally be presented to a Turing machine.*

(*b*) *Instances of* $\mathrm{FEAS}_{R,R}$ *consist of both discrete (e.g., a list of monomials with their multi-degrees) and non-discrete (e.g., coefficients from* R*) information, technically being words from a formal language over alphabet* $\{0, 1\} \cup R$*, while Turing machines are designed for inputs over* $\{0, 1\}$*.*

(*c*) *Moreover, storing the non-recursive constant* $\sum_{\vec{x} \in H} 2^{-\mathrm{bin}(\vec{x})}$ *may be exploited by a BSS machine over* $\mathbb{R}$ *to decide the Halting problem* $H \subseteq \{0, 1\}^*$ *for Turing machines.*

This has suggested restricting to BSS machines with*out* constants—indicated by adding superscript 0 to complexity classes—and to binary instances—called the Boolean part and indicated by the modifier BP [Meer et al. 1997, DEFINITION 3.2] as in the following variant of Example 1.4:

EXAMPLE 1.7. *For* $\mathbb{Z} \subseteq R$*, the following problem,* $\mathrm{FEAS}_{\mathbb{Z},R}$*, belongs to* $\mathrm{BP}(\mathcal{NP}^0_R)$*:*

Given (the coefficients, encoded in binary, of) finitely many polynomials $p_1, \ldots, p_k \in \mathbb{Z}[X_1, \ldots, X_n]$, do they admit a common root in R?

Indeed, no constants are needed for a nondeterministic BSS machine over R to guess an assignment over R and evaluate it on a polynomial from $R[\bar{X}]$, given as input to the machine; thus, $\mathrm{FEAS}_{R,R}$ belongs even to $\mathcal{NP}^0_R$. On the other hand, the machine computing, according to the generalized Cook-Levin Theorem, the reduction from an arbitrary $\mathbb{L} \in \mathcal{NP}_R$ to $\mathrm{FEAS}_{R,R}$ will, in general, employ constants from R if the nondeterministic machine deciding $\mathbb{L}$ in the first place does. Thus, in general, $\mathcal{NP}^0_R$ is not closed under BSS reduction. The following will be crucial for our results.

FACT 1.8.

(*a*) $\mathrm{FEAS}_{R,R}$ *is complete for* $\mathcal{NP}_R$ *under BSS polynomial-time many-one reduction; for short:* $\mathcal{NP}_R$*–complete.*

(*b*) $\mathrm{FEAS}_{\mathbb{Z},R}$ *is complete for* $\mathrm{BP}(\mathcal{NP}^0_R)$ *under Turing polynomial-time many-one reduction; for short:* $\mathrm{BP}(\mathcal{NP}^0_R)$*–complete.*

Fact 1.8(a) has been discussed above. Concerning (b), there is a Turing machine which, given the symbolic description of a non-deterministic polynomial-time constant-free BSS machine $\mathcal{M}$, a polynomial testifying the time bound, "input variables" $\bar{y}$ and "guess variables" $\bar{Z}$ will compute a finite list of polynomials $p_j(\bar{y}, \bar{Z}, \bar{U}) \in \mathbb{Z}[\bar{y}, \bar{Z}, \bar{U}]$, such that for any input $\bar{a}$ and guess $\bar{b}$ in R, the following holds: $\mathcal{M}$ accepts $(\bar{a}, \bar{b})$ iff the polynomials $p_j(\bar{a}, \bar{b}, \bar{U}) \in R[\bar{U}]$ admit a common root in R. Now, put $\bar{X} = (\bar{Z}, \bar{U})$ to obtain $p_j \in \mathbb{Z}[\bar{y}, \bar{X}]$. Cmp. the proof of [Cucker 1993, Theorem 3.1] or [Goode 1994, Theorem 1]. Observe that $p_j(\bar{a}, \bar{X}) \in \mathbb{Z}[X]$ if $\bar{a} \in \{0, 1\}^*$. We also record the following:

OBSERVATION 1.9.

(*a*) *To each* $c \in \mathbb{N}$*, there exists a term* t_c *over* $(1, +, \times)$ *of length* $|t_c| \leq \mathcal{O}(\log c)$ *evaluating to* c *over each ring containing* $\mathbb{N}$*. Moreover, such* t_c *can be computed from* c *in time polynomial in the binary length of* c*.*

(*b*) *Any multivariate polynomial* $p \in R[\bar{X}]$ *can be described (not uniquely) by a ring term* p' *in binary infix operation symbols* $-$ *and* $\times$*, variables* $\bar{X}$*, and the coefficients of* p *as constants.*

In case $R = \mathbb{Z}$*, it suffices to have* $0, 1$ *as constants according to Observation 1.9(a); and a Turing machine can convert* p *to* p' *in time polynomial in the binary input length.*

(*c*) *For* $\mathbb{F}$ *a field, any* $\mathbb{L} \subseteq \mathbb{F}^*$ *decidable by a BSS machine over* $\mathbb{F}$ *can also be decided by one using only the ring operations of* $\mathbb{F}$ *with constant factor slowdown by handling numerators and denominators separately.*

(*d*) $\mathrm{FEAS}_{R,R}$ *is polynomial-time equivalent to* $\mathrm{QUAD}_{R,R}$*: the question of whether a given system of quadratic polynomials over* R *admits a common root over* R*, similarly for* $\mathrm{FEAS}_{\mathbb{Z},R}$ *and* $\mathrm{QUAD}_{\mathbb{Z},R}$.

To keep proofs shorter, we prefer to consider rings with operations $-, \cdot, 0, 1$ since addition can be expressed as $x + y = x - (0 - y)$. In Observation 1.9(b), replace all positive integer coefficients c with terms t_c according to Observation 1.9(a). This, in turn, follows from induction, claiming $|t_c| \leq 2 + 7\log_2(c)$: Indeed, $2c = (1+1) \cdot t_c =: t_{2c}$ and $2c + 1 = (1+1) \cdot t_c + 1 =: t_{2c+1}$ both have length at most $7 + |t_c| \leq 7 + 2 + 7\log_2(c) = 2 + 7\log_2(2c)$ by induction hypothesis. The proof of Observation 1.9(d) employs the well-known technique of intermediate values implicit also, e.g., in the proof of the Cook-Levin-Theorem (cmp. Cucker [1993, p. 403]). It is best explained by an example; a description from the general logical point of view can be found in the work of Hodges [Hodges 1993, Section 2.6.1].

Example 1.10. *Fix some (not necessarily commutative) ring* R *with unit. The evaluation of a* k*-variate polynomial* $p \in R[x_0, x_{-1}, \ldots, x_{-k+1}]$ *decomposes into a series of basic binary operations* $+$*,* $\times$*, and constants (i.e., 0-ary)* $c \in R$*. More precisely, a straight-line program* Γ *of length* N *over* R *calculating* $R^k \ni \bar{r} \to p(\bar{r}) \in R$ *consists of a sequence of assignments "*$x_n := f_n(x_{n_1}, \ldots, x_{n_{k_f}})$*" (*$n = 1, \ldots, N$*), each applying a function* f_n *of arity* $k_{f_n} =: k_n$ *from* R*'s signature to previous intermediate results* x_{n_i} *(*$-k < n_i < n$*), such that* $x_N = p(\bar{x})$ *yields the final result. That is, for each choice of* $r_0, r_{-1}, \ldots, r_{-k+1}, s \in R$*, the following system of equations in variables* $x_1, \ldots, x_N$ *is satisfiable over* R *(and uniquely so), iff* $p(\bar{r}) = s$ *holds:*

$$s = x_N, \quad x_1 = p_1, \quad \ldots, \quad x_N = p_N, \tag{2}$$

where p_n *arises from* $f_n(x_{n_1}, \ldots, x_{n_{k_n}})$ *by substituting the initial values* r_i *for* x_i*,* $i < 1$.

Binary problems raise the question of how BSS machines relate to Turing machines:

Fact 1.11.

(*a*) *It holds* $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{C}}) = \mathrm{BP}(\mathcal{NP}_{\mathbb{C}})$*; see [Michaux 1994,* Proposition *3] or [Blum et al. 1998,* Section *7.4].*

(*b*) *Subject to the* Generalized Riemann Hypothesis*, it holds* $\mathrm{BP}(\mathcal{NP}_{\mathbb{C}}) \subseteq \mathrm{co}\mathcal{RP}^{\mathcal{NP}}$*; cf. Koiran [1996].*

(*c*) *It holds* $\mathcal{NP} \subseteq \mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}}) \subseteq$ PSPACE*; cf., e.g., Grigor'ev [1988], Canny [1988], Heintz et al. [1990], and Renegar [1992].*

(*d*) $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{Z}}) = \mathrm{BP}(\mathcal{NP}_{\mathbb{Z}})$ *coincides with the class of all binary languages recursively enumerable by a Turing machine; cf. Matijasevič [1970].*

(*e*) *The decidability of* $\mathrm{FEAS}_{\mathbb{Q}}$ *is a long-standing open question of extending Hilbert's Tenth Problem from integers to rationals; cf., e.g., Poonen [2009].*

(*f*) $\mathrm{BP}(\mathcal{P}^0_{\mathbb{R}})$ *belongs to the Turing counting hierarchy [Allender et al. 2009].*

It remains an open challenge to tighten the relations in Facts 1.11(b), (c), and (f). In particular, the class $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$ has turned out to be of interest of its own with

several further complete problems [Shor 1991; Cucker and Rosselló 1992; Zhang 1992; Koiran 1999; Richter-Gebert 1999; Schaefer 2010; Herrmann et al. 2013]. Higher BSS complexity classes characterize natural problems in algebraic geometry [Bürgisser and Cucker 2006, 2009].

1.2. Overview: Related Work and Present Results

Dunn et al. [2005] pointed out that TARSKI's famous result [Tarski 1948] includes decidability of the first order theory of any $\mathrm{L}(\mathbb{F}^d)$, where $\mathbb{F}$ is real or algebraically closed. This has been used in the work of Herrmann [2010] to prove decidability of the equational theory of the class comprising all projection ortholattices of finite von Neumann algebra factors. Our subject, here, is the counterpart of validity, namely, satisfiability of equations in a fixed $\mathrm{L}(\mathbb{F}^d)$. As in the Boolean case, satisfiability of a system can be compiled into the (strong) satisfiability of a single equation $t(\bar{x}) = \mathbf{1}$. But, this is no longer the negation of validity of an identity $\forall \bar{x}\ t(\bar{x}) = \mathbf{0}$; this negation $\exists \bar{x}\ t(\bar{x}) \neq \mathbf{0}$ will be called weak satisfiability.

Although computational complexity has become a standard topic of investigation in logic since Cook [1971]—cmp., e.g., Börger et al. [2001]; Marx [2007]—it seems to have passed on quantum logic. We have taken upon this direction of research in Herrmann and Ziegler [2011] and established both strong and weak satisfiability problems for propositional terms over both real and complex unitary spaces of appropriate dimensions to be complete for known complexity classes: 1D quantum logic coinciding with the classical Boolean one, Section 1.4 considers satisfiability problems in 2D; and Sections 2 and 3 the case of dimensions three and higher, but fixed dimension. As an approach to the infinite-dimensional case, Section 4 explores the decidability and complexity of the satisfiability problem in *in*definite finite dimensions.

Results.

(a) In fixed dimension, weak and strong satisfiability (in general differ, but) are polynomial-time equivalent (Theorem 2.11).
(b) Satisfiability in 2D quantum logic is as hard as its classical Boolean (i.e., 1D) variant: $\mathcal{NP}$-complete, regardless of the underlying field $\mathbb{F}$ (Theorem 1.20).
(c) Whereas starting with dimension three, satisfiability over both real *and complex* quantum logic is complete for *real* nondeterministic polynomial-time BSS machines (Theorems 2.3 and 2.7, and Corollary 2.12),
(d) and remains so even when restricting to terms of the form $\bigwedge\bigvee\bigwedge$, but becomes polynomial-time decidable for $\bigwedge\bigvee$-terms (Theorem 3.3(a) and (b)).
(e) Another syntactic variant of quantum satisfiability complete for *complex* nondeterministic polynomial-time BSS machines is presented in Theorem 3.3(c).
(f) Satisfiability over rational 3D quantum logic is equivalent to Hilbert's Tenth Problem over $\mathbb{Q}$ (Corollary 2.8(c))
(g) and validity over 3D rational quantum logic of a Σ_3^0-formula is undecidable (Corollary 3.9). More generally, quantified quantum logics correspond to the Boolean and the BSS polynomial hierarchy (Theorem 3.8).
(h) Weak satisfiability over indefinite finite real or complex dimension (i.e., asking for the existence of both a d and a d-dimensional assignment) is decidable by real nondeterministic polynomial-time BSS machines, but not known hard (Theorem 4.4).
(j) Strong satisfiability over indefinite finite dimension is hard for polynomial-time BSS nondeterminism, but not known decidable yet for polynomial-time equivalent to the feasibility of *non*commutative polynomial equations (Theorem 4.10 and Proposition 4.9).

We regard satisfiability in quantum logic as even more natural a generalization of the classical Boolean satisfiability problem than the feasibility of a system of ring

equations from Fact 1.8. Moreover, the distinction between dimension ≤ 2 and ≥ 3 provides a unified view on both Turing and real BSS complexity theory, resembling those concerning realizability questions for chirotopes [Björner et al. 1999, Section 8] and similar to descriptive complexity theory, where complexity classes are captured in appropriate logics. Machine-independent characterizations of some BSS complexity classes have been obtained in Grädel and Meer [1996] and Bournez et al. [2006].

1.3. Truth, Equivalence, and Satisfiability

The classical Boolean satisfiability problem extends straightforwardly to quantum propositional formulae—although truth ("$= \mathbf{1}$") now has to be distinguished from non-falsity ("$\neq \mathbf{0}$").

Definition 1.13. Let L always denote some Modular Ortholattice (MOL).

(a) A (ortholattice) term or quantum logic propositional formula is a syntactically correct expression over certain variables $x_1, \ldots, x_n$ with infix binary operation symbols $\wedge$ and $\vee$, unary $\neg$, and constants $\mathbf{0}$ and $\mathbf{1}$. We may write $t(\bar{x})$ to emphasize that only variables x_i from $(x_1, \ldots, x_n) =: \bar{x}$ occur in t. Brackets may be saved in an obvious manner. The syntactic *length* of t is denoted by $|t|$, defined recursively as $|x| = 1$, $|\neg t| = |t| + 1$, and $|s \vee t| = |s| + |t| + 1 = |s \wedge t|$.

(b) For $\bar{a} = (a_1, \ldots, a_n) \in L^n$, let $t_L(a_1, \ldots, a_n) = t_L(\bar{a}) \in L$ denote the value of t in L when substituting a_i for x_i.

(c) Elements of L may be considered as parameters and used in place of variables when constructing terms. We then speak of terms with parameters from L. (Formally, a parameter c can be considered as a kind of "new constant," the interpretation of which in L is always the element c of L).

(d) An n-variate term t is strongly satisfiable in L if there is $\bar{a} \in L^n$, such that $t_L(\bar{a}) = \mathbf{1}$. It is weakly satisfiable in L if there is $\bar{a} \in L^n$, such that $t_L(\bar{a}) \neq \mathbf{0}$.

(e) Two n-variate terms s and t are equivalent over L if $s_L(\bar{a}) = t_L(\bar{a})$ for every $\bar{a} \in L^n$. They are equivalent if they are so over all MOL's L.

(f) Strong and weak satisfiability over L are the respective decision problems

$$\mathrm{SAT}_L := \{\langle t(x_1, \ldots, x_n)\rangle \mid n \in \mathbb{N}, t \text{ term}, \exists \bar{a} \in L^n : t_L(\bar{a}) = \mathbf{1}\} \subseteq \{0,1\}^* \quad \text{and}$$
$$\mathrm{sat}_L := \{\langle t(x_1, \ldots, x_n)\rangle \mid n \in \mathbb{N}, t \text{ term}, \exists \bar{a} \in L^n : t_L(\bar{a}) \neq \mathbf{0}\} \subseteq \{0,1\}^*.$$

(g) More generally, for a class $\mathcal{C}$ of MOLs, consider the question of whether a given term t is strongly/weakly satisfiable over *some* $L \in \mathcal{C}$: $\mathrm{SAT}_{\mathcal{C}} := \bigcup_{L\in\mathcal{C}} \mathrm{SAT}_L$, $\mathrm{sat}_{\mathcal{C}} := \bigcup_{L\in\mathcal{C}} \mathrm{sat}_L$.

(h) Returning to single L, strong satisfiability *with parameters* from L is the problem of whether a given MOL term with parameters from L (recall c) admits a strongly satisfying assignment over L. (In case $L := \mathrm{L}(\mathbb{F}^d)$, its formal encoding as a BSS decision problem over $\mathrm{Re}(\mathbb{F})$ will be specified in Proposition 2.1...)

Note that weak satisfiability of t means *in*validity of the identity "$t = \mathbf{0}$" in the model-theoretic sense. Moreover, $\mathrm{SAT}_{\{\mathbf{0},\mathbf{1}\}} = \mathrm{sat}_{\{\mathbf{0},\mathbf{1}\}}$ coincides with the classical Boolean satisfiability problem. We also state (with the obvious extension of the above definitions to direct products):

Observation 1.14. *For the product $L \times L'$ of MOLs L and L', it holds* $\mathrm{SAT}_{L\times L'} = \mathrm{SAT}_L \cap \mathrm{SAT}_{L'}$ *and* $\mathrm{sat}_{L\times L'} = \mathrm{sat}_L \cup \mathrm{sat}_{L'}$.

Furthermore, record that the connective "$\vee$" satisfies the *disjunction property* for weak truth: $x \vee y \neq \mathbf{0}$ holds iff $x \neq \mathbf{0}$ or $y \neq \mathbf{0}$ holds. In dimensions > 1, however, strong truth generally fails this property: $x \vee y = \mathbf{1}$ may well hold with neither $x = \mathbf{1}$ nor $y = \mathbf{1}$ —similarly for the dual connective "$\wedge$". Furthermore, Boolean negation has to be

distinguished from complement: $x \neq \mathbf{0} \overset{\Leftarrow}{\not\Rightarrow} \neg x = \mathbf{0}$. The conjunction of formulae ϕ and ψ in the language of ortholattices is written as ϕ `&&` ψ, using the traditional connective of the programming language `C`—similarly for ϕ `||` ψ.

EXAMPLE 1.15. *$C(x, y) := (x \wedge y) \vee (x \wedge \neg y) \vee (\neg x \wedge y) \vee (\neg x \wedge \neg y)$ is called the* commutator *term. We say that $a, b \in L$* commute *iff $C(a, b) = \mathbf{1}$ holds.*

(a) *For $a, b \in L$, consider the sub-MOLs $\{\mathbf{0}, \mathbf{1}, a, \neg a\} =: L(a)$ and $L(b)$. Whenever $a \in L(b)$ or $b \in L(a)$, it follows $C_L(a, b) = \mathbf{1}$. In particular, $C(x, y)$ is equivalent to $\mathbf{1}$ on $\mathrm{L}(\mathbb{F}^1)$. Over $\mathrm{L}(\mathbb{F}^2)$, however, $C(\mathbb{F}(\binom{1}{r}), \mathbb{F}(\binom{1}{s}))$ evaluates to $\mathbf{0}$ whenever $r \notin \{s, -1/\bar{s}\}$. More generally, in $\mathcal{MO}_m$, $C(a, b)$ evaluates to $\mathbf{1}$ if $\{a, b\} \cap \{\mathbf{0}, \mathbf{1}\} \neq \emptyset$ or $a = \neg b$, to $\mathbf{0}$ otherwise.*

(b) *U, V in $\mathrm{L}(\mathbb{F}^d)$ commute iff $\mathbb{F}^d = (U \cap V) \oplus (U \cap V^\perp) \oplus (U^\perp \cap V) \oplus (U^\perp \cap V^\perp)$, an orthogonal sum.*

(c) *$a_1, \ldots, a_n \in L$ commute pairwise iff they generate a Boolean sub-algebra of L isomorphic to $\{\mathbf{0}, \mathbf{1}\}^k$ for some $k \leq 2^n$.*

(d) *Let $t(x, y) := C(x, y) \vee x \vee y$ and $s(x, y, z) := t(x, y) \wedge t(x, z) \wedge t(y, z)$. Then, s is equivalent to $\mathbf{1}$ on $\mathrm{L}(\mathbb{F}^2)$. Over $\mathbb{F}^3$, however, $s(\mathbb{F}\binom{1}{0}, \mathbb{F}\binom{1}{0}, \mathbb{F}\binom{1}{1}) = \mathbf{0}$.*

(e) *More generally, $\neg C(x, y) = (x \vee y) \wedge (\neg x \vee y) \wedge (x \vee \neg y) \wedge (\neg x \vee \neg y)$ is strongly satisfiable over each $\mathrm{L}(\mathbb{F}^{2m})$, $m \in \mathbb{N}$; but not over $\mathrm{L}(\mathbb{F}^{2m-1})$.*

(f) *According to the de Morgan laws, $\neg x \vee \neg y$ and $\neg(x \wedge y)$ are equivalent terms.*

(g) *$a \leq b$ iff $b \vee \neg(a \vee b) = \mathbf{1}$ and $a = b$ iff $b \leq a$ and $b \vee \neg a = \mathbf{1}$.*

(h) *Let $s_1(\bar{x}), t_1(\bar{x}), \ldots, s_m(\bar{x}), t_m(\bar{x})$ denote n-variate terms and consider an assignment $\bar{a}$ for $\bar{x}$ in L. Then, the following are equivalent:*
   (i) *$\bar{a}$ in L simultaneously satisfies all equations $s_i(\bar{x}) = t_i(\bar{x})$, $1 \leq i \leq m$,*
   (ii) *$\bar{a}$ strongly satisfies the single term $\bigwedge_{i=1}^m ([s_i(\bar{x}) \wedge t_i(\bar{x})] \vee \neg[s_i(\bar{x}) \vee t_i(\bar{x})])$.*

PROOF. Examples 1.15(a), (b), and (d) are straightforward to verify. In Example 1.15(c), if L is an $\mathcal{MO}_m$ then apply Example 1.15(a). So consider $U_i \in L = \mathrm{L}(\mathbb{F}^d)$, such that $C(U_i, U_j) = \mathbf{1}$ for i, j. Let π_i denote the orthogonal projection onto U_i. In view of Example 1.15(b), this implies that all π_i and π_j commute. Thus, the π_i generates a Boolean sub-ring R of the endomorphism ring of $\mathbb{F}^d$. Moreover, all members of R are orthogonal projections and $\mathrm{Card}\,(R) \leq 2^{2^n}$. Finally, $\pi \mapsto \mathrm{range}\,\pi$ is an isomorphism of R onto a Boolean sub-algebra of L. For Example 1.15(e), observe that (U_1, U_2) is a strongly satisfying assignment in $\mathrm{L}(\mathbb{F}^d)$, if and only if $\mathbb{F}^d = V \oplus W$ for any $V \neq W$ in $\{U_1, U_2, U_1^\perp, U_2^\perp\}$; thus, by the dimension formula, all these subspaces have dimension $d/2$. In Example 1.15(g), if $a \leq b$ then $a \vee b = b$ when $b \vee \neg(a \vee b) = \mathbf{1}$. Conversely, assuming the latter one gets, using the modular law, $a \vee b = (a \vee b) \wedge (b \vee \neg(a \vee b)) = b \vee ((a \vee b) \wedge \neg(a \vee b)) = b \vee \mathbf{0} = b$ when $a \leq b$. The second claim follows, immediately. For Example 1.15(h), observe that $a \wedge b \leq a \vee b$ with equality, if and only if $a = b$. □

1.4. 2D Satisfiability is $\mathcal{NP}$–Complete

PROPOSITION 1.16. *SAT_L is $\mathcal{NP}$–hard for any nontrivial MOL L, uniformly in L.*

In particular, for any non-empty class $\mathcal{C}$ of nontrivial MOLs, $\mathrm{SAT}_{\mathcal{C}}$ is $\mathcal{NP}$–hard. Theorem 1.20 below shall extend this to weak satisfiability.

PROOF. Convert a given term $t(x_1, \ldots, x_n)$ to the term $s(\bar{x}) := t(\bar{x}) \wedge \bigwedge_{1 \leq i < j \leq n} C(x_i, x_j)$: this is clearly computable in polynomial time. Moreover, a satisfying Boolean assignment $\bar{b} \in \{\mathbf{0}, \mathbf{1}\}^n$ of t is also one of s in any non-trivial L since $C(\mathbf{0}, \mathbf{0}) = C(\mathbf{0}, \mathbf{1}) = C(\mathbf{1}, \mathbf{0}) = C(\mathbf{1}, \mathbf{1}) = \mathbf{1}$. Conversely, a satisfying assignment of s in L consists of pairwise commuting elements $b_1, \ldots, b_n \in L$; hence, "lives" in a Boolean algebra (isomorphic

to) $\{\mathbf{0},\mathbf{1}\}^k$ according to Example 1.15(c): a satisfying Boolean assignment of t is thus obtained by projecting the b_i onto their respective first components. □

Example 1.17.

(a) *Strengthening Example 1.15(b),* $\bigwedge_{1\le i<j\le 2n}(x_i \vee x_j) \wedge (\neg x_i \vee \neg x_j)$ *is weakly / strongly satisfiable in* $\mathcal{MO}_m$ *if and only if* $m \ge n$.
(b) *For* $a \in \mathcal{MO}_m$ *with* $m \ge 2$, *it holds* $a = \mathbf{1} \Leftrightarrow \exists y, z : \neg C(y,z) \wedge C(a,y) \wedge C(a,z) \wedge a \ne \mathbf{0}$.

By Example 1.17(a), both concepts of satisfiability thus depend on L, at least as far as finite 2D L are concerned. The complexity of SAT_L, however, will turn out to not depend on L as long as it has dimension two.

Recall that the 2D MOLs are uniquely determined up to isomorphism by their cardinality: $L \cong \mathcal{MO}_m$, where $\mathrm{Card}(L) = 2m+2$; and that L' embeds into L if and only if $\mathrm{Card}(L') \le \mathrm{Card}(L)$. Moreover, if L' is the sub-ortholattice generated by some $B \subseteq L$, then $L' = B \cup \{\neg b \mid b \in B\} \cup \{\mathbf{0},\mathbf{1}\}$ when $\mathrm{Card}(L') \le 2\,\mathrm{Card}(B) + 2$. It follows:

Lemma 1.18. *A term* $t(x_1,\ldots,x_n)$ *is weakly / strongly satisfiable over the 2D* L *iff it is so over* $\mathcal{MO}_m$ *for* $m := \min\{n, \mathrm{Card}(L)/2 - 1\}$ *with the convention that* $\infty/2 - 1 = \infty$. *In particular, for infinite* L *we have* $\mathrm{SAT}_L = \mathrm{SAT}_{\mathcal{MO}_\omega}$ *and* $\mathrm{sat}_L = \mathrm{sat}_{\mathcal{MO}_\omega}$.

Checking weak/strong satisfiability according to Definition 1.13(e) naively involves an infinite choice of possible arguments (=subspaces of $\mathbb{F}^d$). However, from Lemma 1.18 we conclude:

Proposition 1.19.

(a) *Consider* $\mathcal{MO}_\omega$ *with* $\mathbf{0},\mathbf{1}$ *encoded as integers* $0,1$ *and atoms* $a_m, \neg a_m$ *as* $2m, 2m+1$, *say. Then, the following evaluation problem is decidable in polynomial time:*

> *Given a term* $t(x_1,\ldots,x_n)$ *as well as an assignment* $b_1,\ldots,b_n \in \mathcal{MO}_\omega$ *and value* $b \in \mathcal{MO}_\omega$, *does it hold* $t_{\mathcal{MO}_\omega}(b_1,\ldots,b_n) = b$?

(b) *For any nonempty class* $\mathcal{C}$ *of 2D MOLs, both* $\mathrm{SAT}_{\mathcal{C}}$ *and* $\mathrm{sat}_{\mathcal{C}}$ *are in* $\mathcal{NP}$.

Proof.

(a) Disregarding parsing details, t can be evaluated by recursion on its subterms. Concerning the recursion bottom, observe that $c \vee d = \mathbf{1}$ holds in $\mathcal{MO}_\omega$ for $\mathbf{0} \ne c \ne d \ne \mathbf{0}$; and the other cases are similar or trivial anyway.
(b) Consider a nondeterministic Turing machine which, on input of an n-variate term $t(\bar{x})$, calculates from fixed $\max\{\min(\omega, \mathrm{Card}(L)) : L \in \mathcal{C}\}$ the m according to Lemma 1.18, and then guesses and verifies an assignment $\bar{b}$ in $\mathcal{MO}_m$, with encoding as in Proposition 1.19(a). □

2D quantum satisfiability is thus computationally as hard as 1D (i.e., Boolean) satisfiability:

Theorem 1.20. *For any 2D MOL* L, *both* SAT_L *and* sat_L *are* $\mathcal{NP}$*–complete.*

Proof. In view of Propositions 1.16 and 1.19, it suffices to show $\mathcal{NP}$–hardness of sat_L. For $L = \mathcal{MO}_m$ when $m \ge 2$, this follows from Example 1.17(b), observing that strong satisfiability $t(\bar{x}) = \mathbf{1}$ here reduces to the weak satisfiability of $\neg C(y,z) \wedge C(t(\bar{x}),y) \wedge C(t(\bar{x}),z) \wedge t(\bar{x})$: clearly in polynomial time. For the remaining 2D MOL $\mathcal{MO}_1 \cong \{\mathbf{0},\mathbf{1}\}^2$ on the other hand, the claim follows from $\mathrm{sat}_{L\times L'} = \mathrm{sat}_L \cup \mathrm{sat}_{L'}$. □

2. STRONG AND WEAK SATISFIABILITY ARE COMPLETE FOR BSS-$\mathcal{NP}$ IN DIM ≥ 3

The main results of this section show that, for any fixed $d \geq 3$, both strong and weak satisfiability in $L = \mathrm{L}(\mathbb{F}^d)$ are $\mathrm{BP}(\mathcal{NP}^0_{\mathrm{Re}\,\mathbb{F}})$–complete; and a suitable variant *with parameters* is $\mathcal{NP}_{\mathrm{Re}(\mathbb{F})}$–complete. The proofs of the lower bounds borrow ideas originally used in coordinatization of synthetic Desarguesian projective spaces and are guided by the model-theoretic concept of an interpretation (with definable parameters).

For $\mathbb{F} \not\subseteq \mathbb{R}$, the scalar product involves conjugation, and computing it requires separate access to real and imaginary parts—which, for instance, a $\mathbb{C}$–machine does not have (Definition 1.2). We, therefore, use $(\mathrm{Re}\,\mathbb{F})$–machines and consider $\mathbb{F}$ as $(\mathrm{Re}\,\mathbb{F}) + i(\mathrm{Re}\,\mathbb{F})$. Furthermore, note that every $U \in \mathrm{L}(\mathbb{F}^d)$ is of the form $U = \mathrm{range}\,\mathcal{A}$ for (in fact many) $\mathcal{A} \in \mathbb{F}^{d\times d}$, where $\mathrm{range}\,\mathcal{A}$ denotes the linear subspace of $\mathbb{F}^d$ spanned by $\mathcal{A}$'s columns.

PROPOSITION 2.1. *Fix a field $\mathbb{F} \subseteq \mathbb{C}$, closed under conjugation.*

(*a*) *Given $d \in \mathbb{N}$ and matrices $\mathcal{A}, \mathcal{B} \in \mathbb{F}^{d\times d}$,*
  (*i*) *a matrix $\mathcal{C} \in \mathbb{F}^{d\times d}$ with $\mathrm{range}(\mathcal{C}) = \mathrm{range}(\mathcal{A}) + \mathrm{range}(\mathcal{B})$ and*
  (*ii*) *a matrix $\mathcal{C}' \in \mathbb{F}^{d\times d}$ with $\mathrm{range}(\mathcal{C}') = \mathrm{range}(\mathcal{A}) \cap \mathrm{range}(\mathcal{B})$*
  can be calculated by a constant-free BSS-machine over $\mathbb{F}$ in time $\mathcal{O}(d^3)$. Similarly,
  (*iii*) *a matrix $\mathcal{C}'' \in \mathbb{F}^{d\times d}$ with $\mathrm{range}(\mathcal{C}'') = \mathrm{range}(\mathcal{A})^\perp$*
  can be calculated by a constant-free BSS-machine $\mathcal{M}$ over $\mathbb{F}$ in time $\mathcal{O}(d^3)$ in case $\mathbb{F} \subseteq \mathbb{R}$; otherwise, $\mathcal{M}$, in general, needs both real part $\mathrm{Re}(\mathcal{A})$ and imaginary part $\mathrm{Im}(\mathcal{A})$.

(*b*) *First, suppose $\mathbb{F} \subseteq \mathbb{R}$. Then, given an n-variate term t and matrices $\mathcal{A}_1, \ldots, \mathcal{A}_n \in \mathbb{F}^{d\times d}$, a constant-free BSS-machine $\mathcal{M}$ over $\mathbb{F}$ can calculate $\mathcal{C} \in \mathbb{F}^{d\times d}$ with $\mathrm{range}(C) = t_{\mathrm{L}(\mathbb{F}^d)}(\mathrm{range}\,\mathcal{A}_1, \ldots, \mathrm{range}\,\mathcal{A}_n)$ in time polynomial in $d + |t|$.*
  In the general case $\mathbb{F} \subseteq \mathbb{C}$, given matrices $\mathrm{Re}(\mathcal{A}_1), \mathrm{Im}(\mathcal{A}_1), \ldots, \mathrm{Re}(\mathcal{A}_n), \mathrm{Im}(\mathcal{A}_n) \in \mathrm{Re}(\mathbb{F})^{d\times d}$, a similar machine over $\mathrm{Re}(\mathbb{F})$ can calculate $\mathrm{Re}(\mathcal{C}), \mathrm{Im}(\mathcal{C}) \in (\mathrm{Re}\,\mathbb{F})^{d\times d}$ with $\mathrm{range}(\mathcal{C}) = t_{\mathrm{L}(\mathbb{F}^d)}(\mathrm{range}\,\mathcal{A}_1, \ldots, \mathrm{range}\,\mathcal{A}_n)$.

(*c*) *Both weak and strong satisfiability over $\mathrm{L}(\mathbb{F}^d)$ of a given term t can be decided by a nondeterministic constant-free BSS-machine over $\mathrm{Re}(\mathbb{F})$ in time polynomial in $d + |t|$. In particular, it holds*

$$\mathrm{sat}_{\mathrm{L}(\mathbb{R}^d)},\ \mathrm{SAT}_{\mathrm{L}(\mathbb{R}^d)},\ \mathrm{sat}_{\mathrm{L}(\mathbb{A}^d)},\ \mathrm{SAT}_{\mathrm{L}(\mathbb{A}^d)},\ \mathrm{sat}_{\mathrm{L}(\mathbb{C}^d)},\ \mathrm{SAT}_{\mathrm{L}(\mathbb{C}^d)} \ \in \mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}}) \subseteq \mathsf{PSPACE}.$$

(*d*) *Concerning satisfiability with parameters make Definition 1.13(h) precise and let*

$$\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d),\mathrm{L}(\mathbb{F}^d)} := \Big\{ \big\langle t(x_1, \ldots, x_n, y_1, \ldots, y_m), \mathcal{C}_1, \ldots, \mathcal{C}_m \big\rangle \;\Big|\; \mathcal{C}_1, \ldots, \mathcal{C}_m \in \mathbb{F}^{d\times d},$$
$$\exists \mathcal{A}_1, \ldots, \mathcal{A}_n \in \mathbb{F}^{d\times d} : t_{\mathrm{L}(\mathbb{F}^d)}(\mathrm{range}\,\mathcal{A}_1, \ldots, \mathrm{range}\,\mathcal{A}_n, \mathrm{range}\,\mathcal{C}_1, \ldots, \mathrm{range}\,\mathcal{C}_m) = \mathbb{F}^d \Big\},$$

where matrices $\mathcal{C}_j$ are encoded as d^2-element sequences over $\mathbb{F}$—similarly for $\mathrm{sat}_{\mathrm{L}(\mathbb{F}^d),\mathrm{L}(\mathbb{F}^d)}$. Then, both decision problems belong to $\mathcal{NP}_{\mathrm{Re}(\mathbb{F})}$.

Proposition 2.1(b) and (c) can be regarded as a natural generalization of Proposition 1.19(a) and (b) to fixed, higher dimensions. Proposition 2.1(b) follows from Proposition 2.1(a) by recursion on subterms. Proposition 2.1(a.i) is provided by applying Gaussian Elimination to the columns of $(\mathcal{A}, \mathcal{B})$, Proposition 2.1(a.ii) by a variant due to Zassenhaus [1948], Proposition 2.1(a.iii) by invoking Gauss on rows of $\mathcal{A}^\dagger$, the adjoint of $\mathcal{A}$. Concerning Propositions 2.1(c) and (d), a nondeterministic constant-free machine guesses the entries of $d \times d$ matrices and evaluates according to Proposition 2.1(b), followed by testing whether the resulting matrix is regular (case of strong satisfiability) or non-zero (case of weak satisfiability).

2.1. Strong Satisfiability with Parameters is $\mathcal{NP}_{\mathsf{Re}(\mathbb{F})}$–Hard in Dimensions ≥ 3

We are going to reduce the problem $\mathrm{FEAS}_{\mathrm{Re}(\mathbb{F}),\mathrm{Re}(\mathbb{F})}$ of Fact 1.8(a) to strong satisfiability *with parameters* over $L := \mathrm{L}(\mathbb{F}^d)$, $d \geq 3$; based on a particular fragment of the encoding $\mathcal{C} \mapsto \mathrm{range}\,\mathcal{C}$: associate with $c \in \mathbb{F}$ the 1D subspace

$$\Theta(c) := \mathbb{F}(\vec{e}_1 - c\vec{e}_2),$$

where $\vec{e}_1, \ldots, \vec{e}_d$ denotes the standard basis of $\mathbb{F}^d$. To furthermore interpret the operations over $\mathbb{F}$ into those over $\mathrm{L}(\mathbb{F})$, consider the following variant $\bar{E}$ of the standard coordinate system of the projective space associated with $\mathbb{F}^d$

$$E_i := E_{ii} := \mathbb{F}\vec{e}_i, \qquad E_{ij} := \mathbb{F}(\vec{e}_i - \vec{e}_j), \quad (i \neq j). \tag{3}$$

For example, for $d = 3$, one has

$$E_1 = \Theta(0) = \mathrm{range}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad E_{12} = \Theta(1) = \mathrm{range}\begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$
$$\text{and } \Theta(c) = \mathrm{range}\begin{pmatrix} 1 & 0 & 0 \\ -c & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The following are easily verified for any $a, b, c \in \mathbb{F}$:

(4.a) $\mathbb{F}(\vec{e}_i - a\vec{e}_k) = (\mathbb{F}(\vec{e}_i - a\vec{e}_j) + E_{jk}) \cap (E_i + E_k)$ for pairwise distinct i, j, k;
(4.b) $\mathbb{F}(\vec{e}_k - a\vec{e}_j) = (\mathbb{F}(\vec{e}_i - a\vec{e}_j) + E_{ik}) \cap (E_j + E_k)$ for pairwise distinct i, j, k;
(4.c) $ab = c$, iff $(\mathbb{F}(\vec{e}_1 - b\vec{e}_3) + \mathbb{F}(\vec{e}_3 - a\vec{e}_2)) \cap (E_1 + E_2) = \Theta(c)$;
(4.d) $a - b = c$, iff $[(\mathbb{F}(\vec{e}_1 - b\vec{e}_3) + E_2) \cap (\Theta(a) + E_{23}) + E_3] \cap (E_1 + E_2) = \Theta(c)$;
(4.e) $a \in \mathrm{Re}(\mathbb{F})$, iff $\Theta(a)^\perp \cap (E_1 + E_2) = \mathbb{F}(\vec{e}_2 + a\vec{e}_1)$.

For example, in 3D, we have in (4.c) the first subterm evalue to $\{(x, 0, -bx)+(0, -ay, y) : x, y\}$ and obtain, intersecting with $\{(u, v, 0) : u, v\}$, the result $\{(x, -abx, 0) : x\}$. Up to permutation of indices, (4.a) and (4.b) are special cases with $a = 1$ or $b = 1$. In (4.d), we get intermediate expressions $(x, y, -bx)$ and $(u, -au - v, v)$ intersecting to $(x, -ax + bx, -bx)$, from which one gets $(x, -(a - b)x, w)$ and then $(x, -(a - b)x, 0)$. Finally, in (4.e), one has $(x, -ax, 0)^\perp = (a^\dagger y, y, z)$, which then yields $(a^\dagger y, y, 0)$.

Now, introduce distinguished variables $\bar{Z} = (Z_{ij} \mid 1 \leq i \leq j \leq d)$, and abbreviate $Z_i := Z_{ii}$ and $Z_{ij} := Z_{ji}$ for $i > j$. Moreover consider the terms

$$\begin{aligned}
\pi^{ij}_{\bar{Z}ik}(X) &:= (Z_i \vee Z_k) \wedge (X \vee Z_{jk}), \\
\pi^{ij}_{\bar{Z}kj}(X) &:= (Z_k \vee Z_j) \wedge (X \vee Z_{ik}), \\
X \otimes_{\bar{Z}} Y &:= \big(\pi^{12}_{\bar{Z}13}(Y) \vee \pi^{12}_{\bar{Z}32}(X)\big) \wedge (Z_1 \vee Z_2), \quad \text{and} \\
X \ominus_{\bar{Z}} Y &:= \big([(\pi^{12}_{\bar{Z}13}(Y) \vee Z_2) \wedge (X \vee Z_{23})] \vee Z_3\big) \wedge (Z_1 \vee Z_2),
\end{aligned}$$

and the following equation $\sigma_{\bar{Z}}(X)$ in the language of ortholattices:

$$Z_1 \ominus_{\bar{Z}} X = (Z_1 \ominus_{\bar{Z}} X) \cap \neg X.$$

For each parameter $\bar{A}$ in L substituted for $\bar{Z}$, one obtains binary operations $\ominus_{\bar{A}}$ and $\otimes_{\bar{A}}$ and a unary predicate $\sigma_{\bar{A}}$ on L

$$(U, V) \mapsto U \ominus_{\bar{A}} V, \qquad (U, V) \mapsto U \otimes_{\bar{A}} V, \qquad \sigma_{\bar{A}} = \{U \in L \mid L \models \sigma_{\bar{A}}(U)\}.$$

Fact 2.2. *The operations $\ominus_{\bar{E}}$ and $\otimes_{\bar{E}}$ on $L = \mathrm{L}(\mathbb{F}^d)$ restrict to binary operations on $\mathcal{R}_{\bar{E}} := \{U \in L \mid U \oplus E_2 = E_1 + E_2\}$; endowed with these and the constants E_1 and E_{12},*

$\mathcal{R}_{\bar{E}}$ becomes a ring which is a copy of $\mathbb{F}$ under the isomorphism $\Theta = \Theta_{\bar{E}}$. Moreover, for $a \in \mathbb{F}$ one has $a \in \mathrm{Re}(\mathbb{F})$, iff $\sigma_{\bar{E}}(\Theta(a))$ holds in L.

Proof. Clearly, Θ is injective. On the other hand, if $U \in \mathcal{R}$, then $\dim(U) < 2$ (from $U \not\supseteq E_2$) when $U = \mathbb{F}(r\vec{e}_1 + s\vec{e}_2)$ and $r \neq 0$ (from $U \not\subseteq E_2$); and so, $U = \Theta(r^{-1}s)$. By definition, $\Theta(0) = E_1$ and $\Theta(1) = E_{12}$. Observe that by (4.a) and (4.b)

$$\pi^{ij}_{\bar{E}ik}(\mathbb{F}(\vec{e}_i - a\vec{e}_j)) = \mathbb{F}(\vec{e}_i - a\vec{e}_k), \quad \pi^{ij}_{\bar{E}kj}(\mathbb{F}(\vec{e}_i - a\vec{e}_j)) = \mathbb{F}(\vec{e}_k - a\vec{e}_j).$$

Thus, $\Theta(ab) = \Theta(a) \otimes_{\bar{E}} \Theta(b)$ follows from (4.c); and $\Theta(a-b) = \Theta(a) \ominus_{\bar{E}} \Theta(b)$ follows from (4.d). $c \in \mathrm{Re}(\mathbb{F})$ means $c = c^\dagger$, equivalent to $\sigma_{\bar{E}}(\Theta(c))$ according to (4.e). □

Theorem 2.3. *For any fixed $\mathbb{F} \subseteq \mathbb{C}$ and $d \geq 3$, both $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d),\mathrm{L}(\mathbb{F}^d)}$ and $\mathrm{sat}_{\mathrm{L}(\mathbb{F}^d),\mathrm{L}(\mathbb{F}^d)}$ are $\mathcal{NP}_{\mathrm{Re}(\mathbb{F})}$-complete.*

Proof. Membership in $\mathcal{NP}_{\mathrm{Re}(\mathbb{F})}$ holds due to Proposition 2.1(d). Concerning hardness, in view of Fact 1.8(a), we consider an instance of $\mathrm{FEAS}_{\mathrm{Re}(\mathbb{F}),\mathrm{Re}(\mathbb{F})}$ involving finitely many $p_j \in (\mathrm{Re}\,\mathbb{F})[X_1, \ldots, X_n]$. Proceed in the following steps, producing ortholattice terms and equations with parameters $\bar{E}, \bar{C}$ in $\mathrm{L}(\mathbb{F}^d)$:

(5.i) For each polynomial p_j, form a ring term p'_j according to Observation 1.9(b). Then, replace each occurrence of $-$ and $\times$ by $\ominus_{\bar{E}}$ and $\otimes_{\bar{E}}$, respectively,
(5.ii) and replace parameters $c \in \mathrm{Re}(\mathbb{F})$ with MOL parameters $C := \Theta(c)$.
(5.iii) From the obtained ortholattice terms with parameters, $t_j(\bar{X}; \bar{C}, \bar{E})$, form the equations $t_j(\bar{X}; \bar{C}, \bar{E}) = E_1$;
(5.iv) for each variable X_i, add the two equations $X_i \vee E_2 = E_1 + E_2$ and $X_i \wedge E_2 = \mathbf{0}$,
(5.v) as well as the equation $\sigma_{\bar{E}}(X_i)$,

and combine the resulting system of ortholattice Equations (5.iii) to (5.v) into one single ortholattice equation "$t_{\bar{p}}(\bar{X}; \bar{C}, \bar{E}) = \mathbf{1}$," according to Example 1.15(h), encoded and output as $\langle t_{\bar{p}}(\bar{X}; \bar{Y}, \bar{Z}), \bar{C}, \bar{\mathcal{E}} \rangle$.

Note that all transformations are purely syntactical or involve parameters taken from the (given!) polynomials' coefficients—and can indeed be performed in polynomial time by a BSS machine over $\mathrm{Re}(\mathbb{F})$. Moreover, any root $\bar{x}$ in $\mathrm{Re}(\mathbb{F}) \subseteq \mathbb{F}$ common to all p_j gives rise to an assignment $\bar{X} := \Theta(\bar{x})$ in $\mathrm{L}(\mathbb{F}^d)$, making all terms $t_j(\bar{X}; \bar{C}, \bar{E})$ evaluate to $\Theta(0) = E_1$ (Equation (5.iii)) as well as satisfying Equations (5.iv) and (5.v) according to Fact 2.2. Conversely, any assignment $\bar{X}$ in $\mathrm{L}(\mathbb{F}^d)$ satisfying condition (5.iv) has the form $X_k = \Theta(x_k)$ for some unique $x_k \in \mathbb{F}$, which Equation (5.v) requires to even belong to $\mathrm{Re}(\mathbb{F})$; and, $p_j(\bar{x}) = 0$ follows from Equations (5.i) to (5.iii). This proves $\mathcal{NP}_{\mathrm{Re}(\mathbb{F})}$–hardness of $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d),\mathrm{L}(\mathbb{F}^d)}$.

Finally, observe that for $U \in \mathrm{L}(\mathbb{F}^d)$, it holds

$$U = \mathbb{F}^d \quad \Leftrightarrow \quad E_0^\perp \cap \bigcap\nolimits_{i=1}^{d} (E_0 + (U \cap E_i)) \neq \mathbf{0}, \qquad \text{where} \quad E_0 := \sum_{j=2}^{d} E_{1j}.$$

This yields a BSS polynomial-time many-one reduction from strong satisfiability with parameters over $\mathrm{L}(\mathbb{F}^d)$ to weak satisfiability with (possibly additional) parameters $\bar{E}$. □

2.2. Strong Satisfiability is BP($\mathcal{NP}^0_{\mathrm{Re}\mathbb{R}}$)-Hard in Dimensions ≥ 3

We now turn to $\mathrm{L}(\mathbb{F}^d)$ considered as an ortholattice with no constants. This means that we cannot use the particular coordinate system $\bar{E}$ to recover $\mathbb{F}$; rather, we have to build our arguments on the set of all (suitable) coordinate systems $\bar{A}$. Here, $\mathbb{F}^d$ figures merely

as an inner product space admitting some orthonormal basis. The calculations of the preceding subsection can be reused, though, due to the following:

OBSERVATION 2.4.

(*a*) *Given a basis* $\vec{v}_1, \ldots, \vec{v}_d$ *of the* $\mathbb{F}$*-vector space* V*, there is a unique isomorphism* ϕ *of* $\mathbb{F}^d$ *onto* V*, such that* $\phi(\vec{e}_i) = \vec{v}_i$ *and a bijection* $\hat{\phi} : \mathrm{L}(\mathbb{F}^d) \ni U \mapsto \{\phi(\vec{u}) \mid \vec{u} \in U\} \in \mathrm{L}(V)$*, constituting a "lattice isomorphism" in the following sense:* $\hat{\phi}(U+W) = \hat{\phi}(U)+\hat{\phi}(W)$*,* $\hat{\phi}(U \cap W) = \hat{\phi}(U) \cap \hat{\phi}(W)$*,* $\hat{\phi}(\mathbf{0}) = \mathbf{0}$*. Moreover,* $\hat{\phi}(\mathbb{F}(\vec{e}_i - a\vec{e}_j)) = \mathbb{F}(\vec{v}_i - a\vec{v}_j)$*.*

(*b*) *If* V *is an inner product space, then* ϕ *is an isometry iff the basis* $\vec{v}_1, \ldots, \vec{v}_d$ *is orthonormal. In this case,* $\hat{\phi} : \mathrm{L}(\mathbb{F}^d) \to \mathrm{L}(V)$ *is an isomorphism of ortholattices.*

Generalizing the definition of $\bar{E}$ in Equation (3), given any basis $\vec{v}_1, \ldots, \vec{v}_d$ of $\mathbb{F}^d$, let $A_i := A_{ii} := \mathbb{F}\vec{v}_i$ and $A_{ij} := \mathbb{F}(\vec{v}_i - \vec{v}_j)$ for $i \neq j$. Obviously, $\bar{A} = (A_{ij} \mid i, j \leq d)$ satisfies the following:

$$\begin{array}{lll} \mathbb{F}^d = A_1 \oplus \ldots \oplus A_d, & & \\ A_i \oplus A_{ij} = A_i + A_j & \text{for all } i, j = 1, \ldots, h,\ i \neq j, \text{ and} & \\ A_{ik} = A_{ki} = (A_i + A_k) \cap (A_{ij} + A_{jk}) & \text{for all } i, j, k = 1, \ldots, d,\ i \neq j \neq k \neq i. & \end{array} \tag{6}$$

Call $\bar{A}$ satisfying Equation (6) a (projective) coordinate system of order d. Any such system has $\dim A_i = 1$; and, choosing $\vec{v}_1$ such that $A_1 = \mathbb{F}\vec{v}_1$ and, for $j > i$, $\vec{v}_j \in A_j$ such that $A_{1j} = \mathbb{F}(\vec{v}_1 - \vec{v}_j)$, gives rise to a basis associated with $\bar{A}$ (unique up to a scalar multiple). $A_{ij} = \mathbb{F}(\vec{v}_i - \vec{v}_j)$ for all $i \neq j$. Combining the isomorphisms of Fact 2.2 and Observation 2.4(a), one gets $\Theta_{\bar{A}} = \hat{\phi} \circ \Theta$ and the following:

FACT 2.5. *For each coordinate system* $\bar{A}$ *of* L *and associated basis* $\vec{v}_1, \ldots, \vec{v}_d$*, there is an isomorphism*

$$\Theta_{\bar{A}} : \mathbb{F} \to \mathcal{R}_{\bar{A}} = \{U \in L \mid U \oplus A_2 = A_1 + A_2\}, \quad \Theta_{\bar{A}}(a) = \mathbb{F}(\vec{v}_1 - a\vec{v}_2)$$

of the ring $\mathbb{F}$ *with operations* $-, \times$ *onto* $\mathcal{R}_{\bar{A}}$ *with induced operations* $\ominus_{\bar{A}}$*,* $\otimes_{\bar{A}}$*,* A_1*,* A_{12}*.*

Since we also have to recover $\mathrm{Re}(\mathbb{F})$, orthogonality has to be taken into account. For $\bar{A}$ derived from an orthogonal basis $\vec{v}_1, \ldots, \vec{v}_d$ of $\mathbb{F}^d$, we may strengthen the first condition in Equation (6) to $\mathbb{F}^d = A_1 \oplus \ldots \oplus A_d$ to obtain the concept of an orthogonal coordinate system. Given such, any associated basis is orthogonal. Though, this is not sufficient to transfer Item (e) from Section 2.1 to this setting: this condition will well exclude all non-real numbers; namely, $\langle \vec{v}_1 - a\vec{v}_2 \mid \vec{v}_2 + a\vec{v}_1 \rangle = 0$ implies $a^\dagger = a\|\vec{v}_1\|/\|\vec{v}_2\|$. But, it also excludes all real ones—unless we can assure that $\|\vec{v}_1\| = \|\vec{v}_2\|$. The latter is achieved (with $a = 1$ in the preceding argument) by considering coordinate systems $\bar{A}$ which are orthonormal, i.e., are orthogonal and satisfy

$$A_1 \ominus_{\bar{A}} A_{12} = (A_1 + A_2) \cap A_{12}^{\perp}.$$

LEMMA 2.6. *For any orthonormal coordinate system* $\bar{A}$ *of* $L = \mathrm{L}(\mathbb{F}^d)$*,* $\Theta_{\bar{A}}$ *restricts to an isomorphism of* $\mathrm{Re}\,\mathbb{F}$ *onto the subring* $\mathrm{Re}\,\mathcal{R}_{\bar{A}} := \{U \in \mathcal{R}_{\bar{A}} \mid L \models \sigma_{\bar{A}}(U)\}$ *of* $\mathcal{R}_{\bar{A}}$*.*

Indeed, by the preceding paragraph, one has $U = \Theta_{\bar{A}}(r)$ with $r \in \mathrm{Re}\,\mathbb{F}$, iff $U \in \mathrm{Re}\,\mathcal{R}_{\bar{A}}$. Fixing an orthonormal coordinate system $\bar{A}$, Fact 2.5 and Lemma 2.6 reveal $\Theta_{\bar{A}}^{-1}$ an *interpretation* (recall Section 1) of the ring $\mathbb{F}$ with unary predicate $\mathrm{Re}(\mathbb{F})$ in $(L, \bar{A})$, the expansion of the ortholattice L by the new constants $\bar{A}$. In particular, as in the proof of Theorem 2.3, one has a translation from the language of $\mathbb{F}$ (with predicate $\mathrm{Re}\,\mathbb{F}$) to that of $(L, \bar{A})$, with $c \in \mathbb{F}$ translated as $\Theta_{\bar{A}}(c)$.

Thus, the orthonormal coordinate systems $\bar{A}$ are the *admissible parameters* on which this kind of translation can be based. To have a translation not referring to new constants $\bar{A}$, we need admissibility to be *definable* (cmp. to Hodges [1993, Section 5.3

Remark 5]). We summarize what is required for this method of *interpretation with definable parameters* to work.

(7.I) Admissible parameters exist (e.g., the 'standard' coordinate system).
(7.II) Admissible parameters can be axiomatically characterized—cmp. conditions of Theorem 2.7(vii') to Theorem 2.7(ix') in the below proof.
(7.III) Each admissible parameter $\bar{A}$ of L gives rise to an isomorphism $\Theta_{\bar{A}}$ of $\mathrm{Re}(\mathbb{F})$ onto $\mathrm{Re}\,\mathcal{R}_{\bar{A}}$, defined within L, uniformly for all $\bar{A}$ (cmp. Lemma 2.6).
(7.IV) The defining formulae are in the language of ortholattices, although the proofs may refer to the inner product space $\mathbb{F}^d$.

THEOREM 2.7. *For every $d \geq 3$, $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d)}$ is $\mathrm{BP}(\mathcal{NP}^0_{\mathrm{Re}\,\mathbb{F}})$–complete.*
More precisely, instances of $\mathrm{FEAS}_{\mathbb{Z},\mathrm{Re}\,\mathbb{F}}$ are many-one reducible to instances of $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d)}$ by a Turing machine with running time polynomial in d and in the input length. The reduction is uniform in $\mathbb{F}$.

PROOF. Modifying the proof of Theorem 2.3, replace the fixed standard coordinate system $\bar{E}$ by the variables $\bar{Z}$ to obtain terms and equations *without parameters*. Here, we reduce from $\mathrm{FEAS}_{\mathbb{Z},\mathrm{Re}\,\mathbb{F}}$ (Fact 1.8(b)), so there are no $c \in \mathrm{Re}(\mathbb{F})$ involved, and the former Equation (5.ii) becomes obsolete. Instead, add axioms for $\bar{Z}$ to constitute

(8.vi') a coordinate system of order d via the following equations:

$$\bigvee_{i=1}^{d} Z_i = \mathbf{1}, \quad Z_i \wedge \bigvee_{j\neq i} Z_j = \mathbf{0}, \quad Z_{ij} \vee Z_j = Z_i \vee Z_j, \quad Z_{ij} \wedge Z_j = \mathbf{0},$$
$$Z_{ik} = Z_{ki} = (Z_i \vee Z_k) \wedge (Z_{ij} \vee Z_{jk}) \quad \text{for pairwise distinct } i, j, k;$$

(8.vii') an orthogonal such system, via equations $Z_i = Z_i \wedge \neg Z_j$ for $i \neq j$;
(8.viii') an orthonormal such system, via equations $Z_1 \ominus Z_{12} = (Z_1 \vee Z_2) \wedge \neg Z_{12}$.
(8.i') Use Observation 1.9(b) to associate p'_j with p_j, and replace in p'_j any occurrence of $-$, $\cdot$, 0, 1 by $\ominus_{\bar{Z}}$, $\otimes_{\bar{Z}}$, Z_1, Z_{12},
(8.iii') and from the thus obtained terms t_j form the equations $t_j(\bar{X};\bar{Z}) = Z_1$.
(8.iv') For each variable X_i, add the two equations $X_i \vee Z_2 = Z_1 + Z_2$ and $X_i \wedge Z_2 = \mathbf{0}$,
(8.v') as well as the equation $\sigma_{\bar{Z}}(X_i)$.

Combine all conditions from (iii') to (viii') into one single ortholattice equation "$t_{\bar{p},d}(\bar{X},\bar{Z}) = \mathbf{1}$." Now, $(\bar{A},\bar{r}')$ is a satisfying assignment of $t_{\bar{p},d}(\bar{X},\bar{Z})$ in $\mathrm{L}(\mathbb{F}^d)$, if and only if $\bar{A}$ is an orthonormal coordinate system of $\mathrm{L}(\mathbb{F}^d)$ of order d (cmp. (7.II)), and if $\bar{r}'$ is the pointwise image under isomorphism $\Theta_{\bar{A}}$ of a common root $\bar{r}$ in $\mathrm{Re}(\mathbb{F})$ of the p_j; (cmp. (7.III)). In view of (7.I), this reduces $\mathrm{FEAS}_{\mathbb{Z},\mathrm{Re}\,\mathbb{F}}$ to $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d)}$ in time polynomial in d and in the length of the (p_j) encoded in binary. □

COROLLARY 2.8. *Let $d, k \geq 3$.*

(*a*) *Both $\mathrm{SAT}_{\mathrm{L}(\mathbb{R}^d)}$ and $\mathrm{SAT}_{\mathrm{L}(\mathbb{C}^d)}$ are $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$–complete.*
(*b*) *For any field $\mathbb{F} \subseteq \mathbb{R}$, $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d)}$ is $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{F}})$–complete.*
(*c*) *Decidability of $\mathrm{SAT}_{\mathrm{L}(\mathbb{Q}^d)}$ for $d \geq 3$ is as open as that of $\mathrm{FEAS}_{\mathbb{Z},\mathbb{Q}}$, (recall Fact 1.11(e)).*
(*d*) *For fixed $\mathbb{F}$, $\mathrm{FEAS}_{\mathbb{Z},\mathbb{F}}$, $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d)}$, and $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^k)}$ are mutually polytime equivalent.*

2.3. Weak versus Strong Satisfiability

We show that, in fixed dimension, strong and weak satisfiability are polynomial time equivalent. To this end, consider an alternative notion of "coordinate system" introduced in Huhn [1972], here in its orthogonal variant: a system $\bar{A} = (A_0, \ldots, A_d)$ in $\mathrm{L}(\mathbb{F}^{d'})$ is a d-diamond if $\mathbb{F}^{d'} = A_1 \oplus \ldots \oplus A_d = A_0 \oplus A_i$ for all $i > 0$. For $d = d'$, this is

equivalent to a orthogonal coordinate system of order d; in particular, $\dim A_i = 1$ for $i > 0$ and $\dim A_0 = d-1$. Now consider the following terms, where $\bar{Z} = (Z_0, Z_1, \ldots, Z_d)$:

$$\begin{aligned}
h_d(\bar{Z}) &:= \big(\bigvee_{i=1}^{d} \big(Z_i \wedge \bigwedge_{i\neq j>0} \neg Z_j\big)\big) \wedge \bigwedge_{i=1}^{d}((Z_0 \vee Z_i) \wedge (\neg Z_0 \vee \neg Z_i)),\\
\tilde{h}_d(X, \bar{Z}) &:= h_d(\bar{Z}) \wedge \hat{h}_d, \quad \text{where } \hat{h}_d(X, \bar{Z}) := \bigvee_{i,j>0}(((X \vee \neg Z_i) \wedge Z_i) \vee Z_0) \wedge Z_j),\\
g_d(\bar{Z}) &:= \neg Z_0 \wedge \bigwedge_{i=1}^{d} \big(Z_0 \vee g_d^i(\bar{Z})\big), \quad \text{where } g_d^i(\bar{Z}) := Z_i \wedge \bigwedge_{i\neq j>0} \neg Z_j \text{ for } i > 0,\\
\tilde{g}_d(X, \bar{Z}) &:= g_d(\bar{Z}) \wedge \bigwedge_{i=1}^{d} \big(Z_0 \vee \big[X \wedge g_d^i(\bar{Z})\big]\big), \quad g_d^0(\bar{Z}) := Z_0.
\end{aligned}$$

LEMMA 2.9. *Abbreviate $L := \mathrm{L}(\mathbb{F}^{d'})$, $1 \le d' \le d$. In Lemmas 2.9 (a), (b), and (d) let $d = d'$.*

a) $\bar{A} \in L^{d+1}$ is a d-diamond of $L = \mathrm{L}(\mathbb{F}^{d'})$, if and only if $h_d(\bar{A}) = \mathbb{F}^d$.

b) Given a d-diamond $\bar{A}$ and B in $L = \mathrm{L}(\mathbb{F}^{d'})$, one has $B \neq \mathbf{0}$, if and only if $\hat{h}_d(B, \bar{A}) = \mathbb{F}^d$. In particular, $B \neq \mathbf{0}$ if and only if $\tilde{h}_d(B, \bar{z})$ is strongly satisfiable in L.

c) Let $L = \mathrm{L}(\mathbb{F}^{d'})$, $1 \le d' \le d$. For any $\bar{A} \in L^{d+1}$, one has $g_d^0(\bar{A}), \ldots g_d^d(\bar{A})$ a d-diamond of L and $d = d'$, if and only if $g_d(\bar{A}) \neq \mathbf{0}$. Moreover, $g_d^i(\bar{A}) = A_i$ if $\bar{A}$ is a d-diamond.

d) For any $B \in L = \mathrm{L}(\mathbb{F}^d)$, one has $B = \mathbb{F}^d$, if and only if $\tilde{g}_d(B, \bar{z})$ is weakly satisfiable in L, namely by a d-diamond.

Dunn et al. [2005, THEOREM 1] and Hagge [2007] provide terms t_d equivalent to $\mathbf{0}$ over $\mathrm{L}(\mathbb{C}^{d-1})$, but not over $\mathrm{L}(\mathbb{C}^d)$. A careful analysis of their construction reveals the length $|t_d|$ to be exponential in d. We observe

COROLLARY 2.10. *The term g_d has length quadratic in d. It is equivalent to $\mathbf{0}$ over $\mathrm{L}(\mathbb{F}^{d-1})$ but not over $\mathrm{L}(\mathbb{F}^d)$, independent of $\mathbb{F}$.*

PROOF OF LEMMA 2.9

a) Observe that for any $i > 0$, one has $A_i \perp A_j$ for all $0 < j \neq i$ if and only if $A_i = A_i \cap \bigcap_{0<j\neq i} A_j^{\perp}$.

b) Given a d-diamond $\bar{A}$, we have $h_d(\bar{A}) = \mathbb{F}^d$. Consider $B \neq \mathbf{0}$. Then, $B \not\subseteq A_i^{\perp}$ for some $i > 0$. It follows $((B + A_i^{\perp}) \cap A_i) + A_0 = A_i + A_0 = \mathbb{F}^d$, when $([(B + A_i^{\perp}) \cap A_i] + A_0) \cap A_j = A_j$ for all $j > 0$ and $\tilde{h}_d(B, \bar{A}) = \mathbb{F}^d$. Conversely, assume $\tilde{h}_d(B, \bar{A}) = \mathbb{F}^d$. Then $h_d(\bar{A}) = \mathbb{F}^d$ and $\bar{A}$ is a d-diamond. Assuming $B = \mathbf{0}$, one has $(B + A_i^{\perp}) \cap A_i = \mathbf{0}$ and $([(B + A_i^{\perp}) \cap A_i] + A_0) \cap A_j = A_0 \cap A_j = \mathbf{0}$, when $\tilde{h}_d(B, \bar{A}) = \mathbf{0}$, a contradiction.

c) Assume $g_d(\bar{A}) \neq \mathbf{0}$ and put $C_i := g_d^i(\bar{A}) = A_i \cap \bigcap_{i\neq j>0} A_j^{\perp}$ for $i > 0$. Assuming $C_i = \mathbf{0}$, we get $g_d(\bar{A}) \subseteq A_0^{\perp} \cap (A_0 + C_i) = A_0 \cap A_0^{\perp} = \mathbf{0}$, a contradiction. Thus, $C_i \neq \mathbf{0}$. Also, by definition, $C_i \subseteq A_i$ and $C_i \subseteq A_j^{\perp} \subseteq C_j^{\perp}$ for $i \neq j > 0$, i.e., the C_i, are pairwise orthogonal. Thus, $d \le \sum_{i=1}^{d} \dim(C_i) = \dim(\bigoplus_{i=1}^{d} C_i) \le d' \le d$, when $d = d'$, $\dim C_i = 1$, and $\sum_{i=1}^{d} C_i = \mathbb{F}^d$. Assuming $C_i \subseteq A_0$ for some $i > 0$ gives $g_d(\bar{A}) \subseteq A_0^{\perp} \cap (A_0 + C_i) = A_0 \cap A_0^{\perp} = \mathbf{0}$, a contradiction. Thus, $A_0 \cap C_i = \mathbf{0}$ and $\dim(A_0 + C_i)/A_0 = 1$ for all $i > 0$. Assuming $A_0 + C_i \neq A_0 + C_j$ for some $i \neq j$, $i, j > 0$ gives $A_0 = (A_0 + C_i) \cap (A_0 + C_j)$, when $g_d(\bar{A}) \subseteq A_0^{\perp} \cap (A_0 + C_i) \cap (A_0 + C_j) = \mathbf{0}$, a contradiction. It follows $A_0 + C_i = A_0 + C_j$ for all $i \neq j$, $i, j > 0$, when $A_0 + C_i \supseteq \sum_{j=1}^{d} C_j = \mathbb{F}^d$.

Conversely, if $g_d^0(\bar{A}), \ldots, g_d^d(\bar{A})$ is d-diamond in $\mathrm{L}(\mathbb{F}^d)$, then one calculates from the relations that $g_d(\bar{A}) = A_0^{\perp}$. Assuming $A_0^{\perp} = \mathbf{0}$ would imply $A_0 = \mathbb{F}^d$, $g_d^i(\bar{A}) = \mathbf{0}$ for all $i > 0$, and $\mathbb{F}^d = \mathbf{0}$: contradiction.

d) If $B = \mathbb{F}^d$, substitute into $\bar{z}$ a d-diamond $\bar{A}$. Conversely, assume $g_d(\bar{A}) \cap \bigcap_{i=1}^{d}(A_0 + (B \cap C_i)) \neq \mathbf{0}$ for some $\bar{A}$, where $C_i = g_d^i(\bar{A})$ for $i > 0$ and $C_0 = A_0$. Then, $g_d(\bar{A}) \neq \mathbf{0}$

and $\bar{A}$ is d-diamond by Proof of Lemma 2.9(c). Assume $\bar{A}$ is a d-diamond, $\tilde{g}_d(B, \bar{A}) \neq \mathbf{0}$ and $B \neq \mathbb{F}^d$. Then, $B \not\supseteq C_i$ for some $i > 0$, when $B \cap C_i = \mathbf{0}$, and it follows $\tilde{g}_d(B, \bar{A}) \subseteq A_0^\perp \cap (A_0 + (B \cap C_i)) = A_0^\perp \cap A_0 = \mathbf{0}$, a contradiction. Thus, $B = \mathbb{F}^d$. □

Based on Lemma 2.9, we conclude:

THEOREM 2.11. *Fix $L = \mathrm{L}(\mathbb{F}^d)$. Then, for any term $t(\bar{X})$, the following hold:*

(*a*) *$t(\bar{X})$ is weakly satisfiable in L iff $\tilde{h}_d(t(\bar{X}), \bar{Z})$ is strongly satisfiable in L.*
(*b*) *$t(\bar{X})$ is strongly satisfiable in L iff $\tilde{g}_d(t(\bar{X}), \bar{Z})$ is weakly satisfiable in L.*

In particular, weak and strong satisfiability over MOLs are mutually reducible in time polynomial in d and in the input length, uniformly in $\mathbb{F}$.

Theorem 2.7 thus extends to

COROLLARY 2.12. *For every $d \geq 3$, $\mathrm{sat}_{\mathrm{L}(\mathbb{F}^d)}$ is $\mathrm{BP}(\mathcal{NP}^0_{\mathrm{Re}\,\mathbb{F}})$–complete.*

Remark 2.13. We refrain from formally defining BSS machines over ortholattices, but mention that the results of Subsection 4.5 of `arXiv:1004.1696v2` (reducing, by the above methods, satisfiability of quantifier-free formulae to strong satisfiability of terms) reveal for $L := \mathrm{L}(\mathbb{F}^d)$, $d \geq 3$, SAT_L and sat_L polynomial-time complete for $\mathrm{BP}(\mathcal{NP}_L)$, and $\mathrm{SAT}_{L,L}$ and $\mathrm{sat}_{L,L}$ (without any encoding in terms of $\mathbb{F}$) polynomial-time complete for $\mathcal{NP}_L$.

3. VARIATIONS OF THE QUANTUM SATISFIABILITY PROBLEM

The first part of this section considers the satisfiability problem for terms with a fixed number of alterations between $\wedge$ and $\vee$ in their negation normal form; the second part studies the complexity of problems induced by quantified formulae.

3.1. Syntactically Restricted Terms

It is well-known that the Boolean satisfiability problem becomes no more simple when restricted to terms in conjunctive form ($\bigwedge\bigvee$–terms), and even with, at most, three literals per clause, a problem known as 3SAT—whereas 2SAT can be decided in polynomial time (cmp., e.g., Papadimitriou [1994, SECTION 9.2]). Schaefer [1978] has succeeded in closely delineating, syntactically, the border between $\mathcal{P}$ and $\mathcal{NP}$-completeness for Boolean satisfiability problems; see Chen [2009] for a modern presentation from the general perspective of *constraint satisfaction*. Regarding quantum logic, however, conjunctive form is semantically a proper restriction:

EXAMPLE 3.1. *$(x \wedge y) \vee (x \wedge \neg y)$ is a term in disjunctive form not equivalent over $\mathrm{L}(\mathbb{F}^2)$ to any term in conjunctive form.*

Thus, more than two alternations of $\bigvee$ and $\bigwedge$ are required to obtain reasonable syntactical restrictions of the satisfiability problem; and Theorem 3.3 below explores the boundary between $\mathcal{P}$ and $\mathrm{BP}(\mathcal{NP}^0_{\mathrm{Re}\,\mathbb{F}})$ in terms of the number of these alternations.

Definition 3.2.

(a) An ortholattice term without any occurrence of $\neg$ is called *positive*.
(b) A positive clause (or $\bigvee$–term) is a join of finitely many variables; a positive $\bigwedge$–term is a meet of finitely many variables.
A positive $\bigwedge\bigvee$–term is a meet of finitely many positive clauses; a positive $\bigvee\bigwedge$–term is a join of finitely many positive $\bigwedge$–clauses;
and so on, inductively.

(c) By recursive application of de Morgan's rules, any (ortholattice) term t is equivalent to a unique term of the form $\hat{t}(x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n)$, where $\hat{t}(x_1, \ldots, x_n; y_1, \ldots y_n)$ is positive: the negation normal form of t.
(d) Call a term t a $\bigwedge\bigvee\bigwedge$–term if its negation normal form is a positive $\bigwedge\bigvee\bigwedge$–term.

THEOREM 3.3.

(a) *Strong satisfiability over* $\mathrm{L}(\mathbb{F}^d)$*,* $d \geq 2$*, of* $\bigwedge\bigvee$*–terms, is independent of* $\mathbb{F}$ *and polynomial-time decidable.*
(b) *For any* $\mathbb{F}$ *and* $d \geq 3$*, strong satisfiability over* $\mathrm{L}(\mathbb{F}^d)$ *of* $\bigwedge\bigvee\bigwedge$*–terms is* $\mathrm{BP}(\mathcal{NP}^0_{\mathrm{Re}\,\mathbb{F}})$*–complete; and the variant with parameters is* $\mathcal{NP}_{\mathrm{Re}(\mathbb{F})}$*–complete.*
For $d \leq 2$*, the problem without parameters is* $\mathcal{NP}$*–complete.*
(c) *For every* $\mathbb{F}$ *and* $d \geq 3$*, the language*

$$\Big\{ \langle t(x_1, \ldots, x_n), s(x_1, \ldots, x_n) \rangle \mid s \text{ positive } \bigvee\bigwedge\bigvee\text{–term}, t \text{ positive } \bigwedge\bigvee\bigwedge\text{–term}, \\ \exists U_1, \ldots, U_n \in \mathrm{L}(\mathbb{F}^d) : t(U_1, \ldots, U_n) = \mathbf{1} \;\&\&\; s(U_1, \ldots, U_n) = \mathbf{0} \Big\} \;\subseteq\; \{0,1\}^*,$$

that is the question of whether two given positive terms t *and* s*, syntactically restricted as indicated, admit a joint assignment over* $\mathrm{L}(\mathbb{F}^d)$ *making* t *evaluate to* $\mathbb{F}^d$ *and* s *to* $\mathbf{0}$*, is complete for* $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{F}})$*. The analogous question in the case* with *parameters is* $\mathcal{NP}_{\mathbb{F}}$*–complete.*

Note that, avoiding complement, Theorem 3.3(c) does not require access to real and imaginary parts, and in particular, yields problems complete for $\mathcal{NP}_{\mathbb{C}}$ and $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{C}})$, respectively.

In view of the gap between Theorem 3.3(a) and (b), we ask:

Question 3.4. What is the computational complexity of the strong satisfiability problem for $\bigvee\bigwedge\bigvee$–terms? Does it depend on dimension or the ground field?

The proof of Theorem 3.3(a) is deferred until later in this subsection, as it relies on some technical details. To deal with Theorem 3.3(b) and (c), we use the following tool.

LEMMA 3.5. *Consider formulae* $\phi(\bar{x})$ *of the form*

$$\exists \bar{y}. \quad t(\bar{x}, \bar{y}) = \mathbf{1} \;\&\&\; s(\bar{x}, \bar{y}) = \mathbf{0}, \quad t \text{ and } s \text{ positive } \bigwedge\bigvee\bigwedge \text{ and } \bigvee\bigwedge\bigvee\text{–terms}. \tag{9}$$

(a) *The Boolean conjunction of finitely-many such formulae is, within MOLs, equivalent to one single such formula;*
(b) *To each of the formulae, (i)* $x \leq y$*, (ii)* $x = y$*, (iii)* $z = x \vee y$*, and (iv)* $z = x \wedge y$*, there exists a formula of the form of Equation (9) equivalent to it within MOLs.*
(c) *For any finite conjunction* $\psi(x)$ *of equations* $t_i(\bar{x}) = s_i(\bar{x})$ *between positive terms* t_i, s_i*, there is a formula* $\phi(\bar{x})$ *of the form of Equation (9) equivalent to* $\psi(\bar{x})$ *within MOLs.*
(d) *For any term* $t(\bar{x})$*, there is a* $\bigwedge\bigvee\bigwedge$*–term* $t'(\bar{x}, \bar{u})$ *such that* $t(\bar{x}) = \mathbf{1}$ *is equivalent to* $\exists \bar{u}.\, t'(\bar{x}, \bar{u}) = \mathbf{1}$ *in all MOLs.*

In all cases, the resulting formula can be computed from the input in polynomial time.

PROOF.

(a) Observe that $\exists \bar{z}: \quad t(\bar{x}, \bar{z}) = \mathbf{1} \;\&\&\; s(\bar{x}, \bar{z}) = \mathbf{0}$ and $\exists \bar{w}: \quad v(\bar{x}, \bar{w}) = \mathbf{1} \;\&\&\; u(\bar{x}, \bar{w}) = \mathbf{0}$ together are equivalent to $\exists \bar{z}, \bar{w}: \quad t(\bar{x}, \bar{z}) \wedge v(\bar{x}, \bar{w}) = \mathbf{1} \;\&\&\; s(\bar{x}, \bar{z}) \vee u(\bar{x}, \bar{w}) = \mathbf{0}$.

(b) Concerning Lemma 3.5(b.i), observe that

$$\begin{aligned} a \le b &\Leftrightarrow \exists v:\ a \vee v = \mathbf{1} \ \&\& \ (a \vee b) \wedge v = \mathbf{0} \\ &\Leftrightarrow \exists v:\ (a \wedge b) \vee v = \mathbf{1} \ \&\& \ b \wedge v = \mathbf{0}. \end{aligned}$$

Indeed, for the first equivalence, argue as in the proof of Example 1.15(g), with $v = \neg(a \vee b)$ in one direction and v in place of $\neg(a \vee b)$ in the other. To prove the second equivalence, replace in this reasoning a by $a \wedge b$ and $a \vee b$ by b. Applying Lemma 3.5(a) to $a \le b$ and $b \le a$, yields

$$\begin{aligned} a = b &\Leftrightarrow \exists v, w:\ (a \vee v) \wedge (b \vee w) = \mathbf{1} \ \&\& \ ((a \vee b) \wedge v) \vee ((a \vee b) \wedge w) = \mathbf{0} \\ &\Leftrightarrow \exists v, w:\ ((a \wedge b) \vee v) \wedge ((a \wedge b) \vee w) = \mathbf{1} \ \&\& \ (a \wedge v) \vee (b \wedge w) = \mathbf{0}. \end{aligned}$$

Now, substituting $b \vee c$ for b in the first line establishes Lemma 3.5(b.iii); and substituting $b \wedge c$ for b in the second line establishes Lemma 3.5(b.iv).

c) The method of intermediate values turns the given equations into ones of the forms from Lemma 3.5(b.iii) and Lemma 3.5(b.iv); which Lemma 3.5(a) combines into a single one.

d) Choose $\hat{t}(\bar{x}, \bar{y})$, a positive term yielding the negation normal form of $t(\bar{x})$. By Lemma 3.5(c), there are positive terms $t^+(\bar{x}, \bar{y}, \bar{u}) \in \bigwedge \bigvee \bigwedge$ and $t^-(\bar{x}, \bar{y}, \bar{u}) \in \bigvee \bigwedge \bigvee$, such that $\hat{t}(\bar{x}, \bar{y}) = \mathbf{1}$ is within MOLs equivalent to $\exists \bar{u}.\ t^+(\bar{x}, \bar{y}, \bar{u}) = \mathbf{1} \ \&\& \ t^-(\bar{x}, \bar{y}, \bar{u}) = \mathbf{0}$. Now put $t'(\bar{x}, \bar{u}) = t^+(\bar{x}, \neg\bar{x}, \bar{u}) \wedge \neg t^-(\bar{x}, \neg\bar{x}, \bar{u})$. □

Proof of Theorem 3.3(b) and (c). In view of Lemma 3.5(d), Theorem 3.3(b) follows from Theorems 2.7 and 1.20.

Concerning Theorem 3.3(c), to see the problem in $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{F}})$ and not just in $\mathrm{BP}(\mathcal{NP}^0_{\mathrm{Re}\,\mathbb{F}})$, observe that, in the proof of Proposition 2.1(a), only evaluating orthocomplements Equation (5.iii) requires access to real and imaginary parts.

Regarding hardness, we modify the proof of Theorem 2.3. First, observe that the terms $X \ominus_{\bar{Z}} Y$ and $X \otimes_{\bar{z}} Y$ are positive and so are all terms occurring in Equations (8.i'), (8.iii'), (8.iv'), and (8.vi'). Use Lemma 3.5(c) to combine the equations obtained by these steps into a formula $\phi(\bar{X}; \bar{Z})$ of the form of Equation (9), and observe that one has $\phi(\bar{A}, \bar{r}')$ valid in L iff $\bar{r}'$ is the point-wise image under $\Theta_{\bar{A}}$ of a common root $\bar{r}$ in $\mathbb{F}$ of the p_j (Equation (5.v)): The non-positive term $\sigma_{\bar{Z}}(X)$, requiring roots in $\mathrm{Re}\,\mathbb{F}$, has been omitted. In the case with parameters, substitute $\bar{E}$ for $\bar{Z}$. □

Preparing for the proof of Theorem 3.3(a), consider the equations

$$\mathbf{1} \ = \ a_k \vee a_\ell \ = \ a_k \vee \neg a_\ell \ = \ \neg a_k \vee a_\ell \ = \ \neg a_k \vee \neg a_\ell \quad (1 \le k < \ell \le n). \tag{10}$$

In particular, elements satisfying these relations exist in $\mathrm{L}(\mathbb{F}^2)$ and, by Observation 1.14, also in $\mathrm{L}(\mathbb{F}^{2d})$ for every $\mathbb{F}$ and d. But Equation (10) cannot be satisfied in odd dimensions. Instead, consider the following:

Example 3.6. *For every $d \ge 2$ and $\mathbb{F}$ and $n \in \mathbb{N}$, there exist $U_1, \ldots, U_n \in \mathrm{L}(\mathbb{F}^d)$ with*

$$\mathbb{F}^d \ = \ U_k + U_\ell^\perp \ = \ U_k^\perp + U_\ell^\perp \ = \ U_k + U_\ell + U_j \quad (k \ne \ell \ne j \ne k).$$

Indeed, the case of even d has been treated above. Whereas the $(3 + 2d)$-dimensional case follows from Observation 1.14 by combining a 3D instance $(U_1, \ldots, U_n)$ with an even-dimensional one $(V_1, \ldots, V_n)$ to $(U_1 \oplus V_1, \ldots, U_n \oplus V_n)$. In the remaining case $d = 3$, observe that for any three distinct $k \in \mathbb{N}$, the vectors $\vec{v}_k := (1, k, k^2) \in \mathbb{F}^3$ form a Vandermonde matrix and are thus linearly independent; hence, $U_k := \mathbb{F}\vec{v}_k$ satisfy $U_k + U_\ell + U_j = \mathbb{F}^d$ for every $k \ne \ell \ne j \ne k$. Moreover, $\langle \vec{v}_k \mid \vec{v}_\ell \rangle = 1 + k\ell + k^2\ell^2 > 0$ shows $\vec{v}_k \not\perp \vec{v}_\ell$; hence, $\dim(U_k + U_\ell^\perp) = \dim(U_k) + 3 - \dim(U_\ell) - \dim(U_k \cap U_\ell^\perp) = 1 + 3 - 1$

by the dimension formula. Similarly, $U_k^\perp \neq U_\ell^\perp$ and $\dim(U_k^\perp) = 2 = \dim(U_\ell^\perp)$ imply $\dim(U_k^\perp + U_\ell^\perp) \geq 3$.

LEMMA 3.7.

(a) *Let $t(x_1, \ldots, x_n)$ denote a $\bigwedge\bigvee$–term with at least two different literals in each clause. Then, t is strongly satisfiable over $\mathrm{L}(\mathbb{F}^{2d})$ for every $\mathbb{F}$ and every d.*
(b) *Let $t(x_1, \ldots, x_n)$ denote a $\bigwedge\bigvee$–term with at least three different literals in each clause. Then, t is strongly satisfiable over $\mathrm{L}(\mathbb{F}^{2d+1})$ for every $\mathbb{F}$ and every $d \geq 1$.*
More precisely, for $U_1, \ldots, U_n \in \mathrm{L}_d(\mathbb{F}^{2d+1})$ according to Example 3.6, every choice of $V_j \in \{U_j, U_j^\perp\}$ gives rise to a strongly satisfying assignment $(V_1, \ldots, V_n)$ of t.
(c) *For a $\bigwedge\bigvee$–term $t(x_1, \ldots, x_n)$ with exactly two different literals in each clause, the following are equivalent:*
  (i) *t is strongly satisfiable over $\mathrm{L}(\mathbb{F}^d)$ for some $\mathbb{F}$ and some odd d.*
  (ii) *t is strongly satisfiable over $\{\mathbf{0}, \mathbf{1}\}$.*
  (iii) *For $U_1, \ldots, U_n \in \mathrm{L}_d(\mathbb{F}^{2d+1})$ from Example 3.6, there exist $V_j \in \{U_j, U_j^\perp\}$, such that $\bar{V}$ constitutes a strongly satisfying assignment of t.*
  (iv) *t is strongly satisfiable over $\mathrm{L}(\mathbb{F}^d)$ for every $\mathbb{F}$ and every odd d.*

PROOF.

(a) As argued before Example 3.6, $\mathrm{L}(\mathbb{F}^{2d})$ contains $U_1, \ldots, U_n$, satisfying Equation (10), i.e., rendering $\mathbb{F}^{2d}$ every clause $u \vee v$ with u, v mapped to distinct members of $\{U_1, U_1^\perp, \ldots, U_n, U_n^\perp\}$.
(b) Similarly, observe that, for any u, v, w mapped to three distinct members of $\{U_j, U_j^\perp, U_k, U_k^\perp, U_\ell, U_\ell^\perp\}$, $u \vee v \vee w$ evaluates to $\mathbb{F}^{2d+1}$.

(c i⇒ii) Let $\bar{V}$ denote a strongly satisfying assignment over $\mathrm{L}(\mathbb{F}^{2d+1})$. We claim that the derived assignment $a_j := \mathbf{1}$ for $\dim(V_j) \geq d+1$ and $a_j := \mathbf{0}$ for $\dim(V_j^\perp) \geq d+1$ is also a satisfying one. To this end, consider an arbitrary clause $u \vee v$ of t with literals $u, v \in \{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$. By hypothesis, it evaluates to $\mathbb{F}^d$ when plugging in $\bar{V}$ for $\bar{x}$, requiring $2d+1 \leq \dim(u[\bar{V}]) + \dim(v[\bar{V}])$, and thus, that at least one of u, v had been assigned a subspace of dimension $\geq d+1$, which in the derived assignment becomes $\mathbf{1}$ and keeps the clause `true`.

(c ii⇒iii) Let $\bar{a}$ denote a satisfying assignment over $\{\mathbf{0}, \mathbf{1}\}$. We claim that the derived assignment $V_j := U_j^\perp$ for $a_j = \mathbf{1}$ and $V_j := U_j$ for $a_j = \mathbf{0}$ is a satisfying one. According to Example 3.6, this makes all clauses $u \vee v$, $(u \neq v)$, evaluate to $\mathbb{F}^d$, for which at least one of the literals u, v are assigned to some $U_j^\perp$. On the other hand, since $u[\bar{a}] \vee v[\bar{a}] = \mathbf{1}$, by construction, also, at least one of $u[\bar{V}]$ and $v[\bar{V}]$ is of the form $U_j^\perp$.

(c iii⇒iv) follows from Example 3.6. And (c iv⇒i) is a tautology. □

PROOF OF THEOREM 3.3(a). Given a $\bigwedge\bigvee$–term $t(x_1, \ldots, x_n)$, first eliminate all clauses with only one literal by substituting it with $\mathbf{1}$—this simplification can obviously be performed in polynomial time and maintains t's $\bigwedge\bigvee$-form, as well as strong satisfiability. If it fails (like for instance in $\neg x \wedge \neg y \wedge (x \vee y)$), reject t. Otherwise, in the even-dimensional case, accept. In odd dimensions, collect all clauses with precisely two (remaining) literals, and report whether this instance of 2SAT is satisfiable—as mentioned above, in polynomial time. It remains to assert the correctness of this algorithm. Regarding the case of even dimensions, this holds due to Lemma 3.7(a). Over $\mathrm{L}(\mathbb{F}^{2d+1})$, any satisfying assignment of t must, in particular, make all its two-literal clauses evaluate to `true`, which requires their conjunction to be a positive instance for 2SAT, according to Lemma 3.7(c i⇒ii). Conversely, if the two-literal clauses are

satisfiable over $\{0,1\}$, then both, they *and* the clauses with at least three literals, admit a joint satisfying assignment from $\{U_1, U_1^\perp, \ldots, U_n, U_n^\perp\} \subseteq \mathrm{L}(\mathbb{F}^{2d+1})$, according to Lemmas 3.7(b) and (c ii⇒iii). □

3.2. Quantified Quantum Propositions and Two Polynomial Hierarchies

Recall that Stockmeyer's polynomial hierarchy starts with $\Sigma_0^{\mathcal{P}} = \mathcal{P} = \Pi_0^{\mathcal{P}}$ and $\Sigma_1^{\mathcal{P}} = \mathcal{NP}$ and $\Pi_1^{\mathcal{P}} = \mathrm{co}\mathcal{NP}$; while higher classes $\Sigma_\ell^{\mathcal{P}}$ and $\Pi_\ell^{\mathcal{P}}$ ($\ell \geq 2$) can equivalently be characterized syntactically and semantically. For the latter, $\Sigma_\ell^{\mathcal{P}}$ contains precisely those decision problems accepted by nondeterministic polynomial-time Turing machines with oracle access to some $V \in \Sigma_{\ell-1}^{\mathcal{P}}$ (equivalently, to some $V' \in \Pi_{\ell-1}^{\mathcal{P}}$); and, $\Pi_\ell^{\mathcal{P}}$ consists of the complements of members from $\Sigma_\ell^{\mathcal{P}}$ [Papadimitriou 1994]. Alternatively, $\Sigma_\ell^{\mathcal{P}}$ and $\Pi_\ell^{\mathcal{P}}$ contain all decision problems of the form

$$\begin{aligned}\big\{\bar{z} \in \{\mathbf{0},\mathbf{1}\}^n \;\big|\; n \in \mathbb{N},\ \exists \bar{y}^{(1)} \in \{\mathbf{0},\mathbf{1}\}^{p(n)}\ \forall \bar{y}^{(2)} \in \{\mathbf{0},\mathbf{1}\}^{p(n)}\ \exists \bar{y}^{(3)} \in \{\mathbf{0},\mathbf{1}\}^{p(n)}\ \forall \bar{y}^{(4)} \ldots \\ \ldots \mathrm{Q}_\ell\, \bar{y}^{(\ell)} \in \{\mathbf{0},\mathbf{1}\}^{p(n)} :\ \langle \bar{z}, \bar{y}^{(1)}, \ldots \bar{y}^{(\ell)} \rangle \in V\big\} \qquad (11)\\ \big\{\bar{z} \in \{\mathbf{0},\mathbf{1}\}^n \;\big|\; n \in \mathbb{N},\ \forall \bar{y}^{(1)} \in \{\mathbf{0},\mathbf{1}\}^{p(n)}\ \exists \bar{y}^{(2)} \in \{\mathbf{0},\mathbf{1}\}^{p(n)}\ \forall \bar{y}^{(3)} \in \{\mathbf{0},\mathbf{1}\}^{p(n)}\ \exists \bar{y}^{(4)} \ldots \\ \ldots \mathrm{Q}'_\ell\, \bar{y}^{(\ell)} \in \{\mathbf{0},\mathbf{1}\}^{p(n)} :\ \langle \bar{z}, \bar{y}^{(1)}, \ldots \bar{y}^{(\ell)} \rangle \in V'\big\},\end{aligned}$$

respectively, with $V, V' \in \mathcal{P}$ and $p \in \mathbb{N}[N]$, a polynomial. Here, Q_ℓ denotes the existential quantifier when ℓ is odd and otherwise the universal one—vice versa for Q'.

Generalizing the Cook-Levin Theorem, a natural problem complete for $\Sigma_\ell^{\mathcal{P}}$ asks for the truth of a given Boolean formula with ℓ blocks of alternating quantifiers, starting with the existential one:

$$\begin{aligned}\mathrm{SAT}^\ell \;=\; \big\{\langle t(\bar{x}^{(1)}, \bar{x}^{(2)}, \ldots \bar{x}^{(\ell)})\rangle \;\big|\; n_1, \ldots n_\ell \in \mathbb{N},\ \exists \bar{a}^{(1)} \in \{0,1\}^{n_1}\ \forall \bar{a}^{(2)} \in \{0,1\}^{n_2}\ \exists \bar{a}^{(3)} \\ \ldots \mathrm{Q}_\ell\, \bar{a}^{(\ell)} \in \{0,1\}^{n_\ell} :\ t(\bar{a}^{(1)}, \bar{a}^{(2)}, \ldots \bar{a}^{(\ell)}) = 1\big\}.\end{aligned}$$

So, binarily encoded terms $\langle t(\bar{x}^{(1)}, \bar{x}^{(2)}, \ldots, \bar{x}^{(\ell)})\rangle$ replace $\bar{z}$ in Equation (11). $\overline{\mathrm{SAT}}^\ell$ is defined similarly but starting with the universal quantifier—and complete for $\Pi_\ell^{\mathcal{P}}$. Moreover, the following problem QSAT is complete for PSPACE:

$$\big\{\langle t(x_1, \ldots x_n)\rangle \;\big|\; n \in \mathbb{N}\ \exists a_1 \in \{0,1\}\ \forall a_2 \in \{0,1\}\ \exists a_3 \ldots \mathrm{Q}_n\, a_n \in \{0,1\} :\ t(a_1, \ldots a_n) = 1\big\}.$$

More generally, sequential polynomial space corresponds to parallel polynomial time, as well as to parallel alternating time [Chandra et al. 1981]; hence, PSPACE is sometimes also denoted as PAR = PAT.

Both the polynomial hierarchy and its two characterizations translate (although with notably different proofs) to the BSS setting [Cucker 1993, Section 4], [Blum et al. 1998, Section 21.4]. $\Sigma_{\ell,\mathbb{F}}^{\mathcal{P}}$ contains precisely those decision problems accepted by nondeterministic polynomial-time BSS machines over $\mathbb{F}$ with oracle access to some $\mathbb{V} \in \Sigma_{\ell-1,\mathbb{F}}^{\mathcal{P}}$ (equivalently, to some $\mathbb{V}' \in \Pi_{\ell-1,\mathbb{F}}^{\mathcal{P}}$); and, $\Pi_{\ell,\mathbb{F}}^{\mathcal{P}}$ consists of the complements of members from $\Sigma_{\ell,\mathbb{F}}^{\mathcal{P}}$. For the former characterization, $\Sigma_{\ell,\mathbb{F}}^{\mathcal{P}}$ and $\Pi_{\ell,\mathbb{F}}^{\mathcal{P}}$ consist of all sets of the form

$$\begin{aligned}&\big\{\bar{z} \in \mathbb{F}^n \;\big|\; n \in \mathbb{N},\ \exists \bar{y}^{(1)} \in \mathbb{F}^{p(n)}\ \forall \bar{y}^{(2)} \in \mathbb{F}^{p(n)}\ \exists \bar{y}^{(3)} \ldots \mathrm{Q}_\ell\, \bar{y}^{(\ell)} \in \mathbb{F}^{p(n)} : \langle \bar{z}, \bar{y}^{(1)}, \ldots \bar{y}^{(\ell)} \rangle \in \mathbb{V}\big\}\\ &\big\{\bar{z} \in \mathbb{F}^n \;\big|\; n \in \mathbb{N},\ \forall \bar{y}^{(1)} \in \mathbb{F}^{p(n)}\ \exists \bar{y}^{(2)} \in \mathbb{F}^{p(n)}\ \forall \bar{y}^{(3)} \ldots \mathrm{Q}'_\ell\, \bar{y}^{(\ell)} \in \mathbb{F}^{p(n)} : \langle \bar{z}, \bar{y}^{(1)}, \ldots \bar{y}^{(\ell)} \rangle \in \mathbb{V}'\big\},\end{aligned}$$

respectively, with $\mathbb{V}, \mathbb{V}' \in \mathcal{P}_{\mathbb{F}}$ and $p \in \mathbb{N}[N]$; cmp., also, Bournez et al. [2006]. And

$$\begin{aligned}
\mathrm{FEAS}^{2\ell-1}_{\mathbb{F},\mathbb{F}} =\big\{\langle p_1, \dots p_k\rangle \;\big|\; & k, n_1, \dots \in \mathbb{N},\ p_j \in \mathbb{F}[\bar{X}^{(1)}, \dots \bar{X}^{(2\ell-1)}],\ \exists \bar{y}^{(1)} \in \mathbb{F}^{n_1}\ \forall \bar{y}^{(2)} \in \mathbb{F}^{n_2} \\
& \exists \bar{y}^{(3)}\ \dots \exists \bar{y}^{(2\ell-1)} \in \mathbb{F}^{n_{2\ell-1}} : p_1(\bar{y}^{(1)}, \dots \bar{y}^{(2\ell-1)}) = 0\ \ \&\& \cdots \&\&\ \ p_k(\bar{y}^{(1)}, \dots \bar{y}^{(2\ell-1)}) = 0\big\} \\
\mathrm{FEAS}^{2\ell}_{\mathbb{F},\mathbb{F}} =\big\{\langle p_1, \dots p_k\rangle \;\big|\; & k, n_1, \dots \in \mathbb{N},\ p_j \in \mathbb{F}[\bar{X}^{(1)}, \dots \bar{X}^{(2\ell)}],\ \exists \bar{y}^{(1)} \in \mathbb{F}^{n_1}\ \forall \bar{y}^{(2)} \in \mathbb{F}^{n_2} \\
& \exists \bar{y}^{(3)}\ \dots \forall \bar{y}^{(2\ell)} \in \mathbb{F}^{n_{2\ell}} : p_1(\bar{y}^{(1)}, \dots \bar{y}^{(2\ell)}) \neq 0\ \ || \cdots ||\ \ p_k(\bar{y}^{(1)}, \dots \bar{y}^{(2\ell)}) \neq 0\big\} \\
\mathrm{FEAS}^{2\ell-1}_{\mathbb{Z},\mathbb{F}} =\big\{\langle p_1, \dots p_k\rangle \;\big|\; & k, n_1, \dots \in \mathbb{N},\ p_j \in \mathbb{Z}[\bar{X}^{(1)}, \dots \bar{X}^{(2\ell-1)}],\ \exists \bar{y}^{(1)} \in \mathbb{F}^{n_1}\ \forall \bar{y}^{(2)} \in \mathbb{F}^{n_2} \\
& \exists \bar{y}^{(3)} \dots \exists \bar{y}^{(2\ell-1)} \in \mathbb{F}^{n_{2\ell-1}} : p_1(\bar{y}^{(1)}, \dots \bar{y}^{(2\ell-1)}) = 0\ \ \&\& \cdots \&\&\ \ p_k(\bar{y}^{(1)}, \dots \bar{y}^{(2\ell-1)}) = 0\big\} \\
\mathrm{FEAS}^{2\ell}_{\mathbb{Z},\mathbb{F}} =\big\{\langle p_1, \dots p_k\rangle \;\big|\; & k, n_1, \dots \in \mathbb{N},\ p_j \in \mathbb{Z}[\bar{X}^{(1)}, \dots \bar{X}^{(2\ell)}],\ \exists \bar{y}^{(1)} \in \mathbb{F}^{n_1}\ \forall \bar{y}^{(2)} \in \mathbb{F}^{n_2} \\
& \exists \bar{y}^{(3)} \dots \forall \bar{y}^{(2\ell)} \in \mathbb{F}^{n_{2\ell}} : p_1(\bar{y}^{(1)}, \dots \bar{y}^{(2\ell)}) \neq 0\ \ || \cdots ||\ \ p_k(\bar{y}^{(1)}, \dots \bar{y}^{(2\ell)}) \neq 0\big\}
\end{aligned}$$

are complete for $\Sigma^{\mathcal{P}}_{2\ell-1,\mathbb{F}}$, $\Sigma^{\mathcal{P}}_{2\ell,\mathbb{F}}$, $\mathrm{BP}(\Sigma^{\mathcal{P},0}_{2\ell-1,\mathbb{F}})$, and $\mathrm{BP}(\Sigma^{\mathcal{P},0}_{2\ell,\mathbb{F}})$, respectively. Note that (Observation 1.5) the matrix form defining $\mathrm{FEAS}^{\ell}_{\mathbb{F},\mathbb{F}}$ and $\mathrm{FEAS}^{\ell}_{\mathbb{Z},\mathbb{F}}$ can be relaxed to arbitrary finite Boolean combinations of, and in the case admitting an order also restricted to one single, polynomial equality or inequality—depending on ℓ's parity!

Space complexity does not translate as nicely to the BSS setting [Michaux 1989; Cucker and Briquel 2007]; however, $\mathsf{PAT}_{\mathbb{F}}$ is a natural counterpart to $\mathsf{PAT} = \mathsf{PSPACE}$ and $\mathrm{QSAT}_{\mathbb{F},\mathbb{F}}$ complete for it, where $\mathsf{PAT}_{\mathbb{F}}$ consists of all subsets of $\mathbb{F}^*$ of the form

$$\big\{\bar{z} \in \mathbb{F}^n \;\big|\; n \in \mathbb{N},\ \exists y_1 \in \mathbb{F}\ \forall y_2 \in \mathbb{F}\ \exists y_3 \in \mathbb{F}\ \forall y_4 \dots\ \dots \mathrm{Q}_n y_n \in \mathbb{F} : \langle \bar{z}, \bar{y}\rangle \in \mathbb{V}\big\} \qquad \text{and}$$

$$\begin{aligned}
\mathrm{QSAT}_{S,R} :=\ \big\{\langle p_1, \dots, p_k\rangle \;\big|\; & k, n \in \mathbb{N},\ p_j \in S[X_1, \dots, X_n], \\
& \exists y_1 \in R\ \forall y_2 \in R\ \exists y_3 \in R\ \forall y_4 \dots\dots \mathrm{Q}_n y_n \in R : p_1(\bar{y}) = \cdots = p_k(\bar{y}) = 0\big\},
\end{aligned}$$

with $\mathbb{V}$ running through $\mathcal{P}_{\mathbb{F}}$ [Cucker 1993, Theorem 4.1]; similarly, for $\mathrm{QSAT}_{\mathbb{Z},\mathbb{F}}$ complete for $\mathrm{BP}(\mathsf{PAT}^0_{\mathbb{F}})$. Natural problems in $\mathsf{PAR}_{\mathbb{C}} \subset \mathsf{PAT}_{\mathbb{C}}$ and $\mathsf{PAR}_{\mathbb{R}} \subset \mathsf{PAT}_{\mathbb{R}}$ traditionally arise in semi-/algebraic geometry [Canny 1988; Giusti and Heintz 1991; Lecerf 2000; Jeronimo et al. 2004; Bürgisser and Scheiblechner 2009; Basu and Zell 2010; Scheiblechner 2012]; cf., also, Cucker and Grigoriev [1997].

In view of our generalization of Boolean satisfiability to MOLs L (Definition 1.13(f)), this suggests to consider first-order quantified quantum (i.e., predicate) logic:

$$\begin{aligned}
\mathrm{SAT}^{\ell}_{L} :=\ & \big\{\langle t(\bar{x}^{(1)}, \dots \bar{x}^{(\ell)})\rangle \;\big|\; n_1, \dots n_\ell \in \mathbb{N},\ \exists \bar{a}^{(1)} \in L^{n_1}\ \forall \bar{a}^{(2)} \in L^{n_2}\ \exists \bar{a}^{(3)} \dots \\
& \qquad \dots \mathrm{Q}_\ell\, \bar{a}^{(\ell)} \in L^{n_\ell} :\ t_L(\bar{a}^{(1)}, \bar{a}^{(2)}, \dots \bar{a}^{(\ell)}) = \mathbf{1}\big\}, \\
\overline{\mathrm{SAT}}^{\ell}_{L} :=\ & \big\{\langle t(\bar{x}^{(1)}, \dots \bar{x}^{(\ell)})\rangle \;\big|\; n_1, \dots n_\ell \in \mathbb{N},\ \forall \bar{a}^{(1)} \in L^{n_1}\ \exists \bar{a}^{(2)} \in L^{n_2}\ \forall \bar{a}^{(3)} \dots \\
& \qquad \dots \mathrm{Q}'_\ell\, \bar{a}^{(\ell)} \in L^{n_\ell} :\ t_L(\bar{a}^{(1)}, \bar{a}^{(2)}, \dots \bar{a}^{(\ell)}) \neq \mathbf{1}\big\}, \\
\mathrm{sat}^{\ell}_{L} :=\ & \big\{\langle t(\bar{x}^{(1)}, \dots \bar{x}^{(\ell)})\rangle \;\big|\; n_1, \dots n_\ell \in \mathbb{N},\ \exists \bar{a}^{(1)} \in L^{n_1}\ \forall \bar{a}^{(2)} \in L^{n_2}\ \exists \bar{a}^{(3)} \dots \\
& \qquad \dots \mathrm{Q}_\ell\, \bar{a}^{(\ell)} \in L^{n_\ell} :\ t_L(\bar{a}^{(1)}, \bar{a}^{(2)}, \dots \bar{a}^{(\ell)}) \neq \mathbf{0}\big\}, \\
\overline{\mathrm{sat}}^{\ell}_{L} :=\ & \big\{\langle t(\bar{x}^{(1)}, \dots \bar{x}^{(\ell)})\rangle \;\big|\; n_1, \dots n_\ell \in \mathbb{N},\ \forall \bar{a}^{(1)} \in L^{n_1}\ \exists \bar{a}^{(2)} \in L^{n_2}\ \forall \bar{a}^{(3)} \dots \\
& \qquad \dots \mathrm{Q}'_\ell\, \bar{a}^{(\ell)} \in L^{n_\ell} :\ t_L(\bar{a}^{(1)}, \bar{a}^{(2)}, \dots \bar{a}^{(\ell)}) = \mathbf{0}\big\}, \\
\mathrm{QSAT}_{L} :=\ & \big\{\langle t(x_1, \dots x_n)\rangle \;\big|\; \exists a_1 \in L\ \forall a_2 \in L\ \exists a_3 \in L\ \forall a_4\ \dots \mathrm{Q}_n\, a_n \in L : t_L(\bar{a}) = \mathbf{1}\big\}, \\
\mathrm{qsat}_{L} :=\ & \big\{\langle t(x_1, \dots x_n)\rangle \;\big|\; \exists a_1 \in L\ \forall a_2 \in L\ \exists a_3 \in L\ \forall a_4\ \dots \mathrm{Q}_n\, a_n \in L :\ t_L(\bar{a}) \neq \mathbf{0}\big\},
\end{aligned}$$

and analogously for terms *with parameters*; cmp., also, Román [2006]. Observe that in all of $\mathrm{QSAT}_{\mathbb{F}}$, QSAT_L, and qsat_L, dummy variables are admitted; in the latter, two such variables x can be camouflaged by meeting with $(x \vee \neg x)$.

We emphasize that the definitions of SAT^{ℓ}_L, sat^{ℓ}_L do *not* depend on the parity of ℓ.

THEOREM 3.8. *Fix* $\ell \in \mathbb{N}$.

(*a*) *For any infinite two-dimensional MOL L, both* SAT_L^ℓ *and* sat_L^ℓ *are* $\Sigma_\ell^{\mathcal{P}}$*–complete; and* $\overline{\mathrm{SAT}}_L^\ell$, $\overline{\mathrm{sat}}_L^\ell$ *are* $\Pi_\ell^{\mathcal{P}}$*–complete; while* QSAT_L *and* qsat_L *are* PSPACE*–complete.*

(*b*) *For* $d \geq 3$*, both* $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d)}^\ell$ *and* $\mathrm{sat}_{\mathrm{L}(\mathbb{F}^d)}^\ell$ *are* $\mathrm{BP}(\Sigma_{\ell,\mathrm{Re}\,\mathbb{F}}^{\mathcal{P},0})$*–complete; and* $\overline{\mathrm{SAT}}_{\mathrm{L}(\mathbb{F}^d)}^\ell$ *and* $\overline{\mathrm{sat}}_{\mathrm{L}(\mathbb{F}^d)}^\ell$ *are* $\mathrm{BP}(\Pi_{\ell,\mathrm{Re}\,\mathbb{F}}^{\mathcal{P},0})$*–complete; while* $\mathrm{QSAT}_{\mathrm{L}(\mathbb{F}^d)}$ *and* $\mathrm{qsat}_{\mathrm{L}(\mathbb{F}^d)}$ *are* $\mathrm{BP}(\mathsf{PAT}_{\mathrm{Re}\,\mathbb{F}}^0)$*–complete.*

(*c*) *Similarly, for* $d \geq 3$*, the above problems with parameters are* $\Sigma_{\ell,\mathrm{Re}(\mathbb{F})}^{\mathcal{P}}$*–complete,* $\Pi_{\ell,\mathrm{Re}(\mathbb{F})}^{\mathcal{P}}$*–complete, and* $\mathsf{PAT}_{\mathrm{Re}(\mathbb{F})}$*–complete, respectively.*

Since Poonen [2009] proved $\mathrm{FEAS}_{\mathbb{Z},\mathbb{Q}}^3$ undecidable, we conclude:

COROLLARY 3.9. $\mathrm{SAT}_{\mathrm{L}(\mathbb{Q}^3)}^3$ *and* $\mathrm{sat}_{\mathrm{L}(\mathbb{Q}^3)}^3$ *are undecidable (to a Turing machine, recall Example 1.6(c)).*

To the best of our knowledge, Theorem 3.8 cannot be just deduced from the satisfiability case $\ell = 1$, but requires additional considerations, including application of Subsection 2.3 to show that Boolean combinations of ortholattice identities are equivalent to existentially (alternatively, universally) quantified identities. We omit the lengthy and technical details here and instead refer to Sections 4.5 and 5.2 in `arXiv:1004.1696v2`.

4. SATISFIABILITY IN INDEFINITE (YET FINITE) DIMENSION

We now consider satisfiability questions quantifying existentially, not just over assignments but also over the (finite) dimension the assignment lives in.

Similar to Observation 1.14, we record

OBSERVATION 4.1. *Let t be any term and* $d = d' + d''$.

(*a*) *If t is weakly satisfiable in* $\mathrm{L}(\mathbb{F}^{d'})$*, then it is so in* $\mathrm{L}(\mathbb{F}^d)$.

(*b*) *If t is strongly satisfiable in both* $\mathrm{L}(\mathbb{F}^{d'})$ *and in* $\mathrm{L}(\mathbb{F}^{d''})$*, then it is so in* $\mathrm{L}(\mathbb{F}^d)$.

EXAMPLE 4.2. *Recall Lemma 2.9.*

(*a*) *For any d, the term* h_d *is strongly satisfiable in* $\mathrm{L}(\mathbb{F}^{d'})$ *if and only if d divides* d'.

(*b*) *For any k, there exists a term* t_k *of length* $\mathcal{O}(k)$ *strongly satisfiable over* $\mathrm{L}(\mathbb{F}^d)$ *for* $d = 2^k$*, but not for* $d < 2^k$.

(*c*) *For any d, the term* g_d *is weakly satisfiable in* $\mathrm{L}(\mathbb{F}^{d'})$ *if and only if* $d \leq d'$.

PROOF.

(a) Suppose $d' = dk$. Considering $\mathbb{F}^{d'}$ as $\mathbb{F}^d \oplus \cdots \oplus \mathbb{F}^d$, there exists a d-diamond $\bar{A}$ in $\mathrm{L}(\mathbb{F}^d)$, and thus, a d'-diamond in $\mathrm{L}(\mathbb{F}^{d'})$ with $A'_i = A_i \oplus \ldots \oplus A_i$, strongly satisfying h_d by Lemma 2.9(a). Conversely, any strongly satisfying assignment $\bar{A}$ of h_d over $\mathbb{F}^{d'}$ constitutes, by Lemma 2.9(a), a d-diamond; hence, d divides d'.

(b) Consider the $(2n+1)$-variate term

$$x_{n+1} \wedge \bigwedge_{i=1}^{n}((x_i \vee \neg y_i) \wedge (y_i \vee \neg x_i) \wedge (\neg x_i \vee \neg y_i) \wedge ((x_{i+1} \wedge (x_i \vee y_i)) \vee (\neg x_{i+1} \wedge \neg(x_i \vee y_i)))).$$

Consider any satisfying assignment $(U_1, V_1, \ldots, U_n, V_n, U_{n+1})$ in $\mathrm{L}(\mathbb{F}^d)$. Note that $U_i + V_i^\perp = \mathbb{F}^d$ implies $\dim(U_i) + \dim(V_i^\perp) \geq d$; hence, the first two terms in the big conjunction require $\dim(U_i) = \dim(V_i)$. The fourth term amounts to condition

$U_{i+1} = U_i + V_i$, according to Example 1.15(h); hence, $\dim(U_{i+1}) = \dim(U_i) + \dim(V_i)$ because of $U_i \cap V_i = \mathbf{0}$ (third term). It follows $\dim(U_{i+1}) = 2 \times \dim(U_i)$. Therefore, $2^n \times \dim(U_1) = \dim(U_{n+1}) = d$ by the very first term. Conversely, the following is easily verified to constitute a satisfying assignment:

$$U_1 := \mathbb{F} \times \{0\}, \quad V_1 := \{(x,x) : x \in \mathbb{F}\}, \quad U_2 := \mathbb{F}^2 \times \{0\}^2, \quad V_2 := \{(\vec{x},\vec{x}) : \vec{x} \in \mathbb{F}^2\},$$
$$\ldots, \quad U_{i+1} := \mathbb{F}^{2^i} \times \{0\}^{2^i}, \quad V_{i+1} := \{(\vec{x},\vec{x}) : \vec{x} \in \mathbb{F}^{2^i}\} \quad \ldots, \quad U_{n+1} = \mathbb{F}^{2^n}$$

(all understood embedded into $\mathbb{F}^{2^n}$ by appending zeros).

(c) As pointed out in Corollary 2.10, g_d is not weakly satisfiable over $\mathrm{L}(\mathbb{F}^{d'})$ for $d' < d$, but weakly satisfiable for $d' = d$. In case $d' > d$, by Observation 4.1(a), g_d is weakly satisfiable also over $\mathrm{L}(\mathbb{F}^{d'})$. □

Definition 4.3.

(a) Call a term weakly respectively strongly satisfiable in $\mathrm{L}(\mathbb{F}^*)$ if and only if it is so in $\mathrm{L}(\mathbb{F}^d)$ for some $d \in \mathbb{N}$.
(b) The corresponding decision problems are abbreviated as $\mathrm{sat}_{\mathrm{L}(\mathbb{F}^*)} := \mathrm{sat}_{\{\mathrm{L}(\mathbb{F}^d):d\in\mathbb{N}\}} = \bigcup_d \mathrm{sat}_{\mathrm{L}(\mathbb{F}^d)}$ and $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^*)} := \mathrm{SAT}_{\{\mathrm{L}(\mathbb{F}^d):d\in\mathbb{N}\}} = \bigcup_d \mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d)}$, respectively.
(c) $\mathbb{F}$ is Pythagorean, if for any $a, b \in \mathbb{F}$ there is $c \in \mathbb{F} \cap \mathbb{R}$, such that $aa^\dagger + bb^\dagger = c^2$.

For Pythagorean $\mathbb{F}$, any subspace of $\mathbb{F}^d$ admits an orthonormal basis (due to the Gram-Schmidt process). $\mathbb{Q}$, for instance, is not Pythagorean.

Theorem 4.4.

(*a*) *For Pythagorean* $\mathbb{F}$ *it holds* $\mathrm{sat}_{\mathrm{L}(\mathbb{F}^*)} \in \mathrm{BP}(\mathcal{NP}^0_{\mathrm{Re}\,\mathbb{F}})$. *In particular,* $\mathrm{sat}_{\mathrm{L}(\mathbb{R}^*)}, \mathrm{sat}_{\mathrm{L}(\mathbb{C}^*)} \in \mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$.
(*b*) *A term is weakly (resp. strongly) satisfiable either in both or in none of* $\mathrm{L}(\mathbb{F}^*)$ *and* $\mathrm{L}(\mathrm{Re}\,\mathbb{F}^*)$*, i.e. it holds* $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}*)} = \mathrm{SAT}_{\mathrm{L}(\mathrm{Re}\,\mathbb{F}^*)}$ *and* $\mathrm{sat}_{\mathrm{L}(\mathbb{F}*)} = \mathrm{sat}_{\mathrm{L}(\mathrm{Re}\,\mathbb{F}^*)}$.

That is, weak satisfiability over $\mathrm{L}(\mathbb{F}^*)$ is decidable by a nondeterministic polynomial-time BSS-machine over $\mathrm{Re}\,\mathbb{F}$ without constants—and thus no more hard than in the fixed-dimensional case.

Proof.

(a) By the work of Herrmann [2010, Lemma 2.2] and Observation 4.1, t is weakly satisfiable over $\mathrm{L}(\mathbb{F}^*)$ iff it is so over $\mathrm{L}(\mathbb{F}^d)$ for $d := |t|$. Now recall (Proposition 2.1(a)) that satisfiability over $\mathrm{L}(\mathbb{F}^d)$ can be decided by a nondeterministic constant-free BSS-machine over $\mathrm{Re}\,\mathbb{F}$ in time polynomial in $|t|$ *and* d.
(b) For $\mathbb{F} \not\subseteq \mathbb{R}$, observe that $\mathrm{L}(\mathbb{F}^d)$ embeds into $\mathrm{L}((\mathrm{Re}\,\mathbb{F})^{2d})$, considering $\mathbb{F}^d$ as an $\mathrm{Re}(\mathbb{F})$–vector space with scalar product, the real part of the given one. □

Question 4.5. Is $\mathrm{sat}_{\mathrm{L}(\mathbb{R}^*)}$ hard for $\mathcal{NP}$ or even for $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$?

The rest of this section explores a strong counterpart to Theorem 4.4(a) and Question 4.5, namely the complexity (and computability) of $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^*)}$. To this end, the next subsection extends Section 2.2 from interpreting into quantum logic, not just the ring $\mathbb{F}$ of scalars but the ring $\mathbb{F}^{m\times m}$ of matrices, uniformly in m, and similarly for $*$-rings. We first discuss the feasibility problems for those.

4.1. Strong Satisfiability in Indefinite Finite Dimension is Hard

In order to prove $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$–hardness of strong satisfiability in indefinite dimension, we shall interpret $\mathrm{Re}(\mathbb{F})$ in $(\mathrm{Re}\,\mathbb{F})^{d\times d}$ in $\mathrm{L}(\mathbb{F}^{3d})$, uniformly in d. The first part is achieved

in Proposition 4.8(b) and (d) by means of the classical *Spectral Theorem*; the latter in Proposition 4.9(b) as a scholium to Theorem 2.7.

Definition 4.6.

(a) A $*$–ring is a (not necessarily commutative) ring with unity, endowed with an *involution* $r \mapsto r^\dagger$, i.e., a map satisfying $(r+s)^\dagger = r^\dagger + s^\dagger$, $(rs)^\dagger = s^\dagger r^\dagger$, and $(r^\dagger)^\dagger = r$.
(b) A $*$–ring is formally real if $\sum_{j=1}^{J} r_j^\dagger \times r_j = 0$ implies $r_j = 0$ $(1 \leq j \leq J)$ for all $J \in \mathbb{N}$.

The examples of interest, here, are the fields $\mathbb{F}$ with conjugation and the matrix rings $\mathbb{F}^{m\times m}$ where $\mathcal{A}^\dagger$ is conjugate transpose of $\mathcal{A}$. Indeed, suppose there is some j and some $\vec{x} \in \mathbb{F}^m$, such that $B_j\vec{x} \neq 0$. Then, $0 = \langle \vec{x} | \sum_j B_j^\dagger \times B_j \vec{x}\rangle = \sum_j \langle B_j\vec{x} | B_j\vec{x}\rangle \geq \|B_j\vec{x}\|^2 > 0$: contradiction.

Dealing with matrices, the commutative rings of polynomials have to be replaced by rings of polynomials $p \in \mathbb{Z}\langle X_1, \ldots, X_n\rangle$ in non-commuting variables and, in the case of $*$–rings, $p \in \mathbb{Z}\langle X_1, \ldots, X_n, X_1^*, \ldots, X_n^*\rangle$ – with the convention that X^* has to be interpreted as $\mathcal{A}^\dagger$ if X is interpreted as $\mathcal{A}$. Observe that the latter ring admits an anti-automorphism $p \mapsto p^*$ which interchanges X and X^*.

Definition 4.7.

(a) For a not necessarily commutative ring $R \supseteq \mathbb{Z}$, let $\mathrm{FEAS}_{\mathbb{Z},R}$ denote the following decision problem:

> Given $p_1, \ldots, p_k \in \mathbb{Z}\langle X_1, \ldots, X_n\rangle$, do they admit a common root in R, i.e., some assignment $\bar{a} \in R^n$ such that $p_1(\bar{a}) = \cdots = p_k(\bar{a}) = 0$?

(b) In case that R is a $*$–ring, $\mathrm{FEAS}^\dagger_{\mathbb{Z},R}$ is the same question referring to (non-commutative) $*$–polynomials.
(c) For $\mathcal{R}$, a class of rings, respectively $*$–rings, we put $\mathrm{FEAS}_{\mathbb{Z},\mathcal{R}} := \bigcup_{R\in\mathcal{R}} \mathrm{FEAS}_{\mathbb{Z},\mathcal{R}}$ and $\mathrm{FEAS}^\dagger_{\mathbb{Z},\mathcal{R}} := \bigcup_{R\in\mathcal{R}} \mathrm{FEAS}^\dagger_{\mathbb{Z},\mathcal{R}}$.
(d) For a $*$–ring $R \supseteq \mathbb{Z}$, let $\mathrm{QUART}^\dagger_{\mathbb{Z},R}$ denote the decision problem of whether a single non-commutative polynomial in variables $X_1, \ldots, X_n^*$ with coefficients from $\{-n, \ldots, 0, \ldots, +n\}$ admits a root over R.

(The complements of) these computational problems arise in practice [Benanti et al. 2003], hence, their complexity is worthwhile investigating.

Proposition 4.8. *Fix* $\mathbb{F}$ *and let* $\mathrm{FEAS}_{\mathbb{Z},\mathbb{F}^*} := \mathrm{FEAS}_{\mathbb{Z},\{\mathbb{F}^{d\times d}:d\in\mathbb{N}\}}$ *and* $\mathrm{FEAS}^\dagger_{\mathbb{Z},\mathbb{F}^*} := \mathrm{FEAS}^\dagger_{\mathbb{Z},\{\mathbb{F}^{d\times d}:d\in\mathbb{N}\}}$ *denote (*$*$*–) polynomial feasibility in some matrix ring over* $\mathbb{F}$.

(*a*) $\mathrm{FEAS}_{\mathbb{Z},\mathbb{F}}$ *and* $\mathrm{FEAS}_{\mathbb{Z},\mathbb{F}^{d\times d}}$ *are polynomial-time equivalent for fixed* $d \in \mathbb{N}$.
(*b*) *For algebraically closed* $\mathbb{F}$ *(say,* $\mathbb{F} = \mathbb{C}$*),* $\mathrm{FEAS}_{\mathbb{Z},\mathbb{F}}$ *reduces polynomially to* $\mathrm{FEAS}_{\mathbb{Z},\mathbb{F}^*}$.
(*c*) $\mathrm{FEAS}_{\mathbb{Z},\mathrm{Re}\,\mathbb{F}}$, $\mathrm{FEAS}^\dagger_{\mathbb{Z},\mathrm{Re}\,\mathbb{F}}$, $\mathrm{FEAS}^\dagger_{\mathbb{Z},\mathbb{F}}$, *and* $\mathrm{FEAS}^\dagger_{\mathbb{Z},\mathbb{F}^{d\times d}}$ *are pairwise polynomial-time equivalent.*
(*d*) *If* $\mathbb{F}$ *is real or algebraically closed (e.g.,* $\mathbb{F} = \mathbb{R}, \mathbb{C}$*), then there is a polynomial time reduction from* $\mathrm{FEAS}^\dagger_{\mathbb{Z},\mathbb{F}}$ *to* $\mathrm{FEAS}^\dagger_{\mathbb{Z},\mathbb{F}^*}$.
(*e*) *Uniformly for all formally real* $*$*–rings* R*, there is a polynomial time reduction from* $\mathrm{FEAS}^\dagger_{\mathbb{Z},R}$ *to* $\mathrm{QUART}^\dagger_{\mathbb{Z},R}$.

Proposition 4.8(e) generalizes the well-known $\mathcal{NP}_{\mathbb{R}}$–completeness of quartic polynomial feasibility [Blum et al. 1998, Sections 5.2+5.4].

PROOF.

(a) Concerning one direction, a polynomial-time nondeterministic BSS machine over $\mathbb{F}$ can guess the entries of a matrix assignment over $\mathbb{F}^{d\times d}$ and verify them by evaluating the polynomials using operations from $\mathbb{F}$. This demonstrates $\mathrm{FEAS}_{\mathbb{Z},\mathbb{F}^{d\times d}} \in \mathrm{BP}(\mathcal{NP}^0_{\mathbb{F}})$. Since $\mathrm{FEAS}_{\mathbb{Z},\mathbb{F}}$ is complete for $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{F}})$, the first reduction follows.

For the converse reduction, consider *d-systems of matrix units* in $\mathbb{F}^{d\times d}$ consisting of matrices $(\mathcal{E}_{ij} \mid 1 \le i, j \le d)$, such that $\sum_{i=1}^{d} \mathcal{E}_{ii} = \mathcal{I}$ and $\mathcal{E}_{k\ell} \times \mathcal{E}_{ij} = \delta_{jk}\mathcal{E}_{i\ell}$, where $\mathcal{I}$ is the unit matrix, and recall that the map $a \mapsto a\mathcal{I}$ is a ring isomorphism of $\mathbb{F}$ onto $\{\mathcal{X} \in \mathbb{F}^{d\times d} \mid \mathcal{X} \times \mathcal{E}_{ij} = \mathcal{E}_{ij} \times \mathcal{X} \text{ for all } i, j\}$. To carry out the reduction, require, in addition to the given equations, the existence of such $\mathcal{E}_{ij}$ commuting with (the evaluations of) all given variables.

(b) Given equations $p_1(\bar{X}) = \ldots = p_k(\bar{X}) = 0$, add all commutativity conditions $X_iX_j - X_jX_i$. Clearly, if $a_1, \ldots a_n$ is a solution in $\mathbb{F}$ for the old system, then $a_1\mathcal{I}, \ldots a_n\mathcal{I}$ is a solution in $\mathbb{F}^{d\times d}$ for any d. Conversely, if $\mathcal{A}_1, \ldots, \mathcal{A}_n$ is a solution of the extended system in some $\mathbb{F}^{d\times d}$, then the $\mathcal{A}_1, \ldots, \mathcal{A}_n$ commute with each other; and thus have a common eigenvector $\vec{v}$ to respective eigenvalues $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$; which constitute a solution in $\mathbb{F}$.

(c) Equivalence of the first three is obvious, in view of the fact that † is identity for $\mathbb{F} \subseteq \mathbb{R}$, or in view of the Cartesian representation of the $*$–field $\mathbb{F}$ over $\mathrm{Re}\,\mathbb{F}$, otherwise. The remaining equivalence follows as in Proposition 4.8(a), using $\mathcal{E}_{ij}$ such that $\mathcal{E}_{ij}^\dagger = \mathcal{E}_{ji}$ to make sure that $a \mapsto a\mathcal{I}$ is a $*$–ring homomorphism.

(d) Add the commutativity conditions and also conditions $X_j = X_j^*$; that is, require the value of X_j to be self-adjoint. As in Proposition 4.8(b), the $\mathcal{A}_i$ have some common eigenvector and the proof proceeds as before.

(e) Again, invoking the method of intermediate results, decompose the evaluation of the given $*$–polynomials into a system of J quadratic $*$–polynomial equations $p_j = 0$, $1 \le j \le J$, with J polynomial in the input size. Moreover, each p_j depends on at most three variables (or their adjoints). And, according to Observation 1.9(b), we may suppose these to only contain coefficients $-1, 0, 1$. Now, R being formally real, these J quadratic polynomial equations can be combined into one single quartic polynomial equation $\sum_j p_j^\dagger \cdot p_j = 0$ in, at most, $3J$ variables. In dense representation, each monomial in $p_j^\dagger \times p_j$ has integer coefficients bounded by 2; which, in $\sum_j$, can sum up to at most $2J$. □

Picking up on Theorem 4.4(a), and since Theorem 2.11 depends on the dimension being fixed, we now consider the complexity and computability of *strong* satisfiability over indefinite finite dimensions—and approach the boundary between complexity and mere computability.

PROPOSITION 4.9. *For a fixed* $\mathbb{F}$*, there are the following polynomial time reductions:*

(*a*) SAT *to* $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^*)}$ *to* $\mathrm{FEAS}^\dagger_{\mathbb{Z},\mathbb{F}^*}$.

(*b*) *For Pythagorean* $\mathbb{F}$, $\mathrm{FEAS}^\dagger_{\mathbb{Z},\mathbb{F}^*}$ *to* $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^*)}$.

(*c*) *For real respectively algebraically closed* $\mathbb{F}$, $\mathrm{FEAS}^\dagger_{\mathbb{Z},\mathbb{F}}$ *to* $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^*)}$.

PROOF.

(a) The first reduction is Proposition 1.16. According to Proposition 2.1(c), $\mathrm{SAT}_{\mathrm{L}(\mathbb{F}^d)}$ reduces in polynomial time to $\mathrm{FEAS}_{\mathbb{Z},\mathrm{Re}\,\mathbb{F}}$, and by Fact 1.8(b), further on to any

problem in $\mathrm{BP}(\mathcal{NP}_{\mathrm{Re}\,\mathbb{F}})$, such as $\mathrm{FEAS}^{\dagger}_{\mathbb{Z},\mathbb{F}^{d\times d}}$. However, both reductions depend on d! A short-cut uniform in d is provided by the following observations: $\mathrm{range}\,\mathcal{A} + \mathrm{range}\,\mathcal{B} = \mathrm{range}\,\mathcal{C}$ iff there are matrices $\mathcal{X}_i$, such that $\mathcal{C} = \mathcal{A}\mathcal{X}_1 + \mathcal{B}\mathcal{X}_2$, $\mathcal{A} = \mathcal{C}\mathcal{X}_3$, and $\mathcal{B} = \mathcal{C}\mathcal{X}_4$; similarly, $\mathrm{range}\,\mathcal{B} = (\mathrm{range}\,\mathcal{A})^{\perp}$ iff $\mathcal{A}^{\dagger}\mathcal{B} = 0$ and there are $\mathcal{X}_i$, such that $\mathcal{A}\mathcal{X}_1 + \mathcal{B}\mathcal{X}_2 = \mathcal{I}$, the unit matrix.

(b) We claim that a Turing machine can translate, in polynomial time, any finite family $\bar{p}$ of $*$–polynomials in non-commuting variables into a term $t_{\bar{p}}$ which, over Pythagorean $\mathbb{F}$, is strongly satisfiable in $\mathrm{L}(\mathbb{F}^k)$ iff $k = 3m$ for some m and any member of $\bar{p}$ admits a solution in $\mathbb{F}^{m\times m}$. Indeed, modify the proof of Theorem 2.7 as follows:
first of all, the notion of a coordinate system of order 3 extends to any MOL, such as $\mathrm{L}(\mathbb{F}^k)$, if one just requires the relations between the A_{ij}; these force $\dim A_i = \dim A_{ij}$ for all i, j when $k = 3m$ and $m = \dim A_1$. Given any basis $\vec{v}^1_1, \ldots, \vec{v}^m_1$ of A_1 for any $j = 2, 3$ and $h = 1, \ldots, m$, there is unique $\vec{v}^h_j \in A_j$ such that $\mathbb{F}(\vec{v}^h_1 - \vec{v}^h_j) \subseteq A_{1j}$. Then, the $\vec{v}^h_i$, $i = 1, 2, 3$; $h = 1, \ldots, m$ forms a basis of $\mathbb{F}^k$, such that $A_I = \sum_{h=1}^m \mathbb{F}\vec{v}^h_i$ and $A_{ij} = \sum_{h=1}^m \mathbb{F}(\vec{v}^h_i - \vec{v}^h_j)$. Thus, in view of Observation 2.4, we may replace $\mathbb{F}^k$ (and $\bar{A}$) by $(\mathbb{F}^m)^3$ with $A_1 = \mathbb{F}^m \times \mathbf{0}^{2m}$, $A_2 = \mathbf{0}^m \times \mathbb{F}^m \times \mathbf{0}^m$, $A_3 = \mathbf{0}^{2m} \times \mathbb{F}^m$, and $A_{ij} = \{\varepsilon_i(\vec{x}) - \varepsilon_j(\vec{x}) \mid \vec{x} \in \mathbb{F}^m\}$, where ε_i is the canonical isomorphism of $\mathbb{F}^m$ onto A_i. For a matrix $\mathcal{A} \in \mathbb{F}^{m\times m}$, define

$$\Theta_{\bar{A}}(\mathcal{A}) = \{\varepsilon_1(\vec{x}) - \varepsilon_2(\mathcal{A}\vec{x}) \mid \vec{x} \in A_1\}.$$

Using "generic vectors" again, this reads as $(\vec{x}, -\mathcal{A}\vec{x}, \vec{0})$, and the calculations underlying the proof of Fact 2.5 show that $\Theta_{\bar{A}}$ is an isomorphism of the ring $\mathbb{F}^{m\times m}$ onto $\mathcal{R}_{\bar{A}} = \{U \in L \mid U \oplus A_2 = A_1 + A_2\}$ with operations $\ominus_{\bar{A}}$, $\otimes_{\bar{A}}$, A_1, and A_{12}.

To deal with the adjoint, too, we now suppose that $\bar{A}$ is an orthonormal coordinate system of order 3 w.r.t. to *some* scalar product $\langle\,|\,\rangle$ on $(\mathbb{F}^m)^3$ (recall that we arrived at $(\mathbb{F}^m)^3$ by a linear isomorphism, only), i.e., we have the orthogonal direct sum $A_1 \oplus A_2 \oplus A_3$ and $A_1 \ominus_{\bar{A}} A_{12} = (A_1 + A_2) \cap A_{12}^{\perp}$. The latter condition reads as

$$0 = \langle(\vec{x}, \vec{x}, \vec{0}) \mid (\vec{y}, -\vec{y}, \vec{0})\rangle = \langle(\vec{x}, \vec{0}, \vec{0}) \mid (\vec{y}, \vec{0}, \vec{0})\rangle - \langle(\vec{0}, \vec{x}, \vec{0}) \mid (\vec{0}, \vec{y}, \vec{0})\rangle,$$

i.e., it means that the isomorphism $(\vec{x}, \vec{0}, \vec{0}) \mapsto (\vec{0}, -\vec{x}, \vec{0})$ of A_1 onto A_2 is an isometry. The latter matches $\vec{v}^h_1$ with $\vec{v}^h_2$ so that $\vec{v}^h_i (i = 1, 2; h = 1, \ldots, m)$ is an orthonormal basis of $A_1 + A_2$ if $\vec{v}^1_1, \ldots, \vec{v}^m_1$ is an orthonormal basis of A_1. Since $\mathbb{F}$ is Pythagorean, the latter can be achieved. Thus, in view of Observation 2.4, we may assume that the scalar product on $\mathbb{F}^m$ and $A_1 + A_2$ is the canonical one, and $A_3 = (A_1 + A_2)^{\perp}$. Now, $\mathcal{B} = \mathcal{A}^{\dagger}$ iff for all $\vec{x}, \vec{y}$

$$0 = \langle\mathcal{B}\vec{x} \mid \vec{y}\rangle - \langle\vec{x} \mid \mathcal{A}\vec{y}\rangle = \langle(\mathcal{B}\vec{x}, \vec{x}, \vec{0}) \mid (\vec{y}, -\mathcal{A}\vec{y}, \vec{0})\rangle,$$

when

$$\Theta_{\bar{A}}(\mathcal{A}^{\dagger}) = (\Theta_{\bar{A}}(\mathcal{A}))^{\textcircled{T}_{\bar{A}}}, \text{ where } X^{\textcircled{T}_{\bar{z}}} := Z_1 \ominus_{\bar{z}} \left(\pi^{13}_{\bar{Z}12}\left[\pi^{23}_{\bar{Z}13}\left(\pi^{21}_{\bar{Z}23}[(Z_1 \vee Z_2) \wedge \neg X]\right)\right]\right).$$

(c) Combine Proposition 4.9(b) with Proposition 4.8(d). □

THEOREM 4.10. $\mathrm{SAT}_{\mathrm{L}(\mathbb{R}^*)} = \mathrm{SAT}_{\mathrm{L}(\mathbb{C}^*)}$ *is* $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$*–hard. Moreover, the following are equivalent:*

(*i*) $\mathrm{SAT}_{\mathrm{L}(\mathbb{C}^*)}$ *is decidable.*
(*ii*) $\mathrm{FEAS}^{\dagger}_{\mathbb{Z},\mathbb{C}^*}$ *is decidable.*

(*iii*) *There exists a total recursive function* $\delta : \mathbb{N} \to \mathbb{N}$*, such that the following holds:*

$$\begin{array}{l}\textit{Whenever a term } t \textit{ is strongly satisfiable over } \mathrm{L}(\mathbb{C}^*),\\ \textit{it is so over } \mathrm{L}(\mathbb{C}^d) \textit{ for some } d \leq \delta(|t|).\end{array} \tag{12}$$

(*iv*) *There exists a total recursive function* $\delta' : \mathbb{N} \to \mathbb{N}$*, such that the following holds:*

$$\begin{array}{c}\textit{Whenever a quartic} q \in \{0, \pm 1, \pm 2, \ldots, \pm N\}\langle X_1, X_1^*, \ldots, X_N, X_N^*\rangle \textit{ admits a}\\ \textit{root over } \mathbb{R}^{m\times m} \textit{ for some } m, \textit{ it also does so over } \mathbb{R}^{m'\times m'} \textit{ for some } m' \leq \delta'(N).\end{array}$$

Note that, according to Example 4.2(b), any bound on δ has to be at least exponential.

Proof of Theorem 4.10. $\mathrm{SAT}_{\mathrm{L}(\mathbb{C}^*)} = \mathrm{SAT}_{\mathrm{L}(\mathbb{R}^*)}$ holds due to Theorem 4.4(b); for hardness, invoke Proposition 4.9(c).

(i)$\Leftrightarrow$(ii) Proposition 4.9(a) and (b).

(i)$\Rightarrow$(iii) Based on an algorithm deciding $\mathrm{SAT}_{\mathrm{L}(\mathbb{C}^*)}$, a function δ as required in Equation (12) can be computed as follows: given n, enumerate all (the finitely many, up to renaming variables) terms t of length n strongly satisfiable over $\mathrm{L}(\mathbb{C}^*)$; for each one, search for the first dimension in which t is strongly satisfiable and return the maximum.

(iii)$\Rightarrow$(i) Given t, calculate $d := \delta(|t|)$ and decide satisfiability of t over $\mathrm{L}(\mathbb{C}^1), \mathrm{L}(\mathbb{C}^2), \ldots, \mathrm{L}(\mathbb{C}^d)$. If none succeeds, then t is not satisfiable over $\mathrm{L}(\mathbb{C}^*)$ either. The proof of (ii)$\Leftrightarrow$(iv) follows the same lines, based on Proposition 4.8(e). □

5. CONCLUSION AND PERSPECTIVES

According to Bohr's Correspondence Principle, Classical Mechanics can be considered as a macroscopic limit of Quantum Mechanics. Similarly, Boolean logic is the "trivial" (namely, 1D) case of geometric quantum logics—syntactically equal, but with the semantics $\wedge$, meaning intersection of subspaces, $\neg$ orthogonal complement, and $\vee$ Minkowski sum. The present work has explored the computational complexity of quantum satisfiability: in dimension one, historically, the first problem shown $\mathcal{NP}$-complete turns out as different from but polynomial-time equivalent to dimension two; while from dimension three on, it characterizes the complexity class $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$ located between $\mathcal{NP}$ and PSPACE. In particular, satisfying assignments cannot, in general, be chosen as rational. Moreover, the quantum satisfiability problem remains complete when syntactically restricting to terms of the form "$\bigwedge\bigvee\bigwedge$"; whereas the case of conjunctive form "$\bigwedge\bigvee$" can be decided in polynomial time from dimension two on. Finally, towards the infinite-dimensional case, we have considered quantum satisfiability in indefinite but finite dimensions.

In the future we will

(a) identify and establish more problems complete for the complexity class $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$;
(b) clarify the connection between quantum logic and quantum computing; and
(c) characterize the expressiveness of quantum logic in terms of algebraic geometry.

Note Added in Proof. Together with Yasuyuki Tsukamoto, we have recently been able to establish $\mathrm{SAT}_{\mathrm{L}(\mathbb{R}^*)}$ as undecidable [Hermann et al. 2015]. In particular, the polynomial-time equivalence between weak and strong satisfiability hinges on the dimension being fixed. Moreover, according to Theorem 4.10, there exist terms t that are strongly satisfiable only in dimensions exceeding any primitive recursive bound in t's length.

REFERENCES

Samson Abramsky and Bob Coecke. 2004. A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science*. IEEE, 415–425.

Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. 2009. On the complexity of numerical analysis. *SIAM J. Comput.* 38, 5 (2009), 1987–2006.

Saugata Basu and Thierry Zell. 2010. Polynomial hierarchy, betti numbers, and a real analogue of todas theorem. *Foundations of Computational Mathematics* 10, 4 (2010), 429–454.

Enrico G. Beltrametti, Gianni Cassinelli, and Gian-Carlo Rota. 1984. *Encyclopedia of Mathematics and Its Applications*. The Logic of Quantum Mechanics, Vol. 15. Cambridge University Press.

Francesca Benanti, James Demmel, Vesselin Drensky, and Plamen Koev. 2003. Computational approach to polynomial identities of matrices—a survey. In *Polynomial Identities And Combinatorial Methods*, Giambruno, Regev, and Zaicev (Eds.). Lectures Notes in Pure and Applied Mathematics, Vol. 234. Dekker, 141–178.

Garrett Birkhoff and John Von Neumann. 1936. The logic of quantum mechanics. *Annals of Mathematics* 37, 4 (1936), 823–843.

A Björner, M Las Vergnas, B Sturmfels, Neil White, and GM Ziegler. 1999. *Oriented matroids*. Encyclopedia of Mathematics and its Applications, Vol. 46.

Lenore Blum, Mike Shub, and Steve Smale. 1989. On a theory of computation and complexity over the real numbers: W-completeness, recursive functions and universal machines. *Bull. Amer. Math. Soc* 21, 1 (1989), 1–46.

Lenore Blum, Steve Smale, Michael Shub, and Felipe Cucker. 1998. *Complexity and Real Computation*. Springer.

Egon Börger, Erich Grädel, and Yuri Gurevich. 2001. *The Classical Decision Problem*. Springer.

Olivier Bournez, Felipe Cucker, Paulin Jacobé De Naurois, and Jean-Yves Marion. 2006. Implicit complexity over an arbitrary structure: Quantifier alternations. *Information and Computation* 204, 2 (2006), 210–230.

Jeffrey Bub. 2007. Quantum computation from a quantum logical perspective. *Quantum Information & Computation* 7, 4 (2007), 281–296.

Peter Bürgisser. 2000. *Completeness and Reduction in Algebraic Complexity Theory*, Vol. 7. Springer.

Peter Bürgisser and Felipe Cucker. 2006. Counting complexity classes for numeric computations II: Algebraic and semialgebraic sets. *Journal of Complexity* 22, 2 (2006), 147–191.

Peter Bürgisser and Felipe Cucker. 2009. Exotic quantifiers, complexity classes, and complete problems. *Foundations of Computational Mathematics* 9, 2 (2009), 135–170.

Peter Bürgisser and Peter Scheiblechner. 2009. On the complexity of counting components of algebraic varieties. *Journal of Symbolic Computation* 44, 9 (2009), 1114–1136.

Stanley Burris and Hantamantagouda P. Sankappanavar. 1981. *A Course in Universal Algebra*. Graduate Texts in Mathematics, Vol. 78. Springer.

John Canny. 1988. Some algebraic and geometric computations in PSPACE. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. ACM, 460–467.

Ashok K. Chandra, Dexter C. Kozen, and Larry J. Stockmeyer. 1981. Alternation. *Journal of the ACM (JACM)* 28, 1 (1981), 114–133.

Hubie Chen. 2009. A rendezvous of logic, complexity, and algebra. *ACM Computing Surveys (CSUR)* 42, 1 (2009), 2.

Bob Coecke, David Moore, and Alex Wilce. 2000. Current research in operational quantum logic. *Fundamental Theories of Physics* 111, Springer. DOI:10.1007/978-94-017-1201-9

Stephen A. Cook. 1971. The complexity of theorem-proving procedures. In *Proceedings of the 3rd Annual ACM Symposium on Theory of Computing*. ACM, 151–158.

David A. Cox, John Little, and Donal O'Shea. 2007. *Ideals, Varieties, and Algorithms*. Springer.

Felipe Cucker. 1993. On the complexity of quantifier elimination: The structural approach. *Computer Journal* 36, 5 (1993), 400–408.

Felipe Cucker and Irénée Briquel. 2007. A note on parallel and alternating time. *Journal of Complexity* 23, 4 (2007), 594–602.

Felipe Cucker and Dima Grigoriev. 1997. On the power of real turing machines over binary inputs. *SIAM J. Comput.* 26, 1 (1997), 243–254.

Felipe Cucker and Francesc Rosselló. 1992. On the complexity of some problems for the Blum, Shub & Smale model. In *LATIN'92*. Springer, 117–129.

Mark De Berg, Marc Van Kreveld, Mark Overmars, and Otfried Cheong. 2000. *Computational Geometry, Algorithms and Applications*. Springer.

J. Michael Dunn, Tobias J. Hagge, Lawrence S. Moss, and Zhenghan Wang. 2005. Quantum logic as motivated by quantum computing. *The Journal of Symbolic Logic* 70, 02 (2005), 353–359.

Hervé Fournier and Pascal Koiran. 1998. Are lower bounds easier over the reals? In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*. ACM, 507–513.

Hervé Fournier and Pascal Koiran. 2000. Lower bounds are not easier over the reals: Inside PH. In *Automata, Languages and Programming*. Springer, 832–843.

Marc Giusti and Joos Heintz. 1991. Algorithmes–disons rapides–pour la décomposition dune variété algébrique en composantes irréductibles et équidimensionnelles. In *Effective Methods in Algebraic Geometry*. Springer, 169–194.

John B. Goode. 1994. Accessible telephone directories. *The Journal of Symbolic Logic* 59, 01 (1994), 92–105.

Erich Grädel and Klaus Meer. 1996. Descriptive complexity theory over the real numbers. In *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing*, James Renegar, Michael Shub, and Steve Smale (Eds.). Lectures in Applied Mathematics, Vol. 32. AMS, 381–403.

D. Yu Grigor'ev. 1988. Complexity of deciding Tarski algebra. *Journal of Symbolic Computation* 5, 1 (1988), 65–108.

Martin Grohe. 2012. Fixed-point definability and polynomial time on graphs with excluded minors. *Journal of the ACM (JACM)* 59, 5 (2012), 27.

Tobias J. Hagge. 2007. QL (n) determines n. *The Journal of Symbolic Logic* 72, 04 (2007), 1194–1196.

John Harding. 2009. A link between quantum logic and categorical quantum mechanics. *International Journal of Theoretical Physics* 48, 3 (2009), 769–802.

Joos Heintz, Marie-Françoise Roy, and Pablo Solernó. 1990. Sur la complexité du principe de Tarski-Seidenberg. *Bulletin de la Société Mathématique de France* 118, 1 (1990), 101–126.

Christian Hermann, Yasuyuki Tsukamoto, and Martin Ziegler. 2015. On the satisfiability problem for classes of structures related to finite dimensional vector spaces. In *Proceedings of the 16th International Workshop on Logic and Computational Complexity*.

Christian Herrmann. 2010. On the equational theory of projection lattices of finite von Neumann factors. *The Journal of Symbolic Logic* 75, 03 (2010), 1102–1110.

Christian Herrmann, Johanna Sokoli, and Martin Ziegler. 2013. Satisfiability of cross product terms is complete for real nondeterministic polytime Blum-Shub-Smale machines. *EPTCS* 128 (2013), 85–92.

Christian Herrmann and Martin Ziegler. 2011. Computational complexity of quantum satisfiability. In *2011 26th Annual IEEE Symposium on Logic in Computer Science (LICS)*. IEEE, 175–184.

Wilfrid Hodges. 1993. *Model Theory*. Vol. 42. Cambridge University Press Cambridge.

András P. Huhn. 1972. Schwach distributive verbände. *I/ /Acta Sci. Math.(Szeged)* 33, 1–4 (1972), 297–305.

Gabriela Jeronimo, Teresa Krick, Juan Sabia, and Martín Sombra. 2004. The computational complexity of the Chow form. *Foundations of Computational Mathematics* 4, 1 (2004), 41–117.

Pascal Koiran. 1996. Hilbert's Nullstellensatz is in the polynomial hierarchy. *Journal of Complexity* 12, 4 (1996), 273–286.

Pascal Koiran. 1999. The real dimension problem is NPR-complete. *Journal of Complexity* 15, 2 (1999), 227–238.

Grégoire Lecerf. 2000. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation*. ACM, 209–216.

G. W. Mackey. 1963. *The Mathematical Foundations of Quantum Mechanics*. Benjamin, New York.

Maarten Marx. 2007. Complexity of modal logic. *Handbook of Modal Logic* 3 (2007), 139–179.

Ju V. Matijasevič. 1970. Enumerable sets are diophantine. *Dokl. Akad. Nauk SSSR* 191, 2 (1970), 279–282.

Klaus Meer, Christian Michaux, and others. 1997. A survey on real structural complexity theory. *Bulletin of the Belgian Mathematical Society– Simon Stevin* 4, 1 (1997), 113–148.

Christian Michaux. 1989. Une remarque á propos des machines sur R introduites par Blum, Shub et Smale. *CR Acad. Sci. Paris* 309, 1 (1989), 435–437.

Christian Michaux. 1994. P$\neq$ NP over the nonstandard reals implies P$\neq$ NP over R. *Theoretical Computer Science* 133, 1 (1994), 95–104.

John Von Neumann. 1955. *Mathematical Foundations of Quantum Mechanics*. Number 2 in Princeton Landmarks in Mathematics. Princeton University Press.

Christos H. Papadimitriou. 1994. *Computational Complexity*. Addison Wesley Pub. Co.

Mladen Pavičić. 2007. Quantum logic and quantum computation. In *Handbook of Quantum Logic and Quantum Structures: Quantum Structures*. Elsevier, 755–792.

Constantin Piron. 1964. Axiomatique quantique. *Helvetica Physica Acta* 37, 4–5 (1964), 439.

Bruno Poizat. 1995. *Les Petits Cailloux: Une Approche Modèle-Théorique de L'algorithmie*. Aléas.

Bjorn Poonen. 2009. Characterizing integers among rational numbers with a universal-existential formula. *American Journal of Mathematics* 131, 3 (2009), 675–682.

Jarosław Pykacz. 2000. Quantum logic as a basis for computations. *International Journal of Theoretical Physics* 39, 3 (2000), 839–840.

James Renegar. 1992. On the computational complexity and geometry of the first-order theory of the reals. *Journal of Symbolic Computation* 13, 3 (1992), 255–352.

Jurgen Richter-Gebert. 1999. The universality theorems for oriented matroids and polytopes. *Contemp. Math.* 223 (1999), 269–292.

Leopoldo Román. 2006. A characterization of quantic quantifiers in orthomodular lattices. *Theory and Applications of Categories* 16, 10 (2006), 206–217.

Marcus Schaefer. 2010. Complexity of some geometric and topological problems. In *Graph Drawing*. Springer, 334–344.

Thomas J. Schaefer. 1978. The complexity of satisfiability problems. In *Proceedings of the Tenth Annual ACM Symposium on Theory of Computing*. ACM, 216–226.

Peter Scheiblechner. 2012. Castelnuovo–Mumford regularity and computing the de Rham cohomology of smooth projective varieties. *Foundations of Computational Mathematics* 12, 5 (2012), 541–571.

Peter Shor. 1991. Stretchability of pseudolines is NP-hard. *Applied Geometry and Discrete Mathematics–The Victor Klee Festschrift*, P. Gritzmann and B. Sturmfels (Eds.). DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Amer. Math. Soc., Providence, RI 4 (1991), 531–554.

Steve Smale. 1998. Mathematical problems for the next century. *The Mathematical Intelligencer* 2, 20 (1998), 7–15.

Alfred Tarski. 1948. *A Decision Method for Elementary Algebra and Geometry*. Technical Report.

Alfred Tarski. 1953. A general method in proofs of undecidability. *Studies in Logic and the Foundations of Mathematics* 13 (1953), 1–34.

John V. Tucker and Jeffery I. Zucker. 2001. Computable functions and semicomputable sets on many-sorted algebras. In *Handbook of logic in computer science*, Abramsky, Gabbay, and Maybaum (Eds.). Vol. 5. 397–525.

Mingsheng Ying. 2005. A theory of computation based on quantum logic (I). *Theoretical Computer Science* 344, 2 (2005), 134–207.

Hans Zassenhaus. 1948. Über einen algorithmus zur bestimmung der raumgruppen. *Commentarii Mathematici Helvetici* 21, 1 (1948), 117–141.

Xiao-Dong Nick Zhang. 1992. Complexity of neural network learning in the real number model. In *Proceedings of the Workshop on Physics and Computation (PhysComp'92)*. IEEE, 146–150.

Received December 2011; revised September 2015; accepted December 2015