2011 26th Annual IEEE Symposium on Logic in Computer Science

Computational Complexity of Quantum Satisfiability

Christian Herrmann and Martin Ziegler
Mathematics Department, Technical University of Darmstadt (GERMANY)

***Abstract*—Quantum logic generalizes, and in dimension one coincides with, Boolean propositional logic. We introduce the weak and strong satisfiability problem for quantum logic formulas; and show both $\mathcal{NP}$-complete in dimension two as well. For higher-dimensional spaces $\mathbb{R}^d$ and $\mathbb{C}^d$ with $d \geq 3$ fixed, on the other hand, we show the problem to be complete for the nondeterministic Blum-Shub-Smale model of real computation. This provides a unified view on both Turing and real BSS complexity theory; and adds (a perhaps more natural and combinatorially flavoured) one to the still sparse list of $\mathcal{NP}_{\mathbb{R}}$-complete problems, mostly pertaining to real algebraic geometry. Our proofs rely on (a careful examination of) works by John von Neumann as well as contributions by Hagge et.al (2005,2007,2009). We finally investigate the problem over *in*definite finite dimensions and relate it to *non*commutative semialgebraic geometry.**

I. Introduction

Putting a mathematical foundation to the new theories describing the paradoxical (yet very real) effects of quantum physics [Mack63] has led to Quantum Logic as a generalization of classical Boolean propositional logic in that it lacks the distributive law. Fortunately our readers need not be familiar with theoretical quantum physics as it already has been boiled down [BiVN36], [Piro64], [BeCa81] to

Definition 1: Fix some integer $d \in \mathbb{N}$ and let $\mathbb{F} \subseteq \mathbb{C}$ denote a field (popular cases being e.g. $\mathbb{F} = \mathbb{C}$ itself, $\mathbb{F} = \mathbb{A}$ algebraic numbers, $\mathbb{F} = \mathbb{R}$ real numbers, $\mathbb{F} = \mathbb{Q}$ rationals, and $\mathbb{F} = \mathbb{A} \cap \mathbb{R}$ algebraic reals). The quantum logic of $\mathcal{H} := \mathbb{F}^d$ consists of the set $\mathrm{Gr}(\mathcal{H}) := \bigcup_{i=0}^{d} \mathrm{Gr}_i(\mathcal{H})$ of all (necessarily closed) subspaces of $\mathcal{H}$ of dimension[†] $0 \leq i \leq d$ (i.e. the Grassmannian stripped of its topology, and instead) equipped with the following connectives:

$\wedge$: $\mathrm{Gr}(\mathcal{H}) \times \mathrm{Gr}(\mathcal{H}) \to \mathrm{Gr}(\mathcal{H})$, $(P,Q) \mapsto P \cap Q$
$\neg$:$\mathrm{Gr}_i(\mathcal{H}) \to \mathrm{Gr}_{d-i}(\mathcal{H})$, $P \mapsto P^{\perp} := \{\vec{y} \in \mathcal{H} : \vec{y} \perp P\}$
$\vee$: $\mathrm{Gr}(\mathcal{H}) \times \mathrm{Gr}(\mathcal{H}) \to \mathrm{Gr}(\mathcal{H})$, $(P,Q) \mapsto P + Q$.

Note that $P + Q = \{\vec{p} + \vec{q} : \vec{p} \in P, \vec{q} \in Q\}$ is the least linear subspace of $\mathcal{H}$ containing $P \cup Q$. We abbreviate $0 := \{0\} \in \mathrm{Gr}(\mathcal{H})$ and $1 := \mathbb{F}^d \in \mathrm{Gr}(\mathcal{H})$.

Fact 2: $\big(\mathrm{Gr}(\mathcal{H}), \neg, \vee, \wedge, 0, 1\big)$ is a modular ortholattice, i.e. a commutative, associative algebraic structure with respect to idempotent operations "$\vee$" and "$\wedge$" with $A \wedge (A \vee B) = A = A \vee (A \wedge B)$ and $A \vee \neg A = 1$ and $A \wedge \neg A = 0$ and $\neg\neg A = A$ and such that the de Morgan laws hold

$$\neg(A \vee B) = \neg A \wedge \neg B, \qquad \neg(A \wedge B) = \neg A \vee \neg B \tag{1}$$

and [Bera85, § II.1] satisfying the modular law

$$A = A \wedge C \quad \Rightarrow \quad A \vee (B \wedge C) = (A \vee B) \wedge C \ . \tag{2}$$

[†]We adopt the affine notion of dimension because it coincides with the height of the induced lattice as opposed to the projective dimension.

A. Motivations from Physics, Geometry, and Logic

We find quantum logic a promising object of study for various reasons and to various communities [CMW00], [EGL07].

1) Physically: it arises from Quantum Mechanical reality. More formally, a classical 0/1-valued observable p ('*property*') corresponds in quantum mechanics to a projection operator $\mathbb{P}$ on some Hilbert space $\mathcal{H}$ of states; which in turn corresponds uniquely to a closed subspace P of $\mathcal{H}$, namely $P = \mathrm{range}(\mathbb{P})$ and $\mathbb{P}$ being the orthogonal projection onto P [Neum55], [Jack06]. That is, P amounts to the collection of states where property $\mathbb{P}$ is present; $\neg P$ where it is absent; $P \wedge Q$ where both $\mathbb{P}$ and $\mathbb{Q}$ are present; and $P \vee Q$ where at least one of $\mathbb{P}$ and $\mathbb{Q}$ are. The subtleties of Quantum Mechanics lead to states where neither a property (e.g. linear polarization at 0°) nor its complement (linear polarization at 90°) need be absent—which classical propositional logic with its (consequence of the distributive) law $Q = (Q \wedge P) \vee (Q \wedge \neg P)$ cannot capture.

2) Geometrically: Quantum Logic captures algebraic aspects of the Grassmannian and thus pertains to the field of Convex and Combinatorial Geometry [MnZi93], [GoOR04]. In fact, this approach makes it particularly accessible to human intuition in low dimensions. For instance the failure of classical laws as mentioned above is instructive to reconstruct in the planar $\mathrm{Gr}(\mathbb{F}^2)$; compare Example 7c) below.

3) Logically: $\mathrm{Gr}(\mathbb{F}^d)$ constitutes a structure which contains (and for $d = 1$ collapses to) the Boolean values $\mathtt{false} = \{0\} = 0$ and $\mathtt{true} = \mathbb{F}^d = 1$. Yet, starting with $d = 2$, $\mathrm{Gr}(\mathbb{F}^d)$ also contains 'intermediate' values like the subspaces $V_n := \mathbb{F} \cdot \binom{1}{n} := \{(t, n \cdot t) : t \in \mathbb{F}\}$, $n \in \mathbb{N}$. This many-valuedness resembles probabilistic/fuzzy logic and, more generally, Gödel Logics which 'interpolate' between 0 (impossibility) and 1 (certainty) with values $r \in [0,1]$ (likelihood). Note, however, that the 'truth values' $\mathbb{F} \cdot \binom{1}{n}$ are pairwise incomparable; cmp. Figure 1a).

B. Varieties of Quantum Logic

Definition 1 and Fact 2 extend to *closed* subspaces of an infinite-dimensional Hilbert space, provided that $P \vee Q$ is understood as the topological closure of $P+Q$ and the modular law (2) is replaced by the the weaker orthomodular law. Quantum Logics $\mathrm{Gr}(\mathcal{H})$ of a Hilbert space $\mathcal{H}$ are sometimes called *Hilbert Lattices*. *Abstract* quantum logic on the other hand takes Fact 2 as axioms and investigates its consequences:

Fact 3: Let $(L, \wedge, \vee, \neg, 0, 1)$ be a modular ortholattice and denote by $C(X,Y) := (X \wedge Y) \vee (X \wedge \neg Y) \vee (\neg X \wedge Y) \vee (\neg X \wedge \neg Y)$ the commutator of $X, Y \in L$. If $C(X,Y) = 1$, then X, Y are said to commute.

a) $C(X,Y) = 1 \Leftrightarrow X = (X \wedge Y) \vee (X \wedge \neg Y)$ [Bera85, §3]

1043-6871/11 $26.00 © 2011 IEEE
DOI 10.1109/LICS.2011.8

IEEE computer society

b) The sublattice generated by $X, Y \in L$ is isomorphic to $\{0,1\}^k$ or to $\{0,1\}^k \times \mathcal{MO}_2$ for some $k \leq 4$ [Kalm83, THEOREM §3.9] where $\mathcal{MO}_n$ is depicted in Figure 1b).

c) If at least one of X, Y, Z commutes with the other two, then the distributive laws $X \wedge (Y \vee Z) = (X \wedge Y) \vee (X \wedge Z)$ and $X \vee (Y \wedge Z) = (X \vee Y) \wedge (X \vee Z)$ do apply [Bera85, THEOREM II.3.10].

d) If $X_1, \ldots, X_n$ pairwise commute, they generate a Boolean algebra isomorphic to $\{0,1\}^k$ for some $k \leq 2n$ [Bera85, top of p.14 and THEOREM II.4.5].

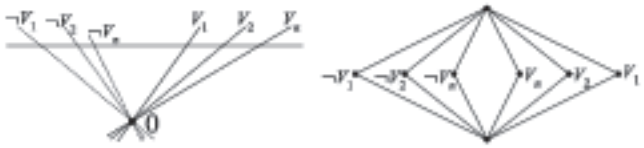

Fig. 1. Prototype $\mathcal{MO}_n$ of a non-distributive modular orthol attice

C. Computational Complexity

The theory of computation is based on classical Boolean logic, providing both a model of computation (namely circuits) and problems characterizing complexity classes $\mathcal{NP}$ (satisfiability, the Cook-Levin Theorem), co$\mathcal{NP}$ (equivalence), and PSPACE (quantified formula).

Quantum logic, on the other hand, has been proposed as an alternative approach to exploit quantum mechanics for computational purposes [Pyka00], [Ying05], [PM07a]. Note that quantum logic subtly differs from common models of quantum computation in that it essentially describes operations on observables, i.e., sequences of measurements, as opposed to operations on states.

D. Blum-Shub-Smale Machines

In algebraic complexity, the BSS machine (also known as *real-RAM* in computational geometry) is a common model [BCSS98] capturing arithmetic on real numbers with unit cost per arithmetic operation; and has led to a rich structural complexity theory [MeMi97]. In particular, the classical question "$\mathcal{P} = \mathcal{NP}$?" naturally transfers to this real (and the similar complex) setting—and has turned out as equally inaccessible [FoKo98], [FoKo00]. As a matter of fact, "$\mathcal{P}$ versus $\mathcal{NP}$" was propagated by STEVE SMALE as *3rd problem for the next century* for both fields $\mathbb{F}_2$ (i.e. the Turing machine model) and for $\mathbb{C}$ [Smal98]. Generalizing the Cook-Levin Theorem, the following problems have been established complete for nondeterministic polynomial-time BSS machines [BSS89] over various ground fields $\mathbb{F}$:

Fact 4: Fix $\mathbb{F}, \mathbb{E} \subseteq \mathbb{C}$ and consider the following decision problem: *Given a polynomial $p \in \mathbb{E}[X_1, \ldots, X_n]$, does it admit a root in $\mathbb{F}$, i.e. some $\vec{x} \in \mathbb{F}^n$ such that $p(\vec{x}) = 0$?* (3)

a) For $\mathbb{E} = \mathbb{R} = \mathbb{F}$ and to nondeterministic polynomial-time BSS-machine model (i.e. the complexity class $\mathcal{NP}_{\mathbb{R}}$) this computational problem is complete [BSS89], [BCSS98], [MeMi97].

More precisely, a polynomial-time Turing machine can, given the description of a BSS machine $\mathcal{M}$ with symbolic names for its real constants and given an input $\vec{y} \in \mathbb{R}^m$, output the dense encoding (coefficient list of its $\mathcal{O}(m^4)$ monomials) of a multivariate polynomial $p_{\mathcal{M}}(X_1, \ldots, X_N; y_1, \ldots, y_m)$ of total degree at most 4 such that the following holds: $\mathcal{M}$ accepts $\vec{y}$ iff $p_{\mathcal{M}}(\cdot; \vec{y})$ admits a real root.

b) For nondeterministic polynomial-time BSS-machines *without constants and on binary inputs* (a complexity class denoted BP$(\mathcal{NP}^0_{\mathbb{R}})$) the above problem (3) is complete in the same sense when restricted to polynomials $p_i(X_1, \ldots, X_N)$ of degree at most 4 and with coefficients in $\mathbb{E} := \{0, \pm 1, \pm 2\}$ (but no symbolic parameters $y_i \in \mathbb{R} =: \mathbb{F}$).

c) In fact in the ordered case $\mathbb{F} \subseteq \mathbb{R}$, the feasibility of a *system* of polynomial in/equalities

$$p_1 = \cdots = p_k = 0, \quad q_1 \neq 0, \ldots, q_\ell \neq 0 \qquad (4)$$

with coefficients from $\mathbb{E} := \mathbb{N}$ can be reformulated (by a Turing machine in time polynomial in the binary description length of the list of nonzero monomials and their coefficients) as the feasibility a single equation $p(\vec{X}) = 0$ with p a sum of squares of quadratic polynomials, each with coefficients from $\{0, \pm 1\}$ (i.e., expanded, from $\{0, \pm 1, \pm 2\}$).

d) For $\mathbb{F} = \mathbb{R}$ and $\mathbb{E} = \mathbb{N}$, a Turing machine can decide the feasibility of Equation (3) in space polynomial in the description length of the input polynomial [Grig88], [HRS90], [Cann88], [MaTo97].

e) For $\mathbb{F} = \mathbb{N} = \mathbb{E}$, the feasibility of (3) is undecidable to a Turing machine [Mati70]. For $\mathbb{F} = \mathbb{Q}$ and $\mathbb{E} = \mathbb{N}$, decidability of (3) is a long-standing open question; cf. e.g. [Poon09].

f) For $\mathbb{F} = \mathbb{C}$, the answer to (3) is trivially positive unless $p \equiv c \neq 0$. However, the feasibility of Equation (4) is non-trivial and complete for BP$(\mathcal{NP}^0_{\mathbb{C}})$ [BCSS98, SECTION 5.4]; yet can, subject to the Generalized Riemann Hypothesis, be decided in $co\mathcal{RP}^{\mathcal{NP}}$ [Koir96].

g) Any problem on binary inputs decidable by a deterministic polynomial-time BSS machine over $\mathbb{F} = \mathbb{R}$ but without constants (i.e. the complexity class BP$(\mathcal{P}^0_{\mathbb{R}})$) belongs to the Turing counting hierarchy [ABKM09].

Note that d), f) and g) relate Turing complexity to BSS complexity by restricting to binary inputs (and prohibiting real constants). It remains an open challenge to tighten these relations [Cuck93]. We also emphasize that the problems above exhibited complete for BSS-machines over $\mathbb{F}$ amount to the question of emptiness of a given (semi-)algebraic set. Several more problems have been shown $\mathcal{NP}_{\mathbb{R}}$-complete [CuRo92], [Koir99] but all pertain to the field of (semi-) algebraic geometry; similarly for higher BSS complexity classes [BuCu06].

E. Related Work

Research trends in quantum logic has, after a digression into event algebras and orthomodular posets, returned to its original motivations: closed subspaces of a Hilbert space [Maye07],

[Herr09], [Megi09]. We focus particularly on the finite-dimensional Hilbert spaces, because they are more tractable. and relevant to quantum computation. Although complexity investigations are common in, say, propositional or modal logic [Marx07], they seem to have passed on quantum logic.

We characterize the complexity classes $\mathcal{NP}$, $\mathcal{NP}_{\mathbb{R}}$, and $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$ as satisfiability problems for real and complex quantum propositional formulas of appropriate dimensions. This provides a unified, resource-free view on both Turing and real BSS complexity theory. It thus resembles descriptive complexity theory, characterizing various Turing complexity classes as appropriate logics. Machine-independent characterizations of some BSS complexity classes have been attained in [BCNM06].

II. Quantum Propositional Formulas: Truth, Equivalence, and Satisfiability

The classical Boolean satisfiability problem extends straightforwardly to quantum propositional formulas—although truth ("$=1$") now has to be distinguished from non-falsity ("$\neq 0$"); and we may or may not permit constants.

Definition 5:
a) A (quantum propositional) formula f over variables $X_1, \ldots, X_n$ is a syntactically correct expression over X_i, $\neg$, $\wedge$, and $\vee$. We may write $f(\vec{X})$ to emphasize the dependence on $(X_1, \ldots, X_n) =: \vec{X}$.
b) For a finite-dimensional inner product space $\mathcal{H}$ over field $\mathbb{F} \subseteq \mathbb{C}$, for subspaces $U_1, \ldots, U_n \in \mathrm{Gr}(\mathcal{H})$, and for a formula $f(X_1, \ldots, X_n)$, let $f_{\mathcal{H}}(U_1, \ldots, U_n) \in \mathrm{Gr}(\mathcal{H})$ denote the value of f when substituting U_i for X_i. Note that negation $\neg U$ is meant relative to the fixed underlying universe $\mathcal{H}$.
c) A formula with constants from $\mathcal{H}$ is a formula where some variables already have been fixed to (i.e. substituted for) elements of $\mathrm{Gr}(\mathcal{H})$.
d) A formula f with arguments $U_1, \ldots, U_n \subseteq \mathcal{H}$ evaluates to `true` if $f_{\mathcal{H}}(\vec{U}) = \mathcal{H}$ holds; it is weakly true if it does not evaluate to 0 (`false`), where $\vec{U} := (U_1, \ldots, U_n)$.
e) An n-variate formula f is strongly satisfiable in $\mathcal{H}$ if there are $U_1, \ldots, U_n \in \mathrm{Gr}(\mathcal{H})$ such that $f_{\mathcal{H}}(\vec{U}) = \mathcal{H}$. It is weakly satisfied by $\vec{U}$ if $f_{\mathcal{H}}(\vec{U}) \neq 0$.
f) Two n-variate formulas f and g are equivalent over $\mathcal{H}$ if $f_{\mathcal{H}}(\vec{U}) = g_{\mathcal{H}}(\vec{U})$ holds for all $U_1, \ldots, U_n \in \mathrm{Gr}(\mathcal{H})$.

Note that weak satisfiability of f means *in*validity of the identify "$f = 0$" in the model-theoretic sense.

Remark 6: The connective "$\vee$" behaves like Boolean disjunction for weak satisfiability: $X \vee Y \neq 0$ holds iff $X \neq 0$ or $Y \neq 0$ holds; but in dimensions > 1, "$\wedge$" differs from Boolean conjunction: $X \wedge Y \neq 0$ may well fail for both $X, Y \neq 0$. Dually, "$\wedge$" behaves in a Boolean way for strong satisfiability but "$\vee$" does not. Furthermore, Boolean negation has to be distinguished from complement: $X \neq 0 \not\Leftrightarrow \neg X = 0$.

Whenever this distinction needs emphasis, we denote the classical propositional connectives as in the C programming language: `||` for "*or*", `&&` for "*and*", `!` for "*not*".

Example 7: We identify $0 \neq \vec{x} \in \mathcal{H}$ with $\mathbb{F} \cdot \vec{x} \in \mathrm{Gr}_1(\mathcal{H})$.

a) $\neg X \vee \neg Y$ and $\neg(X \wedge Y)$ are formulas over variables X, Y. They are equivalent over any Hilbert space.
b) Suppose $X \subseteq \neg Y$ and $X \vee Y = 1$. Then $X = \neg Y$.
c) Recall the commutator $C(X,Y)$ of X, Y. Whenever $X \in \{0, 1, Y, \neg Y\}$ or $Y \in \{0, 1, X, \neg X\}$, it follows $C(X,Y) = 1$. In particular, $C(X,Y)$ is equivalent to 1 on $\mathrm{Gr}(\mathbb{F}^1)$. Over $Z := \mathbb{F}^2$, however, $C(\binom{1}{r}, \binom{1}{s})$ evaluates to 0 whenever $r \notin \{s, -1/s\}$.
d) Let $f(X,Y) := C(X,Y) \vee X \vee Y$ and $g(X,Y,Z) := f(X,Y) \wedge f(X,Z) \wedge f(Y,Z)$. Then g is equivalent to 1 on $\mathrm{Gr}(\mathbb{F}^2)$. Over $\mathbb{F}^3$, however, $g(\binom{1}{0}, \binom{1}{1}, \binom{1}{1}) = 0$.
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 $\mathbb{F}^{2d}$, $d \in \mathbb{N}$; but not over $\mathbb{F}^{2d-1}$.
f) For $X, Y \in \mathrm{Gr}(\mathcal{H})$ it holds: $(X \wedge Y) \vee (\neg X \wedge \neg Y) = 1 \Leftrightarrow (X \vee Y) \wedge (\neg X \vee \neg Y) = 0 \Leftrightarrow X = Y$.

Claims a) and b) can be found in any textbook on Hilbert spaces; compare Fact 2. Claim c) is straightforward to verify. Claim d) has been generalized in [Hagg07] to formulas equivalent to 1 over $\mathbb{F}^{d-1}$, but not over $\mathbb{F}^k$ for every $k \geq d$; see Lemma 10f) below. For Claim e), consider $X := \mathbb{F}^d \times \{0\}^d$ and $Y := \{(\vec{x}, \vec{x}) : \vec{x} \in \mathbb{F}^d\}$ in the even-dimensional case. Conversely, $X \vee \neg Y = 1$ over $\mathbb{F}^D$ implies $D = \dim(X \vee \neg Y) \leq \dim(X) + \dim(\neg Y) = \dim(X) + D - \dim(Y)$; hence $\dim(Y) \leq \dim(X)$. And, by symmetry of $C(X,Y)$, also $\dim(Y) \leq \dim(\neg X)$, $\dim(X) \leq \dim(Y)$, and $\dim(X) \leq \dim(\neg Y)$: Hence $D = \dim(X) + \dim(\neg X)$ must be even.

Claim f) allows to reduce non-equivalence to weak satisfiability. Checking the latter according to Definition 5e) may at first seem to involve an infinite choice of possible arguments (=subspaces of $\mathcal{H}$).

In the sequel we explore the computability and computational complexity of the following type of decision problems: Given a formula f, is it satisfiable over $\mathbb{F}^d$? Different variants distinguish weak and strong satisfiability, over various fields $\mathbb{F} \subseteq \mathbb{C}$, for formulas (unless stated otherwise) without constants. Recall that Boolean satisfiability coincides with satisfiability over $\mathbb{F}^1$, independent of $\mathbb{F}$.

A. 2D Satisfiability is $\mathcal{NP}$-Complete

In dimension 2, both weak and strong satisfiability of formulas without constants turns out as computationally as hard as Boolean satisfiability and independent of $\mathbb{F} \subseteq \mathbb{C}$.

Theorem 8:
a) Consider the 1D subspaces $V_n := \binom{1}{n} \in \mathrm{Gr}_1(\mathbb{Q}^2)$ and note $\neg V_n = \binom{n}{-1}$; cmp. Figure 1. An n-variate formula f without constants is weakly [strongly] satisfiable over $\mathbb{F}^2$ iff there exist $U_1, \ldots, U_n \in \{0, 1, V_1, \neg V_1, \ldots, V_n, \neg V_n\} =: \mathcal{MO}_n$ such that $f(\vec{U}) = 1$ [$f(\vec{U}) \neq 0$].
b) Both weak and strong satisfiability over $\mathbb{F}^2$ without constants do not depend on $\mathbb{F} \subseteq \mathbb{C}$ and can be decided in nondeterministic polynomial time.
c) A polynomial time Turing machine can, given a formula f, produce another formula g having the property that

g is weakly/strongly satisfiable over $\mathbb{F}^2$ iff f is over $\{0,1\}$, again independently of $\mathbb{F} \subseteq \mathbb{C}$.

Proof:

a) Any assignment $U_1, \ldots, U_n \in \mathrm{Gr}(\mathbb{F}^2)$, $\mathbb{F} \subseteq \mathbb{C}$, satisfies

$$U_i \vee U_j, U_i \wedge U_j, \neg U_i \vee \neg U_j, \neg U_i \wedge \neg U_j,$$
$$\neg U_i \vee U_j, \neg U_i \wedge U_j \ \in \ \{0, 1, U_i, U_j, \neg U_i, \neg U_j\} \quad (5)$$

and hence belongs (up to isomorphism) to $\mathcal{MO}_n$.

b) Let f be the given formula. According to a), it suffices to guess an assignment $\vec{U}$ from the restricted set $\{0, 1, V_1, \neg V_1, \ldots, V_n, \neg V_n\}$. And evaluation of f on such an assignment is easy in time polynomial in the length of f, based on Equation (5).

c) We consider strong satisfiability and postpone the weak case to Theorem 14b). Let $g(\vec{X}) := f(\vec{X}) \wedge \bigwedge_{i<j} C(X_i, X_j)$. If $\vec{x} \in \{0,1\}^n$ is a satisfying assignment of f, then it is also one of g because of $C(x_i, x_j) = 1$. Conversely suppose that $g(\vec{U}) = 1$ holds for $U_1, \ldots, U_n \in \mathrm{Gr}(\mathbb{F}^2)$. Then by $C(U_i, U_j) = 1$ and Fact 3d), there also exists a Boolean satisfying assignment. ■

B. On the Dimensional Heredity of Satisfiability

Structural induction on f shows the embedding $\imath : \mathrm{Gr}(\mathbb{F}^d) \ni X \mapsto X \times \{0\} \in \mathrm{Gr}(\mathbb{F}^{d+1})$ to have $f_{\mathbb{F}^{d+1}}\big(\imath(X_1), \ldots, \imath(X_n)\big) \cap \imath(\mathbb{F}^d) = \imath\big(f_{\mathbb{F}^d}(X_1, \ldots, X_n)\big)$. Thus if f is weakly satisfiable over $\mathbb{F}^d$, so is it over $\mathbb{F}^{d+1}$. Corollary 12 shows that the situation with strong satisfiability is more subtle. But first let us record

Definition 9: For $d \in \mathbb{N}$ and n-variate (constant-free) formula f, define

$$\mathrm{maxdim}_{\mathbb{F}}(f, d) \ := \max_{U_1, \ldots, U_n \in \mathrm{Gr}(\mathbb{F}^d)} \dim f(U_1, \ldots, U_n) \ .$$

By $\mathrm{length}(f)$, we mean the encoding length of formula f. For formulas $f(X_1, \ldots, X_n)$ and $g(Y_1, \ldots, Y_m)$, the **restriction** $f(\vec{X})|_{g(\vec{Y})}$ is the following $(n+m)$-variate formula: Using *de Morgan*, write $f(\vec{X}) = f'(\vec{X}, \neg\vec{X})$ where f' has $2n$ variables but no negations; then $f(\vec{X})|_{g(\vec{Y})}$ denotes the formula

$$f'\Big(X_1 \wedge g(\vec{Y}), \ldots, X_n \wedge g(\vec{Y}),$$
$$\neg\big(X_1 \wedge g(\vec{Y})\big) \wedge g(\vec{Y}), \ldots, \neg\big(X_n \wedge g(\vec{Y})\big) \wedge g(\vec{Y})\Big)$$

Intuitively, $f(\vec{X})|_{g(\vec{Y})}$ describes that variables X_j in f be restricted to $\mathrm{Gr}\big(g(\vec{Y})\big)$; see Item b) in

Lemma 10: Let field $\mathbb{F} \subseteq \mathbb{C}$ be quadratically closed, i.e. s.t. $\sqrt{x} \in \mathbb{F}$ for every $0 < x \in \mathbb{F}$.

a) For a unitary matrix $\hat{U} \in \mathbb{F}^{d \times d}$, formula f and $X_1, \ldots, X_n \in \mathrm{Gr}(\mathbb{F}^d)$, it holds $f(\hat{U} \cdot X_1, \ldots, \hat{U} \cdot X_n) = \hat{U} \cdot f(X_1, \ldots, X_n)$. In particular, for any d-dimensional subspace Z of $\mathbb{F}^k$, $\mathrm{maxdim}_{\mathbb{F}}(f, d) = \max_{X_1, \ldots, X_n \in \mathrm{Gr}(Z)} \dim\big(f_Z(X_1, \ldots, X_n)\big)$.

b) It holds $\mathrm{length}(f|_g) \leq \mathrm{length}(f) \cdot \mathrm{length}(g)$ and $\mathrm{maxdim}_{\mathbb{F}}\big(f|_g, d\big) = \mathrm{maxdim}_{\mathbb{F}}\big(f, \mathrm{maxdim}_{\mathbb{F}}(g, d)\big)$.

c) For each formula f and $k, d \in \mathbb{N}$, it holds $\mathrm{maxdim}_{\mathbb{F}}(f, d+k) \geq \mathrm{maxdim}_{\mathbb{F}}(f, d) + \mathrm{maxdim}_{\mathbb{F}}(f, k)$.

d) Let f and g be an n-variate and an m-variate formula, w.l.o.g. in disjoint sets of variables $\vec{X}$ and $\vec{Y}$, respectively. Now consider the $(n+m)$-variate formula $f + g := f(\vec{X}) \vee g(\vec{Y})$. Then $\mathrm{maxdim}_{\mathbb{F}}(f+g, d) = \min\big\{d, \mathrm{maxdim}_{\mathbb{F}}(f, d) + \mathrm{maxdim}_{\mathbb{F}}(g, d)\big\}$.

e) Let $\Pi(X, Z) := Z \wedge (X \vee \neg Z)$ denote the projection of X to Z. Then $\psi_2(X, Z) := \Pi\Big(\Pi\big(\Pi(X, Z), X\big), \neg Z\Big)$ has $\mathrm{maxdim}_{\mathbb{F}}(\psi_2, d) = \lfloor d/2 \rfloor$.

f) To each $d \in \mathbb{N}$ there exists a formula ψ_d independent of $\mathbb{F}$ in $\mathcal{O}(d)$ variables and of length $2^{\mathcal{O}(d)}$ such that $\mathrm{maxdim}_{\mathbb{F}}(\psi_d, d-1) = 0$ but $\mathrm{maxdim}_{\mathbb{F}}(\psi_d, d) = 1$.

Proof: Claim a) is straightforward, b) from [Hagg07, Corollary 3]. For e) note $\dim\big(\Pi(X, Z)\big) \leq \dim(Z)$, hence $\dim\big(\psi_2(X, Z)\big) \leq \min\big\{\dim(Z), \dim(\neg Z)\big\} \leq d/2$; cmp. [Hagg09, Slide #13]. Conversely, $X := \mathbb{F}^{\lfloor d/2 \rfloor} \times \{0\}^{\lceil d/2 \rceil}$ and $Z := \{(\vec{x}, \vec{x}) : \vec{x} \in \mathbb{F}^{\lfloor d/2 \rfloor}\}$ ($\times\{0\}$ in case d is odd) has $\dim\big(\psi_2(X, Z)\big) = \lfloor d/2 \rfloor$. For c), consider assignments $X_j \times Y_j \in \mathrm{Gr}(\mathbb{F}^{d+k})$, where $X_j \in \mathrm{Gr}(\mathbb{F}^d)$ and $Y_j \in \mathrm{Gr}(\mathbb{F}^k)$. Concerning d), $\dim\big(f(\vec{X}) \vee g(\vec{Y})\big) \leq \min\big\{d, \dim f(\vec{X}) + \dim g(\vec{Y})\big\}$ is obvious. Conversely let $\vec{X}$ and $\vec{Y}$ in $\mathrm{Gr}(\mathbb{F}^d)$ such that $V := f(\vec{X})$ has $\dim(V) = \mathrm{maxdim}_{\mathbb{F}}(f, d) =: k$ and $W := g(\vec{Y})$ has $\dim(W) = \mathrm{maxdim}_{\mathbb{F}}(g, d) =: \ell$. W.l.o.g. $\ell + k \leq d$. Exploiting that the fields $\mathbb{F}$ under consideration support taking square roots, we can find two orthonormal bases $\vec{v}_1, \ldots, \vec{v}_d$ and $\vec{w}_1, \ldots, \vec{w}_d$ of $\mathbb{F}^d$ such that $\vec{v}_1, \ldots, \vec{v}_k$ span V and $\vec{w}_1, \ldots, w_{d-\ell}$ span $\neg W$. Then the linear mapping $\hat{U} : \mathbb{F}^d \to \mathbb{F}^d$ defined by $\vec{v}_j \mapsto \vec{w}_j$ is unitary and has $k + \ell = \dim(W \vee \hat{U} \cdot V) = \dim\big(g(\vec{Y}) \vee f(\hat{U} \cdot \vec{X})\big)$ according to a). Regarding f) note that ψ_{2^k}, the k–fold iterated restriction of ψ_2 (e.g. $\psi_8 = \psi_2|_{\psi_2|_{\psi_2}}$) has $\mathrm{maxdim}(\psi_{2^k}, 2^k) = 1$ and $\mathrm{maxdim}(\psi_{2^k}, 2^k - 1) = 0$. More generally, [Hagg07, Theorem 1] establishes that, to each d (not necessarily a power of 2), there exists some formula χ_d that evaluates identically to 0 on $\mathbb{F}^{d-1}$ but not on $\mathbb{F}^d$. Now in case $1 < \mathrm{maxdim}(\chi_d, d) =: \ell$, consider $\psi_{2^k}|_{\chi_d}$ for $k := \lfloor \log_2 \ell \rfloor$ and recall b). ■

The benefit of quadratically closed fields is demonstrated by

(Counter-)Example 11: The 2D subspace $\{(x, x, z) : x, z \in \mathbb{Q}\}$ of $\mathbb{Q}^3$ is not orthogonally equivalent to $\mathbb{Q}^2 \times \{0\}$.

Strong satisfiability of f over $\mathbb{F}^d$ means $\mathrm{maxdim}_{\mathbb{F}}(f, d) = d$, hence we have by Lemma 10c)+d)

Corollary 12: If f is strongly satisfiable in dimension d, then it is also strongly satisfiable in dimensions $2d, 3d, \ldots$

$\psi_2 + \psi_2$ is strongly satisfiable precisely in all even dimensions.

Example 13: For $n \in \mathbb{N}$, the following formula Ψ_{2^n} in $2n+1$ variables has length $\mathcal{O}(n)$ and is strongly satisfiable precisely in dimensions an integer multiple of 2^n.

$$X_{n+1} \ \wedge \ \bigwedge_{i=1}^{n} \Big((X_i \vee \neg Y_i) \ \wedge \ (Y_i \vee \neg X_i) \ \wedge \ (\neg X_i \vee \neg Y_i)$$
$$\wedge \ \Big(\big(X_{i+1} \wedge (X_i \vee Y_i)\big) \vee \big(\neg X_{i+1} \wedge \neg(X_i \vee Y_i)\big) \Big) \Big)$$

Proof: Note that $X_i \vee \neg Y_i = 1$ in $\mathrm{Gr}(\mathbb{F}^d)$ implies $\dim(X_i) + \dim(\neg Y_i) \geq d$; hence the first two terms in the big conjunction require $\dim(X_i) = \dim(Y_i)$. The fourth term amounts to condition $X_{i+1} = X_i \vee Y_i$ according to Example 7f); hence $\dim(X_{i+1}) = \dim(X_i) + \dim(Y_i)$ because of $X_i \wedge Y_i = 0$ (third term). Concluding, any satisfying assignment $(X_1, Y_1, \ldots, X_n, Y_n, X_{n+1})$ of Ψ_{2^n} has $\dim(X_{i+1}) = 2 \cdot \dim(X_i)$. Hence $2^n \cdot \dim(X_1) = \dim(X_{n+1}) = d$ by the very first term of Ψ_{2^n}. Conversely, the following is easily verified to constitute a satisfying assignment of Ψ_{2^n}:

$$X_1 := \mathbb{F} \times \{0\}, \;\; Y_1 := \{(x, x) : x \in \mathbb{F}\},$$
$$X_2 := \mathbb{F}^2 \times \{0\}^2, \;\; Y_2 := \{(\vec{x}, \vec{x}) : \vec{x} \in \mathbb{F}^2\}, \quad \ldots,$$
$$X_{i+1} := \mathbb{F}^{2^i} \times \{0\}^{2^i}, \;\; Y_{i+1} := \{(\vec{x}, \vec{x}) : \vec{x} \in \mathbb{F}^{2^i}\}$$

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

Although a formula may become satisfiable when increasing the dimension, we can now show that the corresponding decision problem does not become easier; and that, moreover, weak and strong satisfiability have equal computational complexity in fixed dimension:

Theorem 14: Fix $1 \leq k < d$ and $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}, \mathbb{A}, \mathbb{A} \cap \mathbb{R}\}$. With respect to polynomial-time Turing many-one reductions,

a) weak satisfiability over $\mathbb{F}^k$ is polynomial-time reducible to weak satisfiability over $\mathbb{F}^d$;
b) and strong satisfiability over $\mathbb{F}^d$ is polynomial-time equivalent to weak satisfiability over $\mathbb{F}^d$.

Proof: Recall that strong satisfiability of f over $\mathbb{F}^d$ means $\mathrm{maxdim}_g(f, d) = d$; and weak satisfiability means $\mathrm{maxdim}_g(f, d) \geq 1$.

b) Hence f is weakly satisfiable over $\mathbb{F}^d$ iff $f + f + \cdots + f$ (d times) according to Lemma 10d) is strongly satisfiable over $\mathbb{F}^d$. Note that, for fixed d, $f \mapsto f + f + \cdots + f$ (d times) is polynomial-time computable. Similarly, f is strongly satisfiable over $\mathbb{F}^d$ iff the restriction $\psi_d|_f$ according to Lemma 10b+f) is weakly satisfiable over $\mathbb{F}^d$. And, again, $f \mapsto \psi_d|_f$ is polynomial-time computable for fixed d.

a) Note that f is weakly satisfiable over $\mathbb{F}^k$ iff the restriction $f|_{\psi_d + \cdots + \psi_d}$ (k times) is weakly satisfiable over $\mathbb{F}^d$. ■

C. Satisfiability in $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$

[DHMW05, Corollary 7] shows (weak) satisfiability over $\mathbb{C}^d$ to be decidable; in fact uniformly in d. The argument proceeds by computationally transforming the given (d, f) into a (both existentially and universally quantified) first-order sentence f^*_d over $\mathbb{R}$ (not over $\mathbb{C}$, since orthogonality involves complex conjugation!) with small integer coefficients which is valid iff f is (weakly) satisfiable over $\mathbb{C}^d$ [DHMW05, Theorem 6]; and truth of f^*_d in turn is algorithmically decidable—although with an excessive complexity [MaMe82].

We observe that a purely existentially quantified first-order sentence suffices for both weak and strong satisfiability:

Lemma 15: Fix $d \in \mathbb{N}$. Both weak and strong satisfiability, over $\mathbb{R}$ and over $\mathbb{C}$, are in BSS complexity class $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$, that is, decidable by a nondeterministic BSS machine over $\mathbb{R}$ devoid of constants.

Note that, even for satisfiability over $\mathbb{C}^d$, real BSS-machines are employed.

Proof: Let the nondeterministic BSS machine guess an assignment $X_1, \ldots, X_n \in \mathrm{Gr}(\mathbb{R}^d)$ by guessing matrices $A_j \in \mathbb{R}^{d \times d}$ representing $X_j = \mathrm{range}(A_j)$. In the complex case, guess matrices $A_j, B_j \in \mathbb{R}^{d \times d}$ representing $X_j = \mathrm{range}(A_j + iB_j)$. In this representation, a constant-free BSS machine can calculate operations $\vee$, $\wedge$, and $\neg$ in time $\mathcal{O}(d^3)$ using Gaussian Elimination. This allows to evaluate f on (i.e. to verify) the guessed assignment in time polynomial in (both d and) $\mathrm{length}(f)$. ■

Together with Fact 4b+d), it follows that both weak and strong satisfiability over $\mathbb{R}^d$ and over $\mathbb{C}^d$ for any fixed d belong to the (classical Turing) complexity class PSPACE.

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

We now show that Lemma 15 is best possible:

Theorem 16: Strong satisfiability over both $\mathbb{R}^3$ and $\mathbb{C}^3$ is $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$–hard.

In view of Fact 4a+b) and Theorem 14, it suffices to reduce real polynomial feasibility (4) to strong satisfiability over both $\mathbb{R}^3$ and $\mathbb{C}^3$. Again, reduction is meant in the many-one sense by a polynomial-time Turing machine.

Our reduction proceeds in two steps, involving a generalization of polynomial feasibility. To this end recall that polynomials are terms over the structure of a commutative ring $(R, +, \times)$. Two extensions, $*$-polynomials are terms over a ring with involution $(R, +, \times, *)$; and noncommutative polynomials are terms over a noncommutative ring structure. This suggests the following variant of the problem from Equation (3) in Fact 4:

Definition 17: Let $p(Y_1, \ldots, Y_n)$ denote a noncommutative $*$-polynomial with coefficients from $\mathbb{E} \subseteq \mathbb{C}$, i.e. an element of the free associative $\mathbb{E}$-algebra generated by $Y_1, \ldots, Y_n, Y_1^*, \ldots, Y_n^*$. Noncommutative $*$-Polynomial Feasibility over $\mathbb{F}^{d \times d}$ is the computational problem of deciding, given such p, whether there exist matrices $\dot{T}_1, \ldots, \dot{T}_n \in \mathbb{F}^{d \times d}$ such that p evaluates to 0, if $\dot{T}_j$ is substituted for Y_j and its adjoint for Y_j^*. ■

Note that this problem captures the emptiness question for noncommutative semialgebraic geometry.

Proposition 18: Fix $d \in \mathbb{N}$ and field $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}, \mathbb{A}, \mathbb{A} \cap \mathbb{R}\}$.

a) In case $\mathbb{F} \subseteq \mathbb{R}$, the feasibility of a given noncommutative integer $*$-polynomial over $\mathbb{F}^{d \times d}$ is reducible to the feasibility of another noncommutative $*$-polynomial over $\mathbb{F}^{d \times d}$ of total degree at most 4 and with coefficients in $\{0, \pm 1, \pm 2\}$.
b) Real polynomial feasibility is reducible to noncommutative $*$-polynomial feasibility over $\mathbb{R}^{d \times d}$.
c) Real polynomial feasibility is also reducible to noncommutative $*$-polynomial feasibility over $\mathbb{C}^{d \times d}$.
d) Noncommutative $*$-polynomial feasibility over $\mathbb{F}^{d \times d}$ is reducible to strong satisfiability over $\mathbb{F}^{3d}$.
e) And (ordinary) polynomial feasibility over $\mathbb{Q}$ (Fact 4e) is polytime equivalent to strong satisfiability over $\mathbb{Q}^3$.

In particular, for any fixed $d \geq 3$, weak/strong satisfiability over $\mathbb{R}^d$ and over $\mathbb{C}^d$ are mutually polynomial-time equivalent and both $\mathrm{BP}(\mathcal{NP}^{\mathcal{Q}}_{\mathbb{R}})$-complete.

Proof of Proposition 18a-c): For a), decompose the evaluation of p into a conjunction of equations about intermediate results and unary $(*)$ or binary $(+,\times)$ operations thereon; similarly for integer constants built up from 1 using addition chains. Then note that, in the ordered case, such a conjunction $0 = p_1(\vec{X}) = \ldots = p_K(\vec{X})$ of degree-two polynomials is equivalent to the single quartic equation $0 = \sum_{k=1}^{K} p_k(\vec{X}) \cdot p_k^*(\vec{X}) =: p(\vec{X})$. Indeed, $p(\vec{T})$ evaluates to a positive semi-definite matrix.

Concerning b+c), add to the conjunction conditions $X_i \cdot X_j = X_j \cdot X_i$ and $X_i^* = X_i$, $1 \leq i < j \leq n$. Then any solution tuple of matrices $T_j \in \mathbb{C}^{d\times d}$ must be hermitian and pairwise commuting; hence, by the Spectral Theorem, is simultaneously diagonalizable, i.e. jointly unitarily equivalent to diagonal real matrices R_j: essentially a d-fold direct product of elements from $\mathbb{R}$. Each component of this tuple $\vec{R}$ thus constitutes a root of the 1D case, that is of the original commutative polynomial; and vice versa. ■

E. Proof of Proposition 18d)+e)

We recall a construction JOHN VON NEUMANN credited to VON STAUDT for interpreting the ring $(\mathbb{F}, 0, 1, -, \times)$ in 3D quantum logic and, more generally, the matrix ring $\mathbb{F}^{d\times d}$ in $\mathrm{Gr}(\mathbb{F}^{3d})$. For instance a scalar $a \in \mathbb{F}$ corresponds to the slope of a line, i.e. of a 1D subspace; and $\hat{A} \in \mathbb{F}^{d\times d}$ to $\{(\vec{x}, -\hat{A}\cdot\vec{x}, 0) : \vec{x} \in \mathbb{F}^d\} \in \mathrm{Gr}_d(\mathbb{F}^{3d})$; cmp. Figure 2b).

Lemma 19: Fix a field $\mathbb{F} \subseteq \mathbb{C}$ and inner product space $\mathcal{H}$ as well as $X, Y \in \mathrm{Gr}(\mathcal{H})$ with $X \perp Y$.

a) Let $\hat{F} : X \to Y$ be a linear map. Then

$$V := \mathrm{graph}(-\hat{F}) := \{\vec{x} - \hat{F}\cdot\vec{x} : \vec{x} \in X\} \qquad (6)$$

has $X \vee Y = V \vee Y$ and $Y \wedge V = 0$.

b) Moreover, $\mathrm{graph}(\hat{0}) = X$. $\hat{F}$ is injective iff $X \wedge V = 0$; and surjective iff $X \vee V = X \vee Y$. If $\hat{F}$ is bijective, then $\mathrm{graph}(-\hat{F}^{-1}) = \mathrm{graph}(-\hat{F})$. The adjoint $\hat{F}^\dagger : Y \to X$ finally has $\mathrm{graph}(-\hat{F}^\dagger) = \neg\,\mathrm{graph}(+\hat{F}) \cap (X \vee Y)$.

c) Conversely, to $W \in \mathrm{Gr}(\mathcal{H})$ with $X \vee Y = W \vee Y$ and $Y \wedge W = 0$, there exists a unique linear map $\hat{G} : X \to Y$ such that $W = \mathrm{graph}(-\hat{G})$.

d) For $Z \in \mathrm{Gr}(\mathcal{H})$ with $Y \perp Z \perp X$ and linear $\hat{G} : Y \to Z$, $\mathrm{graph}(-\hat{G}\circ\hat{F}) = \big(\mathrm{graph}(-\hat{F}) \vee \mathrm{graph}(-\hat{G})\big) \wedge \neg Y$.

e) For $X, Y, Z \in \mathrm{Gr}(\mathcal{H})$ with $X \perp Y \perp Z \perp X$, linear maps $\hat{G}, \hat{H} : Y \to Z$ and isomorphism $\hat{F} : X \to Y$, it holds

$$\Big(\big[(\mathrm{graph}(-\hat{G}) \vee \mathrm{graph}(-\hat{H}\circ\hat{F})) \wedge (Z \vee \mathrm{graph}(-\hat{F}))\big] \vee X\Big) \wedge \Big(Y \vee Z\Big) \;=\; \mathrm{graph}\big(-(\hat{G}-\hat{H})\big)$$

f) Fix $X, Y, Z \in \mathrm{Gr}(\mathcal{H})$ with $X \perp Y \perp Z \perp X$. Let $\hat{F} : X \to Y$ and $\hat{G} : Y \to Z$ be linear isomorphisms. Then $U := \mathrm{graph}(-\hat{F})$ and $V := \mathrm{graph}(-\hat{G})$ satisfy

$$X \vee U = X \vee Y = U \vee Y, \;\; Y \wedge U = 0 = X \wedge U,$$
$$Y \vee V = Y \vee Z = V \vee Z, \;\; Z \wedge V = 0 = Y \wedge V. \qquad (7)$$

Conversely if $U, V \in \mathrm{Gr}(\mathcal{H})$ satisfy Equation (7), then $U = \mathrm{graph}(-\hat{F})$ and $V = \mathrm{graph}(-\hat{G})$ for unique linear isomorphisms $\hat{F} : X \to Y$ and $\hat{G} : Y \to Z$; cmp. Figure 2a).

g) Fix $X, Y, Z \in \mathrm{Gr}(\mathcal{H})$ with $X \perp Y \perp Z \perp X$ and linear isomorphisms $\hat{F} : X \to Y$ and $\hat{G} : Y \to Z$ with corresponding $U = \mathrm{graph}(-\hat{F})$, $V = \mathrm{graph}(-\hat{G})$ as in f). For $\hat{A}, \hat{B} : X \to X$, write $A := \mathrm{graph}(-\hat{F}\circ\hat{A}) \in \mathrm{Gr}(\mathcal{H})$ and $B := \mathrm{graph}(-\hat{F}\circ\hat{B}) \in \mathrm{Gr}(\mathcal{H})$. Then $\mathrm{graph}(-\hat{F}\circ\hat{B}\circ\hat{A}) \in \mathrm{Gr}(\mathcal{H})$ coincides with

$$\Big(V \vee \Big[\Big(\big[\big[(B \vee V) \wedge \neg Y\big] \vee U\big) \wedge \neg X\big] \vee A\Big) \wedge \neg Y\Big]\Big) \wedge \neg Z$$

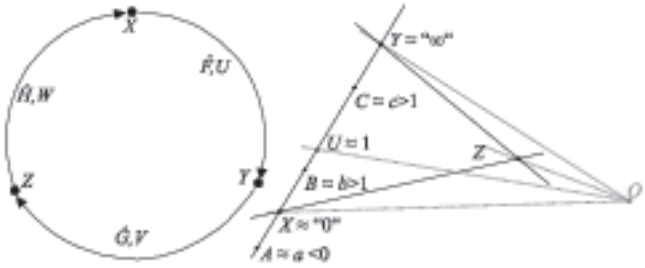

Fig. 2. a) Isomorphisms $\hat{F}, \hat{G}, \hat{H}$ between X, Y, Z and their respective graphs U, V, W employed in Lemma 19e)+f). b) In 3D, encoding real numbers $a < 0 < b < 1 < c$ as slopes of lines in the plane $X \vee Y$.

Subspaces X, Y, Z, U, V satisfying $X \perp Y \perp Z \perp X$ and Equation (7) are known as a (orthogonal von Neumann 3-) *frame*. We call $\dim(X)$ $(= \dim(Y) = \dim(Z))$ its *dimension*; and refer to the following example as *standard* frame in $\mathrm{Gr}(\mathbb{F}^{3d})$: $X = \{(\vec{x}, 0, 0) : \vec{x} \in \mathbb{F}^d\}$, $Y = \{(0, \vec{y}, 0) : \vec{y} \in \mathbb{F}^d\}$, $Z = \{(0, 0, \vec{z}) : \vec{z} \in \mathbb{F}^d\}$, $U = \{(\vec{x}, -\vec{x}, 0) : \vec{x} \in \mathbb{F}^d\}$, $V = \{(\vec{x}, 0, -\vec{x}) : \vec{x} \in \mathbb{F}^d\}$.

Proof of Lemma 19: Items a)-c) are easy linear algebra.

d) Let $\vec{x} - \vec{z} \in \mathrm{graph}(-\hat{G}\circ\hat{F})$, i.e. with $\vec{z} = \hat{G}\cdot\hat{F}\cdot\vec{x}$. Then $\vec{y} := \hat{F}\cdot\vec{x}$ has $\vec{x} - \vec{z} = \vec{x} - \vec{y} + \vec{y} - \vec{z} \in \mathrm{graph}(-\hat{F}) \vee \mathrm{graph}(-\hat{G})$ and $\vec{x} - \vec{z} \in X \vee Z \perp Y$.
Conversely, let $\vec{x} + \vec{y} + \vec{z} \in \big(\mathrm{graph}(-\hat{F}) \vee \mathrm{graph}(-\hat{G})\big) \wedge \neg Y$ with $\vec{x} \in X$, $\vec{y} \in Y$, and $\vec{z} \in Z$. Then necessarily $\vec{y} = 0$ because $X \perp Y \perp Z \perp X$. Moreover, for some $\vec{x}' \in X$, $\vec{y}' \in Y$, it holds $\vec{x} + \vec{z} = (\vec{x}' - \hat{F}\cdot\vec{x}') + (\vec{y}' - \hat{G}\cdot\vec{y}')$; and $X \perp Y \perp Z \perp X$ requires $\vec{x} = \vec{x}'$ and $\vec{z} = -\hat{G}\cdot\vec{y}'$ and $\vec{y}' - \hat{F}\cdot\vec{x}' = 0$.

f) Equation (7) follows from a)+b), the converse from c).

g) Item d) applies only to the composition of linear mappings between distinct ones of the subspaces X, Y, Z, i.e. not to, say, $\hat{F}^{-1}\circ(\hat{F}\circ\hat{A}) : X \to X$. Instead, insert isomorphisms $\hat{F}, \hat{G}$ between X, Y, Z to obtain $\hat{F}\circ\hat{B}\circ\hat{A}$

$$= \hat{G}^{-1}\circ\Big(\big((\hat{G}\circ(\hat{F}\circ\hat{B}))\circ\hat{F}^{-1}\big)\circ(\hat{F}\circ\hat{A})\Big)$$

where each subterm indeed constitutes a linear map between distinct ones of the subspaces X, Y, Z, i.e. such that d) applies. Finally recall $\mathrm{graph}(-\hat{F}) = U = \mathrm{graph}(-\hat{F}^{-1})$ and similarly for $\hat{G}$. ■

From Lemma 19 we conclude

Lemma 20: Let $\mathbb{F} \subseteq \mathbb{C}$ denote a field and $\mathcal{H} := \mathbb{F}^{3d}$, $d \in \mathbb{N}$.

a) There is a quantum propositional formula $f_0(X,Y,Z,U,V)$ independent of $\mathcal{H}$ which, for every $X,Y,Z,U,V \in \mathrm{Gr}(\mathcal{H})$, evaluates to `true` iff X,Y,Z,U,V form a d-dimensional frame.

b) For every d-dimensional frame X,Y,Z,U,V in $\mathrm{Gr}(\mathcal{H})$, there exists an embedding $\Phi = \Phi_{X,Y,Z,U,V} : \mathrm{End}(X) \ni \hat{A} \mapsto \Phi(A) \in \mathrm{Gr}_d(\mathcal{H})$ satisfying $\Phi(0) = X$ and $\Phi(\mathrm{id}_X) = U$. Moreover there exists a quantum propositional formula $f_\dagger(C;X,Y,Z,U,V)$ independent of $\mathcal{H}$ such that, whenever X,Y,Z,U,V constitute a d-dimensional frame, $f_\dagger(C;X,Y,Z,U,V) = 1$ iff $C = \Phi(\hat{C})$ for some $\hat{C} \in \mathrm{End}(X)$.

c) Furthermore there exist quantum propositional formulas $f_\times(A,B;X,Y,Z,U,V)$, $f_-(A,B;X,Y,Z,U,V)$, $f_\dagger(A;X,Y,Z,U,V)$ such that, whenever X,Y,Z,U,V constitute a d-dimensional frame in $\mathrm{Gr}(\mathcal{H})$, the above embedding Φ has $f_\times\big(\Phi(\hat{A}),\Phi(\hat{B})\big) = \Phi(\hat{A}\cdot\hat{B})$ and $f_-\big(\Phi(\hat{A}),\Phi(\hat{B})\big) = \Phi(\hat{A}-\hat{B})$ and $f_\dagger\big(\Phi(\hat{A})\big) = \Phi(\hat{A}^\dagger)$.

d) To each noncommutative $*$-polynomial $p(\hat{A}_1,\dots,\hat{A}_n)$ with integer coefficients, there exists a quantum propositional formula $g_p(A_1,\dots,A_n;X,Y,Z,U,V)$ such that, for each $d \in \mathbb{N}$ and each field $\mathbb{F} \subseteq \mathbb{C}$, g_p is strongly satisfiable over $\mathbb{F}^{d\times d}$ iff p is feasible over $\mathrm{End}(X)$ for some $X \in \mathrm{Gr}_d(\mathbb{F}^{3d})$.

e) Formula g_p according to d) can be computed from p by a Turing machine in polynomial time.

f) For $X \in \mathrm{Gr}_d(\mathcal{H})$, the ring $\mathrm{End}(X)$ of linear endomorphisms is isomorphic to the matrix ring $\mathbb{F}^{d\times d}$; and, considered as a $*$-ring with respect to adjunction, $\mathrm{End}(X)$ is isomorphic to $\mathbb{F}^{d\times d}$ in case $\mathbb{F} \in \{\mathbb{R},\mathbb{C},\mathbb{A},\mathbb{A}\cap\mathbb{R}\}$.

Items a) to d) are well-known in the appropriate community, cmp. [Herr84]. Only our modest strengthening e) seems to be new and establishes, in connection with f), Proposition 18d)+e).

Proof of Lemma 20 (Sketch): a) Consider the conjunction of condition $X \perp Y \perp Z \perp X$ and Equation (7) and $X \vee Y \vee Z$.

b) The claimed embedding is $\mathrm{End}(X) \ni \hat{A} \mapsto \Phi(\hat{A}) := \mathrm{graph}(-\hat{F}\circ\hat{A}) \in \mathrm{Gr}_d(\mathcal{H})$ where $\hat{F} : X \to Y$ is the unique linear isomorphism with $\mathrm{graph}(-\hat{F}) = U$. Formula $f_\dagger(C;X,Y,Z,U,V)$ checks $X \vee Y = C \vee Y$ and $Y \wedge C = 0$ according to Lemma 19a+c).

c) For $f_\times(A,B;X,Y,Z,U,V)$ see Lemma 19g). We refrain from explicitly deducing $f_-(A,B;X,Y,Z,U,V)$ from Lemma 19e) and $f_\dagger$ from Lemma 19b).

d) Given a noncommutative $*$-polynomial $p(\hat{A}_1,\dots,\hat{A}_n)$, replace each occurrence of $\times$, $-$, and $\dagger$ with $f_\times$, f_-, and $f_\dagger$, respectively. (Express $+$ as double $-$.) Require the result to coincide with $X = \Phi(0)$ and conjunctively add the conditions $f_\dagger(A_j) = 1$ for $j = 1,\dots,n$ as well as $f_0(X,Y,Z,U,V)$. The resulting formula g_p then has the property that every satisfying assignment $A_1,\dots,A_n \in \mathrm{Gr}(\mathbb{F}^{3d})$ corresponds to a root $\hat{A}_1,\dots,\hat{A}_n \in \mathrm{End}(X)$ of p for some d-frame X,Y,Z,U,V—and vice versa.

e) The translation described in d) can be carried out in time polynomial in the length of p.

f) Mapping a d-element basis of X to one of $\mathbb{F}^d$ defines a linear isomorphism. Moreover for quadratically closed $\mathbb{F}$, X and $\mathbb{F}^d$ admit orthonormal bases; which define a linear isometry respecting subspace orthogonality. ■

F. Comparing 2D and 3D Satisfiability

We have seen the complexity of satisfiability problem to jump from (Turing-) $\mathcal{NP}$ in dimensions 1 and 2 to the (purportedly larger BSS-class) $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$ in dimensions 3 and above.

1) Fields of Satisfiability: In particular, the computational complexity of satisfiability is independent of underlying field being $\mathbb{R}$ or $\mathbb{C}$. Starting with dimension $d \geq 3$ satisfiability itself, however, does depend on the field:

Proposition 21: a) A formula is weakly/strongly satisfiable over $\mathbb{F}^2$ iff it is over $\mathbb{Q}^2$.

b) If f is weakly/strongly satisfiable over $\mathbb{R}^d$, then also over $\mathbb{C}^d$.

c) Conversely, if f is weakly/strongly satisfiable over $\mathbb{C}^d$, then also over $\mathbb{R}^{2d}$.

d) There is a formula satisfiable over $\mathbb{C}^3$ but not over $\mathbb{R}^3$.

e) There is a formula satisfiable over $\mathbb{R}^3$ but not over $\mathbb{Q}^3$.

f) A formula f is weakly/strongly satisfiable over $\mathbb{C}^d$ iff it is over $\mathbb{A}^d$. Similarly, f is weakly/strongly satisfiability over $\mathbb{R}^d$ iff it is over $(\mathbb{A}\cap\mathbb{R})^d$.

Proof: a) See Theorem 8a). b) Immediate.

c) One can verify that the mapping

$$\mathrm{Gr}_k\left(\mathbb{C}^d\right) \ni X \mapsto \hat{X} \in \mathrm{Gr}_{2k}(\mathbb{R}^{2d}),$$
$$\hat{X} := \{(\vec{v},\vec{w}) : \vec{v},\vec{w} \in \mathbb{R}^d, \vec{v}+i\vec{w} \in X\}$$

is well-defined and satisfies $\neg\hat{X} = \widehat{\neg X}$ and $\widehat{X\wedge Y} = \hat{X} \wedge \hat{Y}$ and $\widehat{X\vee Y} = \hat{X} \vee \hat{Y}$. Hence, for $(X_1,\dots,X_n)$ a weakly/strongly satisfying assignment in $\mathbb{C}^d$, $(\hat{X_1},\dots\hat{X_n})$ constitutes one in $\mathbb{R}^{2d}$.

d) Consider the formula g_{X^2+1} according to Lemma 20d) with $d = 1$. e) Similarly consider g_{X^2-2}.

f) Rewrite weak/strong satisfiability over $\mathbb{R}^d$ as a first-order sentence in the language of $\mathbb{R}$ as in the proof of [DHMW05, Theorem 6]. According to Tarski-Seidenberg [BPR03, Theorem 2.80], such a sentence is valid over $\mathbb{R}$ iff it is valid over $\mathbb{A}\cap\mathbb{R}$. ■

Quantum satisfiability thus exhibits similar properties as the realizability problem for oriented matroids [BL*99, Theorem 8.7.2+Proposition 8.4.2].

2) Number of Nonequivalent Formulas: In the Boolean case $d = 1$, there are exactly 2^{2^n} nonequivalent formulas in n variables: each $f(X_1,\dots,X_n)$ uniquely gives rise to a function $F : \{0,1\}^n \to \{0,1\}$; and conversely any such function can be expressed as a formula in, say, conjunctive normal form. For $d = 2$ we record

Theorem 22: The count of n-variate formulas nonequivalent over $\mathbb{F}^2$ is of order $2^{2^{\Theta(n\log n)}}$, independently of $\mathbb{F} \subseteq \mathbb{C}$.

The exact number has been determined in [HKW97, THEOREM 3.3]. Over $\mathbb{F}^d$, independent of $\mathbb{F}$ and of $d \geq 2$, there are precisely 96 non-equivalent bivariate formulas (recall Fact 3b); these have been listed in [Bera85, FIG.18]. Over $\mathbb{F}^3$, however, there is an infinity of non-equivalent 3-variate formulas [Bera85, EXAMPLE III.2.15].

3) 3D Satisfiability with Constants is $\mathcal{NP}_{\mathbb{R}}$-Complete: We have seen that the satisfiability of a given formula without constants over $\mathbb{C}^3$ or $\mathbb{R}^3$ is complete for nondeterministic polynomial-time BSS machines on binary inputs, i.e. for $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$. Adapting our tools covers also real parameters:

Theorem 23: Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$ and consider formulas *with* constants from $\mathrm{Gr}(\mathbb{F}^3)$. Encode such a constant $V \in \mathrm{Gr}_{1/2}(\mathbb{F}^3)$ as one or two spanning vectors $\vec{a}, \vec{b} \in \mathbb{R}^3$ in the real case; as four vectors $\mathrm{Re}(\vec{a}), \mathrm{Im}(\vec{a}), \mathrm{Re}(\vec{b}), \mathrm{Im}(\vec{b}) \in \mathbb{R}^3$ in the complex case. Regarding this extended satisfiability as a non-discrete decision problem for BSS machines, it holds:

a) Both weak and strong satisfiability over $\mathbb{F}^3$ belong to class $\mathcal{NP}^0_{\mathbb{R}}$, i.e. are decidable by a nondeterministic polynomial-time BSS machine without constants.

b) Strong satisfiability over $\mathbb{F}^3$ is $\mathcal{NP}_{\mathbb{R}}$-hard (w.r.t. Turing polynomial-time many-one reductions performing symbolic transformations on the real number parts of an instance).

c) Strong satisfiability over $\mathbb{F}^3$ and weak satisfiability over $\mathbb{F}^3$ are polynomial-time equivalent.

Proof (Sketch): a) similarly to Lemma 15.

b) According to Fact 4, it suffices to encode the real feasibility of a polynomial p with *real* coefficients as strong satisfiability of a formula over $\mathbb{F}^3$. Now similarly to the proof of Lemma 20d), encode the operations and variables constituting p using formulas $f_\times, f_-, f_\dagger, f_\ddagger, f_0$ into formula g_p. Inspection of the embedding $\Phi_{X,Y,Z,U,V} : \mathbb{F} \to \mathrm{Gr}(\mathbb{F}^3)$ reveals that, for the standard frame from Section II-E, $a \in \mathbb{F}$ gets mapped to $\Phi(a) = (-1, a, 0)$. So, exploiting that the resulting quantum logic formula may contain constants, we fix the (former) variables X, Y, Z, U, V to be the standard frame; and embed the real polynomial coefficients a as further constants $\Phi(a)$: which involves only symbolic manipulations but no real arithmetic.

c) To reduce strong to weak satisfiability, observe that the Definition 9 of the restriction $f|_g$ makes sense also for formulas with constants. Moreover, although Lemma 10a) may fail for formulas with constants, Lemma 10b) does remain valid as long as only g contains constants. In particular, $\psi_d|_f$ is weakly satisfiable over $\mathbb{F}^d$ iff f is strongly satisfiable. The converse reduction follows from the composition of a)+b). ■

III. COMPUTABILITY AND COMPLEXITY IN INDEFINITE (YET FINITE) DIMENSIONS

Both Theorem 14 and Lemma 15 apply to arbitrary but fixed dimensions. We now proceed to indefinite finite dimensions:

Definition 24: Call f weakly/strongly satisfiable over $\mathbb{F}^* := \bigcup_d \mathbb{F}^d$ iff it is weakly/strongly satisfiable over $\mathbb{F}^d$ for *some* d.

According to Proposition 21b+c), satisfiability over $\mathbb{R}^*$ is equivalent to satisfiability over $\mathbb{C}^*$; and moreover recursively enumerable by iteratively applying Lemma 15 to $d = 1, 2, \ldots$

A. Weak Satisfiability over $\mathbb{R}^*$ no more difficult than over $\mathbb{R}^3$

Theorem 25: a) Let g be a formula of length ℓ without negations and $X_1, \ldots, X_n \in \mathrm{Gr}(\mathcal{H})$ be such that $g(\vec{X}) \geq Z \in \mathrm{Gr}_1(\mathcal{H})$. Then there exist $Y_i \in \mathrm{Gr}(\mathcal{H})$ of $\dim(Y_i) \leq \ell$ with $Y_i \leq X_i$ such that $g(\vec{Y}) \geq Z$.

b) Let formula $f(X_1, \ldots, X_n)$ be weakly satisfiable over $\mathbb{R}^*$. Then it is also weakly satisfiable over $\mathbb{R}^{n \cdot \mathrm{length}(f)}$.

c) Weak satisfiability over $\mathbb{R}^*$ (or over $\mathbb{C}^*$) is in $\mathrm{BP}(\mathcal{NP}^0_{\mathbb{R}})$.

We are not aware of a significant lower complexity bound to weak satisfiability over $\mathbb{R}^*$.

Proof:

a) is a refined structural induction on g [Herr10], the start $g = X_i$ being obvious: take $Y_i := Z \leq g(\vec{X}) = X_i$.
For the induction step, first consider the case $g = g_1 \wedge g_2$. By presumption, $g_1(\vec{X}) \wedge g_2(\vec{X}) \geq Z$; i.e. $g_j(\vec{X}) \geq Z$ for $j = 1, 2$. Thus, by induction hypothesis on g_j of length $|g_j| < |g|$, there exist $Y_i^{(j)} \leq X_i$ of $\dim(Y_i^{(j)}) \leq |g_j|$ such that $g_j(\vec{Y}^{(j)}) \geq Z$. Hence, $Y_i := Y_i^{(1)} \vee Y_i^{(2)} \leq X_i$ has $\dim(Y_i) \leq (|g_1| + |g_2|) \leq \ell$ and $g_j(\vec{Y}) \geq g_j(\vec{Y}^{(j)}) \geq Z$ by monotonicity: $g(\vec{Y}) \geq Z$.
It remains to consider the inductive step in case $g = g_1 \vee g_2$. By presumption, $g_1(\vec{X}) \vee g_2(\vec{X}) \geq Z$; i.e. $g_j(\vec{X}) \geq Z_j$ for appropriate $Z_1, Z_2 \in \mathrm{Gr}_{\leq 1}(\mathcal{H})$ with $Z_1 \vee Z_2 \geq Z$. Thus, by induction hypothesis, there exist $Y_i^{(j)} \leq X_i$ of $\dim(Y_i^{(j)}) \leq |g_j|$ such that $g_j(\vec{Y}^{(j)}) \geq Z_j$. Therefore $Y_i := Y_i^{(1)} \vee Y_i^{(2)} \leq X_i$ has $\dim(Y_i) \leq \ell$; and since g_j without negations is monotone, $g_j(\vec{Y}) \geq g_j(\vec{Y}^{(j)}) \geq Z_j$: $g(\vec{Y}) \geq Z$.

b) Write $f(\vec{X}) = g(\vec{X}, \neg\vec{X})$ with negation-free g as in Definition 9. By hypothesis there exists $d \in \mathbb{N}$ and $X_1, \ldots, X_n \in \mathrm{Gr}(\mathcal{H} := \mathbb{F}^d)$ such that $0 \neq f(\vec{X})$, i.e. $g(\vec{X}, \neg\vec{X}) \geq Z$ for some $Z \in \mathrm{Gr}_1(\mathcal{H})$. Now consider $Y_1, \ldots, Y_n, Y_{n+1}, \ldots, Y_{2n}$ according to a), i.e. with with $Y_j \leq X_j$ and $Y_{n+j} \leq \neg X_j$ for $j \leq n$. $Y_1, \ldots, Y_n$ live in the subspace $\mathcal{H}' := \bigvee_{j=1}^n Y_j \subseteq \mathcal{H}$ of $\dim(\mathcal{H}') \leq n\ell$. Moreover, $Y_{n+j} \leq \neg X_j \leq \neg Y_j$ and monotonicity of g shows $0 \neq Z \leq g(Y_1, \ldots, Y_n, Y_{n+1}, \ldots, Y_{2n}) \leq g(Y_1, \ldots, Y_n, \neg Y_1, \ldots, \neg Y_n) = f(Y_1, \ldots, Y_n)$: a weakly satisfying assignment of f.

c) According to b) and Section II-B, it suffices to decide weak satisfiability over $\mathbb{R}^d$ for $d := n \cdot \mathrm{length}(f)$; which a nondeterministic BSS machine can do in polynomial time. ■

B. Strong satisfiability over $\mathbb{R}^*$ is at least as hard as over $\mathbb{R}^3$

Theorem 26: Fix $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}, \mathbb{A}, \mathbb{A} \cap \mathbb{R}\}$.

a) Real polynomial feasibility is polynomial-time reducible to strong satisfiability over $\mathbb{F}^*$.

b) Strong satisfiability over $\mathbb{F}^*$ is polynomial-time equivalent to noncommutative real or complex $*$-polynomial feasibility over *unknown* finite dimensions, that is the question of whether a given $*$-polynomial is feasible over $\mathbb{F}^{d \times d}$ for *some* $d \in \mathbb{N}$.

Proof: Reconsidering the proof of Proposition 18b+c) reveals that the reduction from real polynomial feasibility to

$*$-polynomial feasibility over $\mathbb{F}^d$ is uniform in d, i.e. in fact a reduction to $*$-polynomial feasibility over unknown dimension. Claim a) thus follows from Claim b).

In order to reduce $*$-polynomial feasibility over unknown dimensions to strong satisfiability, we similarly observe that Proposition 18d) holds uniformly in d. As a matter of fact the embeddings $\Phi : \mathbb{F}^{d\times d} \to \mathrm{Gr}_d(\mathbb{F}^{3d})$ described in Section II-E only require the target space to have dimension a multiple of 3: a condition expressible as $\psi_3 + \psi_3 + \psi_3 = 1$ according to Lemma 10d+f).

Finally reducing strong satisfiability over $\mathbb{F}^*$ to $*$-polynomial feasibility over unknown dimensions, represent each $Y \in \mathrm{Gr}(\mathbb{F}^d)$ by any matrix $\hat{Y} \in \mathbb{F}^{d\times d}$ with $Y = \mathrm{range}(\hat{Y})$. Lemma 27b+c) shows how to encode the connectives "$\vee$" and "$\neg$" (and by de Morgan also "$\wedge$") in terms of matrix equations (of degree 2 with constants $0, 1, -1$) by introducing new existentially quantified variables. Combine these into one single $*$-polynomial equation as in the proof of Proposition 18a). This constitutes a polynomial-time reduction from strong satisfiability over $\mathbb{F}^d$ to $*$-polynomial feasibility over $\mathbb{F}^{d\times d}$, independent of d. ■

Lemma 27: Let $\mathbb{F}$ denote any field and $d \in \mathbb{N}$.

a) For $\hat{S}, \hat{T} \in \mathbb{F}^{d\times d}$, it holds

$$\mathrm{range}(\hat{S}) \subseteq \mathrm{range}(\hat{T}) \quad \Leftrightarrow \quad \exists \hat{X} \in \mathbb{F}^{d\times d} : \hat{S} = \hat{T}\cdot\hat{X} \ .$$

b) For $\hat{R}, \hat{S}, \hat{T} \in \mathbb{F}^{d\times d}$, it holds

$$\mathrm{range}(\hat{S}) \vee \mathrm{range}(\hat{T}) = \mathrm{range}(\hat{R}) \quad \Leftrightarrow$$
$$\exists \hat{X}, \hat{Y}, \hat{W}, \hat{Z} \in \mathbb{F}^{d\times d} :$$
$$\hat{R} = \hat{S}\cdot\hat{X} + \hat{T}\cdot\hat{Y} \ \&\& \ \hat{S} = \hat{R}\cdot\hat{W} \ \&\& \ \hat{T} = \hat{R}\cdot\hat{Z} \ .$$

c) For $\hat{R}, \hat{S}, \hat{T} \in \mathbb{F}^{d\times d}$, $\mathrm{range}(\hat{S}) = \neg\,\mathrm{range}(\hat{T}) \Leftrightarrow$

$$\exists \hat{X} \in \mathbb{F}^{d\times d} : \hat{S}\cdot\hat{T}^\dagger = 0 \ \&\& \ (\hat{S}+\hat{T})\cdot\hat{X} = \mathrm{id} \ .$$

C. Dimensions of Satisfiability and Nonuniform Complexity

The question of whether strong satisfiability over $\mathbb{R}^*$ is decidable remains open, cmp. [Herr87], [Rodd89]. If we had, similar to Theorem 25b), a recursive upper bound on the dimension of satisfiability for satisfiable formulas of length n, one could effectively exhaust these dimensions to decide the satisfiability of a given f. And, conversely, if satisfiability over $\mathbb{R}^*$ is decidable one can enumerate all satisfiable formulas f of given length n and, for each such f, determine the first dimension it is satisfiable in: thus obtaining a recursive upper bound on the dimension of satisfiability. Notice that such a bound must be at least exponential in view of Example 13.

For a single (i.e. non-uniformly in) formula f however, the question for which dimensions f is weakly/strongly satisfiable in turns out as computationally surprisingly easy. In fact this holds for an entire family of satisfiability problems including both weak ($\vartheta \equiv 1$) and strong ($\vartheta(d) = d$) as special cases:

Definition 28: Let $\vartheta : \mathbb{N} \to \mathbb{N}$ be subadditive: $\vartheta(d_1+d_2) \le \vartheta(d_1)+\vartheta(d_2)$. Call a formula f ϑ-satisfiable over $\mathbb{F}^*$ if there is some $d \in \mathbb{N}$ such that $\mathrm{maxdim}_{\mathbb{F}}(f,d) \ge \vartheta(d)$. Denote by $\mathrm{Dim}_\vartheta(f) := \{n \in \mathbb{N} : \mathrm{maxdim}(f,n) \ge \vartheta(n)\}$ the set of dimensions which f is ϑ-satisfiable in.

Theorem 29: a) $\mathrm{Dim}_\vartheta(f)$ is an additive semigroup, i.e. $x, y \in \mathrm{Dim}_\vartheta(f) \Rightarrow x+y \in \mathrm{Dim}_\vartheta(f)$.

b) For each formula f and subadditive ϑ, deciding $\mathrm{Dim}_\vartheta(f) \subseteq \mathbb{N}$ is in $\mathcal{NC}^1$.

Proof: a) Observe that $\mathrm{maxdim}(f,x) \ge \vartheta(x)$ and $\mathrm{maxdim}(f,y) \ge \vartheta(y)$ imply $\mathrm{maxdim}(f,x+y) \ge \mathrm{maxdim}(f,x) + \mathrm{maxdim}(f,y) \ge \vartheta(x)+\vartheta(y) \ge \vartheta(x+y)$ because $\mathrm{maxdim}(f,\cdot)$ is superadditive (Lemma 10c) and ϑ subadditive by prerequisite.

b) It is well-known [Grill01, PROPOSITION II.4.1] that every non-empty additive semigroup D of $\mathbb{N}$ is "eventually an arithmetic progression", i.e. there exist $N, d \in \mathbb{N}$ such that $D \cap [N,\infty) = (d\cdot\mathbb{N}) \cap [N,\infty)$. In order to decide $D := \mathrm{Dim}_\vartheta(f)$, it thus suffices to test whether d divides x in case $x \ge N$: This can be performed in $\mathcal{NC}^1$ [CDL01]. The answers to the finitely many cases $x < N$ can be precomputed and take only constant time. ■

IV. CONCLUSION

We have characterized (Turing-) $\mathcal{NP}$ as the class of problems reducible to weak (equivalently: strong) satisfiability over $\mathbb{R}^2$ (equivalently: over $\mathbb{C}^2$); and the BSS complexity class $\mathcal{NP}_\mathbb{R}$ as those reducible to weak (equivalently: strong) satisfiability with constants over $\mathbb{R}^3$ (equivalently: over $\mathbb{C}^3$). These results extend to the polynomial hierarchy for Turing and BSS machines [CuBr07], by considering the following semantics:

Definition 30: a) Let $f(\vec{X}_1, \ldots, \vec{X}_k)$ denote a formula in $n_1 + \cdots + n_k$ variables. Then the expression

$$\exists \vec{X}_1 \ \forall \vec{X}_2 \ \exists \vec{X}_3 \ \ldots \ \mathrm{Q}_k \vec{X}_k : \quad f(\vec{X}_1, \ldots, \vec{X}_k)$$

is called a Σ_k-formula, where Q_k denotes "$\forall$" for k even and "$\exists$" in case k is odd.
Similarly, a Π_k-formula starts with a universal quantifier followed by $k-1$ alternating quantifiers.

b) This Σ_k-formula is `true` (strongly valid) over $\mathbb{F}^d$ if there exists $\vec{X}_1 \in \mathrm{Gr}(\mathbb{F}^d)$ such that for each $\vec{X}_2 \in \mathrm{Gr}(\mathbb{F}^d)$ there exists $\cdots$ such that $f(\vec{X}_1, \ldots, \vec{X}_k) = 1$. Similarly for Π_k formulas and for weak validity.

c) A Σ_k-formula is strongly/weakly valid over $\mathbb{F}^*$ if it is over $\mathbb{F}^d$ for *some* $d \in \mathbb{N}$.
A Π_k-formula is strongly/weakly valid over $\mathbb{F}^*$ if it is over $\mathbb{F}^d$ for *every* $d \in \mathbb{N}$.

Note that the negation of a weakly valid Σ_k formula is a strongly valid Π_k formula; and the negation of a weakly valid Π_k formula is a strongly valid Σ_k formula.

REFERENCES

[ABKM09] E. ALLENDER, P. BÜRGISSER, J. KELDGAARD-PEDERSEN, P. MILTERSEN: "On the Complexity of Numerical Analysis", pp.1987–2006 in *SIAM J. Comput.* vol.**38:5** (2009).

[BCNM06] O. BOURNEZ, F. CUCKER, P.J. DE NAUROIS, J.-Y. MARION: "Implicit complexity over an arbitrary structure: Quantifier alternations", pp.210–230 in *Information and Computation* vol.**204:2** (2006).

[BCSS98] L. Blum, F. Cucker, M. Shub, S. Smale: "*Complexity and Real Computation*", Springer (1998).

[BeCa81] E.G. Beltrametti, G. Cassinelle: "*The Logic of Quantum Mechanics*", vol.**15** in (G.-C. Rota, Editor) the Encyclopedia of Mathematics and Its Applications, Addison-Wesley (1981).

[Bem85] L. Beran: "*Orthomodular Lattices*", Springer (1985).

[BiVN36] G. Birkhoff, J. Von Neumann: "The Logic of Quantum Mechanics", pp.823–843 in *Annals of Mathematics* vol.**37:4** (1936).

[BL*99] A. Bjorner, M. Las Vergnas, B. Sturmfels, N. White, G.M. Ziegler: "*Oriented matroids*" (2nd Edition), Encyclopedia of Mathematics and Applications, Cambridge University Press (1999).

[BPR03] S. Basu, R. Pollack, M.-F. Roy: "*Algorithms in Real Algebraic Geometry*", Springer (2003).

[BSS89] L. Blum, M. Shub, S. Smale: "On a Theory of Computation and Complexity over the Real Numbers: $\mathcal{NP}$-Completeness, Recursive Functions, and Universal Machines", pp.1–46 in *Bulletin of the American Mathematical Society* (AMS Bulletin) vol.**21** (1989).

[BuCu06] P. Bürgisser, F. Cucker: "Counting Complexity Classes for Numeric Computations II: Algebraic and Semialgebraic Sets", pp.147–191 in *Journal of Complexity* vol.**22:2** (2006).

[Can88] J. Canny: "Some Algebraic and Geometric Computations in PSPACE", pp.460–467 in *Proc. 20th annual ACM Symposium on Theory of Computing* (SToC 1988).

[CDL01] A. Chiu, G.I. Davida, B.E. Litow: "Division in logspace-uniform $\mathcal{NC}^1$", pp.259–275 in *Informatique Théoretique et Applications* vol.**35:3** (2001).

[CMW00] B. Coecke, D. Moore, A. Wilce (Editors): "Current research in operational quantum logic", vol.**111** in Series *Fundamental Theories of Physics*, Springer (2000).

[CuBe07] F. Cucker, I. Bezuel: "A Note on Parallel and Alternating Time", pp.594–602 in *Journal of Complexity* vol.**23** (2007).

[Cuck93] F. Cucker: "On the Complexity of Quantifier Elimination: the Structural Approach", pp.400–408 in *The Computer Journal* vol.**36:5** (1993).

[CuRo92] F. Cucker, F. Rosselló: "On the Complexity of Some Problems for the Blum, Shub & Smale model", pp.117–129 in *Proc. LATIN'92*, Springer LNCS vol.**583**.

[DHMW05] J.M. Dunn, T.J. Hagge, L.S. Moss, Z. Wang: "Quantum Logic as Motivated by Quantum Computing", pp.353–359 in *Journal of Symbolic Logic* vol.**70:2** (2005).

[EGLD7] K. Engesser, D.M. Gabbay, D. Lehmann (Editors): "*Handbook of Quantum Logic and Quantum Structures*", Elsevier (2007).

[FoKo98] H. Fournier, P. Koiran: "Are Lower Bounds Easier over the Reals?", pp.507–513 in *Proc. 13th Annual ACM Symposium on Theory of Computing* (SToC'98).

[FoKo00] H. Fournier, P. Koiran: "Lower Bounds Are Not Easier over the Reals", pp.832–843 in *Proc. 27th International Colloquium on Automata, Languages and Programming* (ICALP 2000), Springer LNCS vol.**1853**.

[GoOR04] J.E. Goodman, J. O'Rourke (Editors): "*Handbook of Discrete and Computational Geometry*", Chapman & Hall (2004).

[Grig88] D.Y. Grigoriev: "Complexity of Deciding Tarski Algebra", pp.65–108 in *Journal of Symbolic Computation* vol.**5** (1988).

[Gril01] P.A. Grillet: *Commutative Semigroups*, Kluwer (2001).

[Hagg07] T.J. Hagge: "$QL(\mathbb{C}^n)$ Determines n", pp.1194–1196 in *Journal of Symbolic Logic* vol.**72:4** (2007).

[Hagg09] T.J. Hagge: "Quantum logic on finite dimensional Hilbert spaces", presentation at the *Workshop on Quantum Logic Inspired by Quantum Computation* (M. Dunn, L. Moss, Z. Wang organisers), Indiana University, May 2009; `www.indiana.edu/~iulg/qlqc/hagge_qliqc_talk.pdf`

[Herr84] C. Herrmann: "On the Arithmetic of Projective Coordinate Systems", pp.759–785 in *Transactions of the American Mathematical Society* vol.**284:2** (1994).

[Herr87] C. Herrmann: "The free orthomodular word problem is solved" (review of the paper by G. Kalmbach), in *Zentralblatt für Mathematik* **Zbl 0585.06004** and *Mathematical Reviews* **MR 87K:06023** (1987).

[Herr09] C. Herrmann: "Complemented Modular Lattices with Involution and Orthogonal Geometry", pp.339–364 in *Algebra Universalis* vol.**61** (2009).

[Herr10] C. Herrmann: "On the equational theory of projection lattices of finite von-Neumann factors", pp.1102–1110 in *J. Symbolic Logic* vol.**75:2** (2010).

[HKW97] M. Haviar, P. Konôpka, C.B. Wegener: "Finitely Generated Free Modular Ortholattices II", pp.2661–2679 in *International Journal of Theoretical Physics* vol.**36:12** (1997).

[HRS90] J. Heintz, M.-F. Roy, P. Solernó: "Sur la complexité du principe de Tarski–Seidenberg", pp.101–126 in *Bull. Soc. Math. France* vol.**118** (1990).

[Jack06] J.D. Jackson: "*Mathematics for Quantum Mechanics: An Introductory Survey of Operators, Eigenvalues, and Linear Vector Spaces*", Dover (2006).

[Kalm83] G. Kalmbach: "*Orthomodular Lattices*", Academic Pr. (1983)

[Koir96] P. Koiran: "Hilbert's Nullstellensatz is in the Polynomial Hierarchy", pp.273–286 in *Journal of Complexity* vol.**12:4** (1996).

[Koir99] P. Koiran: "The Real Dimension Problem is $\mathcal{NP}_{\mathbb{R}}$-complete", pp.227–238 in *J. Complexity* vol.**15:2** (1999).

[Mack63] G.W. Mackey: "Mathematical Foundations of Quantum Mechanics", *Mathematical Physics Monograph Series* (1963).

[MaMe82] E.W. Mayr, A.R. Meyer: "The Complexity of Word Problems for Commutative Semigroups and Polynomial Ideals", pp.305–329 in *Advances in Mathematics* vol.**46** (1982).

[Marx07] M. Marx: "Complexity of Modal Logic", pp.139–179 in (P. Blackburn, J.v. Benthem, F. Wolter, Editors) *Handbook of Modal Logic* (2007).

[Mati70] Y.V. Matiyasevich: "Enumerable Sets are Diophantine", pp.354–357 in *Soviet Math.Dokl.* vol.**11** (1970).

[MaTo97] G. Matera, J.M.T. Turull Torres: "The Space Complexity of Elimination Theory: Upper Bounds", pp.267–276 in *Selected Papers of a Conference on Foundations of Computational Mathematics*, Springer (1997).

[Maye07] R. Mayet: "Equations Holding in Hilbert Spaces", pp.1257–1287 in *International Journal of Theoretical Physics* vol.**45:7** (2007).

[Megi09] N.D. Megill: "Quantum Logic Explorer Home Page" at *Metamath*; `http://us.metamath.org/qlegif/mmql.html` (2009).

[MeMi97] K. Meer, C. Michaux: "A Survey on Real Structural Complexity Theory", pp.113–148 in *Bulletin of the Belgian Mathematical Society* vol.**4** (1997).

[MnZi93] N.E. Mnëv, G.M. Ziegler: "Combinatorial Models for the Finite-dimensional Grassmannians", pp.241–250 in *Discrete & Computational Geometry* vol.**3:10**, Springer (1993).

[Neum55] J.von Neumann: "*Mathematical Foundations of Quantum Mechanics*", Princeton (1955).

[Piro64] C. Piron: "Axiomatique Quantique", pp.439–468 in *Helv. Phys. Acta* vol.**37** (1964).

[PM07a] M. Pavičić, N.D. Megill: "Quantum Logic and Quantum Computation", pp.755–792 in [EGLD7].

[Poon09] B. Poonen: "Characterizing Integers among Rational Numbers with a Universal-Existential Formula", in *American Journal of Mathematics* vol.**131:3** (2009).

[Pyka00] J. Pykacz: "Quantum Logic as a Basis for Computations", pp.839–850 in *International Journal of Theoretical Physics* vol.**39:3** (2000).

[Ren92a] J. Renegar: "Recent Progress on the Complexity of the Decision Problem for the Reals", pp.287–308 in *Discrete and Computational Geometry: Papers from the DIMACS Special Year* (J.E. Goodman, R. Pollack, W .Steiger Editors), American Mathematical Society vol.**6** (1992).

[Ren92b] J. Renegar: "On the Computational Complexity and Geometry of the First-order Theory of the Reals", pp.255–352 in *Journal of Symbolic Computation* vol.**13:3** (1992).

[Rodd89] M.S. Roddy: "On the word problem for orthocomplemented modular lattices", pp.961–1004 in *Canadian Journal of Mathematics* vol.**37** (1989).

[Sma98] S. Smale: "Mathematical Problems for the Next Century", pp.7–15 in *Math. Intelligencer* vol.**20:2** (1998).

[Ying05] M. Ying: "A Theory of Computation based on Quantum Logic I", pp.134–207 in *Theoretical Computer Science* vol.**344** (2005).