Progress on the Computability, Complexity, and Expressiveness of Geometric Quantum Logic

Christian Herrmann[a] and Yasuyuki Tsukamoto[a,b] and Martin Ziegler[a]
a) TU Darmstadt (GERMANY) b) Kyoto University (JAPAN)

***Abstract*—This work picks up on previous research about the computability and complexity of geometric quantum logic.**
First we show that strong satisfiability in *in*definite finite dimension $\exists d \in \mathbb{N}\ \exists \bar{x} = (x_1, \ldots, x_n) \in L(\mathbb{C}^d)^n : t(\bar{x}) = \mathbf{1}$ is undecidable.
Second we construct a single term t admitting weakly satisfying assignments $\bar{x} \in L(\mathbb{C}^d)^n : t(\bar{x}) \neq \mathbf{0}$ for all $d \geq 3$, but for none with *rational* $\bar{x}$. Weak satisfiability in indefinite dimension, a decision problem known to belong to the Blum-Shub-Smale complexity class $\mathcal{BP}(\mathsf{NP}^0_{\mathbb{R}})$, thus could exceed NP.
Third we show that, for fixed d, first-order definability within $L(\mathbb{F}^d)$ corresponds, via representing matrices viewed as arrays of elements of $\mathbb{F}$, to definability over $\mathbb{F}$ invariant under unitary transformation; and we apply this to derive that fixed-dimensional first-order quantum logic is 'model-complete' in the sense of admitting quantifier elimination up to one final existential/universal block (but not further in general).

I. Introduction

s:Intro

The properties of a quantum system correspond to self-adjoint operators on a complex Hilbert space $\mathcal{H}$ with spectrum $\{0,1\}$; equivalently: to closed subspaces $V \in L(\mathcal{H})$ of $\mathcal{H}$. Quantum logic captures this propositional structure [BiVN36,Neum55,Mack63,Piro64,BeCa81] by equipping $L(\mathcal{H})$ with the connectives *meet* $\wedge : (U,V) \mapsto U \cap V$, *join* $\vee : (U,V) \mapsto \overline{U+V}$, and *complement* $\neg : U \mapsto U^{\perp}$ with neutral elements $\mathbf{0} = \{\vec{0}\}$ and $\mathbf{1} = \mathcal{H}$. The language of Boolean logic thus coincides with that of ortholattices; their semantics agree in case $\dim(\mathcal{H}) = 1$, but $L(\mathbb{C}^d)$ violates distributivity for $d \geq 2$. In fact the set

$$\mathrm{sat}_{\mathcal{H}} := \big\{ t(x_1,\ldots,x_n) \;\big|\; n \in \mathbb{N} = \{1,2,\ldots\}, \exists V_1,\ldots,V_n \in L(\mathcal{H}) :\ t(V_1,\ldots,V_n) \neq \mathbf{0} \big\}$$

of terms weakly satisfiable over $L(\mathcal{H})$ has been shown to characterize the dimension of $\mathcal{H}$ [DHMW05,Hagg07]. Note that weak truth has the *disjunction property* but strong truth does not (and vice versa for conjunction `&&`); in `Java`–notation:

$$x \vee y \neq \mathbf{0} \;\Leftrightarrow\; x \neq \mathbf{0} \,||\, y \neq \mathbf{0}, \quad x \vee y = \mathbf{1} \;\not\Rightarrow\; x = \mathbf{1} \,||\, y = \mathbf{1}$$

For further background about (not necessarily geometric, i.e. Hilbert Space-based) quantum logic see for example [Svoz98,CMW00,AbCo08,Megi09]. Regarding the connection of quantum logic to computation we refer for instance to [Pyka00,Ying05,Bub07,PM07a]. Quantum satisfiability can also be regarded as theorem proving in Synthetic Geometry [BoSt89].

A. Previous Results

For every fixed $d \geq 2$ we have established [HeZi11, Theorem 14] the decision problem $\mathrm{sat}_{\mathbb{C}^d}$ (different from, but) polynomial-time equivalent to strong satisfiability

$$\mathrm{SAT}_{\mathbb{C}^d} := \big\{ t \;\big|\; \exists V_1,\ldots V_n \in L(\mathbb{C}^d) :\ t(V_1,\ldots,V_n) = \mathbf{1} \big\}\ ,$$

NP–complete in dimension two [HeZi11, §II.A], and from dimension three on complete for $\mathcal{BP}(\mathsf{NP}^0_{\mathbb{R}})$: a natural complexity class between NP and PSPACE [Ren92a] with several equivalent characterizations [Shor91,Koir99,Rich99,Scha10,HSZ13]; note the real subscript in spite of the inner product space being complex. Also, Hilbert's open Tenth Problem over the rationals [Poon08] is equivalent to both $\mathrm{sat}_{\mathbb{Q}^d}$ and $\mathrm{SAT}_{\mathbb{Q}^d}$ [HeZi11, Proposition 18e]. Towards the infinite-dimensional case [Herr87b,Rodd89,HyNa05] we considered the weak and the following strong satisfiability problems in *in*definite finite dimension over a subfield $\mathbb{F} \subseteq \mathbb{C}$ closed under conjugation (and considered as a $*$-*ring* with this involution) and the induced inner product spaces $\mathbb{F}^d$ with canonical scalar product, namely $\mathrm{SAT}_{\mathbb{F}^*} :=$

$$\big\{ t \;\big|\; \exists d \in \mathbb{N},\ \exists V_1,\ldots,V_n \in L(\mathbb{F}^d) :\ t(V_1,\ldots,V_n) = \mathbb{F}^d \big\}\ ,$$
$$\big\{ t \;\big|\; \exists d \in \mathbb{N},\ \exists V_1,\ldots,V_n \in L(\mathbb{F}^d) :\ t(V_1,\ldots,V_n) \neq \{0\} \big\}$$

$=: \mathrm{sat}_{\mathbb{F}^*}$. We could prove $\mathrm{SAT}_{\mathbb{C}^*} = \mathrm{SAT}_{\mathbb{R}^*} = \mathrm{SAT}_{\mathbb{A}^*}$ [HeZi11, Proposition 21] hard for $\mathcal{BP}(\mathsf{NP}^0_{\mathbb{R}})$ [HeZi11, Theorem 26] but no upper complexity bound; and we could prove $\mathrm{sat}_{\mathbb{C}^*} = \mathrm{sat}_{\mathbb{R}^*} = \mathrm{sat}_{\mathbb{A}^*} \in \mathcal{BP}(\mathsf{NP}^0_{\mathbb{R}})$ [HeZi11, Theorem 25] but no lower complexity bound. Here $\mathbb{A}$ denotes the set of algebraic reals. We have also introduced (and elsewhere investigated the computational complexity of) first-order quantum logic over $L(\mathbb{C}^d)$ for fixed d.

In the terminology of algorithmic problems in universal algebra [KhSa95, §2.10], weak satisfiability $\mathrm{sat}_{\mathbb{F}^*}$ amounts to (the complement of) the decision problem of the *equational theory* for the class $\big\{L(\mathbb{F}^d) : d \in \mathbb{N}\big\}$. The decision problem for the *quasi equational theory* or *uniform word problem* for a class $\mathcal{C}$ of structures of fixed signature asks whether a given formula

$$t_1 = s_1 \ \&\&\ t_2 = s_2 \ \&\& \ldots \&\&\ t_k = s_k \quad \rightarrow \quad t = s \qquad (1)$$

holds over all structures in $\mathcal{C}$. The *restricted word problem* is non-uniform in taking k and $t_1, s_1, \ldots, t_k, s_k$ to be arbitrary but fixed with merely t, s as input. Strong satisfiability $\mathrm{SAT}_{\mathbb{F}^*}$ on the other hand amounts to (the complement of) formulae

"$t = \mathbf{1} \to t = \mathbf{0}$" over $\{L(\mathbb{F}^d) : d \in \mathbb{N}\}$. Note that the singleton or trivial ortholattice $L(\mathbb{F}^0)$ strongly satisfies every equation; $\mathrm{SAT}_{\mathbb{F}^*}$ is thus the complement of the *triviality problem* for the class $\mathcal{C} = \{L(\mathbb{F}^d) : d = 0, 1, 2, \dots\}$.

Unsolvability of the restricted word problem for classes of modular lattices (i.e. without orthocomplement) has been shown by Hutchinson [Hutc77] and Lipshitz [Lips74]. The latter observed that von Neumann's frames and coordinatization method allow to reduce the restricted word problem for a semigroup S to that for a presentation embedding into the subspace lattice $L(\mathbb{F}[S])$ of the semigroup algebra $\mathbb{F}[S]$ over any field $\mathbb{F}$ [Lips74, THEOREM 3.2]; and from Gurevich's undecidability of the restricted word problem for finite semigroups [Gure66], [Lips74, THEOREM 3.6] derived the undecidability of the restricted word problem for any class containing the subspace lattices of the $\mathbb{F}^d$ (any fixed $\mathbb{F}$) as reducts. [GuLe84] has established the recursive inseparability of the uniform word problem for in/finite semigroups with zero and syntactically restricted conclusion $t = 0$, that is, the following important and highly non-trivial

f:GL

Fact 1 (Gurevich&Lewis 1984): Let $\mathcal{S}_0$ denote the class of all semigroups with zero, considered as a constant 0 included into the similarity type; and Λ the set of all conjunctions of equations in the language of $\mathcal{S}_0$, that is, each $\pi(\bar{x}) \in \Lambda$ has the form

$$r_1(\bar{x}) = s_1(\bar{x}) \;\&\&\; r_2(\bar{x}) = s_2(\bar{x}) \;\&\&\; \dots \;\&\&\; r_K(\bar{x}) = s_K(\bar{x})$$

with $K \in \mathbb{N}$ and r_k, s_k products of certain variables x_j, including a distinguished variable x_0, and constant zero 0. Then no recursive subset of Λ can separate $\Lambda_0 := \{\pi(\bar{x}) | \mathcal{S}_0 \models \forall \bar{x}\, (\pi(\bar{x}) \Rightarrow x_0 = 0)\}$ from

$$\{\pi(\bar{x}) \mid S \models \exists \bar{x}\, (\pi(\bar{x}) \;\&\&\; x_0 \neq 0) \text{ for some } \textit{finite } S \in \mathcal{S}_0\}$$

$=: \Lambda_1$. ■

Recall that a recursive separation of disjoint sets A, B is a recursive $C \supseteq A$ with $C \cap B = \emptyset$.

B. Overview and New Results

The present contribution picks up on the aforementioned work [HeZi11]. In Section II, strong satisfiability in indefinite dimension is shown undecidable, via its complement, the triviality problem. Section III approaches the computational complexity of weak satisfiability in indefinite dimension: We exhibit a term weakly satisfiable over $L(\mathbb{R}^3)$ but not over $L(\mathbb{Q}^d)$ for any d, thus supporting evidence that the decision problem may have complexity exceeding NP (although we still cannot prove hardness). Section V finally approaches the expressiveness of first-order quantum logic: We establish that $L(\mathbb{C}^d)$ and $L(\mathbb{R}^d)$ 'almost' permit quantifier elimination, namely, every first-order formula with free variables) can be translated computationally into an equivalent one which is an identity $t = \mathbf{1}$ preceded by a block of existential (equivalently: only universal) quantifiers. This is based on establishing, in Section IV, the equivalence of definability in $L(\mathbb{F}^d)$ with definability, invariant under unitary transformation, in $\mathbb{F}$.

Some of our results extend to quantum logics derived from orthosymmetric sesquilinear spaces other than the canonical $\mathbb{F}^d$ contained in $\mathbb{C}^d$ and $\mathbb{R}^d$, see Section VI. Though, for ease of exposition we focus mainly on subfields $\mathbb{F}$ of $\mathbb{C}$ closed under, and endowed with, conjugation as ring involution, the spaces $\mathbb{F}^d$ with canonical scalar product, and subspaces of such. The latter are still *inner product spaces* over $\mathbb{F}$: $\mathbb{F}$–vector spaces with an anisotropic Hermitean form. To wit, for $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ any d-dimensional inner product space is isometrically isomorphic to $\mathbb{F}^d$. This is not longer the case e.g. for $\mathbb{F} = \mathbb{Q}$. The good news is: orthogonal bases always exist.

Our methods heavily employ coordination techniques for lattices developed by von Neumann [Neum60]. Theorem 2 moreover essentially builds on the aforementioned Fact 1 and requires to consider the *bounded lattice* $\mathsf{Sub}(V)$ of all subspaces of a vector space V, endowed with meet $\cap$, join $+$, and bounds $0, V$. Direct sums $U + W$ in $\mathsf{Sub}(V)$, i.e. for $U \cap W = 0$, are written as $U \oplus W$. We use this notation, familiar from Linear Algebra, also in relevant terms, in order to avoid confusion with the operations $\wedge$ and $\vee$ of Grassmann-Cayley algebra,

II. STRONG SATISFIABILITY IN INDEFINITE DIMENSION

s:Strong

We now answer the question left open in [HeZi11, §IV.C] and establish undecidability of strong quantum satisfiability in indefinite finite dimension — in fact independently of the underlying field:

t:Strong

Theorem 2:
a) There is no algorithm deciding for any given conjunction of equations in the language of rings with unit whether there exists some $d > 0$ and a satisfying assignment in $\mathbb{F}^{d\times d}$.
b) The following problem about matrix equations is undecidable: Given quadratic polynomials $p_1(X_1, \dots X_n)$, $\dots$, $p_K(X_1, \dots X_n)$ in n non-commuting variables with coefficients $\{-1, 0, 1\}$, do there exist $d \in \mathbb{N}$ and $A_1, \dots A_n \in \mathbb{F}^{d\times d}$ such that $p_k(A_1, \dots A_n) = 0$ for every $1 \leq k \leq K$ simultaneously?
c) The following problem is undecidable, where $A^\dagger$ denotes the adjoint (transposed conjugate) matrix:
Given a single quartic polynomial $p(X_1, \dots X_n, Y_1, \dots Y_n)$ in $2n$ non-commuting variables with coefficients $\{-2, -1, 0, 1, 2\}$, do there exist $d \in \mathbb{N}$ and $A_1, \dots A_n \in \mathbb{F}^{d\times d}$ such that $p(A_1, \dots A_n, A_1^\dagger, \dots A_n^\dagger) = 0$?
d) There exists a sequence $p_n(X_1, \dots, X_n, Y_1, \dots, Y_n)$ of quartic polynomials in $2n$ non-commuting variables with coefficients $\{-2, -1, 0, 1, 2\}$ and $A_1, \dots, A_n \in \mathbb{C}^{d(n)\times d(n)}$ for some, but for no recursively bounded, $d : \mathbb{N} \to \mathbb{N}$ such that $p_n(A_1, \dots, A_n, A_1^\dagger, \dots, A_n^\dagger) = 0$.
e) There is no algorithm deciding for any given conjunction $s = \mathbf{0}$ && $t = \mathbf{1}$ of equations in the language of bounded lattices (i.e. without orthocomplement), whether there exists some $d > 0$ and a satisfying assignment in $\mathsf{Sub}(\mathbb{F}^d)$.
f) $\mathrm{SAT}_{\mathbb{F}^*}$ is not recursive.

g) There exists a recursive sequence t_m of ortholattice terms of binary length $|t_m| = m$ that are strongly satisfiable over $L(\mathbb{C}^{d(m)})$ for some, but for no recursively bounded, function $d : \mathbb{N} \to \mathbb{N}$.

In a), b), c), and e), $\mathbb{F}$ may vary with d.

The first four items indicate fundamental limitations of computational approaches to polynomial identities of matrices [BDDK03].

Proof: We defer Items a) and e) to separate subsections and prove the rest in different order:

f) Follows from e) with $t \wedge \neg s$.

g) Since there are only finitely (exponentially) many t of given length m, $d_{\mathbb{F}}(m) :=$

$$\max\left\{ \min\{d > 0 \mid t \in \mathrm{SAT}_{\mathbb{F}^d}\} \;\middle|\; t \in \mathrm{SAT}_{\mathbb{F}^*},\ |t| \leq m\right\}$$

defines a total $d_{\mathbb{F}} : \mathbb{N} \to \mathbb{N}$. Recall that $\mathrm{SAT}_{\mathbb{C}^\delta}$ is decidable by means of Tarski's Quantifier Elimination over the reals uniformly in δ, yielding recursive enumerability of $\mathrm{SAT}_{\mathbb{C}^*}$; cmp. [DHMW05, §3] or [HeZi11, PROPOSITION 21]. Now if $d_{\mathbb{C}}$ were to admit some recursive upper bound $d : \mathbb{N} \to \mathbb{N}$, an algorithm could decide $\mathrm{SAT}_{\mathbb{C}^*}$ by checking whether $t \in \mathrm{SAT}_{\mathbb{C}^\delta}$ for $\delta = 1, \ldots, d(|t|)$ — contradicting b). Finally let $(s_m)_m$ denote a recursive enumeration of $\mathrm{SAT}_{\mathbb{C}^*}$ and apply some bi-recursive padding $s \mapsto t := s \wedge \bigwedge_n y_n$ with dummy variables y_n to achieve $|t_m| = m$.

d) follows similarly from c).

b) follows from a) and the fact that, within rings with unit, any term is equivalent ti such polybomial.

c) follows from b) replacing the family $p_1, \ldots, p_n$ of polynomials with the single $\sum_{i=1}^n p_i \cdot p_i^\dagger$. ■

A. Proof of Theorem 2a)

ss:stronga

The goal is encode the semigroup formulas of the Theorem of Gurevich and Lewis into the language of rings with unit. The strength of their inseparabilty result allows to do with a weak version of encoding.

For $\pi(\bar{x}) \in \Lambda$ let $\pi^\#(\bar{x})$ the conjunction of $\pi(\bar{x})$, in the language of rings with unit, and $\sigma(x_0, \bar{y})$ given as $y_1x_0y_2 + y_3x_0y_4 = 1$.

triv

Lemma 3: Given $\pi(\bar{x}) \in \Lambda_1$ there is no satisfying assignment of $\pi^\#$ in any $\mathbb{F}^{d\times d}$, $d > 0$.

Proof: Indeed, having such, x_0 takes values 0 and it follows $0 = 1$. ■

fin

Lemma 4: For any finite $S \in \mathcal{S}_0$ and $r_0 \in S$ there is $d > 0$ and an embedding $\varepsilon : S \to \mathbb{F}^{d\times d}$ such that $\mathbb{F}^{d\times d} \models \exists \bar{y}.\ \sigma(\varepsilon(r_0), \bar{y})$. In particular, for any $\pi(\bar{x}) \in \Lambda_0$ and $\mathbb{F}$, there is a satisfying assignment for $\pi^\#$ in $\mathbb{F}^{d\times d}$ for some $d > 0$.

Proof: Adding new neutral elements step by step (of course, in this process the old neutral element looses its distinction) we may extend S to finite $S' \in \mathcal{S}_0$ such that $r_0h = hr_0 = r_0$ for more than half of the elements in S'. Now, let V the $\mathbb{F}$-vector space with basis $B = S' \setminus \{0\}$ and define $\beta(a)(b) = ab$ for $a, b \in B$ and $0b = b$ for all $b \in B$. This defines an embedding of S' into $\mathsf{End}(V)$ such that $\beta(r_0)$ has rank $m \geq \frac{d}{2}$, $d = \dim V$. Chosing a basis of V, we get an isomorphism $\mathsf{End}(V) \to \mathbb{F}^{d\times d}$, whence an embedding $\varepsilon : S \to \mathbb{F}^{d\times d}$ such that $A_0 = \varepsilon(r_0)$ has rank $m \geq \frac{d}{2}$. In view of Gaussian transformation on left and on the right, there are matrices B_1, B_2 such that $B_1A_0B_2 = \begin{pmatrix} I_m & O \\ O & O \end{pmatrix}$. where I_k denotes the $k \times k$-unit matrix. Now, to obtain $B_1A_0B_2 + B_3A_0B_4 = I_d$, choose

$$B_3 = \begin{pmatrix} O & O & O \\ O & O & O \\ I_{d-m} & O & O \end{pmatrix},\quad B_4 = \begin{pmatrix} O & O & I_{d-m} \\ O & O & O \\ O & O & O \end{pmatrix}$$

■

Coming to the proof of Theorem 2a), let Σ denote the set of all conjunctions of equations in the language of rings with unit. Then the following two sets are recursively inseparable:

- Σ_1 consisting of all formulas in Σ admitting a satisfying assignment in $\mathbb{F}^{d\times d}$ only for $d = 0$.
- Σ_0 consisting of all formulas in Σ such that some $\mathbb{F}^{d\times d}$ with $d > 0$ admits a satisfying assignment.

Now, $\Psi(\pi) = \pi^\#$ defines a recursive map from Λ into Σ with recursive image and recursive inverse on $\Psi(\Lambda)$. By Lemma 3 one has $\Psi(\Lambda_1) \subseteq \Sigma_1$, by Lemma 4, $\Psi(\Lambda_0) \subseteq \Sigma_0$. Now, assume that there exists a Σ_2 recursively separating Σ_1 and Σ_0. Then $\Psi^{-1}(\Sigma_2 \cap \Psi(\Lambda))$ would recursively separate Λ_1 and Λ_0, contradicting Fact 1. ■

B. Proof of Theorem 2e)

ss:stronge

This relies on the well known intepretation of rings within modular lattices, due to von Neumann [Neum60], which is the first step in Coordinatization Theory, In the setting of lattices $\mathsf{Sub}(\mathbb{F}^d)$ it boils down to elementary Linear Algebra (cf. [Her10b]).

For any $\mathbb{F}$-vector space V, we say that $\bar{A} = (A_1, A_2, A_3, A_{12}, A_{13})$ in $\mathsf{Sub}(V)$ forms a 3-*frame* if $V = A_1 \oplus A_2 \oplus A_3$ and $A_{1j} \oplus A_1 = A_{1j} + A_j = A_1 + A_j$ for $j = 2, 3$. Then there are unique linear isomorphisms $\varepsilon_{j\bar{A}} : A_1 \to A_j$ such that $A_{1j} = \{\vec{v} - \varepsilon_{j\bar{A}}\vec{v} \mid \vec{v} \in A_1\}$, $j = 2, 3$. Observe that this concept of frame is equivalent to the von Neumann one; cf. [Herr84]. In the following, (i), (ii), and (iv) are obvious. For (iii) choose a linear isomorphism $f_1 : A_1 \to B_1$ and then the f_j, $j = 2, 3$ so that $\varepsilon_{j\bar{B}} \circ f_1 = f_j \circ \varepsilon_{j\bar{A}}$.

auto

Fact 5:

(i) If $\bar{A}$ is a 3-frame of $\mathsf{Sub}(\mathbb{F}^d)$ then $\mathsf{Sub}(\mathbb{F}^d) = 0$ if and only if $A_1 = 0$ if and only if $A_1 = A_{12}$.

(ii) Given $V \in \mathsf{Sub}(\mathbb{F}^d)$, there is 3-frame $\bar{A}$ such that $V = A_1$ if and only if $\dim V = \frac{d}{3}$.

(iii) Given 3-frames $\bar{A}, \bar{B}$ of $\mathsf{Sub}(\mathbb{F}^d)$ there is an automorphism of $\mathsf{Sub}(\mathbb{F}^d)$ mapping $\bar{A}$ onto $\bar{B}$.

(iv) Choose distinguished variables z_1, z_2, z_3 and z_{11}, z_{13}: shortly, $\bar{z}$. There is a conjunction $\Phi(\bar{z})$ of equations in the language of bounded lattices such that for any $\bar{A} \in L(\mathbb{F}^d)$ one has $\bar{A}$ a 3-frame of $\mathsf{Sub}(\mathbb{F}^d)$ if and only if $\mathsf{Sub}(\mathbb{F}^d) \models \Phi(\bar{A})$.

We define $R(\mathsf{Sub}(\mathbb{F}^d), \bar{A}) = \{U \in \mathsf{Sub}(\mathbb{F}^d) \mid U \oplus A_2 = A_1 + A_2\}$ and $\gamma_{\bar{A}}(\varphi) = \{\vec{v} - \varepsilon_{\bar{A}}\varphi\vec{v} \mid \vec{v} \in A_1\}$, the *negative graph* of the map $\varepsilon_{2A} \circ \varphi$ This yields a bijection

$\gamma_{\bar{A}} : \mathsf{End}(A_1) \to R(L(\mathbb{F}^d), \bar{A})$. The following is well known ([Neum60,Her10b]).

def

Fact 6: There is a conjunction $\sigma(x, \bar{z})$ of term equations and, for each fundamental operation $q(\bar{x})$ of rings with unit, a term $\hat{q}(\bar{x}, \bar{z})$ in the language of lattices such that the following are true for any 3-frame $\bar{A} \in L(\mathbb{F}^d)$. Moreover, in any of these terms each of the variables in $\bar{x}$ occurs exactly once.

(i) for any $U \in \mathsf{Sub}(\mathbb{F}^d)$ one has $U \in R(\mathsf{Sub}(\mathbb{F}^d), \bar{A})$ if and only if $\mathsf{Sub}(\mathbb{F}^d) \models \sigma(U, \bar{A})$.

(ii) $\gamma_{\bar{A}}$ is an isomorphism of $\mathsf{End}(A_1)$ onto $R(L(\mathbb{F}^d), \bar{A})$ endowed with the operations $\bar{x} \mapsto \hat{q}(\bar{x}, \bar{A})$. Here, the ring elements $0, 1$ are mapped onto A_1, A_{12}.

To follows that with any conjunction $\pi(\bar{x}) = \pi(x_1, \ldots, x_n)$ of equations in the language of rings with unit one can effectively associate a conjunction $\hat{\pi}(\bar{x}, \bar{z})$ of equations in the language of bounded lattices such that for any 3-frame $\bar{A}$ in $\mathsf{Sub}(\mathbb{F}^d)$ and any $\bar{U}$ in $\mathsf{Sub}(\mathbb{F}^d)$ one has that $\mathsf{Sub}(\mathbb{F}^d) \models \hat{\pi}(\bar{U}, \bar{A})$ if and only if $U_i \in R(\mathsf{Sub}(\mathbb{F}^d), \bar{A})$ for $i = 1, \ldots, n$ and $R(\mathsf{Sub}(\mathbb{F}^d), \bar{A}) \models \pi(\bar{U})$. Since $\mathsf{End}(A_1)$ is isomorphic to $\mathbb{F}^{m\times m}$, $m = \frac{d}{3}$, an algorithm deciding the problem in e) of Theorem 2 would yield one deciding the problem in a). ■

III. Weak Satisfiability in Indefinite Dimension

s:Weak

In contrast to Theorem 2b) for strong satisfiability, [HeZi11, Theorem 25] has shown that every term t weakly satisfiable in indefinite dimension is also weakly satisfiable in some dimension at most polynomial in t's binary length — and thus concluded $\mathrm{sat}_{\mathbb{C}^*} \in \mathcal{BP}(\mathsf{NP}^0_{\mathbb{R}})$: a complexity class which, as opposed to NP, is defined by polynomial-length witnesses of real, as opposed to bit, sequences which $\mathrm{sat}_{\mathbb{C}^3}$ is complete for. In particular to each polynomial $p \in \mathbb{Z}[X]$ there exists a term t_p that is weakly satisfiable over $L(\mathbb{F}^3)$ iff the field extension $\mathbb{F} \supseteq \mathbb{Q}$ contains some root of p [HeZi11, Lemma 20d]. That 2D quantum satisfiability belongs to NP [HeZi11, Theorem 8] therefore hinges on being able to restrict satisfying assignments to a discrete, finite, and small set. Regarding $\mathrm{sat}_{\mathbb{C}^*}$, although we still cannot prove $\mathcal{BP}(\mathsf{NP}^0_{\mathbb{R}})$–hardness (or even NP–hardness for that matter), the following result demonstrates that satisfying assignments as witnesses to weak satisfiability cannot be restricted, in general, to avoid irrational coefficients even in indefinite finite dimension.

t:Weak

Theorem 7: a) Let $p(X) \in \mathbb{Z}[X]$ have at least one real zero. There exists an ortholattice term t_p — computable from p in time polynomial in the binary length $|p|$ of p — such that, for all $\mathbb{F}$, one has $t_p \in \mathrm{sat}_{\mathbb{F}^*}$

(1) if and only if there are a subspace V of $\mathbb{F}^{3m}$, $m := \dim V \leq \deg p$, and a self-adjoint endomorphism ψ of V such that $p(\psi) = 0$.

(2) if and only if $\alpha \in \mathbb{F}$, provided that α is the unique real zero of $p(X)$ and $\mathbb{F} \subseteq \mathbb{R}$.

(3) if and only if, in case $\mathbb{F} = \mathbb{Q}$, there are $0 < m \leq \deg p$ and $A, D \in \mathbb{Q}^{m\times m}$, D diagonal with positive entries, such that $DA = A^t D$ and $p(A) = 0$.

b) In particular, for every $k \in \mathbb{N}$, $t_{X^{2k+1}-2}$ is weakly satisfiable over $L(\mathbb{R}^3)$ but not over $L(\mathbb{Q}^d)$ for any d.

c) In contrast, if $\mathbb{F}$ is the splitting field of finitely many quadratic $p(X) \in \mathbb{Z}[X]$, then $L(\mathbb{F}^d)$ embeds into $L(\mathbb{Q}^{nd})$ for some sufficiently large n and in particular it holds $\mathrm{sat}_{\mathbb{F}^*} = \mathrm{sat}_{\mathbb{Q}^*}$ and $\mathrm{SAT}_{\mathbb{F}^*} = \mathrm{SAT}_{\mathbb{Q}^*}$.

d) If term t is weakly satisfied by $X_1, \ldots, X_n \in L(\mathbb{F}^d)$, then so is it by $O(X_1 \times Y_1), \ldots, O(X_n \times Y_n) \in L(\mathbb{F}^{d+e})$ for arbitrary $Y_1, \ldots, Y_n \in L(\mathbb{F}^e)$ and every orthogonal/unitary $O \in \mathbb{F}^{(d+e)\times(d+e)}$. (Here we identify $\mathbb{F}^{d+e}$ with $\mathbb{F}^d \times \mathbb{F}^e$.)

Item c) generalizes [HeZi11, Proposition 21c]. Item d) formalizes that the choice of weakly satisfying assignments grows with increasing dimension.

Proof: We defer Items a) and c) to a separate subsections.

b) follows from a) since $\sqrt[2k+1]{2}$ is the unique real root of $p(X) := X^{2k+1} - 2$.

d) holds since $t(X_1 \times Y_1, \ldots, X_n \times Y_n) = t(X_1, \ldots, X_n) \times t(Y_1, \ldots, Y_n)$ and $t(U \cdot X_1, \ldots, U \cdot X_n) = U \cdot t(X_1, \ldots, X_n)$ for every unitary $U \in \mathbb{C}^{d\times d}$. ■

A. Proof of Theorem 7a)

t:Weaka

Having the equivalence of $t_p \in \mathrm{sat}_{\mathbb{F}}$ with (1), the other equivalences follow, readily.

Concerning (2) observe that for V and ψ as in (1), α is the unique real eigenvalue of ψ; since ψ is self-adjoint it follows $\psi = \alpha \cdot \mathsf{id}$ in the tensorial extension of V to an inner product space over the reals, whence also on V.

Concerning (3), necessity is, for all $\mathbb{F} \subseteq \mathbb{R}$, a consequence of the description of the adjoint in terms of an orthogonal basis. Sufficiency follows from the fact that for any finite dimensional inner product space (V, Φ) over the rationals there is, up to scaling, an isometric linear isomorphism onto some subspace of $\mathbb{Q}^d$ for some d: choosing an orthogonal basis $\vec{v}_i$ of (V, Φ), one may assume $\Phi(\vec{v}_i, \vec{v}_i) = n_i$ a positive integer; thus, let $d = \sum_i n_i$, and $k_{i+1} = k_i + n_i$ and map $\vec{v}_i$ onto $\sum_{k=k_{i-1}}^{k_i} \vec{e}_k$, where the $\vec{e}_k$ form the standard basis of $\mathbb{Q}^d$.

The proof concerning (1) relies on a method well known from undecidability results for equational theories cf. [Free80,Herr83]. References mostly concern the general case of modular (ortho)lattices; though, for subspace (ortho)lattices the relevant results may be verified within Linear Algebra, easily.

Given conjunctions $\pi(\bar{x})$ and $\rho(\bar{x})$ of (ortho)lattice equations, we say that a family $\bar{t}(\bar{x})$ of ortholattice terms $t_i(\bar{x})$ *forces* (the relations) ρ *under the proviso* π if for any $L(\mathbb{F}^d)$ and assignment $\bar{a}$ in $L(\mathbb{F}^d)$ satisfying $\pi(\bar{a})$ one has

(a) $\rho(\bar{t}(\bar{a}))$; i.e. assignment $\bar{a}$ satisfies in $L(\mathbb{F}^d)$ the relations $\rho(\bar{x})$

(b) $\bar{t}(\bar{a}) = \bar{a}$ if $\rho(\bar{a})$; that is, the assignment $\bar{a}$ remains unchanged under the term operations induced by $\bar{t}$, if it already satisfies the relations $\rho(\bar{x})$ within $L(\mathbb{F}^d)$.

If there are also terms forcing π under the proviso ρ, then π and ρ are (Tietze) *equivalent* (presentations).

Referring to Subsection II-B, a *sectional orthogonal* 3-*frame*, shortly $SO3$-frame, in $L(\mathbb{F}^d)$ is a (spanning) 3-frame $\bar{A}$ of some section $[0, U]$ of $L(\mathbb{F}^d)$ such that $A_i \perp A_j$ for all $i \neq j$.

Fact 8: There are ortholattice terms $a_i(\bar z), a_{1j}(\bar z)$, shortly $\bar a(\bar z)$, forcing $SO3$-frames.

This is due to [MaRo87] in an equivalent version of orthogonal frames. See [Free79, §1] for the following.

Fact 9: There are terms $\bar b(y_1, \bar z)$ forcing an $SO3$-frame $\bar B$ such that $B_{ij} \subseteq A_{ij}$ for all i, j under the proviso that $\bar A$ is an $SO3$-frame and $B_1 \subseteq A_1$.

For a subspace V of $\mathbb{F}^d$ let $\mathsf{End}^\dagger(V)$ the ring of all endomorphisms of V with *involution*, given by $\varphi \mapsto \varphi^\dagger$ (the adjoint of φ w.r.t. the induced inner product), as additional unary operation and with constant $\frac{1}{2}\mathsf{id}$. Recall $R(L(\mathbb{F}^d), \bar A)$ and $\gamma_{\bar A}$ from Subsection II-B. Observe that $A_1 \cap \gamma_{\bar A}(\varphi) = \ker \varphi$. Also, for a φ-invariant subspace $B_1 \subseteq A_1$ and $\bar B$ arising via Fact 9 one has $B_2 = \varepsilon_{\bar A}(A_1)$ and $\gamma_{\bar B}(\varphi|B_1) = \gamma_{\bar A}(\varphi) \cap (B_1 + B_2)$.

Fact 10: Fact 6(ii) extends to rings with involution and constant $\frac{1}{2}$.

Describing inverses has been done by von Neumann [Neum60], already. A term for the adjoint is in [HeRo99, Lemma 4.11].

Fact 11: For any $p(X) \in \mathbb{Z}[X]$ there is a lattice term $p_{\bar z}(x) := p(x, \bar z)$, of size polynomial in the size of p, such that for any $SO3$-frame $\bar A$ in any $L(\mathbb{F}^d)$ and any $\varphi \in \mathsf{End}^\dagger(A_1)$ one has $\gamma_{\bar A}(p(\varphi)) = p_{\bar A}(\gamma_{\bar A}(\varphi))$. Moreover, if B_1 is a φ-invariant subspace of A_1, $\psi = \varphi|B_1$, and if $\bar B$ arises from B_1 and $\bar A$ as in Fact 9 then $\gamma_{\bar B}(p(\psi)) = p_{\bar B}(\gamma_{\bar B}(\psi))$.

The first claim is immediate by Fact 10, considering $p(X)$ a term in the language of rings. For the second, first observe that, due to the fact that B_1 is φ- and $p(\varphi)$-invariant and $p(\varphi)|B_1 = p(\psi)$ one has $\gamma_{\bar B}(\psi) = \gamma_{\bar A}(\varphi) \cap (B_1 + B_2)$ and $\gamma_{\bar B}(p(\psi)) = \gamma_{\bar A}(p(\varphi)) \cap (B_1 + B_2)$. Since lattice polynomials are order preserving and $B_{ij} \subseteq A_{ij}$, it follows that $p_{\bar B}(\gamma_{\bar B}(\psi)) \subseteq p_{\bar A}(\gamma_{\bar A}(\varphi)) \cap (B_1 + B_2) = \gamma_{\bar B}(p(\psi))$. Equality follows since both are complements of B_2 in $[\mathbf{0}, B_1 + B_2]$.

Fact 12: There is an ortholattice term $s(x, \bar z)$ forcing for any $SO3$-frame $\bar A$ in any $L(\mathbb{F}^d)$ a $\gamma_{\bar A}(\varphi)$ with self-adjoint $\varphi \in \mathsf{End}^\dagger(A_1)$.

[HeRo99, Lemma 4.11] forces an element of $R(L(\mathbb{F}), \bar A)$; which is turned self-adjoint mimicking $\frac{1}{2}(X + X^\dagger)$

Summarizing, in view of Facts 8 and 12 we have ortholattice terms $\bar a(\bar z)$ and $s(x, \bar z)$ forcing an $SO3$-frame $\bar A$ and $\gamma_{\bar A}(\varphi)$ with self-adjoint $\varphi \in \mathsf{End}^\dagger(A_1)$. Now, with $\bar b$ from Fact 9 the terms $\bar c := \bar b(z_1 \cap p_{\bar z}(s(x, \bar z)))$ force, under this proviso, an $SO3$-frame $\bar B$ such that $B_1 = \mathsf{ker}(p_{\bar B}(\psi))$ (that is, $(p_{\bar B}(\psi) = \mathbf{0}$) with self-adjoint $\psi \in \mathsf{End}^\dagger(B_1)$. Indeed, we apply Fact 11 to $B_1 = \mathsf{ker}p(\varphi)$. Thus, if $B_1 \neq 0$, choose $\vec 0 \neq \vec v_1 \in B_1$ and V spanned by the $\psi^k \vec v_1$, $(0 \leq k < \deg p)$, to obtain ψ-invariant V of $\dim V \leq \deg p$, $\psi|V$ self-adjoint, and $p(\psi|V) = 0$. In view of this, define $t_p(x, \bar z) := c_1(x, \bar z)$.

Conversely, if V and ψ are given, let $A_1 = V$ and choose A_2, A_3 such that A_1, A_2, A_3 are pairwise orthogonal and of the same dimension. Choose linear isomorphisms $\varepsilon_i : A_1 \to A_i$, $i = 2, 3$, and put $A_{1i} = \{\vec v - \varepsilon_i \vec v \mid \vec v \in A_1\}$ to obtain an $SO3$-frame. Then $\bar z \mapsto \bar A$, $x \mapsto \gamma_{\bar A}(\psi)$ provides a weakly satisfying assignment for t_p - this is where property (b) of forcing terms is used.

Proof of Theorem 7c)

Recall that a ring R (with unit) is von Neumann regular if any of its principal right ideals is generated by an idempotent; then the principal right ideals form a sublattice $\overline{L}(R)$ of the lattice of all right ideals. In particular, the endomorphisms ring $R = \mathsf{End}(V)$ of a for d-dimensional $\mathbb{F}$-vector space V is von Neumann regular and one has $\overline{L}(R) \cong \mathsf{Sub}(V)$ via $\varphi R \mapsto \mathsf{im}\,\varphi$. Thus, $\mathbb{F}^{d\times d} \cong \mathsf{Sub}(\mathbb{F}^d)$.

A regular $*$-ring with involution $r \mapsto r^\dagger$ is *$*$-regular* if $rr^\dagger = 0$ only for $r = 0$; equivalently: if any principal right ideal is generated by a (unique) projection $e = e^2 = e^\dagger$. The lattice $\overline{L}(R)$ becomes an ortholattice $\overline{L}^*(R)$ under the orthocomplementation $eR \mapsto (1 - e)R$. Since any eR is uniquely determined by the projection e, $\overline{L}^*(S)$ is canonically isomorphic to the *projection ortholattice* $\overline{L}^*_p(R)$ of projections of R.

In particular, this applies to $R = \mathsf{End}^\dagger(V)$ for any finite dimensional inner product space and one has $\overline{L}^*(R)$ isomorphic to $L(V)$ via $\varphi R \mapsto \mathsf{im}\,\varphi$. Thus, $\mathbb{F}^{d\times d}$ is $*$-regular with $A \mapsto A^\dagger$, the conjugate transpose, and $L(\mathbb{F}^d)$ isomorphic to $\overline{L}^*(\mathbb{F}^{d\times d})$. Of course, we also have to consider $\mathbb{F}$ with involution $r \mapsto r^\dagger$.

Fact 13:
(i) $(\mathbb{F}^{d\times d})^{m\times m}$. is isomorphic to $\mathbb{F}^{dm\times dm}$.
(ii) If R, S are $*$-regular rings and if S embeds into R then $\overline{L}^*(S)$ embeds into $\overline{L}^*(R)$.
(iii) $\mathbb{F}(i)$ embeds into $\mathbb{F}^{2\times 2}$.
(iv) For any positive integer n, if $\sqrt{n} \in \mathbb{F}$ then $\mathbb{F}(\sqrt{n+1})$ embeds into $\mathbb{F}^{2\times 2}$.

(ii)–(iii) are well known (e.g. [Her10a, Proposition 3.1] for (ii)). In (iv) let $A = \begin{pmatrix} \sqrt{n} & 1 \\ 1 & -\sqrt{n} \end{pmatrix}$: Then $A^2 = (n+1)I$ and there is an embedding such that $\sqrt{n+1} \mapsto A$.

Now, observe that the splitting field $\mathbb{F}$ from c) is contained in any field $\mathbb{F}'$ containing i and all square roots required for solving the given quadratic equations. Adjoining these step by step to $\mathbb{Q}$, we get by (iii) and (iv) a sequence of embeddings of the form $\mathbb{K} \to \mathbb{K}^{2\times 2}$ which results by (i) into an embedding $\mathbb{F} \to \mathbb{F}' \to \mathbb{Q}^{m\times m}$ whence $\mathbb{F}^{d\times d} \to \mathbb{Q}^{md\times md}$. The claim in Item c) follows by Fact 13(ii). ■

IV. Characterizing definability in terms of coordinates

The following Theorem 14 will be the key to the proof of Theorem 19b), below, in case $d \geq 3$. It requires some comments on concepts and notations. In order to avoid undue complications and misunderstandings caused by messing up mathematical objects and their descriptions in terms of others, we will consider, for fixed $d \geq 3$ and $\mathbb{F}$ (recall that $\mathbb{F}$ is a subfield of $\mathbb{C}$, closed conjugation and considered as a $*$-ring with conjugation as involution) a fixed $\mathbb{F}$-vector space V endowed with an anisotropic Hermitean form and admitting at least one orthonormal basis. Ignoring relativity, the space we live in is a good example of such V (for $\mathbb{F} = \mathbb{R}$). Let R denote the $*$-ring of endomorphisms of V with adjunction w.r.t. the form of V as involtution and L the ortholattice of its (principal) right ideals.

Dealing with R and L as first-order structures we will use, henceforth, the usual lower case letter to denote elements and variables; in particular, frames will be denoted as $\bar{a}$. Also, be aware that "formula" is used in the sense of classical first order logic and that it should not be confused with terms in the language of ortholattices (which sometimes are called "sentential quantum logic formulas"). Though, if we consider the latter language, such terms s, t are used to build the atomic formulas $s = t$.

Now, fixing an orthonormal basis $\bar{v}$ of V one estabishes an isomorphism $V \to \mathbb{F}^d$. Also, R and L allow a matrix description and we are going to speak about the coefficients of the matrices in the language of $\mathbb{F}$. To avoid confusion, we will denote matrices by $\mathcal{A}$ and so, with the corresponding matrices $\mathcal{X}$ of variables. In particular, one has an isomorphism $\gamma_{\bar{a}} : \mathsf{R} \to \mathbb{F}^{d\times d}$ of rings with involution, $\mathcal{A} \mapsto \mathcal{A}^\dagger$, the conjugate transpose, in the $*$-ring $\mathbb{F}^{d\times d}$ of matrices. In thie setting, "basis transformation" is just a matter of commun sense with no complicated formulas to worry about. Moreover, $f\mathsf{R} \mapsto \mathsf{Span}\gamma_{\bar{a}} f$ is an isomorphism of L onto $L(\mathbb{F}^d)$.

The basic relation between L and R is given by $u = fR$. Given an orthonormal basis $\bar{v}$ of V, one includes $\mathbb{F}^{d\times d}$: $\rho_{\bar{v}}(u, \mathcal{A})$ if and only if f is the endomorphism defined by $\bar{\mathcal{A}}$ w.r.t. the basis $\bar{v}$ and $u = f\mathsf{R}$. This extends to n-tuples, component-wise, and will be written as $\rho_{\bar{v}}(\bar{u}, \bar{\mathcal{A}})$. Given formulas $\varphi(\bar{x})$ in ortholattice and $\psi(\bar{\mathcal{X}})$ in $\mathbb{F}$-language and an orthonormal basis $\bar{v}$ we define

$$\mathsf{Mod}^{\mathbb{F}}_{\bar{v}}(\varphi) = \{\bar{\mathcal{A}} \in (\mathbb{F}^{d\times d})^n \mid \exists \bar{u} \in \mathsf{L}^n.\ \rho_{\bar{v}}(\bar{u}, \bar{\mathcal{A}})\}$$

$$\mathsf{Mod}^{\mathsf{L}}_{\bar{v}}(\psi) = \{\bar{u} \in \mathsf{L}^n \mid \exists \bar{\mathcal{A}} \in (\mathbb{F}^{d\times d})^n.\ \rho_{\bar{v}}(\bar{u}, \bar{\mathcal{A}})\}$$

and $\mathsf{Mod}^{\mathbb{F}}$, respectively $\mathsf{Mod}^{\mathsf{L}}$, as the unions ranging over all $\bar{v}$. We use the same notation for relations defined by formulas, if both adhere the same first order language. No parameters are admitted, for the time being.

pro

Theorem 14: a) For any formula $\varphi(x_1, \ldots, x_n)$ in ortholattice language there is a formula $\psi(\bar{\mathcal{X}}_1, \ldots, \bar{\mathcal{X}}_n)$ in $\mathbb{F}$-language such that $\mathsf{Mod}^{\mathbb{F}}(\varphi) = \mathsf{Mod}^{\mathbb{F}}\psi)$ and the latter is invariant under unitary transformation.

b) For a first-order formula $\psi(\bar{\mathcal{X}})$ in the language of $\mathbb{F}$ the following are equivalent

(i) $\mathsf{Mod}^{\mathbb{F}}(\psi)$ is invariant under unitary transformations $\mathcal{A} \mapsto \mathcal{U}\mathcal{A}\mathcal{U}^\dagger$.

(ii) For some/any orthonormal basis $\bar{v}$ of V one has $\mathsf{Mod}^{\exists}_{\bar{v}}(\psi)$ closed under automorphisms of L

(iii) $\mathsf{Mod}^{\mathsf{L}}(\psi) = \mathsf{Mod}^{\mathbb{F}}(\varphi)$ for some first-order φ in the language of ortholattices.

Moreover, in (iii), if ψ is of the form $\exists \mathcal{Z}.\chi$ with quantifier-free χ then one can choose φ of the form $\exists \bar{y}\bar{z}\sigma$ with quantifier-free σ.

c) The analogous results hold for R based on the relation $\kappa_{\bar{v}}(f, \mathcal{A})$ iff and only if $\mathcal{A}$ is the matrix of f w.r.t. $\bar{v}$.

We include the $*$-rings R, a topic of its own interest, since the proof gives an easily accessible pattern for the case of L and since the result is used, there.

Concerning the proof, let us first mention the well known facts behind. The easy part is the same for L and R.

First, recall that $\mathsf{Sub}(R)$ is interpretable within R by positive primitive formulas. Indeed, observe that for any idempotents e, f in R one has $eR \subseteq fR \ \Leftrightarrow \ fe = e$. Thus, for any idempotents e, f, g $gR = eR + fR$ if and only if one has $ge = e$, $gf = f$, and $\exists r \exists s.\, g = er + fs$. Also, using the analogous formula for $R(1 - g) = R(1 - e) + R(1 - f)$ and the fact that the latter means $gR = eR \cap fR$ [Neum60, LEMMA II.2.3] one obtains $gR = eR \cap fR$ if and only if $eg = fg = g$ and $\exists r \exists s.\, (1 - g) = r(1 - e) + s(1 - f)$.

Thus, any orthonormal basis allows to express the operations of R in terms of $\mathbb{F}$ - with formulas invariant under unitary transformation. This proves a). In b), the equivalence of (i) and the two versions of (ii) comes from viewing basis transformations as transformations in the matrix space and the fact that the automorphisms of R resp. L are exactly those maps which are induced by isometries. (iii) implies (i) due to a).

The proof that (ii) implies (iii) is rather easy in the case of R but we will delay it until the relevant tools are discussed. In the case of L it builds on results from Coordinatization Theory: There it is shown that for any modular ortholattice L with fixed orthogonal d-frame $\bar{a}$, $d \geq 4$ (for $d = 3$ one has to require the Arguesian identity), there is a $*$-regular ring $R_{\bar{a}}$ and an isomorphism $\omega_{\bar{a}} : L \to \overline{L}^*(R_{\bar{a}})$. One approach is to choose $R = R(L, \bar{a})^{d\times d}$ which provides a quantifier free formula $\rho_{\bar{z}}(x, \bar{\mathcal{Y}})$ in ortholattice language such that $\rho_{\bar{a}}(u, \mathcal{A})$ if and only $u = \omega_{\bar{a}}^{-1}(\mathcal{A}R)$ well as matrices of terms for the fundamental operations of R, say for $\circ$ terms $\otimes_{ij\bar{z}}(\mathcal{X}, \mathcal{Y})$ such that $(\otimes_{ij\bar{a}}(\mathcal{A}, \mathcal{B}))_{ij} = \mathcal{A} \circ \mathcal{B}$. Supposing the lattice L to be a sublattice of $\mathsf{Sub}(V)$ for some vector space V (as one can do), such formulas and terms (except for adhubction) are easily extracted from [Herr87a, §3] and [Her10b] and verified with calculations that boil down to elementary Linear Algebra; cf. [Her10b]. Moreover, by the same approach and using Fact 10, terms for adjunction are given in [Nie2007, Sect.4.4-5]. Though, our task is to show these definitions invariant under isometries which requires to strengthen to concept of orthogonal frames to one which corresponds to orthonormal bases. To do so, we borrow the concept of partial isometry from the theory of Baer-*-rings or, more elementarily, the concept of $*$-ring matrix units. See details below.

A. Tools for the proofs of Theorem 14b)

ss:pro

Fix d in the sequel. The concepts of a d-frame and of a sectional orthogonal d-frame $\bar{a}$ readily generalize from $d = 3$ to any fixed $d > 3$. For $d \geq 3$, the latter is an *orthogonal* d-frame of L if $\sum_{i=1}^d a_i = V$. It is *orthonormal* if, in addition, $a_{1j}^{\perp} \cap (a_1 + a_j) = \ominus_{\bar{A}^j} a_{1j}$ for all $j > 1$ where $\bar{a}^j$ arises from $\bar{a}$ interchanging a_2 with a_j as well as a_{12} with a_{1j}.

mol

Fact 15: Let $d \geq 3$ in (i), (iii), (iv).

(i) There is a a conjunction $\Phi(\bar{z})$ of term equations such that, for any $\bar{a}$ in L one has $\bar{a}$ an orthonormal d-frame if and only if $\Phi(\bar{a})$ holds.

(ii) If $\vec{v}_i$ form an orthogonal basis of V and have all the same length, then the $a_i = \mathbb{F}\vec{v}_i$, $a_{1j} = \mathbb{F}(\vec{v}_1 - \vec{v}_j)$ form

an orthonormal d frame; any such arises in this way with the $\vec{v}_i$ unique up to a common scalar multiple; in particular the basis may be required to be orthonormal. We say that the frame and the basis are *associated*.

(iii) For any orthonormal d-frames $\bar{a}, \bar{b}$ of V there is an isometry of V inducing an automorphism of L which maps $\bar{a}$ onto $\bar{b}$.

Proof:

(i) Obvious.

(ii) An easy calculation gives $\|\vec{v}_j\| = \|\vec{v}_1\|$ for any basis associated with an orthonormal basis.

(iii) Choose both associated bases orthonormal and match the basis vectors. ■

Recall, that $e \in R$ is a *projection*, if and only if $e = e^\dagger = e^2$. Such is, indeed, the unique orthogonal projection onto $\mathsf{im}\, e$ (if we think of $\mathsf{End}^\dagger(V)$). We say that pairwise orthogonal projections $w_i\, (i \leq d)$ together with w_{1j} in R form an *orthonormal system $\bar{w}$ of matrix units* for R if $\sum_i w_i = 1$ and $w_1 = w_{1j}^\dagger w_{1j}$ and $w_j = w_{1j} w_{1j}^\dagger$ for all $j > 1$ (this is the traditional notation for a "partial isometry"). Recall the ortholattice $\overline{L}^*(R)$ of all (principal) right ideals of R.

unit

Fact 16: (i) The following are equivalent

(1) $\bar{w}$ is an orthonormal system of matrix units.

(2) The $a_i = \mathsf{im}\, w_i = w_i\mathsf{R}$ are pairwise orthogonal and the $w_{1j}, w_{1j}^\dagger$ mutually inverse isometries between a_1 and a_j.

(3) In case $d \geq 3$: The $a_i = w_i\mathsf{R}$ and $a_{1j} = w_{1j}\mathsf{R}$ form an orthonormal d-frame $\bar{a}$ of L.

(ii) For any orthonormal systems $\bar{w}$ and $\bar{v}$ of matrix units there exists an isometry η of V such that $v_i = \eta \circ w_i$ and $v_{1j} = \eta \circ w_{1j}$.

(iii) There are terms $t_{ij}(x, \bar{z})$ in the language of rings with involution such that, for any orthonormal system $\bar{w}$ of matrix units and any $r \in \mathsf{R}$ one has $w_1 t_{ij}(r, \bar{w}) w_1 = t_{ij}(r, \bar{w})$ and the map $\omega_{\bar{w}}(r) = (t_{ij}(r, \bar{w}))_{ij}$ an isomorphism $\mathsf{R} \to \mathbb{F}^{d\times d}$ (by our identification an automorphism) such that the matrix $\omega_{\bar{w}}(w_i)$ has entry $x_{ii} = 1$, zero else, while $\omega_{\bar{w}}(w_{1j})$ has $x_{j1} = 1$, zero else. In particular, $w_1\mathsf{R}w_1$ is a a subring (but with unit w_1) of R closed under involution and isomorphic to $\mathbb{F}$.

Proof:

(i) The equivalence of (1) and (2) is obvious, that with (3) follows from Fact 10.

(ii) Use (i) and Fact 15(iii) in case $d \geq 3$; the case $d \leq 2$ is easily done, directly.

(iii) The terms mimic via w_i and w_{1j} how the coefficients of a matrix are extracted by use of the standard matrix units (which are images of the w_i, w_{1j} or easily computed from them). The w_{1j} are the *negative* graphs of the isometry from a_1 onto a_j. ■

In particular, one has a 1-1-correspondence ((referred to as *assoication* between orthonormal bases $\bar{v}$, orthonormal frames $\bar{a}$, and orthonormal systems $\bar{w}$ of matrix units. Thus, the notations $\mathsf{Mod}_{\bar{a}}$, $\mathsf{Mod}_{\bar{w}}$, $\rho_{\bar{a}}$ and $\kappa_{\bar{w}}$ have an obvious meaning.

B. Proof of Theorem 14b) for R

We are left to show that (ii) implies (iii). First, observe that the entries of a matrix can be recovered via the standard system of matrix units and then represented as elements of $\mathbb{F}^{d\times d} I_{11} \mathbb{F}^{d\times d} \cong \mathbb{F}$, where I_{11} has entry 1 in position $(1,1)$, zero else. By the same token, for any orthonormal system $\bar{w}$ of matrix units there is a unique isomorphism $\theta_{\bar{w}} : \mathsf{R} \to \mathbb{F}^{d\times d}$ (an automorphism if we identify R with $\mathbb{F}^{d\times d}$) matching $\bar{w}$ with the standard matrix units. This yields the following.

Corollary 17: For any orthonormal system $\bar{w}$ of matrix units and associated orthonomal basis $\bar{v}$ one has, for any $\varphi(\bar{x})$ iu the language of R, $\mathsf{Mod}^{\mathbb{F}}_{\bar{w}}(\varphi)$ definable within $\mathbb{F}$ and, for any $\psi(\bar{\mathcal{X}})$ in the language of $\mathbb{F}$, $\mathsf{Mod}^{\mathsf{R}}_{\bar{w}}(\psi)$ definable within R. Moreover, if $\bar{w}$ is added as system of constants to the langiage of R, the above remains true if parameters are admitted, where parameters in R, to be thought of as endomorphisms, are represented by their matrices w.r.t. $\bar{v}$, of parameters in $\mathbb{F}$ and paramters λ in $\mathbb{F}$ as $w_1(\lambda)w_i$, I the unit in R.

Mimicking this, in view of Fact 16(iii), for any $\varphi(\bar{x})$ there is a formula $\varphi_{\bar{z}}(\bar{\mathcal{X}})$ such that, for every orthonormal system $\bar{w}$ of matrix units, $\varphi_{\bar{w}}(\omega_{\bar{w}}(t_{ij}(f_1, \bar{w}))_{ij}, \ldots, \omega_{\bar{w}}(t_{ij}(f_n, \bar{y}))_{ij})$ holds in $\mathbb{F}$ if and only if $\varphi(f_1, \ldots f_n)$ holds in R. In view of Fact 16(ii), the choice of $\bar{w}$ does not matter and we choose ψ as the conjunction of $\mu(\bar{\mathcal{Z}})$, which requires these matrices forming an orthonormal system of matrix units, and of $\varphi_{\bar{z}}$ with any variable x_{kij} substituted by $t_{ij}(x_k)$ and any variable y_l by $z_1(y_l 1)z_1$. It follows that $\mathsf{Mod}^{\mathsf{R}}(\psi) = \mathsf{Mod}(\psi^\exists)$. ■

C. Proof of Theorem 14b) for L

(ii) implies (iii). We first continue the discussion following the statement of the theorem. Fix an orthonormal frame $\bar{a}$. By Fact 10(iii) (and commutativity and rigidity of $\mathbb{F}$) we have a unique isomorphism $\mathbb{F} \to R(L, \bar{a})$. This induces an isomorphism $\mathbb{F}^{d\times d} \to T_{\bar{a}} := R(\mathsf{L}, \bar{a})^{d\times d}$ with inverse $\eta_{\bar{a}}$. Thus, for all $u \in \mathsf{L}$, $f \in \mathsf{R}$, and $\mathcal{A} \in T_{\bar{a}}$, one has $\rho_{\bar{a}}(u, \mathcal{A})$ if and only if $u = f\mathsf{R}$. where $f \in \mathsf{R}$ is defined by $\eta_{\bar{a}}(\mathcal{A})$ w.r.t. the standard basis. Moreover, there are terms defining the $*$-ring operations on $T_{\bar{a}}$ coefficient wise ans so that $\eta_{\bar{a}}$ matches the coefficient wise calculations in both matrix $*$-rings. The following is now obvious.

Corollary 18: For any orthonormal frame $\bar{a}$ and associated orthonomal basis $\bar{v}$ one has, for any $\varphi(\bar{x})$ iu the language of L, $\mathsf{Mod}^{\mathbb{F}}_{\bar{a}}(\varphi)$ definable within $\mathbb{F}$ and, for any $\psi(\bar{\mathcal{X}})$ in the language of $\mathbb{F}$, $\mathsf{Mod}^{\mathsf{R}}_{\bar{a}}(\psi)$ definable within L. Moreover, if $\bar{a}$ is added as system of constants to the langiage of L, the above remains true if parameters are admitted, where parameters u in L are represented by matrices $\mathcal{A}$ such that $\rho_{\bar{a}}(u, \mathcal{A}$ of parameters in $\mathbb{F}$ and parameters λ in $\mathbb{F}$ as $(w_1(\lambda)w_i\mathsf{R})$, I the unit in R, $\bar{w}$ the associated system of matrix units.

Continuing with the proof, observe that the relevant ortholattice formulas and terms do not depend on $\bar{a}$. Also, the isomorphisms η satisfy the obvious commutative diagrams. Thus, for a fixed frame $\bar{e}$, we identify $R(\mathsf{L}, \bar{e})$ with $\mathbb{F}$ and extend this to an identification of $T_{\bar{e}}$ with $\mathbb{F}^{d\times d}$. Then, η_a becomes an isomorphism $T_{\bar{a}} \to \mathbb{F}^{d\times d}$.

In view of the above, given a formula $\psi(\bar{\mathcal{X}})$ in the language of $\mathbb{F}$ one can construct an ortholattice formula $\psi_{\bar{z}}(\mathcal{X})$ with additional variables $\bar{z}$, which requires for every substitution by orthonormal frames $\bar{a}$ for $\bar{z}$ and substitution of the $\mathcal{X}_k$, by $\mathcal{A}_k \in T_{\bar{a}}$, that $\bar{\mathcal{A}}$ satisfies ψ in $T_{\bar{a}}$ which matrix operations described, coefficient-wise, by the ortholattice terms, discussed earlier, Let $\psi^{\exists}(\bar{x})$ be $\exists\bar{z}.\exists\bar{\mathcal{X}}.\big(\Phi(\bar{z})\ \&\&\ \rho_{\bar{z}}(\bar{x},\bar{\mathcal{X}})\ \&\&\ \psi_{\bar{z}}(\bar{\mathcal{X}})\big)$.

By hypothesis, we have $\mathsf{Mod}^{\mathsf{L}}_{\bar{e}}(\psi)$ closed under automorphisms of L. Clearly, by the construction of $\psi^{\exists}$, if we show that $\mathsf{Mod}^{\mathsf{L}}_{\bar{a}}(\psi) = \mathsf{Mod}^{\mathsf{L}}_{\bar{e}}(\psi)$ for all $\bar{a}$ then $\mathsf{Mod}^{\mathsf{L}}(\psi) = \mathsf{Mod}(\psi^{\exists})$.

Indeed, consider $\bar{u} \in \mathsf{Mod}^{\mathsf{L}}_{\bar{a}}(\psi)$. By definition there is $\mathcal{A}$ such that $\rho_{\bar{a}}(\bar{u},\bar{\mathcal{A}})$ and $\psi(\bar{\mathcal{A}})$ valid in $T_{\bar{a}}$. Let $\tau_{\bar{a}}$ the automorphism of L induced by the isometry $\eta_{\bar{a}}$ and the canonical isomorphism of L onto $\overline{L}^{*}(T_{\bar{a}})$. Since $\eta_{\bar{a}} : T_{\bar{a}} \to T_{\bar{e}}$ is induced by the canonical isomorphism $R(\mathsf{L},\bar{a}) \to \mathbb{F}$ it follows, coefficient-wise, that $\psi(\eta_{\bar{a}}(\bar{\mathcal{A}}))$ holds in $\mathbb{F}$. Thus, $\tau_{\bar{a}}(\bar{u}) \in \mathsf{Mod}^{\mathsf{L}}_{\bar{e}}(\psi)$ which was assumed to be closed under automorphism. Thus, $\bar{u} \in \mathsf{Mod}^{\mathsf{L}}_{\bar{a}}(\psi)$. Conversely, use the inverses of $\eta_{\bar{a}}$ and $\tau_{\bar{a}}$. ■

V. 1st-Order Quantum Logic is Model-Complete

s:Model

By the Tarski–Seidenberg Theorem, the first-order theory of real-closed ordered fields admits (computable) quantifier elimination and is therefore complete. The order relation $x \geq 0$ can in turn be expressed using either quantifier as $\exists y : x = y{\cdot}y$ and as $x = 0 \vee \forall z : x \neq -z{\cdot}z$; but not without. Put differently, in the latter theory, all quantifiers can be eliminated except for one final block of either existential or universal ones — a property otherwise called (or rather equivalent to) *model completeness* [Mark02, Exercise 3.4.12d]. This extends to $\mathbb{C}$ (which we consider a ring with conjugation as involution) since real and imaginary parts are definable.

Recall that, for $\mathbb{F} \in \{\mathbb{R},\mathbb{C}\}$, the ring $\mathbb{F}^{d\times d}$ has, besides its canonical involution, also the operation $A \mapsto A^{+}$ of Moore-Penrose-Rickart *pseudo-inversion*, uniquely determined by well known identities.

t:Model

Theorem 19: Let $\mathbb{F} \in \{\mathbb{R},\mathbb{C}\}$ and d fixed.

a) Consider the first-order language of rings with involution. For any formula $\varphi(\bar{x})$ there is a quantifier-free formula $\psi(\bar{x},\bar{y},\bar{z})$ such that $\varphi(\bar{x}) \Leftrightarrow \exists\,\bar{y}\exists\bar{z}.\ \psi(\bar{x},\bar{y},\bar{z})$ is valid $\mathbb{F}^{d\times d}$.
b) Consider the first-order language of ortholattices and $d \geq 3$. For any formula $\varphi(\bar{x})$ there is a term $t(\bar{x},\bar{z})$ such that $\varphi(\bar{x}) \Leftrightarrow \exists\bar{z}.\ t(\bar{x},\bar{z}) = \mathbf{1}$ is valid in L.
c) Consider the first-order language of rings with involution and pseudoinversion and $d \geq 3$. For any formula $\varphi(\bar{x})$ there is a term $t(\bar{x},\bar{y},\bar{z})$ such that $\varphi(\bar{x}) \Leftrightarrow \exists\bar{y}\exists\bar{z}.\ t(\bar{x},\bar{y},\bar{z}) = 0$ is valid in $\mathbb{F}^{d\times d}$.

The above remain valid for formulas with parameters in $\mathbb{F}^{d\times d}$ resp. $L(\mathbb{F}^d)$, provided that the standard system of matrix units resp. the standard frame are added as a systen of constants and that these parameters are represented by matrices of parameters in $\mathbb{F}$

c:Model

Corollary 20: For every $d \in \mathbb{N}$, the quantum logics $L(\mathbb{C}^d)$ and $L(\mathbb{R}^d)$ are model complete.

A. Proof of Theorem 20

Recall (e.g. from the end of Subsection II-A) that, over any fixed ortholattice, equality "$x = y$" is equivalent to strong truth $t(x,y) = \mathbf{1}$ of some ortholattice term t. However $t(x,\mathbf{1})$ might still evaluate at least weakly true for $x < \mathbf{1}$. In fact there obviously exists no univariate term realizing over $\mathcal{MO}_1$ the so-called *indiscrete quantifier* [Roma06]

$$\psi(\mathbf{0}) = \mathbf{0}, \qquad \forall a \neq \mathbf{0} :\ \psi(a) = \mathbf{1}\ .$$

Taking also into account the aforementioned failure of the disjunction/conjunction property, we are (among others) faced with the problem of expressing the Boolean connectives within Quantum Logic. On the other hand [HeZi11, Lemma 10b+f] constructs a term $\psi_d|_X$ in variables $X,\bar{Y}$ such that it holds over $L(\mathbb{F}^d)$:

$$X = \mathbf{1}\ \Rightarrow\ \exists\bar{Y} : \psi_d|_X = \mathbf{1}, \qquad X \neq \mathbf{1}\ \Rightarrow\ \forall\bar{Y} : \psi_d|_X = \mathbf{0}$$

cmp. also [Hagg07, Theorem 1]. So $\neg\psi(\neg X)$ can be expressed in the existential theory of MOLs (of fixed height). Fact 15(ii) generalizes this to arbitrary Boolean combinations.

mol2

Fact 21: Let $d \geq 3$ in (i), (iii), (iv).

(i) There is a term $g(\bar{z})$ such that, for any $\bar{a}$ in $L(\mathbb{F}^d)$ one has $\bar{a}$ an orthonormal frame if and only if $g(\bar{a}) = \mathbf{1}$
(ii) For any Boolean combination $\varphi(\bar{x})$ of in-/equalities of ortholattice terms, there is a term $t(\bar{x},\bar{z})$ such that both $\varphi(\bar{x}) \Rightarrow \exists\bar{z}.\ t(\bar{x},\bar{z}) = \mathbf{1}$ and $\neg\varphi(\bar{x}) \Rightarrow \forall\bar{z}.\ t(\bar{x},\bar{z}) = \mathbf{0}$ are valid in $L(\mathbb{F}^d)$.

Proof:

(i) Combine the equations from Fact 15 into a term as in the proof of Theorem 2b).
(ii) According to [HMR05, Lemma 5] there is a term $d(x,y,\bar{z})$ such that for any d-frame $\bar{a}$ and u,v in $L(\mathbb{F}^d)$ one has $d(u,v,\bar{a}) = 0$ if $u = v$ and $d(u,v,\bar{a}) = \mathbb{F}^d$ if $u \neq v$. We now define by structural induction for each $\varphi(\bar{x})$ a term $s_\varphi(\bar{x},\bar{z})$ such that $\varphi(\bar{x})$ is in $L(\mathbb{F}^d)$ equivalent to $\exists\bar{z}.\ g(\bar{z}) \wedge s_\varphi(\bar{x},\bar{z}) = \mathbf{1}$. The case of equations has been dealt with in the proof of Item b) of Theorem 2. If ψ is the conjunction of φ_1 and φ_2 then s_ψ is just $s_{\varphi_1} \wedge s_{\varphi_2}$. Finally, if ψ is the negation of φ then s_ψ is $\neg d(s_\varphi,\mathbf{1})$. ■

Proof of Theorem 19a) and b): Given a formula $\varphi(\bar{x})$ defining a relation in L resp. R, use Theorem 14 to obtain a formula $\psi(\mathcal{X})$ in $\mathbb{F}$-language. In view of elimination in $\mathbb{F}$, one may assume ψ of the form $\exists\bar{y}.\ \chi(\bar{\mathcal{X}},\bar{y})$ with quantifier free χ. Replacing y by $\mathcal{Y}$ with y in the first entry, zero else, we may assume that χ is of the form $\chi(\bar{\mathcal{X}},\bar{\mathcal{Y}})$ whence ψ of the form $\exists\bar{\mathcal{Y}}.\ \chi(\bar{\mathcal{X}},\bar{\mathcal{Y}})$. The model set of the latter is invariant under unitary transformations (Theorem 14a)) whence, by Theorem 14b), there is quantifier free $\chi^{\#}(\bar{x},\bar{y},\bar{z})$ in the language of L resp. R such that $\exists\bar{y},\exists\bar{z}.\ \chi$ defines $\mathsf{Mod}(\varphi)$. In the case of L, apply Lemma 21(ii) to get the sharper result. For the case with parameters apply Corrollaries 17 and 18. ■

Proof of Theorem 19c): Recall that the pseudo-inverse in the $*$-regular ring $\mathsf{End}^{\dagger}(\mathbb{F}^d)$ is $\varphi^{+} = (\varphi|_{\mathsf{im}\,\varphi^{\dagger}})^{-1} \circ \pi_{\mathsf{im}\,\varphi}$ where π_U denotes the orthogonal projection onto U. Now,

using the methods [Her10b,Nie2007] as in the proof of Theorem 14b), all constituents of this expression can be captured in ortholattice terms over an orthonormal frame $\bar{a}$, independently of the latter in view of Fact 21(iv).

Conversely, in the presence of pseudo-inversion as an additional fundamental operation for the $*$-regular ring R, for any $a \in R$ one has $eR = aR$ and $Re = Ra$ with projections $e = aa^+$ and $f = a^+a$. Thus, the fundamental operations of L are given by terms in the language of $*$-regular rings with pseudo-inversion; see [Berb72, PROPOSITION §I.3.7]. To wit, R and L are bi-interpretable via terms. The claim follows from Fact 21(ii). ■

B. Proof of Corollary 20

The case $d \geq 3$ is covered by Theorem 19b). It thus remains to treat the cases $d \leq 2$; and suffices to show $\forall y : s(\bar{x}, y)$ equivalent to $\exists z : t(\bar{x}, z)$ for some appropriate term t depending on d and s. Now the Boolean case $d = 1$ is trivial: For $\bar{x} = (x_1, \ldots, x_n)$ there are 2^n possible assignments; so let

$$t(\bar{x}) \;:=\; \bigvee\nolimits_{\bar{b} \in \{\mathbf{0},\mathbf{1}\}^n : s(\bar{x},\mathbf{0}) = s(\bar{x},\mathbf{1}) = \mathbf{1}} \text{“}\bar{x} = \bar{b}\text{“} \qquad (2)$$

with the abbreviation

$$\text{“}\bar{x} = \bar{b}\text{“} \quad := \quad \bigwedge\nolimits_{j : b_j = \mathbf{1}} x_j \wedge \bigwedge\nolimits_{j : b_j = \mathbf{0}} \neg x_j \;\; .$$

Regarding the case $d = 2$, observe that every assignment $b_1, \ldots, b_n, a \in L(\mathbb{F}^2)$ 'lives' in (some sublattice of) $\mathcal{MO}_{n+1}$: the free ortholattice of height 2 on $n+1$ generators, see [HeZi11, FIG 1]. And any two of them are isomorphic, so we may replace $L(\mathbb{F}^2)$ with $\mathcal{MO}_{n+1}$. Generalizing Equation (2) let

$$t(\bar{x}) \;:=\; \bigvee\nolimits_{\bar{b} \in \mathcal{MO}_{n+1}^n : \forall y \in \mathcal{MO}_{n+1} : s(\bar{x},y) = \mathbf{1}} \text{“}\bar{x} = \bar{b}\text{“}$$

However “$\bar{x} = \bar{b}$“ cannot be expressed by a term involving only $\bar{x}$ (but not the constants from $\bar{b}$)! l:EvalMO

Lemma 22: For L an ortholattice and $\bar{a} \in L^n$ consider the finite sets $J_{\mathbf{0}}(\bar{a}) := \{j : a_j = \mathbf{0}\}$, $J_{\mathbf{1}}(\bar{a}) := \{j : a_j = \mathbf{1}\}$, $J_{=}(\bar{a}) := \{(i,j) : a_i = a_j\}$, $J_{\neq}(\bar{a}) := \{(i,j) : a_i = \neg a_j\}$. Now let $t(x_1, \ldots, x_n)$ be an ortholattice term with strongly satisfying assignment $\bar{a} \in \mathcal{MO}_n^n$. Suppose furthermore that $\bar{b} \in \mathcal{MO}_n^n$ satisfies $\big(J_{\mathbf{0}}(\bar{a}), J_{\mathbf{1}}(\bar{a}), J_{=}(\bar{a}), J_{\neq}(\bar{a})\big) = \big(J_{\mathbf{0}}(\bar{b}), J_{\mathbf{1}}(\bar{b}), J_{=}(\bar{b}), J_{\neq}(\bar{b})\big)$. Then also $t(\bar{b}) = \mathbf{1}$.

Proof: by immediate structural induction, observing for instance that $b_i \vee b_j = \mathbf{1} = a_i \vee a_j$ and $b_i \wedge b_j = \mathbf{0} = a_i \wedge a_j$ whenever $(i,j) \notin J_{=} \cup J_{\neq}$ for $i, j \notin J_{\mathbf{0}} \cup J_{\mathbf{1}}$. ■

Now resuming with the proof, and justified by Lemma 22, understand “$\bar{x} = \bar{b}$“ to denote the formula $\exists \bar{z}.t(\bar{x}, \bar{z})$ according to Fact 21 equivalent to $\neg\forall \bar{z}.\neg t(\bar{x}, \bar{z})$ over $L(\mathbb{F}^2)$ and to $\big(J_{\mathbf{0}}(\bar{x}), J_{\mathbf{1}}(\bar{x}), J_{=}(\bar{x}), J_{\neq}(\bar{x})\big) = \big(J_{\mathbf{0}}(\bar{b}), J_{\mathbf{1}}(\bar{b}), J_{=}(\bar{b}), J_{\neq}(\bar{b})\big)$, that is, to

$$\mathop{\&\&}_{j \in J_{\mathbf{1}}(\bar{b})} x_j = \mathbf{1} \;\; \&\& \mathop{\&\&}_{j \in J_{\mathbf{0}}(\bar{b})} x_j = \mathbf{0} \;\; \&\& \mathop{\&\&}_{(i,j) \in J_{=}(\bar{b})} x_i = x_j$$

$$\&\& \mathop{\&\&}_{(i,j) \in J_{\neq}(\bar{b})} x_i = \neg x_j \;\; \&\& \mathop{\&\&}_{j \notin J_{\mathbf{1}}(\bar{b})} x_j \neq \mathbf{1} \;\; \&\& \mathop{\&\&}_{j \notin J_{\mathbf{0}}(\bar{b})} x_j \neq \mathbf{0}$$

$$\&\& \mathop{\&\&}_{(i,j) \notin J_{=}(\bar{b})} x_i \neq x_j \;\; \&\& \mathop{\&\&}_{(i,j) \notin J_{\neq}(\bar{b})} x_i \neq \neg x_j \qquad ■$$

VI. EXTENSIONS AND RELATED TOPICS s:ext

A. Strong Satisfiability in Indefinite Dimension

Recall that the *triviality problem* for a class $\mathcal{C}$ asks for an algorithm to decide, for every given conjunction $\pi(\bar{x})$ of term equations, whether the subalgebra generated by (the members of) $\bar{a}$ is trivial for every satisfying assignment $\bar{a}$ of $\pi(\bar{x})$ in every $A \in \mathcal{C}$. The triviality problem has first been formulated in the context of finitely presented algebraic structures (see [BoOt93] for classical undecidability results). Unsolvability of the triviality problem for the class of all finite groups is shown in [BrWi14]. Of course, the proof of Theorem 2 could be simplified if unsolvability of the triviality problem for some class of finite semigroups with zero and unit were known. The proofs of Items a) and e) of Theorem 2 actually yield the following (in the modular lattice case, one has to replace 3-frames by 4-frames $\bar{A}$ in order to have Fact 6).

Corollary 23: The triviality problem is undecidable for any class of algebraic structures of the same similarity type, expanding lattice resp. ring (with unit) signature, such that all corresponding reducts are modular lattices resp. rings with unit including $\mathsf{Sub}(V_d)$ resp. $\mathsf{End}(V_d)$ for some sequence of vector spaces V_d with $\dim V_d$ unbounded.

Recall, that a Grassmann-Cayley algebra (cf [Stur06]) with underlying vector space V has operations $\wedge$ and $\vee$ such that $A \wedge B = A \cap B$ if $A + B = V$ and $A \vee B = A + B$ if $A \cap B = 0$. The lattice terms and equations used in the proof of Theorem 2a) can be modified so that satisfying assignments in $\mathsf{Sub}(V)$ are carried out in the Grassmann-Cayley algebra. This shows that there is no algorithm to decide satisfiability of conjunctions of such equations between such terms, tha latter called *simple Cayley algebra expressions*, in Grassmann-Cayley algebra of indefinite dimension.

On the other hand, the methods of our proof might be used to derive that there is no algorithm to decide for any given finite set of embedded multivalued database dependencies whether it admits a satisfying finite database (cf. [Herr95] for the implication problem).

B. Weak Satisfiability in Indefinite Dimension

Vector spaces with an anisotropic form, Hermitean w.r.t. a fixed antiautomorphism of the field, are essential in Theorem 7; then, for a family of such spaces, in Item a) the equivalence of (1) and weak satisfiability of t_p in some space remains valid. Returning to the classical $\mathbb{C}^d$, Item c) reveals the richness of the ortholattice variety generated by the $L(\mathbb{C}^d)$. Using the methods of [HeSe14] one can show that for real $\mathbb{F}$ and real α,

condition (3) is equivalent to $L(\mathbb{F}(\alpha)^3)$ embeddable into some $L(\mathbb{F}^d)$. In particular, (3) fails for $\mathbb{F}=\mathbb{Q}(\sqrt{2})$ and $\alpha=\sqrt[4]{2}$.

Call a positive-primitive formula $\varphi(\bar{x},y)$ a *quasi-term* (relatively to a class $\mathcal{C}$ of structures) if for any $A\in\mathcal{C}$ and $\bar{a}$ in A there is unique $b\in A$ such that $A\models\varphi(\bar{a},b)$. Call φ *unnested* if it contains atomic subformulas of the forms $y_1=y_1$ and $y_0=q(\bar{y})$, only, with fundamental operation symbols q. Recall, that any term can be translated, in polynomial time, into a logically equivalent unnested quasi-term.

Corollary 24: Let $\mathbb{F}\in\{\mathbb{R},\mathbb{C}\}$. The following decision problems admit mutually polynomial time reductions: both are decidable and within the complexity class $\mathcal{BP}(\mathsf{NP}^0_{\mathbb{F}})$.

(i) To decide for a given term $p(\bar{x})$ in the language of rings with unit, involution, and pseudoinversion whether $\forall\bar{x}.\,p(\bar{x})=0$ holds in $\mathbb{F}^{d\times d}$ for all d?

(ii) To decide for a given unnested quasi-term $\varphi(\bar{x})$ in the language of ortholattices whether $\forall\bar{x}.\ \varphi(\bar{x},0)$ holds in all $L(\mathbb{F}^d)$?

Moreover, in (i) there is $m.$ computable form p in time polynomial in the binary length of p, such that $\forall\bar{x}.\,p(\bar{x})=0$ fails in $\mathbb{F}^{d\times d}$ with $d\leq m$ if it fails for some d.
Thus, one might asl whether $\mathrm{sat}_{\mathbb{F}^*}$ belongs to some generalization of 'randomized polytime with one-sided error" (cf. [MoRa95,HSZ13].

Proof: As observed in the proof of Theorem 19c), each ortholattice term can be captured by an unnested quasi-term in $\mathbb{F}^{d\times d}$-language and the latter may be replaced by a single term as in the proof of Theorem 2c). Conversely, with the methodes of Subsection III-A, any term p in $\mathbb{F}^{d\times d}$-language converts into an ortholattice term $\hat{p}$ (adding only a constant to the number of occurrences of variables) such that, for all $d>0$, one has $\mathbb{F}^{d\times d}\models\forall\bar{x}.\,p(\bar{x})=0$ if and only if $L(\mathbb{F}^{3d})\models\forall\bar{x}.\,\hat{p}(\bar{x},0)$. The latter relies on the fact that subspaces of $\mathbb{F}^M$ are isometrically isomorphic if they have the same dimension. Decidability and dimension bound come from [Her10a] while the upper bound on complexity comes from [HeZi11]. ■

C. Definability and model completeness

For the translation of Section IV between 'geometry' and 'arithmetic', one may admit arbitrary vector spaces or such with an orthosymmetric sesquilinear form. Here, the concept of orthonormal frame has to be modified to capture the form, properly. Also, one has to pay heed to the fact that (ortho)lattice isomorphisms correspond to semilinear "isometries". Here, if instead of a single $t=\mathbf{1}$ one uses a conjunction $s=\mathbf{0}$ and $t=\mathbf{1}$, Theorem 19 remains valid for $\mathbb{R}$ and $\mathbb{C}$ vector spaces with Hermitean form.

For commutative $\mathbb{F}$ and in the absence of orthogonality, Theorem 14 has an analogue: in Grassmann-Cayley algebra of $\mathbb{F}^d$, Given a *simple* term t in these one can derive a certain kind of polynomial p (bracket polynomial) such that $t=\mathbf{0}$ iff $p=0$. The reverse direction is 'Cayley factorization': known to be possible (but up to multiplying with a bracket which mimics a coordinate system) for $d\geq 3$ and p with integer coefficients [StWh91] or for multilinear p [Whit90].

Also, from the representation of elements of $\mathsf{Sub}(\mathbb{F}^d)$ by matrices one might proceed to a representation via Plücker's embedding Π^d_k from $L_k(\mathbb{F}^d)$ (the k-dimensionals) into projective space $\mathbb{P}^{\binom{d}{k}-1}(\mathbb{F})$,

$$\mathrm{lspan}(\vec{a}^{(1)},..\vec{a}^{(k)})\mapsto\mathbb{F}\cdot\left(\det\begin{pmatrix}a^{(1)}_{j_1}&a^{(2)}_{j_1}&\ldots a^{(k)}_{j_1}\\ a^{(1)}_{j_2}&\ddots&a^{(k)}_{j_2}\\ \vdots&\ddots&\vdots\\ a^{(1)}_{j_k}&a^{(2)}_{j_k}&\ldots a^{(k)}_{j_k}\end{pmatrix}_{\substack{1\leq j_1<\ldots\\ \ldots<j_k\leq d}}\right)$$

cmp. [EzSt05, §14.1]. For fixed integers $\vec{k}=(k_1,\ldots,k_n)\in\{0,\ldots,d\}^n$ identify $(u_1,\ldots,u_n)\in L_{k_1}(\mathbb{F}^d)\times\cdots\times L_{k_n}(\mathbb{F}^d)$ with $\big(\Pi^d_{k_1}(u_1),\ldots,\Pi^d_{k_n}(u_n)\big)$.

Now. capturing orthogonality on Plücker coordinates in the obvious fashion, a condition $s(u_1,\ldots,u_n)=\mathbf{1}$ in the language of ortholattices translates into a homogeneous *-polynomial equation in Plücker coordinates; and the set

$$\big\{(u_1,\ldots,u_n):u_j\in L_{k_j}(\mathbb{F}^d),s(u_1,\ldots,u_n)=\mathbf{1}\big\}$$

of solutions thus into a quasialgebraic subset of $\mathbb{P}^{\binom{d}{k_1}-1}(\mathbb{F})\times\cdots\times\mathbb{P}^{\binom{d}{k_n}-1}(\mathbb{F})$; and quantification over $L_\ell(\mathbb{F}^d)$ to quantification over $\mathbb{P}^{\binom{d}{\ell}-1}(\mathbb{F})$. By Tarski-Seidenberg, the latter turns quasialgebraic subsets into semialgebraic ones, that is, projections of quasialgebraic ones. However translating the latter, purely existentially quantified (system of) homogeneous *-polynomial equations back into the language of ortholattices may of may not work with*out* multiplying with some other polynomial — referring to an orthonormal frame.

Acknowledgments

The present work was supported in parts by the *German Research Foundation* (DFG) with project `Zi1009/4-1`; by *7th EU IRSES* project `294962`; and by the *German Academic Exchange Service* (DAAD) under codenumber `91532398-50015537`.

References

[AbCo08] S. Abramsky, B. Coecke: "Categorical Quantum Mechanics", pp.261–323 in [EGL08].

[Artm68] B. Artmann: "On coordinates in modular lattices with a homogeneous basis", pp.626–648 in *Illinois J. Math.* vol.**12** (1968).

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

[BDDK03] F. Benanti, J. Demmel, V. Drensky, P. Koev: "Computational Approach to Polynomial Identities of Matrices—a Survey", pp.141–178 in *Polynomial Identities and Combinatorial Methods* (A. Giambruno, A. Regev, M. Zaicev, Edts), Dekker Series of Lecture Notes in Pure and Applied Mathematics vol.**234** (2003).

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

[Berb72] S.K. Berberian: "Baer $*$-Rings", *Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen* **195**, Springer (1972).

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

[BoOt93] R.V. BOOK, F. OTTO: *String-rewriting systems*, Texts and Monographs in Computer Science. Springer (1993).

[BoSt89] J. BOKOWSKI, B. STURMFELS: *Computational Synthetic Geometry*, Springer Lecture Notes in Mathematics vol.**1355** (1989).

[BrWi14] M.R. BRIDSON, H. WILTON: "The triviality problem for profinite completions" `arXiv:1401.2273v1` (2014).

[Bub07] J. BUB: "Quantum Computation from a Quantum Logical Perspective", pp.281–296 in *Quantum Information and Computation* vol.**7:2** (2007).

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

[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).

[EGL08] K. ENGESSER, D.M. GABBAY, D. LEHMANN (Editors): "*Handbook of Quantum Logic and Quantum Structures*", Elsevier (2008).

[EzSt05] E. MILLER, B. STURMFELS: *Combinatorial Commutative Algebra*, Springer GTM **227** (2005).

[Free79] R. FREESE: "Projective geometries as projective modular lattices", pp.329–342 in *Trans. Amer. Math. Soc.* vol.**251** (1979).

[Free80] R. FREESE: "Free modular lattices", pp.81–91 in *Trans. Amer. Math. Soc.* vol.**261** (1980).

[Gure66] Y. GUREVICH: "The word problem for some classes of semigroups" (Russian), pp.25–35 in *Algebra and Logic* vol.**5:2** (1966).

[GuLe84] Y. GUREVICH, H.R. LEWIS: "The Word Problem for Cancellation Semigroups with Zero", pp.184–191 in *Journal of Symbolic Logic* vol.**49** (1984).

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

[HeHu75] C. HERRMANN, A. HUHN: "Zum Wortproblem für freie Untermodulverbände", pp.449–453 in *Arch. Math.* (Basel) **26:5** (1975).

[HeRo99] C. HERRMANN, M.S. RODDY: "Proatomic modular ortholattices: Representation and equational theory", pp.55–88 in *Note di Matematica e Fisica* vol.**10** (1999), Conference in memory of Herbert Gross, `arXiv:1501.02477`

[Herr83] C. HERRMANN: "On the word problem for the modular lattice with four free generators", pp.513–527 in *Math. Ann.* vol.**265:4** (1983).

[Herr84] C. HERRMANN: "On the arithmetic of projective coordinate systems", pp.759–785 in *Trans. Amer. Math. Soc.* vol.**284:2** (1984).

[Herr87a] C. HERRMANN: "Frames of permuting equivalences", pp.93–101 in *Acta Sci. Math.* vol.**51:1-2** (1987).

[Herr87b] 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).

[Herr95] C. HERRMANN: "On the undecidability of implications between embedded multivalued database dependencies" (English summary), pp.221–235 in *Inform. and Comput.* vol.**122** (1995).

[Her10a] 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).

[Her10b] C. HERRMANN: "Generators for complemented modular lattices and the von Neumann-Jónsson coordinatization theorems", pp.45–64 in *Algebra Universalis* vol.**63:1** (2010).

[HeSe14] C. HERRMANN, M. SEMENOVA: "Rings of quotients of finite AW^*-algebras: Representation and algebraic approximation", pp.298–322 in *Algebra and Logic* vol.**54:4** (2014).

[HSZ13] C. HERRMANN, J. SOKOLI, M. ZIEGLER: "Satisfiability of cross product terms is complete for real nondeterministic polytime Blum-Shub-Smale machines", pp.85–92 in *Proc. 6th Int. Conf. Machines, Computations and Universality*

[HeZi11] C. HERRMANN, M. ZIEGLER*: "Computational Complexity of Quantum Satisfiability", pp.175–184 in* Proc. 26th Annual IEEE Symposium on Logic in Computer Science *(2011).*

[HMR05] C. HERRMANN, F. MICOL, M.S. RODDY*: "On n-distributive Modular Ortholattices", pp.143–147 in* Algebra Universalis *vol.**53** (2005).*

[Hutc77] G. HUTCHINSON*: "Embedding and unsolvability theorems for modular lattices", pp.47–84 in* Algebra Universalis *vol.**7** (1977).*

[HyNa05] M. HYČKO, M. NAVARA*: "Decidability in Orthomodular Lattices", pp.2239–2248 in* Journal of Theoretical Physics *vol.**44:12** (2005).* , EPTCS vol.**128** (2013).

[KhSa95] O.G. KHARLAMPOVICH, M.V. SAPIR: "Algorithmic Problems in Varieties", pp.379–602 in *Internat. J. Algebra Comput.* vol.**5:4–5** (1995).

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

[Lips74] L. LIPSHITZ: "The Undecidability of the Word Problems for Projective Geometries and Modular Lattices", 171–180 in *Transactions of the American Mathematical Society* vol.**193** (1974).

[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).

[Mark02] D. MARKER: *Model Theory: An Introduction*, Springer GTM vol.**217** (2002).

[MaRo87] R. MAYET, M.S. RODDY: "n-Distributivity in Ortholattices", pp.285–294 in (Czermak et al. eds.) *Contributions to General Algebra* vol.**5** (1987).

[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).

[MoRa95] R. MOTWANI, P. RAGHAWAN: "*Randomized algorithms*", Cambridge Univeristy Press (1995).

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

[Neum60] J.VON NEUMANN: *Continuous Geometry*, Princeton Math.Series no.**25** (1960).

[Nie2007] N. NIEMANN:"On Representability of $*$-Regular and Regular Involutive Rings in Endomorphism Rings of Vector Spaces". PhD-Thesis Darmstadt (2007), Logos Verlag Berlin.

[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 [EGL08].

[Poon08] B. POONEN: "Undecidability in Number Theor", pp.344–350 in *Notices of the American Mathematical Society* vol.**55** (2008).

[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), Americal Mathematical Society vol.**6** (1992).

[Rich99] J. RICHTER-GEBERT: "The Universality Theorems for Oriented Matroids and Polytopes", pp.269–292 in *Contemporary Mathematics* vol.**223** (1999).

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

[Roma06] L. ROMÁN: "A Characterization of Quantic Quantifiers in Orthomodular Lattices", pp.206–217 in *Theory and Applications of Categories* vol.**16:10** (2006).

[Scha10] M. SCHAEFER: "Complexity of Some Geometric and Topological Problems", pp.334–344 in *Proc. 17th Int. Symp. on Graph Drawing*, Springer LNCS vol.**5849** (2010).

[Shor91] P. SHOR: "Stretchability of Pseudolines is NP–hard", pp.531–554 in *Applied Geometry and Discrete Mathematics — The Victor Klee Festschrift* (P. Gritzmann and B. Sturmfels Edts), DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol.**4** (1991).

[Stur06] B. STURMFELS: *Algorithms in invariant theory*, Texts and Monographs in Symbolic Computation. Springer (2008).

[StWh91] B. STURMFELS, W. WHITELEY: "On the Synthetic Factorization of Projectively Invariant Polynomials", pp.439–453 in *J. Symbolic Computation* vol.**11** (1991).

[Svoz98] K. SVOZIL: "*Quantum Logic*", Springer (1998).
[Whit90] N. WHITE: "Multilinear Cayley Factorization", pp.421–438 in *J. Symbolic Computation* vol.**11** (1990).
[Ying05] M. YING: "A Theory of Computation based on Quantum Logic I", pp.134–207 in *Theoretical Computer Science* vol.**344** (2005).