ON THE SATISFIABILITY PROBLEM FOR CLASSES OF STRUCTURES RELATED TO FINITE DIMENSIONAL VECTOR SPACES

CHRISTIAN HERRMANN, YASUYUKI TSUKAMOTO, AND MARTIN ZIEGLER

Abstract. We establish unsolvability of the satisfiability problem in the following cases: conjunctions of equations within any class of (bounded) lattices of subspaces resp. endomorphism rings associated with a class of vector spaces, over a fixed or all fields of characteristic 0, of unbounded finite dimension; the same for any expansion of such class, e,g, the ortholattices of subspaces of inner product spaces (in this case, it suffices to consider single equations); conjunctions of equations within finite relation algebras; conjunctions of functional and embedded multivalued dependencies within the class of finite databases; conjunctions of equations between simple expressions within Grassmann-Cayley algebras of unbounded dimension.

1. Introduction

The classical *triviality problem* (cf. [12]), say for groups, asks for an algorithm which, given any finite group presentation, that is a conjunction $\pi(\bar{x})$ of equations, decides whether the group G_π given by the presentation π is trivial. As for many other equationally defined classes this problem is well known to be unsolvable. Based on the undecidability of the universal theory of the class of finite groups, shown by Slobodskoi [15], and advanced methods of geometric group theory, Bridson and Wilton [1] have shown that the triviality problem for finitely presented profinite groups is algorithmically unsolvable: Let $\hat{G}_\pi$ denote the inverse limit of all G_π/N, N a normal subgroup of finite index.

Fact 1. *There is no algorithm which for any π decides whether $\hat{G}_\pi$ is trivial.*

Moreover, they derive that there is no algorithm deciding for every π whether G_π admits a non-trivial finite dimensional F-linear representation, F a fixed or arbitrary field.

As for word problems, the *triviality problem* for a class $\mathcal{C}$ of algebraic structures can be reformulated: to decide for any conjunction $\pi(\bar{x})$ of equations whether there is $A \in \mathcal{C}$ and a satisfying assignment $\bar{x} \mapsto \bar{a}$ for π in A such that the a_i from $\bar{a}$ generate a non-singleton subalgebra of A. Note that, in the case of finite signature, the triviality problem is an instance of the uniform word problem.

The complement of the triviality problem for $\mathcal{C}$ can be understood as *satisfiability problem* for $\mathcal{C}$: to decide for any $\pi(\bar{x})$ whether it has a *non-trivial* (i.e. generating a non-singleton subalgebra) satisfying assignment in some member A of $\mathcal{C}$. In the

2000 *Mathematics Subject Classification.* Primary: 08A50; Secondary: 03B60; 03G15; 06Cxx; 15A24: 51M35.

Key words and phrases. triviality problem; satisfiability ; decidability; subspace lattice; endomorphism ring; relation algebra; database dependencies.

presence of constants $0, 1$ such that $0 = 1$ only in trivial members of $\mathcal{C}$ (as in the case of bounded lattices and rings with unit), the satiafiability problem asks whether there is a satisfying assignment in some non-trivial member of $\mathcal{C}$. In this case, unsolvability of the problem is preserved under expansions.

For a vector space V let $\mathrm{L}(V)$ denote the lattice of all subspaces and $\mathrm{L}_0^1(V)$ the same with bounds $0 = \mathbf{0}$ and $V = \mathbf{1}$ as constants. Let $\mathcal{F}$ be a class of fields containing a field of characteristic 0 or fields of arbitrarily large characteristic and $\mathcal{V}$ a class of finite dimensional F-vector spaces, $F \in \mathcal{F}$, such that for any $F \in \mathcal{F}$ and $d \in \mathbb{N}$ there are an extension F' of F in $\mathcal{F}$, and a F'-vector space $W' \in \mathcal{V}$ with $\dim_{F'} W' \geq d$. In the sequel, $\mathcal{V}$ will always denote such class. One may assume $\mathcal{F}$ closed under isomorphism and $\mathcal{V}$ under semilinear isomorphism. We also say that $\mathcal{V}$ satisfies condition $(*)$ if W', above, can be chosen such that $\dim_{F'} W' = 3md$ for some m. In particular, this applies if $\mathcal{V}$ consists of all finite dimensional F-vector spaces, F in a given class $\mathcal{F}$ of fields as above.

Our main result is the following, based on Fact 1 and the well known interpretation of rings within modular lattices, due to von Neumann [14] (cf. Lipshitz [13], Freee [2,3] which is the first step in Coordinatization Theory (in the setting of lattices $\mathrm{L}_0^1(V)$ relevant proofs can be given within elementary Linear Algebra, cf. [11, §3]).

Theorem 2. *The satisfiability problems for* $\{\mathrm{L}(V) \mid V \in \mathcal{V}\}$ *and* $\{\mathrm{L}_0^1(V) \mid V \in \mathcal{V}\}$ *are algorithmically unsolvable.*

We apply this to the analogous problems: for endomorphism rings (Subsection 3.5); for ortholattices of subspaces and $*$-rings of endomorphisms, in case $\mathcal{V}$ is a class of inner product spaces, answering a question left open in [10, §III.C] (Subsection 3.6); for equations between simple expressions in Grassmann-Cayley algebra (Subsection 3.3): for finite relation algebras and for dependencies in finite databases (Subsection 3.4).

2. Proof of Theorem 2

The following can be seen as a variant of Lemma 3.5 in Lipshitz [13].

Fact 3. *Fix* $d \in \mathbb{N}$. *The universal theory of all* $\mathrm{L}_0^1(V)$, V *ranging over* d*-dimensional vector spaces over fields* F, *coincides with that where the* F *are finite.*

Proof. We may assume $V = F^d$. By tensoring with $\bar{F}$, the algebraic closure of F, we have $\mathrm{L}_0^1(F^d)$ embedded into $\mathrm{L}_0^1(\bar{F}^d)$. The algebraic closure $\bar{P}$ of the prime subfield P of F is elementarily equivalent to $\bar{F}$, and it follows that $\mathrm{L}_0^1(\bar{F}^d)$ and $\mathrm{L}_0^1(\bar{P})$ are elementarily equivalent, too. Being a directed union, the latter is in the universal class generated by the $\mathrm{L}_0^1(K^d)$, $[K : P] < \infty$ – and K is finite if P is finite. Finally, observe that $\bar{\mathbb{Q}}$ embeds into a suitable ultraproduct of the $\bar{P}$, P finite, since that is algebraically closed and of characteristic 0. □

We now give a short review of the basic facts needed from coordinatization theory. All vector spaces will be over fields and of finite dimension. The lattice operations of $\mathrm{L}_0^1(V)$ are the *meet* $U \cap W$ (intersection) and the *join* $U + W$ (sum) – we write $U + W = U \oplus W$ to indicate that also $U \cap W = 0$. 0 and V are considered as constants $\mathbf{0}$, $\mathbf{1}$. For any vector space V, we say that $\bar{A} = (A_1, A_2, A_3, A_{12}, A_{13})$ in $\mathrm{L}_0^1(V)$ forms a 3-*frame* if $V = A_1 \oplus A_2 \oplus A_3$ and $A_{1j} \oplus A_1 = A_{1j} \oplus A_j = A_1 + A_j$ 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. [3]. In the following, (i), (ii), and (iv) are obvious. For (iii) choose a linear isomorphism $f_1 : A_1 \to B_1$ and f_j, $j = 2, 3$ so that $\varepsilon_{j\bar{B}} \circ f_1 = f_j \circ \varepsilon_{j\bar{A}}$.

Fact 4. (i) *If $\bar{A}$ is a 3-frame of $\mathrm{L}_0^1(V)$ then $V = 0$ if and only if $A_1 = 0$ if and only if $A_{12} = 0$.*

(ii) *Given $V \in \mathrm{L}_0^1(V)$, 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 $\mathrm{L}_0^1(V)$ there is an automorphism of $\mathrm{L}_0^1(V)$ mapping $\bar{A}$ onto $\bar{B}$.*

(iv) *Choose distinguished variables z_1, z_2, z_3 and z_{12}, z_{13}: shortly, $\bar{z}$. There is a conjunction $\Phi(\bar{z})$ of bounded lattice equations such that for any $\bar{A} \in \mathrm{L}_0^1(V)$ one has $\bar{A}$ a 3-frame of $\mathrm{L}_0^1(V)$ if and only if $\mathrm{L}_0^1(V) \models \Phi(\bar{A})$.*

We define $R(\mathrm{L}_0^1(V), \bar{A}) = \{U \in \mathrm{L}_0^1(V) \mid U \oplus A_2 = A_1 + A_2\}$ and $\gamma_{\bar{A}}(\varphi) = \{\vec{v} - \varepsilon_{2\bar{A}}\varphi\vec{v} \mid \vec{v} \in A_1\}$, the *negative graph* of the map $\varepsilon_{2\bar{A}} \circ \varphi$. This yields a bijection $\gamma_{\bar{A}} : \mathsf{End}(A_1) \to R(\mathrm{L}_0^1(V), \bar{A})$. The following is well known [3, §1], [7, Theorem 2.2], cf. [11, §3].

Fact 5. *There are conjunctions $\sigma(x, \bar{z})$ and $\sigma^\times(x, \bar{z})$ of term equations and, for each fundamental operation $q(\bar{x})$ of rings with unit and partial inversion, a term $\hat{q}(\bar{x}, \bar{z})$ in the language of bounded lattices such that the following are true for any 3-frame $\bar{A} \in \mathrm{L}_0^1(V)$. Moreover, in any of these terms each of the variables in $\bar{x}$ occurs exactly once.*

(i) *$\gamma_{\bar{A}}$ is an isomorphism of $\mathsf{End}(A_1)$ (with partial inversion) onto $R(\mathrm{L}_0^1(V), \bar{A})$ endowed with the operations $\bar{x} \mapsto \hat{q}(\bar{x}, \bar{A})$. Here, the ring elements 0 and id_{A_1} are mapped onto A_1, A_{12}. In particular, $\gamma_{\bar{A}}$ restricts to an isomorphism of $\mathsf{GL}(A_1)$ onto the group $R^\times(\mathrm{L}_0^1(V), \bar{A})$ of units of $R(\mathrm{L}_0^1(V), \bar{A})$.*

(ii) *For any $U \in \mathrm{L}_0^1(V)$ one has $U \in R(\mathrm{L}_0^1(V), \bar{A})$ if and only if $\mathrm{L}_0^1(V) \models \sigma(U, \bar{A})$; and $U \in R^\times(\mathrm{L}_0^1(V), \bar{A})$ if and only if $\mathrm{L}_0^1(V) \models \sigma^\times(U, \bar{A})$.*

We refer to $R(\mathrm{L}_0^1(V), \bar{A})$ as the *coordinate ring* of the frame $\bar{A}$.

Lemma 6. *With any finite conjunction $\pi(\bar{x})$ of group relations one can effectively associate conjunctions $\hat{\pi}(\bar{x}, \bar{z})$ and $\pi^\#(\bar{x}, \bar{z})$ of equations in the language of bounded lattices (with binary term length a constant multiple of that of $\pi(\bar{x})$) such that the following hold for the group G_π presented by $\pi(\bar{x})$.*

(i) *For any F-vector space V and 3-frame $\bar{A}$ of $L = \mathrm{L}_0^1(V)$*

(a) *If $x_i \mapsto \varphi_i \in \mathsf{GL}(A_1)$ defines a representation of G_π then $x_i \mapsto \gamma_{\bar{A}}(\varphi_i)$, $\bar{z} \mapsto \bar{A}$ is a satisfying assignment for $\hat{\pi}$ in L.*

(b) *If $L \models \hat{\pi}(\bar{g}, \bar{A})$ then $x_i \mapsto \gamma_{\bar{A}}^{-1}(g_i)$ defines a representation of G_π in A_1.*

(ii) *If $0 < \dim V < \infty$ and $\mathrm{L}_0^1(V) \models \exists\bar{x}\exists\bar{z}.\, \hat{\pi} \wedge \pi^\#$ then there is a subspace W of V, $\dim W = \frac{1}{3}\dim V$, and a non-trivial representation of G_π in W.*

(iii) *If G_π has a finite homomorphic image H admitting a non-trivial irreducible representation in W and $\dim V = 3\dim W$ then $\mathrm{L}_0^1(V) \models \exists\bar{x}\exists\bar{z}.\, \hat{\pi} \wedge \pi^\#$.*

Proof. Choice of $\hat{\pi}$ and (i) are obvious by Fact 5. Define $\pi^\#$ as $\Phi(\bar{z}) \wedge u = 0$ where $u := \bigcap_i x_i \cap z_{12}$.

In (ii) choose witnessing $\bar{A}$ and $\bar{g}$ and apply (b) to obtain a representation of G_π within $W = A_1$. Assuming this to have singleton image, we have $x_i \mapsto \mathrm{id}_{A_1}$ for all

i, whence $u \mapsto A_{12}$. In view of $\pi^{\#}$ it follows $A_{12} = 0$ whence $V = 0$ by Fact 4(i); a contradiction. Thus, the representation of G_π has non-singleton image.

Concerning (iii), choose a 3-frame $\bar{A}$ in $\mathrm{L}^1_0(V)$ so that w.l.o.g. $A_1 = W$ and apply (a) substituting $\gamma_{\bar{A}}(\varphi_i)$ for x_i. Let U the value of u in $\mathrm{L}^1_0(V)$, that is

$$U = \{v - \varepsilon_{2\bar{A}} v \mid v \in A_1\} \cap \bigcap_i \{v - \varepsilon_{2\bar{A}}(\varphi_i v) \mid v \in A_1\}.$$

Put $U_0 = \{v \in A_1 \mid v - \varepsilon_{2\bar{A}} v \in U\}$ and observe that $U \neq 0$ implies $U_0 \neq 0$. Now, by definition of U and U_0, the φ_i act on U_0 as identity; in particular U_0 is invariant under the φ_i and their inverses whence under the action of H on A_1. Since that was assumed irreducible it follows $U = U_0 = 0$.

□

Proof of Theorem 2. We reduce the problem in Theorem 1 to the satisfiability problem for $\{\mathrm{L}^1_0(V) \mid V \in \mathcal{V}\}$. First, assume that $\mathcal{V}$ satisfies condition $(*)$.

Assume $\hat{\pi} \wedge \pi^{\#}$ is satisfied in $\mathrm{L}^1_0(V)$, $V \neq 0$ a finite dimensional F-vector space; that is, the universal sentence $\forall \bar{z} \forall \bar{x}.\ \hat{\pi} \wedge \pi^{\#} \Rightarrow 1 = 0$ fails in $\mathrm{L}^1_0(V)$. By Fact 3 it fails as well in $\mathrm{L}^1_0(V')$ for some K-vector space $V' \neq 0$ with K finite, and $\dim_K V' = \dim_F V$. Then by Lemma 6(ii) G_π has a non-trivial representation in some subspace W of V'. Since K is finite, the image H of G_π in $\mathrm{GL}(W)$ is finite, too. Thus, $\hat{G}_\pi$ is non-trivial.

Conversely, assume, that $\hat{G}_\pi$ is non-trivial. Then G_π has a non-trivial finite homomorphic image H. Choose $F \in \mathcal{F}$ of characteristic not dividing the order of H and apply Maschke's Theorem to the regular representation of H to obtain a non-trivial irreducible representation of H (and G_π) within some F-vector space W, $d := \dim_F W < \infty$. By $(*)$ there is an extension F' of F and an F'-vector space $W' \in \mathcal{V}$ with $\dim_{F'} W' = 3md$. By (iii) of Lemma 6 we have $\hat{\pi} \wedge \pi^{\#}$ satisfiable in $L(V)$ if V is any F-vector space with $\dim_F V = 3d$. Since (by tensoring with F') $L(V)$ embeds into $L(V')$ for any F'-vector space V' of $\dim_{F'} V' = \dim_F V$, there is a satisfying assignment ν_k for $\hat{\pi} \wedge \pi^{\#}$ in $L(V_k)$, V_k any subspace V_k of W' with $\dim V_k = 3d$. Take $W' = \bigoplus_k V_k$ and $\nu = \bigoplus \nu_k$ to obtain a satisfying assignment in $L(W')$.

In the general case we have to modify the concept of a 3-frame to that of a *skew 3-frame* in $L(V)$: given by $A_i\,(i = 0, 1, 2, 3)$ and $A_{1i}\,(i = 0, 2, 3)$ such that that the A_i, A_{1i}, $i \neq 0$, form a 3-frame in $U = A_1 + A_2 + A_3$ and, moreover, such that $V = U \oplus A_0$, and $A_{10} \oplus A_0 = A_{10} \oplus (A_1 \cap (A_0 + A_{10})) = A_0 + (A_1 \cap (A_0 + A_{10}))$. In particular, A_{10} is the negative graph of an embedding of A_0 into A_1. Modify Φ in Fact 5(iv) to capture this and modify $\pi^{\#}$, accordingly, to $\pi^{@}$. If $\hat{\pi} \wedge \pi^{@}$ is satisfied in $L(V)$, then the above reasoning is still valid. For the converse, the condition on $\mathcal{V}$ might yield W' with $\dim W' = 3md + k$, $k \in \{1, 2\}$ (and we may assume $md \geq 2$). Then use the given reasoning for a $3dm$-dimensional subspace W'' and 3-frame $\bar{A}$ of W'; and choose $A_0 \oplus W'' = W'$ and A_{10} as the negative graph of an embedding of A_0 into A_1 to achieve a satisfying assignment.

In the absence of constants $\mathbf{0}, \mathbf{1}$, replace $\mathbf{0}$ by $\prod_i z_i$ and $\mathbf{1}$ by $\sum_i z_i$; it suffices to consider the case of condition $(*)$. □

3. Corollaries

3.1. **Special equations.**

Corollary 7. *There is no algorithm deciding for any given terms s, t in the language of bounded lattices whether $s = \mathbf{0} \, \wedge \, t = \mathbf{1}$ is solvable in some* $\mathrm{L}_0^1(V)$*,* $V \in \mathcal{V}$*,* $V \neq 0$*.*

Proof. To reduce the case of arbitrary conjunctions of equations $s_j = t_j$, to that of the special form $s = \mathbf{0} \, \wedge \, t = \mathbf{1}$, observe each $s_j = t_j$ equivalent over every $\mathrm{L}_0^1(V)$ to $\exists v : \tilde{s}_j = \mathbf{0} \, \wedge \, \tilde{t}_j = \mathbf{1}$ for $\tilde{s}_j := (s_j + t_j) \cap v$ and $\tilde{t}_j := (s_j \cap t_j) + v$ (due to modularity and existence of complements); and $\tilde{s}_j = \mathbf{0} \wedge \tilde{t}_j = \mathbf{1} \wedge \tilde{s}_i = \mathbf{0} \wedge \tilde{t}_i = \mathbf{1}$ equivalent to $\tilde{s}_j + \tilde{s}_i = \mathbf{0} \, \wedge \, \tilde{t}_j \cap \tilde{t}_i = \mathbf{1}$. □

3.2. **Fast growth.** In [4] the *bit length* of a group presentation is defined as the total number of bits required to write the presentation; in particular, words are considered as strings of powers of generators and inverses of generators, the exponents encoded in binary. Transferring this to lattice presentations, we allow the use of recursively defined subterms, encoding the number of iteration steps in binary.

Corollary 8. *There are a constant K and for any $n > 7$ a conjunction $\psi_n(\bar{y})$ of bounded lattice equations in 8 variables $\bar{y}$ and of bit length $O(\log n^K)$ such that, $\psi_n(\bar{y})$ is satisfiable in some* $\mathrm{L}_0^1(V)$*,* $V \in \mathcal{V}$*, with* $\dim V = d > 0$ *for* $d = n$ *but not for* $d < n$*.*

Proof. By [4, Theorem C] the alternating groups A_n, $n > 7$, have presentations of bit length $O(\log n)$ in 3 generators $\bar{x} = (x_1, x_2, x_3)$; and any non-trivial irreducible representation of A_n has degree $\geq n - 1$ [17]. Based on such presentation of A_n, define, for each n, $\hat{\pi}_n(\bar{x}, \bar{z})$ and $\pi_n^{\#}(\bar{x}, \bar{z})$ as in Lemma 6 and put ψ_n the conjunction of both. The constant K comes from Fact 4: for every group word $w(\bar{x})$ one has a lattice term $w_{\bar{z}}(\bar{x})$ (in the extended sense) such that $|w_{\bar{z}}(\bar{x})| \leq K|w(\bar{x})|$ and $w_{\bar{A}}(\bar{x})$ evaluates as $w(\bar{x})$ in any $R(\mathrm{L}_0^1(V), \bar{A})$. □

3.3. **Grassmann-Cayley algebra.** Recall, that a Grassmann-Cayley algebra (cf [16]) with underlying vector space V has operations $\wedge$ and $\vee$ and terms built from that (and $\mathbf{0}, \mathbf{1}$) are *simple Cayley algebra expressions.* One has $A \wedge B = A \cap B$ if $A + B = V$ and $A \vee B = A + B$ if $A \cap B = 0$.

Corollary 9. *There is no algorithm to decide satisfiability, of conjunctions of equations between simple expressions. within the class of Grassmann-Cayley algebras over $V \in \mathcal{V}$.*

Proof. We have to show that the lattice terms and equations used in the proof of Theorem 2 can be modified so that satisfying assignments in $\mathrm{L}_0^1(V)$ are carried out subject to the above side condition for any meet or join in the evaluation of terms. First, let $X \in R_{ij}$ iff $X \cap (A_j + A_k) = 0$ and $X + A_j = A_i + A_j$ where i, j, k are pairwise distinct (which obeys the side conditions) and use this to modify the definition of a 3-frame: $A_{1j} \in R_{1j} \cap R_{j1}$. Now multiplication and inversion are obtained via terms like $(X + Y) \cap (A_i + A_k)$ where $X \in R_{ij}$ and $Y \in R_{jk}$. □

3.4. **Relation algebras and databases.** For an abelian group V let $\mathrm{L}_0^1(V)$ denote its lattice of subgroups with bounds 0 and V.

Corollary 10. *The satisfiability problem for the class of all* $\mathrm{L}_0^1(V)$*,* V *a finite abelian group is unsolvable.*

Proof. The primary decomposition shows that $\mathrm{L}_0^1(V)$ is the direct product of the $\mathrm{L}_0^1(V_p)$, V_p the subgroup of elements having order a power of p. Proceeding as in the proof of Theorem 2, obtaining a finite homomorphic image H of G_π uses only Lemma 6(ii) while in the converse direction one chooses $F = \mathbb{Z}/(p)$ with p not dividing the order of H. □

Corollary 11. *The satisfiability problem for the class of finite relation algebras (with or without complementation) is unsolvable.*

Proof. Recall that for an abelian group V, there is a 1-1-correspondence between subgroups and congruence relations, giving rise to an isomorphism of $\mathrm{L}_0^1(V)$ onto the lattice $\mathrm{Con}(V)$ of congruence relations of V. Continuing with the proof of Corollary 10, consider the congruence relations α_i, α_{ij} associated with A_i, A_{ij} and ρ_k with $\gamma_{\bar{A}}(g_k)$. Considering the $\alpha_i, \alpha_{ij}, \rho_k$ as elements of the relation algebra on the set V, one has to introduce relations between them which allow to recapture the group V and to derive that they are congruence relations. First of all, one can encode the fact that these elements of the relation algebra are indeed equivalence relations on the set V. The abelian group V can be recovered requiring that the α_i, α_{ij} permute pairwise and satisfy the relations of a frame w.r.t. intersection and relational product. [8, Theorem 1]. Moreover, by the proof of [8, Corollary 2] (cf. [9, Lemma 32]), the ρ_k are congruences of V iff they permute with the α_i, α_{ij} and satisfy, in terms of α_i, α_{ij}, the relations σ of Fact 5(ii) characterizing elements of the coordinate ring. Thus, having required all the relevant relations, the $\alpha_i, \alpha_{ij}, \rho_k$ generate a sublattice of the lattice of all equivalence relations on V which is isomorphic to the sublattice of $\mathrm{L}_0^1(V)$ generated by $\bar{A}$ and the $\gamma_{\bar{A}}(g_i)$ and in which the join is given by the relational product. Now, the claim follows from Corollary 10. □

Corollary 12. *There is no algorithm to decide for any given finite set of functional and embedded multi-valued database dependencies whether it admits a finite model with more than one data set.*

Proof. Following the approach of Corollaries 10 and 11 use the correspondence between systems of equivalence relations on a finite set and finite databases and [9, Lemma 11] to translate relations in terms of intersection and product into functional and embedded multivalued dependencies. □

Corollary 13. *There is no algorithm to decide for any given finite set of inclusion and conditional independence atoms whether it admits a non-trivial finite model.*

Proof. By [5, Section 2.2], this follows from Corollary 12. □

3.5. **Rings.** Let $\mathsf{End}(V)$ denote the endomorphism ring of the vector space V, with unit id_V. Recall that a ring R with unit is (von Neumann) regular if for any $a \in R$ there is $x \in R$ such that $axa = a$; equivalently, any of its principal right ideals is generated by an idempotent. Then the principal right ideals form a sublattice $\mathsf{L}(R)$ of the lattice of all right ideals. The analogues hold on the left. In particular, the endomorphism ring $R = \mathsf{End}(V)$ of a finite dimensional F-vector space V is regular and one has $\mathsf{L}(R) \cong \mathrm{L}_0^1(V)$ via $\varphi R \mapsto \mathsf{im}\,\varphi$.

Fact 14. *For any idempotents e, f, g in a regular ring R one has*

$$\begin{array}{rcl} eR \subseteq fR & \Leftrightarrow & fe = e \\ eR = fR & \Leftrightarrow & fe = e \wedge ef = f \\ gR = eR + fR & \Leftrightarrow & ge = e \wedge gf = f \wedge \exists r \exists s.\, g = er + fs \\ gR = eR \cap fR & \Leftrightarrow & eg = fg = g \wedge \exists r \exists s.\, 1 - g = r(1-e) + s(1-f). \end{array}$$

Proof. The first claims are obvious, the last one follows from $R(1-g) = R(1-e) + R(1-f)$ and the fact that the latter means $gR = eR \cap fR$ [14, Lemma II.2.3]. □

Corollary 15. *The satisfiability problem for* $\{\mathsf{End}(V) \mid V \in \mathcal{V}\}$ *is unsolvable.*

Proof. Given any signature, call an equation *basic* if it is of the form $y = f(\bar{x})$, f an operation symbol, or $y = x$. Then, for any $t(\bar{x})$ and new variable y one may choose new variables $\bar{z}$ such that $y = t(\bar{x})$ is logically equivalent to some $\exists \bar{z}.\, \varphi(y, \bar{x}, \bar{z})$ where φ is a conjunction of basic equations (actually, one introduces new variables to denote intermediate values). Thus, any equation $t(\bar{x}) = s(\bar{x})$ is logically equivalent to some $\exists \bar{z}.\, \psi(\bar{x}, \bar{z})$, ψ a conjunction of basic equations with new variables $\bar{z}$. Apply this to given lattice equations; associate with each lattice variable x, occurring in the formulas so obtained, a ring variable $\hat{x}$ and let χ be the conjunction of all equations $\hat{x}^2 = \hat{x}$ capturing idempotency. Use Fact 14 to replace basic lattice equations by existentially quantified conjunctions of ring equations e.g. $z = x \cap y$ by

$$\exists u \exists v\, \big(\hat{x}\hat{z} = \hat{y}\hat{z} = \hat{z} \wedge 1 - \hat{z} = u(1-\hat{x}) + v(1-\hat{y})\big)$$

with new rings variables u, v. In this way, from any lattice equation $\varphi(x_1, \ldots, x_n)$ one obtains a positive primitive ring formula $\hat{\varphi}(\hat{x}_1, \ldots, \hat{x}_n)$ such that φ has a satisfying assignment in $\mathsf{L}(\mathsf{End}(V))$ if and only if $\hat{\varphi} \wedge \chi$ has a satisfying assignment in $\mathsf{End}(V)$. Thus, the problem in Theorem 2 reduces to that in the corollary which proves undecidability of the latter. □

3.6. **Ortholattices.** If V is a finite dimensional vector space over a field with involution $r \mapsto r^\dagger$ and endowed with an anisotropic †-hermitean form, then $\mathrm{L}_0^1(V)$ becomes a (modular) *ortholattice* $\mathrm{L}^\perp(V)$ with *orthocomplementation* $U \mapsto U^\perp$. Moreover, $\mathsf{End}(V)$ becomes a $*$-ring $\mathsf{End}^\dagger(V)$ under the involution $f \mapsto f^\dagger$, the adjoint of f w.r.t. the given form. Let $\mathcal{V}^\dagger$ a class of such spaces having reduct $\mathcal{V}$. By Theorem 2 and Corollary 15 one has the following.

Corollary 16. *Then the satisfiability problems for* $\{\mathrm{L}^\perp(V) \mid V \in \mathcal{V}^\dagger\}$ *and* $\{\mathsf{End}^\dagger(V) \mid V \in \mathcal{V}^\dagger\}$ *are unsolvable.*

A particular feature of the theory of these ortholattices is the following; thus, Corollary 16 answers the question left open in [10, §III.C].

Fact 17. *Within the class of all modular ortholattices any conjunction of equations* $s_i = t_i$ *is equivalent to one of the form* $t = \mathbf{1}$.

Proof. Observe that the following are equivalent for any given x, y: $x + x^\perp y^\perp = \mathbf{1}$; $x^\perp = x^\perp(x + x^\perp y^\perp)$; $x^\perp = xx^\perp + x^\perp y^\perp$ (by modularity); $x^\perp \leq y^\perp$; $y \leq x$. □

Corollary 18. *The satisfiability problem for* $\{\mathrm{L}^\perp(V) \mid V \in \mathcal{V}^\dagger\}$ *and equations* $t(\bar{x}) = \mathbf{1}$ *with* 6*-variable terms* $t(\bar{x})$ *is unsolvable.*

Proof. It remains to reduce the number of ortholattice variables. First, assume that for any $F \in \mathcal{F}$ and any d there is a d-dimensional space over F in $\mathcal{V}^{\dagger}$. The concept of k-frame generalizes from $k = 3$ to arbitrary k, obviously (cf. [2]). Recall from [6] that the modular lattice freely generated by a $k+1$-frame is finitely presented as a modular lattice with four generators. Thus, we have terms $\bar{b}(\bar{y})$, $\bar{y} = (y_1, y_2, y_3, y_4)$, and finitely many relations such that $\bar{b}(\bar{E})$ is a $k+1$-frame $\bar{B}$ for any $\bar{E}$ in any $\mathrm{L}_0^1(V)$ satisfying the relations. Dealing with a group presentation with k generators $\bar{x}$ we use a $k+1$-frame $\bar{B}$ to encode these into a single lattice element, as follows. Let the 3-frame $\bar{A}$ given by the B_i, B_{1j}, $i, j \leq 3$ and $L' = [0, \sum_i A_i]$. Then the x_i define $g_i \in R(L', \bar{A})$. Let $B_{2j} = (B_2 + B_j) \cap (B_{12} + B_{1j})$ and $g_i' = (B_1 + B_{i+1}) \cap (B_{2\,i+1} + g_i)$. Then $g_i = (B_1 + B_{i+1}) \cap (B_{2\,i+1} + g_i')$ and $g_i' = (B_1 + B_{i+1}) \cap E$ where $E_5 = \sum_{j=2}^{k+1} g_j'$. Introducing the variable y_5 for the latter, this yields the conjunction ψ of 5-variable lattice relations replacing $\hat{\pi} \wedge \pi^{\#}$ from Lemma 6. Now combine ψ into $t = \mathbf{1}$ via Fact 17.

In the general case, one has to consider skew $k+1$-frames as in the proof of Theorem 2; since A_0 may be chosen as $(\sum_{i=1}^{k+1} A_i)^{\perp}$ only one additional variable is needed to denote A_{10}. □

Acknowledgments

The present work was supported in parts by the *German Research Foundation* (DFG) with project Zi 1009/4-1; by *7th EU IRSES* project 294962; and by the *German Academic Exchange Service* (DAAD) under codenumber 91532398-50015537.

References

[1] M.R. Bridson, H. Wilton, The triviality problem for profinite completions, to appear in *Invent.Math,*, arXiv1401.2273v3.

[2] R. Freese, Projective geometries as projective modular lattices, *Trans. Amer. Math. Soc.* **251** (1979) 329–342.

[3] R. Freese, Free modular lattices, *Trans. Amer. Math. Soc.* **261** (1980) 81–91.

[4] R.M. Guralnick, W.M. Kantor, M.Kassabov, A.Lubotzky, Presentations of finite simple groups: A computational approach, *J. Eur. Math. Soc.* **13** (2011) 391–458.

[5] M. Hannula, J. Kontinen, A finite axiomatization of conditional independence and inclusion axioms, to appear in *Information and Computation.*

[6] C. Herrmann, Rahmen und erzeugende Quadrupel in modularen Verbänden, *Algebra Universalis* **14** (1982) 357–387.

[7] C. Herrmann, On the arithmetic of projective coordinate systems, *Trans. Amer. Math. Soc.* **284**(2) (1984)759–785.

[8] C. Herrmann. Frames of permuting equivalences. *Acta Sci. Math.* **51**(1-2) :93–101, 1987.

[9] C. Herrmann, On the undecidability of implications between embedded multivalued database dependencies, *Informtion and Computation* **122** (1995) 221–235.

[10] C. Herrmann, M. Ziegler, Computational complexity of quantum satisfiability, *Proc. 26th Annual IEEE Symposium on Logic in Computer Science* (2011) 175–184.

[11] C. Herrmann, M. Ziegler, Computational complexity of quantum satisfiability, `arXiv:1004.1696`.

[12] O.G. Kharlampovich, M.V. Sapir. Algorithmic problems in varieties. *Internat. J. Algebra Comput.* **5**(4–5) (1995) 379–602.

[13] L. Lipshitz, The undecidability of the word problems for projective geometries and modular lattices, *Trans. Amer. Math. Soc.* **193** (1974) 171–180.

[14] J.von Neumann. *Continuous Geometry* (Princeton Math.Series no.25, 1960).

[15] A.M. Slobodskoi, Undecidability of the universal theory of finite groups, *Algebra i Logika* **20**(2) (1981) 207–230.

[16] B. Sturmfels, *Algorithms in Invariant Theory* (Springer, New York, 2008).

[17] A. Wiman, Ueber die Darstellung der symmetrischen und alternirenden Vertauschungsgruppen als Collineationsgruppen von möglichst geringer Dimensionenzahl, *Math.Ann.* **52**(2-3) (1899) 243–27.

(Christian Herrmann) Technische Universität Darmstadt FB4, Schlossgartenstr. 7, 64289 Darmstadt, Germany

E-mail address: `herrmann@mathematik.tu-darmstadt.de`

([Yasuyuki Tsukamoto) Department of Mathematics, Faculty of Science, Kyoto University, Kitashirakawa Oiwake-cho, Sakyo-ku, Kyoto 606-8502, Japan

E-mail address: `tsukamoto@i.h.kyoto-u.ac.jp`

(Martin Ziegler) Technische Universität Darmstadt FB4, Schlossgartenstr. 7, 64289 Darmstadt, Germany

E-mail address: `m@zie.de`