International Journal of Algebra and Computation
Vol. 26, No. 8 (2016) 1573–1595
© World Scientific Publishing Company
DOI: 10.1142/S0218196716500697

World Scientific
www.worldscientific.com

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

On the consistency problem for modular lattices and related structures

Christian Herrmann

Technische Universität Darmstadt
FB4 Schloßgartenstr. 7
64289 Darmstadt, Germany
herrmann@mathematik.tu-darmstadt.de

Yasuyuki Tsukamoto

Hakuryo High School
2260 Amida-cho Amida, Takasago-shi
Hyogo 676-0827, Japan
xa74528@ba2.so-net.ne.jp

Martin Ziegler

KAIST, School of Computing
291 Daehak-ro, Yuseong-gu, 34141
Daejeon, Republic of Korea
ziegler@cs.kaist.ac.kr

Received 3 June 2016
Accepted 27 October 2016
Published 12 December 2016

Communicated by K. Kearnes

The consistency problem for a class of algebraic structures asks for an algorithm to decide, for any given conjunction of equations, whether it admits a non-trivial satisfying assignment within some member of the class. For the variety of all groups, this is the complement of the triviality problem, shown undecidable by by Adyan [Algorithmic unsolvability of problems of recognition of certain properties of groups. (Russian) *Dokl. Akad. Nauk SSSR* (*N.S.*) **103** (1955) 533–535] and Rabin [Recursive unsolvability of group theoretic problems, *Ann. of Math. (2)* **67** (1958) 172–194]. For the class of finite groups, it amounts to the triviality problem for profinite completions, shown undecidable by Bridson and Wilton [The triviality problem for profinite completions, *Invent. Math.* **202** (2015) 839–874]. We derive unsolvability of the consistency problem for the class of (finite) modular lattices and various subclasses; in particular, the class of all subspace lattices of finite-dimensional vector spaces over a fixed or arbitrary field of characteristic 0 and expansions thereof, e.g. the class of subspace ortholattices of finite-dimensional Hilbert spaces. The lattice results are used to prove unsolvability of the consistency problem for (finite) rings with unit and (finite) representable relation algebras. These

results in turn apply to equations between simple expressions in Grassmann–Cayley algebra and to functional and embedded multivalued dependencies in databases.

Keywords: Consistency problem; triviality problem; satisfiability; decidability; subspace lattice; endomorphism ring; relation algebra; database dependencies; Grassmann–Cayley algebra.

Mathematics Subject Classification: Primary: 08A50; Secondary: 03B25, 03G15, 06C05, 15A75.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

1. Introduction

The well-known Boolean satisfiability problem asks to decide, given any Boolean term $t(\bar{x})$ in any (number of) variables $\bar{x} = (x_1, \ldots, x_n)$, whether there is an assignment $\bar{x} \mapsto \bar{a}$ within the 2-element (equivalently: some non-singleton) Boolean algebra B, such that $B \models t(\bar{a}) = 1$. This is the prototype of an NP-complete problem. In [19, 20], as an approach to "Modular Quantum Logic" and in analogy to the Boolean case, we have considered the complexity of deciding $\exists\, \bar{x}\ t(\bar{x}) = 1$ in ortholattices $L_d = L^{\perp}(\mathbb{C}^d)$ of subspaces of Hilbert spaces $\mathbb{C}^d$ where $0 < d < \aleph_0$. For fixed d, the problem turned out NP-complete if $d = 1, 2$, complete for a prominent complexity class of real computation, independent of d, if $d > 2$. The problem to decide whether, for given t, there is some $d > 0$ such that $L_d \models \exists\, \bar{x}\ t(\bar{x}) = 1$ was called "strong quantum satisfiability in indefinite dimension" in [19, §III.C] and shown hard for this complexity class; also, a sequence t_k of terms of length $\mathcal{O}(k)$ was constructed such that t_k is satisfiable in L_d only for some $d \geq 2^k$. It remained open, whether the problem is at least decidable.

Here, we show that this is not the case (Corollary 28 in Sec. 8). The proof is based on the undecidability of the triviality problem for profinite completions of groups, a recent deep result due to Bridson and Wilton [5]. The triviality problem for groups, shown undecidable by Adyan [2, 3] and Rabin [30], asks, given a finite list $\bar{g}$ of generator symbols and a conjunction of "relations" (that is, equations $t(\bar{g}) = e$)), whether the group G (freely) given by this presentation is singleton; its "profinite variant" asks whether the profinite completion of G is singleton.

Using these results, we obtain unsolvability of various "triviality problems" for classes of modular lattices and related structures. We prefer to deal with the complementary counterparts: For a class $\mathcal{C}$ of algebraic structures with given finite list of operation symbols, the *consistency problem* asks to decide, given a conjunction $\pi(\bar{x})$ of equations in variables $\bar{x} = (x_1, \ldots, x_n)$, whether there is $A \in \mathcal{C}$ and an assignment $\bar{x} \mapsto \bar{a}$ in A such that $A \models \pi(\bar{a})$ and the $a_1, \ldots, a_n$ generate a non-singleton subalgebra of A.

We show the consistency problem unsolvable e.g. for each of the following classes and its subclass of finite members: modular lattices (our basic result in Sec. 4); representable relation algebras (Sec. 5); rings with unit (Sec. 7). Related problems, shown to be undecidable, concern simple expressions in Grassmann–Cayley algebra (Sec. 9) and functional and embedded multivalued database dependencies (Sec. 6).

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

Sections 5 and 6 are not needed in the subsequent sections. Section 2 presents our central tool: (von Neumann) frames and coordinatization, as used by Lipshitz [26] and Freese [6] to show unsolvability of word problems. Section 3 explains general concepts and facts and recalls the results for groups.

2. Coordinates in Modular Lattices

We consider lattices as algebraic structures with operations join $a+b$ and meet $a\cap b$; in particular, with respect to a suitable partial order $\leq$, one has $a+b=\sup\{a,b\}$ and $a\cap b=\inf\{a,b\}$. A lattice is *modular* if $a\geq b$ implies $a\cap(b+c)=b+a\cap c$. Let $\mathcal{M}_f$ denote the class of all finite modular lattices. The lattice of all equivalence relations on the set S is denoted by $\mathrm{Eq}(S)$. A sublattice L of the latter is a *lattice of permuting equivalences* if, for the relational product $\alpha\circ\beta=\{(x,z):\exists\, y.(x,y)\in\alpha,(y,z)\in\beta\}$, of all $\alpha,\beta\in L$, one has $\alpha\circ\beta=\beta\circ\alpha$; that is, $\alpha\circ\beta$ is the join $\alpha+\beta$ in $\mathrm{Eq}(S)$ and L and, in particular, transitive. In that case, L is a modular lattice [22]. The lattices $L(V)$ of all linear subspaces of the vector space V are isomorphic to such: associate with a subspace U the equivalence relation on V defined by $x-y\in U$. Bounds of a lattice, if considered as constants, will be denoted by 0 (bottom) and 1 (top); in case of $L(V)$ these are $\{0\}$ and V. We write $a\oplus b=c$ if $a+b=c$ and $a\cap b=0$.

An *n-frame in* a lattice L is a system $\bar{a}$ of elements $a_1,\ldots,a_n$, $a_{ij}=a_{ji}(1\leq i<j\leq n)$, and $a_\perp,a_\top$ of L such that, where $\sum_{i\in\emptyset}a_i:=a_\perp$,

$$\left(\sum_{i\in I}a_i\right)\cap\sum_{j\in J}a_j=\sum_{k\in I\cap J}a_k\quad\text{for } I,J\subseteq\{1,\ldots,n\}$$

$a_\top=\sum_\ell a_\ell$, and, for pairwise distinct i,j,k,

$$a_i+a_j=a_i+a_{ij},\quad a_i\cap a_{ij}=a_\perp,\quad a_{ik}=(a_i+a_k)\cap(a_{ij}+a_{jk}).$$

Define

$$G(L,\bar{a})=\{g\in L\mid g+a_1=g+a_2=a_1+a_2,\ g\cap a_1=g\cap a_2=a_\perp\}.$$

If L has bounds $0,1$ and if $a_\perp=0$ and $a_\top=1$ then we speak of an *n-frame of* L. We use $\bar{z}$ to denote a system of variables to be interpreted by 4-frames. Items (i)–(iii)(b) of the following are well known in a broader context [29, 4, 26, 6]; our modest amendment of Item (iv) will turn out as crucial to establish Lemma 10 below. All can be generalized to each fixed $n\geq 4$. We state and prove what is relevant, here. We say that a subgroup G of $\mathrm{GL}(V)$ *acts fixed point free* if $gv=v$ for all $g\in G$ only if $v=0$.

Lemma 1. (i) *For each vector space V with $\dim V=nd$, d any cardinal, and subspace V_1 of V of $\dim V_1=d$ there is a n-frame $\bar{a}$ of $L(V)$ such that $a_1=V_1$.*

(ii) *For each n-frame $\bar{a}$ in a modular lattice, $a_\perp=a_{12}$ implies $a_\perp=a_\top$.*

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

(iii) *There is a lattice term* $t(x, y, \bar{z})$ *such that for each modular lattice* L *and* 4*-frame* $\bar{a}$ *in* L *the following hold*:

(a) $G(L, \bar{a})$ *is a group under the multiplication* $(g, h) \mapsto t(g, h, \bar{a})$ *and with neutral element* a_{12}.

(b) *If* V *is a vector space and* $L = L(V)$, *then there is a unique isomorphism* $\varepsilon_{\bar{a}} : a_1 \to a_2$ *such that* $\Gamma_{\bar{a}}(f) := \{v - \varepsilon_{\bar{a}}(f(v)) \mid v \in a_1\}$ *defines an isomorphism of* $\mathrm{GL}(a_1)$ *onto* $G(L, \bar{a})$.

(c) *In* (*b*), *the subgroup* G *generated by* $f_1, \ldots, f_k$ *in* $\mathrm{GL}(a_1)$ *acts fixed point free on* $V_1 = a_1$ *if and only if* $a_{12} \cap \bigcap_{i=1}^{k} g_i = a_\perp$ *where* $g_i = \Gamma_{\bar{a}}(f_i)$.

(iv) *With each conjunction* $\pi(\bar{x})$ *of group equations one can effectively associate a conjunction* $\pi^{\#}(\bar{x}, \bar{z})$ *of lattice equations such that for each modular lattice* L *and* $\bar{g} = (g_1, \ldots, g_k)$ *and* $\bar{a}$ *in* L *one has* $L \models \pi^{\#}(\bar{g}, \bar{a})$ *if and only if* $\bar{a}$ *is a* 4*-frame in* L, $\bar{g}$ *in* $G(L, \bar{a})$, $G(L, \bar{a}) \models \pi(\bar{g})$, *and* $a_{12} \cap \bigcap_{i=1}^{k} g_i = a_\perp$.

Proof. (i) We may assume $V = \bigoplus_{i=1}^{n} V_i$ with isomorphisms $\varepsilon_j : V_1 \to V_j$ for $j > 1$. Put $a_i = V_i$, $a_{1j} = \{v - \varepsilon_j(v) \mid v \in V_1\}$ and $a_{kj} = (a_k + a_j) \cap (a_{1k} + a_{1j})$ for $j \neq k$ in $\{2, \ldots, n\}$.

(ii) Given a n-frame $\bar{a}$ in L, we may assume $a_\perp = 0$ and $a_\top = 1$. For readability, we write meets as $a \cap b = ab$. Now, if $a_{12} = 0$, then $a_1 = a_1(a_{12} + a_2) = a_1 a_2 = 0$ and then $a_j = a_j(a_1 + a_{1j}) = a_j a_{1j} = 0$ for all $j > 1$. Thus $a_\top = 0$.

(iii) We deal with an arbitrary 4-frame $\bar{a}$, uniformly, so that it is obvious which terms govern the construction. Again, we may assume $a_\perp = 0$ and $a_\top = 1$. Let $a_i' = \sum_{j \neq i} a_j$ and observe that, for $i \neq k$, $a_{ik} \oplus a_i' = 1$. By modularity, $x \mapsto x + a_{ik}$ and $y \mapsto y a_i'$ are isomorphisms $[0, a_k'] \to [a_{ik}, 1]$ and $[a_{ik}, 1] \to [0, a_i']$ between intervals and compose to the isomorphism $\pi_k^i : [0, a_k'] \to [0, a_i']$, that is $\pi_k^i(x) = (x + a_{ik})a_i'$, with inverse π_i^k. Observe that $\pi_k^i(a_i) = a_k$ and $\pi_k^i(a_{ij}) = a_{kj}$ for $j \neq i, k$. Moreover, π_k^i is identity on $[0, \sum_{j \neq i,k} a_j]$; indeed, by modularity, $(x + a_{ik})a_i' = x + a_{ik}a_i' = x$ if $x \leq a_i'$.

Now, let $G_{ij} = \{x \in L \mid a_i \oplus x = a_j \oplus x = a_i + a_j\}$ for $i \neq j$ and observe that π_k^i restricts to a bijection $\pi_{kj}^{ij} : G_{ij} \to G_{kj}$ for $k \neq i, j$. Observe that for $x \in G_{ij}$, one has $xa_i' = x(a_i + a_j)a_i' = xa_j = 0$ and, similarly, $xa_j' = 0$.

For $r \in G_{12}$ define $r_{12} = r$, $r_{1j} = \pi_j^2(r) \in G_{1j}$ and $r_{ij} = \pi_i^1(r_{1j}) \in G_{ij}$ where $1 < i < j$. Observe that, for $r = a_{12}$, this is consistent with the notation for the a_{ij}. Given $r, s \in G_{12}$ one has $x = (r_{12} + s_{23})(a_1 + a_3) \in G_{13}$. Namely, by modularity, $xa_1 = [r_{12} + s_{23}(a_1 + a_2)]a_1 = r_{12}a_1 = 0$, $x + a_1 = (r_{12} + a_1 + s_{23})(a_1 + a_3) = (a_1 + a_2 + s_{23})(a_1 + a_3) = (a_1 + a_2 + a_3)(a_1 + a_3) = a_1 + a_3$, and, similarly, $xa_3 = 0$ and $x + a_3 = a_1 + a_3$. Thus, one obtains a well-defined multiplication on G_{12} such that

$$r \otimes s = t \Leftrightarrow (r_{12} + s_{23})(a_1 + a_3) = t_{13}.$$

a_{12} is a right unit since $(r_{12} + a_{23})(a_1 + a_3) = \pi_3^2(r) = r_{13}$. Given $r \in G_{12}$ has image $s = \pi_2^3 \pi_1^2 \pi_3^1(r)$ in G_{12} and, applying the inverse maps, it follows $s_{23} = \pi_2^1 \pi_3^2(s) = \pi_3^1(r)$. Thus, by modularity, $(r_{12} + s_{23})(a_1 + a_3) = [r + (r + a_{13})(a_2 + a_3)](a_1 + a_3) =$

$(r + a_{13})(r + a_2 + a_3)(a_1 + a_3) = [r(a_1 + a_3) + a_{13}](a_1 + a_2 + a_3) = a_{13}$ which shows that s is a right inverse of r.

In order to establish G_{12} as a group, it remains to prove associativity. Preparing for this, we show for pairwise distinct i, j, k, h

$$\pi^{kj}_{hj}\pi^{ij}_{kj} = \pi^{ij}_{hj}, \quad \pi^{jk}_{hk}\pi^{ij}_{kj} = \pi^{ih}_{kh}\pi^{ji}_{hi}.$$

Indeed, for $x \in G_{ij}$, modularity yields $[(x + a_{ik})(a_j + a_k) + a_{kh}](a_j + a_h) = [(x + a_{ik})(a_j + a_k + a_h) + a_{kh}](a_j + a_h) = (x + a_{ik} + a_{kh})(a_j + a_h) = [x + (a_{ik} + a_{kh})(a_j + a_i + a_h)](a_j + a_h) = (x + a_{ih})(a_i + a_h)$ and $[(x + a_{ik})(a_j + a_k) + a_{jh}](a_h + a_k) = [(x + a_{ik})(a_j + a_k + a_h) + a_{jh}](a_h + a_k) = (x + a_{ik} + a_{jh})(a_h + a_k) = \cdots = [(x + a_{jh})(a_i + a_h) + a_{ik}](a_h + a_k)$.

We now claim that for $r, s, t \in G_{12}$ the following relations are equivalent

$$\begin{aligned}(r_{12} + s_{23})(a_1 + a_3) &= t_{13}\\ (r_{12} + s_{24})(a_1 + a_4) &= t_{14}\\ (r_{13} + s_{34})(a_1 + a_4) &= t_{14}\\ (r_{23} + s_{34})(a_2 + a_4) &= t_{24}\end{aligned}$$

whence each equivalent to $t = r \otimes s$. Namely, the pairs of consecutive relations are equivalent via the isomorphisms π^3_4, π^2_3, and π^1_2, respectively, which match the elements associated with r and, similarly, for s and t. Indeed, $\pi^3_4(s_{23}) = \pi^3_4\pi^1_2\pi^2_3(s_{12}) = \pi^1_2\pi^3_4\pi^2_3(s_{12}) = \pi^1_2\pi^2_4(s_{12}) = s_{24}$, $\pi^3_4(t_{13}) = \pi^3_4\pi^2_3(t_{12}) = \pi^2_4(t_{12}) = t_{14}$, $\pi^2_3(s_{24}) = \pi^2_3\pi^1_2\pi^2_4(s_{12}) = \pi^1_3\pi^2_4(s_{12}) = s_{34}$, while the remaining equalities are obvious.

Now, for $r, s, t \in G_{12}$, it follows by modularity $[(r \otimes s) \otimes t]_{14} = [(r \otimes s)_{13} + t_{34}](a_1 + a_4) = [(r_{12} + s_{23})(a_1 + a_3) + t_{34}](a_1 + a_4) = [(r_{12} + s_{23})(a_1 + a_3 + a_4) + t_{34}](a_1 + a_4) = (r_{12} + s_{23} + t_{34})(a_1 + a_4) = [(r_{12} + (s_{23} + t_{34})(a_1 + a_2 + a_4)](a_1 + a_4) = [(r_{12} + (s \otimes t)_{24}](a_1 + a_4) = [r \otimes (s \otimes t)]_{14}$.

Observe that $G_{12} = G(L, \bar{a})$ as sets. We turn $G(L, \bar{a})$ into the group opposite to G_{12} defining multiplication as $(g, h) \mapsto t(g, h, \bar{a})$, where $t(x, y, \bar{z})$ is the term $([y + ((x + z_{23})(z_1 + z_3) + z_{12})(z_2 + z_3)](z_1 + z_3) + z_{23})(z_1 + z_2)$.

In (b), observe that for all pairs $i \neq j$ there is a 1-1-correspondence between elements $r \in G_{ij}$ and isomorphisms $f : a_i \to a_j$ given by $f(v) = w$ if and only if $v - w \in r$. We write $f = \hat{r}$. For $s \in G_{jk}$ and $t = (r + s) \cap (a_i + a_k)$ it follows $\hat{t} = \hat{s} \circ \hat{r}$. In particular, we have the $\hat{a}_{ij} : a_i \to a_j$ with $\hat{a}_{ji} = \hat{a}^{-1}_{ij}$ and $\hat{a}_{jk} \circ \hat{a}_{ij} = \hat{a}_{ik}$. We have to put $\varepsilon_{\bar{a}} = \hat{a}_{12}$. Now, given $g, h \in GL(a_1)$ and $r = \Gamma_{\bar{a}}(g)$, $s = \Gamma_{\bar{a}}(h)$ one has $\hat{r}_{12} = \hat{a}_{12} \circ g$ and $\hat{s}_{23} = \hat{a}_{23} \circ \hat{a}_{12} \circ h \circ \hat{a}_{21} = \hat{a}_{13} \circ h \circ \hat{a}_{21}$ whence, for $t = r \otimes s$, $\hat{t}_{13} = \hat{s}_{23} \circ \hat{r}_{12} = \hat{a}_{13} \circ h \circ g$ and $\hat{t} = \hat{a}_{31} \circ \hat{t}_{13} = h \circ g$.

(c) Define

$$U = a_{12} \cap \bigcap_{i=1}^{k} g_i = \{v - \varepsilon_{\bar{a}}(v) \mid v \in V_1\} \cap \bigcap_{i=1}^{k} \{v - \varepsilon_{\bar{a}}(f_i v) \mid v \in V_1\}.$$

Consider v such that $v - \varepsilon_{\bar{a}} v \in U$. For every generator f_i of G there is some $w \in V_1$ such that $v - \varepsilon_{\bar{a}}(v) = w - \varepsilon_{\bar{a}}(f_i w)$ whence $w = v$ and $v = f_i v$ since the

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

sum $a_1 \oplus a_2$ is direct. Thus, v is fixed under the action of G on V_1. Conversely, if $v = f_i v$ for all i then $v - \varepsilon_{\bar{a}} v \in U$. Now, observe that $U = 0$ if and only if $\{v \in V_1 \mid v - \varepsilon_{\bar{a}}(v) \in U\} = 0$.

(iv) Is obvious by (iii). □

The following is used to establish the sufficient condition in Lemma 1 (iii)(c). Supposedly, it is well known. To some extend it could be replaced by use of Maschke's Theorem. For a vector space V over a division ring F of characteristic c we write $\chi(F) = \chi(V) = c$. Let $\mathcal{V}_F$ denote the class of all F-vector spaces. A representation ρ of G in V is *fixed point free* if $\rho(g)(v) = v$ for all $g \in G$ only if $v = 0$.

Lemma 2. *Let G be a group and V a vector space where either* $\dim V \geq |G|$ *and G is infinite or* $\dim V = |G| - 1 > 0$ *is finite and $\chi(V)$ does not divide $|G|$. Then there exists a fixed point free faithful representation of G in V.*

Proof. For infinite G, and $\dim V = |G|$, we use the regular representation: We may assume G a basis of V and define $\rho(g)$ given by the basis permutation $h \mapsto gh$. The claim follows from the fact that this action of G on G is transitive: $v \neq 0$ in V has the form $v = \sum_{h \in H} r_h h$ with some finite $H \subseteq G$ and $r_h \neq 0$; choosing $k \in G \setminus H$, there is $g \in G$ with $gh = k$ whence $gv = \sum_{h \in H} r_h gh \neq v$. For $\dim V > |G|$, we use a suitable direct multiple of this representation.

For G the 2-element group $\{e, g\}$, define the action on V by $gv = -v$. For finite G of order > 2, again assuming G a basis of V, we have the 1-dimensional invariant subspace U spanned by $\sum_{g \in G} g$ and the induced action of G on V/U. The $g \in G^+ := G \setminus \{e\}$ form a basis of V/U; that is, each $v + U$ in V/U has a unique representation

$$v + U = \sum_{h \in G^+} r_h h + U = \left(\sum_{h \in G^+, gh \neq e} r_{gh} gh \right) + r_g g + U$$

for all $g \in G^+$, in particular,

$$e + U = \sum_{h \in G^+} -h + U = \left(\sum_{h \in G^+, gh \neq e} -gh \right) - g + U.$$

Thus, for $v + U = \sum_{h \in G^+} r_h h + U$ and $g \in G^+$, one has

$$\begin{aligned} g(v + U) &= \left(\sum_{h \in G^+, gh \neq e} r_h gh \right) - r_{g^{-1}} e + U \\ &= \left(\sum_{h \in G^+, gh \neq e} (r_h - r_{g^{-1}}) gh \right) - r_{g^{-1}} g + U \end{aligned}$$

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

and the last expression returns $g(v+U)$ as a linear combination of basis vectors of V/U. Assume $v+U=g(v+U)$ for all $g\in G$; that is, for all $g,h\in G^+$ one has $r_g=-r_{g^{-1}}$ and

$$r_{gh}=r_h-r_{g^{-1}}=r_h+r_g \quad \text{if } gh\neq e.$$

For all $h\in G^+$, it follows $r_{h^k}=kr_h$, by induction, for all $1\leq k<\ell$ where ℓ is the order of h; in particular, $-r_h=r_{h^{-1}}=r_{h^{\ell-1}}=(\ell-1)r_h$, whence $\ell r_h=0$ and $r_h=0$, due to the assumption on the characteristic. Thus, $v+U=0+U$. □

3. General Concepts

We consider (non-empty) classes $\mathcal{C}$ of algebraic structures with given finite list of operation symbols. Let $\mathsf{S}\mathcal{C}$ denote the class of all substructures of members of $\mathcal{C}$ and $\mathsf{P}\mathcal{C}$ the class consisting of all singleton structures and of all direct products $\prod_i A_i$ where $A_i\in\mathcal{C}$. The class $\mathcal{C}$ is a *quasi-variety* if it is definable by a set of quasi-identities: sentences of the form $\forall\,\bar{x}.\ \pi(\bar{x})\Rightarrow\psi(\bar{x})$, where $\pi(\bar{x})$ is a conjunction of equations, being possibly empty, and $\psi(\bar{x})$ a single equation (more conveniently, a conjunction of equations). Observe that $\mathsf{P}\mathcal{C}\subseteq\mathcal{C}$ and $\mathsf{S}\mathcal{C}\subseteq\mathcal{C}$ for a quasi-variety $\mathcal{C}$. Given a class $\mathcal{C}$, the smallest quasi-variety $\mathsf{Q}\mathcal{C}$ containing $\mathcal{C}$ (i.e. *generated by* $\mathcal{C}$) is the model class of the set of quasi-identities valid in $\mathcal{C}$.

Given a finite list $\bar{g}=(g_1,\ldots,g_n)$ of pairwise distinct constants not in the language of $\mathcal{C}$ (called *generator symbols*), let $\mathcal{C}^{\bar{g}}$ denote the expansion of $\mathcal{C}$ by these constants; that is, the members of $\mathcal{C}^{\bar{g}}$ are given as $(A,\bar{a})$ where $A\in\mathcal{C}$ and where $\bar{a}=(a_1,\ldots,a_n)$ determines the values of the generator symbols. Given a conjunction $\pi(\bar{x})$ of equations in the (pairwise distinct) variables x_i from $\bar{x}=(x_1,\ldots,x_n)$, (all of which occur, be it in a conjunct $x_i=x_i$), we obtain $\pi(\bar{g})$ substituting g_i for x_i and speak of a finite *list of relations*. $(A,\bar{a})$ *satisfies* these relations if $A\models\pi(\bar{a})$, that is, if the a_i constitute a *satisfying assignment* for $\pi(\bar{x})$ respectively $\pi(\bar{g})$ — in case $A\in\mathcal{C}$ we speak also of a satisfying assignment *within* $\mathcal{C}$. Let $C_A(\bar{a})$ denote the subalgebra of A generated by the a_i; we call the assignment *non-trivial* if $C_A(\bar{a})$ is non-singleton; we call $(A,\bar{a})$ a *model* of $\pi(\bar{g})$ if $A\models\pi(\bar{a})$ and $C_A(\bar{a})=A$. Let $\mathsf{Mod}(\pi(\bar{g});\mathcal{C})$ consist of all models of $\pi(\bar{g})$ with $A\in\mathsf{S}\mathcal{C}$.

Fact 3. Given $\mathcal{C}$ and $\pi(\bar{g})$, there is a member $(F,\bar{g}^F)$ of $\mathsf{SPMod}(\pi(\bar{g});\mathcal{C})$, unique up to isomorphism, such that F is generated by $\bar{g}^F$ and such that for every $(A,\bar{a})\in\mathsf{Mod}(\pi(\bar{g});\mathcal{C})$ there is a (unique) homomorphism $\varphi:(F,\bar{g}^F)\to(A,\bar{a})$. Moreover, $(F,\bar{g}^F)$ is a model of $\pi(\bar{g})$ and for any quasi-variety $\mathcal{Q}\supseteq\mathcal{C}$, it is the inverse limit of those quotients of $F(\mathcal{Q};\pi(\bar{g}))$ which are in $(\mathsf{S}\mathcal{C})^{\bar{g}}$ (w.r.t. all homomorphisms between these).

This is well known and easy to prove: Choose a copy from any isomorphism type in $\mathsf{Mod}(\pi(\bar{g});\mathcal{C})$, form the direct product $(B,\bar{b})$ of these and let F the substructure generated by $\bar{b}=:\bar{g}^F$. We refer to $(F,\bar{g}^F)$ as *given by the presentation* $\pi(\bar{g})$ *relatively to* $\mathcal{C}$ and denote it by $F(\mathcal{C};\pi(\bar{g}))$.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

We just mention some examples of lattices given by a presentation relatively to some class of lattices. Given a finite partially ordered set P, consider the elements as generator symbols and let $\pi(\bar{g})$ the conjunction of all equations $p + q = q$ where $p \leq q$ in P. According to Wille [34], such presentation has the 2-element lattice D_2 and the 5-element height 2 lattice M_3 as its only possible subdirectly irreducible modular models if and only if P has no 4 pairwise incomparable elements and no subset with induced order isomorphic to the disjoint union of two 2-element chains and a singleton. Thus, given such P, for any class $\mathcal{C}$ of modular lattices containing D_2 and M_3 one has the same finite $F(\mathcal{C}; P)$. In contrast, considering for fixed n the concept of n-frame as a presentation (the g_{ij} denoting the elements of the frame and $\pi(\bar{g})$ capturing the defining relations) then $F(\mathcal{C}, \pi(\bar{g}))$ depends strongly on $\mathcal{C}$ unless $n \leq 2$: if $\mathcal{C}$ consists just of a single $L(V)$, V a D-vector space, then $F(\mathcal{C}, \pi(\bar{g}))$ is singleton if $\dim V < n$, isomorphic to $L(P_P^n)$ where P is the prime subfield of D, otherwise. If $n \geq 4$ and $\mathcal{C}$ the class of all modular lattices, then the finite subdirectly irreducible members of $\mathsf{Mod}(\pi(\bar{g}); \mathcal{C})$ are the subgroup lattices of C^n, C ranging over all cyclic groups of prime power order; there are also infinite subdirectly irreducibles but $F(\mathcal{C}, \pi(\bar{g}))$ is the same for the class of all modular lattices and its subclass of finite ones [16]. Freese [7] gives a presentation which has infinite modular models but only trivial finite ones.

Preparing for the principal definition in this paper, we list conditions each of which can be used — being obviously pairwise equivalent or negations of each other.

Fact 4. For any $\mathcal{C}$ with nullary operation symbols $c_1, \ldots, c_m$, any $\pi(\bar{x})$ and $\pi(\bar{g})$ as above, and any quasi-variety $\mathcal{Q} \supseteq \mathcal{C}$ the following conditions (i)–(iv) are pairwise equivalent; so are (v)–(vii); (v) is equivalent to the negation of (i).

(i) $F(\mathcal{C}; \pi(\bar{g}))$ is singleton.
(ii) $\mathsf{Mod}(\pi(\bar{g}); \mathcal{C})$ has singleton members, only.
(iii) Every $A \in \mathcal{C}$ is a model of the following quasi-identity (where Ω is the set of operation symbols).

$$\forall \bar{x}.\pi(\bar{x}) \Rightarrow \left(\bigwedge_{i=2}^{n} x_i = x_1 \wedge \bigwedge_{f \in \Omega} f(x_1, \ldots, x_1) = x_1 \right) \quad \text{if } n > 0$$

$$\pi \Rightarrow \left(\bigwedge_{i=2}^{m} c_i = c_1 \wedge \bigwedge_{f \in \Omega} f(c_1, \ldots, c_1) = c_1 \right) \quad \text{if } n = 0.$$

(iv) All homomorphic images of $F(\mathcal{Q}; \pi(\bar{g}))$ in $\mathcal{C}$ are singleton.
(v) There is a satisfying assignment $\bar{x} \mapsto \bar{a}$ in some $A \in \mathcal{C}$ such that the a_i generate a non-singleton subalgebra of A.
(vi) There are terms $t_i(\bar{x})$ such that $\exists \bar{x}.\pi(\bar{x}) \wedge t_1(\bar{x}) \neq t_2(\bar{x})$ is valid in some member of $\mathcal{C}$.
(vii) Within some $A \in \mathcal{C}$, there is a satisfying assignment $\bar{x} \mapsto \bar{a}$ failing some equation in the language of $\mathcal{C}$.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

A solution of the *consistency problem* for $\mathcal{C}$ consists in an algorithm which decides for any given $\pi(\bar{x})$ whether $\mathsf{Mod}(\pi(\bar{g}); \mathcal{C})$ has some non-singleton member ((vii) suggests how to define the consistency problem for more general structures and constraints, cf. Sec. 6). In case of a quasi-variety $\mathcal{C}$, the complement of this problem is commonly called the *triviality problem* for $\mathcal{C}$. Unsolvability for the classes of structures to be considered, here, is shown by reducing from the following deep results of Adyan [2, 3], Rabin [30] and Bridson and Wilton [5]. We refer of (i) in the case of groups, to (iv) with $\mathcal{Q}$ the class of all groups and Fact 3 in the case of finite groups.

Theorem 5. *The consistency problems for the class of all groups and the class of all finite groups are unsolvable.*

Corollary 6. *Let $\mathcal{C}$ be a class of (finite) semigroups or monoids such that each (finite) group embeds into some member of $\mathcal{C}$. Then the consistency problem for $\mathcal{C}$ is unsolvable.*

In particular, we may consider groups just with multiplication.

Proof. In the case of monoids with unit e, given a conjunction $\pi(\bar{x})$ of group equations, form the conjunction $\hat{\pi}(\bar{x}, \bar{y})$ of $\pi(\bar{x})$ and the $x_i y_i = e = y_i x_i$ with new variables y_i. Thus, $\pi(\bar{x})$ admits a non-trivial assignment within some (finite) group if and only $\hat{\pi}$ does so within some (finite) member of $\mathcal{C}$, namely within the group of units. In the absence of constant e, mimic it by a new variable u adding the equations $x_i u = x_i = u x_i$, $y_i u = y_i = u y_i$. □

In view of (iii) in Fact 4, if the uniform word problem for $\mathcal{C}$ is decidable or if $\mathcal{C}$ is a quasi-variety with decidable isomorphism problem (cf. [25] for definitions), then the consistency problem is decidable; this yields decidability e.g. for the classes of all (finite) lattices [31, 9], and all (finite) Heyting algebras [28].

Fact 7. Assume that $\mathcal{C}$ has nullary operation symbols c_0, c_1 such that $c_0 = c_1$ is valid only in singleton members of $\mathcal{C}$), e.g. that $\mathcal{C}$ has bounded lattice or ring with unit reducts. Then (iv) from Fact 4 is equivalent to

(viii) There is a satisfying assignment for $\pi(\bar{g})$ in some non-singleton $A \in \mathcal{C}$.

In particular, if $\mathcal{C}$ has unsolvable consistency problem so does every expansion of $\mathcal{C}$.

Recall that for an expansion $\mathcal{C}'$ of $\mathcal{C}$ the language of $\mathcal{C}'$ has some operation symbols in addition to that of $\mathcal{C}$ and the members of $\mathcal{C}'$ arise from those of $\mathcal{C}$ by adding operations denoted by these additional symbols. And observe that, without the above hypothesis, trivial assignments in $\mathcal{C}$ might generate non-trivial subalgebras in the expansion. The following is obvious in view of (iii) in Fact 4.

Fact 8. A conjunction $\pi(\bar{x})$ of equations admits a non-trivial satisfying assignment within $\mathcal{C}$ if and only if it does so within $\mathsf{Q}\mathcal{C}$. In particular, the consistency problems for $\mathcal{C}$ and $\mathsf{Q}\mathcal{C}$ are equivalent.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

Recall that a *positive primitive* formula is of the form $\exists\, \bar{x}\alpha(\bar{x})$ where α is a conjunction of atomic formulas. By a *basic equation*, we mean an equation of the form $y = x$ or $y = f(\bar{x})$ where f is an operation symbol. An *unnested pp-formula* is of the form $\exists\, \bar{y}.\varphi(\bar{x}, \bar{y})$, where $\varphi(\bar{x}, \bar{y})$ is a conjunction of basic equations. For the following compare [21, Theorem 2.6.1].

Fact 9. Every conjunction $\pi(\bar{x})$ of equations is logically equivalent to an unnested pp-formula $\exists\, \bar{y}.\varphi(\bar{x}, \bar{y})$.

4. Consistency in Modular Lattices

Lemma 10. *There is a recursive set Σ of conjunctions of lattice equations such that the following hold for all $\varphi \in \Sigma$.*

(i) *Given a division ring F and a cardinal $\kappa \geq \aleph_0$. If φ admits a non-trivial satisfying assignment in some modular lattice, then it does so within $\mathrm{L}(V)$ for some $V \in \mathcal{V}_F$ with $\dim V = \kappa$.*

(ii) *If φ admits a non-trivial satisfying assignment in the finite modular lattice L and if F is a division ring of $\chi(F) = 0$ or $\chi(F) > |L|$ (it suffices to require $\chi(F) > |\mathrm{G}(L, \bar{a})|$ for all 4-frames in L) then φ admits a non-trivial satisfying assignment within $\mathrm{L}(V)$ for some $V \in \mathcal{V}_F$ with $\dim V = 4d < \aleph_0$ for some d.*

(iii) *φ is of the form $\varphi(\bar{x}, \bar{z})$, with $\bar{z}$ referring to 4-frames. $\varphi^\exists$ given by $\exists\, \bar{z} \exists\, \bar{x}.\varphi(\bar{x}, \bar{z}) \wedge z_\perp \neq z_\top$ is valid within the modular lattice L if and only if φ admits a non-trivial satisfying assignment within L.*

(iv) *The sets of all $\varphi \in \Sigma$ with $\varphi^\exists$ valid in some, respectively, some finite modular lattice are not recursive.*

The statements remain valid with constants $0 = z_\perp$ and $1 = z_\top$.

Proof. Let Σ consist of all $\pi^\#(\bar{x}, \bar{z})$, according to Lemma 1(iv), with $\pi(\bar{x})$ a conjunction of group equations. We claim:

(*) $\pi(\bar{x})$ admits a non-trivial satisfying assignment within some (finite) group G if and only if $\pi^\#(\bar{x}, \bar{z})$ does so within some (finite) modular lattice L; moreover, given a non-trivial satisfying assignment within G, L can be chosen as $\mathrm{L}(V)$ as in (i) respectively (ii).

Clearly, for a modular lattice L, $(\bar{g}, \bar{a})$ is a satisfying assignment within L if and only if $\bar{g}$ is a satisfying assignment for $\pi(\bar{x})$ in the group $G = \mathrm{G}(L, \bar{a})$ — which is finite if L is finite.

If the assignment $\bar{g}$ in G is trivial, then $g_i = e_G = a_{12}$ for all i. On the other hand, $a_{12} \cap \bigcap_i g_i = a_\perp$ whence $a_{12} = a_\perp$ and the assignment $(\bar{g}, \bar{a})$ is trivial in view of Lemma 1(ii). In other words, if $\pi(\bar{x})$ admits only trivial satisfying assignments within (finite) groups, then $\pi^\#(\bar{x}, \bar{z})$ does so within (finite) modular lattices.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

Now, assume that $\pi(\bar{x})$ has a non-trivial assignment $\bar{h}$ in some (finite) group G: in particular G is not the trivial group. We have to find assignments in suitable $\mathrm{L}(V)$. We may assume that G is at most countable. If G is finite, in (i) we may consider some countably infinite extension, instead. Let $\kappa \geq \aleph_0$ respectively $\kappa = 4(|G|-1)$ if G is finite and choose V of $\dim V = \kappa$ as required in (i) and (ii), respectively. By Lemma 1(i), there is a 4-frame $\bar{a}$ of $L = \mathrm{L}(V)$ such that $\dim V_1 = \kappa$ for $V_1 = a_1$. Lemma 2 provides a fixed point free faithful representation ρ of G in V_1; that is, the $f_i = \rho(h_i)$ generate a subgroup of $\mathrm{GL}(V_1)$ acting fixed point free on V_1. Recall Lemma 1(iii)–(iv) and let $g_i = \Gamma_{\bar{a}}(f_i)$ to obtain a non-trivial assignment $(\bar{g}, \bar{a})$ in L such that $L \models \pi^{\#}(\bar{h}, \bar{a})$.

This proves (*), (i) and (ii). (iii) is obvious and (iv) follows from (*), Theorem 5, and the reduction $\pi \mapsto \pi^{\#}$. □

In view of these Facts, we consider the following *richness conditions* on a class $\mathcal{C}$ of lattices respectively $\mathcal{V}$ of vector spaces.

(I) $\mathrm{L}(V) \in \mathsf{Q}\,\mathcal{C}$ for some vector space V of $\dim V \geq \aleph_0$.

(II_n) For every $0 < d < \aleph_0$ there are a division ring F of characteristic not dividing $d+1$ and an F-vector space V of $\dim V = nd$ such that $\mathrm{L}(V) \in \mathsf{Q}\,\mathcal{C}$.

(III_n) $\mathcal{V}$ consists of finite-dimensional vector spaces over division rings which are finite dimensional over the center; moreover, for all $0 < d < \aleph_0$ there is $V \in \mathcal{V}$ of characteristic not dividing $d+1$ such that $\dim V = nd$.

Clearly, (III_n) implies (II_n) for $\mathrm{L}(\mathcal{V}) := \{\mathrm{L}(V) \mid V \in \mathcal{V}\}$. We refer of ($\mathrm{II}_4$) and ($\mathrm{III}_4$) just as (II) and (III); except for Sec. 9, these are the ones to be used.

Theorem 11. *The consistency problem is unsolvable for any class $\mathcal{C}$ of modular lattices* (*with or without bounds*) *satisfying* (I) *or satisfying $\mathcal{C} \subseteq \mathsf{Q}\,\mathcal{M}_f$ and* (II). *In the bounded case, unsolvability also persists in each expansion of $\mathcal{C}$.*

In particular, in Corollary 27, below, we will show that case (II) applies to $\mathcal{C} = \mathrm{L}(\mathcal{V})$ where $\mathcal{V}$ satisfies (III).

Proof. In view of Lemma 10 and the richness condition a conjunction of lattice equations admits a non-trivial satisfying assignment within $\mathcal{C}$ if and only if it does so within some (finite) modular lattice — in case (II) use Fact 8. □

We conclude the section discussing restricted variants of the consistency problem for modular lattices. These are not needed for the applications to other structures.

Corollary 12. *The decision problems of Theorem* 11 *remain unsolvable if restricted to conjunctions $\pi(x_1, \ldots, x_5)$ of equations.*

Proof. Recall from [15] that the modular lattice freely generated by a $(k+1)$-frame is finitely presented as a modular lattice with four generators, the frame given by

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

a system $\bar{b}(\bar{y})$ of terms, $\bar{y} = (y_1, y_2, y_3, y_4)$, and finitely many relations. Dealing with a conjunction of group equations in k variables $\bar{x}$, encode these adding to $\bar{y}$ a single lattice variable y_5 and finitely many relations. Namely, considering a $(k+1)$-frame $\bar{b}$ in a modular lattice L, let the 4-frame $\bar{a}$ given by the b_i, b_{1j}, $i, j \leq 4$ and $L' = [0, \sum_i a_i]$. Then the x_i correspond to $g_1, \ldots, g_k$ in $\mathrm{G}(L', \bar{a})$. Let $g'_1 = g_1$ and $g'_i = (b_1 + b_{i+1}) \cap (b_{2,i+1} + g_i)$ for $i > 1$. Then $g_i = (b_1 + b_{i+1}) \cap (b_{2,i+1} + g'_i)$ for $i > 1$ and $g'_i = (b_1 + b_{i+1}) \cap c$ where $c = \sum_{i=1}^{k} g'_i$. Introducing the variable y_5 for c and the associated equations, this yields the conjunction ψ of 5-variable lattice equations replacing $\pi^{\#}$ from Lemma 1(iv). In view of Lemma 1(ii), $a_\perp = a_\top$ implies $b_\perp = b_\top$. □

For a field F and $\mathcal{V} = \{F_F^d \mid d < \aleph_0\}$, if satisfiability of conjunctions of ring equations is decidable for F, then the reasoning of [20, Theorem 4.10] shows that the consistency problem for $\mathrm{L}(\mathcal{V})$ is solvable if and only if there is a recursive function δ that for every conjunction ψ of lattice equations one has the following: If ψ is of binary length n and satisfiable in $\mathrm{L}(F_F^d)$ for some d then ψ is also satisfiable in $\mathrm{L}(F_F^d)$ for some $d \leq \delta(n)$. By Theorem 11 (and Corollary 12 if one restricts to the 5-variable case) no such δ exists if F is of characteristic 0. In this case, using an enumeration φ_m of all conjunctions of lattice equations in given 5 variables, those φ_m which are satisfied in some $\mathrm{L}(F_F^d)$ give rise to a (non-recursive) subsequence ψ_n and recursive unboundedness of the function $d(n) = \min\{d \mid \mathrm{L}(F_F^d) \models \exists\, \psi_n\}$.

On the other hand, in the presence of an orthocomplementation, [20, Example 4.2(b)] gives a recursively defined sequence $t_k(\bar{x})$ of terms of length $\mathcal{O}(k)$ in $2k+1$ variables such that $t_k(\bar{x}) = 1$ is satisfiable in $\mathrm{L}(F_F^d)$ if $d = 2^k$ but not for $d < 2^k$. We provide an analogous recursive sequence without orthocomplementation and with fixed number of variables.

In [11], 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 13. *There is a recursively defined sequence of conjunctions $\psi_n(\bar{y})$, $n > 7$, of bounded lattice equations in 5 variables $\bar{y}$ such that ψ_n is of bit length $\mathcal{O}(\log n)$ and such that, for every field of F of characteristic 0, $\psi_n(\bar{y})$ is satisfiable in some $\mathrm{L}(V_F)$, with $\dim V_F = d > 0$ for $d = 4(n-1)$ but not for $d < 4(n-1)$.*

Proof. By [11, Theorem C] the alternating groups A_n, $n > 7$, have presentations of bit length $\mathcal{O}(\log n)$ in 3 generators $\bar{x} = (x_1, x_2, x_3)$; and each non-trivial irreducible representation of A_n has degree $\geq n-1$ [35]. Put $z_\perp = 0$, $z_\top = 1$ and define ψ_n as $\pi_n^{\#}(\bar{x}, \bar{z})$ associated with such presentation of A_n according to Lemma 1(iv). By Lemma 1(iii)(a) there is a constant K such that 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 each $\mathrm{G}(L, \bar a)$. Use the proof of Corollary 12 to replace the 13 variables $\bar x, \bar z$ by 5 new ones.

Now recall Lemma 1(iii) and observe that for each 4-frame $\bar a$ of $\mathrm{L}(V)$ and subgroup G of $\mathrm{GL}(a_1)$ one has a G-invariant subspace $U_1 = \{v \in a_1 \mid v - \varepsilon_{\bar a}(v) \in U\}$ of $V_1 = a_1$ where U is as in the proof of Lemma 10. Now, $U_1 = 0$ if and only if $U = 0$. Thus, every non-trivial irreducible representation of A_n in some V_1 gives rise to a non-trivial satisfying assignment for ψ_n in $L(V)$, $V = V_1^4$. Conversely, given a non-trivial satisfying assignment $\bar g, \bar a$ for ψ_n in some $L(V)$, V a finite-dimensional F-vector space, we may assume $a_\perp = 0$ and $a_\top = V$ and $\bar g$ defines a non-trivial representation of A_n in $V_1 = a_1$ which, by Maschke's Theorem, has a non-trivial direct summand, whence $\dim V \geq 4(n-1)$. □

5. Relation Algebras

A *pre-relation algebra* is an algebraic structure A with two binary operations written as $\cap$ and $\circ$, a unary operation $^{-1}$, and constant Δ. We write $\alpha \in \mathrm{Eq}(A)$ if $\Delta \cap \alpha = \Delta$, $\alpha^{-1} = \alpha$, and $\alpha \circ \alpha = \alpha$. We also consider the partial algebra $A^\#$ where $\circ$ is replaced by the partial operation given by $\alpha + \beta = \gamma$ if and only if $\alpha, \beta \in \mathrm{Eq}(A)$ and $\alpha \circ \beta = \beta \circ \alpha = \gamma$. We write $\alpha \oplus \beta = \gamma$ if $\alpha + \beta = \gamma$ and $\alpha \cap \beta = \Delta$. A system $\bar\alpha$ in $\mathrm{Eq}(A)$ is a *permuting* 4*-frame* of A if the equations defining a 4-frame in a lattice are satisfied by $\bar\alpha$, being evaluated within $A^\#$, and if $\alpha_\perp = \Delta$. Define

$$\mathrm{G}(A, \alpha) = \{\beta \in \mathrm{Eq}(A) \mid \beta \oplus \alpha_1 = \beta \oplus \alpha_2 = \alpha_1 \oplus \alpha_2\}.$$

Given a set S we consider the pre-relation algebras on sets of binary relations on S with the following operations: intersection $\cap$, relational product $\circ$, inversion^{-1}, and $\Delta = \mathsf{id}_S$. We say that A is *represented* on S — Jónsson [23] calls A an *algebra of relations*. Let $\mathcal{R}$ denote the class of all algebras isomorphic to such — the class of *representable* pre-relation algebras; $\mathcal{R}$ is quasi-variety by [23, Theorem 1]. By $\mathcal{R}_f$, we denote the class of finite members of $\mathcal{R}$. The following are immediate by [17, Corollary 2] and Lemma 1(i).

Fact 14. If α is a permuting 4-frame of A which is represented on S, then the subalgebra $L = \mathrm{L}(A, \alpha)$ generated by α together with $\mathrm{G}(A, \alpha)$ consists of pairwise permuting equivalence relations on S; with operations $\cap$ and $+$ it forms a modular sublattice $\mathsf{L}(A, \alpha)$ of $\mathrm{Eq}(S)$; in particular, $L \subseteq \mathrm{Eq}(A)$ and $L^\# = L$. Moreover, α is a 4-frame of L and $\mathrm{G}(A, \alpha) = \mathrm{G}(L, \alpha)$.

Fact 15. For every vector space V of $\dim V = 4d$ there is a pre-relation algebra $A = \mathrm{A}(V)$ represented on V and a permuting 4-frame of A such that $\mathrm{L}(V) = \mathsf{L}(A, \alpha)$.

We consider particular formulas in the language of pre-relation algebras: $\mathrm{Eq}(\bar y)$ is the conjunction of equations such that $A \models \mathrm{Eq}(\bar\xi)$ implies $\beta \in \mathrm{Eq}(A)$ for all β in the list $\bar\xi$. A *type*-1*-formula* $\psi(\bar y)$ is a conjunction of basic equations in the $\cap$-$\circ$-fragment. Let $\tau(u, \bar y, \bar v)$ denote the obvious type-1-formula such that $A \models \tau(\gamma, \bar\delta, \bar\varepsilon)$

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

for some $\bar{\varepsilon}$ if and only if $\gamma = \delta_1 \circ \cdots \circ \delta_n$ and that, in this case, $\gamma = \varepsilon_j = \delta$ for all j if $\delta_i = \delta$ for all i. The richness conditions (I) and (II) are modified to $(I)_A$ and $(II)_A$ replacing $\mathrm{L}(V)$ by $\mathrm{A}(V)$.

Theorem 16. *The consistency problem is unsolvable for any class $\mathcal{A}$ of representable pre-relation algebras satisfying $(I)_A$ or contained in $\mathsf{Q}\mathcal{R}_f$ and satisfying $(II)_A$. More precisely, there is a recursive set Σ' of type-1-formulas such that there is no algorithm which on input $\psi(\bar{y}) \in \Sigma'$ would decide whether $\psi^\exists$ given as*

$$\exists\, \bar{y} \exists\, u \exists\, \bar{v}.\ \mathrm{Eq}(\bar{y}) \wedge \bigcap_i y_i = \Delta \wedge \psi(\bar{y}) \wedge \tau(u, \bar{y}, \bar{v}) \wedge u \neq \Delta$$

is satisfied in some member of $\mathcal{A}$.

Corollary 17. *Unsolvability persists if the total relation is given as constant ∇; in this case, $u = \nabla$ has to be added as a conjunct in forming $\psi^\exists$. Also unsolvability persists in any further expansion of $\mathcal{A}$.*

Proof of Theorem 16. Recall Σ from Lemma 10; to obtain Σ' replace $\varphi(\bar{x}, \bar{z})$ by an equivalent unnested pp-formula in lattice language (Fact 9). In the latter, replace equations of the form $u = v + w$ by $u = v \circ w \wedge u = w \circ v$. This associates with $\varphi(\bar{x}, \bar{z})$ a type-1-formula $\varphi'(\bar{x}, \bar{z}, \bar{y})$ such that in every lattice L of permuting equivalences, one has $(L, \cap, +) \models \varphi(\bar{\xi}, \bar{\alpha})$ if and only if $(L, \cap, \circ) \models \exists\, \bar{y}.\varphi'(\bar{\xi}, \bar{\alpha}, \bar{y})$. Observe that, if ${\varphi'}^\exists$ is valid in $A \in \mathcal{R}$, then $\varphi^\exists$ is valid in $\mathsf{L}(A, \alpha)$ for some witnessing permuting 4-frame α in A. Conversely, if $\varphi^\exists$ is valid in $L = \mathsf{L}(A, \alpha)$, then ${\varphi'}^\exists$ is valid in $A \in \mathcal{R}$ — witnessed by the values for $\bar{z}$ and $\bar{x}$ in $L \subseteq A$. Thus, put $\Sigma' = \{\varphi' \mid \varphi \in \Sigma\}$.

Now, if $\varphi^\exists$ is valid within some (finite) modular lattice, then it is so within suitable $\mathrm{L}(V)$ (Lemma 10(i) and (ii)) whence ${\varphi'}^\exists$ is valid in $\mathrm{A}(V) \in \mathcal{A}$ (cf. Fact 15). Conversely, if ${\varphi'}^\exists$ is valid in $A \in \mathcal{A}$ (by Fact 8, we may assume A finite in case (II)), then $\varphi^\exists$ is valid in the (finite) modular lattice $\mathsf{L}(A, \alpha)$, where $\bar{\alpha}$ is witness for $\bar{z}$. Thus, the claim follows from Lemma 10(iii), (iv) and the reduction $\varphi \mapsto \varphi'$. □

6. Databases

We follow [24] for database concepts, though adapting notation to common use in mathematics. Fix a countably infinite set X_∞ of variables and use $x, y, \ldots$ to denote elements of X_∞. Under the pure universal relation assumption, a *database* D is given by a finite non-empty $U \subseteq X_\infty$ of *attributes*, for each x in U a domain $\Delta[x]$ of *values* of the attribute x, and a non-empty subset (*relation*) R of the direct product $\prod_{x \in U} \Delta[x]$. For a tuple t in R and $X \subseteq U$, let $t[X]$ be the restriction of t to X.

The atomic sentences to be considered are the *functional dependencies* (*fd*'s) $X \to Y$ and the *embedded multivalued dependencies* (*emvd*'s) $[X, Y]$ with non-empty finite $X, Y \subseteq U_\infty$. Validity is defined as follows: $D \models X \to Y$ if and only if for all $s, t \in R$, if $s[X] = t[X]$ then $s[Y] = t[Y]$ — provided X and Y are subsets of

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

U, at all. $D \models [X, Y]$ if and only if for every $t_1, t_2 \in R$ with $t_1[X \cap Y] = t_2[X \cap Y]$ there exists $t \in R$ with $t[X] = t_1[X]$ and $t[Y] = t_2[Y]$; in other words, the restriction of R to $XY = X \cup Y$ is the natural join of the restrictions of X and Y.

A database D with attribute set U is *trivial* if it satisfies all fd's and emvd's (with attributes from U). D is *almost trivial* if each of its attributes is a key, that is if D satisfies all fd's.

Fact 18. A database is almost trivial if $s[x] \neq t[x]$ for all $s \neq t$ in R and $x \in U$. A database is trivial if and only if its attribute set U or its relation R is a singleton set.

Proof. The first claim is obvious and so is the inverse implication in the second. Now, assume D trivial and $U = X \cup Y$ the disjoint union of non-empty X, Y. Consider t_1, t_2 in R. In view of the emvd $[X, Y]$ there must be $t \in R$ such that $t_1[X] = t[X]$ and $t_2[Y] = t[Y]$. The fd's $x \to y$ and $y \to x$ ($x \in X, y \in Y$) imply $t_1[Y] = t[Y]$ and $t_2[X] = t[X]$ whence $t_1 = t = t_2$. □

For a vector space V and injective map $f : U \to \mathrm{L}(V)$, $U \subseteq X_\infty$ finite, consider the database $\mathsf{D}(V, f)$, where $\Delta[x]$ is given as the set of cosets of $f(x)$ and $R = \prod_{x \in U} \Delta[x]$. Let $\mathsf{D}(V)$ denote the set of all $\mathsf{D}(V, f)$ for given V. The richness conditions (I) and (II) are modified to $(I)_D$ and $(II)_D$ replacing $\mathrm{L}(V)$ respectively $\mathrm{A}(V)$ by $\mathsf{D}(V)$.

Theorem 19. *Consider a class $\mathcal{D}$ of databases which either satisfies $(I)_D$ or which consists of finite databases and satisfies $(II)_D$. Then there is no algorithm which on input of a conjunction of fd's and emvd's decides whether there is a member of $\mathcal{D}$ which is not almost trivial* (*respectively, non-trivial*).

While the first problem (as a special case of implication) is decidable for fd's alone, the question for emvd's alone remains open. By [12, Sec. 2.2], the analog of the Theorem follows for models in independence logic with respect to inclusion and conditional independence atoms. In the setting of conditional inclusion and conditional functional dependencies, the second problem has been studied in [27]; undecidability has been shown for the combination of both.

Proof of Theorem 19. Given a database D, one has projection maps $\pi_x : R \to \Delta[x]$ yielding for each $t \in R$ its x-component $\pi_x(t) = t[x]$ in $\Delta[x]$. With each of these maps one has its kernel equivalence relation θ_x. For a set X of attributes write $\theta_X = \bigcap_{x \in X} \theta_x$. Thus, $(s, t) \in \theta_X$ if and only if $s[X] = t[X]$.

Let S denote the factor set R/θ_U of equivalence classes modulo θ_U and, for $X \subseteq U$, η_X^D the equivalence relation on S corresponding to θ_X, that is for all θ_U-classes one has

$$(t/\theta_U, s/\theta_U) \in \eta_X^D \quad \text{iff } (t, s) \in \theta_X.$$

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

Clearly, $\eta^D_X = \bigcap_{x\in X} \eta^D_x$. Let $\mathrm{A}(D)$ the pre-relation algebra represented on S which is generated by the η^D_x, $x \in U$. It follows from [18, Lemma 11]

$$\eta^D_X \subseteq \eta^D_Y \quad \text{iff } D \models X \to Y$$
$$\eta^D_Z = \eta^D_X \cap \eta^D_Y \quad \text{iff } D \models XY \to Z \wedge Z \to XY$$

and, if X, Y, Z are pairwise disjoint, then

$$\eta^D_Z = \eta^D_X \circ \eta^D_Y \quad \text{iff } D \models [XZ, YZ] \wedge X \to Z \wedge Y \to Z.$$

For a tuple $\bar{y}$ from U write $\eta^D(\bar{y}) = (\eta^D_{y_1}, \ldots, \eta^D_{y_n})$.

Conversely, each pre-relation algebra A, represented on a set S, together with an assignment η within $\mathrm{Eq}(A)$ for variables from a finite $U \subseteq X_\infty$ such that $\bigcap_{x\in U} \eta(x) = \Delta$, gives rise to a database $D = \mathsf{D}(A, \eta)$ with $\Delta[x]$ the set of classes of $\eta(x)$ and R the image of S under the map $a \mapsto (a/\eta(x) \mid x \in U)$. For such, $\theta_U = \Delta$ and $(A, \eta) \cong (\mathrm{A}(D), \eta^D)$. Moreover, D is almost trivial if and only if $\mathsf{im}\,\eta$ is a singleton set, namely $\{\Delta\}$.

Given a type-1-formula $\psi(\bar{y})$ let U consist of all variables occurring in $\psi^\exists$ and translate $\psi(\bar{y}) \wedge \tau(u, \bar{y}, \bar{v})$ into a conjunction ψ' of fd's and emvd's in attributes $\bar{y}, u, \bar{v}$ such that $D \models \psi'$ if and only if

$$\mathrm{A}(D) \models \bigcap_i \eta^D(y_i) = \Delta \wedge \psi(\eta^D(\bar{y})) \wedge \tau(\eta^D(u), \eta^D(\bar{y}), \eta^D(\bar{v})).$$

Observe that for a database $D = \mathsf{D}(V, f)$ one has $(\mathrm{A}(D), \eta^D) \cong (\mathrm{A}(V), \hat{f})$ where $\hat{f}(x)$ is the equivalence relation associated with $f(x)$. Thus, Theorem 16 applies to $\mathcal{A} = \{\mathrm{A}(D) \mid D \in \mathcal{D}\}$. We rephrase its statement: There is no algorithm which, on input of a type-1-formula $\psi(\bar{y})$ decides whether there is A in $\mathcal{A}$ and an assignment η for $\bar{y}, u, \bar{v}$ in $\mathrm{Eq}(A)$ such that $A \models \psi(\eta(\bar{y})) \wedge \tau(u, \bar{y}, \bar{v})$ and $\bigcap_i \eta(y_i) = \Delta$ but $\eta(u) \neq \Delta$, the latter being equivalent to $\mathsf{im}\,\eta$ not to be singleton. Deciding the latter reduces to deciding whether there is a non-almost trivial database D with attributes $\bar{y}, u, \bar{v}$ satisfying the conjunction ψ' of fd's and emvd's. This shows unsolvability of the first decision problem in the Theorem. For the second problem, we have to refer to Corollary 17 and translate $u = \nabla$ by $[u, U \setminus u] \wedge U \setminus u \to u$. Indeed, if the latter holds in D, then, by the emvd, for all $t_1, t_2 \in R$ there is $t \in R$ such that $t[u] = t_1[u]$ and $t[U \setminus u] = t_2[U \setminus u]$ whence, by the fd, $t_2[u] = t[u] = t_1[u]$ and so $(t_1, t_2) \in \theta_u$. □

7. Rings

We consider rings R with constants $0, 1$. Let $\mathsf{L}(R)$ denote the (modular) lattice of all right ideals. A ring R is (von Neumann) *regular* if for every $a \in R$ there is $x \in R$ such that $axa = a$; equivalently, each of its principal right ideals is generated by an idempotent. The principal right ideals of a regular ring form a sublattice $\overline{\mathsf{L}}(R)$ of $\mathsf{L}(R)$. The following is well known and easy to prove.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

Fact 20. The endomorphism ring $R = \mathsf{End}(V)$ of an vector space V is regular and one has $\overline{\mathsf{L}}(R) \cong \mathrm{L}(V)$ via $\varphi R \mapsto \mathsf{im}\,\varphi$ for $\varphi \in R$.

Fact 21. There are positive primitive $\sigma(x,y,z)$ and $\mu(x,y,z)$ in the language of rings such that the following hold for all idempotents e, f, g in a ring R:

(a) $R \models \sigma(e,f,g)$ if and only if $gR = eR + fR$.
(b) $R \models \mu(e,f,g)$ implies $gR = eR \cap fR$.

If R is regular, then in (b) holds the converse, too.

Proof. Concerning (a) observe that $gR = eR + fR$ if and only

$$R \models ge = e \wedge gf = f \wedge \exists r \exists s . g = er + fs.$$

Concerning (b) observe that, according to [33, Lemma 8-3.12 (ii)], if

$$\exists r \exists s. \quad (f - ef)r(f - ef) = f - ef \wedge$$
$$g(f - fr(e - ef)) = f - fr(e - ef) \wedge g = (f - fr(e - ef))s.$$

holds in R then $gR = eR \cap fR$ — the first equation encodes that r is a quasi-inverse of $f - ef$ while the last two state that

$$gR = (f - fr(e - ef))R. \qquad \square$$

In the richness conditions replace $\mathrm{L}(V)$ by $\mathsf{End}(V)$ to obtain the conditions $(I)_R$ and $(II)_R$. Let $\mathcal{R}_f$ denote the class of all finite rings.

Theorem 22. *The consistency problem is unsolvable for every class $\mathcal{C}$ of rings satisfying $(I)_R$ or contained in $\mathsf{Q}\,\mathcal{R}_f$ and satisfying $(II)_R$.*

Proof. Consider the language of bounded lattices and recall Σ from Lemma 10. Given $\varphi(\bar{x}) \in \Sigma$, replace it by the equivalent unnested pp-formula $\exists\, \bar{y}.\varphi'(\bar{x}, \bar{y})$ (Fact 9); associate with variables $x, y, \ldots$, in the latter ring variables $\hat{x}, \hat{y}, \ldots$, and let χ be the conjunction of all equations $\hat{x}^2 = \hat{x}$ and $\hat{y}^2 = \hat{y}$. Use Fact 21 to replace the basic lattice equations by existentially quantified conjunctions of ring equations, each with new rings variables. The conjunction of these and of χ is equivalent to a positive primitive ring formula $\hat{\varphi}(\bar{x}, \bar{y})$ such that $\mathsf{L}(R) \models \varphi^{\exists}$ if $R \models \varphi^R$ where φ^R is given as $\exists\, \bar{x} \exists\, \bar{y}.\hat{\varphi}(\bar{x}, \bar{y}) \wedge 0 \neq 1$. Conversely, if $\varphi^{\exists}$ holds in $\mathrm{L}(V)$ then, in view of Fact 20, φ^R holds in $\mathsf{End}(V)$.

In view of the richness conditions and Fact 8, the claim follows from Lemma 10(iii), (iv) as in the proof of Theorem 16. $\square$

Let $\mathcal{N}_f$ denote the class of all finite regular rings. By the Artin–Wedderburn Theorem $\mathcal{N}_f$ consists, up to isomorphism, just of the direct products of matrix rings $F^{d\times d}$, $d < \aleph_0$, F a finite field.

Fact 23. $\mathsf{End}(V) \in \mathsf{Q}\,\mathcal{N}_f$ if V is an F-vector space of $\dim V < \aleph_0$ and if F is finite-dimensional over its center.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

Proof. This can be seen as a variant of Lemma 3.5 in Lipshitz [26]. Since $\mathsf{End}\, V_F$ embeds into $\mathsf{End}\, V_C$, C the center of F, we may assume that F is a field and consider $F^{d\times d} \cong \mathsf{End}(V_F)$. By tensoring with $\bar{F}$, the algebraic closure of F, we have $F^{d\times d}$ embedded into $\bar{F}^{d\times d}$. The algebraic closure $\bar{P}$ of the prime subfield P of F is elementarily equivalent to $\bar{F}$, and it follows that $\bar{F}^{d\times d}$ and $\bar{P}^{d\times d}$ are elementarily equivalent, too. Now, $\bar{P}^{d\times d}$ is the directed union (whence in the quasi-variety) of the $K^{d\times d}$ where K is a subfield of $\bar{P}$ of finite degree, — and finite if P is finite. Finally, observe that $\overline{\mathbb{Q}}$ embeds into a suitable ultraproduct of the $\bar{P}$, P finite, since that is algebraically closed and of characteristic 0. □

In particular, if $\mathcal{F}$ is a class of division rings which are finite-dimensional over the center and if $\mathcal{F}$ contains members of characteristic 0 or infinitely many finite characteristics, then there is no algorithm to decide, for a given finite family of multi-variate polynomials p_i (in non-commuting variables) with integer coefficients, whether there is a common zero in the matrix ring $F^{d\times d}$ for some $F \in \mathcal{F}$ and $0 < d < \aleph_0$. In view of Fact 9, one may restrict to families of quadratic polynomials.

If the matrix rings $F^{d\times d}$ are endowed with an involution $A \mapsto A^*$ such that $\sum_i A_i A_i^* = 0$ implies $A_i = 0$ for all i then a family (p_i) can be replaced by the single $\sum_i p_i p_i^*$, which can be considered a polynomial in variables x_i, x_i^*, to be interpreted such that $x_j^* \mapsto B_j^*$ if $x_j \mapsto B_j$. Again, it suffices to consider a single quartic such polynomial. In particular, this applies if $\mathcal{F}$ consists of subfields of the complex numbers, closed under conjugation, and if A^* is the conjugate transpose of A.

In the context of the categorical approach to Quantum Theory (cf. [1, 13]), Theorem 22 yields the following: Let F be a division ring of characteristic 0 and C the additive category, possibly enriched with additional structure, of finite-dimensional F-vector spaces. Consider C as a partial algebraic structure the underlying "set" of which is the class of all morphisms. Then there is no algorithm to decide, for any given conjunction $\pi(\bar{x})$ of equations, whether $\pi(\bar{x})$ admits an assignment in C which is satisfying (in a particular, having all terms in $\pi(\bar{x})$ evaluated) and non-trivial (that is, not having a 0-morphism as single value). Indeed, the problem of Theorem 22 can be encoded so that satisfying assignments must have values which are endomorphism of a single object.

8. Complemented Modular Lattices

A modular lattice L with bounds $0, 1$ as constants is *complemented* if for every a there is b such that $a \oplus b = 1$ (in the sequel, we consider $0, 1$ as constants). Here, consistency problems can be given a more special form.

Fact 24. Within the class of complemented modular lattices, every conjunction of equations is equivalent to a formula $\exists\, \bar{y}.s(\bar{x}, \bar{y}) = 0 \wedge t(\bar{x}, \bar{y}) = 1$ with terms s, t.

Proof. Given a conjunction of equations $s_j = t_j$, observe each $s_j = t_j$ equivalent to $\exists\, v : \tilde{s}_j = 0 \wedge \tilde{t}_j = 1$ 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 $\tilde{s}_j = 0 \wedge \tilde{t}_j = 1 \wedge \tilde{s}_i = 0 \wedge \tilde{t}_i = 1$ equivalent to $\tilde{s}_j + \tilde{s}_i = 0 \wedge \tilde{t}_j \cap \tilde{t}_i = 1$. □

In particular, the lattices $\mathrm{L}(V)$ of all linear subspaces of vector spaces are complemented modular and so are the lattices $\overline{\mathsf{L}}(R)$ of principal right ideals of regular rings. For the latter, the following is useful in case (II).

Fact 25. For every class $\mathcal{R}$ of regular rings one has $\mathsf{Q}\{\overline{\mathsf{L}}(R) \mid R \in \mathcal{R}\} \subseteq \{\overline{\mathsf{L}}(R) \mid R \in \mathsf{Q}\,\mathcal{R}\}$.

Proof. Since every $R \in \mathsf{Q}\,\mathcal{R}$ embeds into some direct product P of ultra products S_i of members R_{ij} of $\mathcal{R}$ (cf. [10, Corollary 2.3.4]), it suffices to observe that $\overline{\mathsf{L}}(R)$ embeds into $\overline{\mathsf{L}}(P)$ via $eR \mapsto eP$ and $\overline{\mathsf{L}}(P)$ into the direct product of the $\overline{\mathsf{L}}(S_i)$ via $(e_iS_i \mid i \in I) \mapsto (e_i \mid i \in I)P$ (cf. [33, Corollaries 8-3.14-15] and that the $\overline{\mathsf{L}}(S_i)$ satisfy all quasi-identities valid in the $\overline{\mathsf{L}}(R_{ij})$ (which, by Fact 21 translate into sentences in the language of rings). □

The following is a lattice theoretic variant of Fact 23 and can be proved in the same fashion. It follows, immediate, if one combines Facts 20, 23, and 25. Together with Theorem 11 it implies Corollary 27.

Fact 26. $\mathrm{L}(V) \in \mathsf{Q}\,\mathcal{M}_f$ if V is an F-vector space of $\dim V < \aleph_0$ and if F is finite-dimensional over its center.

Corollary 27. *Theorem* 11 *and Corollary* 12 *apply to* $\mathcal{C} = \{\mathrm{L}(V \mid V \in \mathcal{V}\}$, *where* $\mathcal{V}$ *satisfies the richness condition* (*III*).

Of course, if for a class $\mathcal{C}$ of complemented modular lattices choice of some complement is added as fundamental operation, Theorem 11 applies. If $d = \dim V < \aleph_0$, if F is a division ring with involution, and if V is endowed with an anisotropic form Φ Hermitian with respect to this involution, then $U \mapsto U^\perp = \{v \in V \mid \forall\, u \in U.\Phi(v,u) = 0\}$ turns $\mathrm{L}(V)$ into the ortholattice $\mathrm{L}^\perp(V)$. Here, an *ortholattice* is a bounded lattice endowed with a dual automorphism $x \mapsto x^\perp$ of order 2 such that $x \oplus x^\perp = 1$.

In order to have Corollary 27 available, we consider a class $\mathcal{V}$ of such spaces where the class of underlying vector spaces satisfies condition (III). Then, by Corollary 12 and Fact 29, below, we obtain the following.

Corollary 28. *There is no algorithm which, given a* 5*-variable term* $t(\bar{x})$ *in the language of ortholattices, decides whether* $\exists\, \bar{x}.t(\bar{x}) = 1$ *is valid in the ortholattice* $\mathrm{L}^\perp(V)$ *for some* $V \in \mathcal{V}$ *with* $\dim V > 0$.

Natural examples for $\mathcal{V}$ are the classes of all finite-dimensional real, complex, and quaternionian, respectively, Hilbert spaces. Here, in contrast, deciding whether

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

$\exists\, \bar{x} t(\bar{x}) > 0$ holds in some $\mathrm{L}^{\perp}(V)$ ("weak satisfiability") is decidable (cf. [14]) and an upper complexity bound has been derived in [20].

Fact 29. Within the class of modular ortholattices, every conjunction $\pi(\bar{x})$ of equations is equivalent to an equation $t(\bar{x}) = 1$.

Proof. Observe that the following are equivalent for all given x, y: $x + x^{\perp}y^{\perp} = 1$; $x^{\perp} = x^{\perp}(x + x^{\perp}y^{\perp})$; $x^{\perp} = xx^{\perp} + x^{\perp}y^{\perp}$ (by modularity); $x^{\perp} \leq y^{\perp}$; $y \leq x$. Thus, $s_j \leq t_j$ is equivalent to some $u_j = 1$ and $t_j \leq s_j$ to some $v_j = 1$; and $\bigwedge_j s_j = t_j$ to $\bigcap_j u_j \cap v_j = 1$. □

9. Grassmann-Cayley Algebra

Recall that for a finite-dimensional vector space V the Grassmann–Cayley algebra $\mathrm{GC}(V)$ (cf. [32]) has, in particular, operations $\wedge$ and $\vee$ and terms built from them and $0, 1$: the *simple expressions*. These operations are related to the lattice $\mathrm{L}(V)$ as follows: $0, 1$ are the bounds of $\mathrm{L}(V)$, $A \wedge B = A \cap B$ if $A + B = V$ and $A \vee B = A + B$ if $A \cap B = 0$.

Theorem 30. *Let $\mathcal{V}$ be a class of vector spaces which satisfies (III_{16}). There is no algorithm to decide for any given conjunction of equations $t_i(\bar{x}) = s_i(\bar{x})$, with simple expressions t_i, s_i, whether it admits a satisfying assignment within* $\mathrm{GC}(V)$ *for some $V \in \mathcal{V}$, $V \neq 0$.*

The proof needs some preparation. We consider lattices with bounds $0, 1$. For a term $t(\bar{x})$, call the assignment $\bar{x} \mapsto \bar{a}$ in L *admissible* if, for any occurrence of subterms $s(\bar{x})$, $s_1(\bar{x})$, and $s_2(\bar{x})$ in $t(\bar{x})$, the following hold in L:

$$\begin{aligned} &\text{If } s(\bar{x}) = s_1(\bar{x}) + s_2(\bar{x}), \quad \text{then } s_1(\bar{a}) \cap s_2(\bar{a}) = 0; \\ &\text{If } s(\bar{x}) = s_1(\bar{x}) \cap s_2(\bar{x}), \quad \text{then } s_1(\bar{a}) + s_2(\bar{a}) = 1. \end{aligned}$$

We say that $\bar{a}$ is *admissible* for a conjunction $\pi(\bar{x})$ of equations if it is so for any subterm occurrence in $\pi(\bar{x})$. If, in addition, $L \models \pi(\bar{a})$ then we write $L \models_a \pi(\bar{a})$. For an n-frame $\bar{a}$ of a modular lattice L and $i \neq j$ put

$$R_{ij}(L, \bar{a}) = \{x \in L \mid x \oplus a_j = a_i + a_j\}.$$

Fact 31. Fix $n \geq 3$.

(i) There is a conjunction $\varphi(\bar{z})$ of lattice equations such that $\bar{a}$ is a 4-frame of the modular lattice L if and only if $L \models_a \varphi_n(\bar{a})$.

(ii) There are lattice terms $\otimes(x, y, \bar{z})$ and $\ominus(x, y, \bar{z})$ such that for every vector space V and 4-frame $\bar{a}$ of $\mathrm{L}(V)$ there is a (unique) isomorphism $\varepsilon_{\bar{a}} : a_1 \to a_2$ such that $\Gamma_{\bar{a}}(f) := \{v - \varepsilon_{\bar{a}}(f(v)) \mid v \in a_1\}$ defines a ring isomorphism of $\mathsf{End}(a_1)$ onto $R_{12}(L, \bar{a})$ with multiplication $(r, s) \mapsto \otimes(r, s, \bar{a})$, difference $(r, s) \mapsto \ominus(r, s, \bar{a})$, zero a_1, and unit a_{12}. Moreover, the assignments $x, y, \bar{z} \mapsto r, s, \bar{a}$ with $r, s \in R_{12}$ are admissible for the terms $\otimes(x, y, \bar{z})$ and $\ominus(x, y, \bar{z})$.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

(iii) With each conjunction $\pi(\bar{x})$ of ring equations of the form $p_i(\bar{x}) = 0$ one can effectively associate a conjunction $\pi^{\#}(\bar{x}, \bar{z})$ of lattice equations of the form $t_i(\bar{x}, \bar{z}) = z_1$ such that for every vector space V and $\bar{r}, \bar{a}$ in $L = \mathrm{L}(V)$ one has $\mathrm{L}(V) \models_a \pi^{\#}(\bar{r}, \bar{a})$ if and only if $\bar{a}$ is an 4-frame of L, $\bar{r}$ in $R_{12}(L, \bar{a})$, and $R_{12}(L, \bar{a}) \models \pi(\bar{r})$.

Proof of Theorem 30. Observe that the class $\mathcal{C}$ of $\mathsf{End}(V_1)$, where $V_1^4 \cong V \in \mathcal{V}$ satisfies condition (II_R) for rings while $\mathcal{C} \subseteq \mathsf{Q}\,\mathcal{R}_f$ follows from Fact 23. Thus, the claim follows from the reduction in Fact 31(iii) and Theorem 22 where $\mathcal{C} = \{\mathsf{End}(V_1) \mid V_1 \in \mathrm{L}(V), \dim V = 4 \dim V_1\}$. □

Proof of Fact 31. (i) Consider a 4-frame of the modular lattice L. Due to the first condition defining a frame, the assignment $\bar{z} \mapsto \bar{a}$ is admissible for any term arising from $\sum_{k\in K} z_k$ by insertion of brackets. It only remains to deal with the last condition. Observe that $a_{ij} \cap a_{jk} \leq a_{ij} \cap (a_i + a_j) \cap (a_j + a_k) = a_{ij} \cap a_j = 0$, $b + a_{ij} + a_{jk} = 1$, where $b = \sum_{\ell\neq j} a_\ell$, and that the condition is equivalent to $b \cap (a_{ij} + a_{jk}) = a_{ik}$.

(ii) Recall the approach in the proof of Lemma 1(iii) (a), in particular the terms π_k^i. We write $R_{ij} = R_{ij}(L, \bar{a})$. The assignment $x, \bar{z} \mapsto r, \bar{a}$ where $r \in R_{ij}$ or $r \in R_{ji}$ is admissible for π_k^i since $r \cap a_{ik} \leq (a_i + a_j) \cap a_{ik} = 0$ and $\pi_k^i(r) = (r + a_{ik}) \cap b$ where $b = \sum_{\ell\neq i} a_\ell$ and $b + r + a_{ik} = 1$. Also, observe that the map $r \mapsto \pi_k^i(r)$ restricts to a bijection π_{kj}^{ij} of R_{ij} onto R_{kj} and to a bijection π_{jk}^{ji} of R_{ji} onto R_{jk}. For $r \in R_{12}$ and $s \in R_{23}$ one has $r \cap s \leq r \cap_2 = 0$ and $(r + s) \cap b = (r + s) \cap (a_1 + a_3)$, $r + s + b = 1$ where $b = \sum_{i\neq 1,3} a_i$. For $r \in R_{12}$ define r_{ij} as in the proof of Lemma 1. Then the definition $\otimes(s, r, \bar{a}) = (r_{12} + s_{23}) \cap b$ of multiplication is given by a term for which the $x, y, \bar{z} \mapsto s, r, \bar{a}$ with $r, s \in R_{12}$ are admissible. To obtain the same kind of term for difference, put

$$r \ominus s = ([(s_{13} + a_2 + a^+) \cap (r + a_{23})] + a_3 + a_4) \cap (a_1 + a_2).$$

Thus, the lattice terms and equations used in the proof of Lemma 1 and Lemma 10 can be modified to become admissible. That $\Gamma_{\bar{a}}$ is an isomorphism (of rings), is shown by easy Linear Algebra calculations (cf. [29]). (iii) Follows, immediately. □

Acknowledgments

The second author was supported by the *German Academic Exchange Service* (DAAD) under codenumber 91532398-50015537.

References

[1] S. Abramsky and B. Coecke, A categorical semantics of quantum protocols, in *Proc. 19th Annual IEEE Symp. Logic in Computer Science* (LiCS'04) (IEEE Computer Science Press, 2004) (Extended version at arXiv:quant-ph/0402130).

[2] S. I. Adyan, Algorithmic unsolvability of problems of recognition of certain properties of groups. (Russian) *Dokl. Akad. Nauk SSSR* (*N.S.*) **103** (1955) 533–535.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.

[3] S. I. Adyan, Unsolvability of some algorithmic problems in the theory of groups. (Russian) *Trudy Moskov. Mat. Obšč* **6** (1957) 231–298.
[4] B. Artmann, On coordinates in modular lattices with a homogeneous basis, *Illinois J. Math.* **12** (1968) 626–648.
[5] M. R. Bridson and H. Wilton, The triviality problem for profinite completions, *Invent. Math.* **202** (2015) 839–874.
[6] R. Freese, Projective geometries as projective modular lattices, *Trans. Amer. Math. Soc.* **251** (1979) 329–342.
[7] R. Freese, The variety of modular lattices is not generated by its finite members, *Trans. Amer. Math. Soc.* **255** (1979) 277–300.
[8] R. Freese, Free modular lattices, *Trans. Amer. Math. Soc.* **261** (1980) 81–91.
[9] R. Freese and J. B. Nation, Finitely presented lattices, *Proceedings of the American Mathematical Society* **77** (1979) 174–178, https://doi.org/10.1090/S0002-9939-1979-0542080-8.
[10] V. A. Gorbunov, *Algebraic Theory of Quasivarieties* (Novosibirsk, 1998).
[11] R. M. Guralnick, W. M. Kantor, M. Kassabov and A. Lubotzky, Presentations of finite simple groups: A computational approach, *J. Eur. Math. Soc.* **13** (2011) 391–458.
[12] M. Hannula and J. Kontinen, A finite axiomatization of conditional independence and inclusion axioms, arXiv:1309.4927v2 [math.LO].
[13] J. Harding, A link between quantum logic and categorical quantum mechanics, *Int. J. Theor. Phys.* **48** (2009) 769–802.
[14] J. Harding, Decidability of the equational theory of the continuous geometry $CG(\mathbb{F})$, *J. Philos. Logic* **42**(3) (2013) 461–465, http://dx.doi.org/10.1007/S10992-013-9270-X.
[15] C. Herrmann, Rahmen und erzeugende Quadrupel in modularen Verbänden, *Algebra Universalis* **14** (1982) 357–387.
[16] C. Herrmann, On the arithmetic of projective coordinate systems, *Trans. Amer. Math. Soc.* **284** (1984) 759–785, https://doi.org/10.1090/S0002-9947-1984-0743743-8.
[17] C. Herrmann, Frames of permuting equivalences, *Acta Sci. Math.* **51**(1–2) (1987) 93–101.
[18] C. Herrmann, On the undecidability of implications between embedded multivalued database dependencies, *Information and Computation* **122** (1995) 221–235.
[19] C. Herrmann and M. Ziegler, Computational complexity of quantum satisfiability, in *Proc. 26th Annual IEEE Symp. Logic in Computer Science* (2011), pp. 175–184.
[20] C. Herrmann and M. Ziegler, Computational complexity of quantum satisfiability, *J. ACM* **63**(2) (2016) Article ID: 19.
[21] W. Hodges, *Model Theory* (Cambridge University Press, 1993).
[22] B. Jónsson, On the representation of lattices, *Math. Scando.* **1** (1953) 193–206.
[23] B. Jónsson, Representation of modular lattices and of relation algebras, *Trans. Amer. Math. Soc.* **92** (1959) 449–464.
[24] P. C. Kanellakis, Elements of relational database theory, in *Handbook of Theoretical Computer Science, Vol. B: Formal Models and Semantics*, ed. J. van Leeuwen (Elsevier, Amsterdam, 1990), pp. 1073-1156.
[25] O. G. Kharlampovich and M. V. Sapir, Algorithmic problems in varieties, *Internat. J. Algebra Comput.* **5**(4–5) (1995) 379–602.
[26] L. Lipshitz, The undecidability of the word problems for projective geometries and modular lattices, *Trans. Amer. Math. Soc.* **193** (1974) 171–180.
[27] Sh. Ma, W. Fan and L. Bravo, Extending inclusion dependencies with conditions, *Theoret. Comput. Sci.* **515** (2014) 64–95.

[28] J. C. C. McKinsey, The decision problem for some classes of sentences without quantifiers, *J. Symbolic Logic* **8** (1943) 61–76.
[29] J. von Neumann, *Continuous Geometry*, Princeton Mathematical Series, Vol. 25 (Princeton University, 1960).
[30] M. O. Rabin, Recursive unsolvability of group theoretic problems, *Ann. of Math.* (*2*) **67** (1958) 172–194.
[31] Th. Skolem, Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit und Beweisbarkeit mathematischer Sätze nebst einem Theorem über dichte Mengen. *Skr. Vidensk. Krist.* **I**(4) (1920) 1–36.
[32] B. Sturmfels, *Algorithms in Invariant Theory* (Springer, New York, 2008).
[33] F. Wehrung, Congruences of lattices and ideals of rings, Chap. 8 in *Lattice Theory: Special Topics and Applications*, eds. G. Grätzer and F. Wehrung (Birkhäuser, Cham, 2014), pp. 297–335.
[34] R. Wille, Über modulare Verbände, die von einer endlichen halbgeordneten Menge frei erzeugt werden, *Math. Z.* **131** (1973) 241–249.
[35] A. Wiman, Ueber die Darstellung der symmetrischen und alternirenden Vertauschungsgruppen als Collineationsgruppen von möglichst geringer Dimensionenzahl, *Math. Ann.* **52**(2-3) (1899) 243–272.

Int. J. Algebra Comput. 2016.26:1573-1595. Downloaded from www.worldscientific.com
by DARMSTADT UNIVERSITY OF TECHNOLOGY on 02/03/26. Re-use and distribution is strictly not permitted, except for Open Access articles.