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

CHRISTIAN HERRMANN, YASUYUKI TSUKAMOTO, AND MARTIN ZIEGLER

1. Introduction

Recently, Bridson and Wilton [3] have shown that the triviality problem for finitely presented profinite groups is algorithmically unsolvable: Let G_π denote the group with (finite) presentation π and $\hat{G}_\pi$ 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 done for word problems by Gurevich [6], the *triviality problem* for a class $\mathcal{C}$ 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* satisfying assignment in some member A of $\mathcal{C}$, that is generating a non-singleton subalgebra of A. In the 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.

2. Main results

For a vector space V let $\mathrm{L}(V)$, denote the lattice of all subspaces, $\mathrm{L}_0^1(V)$ 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. An obvious example is the class of all finite dimensional F-vector spaces, $F \in \mathcal{F}$.

Our main result is the following, based on Fact 1 and the well known interpretation of rings within modular lattices, due to von Neumann [18] (cf. Lipshitz [16]).

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 unsolvable.*

"Short" conjunctions of equations which require large dimensions for satisfiablity can be constructed, explicitly. In [5] 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. Based on short presentations for alternating groups [5] and the lower bound on non-trivial irreducible representations [22] one obtains the following.

Proposition 3. *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 $O(K \log n)$ such that $\psi_n(\bar{y})$ is satisfiable in $\mathrm{L}_0^1(V)$ for some $V \in \mathcal{V}$ with $\dim V = d > 0$ for $d = n$ but not for $d < n$.*

3. Applications

3.1. **Computational Geometry.** Recall, that a Grassmann-Cayley algebra (cf [21]) 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 $A \cap B = 0$. Inspection of the proof of Theorem 2 yields

Corollary 4. *There is no algorithm to decide satisfiability, of conjunctions of equations between simple expressions. within the class of Grassmann-Cayley algebras over $V \in \mathcal{V}$.*

3.2. **Relation algebras, databases, and Independence Logic.** From Theorem 2 one gets, easily, unsolvability of the satisfiability problem for the class of subgroup lattice of finite abelian groups. Using the approach of [9,10] and [7] we derive the following three corollaries.

Corollary 5. *The satisfiability problem for the class of finite relation algebras (with or without complementation) is unsolvable.*

Corollary 6. *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.*

Cf. [17] for an analogous result on sets of conditional inclusion and conditional functional dependencies.

Corollary 7. *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.*

3.3. **Matrix rings.** Let $\mathsf{End}(V)$ denote the endomorphism ring of the vector space V, with unit id_V. Since the operations of $\mathrm{L}_0^1(V)$ can be defined by positive formulas within $\mathsf{End}(V)$, Theorem 2 implies the following.

Corollary 8. *The satisfiability problem for $\{\mathsf{End}(V) \mid V \in \mathcal{V}\}$ is unsolvable.*

3.4. **Inner product spaces.** If V is a finite dimensional vector space over a field with involution $r \mapsto r^\dagger$ and endowed with an anisotropic $\dagger$-hermitean form, then $\mathrm{L}_0^1(V)$ becomes a (modular) *ortholattice* $\mathrm{L}^\perp(V)$ with *orthocomplementation* $U \mapsto U^\perp$ (observe that here any conjunction of equations is equivalent to an equation $t(\bar{x}) = \mathbf{1}$). 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 8 one has the following.

Corollary 9. *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.*

We have constructed, elsewhere, a sequence $2k+1$-variable ortholattice terms t_k and length in $O(k)$ such that $t_k(\bar{x}) = \mathbf{1}$ is satisfiable in $\mathrm{L}^\perp(V)$ for $\dim V = d = 2^k$ but for no smaller d. The methods of [8] yield

Corollary 10. *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.*

3.5. **Finite dimensional Hilbert spaces.** Motivated by the possible role of these structures in the analysis of Quantum Computation [2,4], in [12] we dealt with the special case where $\mathbb{F}$ is a subfield of $\mathbb{C}$ closed under conjugation and considered as a $*$-ring with this involution; also, we restricted V to have an orthonormal basis, that is to be isometrically isomorphic to $\mathbb{F}^d$ with canonical hermitean scalar product, $d = \dim V$. We considered the satisfiability problem for fixed $\mathrm{L}^\perp(\mathbb{F}^d)$, and showed it NP-complete for $d = 2$ (for $d = 1$ one has the Boolean satisfiability problem) and, for $d \geq 3$ and $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, complete for $\mathcal{BP}(\mathsf{NP}^0_{\mathbb{R}})$: a natural complexity class between NP and PSPACE [19]. Concerning the satisfiability problem for the class $\mathrm{L}^\perp(\mathbb{F}^*) = \{\mathrm{L}^\perp(\mathbb{F}^d) \mid d \in \mathbb{N}\}$, Corollary 9 gives unsolvability answering the question left open in [12, §III.C].

We also showed in [12] the decision problem for the equational theory of fixed $\mathrm{L}^\perp(\mathbb{F}^d)$ is poly-time equivalent to the complement of the satisfiability problem for $\mathrm{L}^\perp(\mathbb{F}^d)$. Concerning the equational theory of $\mathrm{L}^\perp(\mathbb{F}^*)$, if an identity $t = \mathbf{1}$ fails in $\mathrm{L}^\perp(\mathbb{F}^*)$ then it fails in $\mathrm{L}^\perp(\mathbb{F}^d)$ with d the number of occurences of variables in the negation normal form of t [11]. Thus, for $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ these decision problems for the equational theory of $\mathrm{L}^\perp(\mathbb{F}^d)$ resp. $\mathrm{L}^\perp(\mathbb{F}^*)$ belong to $\mathrm{co}\mathcal{BP}(\mathsf{NP}^0_{\mathbb{R}}) \subseteq \mathsf{PSPACE}$. The analoguous results can be shown for the equational theories of $\mathsf{End}^\dagger(\mathbb{F}^d)$ resp. $\{\mathsf{End}^\dagger(\mathbb{F}^d) \mid d \in \mathbb{N}\}$. Compare this with the lower bounds on proof complexity due to Li and Tzameret [15].

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] R.V. Book, F. Otto, String-rewriting Systems. Texts and Monographs in Computer Science. Springer-Verlag, New York (1993).

[2] J. Bub: "Quantum Computation from a Quantum Logical Perspective", pp.281–296 in *Quantum Information and Computation* vol.**7:4** (2007).

[3] M.R. Bridson, H. Wilton: "The Triviality Problem for Profinite Completions", to appear in *Invent.Math,*, arXiv1401.2273v3 (2015).

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

[5] R.M. Guralnick, W.M. Kantor, M.Kassabov, A.Lubotzky: "Presentations of Finite Simple Groups: A Computational Approach", pp. 391–458 in *J. Eur. Math. Soc.* vol. **13** (2011).

[6] Y. Gurevich: "The Word Problem for some Classes of Semigroups" (Russian), pp.25–35 in *Algebra and Logic* vol.**5:2** (1966)

[7] M. Hannula, J. Kontinen: "A Finite Axiomatization of Conditional Independence and Inclusion Axioms", to appear in *Information and Computation* (2015).
[8] C. Herrmann: "Rahmen und erzeugende Quadrupel in modularen Verbänden", pp.357–387 in *Algebra Universalis* vol.**14** (1982).
[9] C. Herrmann: "Frames of Permuting Equivalences", pp.93–101 in *Acta Sci. Math.* vol.**51:1-2** (1987).
[10] C. Herrmann: "On the Undecidability of Implications between Embedded Multivalued Database Dependencies", pp.221–235 in *Inform. and Comput.* vol.**122** (1995).
[11] C. Herrmann: "On the Equational Theory of Projection Lattices of Finite von-Neumann Factors", pp.1102–1110 in *J. Symbolic Logic* vol.**75:2** (2010).
[12] C. Herrmann, M. Ziegler: "Computational Complexity of Quantum Satisfiability", pp.175–184 in *Proc. 26th Annual IEEE Symposium on Logic in Computer Science* (2011).
[13] C. Herrmann, M. Ziegler: "Computational Complexity of Quantum Satisfiability", `arXiv:1004.1696`
[14] O.G. Kharlampovich, M.V. Sapir: "Algorithmic Problems in Varieties", pp.379–602 in *Internat. J. Algebra Comput.* vol.**5:4–5** (1995).
[15] F. Li, I. Tzameret: "Generating Matrix Identities and Proof Complexity", http://eccc.hpi-web.de/report/2013/185
[16] L. Lipshitz: "The Undecidability of the Word Problems for Projective Geometries and Modular Lattices", pp.171–180 in *Trans. Amer. Math. Soc.* vol.**193** (1974).
[17] Sh. Ma, W. Fan, L. Bravo: "Extending Inclusion Dependencies with Conditions", pp.64–95 in *Theoret. Comput. Sci.* vol. **515** (2014).
[18] J.von Neumann: *Continuous Geometry*, Princeton Math.Series no.**25** (1960).
[19] J. Renegar: "Recent Progress on the Complexity of the Decision Problem for the Reals", pp.287–308 in *Discrete and Computational Geometry: Papers from the DIMACS Special Year* (J.E. Goodman et al. eds), vol.**6** Amer. Math. Soc. (1992).
[20] A.M. Slobodskoi: "Undecidability of the universal theory of finite groups". pp. 207–230, 251 in *Algebra i Logika* vol. **20:2** (1981).
[21] B. Sturmfels: *Algorithms in invariant theory*, Texts and Monographs in Symbolic Computation. Springer (2008).
[22] A. Wiman: "Ueber die Darstellung der symmetrischen und alternirenden Vertauschungsgruppen als Collineationsgruppen von möglichst geringer Dimensionenzahl", pp. 243–279 in *Math.Ann.* vol. **52:2-3** (1988).

TU Darmstadt (GERMANY) and Kyoto University (JAPAN)

Full version of paper on
`http://www.mathematik.tu-darmstadt.de/~herrmann/sat6.pdf`
submitted April 19 2015 to: International Journa; of Algebra and Computation; Editor Olga Kharlampovich