Non-effective quantifier elimination

Mihai Prunescu [*]

Abstract

General connections between quantifier elimination and decidability for first order theories are studied and exemplified.
A.M.S.-Classification: 03C10, 03D80.

1 Introduction

We start by recalling the following definition: given a first order formal language L and an L-structure S, one says that (the first order theory of) S admits elimination of quantifiers (shortly E) if for every well formed L-formula φ there is a quantifier-free L-formula ψ such that Free $(\psi) \subseteq$ Free $(\varphi) = \{\vec{x}\}$ and

$$S \models \forall \vec{x} \; (\varphi(\vec{x}) \;\leftrightarrow\; \psi(\vec{x})).$$

We say that (the first order theory of) S allows an effective elimination procedure (shortly EE) iff, in case that L is finite or has a recursive presentation, S allows E and there is a deterministic algorithm finding for all formulas φ a quantifier-free equivalent formula ψ.
The property to eliminate quantifiers is not related to some particular mathematical content. The procedure of introducing new predicates for all formula that doesn't eliminate, called by Bruno Poizat "Morleysation", has the following consequence: If L be a formal language and S is any L-structure, then there is an extension $\tilde{L}$ of L with cardinality $|\, L \,| \leq |\, \tilde{L} \,| \leq \max(|\, L \,|, \; \aleph_0)$ and there is an $\tilde{L}$-expansion $\tilde{S}$ of S such that the theory Th $_{\tilde{L}}$ $(\tilde{S})$ admits quantifier elimination. Most of the usual structures which are known to admit elimination, as like the ring $\mathbb{C}$, the ordered ring $\mathbb{R}$ or appropriated expansions of the rings $\mathbb{Q}_p$ allow in fact effective elimination procedures and have decidable first order theories. This fact contributes to the false belief that quantifier elimination would be always effective, or even that it was enough to get elimination for being decidable. Let us denote by D the property of a structure to have a decidable first order theory. The aim of this note is to show to what extent E, EE and D are relatively independent properties.

[*] Universität Greifswald, Germany, and IMAR, Romania.

Theorem 1: *Let L be a recursively presented formal language. For all L-structure S, the following implications are true:*

$$\begin{aligned} EE &\Rightarrow E, \\ E + D &\Rightarrow EE. \end{aligned}$$

Moreover, if L contains at least a constant, a relation and a function then there are no other generally true statements involving only E, EE and D.

Proof: The first implication is trivial, the second one is easy. We will concentrate on the proof of the second part. The proof will be done by giving counterexamples. It is sufficient to consider the case of L consisting of exactly one constant 0, one unary relation symbol V and one unary function symbol s because L-structures can interpret any other more complicated languages by forgetting variables. For example a binary relation R can always be interpreted as $R(x, y) \leftrightarrow V(x)$ etc.

2 $\mathbb{Z}$-structures

Definition: For the given language L, by a **$\mathbb{Z}$-structure** we mean an L-structure S, whose underlying set is a disjoint union of copies of the set $\mathbb{Z}$ of all rational integers called **components**. The function s acts like the classical successor function in all components. Some element of a component interprets 0.

Over $\mathbb{Z}$-structures it is convenient to write shortly $x + k$ for the term $s^k(x)$, and only k for the term $s^k(0)$. Instead of the formulas $V(x)$ and $\neg V(x)$ we introduce the alternative notation $1(x)$ and $0(x)$. This notation is inspired by the characteristic function of the unary predicate and will be generalized as follows:

Definition: A word $w \in \{0, 1\}^*$ given by $w = \epsilon_0 \dots \epsilon_n$ **occurs** in a $\mathbb{Z}$-structure S iff

$$S \models \exists\, x\; \epsilon_0(x) \wedge \epsilon_1(x + 1) \wedge \dots \wedge \epsilon_n(x + n).$$

We write shortly $S \models \exists\, x\; w(x)$. We will say that the word occurs **infinitely** many times iff the set defined in S by the quantifier-free formula $w(x)$ is infinite.

Theorem 2: *Let S be a $\mathbb{Z}$-structure. If at least one of the following conditions holds:*
a) For all binary words $w \in \{0, 1\}^*$, if $S \models \exists x\; w(x)$ then $S \models \exists^\infty x\; w(x)$.
b) S consists of only one component.
Then the first order theory of S admits quantifier elimination in the language L extended with the predecessor function p.

Proof: It is sufficient to describe the elimination of one existential quantifier. We consider a formula $\exists\, y\; \varphi(\vec{x}, y)$, where φ is quantifier-free. We observe also that the existential quantifier commutes with the principal disjunction of some disjunctive normal form:

$$\exists y \bigvee k_i(\vec{x}, y) \leftrightarrow \bigvee \exists y\ k_i(\vec{x}, y).$$

So we may suppose that φ is a conjunction of atomic formulas and negations of atomic formulas.
If some atomic formula has the form $x_i + k = y + l$ or $k = y + l$, we write it in some equivalent form $y = x_i + m$, $y = m$, $x_i = y + m$ or $y + m = 0$ respectively ($m \in \mathbb{N}$). In the first two cases we delete this atomic formula and the existential quantifier itself, and we substitute every occurrence of y by the term $x_i + m$, respectively m. In the other cases, we make use of the predecessor and pass to equivalent formulas $y = x_i - m$ or $y = -m$. Then we continue like before.
If there is no such atomic formula in the conjunction, we write φ in the form:

$$\exists y \quad \psi(\vec{x}) \wedge \bigwedge y \neq x_{i_j} + k_j \wedge \bigwedge y \neq m_j \wedge \gamma(y).$$

Here contains ψ only the free variables $\vec{x}$ and possibly the constant 0, and γ contains only the variable y, possibly in mixed equalities with the constant 0. There are not negated equalities or formulas containing 0 alone in γ.
All that $\gamma(y)$ could express is some information about a word in S around the individual denoted by y. If every word in S occurs infinitely many times in S, the finitely many middle inequalities do not express any relevant information. Our existential formula is then equivalent with $\exists y\ \psi(\vec{x}) \wedge \gamma(y)$, and finally with

$$\psi(\vec{x}) \wedge \exists y\ \gamma(y).$$

Now, if the statement $\exists y\ \gamma(y)$ is false over S, then the formula is equivalent with the quantifier-free contradiction $0 \neq 0$. If the statement $\exists y\ \gamma(y)$ is true in S, then the formula is equivalent with the quantifier-free formula $\psi(\vec{x})$. If ψ is empty, we write $0 = 0$.
If there was an effective procedure to decide the truth for existential conjunctive statements $\exists y\ \gamma(y)$ over S, then S allows an effective elimination procedure.
If the structure consists of only one component $\mathbb{Z}$ all elements are expressible by constant terms is p, s and 0. Like before, it is sufficient to consider simple existential conjunctive formulas without mixed equalities. In any of the situations met above we are done.
If $\mathbb{Z}_V \models \exists^m y\ \gamma(y)$, these y's interpret constant terms $a_1, \dots, a_m$, and our formula is equivalent with:

$$\psi(\vec{x}) \wedge \bigvee_{i=1}^{m} (\bigwedge_j a_i \neq x_{s_j} + k_j \wedge \bigwedge_j a_i \neq l_j).$$

If a one-component structure has a decidable theory, then there must be an effective elimination procedure for this structure, as remarked in Theorem 1. On the other side, for recursive V is the set of all true quantifier-free statements decidable, thus the existence of an effective elimination procedure implies decidability for the first order theory. □

3 Theories with essentially non-effective elimination

As motivation for the following results, we start by making an inspiring mistake.

Mistake: *There are $2^{\aleph_0}$ possible predicates V over $\mathbb{Z}$ and all the resulting structures admit quantifier elimination. Because there are at most $\aleph_0$ possible elimination procedures, there must be (uncountably many) structures over $\mathbb{Z}$ that admit quantifier elimination but don't allow effective elimination procedures.*

In the next section $2^{\aleph_0}$ different structures over $\mathbb{Z}$ allowing the same elimination procedure will be displayed.

It is not difficult to produce structures without effective elimination using the first part of Theorem 2. Let S_n be the structure $(\mathbb{Z}, s, p, V)$ without 0 with a predicate V whose characteristic sequence is periodic and contains 1-blocks of length $n \geq 0$, creating the sequence $\dots 0\,1^n\,0\,1^n\,0\,1^n\,0 \dots$. For a subset $T \subseteq \mathbb{N}$ let the $\mathbb{Z}$-structure S_T be given by the disjoint union:

$$S_T := \bigsqcup_{n \in T} S_n,$$

where an element in some component S_n interprets 0. All structures S_T admit quantifier elimination, but S_T allows an effective elimination procedure $\Leftrightarrow$ T is recursive.

Theorem 3: *There are recursive $\Theta \subset \mathbb{Z}$ such that the structure $(\mathbb{Z}, 0, s, p, \Theta)$ admits quantifier elimination but does not allow effective elimination procedures.*

Proof: For constructing a recursive predicate Θ over $\mathbb{Z}$ which has the desired properties, we consider a subset $T \subset \mathbb{N}$ that is recursively enumerable but not recursive and a recursive enumeration $(s_n)_{n \geq 1}$ that covers T. The predicate Θ is defined as follows. For the positive part of $\mathbb{Z}$, Θ has the characteristic sequence given by $1^{s_1}\,0\,1^{s_2}\,0 \dots 0\,1^{s_n}\,0 \dots$. For the negative part of $\mathbb{Z}$, let Θ be empty.
Θ is recursive, so the quantifier-free true statements over $\mathbb{Z}_\Theta$ is decidable. $\mathbb{Z}_\Theta$ admits quantifier elimination according to Theorem 2. If there was some effective elimination procedure, the theory of $\mathbb{Z}_\Theta$ should have been decidable. This is not the case, because we cannot decide the existential propositions like $\exists\, x \;\; 01^k0(x)$. □

Corollary: *Using non-recursive sets for T, we get $2^{\aleph_0}$ structures S_T that admit quantifier elimination and do not allow any effective elimination procedure. Over $\mathbb{Z}$ we get also $\aleph_0$ recursively presented structures $\mathbb{Z}_\Theta$ with the same properties.*

We notice the following **conjecture**: *There are uncountably many structures $\mathbb{Z}_\Theta$ with one component and essentially non-effective elimination.*

4 Undecidable theories with effective elimination

Definition: For a subset $T \subseteq \mathbb{N}$ we define a structure $\mathbb{Z}_V = (\mathbb{Z}, 0, s, p, V)$, with the following predicate V: In the negative side of $\mathbb{Z}$, let V be $-T$. For the non-negative elements, the characteristic sequence of V has the form 0110-111001011101111000100110101011 . . . . . . This sequence is constructed in the following way: the natural numbers are represented in the binary system and the representations are concatenated without punctuation. As we observe, the positive part of V is recursive and every binary word $w \in \{0,1\}^*$ occurs infinitely many times in $\mathbb{Z}_V$.

Theorem 4: *$\mathbb{Z}_V$ allows an effective elimination procedure. Moreover, the first order theory of $\mathbb{Z}_V$ is decidable if and only if T is recursive.*

Proof: According to Theorem 2, $\mathbb{Z}_V$ admits elimination. We consider again some conjunctive existential simple statement $\exists\, y\ \gamma(y)$. If some formula $y = y + k$ with $k \neq 0$ **or** some formula $y + k \neq y + k$ **or** for some term t, both formulas $V(t)$ and $\neg V(t)$ occur in the conjunction, then the statement is false. In all other cases, the statement is true.
This is sufficient for $\mathbb{Z}_V$ to have an effective elimination procedure.
Now, if Th $(\mathbb{Z}_V)$ is decidable, one can decide if $k \in T$ by deciding the truth of the statement $V(-k)$. Thus T must be recursive. □

Corollary: *Using non-recursive sets for T, we get $2^{\aleph_0}$ many one-component structures such that all of them allow the same effective elimination procedure but have different undecidable theories.*

5 Commentaries

For a complete proof of Theorem 1 we remark that structures in all remaining situations (D without E, or no such properties) are very easy to find.
In Theorem 3 we have seen recursive predicates without effective elimination procedures and in Theorem 4 non-recursive predicates with effective elimination. All examples were constructed ad-hoc.
The question if some predicate allows elimination procedures is sometimes very difficult for natural predicates. To give an example, consider the structure $\mathbb{Z}_{\mathsf{P}} = (\mathbb{Z}, 0, s, p, \mathsf{P})$, where the predicate P is given by

$$\mathsf{P}(n) \ \Leftrightarrow \ n \in \mathbb{N} \ \wedge n \text{ is a prime.}$$

$\mathbb{Z}_{\mathsf{P}}$ admits quantifier elimination, the set P is recursive, but we don't know if there is an effective elimination procedure for $\mathbb{Z}_{\mathsf{P}}$. This question seems to be more difficult as the well-known Twin Primes Conjecture. If a number-theoretic conjecture of Schinzel would be true, then this structure will be decidable (see [BJW]) and will have consequently an effective quantifier elimination.

We finish by remarking that all structures given here as examples for essentially non-effective quantifier elimination enjoy the property $P \neq NP$ in the sense of computability over algebraic structures introduced by [BSS] and generalized in [H] and [BP]. The general NP-complete problem introduced in [BP] (satisfiability for existential formulas with parameters) cannot be solved effectively in our cases. This is an extreme example of $P \neq NP$ whose complexity lies between the trivial examples without elimination and the more subtle examples with effective elimination, where the assymptotic growth of the exponential function must be used.
We mention that for the structure $(\mathbb{Z}, 0, p, s)$ the P versus NP problem in the sense of [BP] is equivalent with the classical P versus NP. It is true for all examples given by Theorem 4, also.

Acknowledgments: Armin Hemmerling put the initial questions about examples with non-effective quantifier elimination. The question came from the necessity to classify the general behavior of BSS computation systems over algebraic structures. Bruno Poizat gave the great idea to use $\mathbb{Z}$-structures during a discussion in Oberwolfach. Günter Asser was interested in finding examples without effective elimination over $\mathbb{Z}$ itself and proposed the nice example $\mathbb{Z}_\Theta$. Christian Michaux indicated us some classical results and the work of Semenov.

References

[BCSS] **Lenore Blum, Felipe Cucker, Michael Shub, Steven Smale**: *Complexity and Real Computation.* Springer-Verlag, New-York, 1998.

[BJW] **P. T. Bateman, C. G. Jockusch, A. R. Woods**: *Decidability and undecidability of theories with a predicate for the primes.* Journal of Symbolic Logic, 58, 672 - 687, 1993.

[BSS] **Lenore Blum, Michael Shub, Steven Smale**: *On a theory of computation and complexity over the real numbers.* Bulletin A.M.S. 21, 1989.

[H] **Armin Hemmerling**: *On P vs. NP for parameter-free programs over algebraic structures.* Mathematical Logic Quarterly, 2000.

[AP] **Alexander Prestel**: *Einführung in die Mathematische Logik und Modelltheorie.* Vieweg Studium, 1986.

[BP] **Bruno Poizat**: *Les petits cailloux.* ALEAS, 1994.

[S] **A. L. Semenov**: *Decidability of monadic theories.* Lecture notes in computer science, 176, 162 - 175. 1984 by Springer Verlag, Berlin.

[T] **Wolfgang Thomas**: *The theory of successor with an extra predicate.* Math. Annalen 237, 121-132. 1978.