Elimination of bounded universal quantifiers standing in front of a quantifier-free arithmetical formula

Yuri Matiyasevich

Raphael M. Robinson proved in 1956 in [8] the following theorem:

For every polynomial $P(a_1, \ldots, a_n, y)$ with integer coefficients one can effectively find another polynomial $Q(a_1, \ldots, a_n, b)$ also with integer coefficients such that formula

$$\forall y_{\le b}[P(a_1, \ldots, a_n, y) = 0] \tag{1}$$

is equivalent to formula

$$Q(a_1, \ldots, a_n, b) = 0. \tag{2}$$

In other words, bounded universals quantifiers can be eliminated if they stand in front of a polynomial equality.

The proof of R. M. Robinson heavily depends on the special form of formula (1) and cannot be immediately extended to formulas of other kinds, say, of the form

$$\forall y_{\le b}[P(a_1, \ldots, a_n, y) \ne 0]. \tag{3}$$

Clearly, inequality in (3) can be transformed into an equality at the cost of introduction of an additional existential quantifier: formula (3) is equivalent to formula

$$\forall y_{\le b}\exists z[P^2(a_1, \ldots, a_n, y) = z + 1]. \tag{4}$$

A method for elimination of a bounded universal quantifier standing in front of a purely existential arithmetical formula was given in 1961 by Martin Davis, Hilary Putnam and Julia Robinson in their selebrated paper [1].

Namely, they described a method for transforming a formula of the form

$$\forall y_{\leq b} \exists z_1 \dots z_m [P(a_1, \dots, a_n, y, z_1, \dots, z_m) = 0], \tag{5}$$

where P is a polynomial with integer coefficients, into an equivalent formula of the form

$$\exists x_1 \dots x_l [E_{\mathrm{L}}(a_1, \dots, a_n, b, x_1, \dots, x_l) = E_{\mathrm{R}}(a_1, \dots, a_n, b, x_1, \dots, x_l)], \tag{6}$$

where E_{L} and E_{R} are so called *exponential polynomials*, i.e., some expressions constructed using the conventional rules from particular natural numbers and variables $a_1, \dots, a_n$, b and $x_1, \dots, x_l$, by addition, multiplication and exponentiation.

The original technique for eliminating the single universal quantifier was modified by several authors (see [4, 2]). An essentially different technique was introduced in [5]. The technique presented in [6] for Diophantine simulation of partial recursive functions can be also viewed as a method for eliminating a bounded universal quantifier because such a quantifier can be easily modelled by primitive recursion. Yet another method for eliminating bounded universal quantifiers was proposed by the author in [7].

In 1970 the author [3] improved the above mentioned result of Davis-Putnam-Robinson by showing that exponentiation is not necessary in (6), i.e., that one can find a formula which is equivalent to (5) and which has the form

$$\exists x_1 \dots x_l [Q(a_1, \dots, a_n, b, x_1, \dots, x_l) = 0], \tag{7}$$

where Q is a polynomial with integer coefficients.

Applying this technique to formula (4), we would obtain for (3) an equivalent formula of the form (7). Unfortunately, the latter formula is not quantifier-free like formula (2) was.

The goal of the present work is to obtain a kind of extention of the above cited result of R. M. Robinson to formulas of the form (3) and, more generally, to arbitrary universal arithmetical formulas. The interest in getting equivalent quantifier-free formulas is due to some applications in model theory.

In general case we cannot hope to obtain as simple quantifier-free formula as (2). The cost of elimination of a bounded universal quantifier will be the use of extra functions. Namely, besides exponentiation as in (7) we need integer division, i.e. the function $\lfloor \frac{a}{b} \rfloor$. On the other hand, we can reduced exponentiation to one-argument function 2^s.

> **Theorem** *Let $\phi(a_1, \ldots, a_n, y_1, \ldots, y_k)$ a quantifier-free arithmetical formula, i.e., a Boolean combination of polynomial equalities. Then formula*
>
> $$\forall y_{1_{\le b_1}} \ldots y_{k_{\le b_k}} \phi(a_1, \ldots, a_n, y_1, \ldots, y_k) \tag{8}$$
>
> *is equivalent to some formula of the form*
>
> $$Q(a_1, \ldots, a_n, b_1, \ldots, b_k) = 0, \tag{9}$$
>
> *where Q is an expression constructed by conventional rules from particular natural numbers and variables $a_1, \ldots, a_n$, $b_1, \ldots, b_k$ by addition, subtraction, multiplication, integer division and exponentiation with base 2; such a Q can be effectively constructed for given ϕ.*

The proof is based on technique of elimination of bounded universal quantifiers introduced by the author in [5, Section 6.3].

The present work was supported by grant 96-01-01612 from Russian Fund for Basic Research.

References

[1] Davis M., Putnam H., Robinson J. The decision problem for exponential Diophantine equations. *Annals of Mathematics, Second Series*, 74(3):425–436, 1961.

[2] Hirose K., Shigeaki I. A proof of negative answer to Hilbert's 10th Problem. *Proceedings of the Japan Academy*, 49(1):10–12,1973.

[3] Matiyasevich Yu. V. Diofantovost perechislimykh mnozhestv. *Dokl. AN SSSR*, 191(2):278–282, 1970. Translated in: *Soviet Math. Doklady*, 11(2):354-358, 1970.

[4] Matiyasevich Yu. V. Diofantovy mnozhestva. *Uspekhi Mat. Nauk*, 27:5(167), 185–222, 1972. Translated in: *Russian Mathematical Surveys*, 27(5):124–164, 1972.

[5] Matiyasevich Yu.V. *Desyataya Problema Gilberta.* Moscow, Fizmatlit, 1993. English translation: *Hilbert's tenth problem* MIT Press, Cambridge,1993. French translation: *Le dixième problème de Hilbert. Son indécidabilité.* Masson, Paris, Milan, Barcelone, 1995.

[6] Matiysevich Yu. A direct method for simulating partial recursive functions by Diophantine equations. *Annals Pure Appl. Logic*, 67, 325–348, 1994.

[7] Matiyasevich Yu.V. A new Technique for Obtaining Diophantine Representations via Elimination of bounded universal Quantifiers. *Zap. nauchn. seminar. Peterbug. otd. Mat. in-ta RAN*, 220, 83–92, 1995.

[8] R. M. Robinson. Arithmetical representation of recursively enumerable sets. *Journal of Symbolic Logic*, 21(2):162–186, 1956.