Progress in the Formalization of Matiyasevich's theorem in the Mizar system*

Karol Pąk
Institute of Computer Science,
University of Bialystok, Poland
karol@mizar.org

Abstract

We discuss the formal approach to the Matiyasevich's theorem that is known as a negative solution of Hilbert's tenth problem in the Mizar system. We present our formalization of a list of arithmetical properties that are directly used in the theorem in particular, that the equality $y = x^z$ is Diophantine.

1 Introduction

Hilbert's tenth problem is the question about the existence of a method (algorithm) that can decide whether a given polynomial equation with integer coefficients has an integral solution, or in a more modernist way, whether a given Diophantine equation has an integral solution.

The problem has an exceptional history that took seventy years to resolve, described in detail in [Mat93]. The main work to solve the problem has been done by Julia Robinson, Martin Davis and Hilary Putnam who spend a large part of their lives, over twenty years, trying to solve it. They have done a great progress to resolve it, by expressing the problem from computability theory in the notion of a Diophantine set from number theory. They proved the negative solution of Hilbert's tenth problem but under an assumption that the exponential function can be defined in a diophantine way. Yuri Matiyasevich made the final and key step, eliminating this assumption, using Fibonacci numbers which tend to an exponential growth rate. Additionally, he improved his result, using a special case of Pell's Equation, that has the form $x^2 - (a^2 - 1)y^2 = 1$, where $a > 1$ and integer numerical solutions are sought for x and y, and finally he showed that $y = x^z$ is Diophantine. In this way, he provided the crucial step that completed the proof of negative solution of Hilbert's tenth problem theorem, known as the MRDP-theorem (due to Matiyasevich, Robinson, Davis, and Putnam).

As Pell's Equation is more central to matters Diophantine, we decided to formalize Matiyasevich's theorem in a post-Matiyasevich way where the Fibonacci sequence is replaced by Pell's Equation and a Pell's Sequence, as considered by Wiesław Sierpiński [Sie64].

2 Matiyasevich's theorem in Mizar

The proof of Matiyasevich's theorem is elementary but horribly complicated. As we mentioned above, the proof is based on two concepts: the special case of Pell's Equation and Diophantine set that are elementarily-definable.

*The paper has been supported by the resources of the Polish National Science Center granted by decision n°DEC-2015/19/D/ST6/01473.

In: A. Editor, B. Coeditor (eds.): Proceedings of the XYZ Workshop, Location, Country, DD-MMM-YYYY, published at http://ceur-ws.org

Pell's Equation

It is easy to see that $\mathrm{x}_a(0) = 1$, $\mathrm{y}_a(0) = 0$ is an obvious solution of the special case of Pell's Equation. Additionally, if we know a solution of the Pell's equation, we can determine infinitely many solutions as follows:

$$\mathrm{x}_a(n+1) = a \cdot \mathrm{x}_a(n) + (a^2 - 1) \cdot \mathrm{y}_a(n), \ \mathrm{y}_a(n+1) = \mathrm{x}_a(n) + a \cdot \mathrm{y}_a(n). \tag{1}$$

In particular, we get the first non-trivial solution easily $\mathrm{x}_a(1) = a$, $\mathrm{y}_a(1) = 1$, which is not easy to construct in the general case where the equation has form $x^2 - Dy^2 = 1$ and we only know that D is a non-square natural number. Note that the existence of such a non-trivial solution is listed as #39 at Freek Wiedijk's list of "Top 100 mathematical theorems" [Fre100]. It is also important to note that Matiyasevich used dozens of properties of a special case of Pell's Equation in his proof, but he also used the existence of a non-trivial solution in the general case (for more detail see [Sie64]). Therefore, we started our formalization of Matiyasevich's theorem defining a solution of Pell's Equation (see [AP17a, AP17]) as follows:

```
definition
  let D be Nat;
  mode Pell's_solution of D → Element of [:INT,INT:]
    means :: PELLS_EQ:def 1
   (it`1)^2 - D * (it`2)^2 = 1;
end;
```

where we define a solution as a pair it of integers which fulfills the means condition where it`1 denotes the first coordinate of it and it'2 denotes the second ones.

Next we show that there is at least one pair of positive integers that is a non-trivial solution for a given D that is not a square

```
::$N #39 Solutions to Pell's Equation
theorem :: PELLS_EQ:16
  for D be non square Nat
    ex p be Pell's_solution of D st p is positive;
```

as well as that there exist infinitely many solutions in positive integers for a given not square D

```
theorem :: PELLS_EQ:17
  for D be non square Nat holds
    the set of all ab where ab is positive Pell's_solution of D
  is infinite;
```

Then, we introduce the concept of *the least positive solution* of Pell's Equation. We call a pair $\langle x_0, y_0\rangle$ of natural numbers *the least* if is a positive solution of a given Pell's Equation and for each pair $\langle x_1, y_1\rangle$ of natural numbers that also satisfies the equation holds $x_0 \leq x_1$ and $y_0 \leq y_1$. The order is partial and the least element does not have to exist in the general case, but we showed that the order is total on the set of positive solutions. We express this observation in the Mizar system as follows:

```
definition
  let D be non square Nat;
  func min_Pell's_solution_of D → positive Pell's_solution of D
    means :: PELLS_EQ:def 3
  for p be positive Pell's_solution of D holds
    it`1 <= p`1 & it`2 <= p`2;
end;
```

Based on the above functor, we define formally two sequences $\{\mathrm{x}_a(n)\}_{n=0}^{\infty}$, $\{\mathrm{y}_a(n)\}_{n=0}^{\infty}$ defined recursively above as two function Px(a,n), Py(a,n), as follow:

```
definition
  let a,n be Nat;
  assume a is non trivial;
  func Px(a,n) → Nat means :: HILB10_1:def 1
    ex y be Nat st
```

```
    it + y*sqrt (a^2-'1) =
    ( (min_Pell's_solution_of (a^2-'1))`1 +
          (min_Pell's_solution_of (a^2-'1))`2*sqrt(a^2-'1) ) |^ n;
  func Py(a,n) -> Nat means :: HILB10_1:def 2
    Px(a,n) + it*sqrt(a^2-'1) =
   ( (min_Pell's_solution_of (a^2-'1))`1 +
     (min_Pell's_solution_of (a^2-'1))`2*sqrt((a^2-'1)) ) |^ n;
end;
```

and we show the simultaneous recursion equations

```
theorem :: HILB10_1:5
  [a,1] = min_Pell's_solution_of (a^2-'1);

theorem :: HILB10_1:6
  Px(a,n+1) = Px(a,n)*a + Py(a,n)*(a^2-'1) &
  Py(a,n+1) = Px(a,n) + Py(a,n)*a;
```

as well as we prove many dependencies between individual solutions to show congruence rules

```
theorem :: HILB10_1:33
  Py(a,n1),Py(a,n2) are_congruent_mod Px(a,n) & n>0
    implies
  n1,n2 are_congruent_mod 2*n or n1,-n2 are_congruent_mod 2*n;

theorem :: HILB10_1:37
  Py(a,k)^2 divides Py(a,n) implies Py(a,k) divides n;
```

Based on this properties we provide that the equality `Py(a,z) = y` is Diophantine. For this purpose we justify that for a given `a`, `z`, `y` holds `Py(a,z) = y` if and only if the following system has a solution for natural numbers `x`, `x1`, `y1`, `A`, `x2`, `y2`:

```
  a>1 &
  [x,y] is Pell's_solution of (a^2-'1) &
  [x1,y1] is Pell's_solution of (a^2-'1) &
  y1 >= y & A > y & y >= z &
  [x2,y2] is Pell's_solution of (A^2-'1) &
  y2,y are_congruent_mod x1 &
  A,a are_congruent_mod x1 &
  y2,z are_congruent_mod 2*y &
  A,1 are_congruent_mod 2*y &
  y1,0 are_congruent_mod y^2;
```

Next, based on this result we prove that the equality $\mathtt{y} = \mathtt{x}^{\mathtt{z}}$ is also Diophantine.

```
theorem :: HILB10_1:39
   for x,y,z be Nat holds
      y = x|^z
   iff
     (y = 1 & z = 0) or (x = 0 & y = 0 & z > 0) or (x = 1 & y = 1 & z > 0)
    or (x > 1 & z > 0 &
      ex y1,y2,y3,K be Nat st
        y1 = Py(x,z+1) & K > 2*z*y1 & y2 = Py(K,z+1) & y3 = Py(K*x,z+1) &
        (0 <= y-y3/y2 <1/2 or 0 <= y3/y2-y < 1/2));
```

Note that complete formal proofs are available in [Pak17].

Diophantine sets

Diophantine sets are defined in informal mathematical practice as the set of all solutions of a Diophantine equation of the form $P(x_1,\ldots,x_j,y_1,\ldots,y_k) = 0$ (often denoted briefly by $P(\overline{x},\overline{y}) = 0$) where P is a $n+k$–variable polynomial with integer coefficients. However, Diophantine set is parameterized only by natural number n that plays the role of the dimension. Let us consider a subset D of all finite sequences of length n numbered from 0 developed in the Mizar Mathematical Library [BBGKMP] as `n-element XFinSequence`. D is called *Diophantine* if there exist a natural number k and a $n+k$–variable polynomial p such that each coefficient is an integer number and

$$\forall_{x:n\mapsto\mathbb{N}}\, x \in D \Longleftrightarrow \exists_{x:n\mapsto\mathbb{N}}\, p(\overline{x},\overline{y}) = 0. \tag{2}$$

Our Mizar version of the definition is already formulated in [Pak18] as follows:

```
definition
  let n be Nat;
  let D be Subset of n -xtuples_of NAT;
  attr D is diophantine means :: HILB10_2:def 6
    ex m being Nat, p being INT-valued Polynomial of n+m,F_Real st
      for s be object holds
          s in D iff ex x being n-element XFinSequence of NAT,
                         y being m-element XFinSequence of NAT st
                           s = x & eval(p,@(x^y)) = 0;
end;
```

Now we are ready to express and to prove algebraic equivalence formulated above in terms of Diophantine sets as follows.

```
theorem :: HILB10_3:23
  for n  be  Nat
    for i1,i2,i3 be Element of n holds
      {p where p is n-element XFinSequence of NAT: p.i1 = Py(p.i2,p.i3) & p.i2 > 1}
    is diophantine Subset of n -xtuples_of NAT;

theorem :: HILB10_3:24
  for n be Nat
    for i1,i2,i3 be Element of n holds
      {p where p is n-element XFinSequence of NAT: p.i2 = (p.i1) |^ (p.i3)}
    is diophantine Subset of n -xtuples_of NAT;
```

Note that these two theorems can be found in the proof script `HILB10_3.miz` available at the authors' web site `http://alioth.uwb.edu.pl/~pakkarol/FMM2018/`.

3 Conclusions

Our formalization has so far focused on the Diophantine property of two equations. We showed formally in the Mizar system that from the diophantine standpoint these equations can be obtained from lists of several basic Diophantine relations. We introduced also a concept of Diophantine set and we checked the usability of our concept proving that these equations are Diophantine Now we are working on the next equations explored in Matiyasevich's theorm to show finally that *Every computably enumerable set is Diophantine.*

References

[AP17] Marcin Acewicz and Karol Pąk. Formalization of Pell's Equations in the Mizar System. In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017*, pages 223–226, 2017.

[AP17a] Marcin Acewicz and Karol Pąk. The Pell's Equation. *Formalized Mathematics*, 2017.

[BBGKMP] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The Role of the Mizar Mathematical Library for Interactive Proof Development in Mizar. *J. Autom. Reasoning*, 61(1-4):9–32, 2018.

[Mat93] Yuri Matiyasevich. *Hilbert's Tenth Problem.* MIT Press, Cambridge, Massachusetts, 1993.

[Pak17] Karol Pąk. The Matiyasevich Theorem. Preliminaries. *Formalized Mathematics*, 2017.

[Pak18] Karol Pąk. Diophantine Sets. Preliminaries. *Formalized Mathematics*, 2018.

[Sie64] Wacław Sierpiński. *Elementary Theory of Numbers.* Mathematical Institute of the Polisch Academy of Science, 1964.

[Fre100] Freek Wiedijk. Formalizing 100 Theorems.