Jonas Bayer

March 28, 2019

On (Hilbert, Isabelle) and universal pairs

Illustration: Rebecca Wilhelm

Context

1900	ICM in Paris: Hilbert's list of 23 problems
1970	Yuri Matiyasevich publishes answer to the tenth problem
2017	Start of the formalization & universal pairs project
08/03/18	First universal pair $(11, \delta)_{\mathbb{Z}}$ in the integers
24/05/18	"Matiyasevich meets Isabelle"

Content

Hilbert's Tenth Problem

The problem

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von rationalen Operationen entscheiden lässt, ob die Gleichung in ganzen Zahlen lösbar ist.

DEF A **diophantine equation** is a polynomial equation with integer coefficients

Examples:

$$5x - 10 = 0 \qquad x_1^2 - 4x_2 = x_3 \qquad x^3 + y^3 = z^3$$

Diophantine equations and sets

Parametric diophantine equation

$$a - y^2 = 0$$

Parameter a Variable y

Set of square numbers

1 49 4

0

16 ... 25

Diophantine equations and sets

Parametric diophantine equation

$$a - (y_1 + 2)(y_2 + 2) = 0$$

$$a = (y_1 + 2)(y_2 + 2)$$

Composite numbers

6 9 4

8

10 125 …

DEF A set $A \subseteq \mathbb{N}$ is called a **diophantine set** if there is a polynomial $P(a, y_1, \ldots, y_\nu)$ with integer coefficients such that

$$a \in A \Leftrightarrow \exists y_1, \ldots, y_\nu : P(a, y_1, \ldots, y_\nu) = 0$$

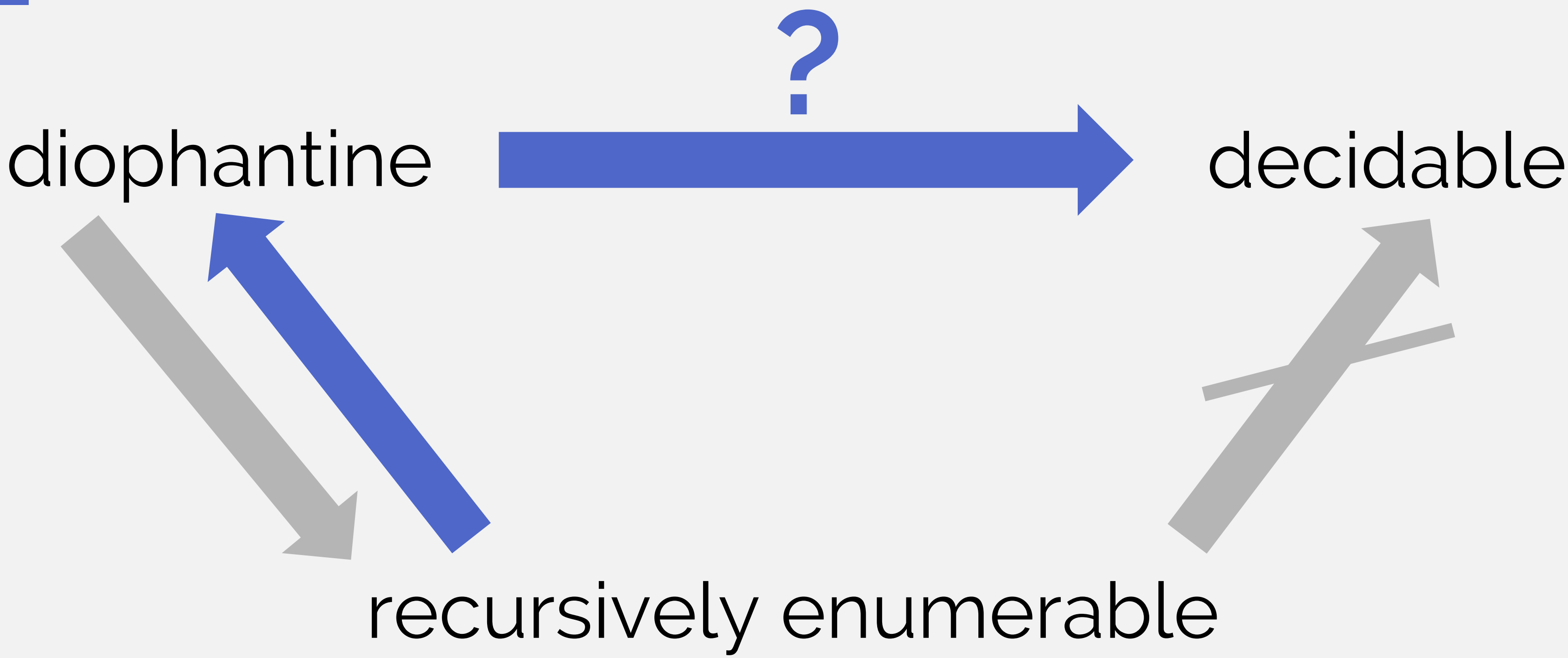
Undecidability of Hilbert's problem

1900

diophantine → decidable

1950 Julia Robinson and Martin Davis conjecture undecidability

Undecidability of Hilbert's problem



THM

DPRM Theorem.

Every recursively enumerable set is diophantine.

Undecidability of Hilbert's problem

diophantine $\not\Longrightarrow$ decidable

=

recursively enumerable

Hilbert's tenth problem is unsolvable!

THM **DPRM Theorem.**

Every recursively enumerable set is diophantine.

Structure of the DPRM Theorem

recursively enumerable → diophantine

recursively enumerable → exponential diophantine

exponential diophantine → diophantine (1970)

Exponential diophantine equations simulate computational model
⟶ Here: Register Machines

Diophantine equation with exponentially growing solutions ⟶ Polynomial representation of $a = b^c$

Questions?

The formalization of the DPRM Theorem or

Hilbert meets Isabelle

Proofs with computers

Proofs using computations
Computations carried out by a computer

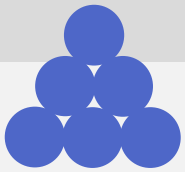
Computer verified proofs
Full verification of all logical steps down to the axioms

Automated Theorem Provers
The computer comes up with a formal proof

$a^2 + b^2 = c^2$

Pythagorean triples problem

Interactive Theorem Provers
A proof is manually implemented



Kepler conjecture and Four Colour theorem

Formalizing a Hilbert Problem

Fall 2017

Yuri Matiyasevich on visit in Bremen:
suggests **formalization** of the DPRM theorem

Students had knowledge from previous project

Tools have advanced

Theorem Prover: Isabelle

Online available at

isabelle.in.tum.de/website-Isabelle2018

Isabelle / HOL

Interactive Theorem Prover

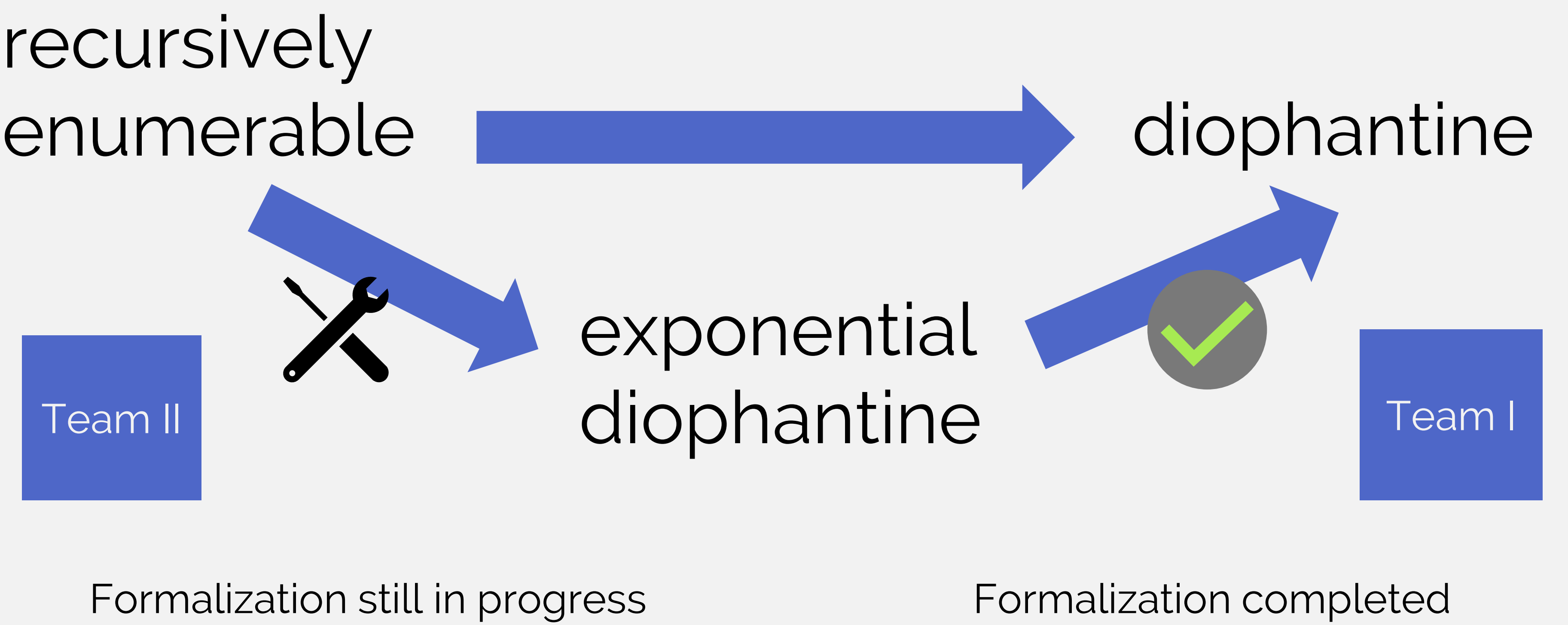
Functional Programming + Higher Order Logic

- Small logic core
- Fixed types

Live Demo

Formalizing the DPRM Theorem

Splitting up the work:



Register machines

Program with instructions:

Active state

Registers that store natural numbers

Challenge for the formalization

Time

	q	$\cdots$	$t+1$	t	$\cdots$	0	
S1	$s_{1,q}$	$\cdots$	$s_{1,t+1}$	$s_{1,t}$	$\cdots$	$s_{1,0}$	s_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Sk	$s_{k,q}$	$\cdots$	$s_{k,t+1}$	$s_{k,t}$	$\cdots$	$s_{k,0}$	s_k
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Sm	$s_{m,q}$	$\cdots$	$s_{m,t+1}$	$s_{m,t}$	$\cdots$	$s_{m,0}$	s_m
R1	$r_{1,q}$	$\cdots$	$r_{1,t+1}$	$r_{1,t}$	$\cdots$	$r_{1,0}$	r_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Rl	$r_{l,q}$	$\cdots$	$r_{l,t+1}$	$r_{l,t}$	$\cdots$	$r_{l,0}$	r_l
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Rn	$r_{n,q}$	$\cdots$	$r_{n,t+1}$	$r_{n,t}$	$\cdots$	$r_{n,0}$	r_n

Lessons learned and outlook

- Formalizing mathematics is feasible
- Isabelle can be learned and handled by non-experts!
- The exact implementation matters a lot
- Spending 10 hours on its proof don’t correct the lemma

What do you think about formalizing mathematics?

On universal pairs

Complicated diophantine equations

Prime numbers are recursively enumerable
$\longrightarrow$ What is their diophantine representation?

$$
\begin{aligned}
(k+2)\Big\{1 &- [wz+h+j-q]^2 \\
&- [(gk+2g+k+1)(h+j)+h-z]^2 \\
&- [2n+p+q+z-e]^2 \\
&- \left[16(k+1)^3(k+2)(n+1)^2+1-f^2\right]^2 \\
&- \left[e^3(e+2)(a+1)^2+1-o^2\right]^2 \\
&- \left[(a^2-1)y^2+1-x^2\right]^2 \\
&- \left[16r^2y^4(a^2-1)+1-u^2\right]^2 \\
&- [n+l+v-y]^2 \\
&- \left[\left((a+u^2(u^2-a))^2-1\right)(n+4dy)^2+1-(x+cu)^2\right]^2 \\
&- \left[(a^2-1)l^2+1-m^2\right]^2 \\
&- \left[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x\right]^2 \\
&- \left[z+pl(a-p)+t(2ap-p^2-1)-pm\right]^2 \\
&- [ai+k+1-l-i]^2 \\
&- \left[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m\right]^2\Big\}.
\end{aligned}
$$

Are there “simpler” equations?

Universal pairs as one measure of complexity

DEF A tuple $(\nu, \delta)_{\mathbb{N}}$ is called a **universal pair** if any diophantine set A can be represented by a diophantine equation in ν variables with degree δ

that is there exists a polynomial $P(a, y_1, \dots, y_\nu)$ of degree δ such that

$$a \in A \Leftrightarrow \exists y_1, \dots, y_\nu \in \mathbb{N}^\nu \colon P(a, y_1, \dots, y_\nu) = 0$$

DEF One defines universal pairs $(\nu, \delta)_{\mathbb{Z}}$ with variables $y_1, \dots, y_\nu$ in $\mathbb{Z}$ analogously.

Alternatively: Consider number of operations

How to find universal pairs

DEF An equation $U(a, i, y_1, \dots, y_\nu) = 0$ is called a **universal diophantine equation**, if for any diophantine set A there is a natural number I such that $U(a, I, y_1, \dots, y_\nu)$ represents A.

Already known and constructed in $\mathbb{N}$
$\longrightarrow$ obtain universal pairs e.g. $(58, 4)_{\mathbb{N}}$ and $(10, 8.6 \times 10^{44})_{\mathbb{N}}$

Four squares theorem:
Any $n \in \mathbb{N}$ is given by
$$x^2 + y^2 + z^2 + w^2$$

Stronger theorem:
Any $n \in \mathbb{N}$ is given by
$$x^2 + y^2 + z^2 + z$$

Using substitution in the integers one has:

$(174, 4)$ $(114, 16)$ $(96, 24)$ $(84, 40)$ $(78, 48)$

$(75, 56)$ $(63, 192)$ $(57, 5336)$ $(42, 4 \times 10^5)$

$(36, 2.6 \times 10^{44})$ $(33, 9.2 \times 10^{44})$ $(30, 1.7 \times 10^{45})$

The universal pair $(11, \delta)_{\mathbb{Z}}$

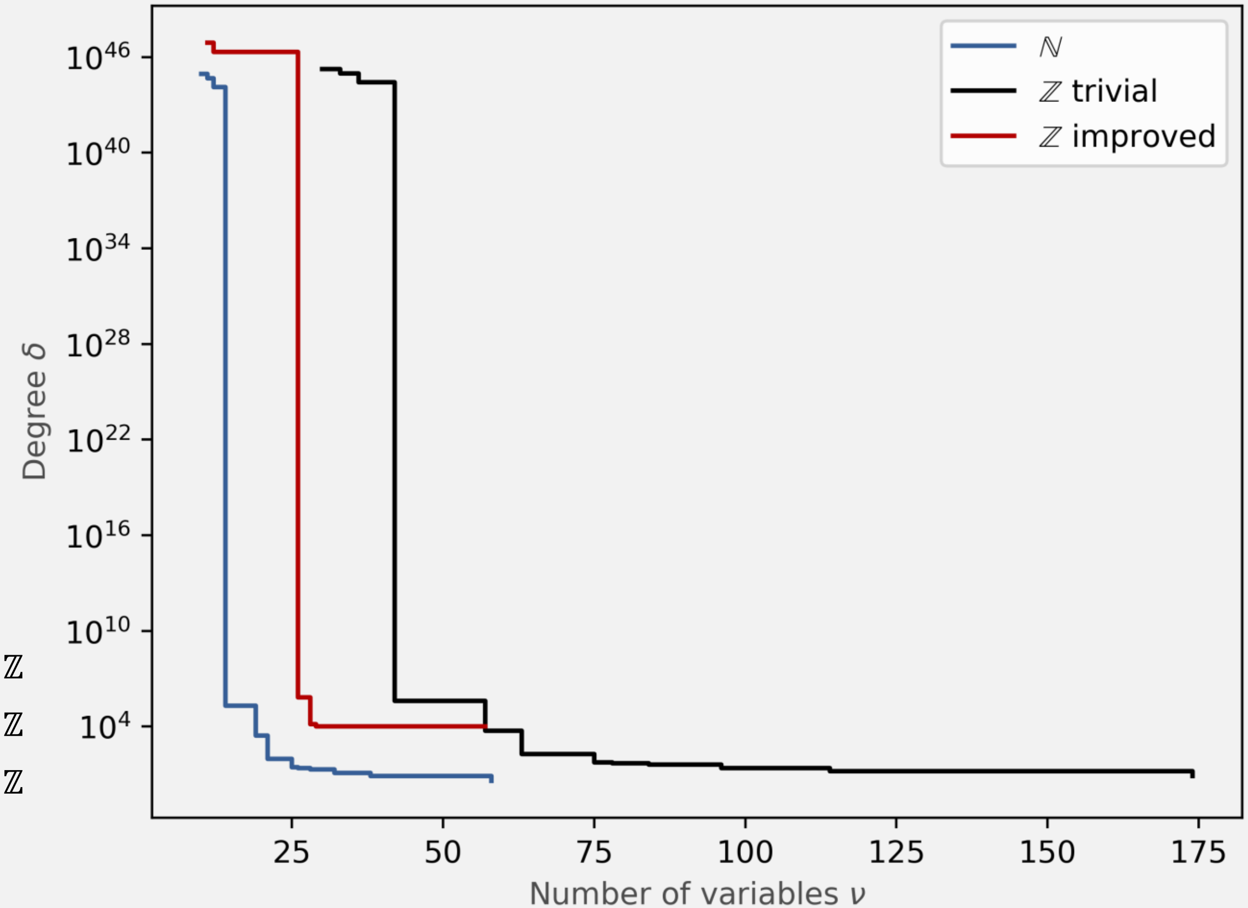
THM: Any diophantine set can be represented using only 11 integer valued variables (Zhi-Wei Sun).

- Proof uses Matiyasevich's *Masking* approach
- Inequalities are avoided
- The necessity to be positive-valued is eliminated for all but one variable

BUT: No calculation of needed degree

THM: $(11,\ 807688886662009041096919362172409149427641 6)_{\mathbb{Z}}$ is a universal pair

How can we improve this?



$(26, 657680)_{\mathbb{Z}}$
$(28, 13640)_{\mathbb{Z}}$
$(29, 10028)_{\mathbb{Z}}$

Questions?

Thank you for your attention!

And a lot of thanks to

- Malte Haßler and Simon Dubischar who worked on universal pairs
- Everyone involved in the formalization workgroup:
  Deepak Aryal, Bogdan Ciurezu, Yiping Deng, Marco David, Prabhat Devkota, Simon Dubischar, Malte Sophian Haßler, Yufei Liu, Maria Oprea, Abhik Pal and Benedikt Stock
- Abhik Pal, Marco David and Benedikt Stock in particular for their promotion of the formalization project at Jugend forscht, EUCYS and many other places
- Dierk Schleicher, our project mentor
- Mathias Fleury, Christoph Benzmüller and everyone else from the theorem proving community who supported us
- Yuri Matiyasevich, who initiated these projects
- Rebecca Wilhelm for the great illustrations of Hilbert, Matiyasevich and the Isabelle logo

jonas.bayer@fu-berlin.de

Resources

The full proof by Yuri Matiyasevich:

Matiyasevich, Y. : Hilbert's tenth problem. MIT Press (1993)

A tutorial/introduction to Isabelle:

Nipkow, T., Klein, G.: Concrete Semantics. Springer (2014)

One can also find an up to date version as a PDF document in Isabelle ("prog-prove" in the menu on the right)

Universal pairs:

Jones, J. P.: Universal Diophantine Equations. In *The journal of Symbolic Logic, Vol. 47, No. 3 (Sep., 1982), pp. 549-571*

Zhi-Wei, S.: Further results on Hilbert's tenth problem. Only on arXiv:1704.03504