Jonas Bayer[1], Marco David[2], Abhik Pal[2],
Benedikt Stock[2] and Dierk Schleicher[3]

September 10, 2019

The DPRM-Theorem in Isabelle

[1] Freie Universität Berlin
[2] Jacobs University Bremen
[3] Technische Universität Berlin and Aix-Marseille Université

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:

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

The problem

Is there an algorithm to determine, if a given diophantine equation has a solution in the integers?

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

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

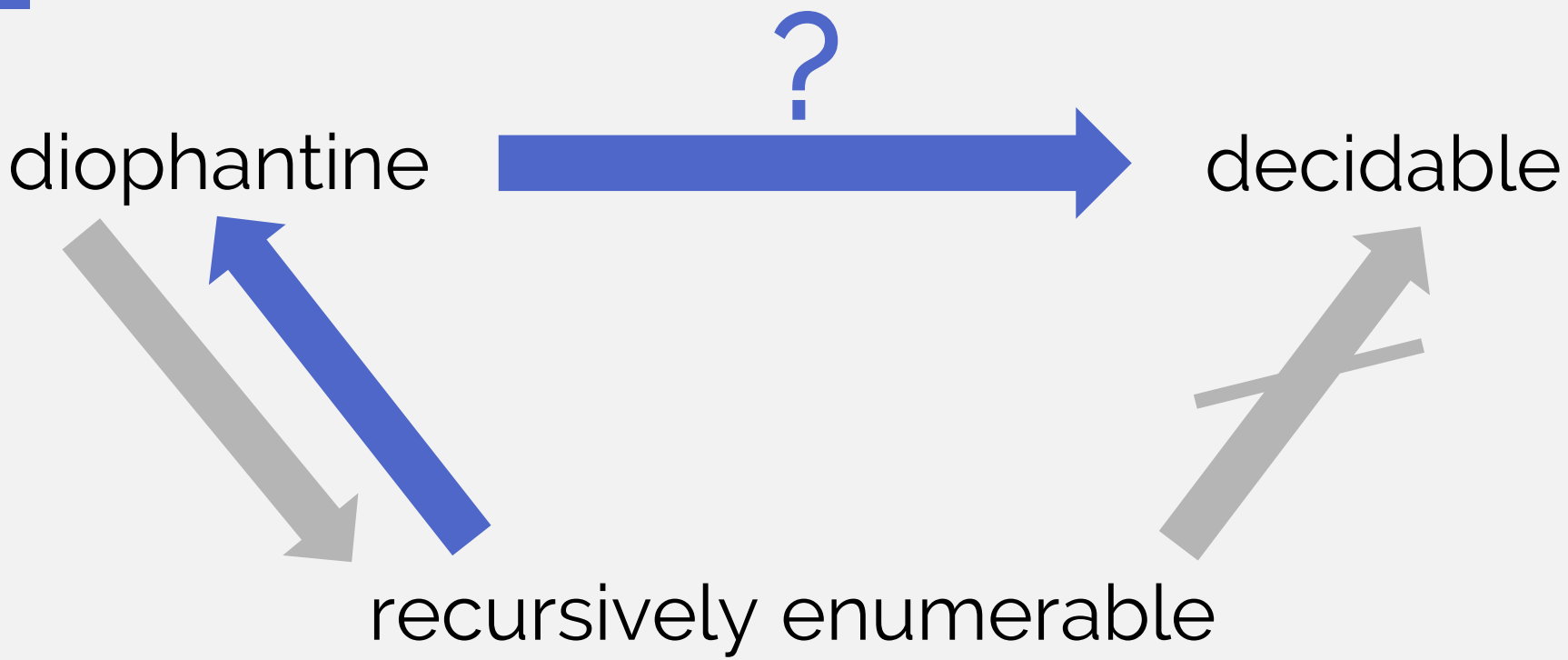
Undecidability of Hilbert's problem

1900

diophantine ? decidable

1950 Julia Robinson and Martin Davis conjecture undecidability

Undecidability of Hilbert's problem

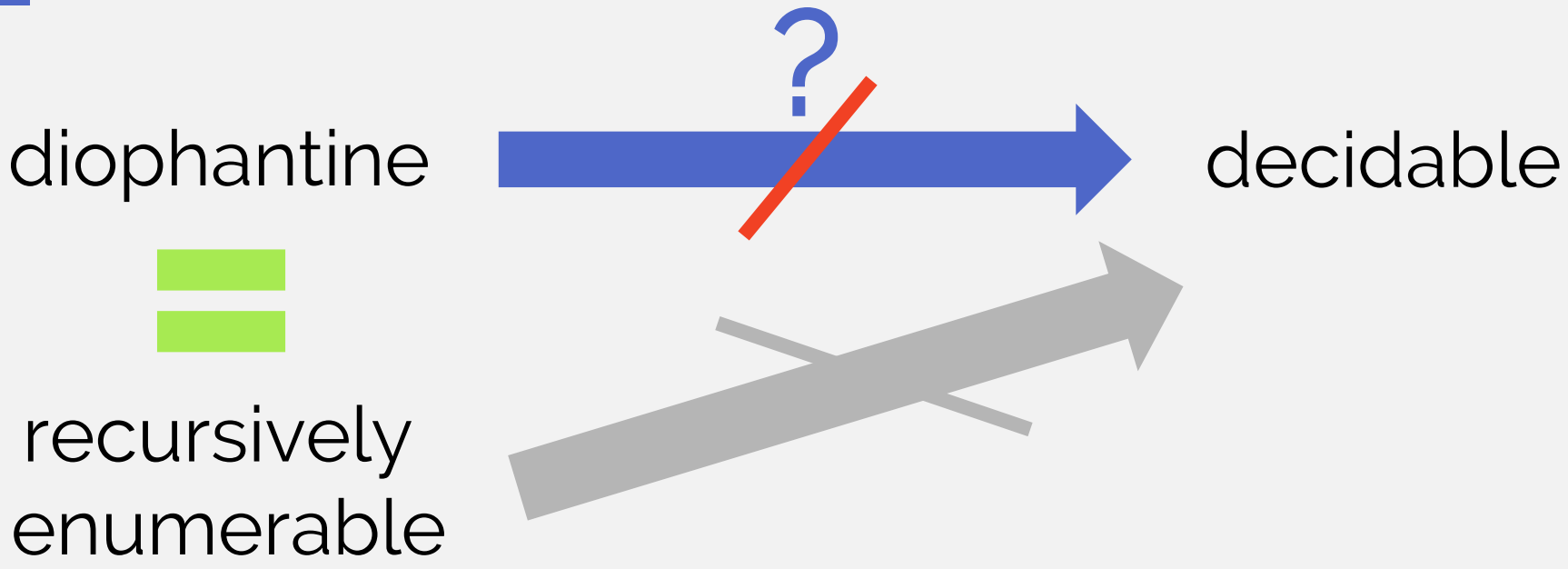


THM

DPRM Theorem.

Every recursively enumerable set is diophantine.

Undecidability of Hilbert's problem

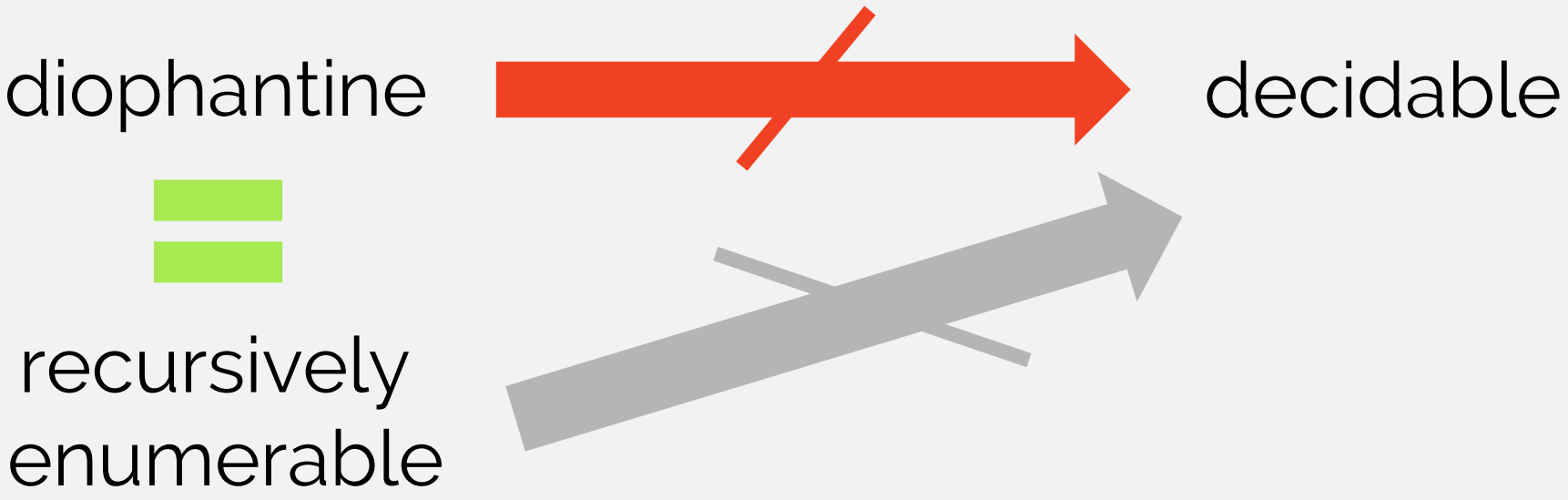


THM

DPRM Theorem.

Every recursively enumerable set is diophantine.

Undecidability of Hilbert's problem

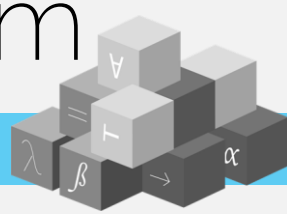


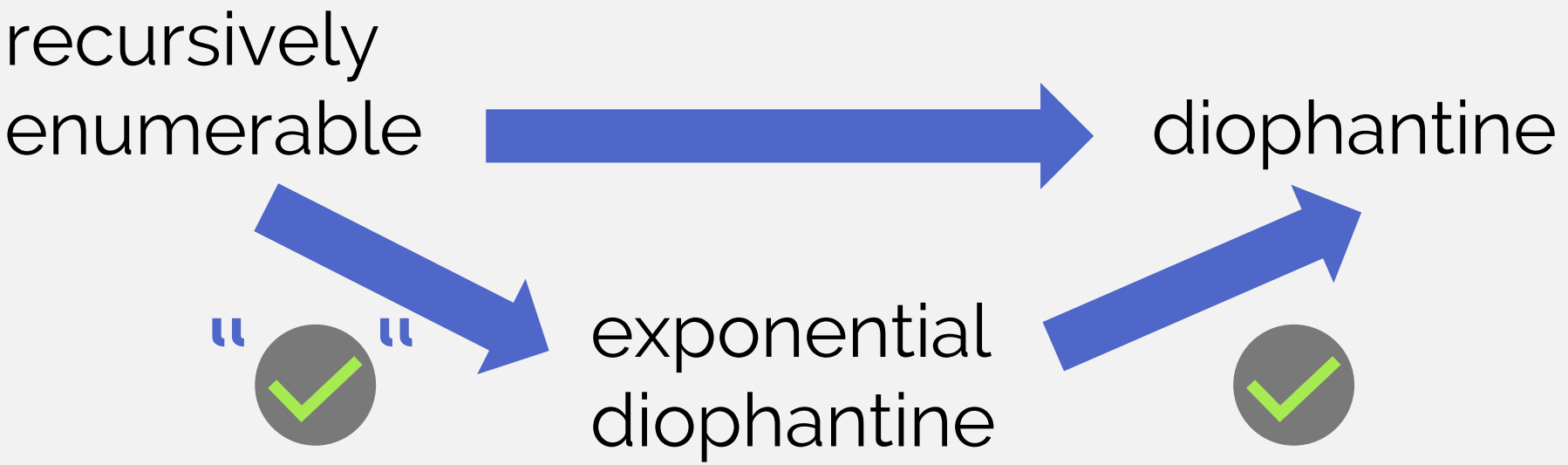
THM

DPRM Theorem.

Every recursively enumerable set is diophantine.

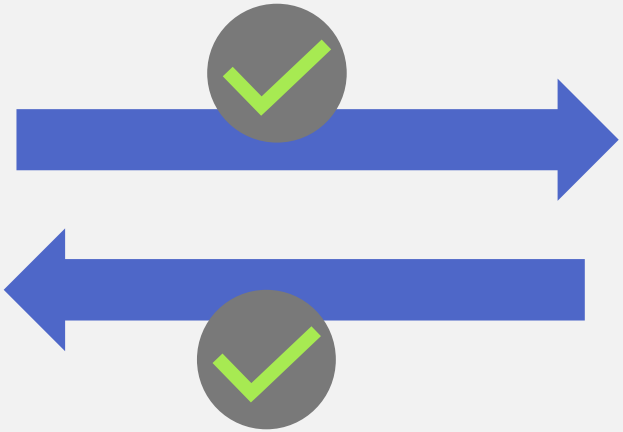
Formalizing the DPRM Theorem





Arithmetization

Register machine



Arithmetization

up to positional
notation lemmas

(exponential)
diophantine

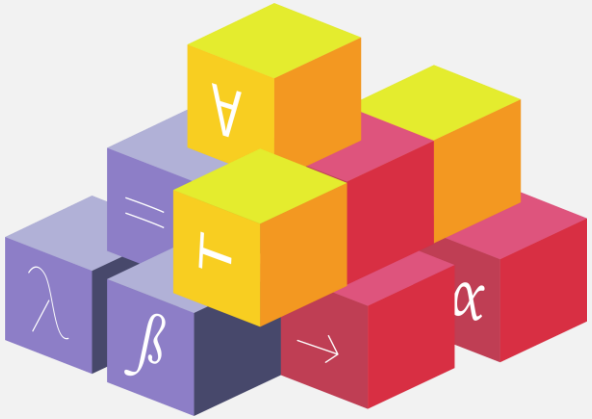
Remaining work

For conditions (4.6) and (4.7), it is very important that during summations there is no carry "across the boundary of a cell" in the protocol.

It can be shown by induction that for every t, among the numbers $s_{1,t}, \ldots, s_{m,t}$ one and only one is equal to 1, others being equal to 0. This is so for $t = 0$ thanks to (4.24) and (4.25). If this is so for some t, then the same holds for $t + 1$. This is so because in the right-hand side of (4.7), all summands but 1 should be equal to 0, the remaining summand being equal to 1; hence, no carry at all occurs in summations (4.24)–(4.25) and relation (4.7) holds.

Similarly, in (4.6), besides the first summand, there can be at most one other summand different from 0. By (4.15), the first summand is at most $2^c - 1$, and the other non-zero summand can be equal only to 1. This implies that no carry "across the boundary of a cell" ever occurs and, hence, relation (4.6) also holds.

Questions?



Thank you for your attention!

And a lot of thanks to

- 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 for his motivation and support
- Mathias Fleury, Christoph Benzmüller and everyone else from the theorem proving community who supported us
- Yuri Matiyasevich, who initiated this project
- Rupert Klein and Kerstin Ernst at Freie Universität Berlin for supporting Jonas to come to ITP