Undecidability Results

Wolfgang Thomas

RWTH AACHEN

Francqui Lecture, Mons, April 2013

Fighting the Undecidable

Overview

1. **Undecidability?**
2. **The grid**
3. **Defining addition and multiplication**
4. **Undecidability in weak arithmetics**
5. **Conclusion**

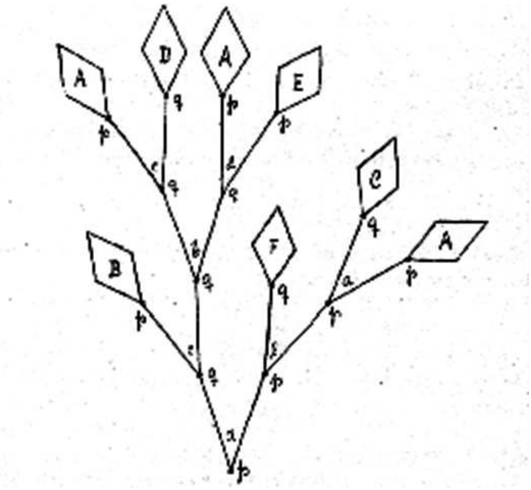
Undecidability?

Example: Hilbert's 10th Problem (1900)

Given a Diophantine equation with any number of unknowns and with rational integral numerical coefficients: To devise a process ("Verfahren") according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

Axel Thue (1863-1922)

The “First Tree”



Thue's Problem (1910)

Given two terms s, t and a set of xioms in the form of equations $u(x_1, \ldots, x_n) = v(x_1, \ldots, x_n)$

decide whether from s one can obtain t in finitely many steps by applications of axioms.

Thue's suspicion:

Eine Lösung dieser Aufgabe im allgemeinsten Falle dürfte vielleicht mit unüberwindlichen Schwierigkeiten verbunden sein.

(A solution of this problem in the general case might perhaps be connected with insurmountable difficulties.)

DIE LÖSUNG EINES SPEZIALFALLES EINES GENERELLEN LOGISCHEN PROBLEMS

Abteilung A.

§ 1.

Es kann eintreffen, dass man aus einem beliebigen Begriffe A einer Begriffskategorie P und aus einem beliebigen Begriffe B einer Begriffskategorie Q durch ein gewisses Verfahren oder Operation θ eindeutig einen Begriff C einer Begriffskategorie R bilden kann.

Wir können C z. B. durch den Ausdruck

$[(A)\ \theta\ (B)]$ bezeichnen.

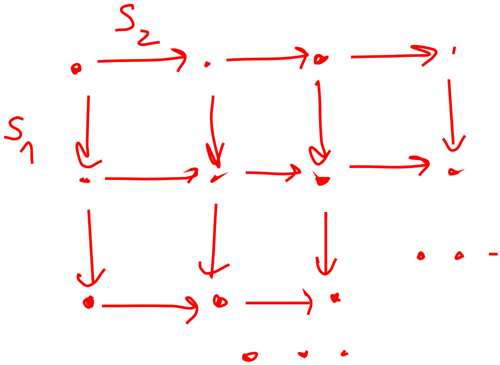
The Grid

The Infinite Grid

The infinite grid is the structure

$$G_2 = (\mathbb{N} \times \mathbb{N}, (0,0), S_1, S_2)$$

where $S_1(i,j) = (i+1, j), \quad S_2(i,j) = (i, j+1)$



Undecidability of Monadic Grid-Theory

The monadic second-order theory of the infinite grid is undecidable.

Proof

by reduction of the halting problem for Turing machines:

For any TM M construct a sentence φ_M of the monadic second-order language of G_2 such that

M halts when started on the empty tape iff $G_2 \models \varphi_M$.

Configurations of M

Assume that M works on a left-bounded tape.

A halting computation of M can be coded by a finite sequence of configuration words

$C_0, C_1, \ldots, C_m$.

We can arrange the configurations row by row in a right-infinite rectangular array:

$$\begin{array}{cccccccc}
q_0 & a_0 & a_0 & a_0 & a_0 & a_0 & a_0 & \ldots \\
a_1 & q_1 & a_0 & a_0 & a_0 & a_0 & a_0 & \ldots \\
q_0 & a_1 & a_2 & a_0 & a_0 & a_0 & a_0 & \ldots \\
a_3 & q_2 & a_2 & a_0 & a_0 & a_0 & a_0 & \ldots
\end{array}$$

etc.

Describing an M-Run

The sentence φ_M will express over G_2 the existence of such an array of configurations.

$a_0, \ldots, a_n$ **are the tape symbols (**a_0 **is the blank)**
$q_0, \ldots, q_k$ **are the states of** M**, special halting state** q_s
We use set variables $X_0, \ldots, X_n, Y_0, \ldots, Y_k$
X_i **collects the grid positions where** a_i **occurs,**
Y_i **collects the grid positions where state** q_i **occurs.**
φ_M **:** $\exists X_0, \ldots, X_n, Y_0, \ldots, Y_k$ (**Partition**$(X_0, \ldots, Y_k)$

$\wedge$ **"the first row is the initial** M**-configuration"**

$\wedge$ **"a successor row is the successor configuration of the preceding one"**

$\wedge$ **"at some position the halting state is reached"**)

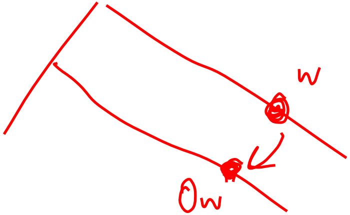
A Hidden Grid

Consider the expansion of the tree T_2 by the two first-letter-adding functions:

$$p_0(w) = 0 \cdot w, \quad p_1(w) = 1 \cdot w$$

The MSO-theory of (T_2, p_0, p_1) is undecidable.

Proof: Define the grid on the domain 0^*1^*.



Another Hidden Grid

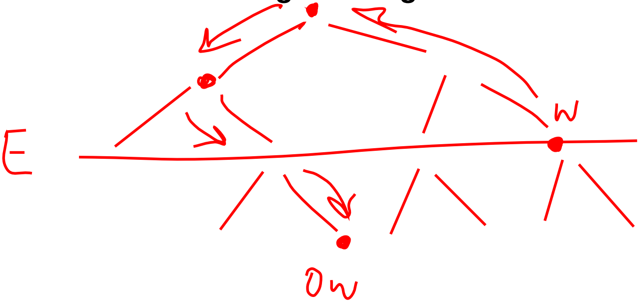
Consider the binary tree with Equal-Level Predicate E

$$E(u,v) \quad :\Leftrightarrow \quad |u| = |v|$$

Obtain (T_2, E).

The MSO-theory of (T_2, E) is undecidable.

Proof: Use E to define again the grid 0^*1^*.



Path Logic over the Grid

In path logic we have first-order quantifiers and set quantifiers ranging only over paths.

The finite-path theory of G_2 is undecidable.

[W. Th. Path logics with synchronization, in K. Lodaya et al., Perspectives in Concurrency Theory, IARCS, Universities Press, India, 2009]

Idea:

Transform 2-counter machine M into a finite-path sentence φ_M such that

M stops when started with counters $(0,0)$ iff $G_2 \models \varphi_M$

M-configuration:
(instruction label, value of counter 1, value of counter 2)

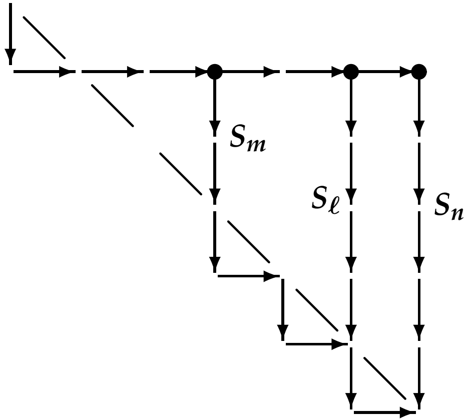
A 2-Counter Machine M

1. if $X_2 = 0$ goto 5
2. decr(X_2)
3. incr(X_1)
4. goto 1
5. stop

Configurations: $(1, 3, 2), (2, 3, 2), (3, 3, 1), (4, 4, 1), \ldots, , (5, 5, 0)$

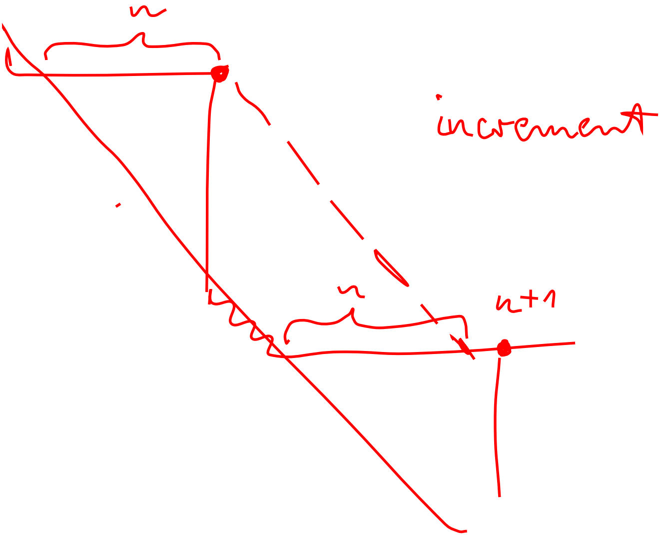
Desribing an M-Configuration over G_2

We use three paths Y, X_1, X_2



Coding configuration $(\ell, m, n) = (4, 2, 5)$.

Update of Configuration



An Intermediate Summary

- **MTh(T_2) is decidable**
- **MTh(T_2, E) is undecidable**
- **MTh(G_2) is undecidable.**
- **PathTh(G_2) is undecidable.**
- **We now show: ChainTh(T_2, E) is decidable.**
  [W. Th., Infinite trees and automaton definable relations over ω-words, TCS 103 (1992)]

Back to Tree with Equal-Level Predicate

We consider a "path logic" over T_2, or even over any regular tree equipped with the equal-level predicate.

We call chain logic the fragment of MSO logic where all set quantifications are restricted to subsets of paths ("chains").

Chain Logic over Regular Trees

The chain theory of a regular (binary) tree with equal level predicate is decidable.

Idea: Reduction to the MSO-theory of $(\mathbb{N}, +1)$

Code a chain C in (T_2, E, P)
by a pair (α_C, β_C) of ω-words over $\{0, 1\}$:

α_C **is the sequence $d_0 d_1 d_2 \ldots$ of "directions"**

$\beta_C(i) = 1$ **iff $d_0 \ldots d_{i-1} \in C$**

A third sequence γ_C signals membership of the reached vertices in P

This result gives decidability of CTL^*-model-checking even when the "synchronization" via E is added.

Defining Addition and Multiplication

Quantification over Binary Relations

By the results of Gödel, Tarski, Turing we know:

The first-order theory of $(\mathbb{N}, +, \cdot, 0, 1)$ is undecidable.

Already Gödel remarked in 1931:

In the second-order language (with quantifiers over elements and relations) one can define define $+$ and $\cdot$ in $(\mathbb{N}, +1)$.

Consequence:

The second-order theory of $(\mathbb{N} + 1)$ is undecidable.

$$x + y = z$$

iff

$$\forall R([R(0, x) \wedge \forall s, t(R(s, t) \rightarrow R(s + 1, t + 1))] \rightarrow R(y, z))$$

Adding Double Function to $(\mathbb{N}, +1)$

$\mathrm{double}(x) := 2x$.

Robinson 1958:

The (weak) MSO-theory of $(\mathbb{N}, +1, \mathrm{double})$ is undecidable.

We follow a proof idea of Elgot and Rabin [JSL 31 (1966)].

Code a relation $R = \{(m_1, n_1), \ldots, (m_k, n_k)\}$

by a set $M_R = \{m'_1 < n'_1 < \ldots < m'_k < n'_k\}$

For each n we need an infinite set of code numbers.

Take as codes of n all numbers $2^i \cdot (\mathrm{double}(n) + 1)$

Example

$$R = \{(2,1),(0,2)\}$$

A code set M_R contains

$$1 \cdot 5 < 2 \cdot 3 < 8 \cdot 1 < 2 \cdot 5$$

5 6 8 10

1. 2. 3. 4. (positions)

A Remark

There is an MSO-formula $\mathrm{OddPos}(X, x)$ that expresses

- $X(x)$
- in the $<$-listing of X-elements, x occurs on an odd position.

Use $\psi(X, z, z')$:

$X(z) \wedge X(z')$

$\wedge$ there is precisely one y between z, z' with $X(y)$

$\mathrm{OddPos}(X, x)$: $\psi^*(X, \min(X), x)$

$\mathrm{Next}(X, x, y)$ says “in X, y is the next element after x

Definability of Decoding

Let $\varphi_2(z, z') := \ \ \mathbf{double}(z) = z'$

Then

"s is a code of x": $\exists y(\mathbf{double}(x) + 1 = y \wedge \varphi_2^*(y, s))$

Translation of $\exists R(R(x, y) \dots)$**:**

$$\exists X(\exists s \exists t(s \text{ is code of } x \wedge t \text{ is code of } y$$
$$\wedge \mathbf{OddPos}(X, s) \wedge \mathbf{Next}(X, s, t))$$

A Sharper Result

Let $f : \mathbb{N} \to \mathbb{N}$ be

- strictly increasing,
- $f - \mathrm{id}_{\mathbb{N}}$ be monotone and unbounded.

Then MTh$(\mathbb{N}, +1, 0, f)$ is undecidable.

[W. Th., A note on undecidable extensions of monadic second order arithmetic, Arch math. Logik 17 (1975)]

Undecidability of Weak Arithmetics

Successor Structure + Unary Predicate

Consider $(\mathbb{N}, +1, P)$

χ_P is the characteristic function of P

$\chi_{\mathbb{P}} = 0\,0\,1\,1\,0\,1\,0\,1\,0\,0\,\ldots$

Consequence of Büchi's analysis of MTh$(\mathbb{N}, +1)$:

For each monadic formula $\varphi(X)$ one can construct a Büchi (or Muller) automaton $\mathcal{A}_\varphi$ such that

$(\mathbb{N}, +1) \models \varphi[P]$ iff $\mathcal{A}_\varphi$ accepts χ_P.

Acceptance Problem $\mathrm{Acc}(P)$:
Given a Büchi autoamaton $\mathcal{A}$, does $\mathcal{A}$ accept χ_P?

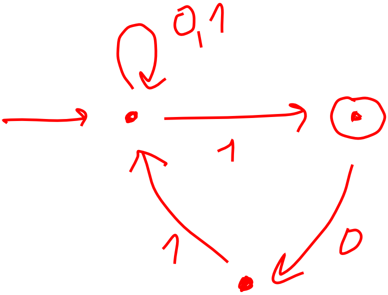
Then

MTh$(\mathbb{N}, +1, P)$ is decidable iff $\mathrm{Acc}(P)$ is decidable.

The Prime Predicate $\mathbb{P}$

Can we decide for any Büchi automaton $\mathcal{A}$ whether

$\mathcal{A}$ accepts $\chi_{\mathbb{P}} = 0\,0\,1\,1\,0\,1\,0\,1\ \ldots$?



Prime Numbers

Decidability of MTh$(\mathbb{N}, +1, \mathbb{P})$ (and even of FOTh$(\mathbb{N}, +1, <, \mathbb{P})$) is open.

Twin prime hypothesis TPH:

$$\forall x \exists y \big(x < y \wedge \mathbb{P}(y) \wedge \mathbb{P}(y + 1 + 1)\big)$$

Dirchlet's Theorem:

Let $A_{m,n} := \{m + i \cdot n \mid i \geq 0\}$

If m, n **are relatively prime, then** $|A_{m,n} \cap \mathbb{P}| = \infty$

For fixed m, n**, this claim is expressible in MTh**$(\mathbb{N}, +1, \mathbb{P})$

More on Arithmetical Progressions

An arithmetic progression of length k in $\mathbb{P}$ is a sequence

$$m, m+d, \ldots, m+(k-1)\cdot d$$

of successive prime numbers

B. Green, T. Tao (2006):

For each k there are infinitely many arithmetical progressions of length k in $\mathbb{P}$.

Illustration (Frind, Underwood, Jobling (2004)):

$$m = 56211383760397, \quad d = 44546738095860, \quad k = 22$$

Undecidability: An Example

There is a recursive set $P \subseteq \mathbb{N}$ such that $\mathrm{FOTh}(\mathbb{N}, +1, P)$ is undecidable.

Proof. **Let M be an enumerable but undecidable set with enumeration $m_0, m_1, m_2, \ldots$.**

Consider the ω-word

$$10^{m_0}10^{m_1}10^{m_2}\cdots$$

Let P be the associated set. It is recursive.

Given m let

$$\varphi_m : \exists x\big(Px \wedge \neg P(x+1) \wedge \neg P(x+2) \wedge \ldots \wedge P(x+m+1)\big)$$

Then

$$m \in M \;\Leftrightarrow\; (\mathbb{N}, +1, P) \models \varphi_m$$

Classifying Undecidability

We identify sentences with natural numbers.

A theory is then coded by a set of natural numbers.

The undecidable sets are classified in the arithmetical hierarchy:

A set A belongs to the class Σ_n^0 iff

for some decidable relation R:

$$x \in A \;\Leftrightarrow\; \exists y_1 \forall y_2 \ldots \exists/\forall y_n R(x, y_1, \ldots, y_n)$$

Π_n^0 contains the complements of the Σ_n^0-sets.

The Σ_1^0-sets are the recursively enumerable ones.

Complexity of $\mathrm{MTh}(\mathbb{N}, +1, P)$

If P is recursive, then $\mathrm{MTh}(\mathbb{N}, +1, P)$ is on level $\Sigma^0_3 \cap \Pi^0_3$ of the arithmetical hierarchy.

Consider Muller automaton $\mathcal{A} = (Q, \{0,1\}, q_0, \delta, \mathcal{F})$

$$\mathcal{A} \text{ accepts } \chi_P \Leftrightarrow \bigvee_{F \in \mathcal{F}} \Big(\bigwedge_{q \in F} \exists^\omega i \;\; \delta(q_0, \chi_P[0,i]) = q \;\wedge \bigwedge_{q \notin F} \exists^{<\omega} i \;\; \delta(q_0, \chi_P[0,i]) = q \Big)$$

This is a Boolean combination of Σ_2-conditions.

So $\{\mathcal{A} \mid \mathcal{A} \text{ accepts } \chi_P\} \in \Sigma_3 \cap \Pi_3$

Consequence: If P is recursive, then in MTh$(\mathbb{N}, +1, P)$ $+$ and $\cdot$ are not definable.
(So MTh$(\mathbb{N}, +1)$ is a "weak arithmetic".)

Expanding T_2 by a Predicate

For recursive $P \subseteq \{0,1\}^*$, the theory $\mathrm{MTh}(\mathcal{S}_2, P)$ belongs to the class Δ^1_2, and there is a recursive $P \subseteq \{0,1\}^*$ such that $\mathrm{MT}(\mathcal{S}_2, P)$ is Π^1_1-hard.

One constructs a recursive P such that a known Π^1_1-complete set is reducible to MT$(\mathcal{S}_2, P)$.

As Π^1_1-complete set use a coding of finite-path trees.

[W. Th., On monadic theories of monadic predicates, LNCS 6300 (2010)]

$(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$

An exercise: MTh$(\mathbb{Q}, <)$ is decidable.

For a hint see Rabin's landmark paper of 1969

M.O. Rabin, Decidability of second-order theories and automata on infinite trees, Trans. AMS 141 (1969)

Much more than an exercise: MTh$(\mathbb{R}, <)$ is undecidable.

For a condensed hint see the last 10 pages of Shelah's landmark paper of 1975

S. Shelah, The monadic theory of order, Ann. Math. 102 (1975)