The Ordering of the Natural Numbers with a Unary Predicate: Approaches to Show Decidability Results

Wolfgang Thomas

RWTH Aachen University

thomas@informatik.rwth-aachen.de

Journées Montoises, Rennes, August 2006

Background I

Büchi 1960: $MTh(\mathbb{N}, +1)$ **is decidable.**

Example sentence:

$$\forall X((X(0) \wedge \forall y(X(y) \rightarrow X(y+1))) \rightarrow \forall y X(y))$$

Method for proof of decidability:

Transformation of monadic formulas $\varphi(X_1, \ldots, X_n)$ **to Büchi automata over** $\{0,1\}^n$

(Later also: deterministic Muller automata)

Solution of emptiness problem

Background II

Expansions of $(\mathbb{N}, +1)$

- **by functions or binary relations:**
  mostly undecidable
  Robinson 1958: $\mathrm{MTh}(\mathbb{N}, +)$ undecidable
- **by unary predicates**
  often decidable

Elgot-Rabin 1966:
$\mathrm{MTh}(\mathbb{N}, +1, P)$ is decidable for the following P:

- **set of factorial numbers**
- **set of powers of k (fixed k)**
- **set of kth powers (fixed k)**

Many more predicates known

Basic Approach for Decidability

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

$\chi_P =$ **characteristic sequence of** P

Example $\mathbb{P} =$ **set of primes**

$$\chi_P = \begin{array}{ccccccccccccccccccc} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & \cdots \\ & & 2 & 3 & & 5 & & 7 & & & & 11 & & 13 & & & & 17 & \end{array}$$

Büchi
McNaughton

$$\varphi \mapsto \mathcal{A}_\varphi$$

Büchi automaton
Muller automaton

such that $(\mathbb{N}, +1, P) \models \varphi \;\Leftrightarrow\; \mathcal{A}_\varphi$ **accepts** χ_P

Solve the Acceptance Problem for χ_P**:**
Decide for any Muller automaton $\mathcal{A}$ **whether** $\mathcal{A}$ **accepts** χ_P**.**

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

If P is recursive, then $\mathrm{MTh}(\mathbb{N}, +1, P)$ is on level $\Sigma_3 \cap \Pi_3$ 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.

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

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

Plan

Study the class of those P such that $\mathrm{MTh}(\mathbb{N}, +1, P)$ is decidable.

Approach 1: Find more and more such P.

Approach 2: Find characterizations of such P.

Here we follow Approach 2.

Plan:

- **I More Background**
- **II Characterizations via Periodicity**
- **III Characterization via Repeated Patterns**
- **IV Perspectives**

I. More Background

Undecidability Results

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

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

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

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

Further Results

There are sets P such that

1. $\mathrm{FOTh}(\mathbb{N}, +1, P)$ **is decidable but** $\mathrm{FOTh}(\mathbb{N}, +1, <, P)$ **is undecidable,**
2. $\mathrm{FOTh}(\mathbb{N}, +1, <, P)$ **is decidable but** $\mathrm{MTh}(\mathbb{N}, +1, P)$ **is undecidable.**

For 1. use in $\mathrm{FOTh}(\mathbb{N}, +1, <)$ **the quantifier "there exist infinitely many** x**"** $(\forall y \exists x (x > y \wedge \ldots))$**.**

For 2. use in $\mathrm{MTh}(\mathbb{N}, +1)$ **definability of divisibility by** k **(and of each arithmetical progression).**

Using $<$

Preparation:

FOTh$(\mathbb{N}, +1, P)$ is decidable if for each word $w \in \{0,1\}^+$ and each number m one can decide whether w occurs m times as segment in χ_P.

Enumerate stepwise ($i = 0, 1, \ldots$) the computations of all Turing machines M_n starting on the empty tape

Build up χ_P by appending in step i the word $0^i 1 0^n 1$ if the M_n-computation is still running, otherwise just $0^i 1$.

Undecidability with $<$:

M_n stops on empty tape iff $10^n 1$ occurs infinitely often in χ_P

Decidability without $<$:

m-fold occurrence of any given segment w can be checked. (The interesting case involves only words from $0^* 1 0^n 1 0^*$)

Using Divisibility by k

Take an enumerable, non-recursive set Q of primes, with enumeration $q_0, q_1, \ldots$

Define an increasing sequence $p_0, p_1, \ldots$ defining a set P:

Let $p_0 = 2q_0^2$

Pick the smallest prime q such that $qq_{i+1}^2 - p_i > p_i - p_{i-1}$ and set $p_{i+1} = qq_{i+1}^2$

P is recursive and has increasing distances between successive elements

FOTh$(\mathbb{N}, +1, <, P)$ is decidable (invoking FO model theory)

On the other hand:

$q \in Q$ iff some P-element is divisible by q^2

Illustration: 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)):

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

II. Characterizations via Periodicity

Colorings

A **finite coloring** over $\mathbb{N}$ is a map c which associates to each pair $i < j$ a value from a finite set C

c is **additive** if $c(i,j)$ and $c(j,k)$ determine $c(i,k)$, written $c(i,j) + c(j,k)$

Example of an additive coloring

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

$\delta(p,u) :=$ is the state reached by $\mathcal{A}$ from p via u

$\Delta(p,u) :=$ the set of states visited by $\mathcal{A}$ from p via u

$$u \sim_{\mathcal{A}} v \;\Leftrightarrow\; \forall p \in Q : \delta(p,u) = \delta(p,v) \wedge \Delta(p,u) = \Delta(p,v)$$

- $\sim_{\mathcal{A}}$ is a congruence.
- Each $\sim_{\mathcal{A}}$-class $[u]_{\mathcal{A}}$ is regular
- Given P, $c(i,j) := [\chi_P[i,j)]_{\mathcal{A}}$ is a finite additive coloring

Ramsey's Theorem A

A set $H = \{h_0 < h_1 < \ldots\}$ is homogeneous for c if $c(h_i, h_j)$ has the same value v for all $i < j$

Note that for additive colorings we then have $v + v = v$

Ramsey's Theorem: For any finite coloring over $\mathbb{N}$, there is an infinite homogeneous set.

Consequence: Given P and a a finite Muller automaton $\mathcal{A}$, there are $\sim_{\mathcal{A}}$-classes U, V such that $\chi_P \in U \cdot V^\omega$
We say: "(U, V) decomposes χ_P"

From such U, V one can determine whether $\mathcal{A}$ accepts χ_P.

RecRamsey(P) $:\Leftrightarrow$ From a Muller automaton $\mathcal{A}$ one can compute (U, V) which decomposes χ_P.

The acceptance problem for χ_P is decidable iff RecRamsey(P).

Types

Instead of $\sim_{\mathcal{A}}$ use $\sim_n$:

$u \sim_n v$ iff for all $\mathcal{A}$ with $\leq n$ states, $u \sim_{\mathcal{A}} v$

Note that $\sim_{n+1}$ refines $\sim_n$
$\sim_n$ refines $\sim_{\mathcal{A}}$ for each $\sim_{\mathcal{A}}$ with $\leq n$ states.

$\sim_n$ is a congruence (and the induced coloring additive).

Similar definition in logic, for monadic formulas:

$u \equiv_n v$ iff for each monadic formula φ with quantifier-rank $\leq n$:
$u \models \varphi$ iff $v \models \varphi$
Equivalence classes of $\equiv_n$ are called "n-types"

Composition Theorem: If $\chi_P \in U \cdot V^\omega$ for n-types U, V, then one can decide for φ of quantifier-depth n whether $\chi_P \models \varphi$.

Illustration: Contractions (Elgot-Rabin)

Given $\mathcal{A}$ and letter a of the input alphabet:
There is a bound B such that each word a^i is $\sim_{\mathcal{A}}$-equivalent to some a^s with $s \leq B$.

Assume the 0-sections of $\chi_P = 0^{i_0}10^{i_1}1\ldots$ are contracted in this way:

$$\chi'_P = 0^{s_0}10^{s_1}1\ldots$$

If for each $\mathcal{A}$ the sequence χ'_P is ultimately periodic then the acceptance problem for χ_P is decidable.

Applications: Factorials, powers of 2, etc.

In these cases, contractions yield, given $\mathcal{A}$, a pair (U, V) of $\sim_{\mathcal{A}}$-classes decomposing χ_P.

Uniformly Homogeneous Sets

Idea: Capture the function

$n \mapsto \sim_n$**-classes** (U_n, V_n) **decomposing** χ_P

by a single decomposition.

Recall $\sim_n$ **and the associated coloring** c_n **given by** χ_P**.**

$\sim_{n+1}$ **is a refinement of** $\sim_n$**.**

$H = \{h_0 < h_1 < \ldots\}$ **is uniformly homogeneous for** $c_0, c_1, \ldots$ **if for each** n

$$H_n = \{h_n < h_{n+1} < \ldots\}$$

is homogeneous for c_n**.**

Since $c_0, c_1, \ldots$ **are determined by** P **we also say that** H **is uniformly homogeneous for** P**.**

Results on Uniformly Homogeneous Sets

If H is recursive and uniformly homogeneous for P, then the acceptance problem for χ_P is decidable.

Method: For $\mathcal{A}$ with n states use H to compute

$U = [\chi_P[0, h_n)]_n$ **and** $V = [\chi_P[h_n, h_{n+1})]_n$

Then (U, V) decomposes χ_P and we can check whether $\mathcal{A}$ accepts χ_P.

Theorem: The following are equivalent:

1. **MTh$(\mathbb{N}, +1, P)$ is decidable.**
2. **The acceptance problem for χ_P is decidable.**
3. **RecRamsey(P).**
4. **There is a recursive uniformly homogeneous set for P.**

$(1) \Leftrightarrow (2) \Leftrightarrow (3) \Rightarrow (4)$ **are clear. We show** $(1) \Rightarrow (4)$

Construction

Assumption: MTh$(\mathbb{N}, +1, P)$ is decidable.

1. **Find $\sim_1$-classes U_1, V_1 decomposing χ_P**
   Find h_1 with $\chi_P[0, h_1) \in U_1$, $\chi_P[h_1, \infty) \in V_1^\omega$
2. **Find $\sim_2$-classes $U_2 \subseteq V_1, V_2 \subseteq V_1$ decomposing $\chi_P[h_1, \infty)$**
   Find $h_2 > h_1$ with $\chi_P[h_1, h_2) \in U_2$, $\chi_P[h_2, \infty) \in V_2^\omega$
3. **etc.**

Then $\{h_1, h_2, \ldots\}$ is uniformly homogeneous for P.

Note: The ”Find”-clauses are effective due to the assumption.

Remark:

1. **Uniformly homogeneous set for χ_P always exists.**
2. **Analogous claims hold for FO logic and FO-types.**

Application

At stage $n+1$: $\chi_P[h_n, h_{n+1}) \in U_{n+1} \subseteq V_n$.

So U_n is the $\sim_n$-class of $\chi_P[0, h_n)$,
and V_n the $\sim_n$-class of $\chi_P[h_n, h_{n+1})$,
and (U_n, V_n) decomposes χ_P.

Thus: Given $\mathcal{A}$ of n states, knowing the words $\chi_P[0, h_n)$ and $\chi_P[h_n, h_{n+1})$ suffices for deciding whether $\mathcal{A}$ accepts χ_P.

Illustration for $\mathbb{P}$: Let H uniformly homogeneous for $\mathbb{P}$.

The Twin Prime Hypothesis TPH is expressed by a 4-state Muller automaton $\mathcal{A}_{\mathrm{TPH}}$.

TPH is true iff $\chi_P[h_4, h_5)$ contains a segment 101.

In this way, the uniformly homogeneous set H for $\chi_{\mathbb{P}}$ encodes a lot of known and unknown number theory.

III. Characterization via Repeated Patterns

Semenov's Theorem

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

(0) P is recursive

(1) for each regular $L \subseteq \{0,1\}^*$ one can decide whether each tail of χ_P has a segment in L

(2) if not, one can compute i^* such that $\chi_P[i^*, \infty)$ has no segment in L.

Condition (1) is "not anchored":
Segments are considered without anchor to the origin.

Preparation of Proof

We have to show, for recursive P:

Conditions (1), (2) $\Rightarrow$ acceptance problem for χ_P is decidable.

With (1), (2) we shall see:

For each Muller automaton $\mathcal{A}$, we can compute the set

$I_{\mathcal{A}} =$ **set of $\mathcal{A}$-states visited infinitely often on χ_P.**

This suffices to decide whether $\mathcal{A}$ accepts χ_P.

Naive Approach

Given $I \subseteq Q$, we have to check whether $I = I_{\mathcal{A}}$

Check whether each tail of χ_P has a segment σ which causes $\mathcal{A}$ to traverse precisely I.

Then check that each $J \supsetneqq I$ violates this.

Problem:

The effect of a segment depends on the state with which it is entered.

The effect of a segment is "anchored" by the preceding prefix.

The proof of Semenov's Theorem has to deduce some anchoring from conditions (1) and (2).

Proof of Bateman, Jockusch, Woods (1993)

Fix χ_P.

Call $(\mathcal{A}, J) \subseteq Q$ good $:\Leftrightarrow I_{\mathcal{A}} \subseteq J$.

Call $(\mathcal{A}, J) \subseteq Q$ bad $:\Leftrightarrow$ not $I_{\mathcal{A}} \subseteq J$.

Show that both the good and the bad $(\mathcal{A}, J)$ can be enumerated,
using Semenov's conditions (1) and (2).

Then one can decide $I_{\mathcal{A}} = J$ and hence whether $I_{\mathcal{A}} \in \mathcal{F}$.

Essential Definition

Given $\mathcal{A}$ and state sets $F, J \subseteq Q$,

define the language $\mathrm{Avoid}(F, J) \subseteq \{0,1\}^*$

$w \in \mathrm{Avoid}(F, J) \;:\Leftrightarrow$

from each $p \in F$, the $\mathcal{A}$-run through w visits some $q \notin J$.

Remark

1. $\mathrm{Avoid}(F, J)$ **is regular.**
2. **If F gets larger, then $\mathrm{Avoid}(F, J)$ gets smaller.**

A Precomputation from $(\mathcal{A}, J)$

Consider $\mathrm{Avoid}(F, J)$, for increasing F
(starting from $F = \emptyset$ and $\mathrm{Avoid}(\emptyset, J) = \{0,1\}^*$)

Using Semenov's condition (1) find maximal F_0 such that

- each χ_P-tail has a segment in $\mathrm{Avoid}(F_0, J)$.

With condition (2), for each $F_1 \supsetneqq F_0$ find i such that

- in $\chi_P[i, \infty)$ there is no segment in $\mathrm{Avoid}(F_1, J)$.

Let i^* be the greatest of these i (ranging over the F_1)

Note: Conditions (1), (2) serve to compute F_0, i^* from $(\mathcal{A}, J)$.

Main Lemma

$I_{\mathcal{A}} \subseteq J$

$\Leftrightarrow$

in $\chi_P[i^*, \infty)$ a segment $\in \mathrm{Avoid}(F_0, J)$ occurs, reached by $\mathcal{A}$ in a state outside F_0.

Note: The condition on F_0 provides an anchor to the origin.

Since χ_P is recursive, his allows us to enumerate the good $(\mathcal{A}, J)$:

For each $(\mathcal{A}, J)$, do the precomputation to obtain F_0, i^* and search through the set of segments $\chi_P[i, j)$ beyond i^*, to find one in $\mathrm{Avoid}(F_0, J)$ reached by $\mathcal{A}$ in a state $\notin F_0$.

Proof of Lemma

$I_{\mathcal{A}} \subseteq J \Rightarrow$
in $\chi_P[i^*, \infty)$ a segment $\in \mathrm{Avoid}(F_0, J)$ occurs, reached by $\mathcal{A}$ in a state outside F_0.

Pick i_0 such that beyond i_0, $\mathcal{A}$ only visits $I_{\mathcal{A}}$-states.

Consider any $\chi_P[i, j] \in \mathrm{Avoid}(F_0, J)$ with $i > i_0, i^*$.

Show $\delta(q_0, \chi_P[0, i)) \notin F_0$.

Otherwise, by definition of $\mathrm{Avoid}(F_0, J)$ a state outside J (and hence outside $I_{\mathcal{A}}$) is reached after i.

Contradiction.

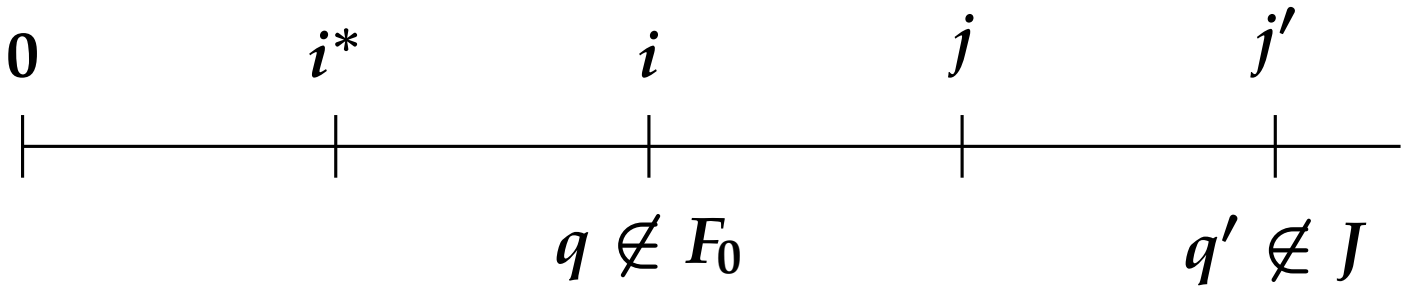
The other Direction

Pick i^* and segment $\chi_P[i,j] \in \mathbf{Avoid}(F_0, J)$ with $i > i^*$

with $\underbrace{\delta(q_0, \chi_P[0,i))}_{q} \notin F_0$.

Show that beyond j, only J-states are visited (hence $I_{\mathcal{A}} \subseteq J$).

For contradiction assume



q' can be included in F_0

Contradiction to maximality of F_0 and definition of i^*.

Enumerating the bad $(\mathcal{A}, J)$

From $(\mathcal{A}, J)$ compute F_0 and i^* as before.

Define the set $\mathrm{ReachAvoid}(G, J)$ of all words with

- $\forall q \in Q$, $w = uv$ with $v \in \mathrm{Avoid}(F_0, J)$ such that from q via u a state outside F_0 is reached.

$\mathrm{ReachAvoid}(G, J)$ is regular.

In analogy to F_0, i^* compute maximal G_0 and $j^* > i^*$

Then show the following Lemma:

$(\mathcal{A}, J)$ is bad (i.e. not $I_{\mathcal{A}} \subseteq J$) iff

beyond j^* there is a segment in $\mathrm{ReachAvoid}(G_0, J)$ reached in a state outside G_0.

The proof is similar to the Lemma before.

IV. Perspectives

Summary

- **The existence of a uniformly homogeneous set provides an "anchored" reduction of the decision problem for MTh$(\mathbb{N}, +1, P)$.**
  It reduces the check of a sentence to analyzing a finite prefix of the structure.
  But: It requires computation of a global object and thus does not help too much in concrete examples.
- **Semenov's criterion seems easier applicable since condition (1) is not anchored.**
- **For the set of primes, Semenov's reduction singles out certain types of open number theoretic problems which precisely capture MTh$(\mathbb{N}, +1, \mathbb{P})$**

Some Problems

- Further enlarge the class of P with decidable MTh$(\mathbb{N}, +1, P)$, similarly for tuples $\overline{P}$.
- Find classes of P where FOTh$(\mathbb{N}, +1, <, P)$ is decidable but this is false or open for MTh$(\mathbb{N}, +1, P)$.
- Is there any P of interest in arithmetic such that MTh$(\mathbb{N}, +1, P)$ is undecidable?
- Conversely: Find more binary relations R (relevant in arithmetic) such that MTh$(\mathbb{N}, +1, R)$ is decidable.
- Study expansions of the binary tree by a unary predicate. For example, study the acceptance problem for Rabin tree automata over Sturmian trees.

Appendix: Main Sources for this Talk

- **For Part I:**

  W. Th., Math. Annalen 237 (1978)

- **For Part II:**

  A. Rabinovich, W. Th., CSL 2006, Springer LNCS, to appear

- **For Part III:**

  P.T. Bateman, C.G. Jockusch, A.R. Woods, JSL 58 (1993)