Decidability issues for infinite integer sequences with finite support

A. Sirokofskich
University of Crete

July 17, 2013

Few words on notation

- $\mathbb{Z}^{<\omega}$ is the set of all infinite sequences over $\mathbb{Z}$, with finite support.

Few words on notation

- $\mathbb{Z}^{<\omega}$ is the set of all infinite sequences over $\mathbb{Z}$, with finite support.
- $(x)_i$ stands for the i co-ordinate of $x \in \mathbb{Z}^{<\omega}$.

Multiplicative group $(\mathbb{Q}^+, \times)$

Consider the set of positive rationals, $\mathbb{Q}^+$.

Multiplicative group $(\mathbb{Q}^+, \times)$

Consider the set of positive rationals, $\mathbb{Q}^+$.

Additive group $(\mathbb{Z}^{<\omega}, +)$ is isomorphic to the multiplicative group $(\mathbb{Q}^+, \times)$.

Multiplicative group $(\mathbb{Q}^+, \times)$

Consider the set of positive rationals, $\mathbb{Q}^+$.

Additive group $(\mathbb{Z}^{<\omega}, +)$ is isomorphic to the multiplicative group $(\mathbb{Q}^+, \times)$.

Let the sequence $(p_i)_{i \in \mathbb{N}}$ be the natural enumeration of the set of primes.

Multiplicative group $(\mathbb{Q}^+, \times)$

Consider the set of positive rationals, $\mathbb{Q}^+$.

Additive group $(\mathbb{Z}^{<\omega}, +)$ is isomorphic to the multiplicative group $(\mathbb{Q}^+, \times)$.

Let the sequence $(p_i)_{i\in\mathbb{N}}$ be the natural enumeration of the set of primes. Then the element $n = \prod p_i^{m_i}$ of $\mathbb{Q}^+$ corresponds to the element $x \in \mathbb{Z}^{<\omega}$ with $(x)_i = m_i$ for $i \in \mathbb{N}$.

'Notion of gcd'

We can define a notion of divisibility $|$ in $\mathbb{Q}^+$ as follows:

'Notion of gcd'

We can define a notion of divisibility $|$ in $\mathbb{Q}^+$ as follows:

let $n_1 = \prod p_i^{m_i}$ and $n_2 = \prod p_i^{k_i}$, then

$$n_1 | n_2 \iff \forall i (m_i \leq k_i).$$

'Notion of gcd'

We can define a notion of divisibility $|$ in $\mathbb{Q}^+$ as follows:

let $n_1 = \prod p_i^{m_i}$ and $n_2 = \prod p_i^{k_i}$, then

$$n_1 | n_2 \iff \forall i (m_i \leq k_i).$$

We extend the usual notation of gcd for n_1, n_2 in $\mathbb{Q}^+$, i.e.,

'Notion of gcd'

We can define a notion of divisibility $|$ in $\mathbb{Q}^+$ as follows:

let $n_1 = \prod p_i^{m_i}$ and $n_2 = \prod p_i^{k_i}$, then

$$n_1 | n_2 \iff \forall i (m_i \leq k_i).$$

We extend the usual notation of gcd for n_1, n_2 in $\mathbb{Q}^+$, i.e.,

$$gcd(n_1, n_2) = \prod p_i^{min\{m_i, k_i\}}.$$

It is well known that gcd is definable from $|$ in the substructure $(\mathbb{Z}^+, |, =)$ of $(\mathbb{Q}^+, |, =)$.

It is well known that gcd is definable from $|$ in the substructure $(\mathbb{Z}^+, |, =)$ of $(\mathbb{Q}^+, |, =)$.

For $x, y \in \mathbb{Z}$ we have that

$$d = gcd(x, y) \text{ if and only if } (d|x) \wedge (d|y) \wedge \forall w[w|x \wedge w|y \rightarrow w|d]. \quad (1)$$

It is well known that gcd is definable from $|$ in the substructure $(\mathbb{Z}^+, |, =)$ of $(\mathbb{Q}^+, |, =)$.

For $x, y \in \mathbb{Z}$ we have that

$$d = gcd(x, y) \text{ if and only if } (d|x) \wedge (d|y) \wedge \forall w[w|x \wedge w|y \rightarrow w|d]. \quad (1)$$

Note that $|$ is existentially definable in $(\mathbb{Z}^+, \times, =)$ by

$$x|y \text{ if and only if } \exists z[x \times z = y]. \quad (2)$$

It is well known that gcd is definable from $|$ in the substructure $(\mathbb{Z}^+, |, =)$ of $(\mathbb{Q}^+, |, =)$.

For $x, y \in \mathbb{Z}$ we have that

$$d = gcd(x, y) \text{ if and only if } (d|x) \wedge (d|y) \wedge \forall w[w|x \wedge w|y \rightarrow w|d]. \quad (1)$$

Note that $|$ is existentially definable in $(\mathbb{Z}^+, \times, =)$ by

$$x|y \text{ if and only if } \exists z[x \times z = y]. \quad (2)$$

The relation (2) does not extend to the multiplicative rationals.

Moreover, the 'gcd' is not definable in $(\mathbb{Q}^+, \times, =)$.

Moreover, the ‘gcd’ is not definable in $(\mathbb{Q}^+, \times, =)$.

Any module over a fixed ring has stable theory in the language of modules.

Moreover, the ‘gcd’ is not definable in $(\mathbb{Q}^+, \times, =)$.

Any module over a fixed ring has stable theory in the language of modules.

On the other hand, the notion of 'gcd' implies some kind of ordering, namely the formula

$$\varphi(x, y) : \text{ ‘gcd’}(x, y) = x$$

is unstable.

Language and structure

$L = \{+;\ min;\ C;\ \{|_n\}_n; \{\delta_c\}_c\}$

$$\mathcal{A} = (\mathbb{Z}^{<\omega};\ +;\ min;\ C; \{|_n\}_{n\in\mathbb{N}};\ \{\delta_c\}_{c\in\mathbb{Z}^{<\omega}}),$$

Language and structure

$L = \{+;\ min;\ C;\ \{|_n\}_n; \{\delta_c\}_c\}$

$$\mathcal{A} = (\mathbb{Z}^{<\omega};\ +;\ min;\ C; \{|_n\}_{n\in\mathbb{N}};\ \{\delta_c\}_{c\in\mathbb{Z}^{<\omega}}),$$

$$x + y = z \iff (x)_i + (y)_i = (z)_i, \text{ for all } i \in \mathbb{N},$$

Language and structure

$L = \{+;\ min;\ C;\ \{|_n\}_n;\{\delta_c\}_c\}$

$$\mathcal{A} = (\mathbb{Z}^{<\omega};\ +;\ min;\ C;\{|_n\}_{n\in\mathbb{N}};\ \{\delta_c\}_{c\in\mathbb{Z}^{<\omega}}),$$

$$x + y = z \iff (x)_i + (y)_i = (z)_i,\ \text{for all } i \in \mathbb{N},$$

$$min(x, y) = z \iff min((x)_i, (y)_i) = (z)_i,\ \text{for all } i \in \mathbb{N},$$

Language and structure

$L = \{+;\ min;\ C;\ \{|_n\}_n; \{\delta_c\}_c\}$

$$\mathcal{A} = (\mathbb{Z}^{<\omega};\ +;\ min;\ C; \{|_n\}_{n\in\mathbb{N}};\ \{\delta_c\}_{c\in\mathbb{Z}^{<\omega}}),$$

$$x + y = z \iff (x)_i + (y)_i = (z)_i, \text{ for all } i \in \mathbb{N},$$

$$min(x, y) = z \iff min((x)_i, (y)_i) = (z)_i, \text{ for all } i \in \mathbb{N},$$

C is a set of constants, exactly one for each element of $\mathbb{Z}^{<\omega}$,

Language and structure

$L = \{+;\ min;\ C;\ \{|_n\}_n; \{\delta_c\}_c\}$

$$\mathcal{A} = (\mathbb{Z}^{<\omega};\ +;\ min;\ C; \{|_n\}_{n\in\mathbb{N}};\ \{\delta_c\}_{c\in\mathbb{Z}^{<\omega}}),$$

$$x + y = z \iff (x)_i + (y)_i = (z)_i, \text{ for all } i \in \mathbb{N},$$

$$min(x, y) = z \iff min((x)_i, (y)_i) = (z)_i, \text{ for all } i \in \mathbb{N},$$

C is a set of constants, exactly one for each element of $\mathbb{Z}^{<\omega}$,

$|_n(x)$ if and only if n divides $(x)_i$, for all $i \in \mathbb{N}$,

Language and structure

$L = \{+;\ min;\ C;\ \{|_n\}_n; \{\delta_c\}_c\}$

$$\mathcal{A} = (\mathbb{Z}^{<\omega};\ +;\ min;\ C; \{|_n\}_{n\in\mathbb{N}};\ \{\delta_c\}_{c\in\mathbb{Z}^{<\omega}}),$$

$$x + y = z \iff (x)_i + (y)_i = (z)_i, \text{ for all } i \in \mathbb{N},$$

$$min(x, y) = z \iff min((x)_i, (y)_i) = (z)_i, \text{ for all } i \in \mathbb{N},$$

C is a set of constants, exactly one for each element of $\mathbb{Z}^{<\omega}$,

$|_n(x)$ if and only if n divides $(x)_i$, for all $i \in \mathbb{N}$,

$\delta_c(x) \iff$ for all $i \in \mathbb{N}$ if $(c)_i \neq 0$ then $(c)_i$ divides $(x)_i$.

The existential theory of $\mathcal{A}$

We give an effective reduction of the problem of truth of existential formulae in $\mathcal{A}$ to that of solvability of systems of equations and inequations in Presburger Arithmetic.

The existential theory of $\mathcal{A}$

We give an effective reduction of the problem of truth of existential formulae in $\mathcal{A}$ to that of solvability of systems of equations and inequations in Presburger Arithmetic.

Theorem

The existential theory of $\mathcal{A}$ is decidable.

Complexity

Complexity

Theorem (V. Weispfenning)

There exists a Q.E. procedure assigning to any prenex formula φ (in the language of Presburger Arithmetic) an equivalent quantifier free formula φ'. If φ has at most a quantifier-blocks each of length at most b, then the algorithm runs in time and space bounded by $2^{c \cdot length(\varphi)^{(4b)^a}}$ for some positive constant c.

Complexity

Theorem (V. Weispfenning)

There exists a Q.E. procedure assigning to any prenex formula φ (in the language of Presburger Arithmetic) an equivalent quantifier free formula φ'. If φ has at most a quantifier-blocks each of length at most b, then the algorithm runs in time and space bounded by $2^{c \cdot length(\varphi)^{(4b)^a}}$ for some positive constant c.

- $a = 1$

Complexity

Theorem (V. Weispfenning)

There exists a Q.E. procedure assigning to any prenex formula φ (in the language of Presburger Arithmetic) an equivalent quantifier free formula φ'. If φ has at most a quantifier-blocks each of length at most b, then the algorithm runs in time and space bounded by $2^{c \cdot length(\varphi)^{(4b)^a}}$ for some positive constant c.

- $a = 1$
- Reduction of $\exists - Th(\mathcal{A})$ to existential theory of Presburger Arithmetic is in time $O(2^{length(\varphi)})$,

Complexity

Theorem (V. Weispfenning)

There exists a Q.E. procedure assigning to any prenex formula φ (in the language of Presburger Arithmetic) an equivalent quantifier free formula φ'. If φ has at most a quantifier-blocks each of length at most b, then the algorithm runs in time and space bounded by $2^{c \cdot length(\varphi)^{(4b)^a}}$ for some positive constant c.

- $a = 1$
- Reduction of $\exists - Th(\mathcal{A})$ to existential theory of Presburger Arithmetic is in time $O(2^{length(\varphi)})$,
- Solving integer inequalities is NP-complete problem.

Complexity

Theorem (V. Weispfenning)

There exists a Q.E. procedure assigning to any prenex formula φ (in the language of Presburger Arithmetic) an equivalent quantifier free formula φ'. If φ has at most a quantifier-blocks each of length at most b, then the algorithm runs in time and space bounded by $2^{c \cdot length(\varphi)^{(4b)^a}}$ for some positive constant c.

- $a = 1$
- Reduction of $\exists - Th(\mathcal{A})$ to existential theory of Presburger Arithmetic is in time $O(2^{length(\varphi)})$,
- Solving integer inequalities is NP-complete problem.
- Time complexity for our algorithm to be $O(2^{2^{2^{length(\varphi)^{4b}}}})$.

Back to rationals

Theorem (F. Maurin)

The first order theory of $(\mathbb{N}, \times, <_P)$, *where* $<_P$ *is a 2-place predicate standing for the usual order relation in* $\mathbb{N}$ *restricted on primes, is decidable.*

Back to rationals

Theorem (F. Maurin)

The first order theory of $(\mathbb{N}, \times, <_P)$, where $<_P$ is a 2-place predicate standing for the usual order relation in $\mathbb{N}$ restricted on primes, is decidable.

Consider the structure $\mathrm{B} = (\mathbb{Q}^+, \times, N, <_P)$, where N is a 1-place predicate standing for the set of natural numbers.

Back to rationals

Theorem (F. Maurin)

The first order theory of $(\mathbb{N}, \times, <_P)$*, where* $<_P$ *is a 2-place predicate standing for the usual order relation in* $\mathbb{N}$ *restricted on primes, is decidable.*

Consider the structure $\mathrm{B} = (\mathbb{Q}^+, \times, N, <_P)$, where N is a 1-place predicate standing for the set of natural numbers.

The decidability of Th(B) follows from the decidability of $(\mathbb{N}, \times, <_P)$.

Intepratation of $\mathcal{A}$ into B

Intepratation of $\mathcal{A}$ into B

- $S_P(x,y) \iff Prime(x) \wedge Prime(y) \wedge \forall z(Prime(z) \rightarrow \neg(x <_P z \wedge z <_P y))$.

Intepratation of $\mathcal{A}$ into B

- $S_P(x,y) \iff Prime(x) \wedge Prime(y) \wedge \forall z(Prime(z) \rightarrow \neg(x <_P z \wedge z <_P y))$.
- $P_0(x) \iff Prime(x) \wedge \forall y(Prime(y) \rightarrow (x <_p y \vee x = y))$.

Intepratation of $\mathcal{A}$ into B

- $S_P(x,y) \iff Prime(x) \wedge Prime(y) \wedge \forall z(Prime(z) \rightarrow \neg(x <_P z \wedge z <_P y))$.
- $P_0(x) \iff Prime(x) \wedge \forall y(Prime(y) \rightarrow (x <_p y \vee x = y))$.
- $P_{i+1}(x) \iff \exists y_1, ..., y_i(\bigwedge_j Prime(y_j) \wedge Prime_0(y_0) \wedge y_i = x \wedge \bigwedge_j S_P(y_j, y_{j+1}))$.

Intepratation of $\mathcal{A}$ into B

- $S_P(x,y) \iff Prime(x) \wedge Prime(y) \wedge \forall z(Prime(z) \rightarrow \neg(x <_P z \wedge z <_P y))$.
- $P_0(x) \iff Prime(x) \wedge \forall y(Prime(y) \rightarrow (x <_p y \vee x = y))$.
- $P_{i+1}(x) \iff \exists y_1, ..., y_i(\bigwedge_j Prime(y_j) \wedge Prime_0(y_0) \wedge y_i = x \wedge \bigwedge_j S_P(y_j, y_{j+1}))$.
- $den(x) = z \iff N(z) \wedge N(x \times z) \wedge \forall w_1[N(w) \wedge N(w_1 \times x) \rightarrow \exists w_2(w_2 \times z = w_1)]$,

where $x = \frac{y}{z}$ and $(y, z) = 1$.

The structure $\mathcal{A}$ is definable in B as follows:

The structure $\mathcal{A}$ is definable in B as follows:

- $d =$'gcd'(x, y) is interpreted by

$$\frac{gcd(lcm(den(x), den(y)) \times x, \quad lcm(den(x), den(y)) \times y)}{lcm(den(x), den(y))}.$$

The structure $\mathcal{A}$ is definable in B as follows:

• $d =$'gcd'(x, y) is interpreted by

$$\frac{gcd(lcm(den(x), den(y)) \times x, \quad lcm(den(x), den(y)) \times y)}{lcm(den(x), den(y))}.$$

• For each constant c of $\mathcal{A}$ with support $\{i_1, ..., i_n\}$ we have $x = c$ is interpreted by
$\exists y_1, ..., y_n(\bigwedge_j P_j(y_j) \wedge x = y_1^{(c)_{i_1}} \times ... \times y_n^{(c)_{i_n}})$.

Complexity

The translation of any existential L-sentence φ into a $\{\times, N, <_P\}$-sentence φ' gives us that φ' is of depth 3.

Complexity

The translation of any existential L-sentence φ into a $\{\times, N, <_P\}$-sentence φ' gives us that φ' is of depth 3. Using the complexity bounds for sentences of depth 3, we obtain time complexity of the algorithm deciding φ' be $O(2^{2^{2^{length(\varphi')}}})$.

Complexity

The translation of any existential L-sentence φ into a $\{\times, N, <_P\}$-sentence φ' gives us that φ' is of depth 3. Using the complexity bounds for sentences of depth 3, we obtain time complexity of the algorithm deciding φ' be $O(2^{2^{2^{length(\varphi')}}})$.

On the other hand $length(\varphi') = length(\varphi) log(length(\varphi))$.

Complexity

The translation of any existential L-sentence φ into a $\{\times, N, <_P\}$-sentence φ' gives us that φ' is of depth 3. Using the complexity bounds for sentences of depth 3, we obtain time complexity of the algorithm deciding φ' be $O(2^{2^{2^{length(\varphi')}}})$.

On the other hand $length(\varphi') = length(\varphi)log(length(\varphi))$.

Time complexity for this algorithm is $O(2^{2^{2^{length(\varphi)log(length(\varphi)}}})$.

Extensions of $\mathcal{A}$

Let G be a finite abelian group.
$a : \mathbb{Z}^{<\omega} \to G$ an recursive homomorphism of groups which is onto.

Extensions of $\mathcal{A}$

Let G be a finite abelian group.
$a : \mathbb{Z}^{<\omega} \to G$ an recursive homomorphism of groups which is onto.
Consider L_a to be the language $L \cup \{P_g\}_{g \in G})$.

Extensions of $\mathcal{A}$

Let G be a finite abelian group.
$a : \mathbb{Z}^{<\omega} \to G$ an recursive homomorphism of groups which is onto.
Consider L_a to be the language $L \cup \{P_g\}_{g \in G})$.

$$\mathcal{A}_a = (\mathbb{Z}^{<\omega};\ +;\ min;\ C; \{|_n\}_{n \in \mathbb{N}}; \{P_g\}_{g \in G}),$$

where $+$, min, C and $|$ are as defined in the introduction and

$$P_g(x) \iff a(x) = g.$$

Extensions of $\mathcal{A}$

Let G be a finite abelian group.
$a : \mathbb{Z}^{<\omega} \to G$ an recursive homomorphism of groups which is onto.
Consider L_a to be the language $L \cup \{P_g\}_{g \in G})$.

$$\mathcal{A}_a = (\mathbb{Z}^{<\omega};\ +;\ min;\ C; \{|_n\}_{n \in \mathbb{N}}; \{P_g\}_{g \in G}),$$

where $+$, min, C and $|$ are as defined in the introduction and

$$P_g(x) \iff a(x) = g.$$

Theorem

The positive existential theory of $\mathcal{A}_a$ is decidable.

Let F be a set of subgroups H of $\mathbb{Z}^{<\omega}$ of finite index in $\mathbb{Z}^{<\omega}$. Consider the structure $\mathcal{A}_F = (\mathbb{Z}^{<\omega};\ +;\ min;\ C; \{|_n\}_{n\in\mathbb{N}}; \{P_H\}_{H\in F})$, where $+$, min, C and $|_n$ are interpreted as usual and $P_H(x) \iff x \in H$.

Let F be a set of subgroups H of $\mathbb{Z}^{<\omega}$ of finite index in $\mathbb{Z}^{<\omega}$. Consider the structure $\mathcal{A}_F = (\mathbb{Z}^{<\omega};\ +;\ min;\ C; \{|_n\}_{n\in\mathbb{N}}; \{P_H\}_{H\in F})$, where $+$, min, C and $|_n$ are interpreted as usual and $P_H(x) \iff x \in H$.

Theorem

The existential theory of $\mathcal{A}_F$ is decidable.

Properties of $\mathcal{A}$ from the model theoretical point of view

Definition

Let T be a complete theory. Then T is unstable if and only if there is a model $\mathcal{M}$ of T, with universe M, an infinite $X \subset M^n$ and a formula $\varphi(\bar{x}, \bar{y})$ ($\bar{x} = (x_1, ..., x_n)$, $\bar{y} = (y_1, ..., y_n)$) defining total ordering on X.

Properties of $\mathcal{A}$ from the model theoretical point of view

Definition

Let T be a complete theory. Then T is unstable if and only if there is a model $\mathcal{M}$ of T, with universe M, an infinite $X \subset M^n$ and a formula $\varphi(\bar{x}, \bar{y})$ ($\bar{x} = (x_1, ..., x_n)$, $\bar{y} = (y_1, ..., y_n)$) defining total ordering on X.

Definition

Let T be a complete theory. We say that a formula $\varphi(\bar{x}, y)$ ($\bar{x} = (x_1, ..., x_m)$) satisfies IP (independence property) in T if and only if in every model M of T there is for each $n \in \mathbb{N}$ a family $b_0, ...b_{n-1}$ such that, for all subsets X of $\{0, ..., n-1\}$ there is $(\bar{a}) \in |M|^m$

$$M \models \varphi(\bar{a}, b_i) \iff i \in X.$$

T is said to satisfy IP if there is a formula which satisfies IP in T.

Definition

We say that a formula $\varphi(x, \bar{y})$, with $\bar{y} = (x_1, ..., x_m)$, has BTP (binary tree property) if there is a set of m-tuples, $\{c_\beta : \beta \in 2^{<\mathbb{N}}\}$, such that

- $\{\varphi(x, c_{\beta|n}) : n \in \mathbb{N}\}$ is consistent, for each $\beta \in 2^{\mathbb{N}}$.
- $\varphi(x, c_{\beta_1}) \wedge \varphi(x, c_{\beta_2})$ is inconsistent, for every incomparable β_1, β_2.

A complete theory T is said to have BTP if there is a formula which satisfies BTP in T.

Definition

We say that a formula $\varphi(x, \bar{y})$, with $\bar{y} = (x_1, ..., x_m)$, has BTP (binary tree property) if there is a set of m-tuples, $\{c_\beta : \beta \in 2^{<\mathbb{N}}\}$, such that

- $\{\varphi(x, c_{\beta|n}) : n \in \mathbb{N}\}$ is consistent, for each $\beta \in 2^{\mathbb{N}}$.
- $\varphi(x, c_{\beta_1}) \wedge \varphi(x, c_{\beta_2})$ is inconsistent, for every incomparable β_1, β_2.

A complete theory T is said to have BTP if there is a formula which satisfies BTP in T.

Definition

We say that a formula $\varphi(x, \bar{y})$, with $\bar{y} = (x_1, ..., x_m)$, has TP_2 (tree property) if there are m-tuples $(\alpha_{i,j})_{i,j \in \mathbb{N}}$ and $k \in \mathbb{N}$ such that

- $\{\varphi(x, \alpha_{i,j}) : j \in \mathbb{N}\}$ is k-incosistent, for each $i \in \mathbb{N}$.
- $\{\varphi(x, \alpha_{i,f(i)}) : i \in \mathbb{N}\}$ is cosistent, for each $f : \mathbb{N} \to \mathbb{N}$.

A complete theory T is said to have TP_2 if there is a formula which satisfies TP_2 in T.

Known fact:

$$\mathrm{TP}_2 \Rightarrow \mathrm{IP} \Rightarrow \mathrm{Unstable}$$

Known fact:

$$\mathrm{TP}_2 \Rightarrow \mathrm{IP} \Rightarrow \mathrm{Unstable}$$

Theorem

$Th(\mathcal{A})$ satisfies TP_2 and BTP.