Incompleteness in the finite domain

Pavel Pudlák[1]

Institute of Mathematics, Czech Academy of Sciences, Prague

Ghent, September 2018

[1]author supported by the ERC advanced grant "FEALORA"

Overview

1. syntactic versus semantic incompleteness
2. **TFNP** problems and unprovable $\forall\Sigma_1^b$ sentences
3. $\forall\Sigma_1^b$ sentences provable in fragments of Bounded arithmetic
4. pairs of disjoint **NP** sets and unprovable $\forall\Sigma_0^b$ sentences

Two types of incompleteness

1. "syntactic" – self-referential sentences, consistency statements (typically, Π_1 sentences)
2. "semantic" – unprovability of fast growing computable functions (Π_2 sentences)

Two types of incompleteness

1. "syntactic" – self-referential sentences, consistency statements (typically, Π_1 sentences)
2. "semantic" – unprovability of fast growing computable functions (Π_2 sentences)

Type 2: Given a formal theory T, diagonalize over all computable functions that are provably total in T to obtain a computable function f growing faster.

Note that

$$T \nvdash \forall x \exists y\ \phi(x, y)$$

for every Σ_1 formula ϕ that defines f in $\mathbb{N}$.

another example

Proof theoretical ordinal of T: the least constructive ordinal α such that T does not prove that an ordering of type α is well-founded **for any Σ_1 definition of the ordering**.

semantic $\mapsto$ computational content

Σ_i^b formulas

Consider arithmetical formulas in a language L where function symbols are polynomial time computable functions.

Suppose L also contains a symbol for function that grows like $\log_2 x$, we will denote it by $|x|$ ("the length of the number x).

bounded quantifiers – as usual.

sharply bounded quantifiers – $\forall x \leq |t|$, $\exists x \leq |t|$, where t is a term (not containing x)

prenex formula ϕ is Σ_i^b if it has i alternation of bounded quantifiers, starting with $\exists$ and ignoring the sharply bounded ones

strict Σ_i^b formula is a Σ_i^b where all sharply bounded quantifiers are after non-sharply bounded ones

Unprovable $\forall\Sigma_1^b$ sentences

Instead of Π_2 sentences, we are interested in Π_1 sentences of the form $\forall x.\phi(x)$ where $\phi(x)$ is Σ_1^b.

Unprovable $\forall\Sigma_1^b$ sentences

Instead of Π_2 sentences, we are interested in Π_1 sentences of the form $\forall x.\phi(x)$ where $\phi(x)$ is Σ_1^b.

Consistency statements can be represented in this form, but we want "semantic independence".

Σ_1^b formulas

Σ_i^b define **NP** predicates, i.e.,

$$\exists y(|y| \leq p(|x|) \wedge \psi(x, y)),$$

where p is a polynomial and ψ is a binary relation computable in polynomial time.

Σ_1^b formulas

Σ_i^b define **NP** predicates, i.e.,

$$\exists y(|y| \leq p(|x|) \wedge \psi(x, y)),$$

where p is a polynomial and ψ is a binary relation computable in polynomial time.

Why a sentence of the form

$$\forall x \exists y(|y| \leq p(|x|) \wedge \psi(x, y)),$$

is unprovable in T?

Σ_1^b formulas

Σ_i^b define **NP** predicates, i.e.,

$$\exists y(|y| \leq p(|x|) \land \psi(x, y)),$$

where p is a polynomial and ψ is a binary relation computable in polynomial time.

Why a sentence of the form

$$\forall x \exists y(|y| \leq p(|x|) \land \psi(x, y)),$$

is unprovable in T?

Conjecture

. . . because finding y, for a given x, is computationally difficult.

TFNP

Definition

1. A **TFNP** problem is given by a binary relation R and a polynomial p such that

$$\mathbb{N} \models \forall x \exists y (|y| \leq p(|x|) \wedge R(x, y)).$$

   The computational task associated with the problem is, given x, to construct y such that $|y| \leq p(|x|) \wedge R(x, y)$.

2. A **TFNP** problem (R, p) is polynomially reducible to (Q, r), if (R, p) can be solved in polynomial time using an oracle for (Q, r).

TFNP

Questions

- Can every **TFNP** problem be solved in polynomial time?
- Does there exist a complete **TFNP** problem?

TFNP

Questions

- Can every **TFNP** problem be solved in polynomial time?
- Does there exist a complete **TFNP** problem?

Facts

- Cryptography is only possible if there are hard **TFNP** problems.
- Many apparently distinct subclasses have been studied (**PLS, PPA, PPAD, PPP,** ...).
- The existence of hard **TFNP**s follows from **P**$\neq$**NP**$\cap$**coNP**, but apparently not from other standard hypotheses such as **P**$\neq$**NP**.

The TFNP conjecture

Conjecture

For every consistent theory[2] T *there exists a* **TFNP** *problem* (R, p) *such that for no formalization of* R *by a* Σ_1^b *formula* ψ, T *proves that the problem is total; i.e.,*

$$T \nvdash \forall x \exists y (|y| \leq p(|x|) \land \psi(x, y)).$$

[2] finitely axiomatized, arithmetical, sufficiently strong, i.e., $T \supseteq S_2^1$,

The TFNP conjecture

Conjecture

For every consistent theory[2] T *there exists a* **TFNP** *problem* (R, p) *such that for no formalization of* R *by a* Σ_1^b *formula* ψ*,* T *proves that the problem is total; i.e.,*

$$T \nvdash \forall x \exists y (|y| \leq p(|x|) \wedge \psi(x, y)).$$

Theorem

The conjecture above is equivalent to:

- *there is no complete problem in* **TFNP***.*

[2] finitely axiomatized, arithmetical, sufficiently strong, i.e., $T \supseteq S_2^1$,

some evidence for the TFNP conjecture

Buss' hierarchy of fragments of Bounded Arithmetic:

$$S_2^i \ := \ BASIC + \Sigma_i^b - PIND$$

some evidence for the TFNP conjecture

Buss' hierarchy of fragments of Bounded Arithmetic:

$$S_2^i \ := \ BASIC + \Sigma_i^b - PIND$$

Theorem

The provably total **TFNP** *problems of* S_2^i *are exactly the problems from* $\mathbf{GPLS}_{i-1}$.

It seems very plausible that the classes increase as i grows.

GPLS$_i$

- **GPLS$_0$** - problems solvable in polynomial time.

GPLS$_i$

- **GPLS**$_0$ - problems solvable in polynomial time.
- **GPLS**$_1$ (= **PLS**) - problems reducible to problems of the following type:

  An instance is given by polynomial time functions $v(x, y), h(x, y)$. For a given a, find b such that

$$v(a, b) \leq v(a, h(a, b)).$$

$\mathbf{GPLS}_i$

- $\mathbf{GPLS}_0$ - problems solvable in polynomial time.
- $\mathbf{GPLS}_1$ ($= \mathbf{PLS}$) - problems reducible to problems of the following type:

  An instance is given by polynomial time functions $v(x, y), h(x, y)$. For a given a, find b such that

  $$v(a, b) \leq v(a, h(a, b)).$$

A solution always exists:
for a given a, take b such that $v(a, b)$ attains the minimum.

- **GPLS$_2$** - problems reducible to problems of the following type:

  An instance is given by polynomial time functions $v(x, y, z), h_1(x, y), h_2(x, y, z)$. For a given a, find b_1, b_2 such that

  $$v(a, b, h_2(a, b, c)) \leq v(a, h_1(a, b), c).$$

- **GPLS$_2$** - problems reducible to problems of the following type:

  An instance is given by polynomial time functions $v(x, y, z), h_1(x, y), h_2(x, y, z)$. For a given a, find b_1, b_2 such that

  $$v(a, b, h_2(a, b, c)) \leq v(a, h_1(a, b), c).$$

A solution always exists:

For a, b, let $\gamma(a, b)$ be such that $v(a, b, \gamma(a, b))$ attains the maximum.
For a given a, let b be such that $v(a, b, \gamma(a, b))$ attains the minimum, and let $c = \gamma(a, b)$.
Then we have

$$v(a, b, h_2(a, b, c)) \leq v(a, b, \gamma(a, b)) \leq v(a, h_1(a, b), \gamma(a, b)) =$$

$$v(a, h_1(a, b), c).$$

Problem

Construct an oracle A such that $\mathbf{GPLS}_i^A \neq \mathbf{GPLS}_{i+1}^A$.

We only know A such that $\mathbf{GPLS}_0^A \neq \mathbf{GPLS}_1^A$.

Problem

Construct an oracle A such that $\mathbf{GPLS}_i^A \neq \mathbf{GPLS}_{i+1}^A$.

We only know A such that $\mathbf{GPLS}_0^A \neq \mathbf{GPLS}_1^A$.

Theorem

There exists an oracle A such that $\mathbf{TFNP}^A$ *does not have a complete problem.*

Herbrand Consistency Search

Proposition

Let $\Phi := \forall x_1 \ldots \forall x_n . \psi(x_1, \ldots, x_k)$ *be a universal sentence. Then* Φ *is consistent iff for every family of terms* $\{t_{ij}\}$*,*

$$\bigwedge_{i=1}^{n} \psi(t_{i1}, \ldots, t_{ik}) \tag{1}$$

is propositionally satisfiable.

Herbrand Consistency Search

Proposition

Let $\Phi := \forall x_1 \ldots \forall x_n.\psi(x_1, \ldots, x_k)$ *be a universal sentence. Then* Φ *is consistent iff for every family of terms* $\{t_{ij}\}$,

$$\bigwedge_{i=1}^{n} \psi(t_{i1}, \ldots, t_{ik}) \tag{1}$$

is propositionally satisfiable.

Definition (Herbrand Consistency Search, HCS(Φ))

Given a consistent universal sentence $\forall x_1 \ldots \forall x_n.\psi(x_1, \ldots, x_k)$ and a family of terms $\{t_{ij}\}$, find an assignment of propositional values to the atomic formulas that makes (1) true.

Fact

If Φ is consistent and sufficiently strong, then Φ does not prove that HCS(Φ) is total for the natural formalization of HCS(Φ).

Fact

If Φ is consistent and sufficiently strong, then Φ does not prove that HCS(Φ) is total for the natural formalization of HCS(Φ).

Conjecture

A consistent Φ does not prove that HCS(Φ) is total for any formalization of HCS(Φ) by a Σ_1^b formula.

Universal-**P** sentences

$$\forall x.\phi(x),$$

where ϕ defines a set in **P**, provably in a weak theory, e.g., S_2^1.

Universal-**P** sentences

$$\forall x.\phi(x),$$

where ϕ defines a set in **P**, provably in a weak theory, e.g., S^1_2.

We want to know if

$$\mathbb{N} \models \forall x.\phi(x).$$

Universal-P sentences

$$\forall x.\phi(x),$$

where ϕ defines a set in **P**, provably in a weak theory, e.g., S_2^1.

We want to know if

$$\mathbb{N} \models \forall x.\phi(x).$$

No computational content unless ϕ has some special structure.

example: disjoint pairs of **NP** sets

Let $A, B \in$**NP**, let

$$\phi(x) := \; x \notin A \vee x \notin B.$$

Thus

$$\forall x . \phi(x) \; \equiv A \cap B = \emptyset,$$

and $\phi(x)$ is provably a **coNP** predicate, hence $\forall x.\phi(x)$ can be represented by a universal-**P** sentence.

[3] Point to one of the two sets in which x is not contained.

example: disjoint pairs of **NP** sets

Let $A, B \in$**NP**, let

$$\phi(x) := \ x \notin A \vee x \notin B.$$

Thus

$$\forall x.\phi(x) \ \equiv A \cap B = \emptyset,$$

and $\phi(x)$ is provably a **coNP** predicate, hence $\forall x.\phi(x)$ can be represented by a universal-**P** sentence.

The computational problem: given x, decide the disjunction.[3]

[3] Point to one of the two sets in which x is not contained.

example: disjoint pairs of **NP** sets

Let $A, B \in$**NP**, let

$$\phi(x) := \; x \notin A \vee x \notin B.$$

Thus

$$\forall x.\phi(x) \; \equiv A \cap B = \emptyset,$$

and $\phi(x)$ is provably a **coNP** predicate, hence $\forall x.\phi(x)$ can be represented by a universal-**P** sentence.

The computational problem: given x, decide the disjunction.[3]

(A, B) is polynomially reducible to (C, D), if there exists a polynomial time computable f such that

$$f(A) \subseteq C \text{ and } f(B) \subseteq D.$$

[3] Point to one of the two sets in which x is not contained.

Questions

- Are there pairs for which the problem is not solvable in polynomial time?
- Does there exist a complete pair?

Fact

- The existence of a hard disjoint **NP** pair follows from **NP**$\cap$**coNP**$\neq$**P**.

equivalent conjectures

Conjecture

There is no complete disjoint **NP** *pair.*

Conjecture

For every consistent[4] *theory T, there exists a pair of disjoint* **NP** *sets (A, B) such that for no formalization of A and B by Σ_1^b formulas, T proves $A \cap B = \emptyset$.*

[4] finitely axiomatized, arithmetical, sufficiently strong

Hard disjoint **NP** pairs

1. cryptographic conjectures give us sets $A \in \mathbf{NP} \cap \mathbf{coNP} \setminus \mathbf{P}$; for such an A, the pair $(A, \overline{A})$ is hard;
2. pairs from reflection principles, called canonical pairs;
3. combinatorial pairs ???

Reflection principles

Let $Prf(x, y)$ be a formalization of y is a proof of x.

Let $Sat(x, z)$ be a formalization of x is satisfied by z.

Reflection principle:

$$Prf(x, y) \rightarrow Sat(x, z)$$

Reflection principles

Let $Prf(x, y)$ be a formalization of y is a proof of x.

Let $Sat(x, z)$ be a formalization of x is satisfied by z.

Reflection principle:

$$\neg Prf(x, y) \vee Sat(x, z)$$

Reflection principles

Let $Prf(x, y)$ be a formalization of y is a proof of x.

Let $Sat(x, z)$ be a formalization of x is satisfied by z.

Reflection principle:

$$\neg Prf(x, y) \vee Sat(x, z)$$

To get a pair of disjoint **NP** sets we need to bound the length of the proof y in the length of x. We can

- consider only proofs of quadratic length, or
- pad x to $x0^n$ and bound $|y| \leq n$.

Questions

- Are such canonical pairs hard?
- Can we find combinatorial characterizations of them?

Questions

- Are such canonical pairs hard?
- Can we find combinatorial characterizations of them?

Facts

- From some cryptographic conjectures, we can prove that canonical pairs of bounded depth Frege proof systems are hard.
- It seems that already the canonical pair of Resolutions is hard.
- We have characterizations of canonical pairs of bounded depth Frege proof systems in terms of some combinatorial games.

Problem

How much stronger a theory S must be than T in order to prove the disjointness of more disjoint **NP** *pairs?*

Problem

How much stronger a theory S must be than T in order to prove the disjointness of more disjoint **NP** *pairs?*

A plausible conjecture is that $S \vdash Con(T)$ suffices.

Finite consistency statements

Let $Con_T(n)$ denote that there is no T-proof of contradiction of length $\leq n$.

Theorem

If T is sequential and finitely axiomatized, then $Con_T(n)$ has proofs of length $\leq p(n)$ for some polynomial.

Finite consistency statements

Let $Con_T(n)$ denote that there is no T-proof of contradiction of length $\leq n$.

Theorem

If T is sequential and finitely axiomatized, then $Con_T(n)$ has proofs of length $\leq p(n)$ for some polynomial.

Theorem

If there does not exist a complete disjoint **NP** *pair, then for every S there exists T such that $Con_T(n)$ does not have polynomial length S-proofs.*

Finite consistency statements

Let $Con_T(n)$ denote that there is no T-proof of contradiction of length $\leq n$.

Theorem
If T is sequential and finitely axiomatized, then $Con_T(n)$ has proofs of length $\leq p(n)$ for some polynomial.

Theorem
If there does not exist a complete disjoint **NP** *pair, then for every S there exists T such that $Con_T(n)$ does not have polynomial length S-proofs.*

Question How much stronger must T be than S.

Conjecture

$Con_{S+Con_S}(n)$ does not have polynomial length S-proofs.

Conjecture

$Con_{S+Con_S}(n)$ does not have polynomial length S-proofs.

Theorem (Ehrenfeucht-Mycielski)

If T is stronger than S, then T has uncomputable speed-up over S w.r.t. sentences provable in both theories.

Conjecture

$Con_{S+Con_S}(n)$ does not have polynomial length S-proofs.

Theorem (Ehrenfeucht-Mycielski)

If T is stronger than S, then T has uncomputable speed-up over S w.r.t. sentences provable in both theories.

Theorem (Hrubeš)

There exists a Π_1 sentence ϕ unprovable in S such that $Con_{S+\phi}(n)$ have polynomial length proofs.

ϕ is a modification of the Rosser sentence.

Conclusions

- We argued that particular Π_1 sentences could be independent due to semantic properties connected with computational complexity.
- We cannot prove such conjectures because they are typically much stronger than $\mathbf{P} \neq \mathbf{NP}$.

Conclusions

- We argued that particular Π_1 sentences could be independent due to semantic properties connected with computational complexity.
- We cannot prove such conjectures because they are typically much stronger than $\mathbf{P} \neq \mathbf{NP}$.

Thank you