Univerzita Karlova

Filozofická fakulta

Katedra logiky

BAKALÁŘSKÁ PRÁCE

Martin Maxa

Polynomiální neúplnost

Feasible Incompleteness

Praha 2019 **Vedoucí práce: prof. RNDr. Pavel Pudlák, DrSc.**

I am very grateful to my supervisor prof. RNDr. Pavel Pudlák, DrSc. for his kind advices and patient guidance.

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In .... date .... signature of the author

Klíčková slova (česky):

Polynomiální neúplnost, Finitní Gödelovy věty, Výpočetní složitost, Finitní Löbova věta, P versus NP problém, Základy matematiky

Klíčková slova (anglicky):

Feasible incompleteness, Finite versions of Gödels theorems, Computational complexity, Finite Löb's theorem, P versus NP probem, Foundations of mathematics

Abstrakt (česky):

V této práci se zabýváme finitními protějšky známých vět, jež se týkají základů matematiky, jako jsou Gödelovy věty o neúplnosti či Löbova věta. Jejich finitní verze jsou již silnější než známé otevřené problémy ve výpoční složitosti jako např. $P \neq NP$. Kromě finitní verze druhé Gödelovy věty, jež byla zavedena v práci [5], představíme i finitní verzy První Gödelovy věty a dokážeme jejich ekvivalenci. Dále představíme i některé další domněnky, jež již implikují finitní verzi První Gödelovy věty a které jsou zajímavé tím, že jde o pozitivní tvrzení. Uvedeme navíc tvrzení, jež by se dalo nazvat finitní verzí Löbovy věty a dokážeme její vztah k ostatním domněnkám.
Cílem této práce je ukázat, že otevřené problémy ve výpočetní složitosti mají velmi blízký vztah k problémům dotýkajících se samých základů matematiky a logiky a že koncept polynomiální dokazatelnosti je podobně důležitý koncept jako koncept dokazatelnosti klasické.

Abstract (in English):

We will present in this thesis finite counterparts to the well known theorems that are connected to the foundations of mathematics such as Gödel's incompleteness theorems or Löb's theorem. Their finite versions go already beyond famous open problems in computational theory, for example $P \neq NP$. Beside finite version of Gödel's second incompleteness theorem that was introduced in [5], we present also finite version of Gödel's first incompleteness theorem and we will prove that they are equivalent. Moreover, we present conjectures that are stronger than finite version of Gödel's first incompleteness theorem and that are interesting as they refer to the positive statements of mathematics. We will also present a conjecture that could be called finite version of Löb's theorem and we will prove relationship of this conjecture to the other conjectures.
The aim of this thesis is to show that open problems in computational complexity are closely connected to the problems of the foundations of mathematics and logic and that the concept of polynomial, or we can say feasible, provability is similarly important as is the concept of classical provability.

Contents

Introduction

We will first recall Hilbert's program. Hilbert wanted to prove by finite means consistency of mathematics. It can be also interpreted that his goal was to prove in arithmetical theory (for example the well known Peano arithmetic) consistency of Zermelo-Fraenkel set theory, ZFC. Gödel later proved that this goal cannot be realized. We can't even prove consistency of Peano arithmetic inside Peano arithmetic. Nevertheless, if we view this problem from the practical standpoint, then it is not necessary to prove consistency of a given theory, it is sufficient to prove consistency for proofs of length up to some practically conceivable number. If we succeed in proving that in a given theory no proof of the length, say, billion symbols contains contradiction, it would be, from the practical viewpoint, realization of Hilbert's program. The most interesting scenario is if we can prove finite consistency of a strong theory in a relatively weak theory in which we believe it is consistent. As we can see, in fact a proof of consistency of T in the theory T itself doesn't tell us any useful new facts as a theory that is not consistent clearly proves its consistency too.

Feasible incompleteness, or we can also say incompleteness in the finite domain, is related to the problem how difficult is to prove finite consistency of a given theory in a weaker theory. There were in [1], [4] and [3] presented several conjectures that state that Hilbert's program cannot be realized even from practical viewpoint. These conjecture have a close relationship to the well known open problems in computational complexity theory, Gödel's theorems and for this reason also to the foundations of mathematics. Thus, it is possible that important conjectures in computational complexity, as is for example $P \neq NP$, and Gödel's theorems are just two facets of the same phenomenon, namely incompleteness.

The goal of this thesis is, on the base of analogy with known results, to state conjectures that are related to feasible incompleteness. A finite version of Gödel's second incompleteness theorem was for the first time stated in [5], p. 193. This conjecture already implies a result stronger than is $P \neq NP$ (in fact, it implies $NEXP \neq coNEXP$ as is proved in the same paper). It is an interesting fact that there exists also finite version of Gödel's first incompleteness theorem and this conjecture is equivalent to the finite version of Gödel's second incompleteness theorem in the same way as in the classical version. At the beginning of the thesis, we will state the finite version of this conjecture.

It is a known fact that proving negative result in mathematics, that something doesn't exist, is in the most cases much more difficult than to prove that something exists. One of such possible negative result is $P \neq NP$. It is a conjecture about non-existence of polynomial algorithm for certain set of problems. The first finite incompleteness theorem suggests that a positive statement in logic can be transformed to a negative statement with the help of the autoreference similarly as has been showed by Kurt Gödel. We will state such possible positive conjectures that already implies first (and second) finite incompleteness theorem. We are not sure if these conjectures are true but as we said, these conjectures may be interesting as they are related to positive aspects of mathematics and logic.

In the next section we introduce a finite version of Rosser's theorem. Moreover, in chapter 5, we will state a conjecture which can be called finite Löb's theorem. We will also mention its uniform stronger version and prove relationships between other conjectures introduced in this thesis.

We believe that this thesis can deepen our understanding about the phenomenon of feasible provability and, last but not least, it can stimulate further research in this fascinating area of mathematics.

1. Preliminaries

1.1 Theories

We suppose that the term "*theory*" means a set of axioms that is decidable in polynomial time. This is an important assumption as we can check in polynomial time if a string of symbols d is a proof of a given formula or not. We will use sufficiently strong fragments of Peano Arithmetic that are already able to formalize various syntactical aspects of the theory. Thus, we will first define our base theory, the weakest theory we assume, and then we consider all consistent arithmetical theories that contain the base theory.

We will first describe the theory S_2. The language of the theory S_2 contains, besides the usual language of arithmetic, the symbols $\lfloor x/2 \rfloor$, $|x|$, $x\#y$. The interpretation of $\lfloor x/2 \rfloor$ is the standard one, the interpretation of $|x|$ is the length of the binary representation of x if $x > 0$ and 0 otherwise. Finally, the interpretation of $x\#y$ is $2^{|x|*|y|}$. Thus, we can in fact express the product of the lengths of x and y. The theory S_2 is axiomatized by a set of axioms called BASIC that introduces the intended interpretation of the symbols and by the following induction scheme for all bounded formulas φ

$$\varphi(\overline{0}) \land \forall x(\varphi(\lfloor x/2 \rfloor) \to \varphi(x)) \to \forall x \varphi(x)$$

The theory S_2^i is then the theory S_2 with induction scheme restricted to Σ_i^b formulas. We will explain the meaning of Σ_i^b formulas below.

1.2 Formulas

It is easily proved that if x is bounded by some term $t(y_1, y_2, \ldots, y_k)$ in the theory S_2, then the length of x is polynomially bounded by the lengths of $y_1, \ldots, y_k$. We can also use *sharp* bounds in the language of S_2, the bounds of the form $x \leq |s(y_1, \ldots, y_k)|$. In this case, the number x is polynomially bounded by the lengths of $y_1, \ldots, y_k$. We can then define *sharply bounded quantifiers*, the bounded quantifiers with sharp bounds. Bounded formulas Σ_n^b, Π_n^b. Σ_n^b and Π_n^b are defined as a formulas with n alternation of bounded quantifiers while we ignore sharply bounded quantifiers.

1.3 Proofs

We suppose in this thesis that the proof system is the classical Hilbert-style proof system.

We moreover assume that the formulas and proofs in this proof system are encoded by binary sequences. A length of proof is then the length of its binary code. A proof in some theory T will be shortly called T-proof.

1.4 Notation

We denote by letters $p, q, r, p_1, q_1 \dots$ polynomial functions.

$\mathcal{T}$ denotes the same class of theories as is defined in [7]. Specifically, $\mathcal{T}$ is a class of all consistent arithmetical theories that extend Buss's theory S^1_2 by a set of axioms that is in the complexity class P.

If T is some theory and φ a sentence, then $T + \varphi$ denotes the extension of the theory T by the sentence φ.

A binary numeral $\overline{n}$ is a closed term such that if binary representation of the number n is of the form $a_1, a_2, \dots, a_k$, then

$$\overline{n} = (\dots((a_1 * \overline{2}) + a_2) * \overline{2} \dots + a_{k-1}) * \overline{2} + a_k$$

where $\overline{2}$ is the term $S(S(0))$. Thus, the term $\overline{n}$ has the length $O(\log(n))$

If φ is a formula with Gödel number n, then $\overline{\varphi}$ denotes a closed term $\overline{n}$. Moreover, if $\varphi(x)$ is a formula with one free variable x, then $\overline{\varphi(\dot{x})}$ denotes a formalization of the function "$n \mapsto$ Gödel number of the sentence $\varphi(\overline{n})$". Similarly, for a polynomial function p, $\overline{\varphi(\overline{p(\dot{x})})}$ denotes a formalization of the function "$n \mapsto$ Gödel number of the sentence $\varphi(\overline{p(n)})$"

We will use a useful notation from [6]

$$||\varphi||_T = \left\{ \begin{array}{c} \text{the least } n \text{ such that } T \vdash^n \varphi, \text{ if } T \vdash \varphi \\ \infty \text{ otherwise} \end{array} \right|$$

We will denote by the formula $Proof_S(x, y)$ a natural formalization of the relation "x is a S-proof of y". We moreover suppose that $Proof_S(x, y)$ is such a formalization that the following holds (cf. Fact 1 in [7])

Fact 1. *Let $T \in \mathcal{T}$ and let m be a Gödel number of a T-proof of a sentence whose Gödel number is n. Then there exists a S^1_2-proof of the sentence $Proof_T(\overline{m}, \overline{n})$ of the polynomial length in n and m*

Another assumption is that a formalization of Fact 1 is already provable in the theory S^1_2 (cf. Lemma 6.2.1. in [6])

A formula $P_T(y)$ is then defined as

$$P_T(y) \equiv_{df} \exists x Proof_T(x, y)$$

That is, $P_T(y)$ is Σ_1-formula that formalizes the relation "there exists an S-proof of y".

With the help of the formula $Proof_S(x, y)$, we define a formula $Pr_S(z, y)$ as a formula that formalizes the relation "there exists a S-proof of y of the length shorter than z"

We also suppose (see 1) that whenever a formula with Gödel number m has a T-proof of the length $\leq n$, then $Pr_T(\overline{n}, \overline{m})$ has a S^1_2-proof of the length $\leq p(n)$ for some polynomial function p. Moreover, a formalization of the above fact is provable in S^1_2 (cf. Corollary 6.1.6., p. 580 and Lemma 6.2.1., p 580 in [6]). See also the finite derivability conditions below.

We denote by $\exists p \forall n Pr_S(\overline{p(\dot{n})}, \overline{\varphi(\dot{n})})$ a natural formalization of the relation "there exists a polynomial function p such that for every n, $Pr_S(\overline{p(n)}, \overline{\varphi(\overline{n})})$"

Consistency of a given theory T, Con_T, is then defined as the sentence

$$Con_T \equiv_{df} \neg P_T(\overline{0 = S(0)})$$

Finite consistency, $Con_T(x)$, is defined with the help of the formula $Pr_T(x, y)$ in the following way

$$Con_T(x) \equiv_{df} \neg Pr_T(x, \overline{0 = S(0)})$$

The above properties of the finite provability predicate $Pr_T(x, y)$ are best expressed as finitistic counterparts of the well known classical derivability conditions that were used for Gödel's second incompleteness theorem.

1.5 The finite derivability conditions

We will often use the finite version of Löb's derivability conditions. These conditions for the predicate $Pr_T(x, y)$ were for the first time formulated in [5]. More specifically, let $T \in \mathcal{T}$ be a theory, then P. Pudlák formulated the following four conditions:

$$T \vdash \forall x \forall x' (x \leq x' \,\&\, Pr_T(x, y) \rightarrow Pr_T(x', y)) \tag{D0}$$

$$||\varphi(\overline{n})||_T \leq n \Rightarrow ||Pr_T(\overline{n}, \overline{\varphi(\overline{n})})||_T \leq p_1(n) \tag{D1}$$

$$T \vdash \forall x (Pr_T(x, \overline{\psi(\dot{x})}) \rightarrow Pr_T(\overline{q_1(\dot{x})}, \overline{Pr_T(\dot{x}, \overline{\psi(\dot{x})})})) \tag{D2}$$

$$T \vdash \forall x (Pr_T(\overline{p_2(\dot{x})}, \overline{\varphi(\dot{x})}) \,\&\, Pr_T(\overline{p_3(\dot{x})}, \overline{\varphi(\dot{x}) \rightarrow \psi(\dot{x})}) \rightarrow Pr_T(\overline{q_2(\dot{x})}, \overline{\psi(\dot{x})})) \tag{D3}$$

Where p_1, p_2, p_3, q_1 and q_2 are suitable polynomial functions. These conditions were for example used for proving a lower bound on the length of proofs of finite consistency statements in a given sufficiently strong theory.

2. Π_2 independent sentence

The following theorem is about independence of the sentence $\forall x P_S(\overline{Con_{S+Con_S}(\dot{x})})$ in a theory $S \in \mathcal{T}$, where moreover S is a Σ_1-sound theory. We suppose, that this result can be caused by computational complexity, more specifically, by exponential length of proofs of the formula $Con_{S+Con_S}(x)$ in the theory S.

Theorem 1. *Let S be a theory such that $S \in \mathcal{T}$ and, moreover, let S be Σ_1-sound. Then*

$$\mathbb{N} \models \forall x P_S(\overline{Con_{S+Con_S}(\dot{x})})$$

$$S \nvdash \forall x P_S(\overline{Con_{S+Con_S}(\dot{x})})$$

Proof. We can create, with the help of Diagonal Lemma, a formula $\varphi(y)$ with one free variable y and a such that

$$S \vdash \forall y(\varphi(y) \equiv \neg Pr_S(y, \overline{P_S(\overline{\varphi(\dot{y})})})) \tag{1}$$

First, we will prove two claims.

Claim 1. *Let φ be as above. Then*

$$\mathbb{N} \models \forall y \varphi(y) \tag{2}$$

$$\mathbb{N} \models \forall y P_S(\overline{\varphi(\dot{y})}) \tag{3}$$

Proof. Assume first that there exists n such that $\neg\varphi(\overline{n})$. From the fact that $\neg\varphi(\overline{n})$ is Δ_0-formula, we obtain by Σ_1-completeness of S that

$$S \vdash \neg\varphi(\overline{n}) \tag{4}$$

From 1, we also have

$$S \vdash Pr_S(\overline{n}, \overline{P_S(\overline{\varphi(\overline{n})})})$$

As S is Σ_1-sound theory, it follows that

$$S \vdash P_S(\overline{\varphi(\overline{n})}) \tag{5}$$

and again from Σ_1-soundness, we obtain from 5

$$S \vdash \varphi(\overline{n}) \tag{6}$$

But 6 and 4 are in contradiction with the fact that S is a consistent theory. Thus

$$\mathbb{N} \models \forall y \varphi(y) \tag{7}$$

From 7 and the fact that $\varphi(\overline{n})$ is Δ_0, we have by Σ_1-completeness of S that

$$\mathbb{N} \models \forall y P_S(\overline{\varphi(\dot{y})})$$

$\square$

Claim 2.
$$S \nvdash \forall y P_S(\overline{\varphi(\dot{y})}) \tag{8}$$

Proof. For the sake of contradiction, suppose that

$$S \vdash \forall y P_S(\overline{\varphi(\dot{y})}) \tag{9}$$

Hence
$$S \vdash^{O(\log(n))} P_S(\overline{\varphi(\overline{n})})$$

because the term $\overline{n}$ has the size $O(\log(n))$. Thus, by the condition D1, for sufficiently large n
$$S \vdash Pr(\overline{n}, \overline{P_S(\overline{\varphi(\overline{n})})}) \tag{10}$$

From 1 and 10, we obtain that for sufficiently large n

$$S \vdash \neg\varphi(\overline{n}) \tag{11}$$

But from 9 and Σ_1-soundness of the theory S, we also have

$$S \vdash \varphi(\overline{n}) \tag{12}$$

Thus, 11 and 12 are in contradiction with the consistency of S.

□

By Σ_1-soundness of the theory S, we can obtain

$$\mathbb{N} \models \forall x Con_{S+Con_S}(x)$$

From this and Σ_1-completeness of S,

$$\mathbb{N} \models \forall x P_S(\overline{Con_{S+Con_S}(\dot{x})})$$

We have by 1 that
$$S \vdash \neg\varphi(x) \equiv Pr_S(x, \overline{P_S(\overline{\varphi(\dot{x})})}) \tag{13}$$

We also have by the second finite derivability condition *D*2 that there exists a polynomial function p such that

$$S \vdash Pr_S(x, \overline{P_S(\overline{\varphi(\dot{x})})}) \to Pr(\overline{p(\dot{x})}, \overline{Pr_S(x, \overline{P_S(\overline{\varphi(\dot{x})})})}) \tag{14}$$

Thus, from 13 and 14 we obtain

$$S \vdash \neg\varphi(x) \to Pr(\overline{p(\dot{x})}, \overline{Pr_S(x, \overline{P_S(\overline{\varphi(\dot{x})})})}) \tag{15}$$

But by 13, $Pr_S(x, \overline{P_S(\overline{\varphi(\dot{x})})})$ in 15 is equivalent to $\neg\varphi(x)$ over S. It follows from 15 that there exists a polynomial function p_1 such that

$$S \vdash \neg\varphi(x) \to Pr_S(\overline{p_1(\dot{x})}, \overline{\neg\varphi(\dot{x})})$$

By the finite derivability condition D2, there exists a polynomial function p_2 such that

$$S \vdash \neg\varphi(x) \to Pr_S(\overline{p_2(\dot{x})}, \overline{P_S(\overline{\neg\varphi(\dot{x})})}) \tag{16}$$

We have also by 1

$$S \vdash \neg\varphi(x) \to Pr_S(x, \overline{P_S(\overline{\varphi(\dot{x})})}) \tag{17}$$

Thus, from 16 and 17, there exists a polynomial function $p_3(n) = O(p_2(n))$ such that

$$S \vdash \neg\varphi(x) \to Pr_S(\overline{p_3(\dot{x})}, \overline{P_S(\overline{0 = S(0)})})$$

That is

$$S \vdash \neg\varphi(x) \to Pr_S(\overline{p_3(\dot{x})}, \overline{\neg Cons_S})$$

or equivalently

$$S \vdash \neg\varphi(x) \to Pr_{S+Cons_S}(\overline{p_3(\dot{x})}, \overline{0 = S(0)})$$

and by contraposition

$$S \vdash \neg Pr_{S+Cons_S}(\overline{p_3(\dot{x})}, \overline{0 = S(0)}) \to \varphi(x) \tag{18}$$

Now, it is sufficient to note that

$$\neg Pr_{S+Cons_S}(\overline{p_3(\dot{x})}, \overline{0 = S(0)}) \equiv_{df} Cons_{S+Cons_S}(\overline{p_3(\dot{x})})$$

Hence, from 18, we obtain immediately that

$$S \vdash Cons_{S+Cons_S}(\overline{p_3(\dot{x})}) \to \varphi(x) \tag{19}$$

By the first and the third standard Löb's derivability condition

$$S \vdash P_S(\overline{Cons_{S+Cons_S}(\overline{p_3(\dot{x})})}) \to P_S(\overline{\varphi(\dot{x})})$$

Finally, the independence of the sentence $\forall y P_S(\overline{Cons_{S+Cons_S}(\dot{y})})$ in the theory S follows from the Claim 2.

$\square$

The proof of the theorem 1 is interesting as it is very similar to the proof of Gödel's second incompleteness theorem from Gödel's first incompleteness theorem. Moreover, the lengths of the proofs of $\varphi(\overline{n})$ and $Cons_{S+Cons_S}(\overline{n})$ in the theory S are polynomially related by the following proposition.

Proposition 1. *Let $S \in \mathcal{T}$ be a theory and let $\varphi(x)$ be as above. Then there exist polynomial functions q_1 and $q_2(n) = O(n)$ such that the following holds*

$$S \vdash \forall x(Cons_{S+Cons_S}(\overline{q_1(\dot{x})}) \to \varphi(x)) \tag{1}$$

$$S \vdash \forall x(\varphi(\overline{q_2(\dot{x})}) \to Cons_{S+Cons_S}(x)) \tag{2}$$

Proof. 1 follows directly from Theorem 1, 19.

Furthermore, there exists a suitable polynomial function $p_1(n) = O(n)$ such that we have the following

$$S \vdash \varphi(\overline{p_1(\dot{x})}) \to \neg Pr_S(\overline{p_1(\dot{x})}, \overline{P_S(\overline{\varphi(\overline{p_1(\dot{x})})})}) \tag{3}$$

because 3 holds according to the definition of $\varphi(\overline{n})$. Moreover, we can suppose that p_1 is such that

$$S \vdash \neg Pr_S(\overline{p_1(\dot{x})}, \overline{P_S(\overline{\varphi(\overline{p_1(\dot{x})})})}) \to \neg Pr_S(x, \overline{\neg P_S(\overline{\varphi(\overline{p_1(\dot{x})})}) \to 0 = S(0)}) \tag{4}$$

From 3 and 4, we obtain

$$S \vdash \varphi(\overline{p_1(\dot{x})}) \to \neg Pr_{S+\neg P_S(\overline{\varphi(\overline{p_1(\dot{x})})})}(x, \overline{0 = S(0)}) \tag{5}$$

As

$$S \vdash \forall x(\neg P_S(\overline{\varphi(\overline{p_1(\dot{x})})}) \equiv Con_{S+\neg\varphi(\overline{p_1(\dot{x})})})$$

it follows from 5, that

$$S \vdash \varphi(\overline{p_1(\dot{x})}) \to \neg Pr_{S+Con_S}(x, \overline{0 = S(0)})$$

and thus

$$S \vdash \forall x(\varphi(\overline{p_1(\dot{x})}) \to Con_{S+Con_S}(x))$$

This proves 2.

□

It is interesting to ask what causes the independence of the sentence from Theorem 1. The sentence

$$\forall x P_S(\overline{Con_{S+Con_S}(\dot{x})})$$

is Π_2 sentence

$$\forall x \exists y Proof_S(y, \overline{Con_{S+Con_S}(\dot{x})}) \tag{1}$$

and Π_2 sentence can be interpreted as a total function defined on N. Thus, there may be a possible analogy with fast growing functions. The unprovability of 1 can be caused by the lengths of proofs of the formula $Con_{S+Con_S}(x)$. The function in 1 may be growing exponentially (see conjecture $\mathrm{CON}^{\mathrm{N+}}$ in [7], p. 12). This may be the reason why this formula is unprovable in a bounded arithmetic because bounded arithmetic does not prove that exponential function is total.

3. A finite version of Gödel's first incompleteness theorem and related conjectures

3.1 Finite versions of Gödel's theorems

We can now state a possible finite version of Gödel's first incompleteness theorem.

Conjecture 1 (Finite version of Gödel's first incompleteness theorem, F1GT)**.** *Let $S \in \mathcal{T}$ and let $\varphi(x)$ be a formula such that*

$$S \vdash \varphi(x) \equiv \neg Pr_S(x, \overline{P_S(\overline{\varphi(\dot{x})})})$$

Then the length of S-proofs of the sentence $\varphi(\overline{n})$ is not bounded by any polynomial function in n.

A possible finite version of Gödel's second incompleteness theorem, the conjecture $\mathrm{CON}^{\mathrm{N}+}$, was formulated in [7], p. 12 (see also [4], chapt. 6., for a readable survey). It is the following conjecture

Conjecture 2 (Finite version of Gödel's second incompleteness theorem, $\mathrm{CON}^{\mathrm{N}+}$)**.** *Let $S, T \in \mathcal{T}$ be theories such that T proves Con_S. Then the length of S-proofs of $Con_T(\overline{n})$ is not bounded by any polynomial function in n.*

Because we want to prove equivalence between conjectures, we mention the following slightly different conjecture that was first introduced in [5], p. 193.

Conjecture 3 (CON)**.** *Let S, $T \in \mathcal{T}$ be theories such that*

$$S + Con_S = T \tag{1}$$

Then the length of S-proofs of $Con_T(\overline{n})$ cannot be bounded by any polynomial function in n.

Clearly the conjecture $\mathrm{CON}^{\mathrm{N}+}$ implies the conjecture CON. We don't know if they are equivalent. Both conjectures go beyond well known open problems in computational complexity. In fact, it was shown in [1] that one can prove the following one.

Fact 2 (Krajíček, Pudlák, 1989)**.** *Suppose the conjecture CON. Then NEXP $\neq$ coNEXP.*

An easy consequence of the proposition 1 is that the conjecture F1GT is equivalent to the conjecture CON similarly as Gödel's first incompleteness theorem is equivalent to the second.

Lemma 1. *The conjecture F1GT is equivalent to the conjecture CON*

Proof. Let $\varphi(\overline{n})$ be a formula from the conjecture F1GT. Suppose that the length of S-proofs of the formula $\varphi(\overline{n})$ is not bounded by any polynomial function in n. Thus, suppose the conjecture $F1GT$. It follows from the proposition 1 that there exists a function $p_1(n) = O(n)$ such that

$$S \vdash^{O(\log(p_1(n)))} Con_{S+Con_S}(\overline{p_1(n)}) \rightarrow \varphi(\overline{n})$$

Thus, the length of S-proofs of $Con_{S+Con_S}(\overline{n})$ is not bounded by any polynomial function in n and we obtain CON.

Suppose now CON. From proposition 1, we have again that there exists a polynomial function p_2 such that

$$S \vdash^{O(\log(p_2(n)))} \varphi(\overline{p_2(n)}) \rightarrow Con_{S+Con_S}(\overline{n})$$

From this, we already have F1GT.

□

3.2 Possible conjectures that already imply the finite versions of Gödel's theorems

As there is an analogy with Gödel's theorems, we can ask how a proof of the conjecture F1GT can look like. If a proof of the first finite version of Gödel's theorem follows again from easy diagonal argument, it suggests interesting conjectures. We are not sure if they have an affirmative answers, at least we present some supporting arguments why these conjecture may be true.

Conjecture 4 (Speed-Up, SU)**.** *Let $S \in \mathcal{T}$ be a Σ_1-sound theory and let $\psi(x)$ be a formula (with one free variable x) such that $\mathbb{N} \models \forall x \psi(x)$ and $S \vdash \forall x(\psi(x) \equiv \neg Pr_S(x, \overline{\varphi(\dot{x})}))$ for some formula $\varphi(x)$. Moreover, assume that for every n, $\psi(\overline{n})$ is provable in S by a proof whose length is bounded by some polynomial function p in n, i.e. suppose that for all $n \in N$*

$$S \vdash^{p(n)} \psi(\overline{n})$$

then

$$S \vdash^{o(n)} P_S(\overline{\psi(\overline{n})})$$

The conjecture SU already implies the conjecture F1GT. The proof is similar to the proof of Gödel's first incompleteness theorem. Take the formula φ from the Theorem 1. That is, the formula $\varphi(y)$ such that

$$S \vdash \forall y(\varphi(y) \equiv \neg Pr_S(y, \overline{P_S(\overline{\varphi(\dot{y})})}))$$

We have proved in Theorem 1 that $\mathbb{N} \models \forall y \varphi(y)$. We show first that

$$S \nvdash^{o(n)} P_S(\overline{\varphi(\overline{n})}) \tag{1}$$

Suppose for the sake of contradiction that

$$S \vdash^{o(n)} P_S(\overline{\varphi(\overline{n})}) \tag{2}$$

From 2 and the first derivability condition D1, for sufficiently large n

$$S \vdash Pr_S(\overline{n}, \overline{P_S(\overline{\varphi(\overline{n})})})$$

From the definition of $\varphi(\overline{n})$, it follows that

$$S \vdash \neg\varphi(\overline{n})$$

As S is Σ_1-sound theory and $\mathbb{N} \models \varphi(\overline{n})$ by Theorem 1, this is a contradiction.

Thus, we obtain from our assumption SU and from 1

$$S \nvdash^{p(n)} \varphi(\overline{n})$$

for every polynomial function p.

The reasons why it is interesting to consider the conjecture SU are the following

- There can be a similar situation as in the case of Gödel's theorems. In the case of Gödel's first incompleteness theorem a positive result, more specifically, that a sufficiently strong theory is able to formalizes certain things, is converted with the help of diagonalization to a negative result. Here may be a similar situation, where the positive statement is the conjecture SU.

- The fact that SU is a positive statement is very interesting. It is usually much more difficult to prove that something does not exist than that something exists. Thus, with the help of diagonalization, a proof that something is possible is converted to the proof that something is not possible.

- The conjecture SU already holds for the finite consistency of the theory S, $Con_S(\overline{n})$. An intuition (rather vague) is that $Con_S(\overline{n})$ is in some way the hardest possible polynomially provable formula and for this reason it may happen that it holds for every formula $\psi(\overline{n})$ that is provable by a proof of polynomial length and that is equivalent over S to $\neg Pr_S(\overline{n}, \overline{\varphi(\overline{n})})$ for some formula φ. .

We can also state a stronger conjecture that implies the conjecture SU.

Conjecture 5 (Polynomial completeness, PC)**.** *Let $S \in \mathcal{T}$ be a theory. Let $\psi(x)$ be a formula (with one free variable x) such that $S \vdash \forall x(\psi(x) \equiv \neg Pr_S(x, \overline{\varphi(\dot{x})}))$ for some formula $\varphi(x)$. Moreover, assume that $\psi(\overline{n})$ is for every $n \in N$ provable in S by a proof that is bounded by some polynomial function in n. Then*

$$S \vdash \exists q \forall x P_S(q(x), \overline{\psi(\dot{x})})$$

The reasons why we consider the conjecture PC are the following

- As in the third point in the preceding conjecture, a sufficiently strong theory S already proves $\exists q \forall x P_S(q(x), \overline{Con_S(\dot{x})})$, see [5], cf. [6], Theorem 6.3.2., p. 582.

- There may be again a possible link to Gödel's theorems. The first incompleteness theorem is proved with the help of positive result:

If

$$S \vdash \varphi$$

then

$$S \vdash P_S(\overline{\varphi})$$

Here we may be in a similar situation, this time for the concept od polynomial provability, i.e.

If for every $n \in N$

$$S \vdash^{p(n)} \psi(\overline{n})$$

then

$$S \vdash \exists q \forall x P_S(q(x), \overline{\psi(\dot{x})})$$

4. A finite version of Rosser's theorem

4.1 Feasible finite independence

In this section, we would like to find a formula $\varphi(n)$ such that the both formulas $\neg Pr_T(\overline{n}, \overline{\varphi(\overline{n})})$ and $\neg Pr_T(\overline{n}, \overline{\neg\varphi(\overline{n})})$ have in $T \in \mathcal{T}$ proofs of the polynomial length in n. The situation here is very similar to Rosser's theorem but we consider its finite or polynomial version.

Let $\psi(x)$ be Rosser's formula without the universal quantifier, that is, define $\psi(x)$ in the following way:

$$T \vdash \psi(x) \equiv (Pr_T(x, \overline{\psi(\dot{x})}) \to \exists v \leq x Pr_T(v, \overline{\neg\psi(\dot{x})}))$$

Theorem 2. *Let $T \in \mathcal{T}$ be a theory and $\psi(x)$ be as above. Then there exists a polynomial function p such that for all $n \in N$*

$$T \vdash^{p(n)} \neg Pr_T(\overline{n}, \overline{\varphi(\overline{n})}) \tag{1}$$

and

$$T \vdash^{p(n)} \neg Pr_T(\overline{n}, \overline{\neg\varphi(\overline{n})}) \tag{2}$$

Proof. We first prove two claims.

Claim 3. *There exists a polynomial function p such that*

$$T \vdash Con_T(\overline{p(\dot{x})}) \to \neg Pr_T(x, \overline{\psi(\dot{x})})$$

Proof. First note that there exists a constant $k \in N$ such that

$$T \vdash Con_T(\overline{k} * x) \,\&\, Pr_T(x, \overline{\psi(\dot{x})}) \to Pr_T(x, \overline{\psi(\dot{x})}) \,\&\, \forall v \leq x \neg Pr_T(v, \overline{\neg\psi(\dot{x})}) \tag{3}$$

and moreover

$$T \vdash Con_T(\overline{k} * x) \,\&\, Pr_T(x, \overline{\neg\psi(\dot{x})}) \to Pr_T(x, \overline{\neg\psi(\dot{x})}) \,\&\, \forall v \leq n \neg Pr_T(v, \overline{\psi(\dot{x})}) \tag{4}$$

The subformula

$$Pr_T(x, \overline{\psi(\dot{x})}) \,\&\, \forall v \leq n \neg Pr_T(v, \overline{\neg\psi(\dot{x})})$$

in 3 is equivalent to $\neg\psi(x)$ over T. Thus, we have

$$T \vdash Con_T(\overline{k} * x) \,\&\, Pr_T(x, \overline{\psi(\dot{x})}) \to \neg\psi(x) \tag{5}$$

By Theorem 5.4 in [5], there exists a polynomial function $q(n)$ such that for all $n \in N$

$$T \vdash^{q(n)} Con_T(\overline{n})$$

Hence, we obtain from 5 that there exists a polynomial function q_1 such that for all $n \in N$

$$T \vdash^{q_1(n)} Pr_T(\overline{n}, \overline{\psi(\overline{n})}) \to \neg\psi(\overline{n})$$

As the above proof can be formalized in the theory T, we have

$$T \vdash \forall x(Pr_T(\overline{q_1(\dot{x})}, \overline{Pr_T(\dot{x}, \overline{\psi(\dot{x})}) \to \neg\psi(\dot{x})})) \tag{6}$$

Moreover, by Lemma 6.3.1 in [6], for all $n \in N$

$$T \vdash^{q_2(n)} Pr_T(\overline{n}, \overline{\psi(\overline{n})}) \to \psi(\overline{n})$$

for some polynomial function q_2. And again, this fact is provable in T. Thus we obtain

$$T \vdash Pr_T(\overline{q_2(\dot{x})}, \overline{Pr_T(\dot{x}, \overline{\psi(\dot{x})}) \to \psi(\dot{x})}) \tag{7}$$

6 together with 7 implies that there exists a polynomial function p such that for every n

$$T \vdash Con_T(\overline{p(\dot{x})}) \to \neg Pr_T(x, \overline{\psi(\dot{x})})$$

This proves 1

□

Claim 4. *There exists a polynomial function $p(n)$ such that*

$$T \vdash Con_T(\overline{p(\dot{x})}) \to \neg Pr_T(x, \overline{\neg\psi(\dot{x})})$$

Proof. Put

$$\sigma(x) \equiv_{df} Pr_T(x, \overline{\neg\psi(\dot{x})}) \;\&\; \forall v \leq n \neg Pr_T(v, \overline{\psi(x)})$$

We can then write 4 as

$$T \vdash Con_T(\overline{k} * x) \;\&\; Pr_T(x, \overline{\neg\psi(\dot{x})}) \to \sigma(x) \tag{8}$$

Now, it is sufficient to note that

$$T \vdash \sigma(x) \to \psi(x)$$

to obtain from 8

$$T \vdash Con_T(\overline{k} * x) \;\&\; Pr_T(x, \overline{\neg\psi(\dot{x})}) \to \psi(x)$$

Again, by the polynomial upper bound on the length of proofs of the finite consistency $Con_T(\overline{n})$ in T there exists a polynomial function $q(n)$ such that for every $n \in N$

$$T \vdash^{q(n)} Pr_T(\overline{n}, \overline{\neg\psi(\overline{n})}) \to \psi(\overline{n})$$

As in the previous case, by the formalization of the above fact in T, we obtain for some polynomial function q_1

$$T \vdash Pr_T(\overline{q_1(\dot{x})}, \overline{Pr_T(\dot{x}, \overline{\neg\psi(\dot{x})}) \to \psi(\dot{x})}) \tag{9}$$

and by the formalization of the fact that there exists a polynomial function q_2 such that for every $n \in N$, $T \vdash^{q_2(n)} Pr_T(\overline{n}, \overline{\neg\psi(\overline{n})}) \to \neg\psi(\overline{n})$

$$T \vdash Pr_T(\overline{q_2(\dot{x})}, \overline{Pr_T(\dot{x}, \overline{\neg\psi(\dot{x})}) \to \neg\psi(\dot{x})}) \tag{10}$$

Thus, as in the previous Claim, from 9 and 10 it follows that there exists a polynomial function p such that

$$T \vdash Con_T(\overline{p(\dot{x})}) \to \neg Pr_T(x, \overline{\neg\psi(\dot{x})})$$

□

To prove the Theorem 2 note, that both $\neg Pr_T(\overline{n}, \overline{\psi(\overline{n})})$ and $\neg Pr_T(\overline{n}, \overline{\neg\psi(\overline{n})})$ have in T proofs of polynomial length in n as it follows directly from the polynomial upper bound on the proofs of finite consistency $Con_T(\overline{n})$ in the theory T and from the above Claims.

□

5. Löb's theorem and its finite version

5.1 The finite Löb's theorem

After Kurt Gödel proved his famous theorems, L. Henkin asked an interesting question of what is equivalent in a sufficiently strong theory T a sentence ψ such that

$$T \vdash \psi \equiv P_T(\overline{\psi})$$

The answer was found by M. Löb in the paper [2]. If ψ is a sentence such that

$$T \vdash P_T(\overline{\psi}) \to \psi$$

then already

$$T \vdash \psi$$

In a similar way we can ask whether on the basis of finite version of Gödel's first incompleteness theorem, the conjecture F1GT, what implies

$$T \vdash^{p(n)} Pr_T(\overline{n}, \overline{P_T(\overline{\psi(\overline{n})})}) \to \psi(\overline{n}) \tag{1}$$

for some formula $\psi(x)$ and a polynomial function p.

Here, the concept of provability is replaced by the concept of polynomial provability or, philosophically speaking, "feasible provability". In this case a possible solution may be similar to Löb's theorem, i.e. it is possible that 1 implies that there exists a polynomial function q such that for all sufficiently large n

$$T \vdash^{q(n)} \psi(\overline{n})$$

Thus, for all sufficiently large n, $\psi(\overline{n})$ is provable and, moreover, there exists a polynomial function q such that the lengths of proofs are bounded by the function q in n The formula from 1 contains two predicates of provability not only because of the conjecture F1GT, but also because if we consider only one predicate of provability, the condition is either too weak of too strong.

Firstly, we state the condition only for the predicate $P_T(x)$.

Proposition 2. *If there exists a polynomial function p such that for all $n \in N$*

$$T \vdash^{p(n)} P_T(\overline{\psi(\overline{n})}) \to \psi(\overline{n})$$

then there exists a polynomial function q such that for all $n \in N$

$$T \vdash^{q(n)} \psi(\overline{n})$$

But the proposition 2 is already provable in a sufficiently strong theory. In fact, we can prove the following

Lemma 2. *Let ψ be an arbitrary formula and $T \in \mathcal{T}$. Then there exists a polynomial function p such that if*

$$T \vdash^m P_T(\overline{\psi}) \rightarrow \psi \tag{1}$$

then

$$T \vdash^{p(m)} \psi \tag{2}$$

Proof. The proof is very similar to the proof of Löb's theorem (cf. [2]). By Diagonal lemma, we can construct a formula φ such that

$$T \vdash^{k(|\varphi|+|\psi|)} \varphi \equiv P_T(\overline{\varphi}) \rightarrow \psi \tag{1}$$

for some constant $k \in N$. First, we show that for every polynomial function q_1 there exists a polynomial function q_2 such that for every $m \in N$

$$T \vdash^{q_1(m)} \varphi \Rightarrow T \vdash^{q_2(m)} \psi \tag{2}$$

To prove 2, suppose that there exists a polynomial function q_1 such that

$$T \vdash^{q_1(m)} \varphi$$

Then by the first finite derivability condition D1

$$T \vdash^{q_3(m)} P_T(\overline{\varphi}) \tag{3}$$

for some polynomial function q_3. 2 then follows from 1 and 3 and the fact that $(|\varphi|+|\psi|) \leq k_0 m$ for some constant k_0.

By the first and third classical Löb's derivability conditions we obtain also

$$T \vdash^{k_1(|\psi|+|\varphi|)} P_T(\overline{\varphi}) \rightarrow P_T(\overline{\psi}) \tag{4}$$

for some constant $k_1 \in N$. From the assumption of the proposition that

$$T \vdash^m P_T(\overline{\psi}) \rightarrow \psi$$

and from 4, we obtain for some constant $k_2 \in N$

$$T \vdash^{m+k_2(|\varphi|+|\psi|)} P_T(\overline{\varphi}) \rightarrow \psi$$

As $|\varphi| + |\psi| \leq k_0 m$, it follows from 1 that

$$T \vdash^{k_3 m} \varphi$$

for some constant k_3. Hence by 2, there exists a polynomial function p such that

$$T \vdash^{p(m)} \psi$$

□

But it is clear that the proposition 2 does not imply the conjecture CON. If there exists an analogy between classical results of provability, then the finite version of Löb's theorem should imply the conjecture CON in the similar way as Löb's theorem implies Gödel's second incompleteness theorem.

If we state the condition with predicate $Pr_T(y, x)$, that is in the following way:

If there exists a polynomial function p such that for all $n \in N$

$$T \vdash^{p(n)} Pr_T(\overline{n}, \overline{\psi(\overline{n})}) \rightarrow \psi(\overline{n}) \tag{1}$$

then for all sufficiently large n

$$T \vdash^{q(n)} \psi(\overline{n})$$

The condition 1 is then too strong as it already holds for the formula $\psi(x) \equiv_{df} x = x + \overline{1}$. This is because

$$T \vdash^{p(n)} Pr_T(\overline{n}, \overline{\overline{n} = \overline{n+1}}) \rightarrow \overline{n} = \overline{n+1} \tag{1}$$

is equivalent to

$$T \vdash^{p(n)} Con_T(\overline{n}) \tag{2}$$

But (2) is a true fact. The theory T proves $Con_T(\overline{n})$ by proofs of polynomial length as was proved in [5]. Thus, by condition 1, we would have

$$T \vdash^{q(n)} \overline{n} = \overline{n+1}$$

Another argument for the validity of the following conjecture is then Theorem 3 that we will prove in the end of this section on the page 23.

We are now ready to state the conjecture FL.

Conjecture 6 (Finite version of Löb's theorem, FL)**.** *Let $T \in \mathcal{T}$ be a theory and $\psi(x)$ a formula. If there exists polynomial function p such that for every n*

$$T \vdash^{p(n)} Pr_T(\overline{n}, \overline{P_T(\overline{\psi(\overline{n})})}) \rightarrow \psi(\overline{n})$$

then there exists a polynomial function q such that for all sufficiently large n

$$T \vdash^{q(n)} \psi(\overline{n})$$

We will also state the stronger uniform version of FL, the conjecture UFL.

Conjecture 7 (Uniform version of finite Löb theorem, UFL)**.** *Let $T \in \mathcal{T}$ be a theory and $\psi(x)$ a formula. Then for every polynomial function p there exists a polynomial function q such that*

$$\mathbb{N} \models \exists y \forall x \geq y (Pr_T(\overline{p(\dot{x})}, \overline{Pr_T(\dot{x}, \overline{P_T(\overline{\psi(\dot{x})})}) \to \psi(\dot{x})}) \to Pr_T(\overline{q(\dot{x})}, \overline{\psi(\dot{x})}))$$

Clearly UFL implies FL but we don't know if they are equivalent.

5.2 Relationship between FL, UFL, and other conjectures

The conjecture FL implies the conjecture CON and the proof is analogous to the proof that classical Löb's theorem implies Gödel's second incompleteness theorem.

Observation 1. *The conjecture FL implies the conjecture CON*

Proof. Let $S \in \mathcal{T}$. It follows from the consistency of S that for every $n \in N$ and every polynomial function q

$$S \nvdash^{q(n)} \overline{n} = \overline{n+1}$$

The conjecture FL implies that for every polynomial function $p(n)$

$$S \nvdash^{p(n)} Pr_S(\overline{n}, \overline{P_S(\overline{\overline{n} = \overline{n+1}})}) \to \overline{n} = \overline{n+1} \tag{1}$$

1 is equivalent to

$$S \nvdash^{p(n)} Pr_S(\overline{n}, \overline{P_S(\overline{0 = S(0)})}) \to 0 = S(0)$$

This is equivalent to

$$S \nvdash^{p(n)} Pr_S(\overline{n}, \overline{\neg P_S(\overline{0 = S(0)}) \to 0 = S(0)}) \to 0 = S(0)$$

Thus

$$S \nvdash^{p(n)} Pr_{S + \neg P_S(\overline{0 = S(0)})}(\overline{n}, \overline{0 = S(0)}) \to 0 = S(0)$$

or equivalently

$$S \nvdash^{p(n)} \neg Pr_{S + Con_S}(\overline{n}, \overline{0 = S(0)})$$

Finally, this is equivalent to

$$S \nvdash^{p(n)} Con_{S + Con_S}(\overline{n})$$

□

We can also state generalized finite versions of Gödel's theorems in the same way as in the case of classical Gödel's theorems (cf. [8])

Conjecture 8 (The generalized first finite Gödel's theorem, GF1GT)**.** *Let $S \in \mathcal{T}$. Then there exists a Π_1^b formula $\psi(x)$ such that $\mathbb{N} \models \forall x \psi(x)$ and a such that the length of S-proofs of the formula*

$$Pr_S(\overline{n}, \overline{Pr_S(\overline{\psi(\overline{n})})}) \to \psi(\overline{n})$$

is not bounded by any polynomial function in n.

A possible candidate is the formula $\varphi(x)$ from finite version of Gödel's first incompleteness theorem.

Conjecture 9 (The generalized second finite Gödel's theorem, GCON)**.** *Let $\forall x \neg\psi(x)$ be a provable sentence in $S \in \mathcal{T}$. Then the length of S-proofs of*

$$Pr_S(\overline{n}, \overline{P_S(\overline{\psi(\overline{n})})}) \to \psi(\overline{n})$$

cannot be bounded by any polynomial function in n

By Theorem 1, if S is a Σ_1-sound theory, we have that the formula $\forall x \varphi(x)$ is valid in $\mathbb{N}$ and $\varphi(x)$ is Π_1^b formula. As FL implies CON and this conjecture is equivalent to the conjecture F1GT as we have proved above, FL implies that for every polynomial function p

$$S \nvdash^{p(n)} \varphi(\overline{n})$$

And it follows from the conjecture FL that

$$S \nvdash^{p(n)} Pr_S(\overline{n}, \overline{P_S(\overline{\varphi(\overline{n})})}) \to \varphi(\overline{n})$$

Thus, from additional assumption that S is Σ_1-sound theory, the conjecture FL implies the conjecture GF1GT above.

Moreover, the conjecture CON is equivalent to the conjecture GCON. If $S \vdash \forall x \neg\psi(x)$, then

$$S \nvdash^{p(n)} Pr_S(\overline{n}, \overline{P_S(\overline{\psi(\overline{n})})}) \to \psi(\overline{n}) \tag{1}$$

is equivalent to

$$S \nvdash^{p(n)} \neg Pr_S(\overline{n}, \overline{P_S(\overline{\perp})})$$

As

$$S \vdash Con_{S+Con_S}(\overline{n}) \equiv \neg Pr_S(\overline{n}, \overline{P_S(\overline{\perp})})$$

1 is equivalent to

$$S \nvdash^{p(n)} Con_{S+Con_S}(\overline{n})$$

Although we don't have a proof for the conjecture FL, we can prove the following.

Theorem 3. *Let $S \in \mathcal{T}$. If*

$$S \vdash \exists q \forall x Pr_S(\overline{q(\dot{x})}, \overline{Pr_S(x, \overline{P_S(\overline{\varphi(\dot{x})})}) \to \varphi(\dot{x})}) \tag{i}$$

then

$$S \vdash \exists q \exists y \forall x \geq y Pr_S(\overline{q(\dot{x})}, \overline{\varphi(\dot{x})}) \tag{ii}$$

Proof. Let $\varphi(x)$ be a formula and let $q(x)$ be a polynomial function such that

$$S \vdash \exists q \forall x S \vdash \exists q \forall x Pr_S(\overline{q(\dot{x})}, \overline{Pr_S(x, \overline{P_S(\overline{\varphi(\dot{x})})}) \to \varphi(\dot{x})}) \tag{1}$$

That is, S formalizes

$$S \vdash^{q(n)} Pr_S(\overline{n}, \overline{P_S(\overline{\varphi(\overline{n})})}) \to \varphi(\overline{n}) \tag{3}$$

On the basis of Diagonal lemma, take a formula $\psi(x)$ such that for a given polynomial function p that we will specify later in the proof

$$S \vdash \psi(x) \equiv \neg Pr_S(x, \overline{P_{S+\neg\varphi(\overline{p(\dot{x})})}(\overline{\psi(\dot{x})})}) \tag{4}$$

Define now for every $n \in N$

$$T(\overline{n}) = S + \neg\varphi(\overline{p(n)})$$

4 is then equivalent to

$$S \vdash \psi(x) \equiv \neg Pr_S(x, \overline{P_{T(\dot{x})}(\overline{\psi(\dot{x})})})$$

Because of 4, we have for some polynomial function $p_1(n)$ by the second derivability condition *D*2.

$$S \vdash \neg\psi(x) \to Pr_S(\overline{p_1(\dot{x})}, \overline{\neg\psi(\dot{x})}) \tag{5}$$

From 4 and 5, there exists $p_2(n) = O(p_1(n))$ such that

$$S \vdash \neg\psi(x) \to Pr_S(\overline{p_2(\dot{x})}, \overline{P_{T(\dot{x})}(\overline{\psi(\dot{x})}) \,\&\, \neg\psi(\dot{x})}) \tag{6}$$

Moreover, from 5 and its contraposition, we obtain

$$S \vdash \neg P_S(\overline{\neg\psi(\dot{x})}) \to \psi(x) \tag{7}$$

From the fact

$$S \vdash Con_{T(\dot{x})} \,\&\, P_{T(\dot{x})}(\overline{\psi(\dot{x})}) \to \neg P_S(\overline{\neg\psi(\dot{x})})$$

and from 6 and 7, it follows that there exists a function $p_3(n) = O(p_1(n))$ such that

$$S \vdash \neg\psi(x) \to Pr_S(\overline{p_3(\dot{x})}, \overline{Con_{T(\dot{x})} \to \bot}) \tag{7}$$

We can suppose that for all n, $p(n) \geq p_3(n)$, because the function p doesn't depend on the function p_3.

7 then implies

$$S \vdash Con_{S+Con_{T(\dot{x})}}(\overline{p(\dot{x})}) \rightarrow \psi(x) \tag{8}$$

From 3, we obtain

$$S + \neg\varphi(\overline{n}) \vdash^{q(n)} \neg Pr_S(\overline{n}, \overline{P_S(\overline{\varphi(\overline{n})})})$$

Thus

$$S + \neg\varphi(\overline{n}) \vdash^{q(n)} \neg Pr_{S+\neg P_S(\overline{\varphi(\overline{n})})}(\overline{n}, \overline{0 = S(0)})$$

and equivalently

$$S + \neg\varphi(\overline{n}) \vdash^{q(n)} Con_{S+Con_{S+\neg\varphi(\overline{n})}}(\overline{n})$$

Hence

$$T(p(n)) \vdash^{q(p(n))} Con_{S+Con_{T_n}}(\overline{p(n)}) \tag{9}$$

It follows from 8 and 9 that

$$T(p(n)) \vdash^{q(p(n))} \psi(\overline{n}) \tag{10}$$

Moreover, a formalization of 10 is already provable in S. Thus, S proves a formalization of

$$S + \neg\varphi(\overline{p(n)}) \vdash^{q(p(n))} \psi(\overline{n}) \tag{11}$$

Thus

$$S \vdash \forall x Pr_{T(\dot{x})}(\overline{q(p(\dot{x}))}, \overline{\psi(\dot{x})}) \tag{12}$$

By 12 and by the first derivability condition D1, for all sufficiently large n

$$S \vdash^{O(\log(n))} Pr_S(\overline{n}, \overline{P_{T_n}(\overline{\psi(\overline{n})})})$$

Thus, by the definition of ψ stated in 4

$$S \vdash^{O(\log(n))} \neg\psi(\overline{n}) \tag{13}$$

By formalization of 4 in S, we obtain for some constant $k \in N$

$$S \vdash Pr_S(\overline{k * \log(\dot{x})}, \overline{\neg\psi(\dot{x})}) \tag{14}$$

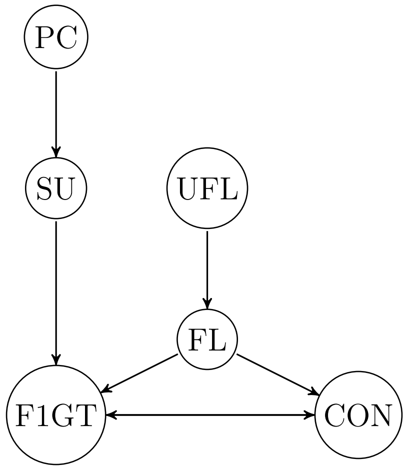
11 and 12 and 14 together implies (ii), that is

$$S \vdash \exists q \exists y \forall x \geq y Pr_S(\overline{q(\dot{x})}, \overline{\varphi(\dot{x})})$$

$\square$

Conclusion

(a)



In this thesis we have stated several conjectures that are related to Gödel's theorems and also to Löb's theorem. We have also proved relationships between these conjectures. Above is a graph of known relationships.

These conjectures indicate that there is a very close relationship between classical provability and polynomial or feasible provability. We present these similarities in the following table.

STANDARD PROVABILITY	FEASIBLE PROVABILITY
Fast growing functions	complexity associated with a proof
Gödel's incompleteness theorems	Finite versions of Incompleteness theorems
Löb's theorem	Finite version of Löb's theorem

We believe that this is not a mere coincidence. From the philosophical standpoint, standard provability and feasible provability are similar concepts. If something is provable, then it is theoretically possible to find that it is true. If something is feasible provable, then its truth is effectively reachable. For this reason we believe that the concept of feasible or polynomial provability is a similarly important concept as is the concept of classical provability.

Furthermore, these similarities indicates that computational complexity theory has a very close relationship to logic and that it is of the same importance for the foundations of mathematics as logic. For this reason it is possible that problems in computational complexity theory will be solved by non-trivial facts in logic.

Bibliography

[1] J. Krajíček and P. Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *J. Symbolic Logic 54(3)*, 1989.

[2] M. H. Löb. Solution of a problem of Leon Henkin. *Journal of Symbolic Logic, 20*, page 115–118., 1955.

[3] P. Pudlák. Gödel and computations. *ACM SIGACT News Vol. 37/4*, pages 13–21, 2006.

[4] P. Pudlák. *Logical Foundations of Mathematics and Computational Complexity: A Gentle Introduction.* Springer Monographs in Mathematics, 2013.

[5] P. Pudlák. On the length of proofs of finitistic consistency statements in first order theories. *Logic Colloquium 84, North Holland P.C.*, 1986.

[6] P. Pudlák. *The lengths of proofs.* In: Handbook of Proof Theory, 1998.

[7] P. Pudlák. Incompleteness in the finite domain. *Bulletin of Symbolic Logic, to appear*, 2017.

[8] C. Smoryński. The incompleteness theorem, in: Handbook of mathematical logic. pages 821–865, 1977.