Notre Dame Journal of Formal Logic
Volume 48, Number 3, 2007

Propositional Proof Systems and Fast Consistency Provers

Joost J. Joosten

Abstract A fast consistency prover is a consistent polytime axiomatized theory that has short proofs of the finite consistency statements of any other polytime axiomatized theory. Krajíček and Pudlák have proved that the existence of an optimal propositional proof system is equivalent to the existence of a fast consistency prover. It is an easy observation that $\mathsf{NP} = \mathsf{coNP}$ implies the existence of a fast consistency prover. The reverse implication is an open question. In this paper we define the notion of an unlikely fast consistency prover and prove that its existence is equivalent to $\mathsf{NP} = \mathsf{coNP}$. Next it is proved that fast consistency provers do not exist if one considers RE axiomatized theories rather than theories with an axiom set that is recognizable in polynomial time.

1 Introduction

There are many interesting relations between computational complexity and arithmetic. In this paper we shall focus on one such relation that involves length of proofs of finite consistency statements. In particular, we shall study *fast consistency provers*. Basically, a fast consistency prover, facop for short, is a certain theory S that has short proofs of the finite consistency statements of any other reasonable theory T. We shall see precise definitions shortly.

Krajíček and Pudlák proved in [5] that if there is no fast consistency prover, then $\mathsf{NP} \neq \mathsf{coNP}$. We shall plead that it is very unlikely that a facop can exist. It is an open question whether the existence of a facop is actually equivalent to $\mathsf{NP} = \mathsf{coNP}$. In Section 4 we shall define the notion of an *unlikely fast consistency prover*, ufacop for short, and show that the existence of a ufacop is equivalent to $\mathsf{NP} = \mathsf{coNP}$.

Before we shall plead that the existence of a facop is unlikely, let us first specify some definitions. In this paper, we shall always mean by the *length* of a proof the number of symbols occurring in it. If S is a theory, we shall denote by $S \vdash_n \varphi$ that

Received September 11, 2006; accepted February 6, 2007; printed August 10, 2007
2000 Mathematics Subject Classification: Primary, 03B70; Secondary, 68Q15
Keywords: computational complexity, bounded arithmetic, length of proofs

φ is provable in S by a proof whose length does not exceed n. We shall denote the formalization/arithmetization of this statement by $\mathsf{Pr}_S(n, \ulcorner\varphi\urcorner)$. For those familiar with formalized provability it is good to stress that there is a logarithm involved here; that is,

$$\mathsf{Pr}_S(x, y) \ := \ \exists\pi \ (|\pi|{\leq}x \ \wedge \ \mathsf{Proof}_S(\pi, y)).$$

Here $\mathsf{Proof}_S(x, y)$ is a natural arithmetization of "x is the Gödel number of a proof in S of a formula with Gödel number y". All theories considered in this paper will be first-order theories of some minimal strength which are sound and hence consistent. With $\mathsf{Con}_T(x)$ we shall denote $\neg\mathsf{Pr}_T(x, \ulcorner 0 = 1\urcorner)$.

If a theory T has a set of axioms which is decidable/recognizable in polynomial time, we shall speak of a *polytime theory*. If φ is provable in S, we shall denote by $||\varphi||_S$ the length of the shortest proof in S of φ. If n is a natural number, we shall denote by $\underline{n}$ its efficient (dyadic) numeral. We are now ready to give the definition of a fast consistency prover.

Definition 1.1 A *fast consistency prover* (facop) is a consistent polytime theory S such that for any other consistent polytime theory T there is a polynomial p such that

$$||\mathsf{Con}_T(\underline{n})||_S \leq p(n).$$

Now, why is it hard to believe in the existence of a facop? First of all, let us remark that a facop is well defined. As, by our assumption, T is consistent, we first remark that $\mathsf{Con}_T(\underline{n})$ is indeed true. But $\mathsf{Con}_T(\underline{n})$ is also provable in S. This is because there are at most 2^n many proofs whose lengths are below n. So in S all this many proofs can be listed and combined with the observation that none of these proofs is a proof of $0 = 1$.

This brings us directly to the question of how a facop could possibly exist. For, if T is completely arbitrary, what else can S do than just give the list of all possible proofs and remark that none is a proof of $0 = 1$? For T weaker than S it seems conceivable that S can do some smart tricks and summarize this long list. But if T is a lot stronger than S, it seems very strange that S would have a short way of proving the finite consistency statements of T.

It is good to realize here that the polytime axiomatizability is not directly saying anything about the proof strength of a theory. For example, a polytime theory may contain an axiom $\mathsf{Con}(\mathsf{ZFC} +$ "there exists a superhuge cardinal") or any other consistent large cardinal assumption.

But it seems hard to relate proof strength to the length of proofs of finite consistency statements. In Section 3 we shall define a hypothetical facop S (in the proof of Theorem 3.1). This S consists of a very weak fragment of arithmetic plus the assumption that some hypothetical propositional proof system only proves tautologies. All these ingredients seem to have little to do with proof strength.

The most tempting way to prove the nonexistence of facops is by using diagonalization, that is, by using fixed points. In Section 6 we set up such an approach for RE-facops. An RE-facop is obtained by replacing "polytime" in Definition 1.1 by "RE". In particular, we show that RE-facops do not exist.

It is good to mention here a result by Pudlák. In [7] and [6] he proved that for a large class of theories T, the values $||\mathsf{Con}_T(\underline{n})||_T$ can be bounded by a polynomial in n.

In addition it is good to mention that questions about the length of proofs of finite consistency statements have an interest in themselves, not related to computational complexity. In particular, they have a close relation to foundations of mathematics and possible partial realizations of Hilbert's program.

2 Preliminaries

In this section we provide the basic definitions that are needed further on in the paper. Probably it is best to skip this section and just turn to it if necessary.

As mentioned in the introduction, in this paper we shall study a relation between arithmetic and computational complexity. By choosing/tailoring the arithmetic language in the right way there are straightforward correspondences.

For this reason we shall in this paper always consider theories in the language of bounded arithmetic (see, e.g., Buss [2]). This language is an extension to the basic language of arithmetic in that it contains symbols for the binary logarithm $|x|$ and for the function $\omega_1(x)$. Here $\omega_1(x) = 2^{|x|^2}$. From now on, all arithmetic formulas in this paper will be in the language of bounded arithmetic.

We shall employ the usual hierarchy of bounded formulas in this paper. Thus, Δ_0^b is the class of formulas (in the language of bounded arithmetic) which contains all open formulas and which is closed under all Boolean connectives and under sharply bounded quantification. Here sharply bounded quantification is quantification of the form $\forall\, x \leq |t|$ or $\exists\, x \leq |t|$, where t is some term in the language of bounded arithmetic that does not contain x as a variable.

Next we define $\Delta_0^b = \Sigma_0^b = \Pi_0^b$. The Σ_{i+1}^b formulas are those obtained by closing off the Π_i^b formulas under bounded existential quantification, Boolean connectives, and sharply bounded universal and existential quantification. The Π_{i+1}^b formulas are defined dually. Bounded quantification is quantification of the form $\forall\, x \leq t$ or $\exists\, x \leq t$. Again, t is some term in the language of bounded arithmetic that does not contain x as a variable.

The language is chosen in such a way that there is a close correspondence between computational complexity classes and definable sets. We say that a formula $\alpha(x)$ defines a set of natural numbers A if $x \in A \quad \Leftrightarrow \quad \mathbb{N} \models \alpha(x)$. It is not too hard to see the following correspondences.

$$\begin{array}{lcl} A \text{ is } \Delta_0^b \text{ definable} & \Rightarrow & A \in \mathsf{P}. \\ A \text{ is } \Sigma_1^b \text{ definable} & \Leftrightarrow & A \in \mathsf{NP}. \\ A \text{ is } \Pi_1^b \text{ definable} & \Leftrightarrow & A \in \mathsf{coNP}. \end{array}$$

This correspondence is pretty straightforward and can be easily continued through all the bounded formula complexity classes by using oracles. Note that for the complexity class P we have no equivalence. In order to get an equivalence some nontrivial mathematics has to be applied. In particular, as a consequence of Buss's Witnessing Theorems we have the following.

$$A \text{ is } \Delta_1^b(S_2^1) \text{ definable} \quad \Leftrightarrow \quad A \in \mathsf{P}.$$

A formula is $\Delta_1^b(S_2^1)$ if it is S_2^1 equivalent to both a Σ_1^b formula and a Π_1^b formula. Here S_2^1 is a pretty weak arithmetic theory with other than the defining axioms of the symbols of the language of arithmetic a weak form of induction for Σ_1^b formulas. We refer the reader to [2] for details. In the rest of this paper, we shall often speak of

$\Delta_1^b(S_2^1)$ theories instead of polytime theories. Moreover, we assume that all theories are consistent and contain S_2^1.

We have seen one correspondence between arithmetic and complexity by the above definability results. Another correspondence goes via propositional proof systems as introduced by Cook and Reckhow [3]. Let us briefly give the basic definitions and facts here.

Definition 2.1 A propositional proof system, a pps for short, is a polytime mapping from the set of all strings onto the set of all tautologies.

Any propositional proof system we know, be it natural deduction, Gentzen, or whatever, can be seen as a pps by mapping a string of syntax which is not a proof in this particular system to the tautology 1 and by mapping a string which is a proof to the tautology it proves. Checking whether a string is a proof or not is for all known proof systems polytime (even cubic time would suffice, as to get parsing of context-free grammars).

An easy correspondence between propositional proof systems and complexity is given by Theorem 2.3 which is due to Cook and Reckhow and relates the existence of so-called super proof systems to $\mathsf{NP} = \mathsf{coNP}$.

Definition 2.2 A pps P is called *super* if there is a polynomial p such that

$$\forall^{\mathsf{Taut}}\tau\ \exists\,|\pi|{<}p(|\tau|)\ P(\pi,\tau).$$

Theorem 2.3 $\mathsf{NP} = \mathsf{coNP}$ *if and only if there exists a super pps.*

It is important to compare different pps's to each other in terms of the *size*, that is, *length* of the proofs, which is nothing but the total number of symbols occurring in it. If π is a proof, we shall denote its length by $|\pi|$. This suggests a logarithmic relation which is good: the length of a string over a finite alphabet is, under efficient coding, linear in the binary logarithm of the code of that string.

Definition 2.4 Let P and Q be pps's and let f be a function. We define

1. $P \geq_{f(x)} Q \ := \ Q(\pi,\tau) \to \exists\pi'\,(|\pi'| \leq f(|\pi|) \wedge P(\pi',\tau))$;
2. $P \geq Q \ :=$ for some polynomial p, $P \geq_{p(x)} Q$; in this case, we say that P *polynomially simulates* Q;
3. $P \equiv Q \ := \ (P \geq Q)\ \&\ (Q \geq P)$.

Throughout this paper we shall assume that our bounding polynomials are monotone increasing which is not an essential assumption, but makes the proofs easier.

In all known propositional proof systems it holds that a tautology is at least as long as any of its proofs. This does not follow from the general definition of a pps. However, the following lemma tells us that we, for many purposes, may assume without loss of generality that indeed a proof of a tautology is at least as long as the tautology itself.

Lemma 2.5 *For every pps P, there is a pps P' such that $P' \equiv P$ and $P'(\pi,\tau) \to |\tau| \leq |\pi|$.*

Proof From P we define P' as

$$P'(\pi',\tau) :\Leftrightarrow [\pi' = (\pi \frown \tau)] \wedge P(\pi,\tau)$$

where $\frown$ denotes concatenation. Clearly, $P \geq_x P'$. If now $P(\pi, \tau)$, we can retrieve τ from π in polytime, so certainly $|\tau| \leq p'(\pi)$ for some polynomial p'. Consequently, $|\pi \frown \tau| \leq p(\pi)$ for some polynomial p and $P' \geq P$. □

We shall often identify a pps and its $\Delta_1^b(S_2^1)$ definition in bounded arithmetic. The following definition is central to the rest of this paper.

Definition 2.6 A pps P is an *optimal propositional proof system*, an opps for short, if $P \geq Q$ for any propositional proof system Q.

It is easy to see that a pps is optimal whenever it is super. Thus via Cook and Reckhow's theorem (Theorem 2.3) we get that

$$\mathsf{NP} = \mathsf{coNP} \Rightarrow \text{there exists an opps.}$$

It is an open question whether the converse implication holds.

3 Fast Consistency Provers and Optimal Propositional Proof Systems

Krajíček and Pudlák proved that the existence of an opps is equivalent to the existence of a facop. In this section we shall give a self-contained version of this proof. The next section will then build on this proof to obtain a similar result.

Theorem 3.1 $\exists$ *facop* $\iff$ $\exists$ *opps.*

Before we can present a proof of this theorem, we should first mention some results involving length of proofs and discuss some coding machinery.

Definition 3.2 A relation R is polynomially numerable in a theory T if for some polynomial p and some formula ρ we have that

$$R(x) \ \Leftrightarrow \ T \vdash \rho(\underline{x}) \ \Leftrightarrow \ T \vdash_{p(|x|)} \rho(\underline{x}).$$

It is good to stress here that $\underline{x}$ denotes the efficient numeral of x so that the length of $\underline{x}$ is logarithmic in x.

Theorem 3.3 *The following are equivalent.*

1. $R \in \mathsf{NP}$*;*
2. *R is polynomially numerable in Robinson's arithmetic* R.

Proof A proof of this theorem can be found in Pudlák [8]. The $\Leftarrow$ is easy and actually holds for any polytime axiomatized theory T. The $\Rightarrow$ direction goes by coding of computations on Turing machines. To get really as low as R here, some additional tricks with definable cuts are needed. □

If $R \in \mathsf{NP}$, it is definable by a Σ (even Σ_1^b) formula ρ and thus, for any (sound, polytime axiomatized) theory T extending Q, we have that

$$\begin{array}{ll} R \text{ is polynomially numerable by } \rho \text{ in } Q & \Leftrightarrow \\ R \text{ is polynomially numerable by } \rho \text{ in } T\ . & \end{array}$$

Having this in mind, we can consider provable Σ_1^b-completeness as expressed in the next theorem as a formalization of the above (Theorem 3.3 plus remark).

Theorem 3.4 *Let T be a $\Delta_1^b(S_2^1)$ theory extending S_2^1. For every Σ_1^b formula $\sigma(x)$, there is a polynomial p such that*

$$S_2^1 \vdash \forall x\ (\sigma(x) \to \mathsf{Pr}_T(p(|x|), \ulcorner\sigma(\dot{x})\urcorner)).$$

Coding of syntax for propositional logic in arithmetic can be done in a standard way. If $\tilde{a}$ is a sequence of zeroes and ones and $\varphi(\vec{p})$ a propositional formula, there is a $\Delta_1^b(S_2^1)$ formula saying that $\varphi(p_i/(\tilde{a})_i)$ evaluates to one. We shall write

$$\tilde{a} \models \varphi.$$

There is a Π_1^b formula $\mathsf{Taut}(\tau)$ saying that $\tau(p_0, \dots, p_n)$ is a tautology. This formula is defined as

$$\mathsf{Taut}(\tau) \ := \ \forall\, |a| \leq (n+1)\ \tilde{a} \models \tau.$$

If Q is a pps, we shall denote by $\mathsf{RFN}(Q)$ the formalized reflection over Q, that is, the following $\forall\Pi_1^b$ formula saying that all provable formulas are true.

$$\mathsf{RFN}(Q) \ := \ \forall\tau\ (\exists\pi\ \ Q(\pi, \tau) \to \mathsf{Taut}(\tau)).$$

In a sense, we can even code arithmetic (and a fortiori syntax) into propositional logic. This is expressed in the following lemma.

Lemma 3.5 *There exists a translation of Π_1^b-formulas $\varphi(x)$ in the language of bounded arithmetic into series of propositional formulas $||\varphi||^m$ such that*

1. *the translation preserves the structure of φ; for example, $||\chi \wedge \psi||^m = ||\chi||^m \wedge ||\psi||^m$, where χ and ψ are subformulas of φ;*
2. *the translation $||\varphi||^m$ contains variables $\vec{q}$ and $p_0, \dots, p_m$; instead of writing in the arithmetically correct way that φ is a tautology when the binary representation $\tilde{a}$ is substituted for the p_i, that is,*

   $$\mathsf{Taut}(||\varphi||^m(\vec{q}, \vec{p}/\tilde{a})),$$

   we shall use the following shorthand notation,

   $$\tilde{a} \models ||\varphi||^m;$$

3. *the translation is provably adequate in the following sense,*

   $$S_2^1 \vdash \forall\, |a| \leq (m+1)\ (\varphi(a) \leftrightarrow \tilde{a} \models ||\varphi||^m);$$

4. *the translation is short in the following sense: for each φ there exists a polynomial p such that*

   $$|(||\varphi||^m)| \leq p(m).$$

Note that $||\varphi||^m$ and $||\varphi||_T$ denote two completely different things. Recall that the $||\varphi||_T$ denotes the length of the shortest proof of φ in T. We are confident that the reader can keep these two notations apart. Now that all coding machinery has been discussed, we are ready to present a proof of Theorem 3.1.

Theorem 3.1 In this proof, we shall denote by $T \vdash_\star \varphi$ the statement that φ is provable in T by a proof whose length is bounded by some polynomial on the (length of) the parameters of φ. Sometimes we shall have to specify the parameters to keep the intended reading clear.

($\Rightarrow$) We repeat the proof from [5] and Krajíček [4] (Theorem 14.1.4). Let S be a facop. We define P and show that P is an opps.

$$\begin{aligned} P(\pi, \tau) \ := \ \ & \mathsf{Proof}_S(\pi, \mathsf{Taut}(\tau)) \ \text{ or} \\ & (\tau = 1 \text{ and } \pi \text{ is not a proof in } S \text{ of } \mathsf{Taut}(\tau') \text{ for any } \tau'). \end{aligned}$$

To see that P is an opps we fix some arbitrary Q and consider some π and τ such that $Q(\pi,\tau)$. By Theorem 3.3 we get that

$$S^1_2 \vdash_\star Q(\pi,\tau). \tag{1}$$

We now define $T_Q := S^1_2 + \mathsf{RFN}(Q)$. Clearly, by (1) and by $\mathsf{RFN}(Q)$, we get $T_Q \vdash_\star \mathsf{Taut}(\tau)$. Here the $\star$ is still dependent on $|\pi|$. Once more, by Theorem 3.3, we get for some polynomial p that

$$S \vdash_\star \mathsf{Pr}_{T_Q}(p(|\pi|), \ulcorner \mathsf{Taut}(\tau)\urcorner). \tag{2}$$

By Theorem 3.4, for some polynomial p' we have that

$$S \vdash \neg\mathsf{Taut}(\tau) \to \mathsf{Pr}_{T_Q}(p'(|\tau|), \ulcorner \neg\mathsf{Taut}(\tau)\urcorner). \tag{3}$$

Combining (2) and (3), we get for some polynomial q that

$$S \vdash_\star \neg\mathsf{Taut}(\tau) \to \mathsf{Pr}_{T_Q}(q(|\pi|), \ulcorner 0 = 1\urcorner),$$

or, equivalently,

$$S \vdash_\star \mathsf{Con}_{T_Q}(q(|\pi|)) \to \mathsf{Taut}(\tau).$$

As S is a facop, we get $S \vdash_\star \mathsf{Con}_{T_Q}(q(|\pi|))$, whence $S \vdash_\star \mathsf{Taut}(\tau)$ and thus, $P \vdash \tau$ by a proof whose length is polynomial in $|\pi|$.

($\Leftarrow$) Let P be an opps. We define

$$S := S^1_2 + \mathsf{RFN}(P)$$

and shall prove that S is a facop. So let T be some $\Delta^b_1(S^1_2)$ theory. We should see that $\mathsf{Con}_T(\underline{x})$ has short proofs in S. For this purpose we define Q as follows.

$$Q := P + \{||\mathsf{Con}_T(|x|)||^m \mid m < \omega\}.$$

Note that, due to the logarithm, $\mathsf{Con}_T(|x|)$ is indeed a Π^b_1 formula. As P is an opps, we get by item 4 of Lemma 3.5 that

$$P \vdash_\star ||\mathsf{Con}_T(|x|)||^m.$$

Here the $\star$ refers to 'polynomial in m'. By Theorem 3.3, we get that

$$S^1_2 \vdash_\star \exists y\ P(y, ||\mathsf{Con}_T(|x|)||^m),$$

and, consequently,

$$S \vdash_\star \mathsf{Taut}(||\mathsf{Con}_T(|x|)||^m).$$

In particular,

$$S \vdash_\star \forall\, |a| \le (m+1)\ \tilde{a} \models ||\mathsf{Con}_T(|x|)||^m.$$

For $a = 2^m$ we get via item 3 from Lemma 3.5 that

$$S \vdash_\star \mathsf{Con}_T(\underline{m}).$$

In other words, for some polynomial p,

$$||\mathsf{Con}_T(\underline{m})||_S \le p(m),$$

and, indeed, S is a facop. □

4 Unlikely Fast Consistency Provers and Unlikely Propositional Proof Systems

In the previous section we have studied facops. As a direct consequence of Theorem 3.1 we get that

$$\mathsf{NP} = \mathsf{coNP} \Rightarrow \text{there exists a facop.}$$

As mentioned before, the converse implication is an open question. In this section we shall define an unlikely fast consistency prover, a ufacop for short, which is a particular sort of facops. We shall then prove that the existence of a ufacop is equivalent to $\mathsf{NP} = \mathsf{coNP}$.

In order to prove this, we shall have to employ a slightly different definition of a pps. However, in light of Lemma 2.5 this alteration is not really essential.

Definition 4.1 A pps P is a polytime mapping from the set of all strings onto the set of all tautologies such that $P(\pi, \tau)$ implies $|\tau| \leq |\pi|$.

To the best of our knowledge, there is no theorem concerning pps's that does not remain valid under this new definition.

Definition 4.2 An *unlikely propositional proof system*—an upps for short—is a pps P such that for some polynomial p we have that

$$\forall^{\mathsf{pps}} Q \; P \geq_{p(x)} Q.$$

Theorem 4.3 $\exists$ upps $\iff$ $\exists$ super pps $\iff$ $\mathsf{coNP} = \mathsf{NP}$.

Proof By a basic Theorem 2.3 we know that $\exists$ super pps $\Leftrightarrow$ $\mathsf{coNP} = \mathsf{NP}$. We relate the existence of an upps to the existence of a super pps by actually proving that P is an upps $\Leftrightarrow$ P is super.

($\Rightarrow$) Let P be an upps with corresponding polynomial p. It follows that P is super. For let τ be some tautology. Then[1]

$$P \geq_{p(x)} P + \tau, \quad \text{whence} \quad P \vdash_{p(|\tau|)} \tau.$$

($\Leftarrow$) Let P be super with corresponding polynomial p. Then P is also an upps. For let Q be an arbitrary pps. If $Q(\pi, \tau)$, then, by our assumption on pps's, we see that $|\tau| \leq |\pi|$. As P is super, we can find π' with $P(\pi', \tau)$ and $|\pi'| \leq p(|\tau|)$. By monotonicity of p, clearly $|\pi'| \leq p(|\pi|)$ and we see that P indeed is a ufacop. □

It is only in this proof (proof of Theorem 4.3) that we need the assumption on an upps P that $P(\pi, \tau)$ implies $|\pi| \leq |\tau|$.

We shall relate uppses to ufacops—*unlikely fast consistency provers*—which are an adaptation of facops. Basically, the idea is that a ufacop is a uniform version of a facop. That is, we swap quantifiers. For a facop S there is, for any polytime theory T, a polynomial p such that $||\mathsf{Con}_T(\underline{n})||_S \leq p(n)$.

If we would simply define a ufacop S to be such that there is a polynomial p such that for any polytime theory T we have $||\mathsf{Con}_T(\underline{n})||_S \leq p(n)$, it would be easy to see that there are no ufacops. This is because the axiomatization of T could be very, very long, so that the length of $\mathsf{Con}_T(\underline{n})$ cannot be bounded. So we define a measure of the complexity of T that will go into the definition of a ufacop.

Definition 4.4 If R is a relation that is decidable in time $\mathcal{O}(|x|^l)$ we shall call l the *decision exponent* of R and write $l = \mathsf{DecExp}(R)$. If T is a theory with a polytime decidable set of axioms, we denote by $\mathsf{DecExp}(T)$ the decision exponent of the set of axioms of T.

Definition 4.5 An *unlikely fast consistency prover*, *ufacop* for short, is a $\Delta^b_1(S^1_2)$ axiomatizable theory S such that there is a polynomial p such that

$$\forall^{\Delta^b_1(S^1_2)} T \ \forall x \ \ ||\mathsf{Con}_T(\underline{x})||_S \leq \ p(x^l).$$

Here $l := \mathsf{DecExp}(T)$.

Before we shall relate uppses to ufacops we first need some additional observations on coding techniques.

Lemma 4.6 *If R is a polytime relation with $\mathsf{DecExp}(R) = l$, then there is a series of propositional formulas ρ_n such that for some polynomial independent of R we have*

1. $a \in R \ \Leftrightarrow \ \tilde{a} \models \rho_n \quad$ *for* $|a| \leq (n+1)$,
2. $|\rho_n| = \mathcal{O}(p(n^l))$.

Proof It is well known that a relation R which is decidable in time $\mathcal{O}(n^l)$ has circuits C_n of size linear in $\mathsf{time} \times \mathsf{space}$. Clearly, the space is bounded by the time, yielding $\mathcal{O}(n^{2l}) = \mathcal{O}((n^l)^2)$. The circuits can be translated in the standard way to propositional formulas which are not much larger than the circuits. All this scaling by coding techniques can be collected in a polynomial p. □

From this lemma it follows that for any $\Delta^b_1(S^1_2)$ relation R, there is an l' such that $\forall n \ |\rho_n| \leq p(n^{l'})$ for the ρ_n and p as in the lemma above. For the sake of readability we shall assume that $l = l'$. Alternatively, one could define $\mathsf{DecExp}(R)$ to be this very l'.

Lemma 4.7 *Let T be a theory with a polytime set of axioms with $\mathsf{DecExp}(T) = l$. There is a translation $\langle| \cdot |\rangle^m$ of specific Π^b_1 formulas into series of propositional formulas such that there is a fixed (independent of T) polynomial q such that*

$$|(\langle|\mathsf{Con}_T(|x|)|\rangle^m)| \leq q(m^l).$$

Proof The formula $\mathsf{Con}_T(|x|)$ says $\forall \, |y| < |x| \ \neg\mathsf{Proof}_T(y, \ulcorner 0 = 1 \urcorner)$. Here,

$$\mathsf{Proof}_T(y, \ulcorner 0 = 1 \urcorner)$$

is as always, saying that y is a sequence (a proof) where some entries are axioms of T. We translate the $\Delta^b_1(S^1_2)$ formula $\mathsf{Axioms}_T(x)$ using Lemma 4.6 and the rest in the structural way as mentioned in Lemma 3.5. □

Note that this translation $\langle| \cdot |\rangle^m$ still has all the structural properties as mentioned in Lemma 3.5. We shall in the sequel refrain from distinguishing $\langle| \cdot |\rangle^m$ and $|| \cdot ||^m$.

Theorem 4.8 *The following are equivalent:*

1. $\exists$ *ufacop,*
2. $\exists$ *upps,*
3. $\exists$ *super pps,*
4. $\mathsf{coNP} = \mathsf{NP}$.

Proof In the light of Theorem 4.3, we only need to concentrate on 1. First we show that 1 $\Rightarrow$ 3 and then we shall show that 2 $\Rightarrow$ 1.

(1 ⇒ 3) Suppose S is a ufacop. We define P_S as follows:

$$\begin{array}{rcl} P_S(\pi,\tau) & := & \mathsf{Proof}_S(\pi,\mathsf{Taut}(\tau)) \text{ or} \\ & & (\tau = 1 \text{ and } \pi \text{ is not a proof in } S \text{ of } \mathsf{Taut}(\tau') \text{ for any } \tau'). \end{array}$$

We shall show that P_S is super. Our proof is a simplification of the proof of the analog of this implication in Theorem 3.1. Moreover, we keep track of the explicit polynomials here. Via Theorem 3.4 we get a polynomial $q(x)$ such that

$$\begin{array}{lr} S \vdash \forall x\ (\neg\mathsf{Taut}(x) \to \mathsf{Pr}_{S^1_2}(q(|x|), \ulcorner\neg\mathsf{Taut}(\dot{x})\urcorner)) & \Leftrightarrow \\ S \vdash \forall x\ (\neg\mathsf{Taut}(x) \to \exists\pi\ (|\pi|<q(|x|) \wedge \mathsf{Proof}_{S^1_2}(\pi, \ulcorner\neg\mathsf{Taut}(\dot{x})\urcorner))) & \Rightarrow \\ S \vdash \forall x\ (\neg\mathsf{Taut}(x) \to \exists\pi\ (|\pi|<q'(|x|) \wedge \mathsf{Proof}_{S^1_2+\mathsf{Taut}(\dot{x})}(\pi, \ulcorner 0 = 1\urcorner))) & \\ \quad \text{for some polynomial } q' \text{ not so different from } q & \Rightarrow \\ S \vdash \forall x\ (\forall\pi\ (|\pi|<q'(|x|) \to \neg\mathsf{Proof}_{S^1_2+\mathsf{Taut}(\dot{x})}(\pi, \ulcorner 0 = 1\urcorner)) \to \mathsf{Taut}(x)) & \Rightarrow \\ S \vdash \forall x\ (\mathsf{Con}_{S^1_2+\mathsf{Taut}(\dot{x})}(q'(|x|)) \to \mathsf{Taut}(x)). & (\dagger) \end{array}$$

Now, as S is a ufacop, there is a polynomial p such that

$$||\mathsf{Con}_{S^1_2+\mathsf{Taut}(\tau)}(q'(|\tau|))||_S \ \leq \ p((q'(|\tau|))^l) \qquad (\dagger\dagger)$$

where $l = \mathsf{DecExp}(S^1_2 + \mathsf{Taut}(\tau))$. Combining (†) and (††) we get that

$$S \vdash_{p'(|\tau|^l)} \mathsf{Taut}(\tau)$$

for some polynomial p'. Note that p' and q' are independent of τ. To conclude our argument we only need to see that $l = \mathsf{DecExp}(S^1_2 + \mathsf{Taut}(\tau))$ is independent of τ.

However, to check whether x is an axiom of $S^1_2 + \mathsf{Taut}(\tau)$, we have to check whether x is an axiom of S^1_2 or whether $x = \mathsf{Taut}(\tau)$. As, by the finite axiomatizability of S^1_2, we may assume that S^1_2 consists of one single axiom, this procedure is linear in $|x|$ (and so are the corresponding circuits). So, indeed, l is independent of τ and P_S is super.

(2 ⇒ 1) So we now prove ∃ upps ⇒ ∃ ufacop. Suppose that P is an upps with corresponding polynomial p. We claim that

$$S := S^1_2 + \mathsf{RFN}(P)$$

is a ufacop. To see this, we consider an arbitrary $\Delta^b_1(S^1_2)$ axiomatized theory T with $l = \mathsf{DecExp}$ and estimate $||\mathsf{Con}_T(\underline{n})||_S$. The theory T will be related to P by defining

$$Q := P + \{||\mathsf{Con}_T(|x|)||^m \mid m < \omega\}.$$

Note that, as we have a logarithm, indeed, $\mathsf{Con}_T(|x|)$ is a Π^b_1 formula and by Lemma 4.7 we get that

$$|(||\mathsf{Con}_T(|x|)||^m)| \leq q(m^l)$$

for some polynomial q independent of T. As P is an upps we get

$$P \vdash_{p(q(m^l))} ||\mathsf{Con}_T(|x|)||^m.$$

By Theorem 3.3, we get some polynomial r, independent of T, such that

$$S \vdash_{r(m^l)} \exists y\ P(y, ||\mathsf{Con}_T(|x|)||^m).$$

As S contains $\mathsf{RFN}(P)$, we can perform the following reasoning inside S. Note that the reasoning is uniform and not dependent on particular properties of T other than l.

$$(\star)$$

$$\begin{array}{lll}
\exists y\ P(y, ||\mathsf{Con}_T(|x|)||^m) & \Rightarrow & \text{by } \mathsf{RFN}(P) \\
\mathsf{Taut}(||\mathsf{Con}_T(|x|)||^m) & \Rightarrow & \text{by definition of } \mathsf{Taut} \\
\forall\, |a| \leq (m+1)\ \ \tilde{a} \models ||\mathsf{Con}_T(|x|)||^m & \Rightarrow & \\
\widetilde{2^m} \models ||\mathsf{Con}_T(|x|)||^m & \Rightarrow & \text{by Lemma 3.5, Item 3} \\
\mathsf{Con}_T(\underline{m}) & &
\end{array}$$

$$(\star\star)$$

As we mentioned, this reasoning is not dependent on T other than via

$$|(||\mathsf{Con}_T(|x|)||^m)| \text{ and } |\mathsf{Con}_T(\underline{m})|.$$

Lemma 4.7 takes care of the first implication. For the second, we shall use an assumption, namely, that $|\mathsf{Con}_T(\underline{m})|$ is not much larger than $t(|m|^l)$ for some polynomial t independent of T. This is not a strange assumption.

When formalizing mathematics, at some stage one should often exclude some pathological codings. In our case, $|\mathsf{Con}_T(\underline{m})|$ is only dependent on $|\mathsf{Axioms}_T(x)|$. By coding the small circuit that decides whether a number is a code of an axiom (see Lemma 4.6) in arithmetic, we get a short way of writing $\mathsf{Axioms}_T(x)$.

If we put no restrictions on the way $\mathsf{Axioms}_T(x)$ is represented, it might very well consist of $10^{10^{99}}$ conjunctions of the short representation. One can even think of worse pathological codings.

Under our assumption, indeed the reasoning between $(\star)$ and $(\star\star)$ can be performed in S in a uniform way; whence for some polynomial p' independent of T we get that

$$S \vdash_{p'(m^l)} \mathsf{Con}_T(\underline{m}).$$

In other words, $||\mathsf{Con}_T(\underline{m})||_S \leq p'(m^l)$ and S is indeed a ufacop. □

Question 4.9 *Under the assumption that* NP $\neq$ coNP, *is there an oracle relativized to which there is a facop which is not a ufacop?*

It is clear that if the answer to this question is positive, then the existence of an opps really is (conditionally) weaker than NP $=$ coNP. In Buhrman et al. [1] an oracle is given under which no pps and a fortiori no facop does exist. In Verbitskiĭ [9] an oracle is given such that optimal proof systems exist, however; still NE $\neq$ coNE, whence coNP $\neq$ NP.

5 Lower Bounds for facops

Of course, having an equivalence of NP=coNP to the existence of a ufacop does not directly help to attack this problem: hard problems are never solved by reformulating them. As expected, problems related to ufacops and facops are likely to be extremely difficult.

For example, it is not even known of specific weak theories such as, for example, S^1_2 or even Robinson's arithmetic Q that they are not a facop. In this section we shall present and reprove some well-known results which are the best lower bound results known when it comes to facops. Friedman and Pudlák independently have shown the following theorem.

Theorem 5.1 *For every polytime axiomatizable theory T extending S^1_2, there is a number* $0 < \epsilon < 1$ *such that*

$$n^{\epsilon} < ||\mathsf{Con}_T(\underline{n})||_T.$$

Proof The proof can also be found in [8]. Our proof is a bit sketchy. More details shall be given in Lemma 6.1 where the proof is milked further.

The proof proceeds by considering a fixed point $\delta(x)$ satisfying the following equivalence.

$$T \vdash \delta(x) \leftrightarrow \neg\mathsf{Pr}_T(x, \ulcorner\delta(\dot{x})\urcorner).$$

Now we reason in T. Suppose $T \vdash_x \delta(\underline{x})$; then, by Theorem 3.4, for some polynomial f we get $T \vdash_{f(x)} \mathsf{Pr}_T(\underline{x}, \ulcorner\delta(\underline{x})\urcorner)$. This yields, combining with properties of the fixed point, that $T \vdash_{g(x)} 0 = 1$, for some function $g(x) = \mathcal{O}(f(x) + x + \log(x)^{\mathcal{O}(1)})$. By contraposition we get that

$$\mathsf{Con}_T(g(x)) \to \neg\mathsf{Pr}_T(x, \ulcorner\delta(\dot{x})\urcorner). \tag{4}$$

Here ends our reasoning inside T. Note that, as δ was externally given, the f and g in this reasoning are actually also externally given.

Now, as T is consistent, we get from (4) that $\neg\mathsf{Pr}_T(x, \ulcorner\delta(\dot{x})\urcorner)$, whence $||\delta(\underline{x})||_T > x$. It is reasonable to assume that $x = \mathcal{O}(f(x))$, whence $g(x) = \mathcal{O}(f(x))$.

Again, using the provable fixed point properties of $\delta(x)$ we obtain from (4) that

$$||\mathsf{Con}_T(g(\underline{x})) \to \delta(\underline{x})||_T = \log(x)^{\mathcal{O}(1)},$$

whence

$$||\mathsf{Con}_T(g(\underline{x}))||_T \geq ||\delta(\underline{x})||_T - \log(x)^{\mathcal{O}(1)} \geq x - \log(x)^{\mathcal{O}(1)}.$$

As $g(x) = \mathcal{O}(f(x))$ we get that (the inverses of polynomials on positive numbers exist from a certain point on) for x large enough

$$\begin{array}{rcl} ||\mathsf{Con}_T(\underline{x})||_T & \geq & ||\mathsf{Con}_T(g^{-1}(g(\underline{x})))||_T \\ & \geq & ||\mathsf{Con}_T(f^{-1}(g(\underline{x})))||_T \\ & \geq & f^{-1}(x - \log(x)^{\mathcal{O}(1)}) \\ & \geq & x^{\epsilon}. \end{array}$$

Here, $\frac{1}{\epsilon}$ is about the size of the degree of f, whence $0 < \epsilon < 1$. □

5.1 Variations Most likely, it is possible to use any variation of the proof of Gödel's second incompleteness theorem to get Theorem 5.1. In particular, one can consider the proof that uses a fixed point of

$$\delta(x) \leftrightarrow \mathsf{Pr}_T(x, \ulcorner\neg\delta(\dot{x})\urcorner).$$

Again, it is easy to see that $T \vdash_x \neg\delta(\underline{x})$ yields a contradiction. An extra application of reflection is needed to show that $T \nvdash_x \delta(\underline{x})$.

It is also possible to run the same argument with the following fixed point.

$$\delta(x) \leftrightarrow \neg\mathsf{Pr}_T(h(x), \ulcorner\delta(\dot{x})\urcorner).$$

Of course, the representation of h should not block the provable completeness for Σ^0_1 (or $\exists\Sigma^b_1$) sentences which is needed in the argument. The function h must thus be Σ^0_1 definable. In other words, h should be a recursive function. With such an h, this fixed point gives rise to true statements with very long proofs. This shall be exploited later on. Therefore, it is worthwhile to restate some easy properties of this fixed point. We shall require that h be some provably unbounded (that is, goes provably to infinity) recursive function. Note that we do not demand that the function h be provably total. Even without the totality being provable, one can find a fixed point and all the reasoning goes through. Thus, for example, $\mathsf{Pr}_S(h(x), \ulcorner\delta(\dot{x})\urcorner)$ can be seen as an abbreviation of $\exists y\ (y = h(x) \wedge \mathsf{Pr}_S(y, \ulcorner\delta(\dot{x})\urcorner))$.

Fact 5.2 Let S be a sound theory and δ such that $S \vdash \delta(x) \leftrightarrow \neg\mathsf{Pr}_S(h(x), \ulcorner\delta(\dot{x})\urcorner)$. Then

1. $||\delta(\underline{n})||_S > h(n)$,
2. $\mathbb{N} \models \forall n\ \delta(n)$,
3. $\forall n\ S \vdash \delta(\underline{n})$,
4. $S \nvdash \forall x\ \delta(x)$.

These facts are pretty easy to verify. At (4) the provable unboundedness of h is used to see that $S \vdash \forall x\ \delta(x) \leftrightarrow \mathsf{Con}(S)$. Now, using these facts, we can give easy proofs of the following two well-known propositions.

Proposition 5.3 *For any recursive function h, there exists a series of provable predicate logical tautologies φ_n of which the length of proofs in predicate logic are not bounded by $h(|\varphi_n|)$.*

Proof Take a strong enough finitely axiomatized arithmetic theory, for example, $\mathrm{I}\Sigma_1$. Consider

$$\mathrm{I}\Sigma_1 \vdash \delta(x) \leftrightarrow \neg\mathsf{Pr}_{\mathrm{I}\Sigma_1}(h(x), \ulcorner\delta(\dot{x})\urcorner).$$

Then $\bigwedge \mathrm{I}\Sigma_1 \to \delta(\underline{n})$ suffices. □

Proposition 5.4 *There is an explicit series of provable predicate logical tautologies ψ_n whose proofs are not bounded by any recursive function.*

Proof By diagonalization from Proposition 5.3. □

6 RE facops Do Not Exist

The existence of a facop or a ufacop is very counterintuitive. However, as is to be expected, every attempt to prove the nonexistence fails. In this section we shall present such an attempt by dropping the requirement that the theories for which a facop should have short proofs be polytime decidable.

So, in this section, we consider sound theories with an RE axiomatization. For this class of theories, we can show that there is no "strongest theory" S having short proofs for finite consistency statements of any other RE theory. The final result is stated in Theorem 6.4. Actually, the result is quite strong. It says that for any theory S, there is a theory T whose proofs in S of its consistency statements have nonrecursive lengths.

The idea of the proof is by generalizing the proof of Theorem 5.1 and Fact 5.2. First we state a lemma that articulates some conditions on S and T under which $||\mathsf{Con}_T(\underline{x})||_S \geq h(x)$. We have chosen S to refer to *slow*. The next two lemmas tell us how to construct, given an S, a theory T such that the conditions hold.

Lemma 6.1 *Let S and T be consistent* RE *theories containing S^1_2. Let $\delta(x)$ be such that*

$$S^1_2 \vdash \forall x\ (\delta(x) \leftrightarrow \neg\mathsf{Pr}_S(h(x), \ulcorner\delta(\dot{x})\urcorner))$$

for a certain recursive h with $h = \Omega(x)$. Furthermore, let S and T be such that T has speed-up over S in the following sense.

(i) $S \vdash_{h(x)} \delta(\underline{x}) \quad \Rightarrow \quad T \vdash_{\mathcal{O}(x)} \mathsf{Pr}_S(h(\underline{x}), \ulcorner\delta(\underline{x})\urcorner)$,
(ii) $S \vdash_{h(x)} \delta(\underline{x}) \quad \Rightarrow \quad T \vdash_{\mathcal{O}(x)} \delta(\underline{x})$.

Moreover, let (i) and (ii) be formalizable in S. Then it holds that

$$||\mathsf{Con}_T(\underline{x})||_S \geq h(\mathcal{O}(x)).$$

Proof Reason in S. Suppose that

$$S \vdash_{h(x)} \delta(\underline{x}). \tag{5}$$

Then, by assumption (i), we get

$$T \vdash_{\mathcal{O}(x)} \mathsf{Pr}_S(h(\underline{x}), \delta(\underline{x})). \tag{6}$$

Combining (5) and (ii), we also get

$$T \vdash_{\mathcal{O}(x)} \delta(\underline{x}).$$

As the fixed point equation is also provable in T, that is,

$$T \vdash_{\mathcal{O}(1)} \forall x \; (\delta(x) \leftrightarrow \neg\mathsf{Pr}_S(h(x), \ulcorner\delta(\dot{x})\urcorner)),$$

we get

$$T \vdash_{\mathcal{O}(x)+\log(x)^{\mathcal{O}(1)}} \neg\mathsf{Pr}_S(h(\underline{x}), \ulcorner\delta(\underline{x})\urcorner).$$

Combining this with (6) we obtain

$$T \vdash_{\mathcal{O}(x)+\log(x)^{\mathcal{O}(1)}} 0 = 1.$$

We now no longer reason in S. Considering the above reasoning, together with the fact that S is sound and T is consistent, we see that

$$||\delta(\underline{x})||_S \geq h(x). \tag{7}$$

Also, from the above reasoning, we have

$$S \vdash \mathsf{Pr}_S(h(x), \delta(x)) \to \neg\mathsf{Con}_T(g(x))$$

for some function $g(x) = \mathcal{O}(x + \log(x)^{\mathcal{O}(1)})$. Consequently, also

$$S \vdash \mathsf{Con}_T(g(x)) \to \delta(x) \quad (\leftrightarrow \neg\mathsf{Pr}_S(h(x), \delta(x))),$$

and we get that

$$||\mathsf{Con}_T(g(\underline{x})) \to \delta(\underline{x})||_S = \log(x)^{\mathcal{O}(1)}.$$

This implies

$$||\mathsf{Con}_T(g(\underline{x}))||_S \geq ||\delta(\underline{x})||_S - \log(x)^{\mathcal{O}(1)}.$$

Because $g(x) = \mathcal{O}(x) = \mathcal{O}(h(x))$, by (7) we obtain the required result; that is,

$$||\mathsf{Con}_T(\underline{x})||_S \geq h(\mathcal{O}(x)). \qquad \square$$

The next lemma provides an approach so that we can concentrate on item (i).

Lemma 6.2 *Let S and T be (sound and* RE*) such that (verifiably in S)*

$$\{\forall\vec{x}\ (\Box_S\varphi(\dot{\vec{x}}) \to \varphi(\vec{x}))\} \subseteq \textit{the axioms of } T$$

and that, moreover, (verifiably in S)

$$S \vdash_{h(x)} \delta(\underline{x}) \Rightarrow T \vdash_{\mathcal{O}(x)} \mathsf{Pr}_S(h(\underline{x}), \delta(\underline{x})), \tag{8}$$

for some fixed formula $\delta(x)$; then it holds (verifiably in S) that

$$S \vdash_{h(x)} \delta(\underline{x}) \Rightarrow T \vdash_{\mathcal{O}(x)} \delta(\underline{x}).$$

Proof (Reason in S.) Suppose that $S \vdash_{h(x)} \delta(\underline{x})$. Because of (8), we get that

$$T \vdash_{\mathcal{O}(x)} \mathsf{Pr}_S(h(\underline{x}), \delta(\underline{x})),$$

hence also

$$T \vdash_{\mathcal{O}(x)} \Box_S\delta(\underline{x}).$$

Adding just one more line to the T-proof consisting of the axiom $\Box_S\delta(\underline{x}) \to \delta(\underline{x})$ gets us the required

$$T \vdash_{\mathcal{O}(x)} \delta(\underline{x}),$$

as the number of symbols in $\Box_S\delta(\underline{x}) \to \delta(\underline{x})$ is just $\mathcal{O}(\log(x))$. □

Note that this proof makes no further assumptions on the nature of $\delta(x)$. For the particular $\delta(x)$ we are interested in, it would suffice to demand that $T \supseteq \{\mathsf{Con(S)}\}$.

Lemma 6.3 *Let S be a given sound and* RE *theory. Let S' be defined so that its axioms are precisely the theorems of S. Next define T so that its axioms are the axioms of S' together with $\{\forall\vec{x}\ (\Box_S\varphi(\dot{\vec{x}}) \to \varphi(\vec{x}))\}$. Then S and T satisfy (i) and (ii) of Lemma 6.1.*

Proof The theory S' is defined from S via a version of Craig's trick in the sense that $\mathsf{Axiom}_{\mathsf{S'}}(\mathsf{x}) \Leftrightarrow \exists \mathsf{y}\ \mathsf{Proof}_{\mathsf{S}}(\mathsf{y}, \mathsf{x})$ whence S and S' are extensionally the same theory. That is, $S = S'$, whence S' and T are also sound RE theories.

Reason in S, and suppose that $S \vdash_{h(x)} \delta(\underline{x})$. Then also $S \vdash \mathsf{Pr}_S(h(\underline{x}), \delta(\underline{x}))$. Notice that the length of $\mathsf{Pr}_S(h(\underline{x}), \delta(\underline{x}))$ is $\mathcal{O}(\log(x))$ so certainly $\mathcal{O}(x)$, whence

$$T \vdash_{\mathcal{O}(x)} \mathsf{Pr}_S(h(\underline{x}), \delta(\underline{x})).$$

Lemma 6.2 now yields the desired result. □

Note that the construction in Lemma 6.3 works simultaneously for all recursive functions. Thus, putting things together, we have now shown the following theorem, as announced at the beginning of this section.

Theorem 6.4 *For any sound* RE *theory S there exists another sound* RE *theory T for which for any recursive function h*

$$||\mathsf{Con}_T(\underline{x})||_S \geq h(\mathcal{O}(x)).$$

Proof For any such theory S, apply the construction as in Lemma 6.3 to obtain a theory T so that Lemma 6.1 yields the required result. □

Question 6.5 *Can Theorem 6.4 also be proved for theories with a primitive recursive set of axioms? Which is the weakest class of theories for which Theorem 6.4 can be proved?*

7 Speculations on Polytime Diagonalizations

Clearly, a theorem such as Theorem 6.4 cannot be proved in full generality for polytime theories. This is due to the observation made before that $||\mathsf{Con}_T(\underline{x})||_S \leq f(x)$ for some f which is exponential in x. Of course, this observation hinges on the fact that it is polytime decidable that an axiom of T is indeed an axiom of T. And thus, by Theorem 3.3, the axiomhood has a short proof in S.

Having this in mind we immediately see why the proof of Theorem 6.4 does not carry over to the setting of polytime theories: If one starts out with a theory S with a $\Delta^b_1(\mathsf{S}^1_2)$ axiomatization, the trick in Lemma 6.3 will yield a genuinely Σ^0_1 axiomatized theory T. One could think of defining the axioms of S consisting of those theorems having a proof in some logarithmically short interval $[a, b]$ which is not too far away from the theorem. However, this is the same problem as we started with: given a provable formula, look for a short proof.

The conditions in Lemma 6.1 are formulated in quite a general way. A more promising way to obtain lower bounds for facops would be to look for other fixed points such that given a theory S, one can define a theory T such that conditions (i) and (ii) of Lemma 6.1 are satisfied for this fixed point.

The following conjecture does not seem fully unfeasible.

Conjecture 7.1 *For every sound $\Delta^b_1(S^1_2)$ theory S and for every $l \in \omega$, there exists a sound $\Delta^b_1(S^1_2)$ theory T such that*

$$||\mathsf{Con}_T(\underline{x})||_S > x^l.$$

It is clear that Conjecture 7.1 is a desirable result as it is just one step away from the required

$$\exists^{\Delta^b_1(S^1_2)} S\, \forall^{\Delta^b_1(S^1_2)} T\, \forall l\ \ ||\mathsf{Con}_T(\underline{x})||_S > x^l.$$

And this last step suggests some compactness or diagonalization argument. However, polytime diagonalization seems to be the hard problem at the core of the $\mathsf{P} \neq \mathsf{NP}$-problem.

We would like to conclude this paper by an easy but interesting observation. Mathematical practice has proved that it is very hard to find strong lower bounds for classical propositional logic. Actually, the state of the art is still stuck at a quadratic lower bound. The following observation might be an explanation for this fact. The observation roughly says that if both optimal proof systems and hard tautologies exist, then these hard tautologies are intrinsically difficult to describe.

Observation 7.2 If optimal proof systems do exist, then any polytime recognizable sequence of tautologies has polynomially bounded proofs. If, moreover, $\mathsf{coNP} \neq \mathsf{NP}$, any hard tautology is not polytime recognizable.

Note

1. There is a subtle technicality here as to the representation of $P + \tau$. It is tempting to define the mapping $P + \tau$ (remember, a proof system is a mapping) to be the identity on τ. By definition P was defined on τ too. The value of $P(\tau)$ should now be given on some other input, etc. We shall not go into the details of this coding here and assume some canonical representation.

References

[1] Buhrman, H., S. Fenner, L. Fortnow, and D. van Melkebeek, "Optimal proof systems and sparse sets," pp. 407–18 in *Proceedings of the 17th Symposium on Theoretical Aspects of Computer Science (STACS'2000)*, vol. 1770 of *Lecture Notes in Computer Science*, Springer, Berlin, 2000. MR 1781750. 391

[2] Buss, S. R., "First-order proof theory of arithmetic," pp. 79–147 in *Handbook of Proof Theory*, edited by S. R. Buss, vol. 137 of *Studies in Logic and the Foundations of Mathematics*, North-Holland, Amsterdam, 1998. MR 1640326. 383

[3] Cook, S. A., and R. A. Reckhow, "The relative efficiency of propositional proof systems," *The Journal of Symbolic Logic*, vol. 44 (1979), pp. 36–50. Zbl 0408.03044. MR 523487. 384

[4] Krajíček, J., *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, vol. 60 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, 1995. Zbl 0835.03025. MR 1366417. 386

[5] Krajíček, J., and P. Pudlák, "Propositional proof systems, the consistency of first order theories and the complexity of computations," *The Journal of Symbolic Logic*, vol. 54 (1989), pp. 1063–79. Zbl 0696.03029. MR 1011192. 381, 386

[6] Pudlák, P., "Improved bounds to the length of proofs of finitistic consistency statements," pp. 309–32 in *Logic and Combinatorics (Arcata CA, 1985)*, edited by S. J. Simpson, vol. 65 of *Contemporary Mathematics*, American Mathematical Society, Providence, 1987. Zbl 0635.03054. MR 891256. 382

[7] Pudlák, P., "On the length of proofs of finitistic consistency statements in first order theories," pp. 165–96 in *Logic Colloquium '84 (Manchester, 1984)*, vol. 120 of *Studies in Logic and the Foundations of Mathematics*, North-Holland, Amsterdam, 1986. Zbl 0619.03037. MR 861424. 382

[8] Pudlák, P., "The lengths of proofs," pp. 547–637 in *Handbook of Proof Theory*, edited by S. R. Buss, vol. 137 of *Studies in Logic and the Foundations of Mathematics*, North-Holland, Amsterdam, 1998. Zbl 0920.03056. MR 1640332. 385, 392

[9] Verbitskiĭ, O. V., "Optimal algorithms for co-NP sets and the problem EXP $\overset{?}{\to}=$ NEXP," *Akademiya Nauk SSSR. Matematicheskie Zametki*, vol. 50 (1991), pp. 37–46, 160. Zbl 0800.68444. MR 1139697. 391

Acknowledgments

This paper is partly written while employed at the Mathematical Institute of the Academy of Sciences of the Czech Republic in Prague. The stay in Prague was also financed by the Netherlands Organization for Scientific Research (NWO). First of all, I would like to thank Pavel Pudlák for help, questions, and improvements. An anonymous referee helped to improve the readability and accuracy of this paper. Next, there are many other people that I would like to mention here: Christian Bennet, Peter van Emde Boas, Harry Buhrman, Rosalie Iemhoff, Emil Jeřábek, Jan Krajíček, Neil Thapen, Leen Torenvliet, Alan Skelley, Vítězslav Švejdar, Oleg Verbitsky, and Albert Visser.

Institute for Logic Language and Computation
University of Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
THE NETHERLANDS
Joost.Joosten@phil.uu.nl