On the Complexity of Gödel's Proof Predicate

Yijia Chen [*] Jörg Flum [†]

March 10, 2009

Abstract

The undecidability of first-order logic implies that there is no computable bound on the length of shortest proofs of valid sentences of first-order logic. Some valid sentences can only have quite long proofs. How hard is it to prove such "hard" valid sentences? The polynomial time tractability of this problem would imply the fixed-parameter tractability of the parameterized problem that, given a natural number n in unary as input and a first-order sentence φ as parameter, asks whether φ has a proof of length $\leq n$. As the underlying classical problem has been considered by Gödel we denote this problem by p-GÖDEL. We show that p-GÖDEL is not fixed-parameter tractable if DTIME$(h^{O(1)}) \neq$ NTIME$(h^{O(1)})$ for all time constructible and increasing functions h. Moreover we analyze the complexity of the construction problem associated with p-GÖDEL.

1. Introduction

We know that the class of valid first-order sentences is not decidable (Church's Undecidability Theorem [4]). In particular, there is no computable function defined on all first-order sentences that assigns to every valid sentence an upper bound for the minimum length of a proof. Moreover, mathematicians' experience seems to indicate that various "interesting" valid sentences φ of first-order logic (like the Four Color Theorem or the Graph Minor Theorem) only have quite long proofs, say, proofs superpolynomial in the length $|\varphi|$ of φ. How hard is it to decide whether such a hard valid sentence has a proof of a length less than a given bound? This problem is in NP; however, (as shown in Lemma 3) it is not NP-hard if the polynomial hierarchy does not collapse. So how do we convince ourselves that it is not decidable in polynomial time?

We approach this question by considering a related parameterized problem. Parameterized complexity is a refinement of classical complexity theory, in which one measures the complexity of an algorithm not only in terms of the total input length m, but one also takes into account other aspects of the input codified as the parameter k. Central to parameterized complexity theory is the notion of fixed-parameter tractability. It relaxes the classical notion of tractability, polynomial time computability, by allowing algorithms whose running time can be exponential but only in terms of the parameter. This is based on the idea to choose the parameter in such a way that it can be assumed to be small (or, at least small compared with the total input size) for the instances one is interested in. To be precise, a problem is said to be *fixed-parameter tractable* if it can be decided by an algorithm whose running time is $f(k) \cdot p(m)$ for an instance of total length m and with parameter k; here f is a computable function and p a polynomial. Parameterized complexity theory not only provides methods for proving problems to be fixed-parameter tractable but also gives a framework for dealing with apparently intractable problems. There is a great variety of classes of intractable parameterized problems. In this paper we will only refer to the class XP of problems decidable by an algorithm whose running time is $O(m^{f(k)})$ (for an instance of total length m and with parameter k), where f is a computable function.

We come back to the problem how hard it is to recognize whether "hard" valid first-order sentences have proofs of a length less than a given bound. It turns out that the polynomial time tractability of this problem would imply the fixed-parameter tractability of the problem p-GÖDEL, that is, of the parameterized problem that asks whether a first-order sentence φ has a proof of length $\leq n$; here φ and n in

[*] Shanghai Jiaotong University, China. Email: yijia.chen@cs.sjtu.edu.cn

[†] Albert-Ludwigs-Universität Freiburg, Germany. Email: joerg.flum@math.uni-freiburg.de

unary form the input and $|\varphi|$ is the parameter. As we are interested in "hard" sentences φ, for the relevant instances the parameter $|\varphi|$ will be small compared with the total input size. In this paper we study the complexity of the parameterized problem p-GÖDEL.

The classical problem underlying p-GÖDEL, namely the problem that, given an arbitrary first-order sentence φ and an arbitrary natural number n in unary, asks whether φ has a proof of length $\leq n$, has been addressed by Gödel in a letter to von Neumann of 1956 (see [8]). Gödel asked whether this problem is solvable in (deterministic) time $O(n^2)$ or even in time $O(n)$. In the meantime we know that it is NP-complete. In the same letter Gödel also asked "how strongly in general the number of steps in finite combinatorial problems can be reduced with respect to simple exhaustive search," that is, in this context he addressed the P-NP-problem.

We show that p-GÖDEL is not fixed-parameter tractable (and hence we cannot recognize hard valid sentences in polynomial time) if P[TC] $\neq$ NP[TC]. Here P[TC] $\neq$ NP[TC] means that for all *time constructible* and increasing functions h the class of problems decidable in *deterministic polynomial time* in h and the class of problems decidable in *nondeterministic polynomial time* in h are distinct, that is, DTIME($h^{O(1)}$) $\neq$ NTIME($h^{O(1)}$). Furthermore a stronger hypothesis where DTIME($h^{O(1)}$) $\neq$ NTIME($h^{O(1)}$) is replaced by NTIME($h^{O(1)}$) $\not\subseteq$ DTIME($h^{O(\log h)}$) implies that p-GÖDEL is not even in the class XP.

In Section 6 we relate these hypotheses to other statements of complexity theory. In particular, we shall see that P[TC] $\neq$ NP[TC] holds if there is a P-bi-immune problem in NP. To the best of our knowledge the statement P[TC] $\neq$ NP[TC] has not been considered in the literature so far, even though it is a quite natural generalization of the hypothesis P $\neq$ NP.

In Section 5 we show that the construction problem associated with p-GÖDEL is not fpt Turing reducible to the decision problem p-GÖDEL (in case p-GÖDEL $\notin$ XP). As Gödel's proof predicate is NP-complete the corresponding (classical) construction problem is polynomial time Turing reducible to its decision problem. However, by the previous result any such reduction, for a first-order sentence φ with a proof of length $\leq n$, in general will ask queries of the form "does ψ have a proof of length $\leq m$" for sentences ψ with $|\psi|$ only bounded by some polynomial in n, *the length of the proof* of φ. The relationship between Gödel's proof predicate and its construction problem has been discussed on an informal level in [2].

Moreover, we show that in case p-GÖDEL is not fixed-parameter tractable there is no way to find for every first-order sentence φ with a proof of length $\leq n$ such a proof efficiently even if we have access to all valid sentences of a length bounded in terms of φ.

2. Preliminaries

In this section we recall the notion of time constructible function and review the basic concepts of parameterized complexity needed in this paper. We refer the reader to [5] and to [7] for thorough introductions to parameterized complexity.

For a natural number k we set $[k] := \{1, \dots, k\}$.

2.1. Time constructible functions. We identify problems with subsets Q of $\{0,1\}^*$. Clearly, as done mostly, we present concrete problems in a verbal, hence uncodified form. All Turing machines have $\{0,1\}$ as alphabet.

A function $f : \mathbb{N} \to \mathbb{N}$ is *time constructible* if there is a deterministic Turing machine that, for all $n \in \mathbb{N}$, halts in exactly $f(n)$ steps on every input of length n. Note that if f is time constructible, then $f(n)$ can be computed in $O(f(n))$ steps. One can easily show that for every computable $f : \mathbb{N} \to \mathbb{N}$ there exists a computable function $g : \mathbb{N} \to \mathbb{N}$ such that:

(1) $f(k) \leq g(k)$ for all $k \in \mathbb{N}$,

(2) g is increasing,

(3) g is time constructible.

We shall make use of the following well-known result.

Proposition 1. *If* P $=$ NP*, then*

$$\mathrm{DTIME}(h^{O(1)}) = \mathrm{NTIME}(h^{O(1)})$$

for every time constructible and increasing function $h : \mathbb{N} \to \mathbb{N}$.

Proof: The proof uses a simple padding argument. In fact, we let $h : \mathbb{N} \to \mathbb{N}$ be time constructible and increasing and assume that $Q \subseteq \{0,1\}^*$ is in NTIME$(h^{O(1)})$. Then

$$Q(h) := \big\{(x, h(|x|)) \mid x \in Q\big\}$$

is in NP, as h is time constructible. Since we assume that P $=$ NP, there is a deterministic algorithm $\mathbb{A}$ deciding $Q(h)$ in polynomial time. Then the algorithm that on input $x \in \{0,1\}^*$ first computes $h(|x|)$ and then decides with $\mathbb{A}$ whether $(x, h(|x|)) \in Q(h)$ (and hence whether $x \in Q$) witnesses that $Q \in$ DTIME$(h^{O(1)})$. □

2.2. Exponentially dense problems. A problem $Q \subseteq \{0,1\}^*$ is *exponentially dense* if for some $\varepsilon > 0$ and infinitely many $n \in \mathbb{N}$ we have

$$\big|\{x \in Q \mid |x| = n\}\big| \geq 2^{n^{\varepsilon}}.$$

We shall need the following result proven in [1].

Theorem 2. *If the problem Q is* NP*-hard, then it is exponentially dense, unless the polynomial hierarchy collapses.*

2.3. Parameterized complexity. We view *parameterized problems* as pairs (Q, κ) consisting of a (classical) problem $Q \subseteq \{0,1\}^*$ and a *parameterization* $\kappa : \{0,1\}^* \to \mathbb{N}$, which is required to be polynomial time computable.

We introduce the parameterized problem p-GÖDEL, thereby exemplifying our way to represent parameterized problems:

p-GÖDEL
Instance: A first-order sentence φ and a natural number n in *unary*.
Parameter: $|\varphi|$.
Question: Does φ have a proof of length $\leq n$?

A parameterized problem (Q, κ) is *fixed-parameter tractable* (or, in FPT) if $x \in Q$ is solvable by an *fpt-algorithm*, that is, by an algorithm running in time $f(\kappa(x)) \cdot |x|^{O(1)}$ for some computable $f : \mathbb{N} \to \mathbb{N}$. The parameterized problem (Q, κ) is in the class XP if $x \in Q$ is solvable in time $O(|x|^{f(\kappa(x))})$ for some computable $f : \mathbb{N} \to \mathbb{N}$.

Besides these classes of (strongly uniform) parameterized complexity theory we need their *uniform* versions FPT$_{\text{uni}}$, XP$_{\text{uni}}$ and their *nonuniform* versions FPT$_{\text{nu}}$, XP$_{\text{nu}}$. For example, $(Q, \kappa) \in$ FPT$_{\text{uni}}$ if there is an algorithm solving $x \in Q$ in time $f(\kappa(x)) \cdot |x|^{O(1)}$ for an *arbitrary* $f : \mathbb{N} \to \mathbb{N}$; and $(Q, \kappa) \in$ FPT$_{\text{nu}}$ if there is a constant c, an arbitrary function $f : \mathbb{N} \to \mathbb{N}$, and for every $k \in \mathbb{N}$ an algorithm solving the problem $x \in Q$ for all x with $\kappa(x) = k$ in time $f(k) \cdot |x|^c$.

Let (Q, κ) and (Q', κ') be parameterized problems over the alphabets Σ and Σ', respectively. We write $(Q, \kappa) \leq^{\text{fpt}} (Q', \kappa')$ if there is an *fpt-reduction* from (Q, κ) to (Q', κ'), that is, a mapping $R : \Sigma^* \to (\Sigma')^*$ such that:

- For all $x \in \Sigma^*$ we have $(x \in Q \iff R(x) \in Q')$.
- R is computable by an fpt-algorithm.
- There is a computable function $g : \mathbb{N} \to \mathbb{N}$ such that $\kappa'(R(x)) \leq g(\kappa(x))$ for all $x \in \Sigma^*$.

Similarly, we write $(Q, \kappa) \leq^{\text{fpt-T}} (Q', \kappa')$ if there is an *fpt Turing reduction*, that is, an algorithm $\mathbb{A}$ with an oracle to Q' such that:

- $\mathbb{A}$ decides (Q, κ).

- $\mathbb{A}$ is an fpt-algorithm.
- There is a computable function $g : \mathbb{N} \to \mathbb{N}$ such that for all oracle queries "$y \in Q'$?" posed by $\mathbb{A}$ on input x we have $\kappa'(y) \leq g(\kappa(x))$.

Note that these concepts of reductions refer to the strongly uniform parameterized complexity theory. We get, say, the notion of *fpt*$_{\text{uni}}$ *Turing reduction* if we allow an *arbitrary* function $g : \mathbb{N} \to \mathbb{N}$ in the last condition and if we replace the condition "$\mathbb{A}$ is an fpt-algorithm" by the condition that the running time of $\mathbb{A}$ can only be bounded by $f(\kappa(x)) \cdot |x|^{O(1)}$ for some *arbitrary not necessarily computable* function f.

3. The problem p-GÖDEL, a parameterized version of Gödel's proof predicate

In the following we refer to any reasonable sound and complete proof calculus for first-order logic (e.g. see [6]). We do not allow proof calculi, which admit all first-order instances of propositional tautologies as axioms (as then it would take superpolynomial time to recognize correct proofs unless P $=$ NP).

The undecidability of the Entscheidungsproblem [4] tells us that the following problem is undecidable.

PROOF
Instance: A first-order sentence φ.
Question: Does φ have a proof?

Hence, we know that there is no computable bound on the length of shortest proofs of valid first-order sentences. We already remarked in the introduction that mathematicians' experience seems to indicate that various valid sentences φ of first-order logic only have quite long proofs, say, proofs superpolynomial in $|\varphi|$. How hard is it to decide whether such a hard valid sentence has a proof of a length less than a given bound? Let us try to make precise this question. We could think of valid sentences like the Four Color Theorem or the Graph Minor Theorem, but also of statements like P $\neq$ NP or the Riemann Hypothesis. Of course, we do not know whether these last two statements are valid sentences; hence the following promise problem could be viewed as the appropriate precise version of our question (note that its promise is equivalent to assuming that either φ is not valid or that φ is valid and has no short proof). Let $\iota : \mathbb{N} \to \mathbb{N}$ be a nondecreasing, unbounded and computable function.

PROMISE-EXP-GÖDEL$_\iota$
Instance: A first-order sentence φ having no proof of length $< |\varphi|^{\iota(|\varphi|)}$ and a natural number n in unary with $n \geq |\varphi|^{\iota(|\varphi|)}$.
Question: Does φ have a proof of length $\leq n$?

One could also consider the following (plain) problem:

EXP-GÖDEL$_\iota$
Instance: A first-order sentence φ and a natural number n in unary with $n \geq |\varphi|^{\iota(|\varphi|)}$.
Question: Does φ have a proof of length $\leq n$?

Clearly, EXP-GÖDEL$_\iota$ is in NP, however:

Lemma 3. *Assume that the polynomial hierarchy does not collapse. Then* PROMISE-EXP-GÖDEL$_\iota$ *and* EXP-GÖDEL$_\iota$ *are not* NP-*hard (for* PROMISE-EXP-GÖDEL$_\iota$ *this means that the set of instances of the problem that satisfy the promise and are positive instances is not* NP-*hard).*

Proof: The proofs for the two problems are similar. We give the argument for PROMISE-EXP-GÖDEL$_\iota$. We fix $m \in \mathbb{N}$ and let P_m be the set of positive instances (φ, n) of length $\leq m$ satisfying the promise. We choose the maximum $r \in \mathbb{N}$ such that $r^{\iota(r)} \leq m$. Then $n \leq m$ and $|\varphi| \leq r$ if $(\varphi, n) \in P_m$. Hence

$$|P_m| \leq 2^{r+1} \cdot m \leq 2^{m^{1/\iota(r)}+1} \cdot m = 2^{m^{o(1)}},$$

the last equality holding as r tends to infinity as m does. Therefore, the problem PROMISE-EXP-GÖDEL$_\iota$ is not exponentially dense and hence by Theorem 2, it is not NP-hard unless the polynomial hierarchy collapses. □

Therefore how do we convince ourselves that the two problems are intractable? For this purpose, we study the parameterized problem p-GÖDEL (see Section 2.3 for its definition), as the following holds:

Proposition 4. *Let ι be a nondecreasing, unbounded and computable function. If* p-GÖDEL *is not fixed-parameter tractable, then* PROMISE-EXP-GÖDEL$_\iota$ *and* EXP-GÖDEL$_\iota$ *are not decidable in polynomial time.*

Proof: By contradiction, we assume that the algorithm $\mathbb{A}$ decides, say, PROMISE-EXP-GÖDEL$_\iota$ in polynomial time. Then the following algorithm $\mathbb{B}$ shows that p-GÖDEL $\in$ FPT: For an arbitrary instance (φ, n) of p-GÖDEL, first by brute force the algorithm $\mathbb{B}$ checks whether any string in $\{0,1\}^*$ of length less than $|\varphi|^{\iota(|\varphi|)}$ is (the code of) a proof of φ; if there is a such a proof, then $\mathbb{B}$ accepts; otherwise the promise of PROMISE-EXP-GÖDEL$_\iota$ is satisfied and thus $\mathbb{B}$ simulates $\mathbb{A}$ and answers accordingly.

As the "brute force check" can be done in time $\leq f(|\varphi|)$ for a suitable computable f, the running time of $\mathbb{B}$ is bounded by $f(|\varphi|) \cdot n^{O(1)}$; thus, $\mathbb{B}$ is an fpt-algorithm. □

Hence, in this paper we try to get evidence that p-GÖDEL $\notin$ FPT. The underlying classical problem

GÖDEL
Instance: A first-order sentence φ and a natural number n in unary.
Question: Does φ have a proof of length $\leq n$?

is NP-complete: Clearly, it is in NP and the following yields a many-one reduction of the satisfiability problem SAT for propositional formulas to GÖDEL. For a propositional formula $\alpha(X_1, \ldots, X_r)$ with the propositional variables $X_1, \ldots, X_r$, we consider the first-order sentence

$$\varphi_\alpha := \exists x \exists y \big(\neg x = y \rightarrow \exists x_1 \exists y_1 \ldots \exists x_r \exists y_r \, \alpha^*(x_1 = y_1, \ldots, x_r = y_r)\big),$$

where the first-order formula $\alpha^*(x_1 = y_1, \ldots, x_r = y_r)$ is obtained from $\alpha(X_1, \ldots, X_r)$ by replacing X_i by $x_i = y_i$ for $i \in [r]$. Then (α is satisfiable if and only if φ_α is valid). Furthermore, if α is satisfiable, then φ_α has a proof of length $|\alpha|^{O(1)}$, since such a proof can be given by using an assignment satisfying α.

We already mentioned that Gödel considered the problem GÖDEL and that he asked whether it is solvable in time $O(n^2)$. He remarks that if this would be the case, then "this would have consequences of the greatest importance. Namely, it would obviously mean that in spite of the undecidability of the Entscheidungsproblem, the mental work of a mathematician concerning Yes-or-No questions could be completely replaced by a machine. After all, one would simply have to choose the natural number n so large that when the machine does not deliver a result, it makes no sense to think more about the problem."

4. The complexity of p-GÖDEL

Let

$$\text{P[TC]} \neq \text{NP[TC]}$$

mean that

$$\text{DTIME}(h^{O(1)}) \neq \text{NTIME}(h^{O(1)})$$

for all time constructible and increasing functions $h : \mathbb{N} \rightarrow \mathbb{N}$. We see that P[TC] $\neq$ NP[TC] implies P $\neq$ NP and E $\neq$ NE by taking as h the identity function and the function 2^n, respectively (here E $=$ DTIME$(2^{O(n)})$ and NE $=$ NTIME$(2^{O(n)})$). We even saw in Proposition 1 that P $\neq$ NP already holds if DTIME$(h^{O(1)}) \neq$ NTIME$(h^{O(1)})$ for some time constructible and increasing function $h : \mathbb{N} \rightarrow \mathbb{N}$. In Section 6 we are going to relate P[TC] $\neq$ NP[TC] to further statements of complexity theory.

The main result of this section is:

Theorem 5. *If* P[TC] $\neq$ NP[TC], *then* p-GÖDEL $\notin$ FPT.

We shall need the following two lemmas in the proof of Theorem 5.

Lemma 6. *For every computable and increasing function $f : \mathbb{N} \to \mathbb{N}$ and every $e_1, e_2 \in \mathbb{N}$ there is a time constructible and increasing function $h : \mathbb{N} \to \mathbb{N}$ such that for all $x, y \in \mathbb{N}$*

$$f\big((e_1 \cdot (x + y^2))^{e_2}\big) \leq h(x) + h(y).$$

Proof: We define $h_0 : \mathbb{N} \to \mathbb{N}$ by

$$h_0(n) := f((2e_1 \cdot n^2)^{e_2})$$

and let $h : \mathbb{N} \to \mathbb{N}$ be a time constructible and increasing function with $h_0(n) \leq h(n)$ for all $n \in \mathbb{N}$. □

Lemma 7. *There exists a polynomial time algorithm $\mathbb{A}$ that assigns to every nondeterministic Turing machine $\mathbb{M}$ a first-order sentence $\varphi_{\mathbb{M}}$ such that for every $n \in \mathbb{N}$,*

$$\mathbb{M} \textit{ accepts the empty input tape in } \leq n \textit{ steps} \quad \Longrightarrow \quad \varphi_{\mathbb{M}} \textit{ has a proof of length } \leq n^{O(1)}. \tag{1}$$

Moreover,

$$\varphi_{\mathbb{M}} \textit{ has a proof} \quad \Longrightarrow \quad \mathbb{M} \textit{ accepts the empty input tape.} \tag{2}$$

Sketch of proof: Let $\mathbb{M}$ be a nondeterministic Turing machine. As in standard proofs of the undecidability of first-order logic (e.g., compare [6, Section X.4]), one can define a first-order sentence $\varphi_{\mathbb{M}}$ of the form

$$(\psi_{\mathbb{M}} \to \xi_{\mathbb{M}})$$

such that for every structure $\mathcal{A}$:

(a) $\mathcal{A} \models \psi_{\mathbb{M}}$ if and only if $\mathcal{A}$ "contains" the full (possibly infinite) computation tree of $\mathbb{M}$ started with empty input tape.

(b) If $\mathcal{A} \models \psi_{\mathbb{M}}$, then ($\mathcal{A} \models \xi_{\mathbb{M}}$ if and only if the state of some element of the (possibly nonstandard) computation tree *in* $\mathcal{A}$ of $\mathbb{M}$ started with empty input tape is accepting).

To show (2) we assume $\varphi_{\mathbb{M}}$ has a proof and choose "the" structure $\mathcal{A}_0$ consisting of the standard computation tree of $\mathbb{M}$ started with empty input tape; thus, by (a), we have $\mathcal{A}_0 \models \psi_{\mathbb{M}}$. Moreover $\mathcal{A}_0 \models \varphi_{\mathbb{M}}$, as $\varphi_{\mathbb{M}}$ is valid. Hence, $\mathcal{A}_0 \models \xi_{\mathbb{M}}$ and by (b) this yields that $\mathbb{M}$ accepts the empty input tape.

We turn to (1) and assume that there is a run of $\mathbb{M}$ of $\leq n$ steps accepting the empty tape. We fix such a run. By (a), every model of $\psi_{\mathbb{M}}$ contains this run. As this run is accepting, we obtain, by (b), that the sentence $\varphi_{\mathbb{M}}$ is valid. "By following this accepting run" we can translate it into a proof of $(\psi_{\mathbb{M}} \to \xi_{\mathbb{M}})$, that is of $\varphi_{\mathbb{M}}$, of length $\leq n^{O(1)}$. The details of such a translation are tedious but routine. □

Proof of Theorem 5: For any nondeterministic Turing machine $\mathbb{M}$ and every $x \in \{0,1\}^*$ we let $\mathbb{M}_x$ be the nondeterministic Turing machine that, started with empty input tape, first writes x on some tape and then simulates $\mathbb{M}$ started with x. Clearly we can define $\mathbb{M}_x$ such that $\|\mathbb{M}_x\| = O(\|\mathbb{M}\| + |x| \cdot \log|x|)$. We choose $e_1 \in \mathbb{N}$ such that

$$\|\mathbb{M}_x\| \leq e_1 \cdot (\|\mathbb{M}\| + |x|^2). \tag{3}$$

Now by contradiction assume that p-GÖDEL $\in$ FPT. Then there is an algorithm $\mathbb{A}_0$ that for every first-order sentence φ and $n \in \mathbb{N}$ decides whether φ has a proof of length $\leq n$ in time

$$f(|\varphi|) \cdot n^{O(1)} \tag{4}$$

for some computable and increasing function $f : \mathbb{N} \to \mathbb{N}$. Furthermore, let $\mathbb{A}$ be the algorithm of Lemma 7. We choose $e_2 \in \mathbb{N}$ such that the running time of $\mathbb{A}$ on every nondeterministic Turing machine $\mathbb{M}$ is bounded by $\|\mathbb{M}\|^{e_2}$. In particular,

$$|\varphi_{\mathbb{M}}| \leq \|\mathbb{M}\|^{e_2}. \tag{5}$$

For the function f we choose $h : \mathbb{N} \to \mathbb{N}$ according to Lemma 6. We show that NTIME($h^{O(1)}$) $\subseteq$ DTIME($h^{O(1)}$).

For this purpose let $Q \subseteq \{0,1\}^*$ be in NTIME($h^{O(1)}$). We choose a nondeterministic Turing machine $\mathbb{M}$ and constants $c, d \in \mathbb{N}$ such that the machine $\mathbb{M}$ decides whether $x \in Q$ in time $c \cdot h(|x|)^d$ and every run of $\mathbb{M}$ on input x is $c \cdot h(|x|)^d$ time-bounded (recall that h is time constructible).

We fix $x \in \{0,1\}^*$ and let $\mathbb{M}_x$ be the nondeterministic Turing machine that, started with empty input tape, first writes x on some tape and then simulates $\mathbb{M}$ started with x. We apply the algorithm $\mathbb{A}$ on $\mathbb{M}_x$ and get a first-order sentence $\varphi_x := \varphi_{\mathbb{M}_x}$. Now we have the following chain of implications (as the first statement and the last one coincide all implications are equivalences):

$$\begin{array}{lll}
x \in Q & & \\
\quad \Rightarrow & \mathbb{M} \text{ accepts } x \text{ in at most } c \cdot h(|x|)^d \text{ steps} & \\
\quad \Rightarrow & \mathbb{M}_x \text{ accepts the empty input tape in at most } |x| + c \cdot h(|x|)^d \text{ steps} & (\text{by definition of } \mathbb{M}_x) \\
\quad \Rightarrow & \mathbb{M}_x \text{ accepts the empty input tape in at most } 2c \cdot h(|x|)^d \text{ steps} & (\text{as } h \text{ is increasing}) \\
\quad \Rightarrow & \varphi_x \text{ has a proof of length at most } (2c \cdot h(|x|))^{O(1)} & (\text{by (1) in Lemma 7}) \\
\quad \Rightarrow & \mathbb{M}_x \text{ accepts the empty input tape} & (\text{by (2) in Lemma 7}) \\
\quad \Rightarrow & \mathbb{M} \text{ accepts } x & (\text{by definition of } \mathbb{M}_x) \\
\quad \Rightarrow & x \in Q. &
\end{array}$$

Hence,

$$\begin{aligned}
x \in Q \quad &\Longleftrightarrow \quad \varphi_x \text{ has a proof of length at most } (2c \cdot h(|x|))^{O(1)} \\
&\Longleftrightarrow \quad \mathbb{A}_0 \text{ accepts } \big(\varphi_x, (2c \cdot h(|x|))^{O(1)}\big).
\end{aligned}$$

By (5) and (3) we have

$$|\varphi_x| = |\varphi_{\mathbb{M}_x}| \leq \|\mathbb{M}_x\|^{e_2} \leq (e_1 \cdot (\|\mathbb{M}\| + |x|^2))^{e_2}. \tag{6}$$

By (4) the running time of $\mathbb{A}_0$ on input $(\varphi_x, (2c \cdot h(|x|))^{O(1)})$ is bounded by

$$\begin{aligned}
f(|\varphi_x|) \cdot (2c \cdot h(|x|))^{O(1)} &\leq f\big((e_1 \cdot (\|\mathbb{M}\| + |x|^2))^{e_2}\big) \cdot h(|x|)^{O(1)} && (\text{by (6)}) \\
&\leq \big(h(\|\mathbb{M}\|) + h(|x|)\big) \cdot h(|x|)^{O(1)} && (\text{by the definition of } h).
\end{aligned}$$

As $h(\|\mathbb{M}\|)$ is a constant, this shows that $Q \in$ DTIME($h(|x|)^{O(1)}$). □

Remark 8. [1] Let $\iota : \mathbb{N} \to \mathbb{N}$ be a nondecreasing and unbounded function computable in polynomial time and with the property that $\iota(n) \leq \log n$ for all $n \in \mathbb{N}$. Then:

> If EE $\neq$ NEE (that is, DTIME($2^{2^{O(k)}}$) $\neq$ NTIME($2^{2^{O(k)}}$)), then PROMISE-EXP-GÖDEL$_\iota$ or EXP-GÖDEL$_\iota$ are not decidable in polynomial time.

In fact, in case that any of the two problems is solvable in polynomial time the proof of Proposition 4 shows that $(\varphi, n) \in p$-GÖDEL is solvable in time $\leq 2^{|\varphi|^{\iota(|\varphi|)+1}} \cdot n^{O(1)} \leq 2^{|\varphi|^{\log |\varphi|}} \cdot n^{O(1)} \leq 2^{2^{O(\sqrt[d]{|\varphi|})}} \cdot n^{O(1)}$ for every $d \in \mathbb{N}$. Then the previous proof shows that NTIME($2^{2^{O(k)}}$) $\subseteq$ DTIME($2^{2^{O(k)}}$).

We can refine the argument of the proof of Theorem 5 to get p-GÖDEL $\notin$ XP; however we need a complexity-theoretic assumption that is (apparently) stronger than P[TC] $\neq$ NP[TC].

Theorem 9. *Assume that*

$$\text{NTIME}(h^{O(1)}) \not\subseteq \text{DTIME}(h^{O(\log h)})$$

*for every time constructible and increasing function h. Then p-*GÖDEL $\notin$ XP.

[1] This remark was pointed out to us by Albert Atserias.

Proof: Assume that p-GÖDEL $\in$ XP. Then there is an algorithm $\mathbb{A}_0$ that for every first-order sentence φ and every natural number n decides whether φ has a proof of length $\leq n$ in time

$$O(n^{f(|\varphi|)})$$

for a computable and increasing function $f : \mathbb{N} \to \mathbb{N}$.

We choose $e_1, e_2 \in \mathbb{N}$ and the time constructible and increasing function $h : \mathbb{N} \to \mathbb{N}$ as in the previous proof. We define $h' : \mathbb{N} \to \mathbb{N}$ by $h'(n) := 2^{h(n)}$; clearly h' is time constructible and increasing, too. We show that NTIME$({h'}^{O(1)}) \subseteq$ DTIME$({h'}^{O(\log h')})$.

Let $Q \subseteq \{0,1\}^*$ be an arbitrary problem in NTIME$({h'}^{O(1)})$. For Q let $\mathbb{M}$ and, for $x \in \{0,1\}^*$, $\mathbb{M}_x$ and φ_x be defined as in the previous proof, however, concerning their running time, now h' takes over the role of h. As there we get

$$x \in Q \quad \iff \quad \mathbb{A}_0 \text{ accepts } (\varphi_x, 2c \cdot h'(|x|)^d).$$

Recall that for $\varphi_x := \varphi_{\mathbb{M}_x}$ the inequality (6) holds. Therefore the running time of $\mathbb{A}_0$ on input $(\varphi_x, h'(x)^{O(1)})$ is bounded by

$$\begin{aligned} h'(|x|)^{O\big(f(|\varphi_x|)\big)} &\leq h'(|x|)^{O\Big(f\big((e_1 \cdot (\|\mathbb{M}\| + |x|^2))^{e_2}\big)\Big)} \\ &\leq h'(|x|)^{O\big(h(\|\mathbb{M}\|) + h(|x|)\big)} \leq h'(|x|)^{O\big(h(\|\mathbb{M}\|) + \log h'(|x|)\big)}. \end{aligned}$$

As $h(\|\mathbb{M}\|)$ is a constant, this shows $Q \in$ DTIME$({h'}^{O(\log h')})$. □

Remark 10. In Theorem 9 we can replace the log-function by any nondecreasing, unbounded and computable function. In fact, along the lines of the previous proof one can show:

Let $\iota : \mathbb{N} \to \mathbb{N}$ be nondecreasing, unbounded, and computable and assume that

$$\text{NTIME}(h^{O(1)}) \not\subseteq \text{DTIME}(h^{O(\iota \circ h)})$$

for every time constructible and increasing function h. Then p-GÖDEL $\notin$ XP.

Here $\iota \circ h$ denotes the function $n \mapsto \iota(h(n))$.

We do not know whether p-GÖDEL $\in$ XP$_{\text{uni}}$ or even p-GÖDEL $\in$ FPT$_{\text{uni}}$. However, from the point of view of nonuniform parameterized complexity the problem p-GÖDEL is fixed-parameter tractable:

Proposition 11. p-GÖDEL $\in$ FPT$_{\text{nu}}$.

Proof: Fix $k \in \mathbb{N}$; then there are only finitely many first-order sentences φ with $|\varphi| = k$, say, $\varphi_1, \ldots, \varphi_s$. For each $i \in [s]$ let ℓ_i be the smallest natural number ℓ such that there exists a proof of φ_i of length ℓ. We set $\ell_i = \infty$ if φ_i is not valid (and hence has no proof). The algorithm $\mathbb{A}_k$ that on any instance (φ, n) of p-GÖDEL with $|\varphi| = k$ first determines the $i \in [s]$ with $\varphi = \varphi_i$, and then accepts if and only if $\ell_i \leq n$ has running time $O(|\varphi| + n)$; thus it witnesses that p-GÖDEL is in FPT$_{\text{nu}}$. □

5. The construction problem associated with p-GÖDEL

Often the construction problem has the same complexity as the corresponding decision problem, that is, the construction problem is reducible to the decision problem. In this section we first analyze this question for the problem p-GÖDEL from the point of view of strongly uniform, uniform, and nonuniform parameterized complexity.

The construction problem associated with p-GÖDEL is the problem:

p-CONSTR-GÖDEL
Instance: A first-order sentence φ and a natural number n in unary.
Parameter: $|\varphi|$.
Problem: Construct a proof of φ of length $\leq n$ if there exists one (and otherwise report that there is no such proof).

For the underlying classical problem, namely for

CONSTR-GÖDEL

Instance: A first-order sentence φ and a natural number n in unary.

Problem: Construct a proof of φ of length $\leq n$ if there exists one (and otherwise report that there is no such proof).

we have by the NP-completeness of GÖDEL:

Proposition 12. *There is a polynomial time Turing reduction from* CONSTR-GÖDEL *to* GÖDEL.

Proof: We consider the problem whose instances consist of a first-order sentence φ, a natural number n in unary, and a string $x \in \{0,1\}^*$ with $|x| < n$ and which asks whether x is an initial segment of a proof of φ of length $\leq n$. Clearly, this problem is in NP and hence it is polynomial time reducible to GÖDEL. Now, using such a reduction and an oracle for GÖDEL, we can stepwise construct a proof of φ of length $\leq n$ (if there is one) in polynomial time. □

Assume that p-GÖDEL $\notin$ XP. Let φ be a first-order sentence (for example, expressing P $\neq$ NP or the Riemann Hypothesis) and assume that it is valid, say, it has a proof of length n. Then the following theorem shows that the polynomial time Turing reduction of the preceding proposition, in general will ask queries "$(\psi, m) \in$ GÖDEL?" for sentences ψ with $|\psi|$ only bounded by some polynomial in n, the length of a proof of φ.

Theorem 13. *If p-*GÖDEL $\notin$ XP*, then there is no fpt Turing reduction from p-*CONSTR-GÖDEL *to p-*GÖDEL.

Proof: By contradiction, assume there is an fpt Turing reduction $\mathbb{A}$ from p-CONSTR-GÖDEL to p-GÖDEL. We show how $\mathbb{A}$ can be turned into an algorithm witnessing p-GÖDEL $\in$ XP.

According to the definition of fpt Turing reduction (see Section 2.3) there are computable functions f, g and $c \in \mathbb{N}$ such that for every instance (φ, n) of p-GÖDEL, the algorithm $\mathbb{A}$ will only make queries "$(\psi, m) \in p$-GÖDEL?" with

$$|\psi| \leq g(|\varphi|) \quad \text{and} \quad m \leq f(|\varphi|) \cdot n^c. \tag{7}$$

There are at most $2^{g(|\varphi|)+1}$ first-order sentences ψ with $|\psi| \leq g(|\varphi|)$. For each such sentence ψ the answer to queries of the form "$(\psi, m) \in p$-GÖDEL?" with $m \leq f(|\varphi|) \cdot n^c$ is determined by everyone of the following $f(|\varphi|) \cdot n^c + 1$ many statements: "the minimum length of a proof of ψ is 1",…, "the minimum length of a proof of ψ is $f(|\varphi|) \cdot n^c$", and "there is no proof of ψ of length $\leq f(|\varphi|) \cdot n^c$." Therefore the table of theoretically possible answers contains at most

$$\big(f(|\varphi|) \cdot n^c + 1\big)^{2^{g(|\varphi|)+1}}$$

entries, that is $O(n^{h(|\varphi|)})$ many for some computable h. For each such possibility we simulate $\mathbb{A}$ by replacing the oracle queries accordingly. For those possibilities where $\mathbb{A}$ yields a purported proof of φ of length $\leq n$, we can check whether it is really such a proof. Altogether, we have shown that p-GÖDEL $\in$ XP. □

However, there is an fpt$_{\text{uni}}$ Turing reduction from p-CONSTR-GÖDEL to p-GÖDEL (see Section 2.3 for the definition of fpt$_{\text{uni}}$ Turing reduction):

Theorem 14. *There is an fpt$_{\text{uni}}$ Turing reduction from p-*CONSTR-GÖDEL *to p-*GÖDEL.

Proof: On an instance (φ, n) of p-CONSTR-GÖDEL the desired reduction $\mathbb{A}$ first asks the oracle query "$(\varphi, n) \in p$-GÖDEL?". If the answer is no, then $\mathbb{A}$ answers accordingly. Otherwise $\mathbb{A}$, by brute force, constructs a proof of φ of length at most n. We analyze the running time of $\mathbb{A}$. For $m \in \mathbb{N}$ let $\varphi_1, \ldots, \varphi_\ell$ be the finitely many valid first-order sentences of length $\leq m$. Let n_i be the minimum length of a proof of φ_i. We set $f(m) := \max\{n_1, \ldots, n_\ell\}$. Now it is not hard to see that the running time of $\mathbb{A}$ on the instance (φ, n) can be bounded by $O(2^{f(|\varphi|)+1})$. □

Similarly as we convinced ourselves that p-GÖDEL $\in$ FPT$_{\text{nu}}$, we get that p-CONSTR-GÖDEL is nonuniformly fixed-parameter tractable and hence p-CONSTR-GÖDEL is trivially fpt$_{\text{nu}}$ reducible to p-GÖDEL (even though we have not defined all these concepts, it should be clear what this means).

Mathematicians only try to find proofs of those statements which they believe or guess to be valid. Thereby, they often first look for appropriate intermediate statements, which are intended to help to get a proof of a given "hard" statement. The question arises whether one can speed up the proof search process asked for in GÖDEL using an oracle that tells us whether (the intermediate and the final) statements are valid, that is, with an oracle to PROOF. Again we will see that the answer depends on whether we look at the classical problems or we consider parameterizations which bound the length of the intermediate statements in terms of the original statement.

Proposition 15. *There is a polynomial time Turing reduction from* CONSTR-GÖDEL *to* PROOF*.*

Proof: By Proposition 12, it suffices to give a polynomial time reduction from GÖDEL to PROOF. That is, given a first-order sentence φ and $n \in \mathbb{N}$, in polynomial time one has to construct a first-order sentence φ_n such that

$$\varphi \text{ has a proof of length} \leq n \quad\iff\quad \varphi_n \text{ has a proof.}$$

The construction is routine but tedious. □

Let us fix a polynomial Turing reduction $\mathbb{A}$ from CONSTR-GÖDEL to PROOF. For a given instance (φ, n) of CONSTR-GÖDEL, if we are interested in bounding in terms of $|\varphi|$ the length of those ψ that occur in oracles queries "$\psi \in$ PROOF?" of $\mathbb{A}$ (that is, the length of the "intermediate statements"), then the following result shows that PROOF is unlikely to help at all. To formulate this result we let:

p-PROOF
Instance: A first-order sentence φ.
Parameter: $|\varphi|$.
Question: Does φ have a proof?

Proposition 16. *If* p-GÖDEL $\notin$ FPT*, then there is no fpt Turing reduction from* p-CONSTR-GÖDEL *to* p-PROOF*.*

This proposition is an easy consequence of the following theorem, which implies that for every polynomial time Turing reduction from CONSTR-GÖDEL to PROOF the *number* of oracle queries "$\psi \in$ PROOF?" on an instance (φ, n) of CONSTR-GÖDEL can not be bounded in terms of $|\varphi|$.

Theorem 17. *If* p-GÖDEL $\notin$ FPT*, then there is no fpt-algorithm* $\mathbb{A}$ *with an oracle to* PROOF *that solves the problem* p-CONSTR-GÖDEL *in such a way that for some computable function* $g : \mathbb{N} \to \mathbb{N}$ *on every instance* (φ, n) *of* p-CONSTR-GÖDEL *the algorithm* $\mathbb{A}$ *makes at most* $g(|\varphi|)$ *many oracle queries to* PROOF*.*

Proof: By contradiction assume that there is an algorithm $\mathbb{A}$ with an oracle to PROOF that solves the problem p-CONSTR-GÖDEL in such a way that for some computable functions $f, g : \mathbb{N} \to \mathbb{N}$ we have for every instance (φ, n) of p-CONSTR-GÖDEL:

(a) the run of $\mathbb{A}$ on input (φ, n) has length $\leq f(|\varphi|) \cdot n^c$;

(b) there are first-order sentences $\psi_1, \psi_2, \ldots, \psi_m$ with $m \leq g(|\varphi|)$ such that for every oracle query "$\psi \in$ PROOF?" of the run of $\mathbb{A}$ on input (φ, n) we have $\psi = \psi_i$ for some $i \in [m]$.

We show how $\mathbb{A}$ can be turned into an algorithm witnessing p-GÖDEL $\in$ FPT.

For every $i \in [m]$ there are two possible answers to the oracle query "$\psi_i \in$ PROOF?," namely "YES" and "NO." Thus for all ψ_i together we have 2^m possibilities, that is, $O(2^{g(|\varphi|)})$ many (note that m only depends on φ). Now, given in addition $n \in \mathbb{N}$, for each such possibility we simulate $\mathbb{A}$ on input (φ, n) by replacing the oracle queries accordingly. For those possibilities where $\mathbb{A}$ yields a purported proof, we can check whether it is really a proof of φ of length $\leq n$. By (a) the overall time needed by this procedure is $O(2^{g(|\varphi|)} \cdot (f(|\varphi|) \cdot n^c + n^{O(1)}))$, which is an fpt-time. □

6. Relating P[TC] $\neq$ NP[TC] to other statements

For the purposes of this section the following lemma will be useful.

Lemma 18. *Let $h : \mathbb{N} \to \mathbb{N}$ be time constructible and increasing and let I_h be the range of h in unary, that is,*

$$I_h = \big\{ \underbrace{11\dots11}_{h(m)\ \textit{times}} \bigm| m \in \mathbb{N} \big\}.$$

If NTIME($h^{O(1)}$) $=$ DTIME($h^{O(1)}$)*, then for every problem $Q \subseteq \{0,1\}^*$ in* NP *the problem $Q \cap I_h$ is in* P.

Proof: Assume that NTIME($h^{O(1)}$) $=$ DTIME($h^{O(1)}$). Let $Q \subseteq \{0,1\}^*$ be in NP. Then, as h is time constructible, the problem

$$Q_0 := \big\{ \underbrace{11\dots11}_{m \text{ times}} \bigm| m \in \mathbb{N} \text{ and } \underbrace{11\dots11}_{h(m) \text{ times}} \in Q \big\}$$

is in NTIME($h^{O(1)}$) and thus, by our assumption, it is in DTIME($h^{O(1)}$). Clearly,

$$Q \cap I_h = \big\{ \underbrace{11\dots11}_{h(m) \text{ times}} \bigm| m \in \mathbb{N} \text{ and } \underbrace{11\dots11}_{m \text{ times}} \in Q_0 \big\}. \tag{8}$$

As h is time constructible and increasing, one can check for every $s \in \{0,1\}^*$ whether $s = \underbrace{11\dots11}_{h(m) \text{ times}}$ for some $m \in \mathbb{N}$ and in the positive case construct such an m in time polynomial in $|s|$. Therefore, as $Q_0 \in$ DTIME($h^{O(1)}$), we see that $Q \cap I_h \in$ P. □

Let C be a classical complexity class, that is, let C be a class of problems. Recall that a problem $Q \subseteq \{0,1\}^*$ is C-*bi-immune* if both Q and the complement of Q do not have an *infinite subset* that belongs to C. It has been conjectured that

$$\text{NP contains a P-bi-immune problem.}^2 \tag{9}$$

Moreover, Mayordomo [10] has proven that (9) is implied by a further conjecture, namely by:

$$\text{NP does not have measure 0 in E.} \tag{10}$$

This statement (10) is sometimes used as a hypothesis in the theory of resource bounded measures [9]. For the corresponding notion of measure we refer to [10]. The conditions (9) and (10) imply P[TC] $\neq$ NP[TC]:

Proposition 19. *Consider the following statements:*

(a) NP *does not have measure 0 in* E.

(b) NP *contains a* P*-bi-immune problem.*

(c) There is no infinite set $I \subseteq \{0,1\}^*$ such that for every $Q \subseteq \{0,1\}^*$ in NP *the problem $Q \cap I$ is in* P.

(d) P[TC] $\neq$ NP[TC].

Then (a) implies (b), (b) implies (c), and (c) implies (d).

Proof: In Lemma 18 we have seen that "not (d) implies not (c)."

(b) $\Rightarrow$ (c): By contradiction assume that there is a set I with the properties mentioned in (c). As $\{0,1\}^* \cap I = I$, the set I is in P. Let $Q \subseteq \{0,1\}^*$ be in NP. Then $Q \cap I$ is in P and hence $(\{0,1\}^* \setminus Q) \cap I = I \setminus (Q \cap I) \in$ P. As at least one of the sets $Q \cap I$ or $(\{0,1\}^* \setminus Q) \cap I$ is infinite, we see that Q is not P-bi-immune. As Q was arbitrary this contradicts (b).

We already mentioned that "(a) $\Rightarrow$ (b)" was shown in Mayordomo [10]. □

Hence, from Theorem 5, we get:

[2] We thank Christian Glaser who draw our attention to the notion of P-bi-immunity.

Corollary 20. *If* NP *contains a* P*-bi-immune problem, then* p-GÖDEL $\notin$ FPT.

Remark 21. Note that the assumption (b) in Proposition 19 seems to be much stronger than the assumption (c). In fact, as shown by the proof of the previous proposition, "not (c)" means

> there is an infinite set $I \in$ P such that for all $Q \in$ NP at least one of the sets $Q \cap I$ and $\big(\{0,1\}^* \setminus Q\big) \cap I$ is an infinite set in P,

while NP contains no P-bi-immune problem can be reformulated as

> for all $Q \in$ NP there is an infinite $I \in$ P such that at least one of the sets $Q \cap I$ or $\big(\{0,1\}^* \setminus Q\big) \cap I$ is an infinite set in P.

Let $\mathrm{E}_2 = \mathrm{DTIME}(2^{n^{O(1)}})$. Then one can show along the lines of the proof of Proposition 19 the following chain of implications, the last one being the assumption used in Theorem 9:

Proposition 22. *Consider the following statements:*

(a) NP *does not have measure 0 in* E_2.

(b) NP *contains an* E*-bi-immune problem.*

(c) There is no infinite set $I \subseteq \{0,1\}^*$ *such that for every* $Q \subseteq \{0,1\}^*$ *in* NP *the problem* $Q \cap I$ *is in* $\mathrm{DTIME}(n^{O(\log n)})$.

(d) For every time constructible and increasing function h

$$\mathrm{NTIME}(h^{O(1)}) \not\subseteq \mathrm{DTIME}(h^{O(\log h)}).$$

Then (a) implies (b), (b) implies (c), and (c) implies (d).

The statements (a) and (b) have been considered in [9, 10].

7. Conclusions

We already remarked that we view the statement P[TC] $\neq$ NP[TC] as a natural generalization of the statements P $\neq$ NP, E $\neq$ NE, ... Therefore we were astonished that P[TC] $\neq$ NP[TC] has not been considered in the literature so far. We introduced this statement when analyzing the parameterized complexity of a parameterized halting problem in [3].

An analysis of the proof of Theorem 5 shows that instead of the assumption P[TC] $\neq$ NP[TC] it would suffice to assume that there is a time constructible and increasing function $h : \mathbb{N} \to \mathbb{N}$ such that for all time constructible and increasing functions $g : \mathbb{N} \to \mathbb{N}$ with $h \leq g$ (that is, with $h(k) \leq g(k)$ for all $k \in \mathbb{N}$) we have $\mathrm{NTIME}(g^{O(1)}) \neq \mathrm{DTIME}(g^{O(1)})$. We do not know whether this assumption is weaker, in particular, we do not know whether

$$\mathrm{NTIME}(h^{O(1)}) = \mathrm{DTIME}(h^{O(1)}) \text{ and } h \leq g \text{ imply } \mathrm{NTIME}(g^{O(1)}) = \mathrm{DTIME}(g^{O(1)}).$$

We do not see any way to prove this using a padding argument as in Proposition 1.

We close by presenting a further parameterized problem for which we can show that it is not fixed-parameter tractable under the assumption P[TC] $\neq$ NP[TC]. We are not able to prove this result under the assumption P $\neq$ NP.

We consider the problem

p-FO-FINITE-MODEL	
Instance:	A first-order sentence φ and a natural number n in unary.
Parameter:	$\lvert\varphi\rvert$.
Question:	Is there a finite model of φ whose universe has cardinality $\leq n$?

Theorem 23. *(1) If* P[TC] $\neq$ NP[TC], *then* p-FO-FINITE-MODEL $\notin$ FPT.

(2) Assume that

$$\mathrm{NTIME}(h^{O(1)}) \not\subseteq \mathrm{DTIME}(h^{O(\log h)})$$

for every time constructible and increasing function h. Then p-FO-FINITE-MODEL $\notin$ XP.

In view of the following proposition these results are immediate consequences of the corresponding results for p-GÖDEL.

Proposition 24. p-GÖDEL $\leq^{\text{fpt}}$ p-FO-FINITE-MODEL.

Proof: By standard means one can construct a first-order formula *proof*(u) with the free variable u such that for some polynomial q we have for all finite structures $\mathcal{A}$ and all first-order sentences φ (we denote by $\ulcorner\varphi\urcorner$ the Gödel number of φ, more precisely, a term representing the Gödel number of φ)

$$\mathcal{A} \models \textit{proof}(\ulcorner\varphi\urcorner) \qquad \text{iff} \qquad \mathcal{A} \text{ encodes a proof } x \text{ of } \varphi \text{ and } |A| = q(|x|)$$

and such that for every proof x of φ there is a structure $\mathcal{A}_{x,\varphi}$ that encodes the proof x with $|A_{x,\varphi}| = q(|x|)$.

Then $(\varphi, n) \mapsto (\textit{proof}(\ulcorner\varphi\urcorner), q(n))$ is the desired reduction. □

References

[1] H. Buhrman and J. M. Hitchcock. NP-hard sets are exponentially dense unless coNP $\subseteq$ NP/poly. In *Proceedings of the 23rd Annual IEEE Conference on Computational Complexity (CCC'08)*, pp. 1-7, 2008.

[2] S. Buss. On Gödel's Theorem on length of proofs II: lower bounds for recognizing k symbol provability. In *Feasible Mathematics II*, P. Clote and J. Remmel (eds.), Birkhauser, 57–90, 1995.

[3] Y. Chen and J. Flum. A logic for PTIME and a parameterized halting problem. In preparation.

[4] A. Church. A note on the Entscheidungsproblem. *Journal of Symbolic Logic*, 1: 40–41, 1936.

[5] R.G. Downey and M.R. Fellows, *Parameterized Complexity*, Springer, 1999.

[6] H.-D. Ebbinghaus, J. Flum, and W. Thomas, *Mathematical Logic*, Springer, 1994.

[7] J. Flum and M. Grohe. *Parameterized Complexity Theory*, Springer, 2006.

[8] K. Gödel. *Collected Works*, vol. VI, 372–376, Clarendon Press, 2003.

[9] J.H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra and A. L. Selman (eds.), *Complexity Theory Retrospective II*, Springer-Verlag, 1997, 225–254.

[10] E. Mayordomo. Almost every set in exponential time is P-bi-immune. *Theoretical Computer Science*, 136(2): 487-506, 1994.