Annals of Pure and Applied Logic 27 (1984) 265–273
North-Holland

TAUTOLOGIES WITH A UNIQUE CRAIG INTERPOLANT, UNIFORM vs. NONUNIFORM COMPLEXITY

Daniele MUNDICI

National Research Council, and Mathematical Institute of the University of Florence, Loc. Romola N.76, 50060 Donnini, Florence, Italy

Communicated by Y. Gurevich
Received 1 September 1983; revised 1 March 1984

If $S \subseteq \{0, 1\}^*$ and $S' = \{0, 1\}^* \setminus S$ are both recognized within a certain nondeterministic time bound T then, in not much more time, one can write down tautologies $A_n \to A'_n$ with unique interpolants I_n that define $S \cap \{0, 1\}^n$; hence, if one can rapidly find unique interpolants, then one can recognize S within deterministic time T^p for some fixed $p > 0$. In general, complexity measures for the problem of finding unique interpolants in sentential logic yield new relations between circuit depth and nondeterministic Turing time, as well as between proof length and the complexity of decision procedures of logical theories.

0. Introduction

The aim of this paper is to relate uniform and nonuniform complexity measures, using Craig's interpolation in sentential logic. We do not need the definition of 'uniform': as in [4, p. 255], our examples of uniform complexity measures are the time and space needed by Turing machines and their variants, where one machine handles inputs of all sizes. In contrast, the circuit size of a set $S \subseteq \{0, 1\}^*$ is measured by providing a suitable circuit α_n for each $S \cap \{0, 1\}^n$: since in general there is no 'simple' rule (see [11]) for constructing the α_n's, circuit size is regarded as a nonuniform complexity measure. Similarly, given a decidable theory Θ, the deterministic Turing time of the decision procedure for Θ, and the proof-length function λ_Θ defined in 4.7 below, are examples of uniform (resp., nonuniform) complexity measures of Θ.

A Δ-tautology in sentential logic is a tautology of the form $H \to K$ having exactly one Craig interpolant J, up to logical equivalence. In Theorem 4.2 we prove that if $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$, then no deterministic Turing machine M can output J within time bounded by a polynomial in the length of $H \to K$. In general, given an upper bound T for the time required by any such M, together with an upper bound λ_Θ for the length of proofs in a complete finitely axiomatizable first-order theory Θ, we obtain an upper bound $T^q \circ \lambda_\Theta^p$ for the deterministic Turing time of the decision procedure of Θ, for suitable p and q in $\mathbb{N}$. In the converse direction, let $\delta(n) =$ least $m \geq 2$ such that every Δ-tautology of length $\leq n$ has an interpolant of length $\leq m$. Then any set S in $\mathrm{NP} \cap \mathrm{coNP}$ is computed by circuits

$\{\alpha_n\}$ such that depth$(\alpha_n) \leq k \log \delta(n^p)$, for suitable $k, p > 0$ only depending on S. See Theorems 4.8 and 3.1.

The author thanks the referee, whose suggestions improved this paper in many respects.

1. Preliminaries

We let $\mathbb{N}$ and $\mathbb{R}$ denote the set of natural and real numbers respectively; $\mathbb{N}^+ = \mathbb{N}\backslash\{0\}$, $\mathbb{R}^+ = \{t \in \mathbb{R} \mid t > 0\}$. For any set Γ, Γ^* is the set of words over Γ, i.e. the set of finite strings of symbols from Γ. For $w \in \Gamma^*$, the length $|w|$ of w is the number of occurrences of symbols in w. In this paper boolean expressions are regarded as particular words over the alphabet

$$\Sigma = \{\wedge, \vee, \neg,), (, X, 0, 1\},$$

according to the usual syntax of sentential logic [2]. Words of the form $Xb_1 \cdots b_n$ with each $b_i \in \{0, 1\}$ and $n \in \mathbb{N}^+$ are (propositional) variables; the string $b_1 \cdots b_n$ is the subscript of $Xb_1 \cdots b_n$; variables inherit the lexicographic order $\prec$ of their subscripts $(0 \prec 1 \prec 00 \prec 01 \prec 10 \prec \cdots)$. For any boolean expression $G \in \Sigma^*$, var G denotes the set of variables occurring in G, and $|\text{var } G|$ is the number of elements of var G. Assume $m = |\text{var } G|$; then for every $x \in \{0, 1\}^m$ we write $x \models G$ iff $\hat{G}(x) = 1$, where $\hat{G}: \{0, 1\}^m \to \{0, 1\}$ is the boolean function determined by G via the familiar identification $1 =$ 'true' and $0 =$ 'false'. The set Mod G is defined by

$$\text{Mod } G = \{x \in \{0, 1\}^m \mid x \models G\} = \hat{G}^{-1}(1);$$

in addition, for arbitrary n with $1 \leq n \leq m$ we define

$$\text{Mod } G \restriction (\text{first } n \text{ bits}) = \left\{x \in \{0, 1\}^n \mid \exists y \in \{0, 1\}^m \text{ with } y \models G \text{ and } \bigwedge_{i=1}^{n} y_i = x_i\right\}.$$

In other words, $x = \langle x_1, \ldots, x_n \rangle \in \text{Mod } G \restriction (\text{first } n \text{ bits})$ iff x has an expansion $y = \langle x_1, \ldots, x_n, x_{n+1}, \ldots, x_m \rangle$ such that $y \models G$. G is a tautology iff Mod $G = \{0, 1\}^m$. See [2] for the semantics of sentential logic.

2. Δ-interpolation

Following common usage, given two boolean expressions $H, K \in \Sigma^*$ we write $H \to K$ as an abbreviation of $((\neg H) \vee K)$. If $H \to K$ is a tautology and var $H \cap$ var $K \neq \emptyset$, then Craig's interpolation theorem in sentential logic [2, ex. 1.2.7] asserts the existence of an interpolant I for $H \to K$, i.e. a boolean expression $I \in \Sigma^*$ such that $H \to I$ and $I \to K$ are tautologies, and var $I =$ var $H \cap$ var K. Of particular interest is the case when the interpolant is unique, up to logical equivalence, in the following sense:

2.1. Definition. A Δ-tautology is a tautology $H \to K$ such that $\mathrm{var}\, H \cap \mathrm{var}\, K \neq \emptyset$ and whenever I and J are interpolants for $H \to K$, then $\mathrm{Mod}\, I = \mathrm{Mod}\, J$. $\square$

Our terminology comes from abstract model theory where Δ- (also called Souslin–Kleene-) interpolation plays a fundamental role [3].

2.2. Proposition. *Let $L', L'' \in \Sigma^*$ be boolean expressions. Assume* $\mathrm{var}\, L' \cap \mathrm{var}\, L''$ *coincides with the set of the first n variables (in lexicographic order), and $n > 0$. If*

$$\mathrm{Mod}\, L' \restriction (\text{first } n \text{ bits}) = \{0, 1\}^n \setminus (\mathrm{Mod}\, L'' \restriction (\text{first } n \text{ bits})),$$

then $L' \to \neg L''$ is a Δ-tautology.

Proof. For any H and K whose common variables are the first n, $H \to K$ is a tautology with interpolant I iff $\mathrm{Mod}\, H \restriction (\text{first } n \text{ bits}) \subseteq \mathrm{Mod}\, I$ and $(\mathrm{Mod}\, \neg K) \restriction (\text{first } n \text{ bits}) \subseteq \mathrm{Mod}\, \neg I$. Equivalently, iff

$$\mathrm{Mod}\, H \restriction (\text{first } n \text{ bits}) \subseteq \mathrm{Mod}\, I \subseteq \{0, 1\}^n \setminus ((\mathrm{Mod}\, \neg K) \restriction (\text{first } n \text{ bits})).$$

Since every subset of $\{0, 1\}^n$ is equal to $\mathrm{Mod}\, I$ for some I, it follows in particular that $H \to K$ is a Δ-tautology iff

$$\mathrm{Mod}\, H \restriction (\text{first } n \text{ bits}) = \{0, 1\}^n \setminus ((\mathrm{Mod}\, \neg K) \restriction (\text{first } n \text{ bits})).$$

Now let $H = L'$ and $K = \neg L''$. $\square$

The following function has a very general role in connecting uniform and nonuniform complexity bounds: see 3.2 below.

2.3 Definition. The function $\delta : \mathbb{N} \to \mathbb{N}$ is defined by $\delta(n) =$ least $m \geq 2$ such that every Δ-tautology of length $\leq n$ has an interpolant of length $\leq m$. $\square$

We refer to [9] for complexity measures on (non-) deterministic Turing machines. Given a set $S \subseteq \{0, 1\}^*$ we write $S \in \mathrm{P}$ (resp., $S \in \mathrm{NP}$) iff S is recognized in deterministic (resp., nondeterministic) polynomial Turing time. As usual, $S \in \mathrm{coNP}$ means that $\{0, 1\}^* \setminus S \in \mathrm{NP}$.

2.4 Lemma. *Let $S \subseteq \{0, 1\}^*$. Let function $T: \mathbb{N} \to \mathbb{R}$ have the property that S is recognized by a nondeterministic Turing machine within time $T(i)$, $i =$ input length. Then there is a function $G: \{1\}^* \to \Sigma^*$ which is computable by a deterministic Turing machine within time $T^8(i)$ for all sufficiently large $i \in \mathbb{N}$, and such that letting $G_n = G(1, 1, \ldots, 1)$, (n times), the following holds, for all $n \in \mathbb{N}^+$:*

$$|\mathrm{var}\, G_n| \geq n \quad \textit{and} \quad S \cap \{0, 1\}^n = \mathrm{Mod}\, G_n \restriction (\text{first } n \text{ bits}).$$

Proof. Almost verbatim from the proof of [8, Lemma 3] (upon replacing the number m therein with our $T(n)$ here). $\square$

3. From uniform to nonuniform upper bounds

We refer to [12] for background on (logical) circuits. All circuits considered in this paper are over the basis $\{\wedge, \vee, \neg\}$ and have a unique output node. For α a circuit, we let size(α) = number of nodes other than inputs, and depth(α) = length of the longest path in α. A circuit α with n inputs computes a uniquely determined boolean function $\hat{\alpha}:\{0,1\}^n \to \{0,1\}$. We say that α has fan out 1 iff each node, except input nodes, has exactly one edge directed away from it. Circuits will be denoted by α, ζ, and σ.

3.1. Theorem. *Let $S \subseteq \{0,1\}^*$ and $T:\mathbb{N} \to \mathbb{R}$. Assume S and its complement $S' = \{0,1\}^* \setminus S$ are recognized by nondeterministic Turing machines M and M' respectively, both within time $T(i)$, i = input length. Then there is a sequence of circuits $\{\sigma_n\}_{n \in \mathbb{N}^+}$ with the following properties:*

(i) *Each σ_n has fan out* 1 *and computes* (*the characteristic function of*) $S \cap \{0,1\}^n$.

(ii) $\text{Depth}(\sigma_n) \leq k \log_2 \delta(3T^8(n))$, *for some $k \in \mathbb{R}^+$ and for all $n \in \mathbb{N}^+$.*

Proof. Let for all n, G_n satisfy Mod $G_n \restriction$ (first n bits) $= S \cap \{0,1\}^n$ as in Lemma 2.4. Let similarly G'_n take care of $S' \cap \{0,1\}^n$. It is no loss of generality to assume that var $G_n \cap$ var G'_n = first n variables, in lexicographic order. By Proposition 2.2 we then have that $G_n \to \neg G'_n$ is a Δ-tautology for each $n \in \mathbb{N}^+$. By definition of δ (2.3) there is an interpolant I_n with $|I_n| \leq \delta(|G_n \to \neg G'_n|)$. Recalling, if necessary, the proof of Proposition 2.2, one sees that Mod $I_n = S \cap \{0,1\}^n$. Each boolean expression I_n canonically determines [12] a circuit α_n with fan out 1 over basis $\{\wedge, \vee, \neg\}$, with

$$\text{size}(\alpha_n) \leq |I_n| \leq \delta(|G_n \to \neg G'_n|) \leq \delta(3T^8(n))$$

for all sufficiently large $n \in \mathbb{N}$.

The last inequality is a consequence of the inequalities $|G_i|, |G'_i| \leq T^8(i)$ established in Lemma 2.4 for all sufficiently large $i \in \mathbb{N}$. By definition, α_n computes the characteristic function of $S \cap \{0,1\}^n$; thus α_n satisfies clause (i) above. By Spira's theorem [12, 2.3.3] we can replace α_n by a circuit σ_n still satisfying (i) and with the additional property that $\text{depth}(\sigma_n) \leq h \log_2(\text{size}(\alpha_n))$, with $h > 0$ independent of n. Therefore we have the inequality $\text{depth}(\sigma_n) \leq h \log_2 \delta(3T^8(n))$ for all sufficiently large $n \in \mathbb{N}$. By suitably choosing $k > 0$, we can now ensure that

$$\text{depth}(\sigma_n) \leq k \log_2 \delta(3T^8(n)) \quad \text{for all } n \in \mathbb{N}^+. \qquad \square$$

3.2. Remark. If, in particular, $S \in \mathrm{NP} \cap \mathrm{coNP}$, then S is computed by a sequence $\{\zeta_n\}$ of circuits with fan out 1 and $\text{depth}(\zeta_n) \leq k \log_2 \delta(n^p)$ for suitable positive numbers k, p only depending on S; this is just an instance of Theorem 3.1.

Following the best linguistic tradition of computation theory [4] we write:

$$\mathrm{NP} \cap \mathrm{coNP} \subseteq \bigcup_r \mathrm{DEPTH}(\log \delta(n^r)).$$

Similarly, the whole of Theorem 3.1 can be condensed into the following formula, upon noting that δ cannot be worse than exponential:

$$\mathrm{NTIME}(T) \cap \mathrm{coNTIME}(T) \subseteq \mathrm{DEPTH}(\log \delta(T^8)).$$

To justify the terminology of our next corollary, recall [4] that $S \subseteq \{0, 1\}^*$ has small circuits by definition iff some sequence of circuits $\{\zeta_n\}$ computes S and size(ζ_n) is bounded by a polynomial in n. Upon restriction to circuits of fan out 1 (called formulas in [12]) one may equivalently say that S is computed by a sequence $\{\zeta_n\}$ where depth(ζ_n) grows proportionally to $\log n$: indeed, for formulas, Spira's theorem holds [12, 2.3.3].

3.3. Corollary. *Assume δ is bounded above by a polynomial. Then every $S \in \mathrm{NP} \cap \mathrm{coNP}$ has small formulas, i.e. there is a sequence $\{\zeta_n\}_{n \in \mathbb{N}^+}$ of circuits, together with some $k \in \mathbb{R}^+$, such that for all $n \in \mathbb{N}^+$ we have:*

(i) *ζ_n has fan out 1 and computes $S \cap \{0, 1\}^n$.*

(ii) Depth$(\zeta_n) \leq k \log_2 n$.

Proof. Immediate from Theorem 3.1. □

3.4. Remarks. (i) Thus, in order to prove that δ is superpolynomial, it suffices to exhibit a set S in $\mathrm{NP} \cap \mathrm{coNP}$ which does not have small formulas; at present no such example is known, but one might try to investigate sets S related to the Transitive Closure operation [14] where elements of $\mathrm{NP} \cap \mathrm{coNP}$ are rather frequently encountered whose best *known* circuits only have $\log^2 n$ depth, or so.

(ii) For a weaker form of Corollary 3.3, also due to the author, see [7, 3.1] and references quoted therein. In the same paper one can also find a nontrivial lower bound on the (depth) complexity of interpolation in sentential logic.

(iii) Without the hypothesis that δ is bounded by a polynomial, one still can prove that every set in P has small circuits (generally with fan out > 1), see [12]. Indeed, Adleman [1] has extended this result to every set recognized in polynomial time by a randomizing Turing machine. Such results, as well as our Theorem 3.1 above, typically obtain a nonuniform upper bound as a consequence of a uniform upper bound. In the converse direction we shall prove Theorem 4.8 below. For further information see, e.g., [4].

4. From nonuniform to uniform bounds

Besides the length of Δ-interpolants, one can study the amount of time required to find them out; the following is a precise definition:

4.1. Definition. The set $\nabla \subseteq {}^{\mathbb{N}}\mathbb{R}$ is defined as follows: for any $T:\mathbb{N} \to \mathbb{R}$ we say that $T \in \nabla$ iff there is a function $\Psi: \Sigma^* \to \Sigma^*$ which is computable by a deterministic Turing machine within time $T(i)$, i = input length, such that for every $W \in \Sigma^*$, if W is a Δ-tautology, then $\Psi(W)$ is an interpolant for W. If ∇ contains no polynomials, then we say that Δ-interpolation is intractable. □

Thus, $T \in \nabla$ iff Δ-interpolants can be found within deterministic Turing time T. Clearly, if the function δ defined in 2.3 grows superpolynomially, then Δ-interpolation is intractable.

4.2. Theorem. *If* $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$, *then Δ-interpolation is intractable.*

For the proof it is sufficient to establish the following:

Lemma. *If Δ-interpolation is tractable* (*viz., not intractable*), *then every set* $S \in \mathrm{NP} \cap \mathrm{coNP}$ *has small formulas* $\{\zeta_n\}$ *as in Corollary* 3.3, *with the additional property that the map* $\langle 1, \ldots, 1\rangle$ (*n times*) $\mapsto \zeta_n \in \Sigma^*$ *is computable in deterministic polynomial time.*

Proof of Lemma. Same as the proof of Theorem 3.1: the circuit ζ_n determined by I_n therein can be identified with I_n; the ζ_n's can be written down, as words over Σ, in deterministic polynomial time, since by hypothesis and by Lemma 2.4 the Δ-interpolant I_n can be written down within deterministic time n^{8r}, for suitable $r \in \mathbb{N}^+$ independent of n. □

4.3. Example. By Theorem 4.2 if Δ-interpolation is tractable then, for instance, the set $\mathrm{PRIM} \subseteq \{0, 1\}^*$ of prime numbers in binary notation is in P: indeed, $\mathrm{PRIM} \in \mathrm{NP} \cap \mathrm{coNP}$, as observed in [10]. Alternatively, one can get $\mathrm{PRIM} \in \mathrm{P}$ assuming the Extended Riemann Hypothesis [6]. See [5] for further examples along these lines.

4.4. Corollary. *If* $\mathrm{P} \neq \mathrm{NP}$, *and* NP *is closed under complementation* (*i.e.*, $\mathrm{coNP} \subseteq \mathrm{NP}$), *then Δ-interpolation is intractable.*

Proof. Evidently, $\mathrm{coNP} \subseteq \mathrm{NP}$ iff $\mathrm{coNP} = \mathrm{NP}$. Then our hypotheses are to the effect that $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$. Now apply Theorem 4.2. □

4.5 Remark. A fortiori, if $\mathrm{P} \neq \mathrm{NP}$ and $\mathrm{coNP} \subseteq \mathrm{NP}$, then (full) interpolation in sentential logic is intractable [8].

4.6. Although the set ∇ arises from interpolation in sentential logic, elements of ∇ provide uniform upper bounds in terms of non-uniform upper bounds for the complexity of first-order theories, as shown by Theorem 4.8 below. We refer to

[2] for background on first-order logic, L. Assume τ is a finite type, i.e. a finite set of constant, relation and function symbols; denote by $L[\tau]$ the set of first-order sentences of type τ. Let $\Theta = \{\vartheta_1, \ldots, \vartheta_m\}$ be an arbitrary finitely axiomatizable theory which is complete in τ; in other words, $\vartheta_1, \ldots, \vartheta_m \in L[\tau]$, Θ has a model of type τ, and any two such models of Θ are elementarily equivalent. As usual, sentences of type τ, as well as proofs of theorems in Θ, are thought of as particular words over some reasonable finite alphabet Γ. Because of Gödel's completeness theorem, the completeness of Θ allows us to give the following:

4.7. Definition. For any theory Θ as above, the function $\lambda_\Theta : \mathbb{N} \to \mathbb{N}$ is defined by: $\lambda_\Theta(n) =$ least $m \in \mathbb{N}$ such that for every $\vartheta \in L[\tau]$ with $|\vartheta| \leq n$ there is $\Pi \in \Gamma^*$ with $|\Pi| \leq m$ such that either Π is a proof of ϑ in Θ, or Π is a proof of $\neg\vartheta$ in Θ. □

Note that $\lambda_\Theta(n) \geq n$. We let $\Theta \vDash \psi$ mean that $\psi \in L[\tau]$ and ψ is a theorem of Θ, i.e. there is a proof of ψ in Θ. The symbol $\circ$ means composition of functions.

4.8. Theorem. *Let Θ be a finitely axiomatizable first-order theory; assume Θ complete in the finite type τ. Then for each $T \in \nabla$ there are $p, q \in \mathbb{N}$, together with a deterministic Turing machine recognizing the set $\{\psi \in \Gamma^* \mid \Theta \vDash \psi\}$ within time $T^q \circ \lambda_\Theta^p$.*

Proof. Let $Y = \{\psi \in \Gamma^* \mid \Theta \vDash \psi\}$, and $Y' = \Gamma^* \setminus Y$. We shall write λ instead of λ_Θ. For any $\psi \in \Gamma^*$ we have: $\psi \in Y$ iff there is a proof $\Pi \in \Gamma^*$ of ψ in Θ with $|\Pi| \leq \lambda(|\psi|)$. By Gödel's theorem, Y is recognized by a nondeterministic Turing machine $M1$ within time, say, $(|\psi| + \lambda(|\psi|))^r$ for suitable $r \in \mathbb{N}$: machine $M1$ guesses a proof $\Pi \in \Gamma^*$, $|\Pi| \leq \lambda(|\psi|)$ and checks if Π is a proof of ψ in Θ; this latter operation requires (low-degree) deterministic polynomial time, as a consequence of our assumption concerning the finite axiomatizability of Θ. Since $\lambda(n) \geq n$, we see that $M1$ acts within time $(2\lambda(|\psi|))^r$. Similarly, for any $\varphi \in \Gamma^*$ we have, by the assumed completeness of Θ: $\varphi \in Y'$ iff either $\varphi \notin L[\tau]$, or there is a proof $\Pi \in \Gamma^*$ of $\neg\varphi$ in Θ, with $|\Pi| \leq \lambda(|\varphi|)$. Now the set of those $\varphi \in \Gamma^*$ which belong to $L[\tau]$ is recognized by a deterministic Turing machine $M2$ within time, say $|\varphi|^s$, for some $s \in \mathbb{N}$ (recall that τ is finite). Hence the set of those $\varphi \in \Gamma^*$ which are members of Y' can be recognized by a nondeterministic Turing machine $M3$ within time $[\lambda(|\varphi|)]^t$ for suitable $t \geq s$, as in the initial part of the present proof. In summary, sets Y and Y' can be recognized by nondeterministic Turing machines $M4$ and $M'4$ respectively, both within time λ^u, for suitable $u \in \mathbb{N}$. Using some reasonable 1–1 map β of Γ^* onto $\{0, 1\}^*$, and letting $S = \beta(Y)$, $S' = \beta(Y')$, one also sees that S and S' can be recognized by nondeterministic Turing machines $M5$ and $M'5$ respectively, both within time λ^v, for suitable $v \in \mathbb{N}$. Now by Lemma 2.4 there are functions $G, G' : \{1\}^* \to \Sigma^*$ which are computable by deterministic Turing machines $M6$ and $M'6$ respectively, both within time λ^h, for suitable $h \in \mathbb{N}$ (and for all $n \in \mathbb{N}^+$, if h is carefully chosen), and have the following properties, in the notation of Lemma 2.4: $|\text{var } G_n|$, $|\text{var } G'_n| \geq n$, $S \cap \{0,1\}^n = \text{Mod } G_n \upharpoonright$ (first n bits), $S' \cap \{0,1\}^n = \text{Mod } G'_n \upharpoonright$ (first n bits), for all $n \in \mathbb{N}^+$. Arguing as in the proof of Theorem 3.1, we may safely assume that var $G_n \cap$ var G'_n = first n variables, in lexicographic order; hence $G_n \to \neg G'_n$ is a Δ-tautology. Since our map T is assumed to be in ∇, there exists a deterministic Turing machine $M7$ which over input $G_n \to \neg G'_n$ outputs an interpolant I_n within time $T(|G_n \to \neg G'_n|)$. Since $|G_n|, |G'_n| \leq \lambda^h(n)$, then for suitable $i \in \mathbb{N}$ we can say that $M7$ outputs I_n within time $T(\lambda^i(n))$. Regarding now each I_n as a circuit σ_n with fan out 1 we have that σ_n computes the characteristic function of $S \cap \{0,1\}^n$, and σ_n, as a word in Σ^*, can be written down within deterministic time $T(\lambda^i(n))$. Consider now the following deterministic Turing machine $M8$ accepting S: over input $x = \langle x_1, \ldots, x_n \rangle \in \{0,1\}^*$, $M8$ first writes down I_n; subsequently $M8$ simulates the computation of circuit σ_n over input $\langle x_1, \ldots, x_n \rangle$, as in the familiar circuit-value operation.

For suitable $j, k \in \mathbb{N}^+$ we can say that $M8$ accepts S within time $T^j(\lambda^k(n))$. Consider finally the following deterministic Turing machine $M9$ accepting Y: over input $\psi \in \Gamma^*$, $M9$ first writes down the binary version $\beta(\psi)$ of ψ, then $M9$ simulates $M8$ over input $\beta(\psi)$. For suitable $p, q \in \mathbb{N}^+$ we can conclude that $M9$ decides whether ψ is a member of Y within time $T^q(\lambda^p(|\psi|))$. $\square$

4.9. Remarks. (i) Thus, starting from a nonuniform upper bound λ_Θ on proof length in Θ, one gets via T a uniform upper bound on the deterministic Turing time complexity of the decision procedure for Θ. Note in particular that if Δ-interpolation turns out to be tractable, then T can be a polynomial, and the decision procedure for Θ has deterministic Turing time bounded by a power of the λ_Θ function.

(ii) Theorem 4.8 still holds, with the same proof, if L is replaced by any formal system [13], or logic [3] where sentences and proofs are finite strings of symbols, the analogue of Gödel's completeness theorem holds, and the predicate "Π is a proof of ϑ in Θ" is decidable within deterministic polynomial time (for Θ a finite and complete set of axioms using a finite set of nonlogical symbols). For further information see [13, p. 36] and references therein.

References

[1] L. Adleman, Two theorems on random polynomial time, in: Proc. 19th IEEE Symp. Foundations of Computer Science (1978) 75–83.

[2] C.C. Chang and H.J. Keisler, Model Theory (North-Holland, Amsterdam, 2nd ed., 1977).

[3] S. Feferman, Applications of many-sorted interpolation theorems, in: Proc. Tarski Symp., AMS Proc. Symp. in Pure Math. 25 (1974) 205–223.

[4] R.M. Karp and R.J. Lipton, Turing machines that take advice, in: Logic and Algorithmic, Internat. Symp. in Honour of E. Specker, L'Enseignement Mathématique, Université de Genève (1982) 255–273.

[5] K.L. Manders, Computational complexity of decision problems in elementary number theory, in: Model Theory of Algebra and Arithmetic, Lecture Notes in Math. 834 (Springer, Berlin, 1980) 211–227.
[6] G.L. Miller, Riemann's hypothesis and tests for primality, J. Comput. System Sci. 13 (1976) 300–317.
[7] D. Mundici, A lower bound for the complexity of Craig's interpolants in sentential logic, Archiv. Math. Logik 23 (1983) 27–36.
[8] D. Mundici, NP and Craig's interpolation theorem, in: Logic Colloquium 82 (North-Holland, Amsterdam, 1984) 345–358.
[9] M. Machtey and P. Young, An Introduction to the General Theory of Algorithms (North-Holland, Amsterdam, 3rd printing, 1979).
[10] V. Pratt, Every prime has a succinct certificate, SIAM J. Comput. 4 (1975) 214–220.
[11] W.L. Ruzzo, On uniform circuit complexity, J. Comput. System Sci. 22 (1981) 365–383.
[12] J.E. Savage, The Complexity of Computing (Wiley, New York, 1976).
[13] A.O. Slisenko, Complexity problems in computational theory, Russian Math. Surveys 36 (6) (1981) 23–125.
[14] M. Tompa, Two familiar transitive closure algorithms which admit no polynomial time sublinear space implementations, SIAM J. Comput. 11 (1) (1982) 130–137.