Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Daniele Mundici

Δ-tautologies, uniform and non-uniform upper bounds in computation theory

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **75** (1983), n.3-4, p. 99–101.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1983_8_75_3-4_99_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1983.

RENDICONTI

DELLE SEDUTE

DELLA ACCADEMIA NAZIONALE DEI LINCEI

Classe di Scienze fisiche, matematiche e naturali

Ferie 1983 (Settembre-Ottobre)

(Ogni Nota porta a pie' di pagina la data di arrivo o di presentazione)

SEZIONE I

(Matematica, meccanica, astronomia, geodesia e geofisica)

Logica matematica. — *Δ-tautologies, uniform and non-uniform upper bounds in computation theory.* Nota (*) di DANIELE MUNDICI, presentata dal Socio G. ZAPPA.

RIASSUNTO. — Una Δ–tautologia è una tautologia del tipo $H \to K$ avente un solo interpolante di Craig J, a meno di equivalenza logica. Utilizzando misure di complessità relative al problema di trovare tale J, mostriamo come si possano ottenere limiti non uniformi di complessità mediante limiti uniformi, e viceversa.

See [1] for background on the syntax and semantics of sentential and first-order logic, [3] for complexity measures on (non) deterministic Turing machines, and [10] for (logical) circuits. Regard boolean expressions as particular words over (i.e., finite strings of symbols from) the alphabet $\Sigma = \{\wedge, \vee, \neg,), (, X, 0, 1\}$. The symbols 0 and 1 are used in subscripts of variable symbols; thus, for example, X0, X1, X0010 are variable symbols; the other symbols of Σ are used according to the familiar syntactical rules of sentential logic. For $W \in \Sigma^*$ a word over Σ, the length of W is the number of occurrences of symbols in W. A Δ-tautology in sentential logic is a tautology of the form $H \to K$ having precisely one Craig interpolant, up to logical equivalence; this terminology is suggested by Abstract Model Theory, where Δ-interpolation plays a central role [2]. The function $\delta : \mathbf{N} \to \mathbf{N}$ is defined by $\delta(x) =$ least $y \in \mathbf{N}$ such that every Δ-tautology of length $\leq x$ has an interpolant of length $\leq y$. $\{0, 1\}^*$ is the set of words over the alphabet $\{0, 1\}$. Given a set $E \subseteq \{0, 1\}^*$ we write $E \in P$ if E is accepted in deterministic polynomial Turing time; NP is the same, for nondeterministic time [3]. $E \in co\,NP$ means $\{0, 1\}^* \setminus E \in NP$. As usual, **N** and **R** are the sets of natural and real numbers, respectively, and $\mathbf{N}^+ = \mathbf{N} \setminus \{0\}$.

(*) Pervenuta all'Accademia il 17 settembre 1983.

THEOREM 1. *Given arbitrary* $E \subseteq \{0,1\}^*$ *and* $T : \mathbf{N} \to \mathbf{R}$, *assume both* E *and* $\{0,1\}^* \setminus E$ *are accepted within non-deterministic Turing time* T. *Then* E *is computed by circuits* $\{\eta_n\}_{n \in \mathbf{N}^+}$ *with fan out* 1 *such that depth* $(\eta_n) \leq$ $\leq k \log_2 \delta(3\, T^8(n))$ *for some* $k \in \mathbf{R}$, *for all* $n \in \mathbf{N}^+$.

For a proof of Theorem 1 see [7]. As an immediate corollary, if $E \in NP \cap$ $\cap\, co\,NP$ then E is computed by circuits $\{\eta_n\}$ with fan out 1 and depth $(\eta_n) \leq$ $\leq k \log_2 \delta(n^p)$ for suitable $k, p > 0$. Define the set $\nabla \subseteq {}^{\mathbf{N}}\mathbf{R}$ by $T \in \nabla$ iff there is a function $J : \Sigma^* \to \Sigma^*$ which is computable within deterministic Turing time T, such that whenever $L \in \Sigma^*$ is a Δ-tautology, J(L) is an interpolant for L.

THEOREM 2. *If* $P \neq NP \cap co\,NP$ *then* ∇ *contains no polynomial.*

For a proof see [7]. As an application of Theorem 2, if ∇ happens to contain a polynomial, then using a result of [9] we have that the set of prime numbers in binary notation is in P. Alternatively, one can reach the same conclusion assuming the Extended Riemann Hypothesis [5], instead of our assumption about ∇. See [4] for further applications along these lines.

As a corollary of Theorem 2 one can prove that if $P \neq NP$ and $co\,NP \subseteq NP$ then (full) interpolation in sentential logic is polynomially intractable [6]. Finding tight bounds for the complexity of (Δ) interpolation in sentential logic is an interesting problem of computation theory. See [8] for a non-trivial lower bound on depth complexity.

Now let Λ be a finite alphabet such that sentences and proofs in first-order logic are words over Λ. For any finitely axiomatizable first-order theory Ψ which is complete in the finite type τ, define $\lambda_\Psi : \mathbf{N} \to \mathbf{N}$ by $\lambda_\Psi(x) =$ least $y \in \mathbf{N}$ such that for every sentence φ of type τ and length $\leq x$ there is $\Pi \in \Lambda^*$ having length $\leq y$ such that either Π is a proof of φ in Ψ, or Π is a proof of $\neg\varphi$ in Ψ. The set of Theorems of Ψ is the set of sentences φ of type τ such that there is a proof of φ in Ψ.

THEOREM 3. *For any finitely axiomatizable first-order theory* Ψ, *complete in the finite type* τ, *and for any* $T \in \nabla$, *the subset of* Λ^* *given by the theorems of* Ψ *is recognized within deterministic Turing time* $T^q \circ \lambda_\Psi^p$, *for suitable* $p, q \in \mathbf{N}$.

For a proof see [7]. Theorem 3 canonically provides a (uniform) upper bound on the deterministic time complexity of the decision procedure for Ψ, given any $T \in \nabla$ together with a (non-uniform) upper bound λ_Ψ for proof length in Ψ. One can replace first-order logic in Theorem 3 by any logic [2], or formal system [11] where the analogue of Gödel's completeness theorem holds, and the predicate "Π is a proof of φ from the axioms $\psi_1, \ldots, \psi_n$" is decidable within deterministic polynomial time.

REFERENCES

[1] CHANG C.C. and KEISLER H.J. (1977) – *Model Theory*. North-Holland, Amsterdam, second edition.

[2] FEFERMAN S. (1974) – *Applications of many-sorted interpolation theorems*. In: Proceedings Tarski Symposium, « AMS Proc. Symp. Pure Math. », *25*, 205-223.

[3] MACHTEY M. and YOUNG P. (1979) – *An Introduction to the General Theory of Algorithms*. North-Holland, Amsterdam, third printing.

[4] MANDERS K.L. (1980) – *Computational complexity of decision problems in elementary number theory*. Springer « Lecture Notes in Mathematics », *834*, 211-227.

[5] MILLER G.L. (1976) – *Riemann's hypothesis and tests for primality*, « Journal of Computer and System Sciences », *13*, 300-317.

[6] MUNDICI D. (1984) – NP *and Craig's interpolation theorem*. In: Logic Colloquium 1982, North-Holland, Amsterdam, to appear.

[7] MUNDICI D. (1984) – *Tautologies with a unique Craig interpolant, uniform vs. nonuniform complexity*, submitted for publication.

[8] MUNDICI D. (1983) – *A lower bound for the complexity of Craig's interpolants in sentential logic*, « Archiv math. Logik », *23*, 27-36.

[9] PRATT V. (1975) – *Every prime has a succinct certificate*, « SIAM J. Computing », *4*, 214–220.

[10] SAVAGE J.E. (1976) – *The Complexity of Computing*. Wiley, New York.

[11] SLISENKO A.O. (1981) – *Complexity problems in computational theory*, « Russian Math. Surveys », *36*, 23-125.