Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Daniele Mundici

Craig's interpolation theorem, in computation theory

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **70** (1981), n.1, p. 6–11.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1981_8_70_1_6_0>

Logica matematica. — *Craig's interpolation theorem in computation theory.* Nota di DANIELE MUNDICI, presentata (*) dal Socio G. ZAPPA.

RIASSUNTO. — Si espongono alcuni risultati, provati dall'Autore negli articoli citati nella bibliografia, a proposito della complessità del teorema d'interpolazione di Craig: con ciò si intende la relazione tra la lunghezza (cioè il numero di simboli) della formula χ e la lunghezza di φ e ψ, ove $\varphi \to \psi$ è un'implicazione valida, e χ è un interpolante, come esibito dal teorema di interpolazione stesso. Si intende altresì sottolineare la rilevanza dello studio della complessità dell'interpolazione per far luce su alcuni importanti problemi della teoria degli algoritmi, con particolare riferimento al problema della complessità dei sistemi naturali di deduzione nella logica delle proposizioni (essenzialmente, problema PNP), oppure il problema di correlare tra loro diverse misure della complessità di una funzione, ad esempio, il tempo occorrente ad una macchina di Turing per calcolare la funzione, rispetto al tempo occorrente ad un circuito « logico ».

1. INTRODUCTION

Craig's interpolation theorem [5] yields, for any valid implication $\varphi \to \psi$ an *interpolant*, i.e. a sentence χ such that both $\varphi \to \chi$ and $\chi \to \psi$ are valid, but χ only uses the primitive notions (viz. the non logical symbols, or the boolean variables in sentential logic) which jointly occur in φ and ψ.

Craig's interpolation theorem is widely reputed to be one of the central tools in logic, see, e.g. [17], [2], [7] for sentential, intuitionistic and first-order logic, see [6], [9], [8] for abstract logic; for one more aspect of interpolation, see the final comments of [10].

In [11] and [12] the present author inaugurated the study of the complexity of Craig's interpolation theorem, i.e. the study of how fast the length $\|\chi\|$ of interpolant χ grows as a function of the length of φ and ψ.

This, too, turns out to be an interesting aspect of interpolation, having a direct relevance for some problems of computation theory, such as (*i*) relating different measures of complexity, e.g., Turing time and network complexity, or (*ii*) evaluating the complexity of " natural " deduction systems for sentential logic.

In addition, the examples of short valid first-order implications $\varphi \to \psi$ given in [11], whose interpolants are all too long to be practically written down, found an application in [13] to the study of the unfeasibility of certain logical operations, in the light of the limitations imposed on computer performance by such natural laws as the Heisenberg uncertainty rule.

(*) Nella seduta del 16 gennaio 1981.

This note is organized as follows: in section 2 we state the results concerning the complexity of Craig's interpolation theorem in first-order logic, proved in [11].

In section 3 we deal with sentential logic, in the light of [11] and of [12]. In section 4 we finally discuss the above mentioned problems of computation theory in the light of the complexity of Craig's interpolation theorem in sentential logic.

For the necessary background in computation theory the reader might consult, e.g., [1], [15] or [14].

2. THE LENGTH OF FIRST-ORDER INTERPOLANTS

In [11], we proved the following result, to the effect that the length $\|\chi\|$ of first-order interpolant χ (i.e. the number of occurrences of symbols in χ) grows faster than any elementary recursive function (see [7]):

2.1 THEOREM. *Let* $m = 1, 2, \cdots$; *then we can write down a valid first-order implication* $\varphi \to \psi$ *with* $\|\varphi\|, \|\psi\| < 1100 + 15\,m$ *such that, whenever* χ *is any interpolant, then*

$$\|\chi\| > 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} \Big\uparrow \text{height } 2m+1 .$$

For the proof of this theorem we used a non-rectangular matrix with m rows of rapidly growing length, together with an Ehrenfeucht-game argument. Notice that already for $m = 3$ we get a very short implication whose interpolants are all impossibly long. In [13] this example found application in a discussion on the practical unfeasibility of logical operations.

If one only takes care of sufficiently long implications $\varphi \to \psi$ then the above result can be strengthened, to the effect that the asymptotic growth of the length of χ, although bounded by some Π_1-function, grows faster than every Σ_1-function (in the arithmetical hierarchy, see [7]) of $\|\varphi\| + \|\psi\|$, as proved in [11]; as a matter of fact, we have:

2.2 THEOREM. *We can give an account of a* Π_1*-function* C *giving an upper bound on the complexity of Craig's interpolation in first-order logic, i.e.*

(*) whenever $\varphi \to \psi$ is valid, then there is an interpolant χ with

$$\|\chi\| \leq C(\|\varphi\| + \|\psi\|) .$$

On the other hand, no Σ_1*-function is able to give an upper bound in the sense of* (*).

To obtain the upper bound, we use Craig's linear deductions in [5] (see also [17]); to obtain our lower bound, see [19, Theorem 1].
The above upper bound is due to J. Mycielski (Private Communication). The present author had previously found a Δ_2-bound.

3. The length of sentential interpolants

The complexity of Craig's interpolation in sentential logic was first studied by the present author in [11] and [12]; in the following section this topic will be shown to be related to some of the deepest problems in computation theory. An exponential upper bound for the length of interpolants was given in [11], as follows:

3.1 Theorem. *For any valid implication* $\varphi \to \psi$ *in sentential logic, an interpolant* χ *can always be found with*

$$\|\chi\| \leq -11 + 6 \cdot 2^{(\|\varphi\| + \|\psi\| + 6)/8}.$$

As for lower bounds, the following theorem (Theorem 2.5 in [12]) gives the first known nontrivial result concerning the (delay) complexity of interpolation; see [15] for the necessary background:

3.2 Theorem. *For infinitely many* $d \in \mathbf{N}$ *(and starting with some* $d \leq 620$*) there is a valid implication* $\varphi \to \psi$ *in sentential logic, with both* φ *and* ψ *having their delay complexity smaller than* d*, such that any interpolant* χ *has a delay complexity greater than* $d + (1/3) \cdot \log_2 (d/2)$.

3.3 *Remark.* Intuitively, the above theorem means that the time required by the fastest network to compute χ (viz. to decide if a sequence of 0's and 1's satisfies χ) may be greater than the time needed to compute φ or ψ, even if χ may happen to have a much smaller number of variables: this is by no means a trivial fact.

4. Applications to computation theory

Problem. Does there exist a polynomial p such that for any valid implication $\varphi \to \psi$ in sentential logic one can find an interpolant χ with $\|\chi\| \leq p(\|\varphi\| + \|\psi\|)$?

In other words, does the length of sentential interpolants grow polynomially? Notice that Theorem 3.1 only gives an exponential upper bound. This turns to be a difficult problem, which has deep connexions with some important problems of computation theory, namely the PNP problem (or rather, its variant for " natural " proof systems), and the relationship between Turing time and delay complexity (or formula size) of boolean functions. We refer the reader to [1], [3], [4], [14], [16], [17], [18] for the necessary background.

The following discussion is intended to show that, whatever the answer of the above problem, one will be able to draw from the latter interesting consequences in computation theory. For $f : \{0, 1\}^\infty \to \{0, 1\}$ we let f_n

be the restriction of f to $\{0,1\}^n$, where $\{0,1\}^\infty = \{0,1\} \cup \{0,1\}^2 \cup \cup \{0,1\}^3 \cup \cdots$; thus f_n is the restriction of f to inputs of length n.

4.1 THEOREM. *Adopt the above notation; assume the length of interpolants grows polynomially: then for any function f such that there is a Turing machine* M *computing each* f_n *in time polynomial in n, there also exists a sequence of circuits* $N_1, N_2, \cdots, N_n, \cdots$ *with* N_n *computing* f_n, *and such that*

$$\text{depth}(N_n) \leq c \cdot \log_2 n \qquad (\textit{for some } c > 0, \textit{ for all } n > 1).$$

In other words, any function f wich can be computed in time T polynomial in the size of the input, also can be computed by circuits of depth proportional to $\log_2 T$.

Proof. By a Cook-like simulation argument (see [3], [1] or [15]) there exist polynomials r, s such that for any n there is a boolean sentence $\varphi(x_1, \cdots, x_n, x_{n+1}, \cdots, x_{r(n)})$ with $\|\varphi\| \leq s(n)$, such that, for any sequence

$$\mathbf{b} = b_1, \cdots, b_n, b_{n+1}, \cdots, b_{r(n)}$$

of bits (i. e. each b_i is either 0 or 1), we have that

$$\mathbf{b} \models \varphi$$

iff **b** is a binary encoding of the record of a computation by M of input $b_1, \cdots, b_n$, with $f(b_1, \cdots, b_n) = 1$.

Here $\models$ is the familiar satisfaction symbol.

Letting now similarly M′ compute in polynomial time function $f' = 1 - f$, there are polynomials r', s' such that for any n there is a boolean sentence $\varphi'(x_1, \cdots, x_n, x'_{n+1}, \cdots, x'_{r'(n)})$ with $\|\varphi'\| \leq s'(n)$ such that for any sequence of bits

$$\mathbf{b}' = b_1, \cdots, b_n, b'_{n+1}, \cdots, b'_{r'(n)}$$

we have that

$$\mathbf{b}' \models \varphi'$$

iff **b′** is a binary encoding of the record of a computation by M′ of input $b_1, \cdots, b_n$, with $f'(b_1, \cdots, b_n) = 1$.

Notice that if $b_1, \cdots, b_n, b_{n+1}, \cdots, b_{r(n)}, b'_{n+1}, \cdots, b'_{r'(n)} \models \varphi \wedge \varphi'$, then $f(b_1, \cdots, b_n) = 1 = f'(b_1, \cdots, b_n)$ which is impossible.

Therefore $\varphi \wedge \varphi'$ is inconsistent, so that $\varphi \to \neg \varphi'$ is valid. Let

$$\psi = \neg \varphi'.$$

Let χ be any interpolant for the valid implication $\varphi \to \psi$ as given by Craig's interpolation theorem: then $\varphi \to \chi$ and $\chi \to \psi$ are both valid, and the only variables of χ are $\{x_1, \cdots, x_n\}$. If $f(b_1, \cdots, b_n) = 1$ then $b_1, \cdots, b_n$ can be expanded to a model of φ, hence $b_1, \cdots, b_n \models \chi$ (since $\varphi \to \chi$); on the other hand, if $f(b_1, \cdots, b_n) = 0$, then $b_1, \cdots, b_n$ can be expanded to a model of φ' hence to a model of $\neg \psi$, so that $b_1, \cdots, b_n \models \neg \chi$ (since $\neg \psi \to \neg \chi$). In definitive we get

$$b_1, \cdots, b_n \models \chi \qquad \text{iff} \quad f(b_1, \cdots, b_n) = 1.$$

Notice that $\|\varphi\|, \|\psi\|$ are both bounded by a polynomial in n, hence, by our assumption about the growth of interpolants, also $\|\chi\|$ is bounded by some polynomial in n. Now

notice that the formula size of f_n is $\leq \|\chi\|$, hence, by Spira's result (see [18], [15] or [14]) the depth of f_n is bounded by some linear function of $\log_2 n$; by our assumption about the Turing time T for f, we also have that the depth of f_n is bounded by some linear function of $\log_2 T$. QED.

4.2 *Remark.* Thus, if the length of interpolants turned out to grow polynomially, then, e.g., the Transitive Closure (TC) of an $n \times n$ boolean matrix (which is well known to be Turing computable in time polynomial in n) would be computable by circuits of depth proportional to $\log_2 n$, while every *known* circuit for this problem has depth growing faster than $(\log_2 n)^2$. Conversely, from a proof that the depth of (*any possible* circuits for) TC cannot grow proportionally to $\log_2 n$, one could infer the superpolynomial complexity of formula size for TC, hence, by Theorem 3.1 above, the superpolynomial complexity of Craig's interpolation in sentential logic. This, in turn, may be used to obtain information about the (non) existence of "natural" deduction systems for sentential calculus, as follows:

First of all, let us make precise our naturality requirement; intuitively, if D is a proof system for sentential logic (see [4]), we can obtain from D another proof system D′ only dealing with sentences of the form $\varphi \rightarrow \psi$: such sentences have the advantage that (*i*) if the implication is valid, then, by Craig's interpolation theorem, we have an interpolant, while (*ii*) if the implication is not valid, then we can find a counterexample, i.e. a sequence of bits which satisfies φ but does not satisfy ψ. Thus we are led to require that, in order that D′ be "natural", D′ at least is able to process $\varphi \rightarrow \psi$ by giving either a counterexample or an interpolant, rather than a mere "yes" or "no", concerning the validity of $\varphi \rightarrow \psi$.

This motivates the following:

4.3 DEFINITION. We say that Turing machine M gives a *Craig deduction system* for sentential logic iff M, when placed on any input of the form $\varphi \rightarrow \psi$, will eventually halt after yielding one of the following two pieces of information:

(*i*) either a sequence **b** of bits such that $\mathbf{b} \models \varphi$ and $\mathbf{b} \models \neg \psi$

(*ii*) or an interpolant χ for the implication $\varphi \rightarrow \psi$.

Concerning Craig deduction systems we have:

4.4 THEOREM. *Assume that the size of sentential interpolants grows superpolynomially or even, in the light of Theorem 4.1, assume that there is a boolean function f which can be computed in Turing time* T *polynomial in the length of the input, but has no circuit with depth proportional to* $\log_2 T$. *Then there does not exist any Craig deduction system for sentential logic, operating in polynomial time.*

Proof. If the size of interpolants grows superpolynomially, then the conclusion is trivial: just apply Definition 4.3. If f can be computed in polynomial Turing time but has no circuits for f_n with depth proportional to $\log_2 T$ (i. e., proportional to $\log_2 n$), then by Theorem 4.1 the size of interpolants grows superpolynomially. Now argue as in the first part to get the conclusion. QED

4.5 *Remark.* Returning to the initial problem of this section, today two cases are possible: (1) the size of interpolants grows polynomially, and then each function computable in polynomial Turing time T is also computable by circuits of depth proportional to $\log_2 T$, or (2) interpolants grow superpolynomially, and then there is no efficient Craig deduction system for sentential logic. Both conclusions are interesting for computation theory.

REFERENCES

[1] A. V. AHO, J. E. HOPCROFT and J. D. ULLMAN (1974) – *The design and analysis of computer algorithms*, Addison–Wesley, Reading, Mass.

[2] J. L. BELL, M. MACHOVER (1977) – *A course in mathematical logic*, North–Holland, Amsterdam.

[3] S. A. COOK (1971) – *The complexity of theorem proving procedures*, « Proc. Third ACM Symposium », 151–158.

[4] S. A. COOK and R. A. RECHKOW (1979) – *The relative efficiency of propositional proof systems*, « J. Symb. Logic », *44.1*, 36–50.

[5] W. CRAIG (1957) – *Linear reasoning. A new form of the Herbrand-Gentzen theorem*, « J. Symb. Logic », *22*, 250–268.

[6] S. FEFERMAN (1974) – *Two notes on abstract model theory*, I, « Fund. Math. », *82*, 153–165, and II, *ibid. 89* (1975) 111–130.

[7] J. D. MONK (1976) – *Mathematical Logic*, Springer–Verlag, Berlin.

[8] D. MUNDICI (1981) – *Robinson's consistency theorem in soft model theory*, « Transactions of the AMS », *263*, 231–241.

[9] D. MUNDICI (1982) – *Compactness = JEP in any logic*, « Fund. Math. », to appear.

[10] D. MUNDICI (1981) – *A group-theoretical invariant for elementary equivalence and its role in representations of elementary classes*, « Studia Logica », to appear.

[11] D. MUNDICI – *Complexity of Craig's interpolation*, to appear.

[12] D. MUNDICI – *A lower bound for the complexity of Craig's interpolants in sentential logic*, « Archv für math. Logik », to appear.

[13] D. MUNDICI (1980) – *Natural limitations of algorithmic procedures in logic*, « Rendiconti Accademia Nazionale Lincei », *69*, 101–105.

[14] M. S. PATERSON (1976) – *An introduction to Boolean function complexity*, « Soc. Math. de France », Astérisque *38–39*, 183–201.

[15] J. E. SAVAGE (1976) – *The complexity of computing*, Wiley, New York.

[16] C. P. SCHNORR (1976) – *The network complexity and the Turing machine complexity of finite functions*, « Acta Informatica », *7*, 95–107.

[17] R. M. SMULLYAN (1971) – *First-order Logic*, Springer–Verlag, Berlin.

[18] P. M. SPIRA (1971) – *On time-hardware complexity tradeoffs for Boolean functions*, Proc. 4th Hawaii Int. Symp. on System Sciences, 525–527.

[19] H. FRIEDMAN (1976) – *The complexity of explicit definitions*, « Advances in Math. », *20*, 18–29.