EXTRACTA MATHEMATICAE Vol. 7, Núm. 1, 35 – 37 (1992)

Lower Bounds for Parallel Arithmetic Computations [1]

J.L MONTAÑA AND L.M. PARDO [2]

Dpto. de Matemáticas, Estadística y Computación, Facultad de Ciencias
Universidad de Cantabria, 39071 *Santander, Spain*

AMS *Subject Class.* (1980): 03D15, 68Q15, 65V05 *Received February* 11, 1992

Arithmetic networks over a field K (see [5]) are *arithmetic circuits*, using inputs, constants from the ground field K, gates from $\{+,-,*,/\}$, boolean gates $\{\vee,\wedge\}$ with inputs in $\{\mathbf{T},\mathbf{F}\}$, selections gates and *sing* gates, of the $sing(a,\triangle)$, that ouputs a boolean value according to whether the sing of a agrees with $\triangle$, where:

i) If our field K is an algebraically closed field, the sing condition $\triangle \in \{=,\neq\}$.

ii) If our field K is a real closed field or $K=\mathbb{Q}$, the sing condition $\triangle \in \{>,=,<\}$.

When dealing with arithmetic circuits -that use only arithmetic gates-, it was shown in [6] that the degree of the rational function they compute is a lower bound for its depth. This is not the case for arithmetic networks, as it was shown in [5], where a nice counterexample is exhibited. For general infinite fields, one can use the "thick-degree" -the maximum of the degrees in the Zariski dense pieces- as lower bound. For algebraically closed fields, a "$log_2 log_2(degree)$" lower bound can be given (see [5]).

Now, for K algebraically closed, let us consider the set

$$V = \bigcup_{n\in\mathbb{N}} \{x \in K : x^{2^n} = 1\} .$$

Let f be the characteristic function of the above set. Applying [5], the best lower bound one can get for the depth of any arithmetic network that computes f is $log_2 n$, since the thick degree is constant. Nevertheless, it seems quite reasonable that this function cannot be solved by any "*polylog*" depth parallel algorithm. Our following analysis of lower bounds shows, in particular, that this problem can not be solved in less than $\sqrt{n}$ parallel steps.

---

[1] KEYWORDS: parallel complexity, algebraic complexity theory, semialgebraic set, arithmetic networks.

[2] Partially supported by DGICYT PB 89/0379.

For any field K and any constructible set W over K denote by $\beta_K(W)$ the number of (semialgebraic) connected components of W if K is a real closed field or the number of connected components with non-empty interior of the euclidean closure of W in $\mathbb{R}^n$ if K is the field of the rational numbers. If K is an algebraically closed field containing the rationals then $\beta_K(W)$ denotes the number of connected components of $W \subset \mathbb{R}^{2n}$.

Assume N is an arithmetic network that evaluates a function

$$\phi : K^n \longrightarrow K^m \times \{\mathbf{F},\mathbf{T}\}^\nu .$$

Write $\phi = (\phi^A, \phi^B)$ where ϕ^A denotes its arithmetic part and ϕ^B denotes the boolean one. For $(x,y) \in K^2$ say $\Delta(x,y) = \mathbf{T}$ if $x - y = 0$ and $\Delta(x,y) = \mathbf{F}$ otherwise. For $(\epsilon,\delta) \in \{\mathbf{F},\mathbf{T}\}^m \times \{\mathbf{F},\mathbf{T}\}^\nu$ define the set

$$W(\epsilon,\delta) = \{(x,y) \in K^n \times K^m : (\Delta(y_i - \phi_i^A(x)), \phi_i^B(x)) = (\epsilon_i,\delta_i)\} .$$

THEOREM. *The depth of N is in the class*

$$\Omega\left[\sqrt{\frac{log_2(\sup_{\epsilon,\delta} \beta_K(W(\epsilon,\delta)))}{n+m}} - log_2(m+\nu)\right].$$

The length of an input $x \in K^*$ is the index of the last non-zero coordinate, i.e. $length(x) = length(x_1,\ldots,x_n,\ldots) = n$, where n is the last non-zero coordinate of x. The elements of K^* of length n can be identified with the subset of K^n with $x_n \neq 0$.

Assume K is either an algebraically closed field or a real closed field or $K = \mathbb{Q}$, NC_K is the class of subsets of K^* recognized by sequences of arithmetic networks with polylogarithmic depth and a polynomial number of processors (in the input length).

Assume K is an algebraically closed field or a real closed field. The class P_K is the class of all those arithmetic problems over K that can be accepted by a *BSS*-machine over K within time polynomial on the input length (see [2]).

COROLLARY. *For a field K either algebraically closed of characteristic zero or real closed, there is an arithmetic problem in P_K, which is not in NC_K. Moreover, this arithmetic problem can be choosen universal (i.e. its description does not depend on the ground field).*

DEFINITION. i) The class $P_{\mathbb{Q}}$ is the class of all arithmetic problems over $\mathbb{Q}$ accepted by a *BSS*-machine within cost polynomial in the input size (see [2]).

ii) The class $GP_{\mathbb{Q}}$ (*genuinely polynomial time over* $\mathbb{Q}$) is the class of all arithmetic problems over $\mathbb{Q}$ accepted by a rational *RAM* within time (uniform cost) polynomial in the input length.

COROLLARY. *There is an arithmetic problem over* $\mathbb{Q}$ *in* $P_{\mathbb{Q}} \cap GP_{\mathbb{Q}}$ *which is not in* $NC_{\mathbb{Q}}$.

COROLLARY. *There is a language* $\mathcal{L} \subset \mathbb{Q}^*$, *such that* $\mathcal{L} \in P$ *and* $\mathcal{L} \notin NC_{\mathbb{Q}}$.

Assume K a real closed or algebraically closed field of characteristic zero. When speaking about K we consider the first order language L together with the non-logic symbols $\{a : a \in \mathbb{Q}\}, +, -, \times, =$. In the real closed case one also includes the relational symbol "$>$" (see [3] and [4] for the complete details).

COROLLARY. *The quantifier elimination in the elementary theory of* K *is simply exponential in parallel time.*

Recall that the "Knapsack problem" is: Given $(x_1, \ldots, x_n)$ decide whether there is $S \subset \{1, \ldots, n\}$ satisfying $\sum_{i \in S} x_i = 1$. Lower bounds for the sequential arithmetical complexity of this last problem can be found in [1].

COROLLARY. *Any parallel machine needs time at least* $\Omega(\sqrt{n})$ *to solve the "Knapsack problem". In particular the "Knapsack problem" is in* $NP_{\mathbb{R}} \setminus NC_{\mathbb{R}}$.

ACKNOWLEDGEMENT

The authors would like to thank Joos Heintz for suggesting the application of the lower bounds obtained to simplify the analysis of the parallel time of quantifier elimination.

REFERENCES

1. BEN-OR, M. "Lower bounds for algebraic computation trees", A.C.M. 15th Symp. on Theory of Computing, pp. 80–86, 1983.
2. BLUM, L., SHUB, M. AND SMALE, S. On a theory of computation and complexity over the real numbers: *NP*-completeness, recursive functions and universal machines, *Bulletin of the A.M.S.* **21**(1) (1989), 1–46.
3. DAVENPORT, J.H. AND HEINTZ, J. Real quantifier elimination is doubly exponential, *J. of Symbolic Computation* **5** (1988), 29–36.
4. FITCHAS, N., GALLIGO, A. AND MORGENSTERN, J. "Algorithmes rapides en séquentiel et en parallele pour l'élimination de quantificateurs en géométrie élémentaire", Seminaire de Structures Algebriques Ordennes, Université de Paris VII, 1987.
5. VON ZUR GATHEN, J. "Parallel arithmetic computations: a survey", Mathematical Foundations on Computer Science, 13th Proc. MFCS, 1986.
6. KUNG, H.T. "New algorithms and lower bounds for the parallel evaluation of certain rational expressions and recurrences", *J. ACM* **23** (1976), 534–543.