ON THE PARALLEL EVALUATION OF MULTIVARIATE POLYNOMIALS

Laurent HYAFIL
IRIA-LABORIA
Domaine de Voluceau
78150 - Le Chesnay
FRANCE

Abstract :

We prove that any multivariate polynomial P of degree d that can be computed with C(P) multiplications-divisions can be computed in O(log d.log C(P)) parallel steps and O(log d) parallel multiplicative steps.

1. Introduction

We prove that any multivariate polynomial P of degree d that can be computed with C(P) multiplications-divisions can be computed in O(log d.log C(P)) parallel steps and O(log d) parallel multiplicative steps. This result has to be compared with the best known lower bound of max(log d, log C(P)). (See for instance [1] for exposition).

If we apply this result to the parallel inversion of a matrix nxn, it shows the existence of an algorithm in $O(\log^2 n)$ parallel steps : the inverse of a matrix nxn is a set of quotients of polynomials of degree $\le$ n and of complexity $O(n^{2,81})$ (determinants). Such a result was already known by a constructive method ([2]).

2. Definitions

- For $R_1, R_2 \ldots R_m \in K(x_1, x_2 \ldots x_n)$, $C^*(R_1, R_2 \ldots R_m)$ will denote the minimum number of scalar multiplications-divisions necessary to compute $R_1, R_2 \ldots R_m$ given $K \cup \{x_1, x_2 \ldots x_n\}$.

- A program β will be called homogeneous of degree d if :

a) For any additive operation of β, $P_i = Q_i \pm R_i$ then Q_i and R_i are homogeneous polynomials of degrees $\le$ d.

b) β has no division

c) For any multiplication $P_i = Q_i x R_i$ of β, Q_i and R_i are homogeneous and the degree of P_i is $\le$ d.

- If $P_1, P_2, \ldots, P_m \in K[x_1, x_2 \ldots x_n]$, $C_d(P_1, P_2 \ldots P_m)$ will denote the minimum number of non scalar multiplications necessary to compute $P_1, P_2 \ldots P_m$ with an homogeneous program of degree d.

3. Statement of the results

Theorem 1

Let H be an homogeneous program computing homogeneous polynomials in n indeterminates $P_1, P_2 \ldots P_m$ of degrees $\le$ d with $C_d(P_1, P_2 \ldots P_m)$ multiplications.

There exist two sets of homogeneous polynomials :

- $U(H) = (U_i)$ for $1 \le i \le I$ where $I \le n + C_d(P_1, P_2 \ldots P_m)$;
- $V(H) = (V_{i,j})$ for $1 \le i \le I$ and $1 \le j \le \lambda$ where λ is the number of operations of H, satisfying :

a) $\frac{d}{3} \le \deg(U_i) \le \frac{2d}{3}$ for $1 \le i \le I$.

b) $\deg(V_{i,j}) \le \frac{2d}{3}$ for $1 \le i \le I$, $1 \le j \le \lambda$.

c) If H computes f_i $(1 \le i \le \lambda)$ and $\frac{d}{3} \le \deg(f_i) \le d$ then $f_i = \sum_{j=1}^{I} U_j V_{j,i}$

d) $C_d(U_i) \le C_d(P_1, P_2 \ldots P_m)$ for $1 \le i \le I$

e) $C_d(V_{i,j}) \le C_d(P_1, P_2 \ldots P_m)$ for $1 \le i \le I$, $1 \le j \le \lambda$.

Proof :

Let $L(P_1, P_2 \ldots P_m)$ be the minimal number of operations of an homogeneous program which computes $P_1, P_2 \ldots P_m$ with $C_d(P_1, P_2 \ldots P_m)$ multiplications.

The proof is on induction on $L(P_1,P_2\ldots P_m)$.

The case $L(P_1,P_2\ldots P_m)=0$ being obvious assume theorem 1 is true for $L(P_1,P_2\ldots P_m) \le \lambda$ and consider a set of polynomials $P_1,P_2\ldots P_m$ such that $L(P_1,P_2\ldots P_m)=\lambda+1$.

The homogeneous program H which computes $P_1,P_2\ldots P_m$ in $\lambda+1$ operations has a last operation which can be assumed to be $P_1=f\circ f'$ without loss of generality. Let H' denote the program H without this last operation.

We denote by V_j and V'_j for $1\le j\le I$ polynomials of $V(H')$ corresponding to f and f' :

- if $\deg(f) \ge \frac{d}{3}$ then $f=\sum_{j=1}^{I} U_jV_j$
- if $\deg(f') \ge \frac{d}{3}$ then $f'=\sum_{j=1}^{I} U_jV'_j$.

Case 1 : $P_1=f+f'$

We first show that

$$C_d(P_1,P_2\ldots P_m)=C_d(f,f',P_2\ldots P_m).$$

It is obvious that

$$C_d(f,f',P_2\ldots P_m) \le C_d(P_1,P_2\ldots P_m).$$

Assume $C_d(f,f',P_2\ldots P_m) < C_d(P_1,P_2\ldots P_m)$. Since we can obviously build an homogeneous program which computes $P_1,P_2\ldots P_m$ in $C_d(f,f',P_2\ldots P_m)$ multiplications, we have a contradiction.

Since $C_d(f,f',P_2\ldots P_m)=C_d(P_1,P_2\ldots P_m)$ then $L(f,f',P_2\ldots P_m)=\lambda$ and we can apply the induction hypothesis to $f,f',P_2\ldots P_m$ obtaining two sets of polynomials $U(H)$ and $V(H')$ satisfying the above conditions a to e.

Since the last operation of H is $P_1=f+f'$ and $P_1=\sum_{j=1}^{I} U_j(V_j+V'_j)$ we can define $U(H)$ and $V(H)$ from $U(H')$ and $V(H')$ by :

- $U(H)=U(H')$
- $V(H)=V(H') \cup \{V_{j,\lambda+1} \mid \text{for } 1\le j\le I\}$, where $V_{j,\lambda+1}=V_j+V'_j$ for $1\le j\le I$.

It is obvious to check that $U(H)$ and $V(H)$ satisfy the above conditions a to e.

Case 2 : $P_1=fxf'$

It is obvious that

$$C_d(P_1,P_2\ldots P_m) \le C_d(f,f',P_2\ldots P_m)+1$$

and since if $C_d(P_1,P_2\ldots P_m) < C_d(f,f',P_2\ldots P_m)+1$ was true an immediate contradiction would appear, we have $C_d(P_1,P_2\ldots P_m)=C_d(f,f',P_2\ldots P_m)+1$ and $L(f,f',P_2\ldots P_m)=\lambda$. We can apply the induction hypothesis to $f,f',P_2\ldots P_m$ obtaining two sets of polynomials $U(H')$ and $V(H')$ satisfying the above conditions a to e.

- α) $\deg(P_1) < \frac{d}{3}$.

If we take $U(H)=U(H')$ and $V(H)=V(H')\cup\{V_{j,\lambda+1} \mid 1\le j\le I\}$ where $V_{j,\lambda+1}=0$ for $1\le j\le I$, $U(H)$ and $V(H)$ obviously satisfy the above conditions a to e.

- β) $\deg(f) \ge \frac{d}{3}$.

$P_1=fxf'=\sum_{j=1}^{I} U_j(V_j\ f')$, and if we choose $U(H)=U(H')$ and $V(H)=V(H')\cup\{V_{j,\lambda+1} \mid 1\le j\le I\}$ where $V_{j,\lambda+1}=V_j\ f'$ for $1\le j\le I$, $U(H)$ and $V(H)$ obviously satisfy conditions a to d. To establish condition e, we use the induction hypothesis :

$$C_d(V_j) \le C_d(f,f',P_2\ldots P_m) \quad \text{for } 1\le j\le I.$$

Hence $C_d(V_j\ f') \le C_d(f,f',P_2\ldots P_m)+1$ and

$$C_d(V_j\ f') \le C_d(P_1,P_2\ldots P_m).$$

- γ) $\deg(f') \ge \frac{d}{3}$

Same proof than in β permuting f and f'.

- δ) $\deg(f) < \frac{d}{3}$ and $\deg(f') < \frac{d}{3}$.

We have $\frac{d}{3} \le \deg(P_1) \le \frac{2d}{3}$.

We take $U(H)=U(H')\cup\{U_{I+1}\}$ with $U_{I+1}=P_1$. $I+1$ satisfies : $I+1 \le n+C_d(P_1,P_2\ldots P_m)$ since we know $I \le n+C_d(f,f',P_2\ldots P_m)$ and $C_d(f,f',P_2\ldots P_m)=C_d(P_1,P_2\ldots P_m)-1$. We take $V(H)=V(H')\cup\{V_{j,\lambda+1} \mid 1\le j\le I\}\cup\{V_{I+1,k} \mid 1\le k\le\lambda+1\}$ with $V_{I+1,\lambda+1}=1$ and $V_{i,j}=0$ for $i=I+1$ and $j\ne\lambda+1$ or $i\ne I+1$ and $j=\lambda+1$. With such a choice $U(H)$ and $V(H)$ satisfy conditions a to e. □

In order to establish Theorem 2 we first show :

Lemma 1

Let P be an homogeneous polynomial of degree $\leq d$ in n indeterminates, then P can be computed in :

$\frac{1}{\log_2 3-1}\log_2 d$ parallel multiplicative steps,

$\frac{\log_2 d}{\log_2 3-1}\left(\lceil \log_2[C_d(P)+n]\rceil+1\right)$ parallel steps.

Proof

The proof is by induction on d. For d = 1, the proof is trivial. Assume it is true for d' < d, and we prove it for d' = d.

From theorem 1 we know that :

$P=\sum_{j=1}^{I} U_j V_j$ with $I \leq n+C_d(P)$ and U_j and V_j are homogeneous polynomials which satisfy for $1 \leq j \leq I$:

a) $\deg(U_j) \leq \frac{2d}{3}$.

b) $\deg(V_j) \leq \frac{2d}{3}$.

c) $C_d(U_j) \leq C_d(P)$,

d) $C_d(V_j) \leq C_d(P)$.

Applying the induction hypothesis shows that U_j and V_j $(1 \leq j \leq I)$ can be computed in less than :

$\frac{1}{\log_2 3-1}\log_2(\frac{2d}{3})$ parallel multiplicative steps

$\frac{\log_2(\frac{2d}{3})}{\log_2 3-1}\left(\lceil \log_2[C_d(P)+n]\rceil+1\right)$ parallel steps.

To compute P, we compute in parallel U_j and V_j for $1 \leq j \leq I$ mulitply U_j by V_j in one parallel multiplicative step and sum up in

$\lceil \log_2(I)\rceil \leq \lceil \log_2[n+C_d(P)]\rceil$ additive steps.

Summing the total number of steps gives the announced result to compute P. □

Lemma 2

Let P be a multivariate polynomial of degree d and $P_1, P_2 \ldots P_d$ the homogeneous terms of P then :

$$C_d(P_1,P_2\ldots P_d) \leq [\frac{d(d-1)}{2}]^2\, C^*(P)$$

Proof :

The proof given in [3] consists in first eliminating division using Strassen's transformation ([4]) then in separating homogeneous components in every intermediary result. □

Theorem 2

A polynomial P of degree $\leq d$ in n indeterminates which can be computed with $C^*(P)$ multiplications-divisions can be computed with no more than :

$\left\lceil [\frac{1}{\log_2 3-1}]\log_2 d\right\rceil$ parallel multiplicative steps

$\left\lceil \frac{\log_2 d}{[\log_2 3-1]}\right\rceil \left\lceil \log_2\left[(\frac{d(d-1)}{2})^2\, C^*(P)+n\right]+1\right\rceil + \lceil \log_2 d\rceil$

parallel steps.

Proof :

To compute P in parallel, we compute in parallel each of the d homogeneous components of P : $P_1, P_2 \ldots P_d$ and then add them in parallel in $\lceil \log_2 d\rceil$ additive steps. The result is then deduced immediately from lemmas 1 and 2. □

4. References

[1] Borodin, A. and Munro, I. "The computational complexity of algebraic and numeric problems", American Elsevier, 1975.

[2] Csanky, L. "Fast parallel matrix inversion" 15th Symposium F.O.C.S. Proc., 1975, 11-12.

[3] Hyafil, L. "The power of commutativity", 18th F.O.C.S. Conference Proc., pp.171-174,1977.

[4] Strassen, V. "Vermeidung von divisionen", J. Revue Angew. Math., vol. n° 264, pp. 184-202, 1973.

5. Aknowledgements

Many thanks to A. Borodin for helpful corrections on the first draft of this paper.