Bestell-Nr: A06558533X lok.Nr:
PPN: 021838194
Bestelldatum 20-12-2005-11:14

GBV-direkt-BESTELLUNG

normal

Tel: 0228/402252

Voelzmann-Scheiding, Anke
MPI fuer Mathematik -Bibliothek-
Vivatsgasse 7
DE-53111 Bonn

Mail: library@mpim-bonn.mpg.de
Fax: 0228/402277

USER-GROUP-1

Kontaktperson

Kunden-/Zugangsnummer
3737153353

Lieferbibliothek:
Staats- und Universitätsbibliothek
Bremen
Bibliothekstraße
D-28359 Bremen

Tel. +49 (0421) 218-3622 (Fr. Fregin), Fax: -2040
E-Mail : fernleihe@suub.uni-bremen.de

Sammelrechnung
Rechnungsanschrift
Voelzmann, Anke
MPI fuer Mathematik -Bibliothek-
Vivatsgasse 7
53111 Bonn

Lieferschein / delivery note

odb. Nr. 98 /__________
Datum / date __________

Lieferung einer Aufsatzkopie per / delivery of article by

Post /mail E-Mail /ARIEL Fax

Eildienst / express delivery

________Kopien / copies

Fernleihe eines Buches - einer Mikroform / lending of book - microform

Wir berechnen für unsere Lieferung / price DM __________

Rechnung folgt - Bitte veranlassen Sie erst dann eine Zahlung, wenn die Rechnung bei Ihnen eingetroffen ist.

Bills are mailed every three months or according to arrangements.

Verfasser: (Aufsatz) Grigoriev

Titel: (Aufsatz) Multiplicative complexity of a bilinear form over a commutative ring

Seiten: 281-286

Standort: 01.f.7003/

Band Heft

Jahrgang 1981-00-00

Titel (Monographie/ Zeitschrift)

Mathematical foundations of computer science 1981 : proceedings, 10th symposium, Berlin [u.a.] Springer

Lieferform: PDF

Lieferart: E-Mail alt. Post

Lieferung erwünscht bis: 23-12-2005

A06558533X

Bemerkungen:

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

118

Mathematical Foundations of Computer Science 1981

Proceedings, 10th Symposium
Štrbské Pleso, Czechoslovakia
August 31 - September 4, 1981

Edited by J. Gruska and M. Chytil

Springer-Verlag
Berlin Heidelberg New York 1981

Editors
Jozef Gruska
Computer Research Centre
Dúbravská 3, 885 31 Bratislava, Czechoslovakia

Michal Chytil
Faculty of Mathematics and Physics, Charles University
Malostranské náměsti 25, 118 00 Praha, Czechoslovakia

CR Subject Classifications (1974): 5.1, 5.2, 5.3.

ISBN 3-540-10856-4 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-10856-4 Springer-Verlag New York Heidelberg Berlin

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2145/3140-543210

MULTIPLICATIVE COMPLEXITY OF A BILINEAR FORM OVER A COMMUTATIVE RING

D.Yu.Grigor'ev

Leningrad Branch of Mathematical V.A.Steklov Institute of Academy of Sciences of the USSR, Fontanka 27, Leningrad, 191011, USSR.

Abstract. We characterize the class of Noetherian commutative rings K such that the multiplicative complexity of a bilinear form over K coincides with its rank. The asymptotic behaviour of the multiplicative complexity of bilinear forms from one special class over the polynomial rings is described, and in particular it is shown that there is no finite upper bound for the difference between the multiplicative complexity of a bilinear form from this class and the rank of this form. The relationship between the multiplicative complexity of a bilinear form over a ring K and homological properties of the ring is explained.

Introduction

Multiplicative complexity of a set of bilinear forms is a very intensively investigated subject in algebraic computational complexity theory (see for instance book [1] and references there). Sometimes instead of a bilinear form we speak about the coefficient matrix of the form. The multiplicative complexity of a set of bilinear forms is defined to be the least number of two-argument multiplications and divisions to be performed in the straight-line computations (containing the arithmetic instructions) which evaluate the set of bilinear forms under consideration. It is proved in [2],[3] that the multiplicative complexity of a set of bilinear forms with coefficient matrices $A_1,\dots,A_\ell$ equals to the rank Rg of this set defined in the following manner:

$Rg(A_1,\dots,A_\ell) = \min\{R:$ $A_1,\dots,A_\ell$ are contained in the linear span of some matrices $C_1,\dots,C_R$ each of which can be presented as a product of a column by a row $\}$.

Multiplicative complexity (or rank $Rg_F(A_1,\dots,A_\ell)$) depends on a choice of a field F when $\ell>1$, but we omit an index F when there is no danger of misunderstanding.

In the previous papers on the multiplicative complexity, only the case in which the matrices $A_1,\dots,A_\ell$ were defined over some field F was considered. The most interesting results in this subject were the discovery of upper bounds for the multiplicative complexity of a set of bilinear forms corresponding to the problem of (1) matrix multiplication (see [4]) and (2) polynomial multiplication (see [5] for the case of an infinite field F and [6] for the case of a finite field F). Obviously $Rg_F(A)$ is equal to the usual rank of the matrix A. Already the determination of the multiplicative complexity of a pair of matrices presents difficulties and only for the case of an algebraically closed field F was the implicit formula for $Rg_F(A,B)$ obtained in [7] and [8] (independently). Concerning the problem of investigating the rank from a general point of view, we mention also that in [9] the group of all linear transformations (over a field) preserving rank is characterized.

The present paper is apparently the first to treat the subject of multiplicative complexity in a more general setting, over a commutative ring rather than over a field. There are new difficulties to be overcome here. In fact here problems arise already when we attempt to evaluate the multiplicative complexity of a set consisting of only a single bilinear form. So we will limit our treatment to this case. In this case the definition of the multiplicative complexity yields the following equality :

$$Rg_K(A) = \min\{R : A = u_1 \otimes v_1 + \dots + u_R \otimes v_R \text{ for some columns } u_1,\dots,u_R \text{ and rows } v_1,\dots,v_R\}.$$

We have found that the multiplicative complexity is closely connected with some homological properties of the ring K (see §§ 1,2).

We mention one interpretation of the multiplicative complexity $Rg_K(A)$ in the case when $K = F[x_1,\dots,x_d]$ is a ring of polynomials over a field F and when $A = x_1A_1 + \dots + x_dA_d$ where each A_i $(1 \le i \le d)$ is a matrix over F (we shall say that such matrix A is <u>square free</u>). Obviously $Rg_K(A) \le Rg_F(A_1,\dots,A_\ell)$. The rank $Rg_K(A)$ can be interpretated as the multiplicative complexity of a bilinear form A with parametric coefficients running over a d-dimensional linear variety. Consideration of multiplicative complexity over a ring (rather than over its field of quotients) ensures that the straight-line computation for calculating a given bilinear form is a correct one (i.e. does not require divisions by zero) for any values which may be assigned to the parameters $x_1,\dots,x_d$.

§ 1. Multiplicative complexity of a bilinear form over a ring and the rank of the form.

For every $n \times m$ matrix A over a commutative (with the unity) ring K we denote by $rg\, A$ the usual rank of A which is equal to the greatest size of the minors (of A) distinguished from zero. For proving of the main theorem of §1 the following reformulation of $Rg_K(A)$ is useful. Let $K^m \supset M$ be the module of the rows of A (K^m is the free module of dimension m). Then $Rg_K(A)$ equals to the least number of generators of the modules M_1 such that $M \subset M_1 \subset K^m$. Obviously $\min\{n,m\} \geqslant Rg_K(A) \geqslant rg\, A$. A noetherian commutative ring K is called <u>Rg-ring</u> if $Rg_K(A) = rg\, A$ for every matrix A over K . All the necessary information from the theory of rings and the homological algebra can be found in [11].

THEOREM 1. A ring K is Rg-ring iff

1) $K = K_1 \oplus \cdots \oplus K_t$ for some integral domains $K_i (1 \leqslant i \leqslant t)$;

2) global homological dimension of the ring K (we denote it by $gldh(K)$) is not greater than 2;

3) every projective K_i -module is free ($1 \leqslant i \leqslant t$).

The proof of the theorem is exposed in [10] and consists of two stages. At the first stage the existence of the decomposition $K = K_1 \oplus \cdots \oplus K_t$ for Rg -ring K is proved with the help of the following lemma.

LEMMA 1. Let K be Rg-ring and K_S be its full quotient ring. Then K_S is a direct sum of some fields.

The second stage consists in proving of the theorem for the case when K is an integral domain, basing on the following lemma.

LEMMA 2. An integral domain K is Rg-ring iff for every K -module $M \subset K^m$ vanishing of the torsion submodule of the factor-module K^m/M entails that M is free.

COROLLARY 1. a) $F[x,y]$ is Rg-ring (F denotes a field here and further);

b) If K is a local ring and $gldh(K) \leqslant 2$ then K is Rg-ring;

c) If $gldh(K) = d \leqslant 2$ and K is an integral domain then $Rg_K(A) \leqslant rg\, A + d$ for each matrix A over K (in particular if K is some Dedekind domain then $Rg_K(A) \leqslant rg\, A + 1$).

Analogously the following problem can be put: to characterize the class of integral domains K such that an equality $Rg_K(A_1,\ldots,A_\ell) = Rg_F(A_1,\ldots,A_\ell)$ is fulfilled for every set of matrices $A_1,\ldots,A_\ell$ over

K where F is the quotient field of K (cf. the theorem 1). It is not difficult to show that under such condition $K=F$.

We define the direct sum $A\oplus B$ of the matrices A,B as the matrix $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. We demonstrate that Rg_K (in distinction from rg) is not an additive function relatively to the operation of the direct sum of matrices over K for some (Dedekind) rings K. Set, for example, $K=\mathbb{Z}[\sqrt{5}]$, $A=\begin{vmatrix} \sqrt{5}-1 & 2 \\ 2 & \sqrt{5}+1 \end{vmatrix}$, and $A_p=A\oplus\cdots\oplus A$ is the direct sum of p copies of A. Then $rg\,A_p=p$ and therefore $Rg_K(A_p)<p+1$ by force of the item c) of the corollary 1. From the other hand it can be easily seen that $Rg_K(A)=2$. Meanwhile the author conjectures that the additivity of Rg_K is valid for the case when $K=F[x_1,\dots,x_d]$.

§2. Multiplicative complexity of a square free bilinear form

We assume in the present paragraph that $K=K_d=F[x_1,\dots,x_d]$ and A (with some indices or without them) is a square free $m\times n$ matrix.

LEMMA 3. ([10]) $Rg_K(A)=\min\{m+n-rg\,V-rg\,W\}$ where minimum is taken over such paires of matrices V, W with their entries in F that $VAW=0$.

COROLLARY 2. $Rg_K(A_1\oplus A_2)=Rg_K(A_1)+Rg_K(A_2)$ (cf. the example at the and of §1).

Set $R^d(\tau)=\sup\limits_{rg A=\tau} Rg_{K_d}(A)$ and $R(\tau)=\sup\limits_{d} R^d(\tau)$.

COROLLARY 3. $R^d(\tau_1+\tau_2)\geqslant R^d(\tau_1)+R^d(\tau_2)$, $R(\tau_1+\tau_2)>R(\tau_1)+R(\tau_2)$.

LEMMA 4. $R^d(\tau)\leqslant \tau+\left[\frac{\tau}{2}\right]+\left[\frac{\left[\frac{\tau}{2}\right]}{2}\right]+\cdots<2\tau$ (if we denote by s_i the i^{th} item of the considered sum then $s_{i+1}=\left[\frac{s_i}{2}\right]$) where the number of the items in the sum equals to $d-1$ ($\tau\geqslant 1$, $d\geqslant 2$, $[e]$ is the entier of e).

This lemma can be ascertained (see [10]) by the induction on d and τ (the base of the induction consisting in the equality $R^2(\tau)=\tau$ is valid by the item a) of the corollary 1).

COROLLARY 4. $R^3(\tau)=\left[\frac{3}{2}\tau\right]$.

THEOREM 2. $\lim_{\tau\to\infty} \frac{R(\tau)}{\tau} = 2$.

The existence of the limit follows from the corollary 3, the upper bound for the limit is a consequence of the lemma 4. We construct a set of matrices $\{A_{s,t}\}_{s,t\geq 1}$ such that $\mathrm{rg}\, A_{s,t} = \binom{s+t-2}{s-1}$, $Rg_{K_{s+t-1}}(A_{s,t}) = \min\left\{\binom{s+t-1}{t}, \binom{s+t-1}{s}\right\}$ (see [10]), the matrix $A_{s,t}$ is of the size $\binom{s+t-1}{t} \times \binom{s+t-1}{s}$ and $A_{s,t}$ has its entries in the ring $K_{s+t-1} = F[x_1,\dots,x_{s+t-1}]$. ($\binom{a}{b}$ is a binomial coefficient). This construction will complete the proof of the theorem because $\frac{Rg_{K_{2t-1}}(A_{t,t})}{\mathrm{rg}\, A_{t,t}} \xrightarrow[t\to\infty]{} 2$.

Set $s\times 1$ column $A_{s,1}$ equal to $(x_s, -x_{s-1}, \dots, (-1)^{s-1} x_1)^T$ and $1\times t$ row $A_{1,t}$ equal to $(x_1,\dots,x_t)$ for each $s,t \geq 1$ .Then we define by recursion

$$A_{s+1,t+1} = \begin{vmatrix} A_{s+1,t} & x_{s+t+1} E \\ 0 & -A_{s,t+1} \end{vmatrix}$$

where E is the unity matrix.

REMARK. Observe that for every fixed $p\geq 1$ the matrices $\{A_{s,t}\}_{s+t=p+1}$ are the maps in Koszul complex of the ring $K = K_p$ relatively to the set of elements $\{x_1,\dots,x_p\}$:

$$0 \to K^1 \xrightarrow{A_{1,p}} K^p \cdots K^{\binom{p}{t}} \xrightarrow{A_{p+1-t,t}} K^{\binom{p}{t-1}} \cdots K^p \xrightarrow{A_{p,1}} K^1 \to 0$$

In conclusion the author conjectures that for each regular ring K $\sup_B \frac{Rg_K(B)}{\mathrm{rg}\, B} < \infty$.

Acknowledgments. I would like to thank A.A.Suslin for useful discussions and A.O.Slisenko for attention.

References

1. Borodin A., Munro M. The computational complexity of algebraic and numeric problems. Ser.Th.of Comput.,Amer.Elsev.,N.Y.,1975.
2. Winograd S. On the number of multiplications necessary to compute certain functions. Communs Pure Appl.Math.,1970,vol.23, p.165-179.
3. Strassen V. Vermeidung von Divisionen. J.reine angew.Math.,1973, B.264,S.184-202.
4. Schönhage A. Partial and total matrix multiplication. Prepr.University Tubingen,1980.
5. Fiduccia C.M., Zalcstein Y. Algebras having linear multiplicative complexity. J.Assoc.Comput.Mach.,1977,vol.24,№ 2,p.311-331.
6. Grigor'ev D.Yu. Multiplicative complexity of a pair of bilinear forms and of the polynomial multiplication. Lect.Notes Comput. Sci.,1978,vol.64,p.250-256.
7. Grigor'ev D.Yu. Some new bounds on tensor rank. Prepr. LOMI E-2-78,Leningrad,1978.
8. Ja'Ja' J. Optimal evaluation of pairs of bilinear forms. Proc. 10-th Ann.ACM Symp.Th.Comput.,San-Diego,California,1978,p.173-183.
9. Grigor'ev D.Yu. Algebraic computational complexity of a set of bilinear forms. Journal of Computational Mathematics and Mathematical Physics,1979,vol.19,№ 3,p.563-580 (in Russian).
10. Grigor'ev D.Yu. Relation between the rank and the multiplicative complexity of a bilinear form over a Noetherian commutative ring. Notes of Scientific Seminars of Leningrad Branch of Mathematical Institute of Academy of Sciences of the USSR,1979,vol.86,p.66-81 (in Russian).
11. Maclane S. Homology. Springer-Verlag,1963.