Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

228

Applied Algebra, Algorithmics and Error-Correcting Codes

2nd International Conference, AAECC-2
Toulouse, France, October 1–5, 1984
Proceedings

Edited by Alain Poli

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo

Editor

Alain Poli
AAECC/LSI Lab., Université P. Sabatier
118, route de Narbonne, 31062 Toulouse Cédex, France

CR Subject Classifications (1985): B.4.5, G.2.0

ISBN 3-540-16767-6 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-16767-6 Springer-Verlag New York Berlin Heidelberg

Printed in Germany

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

PREFACE

The International Colloquium on Applied Algebra and Error Correcting Codes was born in Toulouse (France) in June 1983.

The acts of AAECC-1 are published in Discrete Mathematics (vol 56 n°2-3, Oct.85). The acts of AAECC-2 are contained in this volume.

From 48 talks, we have selected 23 accepted papers, after a (time consuming) system of multiple reviews. I thank those referees who agreed to contribute to the obtained result.

I also thank :

- Mr. A. Oisel and CII-HBull for their financial support,
- Mr. M. Combarnous Scientific Director of CNRS*, for CNRS's financial support,
- Mr. A. Dargent, Director of CNES** Informatic Center, for allowing us the use of the computers before and during the conference,
- The LSI laboratory and University P. Sabatier for their financial support.

As one knows, digitalized data are becoming increasingly important, particularly for transmissions.
For satellite transmissions, the CCSDS (Consultative Committee for Data Space System) had proposed a coding system for international transmissions (see : final report of contract AAECC/CNES n° 84/5417, 1985 (210 pages)).
Also, the target of RACE project is to define and realize a Broadband-IBC european network with security/privacy (cryptography) and reliability (error-correcting codes). AAECC lab. is a participant for the definition phase (in group n°2015).

As digitalized data are being more and more used for images/speech/files transmissions, theoretical tools and practical developments are necessary (for finite algebraic structures and for complexity analyses).
In particular, decomposition of algebras is an interesting topic because it is used for problems involved with complexity (see J. Heintz/J. Morgenstern), for constructive results on idempotents, multivariate codes (see : A. Poli, H. Imai, A. Poli/C. Rigoni), for DFT's problems (see : T. Beth). Many other particular aspects of re-

* CNRS Centre National de la Recherche Scientifique
** CNES Centre National d'Etudes Spatiales (18 Av. BELIN - 31055 TOULOUSE Cédex)

search are developed in this book. Covering radius (G. Cohen/N.J.A. Sloane/A.C. Lobstein, H.F. Mattson Jr., L. Huguet/M. Griera), constructions/automorphisms of codes (J.A. Thiong Ly, J.L. Dornstetter, D.A. Leonard/C.A. Rodger, B. Courteau/J. Goulet), practical aspects of codes (M.C. Gennero, G.L. Feng/K.K. Tzeng), polynomials (P.Piret, D. Lugiez, O. Moreno de Ayala), applied algebra (H.M. Möller/F. Mora, L. Beneteau/J. Lacaze, A. Astie-Vidal/J. Chiffiot), cryptography (P. Camion), computer algebra (J. Calmet, J. Calmet/M. Bergman).

* AAECC Conferences essentially deal with Applied Algebra, Algorithmic and Error Correcting Codes.

The future scheduled AAECC conferences are :

- AAECC-3 (1985, Grenoble (F), Prof. J. Calmet)
- AAECC-4 (1986, Karlsruhe (D), Prof. Dr. T. Beth)
- AAECC-5 (1987, Barcelona (SP), Dr. L. Huguet)
- AAECC-6 (1988, Pisa (I), Prof. A. Miola)
- AAECC-7 (1989, Toulouse (F), Prof. A. Poli)
- AAECC-8 (1990, Yokohama (J), Prof. H. Imai)

We hope that AAECC Conferences, and particularly this Lecture Notes volume, will contribute to the important development of data transmissions.

Finally, a thank you to participants, authors, and also to Miss S. Watson (Springer Verlag Computer Science Editorial) for her patience and very kind help. A particular thanks to the series editors who have accepted this publication.

May 1986 Alain POLI

CONTENTS

ON ASSOCIATIVE ALGEBRAS OF MINIMAL RANK

Joos Heintz[1] and Jacques Morgenstern[2]

[1] Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET)
Universidad Nacional de La Plata
La Plata, Provincia Buenos Aires, Argentina
and
Johann Wolfgang Goethe - Universität, Fachbereich Mathematik
Robert Mayer - Strasse 6 - 10
D - 6000 Frankfurt/Main, FRG (mailing address)

[2] Université de Nice, Institut des Mathématiques et Sciences Physiques
Parc Valrose
F - 06034 Nice Cedex, France
and
INRIA, Sophia Antipolis
F - 06560 Valbonne, France

1. Introduction

In the sequel let k be a field and A an associative k-algebra with unity, of finite dimension over k. We denote the radical of A, the maximal (two-sided) nilpotent ideal contained in A, by $\operatorname{rad} A$.

A quadratic algorithm (for A) is a finite family

$$\beta = ((u_\rho, v_\rho, w_\rho) \in (A \times A)^* \times (A \times A)^* \times A \ ; \ \rho = 1, \dots, R)$$

satisfying $xy = \sum_{\rho=1}^{R} u_\rho(x,y)\, v_\rho(x,y)\, w_\rho$, $\forall\ x,y \in A$.

(Here $(A \times A)^*$ denotes the dual space of the k-vector space $A \times A$.)

Special cases of quadratic algorithms are the bilinear algorithms (for A) which have the form $\beta = ((u_\rho, v_\rho, w_\rho) \in A^* \times A^* \times A \ ; \ \rho = 1, \dots, R)$ with

$$(1) \qquad xy = \sum_{\rho=1}^{R} u_\rho(x)\ v_\rho(y)\ w_\rho \quad , \ \forall\ x,y \in A \ .$$

(Note that $t := \Sigma\, u_\rho \otimes v_\rho \otimes w_\rho \in A^* \otimes_k A^* \otimes_k A$ is the tensor of the multiplication of the algebra A and hence doesn't depend on the particular algorithm β.)

For $\beta = ((u_\rho, v_\rho, w_\rho);\ \rho = 1, \ldots, R)$ a quadratic or bilinear algorithm we call $L(\beta) := R$ the complexity of β. We define the following invariants of A :

$L(A) := \min\{L(\beta);\ \beta$ quadratic algorithm for $A\}$, the complexity of A and

$R(A) := \min\{L(\beta);\ \beta$ bilinear algorithm for $A\}$, the rank of A.

It is well known ([17]) that $L(A)$, the complexity of A, can be interpreted as the computational complexity of multiplying two generic elements of A.

Furthermore, we have $L(A) \leq R(A) \leq 2\,L(A)$.

So, for asymptotic complexity considerations, L and R are equivalent notions. This fact has widely been used for the construction of fast matrix multiplication algorithms (compare e.g. [16],[5],[15],[7]). Fast matrix multiplication and fast convolution algorithms are at the origin of the consideration of bilinear algorithms (compare e.g. [16], [17],[18],[19]).

The rank of an algebra appears to be closer related to the structure of A than its complexity. For this reason we focus our attention on the rank of algebras.

The starting point of our considerations is the following lower bound result for the complexity of associative algebras.

Theorem 1 ([1]) $\quad L(A) \geq 2 \dim_k A - \# \mathcal{M}(A)$,

where $\mathcal{M}(A) := \{m\ ;\ m$ maximal two-sided ideal of $A\}$ and $\# \mathcal{M}(A)$ is its cardinality.

(In the case of $A := M_N(k)$, the algebra of $N \times N$ matrices over k , the result is due to [14].)

We will use the following notions :

Definition 1 We say

(i) the complexity of A is minimal ($L(A)$ minimal)

iff $\quad L(A) = 2 \dim_k A - \# \mathcal{M}(A)$;

(ii) the rank of A is minimal ($R(A)$ minimal)

iff $\quad R(A) = 2 \dim_k A - \# \mathcal{M}(A)$.

Observations 1

1. We conjecture $L(A)$ minimal iff $R(A)$ minimal. This has been shown for A a division algebra ([8],[3]). In general, we only know that $R(A)$ minimal implies $L(A)$ minimal.
2. $M_2(k)$ is of minimal rank ([16]). We conjecture that $M_2(k)$ is the only matrix algebra of minimal rank.
3. Let k be infinite, X an indeterminate over k, and $F(X) \in k[X]$. Then $A := k[X]/(F)$ is of minimal rank ([19]).

We call the k-algebra A *local* if $A/\mathrm{rad}\, A$ is a division algebra. We call A *clean* if for each maximal two-sided ideal m of A the k-algebra A/m is a division algebra. This is equivalent to saying that $A/\mathrm{rad}\, A$ is a finite product of division algebras.

Note that A commutative implies A clean.

An important example of a non commutative clean k-algebra is $T_N(k)$, the algebra of the upper triangular $N \times N$ matrices over k.

We are considering the following class of k-algebras :

Definition 2 Let A be a clean k-algebra with $n := \dim_k A$ and such that $A/\mathrm{rad}\, A$ is a p-fold product of division algebras.
We say that A belongs to the class $\mathcal{M}_k$ (in symbols: $A \in \mathcal{M}_k$), if there exists a pair of bases $\Sigma = ((x_1,\ldots,x_n),(y_1,\ldots,y_n))$ of A which satisfies the following properties :

(i) $x_\nu y_\mu \in k\, x_\nu + k\, y_\mu$ for each $1 \leq \nu,\mu \leq n$;

(ii) $x_\pi = y_\pi$ for $1 \leq \pi \leq p$, and $x_1,\ldots,x_p$ are mutually orthogonal idempotents of A. Furthermore $1 = x_1 + \ldots + x_p$, $x_\pi y_\mu \in k\, y_\mu$ and $x_\nu y_\pi \in k\, x_\nu$ for $1 \leq \pi \leq p$, $1 \leq \nu,\mu \leq n$.

A pair Σ of bases of A which satisfies (i) and (ii) is called a multiplicative pair (for short: an M-pair) of bases of A.

We remark that our notion of class $\mathcal{M}_k$ coincides with the one used in [6] in case of local k-algebras.

It is possible to characterize the class of *commutative* algebras of minimal rank over an infinite field k. In the case that k is algebraically closed, the result can be stated as follows :

Theorem 2 ([13]) Let k be algebraically closed and A be commutative. Then the following three conditions are equivalent :

(i) $R(A)$ minimal.

(ii) $A \in M_k$.

(iii) The radical of A has the form $\operatorname{rad} A = (\omega_1, \dots, \omega_m)$, where $\omega_i \omega_j = 0$ for $1 \leq i \neq j \leq m$.

Condition (iii) is a structural characterization of the class of commutative algebras of minimal rank over k . Our goal is to find such a structural characterization for any associative algebra of minimal rank. In this paper, we resolve this problem for the class of clean k-algebras in case k algebraically closed.

In the statement of our main result (Theorem 3) we use the following notions and notations :

Let A be a finite dimensional clean k-algebra over an algebraically closed field k .

For $\omega \in A$ we denote by $A \omega A$ the k-vector space of A generated by the products $a \omega b$, where $a, b \in A$. $A \omega A$ is the minimal two-sided ideal of A which contains ω .

Furthermore we write L and R for the following two-sided ideals of A : $L := \{ x \in \operatorname{rad} A \ ; \ x (\operatorname{rad} A) = 0 \}$ and $R := \{ y \in \operatorname{rad} A \ ; \ (\operatorname{rad} A) y = 0 \}$.

We have then

Theorem 3 In case k algebraically closed and A clean the following three conditions are equivalent :

(i) $R(A)$ minimal.

(ii) $A \in M_k$.

(iii) There exist $\omega_1, \dots, \omega_m \in \operatorname{rad} A$ such that

$$\operatorname{rad} A = L + A \omega_1 A + \dots + A \omega_m A = R + A \omega_1 A + \dots + A \omega_m A \ .$$

Here, in particular, the two-sided ideals $A \omega_i A$ are as k-vector subspaces of A generated by the products $\omega_i, \omega_i^2, \dots, \omega_i^f, \dots$, $f \in \mathbb{N}$, or equivalently: $A \omega_i A = \sum_{f \in \mathbb{N}} k \, \omega_i^f$.

Furthermore, $\omega_1, \dots, \omega_m$ satisfy $\omega_i \omega_j = 0$ for $1 \leq i \neq j \leq m$.

Theorem 3 is known in special cases :
as Theorem 2 in case A commutative and Theorem 5 in [6] in case A local.

However, the origin of this kind of structure theorems is Theorem I.4 of [11], where a structural characterization of division algebras of minimal rank over an arbitrary but infinite field is given.

Observations 2

1. Principally, we are interested in the structural characterization (iii) of the complexity-theoretically defined class of clean k-algebras A of minimal rank. Motivated by the proof of Theorem 2, we insert the technical notion of class M_k (due to V. Strassen) between the structural notion (iii) and the complexity-theoretical notion (i). This simplifies proofs sensibly. Under the assumptions of Theorem 3 (k algebraically closed and A clean) we will show in Section 2: (i) ⇒ (ii) (Proposition 1), (ii) ⇒ (iii) (Proposition 2); (iii) ⇒ (i) (Proposition 3) follows in almost the same way as Proposition II.3 of [13].
2. Note that for A satisfying (iii) of Theorem 3 the following holds: Let $S \subset A$ any subalgebra with $A = S \oplus \operatorname{rad} A$. Then $B := S[\omega_1, \dots, w_m]$ is a commutative subalgebra of A of minimal rank with $A = \mathcal{L} + B = \mathcal{R} + B$. So, a clean k-algebra A of minimal rank is itself almost (i.e. modulo $\mathcal{L}$ or $\mathcal{R}$) commutative.

The next corollary, due to a generalization [9] of Proposition 1 below, contains further consequences of Theorem 3 :

Corollary 1 Let k be an arbitrary but infinite field and A clean of minimal rank.

(i) $\operatorname{rad} A$ satisfies condition (iii) of Theorem 3.

(ii) If $\mathfrak{a}$ is a two-sided ideal of A then $R(A/\mathfrak{a})$ is minimal.

As an easy application of Theorem 3 via Corollary 1 we obtain

Corollary 2 Let k be an arbitrary but infinite field. Denote by $T_N(k)$ the k-algebra of $N \times N$ upper triangular matrices. Then

$$R(T_N(k)) \text{ minimal } \quad \text{iff} \quad N = 2 .$$

Furthermore $R(T_3(k)) = 10$, the trivial 3×3 matrix multiplication algorithm being optimal in $T_3(k)$.