Algebras of minimal multiplicative complexity

Markus Bläser
Department of Computer Scince
Saarland University
Saarbrücken, Germany
mblaeser@cs.uni-saarland.de

Bekhan Chokaev
Department of Computer Scince
Moscow State University
Moscow, Russia
chokaev@cs.msu.ru

***Abstract*—We prove that an associative algebra A has minimal rank if and only if the Alder–Strassen bound is also tight for the multiplicative complexity of A, that is, the multiplicative complexity of A is $2 \dim A - t_A$ where t_A denotes the number of maximal twosided ideals of A. This generalizes a result by E. Feig who proved this for division algebras. Furthermore, we show that if A is local or superbasic, then every optimal quadratic computation for A is almost bilinear.**

***Keywords*-algebraic complexity theory; complexity of bilinear problems.**

I. Introduction

One of the important problems in algebraic complexity theory is the question about the costs of multiplication. Let A be a finite dimensional associative algebra with identity 1 over some field k. By fixing a basis of A, say $v_1, \ldots, v_N$, we can define a set of bilinear forms corresponding to the multiplication in A. If $v_\mu v_\nu = \sum_{\kappa=1}^{N} \alpha_{\mu,\nu}^{(\kappa)} v_\kappa$ for $1 \leq \mu, \nu \leq N$ with structural constants $\alpha_{\mu,\nu}^{(\kappa)} \in k$, then these constants and the equation

$$\left(\sum_{\mu=1}^{N} X_\mu v_\mu \right) \left(\sum_{\nu=1}^{N} Y_\nu v_\nu \right) = \sum_{\kappa=1}^{N} b_\kappa(X,Y) v_\kappa$$

define the desired bilinear forms $b_1, \ldots, b_N$.

The *rank* (also called *bilinear complexity*) of $b_1, \ldots, b_N$ is the smallest number of essential bilinear multiplications necessary and sufficient to compute $b_1, \ldots, b_N$ from the indeterminates $X_1, \ldots, X_N$ and $Y_1, \ldots, Y_N$. More precisely, the bilinear complexity of $b_1, \ldots, b_N$ is the smallest number r of products $p_\rho = u_\rho(X) \cdot v_\rho(Y)$ with linear forms u_ρ and v_ρ in the X_i and Y_j, respectively, such that $b_1, \ldots, b_N$ are contained in the linear span $\langle p_1, \ldots, p_r \rangle$ of $p_1, \ldots, p_r$. From this definition, it is obvious that the bilinear complexity of $b_1, \ldots, b_N$ is independent of the choice of $v_1, \ldots, v_N$, thus we may speak about the bilinear complexity $R(A)$ of (the multiplication in) A.

While the restriction to bilinear multiplications seems to be natural for bilinear problems, there are bilinear mappings that can be computed faster with non-bilinear computations than with bilinear ones. More general than bilinear computations are quadratic multiplications. Here, $u_\rho(X,Y)$ and $v_\rho(X,Y)$ are both linear forms in the X_i and Y_j. The minimal number of quadratic products $p_1, \ldots, p_\ell$ such that $b_1, \ldots, b_N$ are contained in the linear span of $p_1, \ldots, p_\ell$ is called the *multiplicative complexity* of A.

Strassen [15] proved that over infinite fields, quadratic computations are as powerful as arbitrary computations when computing bilinear mappings. More precisely, if there is a computation for the multiplication in an algebra (or any other bilinear map) with m (nonscalar) multiplications or divisions, then there is one with m quadratic multiplications and no divisions at all.

How are rank and multiplicative complexity related? Obviously, $C(A) \leq R(A)$ and its is not hard to see that $R(A) \leq 2C(A)$. There are examples where multiplicative complexity and rank differ, for instance, the multplicative complexity of the multiplication of 2×2-matrices by 2×3-matrices is ten [16] over fields of characteristic distinct from two whereas its rank is eleven [2]. However, we are not aware of any algebra for which this is provably true.

For a modern introduction to this topic and to algebraic complexity theory in general, we recommend [8].

A fundamental lower bound for the rank of an associative algebra A is the so-called Alder–Strassen bound [1]. It states that the rank of A is bounded by

$$R(A) \geq 2 \dim A - t_A, \tag{1}$$

where t_A is the number of maximal twosided ideals in A. This bound is tight in the sense that there are algebras for which equality holds. Such algebras are called *algebras of minimal rank*. These are the algebraic structures that allow the most efficient multiplication. The property that (1) holds with equality of course completely characterizes the algebras of minimal rank in complexity-theoretic terms. It had been a long-standing open problem to characterize the algebras of minimal rank in terms of their algebraic structure. This was finally achieved in [6].

Alder and Strassen actually prove their lower bound for the multiplicative complexity, that is, we even have

$$C(A) \geq 2 \dim A - t_A. \tag{2}$$

When equality holds in (2) for some algebra A, we call A an *algebra of minimal multiplicative complexity*. Of course, if an algebra has minimal rank it also has minimal

multiplicative complexity. But are there algebras that do not have minimal rank but minimal multiplicative complexity? We prove that this is not that case, i.e., an algebra A has minimal rank if and only if it has minimal multiplicative complexity. We also show that for many classes of algebras of minimal multiplicative complexity, all optimal computations are "almost" bilinear (in a sense to be made precise later).

II. Bilinear and multiplicative complexity

We use a coordinate-free definition of multiplicative complexity and rank, cf. [8, Chap. 14]. For a vector space V, V^* denotes the dual space of V, that is, the vector space of all linear forms on V.

Definition 1: Let k be a field, U, V, and W finite dimensional vector spaces over k, and $\phi : U \times V \to W$ be a bilinear map.

1) A sequence $\beta = (f_1, g_1, w_1, \ldots, f_\ell, g_\ell, w_\ell)$ such that $f_\lambda, g_\lambda \in (U \times V)^*$ and $w_\lambda \in W$ is called a quadratic computation of length ℓ for ϕ if
$$\phi(u,v) = \sum_{\lambda=1}^{\ell} f_\lambda(u,v) g_\lambda(u,v) w_\lambda \text{ for all } u \in U, v \in V.$$
2) The length of a shortest quadratic computation for ϕ is called the multiplicative complexity of ϕ and is denoted by $C(\phi)$.
3) If A is a finite dimensional associative k-algebra, then the multiplicative complexity of A is defined as the multiplicative complexity of the multiplication map of A, which is a bilinear map $A \times A \to A$. The multiplicative complexity of A is denoted by $C(A)$.

If in Definition 1, $f_\lambda \in U^*$ and $g_\lambda \in V^*$, we get bilinear computations and a coordinate-free definition of rank. The rank of ϕ and A, respectively, is denoted by $R(\phi)$ and $R(A)$.

Let $\beta = (f_1, g_1, w_1, \ldots, f_\ell, g_\ell, w_\ell)$ be a quadratic computation for an algebra A. Let $a, b, c \in A^\times$. We have
$$\begin{aligned} xy &= a^{-1}(axb^{-1})(byc^{-1})c \\ &= \sum_{\lambda=1}^{\ell} f_\lambda(axb^{-1}, byc^{-1}) g_\lambda(axb^{-1}, byc^{-1}) a^{-1} w_\lambda c \quad (3) \end{aligned}$$
for all $x, y \in A$. Therefore $\tilde{\beta} = (\tilde{f}_1, \tilde{g}_1, \tilde{w}_1, \ldots, \tilde{f}_r, \tilde{g}_r, \tilde{w}_r)$ is a quadratic computation for A, too, where $\tilde{f}_\lambda$, $\tilde{g}_\lambda$, and $\tilde{w}_\lambda$ are defined by $\tilde{f}_\lambda(x,y) = f_\lambda(axb^{-1}, byc^{-1})$ for all $x, y \in A$, $\tilde{g}_\lambda(x,y) = g_\lambda(axb^{-1}, byc^{-1})$ for all $x, y \in A$, and $\tilde{w}_\lambda = a^{-1} w_\lambda c$. This defines an equivalence relation on the set of all computations of length ℓ for A. This process of replacing β by $\tilde{\beta}$ is called *sandwiching*.

We will mainly use sandwiching in the following situation: Assume that the linear forms $f_1, \ldots, f_N$ of β are linearly independent. Let $(x_1, y_1), \ldots, (x_N, y_N)$ be dual to $f_1, \ldots, f_N$, that is, $f_i(x_j, y_j) = \delta_{i,j}$, where $\delta_{i,j}$ is Kronecker's delta. Now $(a^{-1}x_1 b, b^{-1} y_1 c), \ldots, (a^{-1} x_N b, b^{-1} x_N c)$ is dual to $\tilde{f}_1, \ldots, \tilde{f}_N$.

III. The Alder–Strassen bound and algebras of minimal complexity

A lot of effort has been spent to achieve a characterization of the algebras of minimal rank in terms of their algebraic structure as an attempt to understand the complexity of matrix multiplication. $k^{2\times 2}$, the algebra of 2×2–matrices, is an algebra of minimal rank. It had been a longstanding open problem whether $k^{3\times 3}$ is of minimal rank or not, see [8, Problem 17.1]. One way to solve this problem is to achieve a characterisation of the algebras of minimal rank in terms of their algebraic properties and then check whether $k^{3\times 3}$ fulfills these properties or not.

De Groote [11] was the first to characterise all division algebras D of minimal rank. Over infinite fields, these are all simply generated extension fields of k. If k is finite, then D has minimal rank if in addition $\#k \geq 2 \dim D - 2$, the latter result follows from the classification of the algorithm variety of polynomial multiplication modulo some irreducible polynomial by Winograd [17]. De Groote and Heintz [13] went on with commutative algebras of minimal rank over infinite fields. Next, Büchi and Clausen [7] described all local algebras of minimal rank over infinite fields. Then Heintz and Morgenstern [14] determined all basic algebras over algebraically closed fields. Finally, all semisimple algebras of minimal rank over arbitrary fields and all algebras of minimal rank over algebraically closed field were characterized [4]. Ironically, one important ingredient of this result is a direct proof that $k^{3\times 3}$ is not of minimal rank. Finally, a full characterisation of the algebras of minimal rank was obtained in [6]: An algebra A over an arbitrary field k is an algebra of minimal rank if and only if
$$A \cong C_1 \times \cdots \times C_s \times \underbrace{k^{2\times 2} \times \cdots \times k^{2\times 2}}_{u \text{ times}} \times B \qquad (4)$$
where $C_1, \ldots, C_s$ are local algebras of minimal rank with $\dim(C_\sigma / \operatorname{rad} C_\sigma) \geq 2$ (as characterized by Büchi and Clausen) and B is a superbasic algebra of minimal rank. Any of the integers s or u may be zero and the factor B is optional.

A local algebra C_σ with $\dim(C_\sigma / \operatorname{rad} C_\sigma) \geq 2$ is of minimal rank iff $C_\sigma \cong k[X]/(p_\sigma(X)^{d_\sigma})$ for some irreducible polynomial p_σ with $\deg p_\sigma \geq 2$, $d_\sigma \geq 1$. If k is finite, $\#k \geq 2 \dim C_\sigma - 2$ has to hold in addition.

An algebra B is called superbasic if $B / \operatorname{rad} B = k^t$ for some t. A superbasic algebra B is of minimal rank iff there exist $w_1, \ldots, w_m \in \operatorname{rad} B$ with $w_i^2 \neq 0$ and $w_i w_j = 0$ for $i \neq j$ such that
$$\begin{aligned} \operatorname{rad} B &= L_B + B w_1 B + \cdots + B w_m B \\ &= R_B + B w_1 B + \cdots + B w_m B. \end{aligned}$$

Here L_B and R_B denote the left and right annihilator of $\operatorname{rad} B$ (see Section A for exact definitions). m may be zero. If k is finite, $\#k \geq 2N(B) - 2$ has to hold in addition, where $N(B)$ denotes the largest natural number s such that $(\operatorname{rad} B)^s \neq \{0\}$.

The Alder–Strassen bound, however, also holds for the multiplicative complexity. It is natural to call an algebra an *algebra of minimal multiplicative complexity* if the Alder–Strassen bound is tight, i.e., $C(A) = 2 \dim A - t_A$. Since proving lower bounds for the multiplicative complexity is usually harder than for the rank, much less is known about these algebras. One very interesting result is due to Feig [10], which nicely complements de Groote's characterisation of the division algebras of minimal rank:

Theorem 2 (Feig): 1) A division algebra D has minimal multiplicative complexity if and only if it has minimal rank.

2) Furthermore, every optimal computation for such an algebra is essentially bilinear, that means, after exchanging some of the f_λ with the corresponding g_λ, we have $f_\lambda(x, y) = f_\lambda(x, 0)$ and $g_\lambda(x, y) = g_\lambda(0, y)$ for all $x, y \in D$.

We here extend Feig's result as far as possible. More precisely, we prove the following theorem.

Theorem 3: An algebra A over an arbitrary field has minimal multiplicative complexity if and only if it has minimal rank.

Extending Feig's result to semisimple algebras is rather easy. The lower bounds for matrix algebras $k^{n\times n}$ in [3] are proven for the multiplicative complexity, i.e, $k^{n\times n}$ has minimal multiplicative complexity if and only if $n = 2$. Together with [5], it is quite easy to adapt the proof in [6]. For algebras with radical, in particular local and superbasic algebras, the situation is much more complicated and this part is our main contribution.

We also explore how far one can extend the second part of Feig's result. For some algebras, like the matrix algebras of minimal rank, this is simply not possible. Waksman's algorithm [16] is a quadratic computation for $k^{2\times 2}$ that is not essentially bilinear. However, for the two large classes of algebras of minimal complexity, local and superbasic algebras, respectively, we prove that all optimal quadratic computations are "almost" bilinear. There are examples of local and superbasic algebras of minimal complexity that have an optimal quadratic computation that is not essentially bilinear. However, we can show that "most" of the computation has to be essentially bilinear. Due to space limitations, we only consider a special case in this paper. The complete definition can be found in the appendix.

IV. Superbasic algebras

Assume that A is an arbitrary algebra over some field k and $\beta = (f_1, g_1, w_1, \ldots, f_\ell, g_\ell, w_\ell)$ is an optimal quadratic computation for A. By [8, Prop. 17.20] there exist indices $\nu_1, \ldots, \nu_{2m}$, where $m = \dim \operatorname{rad} A$, such that, after interchanging some f_{ν_μ} with g_{ν_μ}, the set $\{f_{\nu_1}, f_{\nu_2}, \ldots, f_{\nu_{2m}}\}$ separates the points of $\operatorname{rad} A \times \operatorname{rad} A$. That is, for $E := \bigcap_{\mu=1}^{2m} \ker f_{\nu_\mu}$, we have

$$A \times A = E \oplus \operatorname{rad} A \times \operatorname{rad} A. \tag{5}$$

Any $(u, v) \in A \times A$ can be decomposed corresponding to (5):

$$(u, v) = (x, y) + (a, b), \tag{6}$$

where $a, b \in \operatorname{rad} A, (x, y) \in E$. Furthermore we can decompose any function h occuring in the computation β as

$$h(u, v) = \widetilde{h}(x, y) + \widehat{h}(a, b), \tag{7}$$

where $\widetilde{h}, \widehat{h} \in (A \times A)^*$, $\operatorname{rad} A \times \operatorname{rad} A \subseteq \ker \widetilde{h}$, $E \subseteq \ker \widehat{h}$. Note that $\widetilde{f}_{\nu_\mu} \equiv 0$ for $\mu = 1, \ldots, 2m$.

We can assume w.l.o.g. that $\{\nu_1, \ldots, \nu_{2m}\} = \{\ell - 2m + 1, \ldots, \ell\}$. It is easy to prove that the computation $\overline{\beta} = (\overline{f}_1, \overline{g}_1, \overline{w}_1, \ldots, \overline{f}_{\ell-2m}, \overline{g}_{\ell-2m}, \overline{w}_{\ell-2m})$ is an optimal computation for the algebra $A/\operatorname{rad} A$, where $\overline{f}_\sigma(\overline{u}, \overline{v}) = \widetilde{f}_\sigma(x, y)$, $\overline{g}_\sigma(\overline{u}, \overline{v}) = \widetilde{g}_\sigma(x, y)$, and $\overline{w}_\sigma = w_\sigma + \operatorname{rad} A$ for $\sigma = 1, \ldots, \ell - 2m$. Here, $\overline{u}$ and $\overline{v}$ are the canonical projections of u and v and (x, y) is defined by (6).

Theorem 4: A superbasic[1] algebra A over an arbitrary field k has minimal multiplicative complexity if and only if it has minimal rank.

Proof: Assume that $\dim A = n, \dim \operatorname{rad} A = n - t$ and $A/\operatorname{rad} A \cong \underbrace{k \times \ldots \times k}_{t \text{ times}}$. Moreover, let $\beta = (f_1, g_1, w_1, \ldots, f_{2n-t}, g_{2n-t}, w_{2n-t})$ be an optimal quadratic computation for A. W.l.o.g. we can assume that $\{f_{t+1}, f_{t+2}, \ldots, f_{2n-t}\}$ separates the points of $\operatorname{rad} A \times \operatorname{rad} A$, that is, (5) holds with $E := \bigcap_{\nu=t+1}^{2n-t} \ker f_\nu$. In the computation $\overline{\beta} = (\overline{f}_1, \overline{g}_1, \overline{w}_1, \ldots, \overline{f}_t, \overline{g}_t, \overline{w}_t)$ for the algebra $A/\operatorname{rad} A$ (see above), the vectors $\overline{w}_1, \ldots, \overline{w}_t$ must be linearly independent. Therefore, for all scalars $\alpha_1, \ldots, \alpha_t \in k$,

$$\alpha_1 w_1 + \ldots + \alpha_t w_t \in \operatorname{rad} A \Rightarrow \alpha_1 = \ldots = \alpha_t = 0. \tag{8}$$

Consider the decomposition of $(1, 0) \in A \times A$ corresponding to (5):

$$(1, 0) = (1 - a, -b) + (a, b),$$

where $a, b \in \operatorname{rad} A$ and $(1 - a, -b) \in E$. By the definition of E,

$$\begin{aligned}(1 - a) \cdot (-b) &= \sum_{i=1}^{2n-t} f_i(1 - a, -b) g_i(1 - a, -b) w_i \\ &\in \langle w_1, \ldots, w_t \rangle \implies (1 - a) \cdot (-b) = 0.\end{aligned}$$

[1]Recall that an algebra is superbasic if $A/\operatorname{rad} A = k^t$ for some t.

Since $-b \in \operatorname{rad} A$, the last implication follows from (8). Because $1-a$ is invertible by Nakayama's lemma, we have $b=0$ and therefore $(1-a,0) \in E$.

Similarly $(0,1-c) \in E$ for some $c \in \operatorname{rad} A$. By sandwiching, we can achieve $(1,0),(0,1) \in E$.

Our goal is to construct two bases $\{a_i\}$ and $\{b_j\}$ of $\operatorname{rad} A$ such that $a_i \cdot b_j \in \langle a_i, b_j\rangle$ for all i,j. Then we can extend this to an M-pair of bases (see [6, Def. 15] for a definition) and, applying [6, Thm. 22], can get that A is of minimal rank.

Let $(a_{t+1},b_{t+1}),\dots,(a_{2n-t},b_{2n-t})$ denote the dual basis of $f_{t+1}|_{\operatorname{rad} A\times\operatorname{rad} A},\dots,f_{2n-t}|_{\operatorname{rad} A\times\operatorname{rad} A}$[2]. For all $\nu = t+1,\dots,2n-t$, we get

$$a_\nu \cdot b_\nu \in \langle w_1,\dots,w_t\rangle + g_\nu(a_\nu,b_\nu)w_\nu, \tag{9}$$

$$a_\nu + a_\nu \cdot b_\nu = a_\nu \cdot (1+b_\nu) \in \langle w_1,\dots,w_t\rangle + g_\nu(a_\nu,1+b_\nu)w_\nu. \tag{10}$$

If $g_\nu(a_\nu,b_\nu)=0$, then $a_\nu \cdot b_\nu = 0$ by (8). Otherwise, we subtract $\alpha\cdot(9)$ from (10), where $\alpha = g_\nu(a_\nu,1+b_\nu)/g_\nu(a_\nu,b_\nu)$ and obtain $a_\nu + (1-\alpha)a_\nu b_\nu = 0$ by (8). Since $a_\nu, b_\nu \in \operatorname{rad} A$, this is only possible if $a_\nu b_\nu = 0$.

Thus, we get

$$\begin{aligned} a_\nu &\in \langle w_1,\dots,w_t\rangle + g_\nu(a_\nu,1+b_\nu)w_\nu,\\ b_\nu &\in \langle w_1,\dots,w_t\rangle + g_\nu(1+a_\nu,b_\nu)w_\nu. \end{aligned}$$

The first equation follows from (10) and $a_\nu b_\nu = 0$, the second is obtained similarly. In particular, a_ν and b_ν are linearly dependent (project along $\langle w_1,\dots,w_t\rangle$ onto $\operatorname{rad} A$). If $a_\nu \neq 0$, then $g_\nu(a_\nu,1+b_\nu)\neq 0$, and if $b_\nu \neq 0$, then $g_\nu(1+a_\nu,b_\nu)\neq 0$. Furthermore, if $a_\nu \neq 0$ and $b_\mu \neq 0$ then

$$\begin{aligned} (a_\nu + a_\mu)\cdot(b_\nu + b_\mu) &\in \langle w_1,\dots,w_t,w_\nu,w_\mu\rangle\\ &= \langle w_1,\dots,w_t,a_\nu,b_\mu\rangle. \end{aligned}$$

If we project along $\langle w_1,\dots,w_t\rangle$ onto $\operatorname{rad} A$, we get

$$(a_\nu + a_\mu)\cdot(b_\nu + b_\mu) \in \langle a_\nu, b_\mu\rangle.$$

We divide $\{t+1,\dots,2n-t\}$ into the three subsets I, J, and K: $i\in I$ iff $b_i=0$, $j\in J$ iff $a_j=0$, and $k\in K$ iff $a_k\neq 0$ and $b_k\neq 0$. For any $i\in I$, $j\in J$, and $k,\ell\in K$ we get

$$\begin{aligned} a_i\cdot b_j &= (a_i+a_j)\cdot(b_i+b_j) \in \langle a_i,b_j\rangle, \qquad (11)\\ a_i\cdot b_\ell &= (a_i+a_\ell)\cdot(b_i+b_\ell) \in \langle a_i,b_\ell\rangle,\\ a_k\cdot b_j &= (a_k+a_j)\cdot(b_k+b_j) \in \langle a_k,b_j\rangle,\\ a_k\cdot b_\ell + a_\ell\cdot b_k &= (a_k+a_\ell)\cdot(b_k+b_\ell) \in \langle a_k,b_\ell\rangle. \end{aligned}$$

For $k\in K$, we have $a_k = \alpha_k b_k$ for some $\alpha_k\neq 0$, so $a_k\cdot a_k = 0$. Consider the product $a_i\cdot b_\ell$, $i\in I$, $\ell\in K$: $a_i\cdot b_\ell = \beta a_i + \gamma b_\ell$ for appropriate constants β and γ (which depend on i and ℓ). Multiplying this equation by b_ℓ from the right, we get that $\beta a_i\cdot b_\ell = \gamma b_\ell^2 - a_i b_\ell^2 = 0$, because $b_\ell^2 = 0$. Therefore,

$$a_i\cdot b_\ell = 0 \qquad \text{for all } i\in I,\ \ell\in K. \tag{12}$$

(If $\beta=0$, this follows already from $a_i\cdot b_\ell = \gamma b_\ell$.) In similar way we can prove that

$$a_k\cdot b_j = 0 \qquad \text{for all } j\in J,\ k\in K. \tag{13}$$

Next, consider $a_k\cdot b_\ell + a_\ell\cdot b_k$ for $k,\ell\in K$: $a_k\cdot b_\ell + a_\ell\cdot b_k = \beta' a_k + \gamma' b_\ell$. If any of these two coefficients, say β', is not equal to zero, then multiplying this equation by b_ℓ from the right-hand side and the left-hand side, respectively, we get that $a_\ell\cdot b_k\cdot b_\ell = \beta' a_k\cdot b_\ell$ and $b_\ell\cdot a_k\cdot b_\ell = \beta' b_\ell\cdot a_k$ (recall that $b_\ell\cdot b_\ell = a_\ell\cdot b_\ell = 0$). From the properties of the radical, $a_k\cdot b_\ell = 0$ and $a_\ell\cdot b_k = 0$ follows. Therefore, in any case, $a_k\cdot b_\ell + a_\ell\cdot b_k = 0$. From this last equation, we get that for any constants δ_k, $k\in K$,

$$\left(\sum_{k\in K}\delta_k a_k\right)\cdot\left(\sum_{\ell\in K}\delta_\ell b_\ell\right) = 0. \tag{14}$$

Let (a,b) be an arbitrary element of $\operatorname{rad}A\times\operatorname{rad}A$. Since (a_ν,b_ν) is dual to f_ν, $(a,b) = \sum_{\nu=t+1}^{2n-t} f_\nu(a,b)(a_\nu,b_\nu)$. By (12), (13), and (14),

$$\begin{aligned} a\cdot b &= \left(\sum_{i\in I} f_i(a,b)a_i + \sum_{k\in K} f_k(a,b)a_k\right)\cdot \qquad (15)\\ &\quad\cdot\left(\sum_{j\in J} f_j(a,b)b_j + \sum_{\ell\in K} f_\ell(a,b)b_\ell\right)\\ &= \left(\sum_{i\in I} f_i(a,b)a_i\right)\cdot\left(\sum_{j\in J} f_j(a,b)b_j\right). \qquad (16) \end{aligned}$$

Consider the product $a_k\cdot b_\ell$ for any $k,\ell\in K$:

$$\begin{aligned} a_k\cdot b_\ell &= \left(\sum_{i\in I} f_i(a_k,b_\ell)a_i\right)\cdot\left(\sum_{j\in J} f_j(a_k,b_\ell)b_j\right)\\ &= \left(\sum_{i\in I} f_i(a_k,b_\ell)a_i - \underbrace{f_i(a_k,b_k)}_{=0}a_i\right)\cdot\\ &\quad\cdot\left(\sum_{j\in J} f_j(a_k,b_\ell)b_j - \underbrace{f_j(a_k,b_k)}_{=0}b_j\right)\\ &= \left(\sum_{i\in I} f_i(0,b_\ell-b_k)a_i\right)\cdot\left(\sum_{j\in J} f_j(0,b_\ell-b_k)b_j\right)\\ &= 0\cdot(b_\ell-b_k)\\ &= 0, \end{aligned}$$

where the second-last equation follows from (16). Together with (12), (13), $a_k\in L_A$ and $b_\ell\in R_A$ follows.

[2]That is a basis of $\operatorname{rad} A\times\operatorname{rad} A$ such that $f_\nu(a_\mu,b_\mu)=1$ iff $\nu=\mu$ and 0 otherwise.

Therefore, there exist subsets $I' \subseteq I$ and $J' \subseteq J$ such that

$$\operatorname{rad} A = L_A \oplus \langle a_i \mid i \in I' \rangle = R_A \oplus \langle b_j \mid j \in J' \rangle .$$

Consider the algebra $B = k \times \operatorname{rad} A$ with the multiplication $(a, r)(a, r') = (aa', ar' + ra + rr')$. (We get B from A through "replacing" the semisimple part k^t by k.) We can extend 1 and a_i, $i \in I'$, to a basis of B by adding elements from L_B. In the same way, we can extend 1 and b_j, $j \in J'$, to a basis of B by adding elements from R_B. These two bases are an M-pair (see [6, Def. 15] for a definition) by (11). From [6, Thm. 22], it follows that B has minimal rank. Furthermore, there are $w_1, \ldots, w_m \in \operatorname{rad} B$ with $w_i^2 \neq 0$ and $w_i w_j \neq 0$ for $i \neq j$ such that

$$\begin{aligned} \operatorname{rad} B &= L_B + Bw_1B + \cdots + Bw_mB \\ &= R_B + Bw_1B + \cdots + Bw_mB \end{aligned}$$

and $\#k \geq 2N(B) - 2$. But since $\operatorname{rad} A = \operatorname{rad} B$, $N(A) = N(B)$, $L_A = L_B$, and $R_A = R_B$, [6, Thm. 22] also implies that A has minimal rank. ∎

V. Local algebras

For local algebras, we obtain the same result as for superbasic algebras in the previous section. We start by recalling some properties of division algebras of minimal complexity. Let $(f_1, g_1, w_1, \ldots, f_{2t-1}, g_{2t-1}, w_{2t-1})$ be an optimal quadratic computation for a division algebra of dimension t. By Feig's theorem [10], this computation is essentially bilinear, that is, after interchanging some f_σ with g_σ,

$$f_\sigma(u, v) \equiv f_\sigma(u, 0), \qquad g_\sigma(u, v) \equiv g_\sigma(0, v) \tag{17}$$

for all $u, v \in D$ and for all $\sigma = 1, \ldots, 2t - 1$.

Furthermore, by the proof of [12, Thm. IV.18], for any $\sigma_1, \ldots, \sigma_t \in \{1, \ldots, 2t - 1\}$

$$\begin{aligned} \dim\langle f_{\sigma_1}, \ldots, f_{\sigma_t} \rangle &= t, \\ \dim\langle g_{\sigma_1}, \ldots, g_{\sigma_t} \rangle &= t, \\ \dim\langle w_{\sigma_1}, \ldots, w_{\sigma_t} \rangle &= t. \end{aligned} \tag{18}$$

Theorem 5: A local algebra A over an arbitrary field k has minimal multiplicative complexity if and only if it has minimal rank.

Proof: Assume that $\dim A = n, \dim \operatorname{rad} A = n - t$, and $A/\operatorname{rad} A \cong D$ for some division algebra D. Let $\beta = (f_1, g_1, w_1, \ldots, f_{2n-1}, g_{2n-1}, w_{2n-1})$ be an optimal quadratic computation for A. W.l.o.g. we can assume that $\{f_{2t}, f_{2t+1}, \ldots, f_{2n-1}\}$ separates the points of $\operatorname{rad} A \times \operatorname{rad} A$, that is, (5) holds for $E := \bigcap_{\nu=2t}^{2n-1} \ker f_\nu$. $\overline{\beta} = (\overline{f}_1, \overline{g}_1, \overline{w}_1, \ldots, \overline{f}_{2t-1}, \overline{g}_{2t-1}, \overline{w}_{2t-1})$ is a computation for $A/\operatorname{rad} A$, where $\overline{\beta}$ is defined as in the proof of Theorem 4. By (17), $\overline{\beta}$ is essentially bilinear, i.e., w.l.o.g. $\overline{f}_\sigma(\overline{0}, \overline{v}) \equiv 0$ and $\overline{g}_\sigma(\overline{u}, \overline{0}) \equiv 0$ for all $\sigma = 1, \ldots, 2t - 1$.

Let v be an arbitrary element of $A/\operatorname{rad} A$. Consider the decomposition of $(0, v) \in A \times A$ corresponding to (5):

$$(0, v) = (-a, v - b) + (a, b),$$

where $a, b \in \operatorname{rad} A$, $(-a, v-b) \in E$. Since $f_\sigma(-a, v-b) = \overline{f}_\sigma(\overline{0}, \overline{v}) = 0$ for $\sigma = 1, \ldots, 2t - 1$ (see (7)), we get

$$(-a) \cdot (v - b) = \sum_{i=1}^{2n-1} f_i(-a, v - b) g_i(-a, v - b) w_i = 0$$

by the definition of E. Thus $v \notin \operatorname{rad} A$ implies $a = 0$. If we now take a basis $\overline{v}_1, \ldots, \overline{v}_t$ of $A/\operatorname{rad} A$, then $(0, v_1 - b_1), \ldots, (0, v_t - b_t) \in E$ holds for some $b_1, \ldots, b_t \in \operatorname{rad} A$. In the same way, if we take another basis $\overline{u}_1, \ldots, \overline{u}_t$ of $A/\operatorname{rad} A$, $(u_1 - a_1, 0), \ldots, (u_t - a_t, 0) \in E$ for some $a_1, \ldots, a_t \in \operatorname{rad} A$. Therefore, we can write

$$\begin{aligned} &E = S \times R \qquad \text{for some } S, R \text{ with} \\ &A = S \oplus \operatorname{rad} A, \qquad A = R \oplus \operatorname{rad} A. \end{aligned} \tag{19}$$

Consider the decomposition of some (u, v) as in (6) and decompose every linear form in the computation as in (7). Note that $\widetilde{f}_\sigma(0, y) \equiv 0$, since $\widetilde{f}_\sigma(0, v_\tau - b_\tau) = 0$, $\tau = 1, \ldots, t$. Similarly, $\widetilde{g}_\sigma(x, 0) \equiv 0$.

From (18) it follows that for any $\sigma_1, \ldots, \sigma_t \in \{1, \ldots, 2t-1\}$

$$\dim\langle \widetilde{f}_{\sigma_1}(x), \ldots, \widetilde{f}_{\sigma_t}(x) \rangle = t, \ \dim\langle \widetilde{g}_{\sigma_1}(y), \ldots, \widetilde{g}_{\sigma_t}(y) \rangle = t,$$

and for all $\alpha_1, \ldots, \alpha_t$,

$$\alpha_1 w_{\sigma_1} + \ldots + \alpha_t w_{\sigma_t} \in \operatorname{rad} A \ \Rightarrow \ \alpha_1 = \ldots = \alpha_t = 0. \tag{20}$$

Therefore, the system $\{f_1, \ldots, f_t, g_t, g_{t+1}, \ldots, g_{2t-1}, f_{2t}, \ldots, f_{2n-1}\}$ is a basis of $(A \times A)^*$. We denote by $(u_1, v_1), \ldots, (u_t, v_t), (u'_t, v'_t), (u_{t+1}, v_{t+1}), \ldots, (u_{2t-1}, v_{2t-1}), (u_{2t}, v_{2t}), \ldots, (u_{2n-1}, v_{2n-1})$ the corresponding dual basis.

Since E has the form (19), $f_\sigma(0, R) = g_\sigma(S, 0) = 0$ for $\sigma = 1, \ldots, 2t - 1$, and $f_\nu(E) = 0$ for $\nu = 2t, \ldots, 2n - 1$, we can write

$$\begin{aligned} (u_\sigma, v_\sigma) &= (x_\sigma, 0) \quad \text{with } x_\sigma \in S, \quad \sigma = 1, \ldots, t-1, \\ (u_\sigma, v_\sigma) &= (0, y_\sigma) \quad \text{with } y_\sigma \in R, \quad \sigma = t+1, \ldots, 2t-1, \\ (u_t, v_t) &= (x_t, 0) \quad \text{with } x_t \in S \\ (u'_t, v'_t) &= (0, y_t) \quad \text{with } y_t \in R \end{aligned}$$

and

$$\begin{aligned} (u_\nu, v_\nu) = (x_\nu + a_\nu, y_\nu + b_\nu) \quad &\text{with } x_\nu \in S, y_\nu \in R, \\ a_\nu, b_\nu \in \operatorname{rad} A, \quad &\nu = 2t, \ldots, 2n-1, \end{aligned} \tag{21}$$

$$\begin{aligned} &(a_{2t}, b_{2t}), \ldots, (a_{2n-1}, b_{2n-1}) \text{ is a dual basis of} \\ &f_{2t}|_{\operatorname{rad} A \times \operatorname{rad} A}, \ldots, f_{2n-1}|_{\operatorname{rad} A \times \operatorname{rad} A}. \end{aligned} \tag{22}$$

Since x_t and y_t are invertible, w.l.o.g. we can assume that $x_t = y_t = 1$. For all $\nu = 2t, \dots, 2n-1$, we get

$$\begin{aligned} a_\nu \cdot v_\nu = (u_\nu - x_\nu) \cdot v_\nu \in \langle w_1, \dots, w_{t-1} \rangle + \\ + g_\nu(u_\nu - x_\nu, v_\nu) w_\nu, \end{aligned} \tag{23}$$

$$\begin{aligned} a_\nu \cdot v_\nu + a_\nu = (u_\nu - x_\nu) \cdot (v_\nu + 1) \in \langle w_1, \dots, w_{t-1} \rangle + \\ + \langle w_t \rangle + g_\nu(u_\nu - x_\nu, v_\nu + 1) w_\nu. \end{aligned} \tag{24}$$

In (23), the span does not contain w_t, because $g_t(S, 0) = 0$. If $g_\nu(u_\nu - x_\nu, v_\nu) = 0$ then $a_\nu \cdot v_\nu = 0$ by (20) (since $a_\nu \in \operatorname{rad} A$). Otherwise, we subtract $\alpha \cdot (23)$ from (24), where $\alpha = g_\nu(u_\nu - x_\nu, 1 + v_\nu)/g_\nu(u_\nu - x_\nu, v_\nu)$ and obtain $a_\nu + (1-\alpha) a_\nu \cdot v_\nu = 0$ by (20). From any of the two equations,

$$\begin{aligned} a_\nu \cdot v_\nu = a_\nu \cdot y_\nu + a_\nu \cdot b_\nu = 0, \\ a_\nu + (1-\alpha) a_\nu \cdot v_\nu = a_\nu(1 + (1-\alpha) y_\nu) + (1-\alpha) a_\nu \cdot b_\nu \\ = 0 \end{aligned}$$

it follows that $a_\nu b_\nu = 0$, because $a_\nu, b_\nu \in \operatorname{rad} A$ and y_ν and $1 + (1-\alpha) y_\nu$ are either invertible or zero.

Next, we show that $a_\nu \neq 0$ implies $y_\nu = 0$: Assume on the contrary, that $a_\nu \neq 0$ and $y_\nu \neq 0$. Since y_ν is invertible, $a_\nu \cdot y_\nu = a_\nu \cdot v_\nu \neq 0$ and by (23), $g_\nu(u_\nu - x_\nu, v_\nu) \neq 0$. As we just proved, in this case, $a_\nu(1 + (1-\alpha) y_\nu) = 0$. This means that $y_\nu = \beta \cdot 1$ where $\beta = \dfrac{-1}{1-\alpha} \neq 0$ and

$$\begin{aligned} f_t(u_\nu + 1, v_\nu - y_\nu) = f_t(1, -\beta \cdot 1) = f_t(1, 0) = 1 \\ g_t(u_\nu + 1, v_\nu - y_\nu) = g_t(1, -\beta \cdot 1) = g_t(0, -\beta \cdot 1) = -\beta. \end{aligned}$$

Therefore

$$\begin{aligned} x_\nu \cdot b_\nu + b_\nu = (u_\nu + 1) \cdot (v_\nu - y_\nu) \in \langle w_1, \dots, w_{t-1} \rangle - \\ - \beta w_t + g_\nu(u_\nu + 1, v_\nu - y_\nu) w_\nu. \end{aligned} \tag{25}$$

Substracting $\gamma \cdot (23)$ from (25), where $\gamma = g_\nu(u_\nu + 1, v_\nu - y_\nu)/g_\nu(u_\nu - x_\nu, v_\nu)$, we get $\beta = 0$ by (20), a contradiction. Similarly, we can show that $b_\nu \neq 0$ implies $x_\nu = 0$. Furthermore, since $(a_\nu, b_\nu) \neq (0, 0)$ by (22), $u_\nu \neq 0$ and $v_\nu \neq 0$ implies $x_\nu = y_\nu = 0$. Therefore, in all cases, we have $u_\nu \cdot v_\nu = 0$.

We decompose $\{2t, \dots, 2n-1\}$ into three subsets I, J, and K: $i \in I$ iff $v_i = 0$, $j \in J$ iff $u_j = 0$, and $k \in K$ iff $u_k \neq 0$ and $v_k \neq 0$. For all $i \in I$, $j \in J$, $k, \ell \in K$, $\sigma \in \{1, \dots, t-1\}$, $\tau \in \{t+1, \dots, 2t-1\}$ and $\nu \in \{2t, \dots, 2n-1\}$, we get

$$\begin{aligned} x_\sigma \cdot 1 = (x_\sigma + 0) \cdot (0 + 1) \in \langle w_\sigma \rangle, \\ 1 \cdot y_\tau = (1 + 0) \cdot (0 + y_\tau) \in \langle w_\tau \rangle, \end{aligned}$$

$$x_\sigma \cdot y_\tau = (x_\sigma + 0) \cdot (0 + y_\tau) \in \langle w_\sigma, w_\tau \rangle = \langle x_\sigma, y_\tau \rangle, \tag{26}$$

$$\begin{aligned} u_\nu \cdot 1 = (u_\nu + 0) \cdot (0 + 1) \in \langle w_\nu \rangle, \\ 1 \cdot v_\nu = (1 + 0) \cdot (0 + v_\nu) \in \langle w_\nu \rangle, \end{aligned}$$

$$x_\sigma \cdot v_\nu = (x_\sigma + u_\nu) \cdot (0 + v_\nu) \in \langle x_\sigma, v_\nu \rangle, \tag{27}$$

$$u_\nu \cdot y_\tau = (u_\nu + 0) \cdot (v_\nu + y_\tau) \in \langle u_\nu, y_\tau \rangle, \tag{28}$$

$$u_i \cdot v_j = (u_i + 0) \cdot (0 + v_j) \in \langle u_i, v_j \rangle, \tag{29}$$

$$u_i \cdot b_\ell = (u_i + a_\ell) \cdot (0 + b_\ell) \in \langle u_i, b_\ell \rangle, \tag{30}$$

$$a_k \cdot v_j = (a_k + 0) \cdot (b_k + v_j) \in \langle a_k, v_j \rangle, \tag{31}$$

$$a_k \cdot b_\ell + a_l \cdot b_k = (a_k + a_\ell) \cdot (b_k + b_\ell) \in \langle a_k, b_\ell \rangle. \tag{32}$$

From (32), it follows that $a_k \cdot b_\ell + a_\ell \cdot b_k = 0$. Furthermore, by (30), $(x_i + a_i) \cdot b_\ell = \beta(x_i + a_i) + \gamma b_\ell$ for appropriate constants β and γ. Since $b_\ell^2 = 0$, multiplying this equation by b_ℓ from the right-hand side, we get $\beta = 0$ or $x_i = 0$. In the first case, $(x_i + a_i) \cdot b_\ell = \gamma b_\ell$. This means that $a_i \cdot b_\ell = b_\ell \cdot (\gamma - x_i)$, which only possible if $a_i \cdot b_\ell = 0$. In the second case, $\beta \cdot a_i \cdot b_\ell = 0$. Thus $a_i \cdot b_\ell = 0$ in this case, too. Similarly, we can show that $a_k \cdot b_j = 0$. Now completely like in the case of superbasic algebras, we can show that

$$a_k \cdot b_\ell = 0 \tag{33}$$

for all $k, \ell \in K$.

From (26)–(33) it follows that we have an M-pair of bases. By [12, Lem. IV.28] the local algebra A has minimal rank. ∎

VI. Algebras with $A/\operatorname{rad} A = k^{2\times 2}$

In this section, we prove Corollarly 9, which was needed in the proof of our main theorem. We start with some preparatory lemmas.

Lemma 6: Let k be a field. Let $(f_1, g_1, w_1, \dots, f_\ell, g_\ell, w_\ell)$ be a quadratic computation for $k^{2\times 2}$ such that $w_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $w_2 = \left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$ for some λ. Then $\ell \geq 8$.

Proof: W.l.o.g. we can assume that k is infinite. Let $x = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \alpha \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. Choose α such that w_1, w_2, x, and y form a basis. Let π be the projection along $\langle w_1, w_2 \rangle$ onto $\langle x, y \rangle$. The image of an arbitrary matrix in $k^{2\times 2}$ under π is given by

$$\begin{aligned} \pi\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) &= \pi\left(b \cdot w_2 + \left(\frac{\alpha}{\alpha - 1} a - \frac{1}{\alpha - 1} d - \lambda b\right) \cdot w_1\right) \\ &\quad + \pi\left(\left(-\frac{1}{\alpha - 1} a + \frac{1}{\alpha - 1} d\right) x + cy\right) \\ &= \frac{a - d}{1 - \alpha} x + cy. \end{aligned}$$

From β, we get a computation of length $\ell - 2$ that computes

$$\pi(u \cdot v) = \frac{1}{1-\alpha}(aa' + bb' - cc' - dd')x + (ca' + db')y$$

where

$$u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \qquad \text{and} \qquad v = \left(\begin{smallmatrix} a' & c' \\ b' & d' \end{smallmatrix}\right).$$

But these two bilinear forms have multiplicative complexity 6, as follows from the next lemma. ∎

Lemma 7: $C(aa' + bb' - cc' - dd', ca' + db') = 6$.

Proof: The upper bound is obvious. For the lower bound, we use the substitution method. We first substitute a,

b, c', and d'. By [3, Theorem 5.3] we can kill four products. (Setting $a' = 1$ and $b' = c = d = 0$ gives a test for a. In a similar manner, we get tests for b, c', and d'.) Thereafter, we still compute $ca' + db'$. The latter form has multiplicative complexity two. ∎

Lemma 8: Let $A = k^{2\times 2} \times k^{2\times 2}$ with multiplication ϕ: $(a,b)\cdot(c,d) = (ac, ad+bc)$. Then $C(A) \geq 16$.

Proof: Let $\beta = (f_1, g_1, w_1, \ldots, f_\ell, g_\ell, w_\ell)$ be a quadratic computation for A. We can assume without loss of generality that k is algebraically closed.

Case 1. We first assume that there is an i with $w_i \in \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right) \times \left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)$. (The righthand side denotes the linear subspace of all elements of A that we get by substituting arbitrary elements for the $*$.) W.l.o.g. $i = 1$.

β obviously separates $(\{0\}, \{0\}, \langle w_1\rangle)$.[3]

Next, we show that β separates $(\operatorname{rad} A, \{0\}, \langle w_1\rangle)$. Otherwise, there would be an $x \in \operatorname{rad} A \setminus \{0\}$ such that

$$x \cdot A \subseteq \langle w_1\rangle$$

by the extension lemma [8, Lemma 17.18]. This is a contradiction, since the lefthand side has dimension at least two.

Finally, β separates $(\operatorname{rad} A, \operatorname{rad} A, \langle w_1\rangle)$. Otherwise, there is a $y \in \operatorname{rad} A \setminus \{0\}$ such that

$$A \cdot y \subseteq \langle w_1\rangle + \underbrace{\operatorname{rad} A \cdot \operatorname{rad} A}_{=\{0\}},$$

a contradiction.

By [8, Lemma 17.17], $C(\phi) \geq C(\pi\circ\phi/\operatorname{rad} A \times \operatorname{rad} A) + 9$. But $\pi\circ\phi/\operatorname{rad} A \times \operatorname{rad} A$ is the multiplication of 2×2-matrices, which has multiplicative complexity 7.

Case 2. Next comes the case where for all i, $w_i \notin \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right) \times \left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)$. We choose two indices i and j. W.l.o.g. $i = 1$ and $j = 2$. Let $w_1 = (F_1, F_2)$ and $w_2 = (G_1, G_2)$. We can assume that F_1 and G_1 are linearly independent.

Case 2a. If F_1 has rank 1, then we bring F_1 into the form $F_1 = \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$ by sandwiching. We can simultaneously bring G_1 into the form $G_1 = \left(\begin{smallmatrix}1&0\\0&*\end{smallmatrix}\right)$.

Next, we sandwich with $\left(\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \alpha\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)\right)$ from the left and $\left(\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \beta\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\right)$ from the right. This leaves F_1 and G_1 unchanged and replaces

$$F_2 \mapsto F_2 + \alpha\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right) + \beta\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right),$$
$$G_2 \mapsto G_2 + \alpha\left(\begin{smallmatrix}0&*\\1&0\end{smallmatrix}\right) + \beta\left(\begin{smallmatrix}0&1\\*&0\end{smallmatrix}\right).$$

By choosing α and β appropriately, be can achieve that the new F_2 and G_2 have rank two and that $\langle w_1, w_2\rangle \cap \left(\left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)\right) = \{0\}$. For the latter, note that the projection of $\langle w_1, w_2\rangle$ onto $\left(\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)\right)$ along $\left(\left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)\right) = \{0\}$ has dimension two.

Case 2b. If F_1 has rank two, then we can assume that $F_1 = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Then we bring G_1 into Jordan normal form; this leaves F_1 unchanged. If $G_1 = \left(\begin{smallmatrix}\lambda_1&0\\0&\lambda_2\end{smallmatrix}\right)$ with $\lambda_1 \neq \lambda_2$, then we can achieve that w_1 and w_2 have the same properties as in the case that F_1 has rank one, since $\langle F_1, G_1\rangle$ is the same.

Case 2c. Finally, if for all possible choices of i and j, $G_1 = \left(\begin{smallmatrix}\lambda&1\\0&\lambda\end{smallmatrix}\right)$ after transforming F_1 into $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ and G_1 into Jordan normal form, then we do the following. We know that β separates $(\operatorname{rad} A, \operatorname{rad} A, \{0\})$ by the Alder-Strassen theorem. From β, we get a computation of length $\ell - 8$ for $k^{2\times 2}$. In this computation, w.l.o.g. $w_1 = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ and $w_2 = \left(\begin{smallmatrix}\lambda&1\\0&\lambda\end{smallmatrix}\right)$. Thus by Lemma 6, $\ell - 8 \geq 8$ and we are done.

Case 2a + b continued. This means that from now on, we can assume that F_2 and G_2 have rank two and that $\langle w_1, w_2\rangle \cap \left(\left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)\right) = \{0\}$.

We now prove the lower bound by a number of applications of the extension lemma.

1) $(\{0\}, \{0\}, \langle w_1, w_2\rangle)$ is obviously separated by β.
2) $\left(\{0\}, \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right), \langle w_1, w_2\rangle\right)$ is separated by β. Otherwise, there is a $b \in \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right) \times \left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)$, $b \neq 0$, such that
$$\underbrace{A\cdot b}_{\subseteq\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)} \subseteq \langle w_1, w_2\rangle,$$
a contradiction, since F_1 and G_1 are linearly independent.
3) $\left(\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right), \langle w_1, w_2\rangle\right)$ is separated by β. Otherwise, there is an $a \in \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)$, $a \neq 0$, such that
$$a \cdot A \subseteq \underbrace{\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)}_{=\{0\}} + \langle w_1, w_2\rangle,$$
a contradiction.
4) $\left(\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right), \left(\begin{smallmatrix}0&*\\0&*\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right), \langle w_1, w_2\rangle\right)$ is separated by β. Otherwise, there is a $b \in \left(\begin{smallmatrix}0&*\\0&*\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)\setminus\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)$ such that
$$\underbrace{A\cdot b}_{\supseteq\left(\begin{smallmatrix}0&*\\0&*\end{smallmatrix}\right)\times\left(\begin{smallmatrix}0&*\\0&*\end{smallmatrix}\right)} \subseteq \underbrace{\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}0&*\\0&*\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)}_{=\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}0&*\\0&*\end{smallmatrix}\right)} + \langle w_1, w_2\rangle.$$
This is only possible, if $F_1, G_1 \in \left(\begin{smallmatrix}0&*\\0&*\end{smallmatrix}\right)$, a contradiction.
5) $\left(\left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right), \left(\begin{smallmatrix}0&*\\0&*\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right), \langle w_1, w_2\rangle\right)$ is separated by β. Otherwise, there is an $a \in \left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)\setminus\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)$ such that
$$\underbrace{a\cdot A}_{\supseteq\left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right)} \subseteq \underbrace{\left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}0&*\\0&*\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)}_{\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)} + \langle w_1, w_2\rangle.$$
This is a contradiction, since $\langle w_1, w_2\rangle \cap \left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right) \times \left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right) = \{0\}$.[4]

[3] For a definition of "separates", see [8, Not. 17.15].

[4] For this step, it is crucial that A has a radical. Otherwise, we could prove $C(k^{2\times 2}) \geq 8$, which is obviously false.

6) Finally $\left(\left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right), A, \langle w_1, w_2\rangle\right)$ is separated by β. Otherwise, there is a $b \notin \left(\begin{smallmatrix}0&*\\0&*\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)$ such that

$$\begin{aligned}\underbrace{A\cdot b}\qquad &\subseteq \left(\begin{smallmatrix}*&*\\0&0\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)\cdot A + \langle w_1, w_2\rangle \subseteq \\ =\left(\begin{smallmatrix}*&?\\*&?\end{smallmatrix}\right)\times&\left(\begin{smallmatrix}?&?\\?&?\end{smallmatrix}\right) \\ &\subseteq \left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)\times\left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right),\end{aligned}$$

a contradiction.

From this, $C(A) \geq 16$ follows from [8, Lemma 17.17]. ∎

Corollary 9: Let A be an algebra with $A/\operatorname{rad} A = k^{2\times 2}$ and $\operatorname{rad}(A) \neq 0$. Then A is not of minimal complexity.

Proof: $\operatorname{rad} A$ is a $k^{2\times 2}$-bimodule. This means that it is isomorphic to $\bigoplus_{i=1}^{s} k^{2\times 2}$. Let $R' = \{0\} \bigoplus \oplus_{i=2}^{s} k^{2\times 2}$. Since any computation for A separates $(\operatorname{rad} A, \operatorname{rad} A, \{0\})$, it also separates $(R', R', \{0\})$. Let ϕ be the multiplication in A. We have $C(A) \geq C(\phi/R' \times R') + 2\dim R'$. But $\phi/R' \times R'$ is the multiplication of the algebra of the previous lemma. ∎

VII. Main Result

Throughout this section, k denotes an arbitrary field, A denotes a k-algebra of minimal multiplicative complexity, and $A_1 \oplus \cdots \oplus A_t$ denotes the decomposition of $A/\operatorname{rad} A$ into simple algebra (written additively).

Since A is of minimal multiplicative complexity, $A/\operatorname{rad} A$ is an algebra of minimal multiplicative complexity by [8, Prop. 17.20]. And by [8, Prop. 17.22], each A_τ is of minimal multiplicative complexity. Let $A_\tau = D_\tau^{n_\tau \times n_\tau}$, where D_τ is some k-divison algebra.

If $D_\tau = k$, then $n_\tau = 1$ or $n_\tau = 2$ by [3]. If $\dim D_\tau \geq 2$ and $n_\tau = 1$, then A_τ is a division algebra of minimal multiplicative complexity. We claim that $\dim D_\tau \geq 2$ and $n_\tau \geq 2$ cannot happen. [5, Thm. 2] rules out all cases except $\dim D_\tau = 2$ and $n_\tau = 2$. This last case is eliminated by the following lemma.

Lemma 10: Let $A \cong D^{2\times 2}$, where D is division algebra with $\dim D = 2$. Then A is not of minimal multiplicative complexity.

Proof: Let $n = \dim A = 8$. By [5, Lem. 5], if for any basis $x_1, \ldots, x_n$ of A, there exist indices $i_1, \ldots, i_s$ such that the linear span $\langle x_{i_1}, \ldots, x_{i_s}\rangle$ contains an invertible element a and elements b, c such that $[b, c] = b\cdot c - c\cdot b$ is invertible, then $C(A) \geq \frac{5}{2}n - s$. From the proof of [4, Lem. 5.10], it follows that for A, the above property holds with $s = 4$. Thus $C(A) \geq \frac{5}{2}n - 4 = 2\dim A$. ∎

Let e_τ be the identity of A_τ and let $1 = f_1 + \cdots + f_t$ be a decomposition of the identity of A such that

$$e_\tau = f_\tau + \operatorname{rad} A \qquad \text{for all } \tau. \tag{34}$$

Such a decomposition always exist by [9, Cor. 3.3.9]. Assume that say A_1 is either a division algebra of dimension at least two or isomorphic to $k^{2\times 2}$. Moreover, assume that $f_1(\operatorname{rad} A)f_j = f_j(\operatorname{rad} A)f_1 = \{0\}$ for all $j \geq 2$. Then by [6, Lem. 25], we may decompose A into direct product of two algebras:

$$A \cong f_1 A f_1 \times (f_2 + \cdots + f_t)A(f_2 + \cdots + f_t),$$

both of which have to have minimal multiplicative complexity. By [6, Lem. 24(5)], we obtain $(f_1 A f_1)/\operatorname{rad}(f_1 A f_1) \cong A_1$. In the first case, when A_1 is a division algebra, $f_1 A f_1$ is a local algebra of minimal multiplicative complexity. By Theorem 5, it is algebra of minimal rank too, that is, it is isomorphic to $k[X]/(p(X)^m)$ for some irreducible polynomial p with $\deg p \geq 2$ and some integer $m \geq 1$ by [7]. In the second case, by Corollary 9, we necessarily have $f_1 A f_1 \cong k^{2\times 2}$.

By [9, Thm. 3.5.3], $\operatorname{rad}(f' A f') = f'(\operatorname{rad} A)f'$ holds, where $f' = f_2 + \cdots + f_t$. From this it follows that $f' A f'/\operatorname{rad}(f' A f') = e'(A/\operatorname{rad} A)e' = A_2 \oplus \cdots \oplus A_t$, where $e' = e_2 + \cdots + e_t$. Proceeding recursively with $f' A f'$, we get the same result as in [6] for algebras of minimal bilinear complexity: An algebra A is of minimal multiplicative complexity iff

$$A \cong C_1 \times \cdots \times C_s \times k^{2\times 2} \times \cdots \times k^{2\times 2} \times B,$$

where the C_σ are local algebras of minimal multiplicative complexity, the algebra B is an algebra of minimal multiplicative complexity with a decomposition $B_1 \oplus \cdots \oplus B_r$ of $B/\operatorname{rad} B$ into simple factors and with the following property: for all B_ρ such that either B_ρ is a division algebra or is isomorphic to $k^{2\times 2}$, there is an index $j_\rho \neq \rho$ such that $f_\rho(\operatorname{rad} B)f_{j_\rho} \neq 0$ or $f_{j_\rho}(\operatorname{rad} B)f_\rho \neq 0$, where $1 = f_1 + \cdots + f_t$ is a decomposition of the identity of B as in (34).

It is proven in [6, Sect. 5.2] that if the algebra A is of minimal rank, then the algebra B is a superbasic algebra. This proof also works for algebra of minimal multiplicative complexity. This is because all arguments in the proof do not concern complexity at all or have references to statements concerning bilinear complexity, but the proofs of which work word by word for the multiplicative complexity. The statements namely are [4, Lem. 8.7, Lem. 8,8] and [6, Lem. 33, Lem. 34]. (The proofs of all four results use [8, Prop. 17.17, 17.18], which is valid for the multiplicative complexity, and a lower bound for the rank of multiplication of 2×2-matrices with $2 \times m$-matrices by Brockett and Dobkin. The same bound is proven in [3] for the multiplicative complexity.)

Therefore the algebra B is superbasic algebra of minimal multiplicative complexity. Such algebras are characterized by Theorem 4 and have the same structure as superbasic algebra of minimal rank. This finishes the proof of Theorem 3.

VIII. Almost bilinear computations

In this section we prove that all optimal quadratic computations for local and superbasic algebras of minimal complexity are *almost bilinear* in a sense that we

will make precise in the course of this section. We start with local algebras. Let A be a local algebra and let $\beta = (f_1, g_1, w_1, \ldots, f_{2n-1}, g_{2n-1}, w_{2n-1})$ be an optimal quadratic computation for it. From the proof of Theorem 5 it follows that

$$E := \bigcap_{\nu=2t}^{2n-1} \ker f_\nu = S \times R,$$
$$A = S \oplus \operatorname{rad} A,\ A = R \oplus \operatorname{rad} A, \tag{35}$$
$$f_\nu(S, R) = 0, \quad \nu = 2t, \ldots, 2n-1,$$
$$f_\sigma(0, R) = 0, \quad g_\sigma(S, 0) = 0, \quad \sigma = 1, \ldots, 2t-1. \tag{36}$$

Let $(a_{2t}, b_{2t}), \ldots, (a_{2n-1}, b_{2n-1})$ be as in Theorem 5, that is, $(a_{2t}, b_{2t}), \ldots, (a_{2n-1}, b_{2n-1})$ is a basis of $\operatorname{rad} A \times \operatorname{rad} A$, which is dual to $f_{2t}|_{\operatorname{rad} A \times \operatorname{rad} A}, \ldots, f_{2n-1}|_{\operatorname{rad} A \times \operatorname{rad} A}$ and define x_ν, y_ν, u_ν, and v_ν for $\nu = 2t, \ldots, 2n-1$ as in Theorem 5, too.

If $k \in K$, then $a_k \neq 0$, $b_k \neq 0$ and

$$\langle w_k \rangle = \langle a_k \rangle = \langle b_k \rangle \subseteq L_A \cap R_A. \tag{37}$$

By (36) and (21)

$$f_\sigma(a_m, b_m) = 0, \quad m \in J \cup K,\ \sigma = 1, \ldots, 2t-1, \tag{38}$$
$$g_\sigma(a_m, b_m) = 0, \quad m \in I \cup K,\ \sigma = 1, \ldots, 2t-1. \tag{39}$$

Let $x \in S$ be arbitrary. By definition of u_i, $i \in I$,

$$0 = (x + u_i) \cdot (0 + 0) = g_i(x, 0) u_i \implies g_i(S, 0) = 0.$$

Thus

$$g_i(S, 0) = 0, \quad \text{for all } i \in I. \tag{40}$$

Similarly,

$$g_j(0, R) = 0, \quad \text{for all } j \in J. \tag{41}$$

Furthermore for all $i, i' \in I$, $i \neq i'$,

$$0 = (u_i + u_{i'}) \cdot (0 + 0) = g_i(u_{i'}, 0) u_i + g_{i'}(u_i, 0) u_{i'}.$$

Since u_i and $u_{i'}$ must be linearly independent, $g_i(u_{i'}, 0) = 0$ for all $i, i' \in I$, $i \neq i'$. Since $u_{i'} = x_{i'} + a_{i'}$,

$$g_i(a_{i'}, 0) = 0 \quad \text{for } i, i' \in I,\ i \neq i'. \tag{42}$$

Similarly,

$$g_j(0, b_{j'}) = 0 \quad \text{for } j, j' \in J,\ j \neq j'. \tag{43}$$

Furthermore for $i \in I, \ell \in K$

$$\begin{aligned} 0 = a_i \cdot b_\ell &= (u_i - x_i + a_\ell) \cdot (0 + b_\ell) \\ &= g_i(a_\ell, b_\ell) u_i + g_\ell(a_i, 0) a_\ell. \end{aligned}$$

If $g_i(a_\ell, b_\ell) \neq 0$ (which holds iff $g_\ell(a_i, 0) \neq 0$), then u_i and a_ℓ would be linearly dependent. If $g_i(a_{\ell'}, b_{\ell'}) \neq 0$ for some $\ell' \neq \ell$, $\ell' \in K$, then $(u_i, 0), (a_\ell, b_\ell), (a_{\ell'}, b_{\ell'})$ would linearly dependent, which cannot happen since $(u_i, 0), (a_\ell, b_\ell), (a_{\ell'}, b_{\ell'})$ is a part of a basis. Thus for each $i \in I$, there might exist only one index $\ell := \ell(i) \in K$ such that $g_i(a_\ell, b_\ell) \neq 0$. Similarly, from

$$\begin{aligned} 0 = a_k \cdot b_j &= (a_k + 0) \cdot (b_k + v_j - y_j) \\ &= g_j(a_k, b_k) v_j + g_k(0, b_j) a_k, \\ 0 = (a_k + a_\ell) \cdot (b_k + b_\ell) &= g_k(a_\ell, b_\ell) a_k + g_\ell(a_k, b_k) a_\ell \end{aligned}$$

it follows that for each $j \in J$ might exist only one index $k := k(j) \in K$ such that $g_j(a_k, b_k) \neq 0$. And for each $k \in K$, there might exist only one index $m(k) \in I \cup J \cup K$ such that $g_k(a_m, b_m) \neq 0$. Summing up, we get for that any $i \in I$, $j \in J$, and $k \in K$,

$$g_i(a_\ell, b_\ell) = 0 \iff g_\ell(a_i, 0) = 0, \quad \ell \in K, \tag{44}$$
$$g_j(a_\ell, b_\ell) = 0 \iff g_\ell(0, b_j) = 0, \quad \ell \in K, \tag{45}$$
$$g_k(a_\ell, b_\ell) = 0 \iff g_\ell(a_k, b_k) = 0, \quad \ell \in K, \tag{46}$$

$$g_i(a_\ell, b_\ell) = 0, \quad \text{for all but one } \ell \in K, \tag{47}$$
$$g_j(a_\ell, b_\ell) = 0, \quad \text{for all but one } \ell \in K, \tag{48}$$
$$g_k(a_\ell, b_\ell) = 0, \quad \text{for all but one } \ell \in K. \tag{49}$$

Definition 11: A computation $\beta = (f_1, g_1, w_1, \ldots, f_{2n-1}, g_{2n-1}, w_{2n-1})$ for an algebra A is called almost bilinear if it satisfies the conditions (35)–(49).

Note that if $w_\rho \notin L_A \cap R_A$ for all ρ, then by (37), $|K| = 0$ and so $|I| = |J| = n$. Then by conditions (38)–(43), the computation β is even bilinear, i.e., $f_\rho(u, v) = f_\rho(u, 0)$ and $g_\rho(u, v) = g_\rho(0, v)$ for all ρ. (Note that we already exchanged some f_λ with the corresponding g_λ in the course of the proof in Section V.)

To get a similar result for superbasic algebras, we need to prove an analog of Feig's theorem for the quotient algebra $A/\operatorname{rad} A \cong k^t$.

Lemma 12: Let $A \cong k^t$. Then any optimal quadratic computation $(f_1, g_1, w_1, \ldots, f_t, g_t, w_t)$ for A is essentially bilinear, i.e., after interchanging some f_σ with g_σ, we have for all $u, v \in A$,

$$f_\sigma(u, v) = f_\sigma(u, 0),\ g_\sigma(u, v) = g_\sigma(0, v), \quad \sigma = 1, \ldots, t. \tag{50}$$

Proof: Note that $f_1, \ldots, f_t, g_1, \ldots, g_t$ form a basis of $(A \times A)^*$: Otherwise there would exist some nonzero $(a, b) \in A \times A$, such that $(a+x) \cdot (b+y) = x \cdot y$ for all $x, y \in A$, a contradiction. Let $(x_1, y_1), \ldots, (x_t, y_t), (x'_1, y'_1), \ldots, (x'_t, y'_t)$ be the corresponding dual basis of $A \times A$. Then for all $i = 1, \ldots, t$,

$$x_i \cdot y_i = 0, \qquad x'_i \cdot y'_i = 0,$$

and for all $i \neq j$,

$$(x_i + x_j) \cdot (y_i + y_j) = 0,$$
$$(x'_i + x'_j) \cdot (y'_i + y'_j) = 0,$$
$$(x_i + x'_j) \cdot (y_i + y'_j) = 0.$$

Let $e_1, \ldots, e_t$ be a canonical basis of the algebra $A \cong \underbrace{k \times \ldots \times k}_{t \text{ times}}$, i.e., a basis such that

$$e_\sigma^2 = e_\sigma \quad \text{and} \quad e_\sigma \cdot e_\rho = 0 \quad \text{for all } \sigma \neq \rho. \tag{51}$$

Let a be an arbitrary element of A and write $a = \alpha_1 e_1 + \ldots + \alpha_t e_t$. Define $\phi(a) = \{\sigma \mid \alpha_\sigma \neq 0\}$. By the first equation of (35), $\phi(x_i) \cap \phi(y_i) = 0$ for all i. Furthermore, $\phi(x_i) \cap \phi(y_j) = 0$ for all $i \neq j$ follows from $(x_i + x_j) \cdot (y_i + y_j) = x_i \cdot y_j + x_j \cdot y_i = 0$. In the same way, $\phi(x_i) \cap \phi(y_j') = 0$ follows from $(x_i + x_j') \cdot (y_i + y_j') = x_i \cdot y_j' + x_j' \cdot y_i = 0$.

Since $y_1, \ldots y_t, y_1', \ldots, y_t'$ generate A, $\phi(x_i) \subseteq \phi(y_i')$ for all i. Considering y_i' instead x_i gives the inverse relation $\phi(y_i') \subseteq \phi(x_i)$ for all i. Therefore $\phi(x_i) = \phi(y_i')$ for all i. Similarly, $\phi(x_i') = \phi(y_i)$ for all i.

The above argument yields that the disjoint union $\phi(x_1) \sqcup \ldots \sqcup \phi(x_t) \sqcup \phi(x_1') \sqcup \ldots \sqcup \phi(x_t') = \{1, \ldots, t\}$, which means that exactly t vectors of the set $\{x_1, \ldots, x_t, x_1', \ldots, x_t'\}$ are nonzero. Since $x_i = 0$ implies $y_i' = 0$, we have that $x_i = 0$ implies $x_i' \neq 0$ and $x_i \neq 0$ implies $x_i' = 0$. Thus $y_i' \neq 0 \Leftrightarrow x_i \neq 0 \Leftrightarrow x_i' = 0 \Leftrightarrow y_i = 0$ for all i. Interchanging f_σ with g_σ for indices σ for which $x_\sigma = 0$, we get (50). ∎

Using the lemma above, we can show that (35)—(49) holds for optimal computations for superbasic algebras in an analogous way to local algebras. So we get the following result.

Theorem 13: Let A be a local or superbasic algebra of minimal complexity. Then any optimal quadratic computation $\beta = (f_1, g_1, w_1, \ldots, f_\ell, g_\ell, w_\ell)$ for A is almost bilinear. In particular, if $w_\lambda \notin L_A \cap R_A$ for all λ, then β is essentially bilinear.

Example 14: Let k be a field with characteristic distinct from two. The algebra $k[X]/(X^2)$ is local and superbasic, but has a quadratic computation which is not essentially bilinear (but of course almost bilinear): We can compute the coefficients of $(a + bX)(a' + b'X)$ as aa' and $ab' + ba' = \frac{1}{2}(b + b')(a + a') + \frac{1}{2}(b - b')(-a + a')$. Observe that $X \in L_{k[X]/(X^2)} = R_{k[X]/(X^2)}$.

REFERENCES

[1] A. Alder and V. Strassen. On the algorithmic complexity of associative algebras. *Theoret. Comput. Sci.*, 15:201–211, 1981.

[2] Valery B. Alekseyev. On the Complexity of Some Algorithms of Matrix Multiplication. *J. Algorithms*, 6(1):71-85, 1985.

[3] Markus Bläser. Lower bounds for the multiplicative complexity of matrix multiplication. *Comput. Complexity*, 8:203-226, 1999.

[4] Markus Bläser. Lower bounds for the bilinear complexity of associative algebras. *Comput. Complexity*, 9:73-112, 2000.

[5] Markus Bläser. A $2.5n^2$-lower bound for the multiplicative complexity of $n \times n$-matrix multiplication. In *Proc. 18th Int. Symp. on Theoret. Aspects of Comput. Sci. (STACS)*, Lectures Notes in Comput. Sci. 2010, 99-110, 2001.

[6] Markus Bläser. A Complete Characterization of the Algebras of Minimal Bilinear Complexity. *SIAM J. Comput.*, 34(2):277-298, 2004.

[7] Werner Büchi and Michael Clausen. On a class of primary algebras of minimal rank. *Lin. Alg. Appl.*, 69:246–268, 1985.

[8] Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic Complexity Theory*. Springer, 1997.

[9] Yurij A. Drozd and Vladimir V. Kirichenko. *Finite Dimensional Algebras*. Springer, 1994.

[10] Ephraim Feig. On systems of bilinear forms whose minimal division-free algorithms are all bilinear. *J. Algorithms* 2(3): 261–281, 1981.

[11] Hans F. de Groote. Characterization of division algebras of minimal rank and the structure of their algorithm varieties. *SIAM J. Comput.*, 12:101–117, 1983.

[12] Hans F. de Groote. Lectures on the Complexity of Bilinear Problems. Lecture Notes in Comput. Science 245. Springer, 1986.

[13] Hans F. de Groote and Joos Heintz. Commutative algebras of minimal rank. *Lin. Alg. Appl.*, 55:37–68, 1983.

[14] Joos Heintz and Jacques Morgenstern. On associative algebras of minimal rank. In *Proc. 2nd Applied Algebra and Error Correcting Codes Conf. (AAECC)*, Lecture Notes in Comput. Sci. 228, pages 124. Springer, 1986.

[15] Volker Strassen. Vermeidung von Divisionen. *Crelles J. Reine Angew. Math.*, 264:184–202, 1973.

[16] A. Waksman, On Winograd's algorithm for inner products. *IEEE Trans. Comp.* C-19:360–361, 1970.

[17] S. Winograd. On multiplication in algebraic extension fields. *Theoret. Comput. Sci.*, 8:359–377, 1979.

APPENDIX

We collect some elementary properties of associative algebras. The term *algebra* always means a finite dimensional associative algebra with identity 1 over some field k. The term *left module* and *right module* always means a finitely generated left module and right module over some algebra A, respectively. By the embedding $\alpha \mapsto \alpha \cdot 1$, k becomes a subalgebra of A. Hence, every A-left module resp. A-right module is also a finite dimensional k-vector space. If we speak of a basis of an algebra or a module, we always mean a basis of the underlying vector space. Further material as well as proofs of the mentioned properties can be found in [9].

A left ideal I (and in the same way, a right ideal or twosided ideal) is called *nilpotent*, if $I^n = \{0\}$ for some positive integer n.

Fact 15: For all finite dimensional algebras A the following holds:

1) The sum of all nilpotent left ideals of A is a nilpotent twosided ideal, which contains every nilpotent right ideal of A. This twosided ideal is called the *radical* of A and is denoted by $\operatorname{rad} A$.
2) The quotient algebra $A/\operatorname{rad} A$ contains no nilpotent ideals other than the zero ideal.
3) The radical of A is contained in every maximal twosided ideal of A.
4) The algebras A and $A/\operatorname{rad} A$ have the same number of maximal twosided ideals.

We call an algebra A *semisimple*, if $\operatorname{rad} A = \{0\}$. By the above fact, $A/\operatorname{rad} A$ is semisimple. An algebra A is called *simple*, if there are no twosided ideals in A except the zero ideal and A itself.

We now describe some of the most important ways to construct new algebras from given ones: If A and B are k-algebras, then the direct product $A \times B$ with componentwise addition and multiplication is again a k-algebra. The set of all $n \times n$–matrices with entries from A forms a k-algebra (with the usual definition of addition and multiplication of matrices). This algebra is denoted by $A^{n\times n}$.

We denote the set of all units of an algebra A, that is, the set of all invertible elements, by $A^\times$. An algebra D is called a *division algebra*, if $D^\times = D \setminus \{0\}$. An algebra A is called *local*, if $A/\operatorname{rad} A$ is a division algebra, and A is called *basic*, if $A/\operatorname{rad} A$ is a direct product of division algebras. Since we do not know a better name, we call A *superbasic* if $A/\operatorname{rad} A \cong k^t$ for some t.

For an algebra A, L_A and R_A denote the *left and right annihilator* of $\operatorname{rad} A$, that is,

$$L_A = \{x \in \operatorname{rad} A \mid x(\operatorname{rad} A) = \{0\}\} \quad \text{and}$$
$$R_A = \{x \in \operatorname{rad} A \mid (\operatorname{rad} A)x = \{0\}\}.$$

If $x \in A$, we denote by AxA the ideal generated by x. If A is commutative, we will also write (x) for short. Furthermore, $k[x]$ denotes the smallest subalgebra of A that contains x. If $x_1, \ldots, x_m \in A$ mutually commute, then $k[x_1, \ldots, x_m]$ denotes the smallest subalgebra of A that contains $x_1, \ldots, x_m$. For elements $v_1, \ldots, v_n$ of some vector space, $\langle v_1, \ldots, v_n\rangle$ denotes their linear span. Occasionally, we will denote this span also by $kv_1 + \cdots + kv_n$.

The following fundamental theorem describes the structure of semisimple algebras.

Theorem 16 (Wedderburn): Every finite dimensional semisimple algebra is isomorphic to a finite direct product of simple algebras. Every finite dimensional simple k-algebra A is isomorphic to an algebra $D^{n\times n}$ for an integer $n \geq 1$ and a k-division algebra D. The integer n and the algebra D are uniquely determined by A (the latter one up to isomorphism).

Wedderburn's Theorem holds in a similar manner for modules over simple algebras. If A is an algebra, let $A^{n\times m}$ denote the vector space of all $n \times m$–matrices with entries from A.

Theorem 17 (Wedderburn): Let A be a simple algebra with $A \cong D^{n\times n}$ for some division algebra D. For every A-left module $M \neq \{0\}$ there is a (unique) integer $m \geq 1$ such that M is isomorphic to $D^{n\times m}$.

If C and D are algebras and M is a C-left module that is also a D-right module, then the module M is called a (C, D)-*bimodule*, if in addition $(am)b = a(mb)$ for all $a \in C$, $m \in M$, and $b \in D$. If $C = D$, M is also called a C-bimodule for short.