Algebras of Minimal Rank over Perfect Fields

Markus Bläser
Institut für Theoretische Informatik, Med. Universität zu Lübeck
Wallstr. 40, 23560 Lübeck, Germany
blaeser@tcs.mu-luebeck.de

Abstract

Let $R(A)$ denote the rank (also called bilinear complexity) of a finite dimensional associative algebra A. A fundamental lower bound for $R(A)$ is the so-called Alder–Strassen bound $R(A) \geq 2\dim A - t$, where t is the number of maximal twosided ideals of A. The class of algebras for which the Alder–Strassen bound is sharp, the so-called algebras of minimal rank, has received a wide attention in algebraic complexity theory.

We characterize all algebras of minimal rank over perfect fields. This solves an open problem in algebraic complexity theory over perfect fields, see [19, Sect. 12, Problem 4] or [9, Problem 17.5]. As a byproduct, we determine all algebras A of minimal rank with $A/\operatorname{rad} A \cong k^t$ over arbitrary fields.

1. Introduction

A central problem in algebraic complexity theory is the question about the costs of multiplication, say of matrices, triangular matrices, or polynomials modulo a fixed polynomial, just to mention a few. To be more specific, let A be a finite dimensional associative k-algebra with unity 1. By fixing a basis of A, say $v_1, \dots, v_N$, we can define a set of bilinear forms corresponding to the multiplication in A. If

$$v_\mu v_\nu = \sum_{\kappa=1}^{N} \alpha_{\mu,\nu}^{(\kappa)} v_\kappa \quad \text{for } 1 \leq \mu, \nu \leq N$$

with *structural constants* $\alpha_{\mu,\nu}^{(\kappa)} \in k$, then these constants and the identity

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

define the desired bilinear forms $b_1, \dots, b_N$. The *bilinear complexity* or *rank* of these bilinear forms $b_1, \dots, b_N$ is the smallest number of essential bilinear multiplications necessary and sufficient to compute $b_1, \dots, b_N$ from the indeterminates $X_1, \dots, X_N$ and $Y_1, \dots, Y_N$. More precisely, the bilinear complexity of $b_1, \dots, b_N$ is the smallest number r of products $p_\rho = u_\rho(X_i) \cdot v_\rho(Y_j)$ with linear forms u_ρ and v_ρ in the X_i and Y_j, respectively, such that $b_1, \dots, b_N$ are contained in the linear span of $p_1, \dots, p_r$. From this characterization, it follows that the bilinear complexity of $b_1, \dots, b_N$ does not depend on the choice of $v_1, \dots, v_N$, thus we may speak of the bilinear complexity of (the multiplication in) A. For an introduction to this topic and to algebraic complexity theory in general, we recommend [9].

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 from below by twice the dimension of A minus the number of twosided ideals in A. (For basic definitions and facts about associative algebras, the reader is referred to [10, 11, 17].) This bound is sharp in the sense that there are algebras for which equality holds. Since then, a lot of effort has been spent on characterizing these algebras in terms of their algebraic structure. There has been some success for certain classes of algebras, like division algebras, commutative algebras, etc., but up to now, no general result is known. As the main contribution of the present work, we determine *all* algebras of minimal rank over perfect fields, thus providing a general result over perfect fields. As a byproduct, we also obtain a characterization of all algebras A of minimal rank with $A/\operatorname{rad} A \cong k^t$ over arbitrary fields.

Model of computation. In the remainder of this work, we use a coordinate-free definition of rank, which is more appropriate when dealing with algebras of minimal rank, see [9, Chap. 14]. For a given 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 $\beta = (f_1, g_1, w_1, \dots, f_r, g_r, w_r)$ such that $f_\rho \in U^*$, $g_\rho \in V^*$, and $w_\rho \in W$ is called a bilinear computation of length r for ϕ if*

$$\phi(u,v) = \sum_{\rho=1}^{r} f_\rho(u) g_\rho(v) w_\rho \quad \text{for all } u \in U, v \in V.$$

2. *The length of a shortest bilinear computation for ϕ is called the bilinear complexity or the rank of ϕ and is denoted by $R(\phi)$.*

3. *If A is a finite dimensional associative k-algebra with unity, then the rank of A is defined as the rank of the multiplication map of A, which is a bilinear map $A \times A \to A$. The rank of A is denoted by $R(A)$.*

Previous results. Using the notation from the previous definition, the Alder–Strassen bound [1] can be written as

$$R(A) \geq 2 \dim A - t,$$

where t is the number of maximal twosided ideals in A. Algebras for which this bound is sharp are called *algebras of minimal rank*. They have received a wide attention in algebraic complexity theory. One prominent algebra of minimal rank is $k^{2\times 2}$, the algebra of 2×2–matrices [18]. It has been a longstanding open problem whether $k^{3\times 3}$ is of minimal rank or not, see [9, Problem 17.1]. The idea was that if one could characterize all algebras of minimal rank in terms of their algebraic structure, then one simply had to verify whether $k^{3\times 3}$ had this structure or not. Meanwhile, we know that $k^{3\times 3}$ is not of minimal rank [5]. Nevertheless, the characterization of the algebras of minimal rank is an interesting and important topic in algebraic complexity theory on its own.

De Groote [12] determined 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 [21]. De Groote and Heintz [14] characterize all commutative algebras of minimal rank over infinite fields. Next Büchi and Clausen [8] describe all local algebras of minimal rank over infinite fields. Then Heintz and Morgenstern determine 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 fields have been characterized [6]: semisimple algebras of minimal rank are isomorphic to a finite direct product of division algebras of minimal rank (as described by de Groote and Winograd) and of copies of $k^{2\times 2}$. Algebras of minimal rank over algebraically closed fields are isomorphic to a direct product of copies $k^{2\times 2}$ and a basic algebra A' of minimal rank (as characterized by Heintz and Morgenstern).

New Results. As our main result, we characterize all algebras of minimal rank over perfect fields (Theorem 15). Note that almost all "reasonable" fields are perfect (see e.g. [20] for a definition), for example all fields of characteristic zero, all finite fields, or all algebraically closed fields are perfect. Most of the previous results excluded finite fields while our characterization is also valid over finite fields. Thus we also extend all of the previous results to finite fields.

Theorem 15 essentially states that an algebra over a perfect field k has minimal rank if and only if

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

where $C_1, \dots, C_s$ are local algebras of minimal rank with $\dim(C_\sigma / \operatorname{rad} C_\sigma) \geq 2$ (as determined by Büchi and Clausen) and $\#k \geq 2 \dim C_\sigma - 2$, and A' is an algebra of minimal rank such that $A'/\operatorname{rad} A' \cong k^t$ for some t. In the following, we call algebras with $A'/\operatorname{rad} A' \cong k^t$ *superbasic*. Hence it remains to determine all superbasic algebras of minimal rank. This is done in Theorem 10, which is even valid over arbitrary fields: a superbasic algebra has minimal rank if and only if there exist $w_1, \dots, w_m \in \operatorname{rad} A$ with $w_i w_j = 0$ for $i \neq j$ such that

$$\begin{aligned} \operatorname{rad} A &= \mathsf{L}_A + A w_1 A + \cdots + A w_m A \\ &= \mathsf{R}_A + A w_1 A + \cdots + A w_m A \end{aligned}$$

and $\#k \geq 2N(A) - 2$. Here L_A and R_A denote the left and right annihilator of $\operatorname{rad} A$, respectively, and $N(A)$ is the largest natural number s such that $(\operatorname{rad} A)^s \neq \{0\}$.

From our result it follows that there are basically only two "building blocks" for constructing algebras of minimal rank: univariate polynomial multiplication and 2×2-matrix multiplication. The former captures local algebras of minimal rank (which are of the form $k[X]/p(X)^\ell$) as well as superbasic algebras of minimal rank. Up to L_A and R_A, superbasic algebras of minimal consist of subalgebra of the form $k[w_\mu] \cong k[X]/(X^d)$. These algebras of truncated univariate polynomials may only share the constant term and the term X^{d-1}, see also [16].

Organization of the paper. Section 2 contains the classification of all superbasic algebras of minimal rank. In Section 3, we show our main result, the characterization of all algebras of minimal rank over perfect fields. In the proof of our main result, we rely on some lower bound techniques due to Alder and Strassen [1]. An overview of these techniques can be found in [6, Sect. 3.1]. For convenience, we will refer to [6, Sect. 3.1] instead of the original work of Alder and Strassen. [6, Sect. 2] also contains brief definitions of the algebraic terms and concepts utilized in the present paper.

2. Superbasic algebras of minimal rank

In this section, we characterize superbasic algebras of minimal rank, thus generalizing the results of Heintz and Morgenstern [16]. (Note that over algebraically closed fields, the notions of basic and superbasic coincide, since there are no proper division algebras over algebraically closed fields.) Our main result is Theorem 10. This theorem is valid over arbitrary fields (and not only perfect fields). It turns out that over infinite fields, superbasic algebras of minimal rank have the same structure as (super)basic algebras over algebraically closed fields. If the underlying field k is finite, then a superbasic algebra A of minimal rank also fulfils $\#k \geq 2N(A) - 2$, where $N(A)$ denotes the largest natural number s such that $(\operatorname{rad} A)^s \neq \{0\}$.

Throughout the whole section, k denotes a field, and for an algebra A, L_A and R_A denote the left and right annihilator of $\operatorname{rad} A$, that is,

$$\mathsf{L}_A = \{x \in \operatorname{rad} A \mid x(\operatorname{rad} A) = \{0\}\} \text{ and}$$
$$\mathsf{R}_A = \{x \in \operatorname{rad} A \mid (\operatorname{rad} A)x = \{0\}\}.$$

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. For elements $v_1, \dots, v_n$ of some vector space, $\operatorname{lin}\{v_1, \dots, v_n\}$ denotes their linear span. Occasionally, we will denote this span also by $kv_1 + \cdots + kv_n$.

Inspired by Heintz and Morgenstern, we introduce the class M_k of superbasic algebras as an intermediate concept. This class plays an important role in our proof.

Definition 2 *Let A be a superbasic algebra over some field k with $\dim A = n$ and $\dim A/\operatorname{rad} A = t$. The algebra A belongs to the class M_k (or M for short) if there are bases $x_1, \dots, x_n$ and $y_1, \dots, y_n$ of A such that*

1. $x_\mu y_\nu \in kx_\mu + ky_\nu$ *for* $t+1 \leq \mu, \nu \leq n$,
2. $x_\tau = y_\tau$ *for* $1 \leq \tau \leq t$,
3. $x_\tau^2 = x_\tau$ *and* $x_\sigma x_\tau = 0$ *for* $1 \leq \sigma, \tau \leq t$ *and* $\tau \neq \sigma$,
4. $x_1 + \cdots + x_t = 1$, *and*
5. $x_\sigma y_\nu \in ky_\nu$ *and* $x_\mu y_\tau \in kx_\mu$ *for* $1 \leq \sigma, \tau \leq t$ *and* $t+1 \leq \mu, \nu \leq n$.

Such two bases are called an M-pair of bases for A.

Superbasic algebras of minimal rank are in M_k.

Lemma 3 *If a superbasic algebra A has minimal rank, then A is in M_k.*

Proof. Assume that $\dim A = n$ and $\dim A/\operatorname{rad} A = t$. Moreover, let $\beta = (f_1, g_1, w_1, \dots, f_{2n-t}, g_{2n-t}, w_{2n-t})$ be an optimal computation for A. By permuting the products, we can achieve that $f_1, \dots, f_n$ form a basis of A^*. Furthermore, we may assume that for $S := \bigcap_{\nu=1}^{n-t} \ker f_\nu$, $S + \operatorname{rad} A = A$. S contains an invertible element e of A by Nakayama's Lemma [11].

Thus $g_{n-t+1}, \dots, g_{2n-t}$ form a basis of A^*, because otherwise there would be some nonzero $a \in \bigcap_{\nu=1}^{n} \ker g_{n-t+\nu}$. But then

$$e \cdot a = \sum_{\rho=1}^{2n-t} f_\rho(e) g_\rho(a) w_\rho = 0,$$

which is a contradiction. By permuting the products $n-t+1, \dots, 2n-t$, we can achieve that for $T := \bigcap_{\nu=n+1}^{2n-t} \ker g_\nu$, $T + \operatorname{rad} A = A$. This permutation does neither affect $f_1, \dots, f_{n-t}$ nor S. Particularly, we still have $e \in \bigcap_{\nu=1}^{n-t} \ker f_\nu$, Again by Nakayama's Lemma, T contains an invertible element e' of A. With e' instead of e, we can conclude that the new $f_1, \dots, f_n$ form a basis of A^*, in the same way we have shown that $g_{n-t+1}, \dots, g_{2n-t}$ is a basis.

By sandwiching with e^{-1} from the left and $(e')^{-1}$ from the right (see e.g. [6, Sect. 3.3]), we may assume that $e = e' = 1$. Let $x_{t+1}, \dots, x_n, x_1, \dots, x_t$ denote the dual basis of $f_1, \dots, f_n$. (The odd numbering will become clear in a moment.) Furthermore, let $y_1, \dots, y_n$ be the dual basis of $g_{n-t+1}, \dots, g_{2n-t}$. By construction, $x_1, \dots, x_t$ span S and $y_1, \dots, y_t$ span T. By appropriate scaling, we can achieve that $1 = \delta_1 x_1 + \cdots + \delta_t x_t$ with $\delta_\tau \in \{0, 1\}$. Since

$$\begin{aligned} 1 \cdot y = \sum_{\tau=1}^{t} \delta_\tau g_{n-t+\tau}(y) w_{n-t+\tau} \\ + \sum_{\nu=1}^{n-t} f_{n+\nu}(1) g_{n+\nu}(y) w_{n+\nu} \end{aligned}$$

for any $y \in A$,

$$A = \operatorname{lin}\{\delta_1 w_{n-t+1}, \dots \delta_t w_n, w_{n+1}, \dots, w_{2n-t}\}.$$

Thus $\delta_\tau = 1$ for all $1 \leq \tau \leq t$ by a dimension argument. The same reasoning shows $1 = y_1 + \cdots + y_t$. This establishes the fourth condition of M-pair for $x_1, \dots, x_n$ and $y_1, \dots, y_n$.

By the construction of S and T and the definition of dual basis,

$$x_\nu = x_\nu \cdot 1 = \sum_{\rho=1}^{2n-t} f_\rho(x_\nu) g_\rho(1) w_\rho = \underbrace{g_{\nu-t}(1)}_{\neq 0} w_{\nu-t}$$

and

$$y_\nu = 1 \cdot y_\nu = \sum_{\rho=1}^{2n-t} f_\rho(1) g_\rho(y_\nu) w_\rho = \underbrace{f_{n-t+\nu}(1)}_{\neq 0} w_{n-t+\nu}$$

for all $t+1 \leq \nu \leq n$. This yields

$$\begin{aligned} x_\mu y_\nu &= \sum_{\rho=1}^{2n-t} f_\rho(x_\mu) g_\rho(y_\nu) w_\rho \\ &= g_{\mu-t}(y_\nu) w_{\mu-t} + f_{n-t+\nu}(x_\mu) w_{n-t+\nu} \\ &\in k x_\mu + k y_\nu \end{aligned}$$

for $t+1 \leq \mu, \nu \leq n$, which shows that our bases fulfil the first condition.

The second condition follows from the fact that

$$x_\tau = x_\tau \cdot 1 = w_{n-t+\tau} \quad \text{and} \quad y_\tau = 1 \cdot y_\tau = w_{n-t+\tau}.$$

for $1 \leq \tau \leq t$.

This also establishes the third condition, as for $\tau \neq \sigma$

$$x_\tau^2 = x_\tau y_\tau = w_{n-t+\tau} = x_\tau \quad \text{and} \quad x_\sigma x_\tau = x_\sigma y_\tau = 0.$$

It remains to show that the two bases meet the fifth condition: this is again shown by exploiting the property of dual bases. We have

$$x_\sigma y_\nu = f_{n-t+\nu}(x_\sigma) w_{n-t+\nu} \in k y_\nu$$

for $1 \leq \sigma \leq t$ and $t+1 \leq \nu \leq n$. The fact $x_\mu y_\tau \in k x_\mu$ follows in the same manner. ■

The bases of an M-pair can be further normalized.

Definition 4 *A superbasic algebra in M_k has a normalized M-pair of bases $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$, if in addition to the conditions in Definition 2, the bases $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ fulfil*

1. *$x_{t+1}, \ldots, x_n \in \operatorname{rad} A$ and $y_{t+1}, \ldots, y_n \in \operatorname{rad} A$,*
2. *$x_{n-d+1}, \ldots, x_n$ and $y_{n-d+1}, \ldots, y_n$ are both bases of $\mathsf{L}_A \cap \mathsf{R}_A$, and*
3. *$x_{n-\ell+1}, \ldots, x_n$ is a basis of L_A and $y_{n-r+1}, \ldots, y_n$ is a basis of R_A.*

Lemma 5 *Every superbasic algebra $A \in \mathsf{M}_k$ has a normalized M-pair of bases.*

Proof. Since $A \in \mathsf{M}_k$, it has an M-pair of bases $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ by Lemma 3. By the third condition, $x_1, \ldots, x_t$ are a system of mutually orthogonal idempotents of A, none of them being zero, thus their images $\bar{x}_1, \ldots, \bar{x}_t$ under the canonical projection $A \to A/\operatorname{rad} A$ are linearly independent. Comparing dimensions shows that they even form a basis. Thus for any $t+1 \leq \mu \leq n$, there are scalars $\xi_{\mu,\tau}$ such that

$$x'_\mu := x_\mu - \sum_{\tau=1}^{t} \xi_{\mu,\tau} x_\tau \in \operatorname{rad} A.$$

We define scalars $\eta_{\nu,\tau}$ and elements y'_ν in the same manner. We claim that the bases $x_1, \ldots, x_t, x'_{t+1}, \ldots, x_n$ and $y_1, \ldots, y_t, y'_{t+1}, \ldots, y_n$ are an M-pair. By construction, we only have to verify the first and fifth condition in Definition 2. For the first one, note that

$$\begin{aligned} x'_\mu y'_\nu &= (x_\mu - \sum_{\tau=1}^{t} \xi_{\mu,\tau} x_\tau)(y_\nu - \sum_{\tau=1}^{t} \eta_{\nu,\tau} y_\tau) \\ &= \xi x_\mu + \eta y_\nu + \sum_{\tau=1}^{t} \alpha_\tau x_\tau \\ &= \xi x'_\mu + \eta y'_\nu + \sum_{\tau=1}^{t} \alpha'_\tau x_\tau \end{aligned} \tag{1}$$

for suitable scalars $\xi, \eta, \alpha_1, \ldots, \alpha_t, \alpha'_1, \ldots, \alpha'_t$. Since $x'_\mu y'_\nu$, x'_μ, and x'_ν are contained in $\operatorname{rad} A$ but $\operatorname{lin}\{x_1, \ldots, x_t\} \cap \operatorname{rad} A = \{0\}$, $\alpha'_1 = \cdots = \alpha'_t = 0$ in (1).

In a similar manner, one can verify that $x_\tau y'_\nu \in k y'_\nu$ and $x'_\nu y_\tau \in k x'_\nu$ for $1 \leq \tau \leq t$ and $t+1 \leq \nu \leq n$: we have

$$x_\tau y'_\nu = x_\tau (y_\nu - \sum_{\tau=1}^{t} \eta_{\nu,\tau} y_\tau) = \eta y'_\nu + \sum_{\tau=1}^{t} \alpha'_\tau x_\tau$$

for suitable $\eta, \alpha'_1, \ldots, \alpha'_t$. Again we conclude that $\alpha'_1 = \cdots = \alpha'_t = 0$. The statement $x'_\nu y_\tau \in k x'_\nu$ follows alike. Thus $x_1, \ldots, x_t, x'_{t+1}, \ldots, x_n$ and $y_1, \ldots, y_t, y'_{t+1}, \ldots, y'_n$ are an M-pair. For convenience, we call these bases again $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$, respectively.

Let $a_1, \ldots, a_d$ and $b_1, \ldots, b_{\ell-d}, a_1, \ldots, a_d$ and $c_1, \ldots, c_{r-d}, a_1, \ldots, a_d$ be bases of $\mathsf{L}_A \cap \mathsf{R}_A$ and L_A and R_A, respectively. Furthermore, we can achieve that each a_δ, b_λ, and c_ρ is contained in (exactly) one of the subspaces $x_\sigma(\mathsf{L}_A \cap \mathsf{R}_A)x_\tau$, $\mathsf{L}_A x_\tau$, and $x_\sigma \mathsf{R}_A$, respectively. (Note that for any subspace V of A, the pairwise intersections of the $x_\sigma V$, $V x_\tau$, and $x_\sigma V x_\tau$ for $1 \leq \sigma, \tau \leq t$ are the nullspace. To see this, assume that there is an a in say $x_\sigma V \cap x_\tau V$ with $\sigma \neq t$. That means we can write $a = x_\sigma v = x_\tau v'$. But then

$$a = x_\sigma v = x_\sigma^2 v = x_\sigma x_\tau v' = 0.$$

The same holds for the subspaces $V x_\tau$ and $x_\sigma V x_\tau$. Since $1 = x_1 + \cdots + x_t$, also $V = x_1 V \oplus \cdots \oplus x_t V$, etc.)

By a suitable renumbering of $x_{t+1}, \ldots, x_n$ and $y_{t+1}, \ldots, y_n$, we can achieve that

$$\begin{aligned} &x_1, \ldots, x_{n-\ell}, b_1, \ldots, b_{\ell-d}, a_1, \ldots, a_d \quad \text{and} \\ &y_1, \ldots, y_{n-r}, c_1, \ldots, c_{r-d}, a_1, \ldots, a_d \end{aligned}$$

are bases of A. We assert that this is an M-pair for A. To prove this, we have to check the first and fifth condition in Definition 2. The first one is clearly fulfilled, since the x_ν and y_ν with $t+1 \leq \nu$ are in $\operatorname{rad} A$ and L_A and R_A are the left and right annihilator of $\operatorname{rad} A$, respectively.

The fifth condition is also true be construction: each a_δ can be written as $x_\sigma a'_\delta x_\tau$ for some $a'_\delta \in \mathsf{L}_A \cap \mathsf{R}_A$. Thus for $1 \leq i \leq t$, $x_i a_\delta = x_i x_\sigma a'_\delta x_\tau$ is either a_δ or 0 depending on whether $i = \sigma$ or not. The same is true for $a_\delta x_i$, $b_\lambda x_i$, and $x_i c_\rho$. This completes the proof. ■

The next two lemmata describe the structure of the algebras in M_k.

Lemma 6 *Let $A \in \mathsf{M}_k$, let $x_1, \dots, x_n$ and $y_1, \dots, y_n$ be a normalized M-pair of bases for A, and let $\ell = \dim \mathsf{L}_A$ and $r = \dim \mathsf{R}_A$. Then $x_\mu y_\nu = 0$ or $k[x_\mu] = k[y_\nu]$ for all $t+1 \leq \mu, \nu \leq n$. Moreover, $x_\mu^2 \neq 0$ and $y_\nu^2 \neq 0$ for all $1 \leq \mu \leq n-\ell$ and $1 \leq \nu \leq n-r$.*

Proof. If $\mu \geq n-\ell+1$ or $\nu \geq n-r+1$, the first statement of the lemma is true by the definition of L_A resp. R_A. Thus assume that $\mu \leq n-\ell$ and $\nu \leq n-r$. If $x_\mu y_\nu = 0$, we are done. Otherwise, assume that

$$x_\mu y_\nu = \xi x_\mu + \eta y_\nu. \qquad (2)$$

Let m be the largest integer ≥ 1 such that $x_\mu y_\nu \in (\operatorname{rad} A)^m$. Since $x_\mu, y_\nu \in \operatorname{rad} A$, neither $x_\mu \in (\operatorname{rad} A)^m$ nor $y_\nu \in (\operatorname{rad} A)^m$. Thus $\xi \neq 0$ and $\eta \neq 0$ in (2). It follows that $(x_\mu - \eta)(y_\nu - \xi) = \xi\eta \in A^\times$, hence

$$k[x_\mu] = k[x_\mu - \eta] = k[y_\nu - \xi] = k[y_\nu].$$

For the second statement, note that there is an i with $1 \leq i \leq n-r$ such that $x_\mu y_i \neq 0$, particularly $k[x_\mu] = k[y_i]$. Since $k[x_\mu] = k[y_i]$, we can write x_μ as a polynomial in y_i without constant term and nonvanishing linear term, i.e.,

$$x_\mu = \alpha_1 y_i + \alpha_2 y_i^2 + \dots + \alpha_m y_i^m \qquad \text{with } \alpha_1 \neq 0. \quad (3)$$

Since both $x_\mu, y_i \in \operatorname{rad} A$,

$$x_\mu^2 = \underbrace{\alpha_1 x_\mu y_i}_{\neq 0} + \textit{higher order terms} \neq 0.$$

The result $y_\nu^2 \neq 0$ is proven completely alike. ■

Lemma 7 *Let $A \in \mathsf{M}_k$, let $x_1, \dots, x_n$ and $y_1, \dots, y_n$ be a normalized M-pair of bases for A, and let $\ell = \dim \mathsf{L}_A$ and $r = \dim \mathsf{R}_A$. Then either $x_\mu x_\nu = x_\nu x_\mu = 0$ or $k[x_\mu] = k[x_\nu]$ for all $t+1 \leq \mu, \nu \leq n-\ell$. Moreover, $x_1, \dots, x_{n-\ell}$ mutually commute. The same holds for $y_1, \dots, y_{n-r}$.*

Proof. We start with proving the first statement. This also shows that $x_{t+1}, \dots, x_{n-\ell}$ mutually commute. Let x_μ and x_ν with $t+1 \leq \mu, \nu \leq n-\ell$ be given. By assumption, there are $t+1 \leq i, j \leq n-r$ such that $x_\mu y_i \neq 0$ and $x_\nu y_j \neq 0$. Thus $k[x_\mu] = k[y_i]$ and $k[x_\nu] = k[y_j]$ by Lemma 6. We distinguish two cases: $k[x_\mu] \neq k[y_j]$ or $k[x_\mu] = k[y_j]$. In the first case, also $k[x_\nu] \neq k[y_i]$, hence $x_\mu y_j = x_\nu y_i = 0$ by Lemma 6. Since $k[x_\mu] = k[y_i]$, we can write x_μ as a polynomial in y_i as in (3). Therefore,

$$x_\nu x_\mu = x_\nu(\alpha_1 y_i + \alpha_2 y_i^2 + \dots + \alpha_m y_i^m) = 0.$$

In the same way, $x_\mu x_\nu = 0$. In the second case, obviously $k[x_\mu] = k[x_\nu]$. We have to show that $x_\mu x_\nu \neq 0$. But $x_\mu x_\nu = 0$ would mean that $x_\mu \in \mathsf{L}_A$, since $k[x_\mu] = k[x_\nu]$, a contradiction.

To prove the second statement, it suffices to show that $x_\tau x_\nu = x_\nu x_\tau$ for $1 \leq \tau \leq t$ and $t+1 \leq \nu \leq n-\ell$, since $x_1, \dots, x_t$ mutually commute by definition of M-pair. Because $x_\tau = y_\tau$, we have $x_\nu x_\tau = \xi x_\nu$. Since x_τ is idempotent, $\xi \in \{0, 1\}$, that is, $x_\nu x_\tau \in \{0, x_\nu\}$. On the other hand, as $x_\nu \notin \mathsf{L}_A$, there is some y_i such that $x_\nu y_i \neq 0$. By Lemma 6, $k[x_\nu] = k[y_i]$. Like in (3), we can write x_ν as a polynomial in y_i without constant term. A similar argument as above shows that $x_\tau y_i \in \{0, y_i\}$. Together with (3), this implies $x_\tau x_\nu \in \{0, x_\nu\}$.

From $x_\tau x_\nu, x_\nu x_\tau \in \{0, x_\nu\}$, we can conclude that x_τ and x_ν commute. Assume on the contrary that say $x_\tau x_\nu = x_\nu$ but $x_\nu x_\tau = 0$. Then $x_\nu^2 = x_\nu(x_\tau x_\nu) = (x_\nu x_\tau)x_\nu = 0$, contradicting the second statement of Lemma 6.

In a similar fashion, one proves the statement for $y_1, \dots, y_{n-r}$. ■

Corollary 8 *Let $A \in \mathsf{M}_k$. Then there is a commutative subalgebra $S \subseteq A$ such that $S + \mathsf{L}_A = S + \mathsf{R}_A = A$. Moreover, $\operatorname{rad} S = (w_1) + \dots + (w_m)$ with nilpotent $w_1, \dots, w_m$ such that $w_i w_j = 0$ for $i \neq j$.*

Proof. Let $x_1, \dots, x_n$ and $y_, \dots, y_n$ be a normalized M-pair of bases of A. By Lemma 7, $k[x_1, \dots, x_{n-\ell}]$ is a commutative algebra. By Lemma 6, $k[y_1, \dots, y_{n-r}] = k[x_1, \dots, x_{n-\ell}]$. Hence, we set $S := k[x_1, \dots, x_{n-\ell}]$. By the definition of normalized M-pair, $S + \mathsf{L}_A = S + \mathsf{R}_A = A$.

We have $\operatorname{rad} S = (x_{t+1}, \dots, x_{n-\ell})$. We define an equivalence relation $\equiv$ on the elements $x_{t+1}, \dots, x_{n-\ell}$ by

$$x_\mu \equiv x_\nu \quad \text{iff} \quad x_\mu x_\nu \neq 0.$$

By Lemma 7, $k[x_\mu] = k[x_\nu]$ in this case. Take a set $w_1, \dots, w_m$ of the representatives for the $\equiv$–classes. Then $\operatorname{rad} S = (w_1, \dots, w_m) = (w_1) + \dots + (w_m)$. ■

The next lemma basically states that if there is an algebra $A \in \mathsf{M}_k$ with $N(A) = d$, then we can simulate univariate polynomial multiplication $\bmod X^{d+1}$ efficiently.

Lemma 9 *Assume there is an $A \in \mathsf{M}_k$ with $N(A) = d$. Then $k[X]/(X^{d+1})$ has minimal rank, where X denotes some indeterminate.*

Proof. If $d \leq 1$, then $k[X]/(X^{d+1})$ has minimal rank by using the trivial algorithm. So we may assume $d > 1$. Let $x_1, \dots, x_n$ and $y_1, \dots, y_n$ be a normalized M-pair of bases for A as asserted by Lemma 5. There is some index, say $t+1$, such that $x_{t+1}^d \neq 0$. Furthermore $x_{t+1}^d \in \mathsf{L}_A \cap \mathsf{R}_A$ by the maximality of d. By Lemmata 6 and 7, there are indices $i_1 = t+1, \dots, i_{d-1}$ as well as indices $j_1, \dots, j_{d-1}$ such that

$$\begin{aligned} k[x_{t+1}] &= \mathrm{lin}\{1, x_{i_1}, \dots, x_{i_{d-1}}, x_{t+1}^d\} \\ &= \mathrm{lin}\{1, y_{j_1}, \dots, y_{j_{d-1}}, x_{t+1}^d\}. \end{aligned}$$

We claim that $R(k[x_{t+1}]) = 2d + 1$: by the definition of M-pair,

$$x_\mu y_\nu = \xi_{\mu,\nu} x_\mu + \eta_{\mu,\nu} y_\nu \tag{4}$$

for suitable scalars $\xi_{\mu,\nu}$ and $\eta_{\mu,\nu}$.

Define a computation

$$(f_1, g_1, w_1, \dots, f_{2d+1}, g_{2d+1}, w_{2d+1}) \quad \text{for } k[x_{t+1}]$$

as follows: as the elements $w_1, \dots, w_{2d+1}$, we choose $1, x_{i_1}, \dots, x_{i_{d-1}}, x_{t+1}^d, y_{j_1}, \dots, y_{j_{d-1}}, x_{t+1}^d$. Let $f_1, \dots, f_{d+1}$ be the dual basis of $1, x_{i_1}, \dots, x_{i_{d-1}}, x_{t+1}^d$ and $g_1, g_{d+2}, \dots, g_{2d+1}$ be the dual basis of $1, y_{j_1}, \dots, y_{j_{d-1}}, x_{t+1}^d$. Next the f_δ with $d+2 \leq \delta \leq 2d$ are defined by $f_\delta(x_{i_\tau}) = \eta_{i_\tau, j_\delta}$ for $1 \leq \tau \leq d-1$ and $f_\delta(1) = f_\delta(x_{t+1}^d) = 0$. The g_δ with $2 \leq \delta \leq d$ are defined accordingly. Finally, f_{2d+1} is defined by $f_{2d+1}(x_{t+1}^d) = 1$, $f_{2d+1}(1) = 0$, and $f_{2d+1}(x_{j_\tau}) = 0$ for $1 \leq \tau \leq d-1$. The linear form g_{d+1} is defined in the same manner.

Exploiting (4), it is easy to see that this defines a computation for $k[x_{t+1}]$. Noting that $k[x_{t+1}] \cong k[X]/(X^{d+1})$ completes the proof. ∎

Theorem 10 *Let A be a superbasic algebra. Then the following statements are equivalent:*

1. *A has minimal rank.*
2. *$A \in \mathsf{M}_k$.*
3. *There exist $w_1, \dots, w_m \in \mathrm{rad}\, A$ with $w_i w_j = 0$ for $i \neq j$ such that*

$$\begin{aligned} \mathrm{rad}\, A &= \mathsf{L}_A + A w_1 A + \dots + A w_m A \\ &= \mathsf{R}_A + A w_1 A + \dots + A w_m A \end{aligned}$$

and $\#k \geq 2N(A) - 2$.

Proof. "1. $\Rightarrow$ 2.": This follows at once from Lemma 3.

"2. $\Rightarrow$ 3.": Corollary 8 implies the first part of 3. For the second part, let $d = N(A)$. By Lemma 9, the algebra $k[X]/(X^{d+1})$ has minimal rank. From the classification of the algorithm variety of $k[X]/(X^{d+1})$ given by Averbuch, Galil, and Winograd [3], it follows that this can only be the case if $\#k \geq 2d - 2$.

"3. $\Rightarrow$ 1.": We can use the same computation as designed by Heintz and Morgenstern [16, Prop. 3], which also works over arbitrary fields provided that they are large enough. The condition $\#k \geq 2N(A) - 2$ ensures that there are enough elements to perform polynomial multiplication by interpolation. ∎

3. Algebras of minimal rank over perfect fields

In this section, we show the main result of the present work: the characterization of all algebras of minimal rank over perfect fields. The reason for restricting the problem to perfect fields is that we want to utilize the so-called *Wedderburn–Malcev Theorem*, see e.g. [11, Thm. 6.2.1], which in general only holds over perfect fields. From the Wedderburn–Malcev Theorem, it follows that if A is a finite dimensional algebra over a perfect field k, then there exists a semisimple subalgebra B of A such that $B \oplus (\mathrm{rad}\, A) = A$ and $B \cong A/\mathrm{rad}\, A$. (The term "subalgebra" here includes that A and B share the same unit element.) The existence of such an algebra B is crucial for our proof. It is the only time where we rely on the fact that k is perfect. All intermediate results hold over arbitrary fields.

We will frequently use some lower bound techniques used by Alder and Strassen to prove their lower bound [1]. An overview of these techniques can be found in [6, Sect. 3.1]. Particularly, a definition of the term "separate" and the so-called Extension Lemma is given there.

For the rest of this section, k denotes a perfect field, A is a finite dimensional k-algebra, and B is a subalgebra of A that fulfils the assertion of the Wedderburn–Malcev Theorem, that is, $B \oplus (\mathrm{rad}\, A) = A$ and $B \cong A/\mathrm{rad}\, A$. Since B is semisimple, it is isomorphic to a finite product $B_1 \times \dots \times B_t$ of simple algebras B_τ by Wedderburn's Theorem. Let $i : B \to B_1 \times \dots \times B_t$ be an isomorphism of algebras. Since $B_\tau \cong i^{-1}(\{0\} \times \dots \times \{0\} \times B_\tau \times \{0\} \times \dots \times \{0\})$, we may view B_τ via i^{-1} as a subspace of B, which only fails to be a subalgebra of B because it has a different unit element. In this sense, we will write the decomposition $B = B_1 \oplus \dots \oplus B_t$ in an additive way and look at the B_τ as subspaces of B. This is done to simplify notations, mostly to write B_τ instead of the clumsy $\{0\} \times \dots \times \{0\} \times B_\tau \times \{0\} \times \dots \times \{0\}$. It is nevertheless helpful to keep the direct product form of the decomposition in mind, specifically that $B_\tau \cdot B_\sigma = \{0\}$ for $\tau \neq \sigma$.

By [6, Cor. 3.7], B is an algebra of minimal rank. Thus by the classification of the semisimple algebras of minimal rank [6, Thm. 2], either $B_\tau \cong k$ or $B_\tau \cong k^{2\times 2}$ or B_τ is an extension field such that $\#k \geq 2\dim B_\tau - 2$.

Note that the algebras $B_1, \dots, B_t$ are idempotent in the sense that $B_\tau^2 = B_\tau$ and mutually orthogonal, i.e, $B_\sigma \cdot B_\tau = \{0\}$ for $\sigma \neq \tau$. This implies that for any vector space $V \subseteq A$, $(B_\sigma \cdot V) \cap (B_\tau \cdot V) = \{0\}$ resp. $(V \cdot B_\sigma) \cap (V \cdot B_\tau) = \{0\}$ for $\sigma \neq \tau$. In particular, we have the decomposition

$$A = \bigoplus_{1\leq\sigma,\tau\leq t} B_\sigma \cdot A \cdot B_\tau \qquad \text{and}$$
$$\operatorname{rad} A = \bigoplus_{1\leq\sigma,\tau\leq t} B_\sigma (\operatorname{rad} A) B_\tau.$$

Assume that B_1 is either isomorphic to $k^{2\times 2}$ or a proper extension field of k ("proper" here means $\dim B_1 \geq 2$) and that $B_1 \cdot (\operatorname{rad} A) \neq \{0\}$. (In what follows, one has also to consider the case $(\operatorname{rad} A) \cdot B_1 \neq \{0\}$, this is done symmetrically.) Since $1 \in B_1 + \cdots + B_t$, there is some $1 \leq q \leq t$ such that $B_1 \cdot (\operatorname{rad} A) \cdot B_q \neq \{0\}$. First we are interested in the case where the only such q is $q = 1$ and moreover, the only p such that $B_p \cdot (\operatorname{rad} A) \cdot B_1 \neq \{0\}$ is also $p = 1$. In this case, we may decompose A according to the subsequent lemma.

Lemma 11 *Let B be a subalgebra of the algebra A with $A = B \oplus \operatorname{rad} A$ and $B \cong A/\operatorname{rad} A$. Let $B = B_1 \oplus \cdots \oplus B_t$ with simple B_τ. Assume that $B_\tau(\operatorname{rad} A)B_1 = B_1(\operatorname{rad} A)B_\tau = \{0\}$ for all $2 \leq \tau \leq t$. Then with $B' = B_2 + \cdots + B_t$,*

$$A \cong (B_1 + B_1(\operatorname{rad} A)B_1) \times (B' + B'(\operatorname{rad} A)B').$$

Proof. Let $a = b_1 + \cdots + b_t + r$ be an element of A with unique $b_\tau \in B_\tau$ and $r \in \operatorname{rad} A$. Since $\operatorname{rad} A = \bigoplus_{1\leq\sigma,\tau\leq t} B_\sigma(\operatorname{rad} A)B_\tau$, we can write $r = \sum_{1\leq\sigma,\tau\leq t} r_{\sigma,\tau}$ with unique $r_{\sigma,\tau} \in B_\sigma(\operatorname{rad} A)B_\tau$. By assumption $r_{1,q} = r_{q,1} = 0$ for $q > 1$.

We define a mapping

$$A \to (B_1 + B_1(\operatorname{rad} A)B_1) \times (B' + B'(\operatorname{rad} A)B')$$

by

$$b_1 + \cdots + b_t + r \mapsto$$
$$(b_1 + r_{1,1}\,,\, b_2 + \cdots + b_t + \sum_{2\leq\sigma,\tau\leq t} r_{\sigma,\tau}).$$

It is easy to verify that this is an isomorphism of algebras. ∎

Assume that we have a decomposition of an algebra $A \cong A_1 \times A_2$. By [6, Cor. 3.4 and Lem. 3.6(i)],

$$R(A) \geq 2\dim\operatorname{rad} A_1 + R((A_1/\operatorname{rad} A_1) \times A_2).$$

If we now apply [6, Lem. 3.6(ii)], we obtain

$$R(A) \geq 2\dim A_1 - 1 + R(A_2).$$

Thus the below lemma follows.

Lemma 12 *The algebra $A = A_1 \times A_2$ has minimal rank if and only if both A_1 and A_2 have minimal rank.*

Thus in the decomposition of A in Lemma 11, both $(B_1 + B_1(\operatorname{rad} A)B_1) =: C$ and $(B' + B'(\operatorname{rad} A)B')$ have minimal rank if A has. If $B_1 \cong k^{2\times 2}$, this cannot be the case by [6, Lem. 8.6]. If B_1 is a proper extension field of k, then the algebra C is a local algebra with

$$\dim(C/\operatorname{rad} C) = \dim B_1 \geq 2.$$

By the classification results for local algebras of minimal rank due to Büchi and Clausen [8], this can only be the case if $B_1 + B_1(\operatorname{rad} A)B_1$ is simply generated, that is, $B_1 + B_1(\operatorname{rad} A)B_1$ is isomorphic to $k[X]/(p(X)^m)$ for some irreducible polynomial p with $\deg p \geq 2$ and some $m \geq 1$. By the results of Averbuch, Galil, and Winograd [2], such an algebra has minimal rank if and only if $\#k \geq 2m \deg p - 2$.

By induction, the above considerations yield the following result.

Lemma 13 *Let A be an algebra of minimal rank over some field k, B a subalgebra of A with $A = B \oplus \operatorname{rad} A$ and $B \cong A/\operatorname{rad} A$. Let $B = B_1 \oplus \cdots \oplus B_t$ with simple algebras B_τ. Then A is isomorphic to $C_1 \times \cdots \times C_s \times A'$ where the C_σ are local algebras of minimal rank with $\dim(C_\sigma/\operatorname{rad} C_\sigma) \geq 2$ and A' is an algebra of minimal rank such that there is a semisimple subalgebra B' with $B' \oplus \operatorname{rad} A' = A'$, $A'/\operatorname{rad} A' \cong B'$, and w.l.o.g. $B' \cong B_{s+1} \oplus \cdots \oplus B_t$. Furthermore, A' fulfils*

for each factor B_p of B' such that B_p is either isomorphic to $k^{2\times 2}$ or a proper extension field and $B_p(\operatorname{rad} A') \neq \{0\}$ or $(\operatorname{rad} A')B_p \neq \{0\}$, there is some $q \neq p$ such that $B_p(\operatorname{rad} A')B_q \neq \{0\}$ or $B_q(\operatorname{rad} A')B_p \neq \{0\}$, respectively. $(*)$

Hence we are left with characterizing the algebra A' in the above lemma. For convenience, we call this algebra again A, the subalgebra of A as asserted by the Wedderburn–Malcev Theorem again B and the factors of B again $B_1 \oplus \cdots \oplus B_t$. Our main goal is to prove the following lemma.

Lemma 14 *Let A be an algebra of minimal rank over some field k, B a subalgebra of A with $A = B \oplus \operatorname{rad} A$ and $B \cong A/\operatorname{rad} A$. Let $B = B_1 \oplus \cdots \oplus B_t$ with simple algebras B_τ and assume that A fulfils property $(*)$ as stated in Lemma 13. Moreover, assume that either $B_1 \cong k^{2\times 2}$ or B_1 is a proper extension field of k. Then $B_1 \cdot (\operatorname{rad} A) = (\operatorname{rad} A) \cdot B_1 = \{0\}$.*

It is easy to see that the condition $B_1 \cdot (\operatorname{rad} A) = (\operatorname{rad} A) \cdot B_1 = \{0\}$ in the above lemma implies $A \cong B_1 \times (B_2 \oplus \cdots \oplus B_t \oplus \operatorname{rad} A)$. (The proof is similar to the proof of Lemma 11, see [6, Lem. 8.3] for a detailed proof.) Thus once we have proven Lemma 14, we can go on as follows: by renumbering the B_τ, we may assume that $B_1, \ldots, B_s$ are proper extension fields of k with $\#k \geq 2\dim B_\sigma - 2$ for all $1 \leq \sigma \leq s$, $B_{s+1}, \ldots, B_{s+u} \cong k^{2\times 2}$, and $B_{s+u+1}, \ldots, B_t \cong k$. By induction, Lemma 14 together with [6, Lem. 8.3] yields

$$A \cong B_1 \times \cdots \times B_s \times \underbrace{k^{2\times 2} \times \cdots \times k^{2\times 2}}_{u \text{ times}} \times A',$$

where $A'/\operatorname{rad} A' \cong k^{t-s-u}$, in other words, A' is superbasic. By [6, Lem. 3.6(ii)], A' is also of minimal rank. Thus, the final characterization result follows by Theorem 10 and Lemma 13. (Note that a proper extension field K is in particular a local algebra with $\dim(K/\operatorname{rad} K) \geq 2$.)

Theorem 15 *An algebra A over a perfect field k is an algebra of minimal rank if and only if*

$$A \cong C_1 \times \cdots \times C_s \times \underbrace{k^{2\times 2} \times \cdots \times k^{2\times 2}}_{u \text{ times}} \times A' \quad (5)$$

where $C_1, \ldots, C_s$ are local algebras of minimal rank with $\dim(C_\sigma/\operatorname{rad} C_\sigma) \geq 2$, that is, $C_\sigma \cong k[X]/(p_\sigma(X)^{d_\sigma})$ for some irreducible polynomial p_σ with $\deg p_\sigma \geq 2$, $d_\sigma \geq 1$, and $\#k \geq 2\dim C_\sigma - 2$, and A' is a superbasic algebra of minimal rank, that is, there exist $w_1, \ldots, w_m \in \operatorname{rad} A'$ with $w_i w_j = 0$ for $i \neq j$ such that

$$\begin{aligned}\operatorname{rad} A' &= \mathsf{L}_{A'} + A'w_1A' + \cdots + A'w_mA' \\ &= \mathsf{R}_{A'} + A'w_1A' + \cdots + A'w_mA'\end{aligned}$$

and $\#k \geq 2N(A') - 2$. Any of the integers s, u, or m may be zero and the factor A' in (5) is optional.

Remark 16 *The above theorem is also valid over arbitrary fields for the class of algebras A that have a subalgebra B such that $B \oplus \operatorname{rad} A = A$ and $A/\operatorname{rad} A \cong B$.*

Hence it remains to prove Lemma 14. We can restrict ourselves to algebras with $(\operatorname{rad} A)^2 = \{0\}$ as the following lemma shows.

Lemma 17 *Let A be an algebra of minimal rank over some field k, B a subalgebra of A with $A = B \oplus \operatorname{rad} A$ and $B \cong A/\operatorname{rad} A$. Let $B = B_1 \oplus \cdots \oplus B_t$ with simple algebras B_τ. Let $\bar{A}$, $\bar{B}$, and $\bar{B}_\tau$ denote the images of A, B, and B_τ under the canonical projection $A \to A/(\operatorname{rad} A)^2$. Then $\bar{A}$ has minimal rank. Furthermore, if A fulfils property $(*)$, so does $\bar{A}$.*

Proof. The fact that $\bar{A}$ has minimal rank follows from [6, Cor. 3.4 and Lem. 3.6].

The second statement follows from the next claim. For all i, let e_i denote the identity of B_i.

Claim: *For all indices p and q with $p \neq q$ such that $e_p(\operatorname{rad} A)e_q \neq \{0\}$, there is an index q' with $p \neq q'$ such that $\bar{e}_p(\operatorname{rad} \bar{A})\bar{e}_{q'} \neq \{0\}$. In the same way, there is an index p' with $p' \neq q$ such that $\bar{e}_{p'}(\operatorname{rad} \bar{A})\bar{e}_q \neq \{0\}$.*

To see that the Claim is true, let $x \in A$ such that $e_pxe_q \neq 0$ and $e_pxe_q \in e_i(\operatorname{rad} A)e_q$. Since by [11, Thm. 3.5.3], $e_pAe_q = e_p(\operatorname{rad} A)e_q$, we may assume $x \in \operatorname{rad} A$. Let $n \geq 1$ be the uniquely determined number such that $x \in (\operatorname{rad} A)^n \setminus (\operatorname{rad} A)^{n+1}$. By definition, there are $x_1, \ldots, x_n \in \operatorname{rad} A \setminus (\operatorname{rad} A)^2$ such that $x = x_1 \cdots x_n$. Since $1 = e_1 + \cdots + e_t$,

$$\begin{aligned}&e_px_1(e_1 + \cdots + e_t)x_2(e_1 + \cdots + e_t)\cdots \\ &\qquad\cdots(e_1 + \cdots + e_t)x_ne_q = e_pxe_q \neq 0.\end{aligned}$$

Thus there are indices $h_1, \ldots, h_{n-1}$ such that

$$e_px_1e_{h_1}x_2e_{h_2}\cdots e_{h_{n-1}}x_ne_q \neq 0.$$

If all h_ν equal p, then $e_{h_{n-1}}x_ne_q = e_px_ne_q \neq 0$ and we set $q' = q$. Since $e_px_ne_{q'} \in \operatorname{rad} A \setminus (\operatorname{rad} A)^2$, $\bar{e}_p\bar{x}_n\bar{e}_{q'} \neq 0$, hence we are done. Otherwise let ν_0 be the smallest index such that $h_{\nu_0} \neq p$. Now we set $q' = h_{\nu_0}$ and can conclude in the same way as before that $\bar{e}_p(\operatorname{rad} \bar{A})\bar{e}_{q'} \neq \{0\}$.

The index p' is constructed in the same manner. ∎

The next lemma shows that under the assumption that $B_1 \cdot (\operatorname{rad} A) \neq \{0\}$, then we can construct certain algebras of minimal rank. (The case $(\operatorname{rad} A) \cdot B_1 \neq \{0\}$ is treated symmetrically.) Finally, we show that the constructed algebras cannot have minimal rank, if $B_1 \cong k^{2\times 2}$ or B_1 is a proper extension field of k, thus finally proving Lemma 14.

Lemma 18 *Let A be an algebra of minimal rank, B a subalgebra of A with $A = B \oplus \operatorname{rad} A$ and $B \cong A/\operatorname{rad} A$, and $B = B_1 \oplus \cdots \oplus B_t$ with simple algebras B_τ. Assume that A fulfils property $(*)$ and that $B_1 \cdot (\operatorname{rad} A) \neq \{0\}$. Then the following holds: there is a q with $2 \leq q \leq t$ and a nonzero (B_1, B_q)-bimodule M such that the algebra $B_1 \times B_q \times M$ (as vector spaces) with multiplication law $(a, b, x) \cdot (a', b', x') = (aa', bb', ax' + xb')$ has minimal rank.*

Proof. By Lemma 17, we may assume w.l.o.g. that $(\operatorname{rad} A)^2 = \{0\}$. We now decompose $\operatorname{rad} A$ into twosided ideals as

$$\operatorname{rad} A = \bigoplus_{1 \leq \sigma, \tau \leq t} B_\sigma(\operatorname{rad} A)B_\tau$$

Because $B_1 \cdot \operatorname{rad} A \neq \{0\}$, there is some q such that $B_1 \cdot (\operatorname{rad} A) \cdot B_q \neq \{0\}$. By property $(*)$, $q \geq 2$, w.l.o.g. $q = 2$. Let

$$I = \bigoplus_{(\sigma,\tau)\neq(1,2)} B_\sigma (\operatorname{rad} A) B_\tau.$$

It is easy to verify that I is a twosided ideal of A. Since A is of minimal rank and $I \subseteq \operatorname{rad} A$, also A/I is of minimal rank by [6, Cor. 3.4 and Lem. 3.6(i)]. We have

$$A/I \cong B_1 + \cdots + B_t + B_1(\operatorname{rad} A)B_2 \qquad \text{and}$$
$$\operatorname{rad}(A/I) \cong B_1(\operatorname{rad} A)B_2.$$

By [6, Lem. 8.3]

$$A/I \cong (B_1 + B_2 + B_1(\operatorname{rad} A)B_2) \times B_3 \times \cdots \times B_t.$$

By [6, Lem. 3.6(ii)], the algebra A/I is of minimal rank only if $B_1 + B_2 + B_1(\operatorname{rad} A)B_2$ is of minimal rank. Note that $B_1(\operatorname{rad} A)B_2$ is a nonzero (B_1, B_2)-bimodule. Moreover, it is easily checked that the algebra $B_1 + B_2 + B_1(\operatorname{rad} A)B_2$ obeys the multiplications law stated in the assertion of the lemma. ∎

The subsequent lemmata show that none of the algebras in Lemma 18 is of minimal rank if $B_1 \cong k^{2\times 2}$ or B_1 is a proper extension field of k. This finally proves Lemma 14.

We have two possible choices for B_1, namely $B_1 \cong k^{2\times 2}$ and B_1 is a proper extension field of k. We split them into several subcases depending on B_2. The cases $B_1 \cong k^{2\times 2}$ and B_2 is either isomorphic to k or to $k^{2\times 2}$ are treated in [6, Lem. 8.7, 8.8]. The next Lemma 19 treats the case where B_1 is a proper extension field of k and B_2 is either also a proper extension field of k or k itself. Finally, Lemma 20 settles the case where $B_1 \cong k^{2\times 2}$ and B_2 is a proper extension field. By symmetry this also settles the remaining case where the roles of B_1 and B_2 are interchanged.

Lemma 19 *Let K be a proper extension field of k and L be a (not necessarily proper) extension field of k. Let M be a nonzero (K, L)-bimodule and define the algebra $A = K \times L \times M$ (as vector spaces) with multiplication law $(a, b, x) \cdot (a', b', x') = (aa', bb', ax' + xb')$. Then*

$$R(A) \geq 2 \dim L + \dim M + (2 \dim K - 1)(\dim M/\dim K + 1) - 1.$$

In particular, A is not of minimal rank.

Proof. Let $\beta = (f_1, g_1, w_1, \ldots, f_r, g_r, w_r)$ be an optimal computation for A and let $n = \dim A$. We can achieve that $w_1, \ldots, w_n$ form a basis of A. W.l.o.g. we may assume that $\operatorname{lin}\{w_1, \ldots, w_\ell\} + (K \times \{0\} \times M) = A$ where $\ell = \dim L$. Let $W_1 = \operatorname{lin}\{w_1, \ldots, w_{\ell-1}\}$. By definition, β separates the triple $(\{0\}, \{0\}, W_1)$.

Next we show that the computation β also separates the triple $(\{0\} \times \{0\} \times M, \{0\}, W_1)$. If this were not the case, then there would be a nonzero $a \in \{0\} \times \{0\} \times M$ by [6, Lem. 3.5] such that

$$a \cdot A \subseteq (\{0\} \times \{0\} \times M) \cdot \{0\} + W_1 = W_1,$$

which cannot be the case, as $W_1 \cap (\{0\} \times \{0\} \times M) = \{0\}$.

We claim that β even separates $(\{0\} \times L \times M, \{0\}, W_1)$. Otherwise, [6, Lem. 3.5] implies that there would be some $a \in (\{0\} \times L \times M) \setminus (\{0\} \times \{0\} \times M)$ such that

$$a \cdot A \subseteq (\{0\} \times L \times M) \cdot \{0\} + W_1 = W_1.$$

As $a \in (\{0\} \times L \times M) \setminus (\{0\} \times \{0\} \times M)$, we have $\dim a \cdot A \geq \dim L = \ell$, contradicting $\dim W_1 \leq \ell - 1$.

Define $\beta' = (f_1, g'_1, w_1, \ldots, f_r, g'_r, w_r)$ through $g'_\rho = g'_\rho|_{K\times\{0\}\times M}$ for all ρ. From the definition of "separate", it follows that β' also separates $(\{0\} \times L \times M, \{0\}, W_1)$.

Let ϕ be the multiplication map of A. Then β' is a computation for the bilinear map $\psi := \phi|_{A\times(K\times\{0\}\times M)}$, which we can view as the multiplication $a \cdot (a', x') \mapsto (aa', ax')$ of the K-left module $K \times M$. Let π be a projection of A onto $K \times \{0\} \times M$ with $W_1 \subseteq \ker \pi$. Since $\operatorname{im} \psi \subseteq K \times \{0\} \times M$, $\pi \circ \psi = \psi$.

Now by [6, Lem. 3.3]

$$\begin{aligned} R(A) &\geq R(\psi/((\{0\} \times L \times M) \times \{0\})) \\ &\quad + \dim L + \dim M + \#W_1 \\ &\geq R(\psi/((\{0\} \times L \times M) \times \{0\})) \\ &\quad + 2 \dim L + \dim M - 1. \end{aligned} \tag{6}$$

(See e.g. [6, Sect. 3.1] for a definition of the quotient of a bilinear map by two vector spaces.) Since we have $\psi(\{0\} \times L \times M, K \times \{0\} \times M) = \{0\}$, we can still view $\psi/((\{0\} \times L \times M) \times \{0\})$ as the multiplication of the K-left module $K \times M$. By Wedderburn's Theorem for modules [17], $K \times M \cong K^m$ where $m = \dim(K \times M)/\dim K$. (It also follows that m is necessarily an integer strictly greater than one.) By Hartmann's lower bounds for the rank of modules [15, Thm. 2],

$$\begin{aligned} &R(\psi/((\{0\} \times L \times M) \times \{0\})) \\ &\qquad \geq (2 \dim K - 1) \cdot (\dim M/\dim K + 1). \end{aligned}$$

This proves the first claim of the lemma.

To see that the last bound implies that A is not of minimal rank, we rewrite the bound as

$$R(A) \geq 2 \dim L + 3 \dim M + 2 \dim K - \dim M/\dim K - 2.$$

Since A has two maximal ideals, the second claim of the lemma is proven if $\dim M - \dim M/\dim K - 1 \geq 0$. But this is clearly true, because $\dim K \geq 2$ and $\dim M \geq \dim K \geq 2$. ∎

Lemma 20 *Let L be a proper extension field of k and let M be a nonzero $(k^{2\times 2}, L)$-bimodule. Define the algebra $A = k^{2\times 2} \times L \times M$ (as vector spaces) with multiplication law $(a, b, x) \cdot (a', b', x') = (aa', bb', ax' + xb')$. Then*

$$R(A) \geq 2\dim L + \tfrac{5}{2}\dim M + 6.$$

In particular, A is not of minimal rank.

Proof. Let ϕ denote the multiplication of A and define the bilinear map $\psi := \phi|_{A\times(k^{2\times 2}\times\{0\}\times M)}$. The same reasoning as in Lemma 19 shows that

$$R(A) \geq R(\psi/((\{0\} \times L \times M) \times \{0\})) + 2\dim L + \dim M - 1,$$

since we did not made use of fact that K is an extension field in the proof of (6) in Lemma 19.

Since $(\{0\} \times L \times M) \cdot (k^{2\times 2} \times \{0\} \times M) = \{0\}$, $\psi/((\{0\} \times L \times M) \times \{0\})$ is the multiplication of the $k^{2\times 2}$-module $k^{2\times 2} \times M$. By Wedderburn's Theorem for modules, this multiplication corresponds to the multiplication of 2×2–matrices with $2 \times m$–matrices where $m = \frac{1}{2}(\dim k^{2\times 2} \times M) = 2 + \frac{1}{2}\dim M$. Since the rank of the multiplication of 2×2–matrices with $2 \times m$–matrices has the lower bound $3m + 1$ [7], we obtain

$$R(A) \geq 2\dim L + \tfrac{5}{2}\dim M + 6.$$

To see that this implies that the algebra A does not have minimal rank, note that $\dim A = 4 + \dim L + \dim M$, A has two maximal ideals, and $\frac{1}{2}\dim M > 0$. ∎

References

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

[2] Amir Averbuch, Zvi Galil, and Shmuel Winograd. Classification of all minimal bilinear algorithms for computing the coefficients of the product of two polynomials modulo a polynomial, Part I: the algebra $G[u]/\langle Q(u)^\ell\rangle$, $\ell > 1$. *Theoret. Comput. Sci.*, 58:17–56, 1988.

[3] Amir Averbuch, Zvi Galil, and Shmuel Winograd. Classification of all minimal bilinear algorithms for computing the coefficients of the product of two polynomials modulo a polynomial, Part II: the algebra $G[u]/\langle u^n\rangle$. *Theoret. Comput. Sci.*, 86:143–203, 1991.

[4] Markus Bläser. A $\frac{5}{2}n^2$–lower bound for the rank of $n\times n$–matrix multiplication over arbitrary fields. In *Proc. 40th Ann. IEEE Symp. on Foundations of Comput. Sci. (FOCS)*, pages 45–50, 1999.

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

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

[7] Roger W. Brockett and David Dobkin. On the optimal evaluation of a set of bilinear forms. *Lin. Alg. Appl.*, 19:207–235, 1978.

[8] Werner Büchi and Michael Clausen. On a class of primary algebras of minimal rank. *Lin. Alg. Appl.*, 69:249–268, 1985.

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

[10] P. M. Cohn. *Algebra*, volume 3. Wiley, 1991.

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

[12] 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.

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

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

[15] W. Hartmann. On the multiplicative complexity of modules over associative algebras. *SIAM J. Comput.*, 14:383–395, 1985.

[16] 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 1–24. Springer, 1986.

[17] Richard S. Pierce. *Associative Algebras*. Springer, 1982.

[18] Volker Strassen. Gaussian elimination is not optimal. *Num. Math.*, 13:354–356, 1969.

[19] Volker Strassen. Algebraic complexity theory. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science Vol. A*, pages 634–672. Elsevier Science Publishers B.V., 1990.

[20] B. L. van der Waerden. *Algebra I*. Springer, eigth edition, 1971.

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