Algebras of Minimal Rank over Arbitrary Fields

Markus Bläser

Institut für Theoretische Informatik, Universität zu Lübeck
Wallstr. 40, 23560 Lübeck, Germany
blaeser@tcs.uni-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.

As the main contribution of this work, we characterize all algebras of minimal rank over arbitrary fields. This finally solves an open problem in algebraic complexity theory, see for instance [12, Sect. 12, Problem 4] or [6, Problem 17.5].

1 Introduction

One of the most important problems in algebraic complexity theory is the question about the costs of multiplication, say of matrices, triangular matrices, or polynomials (modulo a fixed polynomial). To be more specific, let A be a finite dimensional associative k-algebra with identity 1. 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 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 of (the multiplication in) A. For a modern introduction to this topic and to algebraic complexity theory in general, we recommend [6].

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. 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, the general case is still unsolved. As the main contribution of the present work, we determine *all* algebras of minimal rank over *arbitrary* fields, thus solving this problem completely.

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 [6, 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 $\beta = (f_1, g_1, w_1, \dots, f_r, g_r, w_r)$ 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 identity, 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 $R(A)$.*

Closely related to the bilinear complexity is the *multiplicative complexity.* Here we allow that f_ρ and g_ρ are linear forms on $U \times V$ in the above definition. The multiplicative complexity is clearly a lower bound for the bilinear complexity and it is easy to show that twice the multiplicative complexity is an upper bound for the bilinear complexity, see e.g. [6, Chap. 14].

Structure of associative algebras. Before we discuss the results obtained in this paper, we briefly review some facts about the structure of associative algebras. For detailed informations, the reader is referred to [7]. Throughout this work, the term "algebra" means a finite dimensional associative k-algebra with identity 1.

The first building block of associative algebras are *division algebras.* An algebra D is a division algebra, if all nonzero elements of D are invertible, i.e., for all $d \in D \setminus \{0\}$ there is a $c \in D$ such that $cd = dc = 1$. If D is commutative, too, then D is an *extension field* of k. Such an extension field is called simply generated, if there is an $a \in D$ such that $D = k(a)$. In other words, $D \cong k[X]/(p)$ for some irreducible polynomial $p \in k[X]$. If k is perfect, then each extension field is simply generated by the primitive element theorem. A prominent division algebra that is not commutative are the Hamiltonian quaternions, which form a four-dimensional division algebra over $\mathbb{R}$.

From division algebras, one can construct *simple algebras*: let I be a vector space of some algebra A. I is called a *two-sided ideal* if $A \cdot I \cdot A \subseteq I$ (pointwise multiplication). In other words, I is closed under left and right multiplication with elements from A. Now an algebra A is called simple, if A has only two twosided ideals, the zero ideal $\{0\}$ and A itself. It is a fundamental theorem that every simple algebra A is isomorphic to a matrix algebra over a division algebra D, i.e., $A \cong D^{n \times n}$ for some integer $n \geq 1$.

The next larger class are *semisimple algebras.* A twosided ideal is called maximal, if it is not contained in any other proper twosided ideal. The *radical* of an algebra A, denoted by $\operatorname{rad} A$, is the intersection of all maximal twosided ideals, which is again a twosided ideal. The radical is nilpotent, that means, there is an integer N (for instance $N = \dim A$) such that $(\operatorname{rad} A)^N = \{0\}$. An algebra A is called semisimple if $\operatorname{rad} A = \{0\}$. Wedderburn's structure theorem states that an algebra is semisimple if and only if it is isomorphic to a direct product of simple algebras $A_1 \times \cdots \times A_t$ (with componentwise addition and multiplication). As mentioned above, each such A_τ is isomorphic to a matrix algebra over a division algebra D_τ, i.e., $A_\tau \cong {D_\tau}^{n_\tau \times n_\tau}$. The number t in this decomposition equals the number of maximal twosided of A.

The structure of arbitrary algebras (with $\operatorname{rad} A \neq \{0\}$) in general is complicated (and not understood well). One important fact is that for any algebra A, the quotient algebra $A/\operatorname{rad} A$ is semisimple and has the same number of maximal twosided ideals as A. An algebra A is *basic*, if $A/\operatorname{rad} A$ is a direct product of division algebras, that is, we have $n_\tau = 1$ for all τ in the decomposition of the semisimple algebra $A/\operatorname{rad} A$

Previous results. Using the notations from Definition 1, the Alder–Strassen bound [1] reads 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 [11]. We have $R(k^{2\times 2}) = 7$. It has been a longstanding open problem whether $k^{3\times 3}$ is of minimal rank or not, see [6, Problem 17.1]. This question motivated the concept of algebras of minimal rank. The idea was that if one could characterize all algebras of minimal rank in terms of their algebraic structure, then one simply has to verify whether $k^{3\times 3}$ has this structure or not. Meanwhile, we know that $k^{3\times 3}$ is not of minimal rank [2]. Nevertheless, the characterization of the algebras of minimal rank is an interesting and important topic in algebraic complexity theory on its own, see e.g. [12, Sect. 12, Problem 4] or [6, Problem 17.5].

Let us review which characterization results have already been obtained: De Groote [8] 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 [13]. De Groote and Heintz [9] characterize all commutative algebras of minimal rank over infinite fields. Next Büchi and Clausen [5] classify all local algebras of minimal rank over infinite fields. Then Heintz and Morgenstern [10] determine all basic algebras over algebraically closed fields. Thereafter, all semisimple algebras of minimal rank over arbitrary fields and all algebras of minimal rank over algebraically closed fields have been characterized [3]: first, semisimple algebras of minimal rank are isomorphic to a finite direct product of division algebras of minimal rank (as considered by de Groote and Winograd) and of copies of $k^{2\times 2}$. Second, algebras of minimal rank over algebraically closed fields are isomorphic to a direct product of copies $k^{2\times 2}$ and a basic algebra B of minimal rank (as characterized by Heintz and Morgenstern). In [4], all algebras of minimal rank over perfect fields have finally been characterized. The result proven there states that an algebra over a perfect field k has minimal rank if and only if

$$A \cong C_1 \times \cdots \times C_s \times k^{2\times 2} \times \cdots \times k^{2\times 2} \times B \tag{1}$$

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 B is an algebra of minimal rank such that $B/\operatorname{rad} B \cong k^r$ for some r. In the following, we call algebras with $B/\operatorname{rad} B \cong k^r$ *superbasic*. The proof in [4] then continues by determining the superbasic algebras of minimal rank. This proof is even valid over arbitrary fields: a superbasic algebra B has minimal rank if and only if there exist $w_1, \dots, w_m \in \operatorname{rad} B$ with $w_i w_j = 0$ for $i \neq j$ such that

$$\operatorname{rad} B = \mathsf{L}_B + Bw_1B + \cdots + Bw_mB = \mathsf{R}_B + Bw_1B + \cdots + Bw_mB$$

and $\#k \geq 2N(B) - 2$. Here L_B and R_B denote the left and right annihilator of $\operatorname{rad} B$, that is, the set of all $x \in \operatorname{rad} B$ with $x(\operatorname{rad} B) = \{0\}$ or $(\operatorname{rad} B)x = \{0\}$, respectively. $N(B)$ is the largest natural number s such that $(\operatorname{rad} B)^s \neq \{0\}$.

New results. As our main result, we characterize all algebras of minimal rank over arbitrary fields (Theorem 1). After more than two decades, this answers a major open problem in algebraic complexity theory completely.

It turns out that the structure of the algebras of minimal rank over arbitrary fields is exactly the same as over perfect fields, as stated above in (1). A key tool in the proofs in [4] was a subalgebra B of A with $A/\operatorname{rad} A \cong B$ and $B \oplus \operatorname{rad} A$. Over perfect fields, such an algebra is guaranteed to exist by the Wedderburn–Malcev Theorem [7, Thm. 6.2.1]. (In fact, only the existence of B is needed in [4] and not the perfectness of the underlying field. Thus the results in [4] can be directly transferred to algebras such that $A/\operatorname{rad} A$ is separable.) One is perhaps tempted to conjecture that if such an algebra B does not exists, then the structure of A is "too irregular" and A is not an algebra of minimal rank. This conjecture is however wrong: let $k = \mathit{GF}(2)(t)$ for some indeterminate t and consider $A = k[X]/(X^4 - t^2)$ for some indeterminate X. We have $(X^4 - t^2) = (X^2 - t)^2$. Furthermore, $X^2 - t$ is irreducible, since k does not contain a square root of t. Hence $A \cong k[X]/(p^\ell)$ for some irreducible polynomial p and some $\ell \geq 1$. It is however well known that such algebras have minimal rank (over large enough fields), see [6, Sect. 17.4].

Astonishingly, the solution of the characterization problem over arbitrary fields required more new algebraic insights than novel lower bound techniques. Particularly, we show that the phenomenon of the non-existence of the above mentioned algebra B is in some sense "local". More precisely, we show that there always exists a subalgebra B of A with $B/\operatorname{rad} B \cong A/\operatorname{rad} A$ that has certain properties (Section 2). With this algebra, many of the techniques used in [3] and [4] can be transferred to the case of an arbitrary field. Still, some new lower bounds are needed (Section 3).

Organization of the paper. In Section 2, we derive some structural properties of associative algebras, which will enable us to deal with the difficulty that over non-perfect fields, a subalgebra B with $A/\operatorname{rad} A \cong B$ and $B \oplus \operatorname{rad} A$ need not exist. In Section 3, we prove our characterization results for the algebras of minimal rank over arbitrary fields. In the course of the proof of this main result, we rely on some lower bound techniques due to Alder and Strassen [1]. An overview of these techniques can be found in [3, Sect. 3.1]. For convenience, we will refer to [3, Sect. 3.1] instead of the original work of Alder and Strassen.

2 Structural Insights

In the proof of the characterization results in [4], the existence of a subalgebra B of A with $B \oplus \operatorname{rad} A = A$ and $B \cong A/\operatorname{rad} A$ plays a crucial role. Over perfect fields, such an algebra always exists by the Wedderburn–Malcev Theorem, see [7, Thm. 6.2.1]. Over non-perfect fields, such an algebra need not exist, see [7, Ch. 6, Ex. 4] for an example.

In the present section, we show that this phenomenon is in some sense "local". This enables us to transfer many of the techniques from [4] to the case of non-perfect fields. Instead of the above algebra B, we here use a lifting of the idempotents in $A/\operatorname{rad} A$. Let $\bar{\cdot} : A \to A/\operatorname{rad} A$ denote the canonical projection defined by $a \mapsto \bar{a} = a + \operatorname{rad} A$. Let $A_1 \oplus \cdots \oplus A_t$ be the decomposition of $A/\operatorname{rad} A$ into simple factors. We here write the decomposition of $A/\operatorname{rad} A$ in an additive way, that is, we consider the A_τ as subspaces of $A/\operatorname{rad} A$. This is done to simplify notations, mainly to write A_τ instead of $\{0\} \times \cdots \times \{0\} \times A_\tau \times \{0\} \times \cdots \times \{0\}$, which would be the corresponding subspace of $A_1 \times \cdots \times A_t$. Let e_τ denote the identity of A_τ for $1 \leq \tau \leq t$. Then $e_1 + \cdots + e_t$ is a *decomposition of the identity* of $A/\operatorname{rad} A$, that is,

1. $1 = e_1 + \cdots + e_t$,
2. the e_τ are idempotents, i.e., $e_\tau^2 = e_\tau$ for all τ, and
3. the e_τ annihilate each other, i.e., $e_\sigma e_\tau = 0$ for $\sigma \neq \tau$.

Now the crucial point is that this decomposition can be lifted to A: by [7, Cor. 3.3.9], there is a corresponding decomposition of the identity $1 = f_1 + \cdots + f_t$ in A such that

$$e_\tau = \bar{f}_\tau = f_\tau + \operatorname{rad} A \qquad \text{for all } \tau. \tag{2}$$

We remark that the decomposition $e_1 + \cdots + e_t$ is a *central* decomposition of the identity in $A/\operatorname{rad} A$, i.e., $e_\tau a = a e_\tau$ holds for all τ and for all $a \in A/\operatorname{rad} A$.

The next lemma shows that $B := f_1 A f_1 + \cdots + f_t A f_t$ is a subalgebra of A such that $B/\operatorname{rad} B \cong A_1 \oplus \cdots \oplus A_t$. Note that the algebra B always exists, particularly, its existence does not depend on the perfectness of the ground field. The important point is that we have found an algebra with $B/\operatorname{rad} B \cong A_1 \oplus \cdots \oplus A_t = A/\operatorname{rad} A$ for which $B \cap f_i A f_j = \{0\}$ holds for all $i \neq j$. (This is what we meant by "local".) In Section 3.2, we use this property to transfer many of the results from [4] for the case of a perfect field directly to the general case.

Lemma 1. *Let A be an algebra over an arbitrary field and $A_1 \oplus \cdots \oplus A_t$ be its decomposition into simple algebras. Let $f_1 + \cdots + f_t$ be a decomposition of the identity as in (2). Then the following holds:*

1. *$B := f_1 A f_1 + f_2 A f_2 + \cdots + f_t A f_t$ is a subalgebra of A,*
2. *$B_\tau := f_\tau A f_\tau$ is a subalgebra of B for all τ,*
3. *$B_\sigma \cdot B_\tau = \{0\}$ for all $\sigma \neq \tau$,*
4. *$\operatorname{rad} B_\tau = f_\tau (\operatorname{rad} A) f_\tau$ for all τ, and*
5. *$B_\tau / \operatorname{rad} B_\tau \cong A_\tau$ for all τ.*

Proof. 1. B is clearly closed under addition and scalar multiplication. It remains to show that it is also closed under multiplication. This follows from the fact that the f_τ annihilate each other: we have

$$\begin{aligned}(f_1 a_1 f_1 + \cdots + f_t a_t f_t)&(f_1 b_1 f_1 + \cdots + f_t b_t f_t) \\ &= f_1 a_1 f_1 b_1 f_1 + \cdots + f_t a_t f_t b_t f_t \in B,\end{aligned} \tag{3}$$

since $f_\sigma f_\tau = 0$ for $\sigma \neq \tau$.

2. B_τ is obviously closed under addition, scalar multiplication, and multiplication. Furthermore, f_τ is the identity of B_τ.
3. We have $f_\sigma a f_\sigma \cdot f_\tau a f_\tau = 0$ for all $f_\sigma a f_\sigma \in B_\sigma$ and $f_\tau b f_\tau \in B_\tau$, as $f_\sigma \cdot f_\tau = 0$.
4. Since $e_1 + \cdots + e_t$ is a central decomposition, this follows from [7, Thm. 3.5.3].
5. We have $A_\tau \cong e_\tau (A/\operatorname{rad} A) e_\tau$ where $e_1 + \cdots + e_t$ is a decomposition of the identity of $A/\operatorname{rad} A$ as in (2). On the other hand, $B_\tau = f_\tau A f_\tau / f_\tau (\operatorname{rad} A) f_\tau$ by the second and fourth statement. We define a mapping $i : A_\tau \to B_\tau$ by $e_\tau (a + \operatorname{rad} A) e_\tau \mapsto f_\tau a f_\tau + f_\tau (\operatorname{rad} A) f_\tau$. We claim that i is an isomorphism. First, i is well defined: consider elements a and b fulfilling $e_\tau (a + \operatorname{rad} A) e_\tau = e_\tau (b + \operatorname{rad} A) e_\tau$. Then by (2),

$$\begin{aligned} f_\tau a f_\tau + \operatorname{rad} A &= (f_\tau + \operatorname{rad} A)(a + \operatorname{rad} A)(f_\tau + \operatorname{rad} A) \\ &= (f_\tau + \operatorname{rad} A)(b + \operatorname{rad} A)(f_\tau + \operatorname{rad} A) \\ &= f_\tau b f_\tau + \operatorname{rad} A. \end{aligned} \tag{4}$$

Since $(f_j A f_\ell) \cap (f_{j'} A f_{\ell'}) = \{0\}$ for $j \neq j'$ or $\ell \neq \ell'$ (see for instance [7, Eq. 1.7.1]), (4) implies

$$i(a) = f_\tau a f_\tau + f_\tau(\operatorname{rad} A) f_\tau = f_\tau b f_\tau + f_\tau(\operatorname{rad} A) f_\tau = i(b).$$

Thus i is well defined.
Obviously, $i(\alpha x) = \alpha i(x)$ and $i(x + y) = i(x) + i(y)$ for all $x, y \in A_\tau$. For $x = e_\tau(a + \operatorname{rad} A)e_\tau$ and $y = e_\tau(b + \operatorname{rad} A)e_\tau$ in B_τ, we have

$$xy = e_\tau(a + \operatorname{rad} A)e_\tau \cdot e_\tau(b + \operatorname{rad} A)e_\tau = e_\tau(a f_\tau b + \operatorname{rad} A)e_\tau. \tag{5}$$

Hence,

$$\begin{aligned} i(xy) &= f_\tau a f_\tau b f_\tau + f_\tau(\operatorname{rad} A) f_\tau \\ &= (f_\tau a f_\tau + f_\tau(\operatorname{rad} A) f_\tau)(f_\tau b f_\tau + f_\tau(\operatorname{rad} A) f_\tau) \\ &= i(x) i(y). \end{aligned}$$

Finally, since $f_\tau a f_\tau \in f_\tau(\operatorname{rad} A) f_\tau$ if and only if $e_\tau(a + \operatorname{rad} A)e_\tau \subseteq \operatorname{rad} A$, i is also bijective. $\square$

3 Main Result

Throughout this section, k denotes an infinite field. This is no restriction, since finite fields are perfect and for perfect fields, the characterization results are proven in [4]. A denotes a k-algebra of minimal rank and $A_1 \oplus \cdots \oplus A_t$ denotes the decomposition of $A/\operatorname{rad} A$ into simple algebras. Again we write the decomposition in an additive way.

By [3, Cor. 3.4 & Lem. 3.6(i)], $A/\operatorname{rad} A$ is of minimal rank. By [3, Thm. 2], either $A_\tau \cong k$ or $A_\tau \cong k^{2\times 2}$ or A_τ is a proper extension field of k for all τ.

Let e_τ be the identity of A_τ and let $f_1 + \cdots + f_t$ be a decomposition of the identity of A as in (2). Consider the *Peirce decomposition* (see [7, p. 26]) of A with respect to $f_1, \ldots, f_t$:

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

Since $f_1, \ldots, f_t$ are idempotents that annihilate each other, the pairwise intersections of the $f_\sigma A f_\tau$ equal in fact $\{0\}$.

3.1 A First Decomposition Step

Assume that say A_1 is either an extension field 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 $j \ge 2$. Then we may decompose A according to the subsequent lemma.

Lemma 2. *With the above assumptions,*

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

Proof. Let $f' := f_2 + \cdots + f_t$. First note that $f_1 A f_1$ is an algebra by Lemma 1(2). Along the same lines, it is easy to see that $f' A f'$ is an algebra.

Since $e_\tau = f_\tau + \operatorname{rad} A$ is the identity of A_τ for all τ, e_τ is contained in the center of $A/\operatorname{rad} A$ (i.e., $e_\tau a = a e_\tau$ for all $a \in A/\operatorname{rad} A$). Thus by [7, Thm. 3.5.3], we have $f_\sigma A f_\tau = f_\sigma (\operatorname{rad} A) f_\tau$ for all $\sigma \neq \tau$. In particular, $f_1 A f_j = f_j A f_1 = \{0\}$ for all $j \geq 2$.

Let $a \in A$ be arbitrary. We can write $a = a_1 + a'$ with unique $a_1 \in f_1 A f_1$ and $a' \in f' A f'$, since $f_1 A f_1 \oplus f' A f' = A$. We define a mapping $A \to f_1 A f_1 \times f' A f'$ by $a \mapsto (a_1, a')$. Exploiting the facts that $f_1 A f' = f' A f_1 = \{0\}$ as well as $f_1 f' = f' f_1 = 0$, it is easy to verify that this is an isomorphism of algebras. $\square$

Next we show that if A has minimal rank, both $f_1 A f_1$ and $f' A f'$ have minimal rank. This follows directly from the work of Alder and Strassen.

Lemma 3. *Let B_1 and B_2 be two algebras. The algebra $B = B_1 \times B_2$ has minimal rank if and only if both B_1 and B_2 have minimal rank.*

Proof. Assume that B has minimal rank. Note that $\operatorname{rad} B = \operatorname{rad} B_1 \times \operatorname{rad} B_2$. By [3, Cor. 3.4 & Lem. 3.6(i)], $R(B) \geq 2 \dim \operatorname{rad} B_1 + R((B_1/\operatorname{rad} B_1) \times B_2)$. If we now apply [3, Lem. 3.6(ii)], we obtain $R(B) \geq 2 \dim B_1 - 1 + R(B_2)$. Thus B_2 has to have minimal rank. B_1 is treated completely alike.

The other direction is trivial. $\square$

By Lemma 3, the algebra $f_1 A f_1$ has to have minimal rank. By Lemma 1(5), we obtain $(f_1 A f_1)/\operatorname{rad}(f_1 A f_1) = e_1 (A/\operatorname{rad} A) e_1 \cong A_1$. By our assumption at the beginning of this subsection, A_1 either is an extension field of dimension at least two or isomorphic to $k^{2\times 2}$. In the first case, $f_1 A f_1$ is a local algebra with $\dim f_1 A f_1/(\operatorname{rad} f_1 A f_1) \geq 2$. Such algebras have been characterized by Büchi and Clausen [5]. They are isomorphic to $k[X]/(p(X)^m)$ for some irreducible polynomial p with $\deg p \geq 2$ and some $m \geq 1$. The second case is settled by the following lemma. It turns out that in this case, we necessarily have $f_1 A f_1 \cong k^{2\times 2}$.

Lemma 4. *Let C be an algebra fulfilling $C/\operatorname{rad} C \cong k^{2\times 2}$. Then $R(C) \geq \frac{5}{2} \dim C - 4$. In particular, if $\operatorname{rad} C \neq \{0\}$, then C is not of minimal rank.*

Proof. Let $\beta = (f_1, g_1, w_1, \ldots, f_r, g_r, w_r)$ be a bilinear computation for C. We may assume w.l.o.g. that $f_1, \ldots, f_N$ is a basis of C^*, where $N = \dim C$. Let $u_1, \ldots, u_N$ be its dual basis. Furthermore, assume that $\bar{u}_{N-3}, \ldots, \bar{u}_N$ is a basis of $C/\operatorname{rad} C \cong k^{2\times 2}$, where $\bar{\ } : C \to C/\operatorname{rad} C$ denotes the canonical projection. Choose $\alpha_1, \ldots, \alpha_4$ such that $1 = \alpha_1 \bar{u}_{N-3} + \cdots + \alpha_4 \bar{u}_N$ (in $C/\operatorname{rad} C$). By Nakayama's Lemma [7, Lem. 3.1.4], $\alpha_1 u_{N-3} + \cdots + \alpha_4 u_N$ is invertible in C. Exploiting a technique called sandwiching (see e.g. [3, Sect. 3.3]), we can achieve that $1 = \alpha_1 u_{N-3} + \cdots + \alpha_4 u_N$ in C. Choose $\xi_1, \ldots, \xi_4$ and $\eta_1, \ldots, \eta_4$ such that for $x = \xi_1 u_{N-3} + \cdots + \xi_4 u_N$ and $y = \eta_1 u_{N-3} + \cdots + \eta_4 u_N$,

$$\bar{x} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \bar{y} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

An easy calculation shows that $\bar{x}\bar{y} - \bar{y}\bar{x}$ is invertible in $C/\operatorname{rad} C$. Once more by Nakayama's Lemma, $xy - yx$ is invertible in C. Now by [3, Lem. 3.8] (with $m = N - 4$),

$$r \geq \tfrac{5}{2} \dim C - 4. \tag{6}$$

Since $C/\operatorname{rad} C \cong k^{2\times 2}$, the algebra $C/\operatorname{rad} C$ is separable, that is, for any extension field K of k, $(C/\operatorname{rad} C) \otimes K \cong K^{2\times 2}$ is semisimple. By the Wedderburn–Malcev Theorem [7, Thm. 6.2.1], C contains a subalgebra $C' \cong k^{2\times 2}$ with $C' \oplus \operatorname{rad} C = C$. Hence $\operatorname{rad} C$ is a $k^{2\times 2}$-bimodule. By [3, Fact 8.5], $\operatorname{rad} C \neq \{0\}$ implies $\dim \operatorname{rad} C \geq 4$. Now we can rewrite (6) as

$$r \geq \tfrac{5}{2} \dim C - 4 = 2 \dim C + \underbrace{\tfrac{1}{2}(4 + \dim \operatorname{rad} C) - 4}_{\geq 0 \text{ if } \operatorname{rad} C \neq \{0\}}.$$

This proves the second statement. $\square$

By [7, Thm. 3.5.3], $\operatorname{rad}(f'Af') = f'(\operatorname{rad} A)f'$ holds. From this, it follows that $(f'Af')/\operatorname{rad}(f'Af') = e'(A/\operatorname{rad} A)e' = A_2 \oplus \cdots \oplus A_t$ as in the proof of Lemma 1(5), where $e' = e_2 + \cdots + e_t$. Hence we can proceed recursively with $f'Af'$. The following lemma summarizes the above considerations.

Lemma 5. *Let A be an algebra of minimal rank over an arbitrary field k. Then*

$$A \cong C_1 \times \cdots \times C_s \times \underbrace{k^{2\times 2} \times \cdots \times k^{2\times 2}}_{u \text{ times}} \times B,$$

where

1. *the C_σ are local algebras of minimal rank with $\dim C_\sigma/\operatorname{rad} C_\sigma \geq 2$ and*
2. *B is an algebra of minimal rank.*

Furthermore, if $B_1 \oplus \cdots \oplus B_r$ is a decomposition of $B/\operatorname{rad} B$ into simple factors, e_ρ denotes the identity of B_ρ for $1 \leq \rho \leq r$, and $f_1 + \cdots + f_r$ is a decomposition of the identity of B as in (2), then for all B_ρ such that B_ρ is either isomorphic $k^{2\times 2}$ or a proper extension field of k, there is a $j_\rho \neq \rho$ such that $f_\rho(\operatorname{rad} A)f_{j_\rho} \neq \{0\}$ or $f_{j_\rho}(\operatorname{rad} A)f_\rho \neq \{0\}$. Above, s and u may be zero and the factor B is optional. $\square$

3.2 B is Superbasic

The aim of the present section is to show that the algebra B in Lemma 5 is always superbasic, that is, all the B_ρ in the decomposition of $B/\operatorname{rad} B$ into simple algebras are isomorphic to k. To do so, we construct under the assumption that one of the factors B_ρ is not isomorphic to k, some algebras that have to have minimal rank because B has minimal rank. Then we prove that none of the constructed algebras has minimal rank, obtaining a contradiction.

The next lemma shows that it suffices to consider the problem modulo $(\operatorname{rad} B)^2$. The lemma holds for arbitrary algebras C: let $\tilde{\ } : C \to C/(\operatorname{rad} C)^2$ denote the canonical projection defined by $a \mapsto \tilde{a} = a + (\operatorname{rad} C)^2$.

Lemma 6. *Let C be an algebra and $C_1 \oplus \cdots \oplus C_r$ be the decomposition of $C/\operatorname{rad} C$ into simple factors. Let e_ρ be the unit element of C_ρ for all ρ and let $f_1 + \cdots + f_r$ be a decomposition of the identity as in (2). For all indices i and j with $i \neq j$ such that $f_i(\operatorname{rad} C)f_j \neq \{0\}$, there is an index j' with $i \neq j'$ such that $\tilde{f}_i(\operatorname{rad} \tilde{C})\tilde{f}_{j'} \neq \{0\}$. In the same way, there is an index i' with $i' \neq j$ such that $\tilde{f}_{i'}(\operatorname{rad} \tilde{C})\tilde{f}_j \neq \{0\}$.*

Proof. Let x such that $f_i x f_j \neq 0$ and $f_i x f_j \in f_i(\operatorname{rad} C)f_j$. Since $f_i C f_j = f_i(\operatorname{rad} C)f_j$ by [7, Thm. 3.5.3], we may assume $x \in \operatorname{rad} C$. Let $n \geq 1$ be the unique number such that $x \in (\operatorname{rad} C)^n \setminus (\operatorname{rad} C)^{n+1}$. By definition, there are $x_1, \dots, x_n \in \operatorname{rad} C \setminus (\operatorname{rad} C)^2$ such that $x = x_1 \cdots x_n$. Since $1 = f_1 + \cdots + f_r$,

$$f_i x_1 (f_1 + \cdots + f_r) x_2 (f_1 + \cdots + f_r) \cdots (f_1 + \cdots + f_r) x_n f_j = f_i x f_j \neq 0.$$

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

$$f_i x_1 f_{h_1} x_2 f_{h_2} \cdots f_{h_{n-1}} x_n f_j \neq 0.$$

If all h_ν equal i, then $f_{h_{n-1}} x_n f_j = f_i x_n f_j \neq 0$ and we set $j' = j$. Since $f_i x_n f_{j'} \in \operatorname{rad} C \setminus (\operatorname{rad} C)^2$, $\tilde{f}_i \tilde{x}_n \tilde{f}_{j'} \neq 0$, hence we are done. Otherwise let ν_0 be the smallest index such that $h_{\nu_0} \neq i$. Now we set $j' = h_{\nu_0}$ and can conclude in the same way as before that $\tilde{f}_i(\operatorname{rad} \tilde{C})\tilde{f}_{j'} \neq \{0\}$.

The index i' is constructed completely alike. □

Assume that w.l.o.g. B_1 is either isomorphic to $k^{2\times 2}$ or a proper extension field of k. We first construct two algebras which have to have minimal rank, since B has minimal rank. Next we prove that these algebras cannot have minimal rank if B_1 is isomorphic to $k^{2\times 2}$ or a proper extension field of k. Hence $B_1 \cong k$ must hold. By symmetry, this has to hold for all $B_1, \dots, B_r$. It follows that B is superbasic.

We decompose $\operatorname{rad} B$ as

$$\operatorname{rad} B = \bigoplus_{1 \leq \rho, \eta \leq r} f_\rho (\operatorname{rad} B) f_\eta. \tag{7}$$

By Lemma 5, there is an index $j \geq 2$ such that $f_1(\operatorname{rad} B)f_j \neq \{0\}$. The case where $f_j(\operatorname{rad} B)f_1 \neq \{0\}$ is treated symmetrically. By Lemma 6, there is an $j' \geq 2$ such that $\tilde{f}_1(\operatorname{rad} \tilde{B})\tilde{f}_{j'} \neq \{0\}$. W.l.o.g. $j' = 2$.

Consider $C := f_1 B f_1 + f_2 B f_2$. As in Lemma 1(1), it is easy to see that C is a subalgebra of B. As in Lemma 1(4), $\operatorname{rad} C = f_1(\operatorname{rad} B)f_1 + f_2(\operatorname{rad} B)f_2$. Finally $C/\operatorname{rad} C \cong B_1 \oplus B_2$. Since the pairwise intersection of the $f_\rho(\operatorname{rad} B)f_\eta$ in (7) are the nullspace, we also have $C/\operatorname{rad} B \cong B_1 \oplus B_2$.

Let

$$I = \bigoplus_{(\rho,\eta)\neq(1,2)} f_\rho (\operatorname{rad} B) f_\eta.$$

From $(\operatorname{rad} B)^2 \subseteq I$, it follows that I is a twosided ideal of B (see also [3, p. 105]). Since B is of minimal rank and $I \subseteq \operatorname{rad} B$, B/I is also of minimal rank by [3, Cor. 3.4 & Lem. 3.6(i)]. By [7, Cor. 3.1.14], we have $(\operatorname{rad} B/I) = (\operatorname{rad} B)/I \cong f_1(\operatorname{rad} B)f_2/I \neq \{0\}$. Let $\hat{\ } : B \to B/I$ denote the canonical projection defined by $a \mapsto \hat{a} = a + I$. Since $I \subseteq \operatorname{rad} B$, $\hat{f}_1, \dots, \hat{f}_r$ are idempotent elements that annihilate each other, because this also holds for $f_1, \dots, f_r$. Let $\hat{f} = \hat{f}_3 + \cdots + \hat{f}_r$. Then for all $a \in \hat{f}(B/I)\hat{f}$, we have $a(\operatorname{rad} B/I) = (\operatorname{rad} B/I)a = \{0\}$, since the $\hat{f}_\rho$ annihilate each other. Thus by [3, Lem. 8.3]

$$B/I \cong (\hat{f}_1 + \hat{f}_2)(B/I)(\hat{f}_1 + \hat{f}_2) \times \hat{f}(B/I)\hat{f}.$$

By Lemma 3, B/I is of minimal rank only if $D := (\hat{f}_1 + \hat{f}_2)(B/I)(\hat{f}_1 + \hat{f}_2)$ is of minimal rank. The next two paragraphs show that this cannot be the case. Hence we have obtained the following lemma.

Lemma 7. *The algebra B in Lemma 5 is superbasic.* □

Before we prove the two statements mentioned above, we first collect some structural properties of D. Because $C := f_1 B f_1 + f_2 B f_2$ is a subalgebra of $(f_1 + f_2)B(f_1 + f_2)$, $\hat{C}$ is a subalgebra of D. This subalgebra $\hat{C}$ is isomorphic to $B_1 \oplus B_2$, since $\operatorname{rad} C = f_1(\operatorname{rad} B)f_1 + f_2(\operatorname{rad} B)f_2$. Hence D has a subalgebra that is isomorphic to $B_1 \oplus B_2$. The radical of D is $\operatorname{rad} D \cong f_1(\operatorname{rad} B)f_2/I \neq \{0\}$.

Case 1: B_1 is isomorphic to $k^{2\times 2}$. The radical $\operatorname{rad} D$ is a nonzero B_1-left module and a nonzero B_2-right module. Moreover, D is isomorphic to $B_1 \times B_2 \times \operatorname{rad} D$ equipped with the multiplication law $(a, b, c)(a', b', c') = (aa', bb', ac' + cb')$. Now [3, Lem. 8.7] shows that C is not of minimal rank if $B_2 \cong k$. If $B_2 \cong k^{2\times 2}$, then this follows from [3, Lem. 8.8]. Finally, the case where B_2 is a proper extension field of k is settled by [4, Lem. 20].

Case 2: B_1 is a proper extension field. First note that we may assume that B_2 is also an extension field of k. If B_2 was isomorphic to $k^{2\times 2}$, then we could exchange the roles of B_1 and B_2. But this case has already been treated above. Now [4, Lem. 19] shows that C cannot have minimal rank. This completes the proof of Lemma 7.

3.3 The Final Proof

By Lemma 5, A is isomorphic to

$$A \cong C_1 \times \cdots \times C_s \times \underbrace{k^{2\times 2} \times \cdots \times k^{2\times 2}}_{u \text{ times}} \times B,$$

where the C_σ are local algebras of minimal rank with $\dim C_\sigma / \operatorname{rad} C_\sigma \geq 2$. By Lemma 7, B is a superbasic algebra of minimal rank. By exploiting the characterization results in [4] for superbasic algebras of minimal rank (which were proven there for arbitrary fields), we obtain the desired characterization of algebras of minimal rank over arbitrary fields.

Theorem 1. *An algebra A over an arbitrary field k is an algebra of minimal rank if and only if*

$$A \cong C_1 \times \cdots \times C_s \times \underbrace{k^{2\times 2} \times \cdots \times k^{2\times 2}}_{u \text{ times}} \times B \tag{8}$$

where $C_1, \dots, C_s$ are local algebras of minimal rank with $\dim(C_\sigma / \operatorname{rad} C_\sigma) \geq 2$, i.e., $C_\sigma \cong k[X]/(p_\sigma(X)^{d_\sigma})$ 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 B is a superbasic algebra of minimal rank, that is, there exist $w_1, \dots, w_m \in \operatorname{rad} B$ with $w_i w_j = 0$ for $i \neq j$ such that

$$\operatorname{rad} B = \mathsf{L}_B + Bw_1B + \cdots + Bw_mB = \mathsf{R}_B + Bw_1B + \cdots + Bw_mB$$

and $\#k \geq 2N(B) - 2$. Any of the integers s, u, or m may be zero and the factor B in (8) is optional.

The results for finite fields follow also from [4], because finite fields are perfect.

References

1. A. Alder and V. Strassen. On the algorithmic complexity of associative algebras. *Theoret. Comput. Sci.*, 15:201–211, 1981.
2. Markus Bläser. Lower bounds for the multiplicative complexity of matrix multiplication. *Comput. Complexity*, 8:203–226, 1999.
3. Markus Bläser. Lower bounds for the bilinear complexity of associative algebras. *Comput. Complexity*, 9:73–112, 2000.
4. Markus Bläser. Algebras of minimal rank over perfect fields. In *Proc. 17th Ann. IEEE Computational Complexity Conf. (CCC)*, pages 113–122, 2002.
5. Werner Büchi and Michael Clausen. On a class of primary algebras of minimal rank. *Lin. Alg. Appl.*, 69:249–268, 1985.
6. Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic Complexity Theory.* Springer, 1997.
7. Yurij A. Drozd and Vladimir V. Kirichenko. *Finite Dimensional Algebras.* Springer, 1994.
8. 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.
9. Hans F. de Groote and Joos Heintz. Commutative algebras of minimal rank. *Lin. Alg. Appl.*, 55:37–68, 1983.
10. 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.
11. Volker Strassen. Gaussian elimination is not optimal. *Num. Math.*, 13:354–356, 1969.
12. 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.
13. Shmuel Winograd. On multiplication in algebraic extension fields. *Theoret. Comput. Sci.*, 8:359–377, 1979.