Semisimple algebras of almost minimal rank over the reals

Markus Bläser[1] and Andreas Meyer de Voltaire[2]

[1] Computer Science Department, Saarland University
[2] Chair of Information Technology and Education, ETH Zurich

Abstract. A famous lower bound for the bilinear complexity of the multiplication in associative algebras is the Alder–Strassen bound. Algebras for which this bound is tight are called algebras of minimal rank. After 25 years of research, these algebras are now well understood. We here start the investigation of the algebras for which the Alder–Strassen bound is off by one. As a first result, we completely characterize the semisimple algebras over $\mathbb{R}$ whose bilinear complexity is by one larger than the Alder–Strassen bound.

1 Introduction

A central problem in algebraic complexity theory is the question about the costs of multiplication in associative algebras. 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 $v_\mu v_\nu = \sum_{\kappa=1}^{N} \alpha_{\mu,\nu}^{(\kappa)} v_\kappa$ for $1 \le \mu, \nu \le N$ 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 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 maximal twosided ideals in A. This bound is sharp in the sense that there are algebras for which equality holds. For instance, for $A = k^{2\times 2}$, we get a lower bound of 7, since $k^{2\times 2}$ is a simple algebra and has only one maximal twosided ideal (other than $k^{2\times 2}$). 7 is a sharp bound, since we can multiply 2×2–matrices with 7 multiplications by Strassen's algorithm.

An algebra A has **minimal rank** if the Alder–Strassen bound is sharp, that is, the rank of A equals twice the dimension minus the number of maximal two-sided ideals. After 25 years of effort [7, 8, 5, 9], the algebras of minimal rank were finally characterized in terms of their algebraic structure [4]: An algebra over some 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 characterized in [5]), $\#k \geq 2\dim C_\sigma - 2$, and A' is an algebra of minimal rank such that $A'/\operatorname{rad} A' \cong k^t$ for some t. Such an algebra A' 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

$$\operatorname{rad} A = \mathsf{L}_A + Aw_1A + \cdots + Aw_mA = \mathsf{R}_A + Aw_1A + \cdots + Aw_mA$$

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 $(\operatorname{rad} A)^s \neq \{0\}$.

Algebraic preliminaries. In this work, the term **algebra** always means a finite dimensional associative algebra with unity 1 over some field k. The terms **left module** and **right module** always means a finitely generated left module and right module, respectively, over some algebra A. Every A-left module and A-right module is also a finite dimensional k-vector space (by the embedding $k \mapsto k\cdot 1$). If we speak of a basis of an algebra or a module, we always mean a basis of the underlying vector space.

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. For all finite dimensional algebras A, 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.

We call an algebra A **semisimple**, if $\operatorname{rad} A = \{0\}$. The quotient algebra $A/\operatorname{rad} A$ is semisimple. An algebra A is called **simple**, if there are no twosided ideals in A except the zero ideal and A itself. Wedderburn's theorem states that every semisimple algebra A is isomorphic to a product of simple algebras and every simple algebra is of the form $D^{n\times n}$ for some division algebra D.

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. For a set of vectors U, $\langle U\rangle$ denotes the linear span of U, i.e., the smallest vector space that contains U.

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*

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

2. *The length of a shortest bilinear computation for ϕ is called the bilinear complexity or the rank of ϕ and is denoted by $R(\phi)$ or $R_k(\phi)$ if we want to stress the underlying field k.*
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 $R(A)$ or $R_k(A)$.*

Equivalence of computations. Often, proofs become simpler when we normalize computations. A simple equivalence transformation of computations is the **permutation** of the products.

Trickier is the so-called **sandwiching**. Let $\beta = (f_1, g_1, w_1; \ldots; f_r, g_r, w_r)$ be a computation for an algebra A, i.e.,

$$xy = \sum_{\rho=1}^{r} f_\rho(x) g_\rho(y) w_\rho.$$

Let a, b, c be invertible elements of A. Then

$$xy = a(a^{-1}xb)(b^{-1}yc)c^{-1} = \sum_{\rho=1}^{r} f_\rho(a^{-1}xb) g_\rho(b^{-1}yc) a w_\rho c^{-1}.$$

Thus we can replace each f_ρ by $\hat{f}_\rho$ defined by $\hat{f}_\rho(x) = f_\rho(a^{-1}xb)$, g_ρ by $\hat{g}_\rho$ defined by $\hat{g}_\rho(y) = g_\rho(b^{-1}yc)$, and w_ρ by $\hat{w}_\rho = a w_\rho c^{-1}$.

For the next two equivalence transformations, we assume that A is a simple algebra, that is, $A \cong D^{n \times n}$ for some division algebra A. For an element $x \in A$, x^T denotes the transposed of x. Let $\beta = (f_1, g_1, w_1; \ldots; f_r, g_r, w_r)$ be a computation for an algebra A. Then

$$y^T x^T = (xy)^T = \sum_{\rho=1}^{r} \tilde{g}_\rho(y^T) \tilde{f}_\rho(x^T) w_\rho^T,$$

where $\tilde{g}_\rho(y)$ is defined by $\tilde{g}_\rho(y) := g_\rho(y^T)$ and $\tilde{f}_\rho(x)$ is defined by $\tilde{f}_\rho(x) := f_\rho(x^T)$. So we can change the f's with the g's (at the cost of **transposing** the w's but this will not do any harm since in our proofs, we usually only care about the rank of the w_ρ and other quantities that are invariant under transposing).

Finally, with every matrix $x \in A$, we can associate a linear form, namely, $y \mapsto \langle\langle x, y \rangle\rangle$, where $\langle\langle ., . \rangle\rangle$ denotes the standard inner product. (We here view x and y as vectors in $k^{n^2 \cdot \dim D}$.) In this way, we will often identify f_ρ with an element of A, which we abusively call f_ρ again. For all $x, y \in A$ we have

$$xy = \sum_{\rho=1}^{r} f_\rho(x) g_\rho(y) w_\rho \qquad \text{iff} \qquad \langle\langle xy, z \rangle\rangle = \sum_{\rho=1}^{r} \langle\langle f_\rho, x \rangle\rangle \langle\langle g_\rho, y \rangle\rangle \langle\langle w_\rho, z \rangle\rangle$$

for all $z \in A$. Since $\langle\langle xy, z \rangle\rangle = \langle\langle xyz^T, 1 \rangle\rangle = \mathrm{trace}(xyz^T)$ and $\mathrm{trace}(xyz^T) = \mathrm{trace}(z^T xy) = \mathrm{trace}(yz^T x)$, we can **cyclically shift** the f's, g's, and w's in this way. Altogether, the latter two equivalence transformations allow us to permute the f's, g's, and w's in an arbitrary way.

Our results. It is a natural question to ask which are the algebras whose rank is exactly one larger than the minimum.[3] We say that an algebra has **minimal rank plus one** if

$$R(A) = 2 \dim A - t + 1,$$

where t is the number of maximal twosided ideals in A. We completely solve this question here for semisimple algebras over $\mathbb{R}$. A semisimple $\mathbb{R}$-algebra has minimal rank plus one iff $A = \mathbb{H} \times B$ where B is a semisimple algebra of minimal rank, that is, $B = \mathbb{C}^{2\times 2} \times \cdots \times \mathbb{C}^{2\times 2} \times \mathbb{C} \times \cdots \times \mathbb{C} \times \mathbb{R} \times \cdots \times \mathbb{R}$. Note that over $\mathbb{R}$, there is only one division algebra of dimension two, namely the complex numbers $\mathbb{C}$ (viewed as an $\mathbb{R}$-algebra), and one division algebra of dimension four, the **Hamiltonian quaternions** $\mathbb{H}$. There are no further nontrivial $\mathbb{R}$-division algebras. $\mathbb{C}$ is also the only commutative division algebra, that is, extension field over $\mathbb{R}$.

Characterization results as the one that we prove in this paper are important, since they link the algebraic structure of an algebra to the complexity. We can read off the complexity of the algebra from its structure or get at least lower bounds by inspecting the algebraic structure.

One result on the way of our characterization is a new lower bound of 17 for $\mathbb{C}^{2\times 2}$ (viewed as an $\mathbb{R}$-algebra). This bound holds for any other extension field of dimension two over arbitrary fields. This new bound improves the current best answer to an open question posed by Strassen [10, Section 12, Problem 3].

Outline of the proof. A semisimple algebra A consists of simple factors of the form $D^{n\times n}$, where D is a division algebra. It follows from results by Alder and Strassen that no factor of A can have rank $\geq 2 \dim D^{n\times n} + 1$ and at least one factor has to have rank $2 \dim D^{n\times n}$, i.e., has minimal rank plus one. We show that the only simple $\mathbb{R}$-algebra that has minimal rank plus one is $\mathbb{H}$, the Hamiltonian quaternions. In particular, we show that $\mathbb{C}^{2\times 2}$ does not have minimal rank plus one in Section 3. (This is the "hardest case".) Next, we show that A cannot have two factors of the form $\mathbb{H}$ in Section 2. With this, we show the characterization result in Section 4 (Theorem 3).

2 A lower bound for $\mathbb{H} \times \mathbb{H}$ over $\mathbb{R}$

In this section, we will prove the the following theorem.

Theorem 1. *We have* $R_{\mathbb{R}}(\mathbb{H} \times \mathbb{H}) = 16$.

Proof. It is well known that $R_{\mathbb{R}}(\mathbb{H}) = 8$, which implies that $R_{\mathbb{R}}(\mathbb{H} \times \mathbb{H}) \leq 16$. To prove the lower bound, we first will show the following claim:

Claim. *If x, $y \in \mathbb{H}$ are such that x, y, and 1 are linearly independent over $\mathbb{R}$, then* $\langle 1, x, y, x{\cdot}y \rangle = \mathbb{H}$.

Let x, $y \in \mathbb{H}$ have the above mentioned properties. The inner automorphisms act on $\mathbb{H}$ via rotation in $\mathbb{R}^3$ on the last three coordinates of each quaternion. Hence, we

[3] This already characterizes the algebras in terms of complexity. Of course, we seek a characterization in terms of their algebraic structure.

can assume w.l.o.g. that $x = x_1{\cdot}1 + x_2{\cdot}i$ and $y = y_1{\cdot}1 + y_2{\cdot}i + y_3{\cdot}j$, x_ν, $y_\nu \in \mathbb{R}$. Since 1, x, and y are still linearly independent, we know that $x_2 \neq 0 \neq y_3$ and hence $\langle 1, x, y\rangle = \langle 1, i, j\rangle$. Furthermore, the last coordinate of $x{\cdot}y$ equals $x_2 y_3$ and is hence not equal to zero, which proves the claim.

Let $\beta = (f_1, g_1, w_1; \ldots; f_r, g_r, w_r)$ be a computation for $\mathbb{H} \times \mathbb{H}$. We can choose two elements $\hat{a} = (a, a')$ and $\hat{b} = (b, b') \in \mathbb{H} \times \mathbb{H}$ such that their span is contained in the intersection of at least six of the kernels of $f_1, \ldots, f_r$ and a and b are linearly independent vectors in $\mathbb{R}^4$. W.l.o.g., assume that $\langle \hat{a}, \hat{b}\rangle \subseteq \ker f_1 \cap \cdots \cap \ker f_6$.

If for all possible choices $a' = 0$ and $b' = 0$, then we can split the computation into two separate computations for $\mathbb{H}$ and get a lower bound of $8 + 8 = 16$. Thus we can assume that $a' \neq 0$. Via sandwiching, we can achieve that $a = 1$ and furthermore, by letting inner automorphisms act, that $b \in \langle 1, i\rangle$. Since $a' \neq 0$, it follows that $g_7, \ldots, g_r$ generate $(\mathbb{H} \times \mathbb{H})^*$. Now, choose a vector $\hat{c} = (c, c')$, $c \neq 0$, that is contained in the intersection of the kernels of at least seven of the vectors $g_7, \ldots, g_r$ and use sandwiching to achieve $c = 1$. W.l.o.g., let $\hat{c}$ be contained in $\ker g_7 \cap \cdots \cap \ker g_{13}$. Finally, we can choose an element $\hat{d} = (d, d')$ in the intersection of the kernels of at least six of $g_7, \ldots, g_{13}$ such that 1, b, and d are linearly independent over $\mathbb{R}$. W.l.o.g., assume that $\langle \hat{c}, \hat{d}\rangle \subseteq \ker g_9 \cap \cdots \cap \ker g_{12}$. The above claim shows that $a{\cdot}c = 1$, $a{\cdot}d = d$, $b{\cdot}c = b$, and $b{\cdot}d$ span $\mathbb{H}$. In particular, the products $\hat{a}{\cdot}\hat{c}$, $\hat{a}{\cdot}\hat{d}$, $\hat{b}{\cdot}\hat{c}$, and $\hat{b}{\cdot}\hat{d}$ span a four dimensional vector space over $\mathbb{R}$. On the other hand, we know that by construction, each of these products lies in the span of $\langle w_{13}, \ldots, w_r\rangle$. Hence, r has to be at least 16. $\square$

3 A lower bound for $\mathbb{C}^{2\times 2}$ over $\mathbb{R}$

The goal of this section is to prove the following theorem.

Theorem 2. *We have* $R_{\mathbb{R}}(\mathbb{C}^{2\times 2}) \geq 17$.

We will prove this theorem in two steps. We define the following property for computations. A computation $\beta := (f_1, g_1, w_1; \ldots; f_r, g_r, w_r)$ has the property (*) if the following holds:

(*) Let $x \in \mathbb{C}^{2\times 2} \setminus \{0\}$ such that there exist three different indices ν_1, ν_2, and $\nu_3 \in \{1, \ldots, r\}$ such that

$$\langle x, i{\cdot}x\rangle \subseteq \ker f_{\nu_1} \cap \ker f_{\nu_2} \cap \ker f_{\nu_3} \text{ or}$$
$$\langle x, i{\cdot}x\rangle \subseteq \ker g_{\nu_1} \cap \ker g_{\nu_2} \cap \ker g_{\nu_3} \text{ or}$$
$$\langle x, i{\cdot}x\rangle \subseteq \langle w_{\nu_1}, w_{\nu_2}, w_{\nu_3}\rangle^{\perp},$$

where $V^{\perp}$ is the space of all vectors u that fulfill $\langle\langle v, u\rangle\rangle = 0$ for all $v \in V$. Then x is a matrix of rank two.

In Subsection 3.1 we show that a computation for $\mathbb{C}^{2\times 2}$ of length 16 must satisfy (*) and in Subsection 3.2 we show that no such computation exists.

3.1 Computations not satisfying property (*)

For a field k, let $\langle e,h,l\rangle_k$ denote the matrix multiplication tensor of dimensions $e\times h$, $h\times l$, and $e\times l$ having coefficients in k.

Lemma 1. $R_{\mathbb{R}}(\langle 1,1,2\rangle_{\mathbb{C}})=6$.

Proof. This tensor has rank at most six, since the complex multiplication has rank three over $\mathbb{R}$. Assume that there exists a computation $(f_1,g_1,w_2;\ldots;f_5,g_5,w_5)$ of length five for $\langle 1,1,2\rangle$. Then we can (possibly after permuting the products) assume that f_1, f_2 are a basis of $\mathbb{C}^*$ and that $g_2,\ldots,g_5$ form a basis of $(\mathbb{C}^{1\times 2})^*$. Let x_1, x_2 and $y_1,\ldots,y_4$ be the bases dual to f_1, f_2 and $g_2,\ldots,g_5$, respectively. Then we can choose an index $\nu\in\{2,\ldots,4\}$ such that y_1 and y_ν are linearly independent over $\mathbb{C}$, which means that the span of $\langle x_1y_1,x_1y_\nu,x_2y_1,x_2y_\nu\rangle$ is a four dimensional vector space over $\mathbb{R}$. But for $i\in\{1,2\}$ and $j\in\{1,\nu\}$, $x_iy_j\in\langle w_1,w_2,w_\nu\rangle$. Since the latter is a vector space over $\mathbb{R}$ with dimension at most three, we get a contradiction. □

Lemma 2. *Let u, v, and $w\in\mathbb{C}^{2\times 2}$ and assume that there exists a rank one matrix x such that $\langle x,ix\rangle\subset\langle u,v,w\rangle^\perp$ over $\mathbb{R}$. Then we can find invertible matrices a and b such that $(aub)_{11}=(avb)_{11}=(awb)_{11}=0$, where $(.)_{11}$ denotes the entry in position $(1,1)$.*

Proof. Let $x=(x_{11},x_{12},x_{21},x_{22})$, $x_{\nu\mu}=(x'_{\nu\mu},x''_{\nu\mu})\in\mathbb{C}$, be a matrix with the above property. (To save some space, we write matrices occasionally as column vectors.) Let z be any of the vectors u, v, or w. The vectors $-ix$ (for convenience) and x being perpendicular to $z=(z_{11},z_{12},z_{21},z_{22})$, $z_{\nu\mu}=(z'_{\nu\mu},z''_{\nu\mu})\in\mathbb{C}$, means that we have

$$\sum_{\nu,\mu=1}^{2}\begin{pmatrix}x''_{\nu\mu} & -x'_{\nu\mu}\\ x'_{\nu\mu} & x''_{\nu\mu}\end{pmatrix}\begin{pmatrix}z'_{\nu\mu}\\ z''_{\nu\mu}\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}.\quad\text{Since the matrix}\quad\begin{pmatrix}x''_{\nu\mu} & -x'_{\nu\mu}\\ x'_{\nu\mu} & x''_{\nu\mu}\end{pmatrix}$$

is the left multiplication matrix of $\hat{x}_{\nu\mu}=i\cdot\bar{x}_{\nu\mu}$, we can also write the above sum as $\sum_{\nu,\mu=1}^{2}\hat{x}_{\nu\mu}\cdot z_{\nu\mu}=0$. Note that the matrix $\hat{x}:=(\hat{x}_{11},\hat{x}_{12},\hat{x}_{21},\hat{x}_{22})$ with $\hat{x}_{\nu\mu}:=i\cdot\bar{x}_{\nu\mu}=(x''_{\nu\mu},x'_{\nu\mu})$ has rank one, too. On the other hand, multiplying z from the left by $a=(a_{11},a_{12},a_{21},a_{22})$ an from the right by $b=(b_{11},b_{12},b_{21},b_{22})$ yields $(azb)_{11}=a_{11}b_{11}z_{11}+a_{11}b_{21}z_{12}+a_{12}b_{11}z_{21}+a_{12}b_{21}z_{22}$. Hence, we have to find a_{11}, a_{12}, b_{11}, $b_{21}\in\mathbb{C}$ such that $a_{11}b_{11}=\hat{x}_{11}$, $a_{11}b_{21}=\hat{x}_{12}$, $a_{12}b_{11}=\hat{x}_{21}$, and $a_{12}b_{21}=\hat{x}_{22}$. This is equivalent to finding two 2-dimensional vectors (a_{11},a_{12}) and (b_{11},b_{21}) with complex entries such that

$$(a_{11},a_{12})\otimes(b_{11},b_{21})=\begin{pmatrix}\hat{x}_{11} & \hat{x}_{12}\\ \hat{x}_{21} & \hat{x}_{22}\end{pmatrix}.$$

This is possible if and only if $\hat{x}$ has rank one, which had been one of our assumptions. Furthermore, since $\hat{x}\neq 0$, neither both a_{11} and a_{12} nor both b_{11} and b_{21} can be zero. Hence, we can construct invertible matrices $(a_{11},a_{12},a_{21},a_{22})$ and $(b_{11},b_{12},b_{21},b_{22})$ such that $(azb)_{11}=0$ for all $z\in\{u,v,w\}$. □

Proposition 1. *Let $\beta:=(f_1,g_1,w_1;\ldots;f_r,g_r,w_r)$ be a computation that does not satisfy (*). Then $r\geq 17$.*

Proof. Since β does not satisfy (*), we can find three indices ν_1, ν_2, $\nu_3 \in \{1, \ldots, r\}$ and a rank one matrix x such that $\langle x, i{\cdot}x\rangle \subseteq \ker f_{\nu_1} \cap \ker f_{\nu_2} \cap \ker f_{\nu_3}$, $\langle x, i{\cdot}x\rangle \subseteq \ker g_{\nu_1} \cap \ker g_{\nu_2} \cap \ker g_{\nu_3}$, or $\langle x, i{\cdot}x\rangle \subseteq \langle w_{\nu_1}, w_{\nu_2}, w_{\nu_3}\rangle^{\perp}$. W.l.o.g., assume that $\nu_1 = 1$, $\nu_2 = 2$, and $\nu_3 = 3$ and that $\langle x, i{\cdot}x\rangle \subseteq \langle w_1, w_2, w_2\rangle^{\perp}$, for otherwise, we could exchange the f's or g's with the w's.[4] Then, by Lemma 2, we can achieve (via sandwiching) that

$$W := \langle w_1, w_2, w_3\rangle \subseteq \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}.$$

Define the two left and two right ideals L_1, L_2, R_1, and R_2 as follows:

$$L_1 := \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}, \quad L_2 := \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}, \quad R_1 := \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}, \quad \text{and} \quad R_2 := \begin{pmatrix} 0 & 0 \\ * & * \end{pmatrix}$$

Each ideal is a four dimensional vector space over $\mathbb{R}$. For the following claims, define the computation $\beta' := (\tilde{g}_1, \tilde{f}_1, w_1^T; \ldots; \tilde{g}_r, \tilde{f}_r, w_r^T)$, that is obtained by transposing as described in Section 1.

Claim 1. *The triple $(\{0\}, L_2, W)$ is separable (see [6, Notation 17.15]) by β and the triple $(\{0\}, L_2, W^T)$ is separable by β', where $W^T := \{w^T : w \in W\}$.*

Assume $(\{0\}, L_2, W)$ is not separable by β. By the Extension Lemma [6, Lemma 17.18], there exists an element $l \in L_2 \setminus \{0\}$ such that $\mathbb{C}^{2\times 2}{\cdot}l \subseteq \{0\}{\cdot}l + W = W$. But $\mathbb{C}^{2\times 2}{\cdot}l = L_2$ is four dimensional (over $\mathbb{R}$), whereas W has dimension at most three. The second part of the claim is shown in a similar fashion.

Claim 2. *The triple (R_2, L_2, W) is separable by β or the triple (R_2, L_2, W^T) is separable by β'.*

Assume (R_2, L_2, W) is not separable by β. By the Extension Lemma, there exists an element $r \in R_2 \setminus \{0\}$ such that $r{\cdot}\mathbb{C}^{2\times 2} \subseteq R_2{\cdot}L_2 + W$. Now, $r{\cdot}\mathbb{C}^{2\times 2} = R_2$ and $R_2{\cdot}L_2$ contains exactly all matrices with a nonzero entry only in the lower right corner. We distinguish three different cases:

(i) $\dim(W + R_2) \geq 6$: Then the image of the projection

$$\pi_{12} : W \to \mathbb{C}, \quad \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} \mapsto b,$$

is two dimensional and hence, the space $W \cap R_2$ is at most one dimensional. Furthermore, $R_2{\cdot}L_2$ is two dimensional. Thus the four dimensional space R_2 cannot be contained in $R_2{\cdot}L_2 + W$.

(ii) $\dim(W + L_2) \geq 6$: In this case, we can use the computation β'. But then from $\dim(W + L_2) \geq 6$ it follows that $\dim(W^T + R_2) \geq 6$ and hence, by case (i), (R_2, L_2, W^T) is separable by β'.

(iii) $\dim(W + L_2) \leq 5$: Then the image of the projection

$$\pi_{21} : W \to \mathbb{C}, \quad \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} \mapsto c,$$

[4] Strictly speaking, we can only exchange the adjoints of the f's and g's with the w's, see Section 1. But since "having rank one" is invariant under transposing, this does not matter.

is at most one dimensional, which shows that the whole ideal R_2 cannot lie in the space $R_2{\cdot}L_2 + W$. This proves Claim 2.

W.l.o.g., assume that (R_2, L_2, W) is separable by β and define the projection

$$\pi : \mathbb{C}^{2\times 2} \longrightarrow \mathbb{C}^{2\times 2}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

Let ϕ be the multiplication of $\mathbb{C}^{2\times 2}$. Since $W \subseteq \ker \pi$, it follows that

$$R(\pi \circ \phi / R_2 \times L_2) + \dim(R_2 \times L_2) + \dim W \leq r$$

by [6, Lemma 17.17]. Hence $R(\pi \circ \phi / R_2 \times L_2) + 11 \leq r$. Now, the bilinear map $\pi \circ \phi / R_2 \times L_2$ is a map

$$\pi \circ \phi / R_2 \times L_2 : \mathbb{C}^{2\times 2}/R_2 \times \mathbb{C}^{2\times 2}/L_2 \to \mathbb{C}^{2\times 2}/\ker \pi.$$

But $\mathbb{C}^{2\times 2}/R_2 = R_1$, $\mathbb{C}^{2\times 2}/L_2 = L_1$, and $\mathbb{C}^{2\times 2}/\ker \pi = \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}$. It follows that $\pi \circ \phi / R_2 \times L_2 \cong \langle 1, 2, 1 \rangle$, the complex matrix multiplication tensor $\langle 1, 2, 1 \rangle$ over $\mathbb{R}$. By Lemma 1, the tensor $\langle 1, 1, 2 \rangle$ has rank six. Since this tensor is isomorphic to the tensor $\langle 1, 2, 1 \rangle$, we get $r \geq R(\pi \circ \phi / R_2 \times L_2) + 11 = 6 + 11 = 17$. □

3.2 Computations satisfying property (*)

Lemma 3. *Let $\beta := (f_1, g_1, w_1; \ldots; f_{16}, g_{16}, w_{16})$ satisfy (*). Then we can achieve (possibly after permutation), that $f_1, \ldots, f_8$ and $w_9, \ldots, w_{16}$ are bases of $\mathbb{R}^8$.*

Proof. We can assume that $f_1, \ldots, f_8$ is a basis. We can also assume that $g_9, \ldots, g_{16}$ and $w_9, \ldots, w_{16}$ are linearly dependent (otherwise, after probably exchanging the g's and w's, we are finished). Then the following claim holds:

Claim. *$g_1, \ldots, g_8$ and $w_1, \ldots, w_8$ are bases of $\mathbb{C}^{2\times 2}$ and for all $\nu \in \{1, \ldots, 8\}$,* $\dim\langle g_9, \ldots, g_{16}, g_\nu \rangle = \dim\langle w_9, \ldots, w_{16}, w_\nu \rangle = 8$.

Exchanging the f's and w's (again we can skip the adjoints here) gives a computation $\beta' := (w_1, g_1, f_1; \ldots; w_{16}, g_{16}, f_{16})$ for the same tensor. Assume that a nonzero matrix $y \in \ker g_9 \cap \cdots \cap \ker g_{16}$ has rank one. We know that there is a rank one matrix x such that $x{\cdot}y = 0 = ix{\cdot}y$. But this means that $x{\cdot}y = \sum_{\nu=1}^{8} w_\nu(x) g_\nu(y) f_\nu = 0$ and $ix{\cdot}y = \sum_{\nu=1}^{8} w_\nu(ix) g_\nu(y) f_\nu = 0$. Since $f_1, \ldots, f_8$ are linearly independent, we get $w_\nu(x) g_\nu(y) = w_\nu(ix) g_\nu(y) = 0$ for $\nu \in \{1, \ldots, 8\}$. Now, the image of R_y, the right multiplication with y, is four dimensional, hence, at least four of $g_\nu(y)$, $\nu \leq 8$, are nonzero. But then at least for four indices $\nu \leq 8$ we have $w_\nu(x) = w_\nu(ix) = 0$, which is a contradiction to property (*). This means that the matrix y has rank two and thus the image of $R_y = \sum_{\nu=1}^{8} g_\nu(y) w_\nu \otimes f_\nu$ is full dimensional. On the one hand, this implies that $w_1, \ldots, w_8$ has to be a basis. On the other hand, we see that $g_\nu(y)$ has to be nonzero for all $\nu \leq 8$, which proves the second part of the claim. (Note that $\dim\langle g_9, \ldots, g_{16} \rangle \geq 7$, since otherwise, we could find an invertible matrix in $\ker g_8 \cap \cdots \cap \ker g_{16}$ with the same arguments as above, which is a contradiction.)

Similarly, after exchanging the g's and w's, one can conclude the same assertions for the g's. This proves the claim.

Showing that there exists a partition $I, J \subseteq \{1, \ldots, 16\}$ such that $|I| = |J| = 8$ and $\{f_i : i \in I\}$ and $\{w_j : j \in J\}$ are both bases would prove the lemma.

Now, the claim above shows that if we choose an index set $J' \subset \{9, \ldots, 16\}$, $|J'| = 7$, such that $\{g_j : j \in J'\}$ are linearly independent, every g_ν, $\nu \le 8$, would lead to a basis $\{g_j : j \in J_\nu\}$, where $J_\nu := J' \cup \{\nu\}$. Let μ be such that $\{\mu\} = \{9, \ldots, 16\} - J'$. Then, by Steinitz exchange, there has to be a $\nu \in \{1, \ldots, 8\}$ such that

$$\{w_j : j \in (\{1, \ldots, 8\} - \{\nu\}) \cup \{\mu\}\}$$

is a basis. Exchanging the g's and the f's and setting $I := (\{1, \ldots, 8\} - \{\nu\}) \cup \{\mu\}$ and $J := J_\nu$ gives a partition with the desired properties. $\square$

Lemma 4. *Let $x_1, \ldots, x_5 \in \mathbb{C}^{2\times 2}$ be five matrices that are linearly independent over $\mathbb{R}$. Then $\langle x_1, \ldots, x_5 \rangle$ contains a matrix of rank two.*

Proof. Omitted. $\square$

Lemma 5. *Let $U \subseteq \mathbb{C}^{2\times 2}$ be a three dimensional subspace of rank one matrices. Then there exists an $x \in U$ such that $ix \in U$.*

Proof. Omitted. $\square$

Proposition 2. *There does not exist any computation for $\mathbb{C}^{2\times 2}$ over $\mathbb{R}$ of length 16 that satisfies (*).*

Proof. Assume there exists such a computation $\beta := (f_1, g_1, w_1; \ldots; f_{16}, g_{16}, w_{16})$ that satisfies (*). By Lemma 3, we can assume that $f_1, \ldots, f_8$ and $w_9, \ldots, w_{16}$ are bases. Let $x_1, \ldots, x_8$ be the basis dual to $f_1, \ldots, f_8$.

Claim. *For each $j \le 8$, the rank of x_j is two.*

Assume that the rank of x_j is one. Since the rank of L_{x_j}, the 8×8-matrix induced by the left multiplication with x_j, is four, there are four matrices $y_1, \ldots, y_4$ that are linearly independent over $\mathbb{R}$ such that $x_j \cdot y_k = 0$ for all $k \le 4$. Define the subspace $U := \langle y_1, \ldots, y_4 \rangle \cap \ker g_j$. For each $y \in U$ we then have

$$x_j \cdot y = \sum_{\nu=1}^{16} f_\nu(x_j) g_\nu(y) w_\nu = \sum_{\nu=9}^{16} f_\nu(x_j) g_\nu(y) w_\nu = 0.$$

But $w_9, \ldots, w_{16}$ is a basis. So $(f_9(x_j)g_9(y), \ldots, f_{16}(x_j)g_{16}(y))$ must be the zero vector. Since the rank of L_{x_j} is four, at least three of the $f_\nu(x_j)$, $\nu \ge 9$, are nonzero. This means that at least for three indices $\nu \ge 9$ we have $g_\nu(y) = 0$ for every $y \in U$. But U is at least three dimensional and contains only rank one matrices. Hence, Lemma 5 tells us that we can find a vector $x \in U$ such that $ix \in U$. Now x has rank one and $\langle x, ix \rangle$ is contained in intersection of at least three $\ker g_\nu$, which contradicts property (*) and hence proves the claim.

This shows that via sandwiching we can achieve that $x_1 = I_2$ is the unit matrix and x_2 is in Jordan normal form. We consider three different cases depending on the Jordan normal form of x_2.

(i) x_2 has two different eigenvalues λ_1, $\lambda_2 \in \mathbb{C}$:
In this case, we use [2, Lemma 3.8]. For this, note that since

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}-\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}=\begin{pmatrix} 0 & (\lambda_1-\lambda_2)x_{12} \\ (\lambda_2-\lambda_1)x_{21} & 0 \end{pmatrix},$$

$[x_2, x]$ is invertible if $x_{12} \neq 0 \neq x_{21}$.

Claim. *There is an index $\nu \in \{3, \dots, 8\}$ such that $[x_2, x_\nu]$ is invertible.*
Assume that none of the matrices $x_3, \dots, x_8$ fulfills this property, i.e., that either $(x_\nu)_{12}$ or $(x_\nu)_{21}$ is zero. Then we can find at least three matrices x_{ν_1}, x_{ν_2}, x_{ν_3}, $\nu_j \geq 3$, such that $(x_{\nu_1})_{12} = (x_{\nu_2})_{12} = (x_{\nu_3})_{12} = 0$ or $(x_{\nu_1})_{21} = (x_{\nu_2})_{21} = (x_{\nu_3})_{21} = 0$. W.l.o.g., assume that we are in the first case and that $\nu_1 = 3$, $\nu_2 = 4$, and $\nu_3 = 5$. Then consider the space U defined by

$$U := \langle x_1, \dots, x_5 \rangle \cap \Big\langle \begin{pmatrix} (1,0) & (0,0) \\ (0,0) & (0,0) \end{pmatrix}, \begin{pmatrix} (0,1) & (0,0) \\ (0,0) & (0,0) \end{pmatrix} \Big\rangle^{\perp}.$$

Since $\langle x_1, \dots, x_5 \rangle$ is five dimensional, the dimension of U is at least three. Furthermore, U contains only matrices where the entries in the first row are zero, i.e., only matrices of rank one. By Lemma 5, U contains a rank one matrix x such that $ix \in U$. But, by construction, x and ix are in $\ker f_6 \cap \ker f_7 \cap \ker f_8$, which is a contradiction to property (*).
W.l.o.g., let x_3 be such that $[x_2, x_3]$ is invertible. Then, choosing $m = 8 - 3 = 5$ in [2, Lemma 3.8], we get that the length of the computation is at least

$$m + 8 + \frac{1}{2}\dim([x_2, x_3]\mathbb{C}^{2\times 2}) = 5 + 8 + 4 = 17.$$

(ii) x_2 has twice the same eigenvalue λ and a nilpotent part:
This means, x_2 is of the form $x_2 = \lambda I_2 + n$, where n is the matrix that has a one in the upper right corner and zeros elsewhere. But for any matrix x we then have

$$[x_2, x] = [n, x] = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}-\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} x_{21} & x_{22}-x_{11} \\ 0 & -x_{21} \end{pmatrix},$$

which is an invertible matrix if $x_{21} \neq 0$. Since $x_1, \dots, x_8$ is a basis, we can find an index $\nu \in \{3, \dots, 8\}$, such that $(x_\nu)_{21} \neq 0$. W.l.o.g., let $\nu = 3$ be such an index. Then $[x_2, x_3]$ is invertible and by [2, Lemma 3.8], we get that the computation must have length at least 17 (as in case (i)).

(iii) x_2 has twice the same eigenvalue without a nilpotent part:
Then, since x_2 is also invertible and linearly independent from x_1, we know that $\langle x_1, x_2 \rangle = \langle I_2, i{\cdot}I_2 \rangle$. Since L_{x_1} is invertible, we know that $g_1, g_9, \dots, g_{16}$ generate $\mathbb{C}^{2\times 2}$ as an $\mathbb{R}$ vector space. Hence, we can choose indices $\nu_1 \dots, \nu_8 \in \{1, 9, \dots, 16\}$ such that $g_{\nu_1}, \dots, g_{\nu_8}$ is a basis. Let $y_1, \dots, y_n$ be the corresponding dual basis. W.l.o.g. we can assume that $y_1, \dots, y_4$ generate $\mathbb{C}^{2\times 2}$ as a $\mathbb{C}$-vector space. This means that

$$\langle x_i y_j : 1 \leq i \leq 2, 1 \leq j \leq 4 \rangle = \mathbb{C}^{2\times 2} \tag{1}$$

over $\mathbb{R}$. On the other hand, we have

$$x_i y_j = g_i(y_j) w_i + \sum_{\mu=1}^{4} f_{\nu_\mu}(x_i) g_{\nu_\mu}(y_j) w_{\nu_\mu} + f_l(x_i) g_l(y_j) w_l,$$

where $l = \{1, 9, \ldots, 16\} - \{\nu_1, \ldots, \nu_8\}$, and hence

$$x_i y_j \in \langle w_1, w_2, w_{\nu_1}, w_{\nu_2}, w_{\nu_3}, w_{\nu_4}, w_l \rangle$$

for $1 \leq i \leq 2$ and $1 \leq j \leq 4$. But the latter is a vector space of dimension at most seven, which is a contradiction to (1). □

4 Semisimple algebras of minimal rank plus one

Theorem 3. *Let A be a semisimple algebra over $\mathbb{R}$ of rank $2 \dim A - t + 1$, where t is number of maximal twosided ideals of A. Then A is of the form*

$$A \cong \mathbb{H} \times \mathbb{R}^{2\times 2} \times \cdots \times \mathbb{R}^{2\times 2} \times \mathbb{C} \times \cdots \times \mathbb{C} \times \mathbb{R} \times \cdots \times \mathbb{R}.$$

Proof. Let A be a semisimple $\mathbb{R}$-algebra. By Wedderburn's Theorem, we know that A is isomorphic to an algebra $A_1 \times \cdots \times A_t$, A_τ simple, i.e., $A_\tau \cong D_\tau^{n_\tau \times n_\tau}$, D_τ a division algebra over $\mathbb{R}$. By [6, Lemma 17.23] and using induction, we obtain

$$R(A) \geq 2 \dim A - t - (2 \dim A_\tau - 1) + R(A_\tau).$$

Since A is supposed to have rank $2 \dim A - t + 1$, we see that

$$R(A_\tau) \leq R(A) - 2 \dim A + t + (2 \dim A_\tau - 1) = 2 \dim A_\tau. \qquad (2)$$

Hence, by [2, Theorem 1], no factor can be a matrix algebra of the form $D^{n\times n}$, $n \geq 3$ and $\dim D \geq 2$. If $\dim D = 1$, i.e., $D = \mathbb{R}$, then this follows from the lower bound for matrix multiplication in [3]. Consider an algebra $B = D^{2\times 2}$, D a finite dimensional $\mathbb{R}$-division algebra such that $\dim D \geq 4$. Then [2, Theorem 1] tells us that

$$R(B) \geq \frac{5}{2} \dim B - 6 = 10 \dim_{\mathbb{R}}(D) - 6,$$

which is greater than $2 \dim B$, since $\dim D \geq 4$. Because of (2), this also excludes algebras of the above form from being a factor of A. Furthermore, there is no real division algebra of dimension three and Theorem 2 shows that also $\mathbb{C}^{2\times 2}$ cannot be one of the factors.

This shows that the only factors can be $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^{2\times 2}$, and $\mathbb{H}$. From these factors, only the latter one is an algebra that is not of minimal rank, hence it must be contained in A at least once. On the other hand, from Theorem 1 it follows that

$$R_{\mathbb{R}}(\mathbb{H} \times \mathbb{H}) = 16 > 2 \dim(\mathbb{H} \times \mathbb{H}) - 1,$$

which shows that $\mathbb{H} \times \mathbb{H}$ cannot be a factor of A. □

5 Conclusions

Two natural questions arise. First, can we extend our results to other fields than $\mathbb{R}$? And second, can we extend our results to arbitrary algebras (with radical)?

Over $\mathbb{R}$, there are only two nontrivial division algebras, $\mathbb{C}$ and $\mathbb{H}$. We used this fact several times in our proofs. Over $\mathbb{Q}$, there are more division algebras. The key question to solve the problem over $\mathbb{Q}$ is the following. For any numbers a, b, we can define quaternion algebras $H(a, b)$. Over $\mathbb{R}$, they are all either isomorphic to $\mathbb{R}^{2\times 2}$ or $\mathbb{H}$. Over $\mathbb{Q}$, the situation is more complicated. Question: What is $R_{\mathbb{Q}}(H(a, b))$ (in dependence on a, b)? If $H(a, b)$ is a division algebra, then it is clear that its rank is ≥ 8, since it is not a division algebra of minimal rank. The questions is whether 8 bilinear products are also sufficient.

To the second question, we have the following partial answer: If A is an algebra of minimal rank plus one and $A/\operatorname{rad} A$ contains one factor $\mathbb{H}$, then $A = \mathbb{H} \times B$ where B is an algebra of minimal rank. If $A/\operatorname{rad} A$ does not contain the factor $\mathbb{H}$, then $A = \mathbb{R}^{2\times 2} \times \cdots \times \mathbb{R}^{2\times 2} \times B$ where B is a superbasic algebra of minimal rank plus one. So far, we do not have a complete characterization of the superbasic algebras of minimal rank plus one.

Acknowledgements. We would like to thank the anonymous referees for their helpful comments.

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 bilinear complexity of associative algebras. *Comput. Complexity*, 9:73–112, 2000.
3. Markus Bläser. On the complexity of the multiplication of matrices of small formats. *J. Complexity*, 19:43–60, 2003.
4. Markus Bläser. A complete characterization of the algebras of minimal bilinear complexity. *SIAM J. Comput*, 34(2):277–298, 2004.
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. 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.
8. Hans F. de Groote and Joos Heintz. Commutative algebras of minimal rank. *Lin. Alg. Appl.*, 55:37–68, 1983.
9. 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.
10. 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.