1 Introduction

We consider several problems in representation theory, including the decomposition of semi-simple algebras over finite fields and number fields, and the decomposition of simple algebras over $\mathbf{C}$ and $\mathbf{R}$. The basic concepts of representation theory can be found in several excellent texts; we will refer to the text of Curtis and Reiner [7].

The asymptotic complexity of problems in representation theory has studied quite recently. In 1985, Friedl and Rónyai gave polynomial-time algorithms for the computation of the radical of a finite-dimensional associative algebra, and for the decomposition of a semi-simple algebra, over a finite field or number field — leaving the problem of decomposing simple algebras open (see [9]). Their algorithm for the decomposition of semi-simple algebras over finite fields is (Las Vegas) probabilistic; all others are deterministic. Rónyai later obtained a probabilistic (Las Vegas) polynomial-time algorithm for the decomposition of simple algebras over finite fields and gave evidence that the decomposition of simple algebras over number fields is difficult: Assuming the generalized Riemann hypothesis, and allowing randomized reductions, the problem of factoring squarefree integers is polynomial-time reducible to this problem (see [23, 24]).

The decomposition of semi-simple and simple algebras over $\mathbf{R}$ and $\mathbf{C}$ had been studied earlier by John Gabriel, who obtained algorithms for these problems that use a polynomial number of arithmetic operations and factorizations of polynomials (see [10, 11, 12, 13, 14]). Unfortunately, it is not clear that Gabriel's algorithms can be implemented using a polynomial number of Boolean operations, even assuming that the original matrix algebra has a basis of matrices with rational entries. A bitwise polynomial-time solution has been given more recently by Babai and Rónyai for the problem of decomposing a simple algebra A over $\mathbf{C}$, assuming that A is given by a basis of matrices with entries in a number field (see [1] for a complete solution, completing the partial solution in [8]).

In this paper we present Las Vegas and deterministic polynomial-time algorithms for the decomposition of semi-simple algebras over number fields and finite fields. As noted above, polynomial-time solutions have been given previously by Friedl and Rónyai; our algorithms are somewhat simpler than theirs. Moreover, our Las Vegas algorithm suggests a modification that might improve the performance of Friedl and Rónyai's algorithm in the average case. The new methods also yield parallel (NC) reductions from these problems to those of factoring polynomials over the same fields. As a consequence we obtain an efficient parallel algorithm for the decomposition of semi-simple algebras over (small) finite fields.

We also present Las Vegas polynomial-time algorithms for the decomposition of simple algebras over $\mathbf{R}$, assuming that the matrix algebra to be decomposed is given by a basis of matrices with entries in some number field $F \subseteq R$. The algorithm is an adaptation (and extension) of the recent algorithm of Babai and Rónyai for simple algebras over $\mathbf{C}$. To our knowledge, this is the first known (bitwise) polynomial-time algorithm for this problem.

In Section 2 we present the main technique to be applied in our probabilistic algorithms for these problems. Algorithms for the decomposition of semi-simple algebras over number

fields and finite fields are given in Sections 3–4. Algorithms for the decomposition of algebras over $\mathbf{R}$ or $\mathbf{C}$ are presented in Sections 5–6.

Unless stated otherwise, all logarithms in this paper have base two.

2 Splitting Elements of Algebras

Suppose now that A is an F-linear subspace of $M_{n\times n}(F)$, for some (large) perfect field F, and that $a_1, a_2, \ldots, a_k$ is a basis for A over F. An element a of A is a *splitting element* of A if the minimal polynomial of A over F is squarefree and has degree n.

If A is arbitrary, then A might not contain splitting elements. However, these elements are easily found if they exist.

Lemma 1. *Let $c > 0$ and let H be a finite subset of F of cardinality $|H| = \lceil cn(n-1) \rceil$. Then one of the following holds.*

(i) A does not contain a splitting element.

(ii) If $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in H^k$ is a random element drawn from the uniform distribution over H^k, then with probability at least $1 - (1/c)$, $a = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_k a_k$ is a splitting element of A.

Proof. Let $x_1, x_2, \ldots, x_k$ be indeterminates over F and consider the matrix of polynomials $\mathcal{A}(x_1, x_2, \ldots, x_k) = x_1 a_1 + x_2 a_2 + \cdots + x_k a_k$. The characteristic polynomial $\chi(x_1, x_2, \ldots, x_k, t)$ of $\mathcal{A}(x_1, x_2, \ldots, x_k)$ has total degree n, while the discriminant $d_t(x_1, x_2, \ldots, x_k)$ of $\chi(x_1, x_2, \ldots, x_k, t)$ is a polynomial with degree at most $n(n-1)$ in the indeterminates $x_1, x_2, \ldots, x_k$.

For $\lambda_1, \lambda_2, \ldots, \lambda_k \in H$, the matrix $\mathcal{A}(\lambda_1, \lambda_2, \ldots, \lambda_k) = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_k a_k = a$ is a splitting element of A if and only if $d_t(\lambda_1, \lambda_2, \ldots, \lambda_k) \neq 0$. Lemma 1 of Schwartz [26] can now be applied to obtain the stated result. ∎

If A is a field and α is a splitting element of A then $A = F[\alpha]$ — so the lemma can be used to find a representation of A as a simple extension of F. We will also apply this lemma to obtain the results of Sections 3 and 6.

3 A Las Vegas Algorithm for the Decomposition of Semi-Simple Algebras

Suppose now that F is a perfect field and that $A \subseteq M_{n\times n}(F)$ is a semi-simple algebra over F. We decompose A by computing bases over F for simple algebras $B_1, B_2, \ldots, B_l$ (each a subset of A) such that

$$A \cong B_1 \oplus B_2 \oplus \cdots \oplus B_l.$$

As Friedl and Rónyai show, it is sufficient to compute the identity elements $e_1, e_2, \ldots, e_l$ of $B_1, B_2, \ldots, B_l$. Then a basis for B_i can be obtained using the equality $B_i = e_i A$. Furthermore, it is sufficient to consider the semi-simple commutative algebra Centre(A); for

$$\begin{aligned}\text{Centre}(A) &\cong \text{Centre}(B_1) \oplus \text{Centre}(B_2) \oplus \cdots \text{Centre}(B_l) \\ &= E_1 \oplus E_2 \oplus \cdots \oplus E_l,\end{aligned}$$

where $E_i = \text{Centre}(B_i)$ is a simple algebra over F, as well as a field extension of F.

Friedl and Rónyai's algorithm considers the elements of a basis for Centre(A) one at a time, in order to refine a partial decomposition of this algebra — ending with the unique complete decomposition. We will show that the complete decomposition can be obtained by considering a single element — namely, a splitting element of Centre(A) — if F is sufficiently large. Otherwise, the decomposition can be obtained by considering a single element of a related algebra.

Let k and k_i be the dimensions over F of the algebras Centre(A) and E_i respectively; then $k = k_1 + k_2 + \cdots + k_l$. Furthermore, since Centre(A) is isomorphic to a subalgebra of $M_{k\times k}(F)$, every element of Centre(A) has a minimal polynomial over F with degree less than or equal to k. If F is sufficiently large then elements with squarefree minimal polynomials of degree k exist.

Lemma 2.

(i) Suppose F is a finite field with cardinality less than k. Then there exists a commutative semi-simple algebra A with dimension k over F that does not contain a splitting element.

(ii) If F is a perfect field with cardinality at least k then every commutative semi-simple algebra with dimension k over F contains a splitting element.

We will use Lemma 3, given below, to prove Lemma 2.

Lemma 3. *Let F be a field and let $k \in \mathbf{Z}$ such that $|F| \geq k > 0$. Let $n > 1$. If $F[t]$ includes an irreducible polynomial f of degree n over F then it includes at least $\lceil k(k-1)/n \rceil$ distinct monic irreducible polynomials of degree n that have roots in $F[t]/(f)$.*

Proof of Lemma 3. Suppose $f \in F[t]$ is a monic irreducible polynomial of degree n over F (the result is trivial if no such polynomial exists). Let $E = F[t]/(f)$ and let $\alpha = t + (f) \in E$; then α is a root of f in E.

For elements r and s of F, with $r \neq 0$, let $\alpha_{r,s} = r\alpha + s \in E$. Since $r \neq 0$, $\alpha \in F[\alpha_{r,s}] \subseteq F[\alpha] = E$, so $F[\alpha_{r,s}] = E$. Since E has degree n over F and F is perfect, the minimal polynomial of $\alpha_{r,s}$ is irreducible with degree n over F. Suppose now that $r_1, s_1, r_2, s_2 \in F$

with r_1 and r_2 nonzero such that $\alpha_{r_1,s_1} = \alpha_{r_2,s_2}$. If $r_1 = r_2$ then $s_1 = s_2$ as well. Suppose $r_1 \neq r_2$; then, since $r_1\alpha + s_1 = \alpha_{r_1,s_1} = \alpha_{r_2,s_2} = r_2\alpha + s_2$,

$$\alpha = \frac{s_2 - s_1}{r_1 - r_2} \in F,$$

contradicting the above choice of α (and the fact that $n > 1$). Thus, $\alpha_{r_1,s_1} = \alpha_{r_2,s_2}$ if and only if $r_1 = r_2$ and $s_1 = s_2$. Since $|F| \geq k$ there are at least $k(k-1)$ such elements in E, corresponding to different choices of r and s, and each has a (monic, irreducible) minimal polynomial with degree n over F. Since no polynomial of degree n can have more than n roots in E it follows that there are at least $\lceil k(k-1)/n \rceil$ distinct monic, irreducible polynomials in $F[t]$ with degree n over F that have roots in E, as claimed. ■

Proof of Lemma 2. We first prove (i). Suppose F is a finite field with fewer than k elements, and let $A \subseteq M_{k\times k}(F)$ be the algebra of diagonal matrices of order k over F. Clearly A has dimension k over F, and is commutative and semi-simple (it is the direct sum of copies of F). Every element of this algebra is annihilated by the polynomial $\prod_{\alpha\in F}(x-\alpha)$, which has degree less than k. Thus no element of the algebra has a minimal polynomial with degree k, and no element can be a splitting element of this algebra.

Suppose instead that A is a commutative semi-simple algebra of dimension k over a perfect field F and that F contains at least k distinct elements. Let $E_1, E_2, \ldots, E_l$ be the simple components of A over F, with dimensions $m_1, m_2, \ldots, m_l$ respectively. Then $m_1 + m_2 + \cdots + m_l = k$ and each algebra E_i is a field and a finite algebraic extension of F.

If $l = 1$ then A is a field of degree l over F and, since F is perfect, A contains a splitting element (namely, any element α such that $A = F[\alpha]$). Suppose now that $l > 1$, and let ϕ be an isomorphism from A to $E_1 \oplus E_2 \oplus \cdots \oplus E_l$. For $a \in A$ let $\phi(a) = (\alpha_1, \alpha_2, \ldots, \alpha_l)$ with $\alpha_i \in E_i$ for $1 \leq i \leq l$. We will show later that there exists an element a of A, with corresponding elements α_i of E_i for $1 \leq i \leq l$, such that the minimal polynomial ψ_i of α_i over F is irreducible and has degree m_i for all i, and such that the polynomials $\psi_1, \psi_2, \ldots, \psi_l$ are pairwise relatively prime. Since $\phi(a) = (\alpha_1, \alpha_2, \ldots, \alpha_l)$ and ϕ is an isomorphism, the minimal polynomial of a over F is the lowest common multiple of $\psi_1, \psi_2, \ldots, \psi_l$. Since the ψ_i's are squarefree and pairwise relatively prime, this is the product of the ϕ_i's — a squarefree polynomial with degree $m_1 + m_2 + \cdots + m_l = k$ over F. Hence, a is a splitting element of A.

To complete the proof of (ii) we must show that the element a described above exists. We will construct a by choosing elements $\alpha_1 \in E_1$, $\alpha_2 \in E_2, \ldots, \alpha_l \in E_l$ in turn and then setting $a = \phi^{-1}(\alpha_1, \alpha_2, \ldots, \alpha_l)$. Suppose that $i \leq l$ and that values $\alpha_1 \in E_1, \alpha_2 \in E_2, \ldots, \alpha_{i-1} \in E_{i-1}$ have already been chosen such that $E_j = F[\alpha_j]$ for $1 \leq j < i$ and such that the (monic) minimal polynomials $\psi_1, \psi_2, \ldots, \psi_{i-1}$ are distinct and irreducible. If the degree m_i of E_i over F is one then $E_i \cong F$. Since $|F| \geq k \geq i$, $F[t]$ contains at least i monic linear polynomials. Clearly each of these is irreducible and has a root in E_i. If, instead, $m_i > 1$ then by Lemma 3 there are at least $\lceil k(k-1)/m_i \rceil \geq k \geq i$ monic irreducible polynomials in $F[t]$ with degree m_i over F and with a root in E_i. In

either case we can choose as ψ_i any of these irreducible polynomials that is not in the set $\{\psi_1, \psi_2, \ldots, \psi_{i-1}\}$, and we can choose as α_i any element of E_i such that $\psi_i(a_i) = 0$. By construction the polynomials $\psi_1, \psi_2, \ldots, \psi_l$ are distinct, monic, and irreducible. Thus they are also squarefree and pairwise relatively prime, as required. ■

Suppose now that a is an element of the algebra Centre$(A) \cong E_1 \oplus E_2 \oplus \cdots \oplus E_l$. Then there is an isomorphism ϕ : Centre$(A) \to E_1 \oplus E_2 \oplus \cdots \oplus E_l$ such that

$$\phi(a) = (\alpha_1, \alpha_2, \ldots, \alpha_k)$$

for $\alpha_i \in E_i$, $1 \leq i \leq l$. As noted above, the minimal polynomials of a and of $\alpha_1, \alpha_2, \ldots, \alpha_k$ over F are related as follows.

$$minpol(a) = \text{lcm}(minpol(\alpha_1), minpol(\alpha_2), \ldots, minpol(\alpha_l)).$$

If a is a splitting element of Centre(A) then $minpol(a)$ has degree $k = k_1 + k_2 + \cdots + k_l$ and since $minpol(\alpha_i)$ has degree at most k_i, for $1 \leq i \leq l$,

$$minpol(a) = \prod_{i=1}^{l} minpol(\alpha_i)$$

and polynomials $minpol(\alpha_1), minpol(\alpha_2), \ldots, minpol(\alpha_l)$ are pairwise relatively prime. Consequently, there exist polynomials $g_1, g_2, \ldots, g_l \in F[x]$, each with degree less than k, such that

$$g_i \equiv 1 \bmod minpol(\alpha_i) \quad \text{and} \quad g_i \equiv 0 \bmod minpol(\alpha_j) \quad \text{for } j \neq i, \quad 1 \leq i, j \leq l.$$

It is easily checked that $g_1(a), g_2(a), \ldots, g_l(a)$ are respectively the identity elements of the simple components $E_1, E_2, \ldots, E_l$ of Centre(A) — and also of the simple components $B_1, B_2, \ldots, B_l$ of A.

Our algorithm for decomposing a semi-simple algebra $A \subseteq M_{n \times n}(F)$ over an infinite (or finite but large) perfect field F is now easily described. Solving systems of linear equations over F, we compute a basis $b_1, b_2, \ldots, b_k$ for Centre(A) over F. We choose elements $\lambda_1, \lambda_2, \ldots, \lambda_k$ uniformly and independently from a subset H of F with cardinality $4k(k-1)$, and set

$$a = \lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_k b_k \in \text{Centre}(A).$$

We next compute the minimal polynomial of a over F. If this is not squarefree with degree k then the algorithm fails — with probability at most 1/4. (Centre(A) is isomorphic to a subalgebra of $M_{k \times k}(F)$, so Lemma 1 is applicable.) Otherwise, a is a splitting element of Centre(A), and we can compute the identity elements of the simple components of A by factoring $minpol(a)$ to obtain $minpol(\alpha_i)$ for $1 \leq i \leq l$ and using these polynomials as described above. The algorithm is given in Figure 1.

Algorithm **Semi-Simple Decomposition via Splitting Element (F Large)**

Input.
- Matrices $a_1, a_2, \ldots, a_k \in M_{n\times n}(F)$ forming a basis for a semi-simple algebra A over F

Output.
- Integer $l > 0$, the number of simple components of A
- Integers $m_1, m_2, \ldots, m_l$, the dimensions of the simple components $B_1, B_2, \ldots, B_l$ of A over F
- Matrices $b_{ij} \in A$ for $1 \le j \le m_i$ and $1 \le i \le l$ such that, for $1 \le i \le l$, $b_{i1}, b_{i2}, \ldots, b_{im_i}$ is a basis for B_i over F

OR *failure*, with probability at most 1/2

Constants Required. $4n(n-1)$ distinct elements $\gamma_1, \gamma_2, \ldots, \gamma_{4n(n-1)}$ of F

Note. F is a perfect field with at least $4n(n-1)$ distinct elements

Compute a basis $b_1, b_2, \ldots, b_h$ for the Centre of A over F

Choose elements $\lambda_1, \lambda_2, \ldots, \lambda_h$ uniformly and independently from the set of constants $\{\gamma_1, \gamma_2, \ldots, \gamma_{4n(n-1)}\}$

$a := \lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_h b_h$

Compute the minimal polynomial ψ of a over F

if degree(ψ) $< h$ **then**

report *failure*

(*Note.* This occurs with probability at most 1/4)

else

Compute a factorization $\psi = \psi_1 \psi_2 \cdots \psi_l$ of ψ into a product of distinct monic irreducible polynomials in $F[x]$, or *fail* and stop (with probability at most 1/4)

for $i = 1, 2, \ldots, l$ **do**

Compute the polynomial $g_i \in F[x]$ with degree less than h = degree(ψ) such that $g_i \equiv 1 \pmod{\psi_i}$ and $g_i \equiv 0 \pmod{\psi_j}$ for $1 \le j \le l$ and $j \ne i$

$e_i := g_i(a)$

Compute a basis $b_{i1}, b_{i2}, \ldots, b_{im_i}$ for the semi-simple algebra $B_i = e_i A$ over F

end for

Return the dimensions $m_1, m_2, \ldots, m_l$, and the matrices e_i and b_{ij} (for $1 \le i \le l$ and $1 \le j \le m_i$) computed above

end if

Figure 1

If F is finite and has cardinality at least $4n(n-1)$ then we can decompose a semi-simple algebra $A \subseteq M_{n\times n}(F)$ by this method. (Note that Centre(A) will have dimension at most n over F). Suppose instead that F has cardinality less than $4n(n-1)$, and that $A \subseteq M_{n\times n}(F)$ is semi-simple with dimension k over F and with basis $a_1, a_2, \ldots, a_k$. Let E be a field extension of F, with degree q over F for some prime $q > n$, such that E has at least $4n(n-1)$ distinct elements. The prime q can be chosen to be between $2n$ and $4n$, and the extension E can be constructed using a Las Vegas algorithm in polynomial time (see Rabin [22]). We will consider the semi-simple algebra $A \otimes_F E \subseteq M_{n\times n}(E)$ of dimension k over E obtained from A by *extension of scalars* — consisting of E-linear combinations of $a_1, a_2, \ldots, a_k$.†

We also consider a natural embedding $\phi : A \to A \otimes_F E$ such that $\phi(a_i) = a_i$ for $1 \leq i \leq k$. As stated in the following lemma, the simple components of A over F and of $A \otimes_F E$ over E are related in a useful way.

Lemma 4. *Let F, A, q, and E be as above and suppose A has simple components $B_1, B_2, \ldots, B_l$ over F. Then the algebra $A \otimes_F E$ is semi-simple over E and has simple components $B_1 \otimes_F E$, $B_2 \otimes_F E$, $\ldots$, $B_l \otimes_F E$ over E.*

Proof. Since E is a finite separable extension of F and A is semi-simple over F, $A \otimes_F E$ is semi-simple over E. (See, for example, Section 69 of Curtis and Reiner [7].)

Since A is semi-simple over F with simple components $B_1, B_2, \ldots, B_l$, there exist idempotents $e_1, e_2, \ldots, e_l \in$ Centre(A) such that $B_i \cong e_i A$ for $1 \leq i \leq l$. It is easily checked that $\phi(e_1), \phi(e_2), \ldots, \phi(e_l)$ are idempotents in $A \otimes_F E$ and that each is an element of Centre($A \otimes_F E$). Furthermore, for $1 \leq i \leq l$, the algebra $\phi(e_i)(A \otimes_F E)$ is semi-simple and isomorphic to a direct sum of some of the simple components of $A \otimes_F E$. To complete the proof we need only show that $\phi(e_i)(A \otimes_F E)$ is a simple algebra; since $\phi(e_i)(A \otimes_F E)$ is semi-simple, it is sufficient to show that Centre($\phi(e_i)(A \otimes_F E)$) is a field.

Since the field Centre($e_i A$) is a finite algebraic extension of F and F is perfect, there exists an element α_i of Centre($e_i A$) such that Centre($e_i A$) $= F[\alpha_i]$. Let ψ_i be the minimal polynomial of α_i over F; then ψ_i has degree at most n and is irreducible in $F[x]$. Since the degree q of E over F is relatively prime with the degree of ψ_i, ψ_i is also an irreducible polynomial in $E[x]$ (see Theorem 7.1 of von zur Gathen [16]). Since

$$\text{Centre}(\phi(e_i)(A \otimes_F E)) \cong E[x]/(\psi_i),$$

it follows that Centre($\phi(e_i)(A \otimes_F E)$) is a field, as required to complete the proof. ■

† This nonstandard definition of $A \otimes_F E$ is suitable for our purposes. It should be noted, however, that the algebra $A \otimes_F E$ is independent of the basis used in the construction given here. For a more general definition of $A \otimes_F E$ that does not rely on a basis for A see, for example, Chapter 12 of Curtis and Reiner [7].

Algorithm **Semi-Simple Decomposition via Splitting Element (F Small)**

Input.
- Matrices $a_1, a_2, \ldots, a_k \in M_{n\times n}(F)$ forming a basis for a semi-simple algebra A

Output.
- Integer $l > 0$, the number of simple components of A
- Integers $m_1, m_2, \ldots, m_l$, the dimensions of the simple components $B_1, B_2, \ldots, B_l$ of A over F
- Matrices $b_{ij} \in A$ for $1 \le j \le m_i$ and $1 \le i \le l$ such that, for $1 \le i \le l$, $b_{i1}, b_{i2}, \ldots, b_{im_i}$ is a basis for B_i over F
- Matrix $e_i \in A$, the identity element of B_i, for $1 \le i \le l$

OR *failure*, with probability at most 1/2

Note. F is a perfect field with fewer than $4n(n-1)$ distinct elements

Compute a prime q such that $2n < q < 4n$

Use the algorithm of Rabin [22] to compute a monic irreducible polynomial $f \in F[x]$ with degree q over F, or to *fail* (the latter with probability at most 1/4)

if Rabin's algorithm succeeds **then**

Set $E = F[x]/(f)$

Use two independent executions of the algorithm "Semi-Simple Decomposition via Splitting Element (F Large)", simulating arithmetic over E, to compute the number l, dimensions $m_1, m_2, \ldots, m_l$, and the identity elements $\hat{e}_1, \hat{e}_2, \ldots, \hat{e}_l$ of the simple components $\hat{B}_1, \hat{B}_2, \ldots, \hat{B}_l$ of $A \otimes_F E$ over E, as well as a basis $\hat{b}_{i1}, \hat{b}_{i2}, \ldots, \hat{b}_{im_i}$ for the simple component $\hat{B}_i$, for $1 \le i \le l$ — or to *fail* with probability at most 1/4

if the decomposition of $A \otimes_F E$ was performed successfully **then**

for $i = 1, 2, \ldots, l$ **do**

$e_i := \hat{e}_i$ (*Note.* $\hat{e}_i \in (A \otimes_F E) \cap M_{n\times n}(F) = A$)

Compute a basis $b_{i,1}, b_{i,2}, \ldots, b_{i,m_i}$ for $B_i = e_i A$ over F

end for

Return the desired integers l and $m_1, m_2, \ldots, m_l$ and matrices b_{ij} and e_i for $1 \le i \le l$ and $1 \le j \le m_i$

else

report *failure*

end if

else

report *failure*

end if

Figure 2

Since $|E| = |F|^q \geq 2^{2n} \geq 4n(n-1)$, the identity elements of the simple components of $A \otimes_F E$ over E can be computed by our probabilistic method using arithmetic over E. Since q can be chosen to be less than $4n$, this is easily simulated using arithmetic over the ground field F. Thus the number and dimensions of the simple components of A over F can be obtained. Furthermore, if $e_1, e_2, \ldots, e_l \in A$ are the identity elements of the simple components of A then $\phi(e_1), \phi(e_2), \ldots, \phi(e_l) \in A \otimes_F E$ are the identity elements of the simple components of $A \otimes_F E$. Using our algorithm for simple algebras over large fields, each idempotent $\phi(e_i)$ can be computed as a (unique) linear combination of the basis elements $a_1, a_2, \ldots, a_k$:

$$\phi(e_i) = \lambda_{i1}a_1 + \lambda_{i2}a_2 + \cdots + \lambda_{ik}a_k \in A \otimes_F E;$$

it is clear that $\lambda_{i1}, \lambda_{i2}, \ldots, \lambda_{ik} \in F$ for $1 \leq i \leq l$ and that

$$e_i = \lambda_{i1}a_1 + \lambda_{i2}a_2 + \cdots + \lambda_{ik}a_k \in A,$$

so that the idempotents $e_1, e_2, \ldots, e_l$ can be recovered from the decomposition of $A \otimes_F E$ over E. Our algorithm for the the decomposition of semi-simple algebras over small finite fields is shown in Figure 2.

In combination the two algorithms given here comprise an algorithm "Semi-Simple Decomposition via Splitting Elements" that reduces the decomposition of semi-simple algebras over an arbitrary perfect field F to the factorization of polynomials over F.‡ The algorithm can be applied to decompose algebras over number fields or finite fields using a small number of boolean operations.

Theorem 5. *Let $A \subseteq M_{n\times n}(F)$ be a semi-simple algebra of dimension m over a number field or finite field F.*

(i) Given binary representations of a basis $a_1, a_2, \ldots, a_m$ of a basis for A over F, the algorithm "Semi-Simple Decomposition via Splitting Element" computes the number of simple components of A and the dimension and a basis for each component, or fails (with probability at most $1/2$), using a number of boolean operations that is polynomial in the input size.

(ii) If F is a finite field with $q = p^k$ elements (for p prime) then the above algorithm can be implemented to decompose A (or to fail with probability at most $1/2$) using boolean circuits with size polynomial in $n \log q$ and with depth $O(\log^2 n \log^2(k+1) \log p)$.

Proof. Correctness of the algorithm follows from Lemmas 2 and 4. The cost of implementing the algorithm (sequentially) is dominated by that of factoring a polynomial with degree at most n over F (or possibly over an extension with degree $O(n)$ over F, if F is a small finite field). Polynomial time deterministic algorithms for factorization of polynomials over

‡ Note that if E is an extension of F with small degree over F then factorization of polynomials in $E[x]$ can be reduced to factorization of polynomials in $F[x]$.

the rational numbers and over number fields are given by Lenstra, Lenstra, and Lovász [18] and by Landau [17] respectively. Las Vegas polynomial time algorithms for the factorization of polynomials over finite fields are given by Berlekamp [4] and by Cantor and Zassenhaus [6].

Suppose now that F is a finite field with $q = p^k$ elements. With the exception of factorization of polynomials, the steps of the algorithm "Semi-Simple Decomposition via Splitting Element" can be implemented by solving nonsingular systems of linear equations over F or over an extension E with degree less than $4n$ over F, by computing determinants and characteristic polynomials of matrices over F (or E), and by computing ranks of matrices over these fields. Efficient parallel algorithms for the solution of nonsingular systems of linear equations and for the computation of determinants (and hence of characteristic polynomials) are given by Berkowitz [2] and by Borodin, von zur Gathen, and Hopcroft [5]. Algorithms for solving singular systems are obtained by combining the reductions in [5] with the parallel algorithm for matrix rank given by Mulmuley [20]. Von zur Gathen [15] provides a parallel algorithm for factorization of polynomials over finite fields that can be used to perform the remaining steps of our algorithm efficiently. ■

We obtain a probabilistic algorithm with the expected (sequential) performance of the algorithm sketched in this section, but with worst case performance not much worse than that of Friedl and Rónyai's algorithm, by performing a random change of basis for A, and then starting Friedl and Rónyai's algorithm. With high probability, the first basis element considered will be a splitting element of the centre of the algebra (if F is sufficiently large), and no further elements of the basis need be considered. Otherwise, Friedl and Rónyai's algorithm can be used to complete the decomposition. It seems worthwhile to stop and decide whether we need to continue after processing a single element of the basis, even when the deterministic version of Friedl and Rónyai's algorithm is used.

4 A Divide and Conquer Algorithm for the Decomposition of Semi-Simple Algebras

We now present a new deterministic algorithm for the decomposition of semi-simple algebras over fields of characteristic zero and over finite fields. Rather than using a single splitting element to obtain a complete decomposition of an algebra, the algorithm presented in this section uses each element of a basis to obtain a partial decomposition, then computes a common refinement of these partial decompositions.

Suppose again that $A \subseteq M_{n\times n}(F)$ is a semi-simple algebra over a perfect field F with simple components $B_1, B_2, \ldots, B_l$. Suppose further that $E_i = \text{Centre}(B_i)$ for $1 \leq i \leq l$, so that

$$\text{Centre}(A) \cong E_1 \oplus E_2 \oplus \cdots \oplus E_l;$$

let $e_1, e_2, \ldots, e_l$ be the identity elements of $E_1, E_2, \ldots, E_l$ respectively. Let $a \in \text{Centre}(A)$ with $\phi(a) = (a_1, a_2, \ldots, a_l)$, with $a_i \in E_i$, and let ψ_i be the minimal polynomial of a_i over F for $1 \leq i \leq l$. Since E_i is a field (and an extension of F), each ψ_i is a monic irreducible

polynomial over F. If the polynomials $\psi_1, \psi_2, \ldots, \psi_l$ are distinct then they are also pairwise relatively prime, and a complete decomposition of the algebra A can be obtained from a as in the algorithm "Semi-Simple Decomposition via Splitting Element" of Section 3.

Suppose instead that the polynomials $\psi_1, \psi_2, \ldots, \psi_l$ are *not* distinct. Then the minimal polynomial ψ of a is the lowest common multiple of $\psi_1, \psi_2, \ldots, \psi_l$ and if we use a to decompose the algebra A as in Section 3 then the results will include a set of idempotents $\hat{e}_1, \hat{e}_2, \ldots, \hat{e}_h \in \text{Centre}(A)$, for $h < l$, such that

$$\hat{e}_1 + \hat{e}_2 + \cdots + \hat{e}_h = 1,$$

and such that for $1 \leq i, j \leq h$, $\hat{e}_i \hat{e}_j = \hat{e}_i$ if $i = j$ and $\hat{e}_i \hat{e}_j = 0$ otherwise. Furthermore, each idempotent $\hat{e}_i$ is a sum of some subset of the idempotents $e_1, e_2, \ldots, e_l$ and, for $1 \leq i \leq l$, there exists exactly one idempotent $\hat{e}_j$ (for $1 \leq j \leq h$) such that $e_i \hat{e}_j = \hat{e}_j e_i = e_i$; for any idempotent $\hat{e}_k$ with $k \neq j$, $e_i \hat{e}_k = \hat{e}_k e_i = 0$. We will call e_i a *constituent* of the idempotent $\hat{e}_j$. For $1 \leq i, j \leq l$ the idempotents e_i and e_j are constituents of the same idempotent in $\{ \hat{e}_1, \hat{e}_2, \ldots, \hat{e}_h \}$ if and only if $\psi_i = \psi_j$; this is the case if and only if a_i and a_j are conjugates when both B_i and B_j are embedded in a splitting field for ψ over F.

Let $\{ \hat{e}_{11}, \hat{e}_{12}, \ldots, \hat{e}_{1h_1} \}$ and $\{ \hat{e}_{21}, \hat{e}_{22}, \ldots, \hat{e}_{2h_2} \}$ be two sets of idempotents in the centre of A such that

$$\hat{e}_{11} + \hat{e}_{12} + \cdots + \hat{e}_{1h_1} = 1 = \hat{e}_{21} + \hat{e}_{22} + \cdots + \hat{e}_{2h_2},$$

and such that $\hat{e}_{1a} \hat{e}_{1b} = \delta_{ab} \hat{e}_{1a}$ for $1 \leq a, b \leq h_1$ and $\hat{e}_{2c} \hat{e}_{2d} = \delta_{cd} \hat{e}_{2c}$ for $1 \leq c, d \leq h_2$. A third set of idempotents $\{ \overline{e_1}, \overline{e_2}, \ldots, \overline{e_h} \}$ is a *refinement* of the sets $\{ \hat{e}_{11}, \hat{e}_{12}, \ldots, \hat{e}_{1h_1} \}$ and $\{ \hat{e}_{21}, \hat{e}_{22}, \ldots, \hat{e}_{2h_2} \}$ if the following properties hold:

- $\overline{e_1} + \overline{e_2} + \cdots + \overline{e_h} = 1$;
- For all i, j such that $1 \leq i, j \leq h$, $\overline{e_i}\,\overline{e_j} = \delta_{ij} \overline{e_i}$;
- For all i such that $1 \leq i \leq h$, there exist idempotents $\hat{e}_{1a}$ and $\hat{e}_{2b}$, for $1 \leq a \leq h_1$ and for $1 \leq b \leq h_2$, such that $\overline{e_i} = \hat{e}_{1a} \hat{e}_{2b}$.

The set $\{ \overline{e_1}, \overline{e_2}, \ldots, \overline{e_h} \}$ is the largest set of idempotents that can be formed from products of the idempotents $\hat{e}_{1a}$ (for $1 \leq a \leq h_1$) and $\hat{e}_{2b}$ (for $1 \leq b \leq h_2$).

We can decompose a semi-simple algebra A by forming the set of idempotents corresponding to each element of a basis for Centre(A), and then computing the identity elements of the simple components of A as common refinements of these sets of idempotents. The algorithm is shown in Figure 3.

We conclude this section by showing that this algorithm correctly decomposes semi-simple algebras over finite fields and number fields.

Algorithm **Simple Components via Idempotents of Basis**

Input.
- Matrices $a_1, a_2, \ldots, a_k \in M_{n\times n}(F)$, forming a basis for a semi-simple associative algebra A over a field F

Output.
- Integer $l > 0$, the number of simple components of A
- Integers $m_1, m_2, \ldots, m_l$, the dimensions of the simple components $B_1, B_2, \ldots, B_l$ of A over F
- Matrices $b_{ij} \in A$ for $1 \le j \le m_i$ and $1 \le i \le l$ such that, for $1 \le i \le l$, $b_{i1}, b_{i2}, \ldots, b_{im_i}$ is a basis for B_i over F
- Matrix $e_i \in A$, the identity element of B_i, for $1 \le i \le l$

Note. F is a finite field or has characteristic zero

Compute a basis $b_1, b_2, \ldots, b_h$ for Centre(A) over F

for $i = 1, 2, \ldots, h$ **do**

Compute the minimal polynomial f_i of b_i over F

Compute the factorization $f_i = \psi_{i1}\psi_{i2}\cdots\psi_{ik_i}$ of f_i into a product of distinct monic irreducible polynomials in $F[x]$

for $j = 1, 2, \ldots, k_i$ **do**

Compute the polynomial $g_{ij} \in F[x]$ with degree less than $h_i = \text{degree}(f_i)$ such that $g_{ij} \equiv 1 \pmod{\psi_{ij}}$ and $g_{ij} \equiv 0 \pmod{\psi_{ir}}$ for $1 \le r \le k_i$ and $r \ne j$

$e_{ij} := g_{ij}(b_i)$

end for

end for

Compute a set of idempotents $e_1, e_2, \ldots, e_l$ refining the sets computed above

for $i = 1, 2, \ldots, l$ **do**

Compute a basis $b_{i1}, b_{i2}, \ldots, b_{im_i}$ for the simple algebra $B_i = e_i A$

end for

Return the desired integers l and $m_1, m_2, \ldots, m_l$ and matrices $b_{i,j}$ and e_i for $1 \le i \le l$ and $1 \le j \le m_i$

Figure 3

Once again, suppose $B_1, B_2, \ldots, B_h$ are simple components of $A \subseteq M_{n\times n}(F)$ and suppose that idempotents $e_1, e_2, \ldots, e_l$ (for $l \leq h$) are computed from a basis for A by our algorithm. We say that these idempotents *split* components B_i and B_j if there exists an idempotent e_r such that $e_r B_i = B_i$ and $e_r B_j = (0)$. The algorithm produces a complete decomposition of A into simple components if (and only if) the idempotents it computes split every pair of distinct simple components of A.

Lemma 6. *Let F be a field of characteristic zero or a finite field, let $A \subseteq M_{n\times n}(F)$ be a semi-simple algebra over F with simple components $B_1, B_2, \ldots, B_h$, and let $e_1, e_2, \ldots, e_l$ be idempotents generated by the algorithm "Simple Components via Idempotents of Basis" from a basis for A over F. Then $h = l$ and the idempotents $e_1, e_2, \ldots, e_l$ are the identity elements of the simple components of A over F.*

Proof. Suppose the claim is false; then there must exist simple components B_i and B_j of A (for $i \neq j$) that are not split by any of the idempotents $e_1, e_2, \ldots, e_l$. Suppose $a_1, a_2, \ldots, a_k$ is the basis for A used as input for the algorithm "Simple Components via Idempotents of Basis". Then we can write

$$\begin{aligned} a_1 &= \beta_{11} + \beta_{12} + \cdots + \beta_{1h} \\ a_2 &= \beta_{21} + \beta_{22} + \cdots + \beta_{2h} \\ &\vdots \\ a_k &= \beta_{k1} + \beta_{k2} + \cdots + \beta_{kh} \end{aligned}$$

with $\beta_{rs} \in B_s$ for $1 \leq r \leq k$ and $1 \leq s \leq h$. Since a_r does not split B_i and B_j, β_{ri} and β_{rj} must have the same minimal polynomial over F, for $1 \leq r \leq k$.

Suppose now that F has characteristic zero. Since $a_1, a_2, \ldots, a_k$ is a basis for A over F, there exist elements $\gamma_1, \gamma_2, \ldots, \gamma_k$ of F such that

$$\gamma_1 a_1 + \gamma_2 a_2 + \cdots + \gamma_k a_k = \overline{e_i},$$

for $\overline{e_i}$ the identity element of B_i. It follows that

$$\gamma_1\beta_{i1} + \gamma_2\beta_{i2} + \cdots + \gamma_k\beta_{ik} = 1, \quad \text{and} \quad \gamma_1\beta_{j1} + \gamma_2\beta_{j2} + \cdots + \gamma_k\beta_{jk} = 0.$$

Let E be a finite extension of F that contains the elements β_{ir} and β_{jr} for $1 \leq r \leq k$. (That is, let E be an extension field of F with subfields isomorphic, as extensions of F, to B_i and B_j.) For $\alpha \in E$ let $T_{E/F}(\alpha)$ be the trace of α in E over F. Since β_{ir} and β_{jr} are conjugates over F, $T_{E/F}(\beta_{ir}) = T_{E/F}(\beta_{jr})$, for $1 \leq r \leq k$. Since the trace is an F-linear map, it follows that

$$\begin{aligned} [E : F] &= T_{E/F}(1) \\ &= T_{E/F}(\gamma_1\beta_{i1} + \gamma_2\beta_{i2} + \cdots + \gamma_k\beta_{ik}) \\ &= \gamma_1 T_{E/F}(\beta_{i1}) + \gamma_2 T_{E/F}(\beta_{i2}) + \cdots + \gamma_k T_{E/F}(\beta_{ik}) \\ &= \gamma_1 T_{E/F}(\beta_{j1}) + \gamma_2 T_{E/F}(\beta_{j2}) + \cdots + \gamma_k T_{E/F}(\beta_{jk}) \\ &= T_{E/F}(\gamma_1\beta_{j1} + \gamma_2\beta_{j2} + \cdots + \gamma_k\beta_{jk}) \\ &= T_{E/F}(0) = 0, \end{aligned}$$

contradicting the fact that the field F has characteristic zero and $[E : F] \geq 1$.

Suppose instead that F is a finite field — in particular, that $F = \mathbf{F}_{p^s}$ for some prime p and integer $s \geq 0$. Now the components B_i and B_j are fields, with $B_i = \mathbf{F}_{p^s}[\beta_{i1}, \beta_{i2}, \ldots, \beta_{ik}]$ and $B_j = \mathbf{F}_{p^s}[\beta_{j1}, \beta_{j2}, \ldots, \beta_{jk}]$. We consider both B_i and B_j to be embedded in some larger extension of $\mathbf{F}_{p^s}$. Since they are both finite fields, B_i and B_j are both normal fields. Thus, taking as E a smallest extension of $\mathbf{F}_{p^s}$ containing both B_i and B_j, we see that $\beta_{jr} \in B_i$ for $1 \leq r \leq k$ since β_{jr} and β_{ir} both belong to E and have the same minimal polynomial over F — so $B_j \subseteq B_i \subseteq E$. Similarly, $B_i \subseteq B_j \subseteq E$, and we have $B_i = B_j = E$ (in this embedding). It follows that the components B_i and B_j of A are isomorphic as extensions of F and that the trace of β_{ir} in B_i over F equals the trace of β_{jr} in B_j over F, for $1 \leq r \leq k$.

Since E is a finite algebraic extension of F and F is perfect, there exists some element ζ of B_i such that the trace of ζ over F is nonzero. Since $a_1, a_2, \ldots, a_k$ is a basis of A over F, there exist elements $\gamma_1, \gamma_2, \ldots, \gamma_k$ of F such that $\gamma_1 a_1 + \gamma_2 a_2 + \cdots + \gamma_k a_k = \zeta$. Repeating the argument given for the case that the characteristic of F is zero, we find that $T_{B_i/F}(\zeta) = T_{B_j/F}(0) = 0$, establishing a contradiction and proving the lemma. ■

Like the algorithm of Section 3, "Simple Components via Idempotents of Basis" can be used to decompose semi-simple algebra over number fields and finite fields; unlike the algorithm of Section 3, it is deterministic.

Theorem 7. *Let $A \subseteq M_{n\times n}(F)$ be a semi-simple algebra of dimension m over a number field or finite field F.*

(i) If F is a number field then, given binary representations of a basis $a_1, a_2, \ldots, a_m$ of a basis for A over F, the algorithm "Simple Components via Idempotents of Basis" computes the number of simple components of A and the dimension and a basis for each component using a number of boolean operations that is polynomial in the input size. If F is a finite field then the algorithm can be used to decompose A or to fail (with probability at most $1/2$) using a number of boolean operations polynomial in the input size.

(ii) If F is a finite field with $q = p^k$ elements (for p prime) then the above algorithm can be implemented to decompose A using (deterministic) boolean circuits with size polynomial in nkp and with depth $O(\log^3(nkp))$ or using (probabilistic) boolean circuits, failing with probability at most $1/2$, with size polynomial in $n \log q$ and with depth $O(\log^2 n \log^2(k+1) \log p)$.

Proof. Correctness of the algorithm follows by Lemma 6. We will perform analysis of the cost of the algorithm in two stages, considering the computation of sets of idempotents $e_{i1}, e_{i2}, \ldots, e_{ik_i}$ for $1 \leq i \leq h$, and then considering the computation of a common refinement $e_1, e_2, \ldots, e_l$ of these sets and generation of bases for the simple components of A.

For computations over number fields, or for probabilistic computations over finite fields, the analysis of the first part of the algorithm is similar to the analysis of the algorithm "Semi-Simple Decomposition via Splitting Element" of Section 3: Again, the cost is dominated by the cost of solving systems of linear equations, computing determinants and ranks of matrices, and factoring polynomials; see the proof of Theorem 5 for a discussion of these operations. The deterministic algorithm of Berlekamp [3] for the factorization of polynomials of degree n over a finite field with size p^k can be implemented using boolean circuits with size polynomial in npk and depth $O(\log^3(npk))$; thus the first part of our algorithm can be implemented at the cost stated in the theorem.

A refinement of two sets of idempotents $e_{11}, e_{12}, \ldots, e_{1k_1}$ and $e_{21}, e_{22}, \ldots, e_{2k_2}$ can be obtained by forming all products $e_{1r}e_{2s}$ for $1 \leq r \leq k_1$ and $1 \leq s \leq k_2$ and including all nonzero products in the new set — using circuits of polynomial size and logarithmic depth. The size of the resulting set of idempotents is at most l. A refinement of h sets can be obtained using a divide-and-conquer approach, forming a refinement $\hat{e}_{11}, \hat{e}_{12}, \ldots, \hat{e}_{1k_1}$ of the first $\lceil (h/2) \rceil$ sets and a refinement $\hat{e}_{21}, \hat{e}_{22}, \ldots, \hat{e}_{2k_2}$ of the last $\lfloor (h/2) \rfloor$ sets, then computing a refinement of this new pair. The size of circuits required to refine h sets instead of two is increased by a multiplicative factor of h, while circuit depth increases by a multiplicative factor of $\log h$. Thus a common refinement of the sets of idempotents can be obtained at the cost stated in the theorem. Bases for the simple components can also be computed from the common refinement at this cost. ∎

The algorithm provides an "NC^2"-reduction from the problem of decomposing a semi-simple algebra over a number field F to that of factoring a squarefree polynomial over F. Suppose now that $f \in F[x]$ is monic, squarefree and has degree n. Then the companion matrix of f and a basis for the algebra (of dimension n) generated over F by this matrix are easily computed, while the factors of f can be found given bases for the simple components of this algebra (see [8] for details). Consequently we have an NC^2-reduction in the other direction as well.

5 Decomposing Algebras over R and C

Algorithms for the decomposition of associative algebras over $\mathbf{R}$ and $\mathbf{C}$ are of practical as well as theoretical interest. While we have no hope of representing an arbitrary algebra over $\mathbf{R}$ or $\mathbf{C}$ exactly and uniquely, let alone decomposing such an algebra, we can do better if we restrict attention to an important class of these algebras — those of the form $A \otimes_F \mathbf{R}$ or $A \otimes_F \mathbf{C}$, where A is an associative algebra over a number field F (we require that $F \subset \mathbf{R}$ when considering $A \otimes_F \mathbf{R}$). We discuss the decomposition of these algebras in the next two sections.

We begin with the computation of a basis for the radical of such an algebra. In order to compute a basis for the radical of $A \otimes_F \mathbf{R}$ over $\mathbf{R}$, or of $A \otimes_F \mathbf{C}$ over $\mathbf{C}$, it is sufficient to compute and return a basis for A over F. A polynomial-time algorithm for this computation is given by Friedl and Rónyai [9].

Theorem 8. *Suppose A is a finite-dimensional associative algebra over a number field F and that $b_1, b_2, \ldots, b_r$ is a basis for the radical of A over F. Then $b_1, b_2, \ldots, b_r$ is also a basis for the radical of $A \otimes_F \mathbf{C}$ over $\mathbf{C}$ and, if $F \subset \mathbf{R}$, a basis for the radical of $A \otimes_F \mathbf{R}$ over $\mathbf{R}$.*

Proof. This is a consequence of the correctness of the method of Friedl and Rónyai [9] for the computation of radicals of algebras over fields of characteristic zero — for this algorithm returns the same basis, regardless of the identity of the ground field (F, $\mathbf{R}$, or $\mathbf{C}$). ■

It follows immediately that if A is semi-simple over F then $A \otimes_F \mathbf{C}$ is semi-simple over $\mathbf{C}$ and, if $F \subset \mathbf{R}$, then $A \otimes_F \mathbf{R}$ is semi-simple over $\mathbf{R}$.

We are not so fortunate when considering the decomposition of semi-simple algebras. Indeed, if A is semi-simple and has dimension m over F then there exists an extension $E \supseteq F$ such that if $B_1, B_2, \ldots, B_l$ are the simple components of $A \otimes_F E$ over E, then $B_1 \otimes_E \mathbf{C}, B_2 \otimes_E \mathbf{C}, \ldots, B_l \otimes_E \mathbf{C}$ are the simple components of $(A \otimes_F E) \otimes_E \mathbf{C} \cong A \otimes_F \mathbf{C}$ over $\mathbf{C}$; however, the smallest such extension E may have dimension $m!$ over F. We obtain a smaller (polynomial size) boolean representation of the simple components of $A \otimes_F \mathbf{R}$ (respectively, $A \otimes_F \mathbf{C}$) by associating a different extension of F to each simple component of $A \otimes_F \mathbf{R}$ ($A \otimes_F \mathbf{C}$).

Henceforth we require that a number field F be represented by the minimal polynomial $f \in \mathbf{Q}[x]$ of an algebraic number $\alpha \in F$ such that $F = \mathbf{Q}[\alpha] \cong \mathbf{Q}[x]/(f)$, and by an isolating interval for α in $\mathbf{R}$ if $F \subset \mathbf{R}$ or by an isolating region for α in $\mathbf{C}$ otherwise. The root α is the only root of f in this interval or region — so that the representation specifies a unique embedding of F in $\mathbf{R}$ or $\mathbf{C}$.

Now if $g \in F[x]$ with degree n and $F \subset \mathbf{C}$ then we can list the roots of g (in effect, factoring g over $\mathbf{C}$) by listing the irreducible factors of g in $F[x]$ and listing isolating regions for each of the roots of each of these factors — describing extensions $E_1, E_2, \ldots, E_n$ of F, not necessarily distinct, each corresponding to one of the roots.

If $g \in F[x]$ with degree n and $F \subset \mathbf{R}$ then g has a factorization in $\mathbf{R}[x]$ of the form

$$g = u_1 u_2 \cdots u_r v_1 v_2 \cdots v_s$$

such that $n = r + 2s$, $u_1, u_2, \ldots, u_r \in \mathbf{R}[x]$ with degree one, and $v_1, v_2, \ldots, v_s$ are quadratic polynomials in $\mathbf{R}[x]$ with no real roots. Each single (real or complex) root of g belongs to an extension of F with degree at most n over F, so an extension $\overline{E}_i$ with degree at most n that contains the coefficients of the linear factor u_i can be found for $1 \leq i \leq r$. The coefficients of each quadratic factor v_i lie in a (real) extension of F with degree at most at most $n(n-1)$ over F — namely, a subfield $\hat{E}_i$ of the extension containing both of the complex roots of v_i. Real roots of g can be identified, complex roots can be matched into pairs of complex conjugates, and the minimal polynomials and isolating intervals of real algebraic numbers $\hat{\alpha}_i$ such that $\hat{E}_i = F[\hat{\alpha}_i]$ can be computed in polynomial time using

the algorithms of Loos [19]. Thus we can compute the real factorization of $g \in F[x]$ in polynomial time.

Now suppose A is a simple algebra over F and let a be a splitting element of A; since $\alpha \in \text{Centre}(A)$ and $\text{Centre}(A) = F[\alpha]$, such an element can be found in polynomial time from a basis for $\text{Centre}(A)$ (using, for example, the algorithm SIMPLE of Loos [19]). Now $\text{Centre}(A)$ is isomorphic to $F[x]/(g)$, where g is the minimal polynomial of α over F. If we factor g over $\mathbf{R}$ as described above, and then use the factors of g and the splitting element a as in the algorithm "Semi-Simple Decomposition via Splitting Element" of Section 3, we obtain a set of extensions $E_1, E_2, \ldots, E_l$ of F (each corresponding to and containing the coefficients of one of the real factors of g) and bases for algebras $B_i \in A \otimes_F E_i$ for $1 \leq i \leq l$ such that

$$A \otimes_F \mathbf{R} \cong (B_1 \otimes_F E_1) \oplus (B_2 \otimes_F E_2) \oplus \cdots \oplus (B_l \otimes_F E_l).$$

Furthermore, for $1 \leq i \leq l$, either $(\text{Centre}(B_i)) \otimes_{E_i} \mathbf{R} \cong \mathbf{R}$ or $(\text{Centre}(B_i)) \otimes_{E_i} \mathbf{R} \cong \mathbf{C}$ — so the algebra $B_i \otimes_{E_i} \mathbf{R}$ is simple over $\mathbf{R}$ for $1 \leq i \leq l$ and is isomorphic to a simple component of $A \otimes_F \mathbf{R}$.

If A is semi-simple over F then the simple components $B_1, B_2, \ldots B_l$ of A over F can be computed using the algorithm of Section 4. For $1 \leq i \leq l$, the simple components of $B_i \otimes_F \mathbf{R}$ can be computed using the method described above; taken together, these comprise the simple components of $A \otimes_F \mathbf{R}$. We can compute the simple components of $A \otimes_F \mathbf{C}$ over $\mathbf{C}$ by a similar method. Analysing this method, we obtain the following result.

Theorem 9. *Suppose F is a number field and we are given a basis $a_1, a_2, \ldots, a_m$ for a semi-simple algebra $A \subseteq M_{n\times n}(F)$ over F. Then the dimensions and representations of the simple components of $A \otimes_F \mathbf{C}$ over $\mathbf{C}$, or of $A \otimes_F \mathbf{R}$ over $\mathbf{R}$ if $F \subset R$, can be computed in polynomial time.* ■

We complete our examination of algebras over $\mathbf{R}$ and $\mathbf{C}$ by considering the decomposition of simple algebras over these fields. We consider the more general problem of decomposing simple algebras over perfect fields, and then focus attention on simple algebras over $\mathbf{R}$ and $\mathbf{C}$, in the next section.

6 Decompositions of Simple Algebras

Suppose again that F is a perfect field and that $A \subseteq M_{n\times n}(F)$ is a simple algebra over F. Then $A \cong M_{k\times k}(D)$ for some division algebra D over F. We decompose A by computing k, as well as

- a basis $d_1, d_2, \ldots, d_h$ for D over F,
- a "standard basis" e_{ij}, $1 \leq i,j \leq k$, for A over D,

so that $e_{rs}e_{tu} = \delta_{st}e_{ru}$ for $1 \leq r,s,t,u \leq k$, $d_r e_{st} = e_{st} d_r$ for $1 \leq r \leq h$ and $1 \leq s,t \leq k$, and so that the elements $d_r e_{st}$ (for $1 \leq r \leq h$ and $1 \leq s,t \leq k$) form a basis for A over F.

Suppose we are given a nonzero primitive idempotent e of A (that is, an element $e \neq 0$ such that $e^2 = e$ and such that for all $f \in A$, if $f^2 = f$ then either $ef = fe = e$ or $ef = fe = 0$). Then A can be decomposed in polynomial time by forming and solving nonsingular systems of linear equations over F and by computing bases for null spaces of singular matrices with entries in F, as explained below.

We first use e to find the idempotents $e_{11}, e_{22}, \ldots, e_{kk}$. These are not unique; in particular, they can be chosen as the identity elements of any set of irreducible right modules $R_1, R_2, \ldots, R_k$ over F such that

$$A = R_1 \oplus R_2 \oplus \cdots \oplus R_k.$$

Since e is a primitive idempotent eA is an irreducible right module. Furthermore, for any $a \in A$, $aeA = \{ aex : x \in A \}$ forms an irreducible right module of A (possibly (0)), and any irreducible right module R of A can be expressed as aeA for some $a \in A$. Since the right modules $a_1eA, a_2eA, \ldots, a_neA$ are each either (0) or nonzero and irreducible, and since A is simple and $a_1, a_2, \ldots, a_n$ is a basis for A, there exists a subset $R_1, R_2, \ldots, R_k$ of these modules such that $A = R_1 \oplus R_2 \oplus \cdots \oplus R_k$. We can find such a subset by including the module a_ieA if and only if it is not contained in the module generated by the elements of $a_1eA, a_2eA, \ldots, a_{i-1}eA$, for $1 \leq i \leq n$. Now, for $1 \leq j \leq k$, the idempotent e_{jj} of A can be computed as the identity element of the right module R_j.

We next compute the elements e_{1j} for $2 \leq j \leq k$. These are not unique: Consider, for example, the simple algebra $M_{2\times 2}(F)$. For any nonzero element α of F, the basis

$$e_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad e_{12} = \begin{bmatrix} 0 & \alpha \\ 0 & 0 \end{bmatrix}, \quad e_{21} = \begin{bmatrix} 0 & 0 \\ \alpha^{-1} & 0 \end{bmatrix}, \quad e_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

is a correct decomposition of A. In general we choose e_{1j} as any nonzero solution (for $x \in (e_{11} + e_{jj})A(e_{11} + e_{jj})$) of the system of linear equations

$$e_{11}x = x, \quad xe_{11} = 0, \quad e_{jj}x = 0, \quad xe_{jj} = x.$$

Now, e_{j1} is the unique solution for $y \in (e_{11} + e_{jj})A(e_{11} + e_{jj})$ of the system

$$e_{11}y = 0, \quad ye_{11} = y, \quad e_{jj}y = y, \quad ye_{jj} = 0, \quad e_{1j}y = e_{11}, \quad ye_{1j} = e_{jj}.$$

The remaining elements e_{ij} are determined by the formula $e_{ij} = e_{i1}e_{1j}$. The only elements of A that commute with all of these are the entries of the division algebra D; we use this fact to find a basis for D over F, completing our decomposition of A. This method for decomposing A using a primitive idempotent is shown in Figure 4.

Algorithm **Decomposition of a Simple Algebra from a Primitive Idempotent**

Input.
- Matrices $a_1, a_2, \ldots, a_m \in M_{n\times n}(F)$ forming a basis for a simple algebra A over a perfect field F
- Matrix $e \in A$, a nonzero primitive idempotent in A

Output.
- Integers $h, k > 0$
- Matrices $d_1, d_2, \ldots, d_h \in A$ forming a basis for a division algebra D over F such that $A \cong M_{k\times k}(D)$
- Matrices $e_{ij} \in A$ for $1 \le i, j \le k$ such that
  - $e_{rs}e_{tu} = \delta_{st}e_{ru}$ for $1 \le r, s, t, u \le k$
  - $e_{rs}d_t = d_t e_{rs}$ for $1 \le r, s \le k$ and $1 \le t \le h$
  - the matrices $e_{rs}d_t$ for $1 \le r, s \le k$ and $1 \le t \le h$ form a basis for A over F

$k := 0$

for $i = 1, 2, \ldots, n$ **do**

  if $a_i e$ is not in the right module generated by $e_{11}, e_{22}, \ldots, e_{kk}$ **then**

    $k := k + 1$

    Compute $e_{kk} \in (a_i e)A$ such that $e_{kk}x = x$ for all $x \in (a_i e)A$

  end if

end for

for $i = 2, 3, \ldots, k$ **do**

  Set e_{1i} to be any nonzero element $x \in (e_{11} + e_{ii})A(e_{11} + e_{ii})$ such that $e_{11}x = x = xe_{ii}$ and $e_{ii}x = 0 = xe_{11}$

  Set e_{i1} to be the (unique) nonzero element $y \in (e_{11} + e_{ii})A(e_{11} + e_{ii})$ such that $e_{ii}y = y = ye_{11}$, $e_{11}y = 0 = ye_{ii}$, $ye_{1i} = e_{ii}$, and $e_{1i}y = e_{11}$

end for

for $i = 2, 3, \ldots, k$ **do**

  for $j = 2, 3, \ldots, k$ **do**

    if $i \neq j$ **then**

      $e_{ij} := e_{i1}e_{1j}$

    end if

  end for

end for

Compute the dimension h and a basis $d_1, d_2, \ldots, d_h$ over F for the set of solutions z of the equations $e_{ij}z = ze_{ij}$, $1 \le i, j \le k$

Return the integers h and k and the matrices e_{ij} and d_l (for $1 \le i, j \le k$ and $1 \le l \le h$) computed above

Figure 4

Now we consider the problem of finding a single nonzero primitive idempotent from a basis for a simple algebra A over F. Rónyai has showed that this problem is difficult if $F = \mathbf{Q}$, and that the problem has a Las Vegas probabilistic polynomial-time solution if F is a finite field (see [23, 24]). For the rest of this section we consider the problems of decomposing simple algebras over $\mathbf{R}$ and $\mathbf{C}$. As in Section 5 we consider algebras of the form $A \otimes_F \mathbf{R}$ or $A \otimes_F \mathbf{C}$ for some number field F.

We begin by reviewing the solution for the decomposition of simple algebras over $\mathbf{C}$ given by Babai and Rónyai [1]. We then extend this method to obtain a Las Vegas probabilistic polynomial-time algorithm for the decomposition of simple algebras over $\mathbf{R}$.

Suppose $A = \hat{A} \otimes_F \mathbf{C}$ for a simple algebra $\hat{A} \subseteq M_{n\times n}(F)$ over a number field F, such that A is simple over $\mathbf{C}$. Then, since the only finite-dimensional division algebra over $\mathbf{C}$ is $\mathbf{C}$ itself, $A \cong M_{k\times k}(\mathbf{C})$ for $k = \sqrt{m}$ and for m the dimension of A over $\mathbf{C}$. It is clear, then, that every element α of A has a minimal polynomial with degree at most k over $\mathbf{C}$, and also that there exists some element a of A whose minimal polynomial has degree k and is squarefree. Furthermore, we can find such an element that is an F-linear combination of the elements of a basis for $\hat{A}$ over F, so that this element is a matrix with entries in F. We can find such a splitting element, or fail (with probability at most $1/2$) using the techniques discussed in Sections 2–3.

Now we adjoin a root $\zeta \in \mathbf{C}$ of $minpol(a)$ to F, to obtain an extension $E = F[\zeta]$ with degree at most k over F. Set $h \in E[x]$ such that $minpol(a) = (x - \zeta)h(x)$, and set $g \in E[x]$ to be a polynomial with degree at most k such that $g(x) \equiv 1 \bmod (x - \zeta)$ and $g(x) \equiv 0 \bmod h(x)$. Then $g(a) \in \hat{A} \otimes_F E$ is a nonzero primitive idempotent of A, which can be used to complete the decomposition of this algebra.

Suppose now that $A = \hat{A} \otimes_F \mathbf{R}$ for a simple algebra $\hat{A} \subseteq M_{n\times n}(F)$ over a number field $F \subset \mathbf{R}$, such that A is a simple algebra of dimension m over $\mathbf{R}$. Since the only finite-dimensional division algebras over $\mathbf{R}$ are $\mathbf{R}$, $\mathbf{C}$, and $\mathbf{H}$ (the ring of real quaternions), one of three cases holds.

(i) $A \cong M_{k\times k}(\mathbf{R})$, for $k = \sqrt{m} \in \mathbf{N}$,

(ii) $A \cong M_{k\times k}(\mathbf{C})$, for $k = \sqrt{(m/2)} \in \mathbf{N}$,

(iii) $A \cong M_{k\times k}(\mathbf{H})$, for $k = \sqrt{(m/4)} \in \mathbf{N}$.

The second case is easily distinguished from the other two: If $A \cong M_{k\times k}(\mathbf{C})$ then $\text{Centre}(A) \cong \mathbf{C}$ and has dimension two over $\mathbf{R}$, while $\text{Centre}(A) \cong \mathbf{R}$ and has dimension one in the other cases.

Suppose now that $\text{Centre}(A) \cong \mathbf{C}$; then $\text{Centre}(\hat{A})$ is a field. We can decompose A over $\mathbf{R}$ by finding a basis (of size k^2) for $\hat{A}$ over $E = \text{Centre}(\hat{A})$, and implementing the algorithm for the decomposition of simple algebras over $\mathbf{C}$, replacing complex arithmetic by arithmetic in $\text{Centre}(A)$, taking care to ensure that the only algebraic numbers adjoined to E are real algebraic numbers, and then performing some housekeeping to ensure that the resulting decomposition is given as a basis of matrices with entries in a *real* extension E of F.

Suppose instead that Centre$(A) \cong \mathbf{R}$. If the dimension m of A over $\mathbf{R}$ is odd then $A \cong M_{k\times k}(\mathbf{R})$, for $k = \sqrt{m}$. Again, we can obtain a splitting element a of A, whose minimal polynomial is squarefree and has odd degree k. Furthermore, we can choose this to be an F-linear combination of elements of a basis for $\hat{A}$ over F. The minimal polynomial of a will have at least one irreducible factor of degree one over $\mathbf{R}$, and hence will have at least one real root ζ contained in an extension E with degree at most k over F. The algorithm used to decompose simple algebras over $\mathbf{C}$ can be applied in this case as well.

Finally, we consider the more difficult case that Centre$(A) \cong \mathbf{R}$ and A has dimension $m = 4l^2$ over $\mathbf{R}$ for some positive integer l, so that either $A \cong M_{2l\times 2l}(\mathbf{R})$ or $A \cong M_{l\times l}(\mathbf{H})$. While we cannot guarantee that a splitting element of A will allow us to distinguish between these cases as directly as before, we can show that it provides a reduction to a simpler problem.

Lemma 10. *Let A be a simple algebra of dimension $m = 4l^2$ over $\mathbf{R}$, isomorphic either to $M_{2l\times 2l}(\mathbf{R})$ or to $M_{l\times l}(\mathbf{H})$.*

(i) Every element of A has a minimal polynomial with degree at most $2l$ over $\mathbf{R}$.

(ii) There exists an element a of A whose minimal polynomial over $\mathbf{R}$ has degree $2l$ and is squarefree.

Proof. This is clear if $A \cong M_{2l\times 2l}(\mathbf{R})$. Part (ii) is easily established for the case $A \cong M_{l\times l}(\mathbf{H})$ as well, for if $i \in \mathbf{H}$ such that $i^2 + 1 = 0$ then the matrix

$$a = \begin{bmatrix} i & & & & 0 \\ & 2i & & & \\ & & 3i & & \\ & & & \ddots & \\ 0 & & & & li \end{bmatrix} \in M_{l\times l}(\mathbf{H})$$

has a squarefree characteristic polynomial

$$\psi = \prod_{j=1}^{l} (x^2 + j^2) \in \mathbf{R}[x].$$

ψ is also the minimal polynomial of a over $\mathbf{R}$ and has degree $2l$ as required.

Part (i) can be proved for the case $A \cong M_{l\times l}(\mathbf{H})$ by introducing an injective homomorphism $\phi : M_{l\times l}(\mathbf{H}) \to M_{2l\times 2l}(\mathbf{C})$ such that, for all $\alpha \in M_{l\times l}(\mathbf{H})$, the characteristic polynomial of $\phi(\alpha)$ has real coefficients. Then this polynomial has degree $2l$ in $\mathbf{R}[x]$ and annihilates α; it follows that the minimal polynomial of α divides this and has degree at most $2l$ as well. For the details of this proof see the proof of Lemma 2.5.14 in [8]. ∎

An element a of A whose minimal polynomial over $\mathbf{R}$ has degree $2l$ and is squarefree, and that is an F-linear combination of elements of a basis for $\hat{A}$ over F, can be computed by

the method described for the computation of splitting elements in Sections 2–3. (The proof of Lemma 1 must be adapted slightly, since we have not shown that $M_{l\times l}(\mathbf{H})$ is isomorphic to a subalgebra of $M_{2l\times 2l}(\mathbf{R})$.)

Suppose now that a is as described above, and let f be the minimal polynomial of f over F — so $f \in F[x]$, has degree $2l$, and is squarefree. If f has an irreducible linear factor over $\mathbf{R}$, and hence a root $\zeta \in \mathbf{R}$, then $A \cong M_{2l\times 2l}(\mathbf{R})$ and, once again, we can decompose A over $\mathbf{R}$ using the method described for simple algebras over $\mathbf{C}$. Suppose instead that $f = f_1 f_2 \cdots f_l$ for irreducible monic quadratic polynomials $f_1, f_2, \ldots, f_l \in \mathbf{R}[x]$. The factor f_1 has coefficients in a small and easily computed real extension E of F. Set $h \in E[x]$ such that $f = f_1 h$, and choose a polynomial $g \in E[x]$ with degree at most $2l$ such that

$$g \equiv 1 \bmod f_1 \quad \text{and} \quad g \equiv 0 \bmod h;$$

then $e = g(a)$ is an idempotent in A, and eAe is a simple algebra of dimension 4 over $\mathbf{R}$. Furthermore,

- $eAe \cong M_{2\times 2}(\mathbf{R})$ if $A \cong M_{2l\times 2l}(\mathbf{R})$;
- $eAe \cong \mathbf{H}$ if $A \cong M_{l\times l}(\mathbf{H})$;
- eAe contains a nonzero primitive idempotent, and every such idempotent is also a nonzero primitive idempotent of A.

Thus, we can use a "splitting element" of A either to decompose A completely, or to reduce the decomposition of A to the problem of decomposing a 4-dimensional simple algebra over $\mathbf{R}$. We complete our solution of the general problem by describing a polynomial-time solution for this last problem.

Suppose B is a 4-dimensional simple algebra over $\mathbf{R}$, given by a basis consisting of matrices in $M_{n\times n}(E)$ for some number field $E \subseteq \mathbf{R}$. Then either $B \cong M_{2\times 2}(\mathbf{R})$ or $B \cong \mathbf{H}$ and every element $b \in B$ has a minimal polynomial with degree at most two over $\mathbf{R}$. Furthermore, $B \cong \mathbf{H}$ if and only if B has a basis $1, I, J, K$ such that 1 is the identity element, $I^2 = J^2 = K^2 = -1$, $IJ = -JI = K$, $JK = -KJ = I$, and $KI = -IK = J$. We determine whether $B \cong \mathbf{H}$, and find a nonzero primitive idempotent of B, by attempting to compute such a basis for B. If we fail, we will exhibit a nonzero primitive idempotent $e \neq 1$ in B, proving that $B \cong M_{2\times 2}(\mathbf{R})$.

Choose $b \in B$ to be any E-linear combination of the elements of our basis for B such that $b \notin \text{Centre}(B)$; then b has a minimal polynomial with degree two over $\mathbf{R}$. If this polynomial is reducible then $B \cong M_{2\times 2}(\mathbf{R})$ and b can be used to find a nonzero primitive idempotent. Otherwise, b can be used to find an element I of B such that $I^2 + 1 = 0$. In particular, if b has minimal polynomial $x^2 + \alpha x + \beta \in \mathbf{R}[x]$ then $4\beta - \alpha^2 > 0$ and we can set

$$I = \frac{2}{\sqrt{4\beta - \alpha^2}} \left(a + \frac{\alpha}{2}\right) \in A \otimes_F F[\sqrt{4\beta - \alpha^2}].$$

Suppose such an element has been found; solving a system of linear equations, we can choose a nonzero element $y \in B$ such that $yI = -Iy$.

Lemma 11. *Let B, I, and y be as above. Then the minimal polynomial of y over $\mathbf{R}$ has degree two over $\mathbf{R}$. Furthermore, this polynomial is irreducible over $\mathbf{R}$ if and only if $B \cong \mathbf{H}$.*

Proof. Since $B \cong \mathbf{H}$ or $B \cong M_{2\times 2}(\mathbf{R})$, the minimal polynomial of y over $\mathbf{R}$ has degree at most two, by Lemma 10. Since $y \notin \text{Centre}(B)$ the degree of y's minimal polynomial is also at least two.

Suppose $B \cong \mathbf{H}$ and suppose f is a proper factor of the minimal polynomial of y; then $f(y)$ is a nonzero zero divisor in B, contradicting the fact that B is a division algebra over $\mathbf{R}$. Thus the minimal polynomial of y is irreducible if $B \cong \mathbf{H}$.

Suppose instead that $B \cong M_{2\times 2}(\mathbf{R})$; then there exists an isomorphism $\phi : B \to M_{2\times 2}(\mathbf{R})$ such that

$$\phi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad \phi(I) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Since $\phi(y)\phi(I) = -\phi(I)\phi(y)$ and y is nonzero,

$$\phi(y) = \begin{bmatrix} \alpha & \beta \\ \beta & -\alpha \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

for some $\alpha, \beta \in \mathbf{R}$. Now the minimal polynomial of y has degree two and equals the characteristic polynomial of $\phi(y)$, $x^2 - (\alpha^2 + \beta^2)$, which is reducible in $\mathbf{R}[x]$. ∎

Now we are done. For if y has a reducible minimal polynomial then $B \cong M_{2\times 2}(\mathbf{R})$ and y can be used to find a nonzero primitive idempotent $e \neq 1$ in B. Otherwise, $B \cong \mathbf{H}$, and no such idempotent exists. In fact, the value y can then be used to find an element J of B such that $J^2 + 1 = 0$ and $IJ = -JI$. Setting $K = IJ$ we obtain a basis $1, I, J, K$ for B over $\mathbf{R}$ such that $IJ = K = -JI$, $JK = I = -KJ$, $KI = J = -IK$, and $I^2 = J^2 = K^2 = -1$.

Our algorithm for the decomposition of two-dimensional central simple algebras over $\mathbf{R}$ is shown in Figure 5. It is used as a subroutine by our algorithm for the decomposition of simple algebras over $\mathbf{R}$, which is sketched in Figure 6. Analysis of the algorithm yields the following result.

Theorem 12. *Suppose $F \subset \mathbf{R}$ is a number field and that $\hat{A} \subseteq M_{n\times n}(F)$ is a simple algebra over F such that $\hat{A} \otimes_F \mathbf{R}$ is simple over $\mathbf{R}$. Then the algorithm "Decomposition of a Simple Algebra over $\mathbf{R}$" can be used to decompose $\hat{A} \otimes_F \mathbf{R}$ or to fail (with probability at most 1/2) in polynomial time.* ∎

Algorithm **Decomposition of a Quaternion Algebra over R**

Input.
- Matrices $a_1, a_2, a_3, a_4 \in M_{n\times n}(F)$ forming a basis for a simple algebra A over a number field $F \subset \mathbf{R}$ such that either $A \otimes_F \mathbf{R} \cong \mathbf{H}$ or $A \otimes_F \mathbf{R} \cong M_{2\times 2}(\mathbf{R})$

Output.
- Flag division_algebra with value "hermitian" if $A \otimes_F \mathbf{R} \cong \mathbf{H}$ and with value "real" otherwise
- **if** division_algebra = "real": An irreducible polynomial $f \in F[x]$ and an isolating interval for a real root α of f such that $A \otimes_F F[\alpha] \cong M_{2\times 2}(F[\alpha])$, as well as a primitive idempotent e of $A \otimes_F F[\alpha]$

Set $\lambda \in A$ to be any element that is not in Centre(A)

Compute the minimal polynomial $\phi = x^2 + ax + b$ of λ over F

if $a^2 - 4b \geq 0$ **then** (ϕ has real roots)

division_algebra := "real"

Compute a monic irreducible factor f of ϕ and an isolating interval for a real root α of f

Compute $g \in (F[\alpha])[x]$ such that $g \equiv 1 \bmod (x - \alpha)$ and $g \equiv 0 \bmod \left(\frac{\phi}{x-\alpha}\right)$

$e := g(\lambda) \in A \otimes_F F[\alpha]$

else (ϕ has no real roots)

$\hat{i} := \lambda + \frac{a}{2} \in A$ (*Note.* $\hat{i}$ has minimal polynomial $x^2 + \left(\frac{4b-a^2}{4}\right)$ in $F[x]$)

Set μ to be any nonzero element of A such that $\mu\hat{i} = -\hat{i}\mu$

(*Note.* $\mu i = -i\mu$, for $i \in A \otimes_F F[\sqrt{4b - a^2}]$ such that $i^2 + 1 = 0$)

Compute the minimal polynomial $\psi = x^2 + cx + d$ of μ over F

if $c^2 - 4d \geq 0$ **then** (ψ has real roots)

division_algebra := "real"

Compute a monic irreducible factor f of ψ and an isolating inverval for a real root α of f

Compute $g \in (F[\alpha])[x]$ such that $g \equiv 1 \bmod (x - \alpha)$ and $g \equiv 0 \bmod \left(\frac{\psi}{x-\alpha}\right)$

$e := g(\mu) \in A \otimes_F F[\alpha]$

else

division_algebra := "hermitian"

end if

end if

Return the desired values

Figure 5

Algorithm **Decomposition of a Simple Algebra over R**

Input.
- Matrices $a_1, a_2, \ldots, a_m \in M_{n\times n}(F)$ forming a basis for a simple algebra A over a number field $F \subset \mathbf{R}$ such that either $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{R})$ for $k = \sqrt{m}$, $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{H})$ for $k = \sqrt{(m/4)}$, or $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{C})$ for $k = \sqrt{(m/2)}$

Output.
- Flag division_algebra with value "real" if $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{R})$, "hermitian" if $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{H})$, and "complex" if $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{C})$
- Minimal polynomial f over F and an isolating interval for a real algebraic number α
- Integer l and a basis $d_1, d_2, \ldots, d_l \in A \otimes_F F[\alpha]$ over $F[\alpha]$ for the division algebra D such that $A \otimes_F F[\alpha] \cong M_{k\times k}(D)$
- Integer k and matrices $e_{ij} \in A \otimes_F F[\alpha]$ such that $e_{11}, e_{22}, \ldots, e_{kk}$ are primitive idempotents, $e_{11} + e_{22} + \cdots + e_{kk} = 1$, $e_{rs}e_{tu} = \delta_{st}e_{ru}$ for $1 \le r, s, t, u \le k$, $d_r e_{st} = e_{st} d_r$ for $1 \le r \le l$ and $1 \le s, t \le k$, and such that the matrices $d_r e_{st}$ (for $1 \le r \le l$ and $1 \le s, t \le k$) form a basis for $A \otimes_F F[\alpha]$ over $F[\alpha]$

OR *failure*, with probability at most 1/2

Constants Required. $2n(n-1)$ distinct elements $\gamma_1, \gamma_2, \ldots, \gamma_{2n(n-1)}$ of F

{ *Identify division_algebra and find a primitive idempotent e* }

Compute a basis $b_1, b_2, \ldots, b_h$ for the Centre of A over F

if $h = 1$ **then** { $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{R})$ or $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{H})$ }

Find an element a of A whose minimal polynomial ψ over F has degree $\sqrt{m}$ and is squarefree, or *fail* with probability at most 1/2

if ψ has a real root **then**

division_algebra := "real"

Use ψ and a to compute an irreducible polynomial $f \in F[x]$ with a real root α, and a primitive idempotent e of $A \otimes_F F[\alpha] \cong M_{k\times k}(F[\alpha])$

else

Compute an irreducible polynomial $\hat{f} \in F[x]$ and an isolating interval for a real root $\hat{\alpha}$ of $\hat{f}$ such that ψ has a quadratic factor $\hat{\psi}$ in $(F[\hat{\alpha}])[x]$

Compute a polynomial $\hat{g} \in (F[\hat{\alpha}])[x]$ with degree less than degree(ψ) such that $\hat{g} \equiv 1 \bmod \hat{\psi}$ and $\hat{g} \equiv 0 \bmod (\psi/\hat{\psi})$

$\hat{e} := \hat{g}(a) \in A \otimes_F F[\hat{\alpha}]$

Figure 6

{ *Note.* $\hat{e}$ is a primitive idempotent if $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{H})$ and is the sum of two primitive idempotents if $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{R})$ }

Compute a basis $\hat{a}_1, \hat{a}_2, \hat{a}_3, \hat{a}_4$ for $\hat{e}(A \otimes_F F[\hat{\alpha}])\hat{e}$ over $F[\hat{\alpha}]$

Use the algorithm "Decomposition of a Quaternion Algebra over $\mathbf{R}$" with input $\hat{a}_1, \hat{a}_2, \hat{a}_3, \hat{a}_4$ and performing computations in $F[\hat{\alpha}]$ to set the flag division_algebra

if division_algebra = "real" **then**

Use the remaining output of "Decomposition of a Quaternion Algebra over $\mathbf{R}$", as well as $\hat{f}$ and $\hat{\alpha}$, to find an irreducible polynomial $f \in F[x]$ and isolating interval for a real root α of f such that $A \otimes_F F[\alpha] \cong M_{k\times k}(F[\alpha])$ for $k = \sqrt{m}$, and to find a primitive idempotent e of $A \otimes_F F[\alpha]$

else { division_algebra = "hermitian" }

$\alpha := \hat{\alpha}$

$f := \hat{f}$

$e := \hat{e}$

end if

end if

else { $A \otimes_F \mathbf{R} \cong M_{k\times k}(\mathbf{C})$ }

division_algebra := "complex"

Compute a basis $\hat{a}_1, \hat{a}_2, \ldots, \hat{a}_{m/2}$ for A over the field Centre(A)

Find an element a of A whose minimal polynomial ψ over Centre(A) has degree $\sqrt{m/2}$ and is squarefree, or *fail* with probability at most $1/2$

Compute an irreducible polynomial $f \in F[x]$ and an isolating interval for a real root α of f such that the field $E = \text{Centre}(A \otimes_F F[\alpha])$ contains an element β such that $\psi(\beta) = 0$

Compute a polynomial $g \in E[x]$ with degree less than the degree of ψ such that $g \equiv 1 \bmod (x - \beta)$ and $g \equiv 0 \bmod \left(\frac{\psi}{x - \beta}\right)$

$e := g(a) \in A \otimes_F F[\alpha]$

end if

Use the algorithm "Decomposition of a Simple Algebra from a Primitive Idempotent" with inputs $a_1, a_2, \ldots, a_m$ and the primitive idempotent e generated above, and performing computations over the field $F[\alpha]$, to compute the integers k and l, basis $d_1, d_2, \ldots, d_l$ in $A \otimes_F F[\alpha]$ for division algebra D, and the matrices $e_{ij} \in A \otimes_F F[\alpha]$ for $1 \le i, j \le k$. Return the polynomial f, its real root α, and these values

Figure 6 (Continued)

7 Problems for Further Work

The algorithms for the decomposition of simple algebras over $\mathbf{R}$ and $\mathbf{C}$ presented here and by Babai and Rónyai [1] are probabilistic. No deterministic polynomial-time (Boolean) algorithms for these problems are known.

As Babai and Rónyai note, the algorithm for simple algebras over $\mathbf{C}$ makes unnecessary field extensions. In particular, if a simple algebra A over $\mathbf{C}$ is given by a basis of matrices over a number field F, and it is known that A contains a primitive idempotent $e \neq 0$ which is also an F-linear combination of the elements of this basis, then the algorithm cannot be used reliably to find such a "rational" idempotent. This is also true of our algorithm for the decomposition of simple algebras over $\mathbf{R}$; an efficient algorithm that avoids these unnecessary extensions is preferable.

A numerical approximation of the elements of a set of generators for an associative algebra does not generally identify the decomposition for that algebra. Numerical computations remain attractive, however; and it is conceivable than an efficient numerical algorithm exists which approximates the components of an algebra, reporting "failure" when numerical input does not determine the number and dimensions of these components uniquely. In particular, can Gabriel's methods be adapted to produce efficient (deterministic) numerical algorithms which are correct in this sense?

References

[1] L. Babai and L. Rónyai.
Computing irreducible representations of finite groups.
Proceedings, 30th Annual Symp. Foundations of Computer Science,
Research Triangle Park, NC, 1989, 93–98.

[2] S. J. Berkowitz.
On computing the determinant in small parallel time using a small number of processors.
Information Processing Letters, 18 (1984), 147–150.

[3] E. R. Berlekamp. Factoring polynomials over finite fields.
Bell System Tech. J., 46 (1967), 1853–1859.

[4] E. R. Berlekamp. Factoring polynomials over large finite fields.
Math. Comp., 24 (1970), 713–735.

[5] A. Borodin, J. von zur Gathen, and J. Hopcroft.
Fast parallel matrix and GCD computations.
Information and Control, 52 (1982), 241–256.

[6] D. G. Cantor and H. Zassenhaus.
A new algorithm for factoring polynomials over finite fields.
Math. Comp., 36 (1981), 587–592.

[7] C. W. Curtis and I. Reiner.
Representation Theory of Finite Groups and Associative Algebras.
Wiley, New York, 1962.

[8] W. Eberly. Computations for algebras and group representations.
Department of Computer Science Technical Report 225/89,
University of Toronto, 1989.

[9] K. Friedl and L. Rónyai.
Polynomial time solutions for some problems in computational algebra.
Proceedings, 17th Annual Symp. Theory of Computing,
Providence, RI, 1985, 153–162.

[10] J. Gabriel.
New methods for reduction of group representations using an extension of Schur's lemma.
J. Math. Phys., 5 (1964), 494–504.

[11] J. Gabriel. New methods for reduction of group representations. II
J. Math. Phys., 9 (1968), 973–976.

[12] J. Gabriel. New methods for reduction of group representations. III
J. Math. Phys., 10 (1969), 1789–1795.

[13] J. Gabriel. New methods for reduction of group representations. IV
J. Math. Phys., 10 (1969), 1932–1934.

[14] J. GABRIEL. Numerical methods for reduction of group representations.
Proceedings, 2nd ACM Symp. Symbolic and Algebraic Manipulation,
Los Angeles, CA, 1971, 180–182.

[15] J. VON ZUR GATHEN. Parallel algorithms for algebraic problems.
SIAM J. Comput., 13 (1984), 802–824.

[16] J. VON ZUR GATHEN. Irreducibility of multivariate polynomials.
JCSS, 31 (1985), 225–264.

[17] S. LANDAU. Factoring polynomials over algebraic number fields.
SIAM J. Comput., 14 (1985), 184–196.

[18] A. K. LENSTRA, H. W. LENSTRA, AND L. LOVÁSZ.
Factoring polynomials with rational coefficients.
Math. Ann., 261 (1982), 515–534.

[19] R. LOOS. Computing in algebraic extensions.
In *Computer Algebra, Symbolic and Algebraic Computation,* Second Edition,
Springer-Verlag, New York, 1983, pp. 173–187.

[20] K. MULMULEY.
A fast parallel algorithm to compute the rank of a matrix over an arbitrary field.
Combinatorica, 7 (1987), 101–104.

[21] J. R. PINKERT. An exact method for finding the roots of a complex polynomial.
ACM Transactions on Mathematical Software, 2 (1976), 351–363.

[22] M. RABIN. Probabilistic algorithms in finite fields.
SIAM J. Comput. 9 (1980), 273–280.

[23] L. RÓNYAI. Simple algebras are difficult.
Proceedings, 19th Annual Symp. Theory of Computing,
New York, NY, 1987, 398–408.

[24] L. RÓNYAI. Zero divisors in quaternion algebras.
Journal of Algorithms 9 (1988), 494–506.

[25] A. SCHÖNHAGE.
The fundamental theorem of algebra in terms of computational complexity.
Technical Report, Universität Tübingen, 1982.

[26] J. T. SCHWARTZ.
Fast probabilistic algorithms for verification of polynomial identities.
JACM 27 (1980), 701–717.