

Efficient Decomposition of Associative Algebras*

W. Eberly[†]

Department of Computer Science
University of Calgary
Calgary, Alberta
Canada, T2N 1N4
email: eberly@cpsc.ucalgary.ca

M. Giesbrecht[‡]

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba
Canada, R3T 2N2
email: mwg@cs.umanitoba.ca

Abstract

We present new, efficient algorithms for some fundamental computations with finite-dimensional (but not necessarily commutative) associative algebras. For a semisimple associative algebra \mathfrak{A} over a finite field or number field F , we show how to compute a basis for the centre of \mathfrak{A} and the complete Wedderburn decomposition of \mathfrak{A} as a direct sum of simple algebras. If \mathfrak{A} is given by a generating set of matrices in $F^{m \times m}$ then our algorithm requires about $O(m^3)$ operations in F , plus the cost of factoring a polynomial in $F[x]$ of degree $O(m)$, and the cost of generating a small number of random elements from \mathfrak{A} . We also show how to compute a complete set of orthogonal primitive idempotents in *any* associative algebra over a finite field.

1 Introduction

Determining the structure of an associative algebra \mathfrak{A} and its modules is a fundamental problem in abstract and applied algebra. Here, a *finite dimensional associative algebra*, or algebra for short, is a finite dimensional vector space over a field F equipped with a multiplication under which the space forms an associative (though not necessarily commutative) ring with identity. In this paper we give very efficient algorithms for some fundamental computations with associative algebras over finite fields and number fields.

Recall that the (*Jacobson*) *radical* $\text{Rad}(\mathfrak{A})$ of an algebra \mathfrak{A} is the intersection of all maximal left ideals in \mathfrak{A} . \mathfrak{A} is said to be *semisimple* if $\text{Rad}(\mathfrak{A}) = 0$ and *simple* if \mathfrak{A} has no nontrivial two-sided ideals. The Wedderburn Structure Theorem (Wedderburn, 1907) shows that for any semisimple \mathfrak{A} ,

$$\mathfrak{A} = \mathfrak{A}_1 \oplus \mathfrak{A}_2 \oplus \cdots \oplus \mathfrak{A}_k \quad (1.1)$$

[†]Research was supported in part by Natural Sciences and Engineering Research Council of Canada research grant OGP0089756.

[‡]Research was supported in part by Natural Sciences and Engineering Research Council of Canada research grant OGP0155376 and University of Manitoba research grant 431-1725-80.

*A complete version of this paper is available via anonymous ftp on ftp.cs.umanitoba.ca in /pub/mwg/wedderburn.ps.Z.

Appears in the Proceedings of the ACM International Symposium on Symbolic and Algebraic Computation, 1996 (ISSAC'96), pp. 170-178.

for simple algebras $\mathfrak{A}_1, \dots, \mathfrak{A}_k \subseteq \mathfrak{A}$, and each $\mathfrak{A}_i \cong D_i^{t_i \times t_i}$ where D_i is a division algebra (non-commutative field) with an extension field E_i of F as its centre. We give a fast probabilistic algorithm to compute a basis for the centre of \mathfrak{A} and a representation of the complete Wedderburn decomposition of \mathfrak{A} as a direct sum of simple algebras.

We suppose throughout that \mathfrak{A} is given by some generating set $\mathcal{L} \subseteq \mathfrak{A}$ which allows us to produce random elements of \mathfrak{A} efficiently. We assume that we can select a “random” element α “uniformly” from \mathfrak{A} using $O(\mathcal{R}(\mathfrak{A}))$ operations in F . A more precise definition is given below.

After introducing some special types of elements needed in the computation in Section 2.1, we show how to identify the centre of \mathfrak{A} in Section 2.2. Over a number field or “large” finite field with at least $12n^6$ elements we present an algorithm for this which requires an expected number of $O((m^3 + \mathcal{F}(m) + \mathcal{R}(\mathfrak{A})) \cdot \log(1/\epsilon))$ operations in F , where $\mathcal{F}(m)$ operations in F are sufficient to factor a polynomial in $F[x]$ of degree m . The algorithm is probabilistic of the *Monte Carlo* type; $\epsilon > 0$ is a user-specified tolerance and the answer is guaranteed correct with probability at least $1 - \epsilon$. In Section 2.3 we show how to decompose the centre to obtain a decomposition of the entire algebra. Assuming that the centre was correctly identified, we find central idempotents and a transition matrix which reveals the simple components with an expected number of $O(m^3 + \mathcal{F}(m) + \mathcal{R}(\mathfrak{A}))$ operations in F . This algorithm is probabilistic of the Las Vegas type: it *always* returns the correct answer. Since one expects to require matrix multiplication in such a computation, the cost of this algorithm is surprisingly low. Asymptotically more exact results, in terms of the cost of matrix and polynomial multiplication, are also presented in Theorems 2.8 and 2.10.

Over a small finite field F , with fewer than $12n^6$ elements, things are somewhat trickier because certain types of elements used in the above algorithms are no longer guaranteed to exist. We can make use of the algorithms for large fields by carefully extending the ground field to one which is sufficiently large. To recover the structure correctly we must work in $O(\log m)$ of these extensions. We instead take a different approach described below.

When \mathfrak{A} is a (not necessarily semisimple) associative algebra over a finite field, we show how to compute a complete set of orthogonal primitive idempotents. Recall that an *idempotent* is an element $\omega \in \mathfrak{A}$ such that $\omega^2 = \omega$. Two idempotents are *orthogonal* if their product is zero, and a nonzero idempotent is *primitive* if it cannot be represented as a sum of two or more nonzero orthogonal idempotents. In Section 3.1 we introduce *decomposable elements* which al-

low the generation of non-trivial idempotents. We show how to use these efficiently and that there are many of them in any algebra. These elements are similar to the “Fitting elements” employed for a similar purpose by Schneider (1990), but are much easier to find. In Section 3.2 we show how to use decomposable elements to compute a complete set of orthogonal primitive idempotents. This algorithm requires an expected number of $O((m^3 + m^2 \log q + \mathcal{R}(\mathfrak{A})) \cdot \log^2(m) \cdot \log(1/\epsilon))$ operations in a finite field F of size q , for an algebra presented as above. This is again a Monte Carlo algorithm: for a user specified ϵ the algorithm returns the correct answer with probability at least $1 - \epsilon$.

Finally, in Sections 3.3 and 3.4 we return to the semisimple case for small fields. In Section 3.3 we show how to construct bases for the simple components and central simple idempotents from any set of primitive orthogonal idempotents. This gives a Monte Carlo algorithm for finding these idempotents which requires an expected number of $O((m^3 + m^2 \log q + \mathcal{R}(\mathfrak{A})) \cdot \log^2(m) \cdot \log(1/\epsilon))$ operations in F and returns the correct answer with probability at least $1 - \epsilon$. We then show in Section 3.4 that there is an efficient test for the correctness of the output of the Monte Carlo algorithms in the finite field case for semisimple algebras. This algorithm actually computes an explicit isomorphism between each simple component and a full matrix algebra over an extension field of F . This yields a *Las Vegas* type probabilistic algorithm (i.e., the output is *always* correct) for the decomposition of semisimple algebras over finite fields which requires an expected number of $O((m^3 + m^2 \log q + \mathcal{R}(\mathfrak{A})) \cdot \log^2(m))$ operations in F .

1.1 Historical Perspective. The study of associative algebras goes back to the seminal work of Peirce (1881), the beautiful structure theorem of Wedderburn (1907), and the exploration of the radical (see Jacobson (1956)). As well as standing as a field of active research in its own right, the importance of this theory in the study of groups and their representations has been developed since Noether (1929).

The computational study of associative algebras is obviously considerably younger. The first general algorithms for computing their structure are due to Friedl & Rónyai (1985), who give polynomial-time algorithms to find the Jacobson radical and to decompose a semisimple algebra as a direct sum of simple algebras. Subsequent work by Rónyai (1987, 1990, 1992) examined additional questions over number fields, and in particular showed that finding a complete set of primitive, orthogonal idempotents in a simple algebra over a number field had the same complexity as factoring integers, i.e., it is (currently) intractable. While theoretically of great interest, these algorithms are probably not practical. For commutative algebras, Gianni *et al.* (1988) give an efficient algorithm to decompose an associative algebra over \mathbb{Q} as a direct sum of local algebras.

Much more practical work on a closely related problem was instigated by Parker (1984), who gives a probabilistic algorithm (the “Meat-Axe”) to test for irreducibility of an \mathfrak{A} -module and to split reducible \mathfrak{A} -modules, where \mathfrak{A} is a matrix algebra over a finite field. While the algorithm is apparently not analysed in general, it appears to work very well for algebras over very small finite fields (typically \mathbb{F}_2). This was extended to work over any ground field in Holt & Rees (1994) for all but one family of modules. This difficulty has apparently now been overcome as well.

The Krull-Schmidt theorem guarantees that every \mathfrak{A} -module M can be uniquely decomposed as a direct sum of indecomposable \mathfrak{A} -modules (up to isomorphism). In his

survey paper, Michler (1990) proposes the open problem of finding an efficient algorithm to find this decomposition in the case when \mathfrak{A} is an algebra over a finite field F . It clearly suffices to find a set of orthogonal primitive idempotents $\omega_1, \dots, \omega_s \in \text{End}_{\mathfrak{A}}(M)$ such that $\sum_{1 \leq i \leq s} \omega_i = 1$, which Michler (1990) also proposes as an open problem. We propose a very efficient algorithm for the computation of a set of orthogonal primitive idempotents of an algebra in Section 3.2. This problem was first addressed in Schneider (1990) for small finite fields by the selection of “Fitting elements” in $\text{End}_{\mathfrak{A}}(M)$ which allow its decomposition. In Section 3.1 we present the similar notion of “decomposable elements” which also allow the efficient decomposition of the algebra, but are much easier to find in general.

1.2 Notation. We will generally tie the complexity of our results to that of matrix multiplication. We assume that $O(\mathcal{M}\mathcal{M}(m))$ operations in a field F are sufficient to multiply two matrices in $F^{m \times m}$. Using the standard algorithm requires $\mathcal{M}\mathcal{M}(n) = n^3$ while the currently best known algorithm of Coppersmith & Winograd (1990) allows $\mathcal{M}\mathcal{M}(n) = n^{2.376}$. Also assume that $O(\mathcal{M}(m))$ operations in F are sufficient to multiply two polynomials in $F[x]$ of degree m . Using the standard algorithm allows $\mathcal{M}(m) = m^2$, while the algorithm of Schönhage & Strassen (1971) and Schönhage (1977) allows $\mathcal{M}(m) = m \log m \log \log m$. For notational convenience in the statement of complexity-theoretic results, if a sub-cubic algorithm for matrix multiplication is used we assume that $\mathcal{M}(m) = m \log m \log \log m$ and that $\mathcal{M}\mathcal{M}(m) = m^\theta$ for some $\theta > 2$. Finally, we assume that a polynomial of degree m in $F[x]$ can be factored using $O(\mathcal{F}(m))$ operations in F . If F is a finite field with q elements, then Berlekamp’s (1970) algorithm allows $\mathcal{F}(m) = \mathcal{M}\mathcal{M}(m) + m^2 \log q$ operations in F . If F is a number field then the algorithm of Landau (1985) will factor a polynomial of degree m with a polynomial number of operations.

1.3 Selecting random elements of \mathfrak{A} . To prove correctness of our probabilistic algorithms, we require some technical conditions on the presumed ability to select a random element α from \mathfrak{A} . Recall that this is assumed to be possible with $O(\mathcal{R}(\mathfrak{A}))$ operations in F . If \mathfrak{A} is finite and small we assume that α is selected uniformly from \mathfrak{A} . When \mathfrak{A} is large or infinite we assume that there exists a basis $\gamma_1, \dots, \gamma_n \in \mathfrak{A}$ for \mathfrak{A} and subset S of F of sufficiently large size κ . Elements of \mathfrak{A} are uniformly generated from $\sum_{1 \leq i \leq k} a_i \gamma_i$ for uniformly and independently selected elements $a_i \in S$.

In practice, almost any “reasonable” scheme for generating random elements of \mathfrak{A} will work. However, the only scheme we know of for generating such elements with provable uniformity requires a basis of n matrices in $F^{m \times m}$ for \mathfrak{A} . In this case $\mathcal{R}(\mathfrak{A}) = nm^2$. The requirement for perfect uniformity can be relaxed somewhat while still maintaining provably correct algorithms, though not sufficiently to yield an asymptotic improvement in performance.

2 The Wedderburn Decomposition over Large Fields

In this section we present an algorithm to compute the Wedderburn decomposition of a semisimple algebra \mathfrak{A} over a finite field or number field F . We assume throughout that \mathfrak{A} decomposes as a sum of full matrix rings over division algebras as in (1.1), so that for $1 \leq i \leq k$ the centre of \mathfrak{A}_i is E_i and $[D_i : E_i] = e_i$. If F is finite then $D_i = E_i$ for all i .

Special elements of \mathfrak{A} (separators, splitting pairs, and complemented splitting pairs) which can be used to decompose \mathfrak{A} efficiently are introduced Section 2.1. We show that these are easy to find if one can choose elements randomly from \mathfrak{A} . In Section 2.2 we employ these elements to give a Monte Carlo algorithm for the centre of \mathfrak{A} . This algorithm will produce an element $\alpha \in \mathfrak{A}$ and polynomials $f_1, \dots, f_l \in \mathbb{F}[x]$ such that $f_1(\alpha), \dots, f_l(\alpha) \in \mathfrak{A}$ form a basis for $\text{Centre}(\mathfrak{A})$. If $|\mathbb{F}| \geq 2n^2$, then the algorithm requires an expected number of $O(\mathcal{MM}(m) \log m \cdot \log(1/\epsilon))$ operations in \mathbb{F} , or an expected number of $O(m^3 \cdot \log(1/\epsilon))$ operations in \mathbb{F} using standard matrix and polynomial arithmetic, and computes the correct answer with probability greater than $1 - \epsilon$ for a user specified ϵ .

In Section 2.3 we use the basis for the centre to obtain a set of central primitive idempotents and a “semisimple transition matrix” which induces a change of basis under which the simple components are revealed. The central idempotents are given by an element $\gamma \in \mathfrak{A}$ and polynomials h_1, \dots, h_k such that $h_i(\gamma) \in \mathfrak{A}$ is the central idempotent corresponding to \mathfrak{A}_i (i.e., $h_i(\gamma)$ is the identity in \mathfrak{A}_i and zero in all other components). This is a Las Vegas algorithm, assuming that a basis for the centre is correctly provided and that $|\mathbb{F}| > 2n^2$, and requires an expected number of $O(\mathcal{MM}(m) \log m + \mathcal{F}(m) + \mathcal{R}(\mathfrak{A}))$ operations in \mathbb{F} , or $O(m^3 + \mathcal{F}(m) + \mathcal{R}(\mathfrak{A}))$ operations in \mathbb{F} using standard matrix and polynomial arithmetic.

2.1 Separators and Splitting Pairs

This section introduces some special types of elements of an algebra which are useful in determining the structure of that algebra. These are employed in later sections to obtain algorithms for computation of the centre of a semisimple algebra, and the central idempotents of an associative algebra, over a sufficiently large ground field.

As shown, for example, by Pierce (1982), the dimension of \mathfrak{D}_i over its centre \mathfrak{E}_i is a perfect square. The dimension of \mathfrak{A}_i over \mathfrak{E}_i is therefore a perfect square as well; suppose it is n_i^2 for $1 \leq i \leq k$. Then, $n = e_1 n_1^2 + \dots + e_k n_k^2$.

The first proposition will serve as the basis for a proof of correctness for an algorithm for the decomposition of semisimple algebras over fields, and motivates the definitions that follow it.

Lemma 2.1 *Suppose \mathfrak{A} is a semisimple algebra over a finite field or number field \mathbb{F} . Let k , \mathfrak{A}_i , e_i , and n_i be as above.*

- (i) *The minimal polynomial of any element of \mathfrak{A} has degree at most $e_1 n_1 + \dots + e_k n_k$ over \mathbb{F} .*
- (ii) *If an element α of \mathfrak{A} has a squarefree minimal polynomial of maximal degree $e_1 n_1 + \dots + e_k n_k$ over \mathbb{F} , then for all $\gamma \in \mathfrak{A}$, γ commutes with α if and only if $\gamma \in \mathbb{F}[\alpha]$.*

Elements of \mathfrak{A} whose minimal polynomials are squarefree and of maximal degree are very useful and capture much of the structure of a semisimple algebra.

Definition 2.2 *An element α of a semisimple algebra \mathfrak{A} is a separator for \mathfrak{A} if α is invertible and has a squarefree minimal polynomial of maximal degree $e_1 n_1 + \dots + e_k n_k$ over \mathbb{F} .*

By the above proposition the centre of \mathfrak{A} is contained in $\mathbb{F}[\alpha]$ for any separator α of \mathfrak{A} . If the ground field \mathbb{F} is sufficiently large then there exists a separator α for \mathfrak{A} such

that the centre of the algebra is equal to $\mathbb{F}[\alpha]$. However, it is not clear how such a separator could be found without decomposing the algebra \mathfrak{A} or computing a basis for its centre first. Fortunately, we will see that a pair of separators which determines the centre is easier to find, if the ground field is sufficiently large.

Definition 2.3 *A pair (α, β) of elements of a semisimple algebra \mathfrak{A} is a splitting pair for \mathfrak{A} if α and β are both separators for \mathfrak{A} , and if the centre of \mathfrak{A} is exactly the set of elements commuting with both α and β .*

If (α, β) is a splitting pair for \mathfrak{A} and the minimal polynomial of α over the ground field \mathbb{F} has degree l , then the centre of \mathfrak{A} could be obtained by solving the system of linear equations

$$(y_0 + y_1 \alpha + \dots + y_{l-1} \alpha^{l-1}) \beta - \beta (y_0 + y_1 \alpha + \dots + y_{l-1} \alpha^{l-1}) = 0$$

for the unknowns y_0, \dots, y_{l-1} in \mathbb{F} . Every solution determines an element $y_0 + y_1 \alpha + \dots + y_{l-1} \alpha^{l-1}$ of $\mathbb{F}[\alpha]$ that commutes with β . Since β is a separator for \mathfrak{A} this implies that $y_0 + y_1 \alpha + \dots + y_{l-1} \alpha^{l-1} \in \mathbb{F}[\beta]$, so that it belongs to $\mathbb{F}[\alpha] \cap \mathbb{F}[\beta]$, the centre of \mathfrak{A} . Conversely, every element of the centre belongs to $\{y_0 + y_1 \alpha + \dots + y_{l-1} \alpha^{l-1} : y_0, \dots, y_{l-1} \in \mathbb{F}\}$ and specifies a solution for the above system.

While it is plausible that this method is faster than previous general methods for computation of the centre, it requires that we form and solve a system of m^2 linear equations in l unknowns. We can do considerably better than this by projecting from the space of matrices to the space of vectors. We show that with sufficiently high probability the desired relationships still hold.

Definition 2.4 *A pair (α, β) of elements of a semisimple matrix algebra $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ over a finite field or number field \mathbb{F} is a complemented splitting pair if (α, β) is a splitting pair for \mathfrak{A} and, furthermore, there exists a pair of vectors (u, v) each in $\mathbb{F}^{m \times 1}$ such that, for all $\mu \in \mathbb{F}[\alpha]$ and $\nu \in \mathbb{F}[\beta]$,*

$$(\mu u = \nu u \text{ and } \mu v = \nu v) \implies \mu = \nu \in \mathbb{F}[\alpha] \cap \mathbb{F}[\beta]. \quad (2.1)$$

Any pair of vectors $(u, v) \in \mathbb{F}^{m \times 1}$ satisfying condition (2.1) is said to complement the splitting pair (α, β) .

Theorem 2.5 *Suppose $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ is a semisimple algebra of dimension n over a finite field or number field \mathbb{F} . If $|\mathbb{F}| > 6n^6$ then a complemented splitting pair for \mathfrak{A} exists.*

Theorem 2.6 *Let $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ be a semisimple matrix algebra over a finite field or number field \mathbb{F} . Let S be a finite subset of \mathbb{F} with size $\kappa \geq 4n^6/\epsilon$, for $\epsilon > 0$. If the elements α, β are randomly and independently chosen from \mathfrak{A} as in Section 1.3, and u, v are chosen uniformly and independently from $S^{m \times 1}$, then (α, β) is a complemented splitting pair for \mathfrak{A} that is complemented by (u, v) with probability at least $1 - \epsilon$.*

2.2 Computation of the Centre over Large Fields

The centre of \mathfrak{A} can be computed efficiently if a complemented splitting pair (and a pair of vectors that complements it) is available.

Lemma 2.7 *If $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ is a semisimple matrix algebra over a finite field or number field \mathbb{F} then, given a complemented splitting pair (α, β) for \mathfrak{A} and a pair of vectors (u, v) that complements it, a set of polynomials $f_1, \dots, f_l \in \mathbb{F}[x]$ that each has degree less than m can be computed such that $f_1(\alpha), \dots, f_l(\alpha)$ is a basis for the centre of \mathfrak{A} , using a deterministic algorithm in time $O(\min(m^3, \mathcal{MM}(m) \log m))$.*

Indeed, by Definitions 2.3 and 2.4, it suffices to find a basis for the set of solutions of a homogeneous system of $2m$ linear equations in $2m$ unknowns in order to compute these polynomials if a complemented splitting pair is available.

Theorems 2.5 and 2.6 imply that the a basis for the centre of \mathfrak{A} can be computed efficiently, provided that \mathbb{F} is sufficiently large and \mathfrak{A} is given by a basis over \mathbb{F} .

Theorem 2.8 *Let $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ be a semisimple matrix algebra over a finite field or number field \mathbb{F} with at least $12n^6$ elements. An element α of \mathfrak{A} , and polynomials $f_1, \dots, f_l \in \mathbb{F}[x]$ that have degree less than m such that $f_1(\alpha), \dots, f_l(\alpha)$ is a basis for the centre of \mathfrak{A} , can be computed using a Monte Carlo algorithm that is guaranteed to produce the correct answer with probability at least $1 - \epsilon$ for a user specified parameter $\epsilon > 0$, with $O((\mathcal{M}\mathcal{M}(m) \log m + \mathcal{R}(\mathfrak{A})) \cdot \log(1/\epsilon))$ operations in \mathbb{F} , or $O((m^3 + \mathcal{R}(\mathfrak{A})) \cdot \log(1/\epsilon))$ operations in \mathbb{F} using standard matrix and polynomial arithmetic.*

Proof. Since \mathbb{F} has size greater than $6n^6$, Theorem 2.5 implies that a complemented splitting pair for \mathfrak{A} exists. The algorithm generates random elements $\alpha, \beta \in \mathfrak{A}$ and $u, v \in \mathbb{F}^{m \times 1}$ as in Theorem 2.6. With probability at least $1/2$, (α, β) is a complemented splitting pair for \mathfrak{A} that is complemented by (u, v) . In this case, Lemma 2.7 implies that these values can be used to compute the centre for \mathfrak{A} deterministically at the cost stated in the theorem.

To increase the probability of success to $1 - \epsilon$, we first attempt to determine the degree of the minimal polynomial of a separator in \mathfrak{A} . Choose k_1 elements in \mathfrak{A} and compute the minimal polynomial of each, and let l be the degree of the minimal polynomial which is squarefree of maximal degree. This is the degree of the minimal polynomial of any separator, and hence the dimension of $\text{Centre}(\mathfrak{A})$ over \mathbb{F} , with probability at least $1 - 1/2^{k_1}$.

Now attempt to choose k_2 complemented splitting pairs (α, β) and vectors u, v as above, discarding any where the minimal polynomial of α or β has degree less than l or is not squarefree. Assuming l is correct (i.e., it really is the degree of the minimal polynomial of a separator) these are all separators. Hence $\mathbb{F}[\alpha] \cap \mathbb{F}[\beta]$ is a superset of $\text{Centre}(\mathfrak{A})$, as is the candidate subspace computed for the centre in Lemma 2.7. The correct centre is a candidate subspace of minimal dimension over \mathbb{E} , and we return this correctly with probability $1 - (1/2)^{k_1 + k_2}$. Choosing $k_1, k_2 = 1 + \lceil \log_2(1/\epsilon) \rceil$ yields the desired result. \square

2.3 Identification of Simple Components

Recall that corresponding to the decomposition (1.1) there are orthogonal central idempotents $\omega_1, \dots, \omega_k \in \mathfrak{A}$ such that $\omega_1 + \dots + \omega_k = 1 \in \mathfrak{A}$, $\omega_r \omega_s = 0$ if $r \neq s$, and ω_j is the identity element of the simple algebra $\mathfrak{A}\omega_j \cong \mathfrak{A}_j$, for $1 \leq j \leq k$. In this section an asymptotically fast algorithm will be given for the identification of the simple components of \mathfrak{A} .

Polynomial-time algorithms for this computation have previously been given by Friedl & Rónyai (1985). The algorithm to be given here is based on a later algorithm of Eberly (1991). The new algorithm is asymptotically faster than previous algorithms.

Definition 2.9 *A nonsingular matrix $X \in \mathbb{F}^{m \times m}$ is a semisimple transition matrix for a semisimple matrix algebra $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ over a finite field or number field \mathbb{F} , with k simple components $\mathfrak{A}_1, \dots, \mathfrak{A}_k$, if the following conditions are satisfied.*

- (i) *For all elements η of \mathfrak{A} , $X\eta X^{-1}$ is a block diagonal matrix. In particular, there exist positive integers m_1, \dots, m_k such that $m_1 + \dots + m_k = m$ and, for all $\eta \in \mathfrak{A}$,*

$$\eta = X^{-1} \begin{pmatrix} \eta_1 & & 0 \\ & \ddots & \\ 0 & & \eta_k \end{pmatrix} X,$$

where $\eta_j \in \mathbb{F}^{m_j \times m_j}$ for $1 \leq j \leq k$.

- (ii) *The central primitive idempotents of \mathfrak{A} are $\omega_1, \dots, \omega_k$, where*

$$\omega_j = X^{-1} \begin{pmatrix} D_{j,1} & & 0 \\ & \ddots & \\ 0 & & D_{j,k} \end{pmatrix} X,$$

$D_{j,j}$ is the identity matrix of order m_j and $D_{j,l}$ is the zero matrix of order m_l if $1 \leq l \leq k$ and $l \neq j$.

Theorem 2.10 *Suppose $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ is a semisimple algebra of dimension $n \geq 2$ with k simple components over a finite field or number field with at least $2n^2$ elements. Given a basis for \mathfrak{A} and $\alpha \in \mathfrak{A}$ and $g_1, \dots, g_l \in \mathbb{F}[x]$ such that $g_1(\alpha), \dots, g_l(\alpha) \in \mathfrak{A}$ form a basis for $\text{Centre}(\mathfrak{A})$, we can compute*

- (i) *a semisimple transition matrix X for \mathfrak{A} ,*
- (ii) *positive integers m_1, \dots, m_k such that $m_1 + \dots + m_k = m$ and such that for all $\eta \in \mathfrak{A}$, $X\eta X^{-1}$ has diagonal blocks of orders m_1, \dots, m_k ,*
- (iii) *an element $\gamma \in \text{Centre}(\mathfrak{A})$ that is a separator for the commutative algebra $\text{Centre}(\mathfrak{A})$ over \mathbb{F} , and*
- (iv) *polynomials $h_1, \dots, h_k \in \mathbb{F}[x]$ with degree less than the dimension of the centre of \mathfrak{A} over \mathbb{F} such that $h_1(\gamma), \dots, h_k(\gamma)$ are the central primitive idempotents of \mathfrak{A} ,*

using a Las Vegas algorithm that requires an expected number of $O(\mathcal{M}\mathcal{M}(m) \log m + \mathcal{F}(m))$ operations in \mathbb{F} , or an expected number of $O(m^3 + \mathcal{F}(m))$ operations in \mathbb{F} using standard matrix and polynomial arithmetic.

Proof. Lemmas 2.1 and 3.1 of Eberly (1991) imply that an element of the centre whose minimal polynomial is squarefree and has degree equal to the dimension of the centre over \mathbb{F} can be selected as a random linear combination of $g_1(\alpha), \dots, g_l(\alpha)$. In particular, if values b_1, \dots, b_l are chosen uniformly and independently from a finite subset S of \mathbb{F} with size at least $2n^2$, and $g = b_1 g_1 + \dots + b_l g_l \in \mathbb{F}[x]$, then $\gamma = g(\alpha) = b_1 g_1(\alpha) + \dots + b_l g_l(\alpha)$ has these properties, and is a separator for $\text{Centre}(\mathfrak{A})$, with probability at least $1/2$. Since we know $[\text{Centre}(\mathfrak{A}) : \mathbb{F}]$, we can correctly find such an element with an expected number of 2 choices.

Suppose the minimal polynomial of γ is $f \in \mathbb{F}[x]$. If γ is a separator for the centre then f is squarefree with degree l — and, since the centre is a direct sum of k fields, f has k distinct monic irreducible factors. Suppose $f = \prod_{i=1}^k f_i$ is a factorization of f in $\mathbb{F}[x]$. A result of Giesbrecht (1995) (Theorem 7.4) implies that a “rational Jordan form” can be computed for γ efficiently. That is, one can find a nonsingular matrix X such that

$$X^{-1} \gamma X = \begin{pmatrix} \gamma_1 & & 0 \\ & \ddots & \\ 0 & & \gamma_k \end{pmatrix}$$

is block diagonal, and the i^{th} block γ_i has minimal polynomial f_i , for $1 \leq i \leq k$. Set m_i to be the order of γ_i (so, $\gamma_i \in \mathbb{F}^{m_i \times m_i}$) for $1 \leq i \leq k$.

Finally, let $h_1, \dots, h_k \in \mathbb{F}[x]$ be polynomials with degree less than the degree of the minimal polynomial of γ (and, therefore, less than the dimension of the centre of \mathfrak{A} over \mathbb{F}) such that

$$h_i \equiv \begin{cases} 1 & (\text{mod } f_j) \text{ if } 1 \leq j \leq k \text{ and } j = i, \\ 0 & (\text{mod } f_j) \text{ if } 1 \leq j \leq k \text{ and } j \neq i. \end{cases}$$

Then it is easily checked that

$$h_i(\gamma) = \omega_j = X^{-1} \begin{pmatrix} D_{j,1} & & 0 \\ & \ddots & \\ 0 & & D_{j,k} \end{pmatrix} X,$$

where $D_{j,l} \in \mathbb{F}^{m_l \times m_l}$ is as described in Definition 2.9. Thus, $\omega_1, \dots, \omega_k$ are the central simple idempotents of \mathfrak{A} , X is a semisimple transition matrix for \mathfrak{A} , and the output of this process is correct, provided that the attempt to find a separator γ for the centre was successful.

Since $l \leq m$, the coefficients of a polynomial $g = b_1 g_1 + \dots + b_l g_l$ can be computed using $O(m^2)$ operations. The matrix $\gamma = g(\alpha)$ can be computed using a Las Vegas algorithm of Giesbrecht (1995) in time $O(\mathcal{M}\mathcal{M}(m) \log m)$ or expected time $O(m^3)$ using standard matrix and polynomial arithmetic. The minimal polynomial of this matrix can be computed in at most this cost, using the Las Vegas algorithm of Giesbrecht (1995), and this can be factored with cost $\mathcal{F}(m)$. The transition matrix X can be computed from γ and these polynomials using Giesbrecht's (1995) algorithm for the "rational Jordan form" of a matrix, again at the same cost. The integers m_1, \dots, m_k can be obtained by computing and inspecting the matrix $X^{-1}\gamma X$. Finally, the polynomials h_1, \dots, h_k can be computed using divide and conquer in time $O(m\mathcal{M}(m) \log k)$, or time $O(km^2)$ using standard arithmetic. \square

3 Finding Primitive Orthogonal Idempotents

In this section we give an algorithm which finds a complete set of primitive orthogonal idempotents for any algebra \mathfrak{A} over a finite field \mathbb{F} . The idea is to make use of *decomposable* elements in \mathfrak{A} . These are elements whose minimal polynomials in $\mathbb{F}[x]$ have at least two relatively prime factors in $\mathbb{F}[x]$. A decomposable $\alpha \in \mathfrak{A}$ allows us to compute orthogonal idempotents $\omega_1, \dots, \omega_l \in \mathfrak{A}$ such that $\omega_1 + \dots + \omega_l = 1 \in \mathfrak{A}$ and

$$\mathfrak{A} = \mathfrak{A}\omega_1 \oplus \mathfrak{A}\omega_2 \oplus \dots \oplus \mathfrak{A}\omega_l, \quad (3.1)$$

a direct sum of left ideals. This idea is similar in spirit to the use of *fitting elements* by Schneider (1990). Fitting elements are zero divisors which are not nilpotent and also allow the decomposition of \mathfrak{A} as a sum of left ideals. However, whereas fitting elements are relatively rare in \mathfrak{A} when \mathbb{F} is large — Schneider shows they have density about $1/|\mathbb{F}|$ — decomposable elements have a high density. In Section 3.1 we present a new algorithm which finds decomposable elements efficiently, and constructs a corresponding set of orthogonal idempotents.

This algorithm, with high probability, produces *balanced* decomposable elements, such that the decomposition (3.1) is into ideals of about the same size. In Section 3.2 it is shown how to iterate this algorithm to find a complete set of primitive orthogonal idempotents efficiently.

In Section 3.3, we use these techniques to decompose semisimple algebras over small finite fields as a direct sum of simple algebras, much as we did for large finite fields and number fields in Section 2. Finally, in Section 3.4 we show how to compute an explicit isomorphism between each simple component of a semisimple \mathfrak{A} and a full matrix algebra over an extension field of \mathbb{F} . If these isomorphisms are successfully computed, we obtain a certificate that \mathfrak{A} is indeed semisimple. With this check, our decomposition algorithm for semisimple algebras over finite fields is of the Las Vegas type, i.e., it never produces an incorrect answer.

3.1 Finding balanced decomposable elements efficiently

In this section we introduce the notion of balanced decomposable elements, show how to find them efficiently and how to construct idempotents from them. We assume throughout this section that \mathfrak{A} is a subalgebra of $\mathbb{F}^{m \times m}$ of dimension n (not necessarily semisimple).

For any algebra \mathfrak{A} , a *decomposable element* $\alpha \in \mathfrak{A}$ is defined as an element whose minimal polynomial $f \in \mathbb{F}[x]$ has a factorization $f = f_1 f_2 \dots f_l$ into two or more monic, pairwise relatively prime $f_i \in \mathbb{F}[x] \setminus \mathbb{F}$. In this case we can construct idempotents $\omega_1, \dots, \omega_l \in \mathfrak{A}$ as follows. For $1 \leq i \leq l$, use the Chinese remainder theorem to construct $h_i \equiv 1 \pmod{f_i}$, $h_i \equiv 0 \pmod{f_j}$ for $j \neq i$, and assign $\omega_i = h_i(\alpha) \in \mathfrak{A}$. It follows easily that each ω_i is an idempotent, that $\omega_i \omega_j = 0$ for $i \neq j$ (i.e., they are pairwise orthogonal) and that $\omega_1 + \dots + \omega_l = 1 \in \mathfrak{A}$. We call ω_i the idempotent that *corresponds to* f_i .

Lemma 3.1 *Given a decomposable $\alpha \in \mathfrak{A}$, we can compute*

- (i) *the minimal polynomial $f \in \mathbb{F}[x]$ of α and the factorization $f = f_1 f_2 \dots f_l$ into powers of distinct irreducible polynomials in $\mathbb{F}[x]$,*
- (ii) *polynomials $h_1, \dots, h_l \in \mathbb{F}[x]$ such that $\omega_i = h_i(\alpha)$, $1 \leq i \leq l$, are pairwise orthogonal idempotents with $\sum_{1 \leq i \leq l} \omega_i = 1 \in \mathfrak{A}$,*
- (iii) *$m_1, \dots, m_l \in \mathbb{N}$ such that $m = m_1 + \dots + m_l$ and such that ω_i has rank m_i as a matrix in $\mathbb{F}^{m \times m}$,*
- (iv) *a matrix $U \in \mathbb{F}^{m \times m}$ such that*

$$\hat{\omega}_i = U^{-1} \omega_i U = \begin{pmatrix} D_{i1} & & & \\ & \ddots & & \\ & & D_{ii} & \\ & & & \ddots \\ & & & & D_{il} \end{pmatrix} \in \mathbb{F}^{m \times m}, \quad (3.2)$$

where $D_{ij} \in \mathbb{F}^{m_j \times m_j}$ is the identity matrix when $j = i$ and the zero matrix when $j \neq i$,

with a Las Vegas algorithm using an expected number of $O(\mathcal{M}\mathcal{M}(m) \log m + \mathcal{M}(m) \log q)$ operations in \mathbb{F} , or $O(m^3 + m^2 \log q)$ operations in \mathbb{F} using standard matrix and polynomial arithmetic.

Proof. First, compute the rational Jordan form of $\alpha \in \mathbb{F}^{m \times m}$, and a transition matrix $U \in \mathbb{F}^{m \times m}$ to this form. Recall that this is a block diagonal matrix $J \in \mathbb{F}^{m \times m}$, such that

$$U^{-1} \alpha U = J = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_l \end{pmatrix} \in \mathbb{F}^{m \times m}.$$

Each rational Jordan block $J_i \in \mathbb{F}^{m_i \times m_i}$ is associated to a distinct irreducible factor $g_i \in \mathbb{F}[x]$ of the minimal polynomial $f \in \mathbb{F}[x]$ of α , and

$$J_i = \begin{pmatrix} C_{g_i^{c_{i1}}} & & \\ & \ddots & \\ & & C_{g_i^{c_{ik_i}}} \end{pmatrix} \in \mathbb{F}^{m_i \times m_i},$$

where $C_{g_i^{c_{ij}}}$ is the companion matrix of $g_i^{c_{ij}} \in \mathbb{F}[x]$. We assume that $c_{i1} \geq c_{i2} \geq \dots \geq c_{ik_i}$, so $f_i = g_i^{c_{i1}}$ and the minimal polynomial of α is $f = g_1^{c_{11}} \dots g_l^{c_{l1}}$. Giesbrecht (1995) gives a Las Vegas algorithm to compute this rational Jordan form along with a transition matrix $U \in \mathbb{F}^{m \times m}$ and the minimal polynomial $f \in \mathbb{F}[x]$ using an expected number of $O(\mathcal{MM}(m) \log m + \mathcal{M}(m) \log q)$ operations in \mathbb{F} , or $O(m^3 + m^2 \log q)$ operations in \mathbb{F} using standard arithmetic.

For $1 \leq i \leq l$, let $h_i \in \mathbb{F}[x]$ with $h_i \equiv 1 \pmod{f_i}$, $h_i \equiv 0 \pmod{f_j}$ for $i \neq j$. These can be computed using a divide and conquer application of the Chinese remainder algorithm with $O(m\mathcal{M}(m) \log l)$ operations in \mathbb{F} , or $O(m^2 l)$ operations using standard arithmetic. For $1 \leq i \leq l$, $\omega_i = h_i(\alpha)$. Under the change of basis induced by U , each ω_i has the properties described in (iv). \square

It will be useful to find idempotents which partition \mathfrak{A} into components of approximately the same size. The following theorem addresses this concern for simple algebras. Recall that any simple algebra over \mathbb{F} is isomorphic to $\mathbb{E}^{r \times r}$ over an extension field \mathbb{E} of \mathbb{F} .

Theorem 3.2 *Let $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ be a simple algebra of dimension n with $\mathfrak{A} \cong \mathbb{E}^{r \times r}$, where $\mathbb{E} \cong \mathbb{F}_{q^\mu}$ and $\mathbb{F} \cong \mathbb{F}_q$. The number of $\alpha \in \mathfrak{A}$ with $f = \min_{\mathbb{F}}(\alpha)$ such that there exists a factorization $f = f_1 f_2$ for relatively prime $f_1, f_2 \in \mathbb{F}[x]$ with corresponding idempotents ω and $1 - \omega$, and $n/2 \leq \dim_{\mathbb{F}}(\mathfrak{A}\omega) \leq 3n/4$ is at least $q^n/22$.*

This theorem is a great understatement of the number of such ‘‘balanced’’ reducible elements in \mathfrak{A} . At the very least, the estimate of the density of balanced reducible elements should easily be improved to something approaching 1/5 by a computer aided enumeration of cases creating difficulties, namely when $\mathbb{F} = \mathbb{F}_q$ for very small q .

3.2 Finding primitive orthogonal idempotents

In this section we describe an algorithm to compute a complete set of primitive, orthogonal idempotents $\omega_1, \dots, \omega_s \in \mathfrak{A}$ such that $\sum_{1 \leq i \leq s} \omega_i = 1 \in \mathfrak{A}$. The idea is to iterate the algorithm described in Lemma 3.1 on randomly chosen elements $a \in \mathfrak{A}$.

Suppose we have computed pairwise orthogonal idempotents $\omega_1, \dots, \omega_l \in \mathfrak{A}$ and a transition matrix $U \in \mathbb{F}^{m \times m}$ as in (3.2), so that $U^{-1}\omega_i U$ is zero except for a $d_i \times d_i$ identity block on the diagonal. The two-sided Peirce decomposition of \mathfrak{A} with respect to these idempotents is

$$\mathfrak{A} = \bigoplus_{1 \leq i \leq l} \bigoplus_{1 \leq j \leq l} \omega_i \mathfrak{A} \omega_j.$$

The main idea behind the algorithm is that we only have to work in the subalgebra

$$\bigoplus_{1 \leq i \leq l} \omega_i \mathfrak{A} \omega_i.$$

To see why this is true, note that if ω_i is primitive then $\omega_i \mathfrak{A} \omega_i$ is a local algebra and can be decomposed no further. Conversely, if ω_i is not primitive, that is, $\omega_i = \omega_{i1} + \omega_{i2}$ for orthogonal idempotents $\omega_{i1}, \omega_{i2} \in \mathfrak{A}$, then ω_{i1} and ω_{i2} are in $\omega_i \mathfrak{A} \omega_i$ since $\omega_i \omega_{i1} \omega_i = \omega_{i1}$ and $\omega_i \omega_{i2} \omega_i = \omega_{i2}$. Thus, we need only decompose $\omega_i \mathfrak{A} \omega_i$ to refine the idempotent ω_i .

Suppose we have already computed a transition matrix $U \in \mathbb{F}^{m \times m}$ and orthogonal idempotents $\omega_1, \dots, \omega_l \in \mathfrak{A}$ as in Lemma 3.1. Let $\hat{\mathfrak{A}} = U^{-1} \mathfrak{A} U$ and $\hat{\omega}_i = U^{-1} \omega_i U \in \hat{\mathfrak{A}}$ for $1 \leq i \leq l$. Clearly $\hat{\mathfrak{A}} \cong \mathfrak{A}$, and the element $\hat{\omega}_i$ is filled with zeros except for a $d_i \times d_i$ identity matrix in the i th diagonal block. It is computationally easy to compute a linear map

$$\psi : \mathfrak{A} \rightarrow \bigoplus_{1 \leq i \leq l} \hat{\omega}_i \hat{\mathfrak{A}} \hat{\omega}_i.$$

Simply map $\beta \in \mathfrak{A}$ to

$$\begin{aligned} \beta \mapsto U^{-1} \beta U &= \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1l} \\ b_{21} & b_{22} & & b_{2l} \\ \vdots & & & \vdots \\ b_{l1} & \dots & \dots & b_{ll} \end{pmatrix} \\ \mapsto \begin{pmatrix} b_{11} & 0 & \dots & 0 \\ 0 & b_{22} & & \vdots \\ \vdots & & & 0 \\ 0 & \dots & 0 & b_{ll} \end{pmatrix} &\in \bigoplus_{1 \leq i \leq l} \hat{\omega}_i \hat{\mathfrak{A}} \hat{\omega}_i \end{aligned} \quad (3.3)$$

where $b_{ij} \in \mathbb{F}^{d_i \times d_j}$. A randomly chosen $\beta \in \mathfrak{A}$ will yield randomly and independently chosen components $b_{ii} \in \hat{\omega}_i \hat{\mathfrak{A}} \hat{\omega}_i$.

A refinement of each of the ω_i 's can be computed by decomposing the algebra $\hat{\omega}_i \hat{\mathfrak{A}} \hat{\omega}_i$ as in Lemma 3.1 (assuming for now that we can find a decomposable element), for $1 \leq i \leq l$. Assume we obtain $\hat{\omega}_i = \hat{\omega}_{i1} + \dots + \hat{\omega}_{il_i}$ for pairwise orthogonal idempotents $\hat{\omega}_{i1}, \dots, \hat{\omega}_{il_i} \in \hat{\omega}_i \hat{\mathfrak{A}} \hat{\omega}_i$. Also assume that $V_i \in \mathbb{F}^{d_i \times d_i}$ is the obtained transition matrix, that $\hat{\omega}_{ij}$ has rank d_{ij} , and that $\tilde{\omega}_{ij} = V_i^{-1} \hat{\omega}_{ij} V_i$ is a $d_i \times d_i$ matrix which is all zero except for a $d_{ij} \times d_{ij}$ identity matrix in the j th block on the diagonal. If

$$V = \begin{pmatrix} V_1 & & \\ & \ddots & \\ & & V_l \end{pmatrix} \in \mathbb{F}^{m \times m},$$

then $W = UV$ is a transition matrix for \mathfrak{A} to this refined set of idempotents. That is, if $\omega_{ij} = W^{-1} \tilde{\omega}_{ij} W \in \mathfrak{A}$, we have

$$\sum_{1 \leq i \leq l} \sum_{1 \leq j \leq l_i} \omega_{ij} = 1 \in \mathfrak{A} \quad \text{and} \quad \omega_i = \sum_{1 \leq j \leq l_i} \omega_{ij}$$

for $1 \leq i \leq l$.

Theorem 3.3 *Let $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ be an algebra of dimension n over $\mathbb{F} \cong \mathbb{F}_q$. Then we can compute*

- (i) a transition matrix $U \in \mathbb{F}^{m \times m}$, and
- (ii) $d_1, \dots, d_s \in \mathbb{Z}_{>0}$ such that $m = d_1 + \dots + d_s$,

such that the following holds. For $1 \leq i \leq s$ let

$$\hat{\omega}_i = \begin{pmatrix} D_{i1} & & \\ & \ddots & \\ & & D_{is} \end{pmatrix} \in \mathbb{F}^{m \times m}, \quad \omega_i = U \hat{\omega}_i U^{-1} \in \mathfrak{A},$$

where $D_{ij} \in \mathbb{F}^{d_i \times d_i}$ is the identity matrix if $i = j$ and the zero matrix if $i \neq j$. Then $\omega_1, \dots, \omega_s$ are primitive, pairwise orthogonal idempotents in \mathfrak{A} and $\omega_1 + \dots + \omega_s = 1 \in \mathfrak{A}$.

The computation can be performed with a Monte Carlo algorithm, that returns a correct answer with probability at least $1 - \epsilon$ for a use specified parameter $\epsilon > 0$, using an expected number of $O((\mathcal{M}\mathcal{M}(m) \log m + \mathcal{M}(m) \log q + \mathcal{R}(\mathfrak{A})) \cdot \log^2(m) \cdot \log(1/\epsilon))$ operations in \mathbb{F} , or $O((m^3 + m^2 \log q + \mathcal{R}(\mathfrak{A})) \cdot \log^2(m) \cdot \log(1/\epsilon))$ operations using standard matrix and polynomial arithmetic.

Proof.

First, we note that the above algorithm is correct. At each iteration of the algorithm, suppose we have a transition matrix $U \in \mathbb{F}^{m \times m}$ and d_1, \dots, d_l the ranks of orthogonal idempotents $\omega_1, \dots, \omega_l \in \mathfrak{A}$. Choose a random $\alpha \in \mathfrak{A}$, and find $\psi(\alpha) \in \bigoplus_{1 \leq i \leq l} \hat{\omega}_i \mathfrak{A} \hat{\omega}_i$. Suppose α_i is the image of α in $\hat{\omega}_i \mathfrak{A} \hat{\omega}_i$. The α_i 's are also random and independent. As described above, use Lemma 3.1 to refine each $\hat{\omega}_i$, and compute a new transition matrix W . If ω_i is not primitive, then $\omega_i \mathfrak{A} \omega_i$ is non-local, and such reducible elements α_i exist (if $\omega_i = \omega_{i1} + \omega_{i2}$ for orthogonal idempotents ω_{i1}, ω_{i2} , then these idempotents are reducible).

We prove fast convergence of the algorithm on a complete set of idempotents by examining how $\mathfrak{A}/\text{Rad}(\mathfrak{A})$ decomposes. By the Wedderburn-Malcev principal theorem (see Pierce (1982), Section 11.6), there exists a semisimple subalgebra \mathfrak{S} of \mathfrak{A} such that $\mathfrak{S} \cong \mathfrak{A}/\text{Rad}(\mathfrak{A})$ and $\mathfrak{A} = \mathfrak{S} \oplus \text{Rad}(\mathfrak{A})$ (a direct sum as additive groups). Moreover, if $\omega \in \mathfrak{A}$ is a primitive idempotent and $\omega = \bar{\omega} + \rho$ for $\bar{\omega} \in \mathfrak{S}$ and $\rho \in \text{Rad}(\mathfrak{A})$, then $\bar{\omega}$ is a primitive idempotent in \mathfrak{S} . Suppose that

$$\mathfrak{S} = \mathfrak{S}_1 \oplus \mathfrak{S}_2 \oplus \dots \oplus \mathfrak{S}_k$$

for simple algebras $\mathfrak{S}_1, \dots, \mathfrak{S}_k$, and that $\mathfrak{S}_i \cong \mathbb{E}_i^{r_i \times r_i}$, for an extension field \mathbb{E}_i of \mathbb{F} with $[\mathbb{E}_i : \mathbb{F}] = \mu_i$.

Within any simple component, by Lemma 3.2 with probability $1/22$ we choose a reducible element in \mathfrak{S}_i and obtain an idempotent $\omega_i \in \mathfrak{S}_i$ such that $\mu_i r_i^2 / 2 \leq \dim \mathfrak{S}_i \omega_i \leq 3\mu_i r_i^2 / 4$. Since $(3/4)^{3.5 \log r_i} \leq 1$, we will have constructed a complete set of primitive idempotents for \mathfrak{S}_i with $3.5 \log r_i$ such reducible elements. Hence, with the choice of $77 \log r_i$ elements from \mathfrak{S}_i we will obtain a complete set of primitive idempotents for \mathfrak{S}_i with probability at least $1/2$. Since there are at most m simple components, with $77 \log^2 m$ iterations, we obtain a set of primitive idempotents for all simple components with probability at least $1/2$, and with $77 \log^2(m) \cdot \log(1/\epsilon)$ iterations we expect to find a complete set of primitive idempotents for \mathfrak{A} with probability at least $1 - \epsilon$.

Each iteration of the algorithm uses $O(\mathcal{M}\mathcal{M}(m) \log m + \mathcal{M}(m) \log q + \mathcal{R}(\mathfrak{A}))$ operations in \mathbb{F} or $O(m^3 + m^2 \log q + \mathcal{R}(\mathfrak{A}))$ operations in \mathbb{F} using standard arithmetic, by Lemma 3.1. \square

3.3 Computing simple components of semisimple algebras over finite fields

In this section we employ the algorithms of Sections 3.1 and 3.2 to find the central idempotents and simple components of a semisimple algebra over a finite field. Unlike the algorithms presented in Section 2, these work over any finite field (even very small ones). We assume throughout this section that $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ is a semisimple algebra of dimension n .

$$\mathfrak{A} \cong \mathfrak{S}_1 \oplus \mathfrak{S}_2 \oplus \dots \oplus \mathfrak{S}_k \quad (3.4)$$

where $\mathfrak{S}_i \cong \mathbb{E}_i^{t_i \times t_i}$ for an extension field \mathbb{E}_i of \mathbb{F} .

Using the algorithm from Theorem 3.3 we can compute a transition matrix $U \in \mathbb{F}^{m \times m}$, $d_1, \dots, d_s \in \mathbb{Z}_{>0}$ such that $m = d_1 + \dots + d_s$ and

$$\hat{\omega}_i = \begin{pmatrix} D_{i1} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & D_{is} \end{pmatrix}, \quad \omega_i = U \hat{\omega}_i U^{-1} \in \mathfrak{A}, \quad (3.5)$$

where $D_{ij} \in \mathbb{F}^{d_i \times d_i}$ is the identity matrix if $i = j$ and the zero matrix if $i \neq j$, so that $\hat{\omega}_i \in \mathbb{F}^{m \times m}$ for all $i, \omega_1, \dots, \omega_s$ are primitive, pairwise orthogonal idempotents in \mathfrak{A} , and $\omega_1 + \dots + \omega_s = 1 \in \mathfrak{A}$.

Since \mathfrak{A} is semisimple, $s = t_1 + \dots + t_l$ and each of the ω_i 's correspond to a matrix in exactly one of $\mathfrak{S}_1, \dots, \mathfrak{S}_k$ consisting of a single "1" in some diagonal element and zeros everywhere else. It will be sufficient to group the ω_i 's together according to which simple component they belong to, and produce a new transition matrix which reflects this re-ordering.

Lemma 3.4 *Suppose \mathfrak{A} decomposes as in (3.4) and suppose $\omega_1, \dots, \omega_s \in \mathfrak{A}$ are primitive, orthogonal idempotents with sum $1 \in \mathfrak{A}$. If ω_i and ω_j belong to different simple components, then for all $\alpha \in \mathfrak{A}$, $\omega_i \alpha \omega_j = 0$. If ω_i and ω_j belong to the same simple component \mathfrak{S}_t , then $\omega_i \alpha \omega_j \neq 0$ with probability $1 - 1/|\mathbb{E}_t|$.*

Now suppose U is a transition matrix as in (3.5) and α is a randomly chosen element of \mathfrak{A} . Then

$$U^{-1} \alpha U = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1l} \\ A_{21} & A_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ A_{l1} & \dots & \dots & A_{ll} \end{pmatrix} \quad (3.6)$$

where $A_{ij} \in \mathbb{F}^{d_i \times d_j}$ and $U^{-1} \omega_i \alpha \omega_j U \in \mathbb{F}^{m \times m}$ is the matrix which is 0 except for A_{ij} .

Theorem 3.5 *Let $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ be a semisimple algebra as in (3.4). Given integers d_1, \dots, d_s and transition matrix U to a complete set of primitive orthogonal idempotents as in (3.5), we can find a semisimple transition matrix $W \in \mathbb{F}^{m \times m}$ (see Definition 2.9) and a permutation/re-labeling $d_{11}, \dots, d_{1t_1}, \dots, d_{k1}, \dots, d_{kt_k}$ of d_1, \dots, d_s such that*

- (i) *a complete set of primitive, orthogonal idempotents $\tilde{\omega}_{ij}$ ($1 \leq i \leq k, 1 \leq j \leq t_i$) is formed by*

$$\tilde{\omega}_{ij} = \begin{pmatrix} D_{11} & & & & \\ & \ddots & & & \\ & & D_{1t_1} & & \\ & & & \ddots & \\ & & & & D_{k1} \\ & & & & & \ddots \\ & & & & & & D_{kt_k} \end{pmatrix} \in \mathbb{F}^{m \times m},$$

$$\bar{\omega}_{ij} = W \tilde{\omega}_{ij} W^{-1} \in \mathfrak{A}, \quad (3.7)$$

where $D_{st} \in \mathbb{F}^{d_{st} \times d_{st}}$ is the identity matrix if $i = s$ and $j = t$ and the zero matrix otherwise.

- (ii) *For $1 \leq i \leq k$, $\bar{\omega}_i = \sum_{1 \leq j \leq t_i} \bar{\omega}_{ij}$ is a central idempotent for \mathfrak{A} so that*

$$\mathfrak{A} = \bar{\omega}_1 \mathfrak{A} \bar{\omega}_1 \oplus \bar{\omega}_2 \mathfrak{A} \bar{\omega}_2 \oplus \dots \oplus \bar{\omega}_k \mathfrak{A} \bar{\omega}_k$$

(a direct sum as algebras) and $\bar{\omega}_i \mathfrak{A} \bar{\omega}_i \cong \mathfrak{S}_i$.

This computation can be performed by a Monte Carlo algorithm that returns a correct answer with probability at least $1 - \epsilon$, for a user specified parameter $\epsilon > 0$, using an expected number of $O(\mathcal{MM}(m) \cdot \log(1/\epsilon))$ operations in \mathbb{F} .

Proof. We simply choose random elements of $\alpha \in \mathfrak{A}$ and compute $U^{-1}\alpha U$, which has block form as in (3.6). After each random choice of an α , note which pairs of idempotents are linked by noting non-zero blocks in $U^{-1}\alpha U$: $A_{ij} \neq 0$ implies ω_i and ω_j are in the same simple component. The probability that two idempotents in the same component are not recognized as such is at most $1/|\mathbb{F}|^2 \leq 1/4$. Thus, after $\lceil \log_4(m) \rceil$ attempts we should have identified all such linkages with probability at least $1/2$. Iterating this $\lceil \log(1/\epsilon) \rceil$ times ensures that the probability of success is at least $1 - \epsilon$. Once we have determined which idempotents belong to which simple components, we can construct W from U by a simple permutation. \square

Combining this theorem with Theorem 3.3 we obtain the following corollary

Corollary 3.6 *Let $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ be a semisimple algebra over a finite field $\mathbb{F} \cong \mathbb{F}_q$ as in (3.4). We can find a semisimple transition matrix $W \in \mathbb{F}^{m \times m}$ and $d_{11}, \dots, d_{1t_1}, \dots, d_{k1}, \dots, d_{kt_k} \in \mathbb{Z}$ with sum m such that*

- (i) *a complete set of primitive, orthogonal idempotents $\bar{\omega}_{ij}$ ($1 \leq i \leq k, 1 \leq j \leq t_i$) is formed as in (3.7), and*
- (ii) *for $1 \leq i \leq k$, $\bar{\omega}_i = \sum_{1 \leq j \leq t_i} \bar{\omega}_{ij}$ is a central idempotent for \mathfrak{A} so that*

$$\mathfrak{A} = \bar{\omega}_1 \mathfrak{A} \bar{\omega}_1 \oplus \bar{\omega}_2 \mathfrak{A} \bar{\omega}_2 \oplus \dots \oplus \bar{\omega}_k \mathfrak{A} \bar{\omega}_k$$

(a direct sum as algebras) and $\bar{\omega}_i \mathfrak{A} \bar{\omega}_i \cong \mathfrak{S}_i$,

with a Monte Carlo algorithm that returns a correct answer with probability at least $1 - \epsilon$, for a user specified parameter $\epsilon > 0$, using an expected number of $O((\mathcal{MM}(m) \log m + \mathcal{M}(m) \log q + \mathcal{R}(\mathfrak{A})) \cdot \log^2(m) \cdot \log(1/\epsilon))$ operations in \mathbb{F} , or $O((m^3 + m^2 \log q + \mathcal{R}(\mathfrak{A})) \cdot \log^2(m) \cdot \log(1/\epsilon))$ operations in \mathbb{F} using standard matrix and polynomial arithmetic.

3.4 Las Vegas Decomposition of Semi-Simple Algebras over Finite Fields

Now let $\mathfrak{A} \subseteq \mathbb{F}^{m \times m}$ be an algebra over a finite field $\mathbb{F} \cong \mathbb{F}_q$ which we believe to be simple. Suppose we are given pairwise orthogonal idempotents $\omega_1, \dots, \omega_r \in \mathfrak{A}$, with $\omega_1 + \dots + \omega_r = 1 \in \mathfrak{A}$. We will suppose as well that the dimension of \mathfrak{A} over \mathbb{F} is known and that we have a means of choosing random elements from \mathfrak{A} . In this section, we describe an algorithm that either provides a proof that \mathfrak{A} is simple with primitive idempotents $\omega_1, \dots, \omega_r$ or reports “failure”.

When applied to each of the “simple components” obtained by the Monte Carlo algorithm of Section 3.3, this completes an asymptotically efficient Las Vegas algorithm for the decomposition of semisimple matrix algebras over finite fields.

Assume $\omega_i = \text{diag}(\Delta_{i1}, \dots, \Delta_{ir}) \in \mathbb{F}^{m \times m}$, where $\Delta_{ij} \in \mathbb{F}^{s \times s}$ is the identity matrix if $i = j$ and the zero matrix otherwise. In particular, $\text{rank } \omega_i = s$ for $1 \leq i \leq r$ unless either \mathfrak{A} is not simple or $\omega_1, \dots, \omega_r$ are not all primitive (so that we should report failure if the rank is smaller than s). Suppose then that $\text{rank } \omega_i = s$ for all i . Every $a \in \mathfrak{A}$ can be written as

$$a = \begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \cdots & a_{rr} \end{pmatrix} \in \mathfrak{A},$$

where $a_{ij} \in \mathbb{F}^{s \times s}$, and $\omega_i a \omega_j$ is zero except for the (i, j) block, which equals a_{ij} .

We first find a change of basis for \mathfrak{A} so that $\omega_1 \mathfrak{A} \omega_1$ is in a normal form. If \mathfrak{A} is simple with idempotents $\omega_1, \dots, \omega_r$ then $\omega_1 \mathfrak{A} \omega_1$ is a finite field of (unknown) dimension μ over \mathbb{F} , such that $\mu | s$. Choose a random element $c \in \mathfrak{A}$ and compute the Frobenius form of the leading $s \times s$ submatrix $c_{11} \in \mathbb{F}^{s \times s}$ (the nonzero part of $\omega_1 c \omega_1$): if \mathfrak{A} is simple then there exists an invertible $u \in \mathbb{F}^{s \times s}$ such that

$$\lambda = u^{-1} c_{11} u = \begin{pmatrix} C_f & & \\ & \ddots & \\ & & C_f \end{pmatrix} \in \mathbb{F}^{s \times s}$$

where $C_f \in \mathbb{F}^{\bar{\mu} \times \bar{\mu}}$ is the companion matrix of the minimal polynomial $f \in \mathbb{F}[x]$ of c_{11} , $\bar{\mu} = \text{deg } \mu$ and $\bar{\mu} | \mu$. With probability at least $1/2$ we have $\bar{\mu} = \mu$. If λ has two or more distinct companion matrices in its Frobenius form, or f is not irreducible, then report “failure”. In these cases $\omega_1 \mathfrak{A} \omega_1$ is not a field and hence ω_1 is not primitive or \mathfrak{A} is not simple.

It is convenient to find an element $a \in \mathfrak{A}$ such that $\omega_1 a \omega_i \neq 0$ and $\omega_i a \omega_1 \neq 0$ for $2 \leq i \leq r$. If \mathfrak{A} is simple with primitive idempotents $\omega_1, \dots, \omega_r$ then, for fixed i, j ($1 \leq i, j \leq r$) and randomly chosen $b \in \mathfrak{A}$, $\omega_i b \omega_j \neq 0$ with probability at least $1 - 1/|\mathbb{F}| \geq 1/2$. Thus with an expected number of $O(\log r)$ random choices of elements of such b we can construct $b_{1i}, b_{i1} \in \mathfrak{A}$ such that $\omega_1 b_{1i} \omega_i \neq 0$ and $\omega_i b_{i1} \omega_1 \neq 0$ for $2 \leq i \leq r$. If \mathfrak{A} is simple with orthogonal primitive idempotents $\omega_1, \dots, \omega_r$ then each b_{1i}, b_{i1} has rank s for $2 \leq i \leq r$. If this is not the case then the algorithm should report “failure”. Otherwise, since $\omega_i b \omega_j$ is zero except possibly for the (i, j) th block, we can add together appropriate non-zero blocks of these b_{1k} 's and b_{k1} 's to construct a . Let

$$U = \begin{pmatrix} u & & & \\ & a_{12}^{-1} u & & \\ & & \ddots & \\ & & & a_{1r}^{-1} u \end{pmatrix} \in \mathbb{F}^{m \times m}$$

and $\mathfrak{A}' = U^{-1} \mathfrak{A} U$. Note that since $\omega_1, \dots, \omega_r$ commute with U , these are also idempotents in \mathfrak{A}' and are primitive and orthogonal if and only if they are primitive and orthogonal in \mathfrak{A} .

Consider the elements $a' = U^{-1} a U$ and $\omega_{1k} = \omega_1 a' \omega_k$ of \mathfrak{A}' for $2 \leq k \leq r$. By construction ω_{1k} is zero except for the $(1, k)$ block, which equals $u^{-1} a_{1k} a_{1k}^{-1} u = 1_s$. Also, $\omega_1 U^{-1} c U \omega_1$ generates a finite field of degree $\bar{\mu}$ over \mathbb{F} . Let $\Lambda = \omega_1 U^{-1} c U \omega_1 \in \mathfrak{A}'$ and recall that, with probability at least one half, $\bar{\mu} = \mu$. If this is the case (and, again, \mathfrak{A} is simple with primitive orthogonal idempotents $\omega_1, \dots, \omega_r$) then $\omega_1 \mathfrak{A}' \omega_1 = \omega_1 \mathbb{F}[\Lambda] \omega_1$ and, since $\omega_k a' \omega_1$ is nonzero, $\omega_k \mathfrak{A}' \omega_1 = (\omega_k a' \omega_1) (\omega_1 \mathbb{F}[\Lambda] \omega_1)$.

If \mathfrak{A} is a simple with primitive idempotents $\omega_1, \dots, \omega_r$ then for $2 \leq k \leq r$ there exists an $x \in \mathfrak{A}$ such that $\omega_1 a \omega_k \cdot \omega_k x \omega_1 = \omega_1$. Equivalently, there exists a $y' \in \mathfrak{A}'$ such that $\omega_{1k} \cdot \omega_k y' \omega_1 = \omega_1$, i.e., such that the $(k, 1)$ block of y'_{k1} of y' equals 1_s . We must check that such a $y' \in \mathfrak{A}'$ exists for each k ($2 \leq k \leq r$). Suppose $a'_{k1} \in \mathbb{F}^{s \times s}$ is the $(k, 1)$ block of a' ; if the algorithm has not already failed then this matrix is invertible and we can efficiently check whether $(a'_{k1})^{-1} \in \mathbb{F}[\Lambda]$. If it is, then we can safely conclude that the desired element y' belongs to \mathfrak{A}' , and we can conclude that the element ω_{k1} whose $(k, 1)$ block is 1_s (and which is zero elsewhere) belongs

to \mathfrak{A}' ; if it is not, then the algorithm should report failure. If $\bar{\mu} = \mu$ then the probability of “failure” at this step is less than one half.

Finally, assuming that the algorithm has not failed, we can construct a basis for a simple subalgebra of \mathfrak{A}' as follows. For $2 \leq i, j \leq r$ let $\omega_{ij} = \omega_{i1} \cdot \omega_{1j} \in \mathfrak{A}'$, the matrix which is zero except for the (i, j) block which is equal to 1_s . It is easily shown that the set $\{\omega_{i1} \Lambda^k \omega_{1j} : 1 \leq i, j \leq r, 0 \leq k \leq \bar{\mu}\}$ is a basis for a simple subalgebra \mathfrak{S} of $E^{r \times r}$, where $E = F[\lambda]$ is an extension field of degree $\bar{\mu}$ over F . If $\dim \mathfrak{S} = \dim \mathfrak{A}$ then clearly $\mathfrak{S} \cong \mathfrak{A}$ and \mathfrak{A} is a simple algebra; otherwise, once again, failure should be reported. If reporting “failure” is equated with reporting that “either \mathfrak{A} is not simple or the ω_i 's are not primitive in \mathfrak{A} ” then this establishes the following.

Theorem 3.7 *Let \mathfrak{A} be an algebra and $\omega_1, \dots, \omega_r \in \mathfrak{A}$ be pairwise orthogonal idempotents with $\sum_{1 \leq i \leq r} \omega_i = 1$. The algorithm described above either reports that \mathfrak{A} is simple with primitive idempotents $\omega_1, \dots, \omega_r$ or reports that “either \mathfrak{A} is not simple or the ω_i 's are not primitive in \mathfrak{A} ”. In either case the algorithm requires an expected number of $O(\min(m^3, \mathcal{M}\mathcal{M}(m) \log m) + \mathcal{R}(\mathfrak{A}) \log r)$ operations in F . It returns the correct answer with probability bounded away from zero on all inputs, and it never reports that \mathfrak{A} is simple with primitive idempotents $\omega_1, \dots, \omega_r$ if this is not the case.*

By applying the above algorithm to each simple component in a decomposition of a presumed semisimple algebra, we obtain an efficient proof that the decomposition is indeed correct. Combining this with the algorithm summarized in Theorem 3.8 we obtain the following theorem.

Theorem 3.8 *Let $\mathfrak{A} \subseteq F^{m \times m}$ be a semisimple algebra over a finite field $F \cong \mathbb{F}_q$ as in (3.4). We can find a semisimple transition matrix $W \in F^{m \times m}$ and $d_{11}, \dots, d_{1t_1}, \dots, d_{k1}, \dots, d_{kt_k} \in \mathbb{Z}$ with sum m such that*

- (i) *a complete set of primitive, orthogonal idempotents $\bar{\omega}_{ij}$ ($1 \leq i \leq k, 1 \leq j \leq t_i$) is formed as in (3.7), and,*
- (ii) *for $1 \leq i \leq k, \bar{\omega}_i = \sum_{1 \leq j \leq t_i} \bar{\omega}_{ij}$ is a central idempotent for \mathfrak{A} so that*

$$\mathfrak{A} = \bar{\omega}_1 \mathfrak{A} \bar{\omega}_1 \oplus \bar{\omega}_2 \mathfrak{A} \bar{\omega}_2 \oplus \dots \oplus \bar{\omega}_k \mathfrak{A} \bar{\omega}_k$$

(a direct sum as algebras) and $\bar{\omega}_i \mathfrak{A} \bar{\omega}_i \cong \mathfrak{S}_i$.

using a Las Vegas algorithm that requires an expected number of $O((\mathcal{M}\mathcal{M}(m) \log m + \mathcal{M}(m) \log q + \mathcal{R}(\mathfrak{A})) \cdot \log^2(m))$ operations in F , or $O((m^3 + m^2 \log q + \mathcal{R}(\mathfrak{A})) \cdot \log^2(m))$ operations in F using standard matrix and polynomial arithmetic.

References

- E. R. Berlekamp. Factoring polynomials over large finite fields. *Math. Comp.* **24**, pp. 713–735, 1970.
- D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. *J. Symb. Comp.* **9**, pp. 251–280, 1990.
- W. Eberly. Decompositions of algebras over finite fields and number fields. *Computational Complexity* **1**, pp. 179–206, 1991.
- K. Friedl and L. Rónyai. Polynomial time solutions of some problems in computational algebra. In *7th Ann. Symp. Theory of Comp.*, pp. 153–162, Providence, RI, USA, 1985.

P. Gianni, V. Miller, and B. Trager. Decomposition of algebras. In *Proc. ISSAC'88*, vol. 358 of *Lecture Notes in Computer Science*, Rome, Italy, 1988. Springer-Verlag.

M. Giesbrecht. Nearly optimal algorithms for canonical matrix forms. *SIAM J. Comp.* **24**, pp. 948–969, 1995.

D. F. Holt and S. Rees. Testing modules for irreducibility. *J. Australian Mathematical Society* **57**, pp. 1–16, 1994.

N. Jacobson. *Structure of Rings*, vol. 37. American Math. Soc. Colloquium Publ. (Providence, USA), 1956.

S. Landau. Factoring polynomials over algebraic number fields. *SIAM J. Comput.* **14**, pp. 184–195, 1985.

G. Michler. Some problems in computational representation theory. *J. Symbolic Computation* **9**, pp. 571–582, 1990.

E. Noether. Hyperkomplexe Grössen und Darstellungstheorie. *Math. Zeit.* **30**, pp. 641–692, 1929.

R. A. Parker. The computer calculation of modular characters (the meat-axe). In *Computational Group Theory: Proceedings of the London Mathematical Society Symposium on Computational Group Theory*, pp. 267–274, London, 1984. Academic Press.

B. O. Peirce. Linear associative algebra. *American Journal of Mathematics* **4**, pp. 97–229, 1881.

R. Pierce. *Associative Algebras*. Springer-Verlag (Heidelberg), 1982.

L. Rónyai. Simple algebras are difficult. In *Proc. 19th ACM Symp. on Theory of Comp.*, pp. 398–408, New York, 1987.

L. Rónyai. Computing the structure of finite algebras. *J. Symb. Comp.* **9**, pp. 355–373, 1990.

L. Rónyai. Algorithmic properties of maximal orders in simple algebras over \mathbb{Q} . *Computational Complexity* **2**, pp. 225–243, 1992.

G. J. A. Schneider. Computing with endomorphism rings of modular representations. *J. Symbolic Computation* **9**, pp. 607–636, 1990.

A. Schönhage. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica* **7**, pp. 395–398, 1977.

A. Schönhage and V. Strassen. Schnelle Multiplikation großer Zahlen. *Computing* **7**, pp. 281–292, 1971.

J. H. M. Wedderburn. On hypercomplex numbers. *Proc. London Math. Soc.* **6**(2), pp. 77–118, 1907.

WAYNE EBERLY is an Associate Professor in the Computer Science Department at the University of Calgary. Prof. Eberly is the author of several papers in the areas of parallel algorithms and computational algebra. For more information, see <http://www.cpsc.ucalgary.ca/~eberly>.

MARK GIESBRECHT is an Assistant Professor in the Department of Computer Science at the University of Manitoba. Prof. Giesbrecht obtained his Ph.D. in Computer Science from the University of Toronto. He is the author of a number of papers on computer algebra, algebraic complexity and compiler optimization and automatic parallelization. More information can be found on his WWW homepage: <http://www.cs.umanitoba.ca/~mwg>.