Efficient Decomposition of Associative Algebras over Finite Fields*

W. Eberly[†]
Department of Computer Science
University of Calgary
Calgary, Alberta, Canada T2N 1N4
Email: eberly@cpsc.ucalgary.ca
http://www.cpsc.ucalgary.ca/~eberly

M. Giesbrecht[†]
Department of Computer Science
University of Western Ontario
London, Ontario, Canada N6A 5B7
Email: mwg@csd.uwo.ca
http://www.csd.uwo.ca/~mwg

July 2, 1999

Abstract

We present new, efficient algorithms for some fundamental computations with finite dimensional (but not necessarily commutative) associative algebras over finite fields. For a semisimple algebra $\mathfrak{A}$ we show how to compute a complete Wedderburn decomposition of $\mathfrak{A}$ as a direct sum of simple algebras, an isomorphism between each simple component and a full matrix algebra, and a basis for the centre of $\mathfrak{A}$. If $\mathfrak{A}$ is given by a generating set of matrices in $\mathsf{F}^{m\times m}$ then our algorithm requires about $O(m^3)$ operations in F, in addition to the cost of factoring a polynomial in $\mathsf{F}[x]$ 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 in this same time.

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* 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 finite dimensional associative algebras over finite fields. Henceforth we will use the term *algebra* to refer to a finite dimensional associative algebra over a finite field. Algebras over an infinite field will be considered in a subsequent paper.

[*] An extended abstract of some of this work appears in "Proceedings, International Symposium on Symbolic and Algebraic Computation," Zurich, 1996. ISSAC'96, pp. 170–178.

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

To appear: Journal of Symbolic Computation.

Recall that the *(Jacobson) radical* Rad($\mathfrak{A}$) of an algebra $\mathfrak{A}$ over a finite field F is the intersection of all maximal left ideals in $\mathfrak{A}$. $\mathfrak{A}$ is said to be *semisimple* if 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 $\mathfrak{A}$,

$$\mathfrak{A} = \mathfrak{S}_1 \oplus \mathfrak{S}_2 \oplus \cdots \oplus \mathfrak{S}_k \tag{1.1}$$

for simple algebras $\mathfrak{S}_1, \ldots, \mathfrak{S}_k \subseteq \mathfrak{A}$, and each $\mathfrak{S}_i \cong \mathsf{E}_i^{t_i \times t_i}$ where E_i is a (finite) extension field of F. We give a fast probabilistic algorithm to compute a representation of the complete Wedderburn decomposition of $\mathfrak{A}$ as a direct sum of simple algebras, an explicit isomorphism between each $\mathfrak{S}_i$ and $\mathsf{E}_i^{t_i \times t_i}$, and a basis for the centre of $\mathfrak{A}$.

We suppose throughout that $\mathfrak{A}$ is presented as a subalgebra of dimension n of the full matrix algebra $\mathsf{F}^{m \times m}$. F is generally the finite field with q elements, $\mathbb{F}_q$. The algebra $\mathfrak{A}$ is described computationally by a generating set $\mathfrak{L} \subseteq \mathfrak{A}$ 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.

We begin in Section 2 by showing how, for any (not necessarily semisimple) algebra $\mathfrak{A}$, to compute a complete set of orthogonal primitive idempotents in $\mathfrak{A}$. 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 Subsection 2.1 we introduce *decomposable elements* which allow the generation of non-trivial idempotents. These elements are similar to the "Fitting elements" employed for a similar purpose by Schneider (1990), but are much easier to find. In Subsection 2.2 we show how to use decomposable elements to compute a complete set of orthogonal primitive idempotents, that is, a set of pairwise orthogonal primitive idempotents whose sum is the identity. We represent these using a similarity transformation — a non-singular matrix X — such that in the isomorphic algebra $X^{-1}\mathfrak{A}X$ these idempotents are diagonal matrices with zeroes and ones on the diagonal. The use of such a similarity transformation allows us to apply our techniques in an iterative way to decompose components of the original algebra without a significant increase in cost.

This first 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 $\mathsf{F} \cong \mathbb{F}_q$, for an algebra presented as above. Without a check for correctness (see below), this is a Monte Carlo algorithm: for a user specified ϵ the algorithm returns the correct answer with probability at least $1 - \epsilon$. In particular, a set of orthogonal idempotents for $\mathfrak{A}$ is computed without error, there is a (controllably) small probability that they are not primitive.

In Section 3 we consider the case of a semisimple algebra $\mathfrak{A}$. In Subsection 3.1 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 Subsection 3.2 that there is an efficient test for the correctness of the output of the Monte Carlo algorithms for semisimple algebras. This test 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 deciding whether an algebra over a number field possesses nontrivial idempotents has 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 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 $\omega_1, \ldots, \omega_s \in \mathrm{End}_{\mathfrak{A}}(M)$ such that $\sum_{1 \le i \le s} \omega_i = 1$, which Michler (1990) also proposes as an open problem. We give a very efficient algorithm for the computation of a set of orthogonal primitive idempotents of an algebra in Section 2. This problem was first addressed in Schneider (1990) for small finite fields by the selection of "Fitting elements" in $\mathrm{End}_{\mathfrak{A}}(M)$ which allow its decomposition. In Subsection 2.1 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 $O(\mathcal{MM}(m))$ operations in a field F are sufficient to multiply two matrices in $\mathsf{F}^{m \times m}$. Using the standard algorithm requires $\mathcal{MM}(m) = m^3$ while the currently best known algorithm of Coppersmith & Winograd (1990) allows $\mathcal{MM}(m) = m^{2.376}$. We assume that $O(\mathcal{M}(m))$ operations in F are sufficient to multiply two polynomials in $\mathsf{F}[x]$ 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 $\mathcal{MM}(m) = m^\theta$ for some $\theta > 2$. Finally, we assume that a polynomial of degree m in $\mathsf{F}[x]$ can be factored using $O(\mathcal{F}(m))$ operations in F. Since F is a finite field with q elements, we can use Berlekamp's (1970) algorithm with $\mathcal{F}(m) = \mathcal{MM}(m) + m^2 \log q$ operations in F. Throughout the paper, $\log n$ is defined as the natural logarithm of $n \in \mathbb{R}$.

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 uniformly from $\mathfrak{A}$. As stated above this is assumed to be possible with $O(\mathcal{R}(\mathfrak{A}))$ operations in F. One rigorous way of doing this is to form a basis $\gamma_1, \ldots, \gamma_n \in \mathfrak{A}$ for $\mathfrak{A}$. Our generator of random elements of $\mathfrak{A}$ returns linear combinations $\sum_{1 \le i \le n} a_i \gamma_i$ for uniformly and independently selected elements $a_i \in \mathsf{F}$.

In practice, almost any reasonable scheme for generating random elements of $\mathfrak{A}$ seems to work. However, the only (fairly) efficient scheme we know of for generating such elements with provable uniformity requires a basis of n matrices in $\mathsf{F}^{m \times m}$ 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 Finding Primitive Orthogonal Idempotents

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

$$\mathfrak{A} = \mathfrak{A}\omega_1 \oplus \mathfrak{A}\omega_2 \oplus \cdots \oplus \mathfrak{A}\omega_l, \tag{2.1}$$

a direct sum of left ideals, where $l \ge 2$ is the number of distinct monic irreducible factors of the minimal polynomial of α over F. 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 F is large — Schneider shows they have density about $1/|\mathsf{F}|$ — decomposable elements have a high density. In Subsection 2.1 we present a new algorithm which finds decomposable elements efficiently, and constructs a corresponding set of pairwise orthogonal idempotents.

This algorithm, with high probability, produces *balanced* decomposable elements, such that the decomposition (2.1) is into ideals of about the same size. In Subsection 2.2 it is shown how to iterate this algorithm to find a complete set of primitive pairwise orthogonal idempotents efficiently. Ultimately, we achieve a Monte Carlo probabilistic algorithm which requires $O((\mathcal{MM}(m)\log m + \mathcal{M}(m)\log q + \mathcal{R}(\mathfrak{A}))\cdot\log(m)\cdot\log(1/\epsilon))$ operations in F, or $O((m^3+m^2\log q+\mathcal{R}(\mathfrak{A}))\cdot\log(m)\cdot\log(1/\epsilon))$ operations in $\mathsf{F}\cong\mathbb{F}_q$ using standard arithmetic. As usual, $\epsilon>0$ is a user-defined tolerance and, for any input, on any invocation of the algorithm the output will be correct with probability at least $1-\epsilon$.

Unfortunately we know of no way to guarantee these idempotents correct — and hence obtain a Las Vegas algorithm — with this same cost. This would be equivalent to showing that each of the algebras $\mathfrak{B}_i = \omega_i\mathfrak{A}\omega_i$ is a local algebra, i.e., $\mathfrak{B}_i/\operatorname{Rad}(\mathfrak{B}_i)$ is a finite field for $1\le i\le l$. The algorithm of Rónyai (1990) will perform this task in polynomial-time, but it appears to require about $O(n^2m^4\log^3 q)$ bit operations (Rónyai's algorithm requires computation in $\mathbb{Z}$ rather than in $\mathsf{F}\cong\mathbb{F}_q$, hence bit operations rather than field operations are an appropriate measure of cost). See also Cohen *et al.* (1997).

2.1 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 $\mathsf{F}^{m\times m}$ of dimension n (not necessarily semisimple).

For any algebra $\mathfrak{A}$, a *decomposable element* $\alpha\in\mathfrak{A}$ is an element whose minimal polynomial $f\in\mathsf{F}[x]$ has a factorization $f=f_1\ldots f_l$ into two or more monic, pairwise relatively prime $f_i\in\mathsf{F}[x]\setminus\mathsf{F}$. In this case we can construct idempotents $\omega_1,\ldots,\omega_l\in\mathfrak{A}$ (which are not generally central) as follows. For $1\le i\le l$, use the Chinese remainder theorem to construct $h_i\equiv 1 \bmod f_i$, $h_i\equiv 0\bmod f_j$ for $j\ne i$, 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 $i\ne j$ (i.e., they are pairwise orthogonal) and that $\omega_1+\cdots+\omega_l=1\in\mathfrak{A}$. We call ω_i the idempotent that *corresponds to* f_i.

Lemma 2.1. *Given a decomposable $\alpha\in\mathfrak{A}$, we can compute*

(i) the minimal polynomial $f\in\mathsf{F}[x]$ of α and the factorization $f=f_1\ldots f_l$ into powers of distinct irreducible polynomials in $\mathsf{F}[x]$,

(ii) polynomials $h_1,\ldots,h_l\in\mathsf{F}[x]$ such that $\omega_i=h_i(\alpha)$, $1\le i\le l$, are pairwise orthogonal idempotents with $\sum_{1\le i\le l}\omega_i=1\in\mathfrak{A}$,

(iii) $d_1,\ldots,d_l\in\mathbb{N}$ such that $m=d_1+\cdots+d_l$ and such that ω_i has rank d_i as a matrix in $\mathsf{F}^{m\times m}$,

(iv) a matrix $U\in\mathsf{F}^{m\times m}$ such that

$$\widehat{\omega}_i = U^{-1}\omega_i U = \begin{bmatrix}\Delta_{i1} & & & & \\ & \ddots & & & \\ & & \Delta_{ii} & & \\ & & & \ddots & \\ & & & & \Delta_{il}\end{bmatrix}\in\mathsf{F}^{m\times m}, \tag{2.2}$$

where $\Delta_{ij}\in\mathsf{F}^{d_j\times d_j}$ is the identity matrix when $j=i$ and the zero matrix when $j\ne i$, *with a Las Vegas algorithm using an expected number of $O(\mathcal{MM}(m)\log m + \mathcal{M}(m)\log q)$ operations in F, or $O(m^3 + m^2\log q)$ operations in $\mathsf{F} \cong \mathbb{F}_q$ using standard matrix and polynomial arithmetic.*

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

$$U^{-1}\alpha U = J = \begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_l \end{bmatrix} \in \mathsf{F}^{m\times m}.$$

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

$$J_i = \begin{bmatrix} C_{g_i^{c_{i1}}} & & \\ & \ddots & \\ & & C_{g_i^{c_{ik_i}}} \end{bmatrix} \in \mathsf{F}^{d_i\times d_i},$$

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

For $1 \leq i \leq l$, let $h_i \in \mathsf{F}[x]$ with $h_i \equiv 1 \bmod f_i$, $h_i \equiv 0 \bmod f_j$ 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 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)*. □

Since we wish to find a complete set of pairwise orthogonal primitive idempotents rather than a single one, 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 F is isomorphic to a full matrix ring $\mathsf{E}^{t\times t}$ over an extension field E of F for some positive integer t.

Theorem 2.2. *Let $\mathfrak{A} \subseteq \mathsf{F}^{m\times m}$ be a simple algebra of dimension n over $\mathsf{F} \cong \mathbb{F}_q$. The number of $\alpha \in \mathfrak{A}$ with $f = \min_{\mathsf{F}}(\alpha)$ such that there exists a factorization $f = f_1 f_2$ for relatively prime polynomials $f_1, f_2 \in \mathsf{F}[x]$ with corresponding idempotents ω and $1-\omega$, and such that $n/2 < \dim_{\mathsf{F}}(\mathfrak{A}\omega) \leq 3n/4$, is at least $q^n/22$.*

The proof of this theorem will require a number of lemmas. We assume again that $\mathfrak{A} \cong \mathsf{E}^{t\times t}$, where $\mathsf{E} \cong \mathbb{F}_{q^e}$, so $[\mathsf{E} : \mathsf{F}] = e$ and the dimension of $\mathfrak{A}$ over F is $n = et^2$. The following lemma establishes that most matrices are similar to a companion matrix. This allows us to relate the question of balance in decomposable elements to that of factorization patterns for polynomials in $\mathsf{E}[x]$.

Lemma 2.3. *Let $t \geq 2$ and $B \in \mathsf{E}^{t\times t}$ be such that the minimal polynomial of B over E has (maximal) degree t. Then B is similar to at least $q^{et^2-et} \cdot (1-q^{-e})^{q^e/(q^e-1)}$ distinct matrices in $\mathsf{E}^{t\times t}$, exactly one of which is a companion matrix.*

Proof. Matrices in $\mathsf{E}^{t\times t}$ whose minimal polynomials in $\mathsf{E}[x]$ have degree t are exactly those similar to the companion matrices of their minimal polynomials. Since the minimal polynomial is the only invariant factor if it has degree t, it completely characterizes the similarity class. Since no two distinct companion matrices are similar, we know that B is similar to exactly one companion matrix.

It is well known (see, for example, Hodges 1958) that the number of matrices similar to a given matrix $B \in \mathsf{E}^{t\times t}$ is quotient of the number $\mathcal{L}(\mathsf{E}, t)$ of nonsingular matrices in $\mathsf{E}^{t\times t}$ by the number of nonsingular matrices in $\mathsf{E}^{t\times t}$ which commute with B. In the case of a matrix B whose minimal polynomial has degree t, it is shown by Gantmacher (1990), Section 8.2, that the only matrices commuting with B are in $\mathsf{E}[B]$, whence there are $(q^e)^t$ of them. From (Dickson 1901, Part II, Chapter 1), we have

$$\mathcal{L}(\mathsf{E}, t) = \prod_{0\leq i<t} (q^{et} - q^{ei}) = q^{et^2} \prod_{1\leq i\leq t} (1 - 1/q^{ei}).$$

We bound $\prod_{1\leq i\leq t}(1-q^{-ei})$ from below by considering its natural logarithm

$$\log \prod_{1\leq i\leq t} (1-q^{-ei}) = -\sum_{1\leq i\leq t}\sum_{j\geq 1} \frac{1}{jq^{eij}} = -\sum_{j\geq 1} \frac{1}{j}\cdot\frac{1}{q^{ej}-1}\left(1-\frac{1}{q^{ejt}}\right)$$
$$\geq -\sum_{j\geq 1} \frac{1}{jq^{ej}}\frac{q^{ej}}{q^{ej}-1} \geq \log\left(1-\frac{1}{q^e}\right)^{q^e/(q^e-1)}.$$

Thus $\mathcal{L}(\mathsf{E}, t) \geq q^{et^2}(1-q^{-e})^{q^e/(q^e-1)}$ and the number of non-singular matrices commuting with B is at most q^{et}, so their quotient is at least as large as the given bound. □

The next lemma demonstrates that a fairly large portion of polynomials in $\mathsf{E}[x]$ of degree $t \geq 3$ have a "medium-sized" irreducible factor. Let $N_{q^e}(d)$ be the number of monic, irreducible polynomials of degree d in $\mathbb{F}_{q^e}[x]$. It is well known (see Lidl & Niederreiter (1983), exercises 3.26 and 3.27) that

$$q^{ed}/d - q^e/(q^e-1)\cdot q^{ed/2}/d \leq N_{q^e}(d) \leq q^{ed}/d. \tag{2.3}$$

Lemma 2.4. *The number of monic polynomials $g \in \mathsf{E}[x]$ of degree $t \geq 3$ such that $g = g_1g_2$ where g_1 is monic and irreducible in $\mathsf{E}[x]$ and $t/2 < \deg g_1 \leq 3t/4$ is greater than $q^{et}/4$, except when $t = 6$ when the number is greater than $(q^{6e} - q^{4e})/4$.*

Proof. Since there is at most one such factor g_1 in any such polynomial g, the number is

$$\begin{aligned}
\sum_{t/2<d\leq 3t/4} q^{et-ed} N_{q^e}(d) &\geq q^{et}\cdot \sum_{t/2<d\leq 3t/4} \left(\frac{1}{d} - \frac{q^e}{q^e-1}\cdot\frac{1}{d\cdot q^{ed/2}}\right) \\
&\geq q^{et}\cdot \left(\left(\sum_{t/2<d\leq 3t/4}\frac{1}{d}\right) - \frac{q^e}{q^e-1}\cdot\frac{2}{t}\cdot \sum_{t/2<d\leq 3t/4}\left(\frac{1}{q^{ed/2}}\right)\right) \\
&\geq q^{et}\cdot \left(\log 3 - \log 2 - \frac{2}{3t} - \frac{4}{3t}\left(\frac{3t}{4} - \left\lfloor\frac{3t}{4}\right\rfloor - \frac{t}{2} + \left\lfloor\frac{t}{2}\right\rfloor\right)\right. \\
&\qquad \left. - \frac{2}{t}\cdot\frac{q^e}{q^e-1}\cdot\frac{q^{e/2}}{q^{e/2}-1}\cdot\frac{1}{q^{et/4+e/4}}\right) \\
&\geq q^{et}\cdot\left(\log 3 - \log 2 - \frac{4}{3t} - \frac{2}{t}\cdot\frac{q^e}{q^e-1}\cdot\frac{q^{e/2}}{q^{e/2}-1}\cdot\frac{1}{q^{et/4+e/4}}\right) \\
&\geq q^{et}/4,
\end{aligned}$$

where $t \geq 3$ and $t \neq 6$, using Euler's partial summation formula (see Apostol (1976), Theorem 3.1) and (2.3). When $t = 6$ this number is calculated directly. □

The above lemma concerns polynomials $g_1 \in \mathsf{E}[x]$ whose degree is strictly greater than $t/2$. This ensures that g_1 is not a factor with multiplicity greater than one in g. We will ultimately perform our computation in $\mathsf{F}[x]$ (rather than $\mathsf{E}[x]$) with the polynomial $f \in \mathsf{F}[x]$ of least degree such that $g \mid f$, and our conditions ensure that there is a factorization of $f = f_1 f_2$ into relatively prime polynomials $f_1, f_2 \in \mathsf{F}[x]$ such that $g_1 \mid f_1$ and $g_2 \mid f_2$ (for $g_2 = g/g_1$, as in the lemma).

For $t = 2$, Lemma 2.4 does not apply, and we instead use the following.

Lemma 2.5. *The number of monic quadratic polynomials $g \in \mathsf{E}[x]$, such that the polynomial $f \in \mathsf{F}[x] \setminus \{0\}$ of least degree that is divisible by g is a power of an irreducible in $\mathsf{F}[x]$, is less than $3q^{2e}/4$.*

Proof. In this case, either g is irreducible or it has two linear factors in $\mathsf{E}[x]$. Suppose g has linear factors, and that each of these factors divides a power f of an irreducible polynomial $h \in \mathsf{F}[x]$. Since E and F are finite fields, it must be the case that h factors completely in $\mathsf{E}[x]$. Thus the degree s of h divides $e = [\mathsf{E} : \mathsf{F}]$. Moreover, for each irreducible polynomial h of degree s, there are $\binom{s+1}{2}$ ways to choose two (not necessarily distinct) factors of h in $\mathsf{E}[x]$ whose product is $g \in \mathsf{E}[x]$, such that the minimal degree polynomial $f \in \mathsf{F}[x]$ that is divisible by g is a power of an irreducible in $\mathsf{F}[x]$.

Thus, the number of quadratic polynomials $g \in \mathsf{E}[x]$ such that the minimal degree polynomial $f \in \mathsf{F}[x]$ with $g \mid f$ is a power of an irreducible in $\mathsf{F}[x]$ is

$$\begin{aligned} N_{q^e}(2) + \sum_{s \mid e} N_q(s) \cdot \frac{s(s+1)}{2} &\le \frac{q^{2e}}{2} + \sum_{s \mid e} \frac{q^s(s+1)}{2} \\ &\le \frac{q^{2e}}{2} + \frac{q^e(e+1)}{2} + \sum_{\substack{s \mid e \\ 1 \le s \le e/2}} \frac{q^s(s+1)}{2} \le \frac{q^{2e}}{2} + \frac{q^e(e+1)}{2} + \sum_{1 \le s \le e/2} \frac{q^s(s+1)}{2} \\ &\le \frac{q^{2e}}{2} + \frac{q^e(e+1)}{2} + \frac{q}{(q-1)^2} \cdot \frac{q^{e/2}((e/2+1)q - 2 - e/2) - q + 2}{2} \le \frac{3q^{2e}}{4}, \end{aligned}$$

using (2.3), except when $q = 2$ and $e \le 3$, and when $2 \le q \le 5$ and $e = 1$. It is easily checked that the inequality stated in the lemma is also correct in these cases. □

Now we combine Lemmas 2.3, 2.4 and 2.5 to find the proportion of decomposable elements $\alpha \in \mathfrak{A} \cong \mathsf{E}^{t \times t}$ which yield an idempotent $\omega \in \mathfrak{A}$ such that $n/2 \le \dim_{\mathsf{F}}(\mathfrak{A}\omega) \le 3n/4$.

Proof of Theorem 2.2. When $t > 2$, the number of such elements α is at least the number of matrices in $\mathsf{E}^{t \times t}$ that are similar to a companion matrix whose minimal polynomial $g \in \mathsf{E}[x]$ has an irreducible factor $g_1 \in \mathsf{E}[x]$ such that $t/2 < \deg g_1 \le 3t/4$. When $t \ne 6$ this number is greater than

$$\frac{q^{et}}{4} \cdot q^{et^2 - et} \left(1 - \frac{1}{q^e}\right)^{q^e/(q^e-1)} \ge q^{et^2}/16,$$

by Lemmas 2.3 and 2.4. When $t = 6$ this number is

$$\frac{q^{6e} - q^{4e}}{4} \cdot q^{30e} \left(1 - \frac{1}{q^e}\right)^{q^e/(q^e-1)} \ge q^{36e}/22.$$

When $t = 2$, this is at least the number of matrices $a \in \mathsf{E}^{t \times t}$ that are similar to companion matrices of quadratic polynomials $g \in \mathsf{E}[x]$, such that the minimal degree polynomial $f \in \mathsf{F}[x]$ that is divisible by g is not a power of an irreducible. By Lemmas 2.3 and 2.5, this number is at least

$$\frac{q^{2e}}{4} \cdot q^{2e} \left(1 - \frac{1}{q^e}\right)^{q^e/(q^e-1)} \ge q^{4e}/16.$$

□

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

2.2 Finding Primitive Orthogonal Idempotents

In this section we describe an algorithm to compute a complete set of primitive, pairwise orthogonal idempotents $\omega_1, \ldots, \omega_s \in \mathfrak{A}$ such that $\sum_{1 \le i \le s} \omega_i = 1 \in \mathfrak{A}$. The idea is to iterate the algorithm described in Lemma 2.1 on randomly chosen elements $\alpha \in \mathfrak{A}$.

Suppose we have computed pairwise orthogonal idempotents $\omega_1, \ldots, \omega_l \in \mathfrak{A}$ and a transition matrix $U \in \mathsf{F}^{m \times m}$ as in (2.2), 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

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

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

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

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 $U \in \mathsf{F}^{m \times m}$ and pairwise orthogonal idempotents $\omega_1, \ldots, \omega_l \in \mathfrak{A}$ as in Lemma 2.1. Let $\widehat{\mathfrak{A}} = U^{-1}\mathfrak{A}U$ and $\widehat{\omega}_i = U^{-1}\omega_i U \in \widehat{\mathfrak{A}}$ for $1 \le i \le l$. Clearly $\mathfrak{A} \cong \widehat{\mathfrak{A}}$, and the element $\widehat{\omega}_i$ is zero except for a $d_i \times d_i$ identity matrix in the i^{th} diagonal block. It is easy to compute a linear map

$$\psi : \mathfrak{A} \to \bigoplus_{1 \le i \le l} \widehat{\omega}_i \widehat{\mathfrak{A}} \widehat{\omega}_i.$$

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

$$\beta \mapsto U^{-1}\beta U = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1l} \\ b_{21} & b_{22} & & b_{2l} \\ \vdots & & & \vdots \\ b_{l1} & \cdots & \cdots & b_{ll} \end{bmatrix} \mapsto \begin{bmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & & \vdots \\ \vdots & & & 0 \\ 0 & \cdots & 0 & b_{ll} \end{bmatrix} \in \bigoplus_{1 \le i \le l} \widehat{\omega}_i \widehat{\mathfrak{A}} \widehat{\omega}_i \qquad (2.4)$$

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

A refinement of each of the ω_i's can be computed by decomposing the algebra $\widehat{\omega}_i \widehat{\mathfrak{A}} \widehat{\omega}_i$ as in Lemma 2.1 (assuming for now that we can find a decomposable element), for $1 \le i \le l$. Suppose we obtain pairwise orthogonal idempotents $\widehat{\omega}_{i1}, \ldots, \widehat{\omega}_{il_i} \in \widehat{\omega}_i \widehat{\mathfrak{A}} \widehat{\omega}_i$ whose sum is $\widehat{\omega}_i$. Suppose also that $V_i \in \mathsf{F}^{d_i \times d_i}$ is the obtained transition matrix, that $\widehat{\omega}_{ij}$ has rank d_{ij}, and that $\widetilde{\omega}_{ij} = V_i^{-1}\widehat{\omega}_{ij}V_i$ 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

$$V = \begin{bmatrix} V_1 & & & \\ & V_2 & & \\ & & \ddots & \\ & & & V_l \end{bmatrix} \in \mathsf{F}^{m \times m},$$

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

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

Theorem 2.6. *Let $\mathfrak{A} \subseteq \mathsf{F}^{m\times m}$ be an algebra of dimension n over $\mathsf{F} \cong \mathbb{F}_q$. Then we can compute*

(i) a transition matrix $U \in \mathsf{F}^{m\times m}$, and

(ii) positive integers $d_1, \ldots, d_s$ such that $m = d_1 + \cdots + d_s$,

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

$$\widehat{\omega}_i = \begin{bmatrix} \Delta_{i1} & & \\ & \ddots & \\ & & \Delta_{is} \end{bmatrix} \in \mathsf{F}^{m\times m}, \qquad \omega_i = U\widehat{\omega}_i U^{-1},$$

where $\Delta_{ij} \in \mathsf{F}^{d_i\times d_i}$ is the identity matrix if $i = j$ and the zero matrix if $i \ne j$. Then $\omega_1, \ldots, \omega_s$ are primitive, pairwise orthogonal idempotents in $\mathfrak{A}$ and $\omega_1 + \cdots + \omega_s = 1 \in \mathfrak{A}$.

This computation can be performed 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 $O((\mathcal{MM}(m)\log m + \mathcal{M}(m)\log q + \mathcal{R}(\mathfrak{A}))\cdot\log(m)\cdot\log(1/\epsilon))$ operations in F, or $O((m^3 + m^2\log q + \mathcal{R}(\mathfrak{A}))\cdot\log(m)\cdot\log(1/\epsilon))$ 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 $U \in \mathsf{F}^{m\times m}$ and the ranks $d_1, \ldots, d_l$ of pairwise orthogonal idempotents $\omega_1, \ldots, \omega_l \in \mathfrak{A}$. Choose a random $\alpha \in \mathfrak{A}$, and find $\psi(\alpha) \in \bigoplus_{1\le i\le l} \widehat{\omega}_i\widehat{\mathfrak{A}}\widehat{\omega}_i$. Suppose α_i is the image of α in $\widehat{\omega}_i\widehat{\mathfrak{A}}\widehat{\omega}_i$. The α_i's are also random and independent. Lemma 2.1 implies that it is possible to refine each $\widehat{\omega}_i$ and to 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.

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

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

for simple algebras $\mathfrak{S}_1, \ldots, \mathfrak{S}_k$, and that $\mathfrak{S}_i \cong \mathsf{E}_i^{t_i\times t_i}$, for an extension field E_i of F with $[\mathsf{E}_i : \mathsf{F}] = e_i$.

Within any simple component $\mathfrak{S}_i$, by Theorem 2.2 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 $e_i t_i^2/2 \le \dim \mathfrak{S}_i\omega_i' \le$

$3e_i t_i^2/4$. Since $t_i \cdot (3/4)^{3.5 \log t_i} \leq 1$, we will have constructed a complete set of primitive idempotents for $\mathfrak{S}_i$ with $3.5 \log t_i$ such reducible elements. Hence, with the choice of $77 \log t_i$ 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 we obtain a set of primitive idempotents for all simple components with probability at least $1/2$ after $77 \log m$ iterations, and with $77 \log(m) \cdot \log(1/\epsilon)$ 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 requires $O(\mathcal{MM}(m) \log m + \mathcal{M}(m) \log q + \mathcal{R}(\mathfrak{A}))$ operations in F or $O(m^3 + m^2 \log q + \mathcal{R}(\mathfrak{A}))$ operations in F using standard arithmetic, by Lemma 2.1. □

3 Wedderburn Decomposition of Semisimple Algebras

In this section we use the algorithm of Section 2 for finding a complete set of primitive orthogonal idempotents to determining the Wedderburn decomposition of a semisimple algebra. We are able to explicitly compute this decomposition as described below and get a check that the answer is indeed correct. Thus, the algorithm obtained is ultimately of the Las Vegas type for semisimple algebras, i.e., it never produces an incorrect answer.

In Subsection 3.1, we employ the orthogonal primitive idempotents to decompose semisimple algebras as a direct sum of simple algebras. In Subsection 3.2 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 F. If these isomorphisms are successfully computed, we obtain a certificate that $\mathfrak{A}$ is indeed semisimple and the algorithm is of the Las Vegas type.

3.1 Computing Simple Components of Semisimple Algebras

We first give a Monte Carlo algorithm to find the central primitive idempotents and simple components of a semisimple algebra over a finite field. A correctness test which yields a Las Vegas algorithm is given later. We assume throughout this subsection that $\mathfrak{A} \subseteq \mathsf{F}^{m \times m}$ is a semisimple algebra of dimension n, and that

$$\mathfrak{A} \cong \mathfrak{S}_1 \oplus \mathfrak{S}_2 \oplus \cdots \oplus \mathfrak{S}_k \cong \mathsf{E}_1^{t_1 \times t_1} \oplus \mathsf{E}_2^{t_2 \times t_2} \oplus \cdots \oplus \mathsf{E}_k^{t_k \times t_k} \tag{3.1}$$

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

Using the algorithm from Theorem 2.6 we can compute a transition matrix $U \in \mathsf{F}^{m \times m}$, and positive integers $d_1, \ldots, d_s$ such that $m = d_1 + \cdots + d_s$ and

$$\widehat{\omega}_i = \begin{bmatrix} \Delta_{i1} & & \\ & \ddots & \\ & & \Delta_{is} \end{bmatrix}, \qquad \omega_i = U \widehat{\omega}_i U^{-1}, \tag{3.2}$$

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

Definition 3.1. A nonsingular matrix $X \in \mathsf{F}^{m\times m}$ is a *semisimple transition matrix* for a semisimple matrix algebra $\mathfrak{A} \subseteq \mathsf{F}^{m\times m}$, with k simple components $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$, if the following conditions are satisfied.

(i) There exist positive integers $m_1, \ldots, m_k$ such that $m_1 + \cdots + m_k = m$ and, for all $\eta \in \mathfrak{A}$,

$$\eta = X^{-1} \begin{bmatrix} \eta_1 & & & 0 \\ & \eta_2 & & \\ & & \ddots & \\ 0 & & & \eta_k \end{bmatrix} X,$$

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

(ii) The central primitive idempotents of $\mathfrak{A}$ are $\overline{\omega}_1, \ldots, \overline{\omega}_k$, where

$$\overline{\omega}_j = X^{-1} \begin{bmatrix} \Delta_{j1} & & & 0 \\ & \Delta_{j2} & & \\ & & \ddots & \\ 0 & & & \Delta_{jk} \end{bmatrix} X,$$

and $\Delta_{jl} \in \mathsf{F}^{m_j\times m_j}$ is the identity matrix if $j = l$ and the zero matrix otherwise (for $1 \le l \le k$).

A *semisimple transition* for $\mathfrak{A}$ consists of a semisimple transition matrix X for $\mathfrak{A}$, the number k of simple components of $\mathfrak{A}$, and the positive integers $m_1, \ldots, m_k$ described above that correspond to $\mathfrak{A}$ and X.

Since $\mathfrak{A}$ is semisimple, each central primitive idempotent $\overline{\omega}_j$ is a sum of a subset of the given primitive idempotents $\omega_1, \ldots, \omega_s$, and each primitive idempotent ω_i in this set is a summand for exactly one $\overline{\omega}_j$ (and is annihilated by the rest). Thus, the central primitive idempotents correspond to a partition of $\omega_1, \ldots, \omega_s$. We will produce a semisimple transition by grouping the ω_i's together according to which simple component they belong.

Lemma 3.2. *Suppose $\mathfrak{A}$ decomposes as in* (3.1) *and suppose $\omega_1, \ldots, \omega_s \in \mathfrak{A}$ are primitive, pairwise 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 $\mathfrak{A}_u \cong \mathsf{E}_u^{t_u\times t_u}$ then $\omega_i\alpha\omega_j \neq 0$ with probability* $1 - 1/|\mathsf{E}_u|$.

Proof. Suppose ω_i and ω_j belong to different simple components $\mathfrak{S}_v$ and $\mathfrak{S}_w$ respectively, and that $\overline{\omega}_v$ and $\overline{\omega}_w$ are the central idempotents of $\mathfrak{S}_v$ and $\mathfrak{S}_w$ respectively. Then $\omega_i\overline{\omega}_v = \omega_i$ and $\omega_j\overline{\omega}_w = \omega_j$. Now, $\omega_i\alpha\omega_j = \omega_i\overline{\omega}_v\alpha\omega_j\overline{\omega}_w = \omega_i\alpha\omega_j\overline{\omega}_v\overline{\omega}_w = 0$, since $\overline{\omega}_v$ and $\overline{\omega}_w$ are orthogonal.

If ω_i and ω_j belong to the same simple component $\mathfrak{S}_u$, then the map sending $\alpha \in \mathfrak{A}$ to $\omega_i\alpha\omega_j$ is a homomorphism of additive groups whose image is isomorphic to E_u. For uniformly and randomly chosen $\alpha \in \mathfrak{A}$, $\omega_i\alpha\omega_j = 0$ if and only if α is in the kernel of this homomorphism; the probability that $\omega_i\alpha\omega_j = 0$ is thus $1/|\mathsf{E}_u|$, as claimed. □

Now suppose U is a transition matrix as in (3.2) and α is a randomly chosen element of $\mathfrak{A}$. Then

$$U^{-1}\alpha U = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{ss} \end{bmatrix} \tag{3.3}$$

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

Theorem 3.3. *Let $\mathfrak{A} \subseteq \mathsf{F}^{m\times m}$ be a semisimple algebra as in (3.1). Given integers $d_1, \ldots, d_s$ and a transition matrix U to a complete set of primitive pairwise orthogonal idempotents as in (3.2), we can find a semisimple transition for $\mathfrak{A}$, including a semisimple transition matrix $X \in \mathsf{F}^{m\times m}$, and a permutation and relabeling $d_{11}, \cdots, d_{1t_1}, \ldots, d_{k1}, \cdots, d_{kt_k}$ of $d_1, \ldots, d_s$, such that complete sets of primitive, pairwise orthogonal idempotents $\widetilde{\omega}_{ij} \in X^{-1}\mathfrak{A}X \subseteq \mathsf{F}^{m\times m}$ and $\omega'_{ij} \in \mathfrak{A}$ (for $1 \le i \le k$ and $1 \le j \le t_i$) are given by*

$$\widetilde{\omega}_{ij} = \begin{bmatrix} \Delta_{11} & & & & & & \\ & \ddots & & & & & \\ & & \Delta_{1t_1} & & & & \\ & & & \ddots & & & \\ & & & & \Delta_{k1} & & \\ & & & & & \ddots & \\ & & & & & & \Delta_{kt_k} \end{bmatrix}, \quad \omega'_{ij} = X\widetilde{\omega}_{ij}X^{-1}, \tag{3.4}$$

where $\Delta_{vw} \in \mathsf{F}^{d_{vw}\times d_{vw}}$ is the identity matrix if $v = i$ and $w = j$ and is the zero matrix otherwise. This computation can be performed 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 $O(\mathcal{MM}(m)\log(m) \cdot \log(1/\epsilon))$ operations in F.

Proof. We can simply choose random elements $\alpha \in \mathfrak{A}$ and compute $U^{-1}\alpha U$, which has block form as in (3.3). After each random choice of an α, it suffices to note which pairs of idempotents are linked by noting nonzero 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 $1/|\mathsf{F}|^2 \le 1/4$. Thus, after $\lceil 1/2 + \log_2 m\rceil$ 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 rename the primitive idempotents (in $\mathfrak{A}$) as $\omega'_{11}, \ldots, \omega'_{1t_1}, \cdots, \omega'_{k1}, \ldots, \omega'_{kt_k}$ so that $\overline{\omega}_i = \sum_{1\le j\le t_i} \omega'_{ij}$ is a central primitive idempotent in $\mathfrak{A}$ for $1 \le i \le k$. We then construct a semisimple transition matrix X from U by a simple permutation, set k to be the number of simple components that were found, and compute $m_i = \sum_{1\le j\le t_i} d_{ij}$ for $1 \le i \le k$, to complete a semisimple transition for $\mathfrak{A}$ with the stated properties. □

Combining this theorem with Theorem 2.6 we obtain the following corollary.

Corollary 3.4. *Let $\mathfrak{A} \subseteq \mathsf{F}^{m\times m}$ be a semisimple algebra over a finite field $\mathsf{F} \cong \mathbb{F}_q$ as in (3.1). We can find a semisimple transition for $\mathfrak{A}$, and integers $d_{11}, \ldots, d_{1t_1}, \cdots, d_{k1}, \ldots, d_{kt_k}$ which determine a complete set of primitive pairwise orthogonal idempotents ω'_{ij} in $\mathfrak{A}$ as in (3.4), 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 F, or $O((m^3 + m^2\log q + \mathcal{R}(\mathfrak{A}))\cdot\log^2(m)\cdot\log(1/\epsilon))$ operations in F using standard matrix and polynomial arithmetic, with a Monte Carlo algorithm that returns a correct answer with probability at least $1-\epsilon$ for a user specified parameter $\epsilon > 0$.*

3.2 Las Vegas Decomposition of Semisimple Algebras

Now let $\mathfrak{S} \subseteq \mathsf{F}^{m\times m}$ be an algebra over a finite field $\mathsf{F} \cong \mathbb{F}_q$ which we believe to be simple. Suppose we are given pairwise orthogonal idempotents $\omega_1, \ldots, \omega_t \in \mathfrak{S}$, with $\omega_1 + \cdots + \omega_t = 1 \in \mathfrak{S}$, such that $\omega_i = \operatorname{diag}(\Delta_{i1}, \ldots, \Delta_{it}) \in \mathsf{F}^{m\times m}$, where $\Delta_{ij} \in \mathsf{F}^{d_j\times d_j}$ is the identity matrix if $i = j$ and the zero matrix otherwise. In this subsection, we describe an algorithm which either reports that "algebra is not simple and/or idempotents not primitive" or produces a guaranteed simple algebra $\mathfrak{T}$ which is isomorphic to a subalgebra of $\mathfrak{S}$ and, with high probability, has the same dimension as $\mathfrak{S}$. That is, $\mathfrak{S}$ is isomorphic to $\mathfrak{T}$ with high probability, and hence $\mathfrak{S}$ is guaranteed simple.

When applied to each of the "simple components" (more precisely, the diagonal blocks) of the semisimple algebra denoted $X^{-1}\mathfrak{A}X$ in Subsection 3.1, we effectively construct an algebra isomorphic to a semisimple subalgebra of $X^{-1}\mathfrak{A}X$. If this subalgebra has the same dimension as that of $\mathfrak{A}$, then clearly $\mathfrak{A}$ is semisimple and we have the isomorphic images of each of its simple components. This completes an asymptotically efficient Las Vegas algorithm for the decomposition of semisimple matrix algebras.

If $\mathfrak{S}$ is indeed simple and the idempotents $\omega_1, \ldots, \omega_t$ are primitive, then $d_1 = d_2 = \cdots = d_t = m/t$ and, therefore, each idempotent ω_i has rank $d = d_1$ as a matrix in $\mathsf{F}^{m\times m}$. The algorithm should thus report "algebra not simple and/or idempotents not primitive" immediately unless $d_1 = \cdots = d_t$, and we will assume henceforth that the d_i's are all equal. Now, every $\alpha \in \mathfrak{S}$ can be written as

$$\alpha = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1t} \\ a_{21} & a_{22} & \cdots & a_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t1} & a_{t2} & \cdots & a_{tt} \end{bmatrix} \in \mathfrak{S}, \tag{3.5}$$

where $a_{ij} \in \mathsf{F}^{d\times d}$, and $\omega_i\alpha\omega_j$ is zero except for the $(i,j)^{\text{th}}$ block, which equals a_{ij}.

We first find a change of basis for $\mathfrak{S}$ so that $\omega_1\mathfrak{S}\omega_1$ is in a normal form. If $\mathfrak{S}$ is simple with primitive idempotents $\omega_1, \ldots, \omega_t$ then $\omega_1\mathfrak{S}\omega_1$ is a finite field of (unknown) degree e over F, such that $e \mid d$. Choose a random element $\gamma \in \mathfrak{S}$ and compute the Frobenius form of the leading $d \times d$ submatrix $c_{11} \in \mathsf{F}^{d\times d}$ (the nonzero part of $\omega_1\gamma\omega_1$): if $\mathfrak{S}$ is simple and the idempotent ω_1 is primitive then there exists an invertible $u \in \mathsf{F}^{d\times d}$ such that

$$\lambda = u^{-1}c_{11}u = \begin{bmatrix} C_f & & \\ & \ddots & \\ & & C_f \end{bmatrix} \in \mathsf{F}^{d\times d}$$

where $C_f \in \mathsf{F}^{\overline{e}\times\overline{e}}$ is the companion matrix of the minimal polynomial $f \in \mathsf{F}[x]$ of c_{11}. If λ has two or more *distinct* companion matrices in its Frobenius form, or if f is not irreducible, then the algorithm should report "algebra not simple and/or idempotents not primitive", since $\omega_1\mathfrak{S}\omega_1$ is not a field. Otherwise, if $\overline{e}$ is the degree of f (as above) then $\overline{e} \mid e$, and $\overline{e} = e$ with probability at least 1/2 (see, e.g., Giesbrecht (1995b), Theorem 5.2).

It is convenient to find an element $\alpha \in \mathfrak{S}$ as in (3.5) such that $a_{1i} = \omega_1\alpha\omega_i \neq 0$ and $a_{i1} = \omega_i\alpha\omega_1 \neq 0$ for $2 \leq i \leq t$. If $\mathfrak{S}$ is simple with primitive idempotents $\omega_1, \ldots, \omega_t$ then, for fixed i, j $(1 \leq i, j \leq t)$ and randomly chosen $\beta \in \mathfrak{S}$, $\omega_i\beta\omega_j \neq 0$ with probability at least $1 - 1/|\mathsf{F}| \geq 1/2$. Thus with an expected number of $O(\log t)$ random choices of elements β we can construct $\beta_{1i}, \beta_{i1} \in \mathfrak{S}$ such that $\beta_{1i} = \omega_1\beta_{1i}\omega_i \neq 0$ and $\beta_{i1} = \omega_i\beta_{i1}\omega_1 \neq 0$ for $2 \leq i \leq t$. If $\mathfrak{S}$ is simple with pairwise orthogonal primitive idempotents $\omega_1, \ldots, \omega_t$ then each nonzero β_{1i}, β_{i1} has rank d for $2 \leq i \leq t$. If this is not the case then the algorithm should report "algebra not simple and/or idempotents not primitive", so we will assume henceforth that $\mathrm{rank}(\beta_{1i}) = \mathrm{rank}(\beta_{i1}) = d$. Now, since $\omega_i\beta\omega_j$ is zero except possibly for the $(i,j)^{\text{th}}$ block, we can add together appropriate nonzero blocks of these β_{1i}'s and β_{i1}'s to construct α.

Let

$$U = \begin{bmatrix} u & & & \\ & a_{12}^{-1}u & & \\ & & \ddots & \\ & & & a_{1t}^{-1}u \end{bmatrix} \in \mathsf{F}^{m\times m}$$

and $\mathfrak{S}' = U^{-1}\mathfrak{S}U$. Note that since the idempotents $\omega_1, \ldots, \omega_t$ commute with U, these are also idempotents in $\mathfrak{S}'$ and are primitive and pairwise orthogonal in $\mathfrak{S}'$ if and only if they are primitive and pairwise orthogonal in $\mathfrak{S}$.

Consider the elements $\alpha' = U^{-1}\alpha U$ and $\omega_{1k} = \omega_1\alpha'\omega_k$ of $\mathfrak{S}'$ for $2 \leq k \leq t$. By construction ω_{1k} is zero except for the $(1,k)^{\text{th}}$ block, which equals $u^{-1}a_{1k}a_{1k}^{-1}u = 1_d$, the $d \times d$ identity matrix. Also, $\omega_1 U^{-1}\gamma U\omega_1$ generates a finite field of degree $\overline{e}$ over F. Let $\Lambda = \omega_1 U^{-1}\gamma U\omega_1 \in \mathfrak{S}'$ and recall that, with probability at least 1/2, $\overline{e} = e$. If this is the case (and, again, $\mathfrak{S}$ is simple with primitive pairwise orthogonal idempotents $\omega_1, \ldots, \omega_t$) then $\omega_1\mathfrak{S}'\omega_1 = \omega_1\mathsf{F}[\Lambda]\omega_1$ and, since $\omega_k\alpha'\omega_1$ is nonzero, $\omega_k\mathfrak{S}'\omega_1 = (\omega_k\alpha'\omega_1)(\omega_1\mathsf{F}[\Lambda]\omega_1)$.

If $\mathfrak{S}$ is a simple with primitive idempotents $\omega_1, \ldots, \omega_t$ then for $2 \leq k \leq t$ there exists a $\chi \in \mathfrak{S}$ such that $\omega_1\alpha\omega_k \cdot \omega_k\chi\omega_1 = \omega_1$. Equivalently, there exists a $\zeta' \in \mathfrak{S}'$ such that $\omega_{1k} \cdot \omega_k\zeta'\omega_1 = \omega_1$, i.e., such that the $(k,1)^{\text{th}}$ block y'_{k1} of ζ' equals 1_d. We must check that such a $\zeta' \in \mathfrak{S}'$ exists for each k $(2 \leq k \leq t)$. Suppose $a'_{k1} \in \mathsf{F}^{d\times d}$ is the $(k,1)^{\text{th}}$ block of α'; if the algorithm has not already failed then this matrix is invertible and we can efficiently check whether $(a'_{k1})^{-1} \in \mathsf{F}[\lambda]$. If it is, then we can safely conclude that the desired element ζ' belongs to $\mathfrak{S}'$, and we can conclude that the element ω_{k1} whose $(k,1)^{\text{th}}$ block is 1_d (and which is zero elsewhere) belongs to $\mathfrak{S}'$; if it is not, then the algorithm should report "failure". If $\overline{e} = e$ and, as usual, $\mathfrak{S}$ is simple with primitive idempotents $\omega_1, \ldots, \omega_t$, then the probability of "failure" at this step is less than 1/2.

Finally, assuming that the algorithm has not failed, we can construct a basis for a simple subalgebra of $\mathfrak{S}'$ as follows. For $2 \leq i, j \leq t$ let $\omega_{ij} = \omega_{i1} \cdot \omega_{1j} \in \mathfrak{S}'$, the matrix that is zero except for the $(i,j)^{\text{th}}$ block which is equal to 1_d. It is easily shown that the set $\{\omega_{i1}\Lambda^k\omega_{1j} : 1 \leq i, j \leq t, 0 \leq k \leq \overline{e}\}$ is a basis for a simple subalgebra $\mathfrak{T}$ of $\mathsf{E}^{t\times t}$, where

$\mathsf{E} = \mathsf{F}[\lambda]$ is an extension field of degree $\overline{e}$ over F. If $\dim \mathfrak{T} = \dim \mathfrak{S}$ then clearly $\mathfrak{T} \cong \mathfrak{S}$ and $\mathfrak{S}$ is a simple algebra.

Theorem 3.5. *Let $\mathfrak{S} \subseteq \mathsf{F}^{m\times m}$ be a matrix algebra of known dimension n over a field F, and let $\omega_1, \ldots, \omega_t \in \mathfrak{S}$ be block diagonal matrices, with zero matrices and identity matrices as blocks, such that $\omega_1, \ldots, \omega_t$ are pairwise orthogonal and have sum $1 \in \mathfrak{S}$. There is a Las Vegas algorithm that either confirms that $\mathfrak{S}$ is simple with primitive idempotents $\omega_1, \ldots, \omega_t$, by constructing an isomorphism from $\mathfrak{S}$ to $\mathsf{E}^{t\times t}$ for an extension field E of degree n/t over F, or reports "failure". In either case the algorithm requires an expected number of $O(\min(m^3, \mathcal{MM}(m) \log m) + \mathcal{R}(\mathfrak{S}) \log t)$ operations in F. This algorithm successfully generates an isomorphism with probability bounded away from zero whenever $\mathfrak{S}$ is simple and $\omega_1, \ldots, \omega_t$ are primitive, and never does so if this is not the case.*

The probability of success can be increased to $1 - 1/(2k)$ for $k > 0$ by repeating the above algorithm $O(\log k)$ times.

Now consider again the case of a semisimple algebra $\mathfrak{A}$ and semisimple transition matrix X for $\mathfrak{A}$, with positive integers $d_{11}, \ldots, d_{1t_1}, \cdots, d_{k1}, \ldots, d_{kt_k}$, primitive idempotents $\widetilde{\omega}_{ij} \in X^{-1}\mathfrak{A}X$, and $\omega'_{ij} \in \mathfrak{A}$ as described in Subsection 3.1 (and equation (3.4)). Recall that the semisimple algebra $X^{-1}\mathfrak{A}X \cong \mathfrak{A}$ consists of block diagonal matrices (with simple components corresponding to the diagonal blocks) and that if α is a random element of $\mathfrak{A}$ then $X^{-1}\alpha X$ is a random element of $X^{-1}\mathfrak{A}X$. Therefore, it is possible to select random and independent elements of each of the simple components of $X^{-1}\mathfrak{A}X$ at total cost $O(\mathcal{R}(\mathfrak{A}) + \mathcal{MM}(m))$. Again since $X^{-1}\mathfrak{A}X$ is "block diagonal," all other operations needed to test whether the i^{th} simple component of $X^{-1}\mathfrak{A}X$ can be performed by working in the matrix ring $\mathsf{F}^{m_i\times m_i}$ instead of the larger ring $\mathsf{F}^{m\times m}$ (where $m_1, \ldots, m_k$ are as in Subsection 3.1, so that $m_1 + \cdots + m_k = m$). Therefore, by applying the above construction 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 Corollary 3.4 we obtain the following theorem.

Theorem 3.6. *Let $\mathfrak{A} \subseteq \mathsf{F}^{m\times m}$ be a semisimple algebra over a finite field $\mathsf{F} \cong \mathbb{F}_q$ as in (3.1). We can find a semisimple transition for $\mathfrak{A}$, including a semisimple transition matrix X, and integers $d_{11}, \cdots, d_{1t_1}, \ldots, d_{k1}, \cdots, d_{kt_k} \in \mathbb{Z}$ with sum m that determine a set of pairwise orthogonal primitive idempotents as in (3.4), using a Las Vegas algorithm that requires an expected number of $O((\mathcal{MM}(m) \log m + \mathcal{M}(m) \log q + \mathcal{R}(\mathfrak{A})) \cdot \log^2(m))$ 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. The algorithm never produces the wrong answer and reports "failure" with probability less than $1/2$ on any invocation on any input.*

4 Conclusion

We have shown that for a semisimple algebra $\mathfrak{A}$, we can determine the complete Wedderburn decomposition with an asymptotic cost about as good as one could hope for, on the order of $\log m$ multiplications of elements in $\mathfrak{A}$. While randomness is employed, the algorithm is of the Las Vegas type and never gives an erroneous result. For a similar cost we can also find a complete set of primitive orthogonal idempotents in *any* (not necessarily semisimple) algebra $\mathfrak{A}$, though this algorithm is of the Monte Carlo type and has a controllable, exponentially small probability of error.

Clearly it would be desirable to obtain a complete set of primitive orthogonal idempotents which are *guaranteed correct* in any algebra with the above cost. One possible way to obtain this is with an efficiently computable certificate that an algebra is local. It would also be desirable to compute a basis for a semisimple subalgebra of $\mathfrak{A}$ isomorphic to $\mathfrak{A}/\operatorname{Rad}(\mathfrak{A})$, i.e., a very fast algorithm for (the semisimple part of) the Wedderburn-Malcev decomposition. Neither a Monte Carlo nor Las Vegas algorithm is known with this cost. Finally, finding a basis or generating set for the radical itself within this cost appears to be difficult. Indeed, even an algorithmic representation guaranteed to be of sufficiently small size is not known for algebras over finite fields.

References

T. M. Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag (New York), 1976.

E. R. Berlekamp. Factoring polynomials over large finite fields. *Math. Comp.* **24**, pp. 713–735, 1970.

A. Cohen, G. Ivanyos, and D. Wales. Finding the radical of an algebra of linear transformations. *J. Pure and Applied Algebra* , 1997. To appear.

D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. *J. Symb. Comp.* **9**, pp. 251–280, 1990.

L. E. Dickson. *Linear Groups with an Exposition of the Galois Field Theory.* Teubner, Leipzig, 1901; Dover, New York, 1958 (Leipzig), 1901. Dover, New York, 1958.

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.

F. R. Gantmacher. *The Theory of Matrices, Vol. I.* Chelsea Publishing Co. (New York NY), 1990.

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, 1995a.

M. Giesbrecht. Factoring in skew-polynomial rings over finite fields. *J. of Symbolic Computation* , 1995b. To appear.

J. H. Hodges. Scalar polynomial equations for matrices over a finite field. *Duke Math. J.* **25**, pp. 291–296, 1958.

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.

R. Lidl and H. Niederreiter. *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and its Applications.* Addison-Wesley (Reading MA), 1983.

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.