Computing Decompositions of Modules over Finite-Dimensional Algebras

Klaus M. Lux and Magdolna Szőke

CONTENTS

Based on our method for determining endomorphism rings [Lux and Szőke 03], we describe an algorithm to compute decompositions of modules of finite-dimensional algebras over finite fields. The algorithm is implemented in the C-Meat-Axe [Ringe 94].

1. INTRODUCTION

In this paper we describe a method for computing a decomposition of an A-module M of a finite-dimensional algebra A over a finite field F into indecomposable direct summands. More precisely, we are interested in constructing indecomposable A-submodules $M_1, \dots, M_r$ of M such that M is the (internal) direct sum of $M_1, \dots, M_r$:

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_r.$$

The algorithm assumes that a generating system of $\mathrm{End}_A(M)$, the endomorphism ring of M, is given. This can be achieved by following [Lux and Szőke 03], where an algorithm to compute an F-basis of $\mathrm{End}_A(M)$ is described. In the present paper we give an algebra version of the spinning algorithm to determine a (small) algebra-generating system of $\mathrm{End}_A(M)$; see Algorithm 6.1.

Our algorithm-computing decomposition uses the close relationship between the endomorphism ring and decompositions of M into direct summands. This well-known relationship is described in Section 2. In Section 3 we show how particular elements in $\mathrm{End}_A(M)$ lead to a decomposition of M into indecomposable summands. The algorithm is described in Section 4. Section 5 is dedicated to a detailed description of the implementation of the corresponding algorithm in the C-Meat-Axe. Moreover, timings for some test cases are given at the end of this section. Finally, in Section 6.2 we show how the approach can be used to test constructively whether two given indecomposable A-modules are isomorphic.

2000 AMS Subject Classification: Primary 20C20; Secondary 20C40, 16A65, 68W30

Keywords: Modular representation theory, endomorphism rings, decompositions of modules

2. DECOMPOSITIONS AND LEFT IDEALS

In this section we study the relationship between decompositions of an A-module M into a direct sum of A-submodules and decompositions of the endomorphism ring $E = \mathrm{End}_A(M)$ into a direct sum of left ideals.

Definition 2.1. Let M be a nonzero A-module. We define a *decomposition* of M into a *direct sum* as a list of A-submodules $M_1, \dots, M_r$ satisfying the following two conditions: Firstly $\sum_{i=1}^r M_i = M$ and secondly $M_i \cap \sum_{j \neq i} M_j = 0$ for $i = 1, \dots, r$. We write

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_r$$

for the decomposition of M. The submodules M_i are called *direct summands* of M (for $i = 1, \dots, r$). The set of decompositions of M into A-submodules will be denoted by $\mathcal{D}(M_A)$.

Definition 2.2. For an A-submodule N of M, we define

$$I(N) = \{\varphi \in E \mid M\varphi \subseteq N\}$$

as the set of all endomorphisms of M whose images lie in N.

Note that $I(N)$ is a left ideal of E.

Theorem 2.3. *Decompositions of M into a direct sum of A-submodules correspond bijectively to decompositions of E into a direct sum of left ideals: Define the following two maps:*

$$\Phi\colon \quad \mathcal{D}(M_A) \longrightarrow \mathcal{D}({}_E E)$$
$$M_1, \dots, M_r \longmapsto I(M_1), \dots, I(M_r)$$

and

$$\Psi\colon \quad \mathcal{D}({}_E E) \longrightarrow \mathcal{D}(M_A)$$
$$I_1, \dots, I_r \longmapsto MI_1, \dots, MI_r.$$

The maps Φ and Ψ are bijections, one being the inverse of the other.

A direct summand M_i in the above decomposition of M is indecomposable if and only if the corresponding left ideal $I(M_i)$ is indecomposable as a left E-module.

Proof: For the proof, see [Nagao and Tsushima 88, Theorems 4.2, 5.4, and 5.5]. □

Note that the ideals $I(M_i)$ occurring in Theorem 2.3 are projective left E-modules, that is, direct summands of a free left E-module (in this case of the regular module ${}_E E$ itself).

We remark that Theorem 2.3 is a consequence of a more general theorem: even a Morita equivalence can be given between the categories of the direct sums of direct summands of M_A and of all finitely generated projective left E-modules, as described in [Curtis and Reiner 81, Proposition 6.3].

Remark 2.4. Let $M = M_1 \oplus \cdots \oplus M_r$. For $1 \leqslant i \leqslant r$ we define a projection π_i onto M_i with respect to the above decomposition as follows: $M_j \pi_i = \{0\}$ for all $j \neq i$, while π_i acts as the identity on M_i. Then π_i is an idempotent of E for $i = 1, \dots, r$, which is primitive if and only if M_i is indecomposable. Moreover, $I(M_i) = M\pi_i$ for all $1 \leqslant i \leqslant r$.

We now investigate in further detail the relationship between decompositions of M and the structure of the endomorphism algebra E. Let $J(E)$ be the *Jacobson radical* of E, the intersection of the maximal left ideals of E. We consider the quotient algebra $\bar{E} = E/J(E)$. Note that $\bar{E}$ is the largest semisimple factor of E. Denote the image under the canonical projection of $E \twoheadrightarrow \bar{E}$ of an element $\sigma \in E$ in $\bar{E}$ by $\bar{\sigma}$.

Theorem 2.5. *Let $M = M_1 \oplus \cdots \oplus M_r$ be a decomposition of M into indecomposable summands and let $I_i = I(M_i)$ for $i = 1, \dots, r$. Then the following are equivalent:*

(i) *M_i and M_j are isomorphic as A-modules.*

(ii) *I_i and I_j are isomorphic as left E-modules.*

(iii) *$\bar{I}_i$ and $\bar{I}_j$ are isomorphic as left E-modules.*

In particular, the multiplicity of the indecomposable direct summand M_i as a summand in the above decomposition is equal to the dimension of the corresponding simple E-module $\bar{I}_i$ over its endomorphism ring.

Proof: For the proof, see [Nagao and Tsushima 88, part iii of Theorem 5.4 and Theorem 4.5]. □

3. FINDING A DECOMPOSITION

In the previous section we indicated that a decomposition of M can be derived once we have a decomposition of E into left ideals. By Remark 2.4 these ideals are cyclic, that is, they are generated by a single element, namely, a projection. However, these ideals contain more single generators than projections. So our aim is to find endomorphisms of M determining an ideal decomposition of E. In other words, we want to find elements of E whose images as A-endomorphisms of M are the indecomposable direct summands in a decomposition of M. We are now going to describe how we construct such elements. Instead of looking for such elements in E we first choose nonnilpotent generators for simple left ideals in $\bar{E} = E/J(E)$ such that $\bar{E}$ is the direct sum of these simple left ideals. We then show that M is the direct sum of the images of sufficiently high powers of the preimages in E of these generators.

Now suppose we are given a decomposition of $\bar{E}$ into r (simple) left ideals:

$$\bar{E} = L_1 \oplus \cdots \oplus L_r.$$

According to [Nagao and Tsushima 88, Theorem 4.11], there exist left ideals I_i of E for $i = 1, \ldots, r$ such that

$$E = I_1 \oplus \cdots \oplus I_r$$

and $L_i = \bar{I}_i$ for all i.

Lemma 3.1. *Fix $1 \leqslant i \leqslant r$. Let $\beta_{i,1}, \ldots, \beta_{i,d_i}$ be elements of E such that $\bar{\beta}_{i,j}$ (for $j = 1, \ldots, d_i$) form a basis of L_i. Then there is at least one j_i such that β_{i,j_i} is not nilpotent.*

Proof: Let $1_{\bar{E}} = e_1 + \cdots + e_r$ according to the decomposition of $\bar{E}$. Note that $e_1, \ldots, e_r$ are mutually orthogonal primitive idempotents of $\bar{E}$. There exist $\lambda_1, \ldots, \lambda_{d_i} \in F$ such that

$$e_i = \sum_{j=1}^{d_i} \lambda_j \bar{\beta}_{i,j}.$$

Hence

$$e_i = e_i e_i e_i = \sum_{j=1}^{d_i} \lambda_j e_i \bar{\beta}_{i,j} e_i.$$

Thus, for some j_i, $\bar{\sigma} := e_i \bar{\beta}_{i,j_i} e_i \neq 0$. Furthermore, $e_i \bar{E} e_i$ is a division ring with identity element e_i, so $\bar{\sigma}$ is invertible in $e_i \bar{E} e_i$. Note that $\bar{\beta}_{i,j_i} = \bar{\beta}_{i,j_i} e_i$. Thus

$$e_i \bar{\beta}_{i,j_i}^n = (e_i \bar{\beta}_{i,j_i})^n = \bar{\sigma}^n \neq 0$$

for each natural number n. Hence β_{i,j_i} is not nilpotent. □

By Fitting's lemma, we can choose n_i for $i = 1, \ldots, r$ such that $M \neq \mathrm{Ker}(\beta_{i,j_i}^{n_i}) = \mathrm{Ker}(\beta_{i,j_i}^{n_i+1})$, or equivalently, $\mathrm{Im}(\beta_{i,j_i}^{n_i}) = \mathrm{Im}(\beta_{i,j_i}^{n_i+1})$. Define $\varepsilon_i = \beta_{i,j_i}^{n_i}$. Then $M = \mathrm{Im}(\varepsilon_i) \oplus \mathrm{Ker}(\varepsilon_i)$. We call $M\varepsilon_i$ the *stable image* of β_{i,j_i}.

Theorem 3.2. *The elements ε_i for $i = 1, \ldots, r$ have the following properties:*

(i) $\bar{E}\bar{\varepsilon}_i = L_i$.

(ii) $E\varepsilon_i$ *is a projective indecomposable left E-module.*

(iii) ${}_E E = E\varepsilon_1 \oplus \cdots \oplus E\varepsilon_r$.

Proof: (i) By construction, ε_i is not nilpotent, so $\varepsilon_i \notin J(E)$. Hence $0 \neq \bar{E}\bar{\varepsilon}_i \subseteq L_i$. Since L_i is simple, equality holds.

(ii) We first show that $E\varepsilon_i = I(\mathrm{Im}\,\varepsilon_i)$; see Definition 2.2. Since $\mathrm{Im}\,E\varepsilon_i = \mathrm{Im}\,\varepsilon_i$, we have the containment $E\varepsilon_i \subseteq I(\mathrm{Im}\,\varepsilon_i)$. Let us prove the reverse containment. By definition, $\mathrm{Im}\,\varepsilon_i^2 = \mathrm{Im}\,\varepsilon_i$, so ε_i is invertible on its image. Let $\delta \in E$ be the endomorphism of M having kernel $\mathrm{Ker}\,\varepsilon_i$ and acting as the inverse of ε_i on $\mathrm{Im}\,\varepsilon_i$. Then for each $\sigma \in I(\mathrm{Im}\,\varepsilon_i)$ we have $\sigma = \sigma\delta\varepsilon_i$, so $I(\mathrm{Im}\,\varepsilon_i) \subseteq E\varepsilon_i$.

Now, since $M = \mathrm{Im}\,\varepsilon_i \oplus \mathrm{Ker}\,\varepsilon_i$, by Theorem 2.3, $E\varepsilon_i$ is a projective E-module. Therefore,

$$E\varepsilon_i/J(E\varepsilon_i) = E\varepsilon_i/\left(J(E) \cap E\varepsilon_i\right) = \bar{E}\bar{\varepsilon}_i = L_i.$$

So $E\varepsilon_i$ is indecomposable.

(iii) Since $\bar{E} = L_1 \oplus \cdots \oplus L_r = \bar{E}\bar{\varepsilon}_1 \oplus \cdots \oplus \bar{E}\bar{\varepsilon}_r$, we conclude that

$$E = E\varepsilon_1 + \cdots + E\varepsilon_r + J(E).$$

Therefore, $E = E\varepsilon_1 + \cdots + E\varepsilon_r$ by Nakayama's lemma; see [Nagao and Tsushima 88, part (i) of Theorem 3.6]. Since $E\varepsilon_i/J(E\varepsilon_i) \cong L_i$, we know

$${}_E E \cong \dotplus_{i=1}^{r} E\varepsilon_i,$$

the outer direct sum of $E\varepsilon_1, \ldots, E\varepsilon_r$. Then a dimension argument shows that

$$E = E\varepsilon_1 \oplus \cdots \oplus E\varepsilon_r. \qquad \square$$

Corollary 3.3. *Keeping the notation of the present section, we obtain that the A-module M has the following decomposition into indecomposable direct summands:*

$$M = M\varepsilon_1 \oplus M\varepsilon_2 \oplus \cdots \oplus M\varepsilon_r.$$

Proof: The result follows from Theorems 2.3 and 3.2. □

4. THE ALGORITHM

By the results of Sections 2 and 3, we have the following algorithm for computing a decomposition of an A-module M:

Algorithm 4.1. (Decomposing an A-module M.)

Input: An A-module M.

Calculation:

- Compute a basis $\mathcal{B}$ and an algebra-generating system $\mathcal{G}$ of the endomorphism ring E of M and the left regular representation of E as the action of the generators in $\mathcal{G}$ with respect to the basis $\mathcal{B}$.
- Determine the composition factors of the regular module ${}_EE$.
- Compute a basis $\mathcal{C}$ of ${}_EE$ consisting of a basis $\mathcal{C}_{J(E)}$ of the radical of ${}_EE$ and liftings $\mathcal{C}_1, \dots, \mathcal{C}_r$ of bases $\bar{\mathcal{C}}_1, \dots, \bar{\mathcal{C}}_r$ of the respective direct summands $L_1, \dots, L_r$ of ${}_E\bar{E}$. The basis elements in $\mathcal{C}$ are given by their coefficients with respect to the basis $\mathcal{B}$ of E.
- For each simple direct summand L_i of the head of ${}_EE$ do
  - For all elements b of $\mathcal{C}_i$ do
    - ∗ Calculate the endomorphism β of M described by b.
    - ∗ Calculate the characteristic polynomial χ_β^M of the action of β on M.
    - ∗ If $\chi_\beta^M \neq x^{\dim_F M}$, then
      - · $\varepsilon_i := \beta$.
        While $\mathrm{Ker}(\varepsilon_i) \subsetneq \mathrm{Ker}(\varepsilon_i^2)$ do
        + $\varepsilon_i := \varepsilon_i^2$
        End of while-loop.
      - · Exit the inner for-loop.
    - ∗ End if.
  - End for.
  - Compute a basis of $\mathrm{Im}\,\varepsilon_i$ in M, which is the corresponding direct summand of M.
- End for.
- Compute the action of A on the direct summands.

Output: The direct summands of M and a basis transformation corresponding to the resulting decomposition of M.

5. THE IMPLEMENTATION

The above algorithm has been implemented by the second author in the C-Meat-Axe [Parker 84, Ringe 94]. It is now a standard program of version 2.4.

The actual computations are done by the program `decomp`. Its input is the module (given by matrices of the action of a generating system of the algebra in question) and the following information about its endomorphism ring: a basis, an algebra-generating system, the left regular representation corresponding to it, a basis of the radical, and lifts of the bases of the simple direct summands of the semisimple factor. The endomorphism ring together with its regular representation is made by our previous program `mkhom` (see [Lux and Szőke 03] and Section 6.1 of the present paper). Since the C-Meat-Axe deals with right modules, the radical series has to be computed with a program computing socle series. It can be computed by an algorithm of the first author and M. Wiegelmann [Lux and Wiegelmann 01].

The output of the program `decomp` is a basis of the module reflecting the decomposition. Optionally, `decomp` computes the matrices of the action of the algebra on the module in this new basis and that on the direct summands of the module.

Note that isomorphic indecomposable direct summands can be recognized by Theorem 2.5. This is reflected by the naming of the direct summands in the output.

We compare our programs with the Magma procedure `IndecomposableSummands` [Bosma and Cannon 98, Section 41.10.3, vol. III] in the following. The computations were done with Magma, version 2.8. Since the algorithm used by Magma has not been published, we do not know how the computation in `IndecomposableSummands` is carried out. We used the following script:

```
load "<Mfile>";
V := RModule(<field>, <Mdim>);
M := RModule(V, <Malg>);
IndecomposableSummands(M);
```

Here, `Mfile` contains the matrix algebra `Malg` over the field `field`, which is a representation of the algebra A describing the module M to be decomposed.

For the C-Meat-Axe, we used the following procedure:

```
chop -g <numAgens> <Mname>
pwkond -t <Mname>
rad -l 1 <Mname>
mkhom -H <headdim> -l <Mname> <Nname> <Endoname>
chop -g <numEndogens> <Endoname>.lrr
```

					Magma		C-Meat-Axe			
algebra	n	dim	nns	ns	t	m	t_1	t_2	t	m
$c(\mathbb{F}_2 J_1)$	3	93	3	3	$1.3s$	4.4	$0.13s$	$0.06s$	$0.2s$	0.76
$c(\mathbb{F}_4 J_1)$	3	93	4	4	$6s$	4.7	$0.24s$	$0.09s$	$0.33s$	0.9
$c(\mathbb{F}_2 J_2)$	5	252	2	2	$1.9s$	5.5	$0.7s$	0.08	$0.78s$	0.9
$\mathbb{F}_3 GL_4(3)$	2	361	4	4	$8.95s$	6.9	$3.64s$	$0.29s$	$3.9s$	1.2
$c(\mathbb{F}_3 M_{23})$	4	344	7	17	$365s$	36	$49.7s$	$8.3s$	$58s$	27
$c(\mathbb{F}_3 HS)$	6	683	6	24	$234m$	443	$18m28s$	$95s$	$20m$	304
$c(\mathbb{F}_{25} HN)$	2	800	14	21	$90.5h$	406	$12m20s$	$67s$	$13m$	268
$c(\mathbb{F}_{25} HN)$	2	1564	11	19	?	?	$163m$	$14m$	$177m$	852

TABLE 1. A comparison of the running times of the Magma and C-Meat-Axe algorithms.

```
pwkond -t <Endoname>.lrr
soc -l 1 <Endoname>.lrr
decomp <Mname> <Endoname>
```

For our programs, the running times are divided into two parts: the whole time for computing the endomorphism ring with its regular representation and the rest, namely, computing the radical of the endomorphism ring and then the decomposition.

The computations were done on an Intel Pentium 4 computer with two 3.20-GHz processors and 2 GB main memory under Linux 2.6.7.

In Table 1, we list the following data:

1. the algebra,
2. the number of its generators (n),
3. the dimension of the module (dim),
4. the number of nonisomorphic indecomposable summands (nns),
5. the number of all indecomposable summands (ns),
6. the running times (t) and the memory use (m) for Magma and the C-Meat-Axe, and the two parts of running times (t_1 and t_2) for the C-Meat-Axe.

For the algebra, a letter c indicates that it is a condensation of the group algebra. The memory use is always given in megabytes. All the modules are available on the home page of the first author (http://www.math.arizona.edu/~klux).

We remark that we let the program Magma run once more in the case of the module of the Higman–Sims group, but it was not able to compute a decomposition in about 10 days. In this case, Magma used about 100 MB.

In the case of the module of dimension 1564 of the Harada–Norton group, Magma was unable to do the computation, because all virtual memory was exhausted.

6. APPENDIX

6.1 An Algebra Spinning Algorithm

In this section we present an algorithm to compute an algebra-generating system of an algebra E if a basis of E is given. The procedure is the spinning algorithm for modules [Lux and Szőke 03, Algorithm 3.1], applied to algebras, so we do not give a proof of its correctness.

Algorithm 6.1. (Algebra Spinning.)

Input: A basis Bas of the algebra E.

Calculation:

- $AlgGens := [\,]$, $SpinBas := [\,]$, $randel := 0$.
- While Length($SpinBas$) $<$ Length(Bas) do
  - Make a random linear combination $randel$ of Bas that is independent of $SpinBas$.
  - Append $randel$ to $AlgGens$.
  - Append $randel$ to $SpinBas$.
  - $t :=$ Length($SpinBas$).
  - Do until $t >$ Length($SpinBas$).
    - For $i := 1$ to Length($AlgGens$) do
      - $a := SpinBas[t] \cdot AlgGens[i]$.
      - If $a \notin \langle SpinBas \rangle$, then append a to $SpinBas$.
      - $a := AlgGens[i] \cdot SpinBas[t]$.
      - If $a \notin \langle SpinBas \rangle$, then append a to $SpinBas$.
    - End for.
    - Increment t by 1.
  - End do.
- End do.

Output: An algebra-generating system $AlgGens$ and the spinning basis $SpinBas$ of E.

6.2 An Isomorphism Test

In this last section, we study how to determine whether two indecomposable modules are isomorphic.

Lemma 6.2. *Let M be an indecomposable A-module with endomorphism ring $E := \mathrm{End}_A(M)$. Let $\beta_1, \ldots, \beta_m$ be an F-basis of E. Then β_i is invertible for some $1 \leqslant i \leqslant m$.*

Proof: By [Nagao and Tsushima 88, Theorem 5.10], since E is a local ring, all elements of $E \setminus J(E)$ are invertible. Since $J(E)$ cannot contain all basis elements, one of them is invertible. □

We can generalize the above lemma to determine whether two indecomposable modules are isomorphic.

Theorem 6.3. (Isomorphism test.)
Let M and N be indecomposable A-modules and let $\varphi_1, \ldots, \varphi_m$ be a basis of the homomorphism space $\mathrm{Hom}_A(M, N)$. Then M and N are isomorphic as A-modules if and only if φ_i is an isomorphism for some $1 \leqslant i \leqslant m$.

Proof: If M and N are not isomorphic, then there is no isomorphism from M onto N. Assume $M \cong N$ and let $\sigma \colon N \to M$ be an isomorphism. Then

$$\mathrm{End}_A(M) = \mathrm{Hom}_A(M, N) \cdot \sigma,$$

and the elements $\varphi_i\sigma$ form a basis of $\mathrm{End}_A(M)$. Hence, by Lemma 6.2, $\varphi_i\sigma$ is invertible for some $1 \leqslant i \leqslant m$. Therefore, φ_i is invertible for the same i. □

By Theorem 6.3, we can easily test whether two indecomposable modules of the same dimension are isomorphic, provided that a basis of the homomorphism space is given. We have only to calculate the dimension of the null space of the basis elements. This can be done by the program `znu` of the C-Meat-Axe.

This procedure can be extended to not necessarily indecomposable modules: as a first step, we decompose both modules and then test whether a bijection between their direct summands can be given such that corresponding direct summands are isomorphic.

ACKNOWLEDGMENTS

The first author was partially supported by an NSF grant. The second author was supported by Hungarian Scientific Research Grant OTKA T 034878.

REFERENCES

[Bosma and Cannon 98] W. Bosma and J. Cannon. "Handbook of Magma Functions." Available online (http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm), 1998.

[Curtis and Reiner 81] C. W. Curtis and I. Reiner. *Methods of Representation Theory with Applications to Finite Groups and Orders*, Pure and Applied Mathematics 1. New York: Wiley, 1981.

[Lux and Szőke 03] K. M. Lux and M. Szőke. "Computing Homomorphism Spaces between Modules over Finite-Dimensional Algebras." *Experimental Mathematics* 12:1 (2003), 91–98.

[Lux and Wiegelmann 01] K. Lux and M. Wiegelmann. "Determination of Socle Series Using the Condensation Method." *J. of Symbolic Computation* 31:1/2 (2001), 163–178.

[Nagao and Tsushima 88] H. Nagao and Y. Tsushima. *Representations of Finite Groups*. New York: Academic Press, 1988.

[Parker 84] R. A. Parker. "The Computer Calculation of Modular Characters (the Meat-Axe)." In *Computational Group Theory*, edited by M. D. Atkinson, pp. 267–274. New York: Academic Press, 1984.

[Ringe 94] M. Ringe. "The C-Meat-Axe." Available online (http://www.math.rwth-aachen.de/homes/MTX/), 1994.

Klaus M. Lux, Department of Mathematics, University of Arizona, Tucson, Arizona, USA (klux@math.arizona.edu)

Magdolna Szőke, Department of Algebra, Institute of Mathematics, Technical University Budapest, Sztoczek u. 2., 1111 Budapest, Hungary (mszoke@math.bme.hu)

Received April 20, 2005; accepted August 2, 2005.