Journal of Symbolic Computation 75 (2016) 149–170

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

An isomorphism test for modules over a non-commutative PID. Applications to similarity of Ore polynomials ☆

José Gómez-Torrecillas [a], F.J. Lobillo [a], Gabriel Navarro [b]

[a] Department of Algebra and CITIC, University of Granada, Spain
[b] Department of Computer Science and AI, and CITIC, University of Granada, Spain

ARTICLE INFO

Article history:
Received 5 December 2014
Accepted 10 July 2015
Available online 4 November 2015

MSC:
16S36
16Z05
68W30

Keywords:
Isomorphic modules
Similar Ore polynomials
Canonical matrix form

ABSTRACT

Let R be a non-commutative PID finitely generated as a module over its center C. In this paper we give a criterion to decide effectively whether two given elements $f, g \in R$ are similar, that is, if there exists an isomorphism of left R-modules between R/Rf and R/Rg. Since these modules are of finite length, we also consider the more general problem of deciding when two given left R-modules of finite length are isomorphic. This criterion allows the design of algorithms when R is an Ore extension of a skew-field whose center is a commutative polynomial ring. We propose two methods which, essentially, check the equality of the rational canonical forms of certain matrices with coefficients in C associated to each of the modules. These algorithms are based on the fact that, if R is finitely generated as a C-module, then the existence of an isomorphism of R-modules can be reduced to checking the existence of an isomorphism of C-modules. Actually, we prove this result in the realm of non-commutative principal ideal domains, generalizing a version given by Jacobson for some Ore extensions of a skew field by an automorphism.

☆ Research partially supported by grants MTM2013-41992-P and TIN2013-41990-R from the Ministerio de Economía y Competitividad of the Spanish Government and from FEDER.

E-mail addresses: gomezj@ugr.es (J. Gómez-Torrecillas), jlobillo@ugr.es (F.J. Lobillo), gnavarro@ugr.es (G. Navarro).

http://dx.doi.org/10.1016/j.jsc.2015.11.012
0747-7171/

1. Introduction

In 1933, O. Ore presented the foundations of non-commutative polynomials in one variable, defining what we call nowadays an Ore extension of a skew-field. He established the basic properties of these skew polynomials, including a factorization theory. The factorization was proved to be unique up to similarity of polynomials. In contrast with the commutative case, similar polynomials need not to be associated, and this entails that similar polynomials do not behave so well with respect to arithmetic as associated ones. For instance, products of pairwise similar polynomials are not necessarily similar. Hence, in order to improve the computational treatment of skew polynomials, a procedure to decide if two given polynomials are similar should be provided.

Skew polynomials are relevant in several branches of mathematics. Quantum affine spaces and other quantized versions of classical algebras can be described in terms of iterated Ore extensions. The usual applications to physics are focused in algebras over complex or real numbers. On the other hand, Piret (1976) used skew polynomials over finite fields to introduce Cyclic Convolutional Codes, whose algebraic structure is deeply studied in Gluesing-Luerssen and Schmale (2004) and Gluesing-Luerssen and Tsang (2008), and extended by López-Permouth and Szabo (2013). This connection with Coding Theory suggests that new algorithms over skew polynomials should be developed. For instance, a Las Vegas factorization algorithm of skew polynomials over finite fields was proposed by Giesbrecht (1998), see also Coulter et al. (2004) for an application to the theory of decomposition of linearised polynomials and Coulter et al. (2001) for an attack to the HFE cryptosystem.

An Ore extension $D[X;\sigma,\delta]$ (see Section 3 for the precise definition) of a skew-field D is a (non-commutative) principal ideal domain (PID for short) whenever σ is an automorphism. The basic arithmetical properties of non-commutative PID were settled by Jacobson (1943), where the structure of their finitely generated modules was also studied.

In particular, he stated that, for $R = D[X;\sigma]$ an Ore extension of the skew-field D by an automorphism σ, under suitable finiteness conditions, two given X-torsionfree left R-modules of finite length are isomorphic if and only if they are isomorphic as modules over the center C of R, see Jacobson (1943, Ch. 3, Theorem 33). Jacobson detailed a proof for the case of indecomposable modules, leaving the indication that the Krull–Schmidt Theorem may be used to get the result for decomposable modules. This last step is not trivial, specially in the case of decomposable primary modules. In Section 2, we give a full proof of Theorem 9, a generalization of Jacobson (1943, Ch. 3, Theorem 33). Our proof differs, even in the indecomposable case, in many aspects from that of Jacobson (1943, Ch. 3, Theorem 33). As a consequence, it works over any non-commutative PID finite over its center, and it covers more examples, like Ore extensions of derivation type $D[X;\delta]$ finite over their centers. Theorem 9 is also a slight generalization of Gómez-Torrecillas et al. (2014, Theorem 1), since freeness of the PID over its center is not required. In fact, if R is finite over its center, then this center is a Dedekind domain. This remark helps to simplify some proofs which appeared in Gómez-Torrecillas et al. (2014), our contribution in the Proceedings of ISSAC'14. This theorem, in conjunction with the description from Jacobson (1996, Theorem 1.1.22) of the center of $D[X;\sigma]$ as a commutative polynomial ring over a suitable field, constitutes the key of our algorithms to decide if two given polynomials in $D[X;\sigma]$ are similar (Section 3) and, more generally, to decide whether two given finitely generated modules are isomorphic. In order to design algorithms applicable to any finitely generated module, the case of modules which are not X-torsionfree requires an independent analysis. Similar algorithms may be designed for Ore extensions of derivation type $D[X;\delta]$ under suitable finiteness conditions. We shall pay special attention to the case of an Ore extension $\mathbb{F}[X;\sigma]$ of a finite field $\mathbb{F}$. Both theoretical efficiency and numerical simulations of these algorithms are considered, which do not appear in Gómez-Torrecillas et al. (2014).

The isomorphism test for general finitely generated left modules over $D[X;\sigma]$ is given in Section 4, see Algorithm 6. This is also stated in Gómez-Torrecillas et al. (2014, Algorithm 4). This criterion is based on calculating the so-called rough decomposition of the modules and computing the rational canonical forms of the matrices associated to the decompositions. In order to relax the space requirements of Algorithm 6, we include in this paper a variation of it, see Algorithm 8, which computes the invariant factors of each module and checks their pairwise similarity.