Journal of Algebra 421 (2015) 541–559

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

The module isomorphism problem reconsidered

Peter A. Brooksbank [a], James B. Wilson [b,*]

[a] *Department of Mathematics, Bucknell University, Lewisburg, PA 17837, USA*
[b] *Department of Mathematics, Colorado State University, Ft. Collins, CO 80523, USA*

ARTICLE INFO

Article history:
Received 29 April 2014
Available online 16 September 2014
Communicated by William M. Kantor and Charles Leedham-Green

Keywords:
Isomorphism
Modules
Conjugacy

ABSTRACT

Algorithms to decide isomorphism of modules have been honed continually over the last 30 years, and their range of applicability has been extended to include modules over a wide range of rings. Highly efficient computer implementations of these algorithms form the bedrock of systems such as GAP and Magma, at least in regard to computations with groups and algebras. By contrast, the fundamental problem of testing for isomorphism between other types of algebraic structures – such as groups, and almost any type of algebra – seems today as intractable as ever. What explains the vastly different complexity status of the module isomorphism problem?

This paper argues that the apparent discrepancy is explained by nomenclature. Current algorithms to solve module isomorphism, while efficient and immensely useful, are actually solving a highly constrained version of the problem. We report that module isomorphism in its general form is as hard as algebra isomorphism and graph isomorphism, both well-studied problems that are widely regarded as difficult. On a more positive note, for cyclic rings we describe a polynomial-time algorithm for the general module isomorphism problem. We also report on a Magma implementation of our algorithm.

© 2014 Elsevier Inc. All rights reserved.

* Corresponding author.
E-mail addresses: pbrooksb@bucknell.edu (P.A. Brooksbank), James.Wilson@ColoState.Edu (J.B. Wilson).

http://dx.doi.org/10.1016/j.jalgebra.2014.09.004
0021-8693/© 2014 Elsevier Inc. All rights reserved.

Dedicated to the memory of Ákos Seress

1. Introduction

In the field of computational algebra, the problem of testing isomorphism of modules stands apart from isomorphism tests for other algebraic structures. Decades of progress has brought improvements to existing methods, and new ideas that have broadened the scope of module isomorphism tests [4,5,15,17,23,24,27]. Tools for computing with modules are now an integral part of the infrastructure of systems such as GAP [6] and MAGMA [1]. By contrast, testing isomorphism of other algebraic structures, such as finite groups, rings, and Lie and Jordan algebras, has remained extremely difficult.

In this note, we propose that the current state of play is due not to the relative ease of module isomorphism as an algorithmic problem, but rather to the fact that the problem widely referred to as "module isomorphism" is, in reality, a rather constrained version of the one your typical algebraist would likely write down. We show that, framed in a more general (and, we contend, quite natural) form, the module isomorphism problem is at least as hard as the better known *graph isomorphism problem* (Theorem 1.2). While thus suggesting that a satisfactory solution to our "general" module isomorphism problem will not soon be forthcoming, we also exhibit useful instances that do admit efficient solutions (Theorem 1.3).

It is important to stress that our intent here is not to imply that the computational algebra community has hitherto been interested in the wrong problem. On the contrary, the algorithms that underlie the accepted module isomorphism tests are among the most efficient and widely used in the entire field. It is rather that we foresee a demand for solutions to problems that are most accurately framed as module isomorphism problems of a more general flavor. In fact, as we explain briefly in the concluding section, this work grew from a particular application of such a problem to testing isomorphism of finite p-groups [3].

A motivating example. Suppose M and N are both 1-dimensional modules over a common field, say GF(9). Up to isomorphism there is only one such module, so we would expect any test of module isomorphism to confirm that $M \cong N$.

Consider the experiment in Fig. 1, conducted using the MAGMA system. The same experiment may also be carried out in GAP with the same results.

We note that in systems such as GAP and MAGMA, as well as in the literature [4,5,14,24], an A-module M is input by providing a list $(X_1, \ldots, X_\ell)$ of $(n \times n)$-matrices over a field k, where $n = \dim_k M$. These matrices correspond to the action by a fixed generating set of A on the underlying k-vector space M. Thus, the code represents the field GF(9) as a ring of (2×2)-matrices over the field $k = \mathrm{GF}(3)$, namely

$$A = B = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in k \right\}.$$

Download English Version:

https://daneshyari.com/en/article/4584427

Download Persian Version:

https://daneshyari.com/article/4584427

Daneshyari.com