ARTICLE IN PRESS

Journal of Computational and Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

Computation of isotopisms of algebras over finite fields by means of graph invariants

O.J. Falcón [a], R.M. Falcón [b,*], J. Núñez [a], A.M. Pacheco [c], M.T. Villar [a]

[a] Department of Geometry and Topology. University of Seville, Spain

[b] Department of Applied Mathematics I. University of Seville, Spain

[c] Department of Quantitative Methods. Loyola University Andalusia, Spain

ARTICLE INFO

Article history:
Received 10 June 2016
Received in revised form 2 September 2016

MSC:
05C25
05C30
05B15

Keywords:
Graph theory
Finite field
Isomorphism
Latin square

ABSTRACT

In this paper we define a pair of faithful functors that map isomorphic and isotopic finite-dimensional algebras over finite fields to isomorphic graphs. These functors reduce the cost of computation that is usually required to determine whether two algebras are isomorphic. In order to illustrate their efficiency, we determine explicitly the classification of two- and three-dimensional partial quasigroup rings.

1. Introduction

Graph invariants constitute an interesting tool in Chemistry, Communication or Engineering [1–3]. In Mathematics, one of the topics for which graph invariants have revealed to play an important role is the classical problem of deciding whether two algebras are isomorphic. This problem is usually dealt with by computing the reduced Gröbner basis of the system of polynomial equations that is uniquely related to the structure constants of both algebras. This computation is, however, very sensitive to the number of variables [4] and gives rise to distinct problems of computation time and memory usage even for low-dimensional algebras [5,6]. This paper deals with Graph Theory in order to reduce this cost of computation.

Graph invariants have been proposed in the last years as an efficient alternative to study isomorphisms of distinct types of algebras [7–9]. Nevertheless, the problem of identifying a functor that relates the category of algebras with that of graphs remains still open. Based on a proposal of McKay et al. [10] for identifying isotopisms of Latin squares with isomorphisms of vertex-colored graphs, we describe in Section 3 a pair of graphs that enable us to find faithful functors between finite-dimensional algebras over finite fields and these types of graphs. These functors map isomorphic and isotopic algebras to isomorphic graphs. Reciprocally, any pair of isomorphic graphs is uniquely related to a pair of algebras so that there exists a multiplicative map between them. The main advantage of our proposal, apart from the reduction of the mentioned cost of computation, is the feasibility of studying the possible isomorphism between two given finite-dimensional algebras defined over the same field, whatever the types of both algebras are. As an illustrative example, we focus in Section 4 on the

* Corresponding author.
E-mail addresses: oscfalgan@yahoo.es (O.J. Falcón), rafalgan@us.es (R.M. Falcón), jnvaldes@us.es (J. Núñez), ampacheco@uloyola.es (A.M. Pacheco), villar@us.es (M.T. Villar).

http://dx.doi.org/10.1016/j.cam.2016.09.002

classification of partial quasigroup rings according to the known isotopism classes of partial Latin squares on which they are based.

2. Preliminaries

In this section we expose some basic concepts and results on Graph Theory, isotopisms of algebras, partial Latin squares and Computational Algebraic Geometry that we use throughout the paper. For more details about these topics we refer, respectively, to the manuscripts [11–14].

2.1. Graph theory

A *graph* is a pair $G = (V, E)$ formed by a set V of *vertices* and a set E of 2-subsets of V called *edges*. Two vertices defining an edge are said to be *adjacent*. The *degree* of a vertex v is the number $d(v)$ of edges containing v. The graph G is *vertex-colored* if there exists a partition of V into color sets. The color of a vertex v is denoted as $\text{color}(v)$. An *isomorphism* between two vertex-colored graphs G and G' is any bijective map f between their sets of vertices that preserves collinearity and color sets, that is, such that it maps edges to edges and $\text{color}(f(v)) = \text{color}(v)$, for all vertex v in G.

2.2. Isotopisms of algebras

Two algebras A and A' over a field $\mathbb{K}$ are said to be *isotopic* if there exist three non-singular linear transformations f, g and h from A to A' such that $f(u)g(v) = h(uv)$, for all $u, v \in A$. The triple (f, g, h) is an *isotopism* between A and A'. If $f = g = h$, then this constitutes an *isomorphism*.

The *structure constants* of an n-dimensional algebra A over a field $\mathbb{K}$ of basis $\{e_1, \ldots, e_n\}$ are the numbers $c_{ij}^k \in \mathbb{K}$ such that $e_ie_j = \sum_{k=1}^n c_{ij}^k e_k$, for all $i, j \leq n$. If all of them are zeros, then A is *abelian*. In particular, the n-dimensional abelian algebra is not isotopic to any other n-dimensional algebra.

The *left annihilator* of a vector subspace S of the algebra A is the set $\text{Ann}_{A^-}(S) = \{u \in A \mid uv = 0, \text{ for all } v \in S\}$. Its *right annihilator* is the set $\text{Ann}_{A^+}(S) = \{u \in A \mid vu = 0, \text{ for all } v \in S\}$. The intersection of both sets is the *annihilator* $\text{Ann}_A(S)$.

Lemma 1. *Let (f, g, h) be an isotopism between two n-dimensional algebras A and A', and let S be a vector subspace of A. Then,*

(a) $f(\text{Ann}_{A^-}(S)) = \text{Ann}_{A'^-}(g(S))$.
(b) $g(\text{Ann}_{A^+}(S)) = \text{Ann}_{A'^+}(f(S))$.
(c) $f(\text{Ann}_{A^-}(S)) \cap g(\text{Ann}_{A^+}(S)) = \text{Ann}_{A'}(f(S) \cap g(S))$.

Proof. Let us prove assertion (a). Assertion (b) follows similarly and assertion (c) is a consequence of (a) and (b). Let $u \in g(S)$ and $v \in f(\text{Ann}_{A^-}(S))$. Then, $vu = f(f^{-1}(v))g(g^{-1}(u)) = h(f^{-1}(v)g^{-1}(u)) = h(0) = 0$, because $g^{-1}(u) \in S$ and $f^{-1}(v) \in \text{Ann}_{A^-}(S)$. Hence, $f(\text{Ann}_{A^-}(S)) \subseteq \text{Ann}_{A'^-}(g(S))$. Now, let $u \in \text{Ann}_{A'^-}(g(S))$ and $v \in S$. From the regularity of f, we have that $h(f^{-1}(u)v) = ug(v) = 0$. The regularity of h involves that $f^{-1}(u)v = 0$. Thus, $u \in f(\text{Ann}_{A^-}(S))$ and hence, $\text{Ann}_{A'^-}(g(S)) \subseteq f(\text{Ann}_{A^-}(S))$. □

The *derived algebra* of A is the subalgebra $A^2 = \{uv \mid u, v \in A\} \subseteq A$.

Lemma 2. *Let (f, g, h) be an isotopism between two n-dimensional algebras A and A'. Then, $h(A^2) = A'^2$.*

Proof. The regularity of f and g involves that $f(A) = g(A) = A'$ and hence, $A'^2 = f(A)g(A) = h(A^2)$. □

Let $\cdot$ be a partial binary operation over the set $[n] = \{1, \ldots, n\}$. The pair $([n], \cdot)$ is called a *partial magma* of *order* n. It is *isotopic* to a partial magma $([n], \circ)$ if there exist three permutations α, β and γ in the symmetric group S_n such that $\alpha(i) \circ \beta(j) = \gamma(i \cdot j)$, for all $i, j \leq n$ such that $i \cdot j$ exists. If $\alpha = \beta = \gamma$, then the partial magmas are said to be *isomorphic*. The triple (α, β, γ) is an *isotopism* of partial magmas (an *isomorphism* if $\alpha = \beta = \gamma$).

A *partial magma algebra* $A^{\cdot}$ *based on* a partial magma $([n], \cdot)$ is an n-dimensional algebra over a field $\mathbb{K}$ such that there exists a basis $\{e_1, \ldots, e_n\}$ satisfying that, if $i \cdot j$ exists for some pair of elements $i, j \leq n$, then $e_ie_j = c_{ij}e_{i \cdot j}$ for some non-zero structure constant $c_{ij} \in \mathbb{K} \setminus \{0\}$. If all the structure constants are equal to 1, then this is called a *partial magma ring*.

Lemma 3. *Two partial magma rings are isotopic (isomorphic, respectively) if their respective partial magmas on which they are based are isotopic (isomorphic, respectively).*

Proof. Let $A^{\cdot}$ and A° be two partial magma rings based, respectively, on two isotopic partial magmas $([n], \cdot)$ and $([n], \circ)$. Let $\{e_1, \ldots, e_n\}$ and $\{e'_1, \ldots, e'_n\}$ be the respective bases of these two algebras and let (f, g, h) be an isotopism between their corresponding partial magmas. For each $\alpha \in \{f, g, h\}$, let us define the map $\overline{\alpha}(e_i) = e'_{\alpha(i)}$. Then, $\overline{f}(e_i)\overline{g}(e_j) = e'_{f(i)}e'_{g(j)} = e'_{f(i) \circ g(j)} = e'_{h(i \cdot j)} = \overline{h}(e_{i \cdot j}) = \overline{h}(e_ie_j)$. From linearity, the triple $(\overline{f}, \overline{g}, \overline{h})$ determines an isotopism between $A^{\cdot}$ and A°. If $f = g = h$, then this constitutes an isomorphism. □

Please cite this article in press as: O.J. Falcón, et al., Computation of isotopisms of algebras over finite fields by means of graph invariants, Journal of Computational and Applied Mathematics (2016), http://dx.doi.org/10.1016/j.cam.2016.09.002