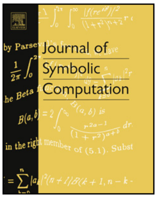
Journal of Symbolic Computation 73 (2016) 153–156

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc



Determining cyclicity of finite modules [☆]

H.W. Lenstra Jr. [a], A. Silverberg [b]

[a] Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands
[b] Department of Mathematics, Rowland Hall, University of California, Irvine, CA 92697, USA

ARTICLE INFO

Article history:
Received 30 December 2014
Accepted 27 March 2015
Available online 12 June 2015

Keywords:
Algebraic algorithms
Finite rings
Cyclic modules

ABSTRACT

We present a deterministic polynomial-time algorithm that determines whether a finite module over a finite commutative ring is cyclic, and if it is, outputs a generator.

1. Introduction

If R is a commutative ring, then an R-module M is cyclic if there exists $y \in M$ such that $M = Ry$.

Theorem 1.1. *There is a deterministic polynomial-time algorithm that, given a finite commutative ring R and a finite R-module M, decides whether there exists $y \in M$ such that $M = Ry$, and if there is, finds such a y.*

We present the algorithm in Algorithm 4.1 below. The inputs are given as follows. The ring R is given as an abelian group by generators and relations, along with all the products of pairs of generators. The finite R-module M is given as an abelian group, and for all generators of the abelian group R and all generators of the abelian group M we are given the module products in M.

Our algorithm depends on R being an Artin ring, and should generalize to finitely generated modules over any commutative Artin ring that is computationally accessible.

[☆] This material is based on research sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750-13-2-0054 and by the Alfred P. Sloan Foundation. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

E-mail addresses: hwl@math.leidenuniv.nl (H.W. Lenstra Jr.), asilverb@uci.edu (A. Silverberg).

http://dx.doi.org/10.1016/j.jsc.2015.06.002
0747-7171/© 2015 Elsevier Ltd. All rights reserved.

Theorem 1.1 is one of the ingredients of our work (Lenstra and Silverberg, 2014; Lenstra and Silverberg, submitted for publication) on lattices with symmetry, and a sketch of the proof is contained in Lenstra and Silverberg (2014). Previously published algorithms of the same nature appear to restrict to rings that are algebras over fields. Subsequently to Lenstra and Silverberg (2014), I. Ciocănea-Teodorescu (2014), using different and more elaborate techniques, greatly generalized our result, dropping the commutativity assumption on the finite ring R and finding, for any given finite R-module M, a set of generators for M of smallest possible size.

See Chapter 8 of Atiyah and Macdonald (1969) for commutative algebra background. For the purposes of this paper, commutative rings have an identity element 1, which may be 0.

2. Lemmas on commutative rings

If R is a commutative ring and $\boldsymbol{a}$ is an ideal in R, let $\mathrm{Ann}_R\,\boldsymbol{a}$ denote the annihilator of $\boldsymbol{a}$ in R. We will use that every finite commutative ring is an Artin ring, that every Artin ring is isomorphic to a finite direct product of local Artin rings, and that the maximal ideal in a local Artin ring is always nilpotent.

Lemma 2.1. *If A is a local Artin ring, $\boldsymbol{a}$ is an ideal in A, and $\boldsymbol{a}^2 = \boldsymbol{a}$, then $\boldsymbol{a}$ is 0 or A.*

Proof. If $\boldsymbol{a}$ contains a unit, then $\boldsymbol{a} = A$. Otherwise, $\boldsymbol{a}$ is contained in the maximal ideal $\boldsymbol{m}$, which is nilpotent. Thus there is an $r \in \mathbb{Z}_{>0}$ such that $\boldsymbol{m}^r = 0$. Now $\boldsymbol{a} = \boldsymbol{a}^2 = \cdots = \boldsymbol{a}^r \subset \boldsymbol{m}^r = 0$. □

Lemma 2.2. *Suppose that A is a finite commutative ring, $\boldsymbol{a}$ is an ideal in A, $\boldsymbol{b} = \mathrm{Ann}_A\,\boldsymbol{a}$, and $\boldsymbol{a} \cap \boldsymbol{b} = 0$. Then:*

(i) $\boldsymbol{a}^2 = \boldsymbol{a}$;
(ii) *there is an idempotent $e \in A$ such that $\boldsymbol{a} = eA$, $\boldsymbol{b} = (1-e)A$, and $A = (1-e)A \oplus eA = \boldsymbol{b} \oplus \boldsymbol{a}$;*
(iii) *if $\boldsymbol{b} = 0$ then $\boldsymbol{a} = A$.*

Proof. Write A as a finite direct product of local Artin rings $A_1 \times \cdots \times A_s$. Then $\boldsymbol{a}$ is a direct product $\boldsymbol{a}_1 \times \cdots \times \boldsymbol{a}_s$ of ideals $\boldsymbol{a}_i \subset A_i$. Assume $\boldsymbol{a}^2 \neq \boldsymbol{a}$. Then there is an i such that $\boldsymbol{a}_i^2 \neq \boldsymbol{a}_i$. Let $\boldsymbol{b}_i = \mathrm{Ann}_{A_i}\,\boldsymbol{a}_i$. Since $\boldsymbol{a} \cap \boldsymbol{b} = 0$, it follows that $\boldsymbol{a}_i \cap \boldsymbol{b}_i = 0$. Since A_i is a local ring, $\boldsymbol{a}_i$ is contained in the maximal ideal of A_i, so $\boldsymbol{a}_i$ is nilpotent. Let r denote the smallest positive integer such that $\boldsymbol{a}_i^r = 0$. Since $\boldsymbol{a}_i \neq 0$ we have $r \geq 2$. Then $\boldsymbol{a}_i^{r-1}$ is contained in $\boldsymbol{a}_i$ and kills $\boldsymbol{a}_i$, so $0 \neq \boldsymbol{a}_i^{r-1} \subset \boldsymbol{a}_i \cap \boldsymbol{b}_i = 0$, a contradiction. This gives (i).

Since A is a finite product of local Artin rings, $\boldsymbol{a}$ is generated by an idempotent e, by Lemma 2.1. Then $\boldsymbol{b} = (1-e)A$ and $A = (1-e)A \oplus eA = \boldsymbol{b} \oplus \boldsymbol{a}$. This gives (ii) and (iii). □

3. Preparatory lemmas

If R is a commutative ring, then a commutative R-algebra is a commutative ring A equipped with a ring homomorphism from R to A. Whenever A is an R-algebra, we let M_A denote the A-module $A \otimes_R M$.

From now on, suppose R is finite commutative ring and M is a finite R-module. Let $\mathcal{S}$ denote the set of quadruples (A, B, y, N) such that:

(i) A and B are finite commutative R-algebras for which the natural map $f : R \twoheadrightarrow A \times B$ is surjective and has nilpotent kernel,
(ii) $y \in M$ is such that the map $B \to M_B = B \otimes_R M$ defined by $b \mapsto b \otimes y$ is an isomorphism and such that $1 \otimes y = 0$ in M_A,
(iii) and N is a submodule of M such that the natural map $N \to M_A$ defined by $z \mapsto 1 \otimes z$ is onto and such that the natural map $N \to M_B$ is the zero map.