Journal of Algebra 489 (2017) 529–551

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

The subpower membership problem for bands ☆

Markus Steindl [a,b,*]

[a] Institute for Algebra, Johannes Kepler University Linz, Altenberger St. 69, 4040 Linz, Austria
[b] Department of Mathematics, University of Colorado Boulder, Campus Box 395, Boulder, CO 80309-0395, United States

ARTICLE INFO

Article history:
Received 20 April 2016
Available online 25 July 2017
Communicated by Derek Holt

MSC:
primary 20M99
secondary 68Q25

Keywords:
Idempotent semigroups
Subalgebras of powers
Membership test
Computational complexity
NP-complete
Quasivariety

ABSTRACT

Fix a finite semigroup S and let $a_1, \dots, a_k, b$ be tuples in a direct power S^n. The subpower membership problem (SMP) for S asks whether b can be generated by $a_1, \dots, a_k$. For bands (idempotent semigroups), we provide a dichotomy result: if a band S belongs to a certain quasivariety, then SMP(S) is in P; otherwise it is NP-complete.
Furthermore we determine the greatest variety of bands all of whose finite members induce a tractable SMP. Finally we present the first example of two finite algebras that generate the same variety and have tractable and NP-complete SMPs, respectively.

1. Introduction

How hard is deciding membership in a subalgebra of a given algebraic structure? This problem occurs frequently in symbolic computation. For instance if F is a fixed field and

☆ Supported by the Austrian Science Fund (FWF): P24285.

* Correspondence to: Institute for Algebra, Johannes Kepler University Linz, Altenberger St. 69, 4040 Linz, Austria.
E-mail address: markus.steindl@colorado.edu.

http://dx.doi.org/10.1016/j.jalgebra.2017.06.034

we are given vectors $a_1, \dots, a_k, b$ in a vector space F^n, we often want to decide whether b is in the linear span of $a_1, \dots, a_k$. This question can be answered using Gaussian elimination in polynomial time in n and k.

Depending on the formulation of the membership problem, the underlying algebra may be part of the input. For example if we are given transformations on n elements, we may have to decide whether they generate a given transformation under composition. These functions belong to the full transformation semigroup T_n on n elements. In this case n and the algebra T_n are part of the input. Kozen proved that this problem is PSPACE-complete [9]. However, if we restrict the input to permutations on n elements, then the problem is in P using Sims' stabilizer chains [3].

In this paper we investigate the membership problem formulated by Willard in 2007 [15]. Fix a finite algebra S with finitely many basic operations. We call a subalgebra of some direct power of S a *subpower* of S. The *subpower membership problem* $\mathrm{SMP}(S)$ is the following decision problem:

$\mathrm{SMP}(S)$
Input: $\{a_1, \dots, a_k\} \subseteq S^n, b \in S^n$
Problem: Is b in the subalgebra of S^n generated by $\{a_1, \dots, a_k\}$?

In this problem the algebra S is not part of the input.

The SMP is of particular interest within the study of the constraint satisfaction problem (CSP) [8]. Recall that in a CSP instance the goal is to assign values of a given domain to a set of variables such that each constraint is satisfied. Constraints are usually represented by constraint relations. In the algebraic approach to the CSP, each relation is regarded as a subpower of a certain finite algebra S. Instead of storing all elements of a constraint relation, we can store a set of generators. Checking whether a given tuple belongs to a constraint relation represented by its generators is precisely the SMP for S. Even though a representation by generators is often very space efficient, it might be inefficient in other aspects. For example, it is not clear whether it is possible to efficiently check that a given tuple belongs to the constraint relation given by generators. Thus it is essential to know the computational complexity of $\mathrm{SMP}(S)$.

Throughout this paper we assume that elements of S consume space 1 and that applying an operation to elements from S takes time 1. This means we need space n to store a tuple from S^n and time n to apply an operation to a set of tuples. Thus the input size of $\mathrm{SMP}(S)$ is $(k+1)n$. Since the size of the subalgebra generated by $a_1, \dots, a_k$ is limited by $|S|^n$, one can enumerate all elements in time exponential in n using a straightforward closure algorithm. This means that $\mathrm{SMP}(S)$ is in EXPTIME for each algebra S. For some algebras there is no faster algorithm. This follows from a result of Kozik [10], who actually constructed a finite algebra with EXPTIME-complete SMP. However, there are structures whose SMP is considerably easier. For example, the SMP for a finite group is in P by an adaptation of Sims' stabilizer chains [16]. Mayr [11] proved that the SMP for Mal'cev algebras is in NP. He also showed that the SMP for every finite Mal'cev algebra which has prime power size and a nilpotent reduct is in P.