Introduction

Throughout this text, rings are assumed to contain a unit element, but are not necessarily commutative. Modules are always left-unital, unless otherwise specified.

The main goal of this PhD thesis is to develop a toolbox for working with finite rings and finite modules within algorithms. The motivation to study problems concerning finite rings and finite modules is twofold. The first reason is a theoretical one and stems from the fundamental nature of the problems that arise. Since we are mostly interested in viewing algorithms as mathematical objects in their own right, the focus will be on deterministic polynomial-time algorithms. The second reason to study these problems refers to the necessity of having as many algorithms as possible available in computer algebra systems to deal with finite rings.

The first chapter of this thesis contains the necessary background theory on algorithms, complexity, rings and modules. Chapters 2 and 3 contain a series of basic algorithms for finitely generated abelian groups and finite rings. These will be used implicitly and extensively in the rest of the algorithms described.

The first algorithmic problem we tackle is the module isomorphism problem. The *module isomorphism problem* can be formulated as follows: design a deterministic algorithm that, given a ring R and two left R-modules M and N, decides in polynomial time whether they are isomorphic, and if yes, exhibits an isomorphism.

Isomorphism problems are some of the most natural algorithmic questions. Given two objects of the same nature, we would like to be able to tell if they are isomorphic, and if so, we would ideally also want to produce an isomorphism. Objects for which isomorphism problems have been extensively studied include graphs, groups and rings. The easy formulation of these problems and their fundamental nature does not however entail that they have a trivial solution. In fact, for many problems of this type, no deterministic polynomial-time algorithms are known ([11, 52, 53]).

Two intermediate results, valuable in themselves, are proved in Chapter 4:

Theorem. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and two finite R-modules M and N, computes a maximum length R-module C that is isomorphic to a direct summand both of M and of N. Moreover, the algorithm computes direct complements of C both in M and in N, together with the corresponding isomorphisms.*

Theorem. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and a finite R-module M, computes a set of generators for M of minimum cardinality.*

Both of these theorems can be used to provide a solution for the module isomorphism problem.

Theorem. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and two finite R-modules M and N, decides whether M and N are isomorphic, and if they are, exhibits an isomorphism.*

Chapter 5 contains a collection of deterministic polynomial-time algorithms for testing properties of rings and modules.

Theorem. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and a finite R-module M, tests whether M is*

(i) *projective,*
(ii) *injective,*
(iii) *simple.*

Theorem. *There exists a deterministic polynomial-time algorithm that, given a finite ring R, tests whether R is*

(i) *simple,*
(ii) *quasi-Frobenius.*

Moreover,

Theorem. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and a finite R-module M, constructs a projective cover and an injective hull of M.*

We also discuss the algorithmic problem of constructively testing for existence of injective and surjective homomorphisms between two finite length modules over a ring R, i.e. the problem of testing for existence and finding such homomorphisms when they do exist. If R is a finite-dimensional algebra over a field, this problem can be cast in the context of matrix completion, and has been shown to be NP-hard. We consider the case where R is a finite ring and one of the modules is either projective or injective over R.

Theorem. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and two finite R-modules M and N, one of which is R-projective, constructively tests for existence of a surjective R-module homomorphism $M \twoheadrightarrow N$.*

Dually:

Theorem. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and two finite R-modules M and N, one of which is R-injective, constructively tests for existence of an injective R-module homomorphism $M \hookrightarrow N$.*

For the remaining cases we obtain negative results:

Theorem. *The problem of deciding existence of an injective module homomorphism between two modules over a finite ring, one of which is projective over that ring, is* NP*-complete.*

A very important class of rings is that of *semisimple rings*. Let R be a ring and M an R-module. Then M is said to be *semisimple* if every R-submodule of M has a direct complement in M. A ring R is said to be *semisimple* if the left-regular (or equivalently right-regular) module is semisimple. Semisimple rings have a lot of structure: everything breaks down in an orderly fashion. Moreover, the Wedderburn theorem gives a complete classification of such rings as finite products of matrix rings over division rings.

The notion of semisimplicity is inextricably linked to that of the *Jacobson radical* of a ring, defined as the intersection of all maximal left ideals. The Jacobson radical of a ring R is a two-sided ideal, and we denote it by $\mathrm{J}(R)$. The rings R and $R/\mathrm{J}(R)$ have the same simple left modules, which suggests that a study of $R/\mathrm{J}(R)$ will reveal much of the structure of R. Moreover, if R is left-artinian, then $\mathrm{J}(R)$ is a nilpotent ideal of R and R is semisimple if and only if $\mathrm{J}(R) = 0$.

When trying to answer questions about left-artinian rings and modules over them, it is often convenient to reduce the problem at hand to the semisimple case, where structures are much more manageable, and then "lift". This places the computation of the Jacobson radical at the heart of many problems. While it can be done deterministically in polynomial time for matrix algebras over a field [15, 18, 27, 75], we cannot expect to have a deterministic polynomial-time algorithm for the general case, since the problem ultimately reduces to finding the squarefree part of an integer (consider the ring $\mathbb{Z}/n\mathbb{Z}$, for some $n \in \mathbb{Z}_{>0}$). In Chapter 6, we attempt to deterministically construct approximations of the Jacobson radical of a finite ring that are "satisfactory" for many practical purposes, that is, two-sided nilpotent ideals such that when we quotient the ring by them, we are left with something that is "almost" semisimple.

The notion used to approximate semisimplicity is that of separability. Given a commutative ring R, an R-algebra S is said to be *separable* over R if S is projective as an $S \otimes_R S^{\mathrm{o}}$-module, where S^{o} denotes the opposite ring of S. A ring is said to be separable if it is separable as a $\mathbb{Z}$-algebra.

Definition. *Let A be a finite ring and $\mathfrak{j}_A \subset A$ an ideal. We say $\mathfrak{j}_A$ is an* approximation of the Jacobson radical *of A if*

(A1) *$\mathfrak{j}_A$ is a two-sided nilpotent ideal of A,*
(A2) *$A/\mathfrak{j}_A$ is finite separable,*
(A3) *$A/\mathfrak{j}_A$ is projective as a module over its prime subring.*

The resulting ring, $A/\mathfrak{j}_A$, has many good properties, e.g. it has "many" projective modules (via *projectivity lift*), it is quasi-Frobenius, it is isomorphic to its opposite as rings. Moreover, finite separable rings can be classified as finite products of matrix rings over certain commutative rings. We show that approximations of Jacobson radicals can be efficiently computed.

Theorem. *There exists a deterministic polynomial-time algorithm that, given a finite ring A, computes an approximation of the Jacobson radical of A.*

We are interested in deterministic polynomial-time algorithms that produce approximations of the Jacobson radical of a finite ring and have the additional property that, when run on two isomorphic rings, they output isomorphic approximations of their Jacobson radicals, even when the ring isomorphism is unknown.

In fact, we exhibit not one, but two algorithms as described by the above theorem. If we denote by $\mathcal{F}$ the class of finite rings, then the two families of ideals $(\mathfrak{j}_A)_{A\in\mathcal{F}}$ and $(\mathfrak{j}'_A)_{A\in\mathcal{F}}$, produced by the two algorithms are functorial under isomorphisms, i.e. if $\phi : A \to B$ is an isomorphism of finite rings, then $\phi(\mathfrak{j}_A) = \mathfrak{j}_B$ and $\phi(\mathfrak{j}'_A) = \mathfrak{j}'_B$.