The Module Isomorphism Problem for Finite Rings and Related Results

Iuliana Ciocănea Teodorescu
Leiden University (Netherlands)

`ciocaneai@math.leidenuniv.nl`

Abstract

Let R be a finite ring and let M, N be two finite left R-modules. We present two distinct deterministic algorithms that decide in polynomial time whether or not M and N are isomorphic, and if they are, exhibit an isomorphism. As by-products, we are able to determine the largest isomorphic common direct summand between two modules and the minimum number of generators of a module. By not requiring R to contain a field, avoiding computation of the Jacobson radical and not distinguishing between large and small characteristic, both algorithms constitute improvements to known results. We have not attempted to implement either of the two algorithms, but have no reason to believe they would not perform well in practice.

Moreover, the second algorithm represents an interesting object *per se*, due to its structure and the techniques it employs. A common approach to this type of problems is to reduce to the semisimple case and then "lift". In our algorithm, we work *as if* the ring were semisimple and we have a list, $S_1, \ldots, S_t$, of candidates for the isomorphism classes of simple modules composing it. During the running of the algorithm, we allow ourselves to be contradicted in our assumption about the simplicity of the S_i, in which case we update our list, quotient the ring by an appropriate two-sided nilpotent ideal and start again. If we are not contradicted, we may still draw conclusions. In this way, there is always a side-exit available and what forces an output in polynomial time is that we cannot take the side-exit too many times.