Splitting full matrix algebras over $\mathbb{F}_q(x)$

May 4, 2016

In this paper we consider the following algorithmic problem. Let $A \cong M_n(K)$ (K is a field) be given by structure constants. Construct an explicit isomorphism between A and $M_n(K)$, or equivalently find a primitive nontrivial idempotent in A. We call this problem the explicit isomorphism problem for the field K.

This problem was solved for several classes of fields. Friedl and Rónyai [1] proposed a polynomial time f-algorithm when K is a finite field. Recall that an f-algorithm is a deterministic algorithm which is allowed to call oracles for factoring polynomials over finite field. The cost of the call is the size of the input. Ivanyos, Karpinski, Rónyai and Saxena [3] proposed a deterministic algorithm algorithm for the same task which runs in polynomial time assuming the dimension of the matrix algebra over K is bounded.

Ivanyos, Rónyai and Schicho [4] considered the case where K is an algebraic number field. They proposed an ff-algorithm (one can also call oracles for factoring integers) which runs in polynomial time assuming the degree of the number field, the discriminant of the number field and the dimension of the matrix algebra are bounded. They introduced techniques from the theory of integer lattices.

In this paper we consider the case $K = \mathbb{F}_q(x)$. We propose a polynomial time f-algorithm which solves this problem. Our main idea is to compute two maximal orders. One over $\mathbb{F}_q[x]$ and one over the subring of $\mathbb{F}_q(x)$ which consists of rational functions where the degree of the numerator is at most the degree of the denominator. The intersection is a finite algebra B which contains a primitive idempotent of A. We prove this fact using lattice reduction over polynomial rings. We can compute a system of primitive idempotents for B. As it turns out one of these idempotents will be a primitive idempotent in A.

An important question would be the case where K is finite extension of $\mathbb{F}_q(x)$ as it is related to factoring Ore polynomials [2]. Using these ideas directly seems to only solve this problem in the small cases, so this still remains an open problem.

References

[1] K. Friedl, L. Rónyai: Polynomial time solutions of some problems in computational algebra; Proceedings of the 17th annual ACM symposium on Theory of computing (1985). Providence, Rhode Island, United States: ACM. pp. 153-162.

[2] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro: Factoring Ore polynomials over $\mathbb{F}_q(t)$ is difficult; (2015)Preprint arXiv:1505.07252.

[3] G. Ivanyos, M. Karpinski, L. Rónyai, N. Saxena: Trading GRH for algebra: algorithms for factoring polynomials and related structures; Matematics of Computation 81 (2012), pp. 493-531.

[4] G. Ivanyos, L. Rónyai, J. Schicho: Splitting full matrix algebras over algebraic number fields; Journal of Algebra 354 (2012), pp. 211-223.