Automorphisms of Rings and Applications to Complexity

Nitin Saxena

February 11, 2006

Abstract

Rings are fundamental mathematical objects with two operations, addition and multiplication, suitably defined. A known way of studying the structure of rings is to consider automorphisms of rings. In my PhD thesis I consider finite dimensional rings represented in terms of their additive basis and study the computational complexity of various automorphism problems of rings in this representation. We show that this framework of ring automorphisms has connections to many well known problems in computer science like primality testing, integer factoring, polynomial factoring, graph isomorphism, polynomial equivalence and identity testing.

Primality testing is the problem of checking whether a given number n is prime or not, in time polynomial in the size of the input. Since a long time, efficient but *randomized* algorithms are known for this problem. We considered the ring $R := Z_n[x]/(x^r - 1)$ having the property that when n is prime then the Frobenius map $\sigma_n : f(x) \mapsto f(x)^n$ is an automorphism of the ring R. We show that if for various "small" r's σ_n is an automorphism of R then n is prime, thus, giving us a deterministic polynomial time primality test [AKS04].

Integer factoring is the problem of finding a nontrivial factor of a given number n. No efficient algorithm is known for this problem yet. We show that integer factoring randomly reduces to computing the number of automorphisms of a given ring. Integer factoring also randomly reduces to the problems of finding nontrivial ring automorphisms and finding ring isomorphisms.

Polynomial factoring is the problem of finding a nontrivial factor of a univariate polynomial $f(x)$ over a given finite field $\mathbb{F}_q$. There are many randomized algorithms for factoring polynomials but no efficient deterministic algorithm is known. We consider the ring $R := \mathbb{F}_q[x]/(f(x))$ and show, assuming the Extended Riemann Hypothesis, that factoring $f(x)$ reduces to the problem of finding a nontrivial automorphism of R.

Graph isomorphism is the problem of checking whether two given undirected graphs are isomorphic or not, in time polynomial in the size of the input. No efficient algorithm is known for this problem to date. This problem however lies in the complexity class NP $\cap$ coAM and not believed to be NP-hard. We show that graph isomorphism reduces to the ring isomorphism problem and hence also reduces to computing the number of automorphisms of a ring [KS05].

Polynomial equivalence is the problem of checking whether two given polynomials over a field $\mathbb{F}$ can be made equal by applying an invertible linear transformation on the variables. We show that even the case of homogeneous cubic polynomials, called cubic forms, is "interesting" in the sense that it is related to the isomorphism problems of graphs and $\mathbb{F}$-algebras. Specifically, we prove that graph isomorphism reduces to $\mathbb{F}$-algebra isomorphism which in turn reduces to cubic form equivalence [AS05, AS06].

Identity Testing is the problem of checking whether a given arithmetic circuit $\mathcal{C} \equiv 0$. No deterministic polynomial time algorithm is known yet for this problem. We consider a restricted case of it – when $\mathcal{C}$ is a depth 3 circuit with bounded top fanin – and give the first deterministic polynomial time algorithm by using the properties of local rings [KS06].

References

[AKS04] M. Agrawal, N. Kayal, N. Saxena. *PRIMES is in P.* Annals of Mathematics, **160**, 2004, 1-13.

[AS05] M. Agrawal, N. Saxena. *Automorphisms of Finite Rings and Applications to Complexity of Problems.* STACS'05, Springer LNCS **3404**, 2005, 1-17.

[AS06] M. Agrawal, N. Saxena. *Equivalence of* $\mathbb{F}$*-algebras and cubic forms.* STACS'06, Springer LNCS, 2006.

[KS05] N. Kayal, N. Saxena. *On the Ring Isomorphism & Automorphism Problems.* Proceedings of 20^{th} IEEE Conference on Computational Complexity, 2005, 2-12.

[KS06] N. Kayal, N. Saxena. *Polynomial Identity Testing for Depth* 3 *Circuits.* submitted to CCC'06.