Rings and Integer Lattices in Computer Science: A Barbados Workshop Proposal

Manindra Agrawal

Finite rings, an algebraic structure, and integer lattices, a geometric structure, play a very useful role in the design of algorithms for algebraic and number theoretical problems. Some examples are polynomial factorization, primality testing, breaking cryptosystems. Nevertheless, one feels that the full potential of these has not been exploited yet in algorithm design. The aim of this workshop is to introduce these structures and computational problems related to them, show how they help in solving some problems, and finally, discuss how they may help in solving a number of other important problems.

1 Finite Rings

Some of the computational problems related with finite rings are

- Given ring R, does it have a non-trivial automorphism?
- Given rings R and S, are they isomorphic?
- Given ring R, compute the entire automorphism group of R.

One can show that the first of these problems is in P, the second is in $\mathrm{NP} \cap \mathrm{coAM}$, and the third is in $\mathrm{P}^{\mathrm{AM} \cap \mathrm{coAM}}$. Further, a number of interesting problems, such as Graph Isomorphism, Integer Factoring, Polynomial Factoring, reduce deterministically to the third problem (GI reduces to the second one, too).

For certain special class of rings these problems admit polynomial time algorithms, and these algorithms play a crucial role in the algorithms for Polynomial Factoring and Primality Testing.

2 Integer Lattices

Integer lattices are integer linear combinations of vectors in n-dimensional spaces. They give rise to a regular tiling of the underlying space. Many properties of numbers, especially related to magnitude, can be derived by studying the structure of appropriate lattices.

The most important computational problems related to lattices are:

- Given a lattice $\mathcal{L}$, find the shortest vector in $\mathcal{L}$.
- Given a lattice $\mathcal{L}$ and a vector v, find the vector in $\mathcal{L}$ that is closest to v.

Both these problems are known to be NP-hard. The famous LLL algorithm gives an approximate solution to the first problem. Even such an approximate solution finds several applications: in Polynomial Factoring, in breaking knapsack-based cryptosystems, in breaking low-exponent RSA, etc.

3 Some Potential Applications

Here I list some problems whose solutions may lie in our understanding of the above two structures.

Graph Isomorphism. One can associate a couple of (non-abelian) rings with a graph. Both the rings can be efficiently computed; one of them provides a coloring of the edges of the graph while the other contains all the automorphisms of the graph. These rings, interacting with graph-theoretic operations, exhibit a very rich structure. Can one exploit this structure to compute all the automorphism of a graph?

Derandomizing Isolation Lemma. The isolation lemma is used to assign minimum weight to one vector out of an exponentially large set. This lemma has found use in several places. A derandomization of the lemma when the set of vectors satisfy some nice properties will have far reaching consequences. For example, it would imply NSPACE($s(n)$) = USPACE($s(n)$), computing matching in a graph is in NC, NP is in $\oplus$P, etc. The sets with nice properties can be defined as *the set of closest vectors to origin in a small dimensional affine lattice*. Can one, using the properties of lattices, find a way of derandomizing the weight assignment to vectors?

Integer Factoring. Short vectors in a lattice are a crucial ingredient in deterministic algorithm for factoring polynomials over rationals. Also, short lattice vectors help break low-exponent version of RSA. Both these problems share some similarities with integer factoring. So, the question is, can we use lattices to help in integer factoring? So far, no fast algorithm for integer factoring has used lattices. There are some ways of associating lattices with the problem, however, it is not clear if any of them leads to a fast algorithm.