Abstract

The study of counting complexity classes has been a very fruitful and promising area in complexity theory. This study has given important insights into the inherent complexity of many natural computational problems. Problems arising from group theory have been studied by many researchers. These problems are interesting from the complexity-theoretic viewpoint since the complexity status of many of these problems is not settled.

In this dissertation, we study some problems from group theory in the context of counting complexity. More specifically, we place some basic computational group-theoretic problems in counting classes of low complexity. These results help in giving further insights into the intriguing nature of the complexity of these problems.

This thesis consists of two parts. In Chapter 4, which comprises the first part, we study the complexity of three basic computational group-theoretic problems over black-box groups. The problems are Membership Testing, Order Verification and Isomorphism Testing. These are computational problems for which no polynomial-time algorithms exist. It was shown that over general black-box groups, Membership Testing is in NP $\cap$ co-AM, Order Verification is in AM $\cap$ co-AM, and Isomorphism Testing is in AM [BS84, Bab92]. We show that these problems, over *solvable* black-box groups, are in the counting class SPP. The proof of this result is built on a constructive version of the fundamental theorem of finite abelian groups. The class SPP is known to be *low* for the counting classes PP, $\mathrm{C_=P}$ and $\mathrm{Mod}_k\mathrm{P}$ for $k \geq 2$ [FFK94]. Since it is unlikely that the class NP is contained in SPP, these upper bounds give evidence that these problems are unlikely to be hard for NP.

In the second part of the thesis we study the problem of computing a generator set of an *unknown* group, given a membership testing oracle for the group. Because of the close relation of this problem with concept learning, we study this problem in the framework of learning theory. In Chapter 5, for analyzing the complexity of learning, we introduce a new model of exact learning called the *teaching assistant* model. This

model can be seen as an enhancement of Angluin's [Ang88] exact learning model. The main ingredient of this model is the notion of a teaching assistant which acts as an intermediate agent between the learner and the teacher. The power of this model for studying the complexity of various concept classes, comes from the fact that it is possible to define *classes* of teaching assistants. These classes are analogous to the known complexity classes. The teaching assistant classes of main interest to us are the ones analogous to the counting complexity classes SPP and LWPP. In Chapter 5, after giving detailed definitions of all the notions involved in this model, we study the complexity of learning three representation classes in this model. These are the classes SYM of permutation groups, $\mathrm{LS}(p)$ of linear spaces over the finite field of size p and the class 3-CNF of boolean functions represented in conjunctive normal form where each clause has at most three literals. We show that the class SYM is learnable with an LWPP-assistant and $\mathrm{LS}(p)$ is learnable with an SPP-assistant. On the other hand, we also show that 3-CNF is not learnable with an SPP-assistant (LWPP-assistant) unless NP $\subseteq$ SPP (respectively, NP $\subseteq$ LWPP). These containments are unlikely. Motivated by these results, in Chapter 6 we define more assistant classes and prove absolute separations among these assistant classes. For separating various assistant classes we use some natural subclasses of the representation class SYM.

All the results leading to this dissertation have been published. The results that we show in Chapter 4 have appeared in [AV97b, Vin97]. The results proved in Chapters 5 and 6 have appeared in [AV96] and [AV97a] respectively.