Abstract

In this thesis, we study algorithms and data structures for problems related to group theory. We design linear and nearly linear-time algorithms for the group isomorphism problem for some restricted group classes. We also design space efficient data structures for groups and compact data structures for Dedekind groups and finite rings.

Given two objects, the problem of checking whether they have the same structure or not is known as the isomorphism problem. Two groups are said to be isomorphic if and only if there exists a bijective homomorphism from one group to the other. Given two input groups by Cayley tables, deciding if the given groups are isomorphic is known as the group isomorphism problem. The group isomorphism problem is polynomial-time reducible to the graph isomorphism problem. The graph isomorphism problem is unresolved, a well-known problem in the field of theoretical computer science and it is interesting to many researchers due to its complexity status. Apart from its connection to the graph isomorphism problem, the group isomorphism problem is also of independent interest. Several attempts have been made in the past to solve the problem efficiently. Designing efficient algorithms for restricted group classes have been explored to a great extent in the past. Several restricted group classes admit polynomial-time algorithms for the group isomorphism problem. We study the group isomorphism problem for restricted group classes. Kavitha gave a linear-time isomorphism algorithm for abelian groups (JCSS 2007). Although there are isomorphism algorithms for certain nonabelian group classes, the complexities of those algorithms are usually super-linear. We design linear and nearly linear-time isomorphism algorithms for some nonabelian groups. In the process, we also design efficient algorithms for several other group theoretic problems. More precisely,

- We design a linear-time algorithm to factor Hamiltonian groups. This allows us to obtain an $\mathcal{O}(n)$ algorithm for the isomorphism problem of Hamiltonian groups, where n is the order of the groups.
- We design a nearly linear-time algorithm to find a maximal abelian direct factor of an input group. As a byproduct we obtain an $\tilde{\mathcal{O}}(n)$ isomorphism for groups that can be decomposed as a direct product of a nonabelian group of bounded order and an abelian group, where n is the order of the groups.
- We observe that testing normality, computing the center of a group, finding a logarithmic sized generating set, computing quotient groups for groups given by their Cayley table could be done in linear or nearly linear-time.

Next, we study space efficient data structures for groups and rings. Our aim in this part is to develop space efficient data structures for groups and finite rings that can answer multiplication queries (and addition queries for rings) quickly. We focus on designing data structures in the standard random access memory (RAM) model and its variants defined in the past. To represent the Cayley table of a group of order n in the RAM model it needs $\mathcal{O}(n^2)$ words. A multiplication query in the Cayley table representation can be answered in time $\mathcal{O}(1)$. Therefore, to ask if

there is a $o(n^2)$ space representation of groups that still has $\mathcal{O}(1)$ query-time is an interesting question. We proved that for any δ with $1/\log n \leq \delta \leq 1$, there is an $\mathcal{O}(n^{1+\delta}/\delta)$ space representation with $\mathcal{O}(1/\delta)$ query-time for groups of order n. We also show that there are $\mathcal{O}(n)$ space representations with logarithmic query-time for simple groups and several group classes specified as a semi-direct product, where n is the group size.

There is a computational model for a group representation described by Farzan and Munro (ISSAC'06). Farzan and Munro proved that abelian groups can be represented in this model with $\mathcal{O}(1)$ space and $\mathcal{O}(1)$ query time. They asked if their result can be extended to categorically larger group classes. For Hamiltonian groups and some other classes of groups, we construct data structures with constant query-time in their model.

A data structure that achieves the optimum information theoretic lower bound asymptotically is known as a compact data structure. Farzan and Munro (ISSAC'06) gave an information theoretic lower bound of $n \log n$ bits to store a group of size n. This lower bound implies an $\Omega(n)$ lower bound on the number of words required to store a group in word-RAM model.

For functions $s, t : \mathbb{N} \longrightarrow \mathbb{R}_{\geq 0}$, we say that a data structure is *an* $(\mathcal{O}(s), \mathcal{O}(t))$-*data structure* if it uses $\mathcal{O}(s)$ space and answers a query in $\mathcal{O}(t)$ time. Except for cyclic groups it was not known if we can design $(\mathcal{O}(n), \mathcal{O}(1))$-data structure for interesting classes of groups. We achieve information theoretic lower bound by designing $(\mathcal{O}(n), \mathcal{O}(1))$-data structures for several classes of groups and for *any* ring. More precisely, we design $(\mathcal{O}(n), \mathcal{O}(1))$-data structures for the following algebraic structures with n elements: Dedekind groups, groups whose indecomposable factors admit $(\mathcal{O}(n), \mathcal{O}(1))$-data structures, groups whose indecomposable factors are strongly indecomposable, groups defined as a semidirect product of groups that admit $(\mathcal{O}(n), \mathcal{O}(1))$-data structures and finite rings.