PROBABILISTIC ALGORITHMS IN GROUP THEORY

John Reif*

Aiken Computation Laboratory
Division of Applied Sciences
Harvard University
Cambridge Massachusetts

0. ABSTRACT

A finite group $G$ is commonly presented by a set of elements which generate $G$. We argue that for algorithmic purposes a considerably better presentation for a fixed group $G$ is given by random generator set for $G$: a set of random elements which generate $G$. We bound the expected number of random elements required to generate a given group $G$.

Our main results are probabilistic algorithms which take as inputs a random generator set of a fixed permutation group $G \subseteq S_n$. We give $O(n^3 \log n)$ expected time sequential RAM algorithms for testing membership, group inclusion and equality. Our bounds hold for any (worse case) input groups; we average only over the random generators representing the groups. Our algorithms are two orders of magnitude faster than the best previous algorithms for these group theoretic problems, which required $O(n^5)$ time even if given random generators.

Furthermore, we show that in the case the input group is a 2-group with a random presentation, then those group theoretic problems can be solved by a parallel RAM in $O((\log n)^3)$ expected time using $n^{\Omega(1)}$ processors.

1. INTRODUCTION

1.1 Group Inference and Representation by Random Examples

In informal mathematical discourse, we often make use of examples to illustrate general principles; and in many cases this suffices to convey the essential ideas. For instance, Euclid never formally stated his algorithm for computing GCD but instead explained it by a series of example computations. On the other hand, a student may illustrate comprehension of a general principle, say Euclid’s algorithm, by producing some examples.

The fields of Inductive Inference and Combinatorial Enumeration concern the dual problems of inference of a combinatorial structure from examples, and generation of sample examples of a given combinatorial structure, respectively. In Section 2, we investigate these problems when the combinatorial structure of interest is a finite group, and the samples are random, with independent uniform distribution. We give upper bounds on the number of random elements of $G$ required to generate a fixed group (generally, the required number of random samples is a logarithm of the group’s order). As an interesting example, consider the group of all permutations of the RUBIC’S cube. Our results imply this group can be generated (with high likelihood) by a very small number of random permutations. Furthermore, the results allow us to verify (within high likelihood) the correctness of a “solution method” to RUBIC’s cube by applying the “solution method” on a small number of random permutations of RUBIC’s cube.

1.2 Group Theoretic Problems

The fundamental groups problems which will concern us are:

1. Group Membership: given an input element $x$, and a group $G$, test $x \in G$.

In these problems, a group is normally assumed to be presented by a sequence of generators. We further assume that a group is randomly presented in the sense defined below.

Let a random generator set of size $k$ for group $G$ be a set of $k$ random, independently chosen elements $g_1, \ldots, g_k$ of $G$, with the condition that $g_1, \ldots, g_k$ generate $G$. We say $<g_1, \ldots, g_k>$ is a random presentation of $G$.

A probabilistic algorithm $A$ for a group problem takes as input a random generator set of a given group. The expected time complexity of $A$ is the average time of $A$ over random generator sets, given worse case groups.

Section 2.4 describes a probabilistic algorithm due to [Bahal, 79] for constructing a strong generator sequence for a randomly presented group.

We also discuss in Sections 2.5 and 2.6 known algorithms for group membership testing, group inclusion, group equality, and random element generation which require strong generator sequences.

* This work was supported by Office of Naval Research Contract N00014-80-C-0647.
1.3 Probabilistic Algorithms for Permutation Groups

The real motivation of our work, and our strongest results, are efficient probabilistic algorithms for the permutation group problems: membership, inclusion, and equality.

[Sims, 78] first gave a well known decision algorithm for these permutation group problems using a construction known as the Sims' Table; others have found it to be very efficient in practice. However, in the worst case, Sims' algorithms were exponential time. [Pursley, Hopcroft, and Luk, 81] later modified Sims' algorithm to yield $O(n^6)$ worst case time bounds for these problems. Still further work by [Jerrum, 82] reduced these worst case time bounds to $O(n^5)$. These worst case time bounds seem to be much larger than would be acceptable in practical applications. This situation motivated us to investigate the expected time complexity of permutation group problems.

Our main results are $O(n^{3\log n})$ expected sequential time probabilistic algorithms for permutation group membership, inclusion, and equality. Our time bounds $O(n^{3\log n})$ are only exceeded with probability $< n^{-\alpha}$ for some constant $\alpha > 1$ that can be set arbitrarily large. In comparison, the previously sighted algorithms for these permutation group problems have expected time complexity which is the same as their worst case complexity $O(n^5)$.

1.4 Parallel Algorithms in Group Theory

We also investigate the use of parallelism for group theoretic problems. Our goal is efficient parallel algorithms requiring polylog time, polynomial number of processors. In Section 4 we give efficient parallel algorithms for the orbits and block systems of permutation groups. A 2-group is a permutation group whose elements are all of order of a power of 2; they arise naturally since a 2-group is a subgroup of automorphisms of binary trees and furthermore the automorphism group of any trivalent graph with a fixed vertex is a 2-group, see [Lukas, 81]. We give in Section 5 efficient parallel algorithms for the problems of membership, inclusion and equality for 2-groups. Our parallel 2-group membership algorithms makes interesting use of our probabilistic techniques: it takes as input a random generator set of a given 2-group, and constructs from them a tower of $O(\log n)$ subgroups with which it is possible to do efficient parallel membership tests.

The parallel complexity of the permutation group membership problem remains open; it is neither known to be log-space complete, for deterministic polynomial time, nor is there a known polylog depth algorithm for group membership. Recently [McKenzie and Cook, 83] have given a polylog time parallel algorithm for Abelian permutation group membership. Their results, and our probabilistic parallel algorithm for 2-group membership, are the only positive results in this regard.

2. PROBABILISTIC ALGORITHMS FOR FINITE GROUPS

2.1 Preliminary Definitions

Let $G$ be a group specified by presenting a finite list of generators, as $G = \langle g_1, \ldots, g_k \rangle$. We often assume $G$ has a finite tower of subgroups $G_0 \supseteq G_1 \supseteq \cdots \supseteq G_h$, where $G_0 = G$ and $G_h = 1$ contains only the identity element. The tower has height $h$. For each $i = 1, \ldots, h$ let $E_i$ be an equivalence relation such that $\forall x, y \in G_{i-1}$, $x E_i y$ iff $y^{-1}x \in G_i$. The blocks of each $E_i$ are the collection of cosets of $G_i$ in $G_{i-1}$, denoted by the quotient $G_{i-1}/G_i$. Let $R_i$ be a complete set of coset representatives for $G_{i-1}/G_i$, i.e., a set containing exactly one element from each coset of $G_{i-1}/G_i$. Since $G = (G_0/G_1)(G_1/G_2)\cdots(G_{h-1}/G_h)$, the sequence of sets $R_1, \ldots, R_h$ is called a sequence of generators for the group $G$, with respect to this subgroup tower.

2.2 Elementary Properties of $\text{RAND}(G)$

We will denote by $\text{RAND}(S)$ the uniformly distributed random variable giving random elements of a set $S$ (with equal probability). If $x_1, x_2$ are random variables, let $x_1 \equiv x_2$ if they have the same probability distribution function.

**Lemma 2.1.** If $G$ is a group and $x \in G$, then $\text{RAND}(G) \equiv x \cdot \text{RAND}(G)$.

For a proof, observe that the function $\pi_x(y) = xy^{-1}$ is 1-1.

**Lemma 2.2.** Let $G'$ be a subgroup of group $G$ and let $R$ be a complete set of coset representatives for $G/G'$. Then $\text{RAND}(G) \equiv \text{RAND}(R)^{-1} \cdot \text{RAND}(G')$.

**Proof.** By Lagrange's theorem, each coset of $G/G'$ has the same size, so $\text{RAND}(G)$ has equal probability of being in any given coset of $G/G'$, say $A$. By definition $\text{RAND}(R)^{-1}$ also has this property. But producing an element of $A$ by an element of $G'$ keeps us in the same coset $A$. Hence $\text{RAND}(R)^{-1} \cdot \text{RAND}(G')$ has the same probability of being in $A$ as does $\text{RAND}(G)$. By definition,