

Decomposing groups in polynomial time

Neeraj Kayal (Advisor), Timur Nezhmetdinov

July 16, 2008

Definition 1. (Group) A group G is a set together with a binary operation $\langle \cdot \rangle: G \times G \mapsto G$ which satisfies the following properties:

1. $\langle \cdot \rangle$ is associative
2. There exists $e \in G$ such that $e \cdot g = g \cdot e = g$ for every $g \in G$
3. For every $g \in G$, there is $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1}g = e$.

Definition 2. (Direct product) *We say that $G = A \times B$ where $A \leq G$, $B \leq G$ when*

1. for every $g \in G$, there is a unique pair $a \in A$, $b \in B$, such that $g = a \cdot b$

2. if $a_1, a_2 \in A$, $b_1, b_2 \in B$, then $(a_1 \cdot b_1) \cdot (a_2 \cdot b_2) = (a_1 \cdot a_2) \cdot (b_1 \cdot b_2)$.

The problem is to find an algorithm to efficiently decompose a given (finite) group as a direct product of its subgroups.

The algorithm must accept the Cayley table of the group G as its input and it must return the lists of elements of each of the factors of the decomposition where each of the factors is itself indecomposable. The running time of the algorithm must be bounded by a polynomial function in the size of the group G .

Notice that it would suffice to find an algorithm to decompose G as a (non-trivial) direct product of *two* of its subgroups: $G = A \times B$. Then we can repeat the algorithm on A and B . Eventually we will find the decomposition of G as a direct product of indecomposable subgroups.

The Remak-Krull-Shmidt theorem states that given two decompositions of a group as a direct product of indecomposable subgroups $G = G_1 \times \cdots \times G_t$ and $G = H_1 \times \cdots \times H_s$, then $t = s$ and after reindexing $G_i \cong H_i$ for all i . In other words, all complete decompositions of G are structurally identical. In this sense the output of our algorithm is determined by the input.

Outline of the algorithm to find a decomposition $G = A \times B$:

- G is abelian
- A is known
 - B is abelian
 - B is nonabelian
- A is unknown
 - B is abelian
 - B is nonabelian

When G is abelian the fundamental theorem of finite abelian groups applies.

Theorem 1. *Every finite abelian group is a direct product of cyclic subgroups of prime power order.*

In fact the theorem is effective. So for this case we already have an algorithm.

The case when A is unknown and B is nonabelian.

Definition 3. *We say that two conjugacy classes C and D commute when for every pair $c \in C$ and $d \in D$, the c and d commute. We say that a conjugacy class E is a product of C and D if C and D commute and $E = \{c \cdot d | c \in C, d \in D\}$.*

Definition 4. *A conjugacy class of G is called irreducible if it is neither a conjugacy class of an element from the center, nor a product of two other conjugacy classes.*

Definition 5. (Graph of a Group) *The graph Γ_G has irreducible conjugacy classes as its nodes and the two nodes are connected iff the corresponding conjugacy classes don't commute.*

Observations:

- Each irreducible conjugacy class of $G = G_1 \times \cdots \times G_t$ is an irreducible conjugacy class of one of G_i for some i .
- The irreducible conjugacy classes of G_i commute with the irreducible conjugacy classes of G_j when $i \neq j$.
- This implies that each of G_i gives rise to at least one connected component of Γ_G .
- The irreducible conjugacy classes of G_i generate G_i .

This motivates us to find the connected components of Γ_G whose nodes are the conjugacy classes of G_i for every i . We have the following results:

Proposition 1. *If the center of G is trivial, then each of the connected components corresponds to (generates) each of G_i .*

This gives us the decomposition of G .

Proposition 2. *The number of connected components is bounded by $\log |G|$.*

This means that we can iterate over all partitions of the set of components and find the partition which corresponds to some decomposition $G = A \times B$. This will give us a decomposition of $G/C = A/C \times B/C$ (C is the center of G). The problem remains to “lift” this decomposition.