

Generating set-checking reduces to membership testing

From Groupprops

Membership testing problem (co-nondeterministic)

Recall that in the membership testing problem, we are given a subset A of G and are required to formulate a test that will take in an element of G and output whether that element is in the subgroup H generated by A .

The generating set-checking problem has a co-nondeterministic reduction to the membership testing problem in the following sense. If a given subset does *not* generate the whole group, then we can find a short proof of the fact invoking the membership testing problem. Namely, pick an element $g \in G$ that is *not* in the subgroup generated by the A , and then prove that it actually is not in the subset by invoking the membership testing problem.

Generating set-finding problem

If we can *find* another set B that is also a generating set for the group, then the problem of checking whether A is a generating set can be solved by invoking the membership testing problem a few times and taking the AND of all the outputs. This gives us a polynomial-time positive truth table reduction from generating set-checking to membership testing.

The idea is as follows: Check that every $b \in B$ is in the subgroup generated by A

Retrieved from "https://groupprops.subwiki.org/w/index.php?title=Generating_set-checking_reduces_to_membership_testing&oldid=5252"

-
- This page was last modified on 7 May 2008, at 23:38.
 - This page has been accessed 375 times.
 - Content is available under Attribution-Share Alike 3.0 Unported unless otherwise noted.