A FAST ALGORITHM FOR THE CONJUGACY PROBLEM ON GENERIC BRAIDS

KI HYOUNG KO

Recently the braid groups have become a potential source for cryptography, especially, for public-key cryptosystems. The braid groups have two important features that are useful for cryptography. Each word can be quickly put into a unique canonical form, which provides a fast algorithm not only for the word problem but also for the group operation. On the other hand no polynomial-time solution to the conjugacy problem in the braid group is known, which provides many interesting one-way functions for public-key cryptosystems. In this talk, we show that there is a polynomial-time solution to the conjugacy problem for generic braids that are either pseudo-Anosov braids or random braids.

Korean Advanced Institute of Science and Technology