Scopus

Documents

Khan, M.A., Mohammad, N., Muhammad, S., Ali, A.

A mining based approach for efficient enumeration of algebraic structures

(2015) *Proceedings of the 2015 IEEE International Conference on Data Science and Advanced Analytics, DSAA 2015*, art. no. 7344827, .

Abstract
Algebraic structures are well studied mathematical structures in abstract algebra with applications in many fields of computer security such as cryptography and authentication. Generating such structures is computationally very expensive because of the huge number of permutations. Also, many of these permutations are redundant as they are symmetrically equivalent. The symmetry breaking (finding symmetrically equivalent structures) is also a computationally challenging task. In this paper, we present a mining based approach for symmetry breaking in algebraic structures. The approach reduces the number of redundant structures by identifying rules based on recurring patterns in the previously known structures. These rules are then used as constraints in a leading constraint solver (Google's or-tools). When applied to IP loop, a special class of algebraic structures, these rules reduced the number of redundant solutions resulting in significant time improvement. © 2015 IEEE.

2-s2.0-84962809886
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus