A Computation Method for Finding Boolean Gröbner Basis Based on Divide and Conquer Algorithm

Sugi Guritman, Teduh Wulandari, Jaharuddin. and Siswandi*

Division of Pure Mathematics
Department of Mathematics
Faculty of Mathematics and Natural Sciences
IPB University
Jln. Meranti, Kampus IPB Dramaga, Bogor, Indonesia, 16680

Abstract

A Gröbner basis is a basis in a ring of multivariate nonlinear polynomials over a field of numbers. The basis has certain properties that allow simple algorithmic solutions for many fundamental problems in mathematics, and natural and technical sciences. In this paper, we propose an algorithm for computing Gröbner basis in binary multivariate polynomial ring $\mathbb{F}_2[x_1, x_2, ..., x_n]$ and for which the main goal is to develop a computation method for solving binary multivariate nonlinear systems. Here, we apply the well-known divide and conquer recurrence as the fundamental idea of the method in which case the usual Buchberger algorithm is applied only at the end of the combining phase. For data representation, we present a new approach in which every single polynomial in the ring can be considered to be a boolean object. So, in a symbolic computation perspective, the polynomial can be represented as a member of a power set of integers and these integers represent the variable symbol of the polynomial. With this point of view, details of the algorithm can be stated in algebraic computation codes of sets and their operations. At the end of the paper, we give a general complexity of the algorithm and also present some facts from the implementation aspect.

Keywords: Boolean Gröbner basis, Divide and conquer algorithm, Set representation, Symbolic computation.

AMS Classif: Primary 03D25, 03C62; Secondary 03G75, 03H15, 13L05, 68W30, 12L15.

Thanks: This paper is in final form and no version of it will be submitted for publication elsewhere.

*sugigu@apps.ipb.ac.id, teduhma@apps.ipb.ac.id, jaharuddin@apps.ipb.ac.id, and siswandi@apps.ipb.ac.id