An Efficient Algorithm for Decomposing Boolean Polynomials and Its Applications

A.V. Trepacheva (CSC SFEDU, Rostov-on-Don)
E-mail address: alina1989malina@yandex.ru

We present an efficient and general algorithm for decomposing Boolean polynomials of the same arbitrary degree. Time complexity of the algorithm is polynomial. The algorithm essentially exploits Grobner basis construction for specific ideal. The paper considers using involutive algorithm for this purpose. Also this paper considers applications of decomposing Boolean polynomials to cryptography and Boolean circuits optimisation.

Эффективный алгоритм декомпозиции булевых полиномов и его приложения

А.В. Трепачева (ЮГИНФО ЮФУ, Ростов-на-Дону)
E-mail address: alina1989malina@yandex.ru

Предлагается алгоритм декомпозиции системы булевых полиномов одинаковой степени. Алгоритм работает за полиномиальное время и использует в качестве составляющей построение базиса Грёбнера специального идеала. Рассматривается вопрос применения инволютивного алгоритма на данном шаге. Рассматриваются криптографические приложения декомпозиции булевых полиномов, а также приложения для оптимизации булевых схем.