

Операторная классификация булевых функций

С. Ф. Винокуров и А. С. Казимиров

Число булевых функций растет быстро при увеличении числа переменных, поэтому иногда для исследований функции удобно объединять в классы эквивалентности. Одним из способов задания классов эквивалентности является использование групп преобразований. Задача построения полной классификации состоит в нахождении классов эквивалентности (или их представителей) относительно таких групп.

В настоящее время задача построения классификаций булевых функций по различным группам преобразований имеет широкие приложения: от задач логического синтеза до криптографии [1].

Одним из способов задания булевых функций является полиномиальное представление — в виде суммы по модулю 2 произведений переменных или их отрицаний.

При исследовании полиномиальных представлений интересны преобразования, которые сохраняют некоторые свойства полинома. Одним из свойств полиномов, представляющих практический интерес, является сложность — количество слагаемых. Среди преобразований, сохраняющих сложность полиномов, наиболее исследованной является группа преобразований, состоящая из операций двух видов: перестановок переменных и замены переменных их отрицаниями (называемая группой Джевонса).

В докладе рассматривается группа, являющаяся расширением группы Джевонса и сохраняющая сложность полиномов. Эта группа была описана с использованием операторного языка [2] и названа группой операторных преобразований.

Для группы операторных преобразований решена задача перечисления — одна из подзадач классификации, заключающаяся в нахождении числа классов эквивалентности.

Литература

1. Логачев О.А., Сальников А.А., Яценко В.В. Булевы функции в теории кодирования и криптологии — М.: МЦНМО, 2004. — 470 с.
2. Избранные вопросы теории булевых функций // Под ред. Винокурова С.Ф. и Перязева Н.А. — М.: ФИЗМАТЛИТ, 2001. — 192 с.

ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
E-mail: vin@math.isu.ru, a.kazimirov@gmail.com