Секция «Дискретная математика и математическая кибернетика»

О неприводимости булевых функций относительно коммутативной ассоциативной операции

Научный руководитель – Боков Григорий Владимирович

Сафонов Георгий Владимирович
Студент (специалист)
Московский государственный университет имени М.В.Ломоносова,
Механико-математический факультет, Кафедра математической теории интеллектуальных систем, Москва, Россия
E-mail: gosha-saf@yandex.ru

Тезисы

В работе исследуется проблема представления булевых функций в виде $f_1 \circ \ldots \circ f_m$, где $\circ$ — коммутативная ассоциативная операция и $f_1, \ldots, f_m$ булевы функции меньшей арности. Для каждой коммутативной ассоциативной операции определены необходимые и достаточные условия отсутствия такого представления и найден соответствующий класс алгоритмической сложности.

Представление булевых функций в виде суперпозиции более простых функций является важной фундаментальной проблемой, остающейся актуальной и по сей день. Разложения булевых функций на простые компоненты используется сегодня в оптимальном синтезе логических устройств [1], в построении алгебраически стойких шифраторов [2] и во многих других областях.

В данной работе рассмотрены разложения булевых функций $f \in \mathbf{P}_2^{(n)}$ арности n в виде

$$f = f_1 \circ \ldots \circ f_m, \tag{1}$$

где $\circ$ — коммутативная ассоциативная операция на $\{0, 1\}$ и $f_1, \ldots, f_m$ — булевы функции арности меньше n. Функции, не представимые в виде (1), называем $\circ$-*неприводимыми*. Например, функция $x_1 \vee x_2$ является $\wedge$-неприводимой, а функция $x_1 \wedge x_2$ является $\vee$- и $\oplus$-неприводимой, где $\vee$, $\wedge$ и $\oplus$ — логическая дизъюнкция, конъюнкция и сумма по модулю 2 соответственно. Нас интересовали условия $\circ$-неприводимости и класс алгоритмической сложности, которому принадлежит $\mathrm{Irred}_\circ$ — проблема проверки $\circ$-неприводимости булевых функций, заданных булевыми формулам. Также в работе была доказана следующая теорема:

Теорема 1. *Теорема 1.* $\mathrm{Irred}_\circ$ *является* **NP***-полной задачей для* $\circ \in \{\wedge, \vee\}$.

Источники и литература

1) *Brzozowski J. A., Luba T.* Decomposition of boolean functions specified by cubes // Journal of Multiple Valued Logic and Soft Computing, vol. 9, 2003, pp. 377-–417.

2) *Meier W., Pasalic E., Carlet C.* Algebraic Attacks and Decomposition of Boolean Functions // Lecture Notes in Computer Science, Advances in Cryptology - EUROCRYPT 2004, vol. 3027, 2004, pp. 474–491.