УДК 519.7 DOI 10.17223/2226308X/9/14

О МНОЖЕСТВЕ ПРОИЗВОДНЫХ БУЛЕВОЙ БЕНТ-ФУНКЦИИ[1]

Н. Н. Токарева

Верно ли, что любая уравновешенная булева функция от n переменных степени меньше $n/2$ является производной некоторой бент-функции от n переменных? В работе исследуется этот вопрос при малом числе переменных.

Ключевые слова: *бент-функции, производная, аффинная классификация.*

В работе продолжено исследование множества булевых бент-функций. Известно, что бент-функции [1] интересны для криптографических приложений [2]; актуальными в данной области остаются вопросы о числе бент-функций и способах их построения.

«Много» или «мало» бент-функций? Этим вопросом озадачиваются многие исследователи. Если исходить из предположения, что бент-функций много и они разнообразны, то разнообразными должны быть и их производные. Так ли это на самом деле? При малом числе переменных мы исследуем этот вопрос.

Производной булевой функции f от n переменных по направлению $y \in \mathbb{F}_2^n$ называется функция $D_y f(x) = f(x) + f(x+y)$. Напомним, что булева функция f от чётного числа переменных n называется *бент-функцией*, если её производная по любому ненулевому направлению y уравновешена, т. е. $D_y f$ одинаково часто принимает значения 0 и 1. Хорошо известно, что степень бент-функции не превосходит $n/2$.

Заметим, что булева функция g является производной некоторой булевой функции f тогда и только тогда, когда найдётся ненулевой вектор y, такой, что $g(x) + g(x+y) = 0$ для всех x. Напомним также, что если функция f отлична от константы, то степень её производной по любому ненулевому направлению меньше степени f.

Несложно доказать, что свойство быть производной некоторой бент-функции сохраняется при аффинном преобразовании, а именно: если булева функция g — производная некоторой бент-функции, то функция $g(Ax + b) + \lambda$ также обладает этим свойством, где A — невырожденная $n \times n$-матрица, b — произвольный вектор, λ — константа из $\mathbb{F}_2$.

В работе исследуется следующая гипотеза: *любая уравновешенная булева функция g от n переменных степени не выше $n/2 - 1$, такая, что $g(x) = g(x + y)$ для всех x при некотором y, является производной некоторой бент-функции от n переменных.*

На основе аффинной классификации булевых функций от малого числа переменных проверено, что при $n = 4, 6$ и в ряде случаев при $n = 8$ гипотеза верна; проверка продолжается.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press. Elsevier, 2015. 220 p.

[1]Работа поддержана грантом РФФИ, проект № 15-07-01328.