

Класс ВКП-функций во многом обобщает класс полиномиальных функций. В частности, можно показать, что системы уравнений, левые части которых являются такими функциями, могут быть решены методом покоординатной линеаризации, предложенным в работе [3] для полиномиальных функций над кольцом Галуа — Эйзенштейна.

ЛИТЕРАТУРА

1. Елизаров В. П. Конечные кольца. М.: Гелиос-АРВ, 2006.
2. Заец М. В., Никонов В. Г., Шшиков А. Б. Функции с вариационно-координатной полиномиальностью и их свойства // Открытое образование. 2012. № 3. С. 57–61.
3. Михайлов Д. А., Нечаев А. А. Решение системы полиномиальных уравнений над кольцом Галуа — Эйзенштейна с помощью канонической системы образующих полиномиального идеала // Дискретная математика. 2004. № 1. Вып. 1. С. 21–51.

УДК 519.7

ОБ АФФИННОСТИ БУЛЕВЫХ ФУНКЦИЙ НА ПОДПРОСТРАНСТВАХ И ИХ СДВИГАХ¹

Н. А. Коломеец

Пусть f — булева функция от n переменных и для любого аффинного подпространства L размерности $\lceil n/2 \rceil$ функция f аффинна на L тогда и только тогда, когда f аффинна на любом сдвиге L . Доказано, что тогда либо степень f не превышает 2, либо не существует ни одного аффинного подпространства размерности $\lceil n/2 \rceil$, на котором f аффинна.

Ключевые слова: булевы функции, бент-функции, квадратичные функции.

Рассматривается свойство булевых функций, связанное с их аффинностью на аффинных подпространствах.

Введём необходимые определения. Отображение $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ называется *булевой функцией* от n переменных. *Алгебраической степенью* или просто *степенью* булевой функции называется степень её алгебраической нормальной формы (полинома Жегалкина). Булева функция называется *аффинной*, если её алгебраическая степень не больше 1, и *квадратичной*, если её степень равна 2. Множество $U \subseteq \mathbb{Z}_2^n$ называется *аффинным подпространством*, если $U = a \oplus L$, где $a \in \mathbb{Z}_2^n$ и L является линейным подпространством в $\mathbb{Z}_2^n$. Будем называть U сдвигом подпространства L . Через Ind_D обозначим характеристическую функцию множества $D \subseteq \mathbb{Z}_2^n$. Через $\langle u, v \rangle$ обозначим скалярное произведение векторов u и v . Булева функция f от n переменных *аффинна на множестве* $D \subseteq \mathbb{Z}_2^n$, если существуют $a \in \mathbb{Z}_2^n$, $c \in \mathbb{Z}_2$, такие, что для любого $x \in D$ верно $f(x) = \langle a, x \rangle \oplus c$. Под *расстоянием* между двумя булевыми функциями подразумевается *расстояние Хэмминга* между их векторами значений.

Все квадратичные булевы функции обладают следующим свойством.

Утверждение 1. Пусть f — квадратичная булева функция от n переменных. Тогда для любого аффинного подпространства L функция f аффинна на L , если и только если f аффинна на любом сдвиге L .

Доказательство утверждения следует из неравенства $\deg(f(x) \oplus f(x \oplus s)) \leq 1$, верного для любого $s \in \mathbb{Z}_2^n$.

¹Исследование выполнено при поддержке РФФИ (проект № 12-01-31097).

Отметим, что не для всех квадратичных функций существует хотя бы одно аффинное подпространство размерности больше чем $\lceil n/2 \rceil$, на котором функция аффинна. Например, если f является бент-функцией (n чётно), то не существует подпространств размерности $n/2 + 1$, на которых f аффинна. Бент-функция — это булева функция от чётного числа переменных, максимально удаленная от множества всех аффинных функций. Понятие бент-функций ввел О. Ротхаус [1]. Бент-функции представляют интерес в криптографии и теории кодирования, поскольку имеют в этих областях множество различных приложений. Тем не менее до сих пор существует большое количество нерешённых проблем, связанных с бент-функциями [2].

Внесём ограничение на размерность подпространств в условие утверждения 1.

Утверждение 2. Пусть f — квадратичная булева функция от n переменных. Тогда для любого аффинного подпространства L размерности $\lceil n/2 \rceil$ функция f аффинна на L , если и только если f аффинна на любом сдвиге L .

Если f является бент-функцией, то по подпространствам размерности $n/2$, на которых она аффинна, можно строить другие бент-функции.

Утверждение 3 [3]. Пусть f — бент-функция от $2k$ переменных и $L \subseteq \mathbb{Z}_2^{2k}$, $|L| = 2^k$. Тогда $f(x) \oplus \text{Ind}_L(x)$ является бент-функцией тогда и только тогда, когда L является аффинным подпространством и f на нём аффинна.

Таким образом, существует взаимно однозначное соответствие между бент-функциями на расстоянии 2^k от f и аффинными подпространствами, на которых f аффинна.

Следующая теорема показывает, для каких функций, помимо квадратичных, справедливо утверждение 2.

Теорема 1. Пусть f — булева функция от n переменных и для любого аффинного подпространства L размерности $\lceil n/2 \rceil$ функция f аффинна на L , если и только если f аффинна на любом сдвиге L . Тогда либо $\deg f \leq 2$, либо не существует ни одного аффинного подпространства размерности $\lceil n/2 \rceil$, на котором функция f аффинна.

ЛИТЕРАТУРА

1. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения. Saarbrücken: LAP LAMBERT Academic Publishing, 2011.
3. Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.

УДК 510.53

ОБ АЛГОРИТМИЧЕСКИХ И ТОПОЛОГИЧЕСКИХ СВОЙСТВАХ ОРБИТ КУСОЧНО-АФФИННЫХ ОТОБРАЖЕНИЙ

А. Н. Курганский

Рассматривается открытая проблема достижимости в одномерных кусочно-аффинных отображениях с двумя интервалами. Найдены частные случаи алгоритмической разрешимости рассматриваемой проблемы, сформулированные на языке топологических свойств орбит в таких системах.

Ключевые слова: кусочно-аффинные отображения, проблема достижимости.