ПДМ. 2013. № 2(20).

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

ŋqdqyey bƎ dәdƎbУзe d eсаbсy Јqdqүqyè

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

О НЕКОТОРЫХ СВОЙСТВАХ СЛАБО ПОЛОЖИТЕЛЬНЫХ И СЛАБО ОТРИЦАТЕЛЬНЫХ БУЛЕВЫХ ФУНКЦИЙ

С. П. Горшков

Институт криптографии, связи и информатики, г. Москва, Россия

E-mail: spg54@bk.ru

Исследуются некоторые свойства слабо положительных (антихорновских) и слабо отрицательных (хорновских) булевых функций. В частности, оценивается сложность задачи построения приведённых представлений этих функций, показывается, что нет ограничений на вес таких функций, оценивается возможная длина записи рассматриваемых функций.

Ключевые слова: *слабо положительная (антихорновская) булева функция, слабо отрицательная (хорновская) булева функция, вычислительная сложность.*

1. Некоторые известные свойства исследуемых функций

Определение 1. Булева функция $f(x_1,\ldots,x_n)$, $n \geqslant 1$, называется:

1) *слабо положительной* (*антихорновской*), если $f \equiv 1$ или существует представление f в виде следующей КНФ:

$$f \equiv \bigwedge_{i=1}^{t} (x_{s_{i1}}^{\alpha_i} \vee x_{s_{i2}} \vee \ldots \vee x_{s_{ik_i}}),$$

где $\alpha_i \in \{0,1\}$, $i = 1,\ldots,t$;

2) *слабо отрицательной* (*хорновской*), если $f \equiv 1$ или существует представление f в виде следующей КНФ:

$$f \equiv \bigwedge_{i=1}^{t} (x_{s_{i1}}^{\alpha_i} \vee \bar{x}_{s_{i2}} \vee \ldots \vee \bar{x}_{s_{ik_i}}),$$

где $\alpha_i \in \{0,1\}$, $i = 1,\ldots,t$.

Множество всех слабо положительных (слабо отрицательных) функций обозначим WP (WN). Указанные записи соответственно функций классов WP, WN называются *приведёнными представлениями*. Функции из классов WP, WN, зависящие от k переменных, обозначим WP_k, WN_k.

Актуальность задачи изучения указанных функций отмечена в работе [1].

Обозначим:

V_k — множество двоичных k-мерных векторов;

$V_k^{(i)} = \{\alpha \in V_k : \|\alpha\| = i\}$, где $i \in \{0,\ldots,k\}$ (слой векторов веса i);

$\lfloor c \rfloor$ — целая часть действительного числа c.

ŋqdqyey bƎ dәdƎbУзe d eсаbсy Јqdqүqyè