

ПОРОГОВЫЕ К-ЗНАЧНЫЕ ФУНКЦИИ, ИХ ХАРАКТЕРИЗАЦИЯ И ПРИМЕНЕНИЕ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Бурделёв А. В.

Белорусский государственный университет, Минск, Беларусь, e-mail: aburd2011@mail.ru

Переход к переработке и передаче информации в оптической среде с высоким быстродействием делает пороговый базис самым удобным и согласованным с логикой переработки такой информации. Исключительное положение пороговых функций при этом определяется, прежде всего, возможностью реализации базовой операции, нахождения скалярного произведения, непосредственно в среде-носителе сигнала. Вычисление скалярного произведения путем прямого сведения оптических потоков приводит к реализации пороговой функции, со скоростями, сопоставимыми со скоростью света. Таким образом, для построения систем защиты информации в оптических каналах связи предпочтительным становится базис пороговых функций.

Одной из классических задач в сфере защиты информации является восстановление аналитического задания функции усложнения $f(x_1, \dots, x_n)$ в узле усложнения на базе регистра сдвига по известному входу и выходу. В случае применения пороговой функции в роли функции усложнения, задача нахождения ее аналитического задания сводится к задаче характеристики пороговой k -значной функции.

Функция k -значной логики $f(x_1, \dots, x_n)$, для которой существует линейная форма

$$L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n, x_i \in \mathbb{Z}_k \quad (1)$$

с вещественными коэффициентами и набор вещественных порогов $b_0 < b_1 < \dots < b_k$ такие, что для всех $i \in \overline{0, k-1}$ выполняется условие

$$f(x_1, \dots, x_n) = i \Leftrightarrow b_i \leq L(x_1, \dots, x_n) < b_{i+1}, \quad (2)$$

называется пороговой k -значной функцией.

Под алгоритмом характеристики пороговой k -значной функции, понимается процедура нахождения какого-либо семейства параллельных гиперплоскостей, разделяющих множества различных значений данной функции, то есть нахождения коэффициентов $a_1, a_2, \dots, a_n$ линейной формы $L(x_1, \dots, x_n)$ и множества порогов $b_0, b_1, \dots, b_{k-1}$.

Известна сводимость к проблеме характеристики пороговой функции целого класса задач математической логики, математической экономики, целочисленного линейного программирования, теории распознавания образов и защиты информации.

В докладе представлен новый геометрический алгоритм характеристики пороговой k -значной функции, разработанный для решения задач анализа систем защиты информации в пороговом базисе, а также его модификация. Введены новые параметры близости и отличия k -значных пороговых функций, исследованы их свойства и показана возможность их применения при решении задачи характеристики пороговой k -значной функции, возникающей при анализе и синтезе узлов защиты информации.

Список литературы

1. Бурделёв А.В., Никонов В.Г. О построении аналитического задания k -значной пороговой функции // Computational nanotechnology. Выпуск № 2, 2015. С. 5-13.
2. Бурделёв А.В., Никонов В.Г., Лапиков И.И. Распознавание параметров узла защиты информации, реализованного пороговой k -значной функцией // Труды СПИИРАН. 2016. Вып. 46. С. 108-127.
3. Бурделёв А.В., Никонов В.Г. О новом алгоритме характеристики k -значных пороговых функций // Computational nanotechnology. Выпуск № 1, 2017. С. 7-14.
4. Бурделёв А.В. О свойствах коэффициентов роста и коэффициентов возрастания // ЛЕСНОЙ ВЕСТНИК / FORESTRY BULLETIN. Выпуск 6, том 21, 2017.
5. Бурделёв А.В. О сходимости нового алгоритма характеристики k -значных пороговых функций // Прикладная дискретная математика. №39, 2018. – С. 98–106.

