# МАТЕМАТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ И АНАЛИЗ ДАННЫХ

## ДИАДИЧЕСКИЙ ДЕФИЦИТ БЕНТ-ПРЯМОУГОЛЬНИКОВ

**С.В. Агиевич**

Белгосуниверситет, НИИ прикладных проблем математики и информатики, Минск, Беларусь
agievich@bsu.by

Пусть $\mathbb{F}_2$ — поле из двух элементов; $\chi : \mathbb{F}_2 \to \mathbb{Z}$, $a \mapsto (-1)^a$ — аддитивный характер $\mathbb{F}_2$; $\mathbb{F}_2^n$ — $n$-мерное векторное пространство над $\mathbb{F}_2$; $\mathcal{F}_n$ — множество всех булевых функций от $n$ переменных, т. е. функций $\mathbb{F}_2^n \to \mathbb{F}_2$; $\deg f$ — степень многочлена Жегалкина для $f \in \mathcal{F}_n$; $\mathbf{x} \cdot \mathbf{u}$ — скалярное произведение векторов $\mathbf{x}, \mathbf{u} \in \mathbb{F}_2$. Преобразование Уолша — Адамара задает переход от функции $f$ к функции

$$\hat{f}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \chi(f(\mathbf{x}) + \mathbf{x} \cdot \mathbf{u}), \quad \mathbf{u} \in \mathbb{F}_2^n.$$

При этом $f$ называется *бент-функцией*, если $|\hat{f}(\mathbf{u})| = 2^{n/2}$ для всех $\mathbf{u}$. Пусть $\mathcal{B}_n$ — множество всех бент-функций от $n$ переменных (множество непусто, только если $n$ — четное).

В [1, 2] было предложено изучать свойства булевых функций с помощью прямоугольников: $(n-k, k)$*-прямоугольник* для $f \in \mathcal{F}_n$ — это функция

$$\overset{\square}{f}(\mathbf{u}, \mathbf{v}) = \sum_{\mathbf{y} \in \mathbb{F}_2^k} \chi(f(\mathbf{u}, \mathbf{y}) + \mathbf{y} \cdot \mathbf{v}), \quad \mathbf{u} \in \mathbb{F}_2^{n-k}, \quad \mathbf{v} \in \mathbb{F}_2^k.$$

Пусть $\overset{\square}{\mathcal{F}}_{n-k,k}$ — множество всех таких прямоугольников, а $\overset{\square}{\mathcal{B}}_{n-k,k} \subset \overset{\square}{\mathcal{F}}_{n-k,k}$ — множество прямоугольников для бент-функций, т. е. *бент-прямоугольников*.

Размерность $k$ может принимать значения от 0 до $n$. При $k = n$ множество $\overset{\square}{\mathcal{F}}_{0,n}$ состоит из функций $\hat{f}$, интерпретируемых как прямоугольники. Если $f \in \mathcal{B}_n$, то $\hat{f}(\mathbf{u}) = 2^{n/2}\chi(f^*(\mathbf{u}))$ для некоторой функции $f^* \in \mathcal{B}_n$. Эта функция называется *дуальной* к $f$.

Для целого $a$ через $\nu_2(a)$ обозначим его диадическое значение, т. е. максимальное неотрицательное целое $s$ такое, что $2^s \mid a$ (считаем, что $\nu_2(0) = \infty$). Диадическим значением целочисленной функции $\varphi$ назовем минимальное диадическое значение ее значений, $\nu_2(\varphi) = \min_x \nu_2(\varphi(x))$.

В докладе рассматривается следующая характеристика прямоугольника $\overset{\square}{f} \in \overset{\square}{\mathcal{F}}_{n-k,k}$, названная *диадическим дефицитом*:

$$\operatorname{dyad}(\overset{\square}{f}) = n/2 + \nu_2(\overset{\square}{f}) - k - 1.$$

Если $f$ — бент-функция, то $\nu_2(\hat{f}) = n/2$ и $\operatorname{dyad}(\hat{f}) = -1$. Для бент-прямоугольников $\overset{\square}{f} \neq \hat{f}$ справедлив следующий результат.

**Предложение 1**. *Пусть* $f \in \mathcal{B}_n$ *и* $\overset{\square}{f} \in \overset{\square}{\mathcal{B}}_{n-k,k}$, *где* $k < n$. *Тогда*

$$\nu_2(\overset{\square}{f}) \leqslant n/2, \quad \operatorname{dyad}(\overset{\square}{f}) \geqslant 0.$$

*Если* $\operatorname{dyad}(\overset{\square}{f}) = 0$, *то* $\deg f^* \geqslant n-k$, *где* $f^*$ — *дуальная к* $f$ *бент-функция. Обратно, если* $\deg f^* = n-k > 0$, *то найдется прямоугольник* $\overset{\square}{g} \sim \overset{\square}{f}$ *такой, что* $\operatorname{dyad}(\overset{\square}{g}) = 0$.

Будем говорить, что прямоугольники $\overset{\square}{f}$ и $\overset{\square}{g}$ *эквивалентны* и писать $\overset{\square}{f} \sim \overset{\square}{g}$, если $\overset{\square}{f}$ и $\overset{\square}{g}$ имеют одинаковые размеры (лежат в одном и том же множестве $\overset{\square}{\mathcal{F}}_{n-k,k}$) и могут быть получены друг из друга аффинными преобразованиями (соответствующие функции $f$ и $g$ аффинно эквивалентны).

**Предложение 2**. *Булева функция* $f$ *от* $n \geqslant 2$ *переменных является бент-функцией тогда и только тогда, когда*:

1) $\operatorname{dyad}(\hat{f}) = -1$;

2) $\operatorname{dyad}(\overset{\square}{g}) = 0$ *для любого прямоугольника* $\overset{\square}{g} \sim \overset{\square}{f} \in \overset{\square}{\mathcal{F}}_{1,n-1}$.

**Литература**

1. Agievich S. *Bent rectangles* // Proceedings of the NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Moscow, September 8–18, 2007). Amsterdam: IOS Press, 2008. P. 3—22.

2. Agievich S. *On the representation of bent functions by bent rectangles* // Probabilistic Methods in Discrete Mathematics: Fifth International Conference (Petrozavodsk, Russia, June 1–6, 2000). Utrecht, Boston: VSP, 2002. P. 121–135.