О расстоянии Хэмминга между почти всеми функциями алгебры логики

А. В. ГАЛАТЕНКО
Московский государственный университет им. М. В. Ломоносова
e-mail: agalat@msu.ru

В. В. ГАЛАТЕНКО
Московский государственный университет им. М. В. Ломоносова
e-mail: vgalat@msu.ru

УДК 519.95

Ключевые слова: булевы функции, расстояние Хэмминга.

Аннотация

В работе оценивается расстояние Хэмминга между почти всеми функциями алгебры логики.

Abstract

A. V. Galatenko, V. V. Galatenko, On Hamming distance between almost all Boolean functions, Fundamentalnaya i prikladnaya matematika, vol. 15 (2009), no. 5, pp. 43—47.

A precise estimation of Hamming distance between almost all Boolean functions is presented.

1. Основные понятия и результаты

Пусть $\mathbb{P}_2^n$ — функции алгебры логики от n переменных. Число наборов переменных обозначим через N: $N = N(n) = 2^n$. Каждой функции поставим в соответствие вектор её значений. Расстоянием Хэмминга ρ между двумя функциями будем называть число позиций, на которых различаются соответствующие векторы значений. Несложно убедиться, что введённое расстояние действительно является метрикой на множествах $\{0,1\}^N$ и $\mathbb{P}_2^n$.

Пусть $F_1, F_2 \colon \mathbb{N} \to \mathbb{N}$ — пара функций. Если выполнено соотношение

$$\lim_{n\to\infty} \frac{|\{(f,g)\colon f,g \in \mathbb{P}_2^n,\ F_1(n) < \rho(f,g) < F_2(n)\}|}{|(\mathbb{P}_2^n)^2|} = 1,$$

будем говорить, что почти все функции алгебры логики удалены друг от друга на расстояние, лежащее между значениями F_1 и F_2.

Фундаментальная и прикладная математика, 2009, том 15, № 5, с. 43—47.

Теорема 1. *Пусть функция* $F\colon \mathbb{N} \to \mathbb{N}$ *такова, что*

$$\lim_{n\to\infty} \frac{\sqrt{n}}{F(n)} = 0.$$

Тогда почти все функции алгебры логики удалены друг от друга на расстояние от $\frac{N}{2} - F(N)$ *до* $\frac{N}{2} + F(N)$.

При переходе от оценок в терминах N к оценкам в терминах n требования примут следующий вид:

$$\lim_{n\to\infty} \frac{2^{n/2}}{H(n)} = 0,$$

и почти все функции алгебры логики удалены друг от друга на расстояние от $2^{n-1} - H(n)$ до $2^{n-1} + H(n)$.

Теорема 2. *Пусть* $\alpha \in \mathbb{R}$, $\alpha > 0$ *и функция* $G\colon \mathbb{N} \to \mathbb{N}$ *такова, что* $G(n) \lesssim \alpha\sqrt{n}$, $n \to \infty$. *Тогда доля пар функций, удалённых друг от друга на расстояние от* $\frac{N}{2} - G(N)$ *до* $\frac{N}{2} + G(N)$, *асимптотически не больше константы* c, $c < 1$.

Авторы выражают глубокую благодарность д. ф.-м. н., профессору В. Б. Кудрявцеву за постановку задачи и внимание к работе.

Работа выполнена при частичной финансовой поддержке РФФИ (проекты 08-01-00799-а и 09-01-12173-офи_м).

2. Вспомогательные утверждения

Лемма 1. *Пусть* $\{f_n\}_{n=1}^{\infty}$ *— произвольная последовательность функций алгебры логики,* $f_n \in \mathbb{P}_2^n$. *Тогда*

$$\lim_{n\to\infty} \frac{|\{g_n \in \mathbb{P}_2^n\colon N/2 - F(N) < \rho(f_n, g_n) < N/2 + F(N)\}|}{2^N} = 1.$$

Доказательство. Обозначим

$$T_1 = \left\{g \in \mathbb{P}_2^n\colon \rho(f,g) \leqslant \frac{N}{2} - F(N)\right\}, \quad T_2 = \left\{g \in \mathbb{P}_2^n\colon \rho(f,g) \geqslant \frac{N}{2} + F(N)\right\}.$$

Пусть $l = \frac{N}{2} - F(N)$ ($N = 2^n$, т. е. N чётное).

Рассмотрим случай, когда $F(N) = o(N)$, $N \to \infty$.

Мощность множества T_1 может быть вычислена по формуле

$$|T_1| = \sum_{k=0}^{l} C_N^k.$$

Рассмотрим отношение $B(l; N, \frac{1}{2}) = \frac{|T_1|}{2^N}$. Несложно заметить, что $B(l; N, \frac{1}{2})$ равно вероятности не более чем l успехов при N испытаниях Бернулли с равновероятными успехом и неудачей [1, гл. VI, § 2]. Обозначим через $b(k; N, \frac{1}{2})$

отношение $\frac{C_N^k}{2^N}$. В [1, гл. VI, § 3] доказывается, что

$$B\left(l;N,\frac{1}{2}\right) < b\left(l;N,\frac{1}{2}\right)\frac{(N-l+1)/2}{(N+1)/2-l}.$$

Так как $l < \frac{N}{2}$, это неравенство можно переписать в виде

$$B\left(l;N,\frac{1}{2}\right) < b\left(\frac{N}{2};N,\frac{1}{2}\right)\frac{(N-l+1)/2}{(N+1)/2-l}.$$

Подставив в правую часть неравенства формулу биномиальных коэффициентов и выражение для l, получим неравенство

$$B\left(l;N,\frac{1}{2}\right) < \frac{N!}{((N/2)!)^2}\,\frac{1}{2^N}\,\frac{N+2F(N)+2}{2+4F(N)}.$$

Применим к первому сомножителю правой части формулу Стирлинга:

$$\frac{N!}{((N/2)!)^2} = \frac{\sqrt{2\pi N}(N/e)^N(1+o(1))}{(\sqrt{\pi N}(N/2e)^{N/2}(1+o(1)))^2} = 2^N\frac{\sqrt{2}+o(1)}{\sqrt{\pi N}(1+o(1))}, \quad N\to\infty.$$

Таким образом,

$$B\left(l;N,\frac{1}{2}\right) < \frac{\sqrt{2}+o(1)}{\sqrt{\pi N}(1+o(1))}\,\frac{N+2F(N)+2}{2+4F(N)}, \quad N\to\infty.$$

Перемножая дроби и учитывая условия леммы и дополнительное условие на $F(N)$, получаем неравенство

$$B\left(l;N,\frac{1}{2}\right) < \frac{\sqrt{2N}(1+o(1))}{\sqrt{\pi}F(N)(1+o(1))} = o(1), \quad N\to\infty.$$

Избавимся от дополнительного ограничения на $F(N)$. Заметим, что в силу положительности слагаемых в формуле для вычисления $B(l;N,\frac{1}{2})$ при выполнении условия $0 \leqslant l' < l$ справедливо неравенство $B(l';N,\frac{1}{2}) < B(l;N,\frac{1}{2})$. Следовательно, оценка $B(l;N,\frac{1}{2}) = o(1)$ при $N\to\infty$ остаётся верной при любой функции $F(N)$, удовлетворяющей условиям леммы.

В силу симметрии биномиальных коэффициентов аналогичная оценка верна и для случая T_2. Заметим, что

$$\left\{g\in\mathbb{P}_2^n\colon \frac{N}{2}-F(n)<\rho(f,g)<\frac{N}{2}+F(n)\right\} = (\mathbb{P}_2^n\setminus T_1)\setminus T_2.$$

Лемма доказана. □

Лемма 2. *Пусть $\alpha\in\mathbb{R}$, $\alpha>0$, N — чётное натуральное число. Тогда*

$$\frac{1}{2^N}\sum_{k=0}^{[\alpha\sqrt{N}]} C_N^{N/2-k} = c+o(1), \quad N\to\infty,$$

причём $c<\frac{1}{2}$.

Доказательство. Преобразуем слагаемые с использованием формулы Стирлинга:

$$C_N^{N/2-k} = \frac{\sqrt{2\pi N}(N/e)^N(1+o(1))}{2\pi\sqrt{N^2/4-k^2}(N/(2e)-k/e)^{N/2-k}(N/(2e)+k/e)^{N/2+k}(1+o(1))}, \quad N\to\infty.$$

Сократив дробь на $(N/e)^N$, получим

$$C_N^{N/2-k} = \frac{2^N\sqrt{N}(1+o(1))}{\sqrt{2\pi}\sqrt{N^2/4-k^2}(1-2k/N)^{N/2-k}(1+2k/N)^{N/2+k}(1+o(1))}, \quad N\to\infty.$$

Преобразуем выражения в знаменателе следующим образом:

$$\left(1-\frac{2k}{N}\right)^{N/2-k}\left(1+\frac{2k}{N}\right)^{N/2+k} = e^{(N/2-k)\ln(1-2k/N)+(N/2+k)\ln(1+2k/N)}.$$

Разложим логарифмы в показателе по формуле Тейлора, учитывая, что k имеет порядок не более $\sqrt{N}$:

$$\ln\left(1\pm\frac{2k}{N}\right) = \pm\frac{2k}{N} - \frac{2k^2}{N^2} + o\left(\frac{1}{N}\right), \quad N\to\infty,$$

где $o(\frac{1}{N})$ равномерно по k, $k\leqslant\alpha\sqrt{N}$. Раскрыв скобки в показателе, получим

$$\left(1-\frac{2k}{N}\right)^{N/2-k}\left(1+\frac{2k}{N}\right)^{N/2+k} = e^{2k^2/N}\big(1+o(1)\big), \quad N\to\infty.$$

Таким образом, имеет место соотношение

$$C_N^{N/2-k} = \frac{2^N}{\sqrt{\pi N/2}}\,e^{-2k^2/N}\big(1+o(1)\big), \quad N\to\infty,$$

где $o(1)$ равномерно по k, $k\leqslant\alpha\sqrt{N}$.

Заметим, что функция $e^{-2k^2/N}$ монотонно убывает по k на промежутке $[0,+\infty)$. Следовательно,

$$\frac{1}{2^N}\sum_{k=0}^{[\alpha\sqrt{N}]}\frac{2^N}{\sqrt{\pi N/2}}e^{-2k^2/N} \leqslant \frac{1}{\sqrt{\pi N/2}} + \frac{1}{\sqrt{\pi N/2}}\int\limits_0^{\alpha\sqrt{N}} e^{-2k^2/N}\,dk, \quad N\to\infty.$$

Первое слагаемое оценивается как $o(1)$ при $N\to\infty$. Во втором слагаемом сделаем замену переменной интегрирования:

$$\int\limits_0^{\alpha\sqrt{N}} e^{-2k^2/N}\,dk = \frac{\sqrt{N}}{\sqrt{2}}\int\limits_0^{\alpha\sqrt{N}} e^{-(\frac{\sqrt{2}k}{\sqrt{N}})^2}\,d\left(\frac{\sqrt{2}k}{\sqrt{N}}\right) = \frac{\sqrt{N}}{\sqrt{2}}\int\limits_0^{\alpha\sqrt{2}} e^{-t^2}\,dt.$$

Заметим, что получившийся после преобразования интеграл не зависит от N и является константой, строго меньшей $\frac{\sqrt{\pi}}{2}$, значения интеграла Эйлера—Пуассона [2, § 455]. Следовательно, выполнено неравенство

$$\frac{1}{2^N}\sum_{k=0}^{[\alpha\sqrt{N}]} C_N^{N/2-k} \leqslant \frac{1}{\sqrt{\pi}}\int_0^{\alpha\sqrt{2}} e^{-t^2}\,dt + o(1) = c + o(1), \quad N \to \infty,$$

где $c < \frac{1}{2}$. Лемма доказана. □

3. Доказательство теорем

Пусть $f' \in \mathbb{P}_2^n$. Так как

$$|\{f, g \in \mathbb{P}_2^n \colon F_1(n) < \rho(f,g) < F_2(n)\}| = \\ = |\mathbb{P}_2^n| \left|\left\{g \in \mathbb{P}_2^n \colon \frac{N}{2} - F(n) < \rho(f',g) < \frac{N}{2} + F(n)\right\}\right|,$$

утверждение теоремы 1 следует из леммы 1.

Утверждение теоремы 2 непосредственно следует из леммы 2.

Литература

[1] Феллер В. Введение в теорию вероятностей и её приложения. Т. 1. — М.: Мир, 1964.

[2] Фихтенгольц Г. М. Курс дифференциального и интегрального исчисления. Т. 2. — М.: Гостехиздат, 1951.