О расстоянии Хэмминга между почти всеми функциями алгебры логики

А. В. Галатенко, В. В. Галатенко

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

1. Основные понятия и результаты

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

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

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

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

Теорема 1. *Пусть функция $F : \mathbb{N} \to \mathbb{N}$ такова, что $\lim\limits_{n\to\infty} \frac{\sqrt{n}}{F(n)} = 0$. Тогда почти все функции алгебры логики удалены 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: $\lim\limits_{n\to\infty} \frac{2^{n/2}}{H(n)} = 0$, и почти все функции алгебры логики удалены 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* $G : \mathbb{N} \to \mathbb{N}$ *такова, что* $G(n) \lesssim \alpha\sqrt{n}$, $n \to \infty$. *Тогда доля пар функций, удаленных 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., проф. 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*

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

Доказательство. Обозначим через T_1 множество $\{g \in \mathbb{P}_2^n \,|\, \rho(f,g) \leqslant \frac{N}{2} - F(N)\}$, а через T_2 — множество $\{g \in \mathbb{P}_2^n \,|\, \rho(f,g) \geqslant \frac{N}{2} + F(N)\}$. Пусть $l = \frac{N}{2} - F(N)$ ($N = 2^n$, то есть N четное).

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 увидеть, 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 работе [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

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

Подставим в правую часть неравенства формулу биномиальных коэффициентов и формулу l, и получим следующее 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:

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

Таким образом,

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

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

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

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 $N \to \infty$ остается верной при любой функции $F(N)$, удовлетворяющей условиям леммы.

В силу симметрии биномиальных коэффициентов, аналогичная оценка верна и для случая T_2. Заметим, что $\{g \in \mathbb{P}_2^n : \frac{N}{2} - F(n) < \rho(f,g) < \frac{N}{2} + F(n)\} = (\mathbb{P}_2^n \setminus T_1) \setminus T_2$. Лемма доказана.

Лемма 2. *Пусть $\alpha \in \mathbb{R}$, $\alpha > 0$, N — четное натуральное число. Тогда $\frac{1}{2^N} \sum\limits_{k=0}^{[\alpha\sqrt{N}]} C_N^{N/2-k} = c + o(1)$ при $N \to \infty$, причем $c < \frac{1}{2}$.*

Доказательство. Преобразуем слагаемые с использованием формулы Стирлинга:

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

$N \to \infty$. Сократив дробь на $(N/e)^N$, получим следующее выражение:

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

$N \to \infty$. Преобразуем выражения в знаменателе следующим образом:

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

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

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

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

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

Таким образом, имеет место следующее соотношение:

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

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,

$$\frac{1}{2^N}\sum_{k=0}^{[\alpha\sqrt{N}]}\frac{2^N}{\sqrt{\pi N/2}}e^{-2k^2/N} \leqslant \frac{1}{\sqrt{\pi N/2}} + \frac{1}{\sqrt{\pi N/2}}\int_0^{\alpha\sqrt{N}} e^{-2k^2/N}dk, N \to \infty.$$

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

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

Заметим, что получившийся после преобразования интеграл не зависит от N и является константой, строго меньшей, чем $\frac{\sqrt{\pi}}{2}$, являющейся значением интеграла Эйлера-Пуасона ([2, §455]). Следовательно, выполнено следующее неравенство:

$$\frac{1}{2^N} \sum_{k=0}^{[\alpha\sqrt{N}]} C_N^{N/2-k} \leqslant \frac{1}{\sqrt{\pi}} \int\limits_0^{\alpha\sqrt{2}} e^{-t^2} dt + o(1) = c + o(1), N \to \infty,$$

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

3. Доказательство теорем

Пусть $f' \in \mathbb{P}_2^n$. Так как $|\{f, g \in \mathbb{P}_2^n : F_1(n) < \rho(f, g) < F_2(n)\}| = |\mathbb{P}_2^n||\{g \in \mathbb{P}_2^n : \frac{N}{2} - F(n) < \rho(f', g) < \frac{N}{2} + F(n)\}|$, утверждение теоремы 1 следует из леммы 1.

Утверждение теоремы 2 непосредственно следует из леммы 2.

Список литературы

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

[2] Фихтенгольц Г. М. Курс дифференциального и интегрального исчисления в 3 томах. Т. 2. М.: Государственное издательство технико-теоретической литературы, 1951.