О числе p-сократимых индуцированных вероятностных функций

Е. Е. Трифонова[1]

Статья посвящена изучению доли булевых функций, индуцирующих p-сократимые функции разного типа, среди всех булевых функций.

Ключевые слова: бернуллиевская случайная величина, конечная порожденность, преобразование случайных величин.

1. Введение

Преобразования бернуллиевских случайных величин с рациональными вероятностями посредством булевых функций рассматривались в работах Р. Л. Схиртладзе, Ф. И. Салимова и Р. М. Колпакова (см. [1, 2, 3], а также обзор в [4]). Р. Л. Схиртладзе [1] показал, что преобразования с помощью конъюнкций и дизъюнкций (& и $\vee$) позволяют породить все множества двоично-рациональных и троично-рациональных распределений, используя конечное множество распределений. Ф. И. Салимов в [2] показал, что множества p-ично-рациональных распределений конечно порождены при преобразованиях операциями системы $\{x_1x_2 \vee \bar{x}_1x_3, 0, 1\}$. В работах Р. М. Колпакова [3] установлена конечная порожденность относительно преобразований системой $\{\&, \vee\}$ множеств рациональных бернуллиевских распределений, у которых в разложении знаменателя на простые множители могут встречаться простые числа из заданного конечного множества мощности не менее 2.

Ранее автором было получено, что преобразования случайных величин с распределениями из конечного множества с помощью функции голосования не позволяют выразить все вероятности, записываемые пятеричными дробями [5]. Этот результат можно также распространить на все p-ичные дроби для произвольного простого p, $p \geq 5$. Кроме того, в статье [6] сформулированы некоторые свойства, которыми должны обладать функции из конечно порождающего множества при условии, что функции индуцируют p-несократимые вероятностные функции. Под p-несократимыми функциями понимаются такие функции, которые при подстановке в качестве значений переменных несократимых правильных дробей, на выходе дают также несократимые дроби со знамена-

[1] *Трифонова Екатерина Евгеньевна* — инженер-исследователь, ИПМ им. М.В.Келдыша РАН, e-mail: etrifonova@keldysh.ru.

Trifonova Ekaterina Evgen'evna — research engineer, Keldysh Institute of Applied Mathematics (Russian Academy of Sciences)

телем, степень которого есть сумма степеней знаменателей подставляемых дробей. Если называть вероятностные функции, не обладающие подобным свойством, p-сократимыми, то возникает вопрос, какова доля p-сократимых вероятностных функций среди всех вероятностных функций, индуцированных булевыми функциями без фиктивных переменных. Решению именно этой задачи посвящена данная работа. Особенно важной эта задача представляется в связи с тем, что универсальная функция, входящая в состав конечно порождающей системы, описанной Ф.И.Салимовым, индуцирует p-сократимую функцию.

2. Основные понятия

Пусть x — случайная величина, принимающая значение 1 и 0 с вероятностью $\widehat{x}$ и $1-\widehat{x}$ соответственно. Тогда распределение этой случайной величины однозначно определяется значением $\widehat{x}$. Будем считать, что каждой случайной величине x, принимающей значения 0 и 1, сопоставлено число $\widehat{x} \in [0;1]$.

Будем рассматривать преобразования, осуществляемые в результате подстановки независимых в совокупности случайных величин со значениями 0 и 1 вместо переменных булевых функций. При этом в качестве преобразователей будем брать только булевы функции без фиктивных переменных.

Пусть задана булева функция $f(x_1,\ldots,x_n)\colon \{0,1\}^n \to \{0,1\}$, тогда *вероятностная функция* $\widehat{f}(\widehat{x}_1,\ldots,\widehat{x}_n)\colon [0;1]^n \to [0;1]$, *индуцированная булевой функцией* $f(x_1,\ldots,x_n)$, определяется соотношением:

$$\widehat{f}(\widehat{x}_1,\ldots,\widehat{x}_n) = \sum_{\substack{(x_1,\ldots,x_n):\\ f(x_1,\cdots,x_n)=1}} \prod_{i=1}^{n} (x_i\widehat{x}_i + (1-x_i)(1-\widehat{x}_i)).$$

Будем обозначать как $H(p^k)$ всевозможные правильные несократимые дроби со знаменателем p^k.

Пусть $f(x_1,\ldots,x_n) \in P_2$, $\widehat{f}(\widehat{x}_1,\ldots,\widehat{x}_n)$ — индуцированная f вероятностная функция, p — простое, $p \geq 5$. Тогда если $\widehat{x}_i \in H(p^{k_i})$ для $i \in \{1,\ldots,n\}$, то значение индуцированной функции $\widehat{f}$ можно представить как $\widehat{f}(\widehat{x}_1,\ldots,\widehat{x}_n) = \frac{D}{p^m}$, $D \bmod p \neq 0$. При этом если $m = k_1+\cdots+k_n$ для заданного p, любых $\widehat{x}_i \in H(p^{k_i})$, а также любых $k_i \in \mathbb{N}, i \in \{1,\ldots,n\}$, то $\widehat{f}$ будем называть *p-несократимой функцией.*

Будем называть индуцированные функции, которые не обладают такими свойствами, *p-сократимыми функциями.* При этом заметим, что для каждой p-сократимой функции найдется хотя бы один такой набор значений переменных $\widehat{x}_i \in H(p^{k_i})$, что $m < k_1 + \cdots + k_n$, а равенство

$m = k_1 + \dots + k_n$ может как выполняться, так и не выполняться при других значения переменных $\widehat{x}_i \in H(p^{k_i})$.

Между булевой функцией и индуцированной ей функцией существует взаимнооднозначное соответствие. Говоря о числе p-сократимых функций, мы одновременно говорим и о числе булевых функций, индуцирующих p-сократимые функции.

Вероятностную функцию, индуцированную булевой функцией, можно записать в виде

$$\widehat{f}(\widehat{x}_1, \dots, \widehat{x}_n) = \sum_{\kappa_1,\dots,\kappa_n: \in \{0;1\}} \alpha_{\kappa_1 \dots \kappa_n} \widehat{x}_1^{\kappa_1} \dots \widehat{x}_n^{\kappa_n},$$

где $\widehat{x}_i^0 = 1$, $\widehat{x}_i^1 = \widehat{x}_i$. Тогда будет ли являться функция p-сократимой или p-несократимой, определяется величиной коэффициента $\alpha_{1\dots 1}$ при $\widehat{x}_1 \dots \widehat{x}_n$. Очевидно, что $\widehat{f}$ будет p-сократимой в двух случаях:

1) $\alpha_{1\dots 1} = 0$, в этом случае функцию $\widehat{f}$ будем называть p-сократимой первого типа;

2) $\alpha_{1\dots 1} = p^t A$, где $t \geq 1$, $A \in \mathbb{Z}$, $A \mod p \neq 0$, в этом случае функцию $\widehat{f}$ будем называть p-сократимой второго типа.

Заметим, что p-сократимые функции первого типа будут p-сократимыми для любого простого $p \geq 5$, а p-сократимые функции второго типа будут являться таковыми для одних p и не будут для других.

Напомним, что для булевой функции $f(x_1, \dots, x_n)$ единичными наборами называются совокупности значений переменных $x_1, \dots, x_n$, на которых функция f принимает единичное значение.

Обозначим число нулей в наборе $(x_1, \dots, x_n)$ как

$$\theta(x_1, \dots, x_n) = \sum_{i=1}^{n} (1 - x_i).$$

Число наборов с нечетным числом нулей среди единичных наборов булевой функции $f(x_1, \dots, x_n)$ запишем как

$$\eta_o(f) = \sum_{\substack{(x_1,\dots,x_n): \\ f(x_1,\dots,x_n)=1}} \theta(x_1, \dots, x_n) \bmod 2.$$

Выразим число наборов с четным числом нулей среди единичных наборов булевой функции $f(x_1, \dots, x_n)$ следующим образом:

$$\eta_e(f) = \sum_{\substack{(x_1,\dots,x_n): \\ f(x_1,\dots,x_n)=1}} (1 - \theta(x_1, \dots, x_n) \bmod 2).$$

Лемма 1. *Для булевой функции $f(x_1, \ldots, x_n)$, не содержащей фиктивных переменных, и индуцированной ей функции $\widehat{f}(\widehat{x}_1, \ldots, \widehat{x}_n)$ выполняется $\alpha_{1\ldots1} = \eta_e(f) - \eta_o(f)$*

Доказательство. Из определения вероятностной функции $\widehat{f}(\widehat{x}_1, \ldots, \widehat{x}_n)$, индуцированной булевой функцией $f(x_1, \ldots, x_n)$, следует, что функцию $\widehat{f}(\widehat{x}_1, \ldots, \widehat{x}_n)$ можно записать в виде:

$$\widehat{f}(\widehat{x}_1, \ldots, \widehat{x}_n) = \sum_{j=1}^{\omega_1(f)} \delta_{1j} \ldots \delta_{nj},$$

где $\delta_{1j} \ldots \delta_{nj}$ соответствует единичному набору функции f следующим образом: $\delta_{ij} = \widehat{x}_i$, если $x_i = 1$, $\delta_{ij} = 1 - \widehat{x}_i$, если $x_i = 0$, $\omega_1(f)$ — число единичных наборов функции f.

Очевидно, что после раскрытия всех скобок у выражения $\delta_{1j} \ldots \delta_{nj}$, коэффициент перед слагаемым $\widehat{x}_1 \ldots \widehat{x}_n$ будет равен либо 1, либо -1. Коэффициент будет равен 1 в том случае, если число скобок вида $1 - \widehat{x}_i$ будет четно, и будет равен -1, если нечетно. Соответственно, для всех единичных наборов получим, что суммарный коэффициент (обозначаемый как $\alpha_{1\ldots1}$) перед $\widehat{x}_1 \ldots \widehat{x}_n$ будет равен $\eta_e(f) - \eta_o(f)$. Таким образом, $\alpha_{1\ldots1} = \eta_e(f) - \eta_o(f)$.

□

Лемма 2. *Если f индуцирует p-сократимую функцию первого типа $\widehat{f}$, то $\eta_e(f) = \eta_o(f)$.*

Доказательство. По определению p-сократимой функции первого типа $\alpha_{1\ldots1} = 0$. Из леммы 1 получаем, что $\alpha_{1\ldots1} = \eta_e(f) - \eta_o(f) = 0$. Следовательно, $\eta_e(f) = \eta_o(f)$. □

Лемма 3. *Если $f(x_1, \ldots, x_n)$ содержит фиктивные переменные, то $\eta_e(f) = \eta_o(f)$.*

Доказательство. Без ограничения общности будем считать, что x_1 — фиктивная переменная. Тогда для любого набора $(x_2, \ldots, x_n)$ будет выполнено $f(0, x_2, \ldots, x_n) = f(1, x_2, \ldots, x_n)$. Отсюда очевидно следует, что $\eta_e(f) = \eta_o(f)$. □

Лемма 4. *Для булевой функции f $\eta_e(f) = \eta_o(f)$ тогда и только тогда, когда либо f содержит не менее одной фиктивной переменной, либо когда f индуцирует p-сократимую функция первого типа.*

Доказательство. Докажем необходимость. Пусть для булевой функции f $\eta_e(f) = \eta_o(f)$, а наше предположение неверно. Т. е. f не будет содержать фиктивных переменных и индуцированная функция $\widehat{f}$ не будет являться p-сократимой первого типа, то есть $\alpha_{1\ldots1} \neq 0$. По лемме 1 имеем

$\alpha_{1\ldots1} = \eta_e(f) - \eta_o(f)$, т. е. $\alpha_{1\ldots1} = 0$. Получили противоречие, необходимость доказана.

Достаточность доказана в леммах 2 и 3.

□

Лемма 5. *Если булевая функция f индуцирует p-сократимую функцию второго типа $\widehat{f}$, то $\eta_e(f) - \eta_o(f)$ будет кратна p.*

Доказательство. Следует из леммы 1 и определения p-сократимых функций второго типа. □

3. Оценка числа p-сократимых функций первого типа

Число булевых функций f таких, что $\eta_e(f) = \eta_o(f)$, мы можем посчитать как

$$\sum_{k=0}^{2^{n-1}} C_{2^{n-1}}^k C_{2^{n-1}}^k.$$

При этом согласно лемме 4 это число будет включать в себя все функции, которые индуцируют p-сократимые первого типа, и также и все функции, которые содержат фиктивные переменные.

Число функций от n, содержащих фиктивные переменные, может быть вычислено как:

$$2^{2^n} - \sum_{k=0}^{n} (-1)^k C_n^k 2^{2^{n-k}} = -\sum_{k=1}^{n} (-1)^k C_n^k 2^{2^{n-k}}.$$

Тогда число p-сократимых функций первого типа, будет равно разности двух выражений, приведенных выше:

$$\sum_{k=0}^{2^{n-1}} C_{2^{n-1}}^k C_{2^{n-1}}^k + \sum_{k=1}^{n} (-1)^k C_n^k 2^{2^{n-k}}.$$

Используя свертку Вандермонда [7], преобразуем первое слагаемое следующим образом:

$$\sum_{k=0}^{2^{n-1}} C_{2^{n-1}}^k C_{2^{n-1}}^k = \sum_{k=0}^{2^{n-1}} C_{2^{n-1}}^k C_{2^{n-1}}^{2^{n-1}-k} = C_{2^{n-1}+2^{n-1}}^{2^{n-1}} = C_{2^n}^{2^{n-1}} = C_{2^n}^{2^n/2}.$$

Теперь оценим величину второго слагаемого.

$$\sum_{k=1}^{n} (-1)^k C_n^k 2^{2^{n-k}} = -n 2^{2^{n-1}} + \ldots.$$

Известно, что его асимптотика равна $-n2^{2^{n-1}}$.

Для оценки значения выражения вида C_{2l}^{l} при $n \to \infty$ будем использовать формулу Стирлинга в виде $l! \sim \sqrt{2\pi l}(\frac{l}{e})^l$. Тогда $C_{2l}^{l} \sim \frac{2^{2l}}{\sqrt{\pi l}}$. Подставим 2^n вместо $2l$, а 2^{n-1} вместо l. Получаем, что $C_{2^n}^{2^{n-1}} \sim \frac{2^{2^n}}{\sqrt{\pi 2^{n-1}}} = \frac{2^{2^n}}{\sqrt{\frac{\pi}{2}}(\sqrt{2^n})} = \sqrt{\frac{2}{\pi}}\frac{2^{2^n}}{2^{n/2}}$.

Оценим асимптотику разности выражений $C_{2^n}^{2^n/2} - n2^{2^{n-1}}$. Для этого представим $n2^{2^{n-1}}$ как $n\sqrt{2^{2^n}}$.

Тогда $C_{2^n}^{2^n/2} - n2^{2^{n-1}} \sim \sqrt{2^{2^n}}(\sqrt{\frac{2}{\pi}}\frac{\sqrt{2^{2^n}}}{2^{n/2}} - n) \sim \sqrt{\frac{2}{\pi}}\frac{2^{2^n}}{2^{n/2}}$.

Заметим, что число всех булевых функций асимптотически равно числу всех булевых функций без фиктивных переменных.

Поскольку число всех булевых функций от n переменных равно 2^{2^n}, то получаем, что доля сократимых функций первого типа при $n \to \infty$ асимптотически убывает как $\sqrt{\frac{2}{\pi}}\frac{1}{2^{n/2}}$.

4. Оценка числа p-сократимых функций второго типа

Для p-сократимых функций второго типа по определению $\alpha_{1\ldots 1} = p^t A$, где $t \geq 1$, $A \in \mathbb{Z}$, $A \mod p \neq 0$. По лемме 1 имеем, что $\eta_e(f) - \eta_o(f) = \alpha_{1\ldots 1} = p^t A$. Тогда можем записать, что $|\eta_e(f) - \eta_o(f)| = sp$, где $s \in \mathbb{N}$, т. е. либо $\eta_e(f) = \eta_o(f) + ps$, если $\eta_e(f) > \eta_o(f)$, либо $\eta_o(f) = \eta_e(f) + ps$, если $\eta_o(f) > \eta_e(f)$. Для фиксированного s число таких функций равно

$$2 \sum_{i=0}^{2^{n-1}-sp} C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^{i},$$

для всех допустимых s получаем, что общее число таких функций равно

$$\sum_{s=1}^{[\frac{2^{n-1}}{p}]} 2 \sum_{i=0}^{2^{n-1}-sp} C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^{i}.$$

Таким образом, число p-сократимых функций второго типа можно записать как

$$2 \sum_{s=1}^{[\frac{2^{n-1}}{p}]} \sum_{i=0}^{2^{n-1}-sp} C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^{i}.$$

Преобразуем выражение $C_{2^{n-1}}^{i}$ следующим образом

$$C_{2^{n-1}}^{i} = C_{2^{n-1}}^{2^{n-1}-i} = C_{2^{n-1}}^{2^{n-1}-i+sp-sp} = C_{2^{n-1}}^{2^{n-1}+sp-(sp+i)}.$$

Запишем число p-сократимых функций второго типа в виде

$$2\sum_{s=1}^{[\frac{2^{n-1}}{p}]}\sum_{i} C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^{2^{n-1}+sp-(sp+i)}.$$

Рассмотрим сумму $\sum\limits_{i} C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^{2^{n-1}+sp-(sp+i)}$. Положим $j = sp+i$. Применяя свертку Вандермонда [7], получаем следующую оценку сверху:

$$\sum_{i} C_{2^{n-1}}^{sp+i} C_{2^{n-1}}^{2^{n-1}+sp-(sp+i)} \quad \leq \quad \sum_{j=0}^{2^{n-1}+sp} C_{2^{n-1}}^{j} C_{2^{n-1}}^{2^{n-1}+sp-j} \quad = \quad C_{2^n}^{2^{n-1}+sp}.$$

Оценим значение

$$2\sum_{s=1}^{[\frac{2^{n-1}}{p}]} C_{2^n}^{2^{n-1}+sp}.$$

Используя метод мультисекции рядов (см., например, [7]), и применяя его к формуле бинома Ньютона, получим $p\sum\limits_{s=0}^{[\frac{n-m}{p}]} C_n^{m+sp} \sim 2^n$ при $m < p$. Следовательно, с учетом симметрии биномиальных коэффициентов можем получить, что

$$2\sum_{s=1}^{[\frac{2^{n-1}}{p}]} C_{2^n}^{2^{n-1}+sp} \sim 2\frac{1}{2p}2^{2^n} = \frac{1}{p}2^{2^n}.$$

Соответственно, доля сократимых функций второго типа при $n \to \infty$ асимптотически не превышает $\frac{1}{p}$.

5. Заключение

Получено, что при $n \to \infty$ доля p-сократимых функций первого типа асимптотически равна $\sqrt{\frac{2}{\pi}}\frac{1}{2^{n/2}}$, а доля p-сократимых функций второго типа асимптотически не превышает $\frac{1}{p}$.

Следовательно, p-несократимые функции составляют асимптотически при $p \geq 5$ «большую часть» всех индуцированных вероятностных функций, однако если с ростом n доля p-сократимых функций первого типа уменьшается, то верхняя оценка доли p-сократимых функций второго типа асимптотически постоянна и зависит только от величины p.

Список литературы

[1] Схиртладзе Р. Л., “О синтезе р-схемы из контактов со случайными дискретными состояниями”, *Сообщ. АН ГрузССР*, **26**:2 (1961), 181—186.

[2] Салимов Ф. И., “Об одном семействе алгебр распределений”, *Изв. вузов. Математика*, 1988, № 7, 64—72.

[3] Колпаков Р. М., “Об оценках сложности порождения рациональных чисел вероятностными контактными π-сетями”, *Вестн. Моск. ун-та. Математика. Механика*, 1992, № 6, 62—65.

[4] Яшунский А. Д., “Алгебры вероятностных распределений на конечных множествах”, *Тр. МИАН*, **301** (2018), 320–335.

[5] Трифонова Е. Е., “О бесконечной порожденности пятеричных дробей в одном классе преобразователей вероятностей”, *Изв. высш. учебн. завед. Поволжский регион. Физ.-мат. науки*, 2021, № 1, 39—48.

[6] Трифонова Е. Е., “О некоторых свойствах конечно порождающих систем преобразователей p-ичных дробей”, *Дискретный анализ и исследование операций*, 2022, в печати.

[7] Риордан Дж., *Комбинаторные тождества*, Наука, Москва, 1982, 255 pp.

On the number of p-reducible induced probability functions

Trifonova E.E.

We study the proportion of Boolean functions inducing p=reducible functions of various types among all Boolean functions.

Keywords: Bernoulli random variable, finite generation, random variable transformation.

References

[1] Skhirtladze R. L., “On synthesis of p-schemes using switches with random discrete states”, *Soobshch. Akad. Nauk Gruz. SSR*, **26**:2 (1961), 181–186 (In Russian)

[2] Salimov F. I., “A family of distribution algebras”, *Izv. vuzov. Matematika*, 1988, № 7, 64–72 (In Russian)

[3] Kolpakov R. M., “On the bounds for the complexity of generation of rational numbers by stochastic contact π-networks”, *Vestn. Moskov. Univ. Ser. 1. Mat. Mekh.*, 1992, № 6, 62–65 (In Russian)

[4] Yashunsky A. D., “Algebras of Probability Distributions on Finite Sets”, *Tr. MIAN*, **301** (2018), 320–335 (In Russian)

[5] Trifonova E. E., “On infinite generativeness of quinary fractions in a class of probability transformers”, *Izv. vyssh. uchebn. zaved. Povolzhskiy region. Fiz.-mat. nauki*, 2021, № 1, 39–48 (In Russian)

[6] Trifonova E. E., “On some properties of finitely generating transformer sets for p-ary fractions”, *Discrete Analysis and Operations Research*, 2022, in print (In Russian)

[7] Riordan J., *Combinatorial identities*, Wiley, New York, 1968, 244 pp.