АКАДЕМИЯ НАУК СССР
СИБИРСКОЕ ОТДЕЛЕНИЕ
ИНСТИТУТ МАТЕМАТИКИ

ДИСКРЕТНЫЙ АНАЛИЗ

5

РЕДАКЦИОННО-ИЗДАТЕЛЬСКИЙ ОТДЕЛ СОАН СССР
НОВОСИБИРСК
1965

С о д е р ж а н и е

А К А Д Е М И Я Н А У К С С С Р
СИБИРСКОЕ ОТДЕЛЕНИЕ
ИНСТИТУТ МАТЕМАТИКИ

Д И С К Р Е Т Н Ы Й А Н А Л И З

Сборник трудов

Выпуск 5

РЕДАКЦИОННО-ИЗДАТЕЛЬСКИЙ ОТДЕЛ СО АН СССР
Н О В О С И Б И Р С К
1 9 6 5

ДИСКРЕТНЫЙ АНАЛИЗ

Сборник трудов

Выпуск 5 Института математики СО АН СССР 1965 г.

О ВОЗМОЖНОСТЯХ ВЫЧИСЛЕНИЯ ДИСКРЕТНЫХ ФУНКЦИЙ С НЕКОТОРОЙ ВЕРОЯТНОСТЬЮ

В.А.Малышев

Дискретной (n,m) – функцией мы будем называть отображение множества B_n двоичных последовательностей длины n в B_m.

Рассмотрим управляющую систему $\mathfrak{A}$, которая вычисляет некоторую (n,m) – функцию φ. Иногда достаточно уметь правильно вычислять функцию для довольно большого числа аргументов.

Будем говорить, что (n,m) – функция f p – вычисляется управляющей системой $\mathfrak{A}$, если функции f и φ совпадают по крайней мере для $[p2^n]$ значений аргументов (здесь $0 \leq p \leq 1$). Если, например, на множестве значений аргументов задано равномерное распределение вероятностей, то функция f p – вычисляется системой $\mathfrak{A}$ тогда и только тогда, когда с вероятностью, не меньшей p, получается правильное значение функции f.

Нашей целью будет получение асимптотики для функции Шеннона для данной задачи. Мы будем постоянно пользоваться методами и терминологией работы [I] и для простоты формулировок ограничимся рассмотрением класса схем из таких функциональных элементов, которые могут реализовать всевозможные функции от двух переменных. Под сложностью схемы понимается число элементов в схеме.

Пусть $L(f,\rho)$ — наименьшая из сложностей схем, ρ — вычисляющих функцию f. Положим

$$L(n,m,\rho) = \max L(f,\rho)$$

(максимум берется по всевозможным (n,m) — функциям f).

ТЕОРЕМА. Если $m(n)\to\infty$ и $\frac{\log_2 m(n)}{n}\to 0$, то

$$L(n,m(n),\rho) \sim \frac{\rho\, m(n) 2^n}{n},$$

причем для любого $\varepsilon>0$ доля $(n,m(n))$-функций f, для которых

$$L(f,\rho) \leqslant (1-\varepsilon)\frac{\rho\, m(n) 2^n}{n}$$

стремится к нулю с ростом n.

При $\rho=1$ мы имеем известный результат О.Б.Лупанова, при $\rho=0$ результат очевиден. Оценка сверху сразу получается из известной оценки для случая $\rho=1$. Действительно, если ρ иррационально, то убывающая последовательность двоично-рациональных $\rho_n=\frac{k'(n)}{2^{k(n)}}$ сходится к ρ, причем $\frac{k(n)}{n}\to 0$. Булевы функции

$$f_j(x_1,\dots,x_n),\ j=1,\dots,m(n),$$

соответствующие $(n,m(n))$ — функции f можно представить в виде:

$$f_j(x_1,\dots,x_n) = \bigvee_{\sigma_1,\dots,\sigma_{k(n)}} x_1^{\sigma_1}\cdot\ldots\cdot x_{k(n)}^{\sigma_{k(n)}}\cdot f_j(\sigma_1,\dots,\sigma_{k(n)},x_{k(n)+1},\dots,x_n).$$

Из функций

$$\psi_j(x_{k(n)+1},\dots,x_n) = f_j(\sigma_1,\dots\sigma_{k(n)},x_{k(n)+1},\dots,x_n)$$

$2^{k(n)}-k'(n)$ можно выбрать какими угодно, а для остальных использовать оценку сверху О.Б. Лупанова. Это и дает искомую оценку сверху, ибо

$$2^{K(n)}+m(n)\frac{2^{n-K(n)}}{n-K(n)}\cdot K!(1+o(1))\sim\frac{\rho m(n)2^n}{n}.$$

Доказательство оценки снизу основывается на следующей ЛЕММЕ: множество (n,m) - функций такое, что любая (n,m) -функция по крайней мере с одной функцией из этого множества совпадает не меньше чем на $[\rho 2^n]$ наборах, содержит не менее $2^{(m\rho-1)2^n}$ функций.

Определим расстояние между двумя (n,m) -функциями f_1 и f_2 как число наборов, на которых значения функций не совпадают. Нетрудно показать, что множество (n,m) - функций с введенным таким образом расстоянием превращается в метрическое пространство $\mathfrak{M}_{n,m}$. Некоторое множество функций $\mathcal{L}$ мощности L только тогда образует $(d+1)$ - сеть в $\mathfrak{M}$, когда L замкнутых шаров радиуса d с центрами в точках множества $\mathcal{L}$ покрывают все пространство, то есть когда

$$L\cdot\left(\sum_{i=0}^{d}C_N^i(M-1)^i\right)\geqslant M^N,$$

где $N=2^n$, $M=2^m$.

Отсюда получается энтропийная оценка снизу для мощности L_{min}, минимальной $[(1-\rho)N+1]$ - сети в $\mathfrak{M}_{n,m}$ (достаточно ограничиться двоично-рациональными ρ):

$$L_{min}\geqslant\frac{1}{\sum\limits_{i=0}^{(1-\rho)N}C_N^i\left(\frac{M-1}{M}\right)^i\cdot\left(\frac{1}{M}\right)^{N-i}}=$$

$$=M^{\rho N}\cdot\frac{1}{\sum\limits_{i=0}^{(1-\rho)N}C_N^i\left(\frac{M-1}{M}\right)^i\left(\frac{1}{M}\right)^{(1-\rho)N-i}}\geqslant\frac{M^{\rho N}}{2^N}=L'.$$

Для доказательства второго утверждения теоремы и оценки снизу достаточно [I] показать, что при $K(n)=(1-\varepsilon)\frac{\rho m(n)2^n}{n}$ и $n\longrightarrow\infty$

$$\frac{N(n,K(n))}{L'}\longrightarrow 0.$$

Здесь, также как в [I], $N(n,K(n))$ есть число схем из функциональных элементов сложности не более $K(n)$, реа -

лизующих $(n, m(n))$ — функции. Методами, аналогичными таковым в [I], можно доказать, что для некоторого C

$$N(n,k(n)) < \left[C(n+k(n))\right]^{n+k(n)+m(n)+c}$$

(единственное отличие состоит в том, что рассматриваются деревья с $m(n)$ корнями).

Действительно, имеем $\log \frac{N(n,k(n))}{L'} =$

$$= (1-\varepsilon)\frac{p\,m(n)2^n}{n}\cdot\log\frac{(1-\varepsilon)p\,m(n)2^n}{n}\cdot(1+o(1)) - p\,m(n)2^n + 2^n =$$

$$= \left[(1-\varepsilon)\frac{p\,m(n)2^n}{n}(n+\log m(n)-\log n+\log p(1-\varepsilon)\right](1+o(1)) - p\,m(n)2^n +$$

$$+ 2^n = -\varepsilon p 2^n m(n)(1+o(1)) \to -\infty .$$

Здесь существенно используется условие $m(n)\to\infty$. Без этого условия теорема, вообще говоря, неверна (например, для случая $p \leq \frac{1}{2}$, $m(n) = const$). Исследование случая $p \geq \frac{1}{2}$, $m(n) = const$ наталкивается на нерешенную задачу получения более точных нижних кодовых границ (заметим, что если функцию рассматривать как набор длины 2^n с 2^m возможными значениями, то $\mathfrak{M}_{n,m}$ превращается в известное в теории кодирования метрическое пространство с расстоянием Хэмминга и границей Гильберта).

Автор благодарит Олега Борисовича Лупанова за внимание к работе и ценные замечания.

Литература

I. О.Б.Лупанов. О синтезе некоторых классов управляющих систем. — Сб. "Проблемы кибернетики", вып. IO, М., Физматгиз, 1963.