ТЕОРЕТИКО-ИНФОРМАЦИОННЫЙ ПОДХОД К ПОЛУЧЕНИЮ НИЖНИХ ОЦЕНОК СЛОЖНОСТИ

Д. Ю. Черухин (Москов)

В работе предложена аксиоматическая теория, описывающая количественные свойства информации. Показана возможность применения этой теории к получению эффективных нижних оценок сложности схем из функциональных элементов (СФЭ, [1]).

Информационным пространством (*ИП*) назовём систему $\mathrm{IS} = (M, \circ, |\cdot|)$, где M — множество объектов, называемых *сообщениями*, $\circ\colon M^2 \to M$ — операция *объединения* сообщений, $|\cdot|\colon M \to \mathbb{R}$ — функционал *нормы* сообщения, причём выполнены следующие аксиомы (для любых $x, y, z \in M$):

I. $x \circ x = x$ (идемпотентность)

II. $x \circ y = y \circ x$ (коммутативность)

III. $(x \circ y) \circ z = x \circ (y \circ z)$ (ассоциативность)

IV. $\exists \Lambda\ (|\Lambda| = 0 \,\&\, \forall t\ \Lambda \circ t = t)$ (существование нуля)

V. $|x \circ y| + |x \circ z| \geqslant |x \circ y \circ z| + |x|$ (сильная субаддитивность)

Отметим, что под сообщением мы понимаем не конкретный текст, а нечто общее, присущее некоторым текстам, несущим одну и ту же информацию; норма сообщения есть количество информации. Отметим также, что теория ИП тесно связана с такими известными структурами, как субмодулярные решётки и матроиды.

Приведём три примера ИП.

1. M — измеримое пространство, $\circ$ — объединение множеств, $|\cdot|$ — мера множества.

2. M — множество подпространств данного линейного пространства, $\circ$ — сумма подпространств, $|\cdot|$ — размерность.

3. M — множество систем булевых функций, зависящих от переменных $x_1, \ldots, x_n$, $\circ$ — объединение систем, норму определим ниже. Для системы $S = \{f_1, \ldots, f_m\}$ введём отношение эквивалентности ρ_S на множестве $\{0,1\}^n$:

$$\tilde{x}\ \rho_S\ \tilde{y} \Longleftrightarrow \forall f \in S\ f(\tilde{x}) = f(\tilde{y}).$$

Пусть $K_1, \ldots, K_t$ — все классы эквивалентности отношения ρ_S. Положим

$$|S| = -\sum_{i=1}^{t} p_i \log_2 p_i, \quad \text{где } p_i = \frac{|K_i|}{2^n},\ i = 1, \ldots, t. \tag{1}$$

Например, если $1 \leqslant i_1 < \ldots < i_k \leqslant n$, то $|\{x_{i_1}, \ldots, x_{i_k}\}| = k$.

В трёх приведённых примерах наибольшую сложность вызывает доказательство сильной субаддитивности энтропии Шеннона (1). Далее мы будем работать только с примером 3.

Назовём *n-сетью* ациклический ориентированный граф с n входами и n выходами, в котором входная степень каждого входа равна 0, а входная степень любой вершины, отличной от входов, равна 2; входы и выходы упорядочены. Сложность сети есть число вершин, отличных от входов. Скажем, что СФЭ C *вписана* в сеть S, если C можно получить из S приписыванием всем вершинам, отличным от входов, двуместных булевых функций (считаем, что входам соответствуют переменные $x_1, \ldots, x_n$).

Рассмотрим оператор циклического сдвига [2] F_n с n информационными входами. Пусть $F_n^0, \ldots, F_n^{n-1}$ — его подоператоры, причём F_n^i получен из F_n подстановкой вместо управляющих переменных констант, образующих двоичную запись числа i. Тогда F_n^i — перестановочный оператор, полученный из тождественного циклическим сдвигом выходов на i позиций. В [2] показано, что сложность F_n в классе СФЭ нелинейна тогда и только тогда, когда нелинейна минимальная сложность сети, в которую можно вписать СФЭ для каждого из операторов $F_n^0, \ldots, F_n^{n-1}$.

Пусть S — сеть, в которую вписаны СФЭ $C^0, \ldots, C^{n-1}$, где C^i реализует оператор F_n^i. Зафиксируем i. Каждой вершине v сети S припишем функцию $f_v^i(x_1, \ldots, x_n)$, вычисляемую в вершине v схемы C^i. Рассмотрим эту функцию, как сообщение ИП из примера 3 (функцию f мы отождествляем с системой $\{f\}$). Тогда, если вершина v непосредственно предшествует вершинам v' и v'', то

$$f_v^i \subseteq f_{v'}^i \circ f_{v''}^i, \tag{2}$$

где под вложением в ИП понимается следующее отношение:

$$x \subseteq y \Longleftrightarrow |x \circ y| = |y|.$$

Прямой суммой ИП $(M_1, \circ_1, |\cdot|_1)$ и $(M_2, \circ_2, |\cdot|_2)$ называется ИП $(M_1 \times M_2, \circ, |\cdot|)$, где объединение $\circ$ выполняется покоординатно, а $|(x, y)| = |x|_1 + |y|_2$. Рассмотрим ИП IS_n, являющееся прямой суммой n экземпляров ИП из примера 3. Каждой вершине v сети S сопоставим сообщение $f_v = (f_v^0, \ldots, f_v^{n-1})$ ИП IS_n. Тогда вложение (2) сохранится, а именно,

$$f_v \subseteq f_{v'} \circ f_{v''}. \tag{3}$$

Отметим также, что норма одной булевой функции не больше единицы, а значит,

$$|f_v| \leqslant n. \tag{4}$$

Введём функцию $\rho(x, y)$, характеризующую меру зависимости сообщений:

$$\rho(x, y) = |x| + |y| - |x \circ y|.$$

В частности, если $\rho(x, y) = 0$, то можно сказать, что сообщения x и y *независимы*. Пусть $X = \{v_1, \ldots, v_k\}$ — множество некоторых входов сети S, а $Y = \{w_1, \ldots, w_l\}$ — множество некоторых её выходов, $|X| = k$, $|Y| = l$. Обозначим $f_X = f_{v_1} \circ \ldots \circ f_{v_k}$, $f_Y = f_{w_1} \circ \ldots \circ f_{w_l}$. Тогда

$$|f_X| = kn, \quad |f_Y| = ln, \quad \rho(f_X, f_Y) = kl. \tag{5}$$

Идея применения теории ИП к получению нижней оценки сложности СФЭ для оператора сдвига состоит в том, чтобы попробовать доказать нижнюю оценку для сложности сети S, в которой каждой вершине сопоставлено сообщение некоторого ИП, причём выполнены соотношения (3)–(5). На этом пути удалось получить нижнюю оценку $2,5n(1 - o(1))$.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.01) и программы "Университеты России" (проект УР.04.02.528).

Список литературы

1. Лупанов О. Б. Нижние оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Черухин Д. Ю. Об информационной составляющей в сложности оператора сдвига // Дискрет. анализ и исслед. операций. — 2005. — Т. 12, No 2. — с. 73–77.