

А. Н. МАСЛОВ

ВЕРОЯТНОСТНЫЕ МАШИНЫ ТЬЮРИНГА И РЕКУРСИВНЫЕ ФУНКЦИИ

(Представлено академиком А. Н. Колмогоровым 5 X 1971)

Целью настоящей работы является описание класса функций, вычисляемых на машинах Тьюринга при использовании датчика случайных чисел.

Частичным распределением называется последовательность действительных чисел $p = (p_0, p_1, p_2, \dots)$ такая, что $\forall i \quad p_i \geq 0$ и $\sum p_i \leq 1$. Множество частичных распределений обозначим через P , а множество натуральных чисел через N .

P -функцией от k переменных будем называть отображение $f: N^k \rightarrow P$. Будем отождествлять частичную функцию $f: N^k \rightarrow N$ с P -функцией $f: N^k \rightarrow P$ такой, что $(f(x))_j = 1$, если $f(x) = j$ и $(f(x))_j = 0$ в остальных случаях. Такие P -функции назовем детерминированными. Для P -функции f содержательно $(f(x))_j$ обозначает вероятность того, что функция f принимает значение j на векторе $x \in N^k$.

Обозначим через ap вектор $(ap_0, ap_1, ap_2, \dots)$, а через $\sum_{j \in J} p^{(j)}$ вектор

$$\left(\sum_{j \in J} p_0^{(j)}, \sum_{j \in J} p_1^{(j)}, \sum_{j \in J} p_2^{(j)}, \dots \right).$$

Определение 1. Пусть даны P -функции f от r переменных и $g_1, g_2, \dots, g_r$ от k переменных каждая. Тогда равенство

$$f(g_1, g_2, \dots, g_r)(x) = \sum_{i_1, i_2, \dots, i_r} (g_1(x))_{i_1} (g_2(x))_{i_2} \dots (g_r(x))_{i_r} f_i(t_1, t_2, \dots, t_r),$$

где $x \in N^k$, определяет их суперпозицию.

Определение 2. Пусть даны две P -функции f_1 от $n-1$ переменных и f_2 от $n+1$ переменных. Равенства

$$g(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) = f_1(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n),$$

и

$$\begin{aligned} &g(x_1, \dots, x_{i-1}, x_i + 1, x_{i+1}, \dots, x_n) = \\ &= \sum_j (g(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n))_j f_2(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n, j) \end{aligned}$$

определяют P -функцию g от n переменных. Будем говорить, что g определена через f_1 и f_2 с помощью примитивной рекурсии по i -му аргументу.

Определение 3. Пусть дана P -функция f от $n+1$ переменных. Оператор минимизации по i -му аргументу μ_{x_i} на P -функции f определяется равенством

$$(\mu_{x_i} f)(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) = (q_0, q_1, q_2, \dots),$$

где

$$q_0 = (f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_k))_0,$$

$$q_{j+1} = (f(x_1, \dots, x_{i-1}, j+1, x_{i+1}, \dots, x_k))_0 \prod_{m \leq j} Q_m,$$

$$Q_m = \sum_{n=1}^{\infty} (f(x_1, \dots, x_{i-1}, m, x_{i+1}, \dots, x_k))_n.$$

Таким образом, $\mu_{x_i} f$ является P -функцией от $k-1$ переменной.

Элемент распределения q_j есть вероятность того, что $f(x_1, \dots, x_{i-1}, j, x_{i+1}, \dots, x_k) = 0$, а для всех $m < j$ $f(x_1, \dots, x_{i-1}, m, x_{i+1}, \dots, x_k) \neq 0$.

Для детерминированных функций наши операции совпадают с одноименными операциями над вычислимыми функциями ⁽¹⁾. Здесь равенство $\sum p_i = 1$ заменяет свойство всюду определенности. Частичное распределение с $\sum p_i = 1$ мы назовем полным распределением или просто распределением. Если $\forall x \in N^k$ $f(x)$ является полным распределением, то P -функцию f назовем также полной. В обозначениях определения 3 для полных функций выполнено равенство

$$q_{j+1} = (f(x_1, \dots, x_{i-1}, j+1, x_{i+1}, \dots, x_k))_0 \cdot \left(1 - \sum_{m \leq j} q_m\right).$$

Определение 4. Класс P -функций называется рекурсивно замкнутым, если он замкнут относительно суперпозиции, примитивной рекурсии и минимизации, а также содержит P -функции $\lambda(x) = x+1$, $O(x) = 0$, $I_k^j(x_1, \dots, x_j, \dots, x_k) = x_j$ для всех $j \leq k$ и $D(x) = (1/2, 1/2, 0, \dots, 0, \dots)$.

Минимальный такой класс назовем классом рекурсивных P -функций или RP -функций.

Машина Тьюринга, которая использует, как в ⁽²⁾, датчик случайных чисел, выдающий 0 с вероятностью p и 1 с вероятностью $1-p$, причем p — конструктивное число (будем называть такую машину вероятностной), вычисляет P -функцию $f(x)$, у которой $(f(x))_i$ есть вероятность получить на выходной ленте число i при входном кортеже $x \in N^k$. Известно, что для всякой вероятностной машины Тьюринга, существует вероятностная машина Тьюринга, использующая датчик с $p = 1/2$ и вычисляющая ту же P -функцию.

Заметим, что машина, пишущая на выходной ленте первое значение датчика, вычисляет $D(x)$, а функции $\lambda(x)$, $O(x)$ и $I_k^j(x_1, \dots, x_k)$ вычисляются без использования датчика.

Лемма 1. Класс P -функций, вычисляемых на вероятностных машинах Тьюринга, замкнут относительно суперпозиции, примитивной рекурсии и минимизации.

Доказательство в точности повторяет доказательство замкнутости в случае детерминированных функций ⁽¹⁾. Например, для минимизации вычисляем $f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_k)$; если получим 0, то на выходной ленте пишем 0; в противном случае вычисляем $f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_k)$; если получим 0, то на выходной ленте пишем 1; в противном случае вычисляем $f(x_1, \dots, x_{i-1}, 2, x_{i+1}, \dots, x_k)$ и т. д.

Лемма 2. Каждая P -функция, вычисляемая на вероятностной машине Тьюринга, является рекурсивной.

Пусть задана функция $p: N^k \rightarrow [0, 1]$. Обозначим $W(p(x), n)$ n -й знак в двоичном разложении числа $1-p(x)$.

Обозначим $p_i(x, i, z)$ вероятность попасть из мгновенного описания (м.о.) вероятностной машины Тьюринга с номером x за i шагов в м.о. с номером z ; $p_2(x, i, z)$ — условную вероятность попасть из м.о. с номером x в м.о. с номером z за i шагов при условии, что попали в заключительное

м.о. впервые на i -м шаге; $p_3(x, i)$ — вероятность попасть из м.о. с номером x впервые на i -м шаге в заключительное м.о.; $p_4(x, i) = p_3(x, i) / (1 - \sum_{j=0}^{i-1} p_3(x, j))$ и $p_5(x, i, z) = p_2(x, i, z) / (1 - \sum_{y=0}^{z-1} p_2(x, i, y))$. Считаем $p_4 = 0$ ($p_5 = 0$), если $p_3 = 0$ ($p_2 = 0$).

Легко проверить, что $W(p_1(x, i, z), n)$, $W(p_2(x, i, z), n)$ и $W(p_3(x, i), n)$ — общерекурсивные функции, а множества $\{(x, i) | p_3(x, i) = 0\}$ и $\{(x, i, z) | p_2(x, i, z) = 0\}$ разрешимы. Поэтому $W(p_4(x, i), n)$ и $W(p_5(x, i, z), n)$ — также общерекурсивные функции.

Введем P -функции $\varphi(x, i) = \mu_z(W(p_5(x, i, z), D_1))$ и $\psi(x) = \mu_i(W(p_4(x, i), D_1))$, где $D_1 = \mu_y D(y) = (1/2, 1/4, 1/8, \dots)$, так что $p_3(x, i) = (\psi(x))_i$ и $p_2(x, i, z) = (\varphi(x, i))_z$.

Пусть $\beta(x)$ — номер начального м.о., когда на входной ленте машины написан вектор $x \in N^k$; $\gamma(x)$ — число на выходной ленте, когда машина пришла в заключительное м.о. с номером x (в других случаях $\gamma(x) = (0, 0, 0, \dots)$). Очевидно β и γ — RP -функции.

RP -функция $\alpha(x) = \gamma(\varphi(\beta(x), \psi(\beta(x))))$ является искомой, так как $(\alpha(x))_j$ равна сумме по i вероятностей взаимоисключающих событий: попасть в заключительное м.о. впервые на i -м шаге и написать при этом j на выходной ленте. Каждая такая вероятность равна произведению вероятности попасть впервые в заключительное м.о. на i -м шаге на условную вероятность написать при этом j на выходной ленте.

Из доказанного немедленно вытекает

Теорема. Класс рекурсивных P -функций совпадает с классом P -функций, вычислимых на вероятностных машинах Тьюринга.

Следствие. Если в наших определениях всюду последовательности чисел $p = (p_0, p_1, p_2, \dots)$ заменить на последовательности из 0 и 1 (0, если $p_i = 0$, и 1, если $p_i > 0$), а операции над числами — соответствующими булевыми операциями, то будет определен класс функций $N^k \rightarrow 2^N$. И этот класс совпадает с классом функций, вычислимых на недетерминированных машинах Тьюринга.

Замечание. Пусть дана P -функция $f: N^k \rightarrow P$ и оракул A_f , ее вычисляющий, т. е., прочитав $x \in N^k$, оракул пишет число i с вероятностью $(f(x))_i$. Машина Тьюринга T , которая может обращаться к оракулу A_f , вычисляет P -функцию T_f . Представляется неясным, будет ли P -функция T_f принадлежать рекурсивному замыканию P -функций $\lambda, 0, I_k^j, D$ и f . В частности, будет ли принадлежать их рекурсивному замыканию P -функция Mf такая, что $(Mf(x))_0 = 0$, и $(Mf(x))_{i+1} = (f(x))_{i+1} / (1 - f(x))_0$ для всех i (если $(f(x))_{i+1} = 0$, то $(Mf(x))_{i+1} = 0$)? Последние два вопроса эквивалентны.

Автор выражает признательность А. А. Мучнику за полезное обсуждение.

Поступило
1 IX 1971

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

- ¹ В. А. Успенский, Лекции о вычислимых функциях, М., 1960. ² К. де Леу, Э. Ф. Мур и др., Сборн. Автоматы, М., 1956.