Задачи по теории

(1) Теорема Храпченко. Доказать, что для функции f от n переменных нижняя оценка сложности $L^\pi(f)$, получаемая по этой теореме, не может быть больше, чем n^2.

(2) Является ли класс $M \cap S$ инвариантным?

(3) Привести пример класса булевых функций, замкнутого относительно переименования (без отождествления) переменных, относительно подстановки констант, но не являющегося инвариантным.

(4) При каких условиях замкнутый класс булевых функций является инвариантным? Привести пример замкнутого, но не инвариантного класса. Привести пример инвариантного, но не замкнутого класса.

(5) Какие из классов булевых функций T_0, T_1, L, M, S являются инвариантными, а какие - нет?

(6) Что такое порождающее множество инвариантного класса? Почему порождающий элемент зависит от всех своих переменных существенно? Найти порождающее множество инвариантного класса M всех монотонных функций.

(7) Найти мощностную константу σ инвариантного класса L всех линейных функций.

(8) Пусть Б $= \{m, \&, \vee, \neg\}$, где $m(x, y, z) = xy \vee xz \vee yz$, конъюнкция и дизъюнкция двухвходовые, а веса элементов равны $L_m = 1$, $L_\& = 2$, $L_\vee = 3$, $L_\neg = 4$. Чему равна асимптотика функций Шеннона $L^C_{\text{Б}}(n)$ и $L^{\Phi}_{\text{Б}}(n)$ для сложности СФЭ и формул в этом базисе?

(9) Селекторное разбиение множества переменных функции. Энтропия разбиения. Для множества булевых переменных функции $\varphi = y_1(y_2 \vee y_3) \vee y_4(y_5 \vee y_6)$ найти селекторное разбиение, энтропия которого равна 1.

(10) Метод Э. И. Нечипорука. Двухуровневая выборка из памяти и применение к ней этого метода для случая формул.

(11) От какого минимального числа переменных может зависеть функция двухуровневой выборки из памяти? Записать формулу для такой функции.

Ответы

(1) Теорема Храпченко. Для произвольной функции $f \in P_2(n)$ и для любых $\mathcal{N}' \subseteq N_f$ и $\mathcal{N}'' \subseteq \overline{N}_f$:

$$L^\pi(f) \geqslant \frac{|\mathcal{R}(\mathcal{N}', \mathcal{N}'')|^2}{|\mathcal{N}'| \cdot |\mathcal{N}''|},$$

где $\mathcal{R}(\mathcal{N}', \mathcal{N}'') = \{(\alpha, \beta) : \alpha \in \mathcal{N}', \beta \in \mathcal{N}'', \rho(\alpha, \beta) = 1\}$.

Справедлива оценка: $|\mathcal{R}(\mathcal{N}', \mathcal{N}'')| \leqslant n \cdot \min(|\mathcal{N}'|, |\mathcal{N}''|)$ (возьмем наименьшее множество, из каждой его вершины выходит не более n ребер). Тогда

$$\frac{|\mathcal{R}(\mathcal{N}', \mathcal{N}'')|^2}{|\mathcal{N}'| \cdot |\mathcal{N}''|} \leqslant \frac{n^2 \cdot (\min(|\mathcal{N}'|, |\mathcal{N}''|))^2}{|\mathcal{N}'| \cdot |\mathcal{N}''|} = \frac{n^2 \cdot \min(|\mathcal{N}'|, |\mathcal{N}''|)}{\max(|\mathcal{N}'|, |\mathcal{N}''|)} \leqslant n^2.$$

(2) Самая «популярная» функция из класса $M \cap S$ — медиана $xy \vee xz \vee yz$. При подстановки $z = 0$ дает функцию xy, не являющуюся самодвойственной.

(3) Класс симметрических функций. Он замкнут относительно переименования (без отождествления) переменных, относительно подстановки констант, но не замкнут относительно добавления фиктивных переменных. Например $f(x, y) = x \oplus y$ ему принадлежит, а $g(x, y, z) = x \oplus y$ ему не принадлежит.

(4) Замкнутый класс булевых функций является инвариантным тогда и только тогда, когда подстановка констант 0 и 1 вместо переменных не приводит к новым функциям. Примеры замкнутого, но не инвариантного класса – класс T_0, класс $\{x\}$. Пример инвариантного, но не замкнутого класса – класс $\{0, 1, \bar{x}\}$.

(5) Классы T_0, T_1, S не являются инвариантными, так как не замкнуты относительно подстановки констант. Классы L и M инвариантны.

(6) $g \in P_2 \setminus Q$ – порождающий элемент инвариантного класса Q, если любая собственная (хотя бы одну константу подставили) квазиподфункция g входит в Q. Порождающий элемент зависит от всех своих переменных существенно, так как иначе, имея, например, фиктивную переменную x_i, можно было бы осуществить подстановку константы вместо нее и получить собственную квазиподфункцию не из Q. Порождающее множество инвариантного класса — максимальное по включению множество попарно не конгруэнтных порождающих элементов. Порождающее множество инвариантного класса M всех монотонных функций — $\{\bar{x}\}$. См. лемму о немонотонной функции — из любой немонотонной функции с помощью подстановок функций 0, 1, x можно получить функцию $\bar{x}$. То есть если бы была еще другая функция, то у нее нашлась бы собственная подфункция $\bar{x}$, не входящая в инвариантный класс M.

[1]Замечания можно присылать на vkonovodov@gmail.com

(7) $|L(n)| = 2^{n+1}$, $\dfrac{\log|L(n)|}{2^n} \to 0$ при $n \to \infty$. То есть мощностная константа равна 0.

(8) Найдем приведенный вес базиса. Приведенные веса элементов, имеющих хотя бы 2 входа: $\rho_m = \frac{1}{2}$, $\rho_{\&} = 2$, $\rho_{\vee} = 3$. Приведенный вес базиса, таким образом, $\frac{1}{2}$. Следовательно,

$$L_{\text{Б}}^{C}(n) \sim \frac{2^{n-1}}{n}, \quad L_{\text{Б}}^{\Phi}(n) \sim \frac{2^{n-1}}{\log n}.$$

(9) Пусть $\varphi(y_1, \ldots, y_N)$ – функция, существенно зависящая от всех своих переменных из множества $Y = \{y_1, \ldots, y_N\}$, а D – разбиение множества Y на компоненеты $Y_1, \ldots, Y_d$. Разбиение D называется селекторным для функции $\varphi(Y)$, если для каждого i, $i = 1, \ldots, d$, и для любой переменной y, $y \in Y_i$, найдутся константы $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_d$, такие, что при подстановке их вместо переменных из $Y_1, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_d$ соответственно, выполняется равенство $\varphi = y \oplus \alpha_i$, $\alpha_i \in \{0, 1\}$. Энтропия разбиения $H(D) = -\sum\limits_{i=1}^{d} \dfrac{|Y_i|}{|Y|} \log \dfrac{|Y_i|}{|Y|}$.

Искомое разбиение для $\varphi = y_1(y_2 \vee y_3) \vee y_4(y_5 \vee y_6)$:

$$\{\{y_1\}, \{y_4\}, \{y_2, y_5\}, \{y_3, y_6\}\},$$

его энтропия равна 1.

(10) Метод Нечипорука. Пусть f – булева функция от переменных $X(n) = \{x_1, \ldots, x_n\}$. Рассмотрим подмножество $X \subseteq X(n)$ и его разбиение на $X_1, \ldots, X_p$. Для каждого i, $1 \leqslant i \leqslant p$, пусть F_i – множество различных остаточных функций функции f, которые зависят только от переменных X_i. Тогда

$$L^K(f) \geqslant \sum_{i=1}^{p} h_i,$$

где h_i – минимальное решение неравенства $(8|X_i|\, h_i)^{h_i} \geqslant |F_i|$, и

$$R_{\text{Б}}(f) \geqslant \frac{1}{k_{\text{Б}} + 2} \sum_{i=1}^{p} \log|F_i|.$$

Двухуровневая выборка из памяти – функция

$$f(x_1, \ldots, x_n) = f(u_1, \ldots, u_{m-q}, z_0, \ldots, z_{s-1}, y_0, \ldots, y_{s-1},$$

где $m = 2^q$, $s = 2^m$, $p = \frac{s}{m} = 2^{m-q}$, определяемая для любого $\alpha \in B^{m-q}$ как

$$f(\alpha, z, y) = y_{\nu\left(z^{(\nu(\alpha))}\right)},$$

переменные группы z разбиты на p групп по m переменных $(Z^{(0)}, \ldots, Z^{(p-1)})$. То есть набор u задает номер группы z, в которой написан номер y, выдаваемого на выход.

В качетсве X_i возьмем $Z^{(i)}$. Найдем множество F_i. Подфункция f будет зависеть от X_i, если $\nu(u) = i$, от переменных остальных групп $Z^{(j)}$, $j \neq i$, зависимости нет. Тогда каждая такая подфункция имеет вид

$Z^{(i)}$			
0	…	0	y_0
	…		…
1	…	1	y_{s-1}

то есть задается однозначно теми константами, которые присваиваются переменным группы y, следовательно, $|F_i| = 2^s = 2^{2^m} = 2^{2^{2^q}}$.

Число переменных функции $n = m - q + 2s = 2^q - q + 2^{2^q} \asymp 2^{2^q}$. Подмножество $X = Z$ разбивается на $p = 2^{2^q - q}$ групп. Потому

$$L_{\text{Б}}^{\Phi}(f) \geqslant \frac{1}{k_{\text{Б}} + 2} \sum_{i=1}^{p} \log|F_i| \asymp 2^{2^q} \cdot 2^{2^q - q} = \frac{2^{2 \cdot 2^q}}{2^q} \asymp \frac{n^2}{\log n}.$$

(11) От 5 переменных:

$$f(u, z_0, z_1, y_0, y_1) = \bar{u}(\bar{z}_0 y_0 \vee z_0 y_1) \vee u(\bar{z}_1 y_0 \vee z_1 y_1).$$