EESTI NSV TEADUSTE AKADEEMIA TOIMETISED. 30. KÖIDE
FÜÜSIKA * MATEMAATIKA. 1981, NR. 4

ИЗВЕСТИЯ АКАДЕМИИ НАУК ЭСТОНСКОЙ ССР. ТОМ 30
ФИЗИКА * МАТЕМАТИКА. 1981, № 4

Т. ЛАУСМАА

ОБ УЧИТЫВАНИИ СИММЕТРИИ ПРЕДСТАВЛЕНИЯ ПРИ ИНФОРМАЦИОННОЙ ОЦЕНКЕ ДИСКРЕТНЫХ ФУНКЦИЙ

(Представил Н. Алумяэ)

В [1], интерпретируя булевую функцию как систему информационных каналов от входа к выходу в форме разбиений, мы ввели для оценки сложности булевых функций понятие комбинаторно-информационной связки (КИС). Однако КИС не учитывала полностью симметрию представления функций, а от симметрии объекта, как известно, в значительной степени зависит его сложность (напр., при периодической последовательности каких-то символов эта последовательность полностью определяется ее периодом, а при случайной последовательности мы не имеем для нее лучшего описания, чем ее полное задание).

Развитый в настоящей работе формальный аппарат позволяет характеризовать симметрию в информационных терминах. В работе вводится в рассмотрение ряд естественных свойств систем пар разбиений, которые используются для характеристики дискретных функций. В результате такого подхода определяется для дискретных функций понятие минимальной информационной связки (МИС), которое, в отличие от КИС, учитывает полностью симметрию в системе пар разбиений и является поэтому лучшим показателем степени сложности, что подтвердилось и на практике при оценке сложности булевых функций.

Пусть дано конечное множество $X = \{x_1, x_2, \ldots, x_m\}$. Для любого подмножества $X' \subset X$ определим его комбинаторный вес $q(X')$ как отношение $q(X') \underset{\text{Df}}{=} \|X'\|/\|X\|$ ($\|X^i\|$ — мощность множества X^i). Разбиение множества X на непересекающиеся подмножества (блоки) $B_i^{(1)}, B_i^{(2)}, \ldots, B_i^{(\alpha)}, \ldots, B_i^{(m_i)}$ обозначим через $\pi_i(X)$. В частности, нулевое разбиение будем обозначать через 0_X, а единичное — через 1_X. Блок разбиения $\pi_i(X)$, содержащий элемент $x_\alpha \in X$, обозначим через $B_i(x_\alpha)$. Для любых $x_i, x_j \in X$ и $\pi_h(X)$ положим $x_i \equiv x_j(\pi_h)$, если и только если найдется $B_h^{(\alpha)} \in \pi_h$ такой, что $x_i, x_j \in B_h^{(\alpha)}$. Разбиения $\pi_i(X')$ и $\pi_j(X'')$ назовем эквивалентными и обозначим $\pi_i(X') \equiv \pi_j(X'')$, если и только если существует биекция $\varphi : \pi_i \to \pi_j$ такая, что для любого $B_i^{(\alpha)} \in \pi_i$ имеет место $q(B_i^{(\alpha)}) = q(\varphi(B_i^{(\alpha)}))$. Сужением разбиения $\pi_i(X)$ на $X' \subset X$ назовем разбиение $\overline{\pi}_i(X') \underset{\text{Df}}{=} \{B_i^{(\alpha)} \cap X' \mid B_i^{(\alpha)} \in \pi_i\}$. Определим для каждого разбиения $\pi_i(X)$ энтропию

$$H(\pi_i) = -\sum_{\alpha=1}^{m_i} q(B_i^{(\alpha)}) \ln q(B_i^{(\alpha)}).$$

Систему разбиений $P(X)$ назовем независимой, если и только если при произвольных $\pi_i \in P(X)$ и $P' \subset P$, где $\pi_i \notin P'$, для любого блока $B \in m(P')$ ($m(P^{(\alpha)}) \underset{\text{Df}}{=} \prod_{\pi_i \in P^{(\alpha)}} \pi_i$) всегда справедливо $\overline{\pi}_i(B) \equiv \pi_i(X)$.

Ясно, что если система P независима, то подсистема $P' \subset P$ тоже независима. Нетрудно доказать следующее утверждение:

Лемма 1. а) *Если* $P = \{\pi_1, \pi_2, \ldots, \pi_w\}$ *является независимой системой разбиений, то для любого набора* $B_1^{(\alpha_1)}, B_2^{(\alpha_2)}, \ldots, B_i^{(\alpha_i)}, \ldots, B_w^{(\alpha_w)}$, *где каждый* $B_i^{(\alpha_i)} \in \pi_i$, $\bigcap_{i=1}^{w} B_i^{(\alpha_i)} \neq \varnothing$.

б) *Если система разбиений* P *независимая и все блоки разбиения* $m(P)$ *равномощные, то и блоки любого разбиения* $\pi_i \in P$ *равномощные.*

Лемма 2. *Свойство независимости для системы разбиений* P *эквивалентно условию* $\sum_{\pi_i \in P} H(\pi_i) - H(m(P)) = 0$.

Доказательство. Пусть $P = \{\pi_1, \pi_2, \ldots, \pi_w\}$ — независимая система разбиений. Тогда, учитывая, что для любых разбиений $\pi_i(X)$ и $\pi_j(X)$ всегда $\pi_i \equiv \pi_j \Rightarrow H(\pi_i) = H(\pi_j)$ и $H(\pi_i \cdot \pi_j) = H(\pi_i) + \sum_{B_i^{(\alpha)} \in \pi_i} q(B_i^{(\alpha)}) H(\bar{\pi}_j(B_i^{(\alpha)}))$ [2], получаем

$$H(m(P)) = H(\pi_1 \cdot m(P \setminus \{\pi_1\})) = \sum_{B^{(\alpha)} \in m(P \setminus \{\pi_1\})} q(B^{(\alpha)}) H(\bar{\pi}_1(B^{(\alpha)})) +$$

$$+ H(m(P \setminus \{\pi_1\})) = H(\pi_1) + H(m(P \setminus \{\pi_1\})) =$$

$$= H(\pi_1) + H(\pi_2 \cdot m(P \setminus \{\pi_1, \pi_2\})) =$$

$$= H(\pi_1) + \sum_{B^{(\beta)} \in m(P \setminus \{\pi_1, \pi_2\})} q(B^{(\beta)}) H(\bar{\pi}_2(B^{(\beta)})) + H(m(P \setminus \{\pi_1, \pi_2\})) =$$

$$= H(\pi_1) + H(\pi_2) + H(m(P \setminus \{\pi_1, \pi_2\})) = \ldots = \sum_{i=1}^{w} H(\pi_i).$$

Пусть, теперь, $\sum_{\pi_j \in P} H(\pi_j) - H(m(P)) = 0$, $\pi_i \in P$ и $P' \subset P$ при $\pi_i \notin P'$. Тогда, в силу свойств субаддитивности энтропии, получаем

$$\sum_{\pi_j \in P} H(\pi_j) - H(m(P)) = 0 \Rightarrow$$

$$\Rightarrow [H(\pi_i) + H(m(P')) - H(\pi_i \cdot m(P'))] +$$

$$+ [H(\pi_i \cdot m(P')) + \sum_{\pi_h \in P \setminus P' \cup \{\pi_i\}} H(\pi_h) - H(m(P))] = 0 \Rightarrow$$

$$\Rightarrow H(\pi_i) + H(m(P')) - H(\pi_i \cdot m(P')) = 0 \Rightarrow$$

$$\Rightarrow H(\pi_i) + H(m(P')) - H(m(P')) - \sum_{B^{(\alpha)} \in m(P')} q(B^{(\alpha)}) H(\bar{\pi}_i(B^{(\alpha)})) = 0 \Rightarrow$$

$$\Rightarrow H(\pi_i) = \sum_{B^{(\alpha)} \in m(P')} q(B^{(\alpha)}) H(\bar{\pi}_i(B^{(\alpha)})).$$

Определим теперь для любого разбиения π_h вектор

$$Q(\pi_h) \underset{\text{Df}}{=} \{q(B_h^{(1)}), q(B_h^{(2)}), \ldots, q(B_h^{(m_h)})\}.$$

Тогда

$$Q(\bar{\pi}_i(B^{(\alpha)})) = \left\{ \frac{\|B_i^{(1)} \cap B^{(\alpha)}\|}{\|B^{(\alpha)}\|}, \frac{\|B_i^{(2)} \cap B^{(\alpha)}\|}{\|B^{(\alpha)}\|}, \ldots, \frac{\|B_i^{(m_i)} \cap B^{(\alpha)}\|}{\|B^{(\alpha)}\|} \right\}.$$

Поскольку функция энтропии H для разбиения π_i определяется полностью вектором $Q(\pi_i)$, то функция f_H на векторах Q определяется следующим образом: $(\forall \pi_h)(f_H(Q(\pi_h)) \underset{\text{Df}}{=} H(\pi_h))$. Итак, учитывая, что $Q(\pi_i) = \sum\limits_{B^{(\alpha)} \in m(P')} q(B^{(\alpha)}) Q(\overline{\pi}_i(B^{(\alpha)}))$, получаем

$$\sum_{B^{(\alpha)} \in m(P')} q(B^{(\alpha)}) H(\overline{\pi}_i(B^{(\alpha)})) = H(\pi_i) \Rightarrow$$

$$\Rightarrow \sum_{B^{(\alpha)} \in m(P')} q(B^{(\alpha)}) f_H(Q(\overline{\pi}_i(B^{(\alpha)}))) = f_H\Big(\sum_{B^{(\alpha)} \in m(P')} q(B^{(\alpha)}) Q(\overline{\pi}_i(B^{(\alpha)}))\Big). \tag{1}$$

Соотношение (1) представляет собой частный случай достижения равенства для неравенства Енсена

$$\sum_{k=1}^{n} \lambda_k f(x_k) \leqslant f\Big(\sum_{k=1}^{n} \lambda_k x_k\Big) \Big(\sum_{k=1}^{n} \lambda_k = 1;\ \lambda_k > 0\Big).$$

Так как функция энтропии вогнутая, а в неравенстве Енсена знак равенства достигается для вогнутых функций f только в случае $x_1 = x_2 = \ldots = x_n$, то из соотношения (1) следует

$$Q(\overline{\pi}_i(B^{(1)})) = Q(\overline{\pi}_i(B^{(2)})) = \ldots = Q(\overline{\pi}_i(B^{(\alpha)})) = \ldots$$

$$\ldots = Q(\overline{\pi}_i(B^{(m_{P'})})) = Q(\pi_i(X)).$$

Из этого непосредственно вытекает, что для любого $B^{(\alpha)} \in m(P')$ справедливо $\overline{\pi}_i(B^{(\alpha)}) \equiv \pi_i(X)$. Лемма доказана.

Лемма 3. *При произвольной независимой системе разбиений P для любых различных π_i, π_j, $\pi_k \in P$ всегда верно* $\pi_i \cdot \pi_j + \pi_i \cdot \pi_k = \pi_i$.

Доказательство. Из утверждения а) леммы 1 вытекает, что для любых различных π_j, $\pi_k \in P$ всегда $\pi_j + \pi_k = 1_X$. Пусть $B_i^{(\alpha)} \in \pi_i$. Учитывая независимость P, убеждаемся, что из равенства $\pi_j + \pi_k = 1_X$ следует $\overline{\pi}_j(B_i^{(\alpha)}) + \overline{\pi}_k(B_i^{(\alpha)}) = 1_{B_i^{(\alpha)}}$. Итак, $B_i^{(\alpha)} \in \pi_i \cdot \pi_j + \pi_i \cdot \pi_k$. Ввиду произвольности блока $B_i^{(\alpha)} \in \pi_i$ очевидно, что если π_i, π_j, $\pi_k \in P$ и $\pi_j \neq \pi_k$, то всегда $\pi_i \cdot \pi_j + \pi_i \cdot \pi_k = \pi_i$.

Любую пару разбиений $\varrho_i(X) = \langle \pi_{i1}(X), \pi_{i2}(X) \rangle$ будем называть каналом на X. Примем, что

$$\langle \pi_h(X'), \pi_j(X') \rangle \equiv \langle \pi_i(X''), \pi_k(X'') \rangle \underset{\text{Df}}{\Leftrightarrow} (\pi_h \equiv \pi_i \wedge \pi_h \cdot \pi_j \equiv \pi_i \cdot \pi_k).$$

Для произвольных каналов $\langle \pi_h, \pi_i \rangle$ и $\langle \pi_j, \pi_k \rangle$ на X положим

$$\langle \pi_h, \pi_i \rangle \cdot \langle \pi_j, \pi_k \rangle \underset{\text{Df}}{=} \langle \pi_h \cdot \pi_j, \pi_i \cdot \pi_k \rangle,$$

$$\langle \pi_h, \pi_i \rangle + \langle \pi_j, \pi_k \rangle \underset{\text{Df}}{=} \langle \pi_h + \pi_j, \pi_i + \pi_k \rangle.$$

Для любой системы каналов $K = \{\varrho_1, \varrho_2, \ldots, \varrho_w\}$ введем обозначение $m(K) \underset{\text{Df}}{=} \prod\limits_{i=1}^{w} \varrho_i$. Сужением канала $\varrho_i(X)$ на $X' \subset X$ назовем канал

$\overline{\varrho}_i(X') \underset{\text{Df}}{=} \langle \overline{\pi}_{i1}(X'), \overline{\pi}_{i2}(X') \rangle$. Для системы каналов $K(X)$ определим сужение на $X' \subset X$ как $\overline{K}(X') \underset{\text{Df}}{=} \{\overline{\varrho}_i(X') \mid \varrho_i \in K(X)\}$.

Определим теперь для каждого канала $\langle \pi_i(X), \pi_k(X) \rangle$ энтропию $H(\langle \pi_i, \pi_k \rangle)$ в виде следующей разности:

$$H(\langle \pi_i, \pi_k \rangle) \underset{\text{Df}}{=} H(\pi_i \cdot \pi_k) - H(\pi_i).$$

Определим проекции для системы каналов:

$$\Pr_1(K) \underset{\text{Df}}{=} \{\pi_{i1} \mid (\exists \pi_{i2})\ (\langle \pi_{i1}, \pi_{i2} \rangle \in K)\},$$

$$\Pr_2(K) \underset{\text{Df}}{=} \{\pi_{i2} \mid (\exists \pi_{i1})\ (\langle \pi_{i1}, \pi_{i2} \rangle \in K)\}.$$

Систему каналов K назовем конвергентной, если и только если все каналы из K имеют одно и то же второе разбиение (т. е. $\|\Pr_2(K)\| = 1$). Для конвергентной системы каналов K обозначим единственный элемент множества $\Pr_2(K)$ через $\pi_{\omega K}$. Учитывая лемму 2 из [2], получаем следующее утверждение.

Лемма 4. *Если каналы* ϱ_i *и* ϱ_j *принадлежат конвергентной системе* K, *то имеет место* $H(\varrho_i \cdot \varrho_j) = \sum_{\alpha=1}^{m_{i_1}} q(B_{i1}^{(\alpha)}) H(\overline{\varrho}_j(B_{i1}^{(\alpha)}))$.

Систему каналов K назовем α-независимой, если и только если $\Pr_1(K)$ — независимая система разбиений.

Из леммы 2 непосредственно вытекает

Теорема 1. *Свойство* α-*независимости для системы каналов* K *эквивалентно условию*

$$\sum_{\pi_i \in \Pr_1(K)} H(\pi_i) - H(m(\Pr_1(K))) = 0.$$

Систему каналов K будем называть при $H(m(K)) = 0$ детерминированной.

Подсистему K' системы K назовем полной относительно K, если и только если $m(\Pr_1(K')) \leqslant m(\Pr_2(K))$. Из определения полноты непосредственно вытекает, что если для системы K найдется полная подсистема K', то обе, K' и K, — детерминированные системы каналов. Итак, полные подсистемы образуют подмножество множества детерминированных подсистем данной детерминированной системы.

Теорема 2. *Если подсистемы* K' *и* K'' α-*независимой системы* K *полные, то подсистемы* $K' \cup K''$ *и* $K' \cap K''$ *тоже полные относительно* K.

Доказательство. Полнота системы $K' \cup K''$ следует непосредственно из определения полноты.

Согласно лемме 3, для любых подсистем K' и K'' α-независимой системы K справедливо $m(\Pr_1(K')) + m(\Pr_1(K'')) = m(\Pr_1(K' \cap K''))$. Поэтому, если $m(\Pr_1(K')) \leqslant m(\Pr_2(K))$ и $m(\Pr_1(K'')) \leqslant m(\Pr_2(K))$, то и $m(\Pr_1(K' \cap K'')) \leqslant m(\Pr_2(K))$. Итак, $K' \cap K''$ — тоже полная подсистема. Теорема доказана.

Из теоремы 2 вытекает, что для α-независимой системы K существует минимальная полная подсистема K_n, определяемая как пересечение всех полных подсистем. Назовем эту подсистему K_n ядром α-независимой системы K. Обозначим операцию нахождения ядра для

системы K через $\mathfrak{N}(K)$, т. е. $\mathfrak{N}(K) \underset{\text{Df}}{=} K_n$ для любого K. Каналы ϱ_i, принадлежащие $\mathfrak{N}(K)$, назовем существенными для K. Систему каналов K назовем стабильной, если и только если $\mathfrak{N}(K) = K$.

Пусть $\mathfrak{K}(X)$ — множество всевозможных систем каналов на X. Определим теперь оператор замыкания $\mathfrak{L}(K)$ на $\mathfrak{K}$ для любой $K \in \mathfrak{K}$ как пересечение всех систем $K' \supset K$, замкнутых относительно умножения и сложения каналов (т. е. если $\varrho_i, \varrho_j \in K'$, то $\varrho_i \cdot \varrho_j \in K'$ и $\varrho_i + \varrho_j \in K'$). Ясно, что $\mathfrak{L}(K)$ представляет собой минимальную решетку каналов, содержащую систему каналов K.

Лемма 5. *Пусть конвергентная система каналов K является α-независимой. Тогда для любого $\varrho_i \in \mathfrak{L}(K)$ $(\pi_{i1} \neq 1_X)$ существует единственное разложение $\varrho_i = \varrho_{j_1} \cdot \varrho_{j_2} \cdot \ldots \cdot \varrho_{j_\alpha} \cdot \ldots \cdot \varrho_{j_r}$, где каждый $\varrho_{j_\alpha} \in K$.*

Доказательство. Из леммы 3 вытекает, что любой $\varrho_i \in \mathfrak{L}(K)$ при $\pi_{i1} \neq 1_X$ может быть представлен в виде $\varrho_i = m(K')$ $(K' \subset K)$. Предположим теперь, что существуют подсистемы K', $K'' \subset K$ такие, что $\varrho_i = m(K') = m(K'')$. Тогда из конвергентности и α-независимости системы K следует, что $m(K') + m(K'') = m(K' \cap K'')$. Но, по предположению, $m(K') + m(K'') = m(K') = m(K'')$, откуда $K' = K''$, что и требовалось доказать.

α-независимую и конвергентную систему каналов $K(X)$ будем называть при $m(\Pi_1(K)) = 0_X$ функциональной.

Дискретной функцией от n дискретных переменных назовем функцию $z = F(y_1, y_2, \ldots, y_n)$, которая реализует отображение $\bar{F}: X \to E$, где $X = E_1 \times E_2 \times \ldots \times E_n$, при $E_i \underset{\text{Df}}{=} \{0, 1, \ldots, m_i - 1\}$ $(i = 1, \ldots, n)$ и $E \underset{\text{Df}}{=} \{0, 1, \ldots, m-1\}$. Легко видеть, что каждой дискретной функции F соответствует функциональная система каналов $K_F(X) = \{\langle \pi_i, \pi_\omega \rangle \mid i = 1, \ldots, n\}$, если $x_\alpha = x_\beta(\pi_i) \underset{\text{Df}}{\Leftrightarrow} \Pr_i(x_\alpha) = \Pr_i(x_\beta)$ ($\Pr_i(x_h)$ — проекция $x_h = \langle y_1^{(h_1)}, y_2^{(h_2)}, \ldots, y_i^{(h_i)}, \ldots, y_n^{(h_n)} \rangle$ на $y_i^{(h_i)}$) и $x_\alpha \equiv x_\beta(\pi_\omega) \underset{\text{Df}}{\Leftrightarrow} \bar{F}(x_\alpha) = \bar{F}(x_\beta)$. Ясно также, что каждой функциональной системе каналов соответствует некоторая дискретная функция. Поэтому функциональные системы каналов можно рассматривать как своеобразное информационное представление дискретных функций.

Определим теперь для любой системы каналов K информационную связку $\mathfrak{I}(K)$ следующим образом: $\mathfrak{I}(K) \underset{\text{Df}}{=} \sum_{\varrho_i \in K} H(\varrho_i) - H(m(K))$.

Теорема 3. *Информационная связка для функциональной системы каналов K имеет вид*

$$\mathfrak{I}(K) = \sum_{\substack{(\alpha) \\ B_{i1} \in \pi_{i1} \\ \varrho_i \in K}} q(B_{i1}^{(\alpha)}) H(\bar{\pi}_{\omega(K)}(B_{i1}^{(\alpha)})).$$

Доказательство следует непосредственно из определения информационной связки для системы каналов и леммы 1 из [2].

Биекцию $\varphi: X \to X$ будем называть ϱ_i-автоморфизмом системы каналов $K(X)$ при $\varrho_i \in K$, если и только если для любых $x_\alpha, x_\beta \in X$ из $(x_\alpha \equiv x_\beta(\pi_{i1}) \Rightarrow \varphi(x_\alpha) \equiv \varphi(x_\beta)(\pi_{i1})) \wedge (x_\alpha \equiv \varphi(x_\alpha)(\pi_{i2}))$ и для каждого $\varrho_j \in K$ при $\varrho_j \neq \varrho_i$ имеет место $x_\alpha \equiv \varphi(x_\alpha)(\pi_{j1} \cdot \pi_{j2})$. Систему каналов K будем называть симметричной относительно канала $\varrho_i \in K$,

если и только если существует группа ϱ_i-автоморфизмов Ψ системы K такая, что если $x_h \in B_{i1}^{(\alpha)}$, то для каждого $B_{i1}^{(\beta)} \in \pi_{i1}$ найдется $\varphi_\beta \in \Psi$ при $\varphi_\beta(x_h) \in B_{i1}^{(\beta)}$.

Следующая теорема показывает, что симметрия представления дискретной функции всегда связана с фиктивностью переменных данной функции.

Теорема 4. *Для функциональной системы каналов подмножество несущественных каналов и подмножество каналов, относительно которых данная система симметрична, совпадают.*

Доказательство. Пусть $K = \{\varrho_1, \varrho_2, \ldots, \varrho_w\}$. Из функциональности системы K вытекает, что $m(\Pi p_1(K)) \leqslant \pi_{\omega(K)}$. Поэтому для произвольного набора блоков $\{B_1^{(\alpha_1)}, B_2^{(\alpha_2)}, \ldots, B_i^{(\alpha_i)}, \ldots, B_w^{(\alpha_w)}\}$, где $B_i^{(\alpha_i)} \in \pi_{i1}\,(i = 1, \ldots, w)$, найдется блок $B_\omega^{(\alpha_\omega)} \in \pi_{\omega(K)}$ такой, что $\bigcap_{i=1}^{w} B_i^{(\alpha_i)} \subset B_\omega^{(\alpha_\omega)}$. Пусть, теперь, система K симметрична относительно канала $\varrho_j \in K$. Тогда, по определению симметричности, существует группа ϱ_j-автоморфизмов Ψ для системы K. Поэтому для любых $B_j^{(\alpha_l)}$, $B_j^{(\beta_l)} \in \pi_{j1}$ найдется $\varphi \in \Psi$ такой, что $\varphi(B_j^{(\alpha_l)}) = B_j^{(\beta_l)}$. Итак,

$$\varphi\Big(\bigcap_{i=1}^{w} B_i^{(\alpha_i)}\Big) \subset \varphi(B_\omega^{(\alpha_\omega)}) \Rightarrow \bigcap_{i=1}^{w} \varphi(B_i^{(\alpha_i)}) \subset \varphi(B_\omega^{(\alpha_\omega)}) \Rightarrow$$

$$\Rightarrow \bigcap_{\substack{i=1 \\ i \neq j}}^{w} B_i^{(\alpha_i)} \subset B_\omega^{(\alpha_\omega)} \Rightarrow m(\Pi p_1(K \setminus \{\varrho_j\})) \leqslant \pi_{\omega(K)} \Rightarrow$$

$$\Rightarrow \varrho_j \text{ — несущественный канал для системы } K.$$

Пусть $\varrho_i \in K$ — несущественный относительно функциональной системы каналов K канал. Тогда, учитывая лемму 1, определим для любых $B_{i1}^{(\alpha)}$, $B_{i1}^{(\beta)} \in \pi_{i1}$ отображение $\varphi_{\alpha\beta} : X \to X$ следующим образом:

а) если $x_h \in B_{i1}^{(\alpha)}$, то при $\bigcap_{\substack{j=1 \\ j \neq i}}^{w} B_{j1}^{(\gamma_l)} \cap B_{i1}^{(\alpha)} = \{x_h\}$ положим

$$\{\varphi_{\alpha\beta}(x_h)\} = \bigcap_{\substack{j=1 \\ j \neq i}}^{w} B_{j1}^{(\gamma_l)} \cap B_{i1}^{(\beta)};$$

б) если $x_h \in B_{i1}^{(\beta)}$, то при $\bigcap_{\substack{j=1 \\ j \neq i}}^{w} B_{j1}^{(\gamma_l)} \cap B_{i1}^{(\beta)}$ положим

$$\{\varphi_{\alpha\beta}(x_h)\} = \bigcap_{\substack{j=1 \\ j \neq i}}^{w} B_{j1}^{(\gamma_l)} \cap B_{i1}^{(\alpha)};$$

в) если $x_h \notin B_{i1}^{(\alpha)}$, $B_{i1}^{(\beta)}$, то $\varphi_{\alpha\beta}(x_h) = x_h$.

Из несущественности канала ϱ_i и определения $\varphi_{\alpha\beta}$ вытекает, что $\varphi_{\alpha\beta}$ является ϱ_i-автоморфизмом системы K. Нетрудно убедиться, что

группа отображений, индуцированная ϱ_i-автоморфизмами $\varphi_{\alpha\beta}$, является группой ϱ_i-автоморфизмов, определяющих симметрию системы K относительно ϱ_i.

Пусть $K(X)$ — произвольная функциональная система каналов, $\varrho_i \in \mathfrak{L}(K)$ и $B \in \pi_{i1}$. Подсистему $K'(B) \underset{\text{Df}}{=} \{\overline{\varrho_h}(B) \mid \varrho_h \in K \wedge \overline{\pi}_{h1}(B) \neq 1_B\}$ назовем подструктурой системы каналов K. Нетрудно видеть, что если $\varrho_i \in \mathfrak{L}(K)$ имеет разложение $\varrho_i = \varrho_{j_1} \cdot \varrho_{j_2} \cdot \ldots \cdot \varrho_{j_p} \cdot \ldots \cdot \varrho_{j_r}$ $(\varrho_{j_p} \in K)$, то для любого $B \in \pi_{i1}$ подсистема $K^{(i)}(B) = \{\overline{\varrho_h}(B) \mid \varrho_h \in K \setminus \{\varrho_{j_1} \cdot \varrho_{j_2} \cdot \ldots \cdot \varrho_{j_r}\}\}$ является подструктурой системы $K(X)$.

Обозначим множество всевозможных подструктур системы K через $\mathfrak{S}(K)$, а подмножество всех стабильных подструктур системы каналов K — через $\tilde{\mathfrak{S}}(K)$. Легко убедиться, что если функциональная система каналов K является информационным представлением булевой функции, то подструктурам этой системы соответствуют подфункции данной булевой функции, а стабильным подструктурам — подфункции без фиктивных переменных.

Сомножителями канала $\langle \pi_i, \pi_j \rangle$ назовем разбиения $\overline{\pi}_j(B_i^{(\alpha)})$ при $B_i^{(\alpha)} \in \pi_i$. Множество сомножителей для канала ϱ_i обозначим через $T(\varrho_i)$. Множество сомножителей $T(K)$ для системы каналов K определим как $T(K) \underset{\text{Df}}{=} \bigcup_{\varrho_i \in K} T(\varrho_i)$.

Пусть K — функциональная система каналов. По теореме 3 информационную связку для системы K можно выразить как взвешенную сумму энтропий сомножителей системы. Из определения подструктуры вытекает, что для каждой подструктуры $K_i \in \mathfrak{S}(K)$ имеет место $T(K_i) \subset T(\mathfrak{L}(K))$ и поэтому $\bigcup_{K_i \in \mathfrak{S}(K)} T(K_i) \subset T(\mathfrak{L}(K))$. Легко установить, что любой отличный от $\pi_{\omega(K)}$ сомножитель $\pi_t \in T(\mathfrak{L}(K))$ принадлежит множеству сомножителей не менее чем одной подструктуры системы K. Итак, получаем, что $T(\mathfrak{L}(K)) = \{\pi_{\omega(K)}\} \cup (\bigcup_{K_t \in \mathfrak{S}(K)} T(K_i))$. Введем обозначение $\mathfrak{T}(K) \underset{\text{Df}}{=} \{\pi_{\omega(K)}\} \cup (\bigcup_{K_j \in \tilde{\mathfrak{S}}(K)} T(K_j))$.

Определим теперь МИС для дискретной функции F в виде

$$\mathfrak{B}(F) \underset{\text{Df}}{=} \sum_{\overline{\pi}_{\omega(K_F)}(B_{i1}^{(\alpha)}) \in \mathfrak{T}(K_F)} q(B_{i1}^{(\alpha)}) H(\overline{\pi}_{\omega(K_F)}(B_{i1}^{(\alpha)})),$$

откуда с учетом теоремы 3 сразу следует, что всегда $\mathfrak{B}(F) \leqslant \mathfrak{I}(\mathfrak{L}(K_F))$.

В содержательном плане интерпретация МИС как показателя сложности означает, что сложность булевой функции определяется теми ее подфункциями, которые содержат только существенные переменные. Зависимость сложности булевой функции от числа ее различных подфункций была показана в [3].

Контрольные машинные эксперименты показали, что использование МИС вместо КИС [1] для оценки сложности булевых функций от 4-х переменных повышает линейную корреляцию между информационной оценкой и различными практическими реализациями для представителей классов однотипных функций в среднем на 0,1. Так, например, программная реализация функций в виде бинарных программ дала корреляцию 0,99, а оптимальная реализация на обычных логических элементах [4] — 0,93. Эти результаты указывают на целесообразность

использования МИС для оценки сложности булевых функций. Для примера в таблице приведены значения МИС и среднее число шагов (через всевозможные упорядочения переменных) реализующей бинарной программы ($БП_{ср}$) для представителей типов булевых функций от 3-х переменных, заданных в виде совокупности номеров их минтермов в десятичной форме записи. В скобках указано число существенных переменных представителей типов.

Номер типа	Представитель типа		МИС, *бит*	$БП_{ср}$, *шаг*
1	—	(0)	0,000	0,000
2	0, 1, 2, 3	(1)	1,000	1,000
3	0, 1	(2)	1,811	2,000
4	0	(3)	2,510	3,000
5	0, 1, 2	(3)	3,671	3,667
6	0, 3	(3)	4,434	4,667
7	0, 1, 6, 7	(2)	3,000	3,000
8	0, 1, 2, 5	(3)	4,123	4,333
9	0, 1, 6	(3)	4,421	4,667
10	0, 1, 2, 4	(3)	4,934	5,000
11	0, 1, 2, 7	(3)	5,061	5,000
12	0, 7	(3)	4,745	5,000
13	0, 3, 5	(3)	5,921	6,000
14	0, 3, 5, 6	(3)	7,000	7,000

Очень высокая корреляция между оценками сложности по МИС и по бинарной программе является практическим подтверждением эквивалентности оценок сложности по формуле Шеннона и по длине алгоритма, которая была при некоторых ограничениях теоретически установлена в [5].

Автор выражает глубокую благодарность А. Таутс за ценные замечания.

ЛИТЕРАТУРА

1. Лаусмаа Т., Изв. АН ЭССР, Физ. Матем., **29**, № 4, 349—355 (1980).
2. Лаусмаа Т., Изв. АН ЭССР, Физ. Матем., **30**, № 3, 226—233 (1981).
3. Улиг Д., Проблемы кибернетики, вып. 26, 183—201 (1973).
4. Cullineу, Y. N., Young, M. H., Nakagawa, T., Muroga, S., IEEE Trans. Comput., **C-27**, № 1, 76—85 (1979).
5. Leung-Yan-Cheong, S. K., Cover, T. M., IEEE Trans. Inform. Theory, **IT-24**, № 3, 331—338 (1978).

Институт термофизики и электрофизики
Академии наук Эстонской ССР

Поступила в редакцию
20/IV 1981

T. LAUSMAA

SÜMMEETRIA OSAST DISKREETSETE FUNKTSIOONIDE INFORMATIIVSEL HINDAMISEL

Artiklis on vaadeldud diskreetsete funktsioonide informatiivset keerukushinnangut, mis erinevalt töös [1] toodust arvestab sümmeetriat funktsiooni esitamisel. Sellise hinnangu ja funktsioonide praktiliste realisatsioonide keerukuse korrelatsioon on keskmiselt 0,1 võrra kõrgem kui eelmise hinnangu puhul.

T. LAUSMAA

ON THE ROLE OF SYMMETRY BY THE INFORMATIONAL MEASURE OF COMPLEXITY FOR DISCRETE FUNCTIONS

A combinative informational measure of complexity for switching functions was introduced in [1]. Informally this measure can be interpreted as a thesis that the complexity of a switching function given by the reduced truth table without any fictitious variables is determined by the set of its subfunctions. But sometimes one and the same function may be included in the set of subfunctions several times depending on the number of fictitious variables in the truth table representing the function. On the other hand, the existence of fictitious variables in some subfunction of the given function is also reflected in the truth table of this function by some kind of symmetry. But, as we know, the symmetry of any kind of an object effects on the complexity of this object (for instance, the periodic sequence of some kind of symbols is always entirely determined by its period, whereas for the random sequence there is no better way for describing the sequence than its full presentation). So in determining the complexity of some object it is natural to try to take into account its symmetry.

In the present paper the mathematical formalism based on the notion of partition pairs is advanced still further, to describe various qualities of discrete functions which enable us to introduce a new informational measure of complexity for discrete functions that takes into account the symmetry in the truth table of the given function. The informal characterization of the present measure lies in the fact that the complexity of a discrete function is characterized by its subfunctions that have no fictitious variables. In order to estimate the difference between the previous measure and the new one for determining the complexity of various practical realizations, the comparison was carried out for the representatives of all PCN equivalent classes for switching functions of 4-variables. The results showed that the linear correlation between the provided measure and the various practical realizations was approximately by 0.1 higher than by the previous measure. For instance, the values of correlation coefficients between the presented measure on the one hand and the practical complexity of optimal feed-forward networks of just AND and OR gates [4] and the average number of steps of binary programmes (over all possible ways of ordering of variables) for the realization of chosen functions on the other, were as high as 0.93 and even 0.99, respectively. The last result is an affirmation of the fact that the complexity estimation by Shannon formula and by the algorithmic measure of Kolmogorov are practically equivalent [5].