EESTI NSV TEADUSTE AKADEEMIA TOIMETISED. 30. KOIDE
FÜÜSIKA * MATEMAATIKA. 1981, NR. 3

ИЗВЕСТИЯ АКАДЕМИИ НАУК ЭСТОНСКОЙ ССР. ТОМ 30
ФИЗИКА * МАТЕМАТИКА. 1981, № 3

https://doi.org/10.3176/phys.math.1981.3.06

УДК 519.722

Т. ЛАУСМАА

КОЛИЧЕСТВЕННАЯ ИНФОРМАЦИОННАЯ МЕРА ДЛЯ ПАР РАЗБИЕНИЙ

(Представил Н. Алумяэ)

В своей классической работе по структурной теории автоматов [1] Дж. Хартманис и Р. Е. Стирнз используют понятие разбиения в качестве алгебраической интерпретации понятия информации, определяя информацию о каком-то конечном множестве заданием соответствующего разбиения на том же множестве. Для представления же «потока информации» ими введено по аналогии понятие пар разбиений. Такой подход к рассмотрению различных задач по структурной теории автоматов оказался чрезвычайно удачным. Однако при решении различных вопросов синтеза автоматов, когда подлежат сравнению качественно несравнимые пары разбиений, требуется и количественная их оценка.

В настоящей работе мы развиваем формальный аппарат [2] для информационной характеристики пар разбиений, базируясь на аксиоматизированном определении функции энтропии для разбиения, т. е. не прибегая к понятию вероятности. Это позволяет получить информационную характеристику для пар разбиений, которая является исключительно их внутренним свойством, а на ее основе — информационную оценку сложности объекта, представленного в виде системы пар разбиений, которая является, естественно, также его внутренней характеристикой. В работе показана также возможность практического применения найденной количественной меры для получения критерия выбора разложения булевой функции по Шеннону при реализации ее в виде сети из мультиплексоров и для оценки различных вариантов декомпозиции абстрактных автоматов.

Разбиение произвольного конечного множества $X=\{x_1, x_2, \ldots, x_m\}$ на непересекающиеся подмножества (блоки) $B_i^{(1)}, B_i^{(2)}, \ldots, B_i^{(\alpha)}, \ldots \ldots, B_i^{(m_i)}$ обозначим через $\pi_i(X)$. В частности, нулевое разбиение (т. е. разбиение, каждый блок которого содержит лишь один элемент из X), будем обозначать через 0_X, а единичное (т. е. разбиение, содержащее только один блок) — 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 $x_i \equiv x_j(\pi_h)$, что равносильно тому, что найдется $B_h^{(\alpha)} \in \pi_h$ такой, что $x_i, x_j \in B_h^{(\alpha)}$. Разбиения $\pi_i(X')$ и $\pi_j(X'')$ будем называть эквивалентными тогда и только тогда, когда существует биекция $\varphi: \pi_i \to \pi_j$ такая, что для любого $B_i^{(\alpha)} \in \pi_i$ имеет место $\|B_i^{(\alpha)}\| / \|\varphi(B_i^{(\alpha)})\| = \|X'\| / \|X''\|$, где $\|X^{(i)}\|$ — мощность множества $X^{(i)}$. Эквивалентность $\pi_i(X')$ и $\pi_j(X'')$ обозначим через $\pi_i(X') \equiv \pi_j(X'')$.

Пусть R^+ — множество положительных вещественных чисел. Мерой на конечном множестве X назовем отображение $\mu: 2^X \to R^+$ такое, что если $B', B'' \subset X$ и $B' \cap B'' = \varnothing$, то $\mu(B' \cup B'') = \mu(B') + \mu(B'')$. Определим, в частности, меру q как такое отображение $q: 2^X \to R^+$, где для любого $X' \subset X$ выполняется $q(X') \underset{\mathrm{Df}}{=} \|X'\|/\|X\|$. Ясно, что меру q можно рассматривать как формальную вероятность на X, ибо $q(X) = 1$.

Разбиение $\pi_j(X')$ будем называть сужением разбиения $\pi_i(X)$ на $X' \subset X$ (обозначение $\bar{\pi}_i(X')$) тогда и только тогда, когда $\pi_j(X') = \{B_i^{(\alpha)} \cap X' \mid B_i^{(\alpha)} \in \pi_i\}$.

В [1] разбиение конечного множества интерпретируется как алгебраическая форма информации об этом множестве в предположении, что информационная содержательность разбиения тем больше, чем меньше разбиение. При таком подходе качественному сравнению поддаются лишь сравнимые между собой разбиения. Однако во многих случаях бывает необходимой количественная оценка информационной содержательности разбиения. При этом вполне разумно предположить, что энтропии $H(\pi_i)$ разбиения π_i как функции с вещественной областью значений присущи следующие свойства:

а) неотрицательность: для любого $\pi_i(X)$ всегда $H(\pi_i) \geqslant 0$;

б) инвариантность: если $\pi_i(X') \equiv \pi_j(X'')$, то $H(\pi_i) = H(\pi_j)$;

в) рекурсивность: для любого конечного множества X существует мера μ_H такая, что если при произвольном разбиении $\pi_i(X)$ на каком-то блоке $B_i^{(\alpha)} \in \pi_i$ определено разбиение $\pi_j(B_i^{(\alpha)})$, то для разбиения

$$\pi_k(X) \underset{\mathrm{Df}}{=} \{B_i^{(1)}, B_i^{(2)}, \ldots, B_i^{(\alpha-1)}, B_j^{(1)}, B_j^{(2)}, \ldots, B_j^{(m_j)}, B_i^{(\alpha+1)}, \ldots, B_i^{(m_i)}\}$$

энтропия может быть представлена как

$$H(\pi_k) = H(\pi_i) + \mu_H(B_i^{(\alpha)})\, H(\pi_j(B_i^{(\alpha)}))\,.$$

Оказывается, что справедливо следующее утверждение:

Теорема 1. *Для совокупности всех разбиений $\pi_i(X)$ на всевозможных конечных множествах X существует единственная с точностью до константы функция $H(\pi_i)$, удовлетворяющая трем перечисленным выше свойствам. При этом $H(\pi_i)$ имеет вид*

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

где C — некоторая положительная константа.

Доказательство. Из свойства б) вытекает, что $H(\pi_i)$ зависит только от совокупности чисел $\{q(B_i^{(\alpha)}) \mid B_i^{(\alpha)} \in \pi_i\}$. Из свойств а) и в) получаем, что если $\pi_i \leqslant \pi_j$, то всегда $H(\pi_i) \geqslant H(\pi_j)$. Поэтому для совокупности разбиений на X энтропия H имеет максимум в случае разбиения 0_X. В силу свойства в) для любых разбиений π_i и π_k справедливо

$$H(\pi_i \cdot \pi_k) = H(\pi_i) + \sum_{\alpha=1}^{m_i} \mu_H(B_i^{(\alpha)})\, H(\bar{\pi}_k(B_i^{(\alpha)}))\,. \tag{2}$$

Если принять $\pi_i = 1_X$, то из соотношения (2) вытекает, что для произвольного разбиения π_k верно $H(\pi_k) = H(1_X) + \mu_H(X) H(\pi_k)$. Поэтому, предполагая нетривиальность H и μ_H, имеем $H(1_X) = 0$ и $\mu_H(X) = 1$.

Допустим теперь, что для разбиения $\pi_i(X)$ найдутся блоки $B_i^{(\alpha)}$ и $B_i^{(\beta)}$ такие, что $\|B_i^{(\alpha)}\| = \|B_i^{(\beta)}\|$. Пусть еще на $B_i^{(\alpha)}$ определены произвольное разбиение $\pi_j(B_i^{(\alpha)})$ и разбиение $\pi_k(X) \underset{\mathrm{Df}}{=}$ $\underset{\mathrm{Df}}{=} \{B_i^{(1)}, B_i^{(2)}, \ldots, B_i^{(\alpha-1)}, B_j^{(1)}, B_j^{(2)}, \ldots, B_j^{(m_j)}, B_i^{(\alpha+1)}, \ldots, B_i^{(m_i)}\}$. Тогда всегда найдется биекция $\varphi: X \to X$ такая, что для любого $x_\delta \in X \setminus B_i^{(\alpha)} \cup B_i^{(\beta)}$ верно $\varphi(x_\delta) = x_\delta$, а для любого $x_\gamma \in B_i^{(\alpha)}(B_i^{(\beta)}) - \varphi(x_\gamma) \in B_i^{(\beta)}(B_i^{(\alpha)})$. Принимая, что $h = j, k$ определим теперь разбиения $\pi'_k(X)$ и $\pi'_j(B_i^{(\beta)})$ следующим образом:

$$x_\alpha \equiv x_\beta (\pi'_h) \underset{\mathrm{Df}}{\Longleftrightarrow} \varphi^{-1}(x_\alpha) \equiv \varphi^{-1}(x_\beta) (\pi_h).$$

Из определения эквивалентности для разбиений непосредственно вытекает, что $\pi_j(B_i^{(\alpha)}) \equiv \pi'_j(B_i^{(\beta)})$ и $\pi_h(X) \equiv \pi'_k(X)$. Поэтому из свойства в) заключаем, что $\mu_H(B_i^{(\alpha)}) = \mu_H(B_i^{(\beta)})$. Итак, для любых $X', X'' \subset X$ при $\|X'\| = \|X''\|$ верно $\mu_H(X') = \mu_H(X'')$. Следовательно, для произвольных $x_\alpha, x_\beta \in X$ справедливо $\mu_H(\{x_\alpha\}) = \mu_H(\{x_\beta\})$. В силу $\mu_H(X) = 1$ и свойства аддитивности меры имеем $\mu_H = q$. Итак, мы установили:

1) $H(\pi_i)$ является неотрицательной симметричной функцией от чисел $\{q(B_i^{(\alpha)}) \mid \alpha = 1, \ldots, m_i\}$ при $\sum_{\alpha=1}^{m_i} q(B_i^{(\alpha)}) = 1$ и имеет максимум при $q_\alpha = 1/m_i$ $(\alpha = 1, \ldots, m_i)$;

2) при $m \geqslant 2$ и $q_{m_i} = q' + q''$ выполняется

$$H(q_1, q_2, \ldots, q_{m_i-1}, q', q'') = H(q_1, q_2, \ldots, q_{m_i}) + q_{m_i} H(q'/q_{m_i}, q''/q_{m_i}).$$

Поэтому, по теореме 1 из [3], существует единственная функция вида

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

Теорема доказана.

Для дальнейшего изложения положим, что константа $C = 1$. Следует обратить внимание на то, что хотя формула (1) формально ничем не отличается от формулы Шеннона для нахождения неопределенности статистического эксперимента [4], в содержательном плане она не имеет ничего общего со статистическим экспериментом и является исключительно внутренней характеристикой рассматриваемого разбиения. Энтропия разбиения конечного множества выражает количественную меру четкости изображения этого множества по данному разбиению, каждому блоку которого принадлежат именно те элементы множества, которые неразличимы по изображению.

Любую пару разбиений $\varrho_i(X) = \langle \pi_{i1}(X), \pi_{i2}(X) \rangle$ будем называть каналом на X, полагая, что $\langle \pi_h(X'), \pi_j(X') \rangle \equiv \langle \pi_i(X''), \pi_k(X'') \rangle \underset{\mathrm{Df}}{\Longleftrightarrow} (\pi_h \equiv \pi_i \wedge \pi_h \cdot \pi_j \equiv \pi_i \cdot \pi_k)$. Для произвольных каналов $\langle \pi_h, \pi_i \rangle$ и $\langle \pi_j, \pi_k \rangle$ на X положим

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

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

$$\langle \pi_h, \pi_i \rangle \geqslant \langle \pi_j, \pi_k \rangle \underset{\mathrm{Df}}{\Longleftrightarrow} (\pi_h \geqslant \pi_j \wedge \pi_i \leqslant \pi_k).$$

Для любой системы каналов K примем, что $m(K) \underset{\mathrm{Df}}{=} \prod_{\varrho_i \in K} \varrho_i$. Сужением канала $\varrho_i(X)$ на $X' \subset X$ будем называть канал $\overline{\varrho_i}(X') \underset{\mathrm{Df}}{=}$

$\underset{\text{Df}}{=}\langle\bar{\pi}_{i1}(X'),\ \bar{\pi}_{i2}(X')\rangle$. Для системы каналов $K(X)$ определим сужение на $X'\subset X$ как $\bar{K}(X')\underset{\text{Df}}{=}\{\bar{\varrho}_i(X')\,|\,\varrho_i\in K(X)\}$. Легко показать, что для произвольных каналов $\varrho_i(X)$ и $\varrho_j(X)$ при любом сужении на $X'\subset X$ верно $\overline{\varrho_i\cdot\varrho_j}(X')=\bar{\varrho}_i(X')\cdot\bar{\varrho}_j(X')$ и из $\varrho_i(X)\leqslant\varrho_j(X)$ следует $\bar{\varrho}_i(X')\leqslant\bar{\varrho}_j(X')$.

Определим теперь для каждого канала $\langle\pi_i(X),\pi_k(X)\rangle$ энтропию

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

Нетрудно проверить, что при таком определении

$$H(\langle\pi_i,\pi_k\rangle)=H(\pi_k/\pi_i)=-\sum_{\alpha=1}^{m_i}q(B_i^{(\alpha)})\sum_{\beta=1}^{m_k}q(B_k^{(\beta)}/B_i^{(\alpha)})\ln q(B_k^{(\beta)}/B_i^{(\alpha)}),$$

где $q(B_k^{(\beta)}/B_i^{(\alpha)})\underset{\text{Df}}{=}q(B_i^{(\alpha)}\cap B_k^{(\beta)})/q(B_i^{(\alpha)})$.

Если разбиение какого-то конечного множества интерпретируется как четкость изображения этого множества, то канал характеризует уже четкость изображения функционального соотношения на данном множестве, а энтропия канала выражает количественную меру четкости этого изображения.

Можно показать, что если $\varrho_i(X')\equiv\varrho_j(X'')$, то $H(\varrho_i)=H(\varrho_j)$, а если $\varrho_i(X)\geqslant\varrho_j(X)$, то $H(\varrho_i)\geqslant H(\varrho_j)$. Нетрудно убедиться также, что если $H(\varrho_i(X))=0$, тогда и для любого $X'\subset X$ верно $H(\bar{\varrho}_i(X'))=0$. Учитывая, что $\mu_H=q$, из соотношения (2) вытекает

Лемма 1. *Для любого канала ϱ_i энтропия выражается в виде*

$$H(\varrho_i)=\sum_{B_{i1}^{(\alpha)}\in\pi_{i1}}q(B_{i1}^{(\alpha)})H(\bar{\pi}_{i2}(B_{i1}^{(\alpha)})).\tag{3}$$

Лемма 2. *Для любых разбиений π_i,π_j и π_k на X справедливо*

$$H(\langle\pi_i\cdot\pi_j(X),\ \pi_k(X)\rangle)=\sum_{\alpha=1}^{m_i}q(B_i^{(\alpha)})H(\langle\bar{\pi}_j(B_i^{(\alpha)}),\bar{\pi}_k(B_i^{(\alpha)})\rangle).$$

Доказательство. В самом деле, из леммы 1 вытекает, что

$$H(\pi_i\cdot\pi_j\cdot\pi_k(X))=\sum_{\alpha=1}^{m_i}q(B_i^{(\alpha)})H(\overline{\pi_j\cdot\pi_k}(B_i^{(\alpha)}))+H(\pi_i(X))$$

и

$$H(\pi_i\cdot\pi_j(X))=\sum_{\alpha=1}^{m_i}q(B_i^{(\alpha)})H(\bar{\pi}_j(B_i^{(\alpha)}))+H(\pi_i(X)).$$

Поэтому

$$H(\langle\pi_i\cdot\pi_j(X),\ \pi_k(X)\rangle)=H(\pi_i\cdot\pi_j\cdot\pi_k)-H(\pi_i\cdot\pi_j)=$$

$$=\sum_{\alpha=1}^{m_i}q(B_i^{(\alpha)})\,(H(\overline{\pi_j\cdot\pi_k}(B_i^{(\alpha)}))-H(\bar{\pi}_j(B_i^{(\alpha)})))=$$

$$= \sum_{\alpha=1}^{m_i} q(B_i^{(\alpha)}) H(\langle \bar{\pi}_j(B^{(\alpha)}), \bar{\pi}_k(B^{(\alpha)}) \rangle).$$

Определим теперь для любой системы каналов K информационную связку $\mathfrak{I}(K)$ следующим образом:

$$\mathfrak{I}(K) \underset{\mathrm{Df}}{=} \sum_{\rho_i \in K} H(\varrho_i) - H(K),$$

где $H(K) \underset{\mathrm{Df}}{=} H(m(K))$. $\mathfrak{I}(K)$ представляет собой обобщение понятия взаимозависимости для разбиений [5, 6] на каналы. Принимая для произвольных каналов $\varrho_i(X)$, $\varrho_j(X)$ и $\varrho_k(X)$, что $H(\varrho_k/\varrho_i) \underset{\mathrm{Df}}{=} H(\varrho_i \cdot \varrho_k) - H(\varrho_i)$, определим количество информации, которой обмениваются каналы ϱ_j и ϱ_k при известном канале ϱ_i, в виде следующей разности:

$$I(\varrho_j \to \varrho_k | \varrho_i) \underset{\mathrm{Df}}{=} H(\varrho_k/\varrho_i) - H(\varrho_k/\varrho_i \cdot \varrho_j).$$

В [2], определяя через $\bar{I}(\varrho_j \to \varrho_h)$ среднее количество информации, которой обмениваются каналы $\varrho_j, \varrho_h \in K$ относительно всех возможных упорядочений системы K, мы доказали, что для любой системы каналов K справедливо

$$\mathfrak{I}(K) = \sum_{\substack{\rho_i, \rho_j \in K \\ \rho_i \neq \rho_j}} \bar{I}(\varrho_i \to \varrho_j).$$

Итак, $\mathfrak{I}(K)$ выражает суммарное количество информации, которой обмениваются различные каналы из K. Можно показать также, что независимо от упорядочения $\varrho_{i_1}, \varrho_{i_2}, \ldots, \varrho_{i_w}$ произвольной системы каналов $K = \{\varrho_1, \varrho_2, \ldots, \varrho_w\}$ верно

$$\mathfrak{I}(K) = \sum_{\substack{j, k=1 \\ j<k}}^{w} I(\varrho_{i_j} \to \varrho_{i_k} | \varrho_{i_1} \cdot \varrho_{i_2} \cdot \ldots \cdot \varrho_{i_{k-1}}).$$

Пусть $E \underset{\mathrm{Df}}{=} \{0, 1\}$, $X = \underbrace{E \times E \times \ldots \times E}_{n \text{ раз}}$ и $z = F(y_1, y_2, \ldots, y_n)$ — булевая функция, реализующая отображение $\bar{F}: X \to E$. Определим на X систему разбиений $K_F = \{\langle \pi_k, \pi_F \rangle | k = 1, \ldots, n\}$, где

$$x_i \equiv x_j (\pi_F) \underset{\mathrm{Df}}{\Longleftrightarrow} \bar{F}(x_i) = \bar{F}(x_j)$$

и для любого $k = 1, \ldots, n$

$$x_i \equiv x_j (\pi_k) \underset{\mathrm{Df}}{\Longleftrightarrow} \mathrm{Пр}_k(x_i) = \mathrm{Пр}_k(x_j)$$

($\mathrm{Пр}_k(x_h)$ — проекция x_h на $y_k^{(h_k)} \in x_h$).

Пусть булевая функция $z = F(y_1, y_2, \ldots, y_n)$ зависит существенно от переменных $y_{i_1}, y_{i_2}, \ldots, y_{i_r}$ $(r \leqslant n)$. В [7] для такой функции была определена комбинаторно-информационная связка (КИС) следующим образом

$$\mathfrak{B}(F) = \sum_{\langle \sigma_k, \pi_F \rangle \in \mathfrak{L}(K'_F)} H(\langle \sigma_k, \pi_F \rangle),$$

где

$$\mathfrak{L}(K'_F) = \{\langle \sigma_k, \pi_F \rangle | \sigma_k = \prod_{\pi_i \in \mathfrak{P}_h} \pi_i, \mathfrak{P}_h \subset \{\pi_{i_1}, \pi_{i_2}, \ldots, \pi_{i_r}\}\}.$$

Из леммы 1 вытекает, что

$$\mathfrak{B}(F) = \sum_{\substack{B_i^{(\alpha)} \in \sigma_i \\ \langle \sigma_i, \pi_F \rangle \in \mathfrak{L}(K'_F)}} q(B_i^{(\alpha)}) H(\bar{\pi}_F(B_i^{(\alpha)})). \tag{4}$$

Ясно, что в формуле (4) $\bar{\pi}_F(B_i^{(\alpha)})$ определяют всевозможные подфункции данной функции F, которой соответствует разбиение $\pi_F(X)$. Выражая для каждой булевой функции F энтропию как $H(\pi_F(X))$, мы можем утверждать, что КИС для F равняется взвешенной сумме энтропий всевозможных подфункций данной функции F. Так как КИС характеризует сложность булевой функции, то мы можем полученный результат переформулировать следующим образом: сложность булевой функции определяется множеством ее подфункций.

Пусть даны произвольные система каналов $K(X)$ и разбиение $\pi_r(X)$. Определим теперь информационный вес $\mathfrak{C}(K(X), \pi_r(X))$ декомпозиций системы каналов $K(X)$ на $\bar{K}(B_r^{(1)})$, $\bar{K}(B_r^{(2)})$, ..., $\bar{K}(B_r^{(m_r)})$ по разбиению π_r в виде следующей разности:

$$\mathfrak{C}(K(X), \pi_r(X)) \underset{\mathrm{Df}}{=} \mathfrak{J}(K(X)) - \sum_{\alpha=1}^{m_r} q(B_r^{(\alpha)}) \mathfrak{J}(\bar{K}(B_r^{(\alpha)})).$$

Теорема 2. *Пусть $K(X)$ — произвольная система каналов при $H(K(X)) = 0$. Тогда для декомпозиции системы $K(X)$ по любому разбиению $\pi_r(X)$ всегда справедливо $\mathfrak{C}(K(X), \pi_r(X)) \geqslant 0$.*

Доказательство. Пусть $K(X) = \{\varrho_1(X), \varrho_2(X), \ldots, \varrho_w(X)\}$. По определению $\mathfrak{J}(K(X)) = \sum_{i=1}^{w} H(\varrho_i(X)) - H(K(X))$. Так как для любого подмножества $X' \subset X$ из $H(K(X)) = 0$ следует $H(\bar{K}(X')) = 0$, то, учитывая предположение теоремы, получаем

$$\mathfrak{C}(K(X), \pi_r(X)) = \sum_{i=1}^{w} H(\varrho_i(X)) - \sum_{\alpha=1}^{m_r} q(B_r^{(\alpha)}) \sum_{i=1}^{w} H(\bar{\varrho}_i(B_r^{(\alpha)})) =$$

$$= \sum_{i=1}^{w} \left(H(\varrho_i(X)) - \sum_{\alpha=1}^{m_r} q(B_r^{(\alpha)}) H(\bar{\varrho}_i(B_r^{(\alpha)})) \right).$$

Для доказательства теоремы достаточно показать, что для любого i ($i = 1, \ldots, w$) имеет место $H(\varrho_i(X)) - \sum_{\alpha=1}^{m_r} q(B_r^{(\alpha)}) H(\bar{\varrho}_i(B_r^{(\alpha)})) \geqslant 0$.

Пусть $\varrho_i(X) \underset{\mathrm{Df}}{=} \langle \pi_{i1}(X), \pi_{i2}(X) \rangle$. Из леммы 2 вытекает, что

$$H(\langle \pi_r \cdot \pi_{i1}(X), \pi_{i2}(X) \rangle) = \sum_{\alpha=1}^{m_r} q(B_r^{(\alpha)}) H(\langle \bar{\pi}_{i1}(B_r^{(\alpha)}), \bar{\pi}_{i2}(B_r^{(\alpha)}) \rangle) =$$

$$= \sum_{\alpha=1}^{m_r} q(B_r^{(\alpha)}) H(\bar{\varrho}_i(B_r^{(\alpha)})).$$

С другой стороны, положив $\varrho_r(X) \underset{\mathrm{Df}}{=} \langle \pi_r(X), 1_X \rangle$, убеждаемся, что $\langle \pi_r \cdot \pi_{i1}(X), \pi_{i2}(X) \rangle = \varrho_i(X) \cdot \varrho_r(X)$. Так как по лемме 2 из [2] справедливо $H(\varrho_i(X)) + H(\varrho_r(X)) \geqslant H(\varrho_i \cdot \varrho_r(X))$, то с учетом $H(\varrho_r(X)) = 0$ для любого $i (i=1, \ldots, w)$ получаем $H(\varrho_i(X)) - \sum_{\alpha=1}^{m_r} q(B_r^{(\alpha)}) H(\overline{\varrho_i(B_r^{(\alpha)})}) \geqslant 0$.

Из этого непосредственно вытекает и утверждение теоремы.

Для любого подмножества $Y_r \underset{\mathrm{Df}}{=} \{y_{i_1}, y_{i_2}, \ldots, y_{i_r}\}$ переменных булевой функции $z = F(y_1, y_2, \ldots, y_n)$ определим $\mathfrak{C}(F, Y_r) \underset{\mathrm{Df}}{=}$ $\underset{\mathrm{Df}}{=} \mathfrak{C}(K_F(X), \prod_{k=1}^{r} \pi_{i_k})$. Если все переменные из Y_r несущественны, то $\mathfrak{C}(F, Y_r) = 0$, ибо тогда $\mathfrak{J}(K_F(X)) = \mathfrak{J}(\overline{K}_F(B_r^{(1)})) = \mathfrak{J}(\overline{K}_F(B_r^{(2)})) = \ldots$ $\ldots = \mathfrak{J}(\overline{K}_F(B_r^{(m_r)}))$, где для любого $\alpha = 1, \ldots, m_r$ имеет место $B_r^{(\alpha)} \in \prod_{k=1}^{r} \pi_{i_k}$. Если $Y_r = \{y_k\}$, то $\overline{K}_F(B_k^{(1)})$ и $\overline{K}_F(B_k^{(2)})$ можно рассматривать как системы каналов для подфункций

$$z = F_{k0}(y_1, y_2, \ldots, y_{k-1}, y_{k+1}, \ldots, y_n) = F(y_1, y_2, \ldots, y_{k-1}, 0, y_{k+1}, \ldots, y_n)$$

и

$$z = F_{k1}(y_1, y_2, \ldots, y_{k-1}, y_{k+1}, \ldots, y_n) = F(y_1, y_2, \ldots, y_{k-1}, 1, y_{k+1}, \ldots, y_n)$$

соответственно. Как видно, информационный вес $\mathfrak{C}(F, \{y_k\})$ характеризует меру несовпадения подфункций для F_{k0} и F_{k1}, ибо $\mathfrak{C}(F, \{y_k\})$ всегда положителен и при совпадении всех подфункций для F_{k0} и F_{k1} равняется нулю. Если мы имеем дело с реализацией булевых функций на мультиплексорах, то информационный вес $\mathfrak{C}(F, Y_r)$ можно использовать в качестве критерия выбора оптимального разложения Шеннона для реализуемой функции. При этом разложение всегда следует выбирать по такому подмножеству переменных Y_i, для которого $\mathfrak{C}(F, Y_i)$ минимален.

Рассмотрим теперь вопрос о применении понятия информационной связки $\mathfrak{J}(K)$ при декомпозиции дискретных автоматов. Имея в виду, что полученные результаты можно легко распространить и на более сложную модель автомата, рассмотрим полуавтомат $A = \langle X, S, \varphi \rangle$, где X — множество входов, S — множество состояний, φ — отображение $X \times S \to S$. В общем декомпозиция автомата начинается с задания ортогональной системы разбиений $P(S)$. Эта система определяет компонентные автоматы и их внутренние состояния, т. е. от выбора $P(S)$ зависит сложность декомпозиции. По процедуре декомпозиции, предложенной в [8], для каждого $\pi_i \in P(S)$ находится соответствующее разбиение $\tau_i = M(\pi_i)$. Разбиение τ_i определяет информацию, которую надо задать на вход компонентного автомата, определенного разбиением π_i, чтобы обеспечить его функционирование в сети компонентных автоматов, реализующей исходный автомат A. Итак, сеть компонентных автоматов по системе $P(S)$ характеризуется системой каналов $K_P(S) \underset{\mathrm{Df}}{=} \{\langle \pi_i, \tau_i \rangle \mid \pi_i \in P(S)\}$, а суммарное количество информации, которой обмениваются между собой компонентные автоматы, выражается через $\mathfrak{J}(K_P(S)) = \sum_{\varrho_i \in K_P(S)} H(\varrho_i)$. При проведении декомпозиции следует выбирать такую ортогональную систему $P(S)$, для которой $\mathfrak{J}(K_P(S))$ минимальна. Если у нас для выбранной $P(S)$ получается сеть параллельных компонентных автоматов, то $\mathfrak{J}(K_P(S)) = 0$, ибо тогда для любого $\langle \pi_i, \tau_i \rangle \in K_P(S)$ имеет место $\pi_i \leqslant \tau_i$.

ЛИТЕРАТУРА

1. Hartmanis, J., Stearns, R. E., Algebraic Structure Theory of Sequental Machines, Prentice-Hall, Inc., Englewood Cliffs, New York, 1966.
2. Лаусмаа Т., Изв. АН ЭССР, Физ. Матем., 28, № 4, 338—345 (1979).
3. Фадеев Д. К., Успехи мат. наук, 11, вып. 1 (67), 227—231 (1956).
4. Шеннон К., Работы по теории информации и кибернетике, М., ИЛ, 1963.
5. Watanabe, S., Knowing and Guessing, John Wiley and Sons, Inc., New York, 1969.
6. Guiasu, S., Reischer, C., R.A.I.R.O. — Theoretical inform., 13, № 4, 395—407 (1979).
7. Лаусмаа Т., Изв. АН ЭССР, Физ. Матем., 29, № 4, 349—355 (1980).
8. Кеэваллик А. Э., Автоматика и вычисл. техн., № 1, 17—24 (1974).

Институт термофизики и электрофизики
Академии наук Эстонской ССР

Поступила в редакцию
6/IV 1981

T. LAUSMAA

TÜKELDUSPAARI KVANTITATIIVNE INFOMÕÕT

Jätkub artiklis [1] alustatud tükelduspaaride informatiivsete omaduste vaatlus. Tükeldusele kui informatsioonile on leitud selle omadustest tulenev ühene kvantitatiivne mõõt, mille kaudu osutub võimalikuks hinnata kvantitatiivselt ka tükelduspaare. On vaadeldud saadud hinnangu rakendusvõimalusi Boole'i funktsioonide multiplekskorrelatsiooni ning diskreetsete automaatide dekomponeerimise korral.

T. LAUSMAA

ON THE QUANTITATIVE INFORMATIONAL MEASURE FOR PARTITION PAIRS

In their classical work about the structure theory of automata [1] J. Hartmanis and R. E. Stearns use the notion of partition as an algebraic interpretation of information. In their approach the information on a finite set is equivalent to a partition defined on this set. Likewise the concept of partition pair is used for representing an «information flow». This approach has proved to be very successful in obtaining various qualitative results in the structure theory of automata. But for solving decompositional problems for automata we need a quantitative informational evaluation of partition pairs. The quantitative approach gives us an opportunity to estimate incomparable partition pairs as well.

The first attempt in obtaining a quantitative informational measure for any arbitary partition pair was made in [2]. The obtained measure was not entirely an inherent characteristic for partition pairs, but depended on the proposed probability distribution on the basic set as well. The present approach, in return, provides us with an entirely inherent quantitative informational measure for partition pairs based on natural informational properties of partition. The characteristic feature of this approach is the fact that it is not based on the notion of probability. As partition pairs describe only functional dependences in an automaton for us, it is important to note that the information we are concerned with does not represent the actual information processed by automaton, but is equivalent to the interdependence between functional dependences in the description of automaton. Therefore, the derived informational criteria are independent any possible mode of operation for the given automaton.

The proposed approach provides us with some interesting applications. In this paper a criterion is given which enables us to estimate different Shannon's expansions of Boolean functions for the optimal realisation of the given function on universal logical moduls. The option of an orthogonal partition set for the decomposition of discrete automata [8] is also discussed. The criterion for that option is based on the proposition that a set of component automata is the more complicated the more functionally related the component automata in this set are. By this criterion the parallel set of component automata is the most uncomplicated one, because in this case there is no functional dependence between component automata.