

Т. ЛАУСМАА

УДК 519.714.4

ИНФОРМАЦИОННАЯ ОЦЕНКА БУЛЕВЫХ ФУНКЦИЙ

(Представил А. Хумал)

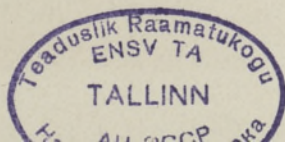
На основе информационной характеристики системы пар разбиений на конечном множестве [1] рассматривается оценка сложности булевых функций с позиций комбинаторного подхода к определению понятия «количество информации». Булевая функция интерпретируется как система параллельных зависимых информационных каналов в предположении, что она тем сложнее, чем больше информации передается между этими каналами. Для оценки этой информации вводится понятие комбинаторно-информационной связки (КИС) и приводится алгоритм вычисления КИС для булевых функций. Показывается, что сомножители КИС разбивают булевы функции на классы, которые совпадают с классами инвариантности относительно перестановки аргументов и инвертирования значений аргументов и функций. Приводится оценка значений КИС для булевых функций от n переменных и показывается, что оценка внутренней сложности булевой функции по КИС имеет сильную корреляцию со сложностью известных на практике реализаций.

В большинстве существующих информационных критериев для оценки сложности используется вероятностный подход к определению понятия «количество информации» [2]. При этом предполагается, что интересующее нас распределение вероятностей задано заранее. Однако на практике это распределение обычно неизвестно, что затрудняет применение этого информационного критерия. Кроме того, зависимость результатов от распределения вероятностей, определяемого режимом работы рассматриваемой системы, вызывает сомнение в правомерности такого критерия, ибо сложность системы, как правило, должна быть инвариантна относительно режима ее работы. Обойти перечисленные недостатки позволяет, как нам кажется, комбинаторный подход к определению понятия информации [2]. При таком подходе из таблицы истинности булевой функции определяют комбинаторные веса (аналог вероятности при вероятностном подходе) для значений входных переменных и функций. Подобный комбинаторный подход был использован в направлении теории информации, представленном работами Б. М. Фитингофа и В. Д. Голпа [3-5]. В этом плане настоящая работа согласуется также с классическими исследованиями Дж. Хартманиса и Р. Е. Стирнза по структурной теории автоматов, развивая алгебраическую интерпретацию понятия информации.

Пусть дано конечное множество $X = \{x_1, x_2, \dots, x_m\}$. Для любого подмножества $X' \subset X$ определим его комбинаторный вес $q(X')$ следующим образом:

$$q(X') = \frac{\|X'\|}{\|X\|},$$

где $\|X^{(i)}\|$ — мощность множества $X^{(i)}$.



Разбиение множества X на непересекающиеся подмножества (блоки) $B_i^{(1)}, B_i^{(2)}, \dots, B_i^{(\alpha)}, \dots, B_i^{(m)}$ обозначим через $\pi_i(X)$. Определим для каждого разбиения $\pi_i(X)$ энтропию $H(\pi_i)$:

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

Любую пару разбиений $q_i = \langle \pi_i', \pi_i'' \rangle$ будем называть каналом. Для каждого канала $\langle \pi_i, \pi_k \rangle$ определим энтропию $H(\langle \pi_i, \pi_k \rangle)$:

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

В [1] было показано, что для любой системы каналов K справедливо неравенство $\sum_{q_i \in K} H(q_i) \geq H(K)$, где $H(K) = H(\prod_{q_i \in K} q_i)$.

Пусть q_i, q_j и q_k — произвольные каналы на X . Принимая, что $H(q_k/q_i) \stackrel{\text{Df}}{=} H(q_i \cdot q_k) - H(q_i)$, определим количество информации, которой обмениваются каналы q_j и q_k при известном канале q_i , в виде следующей разности

$$I(q_j \rightarrow q_k | q_i) \stackrel{\text{Df}}{=} H(q_k/q_i) - H(q_k/q_i \cdot q_j).$$

Рассмотрим теперь среднее количество информации $\bar{I}(q_j \rightarrow q_k)$, которой обмениваются каналы $q_j, q_k \in K(X)$ относительно всех возможных упорядочений системы K . Введем обозначение

$$\mathfrak{S}(K) \stackrel{\text{Df}}{=} \sum_{\substack{q_i, q_j \in K \\ q_i \neq q_j}} \bar{I}(q_i \rightarrow q_j).$$

$\mathfrak{S}(K)$ выражает суммарное количество информации, которой обмениваются различные каналы из K . В [1] доказано, что для любой системы каналов $K = \{q_1, q_2, \dots, q_w\}$ справедливо выражение

$$\mathfrak{S}(K) = \sum_{j=1}^w H(q_j) - H(K).$$

Обозначая через $\mathfrak{Q}(K)$ минимальную решетку каналов, содержащую систему каналов K , определим КИС для системы каналов K следующим образом:

$$\mathfrak{B}(K) \stackrel{\text{Df}}{=} \mathfrak{S}(\mathfrak{Q}(K)) = \sum_{q_j \in \mathfrak{Q}(K)} H(q_j) - H(\mathfrak{Q}(K)).$$

Пусть $E \stackrel{\text{Df}}{=} \{0, 1\}$ и $X = \{x_1, x_2, \dots, x_{2^n}\} \stackrel{\text{Df}}{=} \underbrace{E \times E \times \dots \times E}_{n \text{ раз}}$. Функцию

$z = F(y_1, y_2, \dots, y_n)$, реализующую отображение $\bar{F}: X \rightarrow E$, назовем булевой функцией. Определим теперь на множестве X разбиения $\pi_k (k = 1, \dots, n)$ и π_F :

$$x_i \equiv x_j(\pi_k) \stackrel{\text{Df}}{\iff} \text{Пр}_k(x_i) = \text{Пр}_k(x_j);$$

$$x_i \equiv x_j(\pi_F) \stackrel{\text{Df}}{\iff} \bar{F}(x_i) = \bar{F}(x_j),$$

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

Обозначим $\mathbb{P}_X = \{\pi_1, \pi_2, \dots, \pi_n\}$. Систему разбиений $\mathbb{P}_F = \underset{\text{Df}}{\mathbb{P}_X \cup \{\pi_F\}}$ назовем информационным представлением булевой функции F . Определим систему каналов K_F для любой функции F от n переменных: $K_F = \{(\pi_k, \pi_F) | k = 1, \dots, n\}$. Легко видеть, что

Лемма 1. Для любой булевой функции F справедливо

$$\mathfrak{L}(K_F) = \{(\sigma_k, \pi_F) | \sigma_k = \prod_{\pi_i \in \mathbb{P}'_X} \pi_i, \mathbb{P}'_X \subset \mathbb{P}_X\}.$$

Введем обозначение

$$\mathfrak{S}_F = \{H(q_i) | q_i \in \mathfrak{L}(K_F)\}.$$

Элементы множества \mathfrak{S}_F назовем информационными сомножителями данной функции F . Из леммы 1 вытекает, что любой сомножитель $H(q_k)$ может быть выражен в виде $H(\pi_F/\pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_r})$, где $0 \leq r \leq n$. Сомножители $H(\pi_F/\pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_r})$ назовем сомножителями r -го ранга, полагая, что $H(\pi_F)$ — сомножитель нулевого ранга.

Примем, что булевая функция $z = F(y_1, y_2, \dots, y_n)$ существенно зависит от переменной y_i ($1 \leq i \leq n$) тогда и только тогда, когда для переменных $y_1, y_2, \dots, y_{i-1}, y_{i+1}, \dots, y_n$ найдется набор значений $y_1^{(\alpha_1)}, y_2^{(\alpha_2)}, \dots, y_{i-1}^{(\alpha_{i-1})}, y_{i+1}^{(\alpha_{i+1})}, \dots, y_n^{(\alpha_n)}$ такой, что

$$\begin{aligned} & F(y_1^{(\alpha_1)}, y_2^{(\alpha_2)}, \dots, y_{i-1}^{(\alpha_{i-1})}, 0, y_{i+1}^{(\alpha_{i+1})}, \dots, y_n^{(\alpha_n)}) \neq \\ & \neq F(y_1^{(\alpha_1)}, y_2^{(\alpha_2)}, \dots, y_{i-1}^{(\alpha_{i-1})}, 1, y_{i+1}^{(\alpha_{i+1})}, \dots, y_n^{(\alpha_n)}). \end{aligned}$$

Лемма 2. Для того чтобы булевая функция $z = F(y_1, y_2, \dots, y_n)$ существенно зависела только от переменных $y_{i_1}, y_{i_2}, \dots, y_{i_r}$ ($r \leq n$), необходимо и достаточно, чтобы среди нулевых информационных сомножителей F минимальный ранг имел бы сомножитель $H(\pi_F/\pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_r})$.

Доказательство. Обозначим $R = \{\pi_{i_1}, \pi_{i_2}, \dots, \pi_{i_r}\}$ и $m(R) = \underset{\text{Df}}{\prod_{\pi_k \in R} \pi_k}$. Из того, что $H(\pi_F/m(R)) = 0$, вытекает $m(R) \leq \pi_F$. По-

этому для любого блока $B^{(\alpha)} \in m(R)$ найдется блок $B_{F^{(\alpha)}} \in \pi_F$ такой, что $B^{(\alpha)} \subset B_{F^{(\alpha)}}$. Это означает, что переменные $y_{i_1}, y_{i_2}, \dots, y_{i_r}$, соответствующие разбиениям $\pi_{i_1}, \pi_{i_2}, \dots, \pi_{i_r}$, полностью определяют функцию F . И, напротив, если $H(\pi_F/m(R)) \neq 0$, то переменные $y_{i_1}, y_{i_2}, \dots, y_{i_r}$ не определяют полностью функцию F . Поэтому для любого подмножества $P \subset \mathfrak{L}(\mathbb{P}_X)$ равенство $H(\pi_F/m(P)) = 0$ эквивалентно тому, что подмножество переменных, соответствующее множеству разбиений P , содержит все существенные переменные. Из этого непосредственно вытекает утверждение леммы.

Определим алгоритм нахождения КИС для булевой функции F в соответствии с леммами 1 и 2.

Алгоритм. 1. Из множества информационных сомножителей \mathfrak{S}_F вычисляем сомножители по возрастанию их рангов до тех пор, пока не встретим сомножителя $H(\pi_F/\pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_r})$, равного нулю.

2. Определяем КИС как сумму тех информационных сомножителей из \mathfrak{S}_F , которые выражаются в виде $H(\pi_F/\sigma_j)$ при $\sigma_j \in \mathfrak{L}(\{\pi_{i_1}, \pi_{i_2}, \dots, \pi_{i_r}\})$.

Пусть булевая функция $z = F(y_1, y_2, \dots, y_n)$ существенно зависит от переменных $y_{i_1}, y_{i_2}, \dots, y_{i_r}$ ($r \leq n$). Тогда, как легко убедиться, КИС этой функции, определенная по алгоритму, равняется

$$\mathfrak{B}(F) = \mathfrak{S}(\mathfrak{L}(K'_F)) =$$

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

где $K'_F = \{\langle \pi_j, \pi_F \rangle \mid j = i_1, i_2, \dots, i_r\}$.

Определим теперь на множестве булевых функций от n переменных отношение эквивалентности по однотипности, полагая, что $F^{(i)}$ однотипно $F^{(j)}$ ($F^{(i)} \equiv F^{(j)}$) тогда и только тогда, когда $F^{(j)}$ можно получить из $F^{(i)}$ с помощью следующих операций:

- 1) перестановки аргументов y_1, y_2, \dots, y_n ;
- 2) отрицания любого аргумента y_k ($1 \leq k \leq n$);
- 3) отрицания значения функции $F^{(i)}$.

Теорема 1. Для любых булевых функций F' и F'' справедливо

$$F' \equiv F'' \Leftrightarrow \mathfrak{F}_{F'} = \mathfrak{F}_{F''}.$$

Доказательство. Введем обозначение

$$\mathfrak{Z}_F = \{H(\pi_F \cdot \sigma_i) \mid \sigma_i \in \mathfrak{L}(\mathfrak{P}_X)\}.$$

В [6] доказано, что для любых функций F' и F'' всегда справедливо $F' \equiv F'' \Leftrightarrow \mathfrak{Z}_{F'} = \mathfrak{Z}_{F''}$. Так как $H(\pi_F / \sigma_i) = H(\pi_F \cdot \sigma_i) - H(\sigma_i)$, то $H(\pi_{F'} \cdot \sigma_i) = H(\pi_{F''} \cdot \sigma_i) \Leftrightarrow H(\pi_{F'} / \sigma_i) = H(\pi_{F''} / \sigma_i)$. Поэтому $\mathfrak{Z}_{F'} = \mathfrak{Z}_{F''} \Leftrightarrow \mathfrak{F}_{F'} = \mathfrak{F}_{F''}$, откуда и следует справедливость теоремы.

Из теоремы 1 вытекает

Следствие. Если функции F' и F'' однотипны, то всегда $\mathfrak{B}(F') = \mathfrak{B}(F'')$, т. е. КИС сохраняет классы однотипности.

Для численной характеристики булевых функций удобно воспользоваться КИС, где информация выражается в битах (в формулах будем обозначать через $\mathfrak{B}_2(F)$). В связи с этим при определении КИС вместо $\ln x$ будем употреблять $\log_2 x$.

Теорема 2. Если булева функция $F(y_1, y_2, \dots, y_n)$ существенно зависит от всех переменных y_1, y_2, \dots, y_n , то для $\mathfrak{B}_2(F)$ справедлива оценка $n/2 + (1 - (1 - \ln 2/2)^n) / \ln 2 - C_n < \mathfrak{B}_2(F) \leq 2^n - 1$, где C_n — константа при $\max_{n \rightarrow \infty} C_n < 0,05$ и $\lim_{n \rightarrow \infty} C_n = 0$.

Доказательство. Нетрудно убедиться, что для произвольных $\pi_{i_1}, \pi_{i_2}, \dots, \pi_{i_k}$ из \mathfrak{P}_X получаем $H_2(\pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_k}) = k$. Покажем, что существует бинарное разбиение π_{F^ω} на X такое, что $H_2(\pi_{F^\omega}) = 1$ и для любых $\pi_{i_1}, \pi_{i_2}, \dots, \pi_{i_k}$ при $k < n$ всегда $H_2(\pi_{F^\omega} \cdot \pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_k}) = k + 1$. Так как любое $x_i \in X$ выражается как $x_i = y_1^{i_1} y_2^{i_2} \dots y_n^{i_n}$, где $y_k^{i_k} = 0 \vee 1$ ($k = 1, \dots, n$), то определим:

$$B_{\pi_{F^\omega}}^{(1)} = \{x_i \mid \text{число знаков 1 в } x_i \text{ равняется } 2m \ (m = 0, 1, 2, \dots)\},$$

$$B_{\pi_{F^\omega}}^{(2)} = \{x_j \mid \text{число знаков 1 в } x_j \text{ равняется } 2m + 1 \ (m = 0, 1, 2, \dots)\}.$$

Легко видеть, что при таком определении действительно $H_2(\pi_{F^\omega}) = 1$ и для любого $k < n$ верно $H_2(\pi_{F^\omega} \cdot \pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_k}) = k + 1$. Итак, получаем, что для любых $\pi_{i_1}, \pi_{i_2}, \dots, \pi_{i_k}$ при $k < n$ всегда $H_2(\pi_{F^\omega} / \pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_k}) = 1$. Учитывая еще, что $H_2(\pi_{F^\omega} / \pi_1 \cdot \pi_2 \cdot \dots \cdot \pi_n) = 0$, получаем $\mathfrak{B}_2(F^\omega) = 2^{n-1}$. Нетрудно убедиться, что $F^\omega = y_1 \oplus y_2 \oplus \dots \oplus y_n$, где \oplus — операция сложения по модулю 2. Ясно, что при про-

извольном бинарном разбиении π_F для любых $\pi_{i_1}, \pi_{i_2}, \dots, \pi_{i_k} (k \leq n)$ всегда $H_2(\pi_F/\pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_k}) \leq H(\pi_F) \leq 1$ и поэтому для каждой булевой функции F_n от n переменных $\mathfrak{B}_2(F_n) \leq 2^{n-1}$.

Легко показать, что среди нетривиальных бинарных разбиений на X наименьшую энтропию имеет разбиение $\pi_{F^\alpha} = \{\{x_h\}, X/\{x_h\}\}$, где x_h — произвольный элемент из X . Для любых $\pi_{i_1}, \pi_{i_2}, \dots, \pi_{i_k}$ из \mathfrak{B}_X имеет место

$$H(\pi_{F^\alpha}/\pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_k}) = \\ = q(B_{\sigma_k}^{(h')}) \cdot \log_2 q(B_{\sigma_k}^{(h')}) + q(B_{\sigma_k}^{(h)}) \cdot \log_2 q(B_{\sigma_k}^{(h)}) - q(B_{\sigma_k}^{(h')}) \cdot \log_2 q(B_{\sigma_k}^{(h)}),$$

где $\sigma_k \stackrel{\text{Df}}{=} \pi_{i_1} \cdot \pi_{i_2} \cdot \dots \cdot \pi_{i_k}$, $B_{\sigma_k}^{(h)}$ — блок разбиения σ_k , содержащий элемент x_h , $B_{\sigma_k}^{(h)} = \{x_h\}$, $B_{\sigma_k}^{(h')} = B_{\sigma_k}^{(h)}/B_{\sigma_k}^{(h)}$. Поэтому для любой булевой

функции F_n всегда $\mathfrak{B}_2(F_n) \geq \mathfrak{B}_2(F_n^\alpha)$. Учитывая, что $(2^{n-k}/2^n) \cdot \log_2(2^{n-k}/2^n) - ((2^{n-k}-1)/2^n) \cdot \log_2((2^{n-k}-1)/2^n) - (1/2^n) \cdot \log_2(1/2^n) = (1/2^n)[n-k - (2^{n-k}-1) \cdot \log_2(1 - (1/2)^{n-k})]$, получаем $\mathfrak{B}_2(F_n^\alpha) = (1/2^n) \cdot \sum_{k=0}^n \binom{n}{k} [n-k - (2^{n-k}-1) \cdot \log_2(1 - (1/2)^{n-k})]$.

Воспользуемся разложением: $(2^{n-k}-1) \cdot \log_2(1 - (1/2)^{n-k}) = ((2^{n-k}-1)/\ln 2) \cdot [(1/2)^{n-k} + (1/2) \cdot (1/4)^{n-k} + (1/3) \cdot (1/8)^{n-k} + \dots] = (1/\ln 2) \cdot [1 - (1 - 1/2)(1/2)^{n-k} - (1/2 - 1/3) \cdot (1/4)^{n-k} - (1/3 - 1/4)(1/8)^{n-k} - \dots]$.

Из симметрии $\binom{n}{k} = \binom{n}{n-k}$ следует, что

$$\sum_{k=0}^n \binom{n}{k} (n-k) = (1/2) \sum_{k=0}^n \binom{n}{k} \cdot n = (n/2) \cdot 2^n.$$

Учитывая также, что для произвольного числа p верно

$$\sum_{k=0}^n \binom{n}{k} (1/p)^{n-k} = (1 + (1/p))^n, \text{ получаем}$$

$$\mathfrak{B}_2(F_n^\alpha) = n/2 + 1/\ln 2 - (1/2^n \cdot \ln 2) \sum_{k=1}^{\infty} (1/k) \cdot (1/k+1) (1+1/2^k)^n.$$

Так как $1/2 + 1/2 \cdot (1/2)^2 + 1/3 \cdot (1/2)^3 + \dots = -\ln(1 - 1/2) = \ln 2$, то $\sum_{k=1}^{\infty} (1/k) (1/k+1) (1 + 1/2^k) = 2 - \ln 2$. Учитывая, что $\sum_{k=1}^{\infty} (1/k) \cdot (1/k+1) \cdot (1+1/2^k)^n \approx (\sum_{k=1}^{\infty} (1/k) \cdot (1/k+1) (1+1/2^k))^n$, получаем для $\mathfrak{B}_2(F_n^\alpha)$ следующую оценку:

$$\mathfrak{B}_2(F_n^\alpha) \approx n/2 + 1/\ln 2 - (2 - \ln 2)^n / 2^n \cdot \ln 2 = n/2 + (1 - (1 - \ln 2/2)^n) / \ln 2.$$

Практические расчеты показывают, что

$$\mathfrak{B}_2(F_n^\alpha) > n/2 + (1 - (1 - \ln 2/2)^n) / \ln 2 - C_n,$$

где $\max C_n < 0,05$ и $\lim_{n \rightarrow \infty} C_n = 0$.

Из теоремы 2 можно сделать вывод, что для достаточно больших n справедливо

$$\mathfrak{B}_2(F_n) \geq n/2 + 1/\ln 2.$$

В таблице приведены значения КИС для представителей типов булевых функций от 3-х переменных. Представители типов заданы в виде совокупности номеров их минтермов в десятичной форме записи. В скобках указано число существенных переменных представителей типов.

Номер типа	Представитель типа	КИС, бит
1	—	(0) 0,000
2	0,1,2,3	(1) 1,000
3	0,1	(2) 1,811
4	0	(3) 2,510
5	0,1,2	(3) 4,421
6	0,3	(3) 4,434
7	0,1,6,7	(2) 3,000
8	0,1,2,5	(3) 5,123
9	0,1,6	(3) 5,421
10	0,1,2,4	(3) 4,934
11	0,1,2,7	(3) 5,811
12	0,7	(3) 4,745
13	0,3,5	(3) 5,921
14	0,3,5,6	(3) 7,000

Одним из практических приложений КИС может служить использование ее для оценки сложности булевых функций. Эта оценка основывается на предположении, что всякая система (в данном случае булевая функция) тем сложнее, чем больше информации передается между ее компонентами. В качестве критериев, по которым сравнивали КИС, были выбраны схемная реализация булевых функций на программируемых логических матрицах и программная реализация в виде бинарных программ [7, 8]. Сравнение проводилось для представителей классов однотипных функций от 4-х переменных. Расчеты показали, что в первом случае корреляция равнялась 0,86, а во втором — 0,88. Эти результаты свидетельствуют о том, что КИС является абстрактной характеристикой реальной сложности булевых функций.

ЛИТЕРАТУРА

1. Лаусмаа Т., Изв. АН ЭССР, Физ. Матем., 28, № 4, 338—345 (1979).
2. Колмогоров А. Н., Проблемы передачи информации, 1, вып. 1, 3—11 (1965).
3. Фитингоф Б. М., Проблемы передачи информации, 2, вып. 2, 3—11 (1966).
4. Гоппа В. Д., Проблемы передачи информации, 11, вып. 1, 15—22 (1975).
5. Гоппа В. Д., Проблемы передачи информации, 14, вып. 3, 3—17 (1978).
6. Matheson, W. S., IEEE Trans. Comput., 20, № 6, 691—694 (1971).
7. Lee, C. Y., Bell Syst. Techn. J., 38, № 4, 985—999 (1959).
8. Кузнецов О. П., Автоматика и телемеханика, № 7, 163—174 (1977); № 9, 137—149 (1977).

Институт термофизики и электрофизики
Академии наук Эстонской ССР

Поступила в редакцию
13/V 1980

T. LAUSMAA

BOOLE'I FUNKTSIOONIDE INFORMATIIVNE HINNANG

On vaadeldud artiklis [1] analüüsitud tükelduspaaride süsteemi informatsioonivahetuse rakendust Boole'i funktsioonide keerukuse hindamisel. Informatsiooni hulga mõiste määramisel on kasutatud kombinatoorset lähenemist [2]. Esitatud informatiivne hinnang jagab n -muutuja Boole'i funktsioonid ekvivalentsusklassideks, mis ühtivad PCN-klassidega [6]. On toodud selle hinnangu väärtuste piirkond ning näidatud hinnangu tugevat korrelatsiooni funktsioonide praktiliste realiseerimiste keerukusega.

T. LAUSMAA

ON THE INFORMATIONAL MEASURE OF COMPLEXITY
FOR SWITCHING FUNCTIONS

Lately the rapid progress in integrated circuit technology has caused a need for new design methods of optimal networks synthesis. These methods need a new abstract approach for estimating the complexity of switching functions.

The present paper introduces a combinative informational measure of complexity for switching functions. The basic philosophy of this measure is the thesis that a system is the more complicated, the larger is the amount of information exchanged between its components. As a set of components of a switching function a lattice of partition pairs on the whole set of value combinations of variables is chosen. Assigning a partition pair to each infochannel from an input variable to the output of the given function, we get the generating set of partition pairs for this lattice. The quantitative evaluation of information exchange between partition pairs in the lattice is based on the formulas given in the previous paper [1]. The characteristic feature of the presented measure is the combinative approach to the notion «amount of information» [2]. The used combinative approach is very similar to the trend in the information theory represented in the works by B. Fitingof and V. Goppa [3-5]. The presented approach gives us an inherent measure of complexity for switching functions independent of any specific technical realization and its mode of operation. As for the practical realizations, it is sufficient not to evaluate each switching function apart, but to group the functions into the so-called «PCN-equivalence classes» [6]. Therefore it is remarkable that the factors of proposed combinative informational measure as shown in the present paper partition switching functions exactly into PCN classes. Besides, this paper provides us with the limit values of the proposed complexity measure for the switching functions of n variables. It is shown that the high limit for the values of this measure for the functions of n variables is proportional to n power of number two and the low limit to n . The estimation of proposed measure from the practical point of view is carried out for the functions of 4-variables. For practical realizations the one on the programmed logic array and the other by binary programs [7, 8] are chosen. Comparison between the presented measure of complexity and these practical realizations in the given order gave us the values of correlation coefficients 0.86 and 0.88, correspondingly. These results show that the combinative informational measure of complexity characterizes the inherent complexity of switching functions.