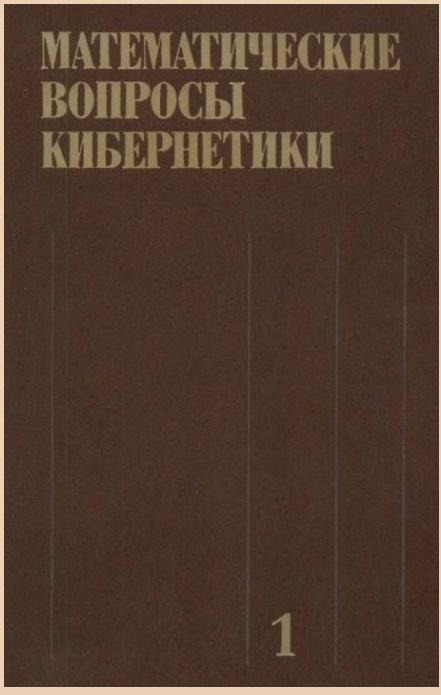
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 1



А. В. Сержантов

Об оптимальном алгоритме расшифровки монотонных функций конечнозначной логики

Рекомендуемая форма библиографической ссылки: Сержантов А. В. Об оптимальном алгоритме расшифровки монотонных функций конечнозначной логики // Математические вопросы кибернетики. Вып. 1. — М.: Наука, 1988. — С. 223–233. URL: http://library.keldysh.ru/mvk.asp?id=1988-223

ОБ ОПТИМАЛЬНОМ АЛГОРИТМЕ РАСШИФРОВКИ МОНОТОННЫХ ФУНКЦИЙ КОНЕЧНОЗНАЧНОЙ ЛОГИКИ

А. В. СЕРЖАНТОВ
(МОСКВА)

Рассматривается задача о «расшифровке, т. е. восстановлении, опознавании монотонной функции по ее значениям в некоторых точках области определения. Решение этой задачи позволяет сократить перебор объектов в некоторых прикладных задачах, таких как выделение всех существенных или тупиковых совокупностей переменных частичной функции алгебры логики [3], построение матрицы оптимального алфавитного кодирования [7], оптимальное восстановление и поиск глобального экстремума функций с ограниченной производной [6], построение таблицы эталонных объектов в распознавании образов, выбор алгоритма планирования эксперимента и др. Решению задачи о расшифровке монотонных функций посвящены работы [1, 2, 4, 5, 8, 9].

Определение 1. *Прямым произведением* $P \times Q$ множеств P и Q называется множество элементов вида (x, y), где $x \in P$ и $y \in Q$.

Определение 2. Пусть задано множество $E \subseteq E_{k_1} \times E_{k_2} \times \ldots \ldots \times E_{k_n}$, где $E_{k_i} = \{0, \ldots, k_i - 1\}$. Функция $f(\tilde{x}) = f(x_1, \ldots, x_n)$, где $x_i \in E_{k_i}$ и $f \in \{0, 1\}$, называется *монотонной* на E, если для любых $\tilde{x} = (x_1, \ldots, x_n)$ и $\tilde{y} = (y_1, \ldots, y_n)$ таких, что $x_i \leqslant y_i$ при $i = 1, \ldots, n$, выполнено неравенство

$$f(\tilde{x}) \leqslant f(\tilde{y}).$$

Постановка задачи. Пусть $f(\tilde{x})$ — неизвестная монотонная функция, значения которой необходимо определить во всех точках $\tilde{x}$ области задания E. Предполагается наличие процедуры, позволяющей запрашивать значение f в произвольной точке $\tilde{x}$ множества E. При этом значения функции определяются не только в точке $\tilde{x}$, но и распространяются по монотонности на часть множества E. Требуется построить алгоритм U последовательного определения значений (расшифровки) f так, чтобы число $t(E, U(f))$ точек, в которых запрашиваются значения f, было минимально.

Определение 3. *Трудоемкостью* алгоритма расшифровки U называется число $t(E, U)$ такое, что справедливо равенство

$$t(E, U) = \max_f t(E, U(f)),$$

где максимум берется по всем монотонным функциям, заданным на множестве E.

Определение 4. Алгоритм расшифровки U_0 называется *оптимальным*, если выполнено равенство

$$t(E, U_0) = \min_U t(E, U).$$

Определение 5. *Слоем* C_p множества E называется множество всех наборов $\tilde{x} = (x_1, \ldots, x_n)$ таких, что

$$p = \sum_{i=1}^{n} x_i.$$

Два слоя C_p и C_q называются соседними, если $|p - q| = 1$.

Обозначим через $g_2(E)$ максимальную суммарную мощность двух соседних слоев множества E. Известна [1] следующая нижняя оценка трудоемкости оптимального алгоритма расшифровки:

$$t(E, U_0) \geqslant g_2(E).$$

Обзор результатов, относящихся к оценке трудоемкости оптимального алгоритма расшифровки, можно найти в [8]. В [8] показано, что если построено покрытие области задания функции f цепями специального вида (A-покрытие), то существует оптимальный алгоритм U_0 с трудоемкостью $t(E, U_0) = g_2(E)$. Простейшим примером A-покрытия является покрытие множества E_p^2, изображенное для $p = 4$ на рис. 1. В [8] указан способ построения A-покрытия для множеств R, представимых в виде

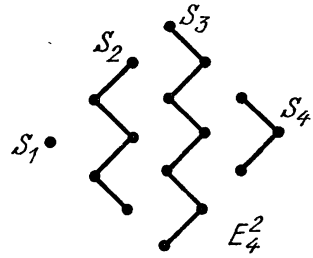


Рис. 1

$$R = E_{k_1}^2 \times E_{k_2}^2 \times \ldots \times E_{k_n}^2.$$

Далее будет указана модификация A-покрытия, позволяющая обобщить оптимальный алгоритм расшифровки на множества вида $Q = E_p^2 \times E_k \times R$, где $p \geqslant k$.

Определение 6. Последовательность $S = (\tilde{x}_1, \ldots, \tilde{x}_r)$ элементов множества E называется *цепью*, если

$$\tilde{x}_{j+1} = \tilde{x}_j + \tilde{e}_{i_j} \quad \text{при} \quad j = 1, \ldots, r-1.$$

Здесь через $\tilde{e}_{i_j}$ обозначен набор, у которого компонента с номером i_j равна 1, а все остальные компоненты нулевые, и знак «+» обозначает обычное покоординатное сложение наборов. Наборы $\tilde{x}_1$ и $\tilde{x}_r$ называются соответственно нижней и верхней вершинами цепи S.

Определение 7. Множество цепей $\{S_i\}$ называется *покрытием* множества E, если $S_i \cap S_j = \varnothing$ при $i \neq j$ и $\bigcup\limits_i S_i = E$.

Определение 8. Покрытие $\{S_i\}$ множества E, цепи которого упорядочены, называется *A-покрытием* и обозначается $A(E)$, если выполнены следующие условия.

1. Цепи $\{S_i\}$ симметричны, т. е. для любой цепи S выполнено равенство

$$\sum_{j=1}^{n} x_1^{(j)} = \sum_{j=1}^{n} \left(k_j - 1 - x_r^{(j)}\right),$$

где $\tilde{x}_1$ и $\tilde{x}_r$ — соответственно нижняя и верхняя вершины цепи S.

2. Если $|S_i| > 3$, то для любых четырех последовательных вершин $\tilde{x}_t$, $\tilde{x}_{t+1}$, $\tilde{x}_{t+2}$, $\tilde{x}_{t+3}$ цепи S_i, т. е. таких, что имеют место равенства

$$\tilde{x}_{t+1} = \tilde{x}_t + \tilde{e}_{t_1}, \quad \tilde{x}_{t+2} = \tilde{x}_{t+1} + \tilde{e}_{t_2}, \quad \tilde{x}_{t+3} = \tilde{x}_{t+2} + \tilde{e}_{t_3},$$

выполнены следующие два условия:

2.1. $(t_1 \neq t_2) \vee (t_2 \neq t_3)$,

2.2. $\exists j\,(j < i \,\&\, (\tilde{x}'_{t+1} \in S_j \vee \tilde{x}'_{t+2} \in S_j))$, где $\tilde{x}'_{t+1} = \tilde{x}_t + \tilde{e}_{t_2}$ и $\tilde{x}'_{t+2} = \tilde{x}_{t+1} + \tilde{e}_{t_3}$. Вершины $\tilde{x}'_{t+1}$ и $\tilde{x}'_{t+2}$ будем называть сопряженными для вершин $\tilde{x}_t$, $\tilde{x}_{t+1}$, $\tilde{x}_{t+2}$ и $\tilde{x}_{t+1}$, $\tilde{x}_{t+2}$, $\tilde{x}_{t+3}$ соответственно.

В [8] доказаны следующие две теоремы.

Теорема 1. *Если на множествах P и Q заданы покрытия $A(P)$ и $A(Q)$, то на множестве $P\times Q$ также существует покрытие $A(P\times Q)$.*

Замечание 1. Далее будет использоваться следующая конструкция из доказательства теоремы 1. Пусть $A(P)=\{S_j\}$ и $A(Q)=\{T_k\}$. В каждом из множеств $S_j\times T_k$ симметричные цепи строятся так, как это показано на рис. 2.

Теорема 2. *Если существует A-покрытие множества E, то существует оптимальный алгоритм расшифровки U_0 с трудоемкостью $t(E, U_0)=g_2(E)$.*

Докажем три вспомогательных утверждения.

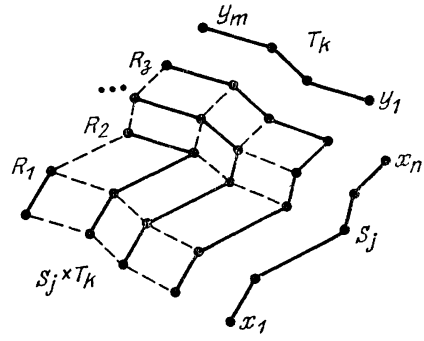


Рис. 2

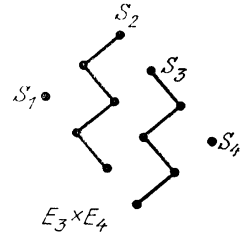


Рис. 3

Лемма 1. *Существует алгоритм расшифровки монотонных функций, заданных на множестве $R=E_p^2\times E_k\times E_{k+1}$, трудоемкость которого равна $g_2(R)$.*

Доказательство. Рассмотрим A-покрытие множества E_p^2 и покрытие множества $E_k\times E_{k+1}$, являющееся очевидной модификацией покрытия $A(E_k^2)$, пример которого для $k=3$ изображен на рис. 3. Легко видеть, что в множестве $E_k\times E_{k+1}$ два средних слоя с номерами $k-1$ и k имеют максимальную мощность. Покрытие множества $E_k\times E_{k+1}$ таково, что все цепи длины 1 лежат в этих двух слоях и для цепей покрытия выполнены условия 2.1 и 2.2 из определения 8. Построим покрытие множества R способом, указанным в замечании 1, из цепей покрытия множества $E_k\times E_{k+1}$ и цепей покрытия $A(E_p^2)$. В силу того что в множестве E_p^2 один слой максимальной мощности, в множестве R два таких слоя. Из способа построения цепей следует, что все цепи проходят через оба этих слоя либо целиком лежат в одном из них. Цепи упорядочены таким образом, что выполнены условия 2.1 и 2.2 из определения A-покрытия. Из доказательства теоремы 2 (см. [8]) следует, что этого достаточно для того, чтобы на множестве R существовал алгоритм расшифровки с трудоемкостью $g_2(R)$. Лемма доказана.

Утверждение леммы 1 можно обобщить.

Следствие 1. *Если в множестве E один средний слой максимальной мощности и существует A-покрытие $A(E)$, то существует оптимальный алгоритм расшифровки монотонных функций, заданных на множестве $E\times E_k\times E_{k+1}$, трудоемкость которого равна $g_2(E\times E_k\times E_{k+1})$.*

Лемма 2. *Пусть даны два множества D и E такие, что справедливы равенства*

$$g_2(D\cup E)=g_2(D)+g_2(E) \quad и \quad D\cap E=\varnothing.$$

Если на множестве D существует алгоритм расшифровки с трудоемкостью $g_2(D)$, после применения которого существует алгоритм расшифровки на множестве E с трудоемкостью $g_2(E)$, то на множестве $D\cup E$ также существует алгоритм расшифровки с трудоемкостью $g_2(D\cup E)$.

Доказательство. Алгоритм расшифровки на множестве $D \cup E$, полученный путем последовательного применения алгоритмов расшифровки на множествах D и E, будет, очевидно, иметь требуемую трудоемкость.

Лемма 3. *Для монотонных функций, заданных на множестве* $E_p^2 \times E_k$, $p \geqslant k$, *существует оптимальный алгоритм расшифровки с трудоемкостью* $g_2(E_p^2 \times E_k)$.

Доказательство. Заметим, что при $k \leqslant 3$ утверждение леммы следует из теорем 1, 2, так как в этом случае на каждом из множеств E_p^2 и E_k существуют A-покрытия.

Рассмотрим утверждение при $k > 3$. Обозначим через I_0 параллелепипед $E_p^2 \times E_k$, а множество всех вершин, принадлежащих его поверхности, обозначим через M_0. Пусть построены параллелепипед I_j и его поверхность M_j. Очевидно, что если выполнено неравенство $k - 2j > 3$, то множество $I_{j+1} = I_j \backslash M_j$ также является параллелепипедом. Обозначим через M_{j+1} поверхность параллелепипеда I_{j+1}. Пусть j_m — минимальный номер j такой, что $k - 2j_m \leqslant 3$. По построению, справедливо соотношение

$$I_{j_m} = E_{p-2j_m}^2 \times E_{k-2j_m}.$$

Следовательно, на множестве I_{j_m} существует алгоритм расшифровки с трудоемкостью $g_2(I_{j_m})$. Произведем расшифровку на множестве I_{j_m}, используя этот алгоритм.

Пусть расшифровка произведена на I_{j+1}. Покажем, что на множестве M_j существует алгоритм расшифровки с трудоемкостью $g_2(M_j)$. Обозначим $a = p - 2j$ и $b = k - 2j$. Рассмотрим развертку поверхности M_j как часть множества $E_{2a+2b-3} \times \times E_{2a+b-2}$ (см. рис. 4). На множестве $E_{2a+2b-3} \times E_{2a+b-2}$ существует покрытие, являющееся очевидным обобщением покрытия множества E_{2a+b-2}^2. Заметим, что ребра $A'B'$, $B'B$, $B'C'$, AD, CD, DD' параллелепипеда I_j входят в развертку дважды. Рассмотрим участки цепей покрытия множества $E_{2a+2b-3} \times \times E_{2a+b-2}$, выделенные на рис. 4 сплошными линиями. Эти участки принадлежат развертке поверхности M_j и покрывают ровно одно из каждой пары указанных ребер. В силу того что на двух экземплярах ребра $A'A$, входящих в развертку, покрытие одинаково, получим некоторое покрытие поверхности M_j. Обозначим его через $H(M_j)$. Легко видеть, что если на какой-либо цепи покрытия $H(M_j)$ значения f определены, то на каждой из остальных цепей значения f определяются по очереди не более чем за два вопроса. Покажем, что после расшифровки функции на множестве I_{j+1} в покрытии $H(M_j)$ найдется цепь, на которой значения f не определяются по монотонности не более чем в трех вершинах. Рассмотрим цепи покрытия $H(M_j)$, проходящие через ребро CC'. По предположению индукции, значения f определены во всех вершинах соответствующего ребра C_1C_1' параллелепипеда I_{j+1}. Если $f = 1$ во всех этих вершинах, то на цепи по-

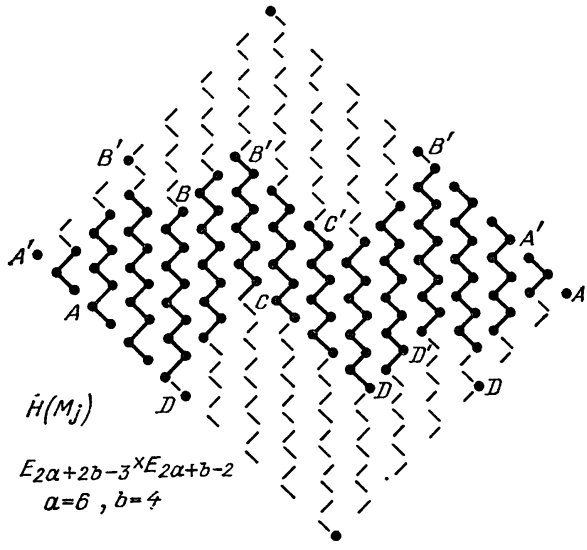


Рис. 4

крытия $H(M_j)$, проходящей через нижнюю вершину ребра CC', значения f определяются по монотонности во всех вершинах кроме трех нижних. Если $f=0$ во всех вершинах ребра C_1C_1', то на цепи покрытия $H(M_j)$, проходящей через верхнюю вершину ребра CC', значения f определяются по монотонности во всех вершинах кроме трех верхних. Если на ребре C_1C_1' найдутся точки $\tilde{x}$ и $\tilde{y}$ такие, что $f(\tilde{x})=0$, а $f(\tilde{y})=1$, тогда можно считать, что эти точки соседние, т. е.

$$\tilde{y}=\tilde{x}+\tilde{e}.$$

Очевидно, что в вершинах $\tilde{x}'$ и $\tilde{y}'$, лежащих на поверхности M_j, значения f определяются по монотонности (рис. 5). Из построения покрытия $H(M_j)$ следует, что на цепи, проходящей через вершину $\tilde{x}'$, не более трех вершин, в которых значения f не определяются по монотонности (рис. 6).

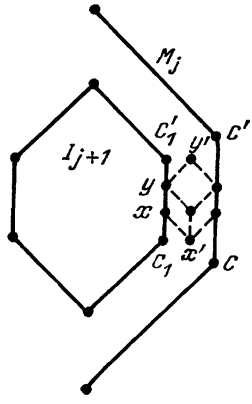
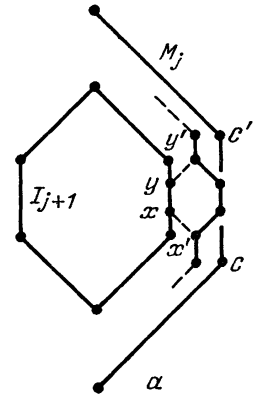


Рис. 5



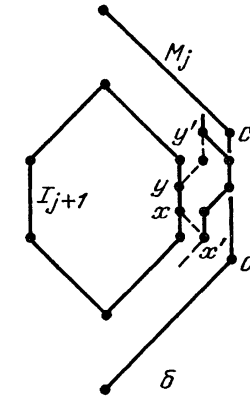


Рис. 6

Заметим, что все цепи покрытия $H(M_j)$ проходят через $k-2j$ средних слоев множества M_j. Поэтому трудоемкость алгоритма расшифровки на M_j равна $g_2(M_j)$. Легко видеть, что множества I_{j+1} и M_j удовлетворяют условиям леммы 2. Применяя лемму 2, получим, что трудоемкость алгоритма расшифровки на множестве $I_j=I_{j+1}\cup M_j$ равна $g_2(I_j)$. Лемма доказана.

Теорема 3. *Если на множестве E задано A-покрытие, то для монотонных функций, определенных на множестве Q вида:*

$$Q=E_p^2\times E_k\times E,\quad p\geqslant k,$$

существует алгоритм расшифровки с трудоемкостью $g_2(Q)$.

Доказательство. Заметим, что при $k\leqslant 3$ утверждение следует из теорем 1, 2. Пусть $k>3$. По условию, на множестве E задано покрытие $A(E)$, цепи $C_1, \ldots, C_m$ которого упорядочены. Рассмотрим множества вида

$$Q_i=E_p^2\times E_k\times C_i$$

при $i=1, \ldots, m$. Упорядочим эти множества по возрастанию i. Алгоритм расшифровки f на Q состоит в последовательном определении значений f на каждом из множеств Q_i в соответствии с указанным порядком. В силу леммы 2, для доказательства теоремы достаточно показать, что при указанном порядке расшифровки на каждом из множеств Q_i существует алгоритм расшифровки с трудоемкостью $g_2(Q_i)$. Обозначим длину цепи C_i через r и рассмотрим 5 случаев.

1. При $r=1$ существование алгоритма расшифровки с трудоемкостью $g_2(Q_i)$ следует из леммы 3.

2. Пусть число r удовлетворяет неравенству $1<r<k$. Множество $E_p^2\times E_k$ представим в виде

$$E_p^2\times E_k = I_t \cup M_{t-1} \cup \ldots \cup M_0,$$

где $t=[(k-r+1)/2]$ и множества I_t, M_j построены так же, как в доказательстве леммы 3. В силу равенства

$$(A\cup B)\times C=(A\times C)\cup(B\times C)$$

имеем $Q_i=(I_t\times C_i)\cup(M_{t-1}\times C_i)\cup\ldots\cup(M_0\times C_i)$. Для множества $I_t\times C_i$ по построению выполнено равенство

$$I_t\times C_i=\begin{cases} E^2_{p-k+r}\times E_r\times C_i, & k-r=2v,\\ E^2_{p-k+r-1}\times E_{r-1}\times C_i, & k-r=2v+1.\end{cases}$$

Так как $|C_i|=r$, то на множестве $E_r\times C_i$ существует A-покрытие. По теореме 1, оно вместе с покрытием $A(E^2_{p-k+r})$ порождает A-покрытие множества $I_t\times C_i$ при $k-r=2v$. При $k-r=2v+1$ существование оптимального алгоритма расшифровки с требуемой трудоемкостью для множества $E^2_{p-k+r-1}\times E_{r-1}\times C_i$ следует из леммы 1.

Множества $M_j\times C_i$ при $j=0,\ \ldots,\ t-1$ упорядочим по убыванию j. Для каждого множества $M_j\times C_i$ справедливо равенство

$$M_j\times C_i=\bigcup_{l=1}^{r} M_j\times\tilde{x}_l,\quad \text{где}\quad C_i=(\tilde{x}_1,\ \ldots,\ \tilde{x}_r).$$

На каждом из множеств $M_j\times\tilde{x}_l$ при $l=1,\ \ldots,\ r$ алгоритм расшифровки с трудоемкостью $g_2(M_j)$ строится подобно алгоритму леммы 3 в предположении, что на множестве $I_{j+1}\times\tilde{x}_l$ расшифровка уже произведена. Легко проверить, что все цепи, построенные на множествах $M_j\times\tilde{x}_l$ при $l=1,\ \ldots,\ r$, проходят через два средних слоя множества $M_j\times C_i$. Поэтому трудоемкость алгоритма расшифровки на множестве $M_j\times C_i$ равна $g_2(M_j\times C_i)$. Множество $I_t\times C_i$ и множества $M_j\times C_i$ при $j=0,\ \ldots,\ t-1$ удовлетворяют условиям леммы 2. Поэтому на множестве Q_i построен алгоритм расшифровки с трудоемкостью $g_2(Q_i)$.

3. При $r=k$ на множестве Q_i можно построить A-покрытие, аналогичное покрытию множества E_k^2 (рис. 1). По теоремам 1, 2 получим, что на множестве Q_i существует алгоритм расшифровки с трудоемкостью $g_2(Q_i)$.

4. При $r=k+1$ на множестве Q_i существует покрытие, аналогичное покрытию множества $E_p^2\times E_k\times E_{k+1}$, построенному в лемме 1. Поэтому на множестве Q_i существует алгоритм расшифровки с требуемой трудоемкостью.

5. Пусть $r>k+1$. Из определения A-покрытия следует, что длина цепи C_1 покрытия $A(E)$ удовлетворяет неравенству $|C_1|\leqslant 3$. Поэтому доказательство существования алгоритма расшифровки на Q_1 с трудоемкостью $g_2(Q_1)$ дано в п. 1 и 2. Предположим, что построен алгоритм расшифровки на множестве $\bigcup_{l=1}^{i-1} Q_l$, трудоемкость которого равна $g_2\left(\bigcup_{l=1}^{i-1} Q_l\right)$. Зададим на множестве E_p^2 A-покрытие $\{S_j\}$, $j=1,\ \ldots,\ p$ (рис. 1). Множество Q_i представим в виде

$$Q_i=E_p^2\times E_k\times C_i=\left(\bigcup_{j=1}^{p} S_j\right)\times E_k\times C_i=\bigcup_{j=1}^{p} S_j\times E_k\times C_i.$$

Обозначим через W_j множество $S_j\times E_k\times C_i$. Множества W_j упорядочим по возрастанию j. Рассмотрим множество W_1. В силу того что в покры-

тии $A(E_p^2)$ длина цепи S_1 равна 1, выполнено равенство

$$W_1 = \tilde{x}_1 \times E_k \times C_i,$$

где $\tilde{x}_1$ — единственная вершина цепи S_1. Построим покрытие множества W_1 цепями $T_1, \ldots, T_k$, пример которого приведен на рис. 7. Рассмотрим множества L_m вида $(m-1)\times C_i$ при $m = 1, \ldots, k$. В каждом из множеств L_m не более трех вершин, в которых значения f не определяются по монотонности, так как по предположению расшифровка на множестве $\bigcup_{l=1}^{i-1} Q_l$ произведена, а цепи C_i образуют A-покрытие. Следовательно, на каждом из множеств $T_m \cap L_m$ значения f не определяются по монотонности не более чем в трех вершинах. Из неравенства $r > k+1$ и способа построения цепей T_m следует, что:

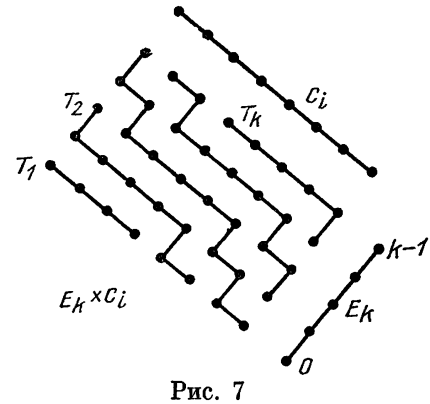


Рис. 7

1) для цепи T_1 справедливо равенство $T_1 = T_1 \cap L_1$, а значит, на цепи T_1 возможна расшифровка не более чем за два вопроса;

2) при $m > 1$ справедливо неравенство $|T_m \cap L_m| \geqslant 4$. Для построения алгоритма расшифровки на цепях T_m при $m = 2, \ldots, k$ рассмотрим три вершины $\tilde{v}_t$, $\tilde{v}_{t+1}$, $\tilde{v}_{t+2}$ множества $T_m \cap L_m$, в которых значения f не определяются по монотонности. Возможны три случая.

1. Вершина $\tilde{v}_{t+2}$ является верхней вершиной множества $T_m \cap L_m$. В этом случае на участке цепи T_m, лежащем ниже вершины $\tilde{v}_t$, значения f определяются по монотонности. Оставшийся участок цепи T_m обозначим через D_m^1.

2. Вершина $\tilde{v}_{t+2}$ не является верхней вершиной множества $T_m \cap L_m$, а вершина $\tilde{v}_t$ не является нижней вершиной этого множества. В этом случае во всех вершинах цепи T_m, за исключением трех, значения f определяются по монотонности. Поэтому значения f на всей цепи T_m могут быть определены не более чем за два вопроса.

3. Вершина $\tilde{v}_t$ является нижней вершиной множества $T_m \cap L_m$. В этом случае на участке цепи T_m, лежащем выше вершины $\tilde{v}_{t+2}$, значения f определяются по монотонности. Оставшийся участок цепи T_m обозначим через D_m^0.

Упорядочим по возрастанию номеров m нижние участки D_m^0 цепей T_m, после этого верхние участки D_m^1 упорядочим по убыванию m. Легко видеть, что из построения цепей T_m и задания порядка участков D_m^0 и D_m^1 следует, что для любых четырех последовательных вершин цепи T_m, в которых значения f не определены, хотя бы одна из сопряженных вершин лежит на участке с меньшим порядковым номером либо на участке, во всех вершинах которого значения f определены по монотонности. Таким образом, для расшифровки f на любой цепи T_m требуется не более двух вопросов. В силу симметричности цепей T_m алгоритм расшифровки на множестве W_1 имеет трудоемкость $g_2(W_1)$. Обозначим построенное покрытие через $B(W_1)$.

Предположим, что на множестве $\bigcup_{l=1}^{j-1} W_l$ построен алгоритм с трудоемкостью $g_2\left(\bigcup_{l=1}^{j-1} W_l\right)$. Чтобы воспользоваться леммой 2, покажем, что на множестве W_j можно построить алгоритм с трудоемкостью $g_2(W_j)$. На каждом из множеств $S_j \times T_m$ при $m = 1, \ldots, k$ зададим покрытие

симметричными цепями $R_1, \ldots, R_z$, используя конструкцию из доказательства теоремы 1 (рис. 2). Обозначим эти покрытия через $B(S_j \times T_m)$. Полученное покрытие множества W_j обозначим $B(W_j)$:

$$B(W_j) = \bigcup_{m=1}^{k} B(S_j \times T_m).$$

В силу симметричности цепей покрытия $B(W_j)$ достаточно показать, что порядок цепей можно задать так, чтобы на каждой из них значения f можно было определить не более чем за два вопроса.

Рассмотрим покрытие $B(S_j \times T_m)$. Если m таково, что выполнено неравенство $|S_j| > |T_m|$, то, как следует из построения, в покрытии $B(S_j \times T_m)$ найдется цепь $R_{0,m}$ вида $R_{0,m} = (\tilde{v}_1, \ldots, \tilde{v}_{t_0})$, где $t_0 = |S_j| - |T_m| + 1$, $\tilde{v}_q = (\tilde{x}_{n-t_0+q}, \tilde{y}_{1,m})$ при $q = 1, \ldots, t_0$, $\tilde{x}_n$ — верхняя вершина цепи S_j, $y_{1,m}$ — нижняя вершина цепи T_m. Множество цепей вида $R_{0,m}$ во всех покрытиях $B(S_j \times T_m)$ при $m = 1, \ldots, k$ обозначим через $V_0(W_j)$. Фиксируем h, $h \geqslant 1$. Среди цепей множества $B(W_j) \setminus V_0(W_j)$ рассмотрим цепи $R_{h,m}$ такие, что их нижние вершины имеют вид $\tilde{v}_1 = (\tilde{x}_{n-k+1}, \tilde{y}_{1,m})$, где $\tilde{x}_n$ — верхняя вершина цепи S_j, $\tilde{y}_{1,m}$ — нижняя вершина цепи T_m. Множество всех цепей $R_{h,m}$ в покрытии $B(W_j)$ обозначим $V_h(W_j)$. Легко видеть, что выполнено равенство

$$\bigcup_{h=0}^{n} V_h(W_j) = B(W_j).$$

Зададим порядок множеств цепей $V_h(W_j)$ по возрастанию h. На рис. 8 приведен пример покрытия $B(W_j)$ и множеств $V_h(W_j)$: $V_0(W_j) = \{R_{0,1}\}$, $V_1(W_j) = \{R_{1,2}, R_{1,3}\}$, $V_2(W_j) = \{R_{2,2}, R_{2,3}\}$, $V_3(W_j) = \{R_{3,1}, R_{3,2}, R_{3,3}\}$, $V_4(W_j) = \{R_{4,1}, R_{4,2}, R_{4,3}\}$, $V_5(W_j) = \{R_{5,1}, R_{5,2}, R_{5,3}\}$.

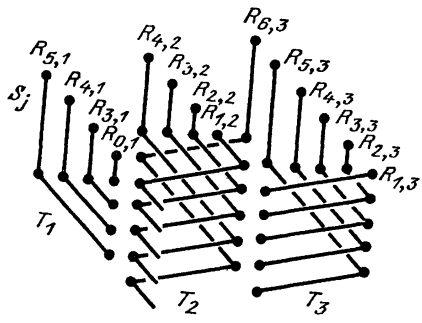


Рис. 8

Рассмотрим множество $V_0(W_j)$. Пусть $R_{0,m}$ — произвольная цепь из $V_0(W_j)$, а $\tilde{v}_q$, $\tilde{v}_{q+1}$, $\tilde{v}_{q+2}$, $\tilde{v}_{q+3}$ — любые последовательные вершины этой цепи. Из построения следует, что сопряженные вершины $\tilde{v}'_{q+1}$ и $\tilde{v}'_{q+2}$ имеют вид $\tilde{v}'_{q+1} = (\tilde{x}'_{n+q-t_0+1}, \tilde{y}_{1,m})$ и $\tilde{v}'_{q+2} = (\tilde{x}_{n+q-t_0+2}, \tilde{y}_{1,m})$, где $\tilde{x}'_{n+q-t_0+1}$ и $\tilde{x}'_{n+q-t_0+2}$ — сопряженные вершины для $\tilde{x}_{n+q-t_0}$, $\tilde{x}_{n+q-t_0+1}$, $\tilde{x}_{n+q-t_0+2}$, $\tilde{x}_{n+q-t_0+3}$. Цепи S_j образуют A-покрытие, поэтому хотя бы одна из сопряженных вершин $\tilde{x}'_{n+q-t_0+1}$ и $\tilde{x}'_{n+q-t_0+2}$ принадлежит цепи $S_{j'}$, причем $j' < j$. Следовательно, вершина $\tilde{v}'_{q+1}$ либо вершина $\tilde{v}'_{q+2}$ лежит в множестве $W_{j'}$, на котором значения f предполагаем уже определенными. Поэтому на цепи $R_{0,m}$ значения f можно определить не более чем за два вопроса.

Будем расшифровывать f по порядку на цепях множеств $V_h(W_j)$ при $h \geqslant 1$. При этом на каждом шаге алгоритма расшифровки определим значения f на всех цепях множества $V_h(W_j)$ и, возможно, на некоторых цепях множества $V_{h+1}(W_j)$. Пусть значения f определены на множестве $\bigcup_{l=0}^{h-1} V_l(W_j)$ и, возможно, на некоторых цепях множества $V_h(W_j)$. Из определения $V_h(W_j)$ следует, что это множество состоит из цепей $R_{h,m_h+1}, \ldots, R_{h,m_h+p_h}$, которые построены из цепи S_j, и цепей $T_{m_h+1}, \ldots, T_{m_h+p_h}$, где $m_h \geqslant 0$ и $m_h + p_h \leqslant k$. При $h > 1$ произвольная

цепь $R_{h,m}$ содержит вершины вида $\tilde{u}_{h,m} = (\tilde{x}_{n-h+1}, \tilde{y}_{q_m})$, $\tilde{v}_{h,m} = (\tilde{x}_{n-h+1}, \tilde{y}_{q_m+1})$, $\tilde{w}_{h,m} = (\tilde{x}_{n-h+2}, \tilde{y}_{q_m+1})$, где $\tilde{x}_{n-h+1}$, $\tilde{x}_{n-h+2} \in S_j$, $\tilde{y}_{q_m}$, $\tilde{y}_{q_m+1} \in T_m$. Вершина $\tilde{v}'_{h-1,m} = (\tilde{x}_{n-h+2}, \tilde{y}_{q_m})$ является сопряженной для вершин $\tilde{u}_{h,m}$, $\tilde{v}_{h,m}$, $\tilde{w}_{h,m}$. По построению, вершина $\tilde{v}'_{h-1,m}$ лежит на цепи $R_{h-1,m}$. По предположению, значение $f(\tilde{v}'_{h-1,m})$ уже определено. Исходя из этого зададим следующий алгоритм расшифровки на цепях множества $V_h(W_j)$.

Будем рассматривать только те цепи $R_{h,m}$, на которых расшифровка еще не производилась.

1. Рассмотрим цепи $R_{h,m}$ такие, что $f(\tilde{v}'_{h-1,m}) = 0$. На участке $D_{h,m}$ цепи $R_{h,m}$, лежащем под вершиной $\tilde{v}_{h-1,m}$, значения f определяются по монотонности (см. рис. 9). На участке $U_{h,m}$ значения f определяются не более чем за два вопроса аналогично расшифровке на цепях из множества $V_0(W_j)$.

2. Рассмотрим цепи $R_{h,m}$ такие, что $f(\tilde{v}'_{h-1,m}) = 1$ либо $h = 1$ (в этом случае вершины $\tilde{v}'_{h-1,m}$ не существует). На участке $U_{h,m}$ значения f определяются по монотонности. Покажем, что на участках $D_{h,m}$ значения f определяются не более чем за два вопроса.

Замечание 2. По построению, участок $D_{h,m}$ представляет собой цепь T_m без $n-h$ верхних вершин (см. замечание 1). Поэтому будем опираться на результаты, полученные для покрытия $B(W_1)$.

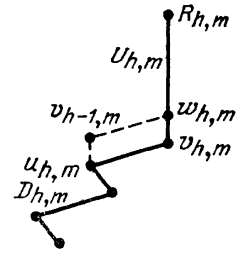


Рис. 9

Участок $D_{h,m}$ состоит, вообще говоря, из трех частей (рис. 9). Из рассмотрения множества W_1 следует, что не более чем на одном из участков $D^0_{h,m}$ и $D^1_{h,m}$ значения f не определяются по монотонности. Если такие участки найдутся, то упорядочим по возрастанию m участки $D^0_{h,m}$, а затем участки $D^1_{h,m}$ упорядочим по убыванию m. Из замечания 2 следует, что для любых четырех последовательных вершин участка $D_{h,m}$, кроме, быть может, верхних, хотя бы одна из сопряженных вершин лежит на цепи с меньшим порядковым номером либо в множестве, на котором значения f уже определены.

Рассмотрим три верхних вершины участка $D_{h,m}$. В зависимости от вида цепи T_m и значения $n-h$ эти три вершины могут принадлежать участку $D^1_{h,m}$ либо участку $D^0_{h,m}$. Заметим, что ни одна из сопряженных вершин для четырех верхних вершин участка $D_{h,m}$ не лежит на участке цепи с меньшим номером лишь в следующих двух случаях.

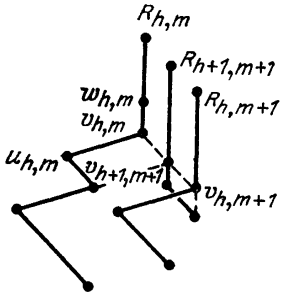


Рис. 10

1. Число $n-h$ нечетно, и четыре верхних вершины множества $D_{h,m}$ принадлежат участку $D^1_{h,m}$ (рис. 10). Из задания порядка участков цепей следует, что в вершине $\tilde{v}_{h,m+1} = (\tilde{x}_{n-h+1}, \tilde{y}_{q_m+1})$ значение уже определено. Если $f(\tilde{v}_{h,m+1}) = 1$, то в вершине $\tilde{v}_{h,m}$ значение f определяется по монотонности. Следовательно, на участке $D^1_{h,m}$ имеем не более трех вершин, в которых значения f не определены. Пусть $f(\tilde{v}_{h,m+1}) = 0$. Легко видеть, что вершина $\tilde{v}_{h,m+1}$ является сопряженной для вершин $\tilde{u}_{h+1,m+1} = (\tilde{x}_{n-h}, \tilde{y}_{q_m+1})$, $\tilde{v}_{h+1,m+1} = (\tilde{x}_{n-h}, \tilde{y}_{q_{m+1}+1})$, $\tilde{w}_{h+1,m+1} = (\tilde{x}_{n-h+1}, \tilde{y}_{q_{m+1}+1})$. В этом случае сначала определим значения f на цепи $R_{h+1,m+1}$. Это можно сделать не более чем за два вопроса подобно расшифровке на цепях множества $V_0(W_j)$. После этого в вершине $\tilde{w}_{h+1,m+1}$ значение f будет опре-

делено. В результате на участке $D^1_{h,m}$ останется не более трех вершин, в которых значения f не определяются по монотонности. Следовательно, значения f на всей цепи $R_{h,m}$ в этом случае можно определить не более чем за два вопроса.

2. Число вершин в $D_{h,m}$ четно и четыре верхних вершины этого множества принадлежат участку $D^0_{h,m}$ (рис. 11). Если $m = m_h + 1$, то, по построению цепи $R_{h,m}$, вершина, сопряженная для трех верхних вершин участка $D^0_{h,m}$, принадлежит цепи $R_{0,m-1}$. Если $m > m_h + 1$, то рассмотрим вершину $\tilde{v}_{h,m-1} = (\tilde{x}_{n-h+1}, \tilde{y}_{q_{m-1}})$. Из задания порядка участков цепей следует, что в вершине $\tilde{v}_{h,m-1}$ значение f уже определено. Если $f(\tilde{v}_{h,m-1}) = 1$, то в вершине $\tilde{v}_{h,m}$ значение f определяется по монотонности.

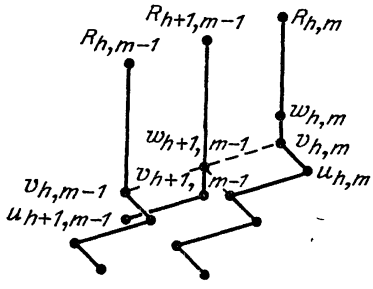


Рис. 11

Пусть $f(\tilde{v}_{h,m-1}) = 0$. Заметим, что вершина $\tilde{v}_{h,m-1}$ является сопряженной для вершин $\tilde{u}_{h+1,m-1} = (\tilde{x}_{n-h}, \tilde{y}_{q_{m-1}})$, $v_{h+1,m-1} = (\tilde{x}_{n-h}, \tilde{y}_{q_{m-1}+1})$, $\tilde{w}_{h+1,m-1} = (\tilde{x}_{n-h+1}, \tilde{y}_{q_{m-1}+1})$. Поэтому на цепи $R_{h+1,m-1}$ значения f можно определить не более чем за два вопроса подобно расшифровке f на цепях множества $V_0(W_j)$. Таким образом, в вершине $\tilde{w}_{h+1,m-1}$ значение f будет определено. После этого на участке $D^1_{h,m}$ останется не более трех вершин, в которых значения f не определяются по монотонности. Следовательно, и в этом случае на цепи $R_{h,m}$ возможна расшифровка не более чем за два вопроса. Итак, при указанном порядке просмотра цепей для определения значений f на каждой из цепей покрытия $B(W_j)$ использовалось не более двух вопросов. Так как все цепи покрытия $B(W_j)$ симметричны, построенный алгоритм расшифровки на W_j имеет трудоемкость $g_2(W_j)$.

По лемме 2 алгоритм расшифровки на множестве $\bigcup_{l=1}^{j} W_l$ имеет трудоемкость $g_2\left(\bigcup_{l=1}^{j} W_l\right)$. Индукцией по j получаем для алгоритма расшифровки на множестве Q_i трудоемкость $g_2(Q_i)$. Индукция по i завершает доказательство.

Следствие 2. Для монотонных функций, заданных на множестве E^n_p, существует оптимальный алгоритм расшифровки с трудоемкостью $g_2(E^n_p)$.

Построенный алгоритм можно использовать и для расшифровки k-значных монотонных функций. Расшифровка k-значной монотонной функции сводится к $(k-1)$-кратной расшифровке двузначной функции (подробнее об этом см. [8]). Через $t_k(E, U_0)$ обозначим трудоемкость оптимального алгоритма расшифровки k-значной монотонной функции, заданной на множестве E. Из теоремы 3 следует верхняя оценка величины $t_k(E^n_p, U_0)$.

Следствие 3. Справедливо неравенство

$$t_k(E^n_p, U_0) \leqslant (k-1)\, g_2(E^n_p).$$

Следствие 4. При $n \to \infty$ и $k = o(\sqrt{n})$ имеем

$$t_k(E^n_p, U_0) \sim g_{2(k-1)}(E^n_p),$$

где через $g_{2(k-1)}(E^n_p)$ обозначена максимальная мощность $2(k-1)$ соседних слоев множества E^n_p.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев В. Б. О расшифровке некоторых классов монотонных многозначных функций // ЖВМ и МФ.— 1976.— 16, № 1.— С. 189—198.
2. Гайанов Д. Н. Об одном критерии оптимальности алгоритма расшифровки монотонных булевых функций // ЖВМ и МФ.— 1984.— 24, № 8.— С. 1250—1257.
3. Журавлев Ю. И. Об алгоритмах выделения совокупностей существенных переменных не всюду определенных функций алгебры логики // Проблемы кибернетики. Вып. 11.— М.: Наука, 1964.— С. 271—275.
4. Коробков В. К. О монотонных функциях алгебры логики // Проблемы кибернетики. Вып. 13.— М.: Наука, 1965.— С. 5—28.
5. Коробков В. К. Некоторые обобщения задачи «расшифровки» монотонных функций алгебры логики // Дискретный анализ. Вып. 5.— Новосибирск: Ин-т мат. СО АН СССР, 1965.— С. 19—25.
6. Коротких В. В. О связи задач оптимального восстановления одного функционального класса с расшифровкой монотонных функций конечнозначной логики // Методы исследования сложных систем: Труды Конференции молодых ученых ВНИСИ.— М.: ВНИСИ, 1983.— С. 18—24.
7. Марков Ал. А. Введение в теорию кодирования.— М.: Наука, 1982.— С. 91.
8. Сержантов А. В. Оптимальный алгоритм расшифровки некоторых классов монотонных функций // ЖВМ и МФ.— 1983.— 23, № 1.— С. 206—212.
9. Hansel G. Sur le nombre des fonctions booleennes monotones de n variables // C. R. Acad. Sci. Paris.— 1966.— V. 262.— P. 1088—1090. (Рус. пер.: Ансель Ж. О числе монотонных булевых функций переменных // Кибернетический сборник. Новая серия. Вып. 5.— М.: Мир, 1968.— С. 53—57.)