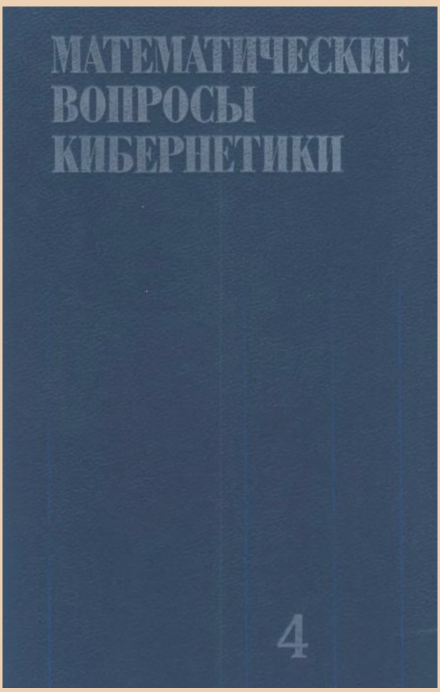


Е. Г. Воробьева

Монотонные преобразования в задачах дискретной оптимизации и минимизация стоимости кодирования в классе самосинхронизирую-щихся кодов

Рекомендуемая форма библиографической ссылки: Воробьева Е. Г. Монотонные преобразования в задачах дискретной оптимизации и минимизация стоимости кодирования в классе самосинхронизирующихся кодов // Математические вопросы кибернетики. Вып. 4. — М.: Наука, 1992. — С. 73–93. URL: http://library.keldysh.ru/mvk.asp?id=1992-73

МОНОТОННЫЕ ПРЕОБРАЗОВАНИЯ В ЗАДАЧАХ ДИСКРЕТНОЙ ОПТИМИЗАЦИИ И МИНИМИЗАЦИЯ СТОИМОСТИ КОДИРОВАНИЯ В КЛАССЕ САМОСИНХРОНИЗИРУЮЩИХСЯ КОДОВ

Е. Г. ВОРОБЬЕВА

(НИЖНИЙ НОВГОРОД)

Введение

1. Рассмотрим следующую задачу дискретной оптимизации. Пусть N — множество неотрицательных целых чисел; пусть на N^m задана линейная форма $c(\mathbf{z})$, $\mathbf{z}=(z_1, \ldots, z_m)$, $c(\mathbf{z}) = \sum_{i=1}^{m} c_i z_i$; задана конечная область оптимизации X, $X \subseteq N^m$. Найти элемент множества X, на котором значение линейной формы минимально. Очевидно, сложность решения этой задачи зависит от области оптимизации X. Для одних X известны или могут быть легко сформулированы эффективные алгоритмы оптимизации, для других задача является универсальной переборной. В качестве примера приведем проблему оптимального алфавитного q-ичного кодирования произвольного языка $\mathscr{L}$ в алфавите B. В [2] показано, что эта проблема сводится к минимизации линейной формы (стоимости кодирования) на конечном множестве целочисленных векторов (спектров), называемом *матрицей оптимального кодирования языка* $\mathscr{L}$. Оптимизация алфавитного q-ичного кодирования многих языков $\mathscr{L}$ — универсальная переборная проблема. Если же $\mathscr{L} = B^*$, то существует эффективный алгоритм оптимального кодирования — алгоритм Хаффмана.

Один из возможных подходов к решению сформулированной задачи — построить конечное расширение Y области оптимизации ($X \subseteq Y \subseteq N^m$) и исследовать некоторую вспомогательную задачу на множестве Y. На этом основан метод построения последовательности планов для решения задач дискретной оптимизации, предложенный в [1]. Чтобы применить этот метод, необходимо построить такое расширение Y области оптимизации и такую миноранту $Q(\mathbf{y})$ (функцию, определенную на Y, удовлетворяющую условию $Q(\mathbf{x}) \leqslant c(\mathbf{x})$ для любого $\mathbf{x} \in X$), для которых существовал бы эффективный алгоритм линейного упорядочивания элементов Y по неубыванию миноранты $Q(\mathbf{y})$. Если удалось выполнить эти требования, то минимизация целевой функции на X осуществляется итеративным процессом, который на первом шаге строит элемент $\mathbf{y}^1$, $Q(\mathbf{y}^1) = \min_{\mathbf{y}\in Y} Q(\mathbf{y})$, на k-м шаге ($k > 1$) строит элемент $\mathbf{y}^k$, $Q(\mathbf{y}^k) = \min_{\mathbf{y}\in Y \setminus \{\mathbf{y}^1,\ldots,\mathbf{y}^{k-1}\}} Q(\mathbf{y})$, и производит проверку выполнения критерия оптимальности $Q(\mathbf{y}^k) \geqslant \min_{\mathbf{x}\in X\cap\{\mathbf{y}^1,\ldots,\mathbf{y}^k\}} c(\mathbf{x}) = c(\mathbf{x}^k)$. Если критерий оптимальности выполняется, то $\mathbf{x}^k$ — оптимальный элемент множества X.

Метод, изложенный в [1], оказался достаточно эффективным для решения многих задач дискретной оптимизации. Однако построение миноранты — нетривиальная проблема.

В данной работе предлагается метод, основанный только на расширении области оптимизации. Для его реализации требуется такое расширение Y, для которого существует эффективный алгоритм частичного упорядочивания элементов Y по неубыванию целевой функции $c(\mathbf{y})$.

Пусть $X \subseteq Y \subseteq N^m$ и $\mathcal{F} = \{\varphi_1, \ldots, \varphi_n\}$ — система преобразований, каждое из которых определено на Y. Будем говорить, что система $\mathcal{F}$ *монотонно полна* (*м-полна*) *относительно* Y, если она обладает следующими свойствами:

1) если $\mathbf{y} \in Y$, то $\varphi_i(\mathbf{y}) \in Y$ для $i = 1, \ldots, n$;

2) если $\mathbf{y} \in Y$, то $c(\varphi_i(\mathbf{y})) \leqslant c(\mathbf{y})$ для $i = 1, \ldots, n$;

3) оптимальный элемент $\mathbf{y}^0$ множества Y $\left(c(\mathbf{y}^0) = \min\limits_{\mathbf{y} \in Y} c(\mathbf{y})\right)$ может быть получен из любого вектора $\mathbf{y} \in Y$ суперпозициями преобразований системы $\mathcal{F}$: $\varphi_{i_s} \ldots \varphi_{i_1}(\mathbf{y}) = \mathbf{y}^0$;

4) для любого $\mathbf{y} \in Y$ существует алгоритм построения множества $\varphi_i^{-1}(\mathbf{y})$, $i = 1, \ldots, n$.

На основе м-полной системы преобразований $\mathcal{F}$ сформулируем алгоритм монотонного поиска.

Шаг 0. Построить оптимальный элемент $\mathbf{y}^0$ множества Y. Если $\mathbf{y}^0 \in X$, то конец. Если $\mathbf{y}^0 \in Y \backslash X$, то переход на шаг 1.

Шаг 1. В качестве начального приближения $\mathbf{x}1$ взять произвольный элемент множества X. Построить множество $\bigcup\limits_{i=1}^{n} \varphi_i^{-1}(\mathbf{y}^0)$; никакой элемент этого множества не просмотрен. Переход на шаг 2.

Шаг 2. Пусть вектор $\mathbf{y}$ не просмотрен.

Если $c(\mathbf{y}) \geqslant c(\mathbf{x}1)$, то $\mathbf{y}$ просмотрен.

Если $c(\mathbf{y}) < c(\mathbf{x}1)$ и $\mathbf{y} \in X$, то перезапоминание: $\mathbf{x}1 := \mathbf{y}$, вектор $\mathbf{y}$ просмотрен.

Если $c(\mathbf{y}) < c(\mathbf{x}1)$ и $\mathbf{y} \in Y \backslash X$, то $\mathbf{y}$ — подозрительный вектор, $\mathbf{y}$ просмотрен.

Шаг повторяется до тех пор, пока не будут исчерпаны все непросмотренные элементы. Переход на шаг 3.

Шаг 3. Если нет подозрительных, то конец, вектор $\mathbf{x}1$ — результат работы алгоритма.

Пусть $\mathbf{y}$ — подозрительный вектор. Построить множество $\bigcup\limits_{i=1}^{n} \varphi_i^{-1}(\mathbf{y})$: каждый элемент этого множества не просмотрен.

Шаг выполняется до тех пор, пока не будут исчерпаны все подозрительные векторы. Переход на шаг 2.

Теорема 1. *Пусть $c(\mathbf{z})$ — линейная форма на N^m, $X \subseteq Y \subseteq N^m$ и $\mathcal{F} = \{\varphi_1, \ldots, \varphi_n\}$ — м-полная относительно Y система преобразований. Тогда вектор, полученный в результате выполнения алгоритма монотонного поиска, минимизирует линейную форму $c(\mathbf{z})$ на X.*

Доказательство. Утверждение очевидно, если $\mathbf{y}^0 \in X$ (работа алгоритма заканчивается на нулевом шаге). Пусть $\mathbf{y}^0 \in Y \backslash X$. Из м-полноты системы преобразований $\mathcal{F}$ следует, что любой элемент множества Y можно получить, выполнив в $\mathbf{y}^0$ конечное число преобразований, обратных преобразованиям системы $\mathcal{F}$. При этом каждое обратное преобразование не уменьшает значения линейной формы. Работа алгоритма монотонного поиска заключается в последовательном выполнении обратных преобразований, начиная с элемента $\mathbf{y}^0$. При этом из полученных векторов, принадлежащих X, запоминается тот ($\mathbf{x}1$), на котором значение линейной формы минимально. Если в ходе выполнения алгоритма получен вектор $\mathbf{y}$, то обратные преобразования проводятся в нем только тогда, когда $c(\mathbf{y})<c(\mathbf{x}1)$ и $\mathbf{y}\in Y\backslash X$ ($\mathbf{y}$ — подозрительный вектор). Работа алгоритма заканчивается, когда нет подозрительных векторов. Это означает, что на любом из оставшихся элементов множества Y значений линейной формы не меньше $c(\mathbf{x}1)$. Отсюда следует, что $\mathbf{x}1$ оптимален на X.

Замечание. Пусть в ходе выполнения алгоритма монотонного поиска получен вектор $\mathbf{y}^1\in X$. Очевидно, что любой вектор $\mathbf{y}^2$, для которого $c(\mathbf{y}^2)\geqslant c(\mathbf{y}^1)$, строить не следует ($\mathbf{y}^2$ и векторы, получающиеся из него обратными преобразованиями, не могут быть оптимальными). Будем говорить, что вектор $\mathbf{y}^2$ мажорируется вектором $\mathbf{y}^1$ (преобразование, приводящее к $\mathbf{y}^2$, мажорируется). Количество векторов, которые будут построены в ходе выполнения алгоритма монотонного поиска, можно сократить, если удастся заранее выделить классы мажорируемых элементов Y.

2. В данной статье на основе подхода, изложенного выше в п. 1, разработан алгоритм минимизации стоимости кодирования языка $\mathscr{L}=B^*$ в классе двоичных самосинхронизирующихся кодов.

Для языка $\mathscr{L}=B^*$ при $q=2$ матрица оптимального кодирования $M(B^*)$ содержит те и только те спектры $(l_1, \ldots, l_m)$, $m=|B|$, которые удовлетворяют равенству Мак-Миллана $\sum_{i=1}^{m} 2^{-l_i}=1$. В [2] показано, что $|M(B^*)|\geqslant\gamma^m$, где $\gamma>1$. Как было отмечено выше, алгоритм минимизации линейной формы на $M(B^*)$ известен (алгоритм Хаффмана).

Слово $\alpha\in A^*$ называется *синхронизатором для префиксного кода* $V\subseteq A^*$, если для любого суффикса s любого кодового слова и любого $v\in V^*$ выполняется $sv\alpha\in V^*$. Код V, имеющий синхронизатор, будем называть *самосинхронизирующимся* *), сокращенно σ-кодом.

Примеры. 1) Для кода $V=\{1, 01, 00\}$ синхронизатором является, например, любое двоичное слово, оканчивающееся символом 1. Это следует из того, что $\{0, 1\}^*1\subseteq V^*$.

2) Для неполного префиксного кода $\{01, 001, 101, 1001, 11\}$ синхронизатором является слово 01.

3) Бипрефиксные (в том числе равномерные) коды не имеют синхронизаторов.

Пусть $\mathscr{P}$ — заданное вероятностное распределение символов алфавита B. Код, стоимость которого для распределения $\mathscr{P}$ минимальна в классе σ-кодов, назовем *σ-оптимальным.*

Если $S=(l_1, \ldots, l_m)$ — спектр двоичного σ-кода, то он удовлетворяет неравенству Мак-Миллана $\sum_{i=1}^{m} 2^{-l_i}\leqslant 1$ и условию НОД $(l_1, \ldots, l_m)=1$, см. [4].

Рассмотрим сначала задачу минимизации стоимости кодирования в классе полных σ-кодов. Спектр $S=(l_1, \ldots, l_m)$ полного σ-кода удовлетворяет равенству Мак-Миллана

$$\sum_{i=1}^{m} 2^{-l_i}=1 \tag{1}$$

и условию

$$\text{НОД}(l_1, \ldots, l_m)=1. \tag{2}$$

Обратно, если вектор $S=(l_1, \ldots, l_m)$ удовлетворяет (1) и (2), то существует σ-код со спектром S (алгоритм построения одного из таких кодов

---

*) Такое название связано с тем, что если при передаче информации использовать самосинхронизирующийся код, то с вероятностью 1 будет происходить автоматическая синхронизация шифрующей и дешифрующей схем. Подробнее об этом см. [2] и [4].

сформулирован и обоснован в [6]). Таким образом, задача минимизации стоимости кодирования в классе полных σ-кодов сводится к минимизации линейной формы на множестве целочисленных векторов, удовлетворяющих условиям (1) и (2), т. е. на матрице M_σ, состоящей из тех строк $M(B^*)$, у которых НОД элементов равен 1 ($M_\sigma \subseteq M(B^*)$).

Теорема 2.

$$|M_\sigma| \geqslant \frac{1}{2}|M(B^*)| \geqslant \frac{1}{2}\gamma^m, \quad \gamma > 1.$$

Доказательство приведено в конце данного пункта.

На основе подхода, изложенного выше в п. 1, получен алгоритм минимизации линейной формы на M_σ. Алгоритм имеет полиномиальную оценку сложности вычислений — hm^4 элементарных операций (сложений и сравнений), h — константа. Показано, что если c_0 — минимальное значение стоимости на $M(B^*)$, c_σ — минимальное значение стоимости на M_σ, $p_{\text{мин}}$ — минимальная вероятность распределения $\mathscr{P}$, то

$$c_0 \leqslant c_\sigma \leqslant c_0 + p_{\text{мин}} \leqslant c_0 + 1/m. \tag{3}$$

Если $S = (l_1, \ldots, l_m)$ — спектр неполного σ-кода, то $\sum_{i=1}^m 2^{-l_i} < 1$ и НОД$(l_1, \ldots, l_m) = 1$. Известно (см. [3]), что если для спектра $S = (l_1, \ldots, l_m)$ выполняется условие $\sum_{i=1}^m 2^{-l_i} < 1$, то существует спектр $S' = (l'_1, \ldots, l'_m)$ такой, что $\sum_{i=1}^m 2^{-l'_i} = 1$, $l'_i \leqslant l_i$ для $i = 1, \ldots, m$ и хотя бы для одного $j \in \{1, \ldots, m\}$ выполняется $l'_j < l_j$. Это означает, что стоимость любого неполного σ-кода не меньше $c_0 + p_{\text{мин}}$. Поэтому код, оптимальный в классе полных σ-кодов, будет σ-оптимальным.

Оценка (3) не может быть улучшена (см. пример 1 в п. 2.3).

В п. 1 построена система преобразований, м-полная на множестве деревьев — реализаций спектров из $M(B^*)$. В п. 2 выделены классы мажорируемых обратных преобразований и сформулирован алгоритм минимизации линейной формы на M_σ с учетом мажорирования.

Доказательство теоремы 2. Матрица $M(B^*)$ вместе с любой строкой содержит любую ее перестановку. Пусть $SM(B^*)$ — сокращенная матрица оптимального кодирования [2], $SM(B^*) \subseteq M(B^*)$, из каждого класса перестановочных векторов-строк она содержит один, тот, в котором компоненты расположены в порядке неубывания слева направо. В [2] доказано, что $|SM(B^*)| \geqslant c^m$, $c > 1$. Пусть $M' = SM(B^*) \setminus M_\sigma = \left\{(l_1, \ldots, l_m) \,\middle|\, \sum_{i=1}^m 2^{-l_i} = 1,\ l_1 \leqslant \ldots \leqslant l_m,\ \text{НОД}\,(l_1, \ldots, l_m) \neq 1\right\}$. Пусть $S = (\underbrace{l_1, \ldots, l_1}_{m_1}, \ldots, \underbrace{l_{k-1}, \ldots, l_{k-1}}_{m_{k-1}}, \underbrace{l_k, \ldots, l_k}_{m_k}) \in M'$; очевидно, $m_k \geqslant 2^{l_k - l_{k-1}} \geqslant 4$. Спектру S поставим в соответствие спектр $\omega(S)$,

$$\omega(S) = (\underbrace{l_1, \ldots, l_1}_{m_1}, \ldots, \underbrace{l_{k-1}, \ldots, l_{k-1}}_{m_{k-1}}, \quad l_k - 1,$$
$$\underbrace{l_k, \ldots, l_k}_{m_k - 3}, \quad l_k + 1, \quad l_k + 1) \in SM(B^*) \setminus M'.$$

Отображение ω является взаимно однозначным. Поэтому

$$|M'| = |\omega(M')| \leqslant |SM(B^*) \cap M_\sigma|.$$

Отсюда

$$|SM(B^*) \cap M_\sigma| \geqslant \frac{1}{2} |SM(B^*)| \geqslant \frac{1}{2} c^m, \quad c > 1.$$

Теорема доказана.

1. Монотонные преобразования реализации произвольного спектра $S \in M(B^*)$ и их свойства

1.1. Предварительное обсуждение. Пусть $\mathcal{P} = (p_1, \ldots, p_m)$ — заданное вероятностное распределение, $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_m > 0$. Пусть $S = (l_1, \ldots, l_m) \in M(B^*)$. Стоимость $c(S)$ спектра S для распределения $\mathcal{P}$ есть $\sum_{i=1}^{m} p_i l_i$.

Реализацией спектра $S = (l_1, \ldots, l_m)$ из $M(B^*)$ (обозначаем $T(S)$) называется двоичное дерево, для которого $(l_1, \ldots, l_m)$ есть набор высот всех его висячих вершин, и для $i = 1, \ldots, m$ висячей вершине высоты l_i приписана вероятность p_i. На рис. 1, *а*, *б* изображены реализации спектров (1, 2, 3, 3) и (2, 3, 3, 1) соответственно.

Через T_M обозначим множество реализаций всех спектров на $M(B^*)$. В качестве области оптимизации вместо матрицы $M(B^*)$ будем рассматривать множество T_M. Если T есть реализация S, будем писать $S = S(T)$. Величину $\sum_{i=1}^{m} p_i l_i$ будем называть также *стоимостью дерева* $T(S)$ и обозначать $c(T)$.

Деревья T_1 и T_2 назовем *эквивалентными*, если $S(T_1) = S(T_2)$ (обозначаем $T_1 \sim T_2$).

Пусть $T \in T_M$. Через $T(v)$ будем обозначать корневое поддерево, включающее вершину v и все ее последователи в дереве T. Высоту v обозначаем $l(v)$.

Вероятность невисячей вершины v дерева T есть сумма вероятностей всех висячих вершин поддерева $T(v)$ (обозначаем $p(v)$).

Пусть v_1 и v_2 — две произвольные вершины T, поддеревья $T(v_1)$ и $T(v_2)$ не имеют общих вершин. В дереве T переставим поддеревья $T(v_1)$ и $T(v_2)$ (пример такой перестановки изображен на рис. 2). Полученное дерево обозначим $T(v_1, v_2)$. Ясно, что $T(v_1, v_2) \in T_M$.

Если $l(v_1) = l(v_2)$, то перестановку $T(v_1)$ и $T(v_2)$ назовем *эквивалентным преобразованием дерева* T. Если $l(v_1) = l(v_2)$, то $T(v_1, v_2) \sim T$. Справедливо и обратное: если $T_1 \sim T_2$, то T_2 можно получить из T_1 эквивалентными преобразованиями.

Лемма 1 ([5]).

$$c(T(v_1, v_2)) - c(T) = (p(v_1) - p(v_2))(l(v_2) - l(v_1)).$$

Будем говорить, что *дерево T приведено относительно множества Q вершин высоты l*, если $|Q| = 2^i$ при некотором целом i и все вершины множества Q являются последователями одной вершины высоты $l - i$ (эту вершину будем обозначать $v(Q)$).

Лемма 2. *В дереве T пусть Q — множество вершин высоты l, $|Q| = 2^i$. Тогда существует дерево T' такое, что $T' \sim T$ и T' приведено относительно Q.*

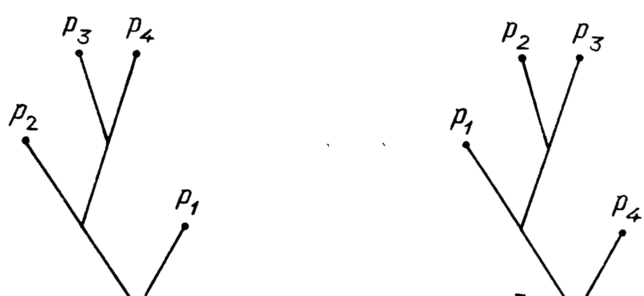


Рис. 1

Пусть $S_0=(\underbrace{l_1, \ldots, l_1}_{m_1}, \ldots, \underbrace{l_k, \ldots, l_k}_{m_k})$ — спектр Хаффмана для распределения $\mathscr{P}$, $l_1<\ldots<l_k$, $\sum_{i=1}^{k} m_i=m$, $m_i>0$. Разобьем $\mathscr{P}=(p_1, \ldots, p_m)$ на k блоков следующим образом: в 1-й блок включим первые m_1 вероятностей, во 2-й — следующие m_2 и т. д., в k-й — последние m_k вероятностей. Пусть $T_0=T(S_0)$. Ярус высоты l_i дерева T_0 назовем *i-м уровнем* этого *дерева*, $i=1, \ldots, k$. Ясно, что висячим вершинам

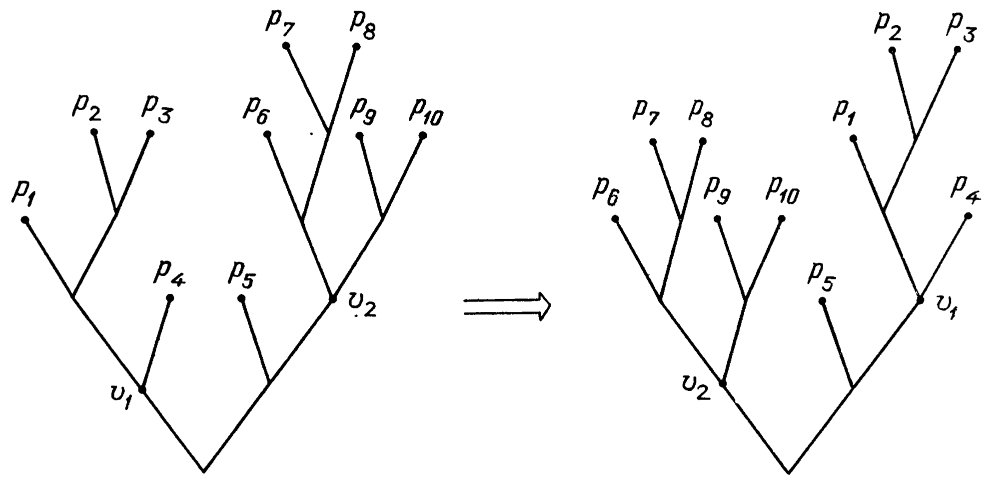


Рис. 2

i-го уровня дерева T_0 (их m_i штук) приписаны вероятности i-го блока, $i=1, \ldots, k$.

Количество всех вершин в i-м уровне T_0 обозначим n_i, $i=1, \ldots, k$; количество невисячих вершин в i-м уровне T_0 есть $n_{i+1}/2^{l_{i+1}-l_i}$, $i=1, \ldots, k-1$.

Свойство 1. *В дереве T_0 пусть z_1, z_2 и z_3 вершины i-го уровня, $1\leqslant i\leqslant k$. Тогда $p(z_1)+p(z_2)\geqslant p(z_3)$.*

Доказательство. Пусть $T_0'\sim T_0$, T_0' приведено относительно множества $Q=\{z_1, z_2\}$. По лемме 1 $c\left(T_0'(v(Q), z_3)\right)=c\left(T_0'\right)+p(v(Q))-p(z_3)$, отсюда $p(v(Q))-p(z_3)=p(z_1)+p(z_2)-p(z_3)\geqslant 0$.

Свойство 2. *В дереве T_0 пусть u — висячая вершина i-го уровня, Q — множество вершин высоты l_{i+1}, $|Q|=2^{l_{i+1}-l_i-1}$. Тогда $\sum_{v\in Q} p(v)\leqslant p(u)$.*

Доказательство. Пусть $T_0'\sim T_0$ и T_0' приведено относительно Q. По лемме 1 $c\left(T_0'(v(Q), u)\right)=c\left(T_0'\right)+p(u)-p(v(Q))$, отсюда $p(u)-p(v(Q))=p(u)-\sum_{v\in Q} p(v)\geqslant 0$.

1.2. M-полная система преобразований на множестве T_M. В данном пункте построена система преобразований, M-полная на T_M относительно линейной формы $\sum_{i=1}^{m} p_i l_i$. Система состоит из локальных преобразований двух типов. Каждое преобразование заключается в перестановке поддеревьев. Точное определение этих преобразований дано ниже непосредственно при описании процесса перехода от дерева $T\in T_M$ к дереву T_0.

Пусть $S=(l_1, \ldots, l_m)$ принадлежит $SM(B^*)$ (в дереве $T(S)$ висячим вершинам большей высоты приписаны меньшие вероятности *)). Преобразование $T(S)$ к T_0 осуществляется за k шагов. Для 1-го шага исход-

*) Заметим, что в ходе преобразований это условие может быть нарушено.

ным является дерево $T_k = T(S)$. Для $(k+1-i)$-го шага, $i = k-1, \ldots, 1$, исходным является дерево T_i, полученное в результате выполнения предыдущего шага. $(k+1-i)$-й шаг, $i = k, \ldots, 1$, заключается в последовательном выполнении нескольких преобразований в дереве T_i; каждое преобразование не увеличивает стоимости дерева. Дерево, полученное в результате выполнения k-го шага, есть реализация S_0. Для $i = k, \ldots, 1$ в дереве T_i выделены некоторые множества вершин $Q_k, \ldots, Q_i$. На первом шаге Q_k есть множество всех вершин дерева $T_k = T(S)$, которым приписаны вероятности k-го блока. Для $j = k, \ldots, i$ количество висячих вершин множества Q_j равно m_j; количество невисячих вершин множества Q_j равно $\frac{n_{j+1}}{2^{l_{j+1}-l_j}}$, $j = k-1, \ldots, i$. Для $j = k, \ldots, i$ набор $\{p(v) \mid v \in Q_j\}$ совпадает с набором вероятностей вершин j-го уровня некоторой реализации спектра S_0. Поэтому для множества вершин Q_j выполняются свойства 1 и 2. Переменное дерево, в котором проводятся преобразования в ходе выполнения $(k+1-i)$-го шага, далее обозначаем также T_i.

$(k+1-i)$-й шаг преобразований $(i = k, \ldots, 1)$.

В дереве T_i пусть d_i — разность высот самой высокой и самой низкой вершин множества Q_i. Рассмотрим отдельно два случая: $d_i \geqslant 2$ и $d_i \leqslant 1$.

1. $d_i \geqslant 2$. Пусть v_1 — прямой предшественник двух самых высоких вершин множества Q_i, v_2 — самая низкая вершина Q_i. Перестановку $T_i(v_1)$ и $T_i(v_2)$ назовем *A-преобразованием*. Если надо подчеркнуть, что преобразование проводится в множестве Q_i, будем обозначать его A_i. По лемме 1

$$c(T_i(v_1, v_2)) - c(T_i) = (p(v_1) - p(v_2))\,(l(v_2) - l(v_1)) \leqslant 0,$$

так как $l(v_1) - l(v_2) = d_i - 1 > 0$, а $p(v_1) \geqslant p(v_2)$ по свойству 1. В результате A_i-преобразования количество вершин множества Q_i высоты $l(v_1)+1$ уменьшится на 2, количество вершин множества Q_i высоты $l(v_2)$ уменьшится на 1, d_i не увеличится. Поэтому, проведя A_i-преобразование конечное число раз, получим дерево, для которого выполнено условие $d_i \leqslant 1$.

2. $d_i \leqslant 1$. В этом случае в дереве T_i вершины множества Q_i располагаются либо на одном ярусе (высоту его обозначим l'_i), либо на двух ярусах, разность высот которых равна 1 (высоты l'_i и $l'_i + 1$). Дальнейшие рассуждения различны для $i > 1$ и $i = 1$. Путь $i > 1$. Пусть l''_i — высота самой высокой вершины, которой приписана вероятность $(i-1)$-го блока, $l''_i \leqslant l'_i$. Пусть $r_i = l'_i - l''_i$.

Лемма 3. а) *Если $r_i \leqslant l_i - l_{i-1} - 2$, то количество вершин множества Q_i высоты l'_i кратно 2^{r_i+1}.*

б) *Если $r_i \geqslant l_i - l_{i-1} - 1$, то количество вершин множества Q_i высоты l'_i кратно $2^{l_i - l_{i-1}}$; количество вершин множества Q_i высоты $l'_i + 1$ кратно $2^{l_i - l_{i-1}}$.*

Доказательство приведено в конце данного пункта.

Пусть имеет место а). Пусть $Q \subseteq Q_i$, $|Q| = 2^{r_i+1}$, и все вершины множества Q имеют высоту l'_i. Пусть $T'_i \sim T_i$ и T'_i приведено относительно Q, см. рис. 3. Назовем *B-преобразованием* (B_{i-1}*-преобразованием*) всякую перестановку поддеревьев $T'_i(v(Q))$ и $T'_i(u)$, где u — висячая вершина высоты l''_i. По лемме 1

$$c\left(T'_i(v(Q), u)\right) - c\left(T'_i\right) = p(v(Q)) - p(u);$$

по свойству 2 эта величина не превосходит 0.

В результате B_{i-1}-преобразования количество вершин множества Q_i высоты l_i' уменьшится на 2^{r_i+1}, количество висячих вершин высоты l'' которым приписаны вероятности $(i-1)$-го блока, уменьшится на 1, r_i не уменьшится. Условие 2) не нарушится. Поэтому проведя B_{i-1}-преобразование конечное число раз, получим дерево, в котором $d_i \leqslant 1$ и $r_i \geqslant l_i - l_{i-1} - 1$.

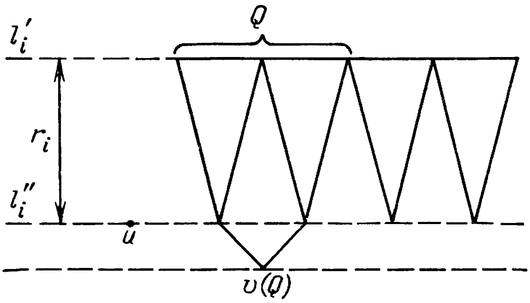


Рис. 3

Пусть имеет место б). Пусть $t = |Q_i|/2^{l_i - l_{i-1}} = n_i/2^{l_i - l_{i-1}}$; пусть $Q_i = \bigcup_{\nu=1}^{t} Q_{i\nu}$, причем $Q_{i\nu} \cap Q_{i\mu} = \varnothing$ при $\nu \neq \mu$, $|Q_{i\nu}| = 2^{l_i - l_{i-1}}$, и все вершины $Q_{i\nu}$ имеют одинаковую высоту $(l_i'$ или $l_i' + 1)$, $\nu = 1, \ldots, t$. Пусть $T_i' \sim T_i$, T приведено относительно всех множеств $Q_{i\nu}$, $\nu = 1, \ldots, t$, см. рис. 4. В дереве T_i' объединение множества $\{v(Q_{i\nu}) \mid \nu = 1, \ldots, t\}$ и множества всех висячих вершин, которым приписаны вероятности $(i-1)$-го блока, есть по определению множество Q_{i-1}. По построению множество Q_{i-1} обладает всеми свойствами, перечисленными в начале данного пункта. $(k+1-i)$-й шаг закончен. Полученное дерево является исходным для следующего, $(k+1-(i-1))$-го шага.

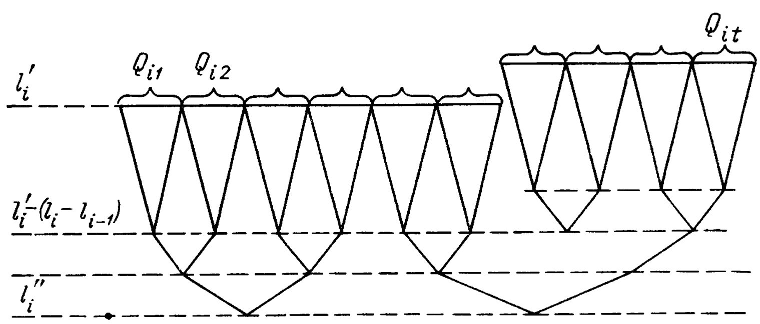


Рис. 4

Пусть $i = 1$ (выполняется последний шаг). В дереве T_1 вершины множества Q_1 расположены либо на одном ярусе (высоты l_1'), либо на двух ярусах (высоты l_1' и $l_1' + 1$). Пусть число вершин высоты l_1, не принадлежащих Q_1, есть α, $0 \leqslant \alpha < 2^{l_1'}$; $|Q_1| = 2^{l_1'} + \alpha = 2^{l_1}$; отсюда $\alpha = 0$ и $l_1' = l_1$. Это означает, что в полученном тупиковом дереве множество Q_1 составляет ярус высоты l_1 (и содержит m_1 висячих вершин); множество Q_2 составляет ярус высоты $l_1 + (l_2 - l_1) = l_2$ (и содержит m_2 висячих вершин) и т. д., множество Q_k составляет ярус высоты $l_{k-1} + (l_k - l_{k-1}) = l_k$ (и содержит m_k висячих вершин). Значит, тупиковое дерево есть реализация S_0. Таким образом, система преобразований $\{A, B\}$ м-полна на T_M.

Пример. Пусть спектр Хаффмана есть $S_0 = (1, 4, 4, 4, 4, 4, 5, 5, 5, 5, 5, 5)$. Здесь $k = 3$, $l_1 = 1$, $l_2 = 4$, $l_3 = 5$, $m_1 = 1$, $m_2 = 5$, $m_3 = 6$. Пусть $S = (2, 2, 2, 4, 5, 5, 5, 5, 5, 6, 7, 7)$. На 1-м шаге выполняется одно A-преобразование (и, возможно, одно эквивалентное преобразование), получается дерево со спектром $S_1 = (2, 2, 2, 4, 5, 5, 5, 5, 6, 6, 6, 6)$. На 2-м шаге выполняются сначала два A-преобразования, затем одно эквивалентное преобразование, затем одно B-преобразование, получается дерево со спектром (1, 4, 4, 4, 4, 4, 5, 5, 5, 5, 5, 5). На 3-м шаге в данном случае преобразований не требуется.

Доказательство леммы 3. Пусть в рассматриваемом дереве T_i количество невисячих вершин высоты l_i'' равно t_1, а количество вершин высоты l_i', не принадлежащих множеству Q_i, равно t_2, см. рис. 5; $|Q_i| = n_i = t_1 2^{r_i} - t_2 + 2t_2 = t_1 2^{r_i} + t_2$. С другой стороны, $|Q_i| = n_i = t \cdot 2^{l_i - l_{i-1}}$, где t — количество невисячих вершин в i-м уровне T_0. Отсюда имеем $t_2 = t \cdot 2^{l_i - l_{i-1}} - t_1 2^{r_i}$. Количество вершин множества Q_i высоты l_i' равно $t_1 2^{r_i} - t_2 = t_1 2^{r_i+1} - t 2^{l_i - l_{i-1}}$. При $r_i \leqslant l_i - l_{i-1} - 2$ оно кратно 2^{r_i+1}; при $r \geqslant l_i - l_{i-1} - 1$ оно кратно $2^{l_i - l_{i-1}}$. Количество вершин множества Q_i высоты $l_i' + 1$ равно $2t_2 = t \cdot 2^{l_i - l_{i-1} + 1} - t_1 2^{r_i+1}$; при $r_i \geqslant l_i - l_{i-1} - 1$ оно кратно $2^{l_i - l_{i-1}}$.

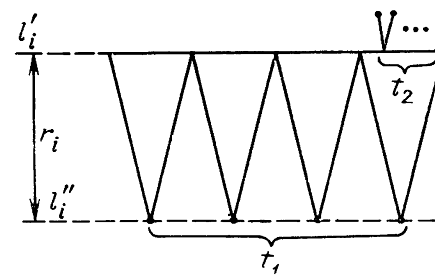


Рис. 5

2. Эффективный алгоритм минимизации линейной формы на M_σ и его обоснование

По теореме 1 алгоритм монотонного поиска, основанный на системе преобразований $\{A, B\}$, решает оптимизационную задачу на M_σ. В пп. 2.1—2.2 построена улучшающая стратегия. В п. 2.3 сформулирован алгоритм монотонного поиска с улучшающей стратегией. В п. 2.4 получена оценка вычислительной сложности этого алгоритма.

2.1. Преобразования A^{-1} и B^{-1} в тупиковых деревьях. Обозначим через K_i^A (соответственно K_i^B) множество всех деревьев, из которых некоторое тупиковое дерево получается A_i-преобразованием, $i = 1, \ldots, k$ (соответственно B_i-преобразованием, $i = 1, \ldots, k - 1$). Если $S = (l_1, \ldots, l_m)$, $S \in M(B^*)$, $T = T(S)$, то НОД $(l_1, \ldots, l_m)$ будем обозначать $d(T)$. Если в точности следовать алгоритму монотонного поиска, надо взять в качестве начального приближения $S1$ произвольный спектр $S \in M_\sigma$, построить множество $\left(\bigcup_{i=1}^{k} K_i^A\right) \cup \left(\bigcup_{i=1}^{k-1} K_i^B\right)$. Затем стоимость каждого построенного дерева сравнить с $c(S1)$, выделить улучшающие и подозрительные деревья (T — улучшающее дерево, если $c(T) < c(S1)$ и $d(T) = 1$; T — подозрительное дерево, если $c(T) < c(S1)$, а $d(T) \neq 1$). Всюду ниже $\alpha \in \{A, B\}$. В данном пункте построена и обоснована процедура, позволяющая выделить все улучшающие и подозрительные деревья класса K_i^α, не выполняя перебора всех элементов этого класса. Эта процедура есть последовательная элиминация элементов множества K_i^α. В пп. 2.1.1 и 2.1.2 описано эффективное построение дерева T_i^α, имеющего минимальную стоимость в классе K_i^α. Если $c(T_i^\alpha) \geqslant c(S1)$, то спектр $S1$ мажорирует весь класс K_i^α. Если $c(T_i^\alpha) < c(S1)$, а $d(T_i^\alpha) = 1$, то T_i^α — улучшающее дерево и оно мажорирует все множество $K_i^\alpha \setminus \{T_i^\alpha\}$. Индуктивно по μ, $\mu \geqslant 1$, пусть $c\left(T_{i_1 \ldots i_\mu}^\alpha\right) < c(S1)$, а $d\left(T_{i_1 \ldots i_\mu}^\alpha\right) \neq 1$, т. е. $T_{i_1 \ldots i_\mu}^\alpha$ — подозрительное дерево. Пусть $\widetilde{K}_{i_1 i_\mu}^\alpha$ — множество деревьев из $K_{i_1 \ldots i_\mu}^\alpha$, эквивалентных $T_{i_1 \ldots i_\mu}^\alpha$. В п. 2.1.3 показано, что тогда $K_{i_1 \ldots i_\mu}^\alpha \setminus \widetilde{K}_{i_1 \ldots i_\mu}^\alpha$ можно представить в виде объединения непересекающихся подмножеств $K^{\alpha}_{i_1\ldots i_\mu} \setminus \widetilde{K}^{\alpha}_{i_1\ldots i_\mu} = \bigcup\limits_{j=i_\mu}^{k} K^{\alpha}_{i_1\ldots i_\mu j}$. В пп. 2.1.4—2.1.6 описано эффективное построение дерева $T^{\alpha}_{i_1\ldots i_\mu j}$, имеющего минимальную стоимость в классе $K^{\alpha}_{i_1\ldots i_\mu j}$. Если $c\left(T^{\alpha}_{i_1\ldots i_\mu j}\right) \geqslant c(S1)$, то весь класс $K^{\alpha}_{i_1\ldots i_\mu j}$ мажорируется спектром $S1$; если $c\left(T^{\alpha}_{i_1\ldots i_\mu j}\right) < c(S1)$, а $d\left(T^{\alpha}_{i_1\ldots i_\mu j}\right) = 1$, то $T^{\alpha}_{i_1\ldots i_\mu j}$ — улучшающее дерево, и $K^{\alpha}_{i_1\ldots i_\mu j} \setminus \left\{T^{\alpha}_{i_1\ldots i_\mu j}\right\}$ мажорируется деревом $T^{\alpha}_{i_1\ldots i_\mu j}$.

Процедура последовательной элиминации элементов класса $K^{\alpha}_{i_1}$ может быть формализована следующим образом.

Шаг 1. Построить дерево $T^{\alpha}_{i_1}$; оно не просмотрено. Переход на шаг 2.

Шаг 2. Пусть $T^{\alpha}_{i_1\ldots i_\mu}$ не просмотрено, $\mu \geqslant 1$. Если $c\left(T^{\alpha}_{i_1\ldots i_\mu}\right) \geqslant c(S1)$, то $T^{\alpha}_{i_1\ldots i_\mu}$ просмотрено. Если $c\left(T^{\alpha}_{i_1\ldots i_\mu}\right) < c(S1)$, а $d\left(T^{\alpha}_{i_1\ldots i_\mu}\right) = 1$, то перезапоминание: $S1 := S\left(T^{\alpha}_{i_1\ldots i_\mu}\right)$, $T^{\alpha}_{i_1\ldots i_\mu}$ просмотрено. Если $c\left(T^{\alpha}_{i_1\ldots i_\mu}\right) < c(S1)$ и $d\left(T^{\alpha}_{i_1\ldots i_\mu}\right) \neq 1$, то $T^{\alpha}_{i_1\ldots i_\mu}$ — подозрительное дерево, оно просмотрено. Шаг выполняется до тех пор, пока не будут исчерпаны все непросмотренные деревья. Переход на шаг 3.

Шаг 3. Если нет подозрительных деревьев, то конец. Пусть $T^{\alpha}_{i_1\ldots i_\mu}$ — подозрительное дерево. Для $j = i_\mu, \ldots, k$, построить $T^{\alpha}_{i_1\ldots i_\mu j}$; каждое из этих деревьев не просмотрено. Шаг выполняется до тех пор, пока не будут исчерпаны все подозрительные деревья. Переход на шаг 2.

2.1.1. Построение дерева T^A_i. В тупиковом дереве T_0 пусть v_1 — вершина высоты $l_i - 1$, v_2 — вершина i-го уровня, $v_2 \notin T_0(v_1)$. Преобразование A_i^{-1} в T_0 заключается в перестановке поддеревьев $T_0(v_1)$ и $T_0(v_2)$.

Лемма 4. *В дереве Хаффмана T_x пусть v_1 — вершина наименьшей вероятности среди вершин высоты $l_i - 1$, v_2 — вершина наибольшей вероятности i-го уровня, $v_2 \notin T_x(v_1)$. Тогда дерево $T_x(v_1, v_2)$ (обозначим его T^A_i) имеет минимальную стоимость в классе K^A_i.*

Доказательство. Пусть v_1 и v_2 — вершины, определенные условиями леммы. Тогда в любом тупиковом дереве вероятность любой вершины i-го уровня не больше $p(v_2)$, а вероятность любой вершины высоты $l_i - 1$ не меньше $p(v_1)$ (этот факт является непосредственным следствием алгоритма Хаффмана). Отсюда следует утверждение леммы.

Замечание. $d\left(T^A_k\right) = 1$, $S\left(T^A_k\right) \in M_\sigma$, поэтому спектр $S\left(T^A_k\right)$ будем брать в качестве начального приближения $S1$.

Перестановку поддеревьев $T_x(v_1)$ и $T_x(v_2)$, где v_1 и v_2 — вершины, определенные условиями леммы 4, назовем *главным A^{-1}-преобразованием в i-м уровне T_x.*

Теорема 3. *Если* $c_0 = \min\limits_{M(B^*)} \sum\limits_{i=1}^{m} p_i l_i$, $c_\sigma = \min\limits_{M\sigma} \sum\limits_{i=1}^{m} p_i l_i$, *то* $0 \leqslant c_\sigma - c_0 \leqslant p_m \leqslant 1/m$.

Доказательство. Неравенство $c_\sigma - c_0 \leqslant p_m$ следует из того, что $c\left(T^A_k\right) \leqslant c_0 + p_m$.

2.1.2. Построение дерева T^B_i. В тупиковом дереве T_0 пусть u_1 — висячая вершина i-го уровня, u_2 — (невисячая) вершина высоты $l_i + 1$. Преобразование B^{-1} в T_0 заключается в перестановке поддеревьев $T_0(u_1)$ и $T_0(u_2)$.

Лемма 5. *В дереве T_x пусть u_1 — вершина наименьшей вероятности среди висячих вершин i-го уровня, u_2 — вершина наибольшей веро-*

ятности среди вершин высоты l_i+1. Тогда дерево $T_x(u_1, u_2)$ (обозначим его T_i^B) имеет минимальную стоимость в классе K_i^B.

Доказательство аналогично доказательству леммы 4.

Перестановку поддеревьев $T_x(u_1)$ и $T_x(u_2)$, где u_1 и u_2 — вершины, определенные условиями леммы 5, назовем *главным B^{-1}-преобразованием в i-м уровне T_x.*

2.1.3. Классы K_i^A и K_i^B. Пусть дерево T получено из T_0 преобразованием A^{-1} или B^{-1}. Множество вершин T, которые в T_0 составляли **j-й уровень**, будем называть *j-м уровнем T*, $j=1, \ldots, k$. Если $T \in K_i^A$, то i-й уровень T содержит одну вершину высоты l_i-1, (n_i-3) вершин высоты l_i и две вершины высоты l_i+1.

Лемма 6. *Пусть $T \in K_i^A$ и в i-м уровне T вершина высоты l_i-1 невисячая. Тогда T мажорируется.*

Доказательство. В дереве T_x пусть v_1 — вершина наименьшей вероятности среди вершин высоты l_i-1, а v_2 — вершина наибольшей вероятности среди невисячих вершин i-го уровня, $v_2 \notin T_x(v_1)$. Дерево $T_x(v_1, v_2)$ имеет минимальную стоимость среди деревьев, удовлетворяющих условиям леммы. Поэтому достаточно доказать, что $T_x(v_1, v_2)$ мажорируется. В дереве T_x пусть v_1' и v_1'' — прямые последователи v_1; их вероятности наименьшие в i-м уровне. Пусть $p(v_1') \leqslant p(v_1'')$.

а) Пусть вершины v_1' и v_1'' обе висячие. Пусть v_2' и v_2'' — прямые последователи v_2, $p(v_2') \leqslant p(v_2'')$. Покажем, что мажорирующим будет дерево T_i^B. Наибольшую вероятность среди вершин высоты l_i+1 имеет v_2'', поэтому $T_i^B = T_x(v_1', v_2'')$, см. рис. 6; $c(T_i^B) = c_0 + p(v_1') - p(v_2'')$. По свойству $2p(v_1'') \geqslant p(v_2')$, поэтому

$$c(T_i^B) \leqslant c_0 + p(v_1') - p(v_2'') + p(v_1'') - p(v_2') =$$
$$= c_0 + p(v_1) - p(v_2) = c(T_x(v_1, v_2));$$
$$d(T_i^B) = 1.$$

б) Пусть хотя бы одна из вершин v_1' и v_1'' невисячая. Пусть в дереве T_x самый высокий уровень, в котором есть последователи и v_1, и v_2,

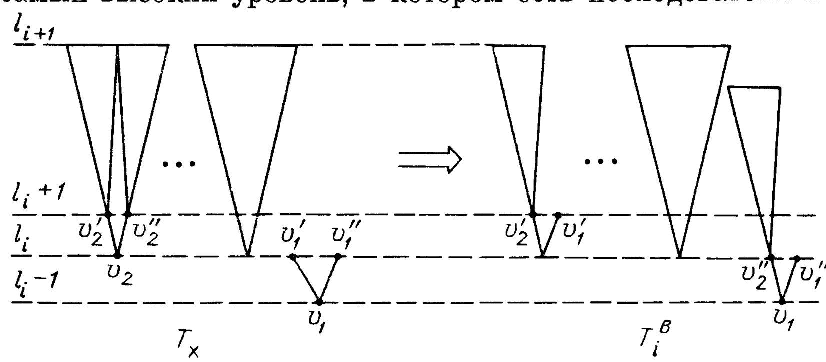


Рис. 6

имеет номер μ, $\mu > i$. Пусть w_2 — вершина наибольшей вероятности в μ-м уровне, w_1 — вершина наименьшей вероятности высоты $l_\mu-1$, $w_2 \in T_x(v_2)$, $w_1 \in T_x(v_1)$. Индукцией по $\mu - i$ можно доказать, что $p(w_2) - p(w_1) \leqslant p(v_2) - p(v_1)$. В μ-м уровне либо все последователи v_1, либо все последователи v_2 висячие; $c(T_\mu^A) = c_0 + p(w_1) - p(w_2) \leqslant c(T_x(v_1, v_2))$. Если вершина w_2 висячая, то $d(T_\mu^A) = 1$, и дерево T_μ^A будет мажорирующим для $T_x(v_1, v_2)$. Если вершина w_2 невисячая, то оба прямых последователя w_1 висячие, т. е. для дерева T_μ^A выполняется условие а). Дерево T_μ^B будет мажорирующим для T_μ^A и $T_x(v_1, v_2)$. Лемма доказана.

Следствие. *Если в i-м уровне $T_\varkappa$, $1 \leqslant i < k$, вершина наибольшей вероятности невисячая, то дерево T_i^A мажорируется (мажорируется весь класс K_i^A),*

Замечание. В силу леммы 6 для $i = 1, \ldots, k-1$ в классе K_i^A мажорируется каждое дерево, у которого вершина i-го уровня высоты $l_i - 1$ невисячая; исключим из K_i^A все такие деревья; для оставшейся части сохраним обозначение K_i^A.

С учетом последнего замечания, если $T \in K_i^\alpha$, $\alpha \in \{A, B\}$, то для каждого j, $i < j \leqslant k$, возможны два случая:

1) вершины j-го уровня T расположены на двух ярусах; если $T \in K_i^A$, то высоты ярусов есть l_j и $l_j + 1$; если $T \in K_i^B$, то высоты ярусов есть $l_j - 1$ и l_j. Будем говорить, что в этом случае j-й уровень T разделен на два подуровня — верхний и нижний. Ясно, что если j-й уровень T разделен, то для любого ν, $i < \nu < j$, ν-й уровень T тоже разделен;

2) все вершины j-го уровня T расположены на одном ярусе, хотя, возможно, его высота и не равна l_j. Будем говорить, что в этом случае j-й уровень T не разделен. Ясно, что если j-й уровень T не разделен, то для любого ν, $j < \nu \leqslant k$, ν-й уровень T тоже не разделен.

Пусть $T \in K_i^\alpha$; спектр $S(T)$ разобьем на блоки следующим образом: в 1-й блок включим первые m_1 элементов, во 2-й — следующие m_2 и т. д., в k-й блок — последние m_k элементов. Очевидно, j-й блок $S(T)$ есть набор высот всех висячих вершин j-го уровня T, $j = 1, \ldots, k$. Заметим, что спектры деревьев из K_i^α могут различаться только в блоках, номера которых не меньше i.

Пусть T_i^α — подозрительное дерево, $\alpha \in \{A, B\}$; для $j = i, \ldots, k$ пусть K_{ij}^α — множество деревьев из K_i^α, у которых для каждого ν, $1 \leqslant \nu < j$, ν-й блок спектра совпадает с ν-м блоком $S(T_i^\alpha)$, а j-й блок отличается от j-го блока $S(T_i^\alpha)$.

Легко видеть, что $K_i^\alpha \setminus \widetilde{K}_i^\alpha = \bigcup\limits_{j=i}^{k} K_{ij}^\alpha$.

Замечание 1. $K_{ii}^B = \varnothing$.

Замечание 2. Если T_i^A — подозрительное дерево, то $m_i \leqslant 3$; при этом если $m_i = 1$, то $K_{ii}^A = \varnothing$.

2.1.4. Класс K_{ii}^A. Лемма 7. *Пусть T_i^A — подозрительное дерево и $m_i = 2$; пусть v_1' — висячая вершина высоты $l_i + 1$, v_3 — (невисячая) вершина наименьшей вероятности высоты l_i в дереве T_i^A. Тогда дерево $T_i^A(v', v_3)$ имеет наименьшую стоимость в классе K_{ii}^A.*

Доказательство. Если T_i^A — подозрительное дерево и $m_i = 2$, то i-й блок $S(T_i^A)$ есть $(l_i - 1,\ l_i + 1)$. Из определения K_{ii}^A следует, что если $T \in K_{ii}^A$, то i-й блок $S(T)$ есть $(l_i - 1,\ l_i)$. В дереве T пусть v_1 есть прямой предшественник двух (невисячих) вершин i-го уровня высоты $l_i + 1$; а v_2 есть (висячая) вершина i-го уровня высоты $l_i - 1$; $c(T) = c_0 + p(v_1) - p(v_2)$; $c(T)$ минимально, когда v_2 имеет наибольшую вероятность среди висячих вершин i-го уровня, а прямыми последователями v_1 являются вершины, вероятности которых — наименьшие среди невисячих вершин i-го уровня. Отсюда следует утверждение леммы.

При $m_i = 2$ перестановку $T_i^A(v_1')$ и $T_i^A(v_3)$, где v_1' и v_3 — вершины, определенные условиями леммы 7, назовем *D_i-преобразованием.* Заметим, что $d(T_i^A(v_1', v_3)) = 1$ — это дерево не может быть подозрительным.

Лемма 8. *Пусть T_i^A — подозрительное дерево и $m_i = 3$; в дереве пусть v_1' и v_1'' — две (висячие) вершины i-го уровня высоты $l_i + 1$,*

$p(v_1') \leqslant p(v_1'')$, v_3 — *вершина наименьшей вероятности среди невисячих вершин i-го уровня. Тогда дерево* $T_i^A(v_1'', v_3)$ *имеет минимальную стоимость в классе.* K_{ii}^A.

Доказательство аналогично доказательству леммы 7.

При $m_i = 3$ перестановку $T_i^A(v_1'')$ и $T_i^A(v_3)$, где v_1'' и v_3 — вершины, определенные условиями леммы 8, назовем *D_i-преобразованием.* Заметим, что $d(T_i^A(v_1'', v_3)) = 1$ — это дерево не может быть подозрительным.

2.1.5. Классы K_{ij}^A и K_{ij}^B при $j > i$. Пусть T_i^α — подозрительное дерево. Из определения K_{ij}^α следует, что если j-й уровень в T_i^α не разделен, $j > i$, то $K_{ij}^\alpha = \varnothing$.

Пусть j-й уровень в T_i^α разделен, $j > i$. В этом случае все висячие вершины j-го уровня T_i^α расположены на одном подуровне.

Пусть все висячие вершины j-го уровня подозрительного дерева T_i^α расположены в нижнем (верхнем) подуровне. Пусть w — висячая вершина j-го уровня наименьшей (наибольшей) вероятности, z — вершина, вероятность которой наибольшая (наименьшая) в верхнем (нижнем) подуровне j-го уровня T_i^α. Перестановку $T_i^\alpha(w)$ и $T_i^\alpha(z)$ назовем *D_j-преобразованием.*

Лемма 9. *Пусть T_i^α — подозрительное дерево; пусть j-й уровень в T_i^α разделен, $j > i$. Дерево T_{ij}^α, получающееся из T_i^α преобразованием D_j, имеет минимальную стоимость в классе K_{ij}^α.*

Доказательство. Пусть в T_i^α все висячие вершины j-го уровня (их m_j штук) расположены в нижнем подуровне (случай, когда все висячие вершины j-го уровня расположены в верхнем подуровне, рассматривается аналогично). Пусть $T \in K_{ij}^\alpha$; из определения класса K_{ij}^α следует, что в T для $\nu = i + 1, \ldots, j$ ν-й уровень разделен, причем количество вершин в нижнем (верхнем) подуровне равно количеству вершин в нижнем (верхнем) подуровне ν-го уровня T_i^α. Если $i \leqslant \nu < j$, то набор высот всех висячих вершин ν-го уровня T совпадает с набором высот всех висячих вершин ν-го уровня T_i^α. Отсюда имеем: в классе K_{ij}^α минимальную стоимость имеет дерево, у которого сумма вероятностей всех вершин верхнего подуровня j-го уровня принимает минимальное возможное значение. Набор вероятностей всех вершин j-го уровня дерева $T \in K_{ij}^\alpha$ совпадает с набором вероятностей всех вершин j-го уровня некоторого тупикового дерева; количество висячих вершин в нижнем подуровне j-го уровня T равно $m_j - q$, в верхнем — q, $1 \leqslant q \leqslant \min\{m_j, n_j'\}$ здесь n_j' — количество вершин в верхнем подуровне. Набор вероятностей всех вершин j-го уровня дерева T_i^α совпадает с набором вероятностей всех вершин j-го уровня $T_\varkappa$. Сумма любых t штук наименьших вероятностей вершин j-го уровня дерева $T_\varkappa$ не превосходит суммы любых t штук вероятностей вершин j-го уровня любой другой реализации спектра S_0. Отсюда следует утверждение леммы.

Замечание. T_{ij}^α может быть подозрительным деревом только тогда, когда $m_j = 1$. В этом случае спектры деревьев из K_{ij}^α могут различаться только в блоках, номера которых больше j.

2.1.6. Классы $K_{i_1 \ldots i_\mu}^\alpha$ при $\mu > 1$. Пусть дерево $T_{i_1 \ldots i_\mu}^\alpha$, имеющее минимальную стоимость в классе $K_{i_1 \ldots i_\mu}^\alpha$, подозрительное, $\mu > 1$. В каждом дереве класса $K_{i_1 \ldots i_\mu}^\alpha$ для каждого j, $i_\mu < j \leqslant k$, j-й уровень либо не разделен, либо разделен на два подуровня, разность высот которых равна 1. Спектры деревьев из $K^{\alpha}_{i_1\ldots i_\mu}$ могут различаться только в блоках, номера которых больше j_μ.

Определение. Для $j=i_\mu+1, \ldots, k$ пусть $K^{\alpha}_{i_1\ldots i_\mu j}$ — множество деревьев из $K^{\alpha}_{i_1\ldots i_\mu}$, у которых для каждого $\nu \in \{1, \ldots, j\}$ ν-й блок соответствующего спектра совпадает с ν-м блоком $S\left(T^{\alpha}_{i_1\ldots i_\mu}\right)$, а j-й блок отличается от j-го блока $S\left(T^{\alpha}_{i_1\ldots i_\mu}\right)$. Легко видеть, что $K^{\alpha}_{i_1\ldots i_\mu}\setminus\widetilde{K}^{\alpha}_{i_1\ldots i_\mu} = \bigcup\limits_{j=i_\mu+1}^{k} K^{\alpha}_{i_1\ldots i_\mu j}$. Если j-й уровень в $T^{\alpha}_{i_1\ldots i_\mu}$ не разделен, $j>j_\mu$, то $K^{\alpha}_{i_1\ldots i_\mu j} = \varnothing$.

Лемма 10. *Пусть $T^{\alpha}_{i_1\ldots i_\mu}$ — подозрительное дерево, пусть j-й уровень в нем разделен, $j>i_\mu$. Тогда дерево $T^{\alpha}_{i_1\ldots i_\mu j}$, получающееся из $T^{\alpha}_{i_1\ldots i_\mu}$ преобразованием D_j, имеет минимальную стоимость в классе $K^{\alpha}_{i_1\ldots i_\mu j}$.*

Доказательство аналогично доказательству леммы 9.

2.2. Преобразования A^{-1} и B^{-1} в подозрительных деревьях. Пусть в результате выполнения процедуры последовательной элиминации элементов класса $K^{\alpha}_{i_1}$ установлено, что дерево $T^{\alpha}_{i_1\ldots i_\mu}$ подозрительное, $\mu \geqslant 1$. Через $\widetilde{K}^{\alpha}_{i_1\ldots i_\mu}$ мы обозначили подкласс деревьев, эквивалентных $T^{\alpha}_{i_1\ldots i_\mu}$; назовем дерево $T^{\alpha}_{i_1\ldots i_\mu}$ главным в подклассе $\widetilde{K}^{\alpha}_{i_1\ldots i_\mu}$. Согласно алгоритму монотонного поиска надо в каждом дереве подкласса $\widetilde{K}^{\alpha}_{i_1\ldots i_\mu}$ выполнить преобразования A^{-1} и B^{-1}. Ясно, что эти преобразования надо проводить только в уровнях, номера которых не меньше i_1.

Лемма 11. *Пусть $T \in K^B_i$, T — подозрительное дерево. Тогда преобразование B_i^{-1} в T мажорируется.*

Лемма 12. *Пусть $T \in K^A_i$, T — подозрительное дерево. Тогда преобразование A_i^{-1} в T мажорируется.*

Лемма 13. *Пусть $T \in K^A_i$, T — подозрительное дерево. Тогда преобразование B_i^{-1} в T мажорируется.*

Лемма 14. *Пусть $T \in K^{\alpha}_i$, $\alpha \in \{A, B\}$, T — подозрительное дерево. Пусть j-й уровень T разделен, $j>i$. Тогда преобразование A_j^{-1} в T мажорируется.*

Лемма 15. *Пусть $T \in K^{\alpha}_i$, $\alpha \in \{A, B\}$, T — подозрительное дерево. Пусть j-й уровень T разделен, $j>i$. Тогда преобразование B_j^{-1} в T мажорируется.*

Доказательство лемм 11—15 приведено ниже в данном пункте.

Из лемм 11—15 следует, что в деревьях класса $\widetilde{K}^{\alpha}_{i_1\ldots i_\mu}$ преобразования A^{-1} и B^{-1} достаточно проводить только в неразделенных уровнях, номера которых больше i_1 (точнее, больше i_μ). Индуктивно, пусть в результате выполнения процедуры последовательной элиминации выделен класс H эквивалентных подозрительных деревьев; пусть Q — главное дерево класса H. Пусть по алгоритму монотонного поиска требуется в каждом дереве класса H выполнить преобразования A^{-1} и B^{-1} в тех неразделенных уровнях, номера которых больше некоторого i. Ясно, что A^{-1} и B^{-1} в неразделенном уровне выполняются так же, как и тупиковом дереве. Аналогично п. 2.1, для $\nu>i$ пусть H^A_ν (соответственно

H_ν^B) есть класс деревьев, получающихся из деревьев класса H преобразованием A_ν^{-1} (соответственно B_ν^{-1}). Аналогично леммам 4 и 5 можно доказать следующие утверждения: дерево Q_ν^A (соответственно Q_ν^B), получающееся из Q главным A_ν^{-1}-преобразованием (соответственно B_ν^{-1}-преобразованием), имеет минимальную стоимость в классе H_ν^A (соответственно H_ν^B). Индуктивно по t, $t \geqslant 1$, если $Q^\alpha_{\nu_1\ldots\nu_t}$ — подозрительное дерево, введем аналогично п. 2.1.3 классы $H^\alpha_{\nu_1\ldots\nu_t j}$, $j = \nu_t + 1, \ldots, k$. Пусть $\widetilde{H}^\alpha_{\nu_1\ldots\nu_t}$ — класс деревьев, эквивалентных $Q^\alpha_{\nu_1\ldots\nu_t}$; тогда $H^\alpha_{\nu_1\ldots\nu_t} \setminus \widetilde{H}^\alpha_{\nu_1\ldots\nu_t} = \bigcup\limits_{j=\nu_t+1}^{k} H^\alpha_{\nu_1\ldots\nu_t j}$. Если $j > \nu_t$ и j-й уровень в $Q^\alpha_{\nu_1\ldots\nu_t}$ не разделен, то $H^\alpha_{\nu_1\ldots\nu_t j} = \varnothing$; если j-й уровень в $Q^\alpha_{\nu_1\ldots\nu_t}$ разделен, то дерево $Q^\alpha_{\nu_1\ldots\nu_t j}$ получающееся из $Q^\alpha_{\nu_1\ldots\nu_t}$ преобразованием D_j, имеет минимальную стоимость в классе $H^\alpha_{\nu_1\ldots\nu_t j}$ (это можно доказать аналогично лемме 9).

Сформулированные утверждения позволяют построить процедуру последовательной элиминации элементов множества $H^\alpha_{\nu_1}$, идентичную процедуре, приведенной в начале п. 2.1. В результате выполнения процедуры будут выделены подклассы эквивалентных подозрительных деревьев класса $H^\alpha_{\nu_1}$. Аналогично леммам 11—15 можно доказать, что преобразования A^{-1} и B^{-1} в этих подклассах достаточно выполнять только в неразделенных уровнях, номера которых больше i_ν.

Лемма 16. *Пусть в дереве T, полученном в ходе обратных преобразований, некоторый уровень содержит две невисячие вершины, разность высот которых равна 2. Тогда T мажорируется.*

Доказательство. Пусть z_1 и z_2 — невисячие вершины j-го уровня T, $l(z_1) - l(z_2) = 2$. Пусть самый высокий уровень, в котором есть как последователи z_1, так и последователи z_2, имеет номер ν, $\nu > j$. Очевидно, что $m_\nu \geqslant 4$ и $c(T) \geqslant c(T_\nu^A)$. Если в ν-м уровне дерева T_x вершина наибольшей вероятности невисячая, то T_ν^A мажорируется (следствие леммы 6), тогда T тоже мажорируется. Если же в ν-м уровне T_x вершина наибольшей вероятности висячая, то $d(T_\nu^A) = 1$, и дерево T мажорируется деревом T_ν^A. Лемма доказана.

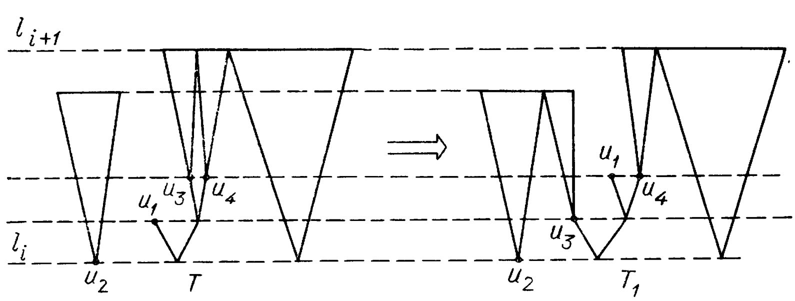


Рис. 7

Доказательство леммы 11. Если $l_{i+1} - l_i = 2$, то преобразование B_i^{-1} к T вообще не применимо. Пусть $l_{i+1} - l_i \geqslant 3$. Преобразование B_i^{-1} в T выполняется таким образом, как изображено на рис. 7. Полученное дерево обозначим T_1; $c(T_1) = c(T) + p(u_1) - p(u_3)$. По свойству 2 $p(u_1) \geqslant p(u_3) + p(u_4)$, поэтому $c(T_1) \geqslant c(T) + p(u_4)$. Пусть самый высокий разделенный уровень дерева T имеет номер ν, $\nu > i$. Очевидно, $m_\nu \geqslant 4$. Проведем в T преобразование D_ν, полученное дерево обозначим T_2. Ясно, что $T_2 \in K_i^B$, $d(T_2)=1$; кроме того, $c(T_2) \leqslant c(T)+p(u_4) \leqslant c(T_1)$ — дерево T_1 мажорируется.

Доказательство леммы 12. Преобразование A_i^{-1} в T может быть двух видов, см. рис. 8. На рис. 8, *а* вершины i-го уровня z_1 и z_2 невисячие, $l(z_1)-l(z_2)=2$. На рис. 8, *б* вершины i-го уровня w_1 и w_2 —

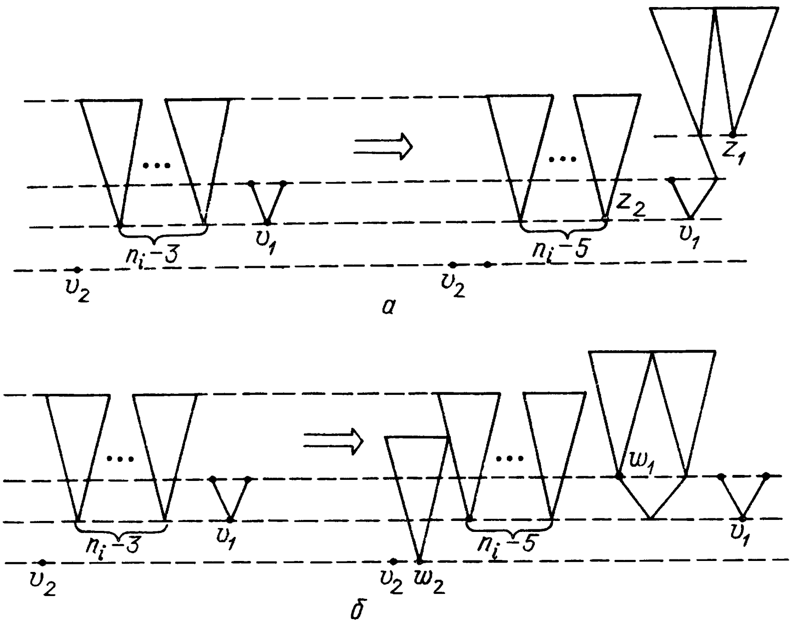


Рис. 8

невисячие, $l(w_1)-l(w_2)=2$. По лемме 16 оба полученных дерева мажорируются.

Доказательство леммы 13. Пусть v_i' и v_1'' — вершины i-го уровня T высоты l_i+1.

1. Пусть v_1' и v_1'' — обе невисячие. В этом случае в i-м уровне T висячая вершина единственная, ее высота равна l_i-1. Величина r_{i+1}

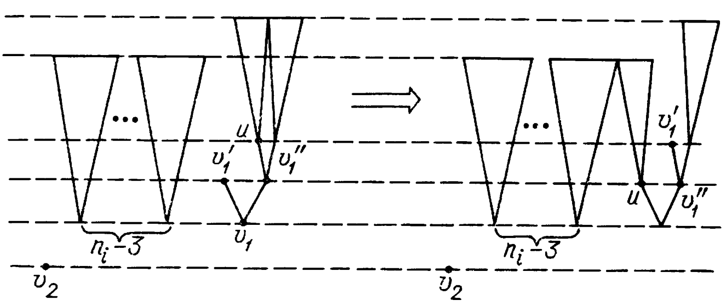


Рис. 9

для дерева T равна $l_{i+1}-(l_i-1)=l_{i+1}-l_i+1$. Преобразование B_i проводится тогда, когда $r_{i+1} \leqslant l_{i+1}-l_i-2$; в результате величина r_{i+1} увеличивается не более чем на 2. Поэтому дерево, у которого $r_{i+1}=l_{i+1}-l_i+1$, не может быть получено преобразованием B_i ни из какого дерева.

2. Пусть одна из вершин v_1', v_1'' висячая, другая невисячая. Преобразование B_i^{-1} в T выполняется таким образом, как изображено на рис. 9. Стоимость полученного дерева есть

$$c(T)+p(v_1')-p(u) \geqslant c_0+p(v_1')-p(u) \geqslant c(T_i^B); \quad d(T_i^B)=1.$$

Дерево T_i^B мажорирует рассматриваемое преобразование.

3. Случай, когда обе вершины v_1', v_1'' висячие, рассматривается аналогично п. 2.

Доказательство леммы 14. Преобразование A_j^{-1} в T может быть трех видов, см. рис. 10. Дерево T — подозрительное, поэтому все

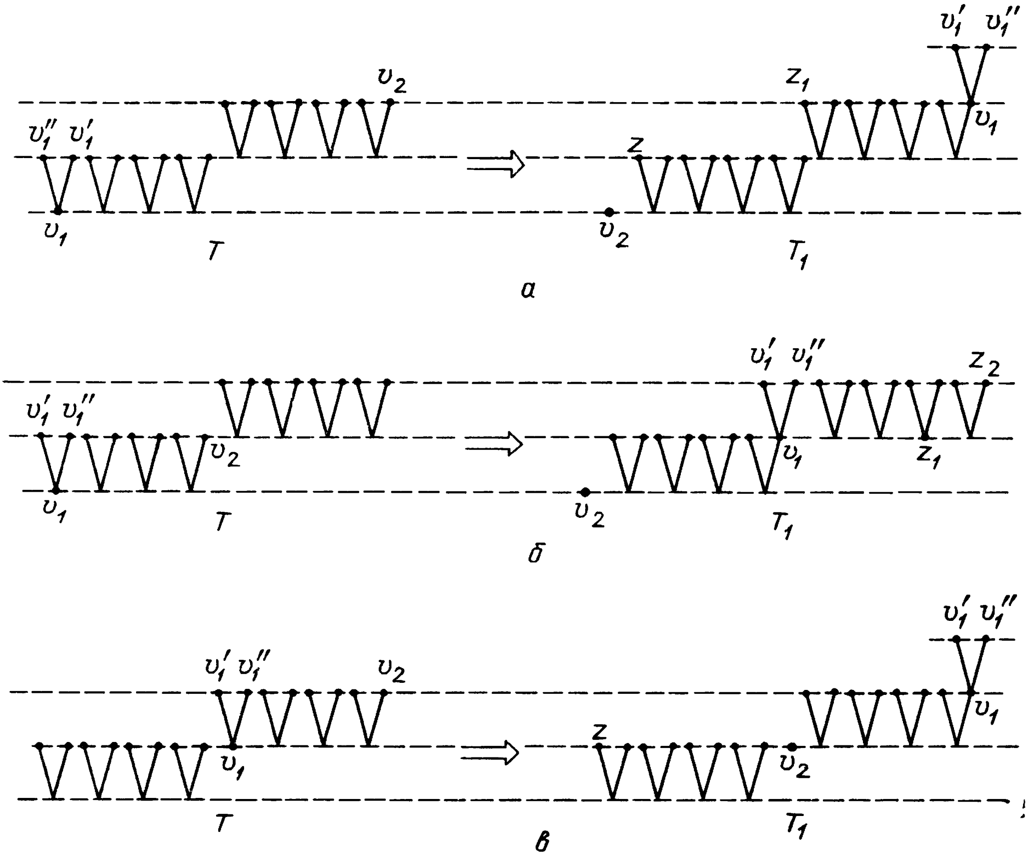


Рис. 10

висячие вершины j-го уровня T расположены либо в верхнем, либо в нижнем подуровне.

Пусть все висячие вершины j-го уровня T расположены в верхнем подуровне (все вершины нижнего подуровня невисячие).

а) В T_1 вершины v_1' и z невисячие, см. рис. 10, *а*; $l(v_1') - l(z) = 2$. По лемме 16 дерево T_1 мажорируется.

б) В T_1 вершины v_1' и v_2 невисячие, см. рис. 10, *б*; $l(v_1') - l(v_2) = 2$. По лемме 16 дерево T_1 мажорируется.

в) Пусть z — произвольная (невисячая) вершина нижнего подуровня j-го уровня T (рис. 10, *в*); $c(T_1(z, v_1)) = c(T_1) + p(z) - p(v_1) \geqslant c_0$; отсюда $c(T_1) \geqslant c_0 + p(v_1) - p(z)$; $T \in K_i^A$ (или $T \in K_i^B$). Выполним в T преобразование A_i (соответственно B_i), получим оптимальное дерево T_0. Перестановка $T_0(z)$ и $T_0(v_1)$ есть A_j-преобразование; $c(T_0(z, v_1)) = c_0 + p(v_1) - p(z) \leqslant c(T_1)$. Дерево $T_0(z, v_1)$ мажорируется, так как z — невисячая вершина (лемма 6), поэтому T_1 тоже мажорируется.

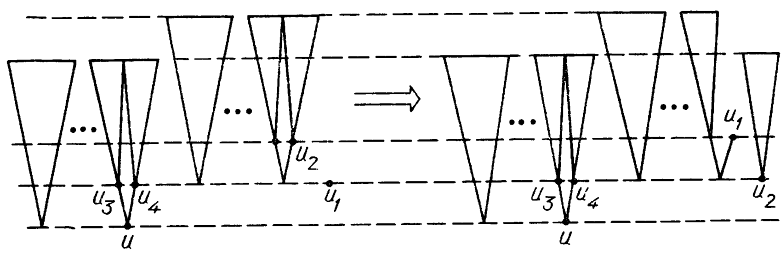
Пусть все висячие вершины j-го уровня T расположены в нижнем подуровне (все вершины верхнего подуровня невисячие).

а) В T_1 вершины z_1 и v_2 невисячие, $l(z_1) - l(v_2) = 2$, см. рис. 10, *а*. По лемме 16 дерево T_1 мажорируется.

б) Пусть z_1 — прямой предшественник двух (невисячих) вершин верхнего подуровня j-го уровня T (рис. 10, *б*), z_2 — произвольная вершина верхнего подуровня, $z_2 \notin T(z_1)$. Пусть самый высокий уровень T, в котором есть последователи и z_1, и z_2, имеет номер μ, $\mu > 1$. В μ-м уровне либо все последователи z_1, либо все последователи z_2 висячие. Пусть $T' \sim T$ и в μ-м уровне T' среди последователей z_1 есть хотя бы одна висячая вершина и среди последователей z_2 есть хотя бы одна висячая вершина. Пусть $T_2 = T'(v_1, v_2)$; очевидно, $c(T_2(z_1, v_2)) = c(T_2) + p(v_2) - p(z_1) \geqslant c_0$, отсюда $c(T_1) = c(T_2) \geqslant c_0 + p(z_1) - p(v_2)$. Выполним в T' преобразование A_i, если $T \in K_i^A$ (соответственно B_i, если $T \in K_i^B$). Полученное оптимальное дерево обозначим T_0. Очевидно, $T_0(z_1, v_2) \in K_j^A$, $c(T_0(z_1, v_2)) = c_0 + p(z_1) - p(v_2)$, $d(T_0(z_1, v_2)) = 1$, поэтому T_1 мажорируется.

в) В T_1 вершины v_1' и v_2 невисячие, $l(v_1') - l(v_2) = 2$, см. рис. 10, *в*. По лемме 16 дерево T_1 мажорируется.

Доказательство леммы 15. Если все висячие вершины j-го уровня T расположены в нижнем подуровне, то величина r_{j+1} равна



T T_1

Рис. 11

$l_{j+1} - l_j$ или $l_{j+1} - l_j + 1$, и дерево T не может быть получено B_j-преобразованием ни из какого дерева. Пусть все висячие вершины j-го уровня T расположены в верхнем подуровне. В этом случае преобразование B_j^{-1} в T выполняется таким образом, как изображено на рис. 11. Пусть u — вершина нижнего подуровня j-го уровня T, u_3 и u_4 — ее прямые последователи. Пусть самый высокий уровень, в котором есть последователи и u_3, и u_4, имеет номер μ, $\mu > j$. В μ-м уровне либо все последователи u_3, либо все последователи u_4 висячие; количество таких вершин не меньше 2. Пусть $T' \sim T$, и в μ-м уровне T среди последователей u_3 есть висячая вершина и среди последователей u_4 есть висячая вершина. Пусть $T_2 = T'(u_1, u_2)$. Ясно, что $T_2 \sim T_1$; $c(T_2(u_1, u_3)) = c(T_2) + p(u_3) - p(u_1) \geqslant c_0$; $c(T_1) = c(T_2) \geqslant c_0 + p(u_1) - p(u_3)$. Если $T' \in K_i^A$, выполним в T' преобразование A_i (соответственно B_i, если $T' \in K_i^B$). Полученное оптимальное дерево обозначим T_0. Очевидно, $T_0(u_1, u_3) \in K_j^B$; $c(T_0(u_1, u_3)) = c_0 + p(u_1) - p(u_3) \leqslant c(T_1)$; $d(T_0(u_1, u_3)) = 1$. Дерево $T_0(u_1, u_3)$ будет мажорирующим для T_1.

2.3. Формальное описание алгоритма минимизации линейной формы на M_σ. Сформулированный ниже алгоритм представляет собой соединение алгоритма монотонного поиска (с учетом мажорирования) и процедуры последовательной элиминации.

Шаг 0. Для заданного распределения P методом Хаффмана построить оптимальное дерево T_x. Если $d(T_x) = 1$, то конец, в противном случае переход на шаг 1.

Шаг 1. Построить T_k^A, $S1 := S(T_k^A)$. Для каждого $i = 1, \ldots, k-1$ выполнить главное B_i^{-1}-преобразование в дереве T_x. Для каждого $i = 1, \ldots, k-1$ такого, что вершина наибольшей вероятности i-го уровня T_x висячая, выполнить главное A_i^{-1}-преобразование в дереве T_x. Каждое из построенных деревьев не просмотрено. Переход на шаг 2.

Шаг 2. Пусть дерево T не просмотрено. Если $c(T) \geqslant c(S1)$, то T просмотрено. Если $c(T) < c(S1)$, а $d(T) = 1$, то перезапоминание: $S1 := S(T)$, T просмотрено. Если $c(T) < c(S1)$, а $d(T) \neq 1$, то T — подозрительное дерево, T просмотрено. Шаг выполняется до тех пор, пока не будут исчерпаны все непросмотренные деревья. Переход на шаг 3.

Шаг 3. Если нет подозрительных деревьев, то конец, $S1$ — искомый спектр. Пусть T — подозрительное дерево, T получено из некоторого дерева преобразованием A^{-1}, B^{-1} или D в i-м уровне. Для каждого j такого, что $i < j < k$ и j-й уровень в T разделен, выполнить преобразование D_j в T. Для каждого j такого, что $i < j < k$ и j-й уровень в T не разделен, а вершина наибольшей вероятности j-го уровня висячая, выполнить главное A_j^{-1}-преобразование в дереве T. Для каждого j такого, что $i < j < k$ и j-й уровень в T не разделен, выполнить главное B_j^{-1}-преобразование в дереве T. Если T получено из некоторого дерева преобразованием A_i^{-1}, а $m_i \geqslant 2$, то в T надо еще выполнить преобразование D_i. Все построенные деревья не просмотрены. Шаг 3 выполняется до тех пор, пока не будут исчерпаны все подозрительные деревья. Переход на шаг 2.

Примеры. 1. Пусть $m = 2^l$, $l > 1$, $\mathscr{P} = (1/m, \ldots, 1/m)$. Спектр Хаффмана для данного распределения есть $S(T_x) = (\underbrace{l, \ldots, l}_{m})$. Дерево T_x имеет один уровень. Работа алгоритма заканчивается построением T_1^A; $S(T_1^A) = (l-1, \underbrace{l, \ldots, l}_{m-3}, l+1, l+1)$, $d(T_1^A) = 1$, $c_\sigma = c(T_1^A) = c_0 + 1/m = l + 1/m$.

2. Пусть $m = 169$, коэффициенты линейной формы заданы следующим образом: $c_1 = 256 - \varepsilon$, $0 < \varepsilon < 1$, $c_i = 17$ для $i = 2, \ldots, 41$, $c_i = 2$ для $i = 42, \ldots, 169$;

$$S(T_x) = (3, \underbrace{6, \ldots 6}_{40}, \underbrace{9, \ldots 9}_{128}) \quad d(T_x) = 3;$$

$$S(T_1^A) = (2, \underbrace{6, \ldots 6}_{40}, \underbrace{10, \ldots 10}_{128}) \quad d(T_1^A) = 2,$$

$$c(T_1^A) = c_0 + \varepsilon;$$

$$S(T_2^A) = (3, 5, \underbrace{6, \ldots 6}_{39}, \underbrace{9, \ldots 9}_{112}, \underbrace{10, \ldots 10}_{16}), \quad d(T_2^A) = 1,$$

$$c(T_2^A) = c_0 + 15;$$

$$S(T_3^A) = (3, \underbrace{6, \ldots 6}_{40}, 8, \underbrace{9, \ldots 9}_{125}, 10, 10), \quad d(T_3^A) = 1,$$

$$c(T_3^A) = c_0 + 2;$$

$$S(T_1^B) = (4, 5, 5, 5, 5, \underbrace{6, \ldots 6}_{39}, \underbrace{9, \ldots 9}_{128}), \quad d(T_1^B) = 1,$$

$$c(T_1^B) = c_0 + 188 - \varepsilon;$$

$$S(T_2^B) = (3, \underbrace{6, \ldots 6}_{39}, 7, 8, 8, 8, 8, \underbrace{9, \ldots 9}_{124}), \quad d(T_2^B) = 1,$$

$$c(T_2^B) = c_0 + 9.$$

На 1-м шаге $S1 := S(T_3^A)$, дерево T_1^A подозрительное,

$$S(T_{1,2}^A) = (2, \underbrace{6, \ldots 6}_{39}, 7, \underbrace{9, \ldots 9}_{8}, \underbrace{10, \ldots 10}_{120}),$$

$$d(T_{1,2}^A) = 1, \quad c(T_{1,2}^A) = c_0 + \varepsilon + 1.$$

Спектр $S(T_{1,2}^A)$ является оптимальным в матрице M_σ.

2.4. Оценка вычислительной сложности алгоритма.

Теорема 4. *Количество деревьев, построенных в ходе выполнения алгоритма, не превосходит* $3em^2$.

Доказательство. Ход алгоритма можно представить в виде неоднородного дерева. Вершины этого дерева — деревья, построенные при выполнении алгоритма. Корень — дерево T_x для заданного вероятностного распределения $\mathscr{P}$. Вершины первого яруса — деревья T_i^α, $\alpha \in \{A, B\}$, $i = 1, \ldots, k-1$. Если дерево T подозрительное и T_1 получено из T преобразованием A^{-1}, B^{-1} или D, то в дереве алгоритма вершина T_1 является прямым последователем T.

Лемма 17. *Пусть T — произвольная вершина дерева алгоритма. Пусть $T_0 = T_x$, $T_1, \ldots, T_n = T$ — вершины простого пути из корня в T. Тогда числа $d(T_0)$, $d(T_1)$, $\ldots$, $d(T_n)$ попарно взаимно просты.*

Доказательство. Зафиксируем произвольное $j \in \{0, \ldots, n-1\}$. Пусть дерево T_{j+1} получено из T_j главным преобразованием A_i^{-1}, или главным преобразованием B_i^{-1}, или преобразованием D_i. Каждое из этих преобразований заключается в перестановке висячей и невисячей вершин. При этом висячая вершина (обозначим ее v) меняет свою высоту на 1. Дальнейшие преобразования над деревом T_{j+1}, приводящие к деревьям $T_{j+2}, \ldots, T_n$, не меняют высоты v. Таким образом, $l(v)$ делится на $d(T_j)$, а $l(v)+1$ или $l(v)-1$ делится на $d(T_{j+1}), \ldots, d(T_n)$. Поэтому для каждого $j \in \{0, \ldots, n-1\}$ число $d(T_j)$ попарно взаимно просто с $d(T_{j+1}), \ldots, d(T_n)$. Лемма доказана.

Лемма 18. *Пусть T_1 и T_2 — соседние вершины дерева алгоритма. Тогда* НОД $(d(T_1), d(T_2)) = 1$.

Доказательство. Пусть T_1 получено из дерева T преобразованием A^{-1}, B^{-1} или D в i-м уровне, T_2 получено из T преобразованием A^{-1}, B^{-1} или D в j-м уровне. Рассмотрим сначала случай $i \neq j$. Пусть для определенности $i < j$. При преобразовании A_i^{-1}, B_i^{-1} или D_i в T висячая вершина i-го уровня (обозначим ее v) меняет свою высоту на 1; $l(v)+1$ или $l(v)-1$ делится на $d(T_1)$. При преобразовании A_j^{-1}, B_j^{-1} или D_j в T, $j > i$, высоты висячих вершин i-го уровня не меняются. Значит, $l(v)$ делится на $d(T_2)$. Отсюда следует утверждение леммы. Пусть $i = j$. В этом случае i-й уровень в T не разделен, и одно из деревьев T_1, T_2 (допустим, T_1) получено из T главным A_i^{-1}-преобразованием, другое (T_2) получено из T главным B_i^{-1}-преобразованием. В дереве T пусть l_i' — высота i-го уровня, v_1 — вершина высоты $l_i'-1$ наименьшей вероятности, v_2 — вершина наибольшей вероятности i-го уровня (висячая), u — вершина наибольшей вероятности среди невисячих вершин i-го уровня, u_1 и u_2 — прямые последователи u, $p(u_1) \geqslant p(u_2)$. Если $u \notin T(v_1)$, то высота u_1 в T_1 равна $l_i'+1$, а в T_2 она равна l_i'. Отсюда следует утверждение леммы. Если же $u \in T(v_1)$, то высота u_2 в T_1 равна $l_i'+2$, а в T_2 — $l_i'+1$. Отсюда следует утверждение леммы.

Итак, в дереве алгоритма каждой вершине T ставится в соответствие число $d(T)$, причем если T_1 и T_2 — соседние вершины, то НОД $(d(T_1), d(T_2)) = 1$, если T_1 есть последователь T_2, то НОД $(d(T_1), d(T_2)) = 1$.

Лемма 19. *Если S — спектр мощности m, $d(S) = d$, то $(m-1)/ /(2^d-1)$ — целое число.*

Этот факт хорошо известен [2].

Лемма 20. *Если* НОД$(d_1, d_2) = 1$, *то* НОД $\left(2^{d_1}-1,\ 2^{d_2}-1\right) = 1$.

Доказательство легко провести индукцией по $d_1 + d_2$.

Теперь каждой вершине T дерева алгоритма поставим в соответствие число $\mu(T) = 2^{d(T)} - 1$. Из лемм 19 и 20 следует, что $\mu(T)$ является делителем $m-1$, и если T_1 и T_2 — соседние вершины, то НОД$(\mu(T_1)$,

$\mu(T_2))=1$; если T_1 является последователем T_2, то НОД$(\mu(T_1), \mu(T_2))=1$.

Пусть $m-1=\mu_1^{\alpha_1}\ldots\mu_r^{\alpha_r}$ — разложение числа $m-1$ на простые множители; ясно, что $m-1\geqslant r!$

Лемма 21. *Для $i=0, \ldots, r-1$ количество невисячих вершин в i-м ярусе дерева алгоритма не превосходит* $(r-1)!/(r-1-i)!$

Доказательство. Индукция по i. Для $i=0$ утверждение леммы очевидно. Пусть количество невисячих вершин в i-м ярусе не более $(r-1)!/(r-1-i)!$, $i\geqslant 0$. Каждая невисячая вершина i-го яруса имеет не более $r-(i+1)$ прямых невисячих последователей. Поэтому количество невисячих вершин в $(i+1)$-м ярусе не более $(r-1)!(r-(i+1))/ /(r-1-i)!=(r-1)!/(r-1-(i+1))!$. Лемма доказана.

Количество невисячих вершин в дереве алгоритма не более

$$\sum_{i=0}^{r-1}\frac{(r-1)!}{(r-1-i)!}=(r-1)!\sum_{i=0}^{r-1}\frac{1}{(r-1-i)}<(r-1)!\,e<me.$$

Каждая невисячая вершина дерева алгоритма имеет не более $2m$ прямых висячих последователей, поэтому всего в дереве алгоритма не более $3em^2$ вершин. Теорема доказана.

Оценим число выполняемых элементарных операций. Количество подозрительных деревьев, построенных в ходе выполнения алгоритма, не превосходит em. Пусть T — подозрительное дерево, T получено из некоторого дерева преобразованием A^{-1}, B^{-1} или D в i-м уровне. Тогда по алгоритму надо выполнить следующее.

1) Для каждого уровня, номер которого больше i, выяснить, разделен он или нет — не более h_1m сравнений.

2) В каждом разделенном уровне, номер которого больше i, найти вершины, необходимые для D-преобразования — не более h_2m сравнений.

3) В каждом неразделенном уровне, номер которого больше i, найти вершины, необходимые для преобразований A^{-1} и B^{-1}. Это достаточно сделать однажды — в дереве Хаффмана.

4) В каждом уровне, номер которого больше i, выполнить соответствующее преобразование; количество полученных деревьев не больше h_3m. Подсчитать высоты висячих вершин каждого полученного дерева — не более h_3m^2 сравнений.

5) Для каждого из полученных деревьев подсчитать НОД высот его висячих вершин — не более $h_3m\cdot h_4m^2$ сравнений и сложений.

6) Для каждого полученного дерева подсчитать стоимость и сравнить ее с $c(S1)$ — не более $h_3m\cdot 2m$ сравнений и сложений.

Таким образом, число выполняемых элементарных операций не превосходит hm^4.

СПИСОК ЛИТЕРАТУРЫ

1. Емеличев В. А., Комлик В. И. Метод построения последовательности планов для решения задач дискретной оптимизации.— М.: Наука, 1981.
2. Марков А. А. Введение в теорию кодирования.— М.: Наука, 1982.
3. Яблонский С. В. Введение в дискретную математику.— М.: Наука, 1986.
4. Gilbert E. N., Moor E. F. Variable-length binary encoding // Bell. Syst. Techn. J.— 1959.— V. 38, N 4.— P. 933—967.
5. Picard C. F. Theorie der Fragebogen. Mit einem Anhang von E. Lüdde und H. Thiele.— Berl.: Academie.— Verl., 1973.
6. Schützenberger M. P. On synchronising prefix codes // Inf. and Control.— 1967.— V. 11, N 4.— P. 396—401.

Поступило в редакцию: первый вариант 18.IX.83,
окончательный вариант 15.VII.89