УДК 681.325

В. П. Семеренко, канд.техн.наук
(Винницкий государственный технический ун–т, Украина)

Параллельное декодирование кодов Бауза–Чоудхури–Хоквингема

(Статью представил д-р техн. наук В.Г.Тоценко)

Рассмотрен новый метод декодирования двоичных кодов Боуза—Чоудхури—Хоквингема (БЧХ) на основе теории линейной последовательностной машины. Задача обнаружения и исправления кратных ошибок интерпретируется как поиск пути по дереву связей диаграммы переходов автомата. Предложена аппаратная реализация алгоритма декодирования.

Розглянуто новий метод декодування двійкових кодів Боуза—Чоудхури—Хоквингема на основі теорії лінійної послідовнісної машини. Задача виявлення та виправлення кратних помилок інтерпретується як пошук шляху по дереву зв'язків діаграми переходів автомата. Запропоновано апаратну реалізацію алгоритму декодування.

К л ю ч е в ы е с л о в а: циклические коды, коды БЧХ, декодеры, линейная последовательностная машина, графы, параллельная обработка.

В системах передачи данных и в других областях техники широко используются коды с обнаружением и использованием ошибок, особенно коды БЧХ [1—3]. Но, несмотря на многолетние исследования, теория кодов БЧХ пока не дала инженерной практике эффективных способов декодирования кратных ошибок.

Известные алгебраические методы декодирования кодов БЧХ наиболее универсальны, имеют строгое математическое обоснование, но требуют больших вычислительных затрат. Для n-разрядного кода один из самых быстродействующих алгоритмов — реккурентный алгоритм Берлекэмпа—Месси — относительно операций умножения имеет сложность чуть больше, чем $0\,(n \log_2 n)$ [1].

Известные неалгебраические (перестановочные, пороговые) методы декодирования значительно проще в реализации, однако они могут быть применены или для коротких длин кодов, или для кодов с особой структурой. Из-за отсутствия общей процедуры декодирования эти методы часто сводятся к случайному перебору всех возможных вариантов [2].

Для решения указанных проблем предлагается новый метод декодирования двоичных кодов БЧХ на основе теории линейной последовательностной машины (ЛПМ) [4].

Анализ диаграммы переходов ЛПМ. Двоичные регистры сдвига, используемые в циклических кодах, являются частным случаем ЛПМ и поэтому

они могут быть представлены в виде модели автомата Мура над полем Галуа GF (2):

$$\overline{S}(t+1) = \overline{A} \cdot \overline{S}(t) + \overline{B} \cdot \overline{U}(t),\ GF(2),$$

$$\overline{Y}(t) = \overline{S}(t),\ GF(2), \qquad (1)$$

где $\overline{S}(t)$, $\overline{U}(t)$, $\overline{Y}(t)$ — соответственно векторы состояний, входной и выходной; $\overline{A} = |a_{ij}|_{r \times r}$ — основная характеристическая матрица ЛПМ, $\overline{B} = |b_i|_r$ — характеристическая матрица ЛПМ.

На практике формулы (1) можно заменить следующими:

$$\overline{S}(t+1) = \begin{cases} \overline{A} \cdot \overline{S}(t) + \overline{B}, & \text{если } \overline{U}(t) = 1, \quad GF(2); \\ \overline{A} \cdot \overline{S}(t), & \text{если } \overline{U}(t) = 0. \end{cases} \qquad (2)$$

Удобным способом задания ЛПМ, как и любого автомата, является также диаграмма переходов $G(V, E)$. Для n-мерной ЛПМ над полем $GF(2)$ диаграмма переходов представляет собой ориентированный граф, состоящий из 2^n вершин, соответствующих 2^n состояниям автомата. Из любой вершины v_i графа G всегда выходят нулевая дуга $e^0_{\text{вых}}$ и единичная дуга $e^1_{\text{вых}}$ соответственно к вершинам $v^0_{\text{вых}}$ и $v^1_{\text{вых}}$, а также в вершину v_i всегда входят нулевая дуга $e^0_{\text{вх}}$ и единичная дуга $e^1_{\text{вх}}$ соответственно от вершин $v^0_{\text{вх}}$ и $v^1_{\text{вх}}$ (v_i, $v^0_{\text{вых}}$, $v^1_{\text{вых}}$, $v^0_{\text{вх}}$, $v^1_{\text{вх}} \in V$).

Если вершинам v_i, $v^0_{\text{вых}}$, $v^1_{\text{вых}}$, $v^0_{\text{вх}}$, $v^1_{\text{вх}}$ соответствуют состояния $\overline{S}_i$, $\overline{S}^0_{\text{вых}}$, $\overline{S}^1_{\text{вых}}$, $\overline{S}^0_{\text{вх}}$, $\overline{S}^1_{\text{вх}}$, то между указанными состояниями существуют следующие зависимости:

$$\overline{S}^0_{\text{вых}} = \overline{A} \cdot \overline{S}_i, \qquad \overline{S}_i = \overline{A} \cdot \overline{S}^0_{\text{вх}}, \qquad GF(2),$$

$$\overline{S}^1_{\text{вых}} = \overline{A} \cdot \overline{S}_i + \overline{B}, \quad \overline{S}_i = \overline{A} \cdot \overline{S}^1_{\text{вх}} + \overline{B}, \quad GF(2).$$

В том случае, когда $\overline{S}_i = \overline{S}^0_{\text{вых}} = \overline{S}^0_{\text{вх}}$ ($\overline{S}_i = \overline{S}^1_{\text{вых}} = \overline{S}^1_{\text{вх}}$), на графе G дуги $e^0_{\text{вых}}$ и $e^0_{\text{вх}}$ ($e^1_{\text{вых}}$ и $e^1_{\text{вх}}$) образуют петлю.

Если ЛПМ описывается матрицами $\overline{A}$ и $\overline{B}$ вида

$$\overline{A} = \begin{vmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ p_0 & p_1 & p_2 & \dots & p_{r-1} \end{vmatrix}; \quad \overline{B} = \begin{vmatrix} 0 \\ \dots \\ \dots \\ 0 \\ 1 \end{vmatrix}, \qquad (3)$$

или

$$\overline{A} = \begin{vmatrix} 0 & 0 & \dots & 0 & p_0 \\ 1 & 0 & \dots & 0 & p_1 \\ 0 & 1 & \dots & 0 & p_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & p_{r-1} \end{vmatrix}; \quad \overline{B} = \begin{vmatrix} 1 \\ 0 \\ \dots \\ \dots \\ 0 \end{vmatrix}, \qquad (4)$$

причем элементы в последней строке матрицы $\overline{A}$ из (3) и элементы последнего столбца матрицы $\overline{A}$ из (4) представляют собой коэффициент неприводимого многочлена

$$P(x) = p_0 + p_1 x + \ldots + p_r x^r, \quad GF(2),$$

то граф G такой ЛПМ является сильносвязным.

Для исследования свойств циклических кодов рассмотрим остовный подграф $G_0(V, E_0)$ графа $G(V, E)$, содержащий только входные и выходные нулевые дуги ($E_0 \subset E$), которые образуют нулевые циклы (НЦ). В [4] такой подграф G_0 называется внутренней сетью.

Порождающий многочлен $P(x)$ примитивного кода БЧХ длины $n = 2^m - 1$ над полем $GF(2)$, исправляющего τ ошибок, является наименьшим общим кратным (НОК) нечетных минимальных многочленов $m_1, \ldots, m_{2\tau-1}$, принадлежащих показателям $n_1, \ldots, n_{2\tau-1}$, [2]:

$$P(x) = \text{НОК}\left\{m_1(x)\, m_3(x) \ldots m_{2\tau-1}(x)\right\}. \tag{5}$$

Поскольку минимальные многочлены $m_i(x)$ являются простыми неприводимыми многочленами, то число НЦ подграфа G_0 диаграммы переходов кода БЧХ с неприводимым многочленом вида (5) равно произведению формальных сумм, соответствующих каждому многочлену $m_i(x)$ [3]:

$$\{1\,[1] + \mu_1\,[n_1]\}\,\{1\,[1] + \mu_2\,[n_2]\} \ldots \{1\,[1] + \mu_h\,[n_h]\},$$

где $\mu_i(n_i)$ — число НЦ многочлена $m_i(x)$ ($i = 1 \div 2\tau - 1$).

Например, многочленом

$$g(x) = (1 + x + x^2 + x^3 + x^4)(1 + x + x^4) = 1 + x^4 + x^6 + x^7 + x^8 \tag{6}$$

порождается (15,7)-код БЧХ, подграф G_0 которого состоит из одного цикла длиной 1, трех циклов длиной 5 и 16 циклов длиной 15:

$$\sum = \{1\,[1] + 1\,[15]\}\,\{1\,[1] + 3\,[5]\} = \{1\,[1] + 3\,[5] + 16\,[15]\}.$$

Поскольку граф G сильносвязный, то все НЦ графа G связаны между собой с помощью единичных дуг. Взаимосвязь НЦ графа G удобно представить в виде неориентированного дерева связей $T(V_T, E_T)$, в котором вершинами V_T служат НЦ графа G, а ребрами E_T — единичные дуги графа G, связывающие между собой НЦ.

Для построения дерева T необходимо все НЦ графа G распределить по уровням с помощью следующей итеративной процедуры.

К нулевому уровню относится тривиальный НЦ (ТНЦ), единственная вершина которого соответствует начальному нулевому состоянию $S(0)$ ЛПМ. К первому уровню будет относиться тот единственный НЦ (будем называть его основным НЦ (ОНЦ)), который связан с ТНЦ парой противоположно направленных единичных дуг. На следующей итерации определяются только те НЦ (будем именовать их периферийными НЦ (ПНЦ) второго уровня), которые связаны с ОНЦ противоположно направленными единичными дугами.

На i-й итерации определяются ПНЦ i-го уровня, к которым относятся НЦ, связанные противоположно направленными единичными дугами с ранее отобранными ПНЦ $(i - 1)$-го уровня.

Количество полученных уровней НЦ определяет число уровней i_T дерева T, а количество НЦ i-го уровня — число вершин i-го уровня дерева T ($i = 1 \div i_T$). Вершиной дерева T служит вершина v^0, соответствующая ГНЦ. В дереве T любые две вершины v_h^i и v_l^{i-1} соединяются только одним ребром на основании следующего правила.

Если ПНЦ i-го уровня связан единичными дугами с несколькими ПНЦ $(i-1)$-го уровня, то в дереве T отображается связь ПНЦ i-го уровня только с тем ПНЦ $(i-1)$-го уровня, с которым имеется наибольшее число единичных дуг (при равенстве числа единичных дуг для нескольких ПНЦ $(i-1)$-го уровня берется любая из них). Два ПНЦ одного уровня также могут быть связаны между собой противоположно направленными единичными дугами, однако в дереве T такие связи не будут отражены.

Под расстоянием между двумя НЦ, относящихся соответственно к i-му и j-му уровням ($i < j$), будем понимать величину $(j - i)$.

Связывающие состояния нулевых циклов графа. Для построения дерева T конкретного кода БЧХ необходимо определить вершины графа G, которые связывают между собой НЦ по единичным дугам.

Если из вершины $v_h^{i,\,i\to j}$, принадлежащей h-му НЦ i-го уровня, выходит единичная дуга к вершине $v_f^{i,\,i\to j}$, принадлежащей f-му НЦ j-го уровня, то вершину $v_h^{i,\,i\to j}$ будем именовать начальной связывающей вершиной h-го НЦ с f-м НЦ, вершину $v_f^{i,\,i\to j}$ — конечной связывающей вершиной f-го НЦ с h-м НЦ, а обе вершины — соседними. Соответствующие указанным вершинам соседние состояния $\overline{S}_h^{i,\,i\to j}(t)$ и $\overline{S}_f^{i,\,i\to j}(t)$ ЛПМ будем именовать аналогично $\overline{S}_h^{i,\,i\to j}(t)$ — начальное связывающее состояние h-го НЦ с f-м НЦ, а $\overline{S}_f^{i,\,i\to j}(t)$ — конечное связывающее состояние f-го НЦ с h-м НЦ.

Рассмотрим алгоритм нахождения связывающих состояний для построения двухуровневого дерева T n-мерной ЛПМ.

Алгоритм 1. 1. Приняв в качестве начального связывающего состояния $\overline{S}^{0,0\to 1}(0)$ ТНЦ состояние $\overline{S}(0)$, вычислить конечное связывающее состояние $\overline{S}^{1,0\to 1}(1)$ ОНЦ по формуле $\overline{S}^{1,0\to 1}(1) = \overline{A} \cdot \overline{S}^{0,0\to 1}(0) + \overline{B}$, $GF(2)$.

2. Определить начальные связывающие состояния ОНЦ со всеми ПНЦ второго уровня:

$$\overline{S}^{1,1\to 2}(2) = \overline{A} \cdot \overline{S}^{1,0\to 1}(1),\ \overline{S}^{1,1\to 2}(t+2) = \overline{A} \cdot \overline{S}^{1,1\to 2}(t+1),\ t = 1 \div n-2. \quad (7)$$

Полученные состояния вместе с состоянием $\overline{S}^{1,0\to 1}(1)$, составляют ОНЦ.

3. Определить конечные связывающие состояния ПНЦ второго уровня:

$$\overline{S}^{2,1\to 2}(t+2) = \overline{S}^{1,1\to 2}(t+2) + B,\ t = 0 \div n-2. \quad (8)$$

4. Полученные в п. 3 состояния сгруппировать по признаку принадлежности к одному ПНЦ второго уровня следующим образом: зафиксировав состояние $\overline{S}^{2,1\to 2}(t)$, в качестве исходного состояния ЛПМ $\overline{S}_z^{2,1\to 2}(0) = \overline{S}^{2,1\to 2}(z)$ для $z = 2 \div n$, последовательно вычислить $(n-1)$ последующих состояний по формуле $\overline{S}^{2,1\to 2}(t+1) = \overline{A} \cdot \overline{S}^{2,1\to 2}(t)$ для $t = 0 \div n-1$, сравнивая их со всеми $(n-1)$ значениями состояний (8). При совпадении соответствующие состояния включаются в одну группу. Количество состояний в γ-й группе определяет число пар единичных дуг между ОНЦ и γ-м ПНЦ второго уровня.

5. Из полученных п. 4 состояний выбрать минимальное множество $M^{1\to 2}$ состояний, охватывающих все ПНЦ второго уровня.

6. Конец.

Для построения многоуровневого дерева T п. 2—5 алгоритма 1 повторяются для связывающих состояний каждой соседней пары уровней.

Пример 1. Рассмотрим алгоритм формирования связывающих состояний для (15,7)-кода БЧХ, который порождается многочленом (6) и имеет такие характеристические матрицы ЛПМ:

$$\overline{A} = \left|\begin{array}{ccccccccc} 0&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&1 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&1&1 \end{array}\right|, \quad \overline{B} = \left|\begin{array}{c} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{array}\right|. \tag{9}$$

1. Для этого кода пара связывающих состояний между ТНЦ и ОНЦ имеет вид (для экономии места векторы состояний будем записывать в транспонированном виде)

$$\overline{S}^{0,0\to 1}(0) = |0\,0\,0\,0\,0\,0\,0\,0|, \; \overline{S}^{1,0\to 1}(1) = |1\,0\,0\,0\,0\,0\,0\,0|.$$

2. Начальное связывающее состояние ОНЦ с первым ПНЦ второго уровня $\overline{S}^{1,1\to 2}(2) = |0\,1\,0\,0\,0\,0\,0\,0|$. Остальные состояния, входящие в ОНЦ для данного примера, приведены в [2, с. 98] и обозначены как цикл A.

3. Вектор состояния $\overline{S}^{2,1\to 2}(2)$ вычисляется следующим образом: $\overline{S}^{2,1\to 2}(2) = |0\,1\,0\,0\,0\,0\,0\,0| + |1\,0\,0\,0\,0\,0\,0\,0| + |1\,1\,0\,0\,0\,0\,0\,0|$.

Аналогично вычисляются остальные связывающие состояния (таблица).

4. Первые 7 конечных связывающих состояний принадлежат разным циклам (по обозначению в [2] — циклам *B, D, F, C, I, L, H*), а остальные состояния — тем же циклам, но взятым в обратном порядке. Таким образом, число ПНЦ второго уровня равно 7, и все конечные связывающие состояния могут быть распределены на 7 групп по два состояния, принадлежащих одному циклу.

5. В минимальное множество $M^{1\to 2}$ могут войти по одному состоянию из каждой группы, например первые 7 состояний из таблицы. Остальные НЦ (циклы *K, M, J, E, G, N, O, P, R, S, T*) являются ПНЦ третьего уровня.

Удобным способом машинного представления дерева является его связанное представление [5], при котором каждой вершине, кроме корневой, ставится в соответствие указатель на связанную с ней предыдущую родительскую вершину, т. е. каждой вершине дерева T будет соответствовать несколько векторов состояний ЛМП.

Для представления вершины дерева T, соответствующей f-у НЦ $(i+1)$-го уровня, в общем случае необходимо $(q+1)$ векторов: указателя на соседнюю вершину h-го НЦ i-го уровня, в качестве которого выбирается конечное связывающее состояние $\overline{S}_h^{i,(i-1)\to i}(t)$ h-го НЦ i-го уровня с l-м НЦ $(i-1)$-го уровня и q идентификаторов, в качестве которых могут служить конечные

связывающие состояния $\overline{S}_f^{i+1,i\to(i+1)}(t)$ с h-м НЦ i-го уровня. Число q идентификаторов для НЦ $(i+1)$-го уровня определяется числом пар единичных дуг между f-м НЦ $(i+1)$-го уровня и h-м НЦ i-го уровня ($i = 3, 4, \ldots$).

Для представления вершины дерева T, соответствующей ОНЦ, достаточно двух векторов: указателя на ТНЦ, в качестве которого служит состояние $\overline{S}^{0,0\to1}(t)$, и идентификатора ОНЦ, в качестве которого можно выбрать его конечное связывающее состояние $\overline{S}^{1,0\to1}(t)$.

Для представления вершины дерева T, соответствующей h-у ПНЦ второго уровня, также достаточно двух векторов: указателя на ОНЦ, в качестве которого берется состояние $\overline{S}^{1,0\to1}(t)$, и идентификатора самой вершины, в качестве которого берется конечное связывающее состояние $S^{2,1\to2}(t)$ h-го ПНЦ с ОНЦ.

Поскольку одному графу G может соответствовать несколько эквивалентных вариантов дерева T, то возможно также несколько эквивалентных вариантов связанного представления дерева T. На рис. 1 показан один из вариантов связанного представления дерева для примера 1.

Интерпретация ошибок для кодов БЧХ на основе теории ЛПМ. В общем случае для исправления τ-кратной ошибки необходимо определить следующий вектор ошибки:

$$\overline{E}^{(\tau)}(x) = \overline{C}(x) - C_{\text{ош}}^{(\tau)}(x),\ GF(2), \qquad (10)$$

где $\overline{C}_{\text{ош}}^{(\tau)}(x)$ — кодовый вектор с τ-кратной ошибкой.

Лемма. ЛПМ, определяемая характеристическими матрицами вида (3) или (4) и порождающим многочленом вида (5), из состояния $\overline{S}(0)$ перейдет в одно и то же состояние $S_{\text{ош}}^{(\tau)}(n)$ при подаче на ее вход как вектора $\overline{C}_{\text{ош}}^{(\tau)}(x)$, так и вектора $\overline{E}^{(\tau)}(x)$.

Справедливость леммы основывается на том, что под воздействием кодового вектора $\overline{C}(x)$ ЛПМ из состояния $\overline{S}(0)$ основа перейдет в нулевое состо-

Связывающие состояния для двухуровневого дерева (15, 7)-кода БЧХ, порождаемого многочленом $g(x) = 1 + x^4 + x^6 + x^7 + x^8$

№ п. п	Начальное связывающее состояние ОНЦ с ПНЦ 2-го уровня	Конечное связывающее состояние ПНЦ с ОНЦ 2-го уровня
1	0 1 0 0 0 0 0 0	1 1 0 0 0 0 0 0
2	0 0 1 0 0 0 0 0	1 0 1 0 0 0 0 0
3	0 0 0 1 0 0 0 0	1 0 0 1 0 0 0 0
4	0 0 0 0 1 0 0 0	1 0 0 0 1 0 0 0
5	0 0 0 0 0 1 0 0	1 0 0 0 0 1 0 0
6	0 0 0 0 0 0 1 0	1 0 0 0 0 0 1 0
7	0 0 0 0 0 0 0 1	1 0 0 0 0 0 0 1
8	1 0 0 0 1 0 1 1	0 0 0 0 1 0 1 1
9	1 1 0 0 1 1 1 0	0 1 0 0 1 1 1 0
10	0 1 1 0 0 1 1 1	1 1 1 0 0 1 1 1
11	1 0 1 1 1 0 0 0	0 0 1 1 1 0 0 0
12	0 1 0 1 1 1 0 0	1 1 0 1 1 1 0 0
13	0 0 1 0 1 1 1 0	1 0 1 0 1 1 1 0
14	0 0 0 1 0 1 1 1	1 0 0 1 0 1 1 1

яние. Следовательно, при графической интерпретации формулы (10) член $\overline{C}(x)$ можно исключить.

Теорема. ЛПМ, определяемая характеристическими матрицами вида (3) или вида (4) и порождающим многочленом вида (5), под воздействием кодового вектора $\overline{C}^{(\tau)}_{\text{ош}}(x)$ из состояния $\overline{S}(0)$ перейдет в состояние $\overline{S}^{(\tau)}_{\text{ош}}(n)$, принадлежащее НЦ, которое находится на расстоянии τ от ТНЦ. (Состояние $\overline{S}^{(\tau)}_{\text{ош}}(n)$ в дальнейшем будем именовать синдромом ошибки.)

Доказательство. Согласно лемме вместо вектора $\overline{C}^{(\tau)}_{\text{ош}}(x)$ можно рассматривать вектор ошибки $\overline{E}^{(\tau)}(x)$, содержащий τ единиц, которые расположены в тех позициях, где произошли ошибки. На графовой модели вектор ошибки $\overline{E}^{(\tau)}(x)$ соответствует последовательности из τ единичных и $(n-\tau)$ нулевых дуг. По τ единичным дугам из ТНЦ можно попасть только в НЦ, находящийся от него на расстоянии τ.

С помощью теоремы можно найти новый способ поиска ошибок в кодах БЧХ.

Известно, что для циклического кода с кодовым расстоянием d каждому ненулевому синдрому можно сопоставить единственную конфигурацию ошибок кратности τ ($d = 2\tau + 1$). Поэтому теоретически достаточно запомнить все необходимые синдромы. Очевидно, что для (n, k)-кодов с большими значениями n и r такой способ очень неэффективен.

Точно идентифицировать синдром ошибки $\overline{S}^{(\tau)}_{\text{ош}}(n)$ можно также, если по графу G определить путь от него к состоянию $\overline{S}(0)$.

Анализ структуры графа G показывает, что данную задачу можно решить в два этапа: нахождение $w_{\text{ош}}$-го НЦ, содержащего синдром $\overline{S}^{(\tau)}_{\text{ош}}(n)$ (этап 1); построение взаимосвязанной цепочки нулевых циклов от $w_{\text{ош}}$-го НЦ к ТНЦ и нахождение соответствующей последовательности переходов от $\overline{S}^{(\tau)}_{\text{ош}}(n)$ к $\overline{S}(0)$ (этап 2). В терминах графовой модели указанная задача эквивалентна задаче нахождения пути в дереве T от вершины дерева, соответствующей НЦ с синдромом ошибки $\overline{S}^{(\tau)}_{\text{ош}}(n)$, к его корню. Использование дерева T вместо графа G позволяет заменить общую задачу поиска пути по графу, имеющую переборный характер, задачей направленного поиска пути от листьев дерева к его корню.

Алгоритм исправления кратной ошибки в кодах БЧХ. После получения ненулевого синдрома ошибки $\overline{S}^{(\tau)}_{\text{ош}}(n)$ вначале предполагается, что произошла одиночная ошибка и предпринимается попытка ее исправления по простому алгоритму, приведенному в [6]. Если исправить ошибку не удалось, то выполняется алгоритм исправления ошибки кратности τ в (n, k)-коде БЧХ ($\tau > 1$). Исходными данными для этого алгоритма являются кодовый вектор с ошибкой $\overline{C}^{(\tau)}_{\text{ош}}(x)$, синдром ошибки $\overline{S}^{(\tau)}_{\text{ош}}(n)$, а также характеристические матрицы A и B той ЛПМ, которая использовалась при кодировании кода БЧХ, и связанное представление дерева T в виде трехмерного массива

$$\overline{\text{MAS}}\,[i_{\max}]\,[w_{\max}]\,[q_{\max}+1], \tag{11}$$

где $i_{\max}$ — максимальное количество уровней дерева T; $w_{\max}$ — максимальное количество вершин одного уровня дерева T; $q_{\max}$ — максимальное количество конечных связывающих состояний между двумя соседними вершинами дерева T.

Алгоритм 2. Э т а п 1. 1. Положить $i = 1$.

2. Положить $i_3 = 0$.

3. Положить $i_2 = 0$.

4. Если $\overline{S}^{(\tau)}_{\text{ош}}(n + i_3) = \overline{\text{MAS}}[i][i_2][1]$, то синдром ошибки содержится в $w_{\text{ош}}$-м НЦ $i_{\text{ош}}$-го уровня, и минимальная кратность ошибки $\tau_{\min} = i_{\text{ош}}$ ($w_{\text{ош}} = i_2 + 1$, $i_{\text{ош}} = i + 1$). Перейти к этапу 2.

5. Положить $i_2 = i_2 + 1$. Если $i_2 < w_{i+1}$ (w_{i+1} — количество вершин дерева T на $(i + 1)$-м уровне), то перейти к п.4.

6. Вычислить $\overline{S}^{(\tau)}_{\text{ош}}(n + i_3 + 1) = \overline{A} \cdot \overline{S}^{(\tau)}_{\text{ош}}(n + i_3)$.

7. Положить $i_3 = i_3 + 1$. Если $i_3 < n$, то перейти к п.3.

8. Положить $i = i + 1$. Если $i < i_{\max}$, то перейти к п.2.

Э т а п 2. 1. Положить номер q первого конечного связывающего состояния НЦ, содержащего $\overline{S}^{(\tau)}_{\text{ош}}(n) : q = 1$.

2. Задать исходные значения: текущий номер w НЦ ($w = w_{\text{ош}}$), текущий номер i-го уровня НЦ ($i = i_{\text{ош}}$), текущее состояние $\overline{S}^{\,i}(j)$ ЛПМ ($\overline{S}^{\,i}(j) = \overline{S}^{(\tau)}_{\text{ош}}(n)$, $j = 1$), текущий номер y позиции ошибки в кодовом векторе ($y = 0$).

3. Если состояние $\overline{S}^{\,i}(j)$ равно q-му конечному связывающему состоянию w-го НЦ i-го уровня ($\overline{S}^{\,i}(j) = \text{MAS}[i][w][q]$), то перейти к п.5.

4. Вычислить новое состояние ЛПМ: $\overline{S}^{\,i}(j + 1) = \overline{A} \cdot \overline{S}^{\,i}(j)$. Перейти к п.3.

5. Номер y позиции ошибки в кодовом векторе $y = (y + j) \bmod n$. Исправить значение разряда y в векторе $\overline{C}^{(\tau)}_{\text{ош}}(x)$. Присвоить $\overline{C}(x) = \overline{C}^{(\tau)}_{\text{ош}}(x)$.

6. Уменьшить номер i : $i = i - 1$. Если $i = 0$, то перейти к п.8.

7. Вычислить соседнее связывающее состояние НЦ i-го уровня: $\overline{S}^{i,i\to(i+1)}(j) = \overline{S}^{i}(j) = \overline{S}^{\,i+1}(j) + \overline{B}$. Найти номер w НЦ, содержащего состояние $S^{i}(j)$. Перейти к п.3.

8. Вычислить по формулам (2) состояние $\overline{S}(n)$, в которое перейдет ЛПМ из нулевого состояния $S(0)$ при подаче на ее вход вектора $\overline{C}(x)$.

9. Если $\overline{S}(n) = \overline{S}(0)$, то такое сочетание ошибок возможно, перейти к п.10; иначе — такое сочетание ошибок неисправляемо, перейти к п.11.

10. Положить $q = q + 1$. Если $q < q_i$ (q_i — количество конечных связывающих состояний для $w_{\text{ош}}$-го НЦ $i_{\text{ош}}$-го уровня), то перейти к п.2.

11. Конец.

Пример 2. Пусть известны кодовый вектор $\overline{C}^{(\tau)}_{\text{ош}}(x)$ и синдром $\overline{S}^{(\tau)}_{\text{ош}}(n)$:

$$\overline{C}^{(\tau)}_{\text{ош}}(x) = |\,1\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\,|, \qquad (12)$$

$$\overline{S}^{(\tau)}_{\text{ош}}(n) = |\,1\,1\,0\,0\,1\,0\,0\,1\,|, \qquad (13)$$

и необходимо определить номера позиций ошибочных разрядов в векторе (12) для кода БЧХ, задаваемого матрицами (9).

Э т а п 1. Поскольку синдром (13) не совпадает ни с одним из связывающих состояний (см. рис.1), то, приняв его в качестве исходного состояния ЛПМ, будем последовательно вычислять очередные состояния ЛПМ:

$$\overline{S}^{(\tau)}_{\text{ош}}(n + 1) = \overline{A} \cdot \overline{S}^{(\tau)}_{\text{ош}}(n) = |\,1\,1\,1\,0\,1\,1\,1\,1\,|,$$

$$\overline{S}^{(\tau)}_{\text{ош}}(n + 2) = \overline{A} \cdot \overline{S}^{(\tau)}_{\text{ош}}(n + 1) = |\,1\,1\,1\,1\,1\,1\,0\,0\,|.$$

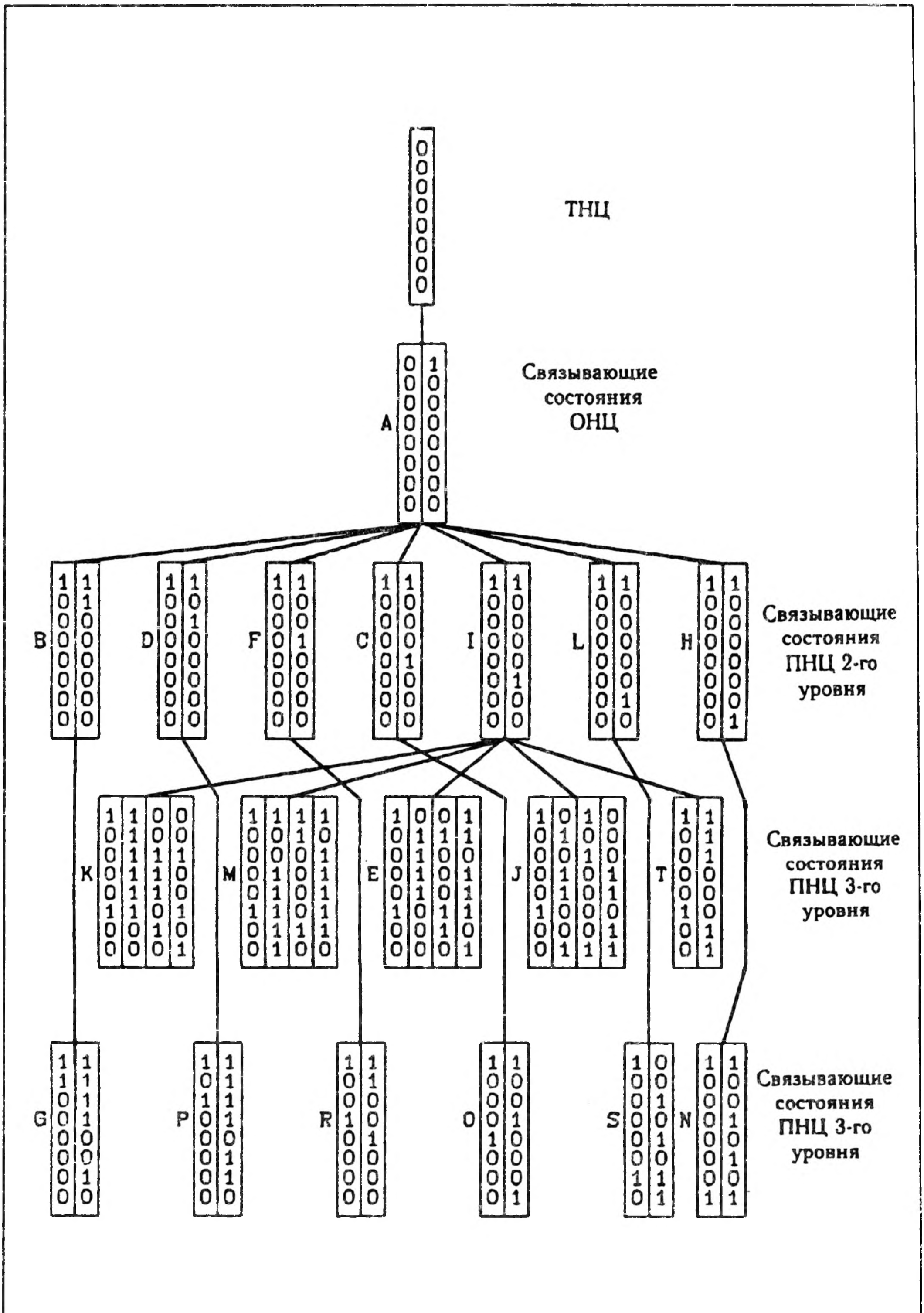

Рис. 1. Связанное представление дерева для (15, 7)-кода БЧХ, порождаемого многочленом $g(x) = 1 + x^4 + x^6 + x^7 + x^8$

Синдром $\overline{S}^{(\tau)}_{\text{ош}}(n+2)$ совпадает с первым конечным связывающим состоянием цикла K. Поэтому синдром (13) принадлежит 0-му ПНЦ третьего уровня ($i_{\text{ош}} = 3$, $w_{\text{ош}} = 0$), и минимальная кратность ошибки в (12) равна $\tau_{\min} = 3$.

Э т а п 2. Начальные действия связаны с подсчетом числа переходов от синдрома (13) к одному из конечных связывающих состояний $w_{\text{ош}}$-го НЦ (цикла K). Эти действия уже по сути выполнены на этапе 1, и позиция первой ошибки известна: $y = 0 + 2 = 2$.

От цикла K имеется указатель на ПНЦ второго уровня (цикла I, $i = 2$, $w = 4$). Определим соседнее связывающее состояние цикла I:

$$\overline{S}^{2,2\to3}(2) = \overline{S}^{(\tau)}_{\text{ош}}(n+2) + \overline{B} = |\,0\,1\,1\,1\,1\,1\,0\,0\,|.$$

Затем снова вычисляем состояния ЛПМ:

$$\overline{S}^{\,2}(1) = \overline{A} \cdot \overline{S}^{2,2\to3}(2) = |\,0\,0\,1\,1\,1\,1\,1\,0\,|,$$

$$\overline{S}^{\,2}(2) = \overline{A} \cdot \overline{S}^{2}(1) = |\,0\,0\,0\,1\,1\,1\,1\,1\,|,$$

$$\overline{S}^{2}(3) = \overline{A} \cdot \overline{S}^{2}(2) = |\,1\,0\,0\,0\,0\,1\,0\,0\,|.$$

Состояние $\overline{S}^{2}(3)$ совпадает с первым конечным связывающим состоянием цикла I с циклом A, значит, вторая ошибка содержится в позиции $y = 2 + 3 = 5$. Далее определяем соседнее связывающее состояние цикла A ($i = 1$, $w = 0$): $\overline{S}^{\,1,1\to2}(3) = \overline{S}^{\,1}(3) = \overline{S}^{\,2}(3) + \overline{B} = |\,0\,0\,0\,0\,0\,1\,0\,0\,|$. Затем последовательно определяем очередные состояния ЛПМ:

$$\overline{S}^{1}(1) = \overline{A} \cdot \overline{S}^{\,1,1\to2}(3) = |\,0\,0\,0\,0\,0\,0\,1\,0\,|,$$

. . . . . .

$$\overline{S}^{1}(10) = \overline{A} \cdot \overline{S}^{1}(9) = |\,1\,0\,0\,0\,0\,0\,0\,0\,|.$$

Состояние $\overline{S}_1(10)$ совпадает с конечным связывающим состоянием цикла A. Следовательно, третья ошибка содержится в позиции $y = 5 + 10 = 15$. Таким образом, исправленный кодовый вектор будет иметь вид

$$\overline{C}(x) = |\,1\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,0\,0\,0\,|.$$

Поскольку в цикле K имеется еще два конечных связывающих состояния, то с помощью этапа 2 можно получить еще два сочетания ошибок (1, 6, 12 и 7, 9, 14), приводящих к синдрому (13).

Как видно из приведенного примера, с помощью данного кода, предназначенного для исправления двойных ошибок, можно также обнаруживать и исправлять большое число тройных ошибок. Те тройные ошибки, синдромы которых попадают в циклы G, N, O, P, T, исправляются, а ошибки, синдромы которых попадают в циклы K, M, J, E, R, S, только обнаруживаются с указанием трех возможных сочетаний ошибок.

Аппаратная реализация кодера — декодера кодов БЧХ. Задачи кодирования и декодирования кодов БЧХ в основном совпадают с аналогичными задачами для обычных циклических кодов, отличие состоит лишь в необходимости операции по локализации и исправлению кратных ошибок. Поэтому устройство для кодирования, обнаружения и исправления одиноч-

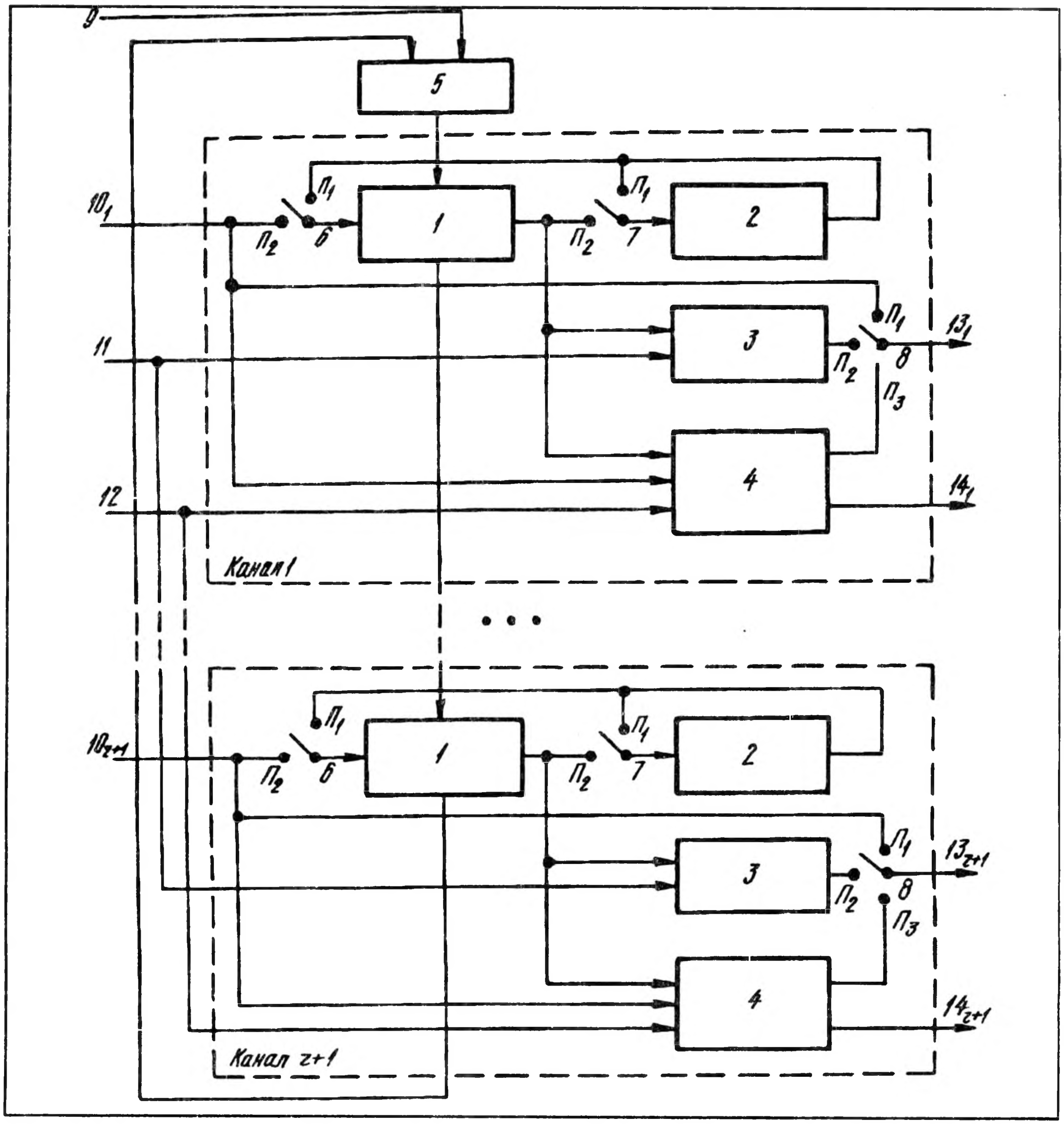

Рис. 2. Схема универсального кодера — декодера циклических кодов

ных ошибок в циклических кодах, которое было разработано в [6], будет пригодным и для кодов БЧХ. Схема такого устройства (рис. 2) является более общей ($(r + 1)$ канал вместо 4) и его функционирование более точно соответствует описанию, приведенному в [6].

Предлагаемый метод исправления кратных ошибок в кодах БЧХ предполагает наличие дерева связей T. Поскольку структура дерева T не зависит от вида обрабатываемых кодовых векторов, то алгоритм *1* может быть выполнен заранее и целесообразнее реализовать его не аппаратно, а программно.

Собственно исправление кратных ошибок осуществляется с помощью отдельного блока (рис.3), который является дополнительной частью каждого канала упоминаемого ранее устройства. В режиме программирования в узел *1* памяти по информационному входу записывается массив *11*, счетчик *5* обнуляется, а в счетчики *2, 3* и *4* записываются единицы. В режиме исправления

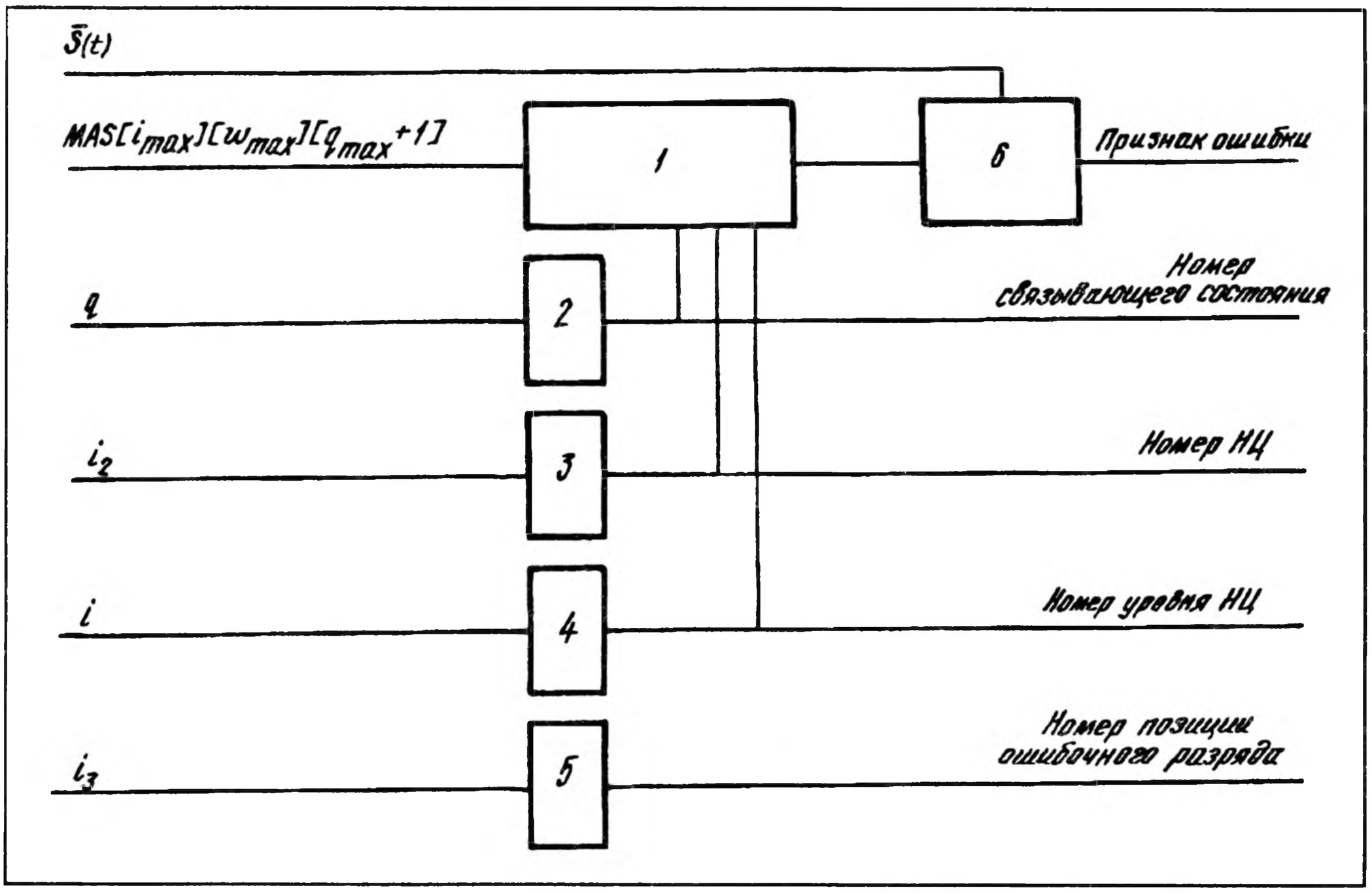

Рис.3. Схема блока исправления кратных ошибок в двоичных кодах БЧХ

кратных ошибок на первый вход схемы сравнения *6* от ЛПМ, реализованной в основном устройстве, поступают векторы состояний, которые сравниваются с векторами, поступающими на второй вход от узла *1*. После выполнения этапа 1 алгоритма 2 в счетчике *3* будет номер НЦ, содержащий синдром ошибки, в счетчике *4* — номер уровня указанного НЦ, а в счетчике *2* — количество использованных связывающих состояний в каждом НЦ. Этап 2 алгоритма 2 также сводится к сравнению векторов от ЛПМ и узла *1*, и каждый момент из совпадения свидетельствует о нахождении очередного номера позиции ошибочного разряда в кодовом векторе $C_{ош}^{(\tau)}(x)$ (значение счетчика *5*). Узел *1* и схема *2* работают по параллельно-конвейерному принципу, что обеспечивает одновременную обработку всех векторов массива *11*.

Рассмотренный в настоящей статье алгоритм 1 имеет сложность относительно операций булевого умножения матрицы на вектор порядка $O(n^2)$. В общем случае для нахождения конечных связывающих состояний НЦ i-го уровня алгоритм 1 будет иметь сложность порядка $O(n^i)$. Несмотря на резкое возрастание сложности, алгоритм 1 выполняется только один раз для заданного порождающего многочлена кода БЧХ.

Для исправления τ ошибок постоянно используется лишь алгоритм 2, сложность которого относительно тех же операций порядка $O\left(\sum_{i=1}^{\tau} \frac{n}{m_i}\right)$, где m_i — число хранимых в НЦ i-го уровня конечных связывающих состояний с НЦ $(i-1)$-го уровня.

При малой кратности ошибок и использовании всех связывающих состояний НЦ алгоритм 2 имеет почти линейную сложность. При минимальном

размере дерева T, когда $m_i = 1$ для всех i, алгоритм 2 будет иметь верхнюю границу сложности порядка $O(\tau n)$.

Несмотря на необходимость дополнительной памяти для хранения дерева T, существенно упрощается логика декодера, благодаря регулярности алгоритма 2, и обеспечивается параллельная обработка данных в основном устройстве и в блоке исправления ошибок.

Важным преимуществом разработанного метода является также его способность декодирования за пределами границы кода БЧХ.

В настоящее время оба алгоритма реализованы программно на языке Си.

A new method of decoding binary Bose-Chaudhuri-Hocquenghem codes on the basis of the theory of linear sequential computer is considered. Error detection and multi-error correction problem is interpreted as the path search over tree connections of automaton transition graph. Hardware support of decoding algorithm is proposed.

1. *Блейхут Р.* Теория и практика кодов, исправляющих ошибки / Пер. с англ. — М.:Мир, 1986. — 576 с.
2. *Кларк Дж. мл., Кейн Дж.* Кодирование с исправлением ошибок в системах цифровой связи/ Пер. с англ. —М.: Радио и связь, 1987. — 392 с.
3. *Колесник В.Д., Мирончиков Е.Т.* Декодирование циклических кодов. — М.: Связь, 1968. — 252 с.
4. *Гилл А.* Линейные последовательностные машины / Пер. с англ. — М.: Наука, 1974. — 288 с.
5. *Лэнгсам И., Огенстайн М., Тененбаум А.* Структуры данных для персональных ЭВМ/ Пер. с англ. — М.: Мир, 1989. — 568 с.
6. *Семеренко В.П.* Разработка универсального кодера — декодера циклических кодов // Электрон. моделирование. — 1995. — №4. — С. 26—31.

Поступила 05.09.96;
после доработки 23.01.97

СЕМЕРЕНКО Василий Петрович, канд. техн. наук, доцент Винницкого государственного технического университета. В 1976 г. окончил Винницкий политехнический ин-т. Область научных исследований — параллельная обработка данных в различных системах: передачи данных, искусственного интеллекта, технической диагностики и др.