УДК 519.725

В.П. СЕМЕРЕНКО

ПАРАЛЛЕЛЬНОЕ ДЕКОДИРОВАНИЕ УКОРОЧЕННЫХ ЦИКЛИЧЕСКИХ КОДОВ

Винницкий национальный технический университет,
21021, Хмельницкое шоссе, 95, Винница, Украина
Тел.: +38(0432)598379, E-mail:vpsemerenko@mail.ru

Анотація. Запропонована багаторівнева графова і автоматна моделі вкороченого двійкового циклічного коду та вкороченого коду Ріда-Соломона (РС) на основі теорії лінійних послідовнісних схем (ЛПС). Введені обернені автономні ЛПС з характеристичними матрицями типу Фібоначчі і типу Галуа, які функціонують по оберненій шкалі часу. Розглянуто алгоритми пошуку помилок у вкороченому двійковому циклічному коді та вкороченому коді РС з використанням паралельної обробки даних.

Ключові слова: вкорочені циклічні коди, вкорочені коди Ріда-Соломона, лінійні послідовнісні схеми, граф, паралельна обробка

Abstract. The graphical and automatical models of the shortened cyclic codes and shortened Reed-Solomon (RS) codes based on the theory of linear finite-state machines (LFSM) are suggested. The inverse autonomous LFSM with characteristic matrixes of Fibonacci type and Galois type which function on the inverse time scale are offered. The methods of the random errors correction for the shortened cyclic codes and shortened RS codes with the parallel processing are considered.

Keywords: shortened cyclic codes, and shortened Reed-Solomon codes, linear finite-state machines, graph, parallel processing

Аннотация. Предложена многоуровневая графовая и автоматная модели укороченного двоичного циклического кода и укороченного кода Рида-Соломона (РС) на основе теории линейных последовательностных схем (ЛПС). Введены обратные автономные ЛПС с характеристическими матрицами типа Фибоначчи и типа Галуа, которые функционируют по обратной шкале времени. Рассмотрены алгоритмы поиска ошибок в укороченном двоичном циклическом коде и укороченном коде РС с использованием паралелльной обработки данных.

Ключевые слова: укороченные циклические коды, укороченные коды Рида-Соломона, линейные последовательностные схемы, граф, параллельная обработка

ВВЕДЕНИЕ

Параметры циклических кодов определяются, с одной стороны, математическими законами линейной алгебры и, с другой стороны, практическими ограничениями тех систем, где они используются [1]. Например, в системах передачи данных длина кодовых последовательностей должна быть кратной байту и очень трудно подобрать порождающий многочлен кода с заданными корректирующими способностями. Поэтому на практике (в цифровом телевидении, в QR-кодах, в оптических дисках) используют укороченные циклические коды [2].

Обычно укорочение состоит в заполнении h информационных разрядов нулями. В результате получается укороченный циклический ($n-h, k-h$)-код. На приемной стороне можно добавить h нулей в соответствующие позиции и выполнить декодирование полученного кодового слова обычным способом.

В результате укорочения получается код с тем же самым минимальным кодовым расстоянием. Кроме сохранения корректирующих способностей укороченные циклические коды сохраняют и большинство других свойств исходного кода, имеют те же самые схемы кодирования и декодирования. Единственное существенное отличие укороченного кода состоит в том, что циклический сдвиг кодовой комбинации не всегда будет приводить к получению очередной разрешенной кодовой комбинации. Поэтому укороченные коды не являются строго циклическими и их часто называют псевдоциклическими.

Основная идея помехоустойчивого кодирования заключается во введении искусственной избыточности для получения возможности обнаружения и исправления ошибок в кодовых последовательностях. В укороченных циклических кодах часть разрядов не содержат полезной информации, т.е. вводится дополнительная избыточность. Поэтому полезно провести исследование, посвященное использованию такой дополнительной избыточности для упрощения декодирования этого класса циклических кодов.

Для решения этой задачи будем использовать их автоматное и графовое представления с помощью теории линейных последовательностных схем (ЛПС).

АВТОМАТНОЕ ПРЕДСТАВЛЕНИЕ УКОРОЧЕННЫХ ЦИКЛИЧЕСКИХ КОДОВ

Будем рассматривать циклический (n,k)-код Ω над полем Галуа $GF(2)$ с минимальным кодовым расстоянием $d_{\min}$.

Известны различные способы представления циклических кодов: полиномиальное, матричное, через корни порождающего многочлена [3]. Для нашей задачи наиболее удобным способом представления циклических кодов является их представление с помощью математического аппарата линейных последовательностных схем (ЛПС) [4].

Дадим формальное определение ЛПС в общем виде.

ОПРЕДЕЛЕНИЕ 1. ЛПС Λ – это конечный автомат линейного типа (линейный автомат), который над полем Галуа $GF(q)$ описывается функцией состояний (переходов)

$$S(t+1) = A \times S(t) + B \times U(t), \qquad GF(q), \tag{1}$$

и функцией выходов

$$Y(t) = C \times S(t) + D \times U(t), \qquad GF(q), \tag{2}$$

где t – дискретное время; $A = \left\| a_{ij} \right\|_{r \times r}$, $B = \left\| b_{ij} \right\|_{r \times l}$, $C = \left\| c_{ij} \right\|_{m \times r}$, $D = \left\| d_{ij} \right\|_{m \times l}$ – характеристические матрицы ЛПС; $S = \left\| s_i \right\|_r$, $U = \left\| u_i \right\|_l$, $Y = \left\| y_i \right\|_m$ – векторы состояний, входной и выходной.

Выбор характеристических матриц ЛПС определяется требованием r-управляемости ЛПС, т. е. возможности перехода из любого состояния S_i в состояние S_j не более, чем за r тактов работы автомата.

Обычно применяются две разновидности ЛПС. Первая разновидность ЛПС описывается характеристическими матрицами вида:

$$A = \begin{vmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \cdots & 1 \\ g_0 & g_1 & g_2 & \cdots & g_{r-1} \end{vmatrix}, \quad B = \begin{vmatrix} 0 \\ 0 \\ \dots \\ 0 \\ 1 \end{vmatrix}, \quad C = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \end{vmatrix}, \quad D = \begin{vmatrix} 0 \end{vmatrix}. \tag{3}$$

Вторая разновидность ЛПС описывается характеристическими матрицами вида:

$$A = \begin{vmatrix} 0 & 0 & 0 & \dots & g_0 \\ 1 & 0 & 0 & \dots & g_1 \\ 0 & 1 & 0 & \dots & g_2 \\ \dots & \dots & \dots & \cdots & \dots \\ 0 & 0 & 0 & 1 & g_{r-1} \end{vmatrix}, \quad B = \begin{vmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \end{vmatrix}, \quad C = \begin{vmatrix} 0 & 0 & \dots & 0 & 1 \end{vmatrix}, \quad D = \begin{vmatrix} 0 \end{vmatrix} \tag{4}$$

.

Матрицу A в (3) называют также сопровождающей или матрицей Фибоначчи, а матрицу A в (4) – транспонированная сопровождающей или матрицей Галуа.

Элементы последней строки матрицы A из (3) и последнего столбца матрицы A из (4) представляют собой коэффициенты порождающего многочлена циклического кода Ω :

$$g(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_{r-1} x^{x-1} + g_r x^r . \quad (5)$$

Размерности матриц ЛПС Λ и параметры циклического кода Ω связаны через коэффициент r, который для кода равен числу контрольных разрядов кодового вектора $C(x)$ при систематическом кодировании ($r = n - k$).

При аппаратной реализации ЛПС Λ над полем Галуа $GF(2)$ соответствует регистр сдвига с линейными обратными связями (РСЛОС) с l входами, m выходами и r элементами памяти.

Одним из частных случаев ЛПС является автономная ЛПС.

ОПРЕДЕЛЕНИЕ 2. Автономной ЛПС над полем Галуа $GF(2)$ называется такая ЛПС, функционирование которой не зависит от входных воздействий и описывается функцией состояний (переходов)

$$S(t+1) = A \times S(t), \qquad GF(2), \quad (6)$$

и функцией выходов

$$Y(t) = C \times S(t), \qquad GF(2). \quad (7)$$

Характеристические матрицы B и D автономной ЛПС равны нулю.

Как отмечается в [4], автономная ЛПС не преобразует приложенные извне воздействия, а генерирует периодическую последовательность символов поля Галуа $GF(2)$. Период r-мерной ЛПС определяется видом порождающего многочлена (5): для примитивного многочлена период будет максимальным, т.е. $2^r - 1$.

ГРАФОВОЕ ПРЕДСТАВЛЕНИЕ УКОРОЧЕННЫХ ЦИКЛИЧЕСКИХ КОДОВ

Поскольку ЛПС является конечным автоматом, поэтому для задач кодирования и декодирования укороченных циклических кодов удобно перейти к графу переходов-выходов этого автомата [5]. Для r-мерной ЛПС над полем $GF(2)$ такой граф представляет собой ориентированный граф $G_{FA}(V_{FA}, E_{FA})$, в котором 2^r вершин из множества вершин V_{FA} соответствуют 2^r внутренним состояниям автомата, а дуги из множества дуг E_{FA} показывают направления переходов между внутренними состояниями ($r = n - k$). Каждой дуге поставим в соответствие метку входа и метку выхода.

Метка входа дуги равна значению входного сигнала, под воздействием которого происходит переход между соответствующими состояниями. Если метка входа дуги равна нулю, назовем такую дугу нулевой, а если равна единице – единичной. Метка выхода дуги равна значению выходного сигнала автомата в состоянии, соответствующего вершине, из которого выходит данная дуга.

В общем случае из вершины v_j может выходить нулевая дуга e_0^{out} и единичная дуга e_1^{out} соответственно к вершинам v_0^{out} и v_1^{out}, а также могут входить нулевая дуга e_0^{in} и единичная дуга e_1^{in} соответственно от вершин v_0^{in} и v_1^{in} ($v_j, v_0^{out}, v_1^{out}, v_0^{in}, v_1^{in} \in V_{FA}$, $e_0^{out}, e_1^{out}, e_0^{in}, e_1^{in} \in E_{FA}$, $i = 0 \div n-1,\ j = 1 \div 2^r$).

Если вершине v_j в момент времени t поставить в соответствие состояние $S_j(t)$, а вершинам $v_0^{out}, v_1^{out}, v_0^{in}, v_1^{in}$ в моменты времени $(t-1)$ и $(t+1)$ поставить в соответствие состояния $S_0^{out}(t-1)$, $S_1^{out}(t-1)$, $S_0^{in}(t+1)$, $S_1^{out}(t+1)$ ЛПС, тогда между указанными состояниями существуют следующие зависимости:

$$\begin{aligned} &S_0^{out}(t+1) = A \times S_j(t), && S_j(t) = A \times S_0^{in}(t-1) \\ &S_1^{out}(t+1) = A \times S_j(t) + B, && S_j(t) = A \times S_1^{in}(t-1) + B, \qquad GF(2). \end{aligned} \quad (8)$$

Зависимости (8) непосредственно следуют из формулы (1).

Если ЛПС описывается характеристическими матрицами A и B типа Фибоначчи или типа Галуа и порождающий многочлен (5) циклического кода является примитивным, тогда граф G_{FA} имеет

следующую структуру: имеется одна вершина v_{null}, для которой входящая и выходящая нулевые дуги объединяются и образуют петлю, а остальные $2^r - 1$ вершин связаны последовательно нулевыми дугами. Будем полагать, что такой граф G_{FA}, состоит из тривиального нулевого цикла (ТНЦ), куда входит вершина v_{null}, и основного нулевого цикла (ОНЦ), куда входят все остальные вершины графа G_{FA}.

Если же порождающий многочлен (5) циклического кода является непримитивным, тогда граф G_{FA} содержит некоторое количество нулевых циклов (НЦ) длины не более n, образованных нулевыми дугами. Эти НЦ можно упорядочить по следующим уровням.

На нулевом уровне будет располагаться ТНЦ. Далее, на первом уровне находится ОНЦ длины n, который связан с ТНЦ парой противоположно направленных единичных дуг. Все остальные НЦ, которые будем именовать периферийными НЦ (ПНЦ), распределяются по следующим уровням таким образом. На втором уровне располагаются те ПНЦ, каждый из которых связан с ОНЦ парой единичных дуг. На ($\tau+1$)-ом уровне каждый ПНЦ имеет единичные дуги с НЦ τ-го уровня и отсутствуют единичные дуги с НЦ уровней ($\tau-1$) и менее (τ=1,2,3, …).

Более подробно многоуровневая графовая модель изложена в [5].

В графе G_{FA} последовательность из n нулевых и ненулевых дуг $e_0, e_1, \ldots, e_{n-1}$ ($e_i \in E_{FA}, i = 0 \div n-1$), которая начинается и заканчивается в вершине v_{null} (т.е. в ТНЦ), представляет собой кодовый путь η и соответствует кодовому вектору Z.

В канале связи с помехами на кодовый вектор Z накладывается вектор ошибок $R_{err}^{(\tau)}$, в результате чего получается кодовый вектор $Z_{err}^{(\tau)}$ с независимыми ошибками кратности τ.

$$Z_{err}^{(\tau)} = R_{err}^{(\tau)} + Z, \quad GF(2)$$

Кодовому вектору $Z_{err}^{(\tau)}$, содержащему τ независимых ошибок, будет соответствовать прямой кодовый путь ошибки η_{for}, который начинается в вершине v_{null}, и заканчивается в некоторой вершине ошибки v_{err}. Кодовый путь, который начинается в вершине ошибки v_{err}, и заканчивается в вершине v_{null}, будем называть обратным кодовым путем ошибки η_{rev}. Тот НЦ, который содержит вершину v_{err}, будем в дальнейшем именовать НЦ ошибки. Для независимой ошибки кратности τ НЦ ошибки находится на τ-м уровне графа G_{FA}.

В автоматной модели циклических кодов вершинам графа G_{FA}. соответствуют внутренние состояния ЛПС. Последовательность векторов внутренних состояний ЛПС, которые соответствуют вершинам одного НЦ в графе G_{FA}, также образуют цикл. Поскольку совокупность циклов из векторов состояний имеет такую же структуру, что и совокупность циклов из вершин, поэтому для их характеристики можно использовать те же термины: ТНЦ, ОНЦ и ПНЦ.

Под воздействием входного вектора Z ЛПС из нулевого начального состояния $S(0)$ перейдет в состояние $S(n)$, совпадающее с исходным состоянием, т.е. будет получен нулевой синдром: $S(n) = S(0)$. Под воздействием входного вектора $Z_{err}^{(\tau)}$ ЛПС из состояния $S(0)$ перейдет в некоторое ненулевое состояние $S_{err}^{(\tau)}(n)$, которое будем именовать синдромом ошибки кратности τ. Нетрудно показать, что вершина v_{null} графа G_{FA} соответствует состоянию $S(0)$ ЛПС, а вершина v_{err} – состоянию $S_{err}^{(\tau)}(n)$ ЛПС.

Для нахождения и исправления независимых ошибок необходимо построить обратный кодовый путь ошибки η_{rev} между вершинами v_{err} и v_{null} в терминах графовой модели или найти цепочку переходов от состояния $S_{err}^{(\tau)}(n)$ к состоянию $S(0)$ в терминах автоматной модели. Этот путь

строится через цепочку специальных опорных вершин, называемых конечными вертикальными связывающими вершинами (ВСВ).

Теперь рассмотрим особенности структуры графа G_{FA} для укороченных циклических кодов.

ВАРИАНТ 1. Пусть в n-разрядном кодовом векторе Z h укороченных разряда, заполненных нулями, находятся после ($k-h$) информационных разрядов:

$$Z = z_1\, z_2 \ldots z_{k-h}\, 0 \ldots 0\, z_{k+1} \ldots z_n \ .$$

Как при кодировании, так и процессе декодирования, необходимо пройти путь по графу G_{FA} длины n от вершины v_{null} снова в вершину v_{null}. И хотя заполненные нулями разряды $z_{k-h+1} \ldots z_k$ не несут полезной нагрузки, они участвуют в построении кодового пути, поэтому никакого выигрыша от укорочения мы не получаем.

ВАРИАНТ 2. Пусть в n_1-разрядном кодовом векторе Z h укороченных разряда, заполненных нулями, находятся в самом начале:

$$Z = 0 \ldots 0\, z_{h+1}\, z_{h+2} \ldots z_k\, z_{k+1} \ldots z_n \ .$$

В этом случае нулевые информационные разряды соответствуют нулевым дугам, исходящих из вершины v_{null}. Поскольку нулевые дуги образуют петлю вокруг вершины v_{null}, поэтому никакого движения по графу не происходит. Построение кодового пути начинается с первого ненулевого разряда z_{h+1}, следовательно, длина кодового пути составит $n-h$. Аналогично, при декодировании необходимо пройти путь по графу G_{FA} длины $n-h$. Таким образом, при втором варианте укорочения можно действительно отбросить начальные нулевые разряды кодового вектора и сократить продолжительность процедур кодирования и декодирования укороченного циклического кода.

Однако, при поиске ошибок в таких кодах получить экономию во времени не удается, если использовать для этого те же подходы, что и для полных кодов.

Поясним суть проблемы на графовой модели укороченного циклического кода. Все вершины графа G_{FA}, кроме вершины v_{null}, соответствуют синдромам независимых ошибок полного циклического кода. В укороченном ($n-h, k-h$)-коде количество ошибок будет меньше на величину 2^h. В каждом НЦ из n вершин всегда будет h вершин, которые будут соответствовать h укорачиваемым разрядам кода. Расположение этих вершин определяется местоположением укорачиваемым разрядам в кодовом векторе. Для варианта 2, который мы будем в дальнейшем рассматривать, указанные вершины имеют такую нумерацию: $n-h+1, n-h, \ldots, n$ (нумерацию будем вести с той вершины, в которую входит первая единичная дуга из НЦ предыдущего уровня).

В качестве примера рассмотрим случай с ошибкой в одном разряде кодового вектора, тогда вершина v_{err} будет находиться в ОНЦ. Для нахождения ошибки по графовой модели ЛПС [5], необходимо построить отрезок пути η_{rev} от вершины v_{err} к вершине v_n, которая связана единичной дугой с вершиной v_{null}, т.е. с ТНЦ (Рис.1). Длина отрезка пути η_{rev} и будет указывать на местоположение ошибочного разряда в кодовом векторе $Z_{err}^{(\tau)}$. Этот путь проходит по направлению нулевых дуг, поэтому он обязательно пройдет через h вершин, которые соответствуют укорачиваемым разрядам кодового вектора. Аналогичная ситуация будет и в других НЦ, через которые будет пролегать путь η_{rev}. Таким образом, неиспользуемые в кодовом векторе укорачиваемые разряды будут "участвовать" в процедуре поиска и исправления ошибок.

Такая же ситуация будет и при использовании автоматной модели ЛПС: при вычислении очередных состояний $S(t)$ будут использованы и состояния, соответствующие укорачиваемым разрядам кодового вектора, т.е. экономии времени не будет.

И все же решение этой проблемы возможно. Основная идея предлагаемого подхода состоит в использовании специального конечного автомата, способного функционировать по обратной шкале времени – обратной ЛПС.

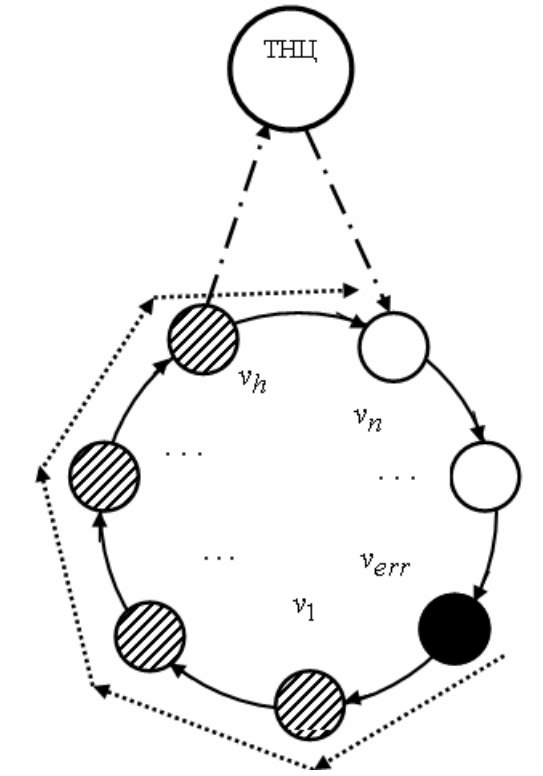

Рис. 1. Поиск кодового пути по графовой модели в прямом направлении (условные обозначения: сплошная линия – нулевые дуги,штрихпунктирная линия – ненулевые дуги, прерывистая линия – кодовый путь в прямом направлении, диагональной штриховкой обозначены вершины, соответствующие укорачиваемым разрядам кодового вектора)

ОБРАТНАЯ АВТОНОМНАЯ ЛПС ДЛЯ ЦИКЛИЧЕСКОГО КОДА

Для любой автономной ЛПС, определяемой функциями (6) и (7) можно построить обратную автономную ЛПС. Ограничимся пока циклическими кодами над полем $GF(2)$.

ОПРЕДЕЛЕНИЕ 3. Обратной автономной ЛПС Λ_{inv} над полем $GF(2)$ называется такая ЛПС, функционирование которой не зависит от входных воздействий и описывается функцией состояний (переходов)

$$S(t) = A_{inv} \times S(t+1), \qquad GF(2), \tag{9}$$

и функцией выходов

$$Y(t) = C \times S(t), \qquad GF(2). \tag{10}$$

Матрицу A_{inv} будем называть характеристической матрицей ЛПС Λ_{inv}.

Если обычная ЛПС Λ является линейным конечным автоматом, то обратная автономной ЛПС Λ_{inv} является обратным линейным конечным автоматом. В отличие от традиционного конечного автомата, который описывает свое функционирование по прямой шкале времени (от “прошлого” к “настоящему”), обратный конечный автомат описывает свое функционирование по обратной шкале времени (от “настоящего” к “прошлому”).

По прямому автомату всегда можно определить обратный автомат, и наоборот. Фактически прямой и обратный автоматы – это две стороны одного автомата, как и в [6], мы будем их рассматривать в неразрывном единстве.

Рассматриваемые автономные ЛПС реализуют очень простой закон функционирования, в котором отсутствуют какие-либо условия. Поэтому, в отличие от [6], для нахождения обратного автомата совсем не нужно хранить последовательность действий прямого автомата, следовательно, в

нашем случае отсутствует дополнительные затраты памяти. Для перехода от прямого автомата к обратному, или наоборот, необходимо лишь разработать способ перехода от известной матрицы A к матрице A_{inv}, либо от известной матрицы A_{inv} к матрице A.

ТЕОРЕМА 1. Для автономной ЛПС Λ с характеристической матрицей A типа Фибоначчи (3) обратная характеристическая матрица A_{inv} типа Фибоначчи обратной автономной ЛПС Λ_{inv} над полем $GF(2)$ имеет вид:

$$A_{inv} = \begin{vmatrix} g_1 & g_2 & \cdots & g_{r-1} & g_0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \cdots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{vmatrix}. \qquad (11)$$

Доказательство. Подставляя вектор $S(t+1)$ из формулы (6) в (9) получим:

$$S(t) = A_{inv} \times A \times S(t), \qquad GF(2). \qquad (12)$$

Равенство (12) будет справедливо, если произведение матриц A и Λ_{inv} ЛПС одного вида и размерности даст единичную матрицу E:

$$A_{inv} \times A = E, \qquad GF(2). \qquad (13)$$

В результате решения матричного уравнения (13) относительно известной матрицы A типа (3) и неизвестных элементов матрицы A_{inv} мы получим (11).

На основании Теоремы 1 можно сформулировать следующее правило перехода от матрицы A к матрице A_{inv}:

1) циклически сдвинуть влево первый столбец матрицы A,
2) в полученной матрице циклически сдвинуть вниз последнюю строку.

ТЕОРЕМА 2. Для автономной ЛПС Λ с характеристической матрицей A типа Галуа (4) обратная характеристическая матрица A_{inv} типа Галуа обратной автономной ЛПС Λ_{inv} над полем Галуа $GF(2)$ имеет вид:

$$A_{inv} = \begin{vmatrix} g_1 & 1 & 0 & \dots & 0 \\ g_2 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ g_{r-1} & 0 & 0 & \cdots & 1 \\ g_0 & 0 & 0 & \dots & 0 \end{vmatrix}. \qquad (14)$$

Доказательство Теоремы 2 аналогично доказательству Теоремы 1.

На основании Теоремы 2 можно сформулировать следующее правило перехода от матрицы A к матрице A_{inv}:

3) циклически сдвинуть вверх первую строку матрицы A,
4) в полученной матрице циклически сдвинуть вправо последний столбец.

ПРИМЕР 1. Характеристические матрицы ЛПС типа Фибоначчи (A_1) и типа Галуа (A_2) на основе порождающего многочлена $g(x) = 1 + x + x^3$ имеют следующий вид:

$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}; \qquad A_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Найдем характеристическую матрицу $A_{inv,1}$ типа Фибоначчи обратной ЛПС:

$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = A_{inv,1}.$$

Аналогично найдем характеристическую матрицу $A_{inv,2}$ типа Галуа обратной ЛПС:

$$A_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = A_{inv,2}.$$

АВТОМАТНОЕ И ГРАФОВОЕ ПРЕДСТАВЛЕНИЯ УКОРОЧЕННЫХ КОДОВ РИДА-СОЛОМОНА

Для представления кодов Рида-Соломона также можно использовать графовую и автоматную модели, только, в отличии от двоичных циклических кодов, эти модели имеют большую сложность. Например, на первом уровне графа G_{FA} находится не один ОНЦ длины n, а n ОНЦ длины n. Соответственно увеличивается и количество ПНЦ, но всех их можно упорядочить по уровням.

ОПРЕДЕЛЕНИЕ 4. Автономной ЛПС над полем Галуа $GF(q)$ называется такая ЛПС, функционирование которой не зависит от входных воздействий и описывается функцией состояний (переходов)

$$S(t+1) = A \times S(t), \qquad GF(q), \tag{15}$$

и функцией выходов

$$Y(t) = C \times S(t), \qquad GF(q). \tag{16}$$

Порождающий многочлен кода РС, позволяющего исправлять $\tau_{\min}$ ошибок, обычно задается через корни последовательности степеней α^i примитивного элемента α поля $GF(q)$:

$$g(x) = (x-\alpha)(x-\alpha^2)\ldots(x-\alpha^{2\tau_{\min}}), \tag{17}$$

Если порождающий полином (17) преобразовать к виду

$$g(x) = \alpha_0^i + \alpha_1^i X + \alpha_2^i X^2 + \ldots + \alpha_{r-1}^i X^{r-1} + X^r, \quad r = 2\tau_{\min}, \tag{18}$$

тогда матрицы ЛПС типа Фибоначчи над полем $GF(q)$ можно записать следующим образом:

$$A = \begin{vmatrix} 0 & \alpha^0 & 0 & \ldots & 0 \\ 0 & 0 & \alpha^0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_0^i & \alpha_1^i & \alpha_2^i & \ldots & \alpha_{r-1}^i \end{vmatrix}, \; B = \begin{vmatrix} 0 \\ 0 \\ 0 \\ \ldots \\ \alpha^0 \end{vmatrix}, \; i = 0,1,2,\ldots,n-1. \tag{19}$$

и матрицы ЛПС типа Галуа над полем $GF(q)$ можно записать следующим образом:

$$A=\begin{vmatrix} 0 & 0 & \cdots & 0 & \alpha_0^i \\ \alpha^0 & 0 & \cdots & 0 & \alpha_1^i \\ 0 & \alpha^0 & \cdots & 0 & \alpha_2^i \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \alpha^0 & \alpha_{r-1}^i \end{vmatrix}, \quad B=\begin{vmatrix} \alpha^0 \\ 0 \\ 0 \\ \cdots \\ 0 \end{vmatrix}, \quad i=0,1,2,\ \ldots, n-1 \tag{20}$$

По аналогии с Определением 3 определим обратную автономную ЛПС Λ_{inv} над полем $GF(q)$.

ОПРЕДЕЛЕНИЕ 5. Обратной автономной ЛПС Λ_{inv} над полем $GF(q)$ называется такая ЛПС, функционирование которой не зависит от входных воздействий и описывается функцией состояний (переходов)

$$S(t) = A_{inv} \times S(t+1), \qquad GF(q), \tag{21}$$

и функцией выходов

$$Y(t) = C \times S(t), \qquad GF(2q). \tag{22}$$

Теперь найдем структуру обратной характеристической матрицы A_{inv} для таких ЛПС.

ТЕОРЕМА 3. Для автономной ЛПС Λ с характеристической матрицей A типа Фибоначчи (19) характеристическая матрица A_{inv} типа Фибоначчи обратной автономной ЛПС Λ_{inv} над полем $GF(q)$ имеет вид:

$$A_{inv}=\begin{vmatrix} \beta_0^i & \beta_1^i & \ldots & \beta_{r-2}^i & \beta_{r-1}^i \\ \alpha^0 & 0 & \ldots & 0 & 0 \\ 0 & \alpha^0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \alpha^0 & 0 \end{vmatrix}, \tag{23}$$

где элементы первой строки матрицы (23) определяются через элементы последней строки матрицы (19) следующим образом:

$$\beta_{r-1}^i = \frac{\alpha^0}{\alpha_0^i}, \quad \beta_j^i = \frac{\alpha_{j+1}^i}{\alpha_0^i} \quad для\ j=0,1,\ldots,r-2.$$

ТЕОРЕМА 4. Для автономной ЛПС Λ с характеристической матрицей A типа Галуа (20) характеристическая матрица A_{inv} типа Галуа обратной автономной ЛПС Λ_{inv} над полем $GF(q)$ имеет вид:

$$A_{inv}=\begin{vmatrix} \beta_0^i & \alpha^0 & 0 & \ldots & 0 \\ \beta_1^i & 0 & \alpha^0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta_{r-2}^i & 0 & 0 & \cdots & \alpha^0 \\ \beta_{r-1}^i & 0 & 0 & \ldots & 0 \end{vmatrix}. \tag{24}$$

где элементы первого столбца матрицы (24) определяются через элементы последнего столбца матрицы (20) следующим образом:

$$\beta^i_{r-1} = \frac{\alpha^0}{\alpha^i_0}\ , \quad \beta^i_j = \frac{\alpha^i_{j+1}}{\alpha^i_0} \quad для\ j = 0,1,\ldots,r-2\,.$$

Доказательство Теорем 3 и 4 аналогично доказательству Теорем 1 и 2.

Правила перехода от матрицы A к матрице A_{inv} соответствующего типа над полем Галуа $GF(q)$ такое же, как и над полем Галуа $GF(2)$.

ПРИМЕР 2. Характеристические матрицы ЛПС типа Фибоначчи (A_1) и типа Галуа (A_2) на основе порождающего многочлена $g(x) = \alpha^3 + \alpha^1 x + \alpha^0 x^3 + \alpha^3 x^4$ над полем $GF(8)$ имеют следующий вид:

$$A_1 = \begin{vmatrix} 0 & \alpha^0 & 0 & 0 \\ 0 & 0 & \alpha^0 & 0 \\ 0 & 0 & 0 & \alpha^0 \\ \alpha^3 & \alpha^1 & \alpha^0 & \alpha^3 \end{vmatrix} \qquad A_2 = \begin{vmatrix} 0 & 0 & 0 & \alpha^3 \\ \alpha^0 & 0 & 0 & \alpha^1 \\ 0 & \alpha^0 & 0 & \alpha^0 \\ 0 & 0 & \alpha^0 & \alpha^3 \end{vmatrix}$$

Характеристические матрицы $A_{inv,1}$ и $A_{inv,2}$ соответственно обратной ЛПС типа Фибоначчи и обратной ЛПС типа Галуа имеют следующий вид:

$$A_{inv,1} = \begin{vmatrix} \alpha^5 & \alpha^4 & \alpha^0 & \alpha^4 \\ \alpha^0 & 0 & 0 & 0 \\ 0 & \alpha^0 & 0 & 0 \\ 0 & 0 & \alpha^0 & 0 \end{vmatrix} \qquad A_{inv,2} = \begin{vmatrix} \alpha^5 & \alpha^0 & 0 & 0 \\ \alpha^4 & 0 & \alpha^0 & 0 \\ \alpha^0 & 0 & 0 & \alpha^0 \\ \alpha^4 & 0 & 0 & 0 \end{vmatrix}$$

МЕТОД ПОИСКА ОШИБОК В УКОРОЧЕННЫХ КОДАХ РИДА-СОЛОМОНА

Общая стратегия поиска независимых ошибок в кодах Рида-Соломона подробно изложена в [7]. Здесь лишь отметим ее особенности для укороченных кодов Рида-Соломона.

В течение первых n_1 тактов происходит процесс декодирования полученного кодового вектора,

$$S(t+1) = A \times S(t) + B \times U(t), \qquad GF(2) \tag{25}$$

который заканчивается вычислением синдрома $S(n_1)$, т.е. последнего состояния ЛПС.

Если в качестве входного вектора в (25) используется кодовый вектор $Z^{(\tau)}_{err}$ с независимыми ошибками кратности τ, тогда мы получаем ненулевой синдром ошибки $S^{(\tau)}_{err}(n_1)$, и далее начинается процесс определения параметров возникших ошибок.

Как уже ранее отмечалось, для этого необходимо построить обратный кодовый путь ошибки η_{rev} через множество опорных вершин – конечных ВСВ. Часть конечных ВСВ являются регулярными, т.е. имеют простую структуру и их не нужно заранее вычислять и хранить.

В автоматной модели кодов Рида-Соломона конечной ВСВ соответствует конечное вертикальное связывающее состояние (ВСС). Для вычисления конечных ВСС не используются входные воздействия, т.е. мы фактически работаем либо с автономной ЛПС по формулам (15) и (16), либо с обратной автономной ЛПС по формулам (21) и (22). При нахождении регулярного конечного ВСС очень быстро определяется вектор ошибок $R^{(\tau)}_{err}$, в противном случае продолжается итеративный процесс либо нахождения последующих регулярных конечных ВСС, либо сравнения очередного состояния $S(t)$ ЛПС с хранимыми нерегулярными конечными ВСС.

Снова вернемся к графовой модели кодов Рида-Соломона. Если произошла ошибка кратности τ,

тогда обратный кодовый путь ошибки η_{rev} проходит через τ НЦ. В каждом из этих НЦ имеются свои конечные ВСВ и только одна из них может быть регулярной ВСВ. Задача состоит в поиске наикратчайшего отрезка пути в данном НЦ к регулярной ВСВ, либо к другой ВСВ при отсутствии регулярной.

Традиционный способ решения этой задачи состоит в построении пути по направлению нулевых дуг. Неэффективность такого способа очень хорошо видна именно в случае укороченных кодов. В известных укороченных кодах Рида-Соломона используется лишь около 10% кодовых комбинаций. Если конечная ВСВ находится перед вершиной ошибки v_{err}, тогда по прямым дугам придется обойти почти весь НЦ длины n. Очевидным решением этой проблемы является движение от вершины ошибки v_{err} в обратном направлении (Рис. 2).

В автоматной модели этому способу соответствует применение обратной ЛПС. Использование обратной ЛПС позволит значительно сократить продолжительность процедуры поиска ошибок.

Естественно заметить, что заранее неизвестно взаимное расположение конечных ВСВ и вершины ошибки v_{err}, и в ряде случаев прямой путь окажется короче.

Предлагается строить внутри НЦ оба пути (в прямом и обратном направлении), но делать это не последовательно, а параллельно. Процесс построения обоих отрезков путей стартует одновременно, и, если более короткий отрезок пути будет найден, построение второго отрезка пути прекращается. Параллельный подход может быть распространен и на весь обратный кодовый путь ошибки η_{rev}, т.е. можно попытаться одновременно строить пути через различные НЦ.

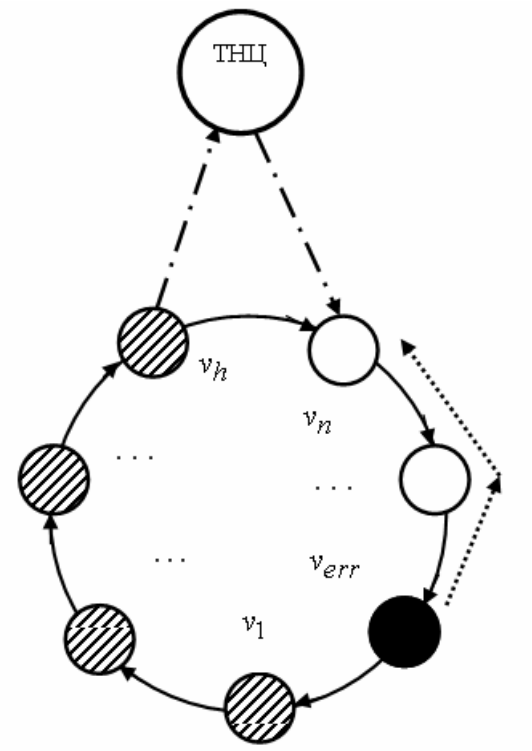

Рис. 2. Поиск кодового пути по графовой модели в обратном направлении

Теперь дадим интерпретацию параллельной обработки в автоматной модели: одновременное использование прямой и обратной ЛПС, одновременный поиск регулярных и нерегулярных конечных ВСС. Регулярные ВСС определяются по их структуре (количеству нулевых символов), а нерегулярные ВСС ищутся среди множества заранее вычисленных.

ВЫВОДЫ

В работе показано, что для представления укороченных циклических кодов над полем Галуа $GF(2)$ и укороченных кодов Рида-Соломона может быть использована многоуровневая графовая и автоматная модели на основе теории линейных последовательностных схем (ЛПС). Впервые введены понятия обратных

автономных ЛПС различных видов, которые могут функционировать по обратной шкале времени.

Использование обратной ЛПС позволит использовать дополнительную избыточность укороченных кодов и значительно сократить для них продолжительность процедуры поиска ошибок. Еще большего выигрыша во времени можно достичь при использовании параллельной обработки данных на различных этапах поиска ошибок. Предложенные подходы могут быть использованы и для полных циклических кодов.

Полученные результаты могут иметь значения в различных сферах, где используются укороченные коды Рида-Соломона, например, для ускорения считывания информации в оптических дисках.

СПИСОК ЛИТЕРАТУРЫ

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение: / Б. Скляр. Изд. 2-е, испр. – М.: Издательский дом “Вильямс”, 2004. – 1104 с.
2. Hankerson D.R. Coding Theory and Cryptography. The Essentials / D. R. Hankerson, D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall. Second Edition, Revised and Expanded. – New York, CRC Press. – 2000. – 350 p.
3. Блейхут Р. Теория и практика кодов, исправляющих ошибки: / Р. Блейхут. – М.: Мир, 1986. – 576 с.
4. Гилл А. Линейные последовательностные машины: / А. Гилл. – М.: Наука, 1974. – 288 с.
5. Семеренко В. П. Высокопроизводительные алгоритмы для исправления независимых ошибок в циклических кодах // Системи обробки інформації: зб. наук. пр. – Харків: ХУПС, 2010. – Вип. 3(84). – С. 80-89.
6. Казаков М.А. Разработка логики визуализаторов алгоритмов на основе конечных автоматов: / М.А. Казаков, Г.А. Корнеев, А.А. Шалыто. Телекоммуникации и информатизация образования. 2003. – № 6. – С. 27–58.
7. Семеренко В. П. Декодирование кодов Рида-Соломона на основе графовой и автоматной моделей // Электронное моделирование. – 2011. – № 1. – С. 57-72.

Надійшла до редакції 19.06.2012р.

СЕМЕРЕНКО ВАСИЛЬ ПЕТРОВИЧ - к.т.н., доцент, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, Україна, тел.: +38(0432) 598379, E-mail: *vpsemerenko@mail.ru*.