3. *Manfred Schimmler, Viktor Bunimov, Boris Tolg. Area-Time-Efficient Montgomery Modular Multiplication. http://www.ece.rochester.edu/~albonesi/wced02/slides/bunimov.pdf.* ***4.*** *Jhing-Fa Wang, Po-Chuan Lin, Ping-Kun Chiu. A Staged Carry-Save-Adder Array for Montgomery Modular Multiplication. http://www.ap-asic.org/2002/proceedings/2B/2B-5.PDF.* ***5.*** *Koon-Shik Cho, Je-Hyuk Ryu, Jun-Dong Cho. High-Speed Modular Multiplication Algorithm for RSA Cryptosystem. http://vada.skku.ac.kr/Research/published/final_rsa1024_koonshik.pdf.* ***6.*** *Sungwook Kim, Gerald E. Sobelman. Digit-Serial Modular Multiplication Using Skew-Tolerant Domino Cmos. http://www-mount.ee.umn.edu/~sobelman/papers/skim_icassp01.pdf.* ***7.*** *Konrad Walus. Montgomery Modular Multiplication Method For Exponention Tutorial. http://people.atips.ca/~walus/Mont/montgomery.html.* ***8.*** *D. J. Guan. Montgomery Algorithm for Modular Multiplication http://guan.cse.nsysu.edu.tw/data/montg.pdf.* ***9.*** *Kazuo Sakiyama, Sungha Kim. An FPGA implementation and Performance Evaluation of Modular Multiplication Operation for RSA Cryptography algorithm. http://www.ee.ucla.edu/~kazuo/cs252apj.pdf.* ***10.*** *Colin D. Walter. Space/Time Trade-Offs for Higher Radix Modular Multiplication Using Repeated Addition. http://islab.oregonstate.edu/documents/Papers/t0139.pdf.* ***11.*** *Alvaro Bernal, Alain Guyot. Hardware for Computing Modular Multiplication Algorithm. http://www.math.ucalgary.ca/~kjell/papers/hardware/hardware-for-computing-modular.pdf.* ***12.*** *Jean-Claude Bajard, Laurent-Stéphane Didier, and Peter Kornerup. An RNS Montgomery Modular Multiplication Algorithm. http://www.math.ucalgary.ca/~kjell/papers/hardware/TCmultmod.pdf.*

УДК 621.391:519.27

ДЕКОДИРОВАНИЕ ПАКЕТОВ ОШИБОК В ПРОСТРАНСТВЕННО-ВРЕМЕННЫХ ЦИКЛИЧЕСКИХ КОДАХ

Василий Семеренко
Винницкий национальный технический университет

Анотація: **Пропонується новий клас циклічних кодів для бездротових систем зв'язку: просторово-часові циклічні коди (ПЧЦК). Досліджується кодування і декодування ПЧЦК на основі діаграми переходів лінійної послідовнісної машини. Розглядається алгоритм пошуку поодиноких пакетів помилок довільної довжини за допомогою ПЧЦК.**

Summary: **The new class of cyclic codes for wireless systems of communication is proposed: space- time cyclic codes (STCC). The coding and decoding STCC is investigated on the basis of the diagram of transitions of the linear sequential circuit. The algorithm of search of single burst errors of any length with the help STCC is considered.**

Ключові слова **Диверсификация, пространственно-временные коды, циклические коды, линейная последовательностная машина, пакеты ошибок, графы.**

Введение

Одной из самых важных задач в области телекоммуникаций является внедрение беспроводных систем связи [1].

Значительно увеличить пропускную способность таких систем связи позволяют различные методы диверсификации. Основная идея пространственной диверсификации заключается в повышении производительности передачи путем создания нескольких независимых путей сигналов между передатчиком и приемником с помощью нескольких передающих и приемных антенн [2]. Однако, использование нескольких параллельных путей передачи сигналов вызывает их взаимную интерференцию. Кроме этого недостатка, для беспроводных каналов характерны большие потери мощности, различные нелинейности, а отношение сигнал/шум становится случайной величиной.

Решением этих проблем является применение временной диверсификации на основе кодирования информации. Использование специальных методов кодирования позволяет организовать эффективную защиту передаваемой информации. Совместное использование кратных антенн и контролирующих кодов позволит ускорить практическое применение систем сотовой связи третьего поколения, в частности технологии CDMA [3].

За последние годы предложено много видов пространственно-временных кодов [4, 5]. Однако и широко известные коды, применяемые для передачи одним путем, могут быть обобщены для беспроводных систем связи с несколькими антеннами. Предлагается новая разновидность циклических кодов для передачи по каналам связи с несколькими антеннами – пространственно-временные циклические коды (ПВЦК).

I Математические основы пространственно-временных циклических кодов

Для описания ПВЦК, как и для традиционных циклических кодов, можно применить известные способы: полиномиальный (на основе порождающих многочленов), матричный (на основе порождающей или проверяющей матрицы) [6] либо на основе теории линейной последовательностной машины (ЛПМ) [7].

Словосочетание ЛПМ является не самым удачным переводом оригинального английского термина "linear sequential circuit", но, в силу сложившихся традиций, будем в дальнейшем его придерживаться. Неудачным является также и термин "фильтр" [8].

Математический аппарат ЛПМ является наиболее подходящим для ПВЦК, поскольку уже фактически содержит весь теоретический базис для таких кодов. Кодер и декодер пространственно-временного циклического $(m \times (n,k))$-кода представляют по сути m –входовую z-выходную ЛПМ, которая над полем Галуа $GF(q)$ задается функцией состояний (переходов)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(q),$$

и функцией выходов

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

где $A = \|a_{ij}\|_{r\times r}$, $B = \|b_{ij}\|_{r\times m}$, $C = \|c_{ij}\|_{z\times r}$, $D = \|d_{ij}\|_{z\times m}$ – характеристические матрицы ЛПМ;

$U(t) = \|u_j\|_m$ – вектор входных сигналов; $S(t) = \|s_i\|_r$ – вектор состояний, $r = n - k$.

Для практической реализации кодирования и декодирования с помощью ПВЦК можно ограничиться m – входовой одновыходной ЛПМ над полем Галуа $GF(2)$ в виде модели автомата Мура, для описания смены состояний в которой удобно пользоваться следующими формулами:

$$S(t+1) = \begin{cases} A \times S(t), \text{ если } U(t) - \textit{нулевой вектор} - \textit{столбец} \\ A \times S(t) + U(t), \text{ если } U(t) - \textit{ненулевой вектор} - \textit{столбец} \end{cases} GF(2),$$

В дальнейшем все вычисления относятся к полю Галуа $GF(2)$ и могут быть легко обобщены и для полей Галуа $GF(q)$, $q > 2$.

В настоящее время достаточно изучены и широко используются различные устройства на основе модели одновходовой ЛПМ. Поэтому целесообразно максимально использовать весь ранее накопленный теоретический материал для новых видов кодов. Такой подход вполне возможен при использовании специальных видов характеристических матриц ЛПМ.

Основной критерий в выборе матриц A и B состоит в необходимости обеспечения *r*-управляемости ЛПМ, т. е. возможности перехода из любого состояния S_i в состояние S_j не более, чем за *r* тактов работы автомата. Как показано в [7], ЛПМ является *r*-управляемой только в том случае, если $(n \times (r,m))$-матрица

$$L_{r,m} = \left\| A^{r-1} \times B, A^{r-2} \times B, \text{ К } , A \times B, B \right\| \qquad GF(2)$$

имеет ранг *r*.

При аппаратной реализации ЛПМ наиболее удобно использовать следующие два вида матриц A и B, которые удовлетворяют условию *r* –управляемости ЛПМ:

$$A = \begin{Vmatrix} 0 & 0 & 0 & \Lambda & 0 & p_0 \\ 1 & 0 & 0 & \Lambda & 0 & p_1 \\ 0 & 1 & 0 & \Lambda & 0 & p_2 \\ \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda \\ 0 & 0 & 0 & \Lambda & 0 & p_{r-2} \\ 0 & 0 & 0 & \Lambda & 1 & p_{r-1} \end{Vmatrix}, \quad B = \begin{Vmatrix} b_1 & 0 & \Lambda & 0 & \Lambda & 0 \\ 0 & b_2 & \Lambda & 0 & \Lambda & 0 \\ \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda \\ 0 & 0 & \Lambda & b_m & \Lambda & 0 \\ \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda \\ 0 & 0 & \Lambda & 0 & \Lambda & b_r \end{Vmatrix}, \tag{1}$$

или

$$A=\begin{Vmatrix} 0 & 1 & 0 & \Lambda & 0 & 0 \\ 0 & 0 & 1 & \Lambda & 0 & 0 \\ 0 & 0 & 0 & \Lambda & 0 & 0 \\ \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda \\ 0 & 0 & 0 & \Lambda & 0 & 1 \\ p_0 & p_1 & p_2 & \Lambda & p_{r-2} & p_{r-1} \end{Vmatrix},\quad B=\begin{Vmatrix} 0 & 0 & \Lambda & 0 & \Lambda & b_r \\ \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda \\ 0 & 0 & \Lambda & b_m & \Lambda & 0 \\ \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda \\ 0 & b_2 & \Lambda & 0 & \Lambda & 0 \\ b_1 & 0 & \Lambda & 0 & \Lambda & 0 \end{Vmatrix}, \qquad (2)$$

где $b_1 = \Lambda = b_m = 1, b_{m+1} = \Lambda = b_r = 0$.

Элементы в последнем столбце матрицы A из (1) и элементы последней строки матрицы A из (2) представляют собой коэффициенты порождающего многочлена

$$P(x) = p_0 + p_1 x + p_2 x^2 + \Lambda + p_{r-2} x^{r-2} + p_{r-1} x^{r-1}, \qquad GF(2) \qquad (3)$$

Для *m*-входовой ЛПМ $(r \times r)$ матрица B из (1) и из (2) имеет *m* ненулевых строк и столбцов $(m \le r)$.

II Графовые модели пространственно-временных циклических кодов

Так как корректирующие свойства циклических кодов непосредственно связаны со структурой диаграммы переходов ЛПМ, то проведем ее краткий анализ для выбранных типов характеристических матриц A и B.

Полная диаграмма переходов *m* – входовой ЛПМ представляет собой сильносвязный граф $G(V, E)$, где V – множество вершин, а E – множество дуг. Из каждой вершины $v_i (v_i \in V)$ выходит 2^m дуг и входит 2^m дуг. Дуга e^σ, направленная от вершины v_i к вершине v_j $(e^\sigma \in E, v_i, v_j \in E)$, будет принадлежать к классу σ входящих и выходящих дуг, если соответствующие указанным вершинам состояния $S_i(t)$ и $S_j(t+1)$ ЛПМ связаны между собой соотношением

$$S_j(t+1) = A \times S_i(t) + B \times U^{(\sigma)}(t), \qquad GF(2)$$

где $U^{(\sigma)}(t)$ – вектор-столбец с σ-м вариантом двоичного набора сигналов, поступающих на m входов ЛПМ в момент времени t ($\sigma = 0 \div 2^m$).

Из графа G можно выделить 2^m несвязных ориентированных подграфов, в каждом из которых вершины связаны между собой только дугами одного класса. Для задач кодирования и декодирования практический смысл имеют только два следующих подграфа.

В первом подграфе графа G (будем называть его нулевым подграфом) вершины связаны дугами класса $\sigma = 0$ (будем называть их нулевыми), которые соответствуют отсутствию сигналов на всех входах ЛПМ. От вершины v_i к вершине v_j $(e^\sigma \in E, v_i, v_j \in E)$ будет направлена нулевая дуга, если соответствующие указанным вершинам состояния $S_i(t)$ и $S_j(t+1)$ ЛПМ связаны между собой соотношением

$$S_j(t+1) = A \times S_i(t), \qquad GF(2) \qquad (4)$$

Формула (4) полностью совпадает с формулой, которая задает функцию состояний (переходов) одновходовой ЛПМ, у которой отсутствуют единичные дуги.

Подграф с отсутствующими единичными дугами является диаграммой переходов автономной ЛПМ (АЛПМ) и представляет собой множество несвязанных между собой нулевых циклов (НЦ). Структура этого множества НЦ определяется свойствами порождающего многочлена (3) характеристических матриц АЛПМ.

Если этот многочлен принадлежит максимальному показателю $f_{\max}$ ($f_{\max} = 2^r - 1$), то неповторяющаяся последовательность кодов внутренних состояний АЛПМ имеет максимальный период $T = 2^r - 1$, а ее диаграмма переходов имеет следующую структуру: имеется одна вершина, для которой входящая и выходящая нулевые дуги образуют петлю, и $(2^r - 1)$ вершин, которые последовательно связаны

нулевыми дугами. По терминологии из [9], которой будем придерживаться, такой подграф состоит из одного тривиального нулевого цикла (ТНЦ) длины 1 и основного нулевого цикла (ОНЦ) длины ($2^r - 1$).

Добавим к этому подграфу две единичные дуги из множества E графа G для связывания между собой ТНЦ и ОНЦ и обозначим полученный граф как $G^{(0)}(V^{(0)}, E^{(0)})$, где $V^{(0)} = V$, $E^{(0)} \subseteq E$.

Если порождающий многочлен не принадлежит максимальному показателю $f_{\max}$, то диаграмма переходов АЛПМ имеет большее число НЦ, но меньшей длины: обычно длина НЦ равна длине n кода или кратна числу n. Снова добавим к АЛПМ некоторое количество единичных дуг из множества E графа G для связывания и упорядочения всех НЦ. В полученном графе, также обозначенном как $G^{(0)}(V^{(0)}, E^{(0)})$, НЦ будут располагаться по уровням следующим образом: на нулевом уровне – ТНЦ, на первом уровне – ОНЦ, на втором уровне – только те НЦ, которые связаны единичными дугами с ОНЦ. Далее последовательно формируются новые уровни таким образом, чтобы на i-ом уровне находились только те НЦ, которые были бы связаны хотя бы одной парой противоположно направленных единичных дуг с НЦ (i-1)-го уровня. НЦ, начиная со второго уровня, будем именовать периферийными НЦ (ПНЦ). Алгоритм упорядочения НЦ по уровням полностью совпадает с алгоритмом упорядочения для одновходовых ЛПМ [9].

Во втором подграфе графа G (будем называть его единичным подграфом) вершины связаны дугами класса σ=1 (будем называть их единичными), которые соответствуют наличию сигнала только на одном из m входов ЛПМ. От вершины v_i к вершине $v_j, (e^{\sigma} \in E, v_i, v_j \in E)$ будет направлена единичная дуга, если соответствующие указанным вершинам состояния $S_i(t)$ и $S_j(t+1)$ ЛПМ связаны между собой соотношением

$$S_j(t+1) = A \times S_i(t) + B \times U^{(1)}(t) \qquad GF(2), \tag{5}$$

где $U^{(1)}(t)$ – вектор-столбец с двоичным набором сигналов с одной единицей, поступающих на m входов ЛПМ в момент времени t.

Для приведенных выше характеристических матриц В вида (1) или (2) формулу (5) можно записать проще:

$$S_j(t+1) = A \times S_i(t) + U^{(1)}(t) \qquad GF(2). \tag{6}$$

Единичный подграф графа G также представляет собой множество несвязанных между собой единичных циклов (ЕЦ), структура которого определяется свойствами порождающего многочлена (3) характеристических матриц ЛПМ.

Добавим к этому подграфу несколько нулевых дуг из множества E графа G для связывания всех ЕЦ между собой и обозначим полученный граф как $G^{(1)}(V^{(1)}, E^{(1)})$, где $V^{(1)} = V$, $E^{(1)} \subseteq E$.

Если этот многочлен принадлежит максимальному показателю $f_{\max}$, тогда граф $G^{(1)}$ будет состоять из тривиального ЕЦ (ТВЦ) длины 1 и основного ЕЦ (ОЕЦ) длины ($2^r - 1$).

Если порождающий многочлен не принадлежит максимальному показателю $f_{\max}$, граф $G^{(1)}$ будет состоять из ТВЦ длины 1, ОЕЦ длины n и некоторого количества периферийных ЕЦ (ПЕЦ) длины n или кратных числу n и упорядоченных по уровням, аналогично ПНЦ.

Поскольку вектор-столбец $U^{(1)}(t)$ из (6) совпадает с характеристической матрицей-вектором B одновходовой ЛПМ, то единичный подграф графа G эквивалентен подграфу переходов одновходовой ЛПМ, у которой отсутствуют нулевые дуги.

Эквивалентность графовых моделей нулевого и единичного подграфов графа G графовой модели одновходовой ЛПМ позволяет использовать свойства последней для изучения многовходовых ЛПМ. Свойство эквивалентности не будет нарушено и при переходе к графам $G^{(0)}$ и $G^{(1)}$.

III Кодирование пространственно-временных циклических кодов

Основная стратегия кодирования для ПВЦК остается такой же, как и для обычных циклических кодов.

Имеется некоторая информационная последовательность $I_m(x)$ сигналов, предназначенных для

передачи по m независимым путям канала связи. При подаче на m входов ЛПМ с матрицей управляемости $L_{k,m}$ последовательности $I_m(x)$ длины k произойдет переход ЛПМ из начального состояния $S_{beg}(0)$, обычно нулевого состояния $S(0)$, в состояние $S(k)$, определяемое из уравнения

$$S(k) = L_{k,m} \times I_m(x) + A^k \times S_{beg}(0), \qquad GF(2) \tag{7}$$

где $L_{k,m} = \left\| A^{k-1} \times B, A^{k-2} \times B, \text{ K }, A \times B, B \right\| \qquad GF(2)$.

Необходимо определить такую контрольную последовательность $R_m(x)$ длины *r*, при подаче которой на m входов ЛПМ произойдет ее переход из состояния (7) в состояние $S_{end}(0)$, совпадающее с начальным состоянием $S_{beg}(0)$:

$$S_{end}(0) = S_{beg}(0),\ n = k + r. \tag{8}$$

Последовательность $I_m(x)$ представляет собой $(m \times k)$-матрицу, а последовательность $R_m(x)$ – $(m \times r)$-матрицу. Конкатенация матриц $I_m(x)$ и $R_m(x)$ образует $(m \times n)$-матрицу кодовой последовательности $C_m(x)$, которая и передается по каналу связи:

$$C_m(x) = I_m(x) R_m(x).$$

Процедура нахождения контрольной последовательности $R_m(x)$ является обобщением алгоритма кодирования циклических кодов на основе одновходовой ЛПМ [10].

Отличительной особенностью ПВЦК является структура последовательности $R_m(x)$. В минимальном варианте для подтверждения факта безошибочной передачи данных по каналу связи достаточно лишь одной строки матрицы $R_m(x)$. Однако, для повышения надежности процесса передачи можно либо сделать все строки матрицы $R_m(x)$ одинаковыми, либо четные строки сделать одинаковыми, а нечетные – нулевыми.

IV Декодирование пространственно-временных циклических кодов

После получения из канала связи переданной кодовой последовательности $C_m(x)$ необходимо далее подать ее на m входов ЛПМ такой же структуры, которая использовалась при кодировании ПВЦК. При отсутствии заданного класса ошибок ЛПМ из известного начального состояния $S_{beg}(0)$ должна снова перейти в это же состояние для обеспечения равенства (8). При наличии ошибок в переданной кодовой последовательности, которую обозначим как $C_{err}(x)$, ЛПМ перейдет в некоторое состояние, именуемое по традиции синдромом независимых ошибок $S_{err}(n)$.

Рассмотрим особенности декодирования и локализации одиночных пакетов ошибок ПЦВК с помощью их графовых моделей.

Будем различать такие виды одиночных пакетов ошибок:

- i-й “горизонтальный” пакет ошибок длины λ, представляющий собой циклически непрерывную последовательность из λ искаженных разрядов i-й строки матрицы $C_{err}(x)$ ($i = 1 \div m$, $m \le r$);

- j-й “вертикальный” пакет ошибок длины λ, представляющий собой циклически непрерывную последовательность из λ искаженных разрядов j-го столбца матрицы $C_{err}(x)$ ($j = 1 \div n$).

При наличии “горизонтального” пакета ошибок длины λ в матрице $C_{err}(x)$ ЛПМ перейдет в некоторое состояние, которое будем именовать синдромом “горизонтального” пакета ошибки $S^{\lambda}_{err,g}(n)$. При наличии “вертикального” пакета ошибок длины λ в матрице $C_{err}(x)$ ЛПМ перейдет в некоторое состояние, которое будем именовать синдромом “вертикального” пакета ошибки $S^{\lambda}_{err,v}(n)$.

Задача декодирования всех классов ошибок состоит в поиске по графовой модели ЛПМ пути от вершины v_{err}, соответствующей состоянию синдрома ошибки, к вершине v_0, соответствующей начальному

состоянию $S_{beg}(0)$ ЛПМ. При этом для поиска независимых ошибок лучше использовать граф $G^{(0)}$, а для поиска пакетов ошибок – граф $G^{(1)}$.

Нахождение вершины v_{err} в графе $G^{(1)}$ зависит от вида пакета ошибки. "Горизонтальные" пакеты ошибок, которые начинаются с первой позиции первой строки матрицы $C_{err}(x)$, попадают в ОЕЦ. "Горизонтальные" пакеты ошибок, которые начинаются с j-ой позиции первой строки матрицы $C_{err}(x)$, попадают в тот ПЕЦ, который находится на расстоянии (j–1) нулевых дуг от ОЕЦ. Указанные (j–1) нулевые дуги образуют один из НЦ. Следовательно, путь от вершины v_0 к вершине v_{err}, и наоборот, будет происходить поочередно по совокупности взаимосвязанных ЕЦ и НЦ.

Задача локализации одиночного пакета ошибок сводится к нахождению кратчайшего пути вначале от НЦ к ОЕЦ (если синдром ошибки попадает в НЦ), а затем по ОЕЦ к нулевому начальному состоянию ЛПМ.

Для поиска "горизонтального" пакета ошибок введем понятие матрицы $F_g^{\lambda}(x)$ "горизонтального" пакета ошибок длины λ.

$$F_g^{\lambda}(x) = C_{err,g}(x) + C_m(x) \qquad GF(2).$$

Аналогичным образом введем понятие матрицы $F_v^{\lambda}(x)$ "вертикального" пакета ошибок длины λ.

$$F_v^{\lambda}(x) = C_{err,v}(x) + C_m(x) \qquad GF(2).$$

ЛЕММА 1. Под воздействием векторов $C_{err}(x)$ и $F_g^{\lambda}(x)$ ЛПМ из начального состояния $S_{beg}(0)$ перейдет в одно и то же состояние синдрома ошибки $S_{err,g}^{\lambda}(n)$.

ЛЕММА 2. Под воздействием векторов $C_{err}(x)$ и $F_v^{\lambda}(x)$ ЛПМ из начального состояния $S_{beg}(0)$ перейдет в одно и то же состояние синдрома ошибки $S_{err,v}^{\lambda}(n)$.

Справедливость Леммы 1 и Леммы 2 следует из эквивалентности графа $G^{(1)}$ диаграмме переходов одновходовой ЛПМ, для которой аналогичные леммы были доказаны в [9].

Ограничимся далее анализом только одиночного "горизонтального" пакета ошибок. В этом случае матрицу $F_g^{\lambda}(x)$ можно рассматривать как путь по графу $G^{(1)}$, причем "нулевому" столбцу (состоящему только из нулей) этой матрицы соответствует переход по нулевой дуге графа $G^{(1)}$, а "единичному" столбцу (содержащему только одну единицу) этой матрицы соответствует переход по единичной дуге графа $G^{(1)}$,

ТЕОРЕМА 1. Многовходовая ЛПМ, определяемая характеристическими матрицами вида (1) или (2), под воздействием кодовой последовательности $C_{err,g}(x)$ из состояния $S_{beg}(0)$ перейдет в состояние $S_{err,v}^{\lambda}(n).$, для перехода из которого снова в $S_{beg}(0)$ необходимо подать на ее входы матрицу $F_g^{\lambda}(x)$.

ТЕОРЕМА 2. К одному ненулевому синдрому ошибки $S_{err,g}^{\lambda}(n)$ могут привести два различных одиночных "горизонтальных" пакетов ошибок в i-ой строке матрицы $C_{err,g}(x)$, параметры которых связаны следующими соотношениями:

$$\begin{cases} \lambda_1 + \lambda_2 = n, \\ (\mu_2^i - \mu_1^i) \bmod n = \lambda_1, \\ (\mu_1^i - \mu_2^i) \bmod n = \lambda_2 \end{cases} \qquad (9)$$

где λ_1, λ_2 - длина соответственно первого и второго "горизонтальных" пакетов ошибок; μ_1^i, μ_2^i – начальные позиции в i-ой строке матрицы $C_{err,g}(x)$ соответственно первого и второго "горизонтальных" пакетов ошибок.

Два пакета ошибок в одной строке матрицы $C_{err,g}(x)$, параметры которых связаны соотношениями (9), будем называть инверсными. Свойство инверсности присуще всем классам циклических кодов – как обычным, так и ПВЦК. Если в обычных циклических кодах инверсные пакеты ошибок действительно нельзя различить между собой, ПЦВК благодаря своей избыточности и регулярности структуры позволяют решить эту задачу. Как уже ранее отмечалось, матрица $R_m(x)$ имеет очень простую структуру: либо все строки, либо часть строк одинаковы. Это позволяет легко распознать искаженные разряды в матрице $R_m(x)$, т. е. различить между собой инверсные пакеты ошибок. Благодаря свойству инверсности отпадает необходимость поиска пакетов ошибок длины более чем $(n-1)/2$.

Таким образом, общее количество неповторяющихся синдромов "горизонтальных" пакетов ошибок в одной строке матрицы $C_{err,g}(x)$ составляет $(n-1)/2$. Для обеспечения возможности исправления одиночных пакетов ошибок необходимо, чтобы, во-первых, количество генерируемых ЛПМ состояний не было меньше количества синдромов этого класса ошибок, во-вторых, количество НЦ в диаграмме переходов должно быть не меньше длины исправляемых пакетов ошибок. Как показано в [11], для обычного циклического (n,k)-кода, задаваемого порождающим многочленом степени *r*, необходимо выполнение условия:

$$r \geq \log_2(n(n-1/2) \tag{10}$$

Если ПВЦК определяется порождающимся многочленом, который для обычного циклического (n,k)-кода удовлетворяет условию (10), то m различных одиночных "горизонтальных" пакетов ошибок в матрице $C_{err,g}(x)$ имеют одинаковые синдромы. Практически нереально найти такую ЛПМ, у которой диаграмма переходов содержала бы необходимое количество состояний и циклов для различения всех одиночных пакетов ошибок.

Тем не менее можно довести точность локализации пакетов ошибок до практически приемлемых значений, если после жесткого алгоритмического декодирования использовать дополнительную информацию, предоставляемую регулярностью структуры матрицы $R_m(x)$, а также методы мягкого декодирования [12].

Аналогичные рассуждения справедливы и для "вертикальных" пакетов ошибок.

Рассмотрим алгоритм поиска одиночных "горизонтальных" пакетов ошибок в кодовой последовательности $C_{err,g}(x)$. Исходными данными для этого алгоритма являются характеристические матрицы A и B *m*-входовой одновыходной ЛПМ над полем Галуа $GF(2)$, а также ненулевой синдром шибок $S^{\lambda}_{err,g}(n)$.

АЛГОРИТМ 1.

1. Начальному состоянию ЛПМ присвоить значение полученного синдрома ошибок:

$$S(t) = S^{\lambda}_{err,g}(n), \quad t=1.$$

2. Ввести вспомогательный вектор $Z(t)$ и присвоить ему значение единичного столбца матрицы ошибок $F^{\lambda}_{g}(x)$.

3. Положить $h=1$.

4. Положить $j=1$.

5. Проверить значение очередного состояния $S(t)$ ЛПМ на равенство вектору $Z(t)$.

Если $S(t) = Z(t)$, то перейти к п. 11.

6. Вычислить очередное значение вектора состояния ЛПМ:

$$S(t+1) = A \times S(t) \qquad GF(2).$$

7. Положить $j = j+1$. Если $j < n$, то перейти к п. 5.

8. Вычислить очередное значение вектора $Z(t)$:

$$Z(t+1) = A \times Z(t) + U^{(1)}(t) \qquad GF(2).$$

9. Положить $h = h+1$. Если $h < (n-1)/2$, то перейти к п. 4.

10. В кодовой последовательности $C_{err,g}(x)$ имеются многократные пакеты ошибок. Перейти к п. 15.

11. Положить i=1.

12. Вычислить значения возможного “горизонтального” пакета ошибок длины λ_1 в начальной позиции μ_1^i i-ой строки матрицы $C_{err,g}(x)$:

$$\lambda_1 = h, \qquad \mu_1^i = (j - h + i - 1) \bmod n .$$

13. Вычислить значения возможного инверсного “горизонтального” пакета ошибок длины λ_2 в начальной позиции μ_2^k k-ой строки матрицы $C_{err,g}(x)$ по формулам (9).

14. Положить $i = i$+1. Если $i < m$, то перейти к п. 12.

15. Конец.

Алгоритм 1 находит $2m$ одиночных “горизонтальных” пакетов ошибок в строках матрицы $C_{err,g}(x)$. Подавляющее большинство из них может быть отброшено после несложного анализа на соответствие известной структуре матрицы $R_m(x)$. И лишь оставшиеся варианты пакетов ошибок могут быть оставлены для дальнейшего анализа и уточнения.

Аналогичный алгоритм можно привести и для “вертикальных” пакетов ошибок.

V Пример

Пусть задана 4-входовая ЛПМ (m=6, r=6, k=3, n=9), которая определяется такими характеристическими матрицами:

$$\mathrm{A} = \begin{Vmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{Vmatrix}; \qquad \mathrm{B} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{Vmatrix}. \tag{11}$$

Элементы последнего столбца матрицы A из (19) представляют собой коэффициенты порождающего многочлена

$$P(x) = 1 + x^3 + x^6, \qquad GF(2). \tag{12}$$

Информационной последовательности $I_6(x)$:

$$I_6(x) = \begin{Vmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{Vmatrix},$$

может соответствовать такая контрольная последовательность $R_6(x)$, в которой нечетные строки одинаковые, а четные – нулевые:

$$R_6(x) = \begin{Vmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{Vmatrix}.$$

Конкатенация матриц $I_6(x)$ и $R_6(x)$ дает кодовую последовательность $C_6(x)$:

$$C_6(x) = \begin{Vmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{Vmatrix}.$$

Многочлен (12) удовлетворяет условию (10), т. е. обычный циклический (9,3)-код на его основе позволяет исправлять одиночные пакеты ошибок. Соответствующий ПВЦК с характеристическими матрицами (11) позволяет находить наборы из нескольких одиночных пакетов ошибок, которые далее следует уточнять.

Заключение

К многочисленным областям использования циклических кодов можно теперь добавить еще и беспроводные каналы связи на основе кратных передающих и приемных антенн. Такое обобщение этих широкоизвестных кодов стало возможным благодаря использованию математического аппарата линейной последовательностной машины. Графовые модели многовходовой ЛПМ позволяют наглядно и строго формально обосновать процедуры кодирования и декодирования ПЦВК. Предлагаемый класс кодов содержит очень много интересных и полезных качеств. Несмотря на кажущееся усложнение процессов кодопреобразования, увеличение времени кодирования и декодирования с помощью многовходовой ЛПМ не происходит и лишь при локализации ошибок требуется дополнительная обработка. Весьма неожиданным свойством является наличие по сути одного контрольного вектора для m информационных векторов. Это свойство может обеспечить сжатие m одновременно кодируемых кодовых векторов в традиционных однопутевых каналах и возможность уточнения расположения возможных ошибок при декодировании в беспроводных многопутевых каналах.

Как отмечается в [3], использование контролирующих кодов станет в ближайшем будущем обязательным атрибутом систем сотовой связи третьего и последующих поколений. Использование кратных передающих и приемных антенн вместе с кодированием информации с помощью предложенных пространственно-временных циклических кодов позволит значительно увеличить пропускную способность беспроводных систем связи.

*Литература: **1**. Гряник М., Карнаухов Г., Пасечник С., Фролов В. Перспективы внедрения в Украине систем сотовой связи 3-го поколения//"Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вып. 6, 2003 р. - С.110-112. **2**. P. Viswanath, David N. C. Tse, R. Laraia, "Opportunistic Beam Forming Using Dumb Antennas," IEEE Trans. Inform. Theory, vol.52, pp. 1277-1294, Juny 2002. **3**. E. Bigliery, "Digital Transmission in the 21st Century: Conflating Modulation and Coding," IEEE Communications Magazine, vol. 40, pp. 128-137, May,2002. **4**. V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communica-tion: Performance criteria and code construction," IEEE Trans. Inform. Theory, vol. 44, pp. 744-765, Mar. 1998.**5**. X. Lin, Rick S. Blum, "Systematic Design of Space Time Codes Employing Multiple Trellis Coded Modulation," IEEE Trans. On Communication, 2002, N 4, pp. 608-615. **6**. Блейхут Р. Теория и практика кодов, исправляющих ошибки: Пер. с англ. - М.: Мир, 1986. - 576 с. **7**. Гилл А. Линейные последовательностные машины: Пер. с англ. - М.: Наука, 1974. - 288 с. **8**. Колесник В. Д., Мирончиков Е. Т. Декодирование циклических кодов. - М.: Связь, 1968. - 252 с. **9**. Семеренко В. П. Параллельное декодирование циклических кодов Боуза-Чоудхури-Хоквингема // Электронное моделирование.*