8. Peter, J. H. An Optimised Density Based Clustering Algorithm [Text] / J. H. Peter, A. Antonysamy // International Journal of Computer Applications. – 2010. – Vol. 6, Issue 9. – P. 20–25. doi: 10.5120/1102-1445
9. Wei, W. Improved VDB scan with global optimum K [Text] / W. Wei, Z. Shuang, R. Bingfei, H. Suoju. – 2013.
10. Birant, D. ST-DBSCAN: An algorithm for clustering spatial-temporal data Data Knowl [Text] / D. Birant, A. Kut // Data & Knowledge Engineering. – 2007. – Vol. 60, Issue 1. – P. 208–221. doi: 10.1016/j.datak.2006.01.013
11. Navneet, G. An Efficient Density Based Incremental Clustering Algorithm in Data Warehousing Environment [Text] / G. Navneet, G. Poonam, K. Venkatramaiah, P. C. Deepak, P. S. Sanoop // 2009 International Conference on Computer Engineering and Applications IPCSIT. – 2011. – Vol. 2.
12. Rehman, M. Comparison of density-based clustering algorithms [Electronic resource] / M. Rehman, S. A. Mehdi. – Available at: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.researchgate.net%2Fprofile%2FSyed_Atif_Mehdi%2Fpublication%2F242219043_COMPARISON_OF_DENSITY-BASED_CLUSTERING_ALGORITHMS%2Flinks%2F5422e1120cf26120b7a6b36e.pdf&ei=LHgRVaSTA6Gv7Abh34CACw&usg=AFQjCNFA9JnzuIbam4BOKYCS_30Yw8Czmg&sig2=wNiTYQiNzFKcDOfEV3mLFw&cad=rja
13. Berkhin, P. Survey Of Clustering Data Mining Techniques [Electronic resource] / P. Berkhin. – 2002. – Available at: http://www.cc.gatech.edu/~isbell/reading/papers/berkhin02survey.pdf
14. Abu Abbas, O. Comparison Between Data Clustering Algorithms [Text] / O. Abu Abbas // The International Arab Journal of Information Technology. – 2008. – Vol. 5, Issue 3. – P. 320–325.
15. Gan, G. Data Clustering: Theory, Algorithms, and Applications [Text] / G. Gan, M. Chaoqun, W. Jianhong. – ASA-SIAM Series on Statistics and Applied Probability, SIAM, Philadelphia, ASA, Alexandria, 2007. – 466 p. doi: 10.1137/1.9780898718348
16. Jiawei, H. Data Mining: Concepts and Techniques. Second Edition [Text] / H. Jiawei, M. Kamber, J. Pei. – Series Editor Morgan Kaufmann Publishers, 2006. – 800 p.
17. Riley, K. F. Mathematical methods for physics and engineering [Text] / K. F. Riley, M. P. Hobson, S. J. Bence. – Cambridge University Press, 2010. – 1359 p.
18. Anil, K. J. Algorithms for clustering data [Text] / K. J. Anil, R. C. Dubes. – Prentice-Hall, Inc. Upper Saddle River, NJ, USA, 1988.

Проведено дослідження коректувальної здатності різних підкласів циклічних кодів з використанням кінцевих автоматів в двійкових полях Галуа – лінійних послідовнісних схем (ЛПС). Показано, що структура нульових циклів ЛПС однозначно визначає кількість випадкових помилок і пакетів помилок, які виявляються та виправляються. Введені нові характеристики коректувальної здатності циклічних кодів

Ключові слова: циклічні коди, кодова відстань, коректувальна здатність коду, лінійна послідовнісна схема

Проведено исследование корректирующей способности различных подклассов циклических кодов с использованием конечных автоматов в двоичных полях Галуа – линейных последовательностных схем (ЛПС). Показано, что структура нулевых циклов ЛПС однозначно определяет количество обнаруживаемых и исправляемых случайных ошибок и пакетов ошибок. Введены новые характеристики корректирующей способности циклических кодов

Ключевые слова: циклические коды, кодовое расстояние, корректирующая способность кода, линейная последовательностная схема

УДК 681.32
DOI: 10.15587/1729-4061.2015.39947

ОЦЕНКА КОРРЕКТИРУЮЩЕЙ СПОСОБНОСТИ ЦИКЛИЧЕСКИХ КОДОВ НА ОСНОВЕ ИХ АВТОМАТНЫХ МОДЕЛЕЙ

В. П. Семеренко
Кандидат технических наук, доцент
Кафедра вычислительной техники
Винницкий национальный
технический университет
Хмельницкое шоссе, 95,
г. Винница, Украина, 21021
E-mail: VPSemerenko@ukr.net

1. Введение

Развитие средств связи и растущий спрос на телекоммуникационные услуги требует дальнейшего улучшения качества таких услуг для пользователей: увеличения пропускной способности (числа абонентов в случае мобильной связи), повышения достоверности передачи, снижения потребляемой мощности аппаратурой.

Все эти требования взаимно противоречивы: улучшение одних параметров связи часто ведет к ухудшению других. Эффективным решением этой задачи является использование помехоустойчивого кодирования передаваемых данных [1].

Безусловно, введение кодов для обнаружения и исправления ошибок также требует своей платы: уменьшение скорости передачи, увеличение полосы пропускания. Для того, чтобы сопоставить выигрыш от введения помехоустойчивых кодов и возникающих при этом неизбежных потерь необходимо иметь критерий эффективности кодирования. В первую очередь важно знать точную либо приближенную оценку количества обнаруживаемых и исправляемых ошибок. Другими словами, полезно знать, насколько хороши (оптимальны) помехоустойчивые коды и каковы характеристики наилучших кодов.

Очевидно, что мы имеем дело с многокритериальной задачей, поскольку приходится учитывать несколько взаимосвязанных параметров кодов. Для корректного решения всей задачи необходимо вначале разобраться с самыми критериями. Ограничимся рассмотрением только наиболее распространённых помехоустойчивых кодов – двоичных циклических кодов.

2. Анализ литературных источников и постановка проблемы

Важнейшей характеристикой кода является количество обнаруживаемых и исправляемых ошибок и критерием оценки этой характеристики принято считать минимальное кодовое расстояние d_{min} [1, 2].

В общем случае должно выполняться следующее соотношение между d_{min} и минимальным числом τ_c исправляемых и числом τ_d обнаруживаемых ошибок:

$$d_{min} \geq \tau_d + \tau_c + 1 = 2\tau_c + 1 = \tau_d + 1. \quad (1)$$

Универсальный способ точного вычисления параметра d_{min} для произвольного блокового линейного кода основан на анализе спектра весов кода – совокупности чисел, указывающих, сколько кодовых слов данного веса имеются у анализируемого кода.

Напомним, что весом $w(y)$ n-разрядного двоичного слова y называется количество его ненулевых компонентов. Два кодовых слова y_i и y_j могут различаться в m позициях (разрядах), в таком случае говорят, что расстояние по Хэммингу $d(y_i, y_j)$ между ними равно m. Тогда минимальное кодовое расстояние равно наименьшему из всех расстояний по Хэммингу между различными парами кодовых слов y_i и y_j.

$$d_{min} = \min d(y_i, y_j), \quad y_i, y_j \in \Omega, \quad i \neq j.$$

Весовой спектр можно задать как весовую функцию

$$A_w(x) = \sum_{i=0}^{n} A_{w,i} x^{(i)},$$

где $A_{w,i}$ – число кодовых слов веса i.

Для некоторых подклассов циклических кодов (Хэмминга, Голея, Рида-Соломона) известно распределения весов кода, даже в аналитическом виде. Однако, для всех кодов эта задача до сих пор не решена, поскольку спектр весов кода находится, как правило, простым перебором. Соответственно, для многих кодов до сих пор неизвестно точное значение d_{min} [3].

Проблема вычисления минимального кодового расстояния и определения корректирующей способности кодов на протяжении многих десятилетий является фундаментальной проблемой в теории помехоустойчивого кодирования.

Сложность проблемы нахождения d_{min} впервые была четко поставлена Бэрлекемпом, Мак-Эллисом и ван Тилборгом [4] еще в 1978 году. В 1997 году Варди [5] доказал, что для произвольного линейного блокового кода d_{min} не может быть вычислено за полиномиальное время. Этот вывод был подтвержден также в статье [6], в которой авторы заявляют, что нахождение d_{min} остается нерешенной вычислительной проблемой.

Поскольку еще не известны в общем виде аналитические зависимости между длиной кода n, числом контрольных разрядов r (r=n–k) и расстоянием d_{min}, поэтому часто используются различные нижние и верхние границы, устанавливающие асимптотические оценки взаимосвязей указанных параметров [1]. Наиболее известной из верхних границ является граница Хэмминга:

$$r \geq \log_2 \left(1 + \sum_{i=1}^{\frac{d_{min}-1}{2}} \binom{n}{i} \right). \quad (2)$$

По сути эта граница указывает на условия существования корректирующих кодов.

Для учета особенностей циклических кодов разработано большое количество различных границ (в основном, нижних) кодового расстояния. Наиболее ранней из них является БЧХ-граница, предложенная Бэрлекемпом. Известно, что порождающий многочлен $g(x)$ кода БЧХ равен наименьшему общему кратному (НОК) минимальных многочленов $f_i(x)$ корней $g(x)$:

$$g(x) = НОК\{f_1(x), f_2(x), \ldots f_{d-2}(x)\}. \quad (3)$$

Значение d в (3) и является нижней границей кодового расстояния, называемого конструктивным. Истинное минимальное расстояние кода во многих случаях больше конструктивного [2].

Граница Хартмана-Тзенга [7] улучшает указанную границу БЧХ, давая более точные нижние оценки расстояния d_{min}. Предложенные за последние годы асимптотические оценки d_{min} базируются на одной парадигме: представление циклического кода на основе корней его порождающего многочлена и использование определяющего множества (defining set) в качестве исходных данных для дальнейших вычислений. Эти оценки можно разбить на два типа: корневые (root) и предельные (border). К первому типу [8, 9] относятся оценки, являющиеся обобщением классической границы БЧХ, их сложность вычислений полиномиальна. Второй тип оценок [10] использует дополнительную информацию о коде и поэтому они более точны, но имеют экспоненциальную сложность. Для уменьшения сложности вычислений авторы в [11] предлагают использовать дискретное преобразование Фурье.

Таким образом, возникает проблема использования параметра d_{min} как критерия оценки циклических кодов.

Во-первых, требует обоснования правомерности использования минимального расстояния d_{min} для полной оценки потенциальной возможности обнаружения и исправления ошибок заданным кодом. Этот критерий не охватывает все виды возможных ошибок (только случайные ошибки) и все разновидности кодов (например, нельзя описать обнаруживающую способность CRC-кодов). Нельзя также представить возможность кода исправлять часть ошибок определенной кратности.

Во-вторых, очень сложно определить точное значение d_{min} для произвольного кода: приходится либо решать NP-полную задачу нахождения весового спектра кода, либо довольствоваться неточными границами для кодового расстояния. Интересно заметить, что расстояние d_{min} по своей сути является границей относительно количества обнаруживаемых и исправляемых ошибок и для его нахождения также используются различные границы.

Возникает закономерный вопрос: а нужно ли тратить вычислительные ресурсы на определение минимального кодового расстояния, если этот параметр не является сам по себе исчерпывающей характеристикой корректирующей способности кода? Может быть, следует направить усилия на непосредственное определение количества обнаруживаемых и исправляемых ошибок и уже на основе этих данных определить точное значение d_{min}?

3. Цель и задачи исследований

Целью данной работы является решение ключевой проблемы теории помехоустойчивого кодирования для одного класса помехоустойчивых кодов – нахождения достоверного критерия оценки обнаруживающей и корректирующей способностей циклических кодов.

Для достижения поставленной цели были решены следующие задачи:

– разработаны принципиально новые методы оценки обнаруживающей и корректирующей способностей циклических кодов на основе их автоматных моделей;

– введены новые выражения для точного аналитического представления количества исправляемых и обнаруживаемых ошибок заданным кодом.

4. Спектры ошибок циклических кодов

Пусть имеется циклический (n, k)-код с длиной n кодового слова и длиной k информационного слова над полем Галуа GF(2). Сформированное на стороне источника сообщений кодовое слово Z передается по каналу связи и принимается декодером на стороне приемника сообщений. В результате действия помех в канале связи может быть принято кодовое слово с ошибками Z_{err}. Декодер вычисляет синдром, по значению которого обнаруживаются и исправляются ошибки в кодовом слове.

Уточним виды возможных типов ошибок с позиций синдромного декодирования циклических кодов и введем новые выражения для точного аналитического представления количества исправляемых и обнаруживаемых ошибок заданным кодом.

ОПРЕДЕЛЕНИЕ 1. Случайная ошибка в кодовом слове Z_{err} называется обнаруживаемой кратности τ_o, если ее синдром является ненулевым и может совпадать с синдромами других ошибок кратности τ_o и меньше.

ОПРЕДЕЛЕНИЕ 2. Случайная ошибка в кодовом слове Z_{err} называется исправляемой кратности τ, если ее синдром является ненулевым и не совпадает с синдромами других ошибок кратности τ и меньше.

ОПРЕДЕЛЕНИЕ 3. Случайная ошибка в кодовом слове Z_{err} называется исправляемой минимальной кратности τ_{min}, если могут быть исправлены все ошибки кратности 1, 2, ... , τ_{min}.

ОПРЕДЕЛЕНИЕ 4. Случайная ошибка в кодовом слове Z_{err} называется h-вариантно исправляемой кратности τ_h, если ее ненулевой синдром совпадает только с синдромами h ошибок кратности τ_h ($\tau_h > \tau_{min}$).

ОПРЕДЕЛЕНИЕ 5. Случайная ошибка в кодовом слове Z_{err} называется частично исправляемой кратности τ_{max}, если могут быть исправлены только часть ошибок кратности τ_{max} и ошибки меньшей кратности ($\tau_{max} > \tau_{min}$).

Теперь введем новые характеристики корректирующей способности циклических кодов.

ОПРЕДЕЛЕНИЕ 6. Спектром исправляемых случайных ошибок циклического (n, k)-кода называется список вида

$$\Phi_r = \{\tau_1 : m_1; \ldots; \tau_{min} : m_{min}; \ldots, \tau_{max} : m_{max}\}, \quad (4)$$

где m_i – количество исправляемых ошибок кратности τ_i ($i = 1 \div \tau_{max}$).

Более наглядным может быть спектр исправляемых случайных ошибок в процентном отношении, в котором указывается процент исправляемых ошибок каждой кратности:

$$\Phi_r = \{\tau_1 : l_1\%; \ldots; \tau_{min} : l_{min}\%; \ldots, \tau_{max} : l_{max}\%\}. \quad (5)$$

где l_i % – процент исправляемых ошибок кратности τ_i.

ОПРЕДЕЛЕНИЕ 7. Спектром случайных ошибок циклического (n, k)-кода, которые h-вариантно исправляются, называется список вида

$$\Phi_h = \{\tau_1 : m_1; \ldots; \tau_h : m_h\}, \quad (6)$$

где $m_1, \ldots, m_h$ – количество ошибок кратности $\tau_1, \ldots, \tau_h$, которые h-вариантно исправляются.

ОПРЕДЕЛЕНИЕ 8. Спектром исправляемых пакетов ошибок циклического (n, k)-кода называется список вида

$$\Phi_b = \{\tau_1 : m_1; \ldots; \tau_b : m_b\}, \quad (7)$$

где $m_1, \ldots, m_b$ – количество исправляемых пакетов ошибок длины $\tau_1, \ldots, \tau_b$.

ОПРЕДЕЛЕНИЕ 9. Спектром исправляемых стираний циклического (n, k)-кода называется список вида

$$\Phi_e = \{\tau_1 : m_1; \ldots; \tau_e : m_e\}, \quad (8)$$

где $m_1,\ldots,m_e$ – количество исправляемых стираний кратности $\tau_1,\ldots,\tau_e$.

Спектры ошибок (6)–(8) по аналогии с (5) также могут быть представлены в процентном отношении.

Все спектры различных видов ошибок могут быть определены на основе автоматных моделей циклических кодов.

5. Автоматные модели циклических кодов

Автоматные модели циклических кодов основаны на специальном классе конечных автоматов в полях Галуа – линейных последовательностных схемах (ЛПС). Согласно [12] ЛПС с l входами, m выходами и r элементами памяти в дискретные моменты времени t над полем Галуа $GF(2)$ описывается функцией переходов

$$S(t+1)=A\times S(t)+B\times X(t), \qquad GF(2) \tag{9}$$

и функцией выходов

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

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

Размерности матриц ЛПС и параметры циклического (n, k)-кода Ω связаны через коэффициент r, который для кода равен числу контрольных разрядов кодового слова Z при систематическом кодировании $(r=n-k)$. Над полем Галуа $GF(2)$ в ЛПС с одним входом и одним выходом могут быть использованы такие матрицы:

$$A=\begin{vmatrix} 0 & 0 & 0 & \ldots & g_0 \\ 1 & 0 & 0 & \ldots & g_1 \\ 0 & 1 & 0 & \ldots & g_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 1 & g_{r-1} \end{vmatrix},$$

$$B=\begin{vmatrix} 1 \\ 0 \\ 0 \\ \ldots \\ 0 \end{vmatrix}, C=\begin{vmatrix} 0 & \ldots & 0 & 1 \end{vmatrix}, D=\begin{vmatrix} 0 \end{vmatrix}. \tag{11}$$

Элементы последнего столбца матрицы A из (11) представляют собой коэффициенты порождающего многочлена (n, k)-кода Ω:

$$g(x)=g_0+g_1x+g_2x^2+\ldots+g_{r-1}x^{x-1}+g_rx^r. \tag{12}$$

На основе ЛПС можно построить автоматно-графовую и автоматно-аналитическую модели циклического (n, k)-кода [13]. Рассмотрим вкратце их суть.

Поскольку ЛПС является конечным автоматом, поэтому в качестве автоматно-графовой модели можно выбрать граф переходов-выходов этого автомата [13]. Для r-мерной ЛПС над полем $GF(2)$ такой граф переходов-выходов 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 $(r=n-k)$. В общем случае из вершины v_j $(v_j\in V_{FA})$ могут выходить нулевая и единичная дуги, а также входить нулевая и единичная дуги.

Если порождающий многочлен (12) является неприводимым и непримитивным или равен произведению нескольких неприводимых многочленов, тогда граф переходов 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 тривиальный НЦ (ТНЦ), состоящий из одной вершины v_0, для которой входящая и выходящая нулевые дуги объединяются и образуют петлю. Далее, на первом уровне находится основной НЦ (ОНЦ) длины n, который связан с ТНЦ парой противоположно направленных единичных дуг. Все остальные НЦ, которые именуются периферийными НЦ (ПНЦ), распределяются по следующим уровням таким образом. На втором уровне располагаются те ПНЦ, каждый из которых связан с ОНЦ с помощью двух пар противоположно направленных единичных дуг. На $(\tau+1)$-ом уровне каждый ПНЦ имеет $(\tau+1)$ пар противоположно направленных единичных дуг с ПНЦ τ-го уровня и отсутствуют единичные дуги с ПНЦ уровней $(\tau-1)$ и менее $(\tau\le\tau_{min})$. Единичные дуги между НЦ разных уровней будем именовать “вертикальными”, а между НЦ одного уровня либо внутри НЦ – “горизонтальными”.

Если порождающий многочлен (11) является неприводимым и примитивным, тогда граф переходов G_{FA} содержит только ТНЦ и ОНЦ длины (2 1).

Для проведения анализа корректирующей способности циклического кода часто бывает достаточной лишь обобщенная структура его автоматно-графовой модели. Тогда можно перейти к более компактной графовой модели – неориентированному графу единичных связей $G_{com}(V_{com},E_{com})$, в котором вершины из множества вершин V_{com} соответствуют НЦ графа G_{FA} (назовем такие вершины объединенными), а ребра из множества ребер E_{com} – только единичным “вертикальным” дугам графа G_{FA}. Дуги между НЦ в графе G_{FA} заменяются ребрами таким образом, чтобы каждая объединенная вершина в графе G_{com} была связана хотя бы одним ребром с одной объединенной вершиной меньшего уровня. Поэтому может быть несколько вариантов графа G_{com}, отличающихся структурой взаимосвязей объединенных вершин нижних уровней.

ПРИМЕР 1. Рассмотрим (15,7)-код БЧХ с порождающим многочленом $g(x)=1+x^4+x^6+x^7+x^8$. Граф G_{com} этого кода содержит 19 объединенных вершин: одну на первом уровне, семь на втором уровне и 11 на третьем (рис. 1). В графе G_{FA} указанным вершинам соответствуют ОНЦ (цикл a), семь ПНЦ второго уровня (циклы b, c, d, f, h, i, l) длины 15, восемь ПНЦ 3-го уровня (циклы e, g, j, k, m, n, o, p) длины 15 и три ПНЦ 3-го уровня (циклы r, s, t) длины 5. Названия циклов дано в обозначениях [14].

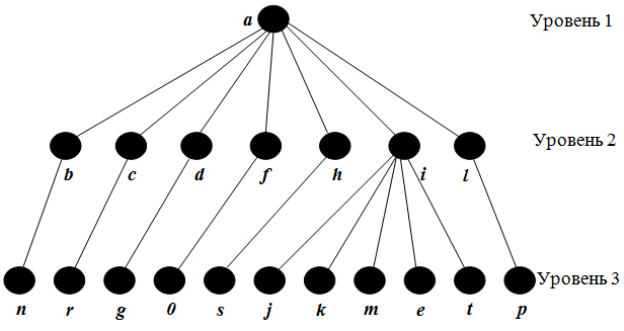

Рис. 1. Граф G_{com} (15,7)-кода БЧХ с порождающим многочленом $g(x)=1+x^4+x^6+x^7+x^8$

Отметим ряд важных свойств графа G_{FA} для циклического кода с неприводимым непримитивным порождающим многочленом, который позволяет исправлять τ_{min} случайных ошибок.

1. На τ-м уровне ($\tau \le \tau_{min}$) графа G_{FA} длина каждого НЦ равна n. В каждом НЦ имеется τ пар противоположно направленных "вертикальных" единичных дуг от НЦ $(\tau-1)$-го уровня.

2. На τ-м уровне ($\tau > \tau_{min}$) графа G_{FA} длина НЦ может быть равной m ($m = n/l, l = 1,2,3,...$), также возможно большее количество "вертикальных" единичных дуг с НЦ предыдущего уровня. На этих уровнях будем различать два вида НЦ длины m:

– НЦ вида 1, если он связан с разными НЦ $(\tau-1)$-го уровня с помощью N_τ пар противоположно направленных "вертикальных" единичных дуг:

$$N_\tau^{(1)} = \frac{\tau m}{n}, \quad \tau > \tau_{min}, \qquad (13)$$

– НЦ вида 2, если он связан с разными НЦ $(\tau-1)$-го уровня с помощью $N_\tau^{(2)} > N_\tau^{(1)}$ пар противоположно направленных "вертикальных" единичных дуг.

Для построения НЦ рассмотрим автоматно-аналитическую модель циклического кода на основе функций (9) и (10).

Вершинам графа G_{FA} соответствуют внутренние состояния ЛПС. Последовательность слов внутренних состояний ЛПС, которые соответствуют вершинам одного цикла в рассмотренных графовых моделях, также образуют цикл. Поскольку совокупность циклов из слов состояний имеет такую же структуру, что и совокупность циклов из вершин, поэтому для характеристики циклов из слов состояний будем использовать те же термины: ТНЦ, ОНЦ и ПНЦ. В автоматно-аналитической модели цикл ТНЦ будет представлен как r-разрядное нулевое слово, а остальные НЦ – множества из m r-разрядных слов (m=n либо является делителем n).

В дальнейшем различие между НЦ, образованных вершинами графа, и НЦ, образованных словами состояний ЛПС, определяется контекстом: в графовых моделях подразумеваются автоматно-графовые НЦ, а при математических преобразованиях – автоматно-аналитические НЦ.

Прежде, чем упорядочить все НЦ по уровням, необходимо вначале сформировать эти НЦ, т. е. построить граф G_{FA}. Операции формирования НЦ и их упорядочения можно выполнять одновременно. Рассмотрим алгоритм формирования ОНЦ и ПНЦ 2-го уровня на основе заданных матриц ЛПС.

АЛГОРИТМ ФОРМИРОВАНИЯ НУЛЕВЫХ ЦИКЛОВ.

Исходные данные:

– характеристические матрицы $A = |a_{ij}|_{r\times r}$, $B = |b_{ij}|_{r\times 1}$.

Результат: ТНЦ, ОНЦ, все ПНЦ второго уровня.

1. Сформировать цикл ТНЦ: $S(0) = 0$. Положить $t = 1$.
2. Вычислить: $S^{(1)}(t) = S(0) + B$, GF(2).
3. Положить $t = t + 1$.
4. Вычислить: $S^{(1)}(t) = A \times S^{(1)}(t-1)$, GF(2).
5. Если $S^{(1)}(t) \ne S^{(1)}(0)$, то перейти к п. 3.
6. Положить $n = t$. Сформировать ОНЦ из

$S^{(1)}(1), S^{(1)}(2), \ldots, S^{(1)}(n)$.

7. Для i от 1 до $\left\lfloor \frac{n}{2} \right\rfloor$ выполнить:

7. 1. Присвоить: $S_{beg}^{1\to 2}(i) = S^{(1)}(i)$.

7. 2. Вычислить: $S_{end}^{1\to 2}(i) = S_{beg}^{1\to 2}(i) + B$, GF(2)

7. 3. Присвоить: $S_i^{(2)}(1) = S_{end}^{1\to 2}(i)$.

7. 4. Для t от 1 до $n-1$ выполнить:

$S_i^{(2)}(t+1) = A \times S_i^{(2)}(t)$, GF(2)

7. 5. Сформировать i-й ПНЦ второго уровня:

$S_i^{(2)}(1), S_i^{(2)}(2), \ldots, S_i^{(2)}(n)$.

8. Конец.

Если общее количество слов состояний сформированных НЦ будет меньшей, чем 2^r, это будет означать возможность наличия в графе G_{FA} ПНЦ последующих уровней.

В основе алгоритма формирования НЦ лежит единственная операция рекурсивного вычисления внутренних состояний ЛПС. Сложность формирования ОНЦ линейна: $O(n)$. Сложность формирования ПНЦ второго уровня квадратична: $O(n^2)$.

Способ нахождения ПНЦ i-го уровня по известному ПНЦ $(i-1)$-го уровня аналогичен способу нахождения ПНЦ 2–го уровня из ОНЦ, который изложен в Алгоритме. Сложность формирования ПНЦ i-го уровня: $O(n \times n_{i-1} \times n_i)$, где n_{i-1} и n_i – количество НЦ соответственно на $(i-1)$-м и i-м уровнях.

6. Принцип поиска ошибок на основе автоматных моделей

Рассмотрим интерпретацию процедуры декодирования циклического (n, k)-кода в терминах введенных автоматных моделей.

Введем понятие кодового пути η, который состоит из n однонаправленных дуг в графе G_{FA}, в причем i-а нулевая (единичная) дуга соответствует разряду $z_i = 0$ ($z_i = 1$) кодового слова Z ($z_i \in Z, i = 1 \div n$). Основным свойством кодового пути η есть то, что он начинается и заканчивается в одной и той же вершине графе G_{FA}. Наиболее часто такой вершиной выбирают начальную вершину v_0, которая соответствует нулевому состоянию S(0) ЛПС.

При передаче данных по каналу связи вследствие различных помех некоторые разряды кодового слова случайным образом могут быть искажены, т.е. будет получено кодовое слово $Z_{err}^{(\tau)}$ со случайной ошибкой кратности τ. Взаимосвязь между кодовыми словами Z и $Z_{err}^{(\tau)}$ выражается через слово ошибки $E_{err}^{(\tau)}$:

$$E_{err}^{(\tau)} = Z + Z_{err}^{(\tau)}, \quad GF(2). \qquad (14)$$

Под воздействием случайной ошибки кратности τ кодовый путь η_{st} в графе G_{FA} начинается в вершине v_0 и оканчивается в некоторой вершине ошибке, которую обозначим как v_{err}. Назовем кодовый путь η_{st} от вершины v_0 к вершине v_{err} прямым. НЦ, который содержит вершину v_{err}, назовем НЦ ошибки.

ТЕОРЕМА 1. НЦ ошибки, в котором оканчивается прямой кодовый путь η_{st}, находится на уровне τ графа $G_{FA}, \tau = 1 \div \tau_{min}$.

Доказательство. Кодовому слову Z соответствует путь, который начинается и оканчивается в одной и той же вершине v_0. Кодовому слову $Z_{err}^{(\tau)}$ соответствует прямой кодовый путь η_{st} ошибки. Равенство (14) будет справедливо в рамках графовой модели лишь тогда, когда слову ошибки $E_{err}^{(\tau)}$ будет соответствовать путь от вершины v_0 к вершине v_{err}, но не обязательно прямой кодовый путь η_{st} ошибки.

Таким образом, в графовой модели слова $Z_{err}^{(\tau)}$ и $E_{err}^{(\tau)}$ эквивалентны относительно вершин v_0 и v_{err}. Для дальнейшего доказательства перейдем к слову ошибки $E_{err}^{(\tau)}$, которое содержит τ единиц и $(n-\tau)$ нулей. Каждая единица в слове ошибки соответствует переходу по "вертикальной" единичной дуге графа G_{FA}, а каждый ноль – переходу по нулевой дуге этого графа. Если по нулевым дугам можно переходить между вершинами одного НЦ, то по "вертикальным" единичным дугам можно переходить между НЦ соседних уровней, следовательно, по τ таким дугам можно осуществить "спуск" до одного из НЦ уровня τ графа G_{FA}. Именно этот НЦ и содержит вершину v_{err}.

⊥

В общем случае декодирование циклических кодов состоит из двух этапов: установление факта отсутствия или наличия ошибки, и определение параметров ошибки при ее наличии.

В терминах автоматно-графовой модели первый этап декодирования состоит в нахождении вершины v_{err} а второй этап – в построении обратного кодового пути η_{rv} от вершины v_{err} к вершине v_0.

В терминах автоматно-аналитической модели первый этап декодирования состоит в подаче на входы ЛПС, находящейся в нулевом начальном состоянии S(0), кодового слова $Z_{err}^{(\tau)}$. Через n тактов времени ЛПС, согласно формулы (9), перейдет в некоторое ненулевое состояние $S_{err}^{(\tau)}(n)$, именуемое синдромом ошибки кратности τ.

7. Анализ корректирующей способности циклических кодов по случайным ошибкам

Последующие теоремы устанавливают взаимосвязь корректирующей способности циклических кодов со структурой его графа G_{FA}.

ТЕОРЕМА 2. Циклический (n, k)-код способен исправить все $N_{min} = \sum_{\tau=0}^{\tau_{min}} N_\tau$ случайных ошибок кратности τ_{min} и менее, если для его графа G_{FA} выполняются следующие условия:

1) имеется не менее τ_{min} уровней, на котором расположены НЦ; на τ-ом уровне общее количество N_τ вершин всех НЦ равно:

$$N_\tau = \binom{n}{\tau},$$

где $\binom{n}{\tau}$ – число сочетаний из n по τ $(\tau = 1 \div \tau_{min})$.

Доказательство. Количество исправляемых ошибок кратности τ должно соответствовать количеству синдромов этих ошибок. Количество N_τ синдромов ошибок кратности τ равно $\binom{n}{\tau}$. Каждый синдром ошибки соответствует одной вершине в графе G_{FA}. На τ-ом уровне графа $_{FA}$ количество вершин равно $\binom{n}{\tau}$, т. е. достаточно для отображения всех случайных ошибок кратности τ. Общее количество вершин на всех τ_{min} уровнях графа G_{FA} равно

$$N_{min} = \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{\tau_{min}}$$

и достаточно для отображения всех случайных ошибок кратности 1, 2, ... , τ_{min}. Следовательно, все случайные ошибки кратности 1, 2, ..., τ_{min} могут быть исправлены.

⊥

После построения автоматно-графовой модели и нахождения количества исправляемых ошибок можно по формуле (1) определить точное значение кодового расстояния, т.е. параметр d_{min} будет в таком случае выступать как производное от найденного числа ошибок.

СЛЕДСТВИЕ 1. Циклический (n, k)-код, удовлетворяющий условию Теоремы 2, имеет спектр исправляемых случайных ошибок и кодовое расстояние d_{min}:

$$\{1: \binom{n}{1}; 2: \binom{n}{2}; \ldots; \tau_{min}: \binom{n}{\tau_{min}}\}, \; d_{min} = 2\tau_{min} + 1. \qquad (15)$$

СЛЕДСТВИЕ 2. Если в графе G_{FA} циклического (n, k)-кода отсутствуют НЦ на $(\tau_{min}+1)$-ом уровне и выше, тогда

$$\binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{\tau_{min}} = 2^{n-k} - 1, \qquad (16)$$

и такой код называется совершенным.

ПРИМЕР 2. Если по изложенному Алгоритму построить граф G_{FA} для (23,12)-кода Голея с порождающим многочленом $g(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$, тогда можно убедиться, что этот граф содержит ТНЦ и 89 НЦ длины 23: ОНЦ, 11 ПНЦ 2-го уровня и 77 ПНЦ 3-го уровня. Количество вершин на i-ом уровне графа

G_{FA} соответствует количеству исправляемых ошибок i-й кратности. Следовательно, исправляются все одиночные, двойные и тройные случайные ошибки. Спектр исправляемых ошибок согласно (4) имеет вид:

{1:23; 2:253; 3:1771},

или в процентном отношении, согласно (5):

{1:100 %; 2:100 %; 3:100 %}.

Далее можно определить кратности исправляемых ошибок и вычислить минимальное кодовое расстояние:

$$\tau_{max} = \tau_{min} = 3,\ d_{min} = 2\times 3+1 = 7.$$

Несложно убедиться в выполнении условий (15) и (16) для кода Голея.

⊥

ТЕОРЕМА 3. Циклический (n,k)-код, удовлетворяющий условиям Теоремы 2, способен также исправить $N_{max} = \sum_{\tau=\tau_{min}+1}^{\tau_{max}} N_\tau$ случайных ошибок кратности $(\tau_{min}+1,\ldots,\tau_{max})$, если для его графа G_{FA} выполняются дополнительные условия:

1) имеется более, чем τ_{min} уровней, на котором расположены НЦ;

2) на $(\tau_{min}+1)$-м и последующих уровнях имеются НЦ вида 1 с общим количеством вершин N_τ:

$$N_\tau < \binom{n}{\tau}, \text{ для } \tau = \tau_{min}+1,\ldots,\tau_{max}. \quad (17)$$

Доказательство. Для исправления ошибок кратности $\tau > \tau_{min}$ НЦ ошибки в графе G_{FA} должен находиться на расстоянии $\tau > \tau_{min}$ от ТНЦ, т. е. обратный кодовый путь должен включать $\tau > \tau_{min}$ "вертикальных" единичных дуг между НЦ. Поэтому, граф G_{FA} должен иметь дополнительные уровни. Циклический (n, k)-код с кодовым расстоянием d_{min}, позволяет исправить только часть ошибок кратности $\tau > \tau_{min}$, а не все ошибки этой кратности, иначе выполнялось бы равенство

$$N_\tau = \binom{n}{\tau},$$

что противоречит (17). Поэтому для частично исправляемой ошибки справедливо неравенство (17), и с его учетом получаем значение N_{max}.

Для исправления случайной ошибки кратности $\tau > \tau_{min}$ необходимо, чтобы в графе G_{FA} НЦ ошибки длины m $(m \le n)$ был связан с другими НЦ $(\tau-1)$-го уровня с помощью $\frac{\tau m}{n}$ пар противоположно направленных "вертикальных" единичных дуг. Таким условиям отвечают НЦ вида 1.

Если НЦ ошибки длины m $(m \le n)$ был связан с другими НЦ $(\tau-1)$-го уровня с помощью $\frac{\tau mh}{n}$ пар противоположно направленных "вертикальных" единичных дуг, тогда такие ошибки будут h-вариантно исправляемыми.

⊥

СЛЕДСТВИЕ 3. Циклический (n, k)-код, удовлетворяющий условию Теоремы 3, имеет кодовое расстояние d_{min} и спектр исправляемых случайных ошибок

$$\{1:\binom{n}{1};\ 2:\binom{n}{2};\ \ldots;\ \tau_{min}:\binom{n}{\tau_{min}};$$

$$\tau_{min}+1:\ N_{\tau_{min}+1}\ \ldots,\ \tau_{max}:\ N_{\tau_{max}}\}.$$

Говорят, что циклический код, удовлетворяющий условию Теоремы 3, может исправлять ошибки за пределами кодового расстояния d_{min}.

ПРИМЕР 3. Рассмотрим снова (15,7)-код БЧХ из Примера 1. Наличие НЦ на третьем уровне свидетельствует о потенциальной возможности исправления тройных случайных ошибок. Далее рассмотрим возможность выполнения второго условия Теоремы 3. С этой целью проведем исследование структуры связей между отдельными НЦ второго и третьего уровней. В табл. 1 в (i, j)-й клетке записано количество пар противоположно направленных "вертикальных" единичных дуг графа G_{FA} между i-м НЦ третьего уровня и j-м НЦ второго уровня.

Таблица 1

Структура взаимосвязей НЦ второго и третьего уровней графа G_{FA} кода БЧХ с порождающим многочленом $g(x) = 1+x^4+x^6+x^7+x^8$

НЦ	цикл *b*	цикл *d*	цикл *f*	цикл *c*	цикл *i*	цикл *l*	цикл *h*	Итого
цикл *e*	1	0	1	2	3	1	1	9
цикл *j*	1	1	1	0	3	1	2	9
цикл *n*	1	0	0	0	0	1	1	3
цикл *m*	2	1	1	1	3	1	0	9
цикл *g*	1	1	1	0	0	0	0	3
цикл *k*	0	2	1	1	3	1	1	9
цикл *p*	0	1	0	1	0	1	0	3
цикл *o*	0	0	1	1	0	0	1	3
цикл *r*	1	0	1	1	0	0	0	3
цикл *s*	0	1	0	0	0	1	1	3
цикл *t*	0	0	0	0	1	0	0	1

Как видно из табл. 1, пять ПНЦ третьего уровня (циклы g, o, n, p, t) относятся к НЦ вида 1, поскольку выполняется равенство (13): циклы g, o, n, p связаны з разными ПНЦ второго уровня с помощью только трех пар, короткий цикл t – с помощью одной пары противоположно направленных "вертикальных" единичных дуг. Циклы g, o, n, p длины 15 дают 4×15 синдромов тройных ошибок, которые исправляются, а цикл t длины 5 дает еще 5 синдромов исправляемых тройных ошибок. В результате исправляется 65 тройных ошибок, или 14 % от их общего количества для этого кода. Остальные ПНЦ третьего уровня (циклы e, j, k, m, r, s) относятся к НЦ вида 2, поскольку циклы e, j, k, m связаны с разными ПНЦ 2-го уровня с помощью девяти пар противоположно направленных "вертикальных" единичных дуг, а короткие циклы r, s – с помощью трех пар противоположно направленных "вертикальных" единичных дуг.

Таким образом, для рассматриваемого кода БЧХ одиночные и двойные ошибки полностью исправляются, а тройные ошибки только частично: только те,

синдромы которых попадают в циклы g, o, n, p, t. Тройные ошибки, синдромы которых попадают в циклы e, j, k, m, r, s – 3-вариантно исправляются. Следовательно, спектр исправляемых случайных ошибок в процентном отношении, согласно (5) и (6):

Φ_r ={1:100%; 2:100%; 3:14%}, Φ_h ={3:15%}.

Минимальное кодовое расстояние для (15,7)-кода БЧХ:

$$\tau_{min} = 2,\ \tau_{max} = 3,\ d_{min} = 2\times 2+1 = 5.$$

⊥

С позиций автоматного представления циклических кодов можно легко доказать следующие теоремы.

ТЕОРЕМА 4. В графе G_{FA} квадратично-вычетного (n, k)-кода и (n, k)-кода БЧХ, позволяющих исправить все случайные ошибки кратности τ_{min} и менее, отсутствуют "горизонтальные" единичные дуги на уровнях 1, 2, ..., τ_{min}–1.

СЛЕДСТВИЕ 4. Если для квадратично-вычетного кода или кода БЧХ, в процессе построения графа G_{FA} "горизонтальные" единичные дуги между соседними НЦ появляются, начиная с i-го уровня, тогда можно утверждать, что минимальное кодовое расстояние для анализируемого кода равно $d_{min} = 2i+1$.

ТЕОРЕМА 5. Циклический (n, k)-код Файра не может исправлять случайные ошибки двойной кратности и более.

Очень интересная ситуация с исправляемыми и обнаруживаемыми ошибками имеет место в кодах CRC (*Cyclic Redundancy Code* - циклические избыточные коды). Принято считать [15], что кодовое расстояние для CRC-кода равно d_{min}=4. С точки зрения корректирующей способности этого кода такая оценка точна. Однако, CRC-код обнаруживает также все ошибки нечетной кратности, и это свойство кода невозможно отразить с помощью традиционного кодового расстояния. Более точной характеристикой является спектр обнаруживаемых случайных ошибок, который для CRC-кода в процентном отношении равен:

{1:100%; 2:100%; (2i+1):100%}, i=1, 2, 3, ...

8. Анализ корректирующей способности циклических кодов по пакетам ошибок

Введем вначале необходимые определения [16].

ОПРЕДЕЛЕНИЕ 10. Циклическим пакетом Δ^b ошибок длины τ_b называется пакет, в котором первая ошибка расположена в позиции i, а последняя – в позиции $(i+\tau-1) \bmod n \ \ (i=1\div n)$.

ОПРЕДЕЛЕНИЕ 11. Циклическим разреженным пакетом Δ^b_{any} ошибок длины τ_b называется циклический пакет, внутри которого могут быть безошибочные символы.

ОПРЕДЕЛЕНИЕ 12. Циклическим плотным пакетом $\Delta^b_{\text{п}}$ ошибок длины τ_b называется циклический пакет, состоящий только из τ_b ошибочных символов.

Установим взаимосвязь корректирующей способности циклических кодов по разреженным пакетам ошибок со структурой его графа G_{FA}.

ТЕОРЕМА 6. Циклический (n, k)-код способен исправить все N_b разреженных пакетов ошибок длины τ_b ($\tau_b \geq 2$) и менее

$$N_b = \sum_{i=0}^{\tau_b-2} 2^i = 2^{\tau_b-1} - 1, \qquad (18)$$

если его граф G_{FA} содержит не менее (N_b+1) НЦ длины n.

Доказательство. Поскольку возможно 2^i вариантов пакетов ошибок длины i, поэтому суммарное количество пакетов ошибок длины 1, 2, ..., b равно N_b (18). Для исправления каждого варианта пакета ошибок и его n циклических сдвигов должен быть отдельный НЦ длины n. С учетом необходимости отдельного НЦ для одиночных ошибок его граф G_{FA} должен содержать не менее (N_b+1) НЦ длины n.

Приведем без доказательства ряд теорем относительно некоторых подклассов циклических кодов.

ТЕОРЕМА 7. Квадратично-вычетные (n, k)-коды и (n, k)-коды БЧХ, исправляющие τ_{min} случайных ошибок, способны исправить все разреженные пакеты ошибок длины не более τ_b ($\tau_b \geq 2$):

$$\tau_b < \log_2\left(\sum_{i=0}^{\tau_{min}} \binom{n-1}{i}\right)+1.$$

ТЕОРЕМА 8. Циклический (n, k)-код Файра способен исправить одиночные ошибки и все разреженные пакеты ошибок длины τ_b ($\tau \geq$) и менее, если для его графа G_{FA} выполняются следующие условия:

1) имеется не менее τ_b уровней, на котором расположены НЦ; справедливо соотношение:

$$\tau_b \leq \left\lfloor \log_2 \left\lfloor \frac{2^c}{c} \right\rfloor \right\rfloor.$$

где $\lfloor * \rfloor$ означает округление до ближайшего целого в меньшую сторону.

ПРИМЕР 4. Рассмотрим циклический (105,94)-код Файра с порождающим многочленом $g(x)=(1+x^7)(x^4+x+1)$. Графовая модель этого кода содержит на шести уровнях следующее количество НЦ длины 105 (НЦ длины 7 и длины 15 для нашей задачи не играют роли): ОНЦ, 3 ПНЦ второго уровня, 5 ПНЦ третьего уровня, 5 ПНЦ четвертого уровня, 3 ПНЦ пятого уровня и один ПНЦ шестого уровня. В ОНЦ содержатся синдромы всех одиночных ошибок, в ПНЦ второго уровня – синдромы пакетов ошибок длин 2, 3 и 4, в ПНЦ третьего уровня – синдромы пакетов ошибок длин 3, 4 и 5, в ПНЦ четвертого уровня – синдромы пакетов ошибок длин 4, 5 и 6, в ПНЦ пятого уровня – синдромы пакетов ошибок длин 5 и 6, в ПНЦ шестого уровня – синдром пакетов ошибок длины 6. Код позволяет исправлять все одиночные случайные ошибки, все пакеты ошибок длины 4 и менее, а также 62,5 % пакетов ошибок длины 5 и 31,25 % пакетов ошибок длины 6. Более точно корректирующую способность кода показывает его спектр исправляемых разреженных пакетов ошибок в процентном отношении:

{1:100%; 2:100%; 3:100%; 4:100%; 5:62,5%; 6:31,3%}.

Код позволяет исправлять также некоторое количество случайных ошибок, о чем показывает его спектр

исправляемых случайных ошибок в процентном отношении:

{1:100%; 2:5,7%; 3:0,3%}.

Рассмотрим вкратце плотные пакеты ошибок длины τ_s не менее, чем $r/2$.

ТЕОРЕМА 9. Циклический (n, k)-код способен исправить одиночные плотные пакеты ошибок длины $\frac{n-k}{2} < \tau_s \le \frac{n-1}{2}$, если выполняется условие

$$r \ge \log_2((n^2 - n + 2)/2).$$

СЛЕДСТВИЕ 5. Циклический (n, k)-код Файра не может исправлять плотные пакеты ошибок длины

$$\frac{n-k}{2} < \tau_s \le \frac{n-1}{2}.$$

Таким образом, на основе автоматного представления циклических кодов можно точно оценить их корректирующие способности по разным типам ошибок и представить их в наглядной форме с помощью спектров исправляемых ошибок.

9. Выводы

Предлагается принципиально новый метод вычисления обнаруживающей и корректирующей способностей циклических кодов с помощью их автоматных моделей на основе теории линейных последовательностных схем (ЛПС). Структура нулевых циклов графа переходов ЛПС однозначно определяет количество обнаруживаемых и исправляемых случайных ошибок и, соответственно, минимальное кодовое расстояние. Анализ графовой модели циклического кода позволяет также вычислить корректирующую способность кода относительно разреженных и полных пакетов ошибок. Такой подход позволяет с единых позиций произвести сравнение корректирующих способностей различных подклассов циклических кодов (CPC, Хэмминга, БЧХ, Файра и других).

Построение полной графовой модели циклического кода представляет собой трудоемкую задачу, однако для решения разработан строго формализованный алгоритм, в отличии от полного перебора при поиске весового спектра кода. Суть этого алгоритма состоит в вычислении множества нулевых циклов графа на основе единственной операции рекурсивного вычисления внутренних состояний ЛПС, что позволяет эффективно использовать различные способы параллельной обработки данных. Важным достоинством алгоритма является его итеративный характер, что позволяет на τ-й итерации ограничиться τ-уровневой графовой моделью кода, если для анализируемого кода поставлена задача подтверждения способности исправления лишь τ ошибок ($\tau = 1 \div \tau_{max}$).

Вместо спектра весов и минимального кодового расстояния предлагается использовать спектры ошибок различных типов, полученных на основе анализа автоматно-графовой модели кода.

Литература

1. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] / Б. Скляр; пер. с англ.; 2-е изд., перер. – М.: Издательский дом “Вильямс”, 2004. – 1104 с.
2. Блейхут, Р. Теория и практика кодов, исправляющих ошибки [Текст] / Р. Блейхут; пер. с англ. – М. : Мир, 1986. – 576 с.
3. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение [Текст] / Р. Морелос-Сарагоса; пер. с англ. – М.: Техносфера, 2006. – 320 с.
4. Berlecamp, E. Hardness of Approximating the Minimum Distance of a Linear Code [Text] / E. Berlecamp, R. McEliece, H. van Tilborg // IEEE Trans. Inform. Theory. – 1978. – Vol. 21, Issue 5. – P. 384–386.
5. Vardy, A. The Intractability of Computing the Minimum Distance of a Code [Text] / A. Vardy // IEEE Transactions on Information Theory. – 1997. – Vol. 43, Issue 6. – P. 1757–1766. doi: 10.1109/18.641542
6. Dumer, I. Hardness of Approximating the Minimum Distance of a Linear Code [Text] / I. Dumer, D. Micciancio, M. Sudan // 2000 IEEE International Symposium on Information Theory. – 2003. – Vol. 49, Issue 1. – P. 22–37. doi: 10.1109/isit.2000.866550
7. Hartmann, C. Generalizations of the BCH Bound [Text] / C. Hartmann, K. Tzeng // Information and Control – 1972. – Vol. 20, Issue 5. – P. 489–498. doi: 10.1016/s0019-9958(72)90887-x
8. Roos, C. A Generalization of the BCH Bound for Cyclic Codes, Including the Hartmann-Tzeng Bound [Text] / C. Roos // Journal of Combinatorial Theory, Series A. – 1982. – Vol. 33, Issue 2. – P. 229–232. doi: 10.1016/0097-3165(82)90014-0
9. Boston, N. Bounding Minimum Distances of Cyclic Codes Using Algebraic Geometry [Text] / N. Boston // Electronic Notes in Discrete Mathematics. – 2001. –Vol. 6, Issue 5. – P. 384–386. doi: 10.1016/s1571-0653(04)00190-8
10. van Lint, J. On The Minimum Distance of Cyclic Codes [Text] / J. van Lint, R. Wilson // IEEE Transactions on Information Theory. – 1986. –Vol. 32, Issue 1. – P. 23-40. doi: 10.1109/tit.1986.1057134
11. Kaida, T. A Note on the Rank Bounded Distance and Its Algorithms for Cyclic Codes [Text] / T. Kaida, J. A. Zheng // Pure and Applied Mathematics Journal. – 2015. – Vol. 4, Issue 2-1. – P. 36–41. – Available at: http://article.sciencepublishinggroup.com/pdf/10.11648.j.pamj.s.2015040201.17.pdf doi: 10.11648/j.pamj.s.2015040201.17
12. Гилл, А. Линейные последовательностные машины [Текст] / А. Гилл; пер. с англ. – М. : Наука, 1974. – 288 с.
13. Семеренко, В. П. Высокопроизводительные алгоритмы для исправления независимых ошибок в циклических кодах [Текст] / В. П. Семеренко // Системи обробки інформації: зб. наук. праць – 2010. – Вип. 3 (84). – С. 80–89.
14. Кларк, Дж. Кодирование с исправлением ошибок в системах цифровой связи [Текст] / Дж. Кларк, Дж. Кейн; пер. с англ. – М. : Радио и связь, 1987. – 392 с.
15. Вернер, М. Основы кодирования [Текст] / М. Вернер; пер. с англ. – М.: Техносфера, 2004. – 288 с.
16. Semerenko, V. P. Burst-Error Correction for Cyclic Codes [Text] / V. P. Semerenko // Proceeding of International IEEE Conference EUROCON2009, 2009. – P. 1646–1651. doi: 10.1109/eurcon.2009.5167864