ПОСТРОЕНИЕ АЛГОРИТМОВ НА ОСНОВЕ КОДОВ РИДА СОЛОМОНА ДЛЯ КОРРЕКЦИИ ОШИБОК В ДВУХМЕРНЫХ МАССИВАХ ЦИФРОВЫХ ДАННЫХ

Гарнышев И.Н.[1], Казанцев С.В.[2], Мальков Р.Ю.[3], Семенов И.Д.[4], Юдин С.В.[5]
Email: Garnyshev672@scientifictext.ru

[1]Гарнышев Игорь Николаевич - сетевой инженер,
Отдел администрирования сетей передачи данных,
Тинькофф Банк;
[2]Казанцев Сергей Владимирович - главный инженер,
Департамент сетей передачи данных,
Сбербанк;
[3]Мальков Роман Юрьевич – эксперт,
Центр компетенций по облачным решениям,
Техносерв,
г. Москва;
[4]Семенов Иван Дмитриевич - старший инженер,
Департамент сетей передачи данных,
Servers.com Лимассол, Кипр;
[5]Юдин Степан Вячеславович - администратор сети,
Департамент технического обеспечения и развития инфраструктуры информационных систем,
Спортмастер, г. Москва

Аннотация: *в статье проведен анализ принципов помехоустойчивого кодирования и эффективного декодирования блоков двоичных данных, представленных в виде двумерных массивов. Предложенный математический аппарат базируется на принципах модулярной арифметики и модели линейного блочного кодирования. Разработана схема построения последовательностей кода Рида-Соломона на базе порождающего полинома. Предложена математическая модель представления двумерных последовательностей кода Рида-Соломона, которая основывается на теории биграфов. Построена комплексная методология помехоустойчивого кодирования данных и восстановления частично поврежденных кодовых последовательностей.*
Ключевые слова: *коды Рида-Соломона, составное изображение, модулярная арифметика, простое расширение поля, порождающий полином, расширение графа, двудольный граф.*

DEVELOPMENT OF ALGORITHMS BASED ON THE REED SOLOMON CODES FOR ERROR CORRECTION OF TWO-DIMENSIONAL ARRAYS OF DIGITAL DATA

Garnyshev I.N.[1], Kazantsev S.V.[2], Malkov R.Yu.[3], Semenov I.D.[4], Iudin S.V.[5]

[1]Garnyshev Igor Nikolaevich - Network Engineer,
DATA NETWORK ADMINISTRATION DEPARTMENT,
TINKOFF BANK;
[2]Kazantsev Sergei Vladimirovich - Senior Engineer,
NETWORK DEPARTMENT,
SBERBANK;
[3]Malkov Roman Yurevich – Expert,
CLOUD SOLUTIONS DEPARTMENT,
TECHNOSERV CLOUD,
MOSCOW;
[4]Semenov Ivan Dmitrievich - Senior Engineer,
NETWORK DEPARTMENT.
SERVERS.COM LIMASSOL, CYPRUS;
[5]Iudin Stepan Vyacheslavovich - Network Administrator,
DEPARTMENT OF TECHNICAL SUPPORT AND INFORMATION SYSTEMS INFRASTRUCTURE DEVELOPMENT,
SPORTMASTER, MOSCOW

Abstract: *the article analyzes the principles of error-correcting coding and efficient coding of binary data arrays presented in the form of two-dimensional arrays. The proposed mathematical apparatus is based on the principles of modular arithmetic and a linear block coding model. A scheme for constructing Reed-Solomon code sequences on the basis of a generating polynomial is developed. A mathematical model is presented for representing two-dimensional sequences of the Reed-Solomon code, which is based on the theory of bipartite*

graphs. A comprehensive methodology for the error-correcting data coding and restoration of partially damaged code sequences has been built.
Keywords: *Reed–Solomon codes, compound image, modular arithmetic, primitive element, generator polynomial, graph expansion, bipartite graph.*

УДК 004.052.4

Введение

Коды Рида-Соломона (RS: Reed–Solomon codes) на базе расширенного конечного алфавита [1-3] являются основным инструментом помехоустойчивого кодирования двоичных данных, в том числе при работе с составными изображениями (compound image) и видеоматериалами [4-6]. При разработке систем представления блоков данных в виде длинного помехоустойчивого кода особенно актуальной задачей является рассмотрение вопроса кодирования данных при помощи двумерных массивов. В общем случае однозначных связей между двумерной структурой информационной среды и кодом может не быть, поэтому важно задать соотнесение между элементами массива на уровне логических правил. Такой подход позволит воспроизвести этап частичного декодирования с дальнейшим извлечением подмножества информационных элементов в случае повреждения регистрирующей среды носителя информации [7-9].

Анализ последних исследований и публикаций в данной области позволил обобщить представления о принципах помехоустойчивого кодирования и эффективного декодирования блоков двоичных данных, представленных в виде двумерных массивов [1-9]. С этой целью были рассмотрены принципы модулярной арифметики и методика сравнения по модулю в рамках теории кодирования [10, 11], а также модель линейного блочного кодирования [12-15]. Кроме того изучены принципы кодирования двудольных графов, на основе которых можно построить алгоритмы помехоустойчивого кодирования данных с низкой ресурсоемкостью и эффективным частичным декодированием выбранных фрагментов кодовой последовательности [16-18], в том числе в рамках геометрии конечных полей [19-22].

Целью работы стало построение методологии помехоустойчивого кодирования данных и восстановления данных при частичном повреждении носителей информации.

1. Кодирование изображений при помощи кодов Рида-Соломона

В рамках модулярной арифметики (modular arithmetic) [10, 11], массив цифровых данных как набор целых чисел может быть представлен через сравнение по модулю как множество $[0, 1, \dots i, j, \dots I]$ для которого величина $(I+1)$ одновременно является модулем умножения и модулем сложения. Для ненулевого элемента x можно рассмотреть ряд произведений $[0 \cdot x, 1 \cdot x \dots i \cdot x, j \cdot x, , \dots I \cdot x]$. При двоичном кодировании конечное поле на базе кода Рида-Соломона будет включать в себя $2^{(I+1)}$ элементов. Таким образом, для последовательностей кода Рида-Соломона может быть использован тот же математический аппарат, что и для блочного линейного кода (N, K). Входной набор данных, который подлежит кодированию, представляется через K символов, а для их передачи необходимо использовать дискретный канал N раз [2, 3, 12, 13]. Далее в рамках модели предлагается перейти к полиному, в котором используется простое расширение поля a (primitive element), т.е. расширение конечного поля, обусловленное добавлением к полю одного элемента. Таким образом, элементы кода могут быть представлены через векторы в $(I+1)$-бит, что соответствует степеням полинома меньшим или равным I. В соответствии с данным подходом можно ввести для последовательностей кода Рида-Соломона понятие порождающего полинома (generator polynomial):

$$G(x) = \prod_{l=1}^{(N-K)} (x - a^l). \qquad (1)$$

Описание возможных комбинаций кодовой последовательности, представленной в виде конечного поля, как полинома $F\left(2^{(I+1)}\right)$, определяется через следующие полиномы:

$$F\left(2^{(I+1)}\right): \sum_{n=0}^{N} (f_n \cdot x^n), \qquad (2)$$

где f_n — элементы $F\left(2^{(I+1)}\right)$. Представление бинарного графического изображения при помощи кода Рида-Соломона (N, K) является линейным бинарным кодом $(N \cdot I, K \cdot I)$. В кодовой RS-последовательности любой произвольный элемент b полинома $F\left(2^{(I+1)}\right)$ замещается бинарной матрицей размерности $I \times I$, строки которой определяются как $\{b, b \cdot a, \dots, b \cdot a^I\}$, т.е. $\{b \cdot a^i\}$, где $i \in [0; I]$. Поскольку исходная кодовая последовательность масштабируется элементами полинома $F\left(2^{(I+1)}\right)$,

соответствующая последовательность при кодировании двоичного изображения должна быть представлена в виде линейной комбинации $(I+1)$ двоичных строк. Аналогично, если RS-генераторная матрица имеет размерность $K \times N$, причем все ее элементы входят в $F\left(2^{(I+1)}\right)$, значит, она может быть получена путем замены каждого элемента соответствующей двоичной матрицей размерности $I \times I$. Соответственно, если минимальное расстояние для элементов последовательности исходного кода составляет $D_{RS} = N + 1 - K$, минимальное расстояние для элементов двоичного изображения составляет $D_{BI} \geq D_{RS}$.

Следует отметить, что в ряде практических приложений по оцифровке графических изображений рассматриваются кодовые последовательности длиной $N \cdot I$ с большими минимальными расстояниями, но это вынуждает разработчиков изменять базовые алгоритмы представления элементов поля [14, 15].

2. Кодирование графов при восстановлении двумерных массивов

Методы анализа двумерных последовательностей RS-кода большого размера могут быть расширены до алгоритмов на основе теории графов, в частности кодирования двудольных графов [16-18]. Двудольный граф, также называемый биграфом — это граф, полное множество вершин которого можно разделить на две группы таким образом, что каждое ребро графа будет соединять вершину из первой группы с вершиной из второй группы.

В рамках данной модели в целях упрощения общей схемы алгоритма рассматривается случай регулярного биграфа, т.е. биграфа все вершины которого имеют n ребер, причем величина n соответствует длине компонент-кода. При этом если общее количество вершин равно v, общая длина кода N равна $n \cdot v$. Очевидно, что для получения кода большей длины, чем двумерный код необходимо выбрать $v \gg n$. Поскольку количество проверок четности в общем коде равно $2v \cdot (n-k)$, размерность полного кода с учетом линейно зависимых проверок составляет $K \geq 2v \cdot (k-n)$. Преимущество данного подхода состоит в том, что на его основе большие информационные блоки могут быть кодированы и декодированы на основе короткого компонент-кода с низкой нагрузкой на программно-аппаратную платформу. При этом обеспечивается высокая производительность при обеспечении доступа к определенному фрагменту кода, т.е. при частичном декодировании.

При разработке алгоритмов декодирования для обеспечения предпосылок построения эффективного механизма исправления ошибок в кодовой последовательности необходимо продумать вопрос связности графа и представить его в виде математической модели и ввести следующие понятия:

- расстояния между двумя вершинами графа;
- диаметр графа;
- обхват графа (graph girth), как длину наименьшего цикла;
- расширение графа (graph expansion).

В рамках предложенной модели расстояние между двумя вершинами графа может быть определено как длина кратчайшего пути от одной вершины к другой, что, в свою очередь, должно быть выражено через число ребер. Соответственно, диаметром графа, который для заданных значений n и v должен быть минимальным, будет наибольшим расстоянием между двумя точками. Обхват графа (graph girth) представляет собой полный путь от вершины к себе, который исчисляется в ребрах, т.е., обхват графа определяется как длина самой короткой цепи. Граф, который может быть эффективно использован в системах помехоустойчивого кодирования, должен иметь большой обхват. Показатель расширения графа для алгоритмов выбираются индивидуально, это свойство указывает на то, что для любого небольшого набора вершин Δ на минимальном расстоянии находится другое, существенно большее подмножество других вершин. Таким образом, возможные ошибки в одной части кодовой последовательности могут быть исправлены путем включения символов в другие части графа.

Эффективная работа с биграфами возможна через рассмотрение геометрии конечных полей [19-22]. Конечная евклидова плоскость конечного поля $F(Q)$ состоит из точек (x, y), соотношение между которыми описывается через линейное уравнение $y = a \cdot x + b$, причем коэффициенты a и b постоянны для $F(Q)$. Для соотношения типа $x = c$ введем множество вершин Q^2. Соответственно на основе этого подхода можно ввести понятие биграфа, для которого точечные вершины (x, y) и линейные вершины (a, b) соединяются ребрами для $y = a \cdot x + b$.

Кроме того, можно доказать, что при минимальной длине между элементами полной кодовой последовательности равной D, все частные кодовые последовательности (кодовые слова) характеризуются минимальным весом:

$$D_{CW} \geq D^3 - 2 \cdot D^2 + D. \qquad (3)$$

Соответственно, для ненулевых вершин существует D и более ребер, каждое из которых соединяется с $D \cdot (D-1)$ и более другими ребрами.

Выводы

В результате проведенного исследования был разработаны основы для построения математического аппарата, который в дальнейшем может быть использован для разработки систем помехоустойчивого кодирования двумерных блоков цифровых данных составных изображений. В частности были предложены:

- схема построения последовательностей кода Рида-Соломона на базе порождающего полинома;
- математическая модель представления двумерных последовательностей кода Рида-Соломона большого размера, которая основывается на теории кодирования двудольных графов;
- принципы работы с двудольными графами через рассмотрение геометрии конечных полей.

Разработанные модели, схемы и алгоритмы могут быть эффективно использованы при построении комплексной методологии помехоустойчивого кодирования данных и восстановления информация из частично поврежденных кодовых последовательностей.

Список литературы / References

1. *Stamplecoskie S.*, 2006. A study of the concatenated Reed Solomon: convolutional coding performance used in WiMAX. Ottawa: Defence R&D Canada - Ottawa.
2. *Sungkar M. & Berger T.*, 2018. Discrete Reconstruction Alphabets in Discrete Memoryless Source Rate-Distortion Problems. 2018 IEEE International Symposium on Information Theory (ISIT). doi:10.1109/isit.2018.8437835.
3. *Lei W., Yizhou G., Fucai Z. & Yong W.*, 2018. The Method to Recognize Linear Block Code Based on the Distribution of Code Weight. 2018 13th APCA International Conference on Control and Soft Computing (CONTROLO). doi:10.1109/controlo.2018.8439758.
4. *Ding W., Lu Y. & Wu F.*, 2007. Enable Efficient Compound Image Compression in H.264/AVC Intra Coding. 2007 IEEE International Conference on Image Processing. doi: 10.1109/icip.2007.4379161.
5. *Zhu W., Ding W., Xiong R., Shi Y. & Yin B.*, 2012. Compound image compression by multi-stage prediction. 2012 Visual Communications and Image Processing. doi: 10.1109/vcip.2012.6410758.
6. *Andre J., Owens D.A. & Harvey L.O.*, 2003. Visual perception: the influence of H.W. Leibowitz. Washington, DC: American Psychological Association.
7. *Slovak J., Bornholdt C., Bauer S., Kreissl J., Schlak M. & Sartoriu B.*, 2006. Novel concept for all-optical clock recovery from NRZ format PRBS data streams. 2006 Optical Fiber Communication Conference and the National Fiber Optic Engineers Conference. doi: 10.1109/ofc.2006.215908.
8. *Milster T.D. & Kim Y.S.*, 2017. Adaptive optics for data recovery on optical disk fragments (Conference Presentation). Optical Data Storage 2017: From New Materials to New Systems. doi: 10.1117/12.2277078.
9. *Masters G. & Turner P.*, 2007. Forensic data recovery and examination of magnetic swipe card cloning devices. Digital Investigation, 4, 16–22. doi: 10.1016/j.diin.2007.06.018.
10. *Sato N.*, 2009. Modular arithmetic. Ottawa: Canadian Mathematical Society = Société mathématique du Canada.
11. Hunter D.J., 2017. Essentials of discrete mathematics. Burlington, MA: Jones & Bartlett Learning.
12. *Jadhao M.G.*, 2012. Performance Analysis of Linear Block Code, Convolution code and Concatenated code to Study Their Comparative Effectiveness. IOSR Journal of Electrical and Electronics Engineering, 1(1), 53-61. doi:10.9790/1676-0115361.
13. *Mei T., Zhang C. & Dai Q.*, 2011. Using Linear Block Code and Concatenated Code to Build (k,n) Threshold Scheme. 2011 International Conference on Internet Technology and Applications. doi:10.1109/itap.2011.6006219.
14. *Kim S.*, 2017. Reversible Data-Hiding Systems with Modified Fluctuation Functions and Reed-Solomon Codes for Encrypted Image Recovery. Symmetry, 9(5), 61. doi: 10.3390/sym9050061.
15. *Chaari L., Fourati M. & Kamoun L.*, 2010. Image transmission quality analysis over adaptive Reed-Solomon coding. Melecon 2010 - 2010 15th IEEE Mediterranean Electrotechnical Conference. doi: 10.1109/melcon.2010.5476245.
16. Matching Viterbi Decoders and Reed-Solomon Decoders in a Concatenated System, 2009. Reed-Solomon Codes and Their Applications. doi: 10.1109/9780470546345.ch11.
17. Yedidia J. (n.d.). Sparse factor graph representations of reed-solomon and related codes. International Symposium OnInformation Theory, 2004. ISIT 2004. Proceedings. doi: 10.1109/isit.2004.1365296.
18. *Hoholdt T. & Justesen J.*, 2006. Graph Codes with Reed-Solomon Component Codes. 2006 IEEE International Symposium on Information Theory. doi: 10.1109/isit.2006.261904.
19. *Hirschfeld J.W.P., Korchmáros G. & Torres F.*, 2008. Algebraic curves over a finite field. Princeton (New Jersey): Princeton University Press.
20. *Nasseri M., Xiao X., Zhang S., Wang T. & Lin S.*, 2017. Concatenated finite geometry and finite field LDPC codes. 2017 11th International Conference on Signal Processing and Communication Systems (ICSPCS). doi: 10.1109/icspcs.2017.8270513.

21. *Lavrauw M. & Voorde G.V.D.*, 2015. Field reduction and linear sets in finite geometry. Topics in Finite Fields Contemporary Mathematics, 271–293. doi: 10.1090/conm/632/12633.
22. *Lavrauw M. & Zanella C.*, 2013. Geometry of the inversion in a finite field and partitions of PG(2k − 1, q) in normal rational curves. Journal of Geometry. 105 (1), 103–110. doi: 10.1007/s00022-013-0197-8.