УДК 681.391

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КОРРЕКЦИИ НЕИСПРАВНОСТЕЙ НА ОСНОВЕ КОДА ГАЛУА

Шаньгин В.Ф.[1], Зо Вин Хтет[1], Ян Наинг Со[2]

[1,2]Национальный исследовательский университет «МИЭТ», kyawzawye85@gmail.com
[2]Московский физико-технический институт, yannaingsoemephi@gmail.com

Предложен метод нерезервированной защиты от ошибок информационных потоков данных на основе нового класса кодов коррекции сигнала, в котором используются повторяющиеся свойства линейных и спиральных кодов полей Галуа. При передаче и приеме на основе предложенных кодов, дополнительные сигналы формируются на основе четырех знаков, которые связаны с элементами информационного сообщения в соответствии с кодами полей Галуа. В данной статье рассматривается использование коды полей Галуа для защиты информации от несанкционированного доступа и описывается математическая модель коррекции неисправностей на основе кода ГАЛУА.

Ключевые слова: код Галуа, кодовая последовательность, символические знаки, информационные биты.

MATHEMATICAL MODEL OF FAULTS CORRECTION BASE ON CODE GALOIS

Shangin V.F.[1], Zaw Win Htet[1], Yan Naing Soe[2]

[1]National Research University of Electronic Technology «MIET», kyawzawye85@gmail.com, [2]Moscow Institute of Physics and Technology, yannaingsoemephi@gmail.com

A method of non-redundant information for error protection of data streams based on a new class of signal-correcting codes, which are used in the linear properties and repetitive spiral Galois field codes. Transmission and reception on the basis of the proposed codes, additional signals are formed on the basis of four characters that are associated with elements of an information message according to the codes of Galois fields. This article discusses the use of codes of Galois fields to protect information from unauthorized access and describes a mathematical model based on fault correction code GALOIS. s development of electronic databases and technology elements packet data in a wireless network, introduction of new frequency bands, and the development of effective protocols functioning decentralized network with self-organizing data provide the conditions for large-scale penetration of radio technologies in the construction of industrial systems perspective.

Keywords: Galois code, code sequence, symbolic signs, information bits.

Современные тенденции развития электронных баз элементов и технологий пакетной передачи данных в беспроводной сети, внедрение новых частотных диапазонах, и разработка эффективных протоколов функционирования децентрализованной сети с самоорганизацией передачи данных обеспечивают условия для широкомасштабного проникновения радио технологий в области строительства перспективных систем промышленных.

Постановка задачи

В настоящее время коды полей Галуа широко используются для защиты информации от несанкционированного доступа [1-3]. Преимущества основы Галуа можно наиболее эффективно использовать при кодировании целых значений. Матрица кода Галуа нахождения и коррекции ошибок показана в рис.1.

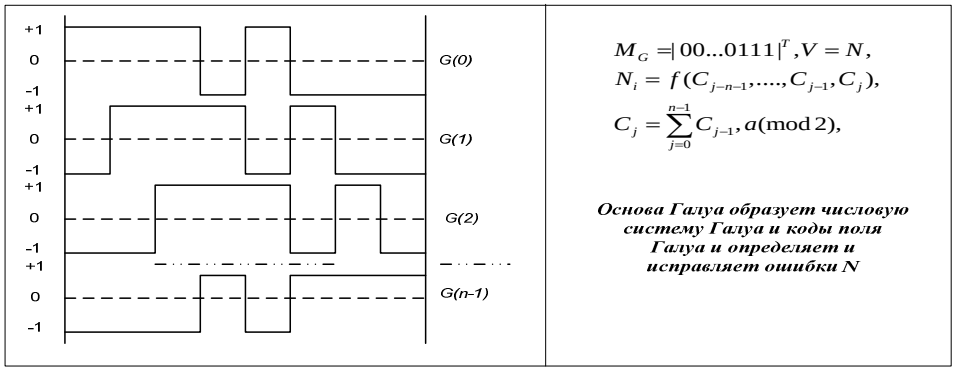

Рис.1. Матрица кода Галуа нахождения и коррекции ошибок

Для генерации Галуа коды полей $G\begin{pmatrix} n \\ 2 \end{pmatrix}$, Используются следующие примитивные алгебраические многочлены *[10]:*

$$4: x_1 \oplus x_4; 5: x_2 \oplus x_5; 6: x_1 \oplus x_6; 7: x_3 \oplus x_7; 8: x_2 \oplus x_4 \oplus x_3 \oplus x_8; 9: x_4 \oplus x_9;$$
$$10: x_3 \oplus x_{10}; 11: x_2 \oplus x_{11}; 12: x_1 \oplus x_4 \oplus x_6 \oplus x_{12}; 13: x_1 \oplus x_3 \oplus x_4 \oplus x_{13}; 14: x_1 \oplus x_6 \oplus x_{10} \oplus x_{14}; 15: x_1 \oplus x_{15};$$
$$16: x_1 \oplus x_3 \oplus x_{12} \oplus x_{16}; 17: x_3 \oplus x_{17}; 18: x_7 \oplus x_{18}; 19: x_1 \oplus x_2 \oplus x_5 \oplus x_{19}; 20: x_3 \oplus x_{20}; 21: x_2 \oplus x_{21};$$

$$22: x_1 \oplus x_{22}; 23: x_5 \oplus x_{23}; 24: x_1 \oplus x_3 \oplus x_4 \oplus x_{24}; 25: x_3 \oplus x_{25}; 26: x_1 \oplus x_2 \oplus x_6 \oplus x_{26}; 27: x_1 \oplus x_2 \oplus x_5 \oplus x_{27};$$
$$28: x_3 \oplus x_{28}; 29: x_2 \oplus x_{29}; 30: x_1 \oplus x_4 \oplus x_6 \oplus x_{30}; 31: x_7 \oplus x_{31}; 32: x_2 \oplus x_6 \oplus x_7 \oplus x_{32}. \quad (1)$$

Существуют также примитивные алгебраические многочлены для полей более высокого порядка $G\begin{pmatrix} n \\ p \end{pmatrix}$, где ***p*** является простым числом.

Важным преимуществом кодовой последовательности Галуа является простая генерация кодов на основе уравнения повторения.

Простейшие ключи кодов полей Галуа описываются выражением

$$G_i = G_{i-1} \oplus G_{1-m}; m \le n \quad (2)$$

Важным математическим и практически исключительным свойством последовательности Галуа является наличие повторяющихся соединений через уровни [3] с высокой энтропии характеристиками.

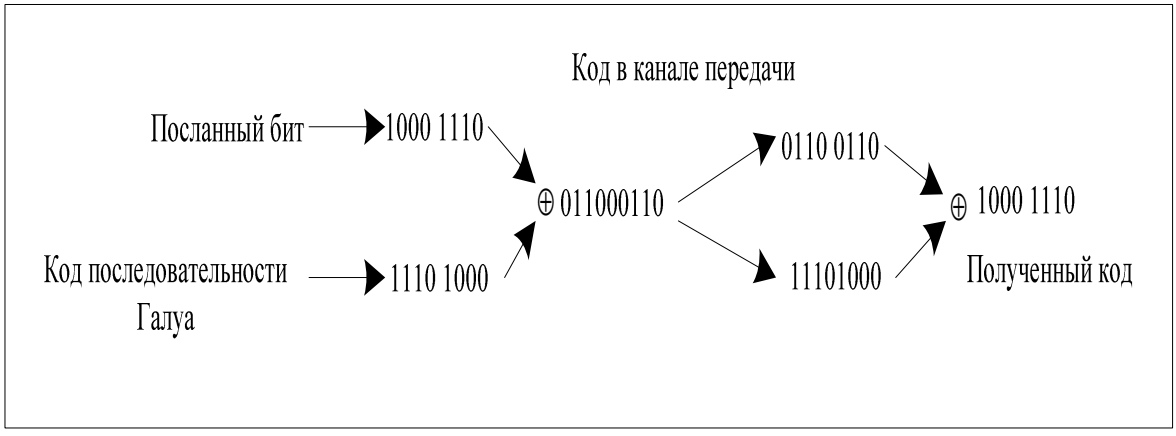

Рис.2. Кодирование данных на основе последовательности кода *G*.

Пусть следующий код поля Галуа с ключам $G_i = G_{i-1} \oplus G_{i-4}$ будет $G\begin{pmatrix}4\\2\end{pmatrix}$:

$G\begin{pmatrix}4\\2\end{pmatrix}$ =1111 01011 0010 0011 1101 0110 0100 0111 1010 1100 1000 1111 0101

Этот код может быть сложен в спираль , и для каждого из четырех образующих, получается повторяющаяся последовательность, имеющая соответствующие периодические свойства кода в базе Галуа [2, 4].

После разматывания спирали, которая кодируется повторяющимся кодом поля Галуа, повторная последовательность формируется путем уровней в соответствии с выражением

$$G_{i-j} = G_{i-4,j} \oplus G_{i-16,j}, \; j = \overline{1,4}, \tag{3}$$

или в общем случае,

$$G_i = G_{i-4^v} \oplus G_{i-4^{v+1}}, v = 0,1,2,3, \tag{4}$$

С учетом свойств спирали, повторный код сигнала может быть использован для обнаружения и коррекции совокупности ошибок, так как ошибки сначала находятся и исправлены в соответствии с выражением (2), а затем в соответствии с выражением (3) вдоль образующих спирали [4].

Предложен метод нерезервированной защиты от ошибок информационных потоков данных на основе нового класса кодов коррекции сигнала, в котором используются повторяющиеся свойства линейных и спиральных кодов полей Галуа. При передаче и приеме на основе предложенных кодов, дополнительные сигналы формируются на основе четырех знаков $(\downarrow, \uparrow, +, -)$, которые связаны с элементами информационного сообщения в соответствии с кодами полей Галуа [2, 3, 4]. Принцип формирования код полей Галуа для коррекции сигнала выглядит следующим образом: биты, равные «1», пронумерованы в совокупности данных с помощью повторного кода поля Галуа $G\begin{pmatrix}n\\2\end{pmatrix}$ [4]. В этом случае, для единиц совокупности данных, бит Галуа равный «1» передается знаком ($\uparrow$) ,а бит Галуа равный «0» передается знаком ($\downarrow$). Биты, равные нулям, совокупности данных также пронумерованы повторным кодом поля Галуа $G\begin{pmatrix}n\\2\end{pmatrix}$. Для нулей в совокупности данных, Галуа бит, равный «1», передается положительным потенциалом « + » , и бит Галуа, равный «0» передается отрицательным потенциалом « - » . В качестве этих четырех знаков манипуляции на физическом уровне, можно использовать коллекции, состоящие из четырех

фаз, частоты, *M* - последовательности, коды Баркера, шум подобные сигналы, а также их другие варианты.

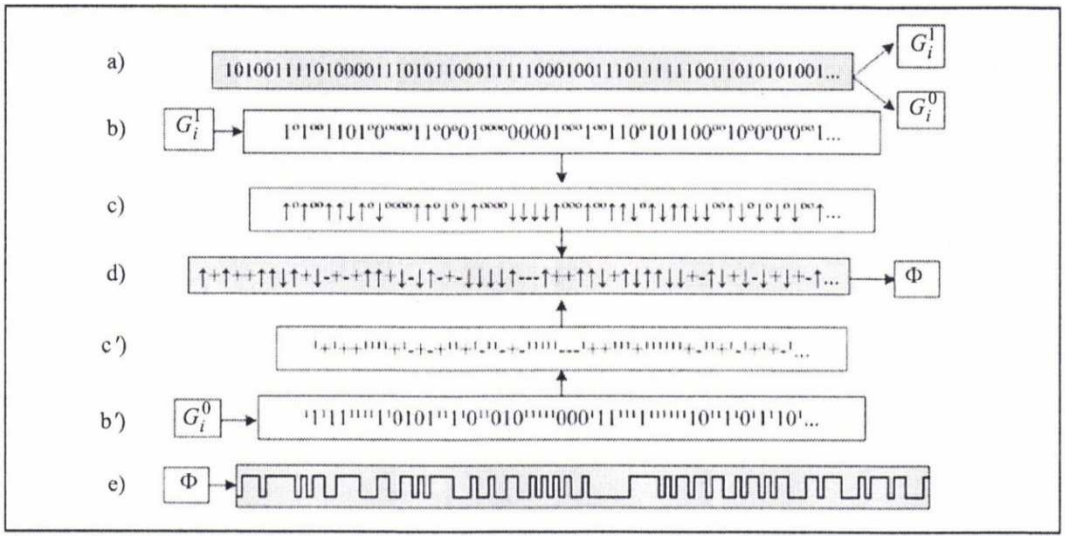

Рис.3. Структура формирования сигналов, обработанных кодом на основе полевых кодов *G*

Структура формирования сигналов на основе кодов полей Галуа представлена на рис.3, где G_i^1 и G_i^0 являются генераторами битов Галуа для символов «1» и «0», соответственно, а *Ф* образует выходные дополнительные сигналы; Здесь,

(a) разделение входного потока информации на «0» и «1»;

(b, b') кодирование потоков единиц и нулей кодов Галуа;

(c,c') представление битов Галуа символическими знаками;

(d) мультиплексирование символических знаков «1» и «0»;

(e) манипулирование высокой энтропии выходного сигнала на физическом уровне.

Результаты и заключение

На Рисунке (4) показана схема реализации обнаружения и исправления ошибок в сигналах, образованных кодом на физическом уровне, где *N*- это количество позиций битов в информационном сообщении,*D* - это информационные биты полученных данных с обнаруженными и исправленными ошибками, S_gC - код сигнала, $G_2^4(1)$ и $G_2^4(0)$ соответственно, биты Галуа $G\binom{4}{2}$ для информационных битов «1»и «0» с обнаружением и исправлением ошибок, и «0 *» и «1 *» - это ошибочные биты. Возможны еще следующие два случая идентификации битов Галуа: инвертирование знака бита Галуа, равного «1» или «0» и замена сигнальных знаков (↑) и (↓) на «+» или « - » и наоборот. Во всех случаях, ошибка обнаруживается и исправляется декодером Галуа аппаратно-программного обеспечения.

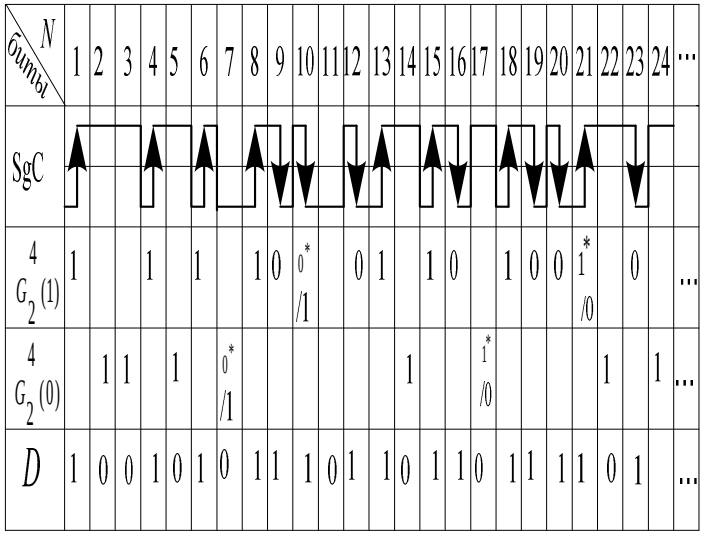

Рис.4. Схема реализации нахождения и коррекции ошибок в сигналах, обработанных кодом

Таким образом, эффективное симметричное кодирование приводится в форме кодов полей Галуа последовательностью нулей и единиц блока данных с однозначным определением их числа $N_0+N_1=N_D$, используемое для выявления и исправления ошибок, т.е. обнаружения выпадений и вставок отдельных битов или их совокупностей после передачи данных.

Список литературы

1. Лисов О.И., Чжо Зо Е, Пайе Тэйн Наинг, Марков А. Б. Оценка качества систем управления технологическими процессами на этапах жизненного цикла// Оборонный комплекс − научно-техническому прогрессу России. -М.: ФГУП “ВИМИ”, 2014.- № 2. .- С.34-37.
2. ЧжоЗо Е, Кукушкин Е.С., Лисов О.И. Методика поиска неисправностей в многокомпьютерных вычислительных системах на основе “И-ИЛИ” графов// Оборонный комплекс − научно-техническому прогрессу России. -М.: ФГУП “ВИМИ”, 2012.- № 1.- С.71-75.
3. ЧжоЗо Е, ТайкАунгЧжо, ПайеТэйнНаинг. Модели обнаружения и технической диагностики неисправностей объектов в приборостроении// вести высших учебных заведений черноземья- №3 (33) 2013- С.32-36.
4. ЧжоЗо Е. Методика синтеза оптимальной структуры распределенной вычислительной системы // Журнал «Оборонный комплекс − научно-техническому прогрессу России». -М.: ФГУП “ВИМИ”,2014.- № 1.- С.25-29.

5. Чжо Зо Е, Хтет Мин Пью, Гагарина Л.Г. Методика оптимизации однопроцессорной обработки запросов баз данных// Журнал «Межотраслевая информационная служба». - М.: ФГУП “ВИМИ”,2014.- № 2 .- С.35-41.

6. KyawZaw Ye, HtikeAungKyaw, Portnov E. M., Gagarina L. G., Bain A. M. Development of algorithm and method for multi-machine troubleshooting systems based on technical diagnostics// World Applied Sciences Journal 32 (6): 1121-1129, 2014; ISSN 1818-4952 © IDOSI Publications, 2014; DOI: 10.5829/idosi.wasj. 2014.32.06.657.

Рецензенты:

Гагарина Л. Г., д.т.н., профессор, заведующий кафедрой «Информатика и программное обеспечение вычислительных систем» Национального исследовательского университета «МИЭТ», г.Москва;

Портнов Е.М., д.т.н., профессор кафедры «Информатика и программное обеспечение вычислительных систем», начальник научно-исследовательской лаборатории «Управляющие информационные системы» Национального исследовательского университета «МИЭТ», г.Москва.