http://dx.doi.org/10.35596/1729-7648-2020-18-4-20-27

Оригинальная статья
Original paper

УДК 004.056.55

АВТОМОРФИЗМЫ И ОРБИТЫ ОШИБОК КОДОВ РИДА – СОЛОМОНА

СЕМЁНОВ С.И., ЛИПНИЦКИЙ В.А.

Военная академия Республики Беларусь (г. Минск, Республика Беларусь)

Поступила в редакцию 14 октября 2019

Аннотация. Цель работы, результаты которой представлены в рамках статьи, заключалась в развитии и переносе на класс кодов Рида – Соломона (РС-кодов) базовых положений теории норм синдромов (ТНС), разработанных ранее для активно применяемого в теории и практике помехоустойчивого кодирования класса кодов Боуза – Чоудхури – Хоквингема (БЧХ-кодов). Для достижения поставленной цели осуществлен переход в изложении теории РС-кодов с полиномиального языка на матричный. Такой подход позволяет в полной мере использовать возможности теории полей Галуа. Главная сложность РС-кодов в том, что они опираются на недвоичный алфавит. Этот же фактор является привлекательным для практических применений РС-кодов. Матричный язык позволяет разбивать синдромы ошибок на компоненты, являющиеся элементами поля Галуа – поля определения РС-кодов. ТНС для БЧХ-кодов опирается на применение автоморфизмов этих кодов – циклических и циклотомических подстановок. В работе подробно изучены автоморфизмы РС-кодов. Циклическая подстановка относится к разрядам автоморфизмов РС-кодов и порождает подгруппу Г порядка N (длина кода). Циклотомическая подстановка не принадлежит классу автоморфизмов РС-кодов – мощность алфавита, большая 2, препятствует этому. При расширении понятия автоморфизма кода за рамки перестановок координат векторов к автоморфизмам РС-кодов можно отнести и гомотетии, или аффинные подстановки, поскольку они также образуют циклическую группу А порядка N. Показано, что циклическая и аффинная подстановки коммутируют друг с другом, что, вообще говоря, не типично для линейных операторов и подстановок. Группа Г циклических подстановок, группа А аффинных подстановок и объединенная АГ группа порядка N^2 порождают 3 вида орбит ошибок в РС-кодах. Изучено строение орбит ошибок относительно действия групп А, Г и объединенной группы АГ {231 слово}.

Ключевые слова: линейный код, РС-код, синдромы ошибок, автоморфизмы кодов, циклическая подстановка, аффинная подстановка, орбиты векторов-ошибок, теория норм синдромов.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Семёнов С.И., Липницкий В.А. Автоморфизмы и орбиты ошибок кодов Рида – Соломона. Доклады БГУИР. 2020; 18(4): 20-27.

AUTOMORPHISMS AND ERROR ORBITS OF REED – SOLOMON CODES

SERGEY I. SEMYONOV, VALERY A. LIPNITSKY

Military academy of the Republic of Belarus (Minsk, Republic of Belarus)

Submitted 14 Oktober 2019

Abstract. The purpose of this work with its results presented in the article was to develop and transfer to the class of Reed – Solomon codes (RS-codes) the basic provisions of the theory of syndrome norms (TNS), previously developed for the noise-resistant coding of the class of Bose – Chaudhuri – Hocquenghem codes (BCH-codes), which is actively used in theory and practice. To achieve this goal, a transition has been made in the interpretation of the theory of RS-codes from polynomial to matrix language. This approach allows you to fully use the capabilities of Galois field theory. The main difficulty of RS-codes is that they rely on a non-binary alphabet. The same factor is attractive for practical applications of RS-codes. The matrix language allows you to break the syndromes of errors into components that are elements of the Galois field – the field of definition of RS-codes. The TNS for BCH codes is based on the use of automorphisms of these codes – cyclic and cyclotomic substitutions. Automorphisms of RS-codes are studied in detail. The cyclic substitution belongs to the categories of automorphisms of RS-codes and generates a subgroup Γ of order N (code length). The cyclotomic substitution does not belong to the class of automorphisms of RS-codes – the power of the alphabet greater than 2 prevents this. When expanding the concept of automorphism of a code beyond substitutions of coordinates of vectors to automorphisms of RS-codes, homotheties or affine substitutions can be attributed, since they also form a cyclic group A of order N. It is shown that cyclic and affine substitutions commute with each other, which, generally speaking, is not typical for linear operators and substitutions. The group Γ of cyclic substitutions, the group A of affine substitutions, and the combined AΓ group of order N^2 generate 3 types of error orbits in RS-codes. The structure of the orbits of errors with respect to the action of groups A, Γ and the combined group AΓ is studied {231 words}.

Keywords: linear code, RS-code, error syndromes, automorphisms of codes, cyclic substitution, affine substitution, orbits of error vectors, theory of norms of syndromes.

Conflict of interests. The authors declare no conflict of interests.

For citation. Semyonov S.I., Lipnitsky V.A. The automorphisms and error orbits of Reed – Solomon codes. Doklady BGUIR. 2020; 18(4): 20-27.

Введение

Одним и самым главным из средств повышения помехоустойчивости в цифровых системах передачи и обработки данных является использование помехоустойчивого кодирования. Среди массово применяемых линейных помехоустойчивых кодов следует отметить коды Рида – Соломона [1–4]. Эти коды нашли широкое применение в самых различных современных системах передачи и хранения информации [4].

Эффективному применению РС-кодов способствовали следующие их преимущества:

– алфавит не двоичный, что позволяет сделать компактной обработку РС-кода и работу с ним;

– благодаря мощности алфавита при относительно малых длинах спектр исправляемых ошибок весьма широк.

Определение РС-кодов близко к определению БЧХ-кодов. Однако разработанная для БЧХ-кодов теория норм синдромов, позволяющая широко и эффективно использовать теорию полей Галуа при их обработке, остается пока не развитой на класс РС-кодов. Именно разработке и развитию последнего вопроса и посвящена данная статья.

Необходимые сведения о кодах Рида – Соломона

Коды Рида – Соломона – линейные блоковые коды [5], обнаруживающие и исправляющие ошибки, которые возникают под влиянием помех в каналах передачи информации. В общем случае код Рида – Соломона представляет собой БЧХ-код длиной $N = q - 1$ над полем Галуа $GF(q)$ из q элементов, где $q = p^m > 2$ для простого числа p и натурального $m \geq 1$ [3]. Так как РС-коды являются линейными, то они обладают следующими важными свойствами: 1) сумма двух кодовых слов является кодовым словом; 2) произведение любого кодового слова на элемент поля Галуа также является кодовым словом.

Для работы применяют полиномиальный или матричный способы задания РС-кодов.

В первом случае РС-код задается с помощью порождающего многочлена вида $g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \cdot \ldots \cdot (x - \alpha^{b+\delta-2})$, где α – примитивный элемент поля $GF(q)$, b и δ – фиксированные целые числа.

Кодирование осуществляется с помощью сдвига полинома сообщения $m(X)$ в первые k разряды регистра кодового слова и прибавлением в крайние левые $n–k$ разряды полинома четности $p(x) = (X^{n-k} m(X)) \bmod g(X)$.

Декодирование осуществляется с помощью вычисления синдромов ошибок и дальнейшим нахождением локатора и полинома ошибок на основании полученных значений синдромов по известным алгоритмам Питерсона – Горенстейна – Цирлера, Берлекэмпа – Месси и алгоритму Форни [1, 4, 7].

Во втором случае кодирование осуществляется с помощью порождающей матрицы кода G по формуле $\overline{c} = \overline{i} \cdot G$, где $\overline{i}$ – информационный вектор с K координатами.

Проверочная матрица РС-кода совпадает с матрицей H БЧХ-кода с элементами, принадлежащими полю $GF(q)$:

$$H = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \ldots & \alpha^{(N-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \ldots & \alpha^{(N-1)(b+1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \ldots & \alpha^{(N-1)(b+\delta-2)} \end{bmatrix}. \quad (1)$$

Матрица имеет размерность $(\delta - 1) \times N$ и ранг δ–1 над полем $GF(q)$.

На практике, как правило, используют РС-коды с b=1. Тогда проверочная матрица (1) принимает вид

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(N-1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \ldots & \alpha^{(N-1)(\delta-1)} \end{bmatrix} = [\alpha^i, \alpha^{2i}, ..., \alpha^{(\delta-1)i}]^T. \quad (2)$$

Как можно заметить, проверочная матрица (1) задает циклический код с порождающим полиномом $g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \cdot \ldots \cdot (x - \alpha^{b+\delta-2})$.

РС-коды будем в дальнейшем обозначать через $RS(N, K)$ [6], где N – длина РС-кода, $K = N - \deg g(x) = N - \delta + 1$ – количество информационных символов, размерность кода. Минимальное расстояние РС-кода равно $D = N - K + 1 = \delta$ ([1], с. 289).

Векторы ошибок в РС-кодах

Векторы-ошибки в кодах $RS(N, K) = RS(q - 1, q - \delta)$ принадлежат $(q-1)$-мерному векторному пространству $V_N(GF(q))$ над полем Галуа $GF(q)$. Поэтому в данном коде имеется: всего $(q-1)^2$ ошибок весом 1; двойных – $C_{q-1}^2 \cdot (q-1)^2$; ошибок весом $\omega \geq 1$ – $C_{q-1}^{\omega} \cdot (q-1)^{\omega}$,

что в $(q-1)^{\omega}$ раз больше, чем у двоичного БЧХ-кода той же длины. Как видим, с ростом N и ω количество исправляемых РС-кодом ошибок стремительно растет. Конечно, появление векторов ошибок, вес которых больше минимального расстояния D, должно быть крайне маловероятным, иначе возникнут проблемы с работой ТКС. Все же векторы ошибок весом, меньшим D, обнаруживаемы кодом $RS(N,K)$ и исправляемы, если их вес $t \le \dfrac{D-1}{2}$ для нечетных D и $t \le \dfrac{D-2}{2}$ – для четных значений D.

Декодирование ошибок весом, больше 1, при полиномиальном задании РС-кодов реализуется достаточно громоздкими процедурами, что достаточно ярко показали исследования в работе [7]. Теория норм синдромов продемонстрировала эффективность применения орбит ошибок в БЧХ-кодах. Построение аналогичной теории для РС-кодов еще предстоит и требует рассмотрения автоморфизмов этих кодов, имеющих, однако, определенную специфику.

Автоморфизмы РС-кодов

Данное понятие в помехоустойчивом кодировании введено с сильной ориентацией на двоичные коды [1]. По сути, это перестановки координат векторов, переводящие все кодовые слова в кодовые. Первый, хорошо известный пример таких перестановок дает лемма 1.

Лемма 1. РС-код с проверочной матрицей (1) является циклическим, то есть оператор σ, действующий на каждый вектор $\overline{e} = (e_1, e_2, ..., e_N) \in V_N(GF(q))$ по правилу $\sigma(\overline{e}) = (e_N, e_1, e_2, ..., e_{N-1})$, кодовые слова кода $RS(N,K) = RS(q-1, q-\delta)$ преобразует в кодовые.

Доказательство повторяет обоснование аналогичного утверждения для БЧХ-кодов.

Повторное применение оператора σ порождает его степени σ^2, σ^3 и т. д. Эти степени составляют циклическую группу $\Gamma = \{\sigma, \sigma^2, ..., \sigma^N = e\}$ порядка N. Здесь e, разумеется, есть тождественный оператор.

Однако следует признать, что полной аналогии с БЧХ-кодами здесь не наблюдается. К примеру, циклотомическая подстановка [1, 2] в циклических двоичных БЧХ-кодах, кодах Хемминга и реверсивных кодах – есть автоморфизм в названных кодах. Но из-за наличия ненулевых и неединичных координат у кодовых слов РС-кодов к автоморфизмам кодов $RS(N,K)$ циклотомическая подстановка принадлежать не может.

Вспомним, что РС-коды принадлежат классу линейных кодов. Всякий же линейный (N,K)-код есть K-мерное подпространство в N-мерном линейном пространстве над полем определения кода. Одними из базовых понятий линейной алгебры являются понятия линейного оператора и линейного преобразования векторных пространств [8]. Линейные невырожденные преобразования векторных пространств – математический синоним автоморфизмов этих пространств.

Пусть $GF(q)^*$ – мультипликативная группа поля $GF(q)$, то есть множество всех ненулевых элементов этого поля, образующих группу относительно операции умножения, причем группу циклическую [9, 10]. Естественный пример автоморфизмов кодов как невырожденных линейных операторов, не относящихся к классу перестановок координат векторов, предоставляет лемма 2.

Лемма 2. Преобразования $f_\gamma : \overline{x} \to \gamma\overline{x}$ $(q-1)$-мерного векторного пространства E_{q-1} над полем $GF(q)$ – пространства ошибок кода $RS(N,K) = RS(q-1, q-\delta)$ – являются невырожденными линейными преобразованиями этого пространства для всякого $\gamma \in GF(q)^*$, преобразуют кодовые слова кода $RS(N,K)$ в кодовые слова этого же кода.

Доказательство первой части леммы очевидно. Если вектор $\overline{x}$ принадлежит коду $RS(N,K)$, то для проверочной матрицы H этого кода $\overline{x}H^T = \overline{0}$. При этом $f_\gamma(\overline{x}) \cdot H^T = (\gamma\overline{x})H^T = \gamma(\overline{x}H^T) = \gamma\overline{0}$. Следовательно, $f_\gamma(\overline{x})$ также принадлежит коду $RS(N,K)$.

Преобразования f_γ носят название гомотетий, или аффинных преобразований. Легко видеть, что они образуют группу относительно операции композиции отображений, изоморфную циклической группе $GF(q)^*$ порядка $q-1$. Группу аффинных преобразований, в соответствии с их названием, будем обозначать символом А. В силу своей цикличности группа А имеет следующую структуру: $\mathrm{A} = < f_\alpha > = \left\{ f_\alpha, f_{\alpha^2}, ..., f_{\alpha^N} = e \right\}$ для примитивного элемента α поля $GF(q)$, образующей мультипликативной группы $GF(q)^*$.

Автоморфизмы любого линейного кода C образуют группу $AutC$ относительно операции композиции отображений. Группы Г и А являются подгруппами группы $Aut(RS(N,K))$. Они не имеют общих элементов, за исключением тождественного оператора e. Имеет место следующее, довольно редкое для подстановок и линейных операторов свойство.

Лемма 3. Операторы f_γ и σ коммутируют друг с другом: $\sigma f_\gamma = f_\gamma \sigma$.

Доказательство. Для произвольного вектора $\overline{e} = (e_1, e_2, ..., e_N) \in V_N(GF(q))$ вектор $f_\gamma(\sigma(\overline{e})) = (\gamma e_N, \gamma e_1, \gamma e_2, ..., \gamma e_{N-1})$, а вектор $\sigma(f_\gamma(\overline{e})) = (\gamma e_N, \gamma e_1, \gamma e_2, ..., \gamma e_{N-1}) = f_\gamma(\sigma(\overline{e}))$, что и требовалось доказать.

В силу леммы 3 минимальная подгруппа группы $Aut(RS(N,K))$, содержащая подгруппы А и Г, совпадает с их прямым произведением АГ$= \left\{ f_\alpha^i \cdot \sigma^j \,\middle|\, 0 \le i \le q-2; 0 \le j \le q-2 \right\}$ и имеет порядок $(q-1)^2$.

Орбиты ошибок в РС-кодах

Как предлагает теория норм синдромов [2], все векторы-ошибки в коде $RS(N,K)$ будем распределять по небольшим попарно-непересекающимся множествам – орбитам. Если на множестве векторов-ошибок действует некоторая группа G, то G-орбита $< \overline{e} >_G$ представляет собой совокупность всех попарно различных векторов-ошибок $g(\overline{e})$ для заданного фиксированного вектора-ошибки $\overline{e}$ и всех элементов $g \in G$. Естественно, структура всякой G-орбиты существенно зависит от свойств, сложности и строения самой группы G. G-орбита называется полной, если ее мощность равна мощности группы G.

Так, для $G = \Gamma$ имеем хорошо описанное для двоичных кодов в монографии [2] циклическое строение Г-орбит: $< \overline{e} >_\Gamma = \left\{ \overline{e}, \sigma(\overline{e}), \sigma^2(\overline{e}), ..., \sigma^{\nu-1}(\overline{e}) \right\}$. Здесь ν – наименьшее целое положительное число с условием $\sigma^\nu(\overline{e}) = \overline{e}$; как правило, $\nu = N$, и в отдельных, редких случаях ν является делителем N. При $\nu = N$ Г-орбита содержит максимально возможное количество векторов и потому является полной.

Значение $\nu < N$ возможно только в случае, когда вес вектора $\overline{e}$ является делителем числа N при внутренней симметрии расположения ненулевых координат.

Пример 1. В пространстве $V_{15}(GF(2^4))$ вектор $\overline{e} = (\beta,0,0,0,0,\beta,0,0,0,0,\beta,0,0,0,0)$ с произвольной координатой $\beta \in GF(2^4)^*$ порождает Г-орбиту мощностью $\nu = 5$.

Лемма 4. Для каждого $\beta \in GF(q)^*$ и всех степеней $\alpha^i, 0 \le i \le q-2$, примитивного элемента $\alpha \in GF(q)$ справедливо неравенство $\beta \cdot \alpha^i \ne \beta \cdot \alpha^j$ при $0 \le i < j \le q-2$.

Благодаря лемме 4, имеем следующую структуру А-орбит для всякого вектора $\overline{e} \ne \overline{0}$: $< \overline{e} >_\mathrm{A} = \left\{ \overline{e}, f_\alpha(\overline{e}), f_{\alpha^2}(\overline{e}), ..., f_{\alpha^{N-1}}(\overline{e}) \right\}$. Все ненулевые А-орбиты являются полными.

Лемма 5. Под действием оператора σ всякая А-орбита $<\overline{e}>_{\text{А}}$ преобразуется в А-орбиту $<\sigma(\overline{e})>_{\text{А}}$. Под действием оператора f_γ всякая Г-орбита $<\overline{e}>_{\Gamma}$ преобразуется в Г-орбиту $<f_\gamma(\overline{e})>_{\Gamma}$. Мощности Г-орбит $<\overline{e}>_{\Gamma}$ и $<f_\gamma(\overline{e})>_{\Gamma}$ совпадают.

Из леммы 5 вытекает строение АГ-орбит.

Теорема 1. Для каждого вектора $\overline{e}\neq\overline{0}$ АГ-орбита $<\overline{e}>_{\text{АГ}}$ состоит из $\nu(q-1)$ векторов для $\nu=N$ или для ν, делящего N, и имеет следующую структуру: $<\overline{e}>_{\text{АГ}}=\left\{<\overline{e}>_{\text{А}},<\sigma(\overline{e})>_{\text{А}},...,<\sigma^{\nu-1}(\overline{e})>_{\text{А}}\right\}$ или $<\overline{e}>_{\text{АГ}}=\left\{<\overline{e}>_{\Gamma},<(\alpha\overline{e})>_{\Gamma},...,<(\alpha^{q-2}\overline{e})>_{\Gamma}\right\}$.

В качестве примера представим на рис. 1 изображение полной АГ-орбиты векторов-ошибок в РС-коде длиной N.

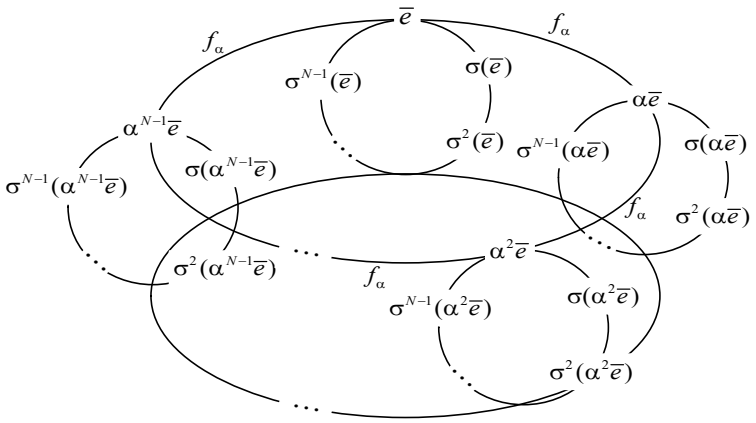

Рис. 1. Схема полной АГ-орбиты в РС-коде длиной N
Fig. 1. Diagram of a complete АГ-orbit in a RS-code of length N

Здесь малые овалы представляют собой Г-орбиты, переходящие друг в друга под действием автоморфизма f_α – умножения координат векторов на примитивный элемент α поля Галуа $GF(q)$.

Пусть K – множество всех корректируемых кодом $RS(N,K)$ векторов-ошибок мощностью $|K|$. Множество K разбивается на множества Г-орбит K_Γ, А-орбит $K_{\text{А}}$ и АГ-орбит $K_{\text{АГ}}$. Очевидно, $|K_{\text{А}}|=\dfrac{1}{q-1}\cdot|K|$. Мощность K_Γ оценивается той же величиной $|K_\Gamma|=\dfrac{1}{q-1}\cdot|K|$. На деле $|K_{\text{А}}|$ может оказаться несколько больше при наличии неполных Г-орбит. Аналогично $|K_{\text{АГ}}|$ оценивается величиной $|K_{\text{АГ}}|=\dfrac{1}{(q-1)^2}\cdot|K|$.

Далее, в данной работе конкретные вычисления будем проводить с кодами $RS(N,K)$, у которых $b=1$, $\delta=5$, $q=2^m$, $m>1$, а проверочная матрица имеет вид

$$H=\begin{bmatrix}1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1}\\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(N-1)}\\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(N-1)}\\ 1 & \alpha^4 & \alpha^8 & \cdots & \alpha^{4(N-1)}\end{bmatrix}=[\alpha^i,\alpha^{2i},\alpha^{3i},\alpha^{4i}]^T. \qquad (3)$$

В этом коде множество K состоит из векторов-ошибок весом 1 и 2, общее количество которых $|K|=(q-1)^2+C_N^2(q-1)^2=(q-1)^2\left(1+C_N^2\right)$. Следовательно, $|K_{\text{А}}|=(q-1)\left(1+C_N^2\right)$. Поскольку $N=q-1$ нечетно, то все Г-орбиты двойных ошибок являются полными, а потому

$|K_{\Gamma}| = (q-1)\left(1+C_N^2\right)$. Все ошибки весом 1 образуют, очевидно, одну полную АГ-орбиту. Двойные ошибки также делятся на полные АГ-орбиты. Поэтому $|K_{АГ}| = 1+C_N^2$. В частности, при $N = 7$ $|K| = 1078$, $|K_{А}| = |K_{\Gamma}| = 154$, $|K_{АГ}| = 22$.

Заключение

В работе предпринято развитие основ теории норм синдромов на семейства кодов Рида – Соломона. В основу исследований положено матричное задание этих кодов. Изучены естественные автоморфизмы на РС-кодах – циклические и аффинные подстановки. Исследованы основные свойства названных автоморфизмов, группы, ими порожденные, а также строение орбит ошибок в РС-кодах относительно группы Г циклических, группы А аффинных подстановок и объединенной АГ-группы.

Список литературы

1. MacWilliams F.J., Sloan J.J. *The Theory of Error-Correcting Codes*. Amsterdam: North-holland publishing company; 1977.
2. Липницкий В.А., Конопелько В.К. *Норменное декодирование помехоустойчивых кодов и алгебраические уравнения*. Минск: БГУ; 2007.
3. Кудряшов Б.Д. *Основы теории кодирования*. Санкт-Петербург: БХВ-Петербург; 2016.
4. Скляр Б. *Цифровая связь. Теоретические основы и практическое применение*. Изд. 2. Москва: Вильямс; 2003.
5. Блэйхут Р. *Теория и практика кодов, контролирующих ошибки*. Москва: Мир; 1986.
6. Moon T.K. *Error correction coding, mathematical methods and algorithms*. New Jersey U.S.A: John Wiley & Sons; 2005.
7. Липницкий В.А., Семёнов С.И. Преимущества применения теории полей Галуа для обработки РС-кодов. *Сборник научных статей Военной академии Республики Беларусь*. 2019;36:84-93.
8. Липницкий В.А. *Высшая математика. Основы линейной алгебры и аналитической геометрии*. Минск: ВА РБ; 2015.
9. Лидл Р., Ниддеррайтер Г. *Конечные поля*. Москва: Мир; 1988.
10. Липницкий В.А. *Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа*. Минск: БГУИР; 2006.

References

1. MacWilliams F.J., Sloan J.J. *The Theory of Error-Correcting Codes*. Amsterdam: North-holland publishing company; 1977.
2. Lipnitsky V.A., Konopelko V.K. [*Norm decoding of noise-resistant codes and algebraic equations*]. Minsk: BGU; 2007. (In Russ.)
3. Kudryashov B.D. [*Fundamentals of coding theory*]. St. Petersburg: BHV-Petersburg; 2016. (In Russ.)
4. Sclyar B. [*Digital communications. Fundamentals and Applications*]. Ed. 2. Moscow: Wil'ams; 2003. (In Russ.)
5. Blejhut R. [*Theory and practice of error control codes*]. Moscow: Mir; 1986. (In Russ.)
6. Moon T.K. *Error correction coding, mathematical methods and algorithms*. New Jersey U.S.A: John Wiley & Sons; 2005.
7. Lipnitsky V.A., Semyonov S.I. [Advantages of using Galois field theory for processing RS-codes]. *Sbornik nauchnyh statey Voennoy academii Respubliki Belarus = Sbornik nauchnyh statey Voennoy academii Respubliki Belarus*. 2019:36:84-93. (In Russ.)
8. Lipnitsky V.A. [*Higher mathematics. Fundamentals of linear algebra and analytic geometry*]. Minsk: VA RB; 2015. (In Russ.)
9. Lidl R., Nidderrajter G. [*Finite fields*]. Moscow: Mir; 1988. (In Russ.)
10. Lipnitsky V.A. [*Modern applied algebra. Mathematical fundamentals of protecting information from interference and unauthorized access*]. Minsk: BGUIR; 2006. (In Russ.)

Вклад авторов

Семёнов С.И. провел компьютерные вычисления, необходимые по содержанию статьи, непосредственно оформлял текст статьи.

Липницкий В.А. определил тему статьи и ее структуру, осуществлял консультативное руководство по работе над статьей.

Authors' contribution

Semyonov S.I. conducted computer calculations necessary for the content of the article and directly designed the text of the article.

Lipnitsky V.A. determined the topic of the article and its structure and provided advisory guidance on the work on the article.

Сведения об авторах

Семёнов С.И., м.т.н., адъюнкт кафедры информационно-вычислительных систем Военной академии Республики Беларусь.

Липницкий В.А., д.т.н, профессор, заведующий кафедрой высшей математики Военной академии Республики Беларусь.

Адрес для корреспонденции

220057, Республика Беларусь,
г. Минск, пр-т Независимости, 220,
Военная академия Республики Беларусь
тел. +375-29-593-24-07;
e-mail: semyonov4213@gmail.com
Семёнов Сергей Иванович

Information about the authors

Semyonov S.I., M.Sci., PG student of Information and Computing Systems Department of Military Academy of the Republic of Belarus.

Lipnitsky V.A., D.Sci., Professor, Head of High Mathematics Department of Military Academy of the Republic of Belarus.

Address for correspondence

220057, Republic of Belarus,
Minsk, Nezavisimosty ave., 220,
Military Academy of the Republic of Belarus
tel. +375-29-593-24-07;
e-mail: semyonov4213@gmail.com
Semyonov Sergey Ivanovich