ISSN 1561-8358 (Print)
ISSN 2524-244X (Online)

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

INFORMATION TECHNOLOGIES AND SYSTEMS

УДК 004.056.55 Поступила в редакцию 25.03.2020
https://doi.org/10.29235/1561-8358-2021-66-1-110-116 Received 25.03.2020

В. А. Липницкий, С. И. Семёнов

Военная академия Республики Беларусь, Минск, Республика Беларусь

КОРРЕКЦИЯ ОШИБОК В КОДАХ РИДА–СОЛОМОНА С ПОМОЩЬЮ ИХ АВТОМОРФИЗМОВ

Аннотация. Исследованы синдромные инварианты АΓ-группы автоморфизмов кодов Рида–Соломона (РС-кодах) – совместной группы аффинных и циклических подстановок. Найденные реальные инварианты представляют собой совокупность норм N Γ-орбит, составляющих ту или иную АΓ-орбиту. Нормы Γ-орбит, как известно, являются векторами с $C^2_{\delta-1}$ координатами из поля Галуа – поля задания РС-кода, которые определяются всевозможными парами компонент синдромов ошибок. В таком виде инварианты АΓ-орбит оказались громоздкими и тяжеловесными в обращении. Поэтому предложена компромиссная их замена на условные, частичные инварианты. Эти квази-инварианты получили название норм-проекций. Норма-проекция однозначно идентифицирует свою АΓ-орбиту и потому служит адекватным инструментом для формулировки метода коррекции ошибок РС-кодами на основе АΓ-орбит. Мощность АΓ-орбит оценивается величиной N^2, равной квадрату длины РС-кода. Поиск векторов-ошибок в передаваемых сообщениях новым методом сводится к перебору АΓ-орбит, а реально – их норм-проекций, с последующим поиском этих ошибок внутри конкретной АΓ-орбиты. Следовательно, предложенный метод работает практически в N^2 раз быстрее традиционных синдромных методов, действующих по принципу «синдром-ошибки», что, так или иначе, сводится к перебору всего множества корректируемых кодом векторов-ошибок до нахождения конкретного вектора.

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

Для цитирования: Липницкий, В. А. Коррекция ошибок в кодах Рида–Соломона с помощью их автоморфизмов / В. А. Липницкий, С. И. Семёнов // Вес. Нац. акад. навук Беларусі. Сер. фіз.-тэхн. навук. – 2021. – Т. 66, №1. – С. 110–116. https://doi.org/10.29235/1561-8358-2021-66-1-110-116

Valery A. Lipnitsky, Sergey I. Semyonov

Military Academy of the Republic of Belarus, Minsk, Republic of Belarus

ERROR CORRECTION BY REED–SOLOMON CODES USING ITS AUTOMORPHISMS

Abstract. The article explores the syndrome invariants of AΓ-group of automorphisms of Reed–Solomon codes (RS-codes) that are a joint group of affine and cyclic permutations. The found real invariants are a set of norms of N Γ-orbits that make up one or another AΓ-orbit. The norms of Γ-orbits are vectors with $C^2_{\delta-1}$ coordinates from the Galois field, that are determined by all kinds of pairs of components of the error syndromes. In this form, the invariants of the AΓ-orbits were cumbersome and difficult to use. Therefore, their replacement by conditional partial invariants is proposed. These quasi-invariants are called norm-projections. Norm-projection uniquely identifies its AΓ-orbit and therefore serves as an adequate way for formulating the error correction method by RS-codes based on AΓ-orbits. The power of the AΓ-orbits is estimated by the value of N^2, equal to the square of the length of the RS-code. The search for error vectors in transmitted messages by a new method is reduced to parsing the AΓ-orbits, but actually their norm-projections, with the subsequent search for these errors within a particular AΓ-orbit. Therefore, the proposed method works almost N^2 times faster than traditional syndrome methods, operating on the basic of the “syndrome – error” principle, that boils down to parsing the entire set of error vectors until a specific vector is found.

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

For citation: Lipnitsky V. A., Semyonov S. I. Error correction by Reed–Solomon codes using its automorphisms. *Vestsi Natsyyanal'nai akademii navuk Belarusi. Seryya fizika-technichnych navuk = Proceedings of the National Academy of Sciences of Belarus. Physical-technical series,* 2021, vol. 66, no. 1, pp. 110–116 (in Russian). https://doi.org/10.29235/1561-8358-2021-66-1-110-116

Введение. Коды Рида–Соломона (РС-коды) известны с начала 60-х годов XX в. [1, 2]. РС-коды получили широчайшее применение в радиоэлектронике и обработке информации для коррекции модульных ошибок, благодаря недвоичному алфавиту их задания. Широкий спектр исправляемых ошибок способствует росту популярности РС-кодов [3, 4]. Еще больше возможности РС-кодов раскрываются с переходом их теории на матричный язык [5]. При этом расширяются возможности применения теории полей Галуа в обработке РС-кодов [6] и, в частности, появляются перспективы развития на этот класс кодов теории норм синдромов (ТНС) [7, 8]. Формальная близость определений кодов Боуза–Чоудхури–Хоквингема (БЧХ-кодов) и РС-кодов, одинаковое действие циклических подстановок на координатах векторов-ошибок в обоих классах кодов позволили формально перенести определение нормы синдрома с БЧХ-кодов на РС-коды [7, 8]. Однако недвоичный алфавит последних вызвал существенное различие в содержании свойств норм синдромов этих кодов, что потребовало немалых усилий в их обосновании и в разработке норменных методов коррекции ошибок РС-кодами (детали см. в [8]).

Норменные методы декодирования, как известно, действуют на порядок быстрее классических синдромных. В данной работе исследованы инварианты совместной группы аффинных и циклических подстановок с перспективой получения новых методов обработки РС-кодов, действующих на порядок быстрее норменных.

Коды Рида–Соломона. В данной работе будем рассматривать коды Рида–Соломона, которые задаются проверочными матрицами вида

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

где $0 \leqslant i \leqslant N-1$, $N = q-1$, $\delta \geqslant 3$, с элементами α^i, принадлежащими полю $GF(q) = GF(2^m)$, $m \geqslant 3$, α – фиксированный примитивный элемент этого поля [9, 10]. Матрица (1) имеет размерность $(\delta-1)\times N$ и ранг $\delta-1$, очевидно, длина кода равна N, а размерность – $K = N-\delta+1$. В силу сказанного этот код естественно обозначать через $RS(N, K)$. Как известно, минимальное расстояние данного кода равно $D = N-K+1 = \delta$ [1, 2].

Приемное устройство инфокоммуникационной системы (ИКС), функционирующее на основе РС-кода, как и на основе любого линейного кода, проверяет очередное принятое сообщение $\overline{x}$ на наличие ошибок вычислением синдрома $S(\overline{x})=H\cdot\overline{x}^T$. Из структуры проверочной матрицы (1) следует, что синдром $S(\overline{x})$ здесь представляет собой вектор $S(\overline{x})=(s_1,s_2,...,s_{\delta-1})$ с $\delta-1$ координатами из поля $GF(q)$. Если $S(\overline{x})\neq 0$, то $\overline{x}=\overline{c}+\overline{e}$, где $\overline{c}$ – истинное передаваемое сообщение, а $\overline{e}$ – наложившийся в процессе передачи информации в канале с «шумами» на правильное сообщение $\overline{c}$ ненулевой вектор ошибок, который подлежит дальнейшей идентификации и устранению.

Синдром является единственным и главным свидетелем ошибок в принятом сообщении, только по нему мы можем определить структуру, вид и точное значение вектора $\overline{e}$. Априори синдром $S(\overline{x})$ может быть любым вектором δ–1-мерного пространства над полем $GF(q)$. Таким образом, в РС-коде имеется $q^{\delta-1}$ различных синдромов векторов-ошибок.

Орбиты ошибок и их инварианты в РС-кодах. В ИКС на основе линейных кодов ТНС предлагает применять эффективные методы и алгоритмы декодирования ошибок, которые базируются на автоморфизмах кодов. Согласно [8], в РС-кодах рассматриваются два вида автоморфизмов – циклические и аффинные подстановки. Они образуют соответственно циклическую группу Γ, порожденную автоморфизмом σ, который действует на каждый вектор $\overline{x}=(x_1,x_2,...,x_N)$ по правилу: $\sigma(\overline{x})=(x_N,x_1,x_2,...,x_{N-1})$, и циклическую группу A, порожденную аффинной подстановкой f_α, такой, что $f_\alpha(\overline{x})=(\alpha x_1,\alpha x_2,...,\alpha x_N)$, обе группы порядка N, а также совместную группу АГ порядка N^2. Под действием этих групп многообразие корректируемых векторов-ошибок разбивается на три вида орбит ошибок. Каждая орбита однозначно определяется действием соответствующей группы автоморфизмов на любой из векторов этой орбиты. Выбранный вектор $\overline{e}$ можно считать задающим свою орбиту: Г-орбиту $<\overline{e}>_{\Gamma}$, А-орбиту $<\overline{e}>_{\mathrm{A}}$, АГ-орбиту $<\overline{e}>_{\mathrm{A}\Gamma}$. Г-орбита $<\overline{e}>_{\Gamma}$ состоит из всевозможных векторов-ошибок, которые получаются циклическими сдвигами вправо всех координат вектора $\overline{e}=\left(e_1,e_2,\ldots,e_N\right)$. Как правило, Г-орбиты содержат по N векторов, но могут, при наличии внутренней симметрии, содержать и меньшее число $\nu < N$ векторов. Тогда мощность ν самой Г-орбиты является делителем числа N (детали см. в [7], гл. 2). Все А-орбиты имеют одинаковую мощность и одинаковую структуру: $<\overline{e}>_{\mathrm{A}}=\left\{\left(\alpha^i e_1,\alpha^i e_2,...,\alpha^i e_N\right), 0\leqslant i\leqslant N-1\right\}$. Всякая АГ-орбита состоит из N Г-орбит одинаковой мощности: $<\overline{e}>_{\mathrm{A}\Gamma}=\left\{<\overline{e}>_{\Gamma},<\alpha\overline{e}>_{\Gamma},...,<\alpha^{N-1}\overline{e}>_{\Gamma}\right\}$.

Несложно видеть, что действия названных подстановок синхронно отражаются на синдромах ошибок по формулам:

$$S\left(\sigma\left(\overline{e}\right)\right)=\left(\alpha s_1,\alpha^2 s_2,...,\alpha^{\delta-1}s_{\delta-1}\right), \tag{2}$$

$$S\left(f_{\gamma}\left(\overline{e}\right)\right)=\left(\gamma s_1,\gamma s_2,...,\gamma s_{\delta-1}\right)=\gamma S\left(\overline{e}\right). \tag{3}$$

Из данных формул следует, что спектры синдромов орбит ошибок $S(J)$, то есть множества синдромов ошибок тех или иных орбит J, копируют структуру самих орбит и совпадают с ними по мощности. Также на основании формулы (2) дается определение нормы синдрома (для сравнения см. [7], гл. 4).

О п р е д е л е н и е 1. Нормой синдрома $S\left(\overline{e}\right)$ в коде $RS(N, K)$ называется вектор $\overline{N}\left(S\left(\overline{e}\right)\right)=\left(N_{12},N_{13},...,N_{1(\delta-1)},N_{23},...,N_{(\delta-2)(\delta-1)}\right)$ с $C_{\delta-1}^2$ координатами N_{ij}, $1\leqslant i<j\leqslant\delta-1$, которые вычисляются следующим образом:

$$\begin{gathered} N_{ij}=s_j^{\,i/h_{ij}}\,/\,s_i^{\,j/h_{ij}}, \text{ если } s_i\neq 0;\text{ здесь } h_{ij}=\text{НОД}(i,j);\\ N_{ij}=\infty, \text{ если } s_j\neq 0,\ s_i=0;\\ N_{ij}=-\ (\text{не существует}), \text{ если } s_i=s_j=0. \end{gathered} \tag{4}$$

П р и м е р 1. Для РС-кода с проверочной матрицей $H=\left[\alpha^i,\alpha^{2i},\alpha^{3i},\alpha^{4i}\right]^T$ синдром каждого вектора-ошибки $\overline{e}$ представляет собой вектор $S\left(\overline{e}\right)=\left(s_1,s_2,s_3,s_4\right)$. Пусть первые три компоненты этого синдрома отличны от нуля. Тогда нормой синдрома $S\left(\overline{e}\right)$ является вектор $\overline{N}\left(S\left(\overline{e}\right)\right)=\left(N_{12},N_{13},N_{14},N_{23},N_{24},N_{34}\right)$, координаты которого, в соответствии с формулой (4), вычисляются следующим образом:

$$N_{12}=s_2\big/s_1^2;\ N_{13}=s_3\big/s_1^3;\ N_{14}=s_4\big/s_1^4;\ N_{23}=s_3^2\big/s_2^3;\ N_{24}=s_4\big/s_2^2;\ N_{34}=s_4^3\big/s_3^4. \tag{5}$$

Нормы синдромов обладают широким спектром свойств, формулировка и обоснование которых составляют суть и содержание теории норм синдромов для кодов Рида–Соломона (см. [8]). Приведем наиважнейшие из этих свойств.

С в о й с т в о 1. Норма синдрома для любого вектора-ошибки $\overline{e}$ не меняется при действии на этот вектор автоморфизма σ: $\overline{N}\left(S\left(\sigma\left(\overline{e}\right)\right)\right)=\overline{N}\left(S\left(\overline{e}\right)\right)$.

Следовательно, норма синдрома всех векторов ошибок каждой отдельно взятой Г-орбиты $J=<\overline{e}>_{\Gamma}$ принимает одно и то же значение. Данное обстоятельство позволяет ввести следующее

О п р е д е л е н и е 2. Для всякой Г-орбиты $J=<\overline{e}>$ ее нормой $\overline{N}(J)$ или $\overline{N}\left(<\overline{e}>\right)$ называется норма синдрома любого вектора-ошибки из этой орбиты.

Нормы Г-орбит, принадлежащих одной АГ-орбите, как и сами Г-орбиты, четко и однозначно взаимосвязаны.

С в о й с т в о 2. Пусть в РС-коде с проверочной матрицей (1) норма $\overline{N}\left(S\left(\overline{e}\right)\right)=\left(N_{12},N_{13},...,N_{(\delta-2)(\delta-1)}\right)$. Тогда $\overline{N}\left(S\left(f_{\gamma}\left(\overline{e}\right)\right)\right)=\left(N_{12}^{\gamma},N_{13}^{\gamma},...,N_{(\delta-2)(\delta-1)}^{\gamma}\right)$, где

$$N_{ij}^{\gamma}=N_{ij}\Big/\gamma^{(j-i)/h_{ij}},\ 1\leqslant i<j\leqslant\delta-1,\ h_{ij}=\text{НОД}(i,j). \tag{6}$$

В частности, для РС-кода из примера 1 норма $\overline{N}\left(S\left(f_\gamma\left(\overline{e}\right)\right)\right)=\left(N_{12}^{\gamma}, N_{13}^{\gamma}, N_{14}^{\gamma}, N_{23}^{\gamma}, N_{24}^{\gamma}, N_{34}^{\gamma}\right)$, где $N_{12}^{\gamma}=N_{12}/\gamma$; $N_{13}^{\gamma}=N_{13}/\gamma^2$; $N_{14}^{\gamma}=N_{14}/\gamma^3$; $N_{23}^{\gamma}=N_{23}/\gamma$; $N_{24}^{\gamma}=N_{24}/\gamma$; $N_{34}^{\gamma}=N_{34}/\gamma$.

Координат у норм синдромов существенно больше, чем компонент у синдромов, из которых они получены. Поэтому между координатами $\overline{N}\left(S\left(\overline{e}\right)\right)$ существует взаимосвязь.

Свойство 3. Пусть в коде $RS(N, K)$ у синдрома $S\left(\overline{e}\right)$ компонента $s_1 \neq 0$. Тогда у нормы синдрома $\overline{N}\left(S\left(\overline{e}\right)\right)$ координаты N_{kj}, $2 \leqslant k < j \leqslant \delta - 1$ при условии $N_{1k} \neq 0$ выражаются через координаты N_{1j}, $2 \leqslant j \leqslant \delta - 1$ по формуле

$$N_{kj}=N_{1j}^{k/h_{kj}} \Big/ N_{1k}^{j/h_{kj}}, \tag{7}$$

если $N_{1k} = 0$, $N_{1j} \neq 0$, то $N_{kj} = \infty$; если же $N_{1k} = 0$, $N_{1j} = 0$, то N_{kj} не существует.

Свойство 3 разбивает многообразие $K_{\text{АГ}}$ всех АГ-орбит векторов-ошибок, корректируемых кодом $RS(N, K)$, на два непересекающихся класса в соответствии с неравенством или равенством нулю первой компоненты s_1 синдрома образующей каждой орбиты ошибок. Для всякой АГ-орбиты $<\overline{e}>_{\text{АГ}}$ с $s_1 \neq 0$ и для каждой Г-орбиты $<\overline{e_i}>_{\Gamma} \in <\overline{e}>_{\text{АГ}}$ достаточно сохранять от вектора $N\left(S\left(\overline{e_i}\right)\right)$ только первые $\delta - 2$ координаты $N_{12}, N_{13},\ldots, N_{1(\delta-1)}$ согласно свойству 3. У всех орбит $<\overline{e}>_{\text{АГ}}$ с компонентой $s_1 = 0$ синдрома $S\left(\overline{e}\right)$ (составляющих второй класс) для каждой Г-орбиты $<\overline{e_i}>_{\Gamma} \in <\overline{e}>_{\text{АГ}}$ названные $\delta - 2$ координаты являются вырожденными, а потому существенными и значимыми у вектора $N\left(S\left(\overline{e_i}\right)\right)$ являются остальные $C_{\delta-1}^{2}-(\delta-2)$ координаты: $N_{23}, N_{24},\ldots, N_{(\delta-2)(\delta-1)}$.

Аналогичную дихотомию можно совершить и со вторым классом АГ-орбит.

Свойство 4. Если у синдрома $S\left(\overline{e}\right)$ компоненты $s_1 = 0$, $s_2 \neq 0$, то у нормы синдрома $N\left(S\left(\overline{e}\right)\right)$ координаты N_{kj}, $3 \leqslant k < j \leqslant \delta - 1$ функционально выражаются через координаты $N_{2k} \neq 0$, N_{2j} (в количестве $\delta - 3$, по формулам, более сложным, чем формулы (7), см. [8]).

Свойство 5. Пусть в коде $RS(N, K)$ из примера 1 две Г-орбиты J_1, J_2 имеют одинаковые нормы $N(J_1) = N(J_2)$, отличные от нормы $N\left(S\left(\overline{e}\right)\right)=(-,-,-,-,-,-)$. Пусть Г-орбита J_1 является полной с полным спектром синдромов. Тогда для всякого вектора $\overline{g} \in J_2$ с синдромом $S\left(\overline{g}\right)=S$ найдется вектор-ошибка $\overline{f} \in J_1$, синдром которого $S\left(\overline{f}\right)=S$.

Нормы АГ-орбит и их проекции. Каждая АГ-орбита представляет собой объединение N Г-орбит, переходящих друг в друга под действием аффинной подстановки f_α, где α – примитивный элемент поля Галуа $GF(2^m)$. Это действие синхронно отражается на синдромах образующих Г-орбит (формула (3)) и на нормах синдромов образующих (формула (6)). Для всякой Г-орбиты $J=<\overline{e}>_{\Gamma}$ ее норма $\overline{N}(J)$ является инвариантом относительно действия группы Г. Тогда набор норм $H=\left\{\overline{N}(J),\ \overline{N}\left(f_\alpha(J)\right),\ \overline{N}\left(f_{\alpha^2}(J)\right),\ \ldots,\ \overline{N}\left(f_{\alpha^{N-1}}(J)\right)\right\}$ инвариантен относительно действия всех подстановок из группы АГ, то есть является фактическим АГ-инвариантам. Для краткости множество H (или, более точно, множество H_J) будем называть нормой АГ-орбиты J.

Свойство 2 означает, что, если у нормы $N\left(S\left(\overline{e}\right)\right)$ координата N_{ij} принадлежит $GF(2^m)^*$, то в норме H_J АГ-орбиты $J=<\overline{e}>_{\text{АГ}}$ координата N_{ij} пробегает все N значений мультипликативной группы $GF(2^m)^*$. Исключение составляют лишь те редкие значения ij, для которых НОД$(l_{ij}, N) = d > 1$, $l_{ij} = (j - i)/h_{ij}$. Например $ij = 14$. Тогда $h_{ij} = 1$; $l_{ij} = 3$. Для четных $m = 2\mu$, $\mu \geqslant 1$, величина N, как известно, делится на 3. Поэтому величина α^3 порождает подгруппу $<\alpha^3>$ порядка $N/3$ в группе $GF(2^{2\mu})^*$. Следовательно, значения $N_{14}^{\gamma}=N_{14}/\gamma^3$, когда γ пробегает все значения группы $GF(2^{2\mu})^*$, будут пробегать все значения одного из смежных классов группы $GF(2^{2\mu})^*$ по подгруппе $<\alpha^3>$, то есть лишь $N/3$ значений.

В силу сказанного считаем, что у всех АГ-орбит J корректируемого многообразия K векторов-ошибок норма H_J содержит в качестве первой координаты N_{ij}, принадлежащей $GF(2^m)^*$, такую, что НОД$(l_{ij}, N) = 1$. Пусть у нормы фиксированной Г-орбиты $<\overline{e}_J>_{\Gamma} \in J$ координата $N_{ij} = 1$. Тогда вектор $\overline{e}_J$ берем в качестве образующего АГ-орбиты J, все остальные Г-орбиты из J задаем посредством аффинных преобразований Г-орбиты $<\overline{e}_J>_{\Gamma}$. Норму $N(S(\overline{e}_{\Gamma}))$ синдрома $S(\overline{e}_{\Gamma})$ назовем проекцией нормы H_J АГ-орбиты J и будем обозначать через $\mathrm{Pr}H_J$. Г-орбиту $<\overline{e}>_{\Gamma}$ с нормой $\mathrm{Pr}H_J$ будем называть проекцией АГ-орбиты J.

Декодирование ошибок РС-кодами с помощью АГ-орбит. АГ-орбиты и их проекции позволяют сформулировать эффективный метод коррекции ошибок в РС-кодах, альтернативный традиционным методам. Для его реализации множество K всех декодируемых ошибок распределяем по Г-орбитам (множество K_{Γ}), а затем – и по АГ-орбитам (множество $K_{\text{АГ}}$). Все Г-орбиты множества K_{Γ} считаются полными с полными спектрами синдромов. Так, для РС-кодов из примера 1 это заведомо гарантировано. Отмеченной выше процедурой строим проекции АГ-орбит и их норм. Таким образом, множество $K_{\text{АГ}}$ должно быть представлено списком 1 – образующих $\overline{g}_J$ Г-обит-проекций каждой АГ-орбиты $J \in K_{\text{АГ}}$, списком 2 – синдромов образующих $S(\overline{g}_J)$ и списком 3 – норм-проекций $\Pr H_J$.

Пусть ИКС функционирует на основе конкретного кода $RS(N, K)$. Приняв очередное сообщение $\overline{x}$, ИКС вычисляет его синдром $S(\overline{x})$. Неравенство $S(\overline{x}) \neq 0$ свидетельствует о наличии ошибок в принятом сообщении: $\overline{x} = \overline{c} + \overline{e}$, $\overline{e} \neq \overline{0}$, $\overline{c}$ – истинное передаваемое сообщение. В этом случае декодер включает процедуры идентификации вектора-ошибки $\overline{e}$ в сообщении $\overline{x}$ и его устранения. Для этого вычисляем норму синдрома $\overline{N}^* = \overline{N}(S(\overline{x}))$, точнее, одну из частей норменного вектора, определяемую свойством 3 или 4. Находим первую ненулевую координату $N_{ij}^*, 1 \leqslant i < j \leqslant \delta - 1$, вектора $\overline{N}^*$. Определяем показатель λ этой компоненты $\left(N_{ij}^* = \alpha^{\lambda}, 0 \leqslant \lambda < N\right)$.

Если у координаты N_{ij}^* величина $l_{ij} = 1$, то к вектору $\overline{x}$ применяем аффинную подстановку $f_{\alpha^{\lambda}}$, соответственно преобразуем $S(\overline{x})$ и норму $\overline{N}^*$. В силу формул (6) координата N_{ij}^* при этом преобразуется в 1, тем самым вектор $\overline{N}^*$ преобразуется в одну из норм-проекции $f_{\alpha^{\lambda}}(\overline{N}^*)$ списка 3. Пусть $f_{\alpha^{\lambda}}(\overline{N}^*) = \Pr H_{\tilde{J}}$ из этого списка. Следовательно, неизвестная вектор-ошибка $f_{\alpha^{\lambda}}(\overline{e}) = \alpha^{\lambda} \cdot \overline{e}$ принадлежит АГ-орбите $\tilde{J}$, а точнее, Г-орбите $< \overline{g}_{\tilde{J}} >_{\Gamma}$. Согласно формуле (3) синдром $S\left(f_{\alpha^{\lambda}}(\overline{e})\right) = \alpha^{\lambda} \cdot S(\overline{e}) \in S\left(< \overline{g}_{\tilde{J}} >\right)$. Сравнивая компоненты синдромов $S\left(\alpha^{\lambda}\overline{e}\right)$ и $S\left(\overline{g}_{\tilde{J}}\right)$, определяем величину μ такую, что $\sigma^{\mu}\left(g_{\tilde{J}}\right) = \alpha^{\lambda}\overline{e}$. Тогда вектор $\alpha^{\lambda} \cdot \overline{x} + \sigma^{\mu}\left(\overline{g}_{\tilde{J}}\right) = \alpha^{\lambda} \cdot \overline{c}$ не содержит ошибок и вектор $\alpha^{N-\lambda} \cdot \left(\alpha^{\lambda} \cdot \overline{c}\right) = \overline{c}$ – исправленное истинное передаваемое сообщение.

Пусть у координаты N_{ij}^* величина $l_{ij} > 1$, но НОД$(l_{ij}, N) = 1$. Тогда, согласно соотношению Безу, существуют целые числа u, v, такие, что $l_{ij}u + Nv = 1$. Следовательно, $l_{ij}u\lambda + Nv\lambda = \lambda$. Пусть $w = uv(\text{mod}N)$. Тогда к вектору $\overline{x}$ применяем аффинную подстановку $f_{\alpha^{w}}$ вместо $f_{\alpha^{\lambda}}$ и добьемся тех же результатов.

П р и м е р 2. Код $RS(7, 3)$ из примера 1 исправляет ошибки весом 1, 2 в количестве $|K| = (q-1)^2\left(1 + C_N^2\right) = 1078$. Они делятся на 154 полные Г-орбиты и 22 полные АГ-орбиты. Таблица содержит списки всех 21 проекций-образующих АГ-орбит векторов-ошибок весом 2, синдромов образующих и их норм синдромов. Здесь примитивный элемент α является корнем неприводимого полинома $p(x) = x^3 + x^2 + 1$.

Проекции-образующие АГ-орбит, их синдромы и нормы синдромов в (7,3)-РС-коде

Projection-generating АГ-orbits, their syndromes and norms of syndromes in the (7,3)-RS-code

№ п/п	$\overline{g}$	$S(\overline{g})$	$\overline{N}(S(\overline{g}))$	№ п/п	$\overline{g}$	$S(\overline{g})$	$\overline{N}(S(\overline{g}))$
1	$(1,1,0,0,0,0,0)$	$(\alpha^5,\alpha^3,\alpha^2,\alpha^6)$	$(1,\alpha,1)$	11	$(\alpha^6,0,\alpha,0,0,0,0)$	$(\alpha^5,\alpha^3,\alpha^4,\alpha)$	$(1,\alpha^3,\alpha^2)$
2	$(1,\alpha^5,0,0,0,0,0)$	$(\alpha^4,0,\alpha^5,\alpha^3)$	$(0,1,\alpha)$	12	$(\alpha^4,0,\alpha^5,0,0,0,0)$	$(\alpha^6,\alpha^5,0,1)$	$(1,0,\alpha^4)$
3	$(\alpha^2,\alpha^6,0,0,0,0,0)$	$(\alpha^3,\alpha^6,0,1)$	$(1,0,\alpha^2)$	13	$(1,0,0,1,0,0,0)$	$(\alpha^2,\alpha^4,\alpha^3,\alpha)$	$(1,\alpha^4,1)$
4	$(\alpha^3,\alpha^6,0,0,0,0,0)$	$(\alpha^2,\alpha^4,1,0)$	$(1,\alpha,0)$	14	$(\alpha^2,0,0,\alpha,0,0,0)$	$(\alpha^5,\alpha^3,1,\alpha)$	$(1,\alpha^6,\alpha^2)$
5	$(\alpha^2,\alpha^4,0,0,0,0,0)$	$(\alpha^4,\alpha,\alpha^3,\alpha^6)$	$(1,\alpha^5,\alpha^4)$	15	$(\alpha^3,0,0,\alpha,0,0,0)$	$(\alpha,\alpha^2,0,\alpha^5)$	$(1,0,\alpha)$
6	$(\alpha^3,\alpha^4,0,0,0,0,0)$	$(\alpha^6,\alpha^5,\alpha^2,\alpha^4)$	$(1,\alpha^5,\alpha)$	16	$(\alpha^2,0,0,\alpha^5,0,0,0)$	$(\alpha^6,\alpha^5,\alpha^3,1)$	$(1,\alpha^6,\alpha^4)$
7	$(1,0,1,0,0,0,0)$	$(\alpha^3,\alpha^6,\alpha^4,\alpha^5)$	$(1,\alpha^2,1)$	17	$(\alpha^3,0,0,\alpha^5,0,0,0)$	$(\alpha^4,\alpha,1,0)$	$(1,\alpha^4,0)$
8	$(\alpha^6,0,\alpha^5,0,0,0,0)$	$(\alpha^4,\alpha,1,0)$	$(1,\alpha^2,0)$	18	$(\alpha^6,0,0,1,0,0,0)$	$(\alpha^5,0,\alpha,\alpha^3)$	$(0,1,\alpha^4)$
9	$(\alpha^4,0,\alpha,0,0,0,0)$	$(\alpha,\alpha^2,\alpha^6,\alpha^5)$	$(1,\alpha^3,\alpha)$	19	$(\alpha^5,\alpha^4,0,0,0,0,0)$	$(0,\alpha^3,\alpha,1)$	$(\infty,\infty,\infty,1,\alpha)$
10	$(1,0,\alpha^3,0,0,0,0)$	$(\alpha,0,\alpha^3,\alpha^6)$	$(0,1,\alpha^2)$	20	$(\alpha^3,0,\alpha,0,0,0,0)$	$(0,\alpha^6,\alpha^2,1)$	$(\infty,\infty,\infty,1,\alpha^2)$
				21	$(\alpha^2,0,0,\alpha^6,0,0,0)$	$(0,\alpha^4,\alpha^6,\alpha^5)$	$(\infty,\infty,\infty,1,\alpha^4)$

Пусть ИКС на основе кода $RS(7, 3)$ приняла сообщение $\overline{x} = (\alpha^3, \alpha^6, \alpha^3, \alpha^2, 1, 0, \alpha^5)$. Его синдром $S(\overline{x}) = (\alpha^2, \alpha^5, \alpha^3, 0)$, а норма синдрома $\overline{N}^* = \overline{N}(S(\overline{x})) = (\alpha, \alpha^4, 0, \alpha^5, 0, 0)$. По первой ненулевой координате нормы синдрома определяем, что аффинная подстановка f_α преобразует принятое сообщение в вектор $\overline{x}^* = f_\alpha(\overline{x}) = (\alpha^4, 1, \alpha^4, \alpha^3, \alpha, 0, \alpha^6)$ с синдромом $S(\overline{x}^*) = (\alpha^3, \alpha^6, \alpha^4, 0)$ и нормой синдрома $\overline{N}(S(\overline{x}^*)) = (1, \alpha^2, 0, \alpha^4, 0, 0)$. Сравним полученную норму с данными таблицы. Она совпадает с нормой-проекцией АГ-орбиты под номером 8. В 8-й строке находится образующая проекция $\overline{g}_8 = (\alpha^6, 0, \alpha^5, 0, 0, 0)$ с синдромом $S(\overline{g}_8) = (\alpha^4, \alpha, 1, 0)$. Вектор $\overline{e}^*$ в сообщении $\overline{x}^*$ принадлежит Г-орбите $< \overline{g}_8 >_\Gamma$. Отношение первых компонент синдромов $S(\overline{x}^*) = S(\overline{e}^*)$ и $S(\overline{g}_8)$ – это величина $\alpha^3 / \alpha^4 = \alpha^6$, которая говорит о том, что вектором-ошибкой в сообщении $\overline{x}^*$ является вектор $\overline{e}^* = \sigma^6(\overline{g}_8) = (0, \alpha^5, 0, 0, 0, \alpha^6)$. Тогда сумма $\overline{x}^* + \overline{e}^* = \overline{c}^* = (\alpha^4, \alpha, \alpha^4, \alpha^3, \alpha, 0, 0)$ является вектором без ошибок. Отсюда следует, что $\overline{c} = \alpha^6(\overline{c}^*) = \alpha^6(\alpha^4, \alpha, \alpha^4, \alpha^3, \alpha, 0, 0) = (\alpha^3, 1, \alpha^3, \alpha^2, 1, 0, 0)$ – истинное переданное сообщение. Контрольная проверка: равенство $H \cdot \overline{c}^T = \overline{0}$ подтверждает правильность проведенных вычислений.

Классические синдромные методы работают по принципу «синдром-ошибка» и, так или иначе, реализуют процедуру поиска конкретной ошибки во всем многообразии корректируемых кодом ошибок. Норменные методы оперируют с Г-орбитами ошибок, содержащими, в основном, по N векторов-ошибок: перебирается список Г-орбит до нахождения нужной нормы, дальнейшая идентификация ошибки осуществляется внутри найденной Г-орбиты. Поисковые процедуры среди Г-орбит, несомненно, в N раз короче классических синдромных методов. Предложенный в данной работе метод коррекции ошибок, основанный на поиске нужной АГ-орбиты среди многообразия подобных и содержащих, как правило, по N^2 векторов-ошибок, является в N раз эффективнее норменных методов.

Заключение. Группы Г и А циклических и аффинных подстановок, их произведение АГ действуют на линейных кодах Рида–Соломона, разбивают многообразие ошибок в этих кодах соответственно на три вида орбит: Г-орбиты, А-орбиты, АГ-орбиты. Строение каждой орбиты имеет синхронное отражение на синдромных спектрах этих орбит. Нормы синдромов – инварианты группы Г – являются своеобразными метками, идентификаторами Г-орбит векторов-ошибок, обладают рядом важных свойств, обеспечивающих высокоскоростные норменные методы коррекции ошибок РС-кодами. Эти методы действуют на порядок быстрее классических синдромных методов.

В данной работе исследована идея применения АГ-орбит с целью создания методов декодирования РС-кодов, на порядок более быстрых по сравнению с норменными методами. В процессе исследования выяснилось, что, к сожалению, реальный синдромный инвариант группы АГ в РС-кодах – совокупность норм Г-орбит, составляющих АГ-орбиты, – оказался слишком громоздким для применения. Замена ему найдена в квази-нормах, нормах-проекциях, которые находятся единой, простой и обезличенной процедурой внутри спектра норм каждой АГ-орбиты. В завершение сформулирован обобщенный перестановочный метод коррекции ошибок РС-кодами с помощью норм-проекций, то есть с помощью АГ-орбит. Для его реализации требуются несложные вычисления в полях Галуа с периодическим обращением к устройствам хранения информации. Конкретный пример наглядно демонстрирует эффективность разработанного метода.

Список использованных источников

1. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М.: Связь, 1979. – 744 с.

2. Блейхут, Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М.: Мир, 1986. – 576 с.

3. Скляр, Б. Цифровая связь: теоретические основы и практическое применение: учеб. пособие / Б. Скляр. – 2-е изд., испр. – М.: Вильямс, 2003. – 1104 с.

4. Кудряшов, Б. Д. Основы теории кодирования: учеб. пособие / Б. Д. Кудряшов. – СПб.: БХВ-Петербург, 2016. – 400 с.

5. Маров, А. В. Матричный формализм кодов Рида–Соломона / А. В. Маров, А. Ю. Утешев // Вестн. СПбГУ. Сер. 10, Прикладная математика. Информатика. Процессы управления. – 2016. – Вып. 4. – С. 3–17. https://doi.org/10.21638/11701%2Fspbu10.2016.401

6. Семенов, С. И. Преимущества применения теории полей Галуа для обработки РС-кодов / С. И. Семенов, В. А. Липницкий // Сборник научных статей Военной академии Республики Беларусь. – Минск: Воен. акад. Респ. Беларусь, 2019. – Вып. 36. – С. 84–93.

7. Липницкий, В. А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения / В. А. Липницкий, В. К. Конопелько. – Минск: Изд. центр БГУ, 2007. – 239 с.

8. Липницкий, В. А. Нормы синдромов и их свойства в кодах Рида–Соломона / В. А. Липницкий, С. И. Семенов // Вестн. Полоц. гос. ун-та. Сер. С. Фундаментальные науки. – 2020. – №4. – С. 2–9.

9. Лидл, Р. Конечные поля: в 2 т. / Р. Лидл, Г. Нидеррайтер. – М.: Мир, 1988. – 822 с.

10. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа / В. А. Липницкий. – Минск: БГУИР, 2006. – 88 с.

References

1. MacWilliams F. J., Sloan N. J. A. *The Theory of Error-Correcting Codes*. North Holland, 1977. XII, 762 p. (North-Holland Mathematical Library ; Vol. 16).

2. Blejhut R. *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983. 500 p.

3. Sklar B. *Digital Communication. Fundamentals and Applications*. 2nd ed. Prentice Hall PTR, 2001. 1104 p.

4. Kudryashov B. D. *Fundamentals of Coding Theory*. St. Petersburg, BHV-Petersburg Publ., 2016. 400 p. (in Russian).

5. Marov A. V., Uteshev A. Yu. Matrix formalism of the Reed–Solomon codes. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta. Seriya 10, Prikladnaya matematika. Informatika. Protsessy upravleniya = Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2016, issue 4, pp. 3–17. https://doi.org/10.21638/11701%2Fspbu10.2016.401

6. Semyonov S. I., Lipnitsky V. A. Advantages of using Galois field theory for processing RS-codes. *Sbornik nauchnyh statei Voennoi academii Respubliki Belarus'* [Collection of Scientific Articles of the Military Academy of the Republic of Belarus], 2019, iss. 36, pp. 84–93 (in Russian).

7. Lipnitsky V. A., Konopel'ko V. K. *Norm Decoding of Error-Correcting Codes and Algebraic Equations*. Minsk, BSU Publ. Center, 2007. 239 p. (in Russian).

8. Lipnitsky V. A., Semyonov S. I. Norms of syndromes and their properties in Reed-Solomon codes. *Vestnik Polotskogo gosudarstvennogo universiteta. Seriya C. Fundamental'nye nauki = Vestnik of Polotsk State University. Part C. Fundamental Sciences*, 2020, no. 4, pp. 2–9 (in Russian).

9. Lidl R., Niderrajter G. *Finite Fields (Encyclopedia of Mathematics and its Applications).* 2nd ed. Cambridge University Press, 2008. 772 p. https://doi.org/10.1017/CBO9780511525926

10. Lipnitsky V. A. *Modern Applied Algebra. The Mathematical Foundations of Protecting Information from Interference and Unauthorized Access*. Minsk, BSUIR, 2006. 88 p. (in Russian).

Информация об авторах

Липницкий Валерий Антонович – доктор технических наук, профессор, заведующий кафедрой высшей математики, Военная академия Республики Беларусь (пр. Независимости, 220, 220057, Минск, Республика Беларусь). E-mail: valipnitski@yandex.by

Семёнов Сергей Иванович – магистр технических наук, адъюнкт кафедры информационно-вычислительных систем, Военная академия Республики Беларусь (пр. Независимости, 220, 220057, Минск, Республика Беларусь). E-mail: semyonov4213@gmail.com

Information about the authors

Valery A. Lipnitsky – D. Sc. (Engineering), Professor, Head of the Department of High Mathematics, Military Academy of the Republic of Belarus (220, Nezavisimosti Ave., 220057, Minsk, Republic of Belarus). E-mail: valipnitski@yandex.by

Sergey I. Semenov – Graduate Student (Engineering), Adjunct of Chair of Information and Computing Systems, Military Academy of the Republic of Belarus (220, Nezavisimosti Ave., 220057, Minsk, Republic of Belarus). E-mail: semyonov4213@gmail.com