ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.55

НОРМЫ СИНДРОМОВ И ИХ СВОЙСТВА В КОДАХ РИДА – СОЛОМОНА

д-р техн. наук, проф. В.А. ЛИПНИЦКИЙ, С.И. СЕМЁНОВ
(Военная академия Республики Беларусь, Минск)

Разработана теория норм синдромов (ТНС) для семейства кодов Рида – Соломона, являющаяся развитием ТНС для класса БЧХ-кодов. РС-коды построены на недвоичных алфавитах, поэтому, в отличие от кодов Боуза – Чоудхури – Хоквингема, РС-коды содержат исключительно большое количество корректируемых ошибок. Для коррекции этих ошибок предлагается систематическое применение автоморфизмов кодов. Характерными автоморфизмами РС-кодов являются циклические и аффинные подстановки, образующие циклические группы Г и А соответственно, порядки которых совпадают с длиной кода. Циклическая и аффинная подстановки коммутируют друг с другом и порождают совместную АГ-группу. Эти три группы действуют на пространстве векторов-ошибок РС-кодов, разбивая это пространство на три вида орбит ошибок. Как правило, эти орбиты являются полными, то есть содержат максимально возможное количество ошибок. Спектры синдромов орбит ошибок также, как правило, являются полными. Структура спектров синдромов копирует структуру самих орбит, которые, в свою очередь, копируют структуру групп автоморфизмов кода. Введено понятие нормы синдрома вектора-ошибки – векторной величины, координаты которой определяются всевозможными парами компонент синдрома. Доказано, что норма синдрома инвариантна относительно действия подстановок группы Г, поэтому нормы синдромов являются инвариантами каждой отдельно взятой Г-орбиты. В работе доказан ряд предложений, отражающих базовые свойства норм синдромов. Эти результаты составляют теоретическую основу норменных методов коррекции ошибок РС-кодами.

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

Введение. Коды Рида – Соломона попали в сферу внимания исследователей достаточно давно – в 1960-е гг. [1; 2]. Тем не менее, интерес к ним не ослабевает и поныне [3; 4]. Систематическое применение современного матричного языка в теории РС-кодов позволяет максимально использовать возможности теории полей Галуа и открывает перспективы развития теории норм синдромов (ТНС) [5; 6] на коды Рида – Соломона.

В данной работе всесторонне исследуются свойства циклических подстановок на конечномерных векторных пространствах над полями Галуа характеристики два, их отражение на РС-кодах. Вводится понятие нормы синдрома, внешне похожее на такое же понятие в БЧХ-кодах [5; 6]. Однако в условиях недвоичного алфавита при двукратно увеличенном количестве компонент синдромов в РС-кодах и соответствующем росте числа координат норм синдромов доказательство основных результатов ТНС приходится проводить независимо, с разработкой и применением самостоятельных подходов. Иное, более весомое значение приобретают и сами структурные теоремы теории норм синдромов РС-кодов.

Некоторые сведения об РС-кодах. В данной работе рассматриваются РС-коды, определенные над полями Галуа $GF(q)=GF(2^m),\ m>1,$ характеристики два с 2^m элементами. Зафиксируем примитивный элемент α поля $GF(2^m)$ и неприводимый над полем $GF(2)$ полином $p(x)$ степени m с корнем α. Зафиксируем также целые числа $b\ge 0$, $\delta>1$, $N=q-1$, $(\delta-1)\times N$ – матрица (1), имеющая ранг $\delta-1,$ поскольку ее минор из первых $\delta-1$ столбцов является определителем Вандермонда [7], отличным от нуля. Более того, по тем же причинам любой минор этой матрицы порядка $\delta-1$ также отличен от нуля. Следовательно, линейный код длиной N с проверочной матрицей H имеет размерность $K=N-\delta+1$ и минимальное расстояние $D=N-K+1=\delta$ [1]. Это классический код Рида – Соломона $RS(N,K)$.

$$H=\begin{bmatrix} 1 & \alpha^{b} & \alpha^{2b} & \dots & \alpha^{(N-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(N-1)(b+1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \dots & \alpha^{(N-1)(b+\delta-2)} \end{bmatrix}=\left(\alpha^{bi},\alpha^{(b+1)i},...,\alpha^{(b+\delta-2)i}\right)^{T},\quad 0\le i\le N-1. \qquad (1)$$

На самом деле, за обозначением $RS(N,K)$ скрыто целое семейство РС-кодов, зависящих от выбора примитивного элемента α и полинома $p(x)$, от значений $b = 0, 1, 2, \ldots$. Поскольку $\alpha^N = 1$, то реальный смысл имеет лишь приведенная система значений b: $b = 0, 1, 2, ..., N-1$.

В теории и практике БЧХ-кодов, формально имеющих практически аналогичное определение, предпочтение отдается значению $b = 1$ [1; 5]. Здесь же для РС-кодов проверочная матрица H принимает вид

$$H = [\alpha^i, \alpha^{2i}, ..., \alpha^{(\delta-1)i}]^T, \quad 0 \le i \le N-1, \tag{2}$$

что лишь слегка упрощает формулы и вычисления с ней.

Как и кодовые слова, векторы-ошибки в кодах $RS(N,K) = RS(q-1, q-\delta)$ принадлежат N-мерному векторному пространству $V_N(GF(q))$ над полем Галуа $GF(q)$. Легко видеть, что в коде $RS(N,K)$ имеется $(q-1)^2$ ошибок весом 1; двойных – $C_{q-1}^2 \cdot (q-1)^2$; ошибок весом $\omega \ge 1$ – $C_{q-1}^{\omega} \cdot (q-1)^{\omega}$. Векторы-ошибки, вес которых меньше D, обнаруживаются кодом $RS(N,K)$ и исправляются, если их вес $t \le (D-1)/2$ для нечетных и $t \le (D-2)/2$ для четных значений D [1].

Единственным необходимым и достаточным средством обнаружения и исправления ошибок в линейных кодах в каждом принятом сообщении $\bar{x}$ является их синдром $S(\bar{x}) = H \cdot \bar{x}^T$. В соответствии со структурой проверочной матрицы (1) или (2) синдром представляет собой вектор $S(\bar{x}) = (s_1, s_2, ..., s_{\delta-1})$ с $\delta - 1$ координатами $s_i \in GF(2^m), 1 \le i \le \delta - 1$. Априори $\bar{x}$ – любой вектор из пространства $V_N(GF(2^m))$, поэтому в силу свойств векторно-матричных умножений [7] синдром $S(\bar{x})$ может быть любым вектором пространства $V_{\delta-1}(GF(2^m))$. Таким образом, в РС-коде имеется $q^{\delta-1} = 2^{m(\delta-1)}$ различных синдромов векторов-ошибок. Это потенциал, достаточный для декодирования всех ошибок весом $1, 2, ..., t$, где t – целая часть числа $(D-1)/2$. Классические методы коррекции ошибок в РС-кодах – методы Форни, Берлекемпа-Месси [2; 3] – эффективны, когда вес этих ошибок равен 1, 2. Однако работа декодеров, основанных на этих методах, резко замедляется с ростом N и ω – веса исправляемых ошибок. Хорошим решением этой проблемы авторы данной статьи считают применение автоморфизмов кодов.

Автоморфизмы РС-кодов и их влияние на синдромы ошибок. В РС-кодах будем рассматривать циклическую и аффинную подстановки σ и f_γ [5]. Степени этих подстановок образуют циклические группы Г и А порядка N, а также их прямое произведение АГ порядка N^2 в группе автоморфизмов $Aut(RS(N,K))$ [8].

Пусть $\bar{e} = (e_1, e_2, ..., e_N)$ – вектор-ошибка в коде $RS(N,K)$. Автоморфизм σ циклического сдвига координат векторов действует на $\bar{e}$ по правилу: $\sigma(\bar{e}) = (e_N, e_1, e_2, ..., e_{N-1})$. В силу формулы (1) это действие сказывается на синдроме следующим образом:

$$S(\sigma(\bar{e})) = (\alpha^b s_1, \alpha^{2b} s_2, ..., \alpha^{(\delta-1)b} s_{\delta-1}). \tag{3}$$

Аффинная подстановка действует таким образом: $f_\gamma(\bar{e}) = (\gamma e_1, \gamma e_2, ..., \gamma e_N) = \gamma \bar{e}$. В силу линейности векторно-матричных умножений [7] имеем

$$S(f_\gamma(\bar{e})) = (\gamma s_1, \gamma s_2, ..., \gamma s_{\delta-1}) = \gamma S(\bar{e}). \tag{4}$$

Нормы синдромов в кодах Рида – Соломона.

Определение 1. Нормой синдрома $S(\bar{e})$ в коде $RS(N,K)$ называется вектор $\bar{N}(S(\bar{e})) = (N_{12}, N_{13}, ..., N_{1(\delta-1)}, N_{23}, ..., N_{(\delta-2)(\delta-1)})$ с $C_{\delta-1}^2$ координатами N_{ij}, $1 \le i < j \le \delta - 1$, которые вычисляются следующим образом:

$$N_{ij} = s_j^{(b+i-1)/h_{ij}} / s_i^{(b+j-1)/h_{ij}}, \text{ если } s_i \ne 0,$$

где $h_{ij} = НОД(b+i-1, b+j-1)$;

$$N_{ij} = \infty, \text{ если } s_j \ne 0,\ s_i = 0; \tag{5}$$

N_{ij} не существует, если $s_i = s_j = 0$.

Отметим, что для РС-кода с проверочной матрицей (2) формула (5) в определении нормы имеет более простой вид:

$$N_{ij} = s_j^{\,i/h_{ij}} / s_i^{\,j/h_{ij}}, \qquad (5')$$

где $h_{ij} = НОД(i, j);\ 1 \le i < j \le \delta - 1.$

Пример 1. Для кода $RS(N, K)$, с проверочной матрицей

$$H = [\alpha^i, \alpha^{2i}, \alpha^{3i}, \alpha^{4i}]^T \qquad (6)$$

синдром каждого вектора-ошибки $\bar{e}$ представляет собой вектор $S(\bar{e}) = (s_1, s_2, s_3, s_4)$. Пусть первые три компоненты этого синдрома отличны от нуля. Тогда нормой синдрома $S(\bar{e})$ является вектор $\bar{N}(S(\bar{e})) = (N_{12}, N_{13}, N_{14}, N_{23}, N_{24}, N_{34})$, координаты которого в силу формулы (5′) вычисляются следующим образом:

$$N_{12} = s_2 / s_1^2;\ N_{13} = s_3 / s_1^3;\ N_{14} = s_4 / s_1^4;\ N_{23} = s_3^2 / s_2^3;\ N_{24} = s_4 / s_2^2;\ N_{34} = s_3^4 / s_4^3. \qquad (7)$$

Норма синдрома обладает рядом замечательных свойств. Важнейшее из них отражает предложение 1.

Предложение 1. В коде $RS(N, K)$ с проверочной матрицей (1) норма синдрома любого вектора-ошибки $\bar{e}$ не меняется при действии на этот вектор автоморфизма σ: $\bar{N}(S(\sigma(\bar{e}))) = \bar{N}(S(\bar{e}))$.

Доказательство вытекает из формул (3) и (5). Пусть у синдрома $S(\bar{e})$ компонента $s_i \neq 0$. Тогда согласно формуле (5) координата N_{ij} вектора-нормы $\bar{N}(S(\bar{e}))$ есть элемент поля Галуа $GF(2^m)$, равный $N_{ij} = s_j^{\,(b+i-1)/h_{ij}} / s_i^{\,(b+j-1)/h_{ij}}$. При этом у нормы синдрома $\bar{N}(S(\sigma(\bar{e})))$ вектора $\sigma(\bar{e})$ в силу предложения 1 координата $N_{ij}^{\sigma} = (\alpha^{b+j-1} s_j)^{(b+i-1)/h_{ij}} / (\alpha^{b+i-1} s_i)^{(b+j-1)/h_{ij}} = \left(\alpha^{(b+j-1)(b+i-1)/h_{ij}} / \alpha^{(b+i-1)(b+j-1)/h_{ij}}\right) \cdot \left(s_j^{\,(b+i-1)/h_{ij}} / s_i^{\,(b+j-1)/h_{ij}}\right) = s_j^{\,(b+i-1)/h_{ij}} / s_i^{\,(b+j-1)/h_{ij}} = N_{ij}$, что и требовалось доказать.

Кратным применением предложения 1 получается доказательство следующего утверждения.

Предложение 2. Для всех векторов каждой отдельно взятой Г-орбиты $J = <\bar{e}>_\Gamma$ норма синдрома принимает одно и то же значение и представляет собой инвариант этой Г-орбиты относительно действия циклических подстановок.

Предложение 2 является основой для того, чтобы ввести следующее определение.

Определение 2. Для всякой Г-орбиты $J = <\bar{e}>$ ее нормой $\bar{N}(J)$ или $\bar{N}(<\bar{e}>)$ 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.

Предложение 3. Пусть в РС-коде с проверочной матрицей (1) норма $\bar{N}(S(\bar{e})) = (N_{12}, N_{13}, ..., N_{(\delta-2)(\delta-1)})$. Тогда $\bar{N}(S(f_\gamma(\bar{e}))) = (N_{12}^\gamma, N_{13}^\gamma, ..., N_{(\delta-2)(\delta-1)}^\gamma)$, где

$$N_{ij}^\gamma = N_{ij} / \gamma^{(j-i)/h_{ij}},\ 1 \le i < j \le \delta - 1, \qquad (8)$$

где $h_{ij} = НОД(b+i-1, b+j-1)$ для всех целых i, j;

$1 \le i < j \le \delta - 1$.

Доказательство. Пусть $\bar{e} = (e_1, e_2, ..., e_N)$ и $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1})$. Тогда $f_\gamma(\bar{e}) = (\gamma e_1, \gamma e_2, ..., \gamma e_N)$ и согласно формуле (4) $S(f_\gamma(\bar{e})) = (\gamma s_1, \gamma s_2, ..., \gamma s_{\delta-1}) = \gamma S(\bar{e})$. Согласно определению нормы вычисляемая формулой (5) координата $N_{ij}^\gamma = (\gamma s_j)^{(b+i-1)/h_{ij}} / (\gamma s_i)^{(b+j-1)/h_{ij}} = (s_j^{\,(b+i-1)/h_{ij}} / s_i^{\,(b+j-1)/h_{ij}}) \cdot (\gamma^{(b+i-1-b-j+1)/h_{ij}}) = N_{ij} / \gamma^{(j-i)/h_{ij}} = N_{ij}^\gamma$, что и доказывает предложение 3.

Следствие 1. Для РС-кода с $\delta = 5,\ b = 1$, норма $\bar{N}(S(f_\gamma(\bar{e}))) = (N_{12}^\gamma, N_{13}^\gamma, N_{14}^\gamma, N_{23}^\gamma, N_{24}^\gamma, N_{34}^\gamma)$, где $N_{12}^\gamma = N_{12}/\gamma;\ N_{12}^\gamma = N_{12}/\gamma;\ N_{13}^\gamma = N_{13}/\gamma^2;\ N_{14}^\gamma = N_{14}/\gamma^3;\ N_{23}^\gamma = N_{23}/\gamma;\ N_{24}^\gamma = N_{24}/\gamma;\ N_{34}^\gamma = N_{34}/\gamma$.

Из предложения 3 следует, что циклическое преобразование Г-орбит внутри АГ-орбиты под действием f_α сопровождается преобразованием норм этих Г-орбит в соответствии с формулой (8).

Взаимосвязь координат норменного вектора. Координат у норм синдромов существенно больше, чем компонент у синдромов, из которых они получены, поэтому между координатами N_{kj}, $1 \le k \le \delta - 1$ неизбежно должны существовать функциональные зависимости. Об одном классе таких зависимостей ярко свидетельствует следующее утверждение.

Предложение 4. Пусть в коде $RS(N, K)$ с проверочной матрицей (2) у синдрома $S(\bar{e})$ компонента $s_1 \neq 0$. Тогда у нормы синдрома $\bar{N}(S(\bar{e}))$ координаты $N_{1j}, 1 < j \le \delta - 1$ (в количестве $\delta - 2$) вычисляются по формуле (5′), а остальные координаты N_{kj}, $2 \le k < j \le \delta - 1$ при условии $N_{1k} \neq 0$ выражаются через вычисленные по формуле

$$N_{\kappa j} = N_{1j}^{k/h_{kj}} \Big/ N_{1k}^{j/h_{kj}}, \tag{9}$$

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.

Доказательство. Пусть у синдрома $S(\bar{e})$ компонента $s_1 \neq 0$. Тогда по формуле (5′) вычислены координаты $N_{1j}, 1 < j \le \delta - 1$. В частности, для конкретных значений $j, k, 2 \le j < k \le \delta - 1$ координаты $N_{1j} = s_j / s_1^{\,j};\ N_{1k} = s_k / s_1^{\,k}$. Тогда $N_{1j}^{k/h_{kj}} \Big/ N_{1k}^{j/h_{kj}} = (s_j / s_1^{\,j})^{k/h_{kj}} \Big/ (s_k / s_1^{\,k})^{j/h_{kj}} = s_j^{\,k/h_{kj}} / s_k^{\,j/h_{kj}} = N_{kj}$, что доказывает формулу (9).

Следствие 1. Пусть условия предложения 4 выполняются для Г-орбиты $J = <\bar{e}>_{\Gamma}$. Тогда это же предложение справедливо и для всех Г-орбит, составляющих АГ-орбиту $<\bar{e}>_{\text{АГ}}$.

Доказательство вытекает из предложения 4 и следствия из предложения 1.

Следствие 2. Многообразие $K_{\text{АГ}}$ всех АГ-орбит векторов-ошибок, корректируемых кодом $RS(N, K)$ с проверочной матрицей (1) или (2), разбивается по виду синдромов образующих этих орбит и по строению векторов-норм синдромов этих образующих на два непересекающихся класса. В первый класс попадают все орбиты $<\bar{e}>_{\text{АГ}}$, у которых первая компонента синдрома образующей $s_1 \neq 0$. Для всякой АГ-орбиты $<\bar{e}>_{\text{АГ}}$ из этого класса и для Г-орбиты $<\bar{e}_i>_{\Gamma} \in <\bar{e}>_{\text{АГ}}$ сохраняем от вектора $N(S(\bar{e}_i))$ только первые $\delta - 2$ координат: $N_{12}, N_{13}, \ldots, N_{1(\delta-1)}$. Во второй класс попадают все орбиты $<\bar{e}>_{\text{АГ}}$, у синдромов $S(\bar{e})$ образующих которых $s_1 = 0$. Для всякой АГ-орбиты $<\bar{e}>_{\text{АГ}}$ из этого класса и для Г-орбиты $<\bar{e}_i>_{\Gamma} \in <\bar{e}>_{\text{АГ}}$ сохраняем в силу предложения 4 от вектора $N(S(\bar{e}_i))$ остальные $C_{\delta-1}^2 - \delta - 2$ координаты: $N_{23}, N_{24}, \ldots, N_{(\delta-2)(\delta-1)}$.

Следует отметить, что возможно развитие следствия 2 в сторону подобного же разбиения второго класса АГ-орбит – с компонентой синдромов $s_1 = 0$. К сожалению, таких же четких и однозначных формул, аналогичных формуле (9), здесь не наблюдается.

Пусть в орбите $<\bar{e}>_{\text{АГ}}$ у всех векторов-ошибок первая компонента синдрома равна нулю, но $s_2 \neq 0$. Пусть по формуле (5′) вычислены координаты $N_{23}, N_{24}, \ldots, N_{2(\delta-1)}$ вектора $\bar{N}(S(\bar{e}))$. Выразим через них последующие координаты вектора $\bar{N}(S(\bar{e}))$. Для четных $k, j,\ 2 < k < j \le \delta - 1$ и для $h_{kj} = НОД(k, j) = 2 \cdot s$, где $s = НОД(\frac{k}{2}, \frac{j}{2})$, для $s_k \neq 0$ согласно формуле (5′) $N_{\kappa j} = s_j^{k/h_{kj}} \Big/ s_k^{j/h_{kj}} = \dfrac{s_j^{k/2s}}{s_k^{j/2s}}$. Частное $\dfrac{N_{2j}^{k/2s}}{N_{2k}^{j/2s}} =$

$$= \left(\frac{s_j}{s_2^{j/2}}\right)^{k/2s} \Bigg/ \left(\frac{s_k}{s_2^{k/2}}\right)^{j/2s} = \frac{s_j^{k/2s}}{s_2^{jk/4s}} \cdot \frac{s_2^{jk/4s}}{s_k^{j/2s}} = N_{kj}.$$

Для нечетных $k, j,\ 2 < k < j \le \delta - 1$ и для $h_{kj} = НОД(k, j)$ частное $\dfrac{N_{2j}^{k/h_{kj}}}{N_{2k}^{j/h_{kj}}} = \left(\dfrac{s_j^2}{s_2^j}\right)^{k/h_{jk}} \Bigg/ \left(\dfrac{s_k^2}{s_2^k}\right)^{j/h_{jk}} =$

$$= \frac{s_j^{2k/h_{jk}}}{s_2^{jk/h_{jk}}} \cdot \frac{s_2^{jk/h_{jk}}}{s_k^{2j/h_{jk}}} = N_{kj}^2.$$ Возведем обе части последнего равенства в степень 2^{m-1}. Справа получим в точности величину N_{kj}.

Пусть при тех же условиях k является нечетным числом, а j – четным, $2 < k < j \le \delta - 1$. Вычисления показывают, что $\dfrac{((N_{2j})^2)^{k/h_{kj}}}{N_{2k}^{j/h_{kj}}} = N_{kj}^2$. Если же k является четным числом, а j – нечетным, $2 < k < j \le \delta - 1$, то $\dfrac{N_{2j}^{k/h_{kj}}}{((N_{2k})^2)^{j/h_{kj}}} = N_{kj}^2$. Таким образом, во всех случаях N_{kj}, $2 < k < j \le \delta - 1$ функционально выражается через N_{2j}, N_{2k}.

Следовательно, обосновано следующее предложение.

Предложение 5. Пусть в коде $RS(N,K)$ с проверочной матрицей (2) у синдрома $S(\bar{e})$ компоненты $s_1 = 0$, $s_2 \neq 0$. Тогда у нормы синдрома $\bar{N}(S(\bar{e}))$ координаты N_{2j}, $2 < j \le \delta - 1$ (в количестве $\delta - 3$) вычисляются по формуле (5′), а остальные координаты N_{kj}, $3 \le k < j \le \delta - 1$ функционально выражаются через N_{2k}, N_{2j}: для четных k, j $N_{kj} = N_{2j}^{k/2s} \big/ N_{2k}^{j/2s}$; для нечетных k и четных j величина $N_{kj} = \left(((N_{2j})^2)^{k/h_{kj}} \big/ N_{2k}^{j/h_{kj}}\right)^{2^{m-1}}$; для четных k и нечетных j $N_{kj} = \left(N_{2j}^{k/h_{kj}} \big/ ((N_{2k})^2)^{j/h_{kj}}\right)^{2^{m-1}}$; для нечетных k и четных j координата $N_{kj} = \left(N_{2j}^{k/h_{kj}} \big/ N_{2k}^{j/h_{kj}}\right)^{2^{m-1}}$.

О количестве норм синдромов в РС-кодах. Установленная выше внутренняя зависимость между координатами норменных векторов ставит вопрос о количестве различных норм синдромов. Рассмотрим его для частного случая РС-кодов.

Лемма 1. Пусть код $RS(N,K)$ задан проверочной матрицей (2). Пусть в условиях следствия 2 из предложения 4 $s_1 \neq 0$, и, более того, $s_1 = 1$. Тогда $N_{12} = s_2, N_{13} = s_3, \ldots, N_{1(\delta-1)} = s_{\delta-1}$. Пусть $s_1 = 0, s_2 = 1$, тогда $N_{23} = s_3^2, N_{24} = s_4, \ldots, N_{2j} = s_j^2$ для нечетных j, $2 < j \le \delta - 1$ и $N_{2j} = s_j$ для четных j, $2 < j \le \delta - 1$.

Доказательство вытекает из определения нормы синдрома и формулы (5′).

Таким образом, лемма 1 дает естественные примеры векторов-ошибок, нормы синдромов которых получаются практически без вычислений.

Предложение 6. В коде $RS(N,K)$ с проверочной матрицей (6) имеется $(N+1)^3 + (N+1)^2 + N + 3$ различных норм синдромов.

Доказательство. Пусть выполняются условия предложения 6. Согласно следствию 2 из предложения 4 у всех синдромов $S(\bar{e}) = (s_1, s_2, s_3, s_4)$ с компонентой $s_1 \neq 0$ нормы синдромов определяются первой тройкой координат $\{N_{12}, N_{13}, N_{14}\}$, каждая из которых принадлежит полю $GF(2^m)$ определения кода $RS(N,K)$. Как известно, в данном коде имеется q^4 различных синдромов, в частности, q^3 различных синдромов вида $S(\bar{e}) = (1, s_2, s_3, s_4)$. Тогда согласно лемме 1 имеется q^3 различных троек $\{N_{12}, N_{13}, N_{14}\}$. В таком случае первый класс Г-орбит $<\bar{e}>_\Gamma$ с компонентой синдрома $s_1 \neq 0$ имеет $q^3 = (N+1)^3$ различных норм синдромов.

Пусть $s_1 = 0$. Тогда первые три координаты норменного вектора вырождены и количество векторов $\bar{N}(S(\bar{e}))$ определяется количеством различных троек $\{N_{23}, N_{24}, N_{34}\}$. Пусть $s_1 = 0$, $s_2 \neq 0$. Тогда согласно предложению 5 N_{34} функционально выражается через N_{23}, N_{24} и на количество различных троек $\{N_{23}, N_{24}, N_{34}\}$ не влияет. Иными словами, в этом случае количество троек равно количеству различных пар $\{N_{23}, N_{24}\}$. Согласно второй части леммы 1 при $s_2 = 1$ $\{N_{23}, N_{24}\} = \{s_3^2, s_4\}$. Количество различных синдромов вида $S(\bar{e}) = (0, 1, s_3, s_4)$ в коде $RS(N,K)$ равно $q^2 = (N+1)^2$. Операция возведения в квадрат является автоморфизмом поля Галуа $GF(2^m)$. Отсюда следует, что мощности множеств всевозможных различных пар $\{s_3^2, s_4\}$ и $\{s_3, s_4\}$ совпадают. Таким образом, количество различных пар $\{N_{23}, N_{24}\}$ равно $q^2 = (N+1)^2$.

Пусть $s_1 = 0$, $s_2 = 0$, $s_3 \neq 0$. У всех векторов-ошибок с таким синдромом норма синдрома в условиях предложения 6 имеет единственную невырожденную координату $N_{34} = s_4^3 / s_3^4$. Пусть в этой формуле $s_4 = 1$, а s_3 принимает все возможные значения поля $GF(2^m)$. Операция возведения в четвертую степень также остается автоморфизмом поля $GF(2^m)$. Это означает, что s_3^4 будет принимать значения всех ненулевых

элементов поля Галуа. То же самое можно сказать и об обратных к ним величинах $1/s_3^4$. Таким образом, координата N_{34} принимает N различных значений. При $s_3 \neq 0,\ s_4 = 0$ координата $N_{34} = 0$. Итак, для всевозможных синдромов $S(\bar{e}) = (0,0,s_3,s_4),\ s_3 \neq 0,$ найдется $N+1 = q$ различных норменных векторов.

Векторы $\bar{e}$ с синдромом $S(\bar{e}) = (0,0,0,s_4),\ s_4 \neq 0,$ имеют одну и ту же норму $\bar{N}(S(\bar{e})) = (-,-,\infty,-,\infty,\infty)$. Вектор $\bar{e} = \bar{0}$ и все векторы $\bar{e}$, совпадающие с кодовыми словами, имеют один и тот же синдром $S(\bar{e}) = (s_1,s_2,s_3,s_4) = (0,0,0,0)$. Здесь $\bar{N}(S(\bar{e})) = (-,-,-,-,-,-)$.

Суммируя рассмотренные случаи, приходим к выводу, что в РС-коде с проверочной матрицей (6) имеется в точности $q^3 + q^2 + q + 2$ различных норменных векторов, что полностью доказывает предложение 6.

О равномерном распределении синдромов по нормам.

Лемма 2. В условиях предложения 6 каждое значение норменного вектора $\bar{N}(S(\bar{e})) = (N_{12},N_{13},N_{14},N_{23},N_{24},N_{34})$, кроме $\bar{N}(S(\bar{e})) = (-,-,-,-,-,-)$, принимает как минимум $q-1 = N$ различных синдромов векторов-ошибок.

Доказательство. Подавляющее большинство норменных векторов содержат хотя бы одну координату, принадлежащую мультипликативной группе $GF(2^m)^*$, то есть являющуюся ненулевым элементом поля Галуа $GF(2^m)$. Пусть такой координатой является $N_{12} = s_2 / s_1^2 = \gamma \in GF(2^m)^*$. Это означает, что существует вектор-ошибка $\bar{e}^*$ с таким синдромом $S(\bar{e}^*) = (s_1^*, s_2^*, s_3^*, s_4^*)$, у которого $s_1^* \neq 0,\ s_2^* \neq 0$ и у нормы $\bar{N}^* = \bar{N}(S(\bar{e}^*)) = (N_{12}^*, N_{13}^*, ..., N_{34}^*)$ первая координата $N_{12}^* = s_2^* / (s_1^*)^2 = \gamma$. В силу формулы (5) то же самое значение γ первой координаты N_{12} имеют и норменные векторы $\bar{N}(\sigma^i(S(\bar{e}^*)))$ синдромов $S(\sigma^i(\bar{e}^*)) = = (\alpha^i \cdot s_1^*, \alpha^{2i} \cdot s_2^*, \alpha^{3i} \cdot s_3^*, \alpha^{4i} \cdot s_4^*),\ 0 \le i \le N-1$. У названных синдромов первые компоненты попарно различны. Попарно различны и вторые компоненты этих синдромов, потому что, как уже упоминалось выше, операция возведения в квадрат является автоморфизмом группы $GF(2^m)^*$. Итак, названо как минимум N различных синдромов, у нормы которых координата N_{12} одинакова. Заметим еще, что перечисленные синдромы образуют полный спектр синдромов полной Г-орбиты $< \bar{e}^* >_\Gamma$. Предложение 2 утверждает, что не только координата N_{12}, но и все координаты векторов $\bar{N}(\sigma^i(S(\bar{e}^*)))$ совпадают друг с другом, то есть совпадают сами норменные векторы. Тем самым лемма 2 в первом случае полностью доказана. Точно также последовательно доказывается лемма 2 и для ненулевых значений координат $N_{13}, N_{14}, N_{24}, N_{23}, N_{34}$.

Пусть теперь норменный вектор не содержит координат, принадлежащих $GF(2^m)^*$, но некоторые из его координат равны 0, например, координата N_{12}. Значит, существует конкретная вектор-ошибка $\bar{e}$ в коде $RS(N,K)$ с синдромом $S(\bar{e}) = (\gamma,0,0,0),\ \gamma \in GF(2^m)^*$. У этого синдрома ни одна из компонент s_3 или s_4 не может быть отличной от нуля, иначе мы получаем уже рассмотренный выше случай с ненулевой координатой у вектора $\bar{N}(S(\bar{e}))$. С таким синдромом Г-орбита $J = < \bar{e} >_\Gamma$ является полной, потому что у нее полный спектр синдромов $S(< \bar{e} >_\Gamma) = \{(\alpha^i \cdot \gamma, 0,0,0)\},\ 0 \le i \le N-1$. Норма этой орбиты есть вектор $\bar{N}(J) = (0,0,0,-,-,-)$. Эту норму, как уже сказано, принимают не менее N различных синдромов. Значит, и в данном случае лемма 2 доказана. Приведенный пример одновременно доказывает лемму 2 и для значений $N_{13} = 0$ и $N_{14} = 0$.

Пусть координаты норменного вектора $\bar{N}(S(\bar{e}))$ могут принимать три значения: 0, ∞, −, и при этом первой нулевой координатой является N_{23}. Это возможно только для синдрома $S(\bar{e}) = (0,\gamma,0,0)$, $\gamma \in GF(2^m)^*$. С таким синдромом Г-орбита $J = < \bar{e} >_\Gamma$ является полной, потому что у нее полный спектр синдромов $S(< \bar{e} >_\Gamma) = \{(0,\alpha^i \cdot \gamma,0,0)\},\ 0 \le i \le N-1$. Норма этой орбиты есть вектор $\bar{N}(J) = (\infty,-,-,0,0,-)$. Эту норму, как уже отмечено, принимают не менее N различных синдромов. Следовательно, и в рассматриваемом случае лемма 2 доказана. Отметим, что данный пример доказывает лемму 2 и для значения $N_{24} = 0$.

Пусть по-прежнему координаты норменного вектора $\bar{N}(S(\bar{e}))$ могут принимать три значения: 0, ∞, −, и нулевой координатой является N_{34}. Следовательно, в коде $RS(N,K)$ существует вектор-

ошибка $\bar{e}$ с синдромом $S(\bar{e}) = (0,0,\gamma,0),\ \gamma \in GF(2^m)^*$. С таким синдромом Г-орбита $J = <\bar{e}>_\Gamma$ является полной, потому что у нее полный спектр синдромов $S(<\bar{e}>_\Gamma) = \{(0,0,\alpha^i \cdot \gamma,0)\}, 0 \le i \le N-1$. Норма этой орбиты есть вектор $\bar{N}(J) = (-,\infty,-,\infty,-,0)$. Эту норму, как уже отмечено, принимают не менее *N* различных синдромов. Следовательно, и для данной нормы лемма 2 доказана.

Осталось рассмотреть норменные векторы $\bar{N}$, координаты которых принимают только два значения: ∞, $-$. Такие ситуации возможны лишь для отдельных значений векторов-синдромов. У синдромного вектора не должно быть двух ненулевых координат, иначе у $\bar{N}$ появится координата $N_{ij} \in GF(2^m)^*$. Таким образом, $S(\bar{e})$ может содержать лишь одну ненулевую координату. Три приведенных выше примера $S(\bar{e}) = (\gamma,0,0,0)$; $S(\bar{e}) = (0,\gamma,0,0)$; $S(\bar{e}) = (0,0,\gamma,0),\ \gamma \in GF(2^m)^*$ имеют нормы $\bar{N}(S(\bar{e}))$, обязательно содержащие нулевую координату. Последний нерассмотренный случай: $S(\bar{e}) = (0,0,0,\gamma),\ \gamma \in GF(2^m)^*$. Здесь $\bar{N}(S(\bar{e})) = (-,-,\infty,-,\infty,\infty)$. Данное значение нормы принимают как минимум *N* синдромов $S(<\bar{e}>_\Gamma) = \{(0,0,0,\alpha^i \cdot \gamma)\}, 0 \le i \le N-1$.

Лемма 2 полностью доказана.

Предложение 7. В коде $RS(N,K)$ с проверочной матрицей (6) каждое значение норменного вектора $\bar{N}$, кроме $\bar{N}(S(\bar{e})) = (-,-,-,-,-,-)$, принимают в точности *N* различных синдромов. Исключенное значение $\bar{N}(S(\bar{e})) = (-,-,-,-,-,-)$ принимают вектор-ошибки $\bar{e} = \bar{0}$ и $\bar{e} = \bar{c}$ – любое кодовое слово с одинаковым синдромом $S(\bar{e}) = (0,0,0,0)$.

Доказательство. В рассматриваемом коде $RS(N,K)$ имеется в точности q^4 различных синдромов. Согласно предложению 6 эти синдромы определяют $(N+1)^3 + (N+1)^2 + N + 3$ различных норменных векторов $\bar{N}(S(\bar{e}))$. Лемма 2 утверждает, что $(N+1)^3 + (N+1)^2 + N + 2$ из них принимают как минимум *N* различных синдромов. В общей сложности на перечисленные норменные векторы приходится $\left((N+1)^3 + (N+1)^2 + N + 2\right) \cdot N = (q^3 + q^2 + q + 1) \cdot (q-1) = q^4 - 1$ синдромов.

Предложение 7 полностью доказано.

Предложение 8. Пусть две Г-орбиты J_1, J_2 имеют одинаковые нормы $N(J_1) = N(J_2)$ отличные от нормы $\bar{N}(S(\bar{e})) = (-,-,-,-,-,-)$. Пусть Г-орбита J_1 является полной с полным спектром синдромов. Тогда для всякого вектора $\bar{g} \in J_2$ с синдромом $S(\bar{g}) = S$ найдется вектор-ошибка $\bar{f} \in J_1$, синдром которого $S(\bar{f}) = S$.

Доказательство непосредственно следует из предложения 7.

Предложение 8 завершает построение теории, необходимой для корректной формулировки норменных методов декодирования ошибок РС-кодами. Для реализации норменного метода необходимо составить список 1 всех образующих $\bar{e}_i$ Г-орбит ошибок корректируемой совокупности, список 2 синдромов образующих $S(\bar{e}_i)$ и список 3 норм синдромов образующих $\bar{N}_i = \bar{N}(S(\bar{e}_i))$ (можно без учета зависимых координат норменных векторов), то есть норм соответствующих Г-орбит. Инфокоммуникационная система, приняв очередное сообщение $\bar{x}$, в обязательном порядке вычисляет синдром $S(\bar{x})$. Если $S(\bar{x}) \neq \bar{0}$, вычисляем $\bar{N} = \bar{N}(S(\bar{x}))$. Вектор $\bar{N}$ сравниваем с данными списка 3. Если $\bar{N} = \bar{N}_j$ из списка 3, то сравниваем $S(\bar{x})$ с $S(\bar{e}_j)$. Тем самым определяем показатель ν такой, что $S(\bar{x}) = S(\sigma^\nu(\bar{e}_j))$. Тогда $\bar{c} = \bar{x} + \sigma^\nu(\bar{e}_j)$ – исправленное истинное сообщение.

Заключение. Спектры синдромов орбит ошибок, как правило, являются полными. Структура спектров синдромов копирует структуру самих орбит, которые в свою очередь копируют структуру групп автоморфизмов кода. По аналогии с БЧХ-кодами введено понятие нормы синдрома вектора-ошибки и для кодов Рида – Соломона. Это векторная величина, координаты которой определяются всевозможными парами компонент синдрома. Доказано, что норма синдрома инвариантна относительно действия подстановок группы Г. Поэтому нормы синдромов являются инвариантами каждой отдельно взятой Г-орбиты векторов-ошибок. В работе доказан ряд предложений, отражающих базовые свойства норм синдромов в РС-кодах. Эти результаты составляют теоретическую основу норменного метода коррекции ошибок в классе РС-кодов, формулировкой которого и завершается данная работа.

От классических методов обработки РС-кодов предлагаемый норменный метод отличается прозрачностью, опорой на несложные, легко поддающиеся алгоритмизации, вычисления с синдромами в полях Галуа, периодическими обращениями к устройствам памяти, в которых и сосредоточена наиболее громоздкая, переборная часть метода – поиск нужной нормы Г-орбиты. Здесь поисковая работа осуществляется как минимум на порядок быстрее классических методов, нацеленных на непосредственный поиск конкретной ошибки в сообщении. Соответственно, норменные декодеры РС-кодов обещают быть на порядок быстрее уже известных декодеров.

ЛИТЕРАТУРА

1. MacWilliams, F.J. The Theory of Error-Correcting Codes / F.J. MacWilliams, J.J. Sloan. – Amsterdam : North-holland publishing company, 1977. – 762 с.
2. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение : пер. с англ. / Б. Скляр – Изд. 2-е, испр. – М. : Вильямс, 2003. – 1104 с.
3. Кудряшов, Б.Д. Основы теории кодирования : учеб. пособие / Б.Д. Кудряшов. – СПб. : БХВ-Петербург, 2016. – 400 с.
4. Маров, А.В. Матричный формализм кодов Рида – Соломона / А.В. Маров, А.Ю. Утешев // Вестн. С.-Петерб. ун-та, Сер. 10. – 2016. – Вып. 4.– С. 4–17.
5. Липницкий, В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения : монография / В.А. Липницкий, В.К. Конопелько. – Минск : Изд. центр БГУ, 2007. – 239 с.
6. Липницкий, В.А. Теория норм синдромов : метод. пособие / В.А. Липницкий. – Минск : БГУИР, 2011. – 96 с.
7. Липницкий, В.А. Высшая математика. Основы линейной алгебры и аналитической геометрии / В.А. Липницкий. – Минск : ВА РБ, 2015. – 240 с.
8. Семёнов, С.И. Автоморфизмы и орбиты ошибок кодов Рида – Соломона [в печати] / В.А. Липницкий, С.И. Семёнов // Доклады БГУИР, 2020.

Поступила 04.02.2020

BASICS OF THE THEORY OF SYNDROME NORMS FOR REED-SOLOMON CODES

V. LIPNITSKI, S. SEMYONOV

The theory of syndrome norms (TNS) is developed for Reed-Solomon codes (RS-codes), the extension of TNS, which was developed 20 years ago for the class of the class of Bose-Chaudhuri-Hocquenghem codes (BCH-codes). RS-codes are built on non-binary alphabets, therefore it contain an extremely large variety of correctable errors in contrast to BCH-codes. To correct errors, a systematic application of automorphisms of codes is proposed. Characteristic automorphisms of RS-codes are cyclic and affine substitutions forming cyclic groups Г and A whose orders coincide with the code length. Cyclic and affine substitutions commute with each other and generate a joint АГ group. These three groups act on the space of error vectors of RS-codes, breaking this space into three types of error orbits. As a rule, these orbits are complete, that is, they contain the maximum possible number of errors. The spectra of the syndromes of error orbits are also complete. The structure of the syndrome spectrums copies the structure of the orbits themselves, which in turn copy the structure of groups of code automorphisms. The concept of the norms of the error syndrome is introduced. This is vector quantity whose coordinates are determined by all kinds of pairs of components of the syndrome. It is proved that the norm of the syndrome is invariant under the action of substitution of group Г. So the norms of syndromes are invariants of each individual Г-group. The article proves a number of proposals that reflect the basic properties of the norms of syndromes. These results form the theoretical basic of the norm error correction methods by RS-codes.

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