Владикавказский математический журнал
2016, Том 18, Выпуск 4, С. 23–33

УДК **519.725**

ОБ УСЛОВИЯХ КОРРЕКТНОСТИ ДЕКОДЕРА МЯГКИХ РЕШЕНИЙ ТРОИЧНЫХ КОДОВ РИДА — МАЛЛЕРА ВТОРОГО ПОРЯДКА

В. М. Деундяк, Н. С. Могилевская

Теоретически изучаются условия корректности работы нового декодера мягких решений кодов Рида — Маллера второго порядка над полем $\mathbb{F}_3$, экспериментальное исследование которого показало, что по корректирующей способности он значительно превосходит декодер по минимальному кодовому расстоянию Хемминга. Для дискретного канала передачи данных выделено условие гладкости, при выполнении которого доказано, что исследуемый декодер гарантировано исправляет все ошибки, число которых не превышает допустимое количество ошибок, предусмотренное конструкцией кода.

Ключевые слова: коды Рида — Маллера, мягкий декодер, доказательство корректности декодера.

Введение

Рассмотрим схему прохождения данных в моделях помехоустойчивых каналов связи с дискретным входом: источник сообщений, кодер канала, передатчик, линия связи с шумом, приемник, декодер канала и получатель сообщений [1]. При этом если приемник выдает дискретные данные, то говорят о дискретных каналах и жестких решениях приемника, а если приемник выдает аналоговые сигналы, то говорят о полунепрерывном канале и мягких решениях приемника [2]. В последнем случае имеет смысл использовать декодер мягких решений (ДМР), который обычно дает лучшие результаты по сравнению с декодированием жестких решений; эффективность ДМР основана на том, что в отсутствии демодулятора не накапливаются ошибки квантования. Обычно ДМР обладают большей сложностью [2, с. 357]. К декодерам такого типа относится обладающий значительной корректирующей способностью декодер двоичных кодов Рида — Маллера второго порядка с вещественным входом, предложенный В. М. Сидельниковым и А. С. Першаковым [3], который исследовался в работах [4, 5]. В [6] построен новый ДМР с входными данными из поля комплексных чисел, распространяющий алгоритмы декодирования из [3, 4] на случай кодов Рида — Маллера второго порядка над полем Галуа $\mathbb{F}_3$.

В настоящей работе исследуются условия корректности работы декодера из [6]. Математическая суть этого декодера состоит в том, что для поиска верного кодового слова $\bar{c}$, соответствующего информационному полиному нескольких переменных f, декодер по полученному из канала зашумленному слову $\bar{z}$ строит зашумленные версии кодовых слов для всех производных полинома f, а затем декодирует их в L_1-метрике, пропорциональной метрике Хемминга, и на основе полученных результатов восстанавливает слово $\bar{c}$. Таким образом, поиск по слову $\bar{z}$ ближайшего по метрике Хемминга слова $\bar{c}$

происходит в некотором смысле на основе применения аналога соболевской нормы [7]. Для дискретного канала передачи данных выделено условие гладкости, при выполнении которого сформулирована и доказана теорема о корректности работы этого декодера в ситуации, когда число ошибок в кодовом слове не превосходит половину минимального кодового расстояния.

Отметим, однако, что этот декодер может исправлять часть ошибок и за границей половины минимального кодового расстояния, что подтверждается проведенными экспериментами [8]. Таким образом, естественной областью применения разработанного декодера являются каналы связи низкого качества, используемые для передачи ценных сообщений, какими являются, например, отводные каналы утечки информации [9–11].

1. Коды $RM_3(2,m)$ и разностные операторы

Над полем Галуа $\mathbb{F}_3$ рассмотрим алгебру полиномов от m переменных $\mathbb{F}_3[x_1,\ldots,x_m]$, при этом, не теряя общности, будем полагать, что все мономы имеют вид $ax_1^{\gamma_1}\ldots x_m^{\gamma_m}$, $0\leqslant\gamma_j\leqslant 2$. Для произвольного $\bar\alpha=(\alpha_1,\ldots,\alpha_m)$ из линейного пространства $\mathbb{F}_3^m$ через $\rho(\bar\alpha)$ обозначим сумму координат как сумму натуральных чисел. В пространстве $\mathbb{F}_3^m$ мощности $n=3^m$ зафиксируем линейное упорядочение

$$\{\bar\alpha_1;\ldots;\bar\alpha_n\}\quad(\bar\alpha_{\rm j}=(\alpha_{j_1},\alpha_{j_2},\ldots,\alpha_{j_m})), \tag{1}$$

по параметру $\rho(\bar\alpha)$ от меньшего к большему, а при одинаковых значениях $\rho(\bar\alpha)$ предполагается лексикографический порядок слева направо от большего к меньшему. Полиномы из $\mathbb{F}_3[x_1,\ldots,x_m]$ будем записывать в каноническом виде

$$f(\bar x)=\sum_{\bar\alpha\in\mathbb{F}_3^m} f_{\bar\alpha}\,\bar x^{\bar\alpha},$$

где $\bar\alpha=(\alpha_1,\ldots,\alpha_m)$, $\bar x=(x_1,\ldots,x_m)$, $\bar x^{\bar\alpha}=x_1^{\alpha_1}\ldots x_m^{\alpha_m}$, а порядок слагаемых в сумме соответствует упорядочению (1). Для ненулевого монома $a\bar x^{\bar\alpha}$ степень определяется как $\rho(\bar\alpha)$, а степень $\deg(f)$ полинома f определяется как максимальная степень составляющих его ненулевых мономов. Множество полиномов из $\mathbb{F}_3[x_1,\ldots,x_m]$ степени не выше r обозначим через $\mathbb{F}_3^{(\mathrm{r})}[x_1,\ldots,x_m]$. По аналогии с определением производной в булевом случае (см. [12, с. 89]) определим оператор дифференцирования по направлению $\bar b$ $(\in\mathbb{F}_3^m)$

$$D_{\bar b}:\mathbb{F}_3^{(r)}[x_1,\ldots,x_m]\to\mathbb{F}_3^{(r-1)}[x_1,\ldots,x_m]$$

правилом

$$(D_{\bar b}f)(\bar x)=f_{\bar b}(\bar x)-f(\bar x),\quad f_{\bar b}(\bar x)=f(\bar x+\bar b). \tag{2}$$

Легко видеть, что этот оператор определен корректно и является линейным.

Приведем необходимые сведения о кодах Рида — Маллера над полем $\mathbb{F}_3$:

$$RM_3(r,m)=\left\{(f(\bar\alpha_1),\ldots,f(\bar\alpha_n)):\ f\in\mathbb{F}_3^{(\mathrm{r})}[x_1,\ldots,x_m]\right\}$$

(см., например, [13]). Параметр r $(\leqslant m)$ называется порядком кода $RM_3(r,m)$. Рассмотрим оператор кодирования $C:\mathbb{F}_3^{(r)}[x_1,\ldots,x_m]\to\mathbb{F}_3^n$, определяемый равенством

$$C(f)=(f(\bar\alpha_1),\ldots,f(\bar\alpha_n)),\quad f\in\mathbb{F}_3^{(\mathrm{r})}[x_1,\ldots,x_m]. \tag{3}$$

Полиномы из $\mathbb{F}_3^{(\mathrm{r})}[x_1,\ldots,x_m]$ назовем *информационными*, а вектор, составленный из коэффициентов информационного полинома f, будем называть *информационным вектором* и обозначать через $\bar{f}$. Далее будем рассматривать коды Рида — Маллера порядка 1 и 2. Опишем параметры кода $RM_3(1,m)$: длина кода $n=3^m$, размерность $k=1+m$, минимальное кодовое расстояние $d=2\cdot 3^{m-1}$, число гарантированно исправляемых ошибок $t=3^{m-1}-1$, информационные полиномы кода имеют вид

$$a(\bar{x}) = a_{\bar{0}} + \sum_{\rho(\bar{\alpha})=1} a_{\bar{\alpha}}\bar{x}^{\bar{\alpha}}.$$

Опишем параметры кода $RM_3(2,m)$:

$$n=3^m,\quad k=1+m+C_{m+1}^2,\quad d=3^{m-1},\quad t=\frac{3^{m-1}-1}{2},$$

информационные полиномы кода имеют вид

$$f(\bar{x}) = a_{\bar{0}} + \sum_{\rho(\bar{\alpha})=1} a_{\bar{\alpha}}\,\bar{x}^{\bar{\alpha}} + \sum_{\rho(\bar{\alpha})=2} a_{\bar{\alpha}}\,\bar{x}^{\bar{\alpha}}.$$

В этом равенстве полином $f(\bar{x})$ является суммой скаляра, линейной формы и квадратичной формы, поэтому далее будем его записать следующим образом:

$$f(\bar{x}) = a_{\bar{0}} + \langle \bar{x}, \bar{a}\rangle + \bar{x}A\bar{x}^T, \tag{4}$$

где $\bar{a} = (f_{10\ldots00}, f_{01\ldots00}, \ldots, f_{00\ldots01})$, $\langle\cdot,\cdot\rangle$ — знак скалярного произведения в $\mathbb{F}_3^m$ и

$$A = \begin{pmatrix} f_{200..00} & 2f_{110\ldots00} & 2f_{101\ldots00} & & 2f_{100\ldots10} & 2f_{100\ldots01} \\ 2f_{110\ldots00} & f_{020..00} & 2f_{011\ldots00} & \cdots & 2f_{010\ldots10} & 2f_{010\ldots01} \\ 2f_{101\ldots00} & 2f_{011\ldots00} & f_{002..00} & & 2f_{001\ldots10} & 2f_{001\ldots01} \\ & \vdots & & \ddots & \vdots & \\ 2f_{100\ldots10} & 2f_{010\ldots10} & 2f_{001\ldots10} & & f_{000..20} & 2f_{000\ldots11} \\ 2f_{100\ldots01} & 2f_{010\ldots01} & 2f_{001\ldots01} & \cdots & 2f_{000\ldots11} & f_{000..02} \end{pmatrix}.$$

Отметим, что в поле $\mathbb{F}_3$ выполняется равенство $2^{-1}=2$.

Прямыми выкладками проверяется, что для произвольного полинома f вида (4) и произвольного вектора $\bar{b}$ $(\in \mathbb{F}_3^m)$

$$(D_{\bar{b}}f)(\bar{x}) = 2\bar{x}A\bar{b}^T + f(\bar{b}) - f_{00\ldots00}. \tag{5}$$

Чтобы ввести в пространстве $\mathbb{F}_3^n$ аналог оператора $D_{\bar{b}}$, рассмотрим сначала для $\bar{b}\in\mathbb{F}_3^m$ оператор сдвига $\tau_{\bar{b}}:\mathbb{F}_3^n\to\mathbb{F}_3^n$, определяемый равенством

$$\tau_{\bar{b}}(\bar{a}) = (a_{\bar{\alpha}_1+\bar{b}}, \ldots, a_{\bar{\alpha}_n+\bar{b}}), \tag{6}$$

где $\bar{a} = (a_{\bar{\alpha}_1},\ldots,a_{\bar{\alpha}_n}) \in \mathbb{F}_3^n$ (см. (1)). Отметим, что $\tau_{\bar{b}}$ является перемешивающим биективным отображением. Разностный оператор $\Delta_{\bar{b}}:\mathbb{F}_3^n\to\mathbb{F}_3^n$ определим формулой

$$\Delta_{\bar{b}}(\bar{a}) = \tau_{\bar{b}}(\bar{a}) - \bar{a}. \tag{7}$$

Далее $\Delta_{\bar{b}}(\bar{a})$ будем называть *производным вектором* вектора $\bar{a}$ по направлению $\bar{b}$.

Установим связь между введенными выше операторами.

Лемма 1. *Пусть* $f \in \mathbb{F}_3^2[x_1,\ldots,x_m]$, $\bar{b} \in \mathbb{F}_3^m$. *Тогда*

$$\tau_{\bar{b}}(C(f)) = C(f_{\bar{b}}), \quad C(D_{\bar{b}}f) = \Delta_{\bar{b}}(C(f)).$$

$\lhd$ Для проверки первого равенства следует использовать (3) и (6), а второе вытекает из линейности оператора кодирования C и равенств (2), (7). $\rhd$

2. Помехоустойчивый канал на кодах $RM_3(2,m)$. Гладкость канала

Рассмотрим стандартную схему прохождения данных над алфавитом $\mathbb{F}_3$ в математической модели помехоустойчивого канала связи, основанного на применении описанных выше $[n,k,d]_3$-кодов $RM_3(2,\mathrm{m})$: источник сообщений (ИС), кодер канала (КК), передатчик, линия связи с шумом (ЛСШ), приемник, декодер канала (ДК) и получатель сообщений (ПС) (см. [6]). Из ИС на вход КК поступают информационные векторы $\bar{m} \in \mathbb{F}_3^k$, на выходе КК формируются кодовые векторы $\bar{c} \in \mathrm{RM}_3(2,\mathrm{m})$ $(\subset \mathbb{F}_3^n)$. Чтобы описать работу передатчика рассмотрим мультипликативную группу $\mathbb{C}_3 = \left\{e^{i\frac{2\pi}{3}j}\right\}_{j=0,1,2}(\subset \mathbb{C})$ корней третьей степени из 1, изоморфизм μ группы $\mathbb{C}_3$ на аддитивную группу поля $\mathbb{F}_3$, который определяется равенством $\mu^{-1}(j) = e^{i\frac{2}{3}\pi j}$, $j \in \mathbb{F}_3$, и соответствующее отображение пространств векторов

$$\mu_n : \ \mathbb{C}_3^n \to \mathbb{F}_3^n. \tag{8}$$

Передатчик на физическом уровне конвертирует элементы поля $\mathbb{F}_3$ в комплексные числа из $\mathbb{C}_3$, например, с помощью модуляции с непрерывной фазой (см. [2, с. 170]), и полученные на выходе КК кодовые векторы $\bar{c} \in \mathrm{RM}_3(2,\mathrm{m})$ $(\subset \mathbb{F}_3^n)$ преобразует в $\bar{z} = \mu_n(\bar{c}) \in \mathbb{C}_3^n$. Эти векторы передатчик отправляет в ЛСШ, где в силу искажений они модифицируются в векторы $\bar{z}' \in \mathbb{C}^n$ с ненулевыми координатами. Векторы $\bar{z}' = (z_1', \ldots, z_n')$ поступают на вход приемника, который в зависимости от настроек может выдавать мягкие или жесткие решения о принятом сигнале.

В случае мягких решений приемник преобразует значение каждого сигнала $z_s' \in \mathbb{C} \setminus \{0\}$ с помощью фильтрующей функции

$$\zeta : \mathbb{C}\backslash\{0\} \to \Xi_\varepsilon = \left\{\xi \in \mathbb{C} : \ \varepsilon \leqslant |\xi| \leqslant \varepsilon^{-1}\right\}, \tag{9}$$

с параметром $\varepsilon \in (0;1]$, которая определяется по следующему правилу: если $\varepsilon \leqslant |\xi| \leqslant \varepsilon^{-1}$, то $\zeta(\xi) = \xi$; если $0 < |\xi| < \varepsilon$, то $\zeta(\xi) = \xi|\xi|^{-1}\varepsilon$; если $\varepsilon^{-1} < |\xi|$, то $\zeta(\xi) = \xi|\xi|^{-1}\varepsilon^{-1}$.

В случае жестких решений приемник преобразует вектор $\bar{z}' \in \mathbb{C}^{\mathrm{n}}$ в вектор $\overline{Y} \in \mathbb{C}_3^n$, используя, например, для каждой координаты принцип решающих областей [2]. В этом случае преобразованный вектор $\overline{Y}$ также принадлежит Ξ_ε^n, так как $\mathbb{C}_3^n \subset \Xi_\varepsilon^n$.

Отметим, что вне зависимости от настроек с выхода приемника вектор $\overline{Y} \in \Xi_\varepsilon^n$ направляется в декодер мягких решений, конструкция которого представлена ниже. Этот декодер вычисляет некоторый информационный вектор $\bar{m}' \in \mathbb{F}_3^k$ и передает его в ПС. Очевидно, что с учетом искажений в ЛСШ вектор $\bar{m}'$ может отличаться от исходного вектора $\bar{m}$, отправленного ИС в канал, в таком случае говорят об ошибке декодирования. В зависимости от настроек приемника можно вести речь о помехоустойчивом полунепрерывном или дискретном канале передачи.

Внутри описанного выше помехоустойчивого канала связи можно выделить внутренний непомехоустойчивый канал, свойства которого влияют на корректирующую способность кодека исходного канала. Действительно, если в описанной выше модели помехоустойчивого канала связи убрать блоки КК и ДК, то в режиме жестких решений приемника реализуется дискретный непомехоустойчивый канал, а в режиме мягких решений

приемника — полунепрерывный непомехоустойчивый канал. Тогда схема прохождения данных по каналу следующая: ИС, передатчик, ЛСШ, приемник и ПС. В отсутствии кодека канала предполагается, что ИС формирует векторы, а ПС получает векторы длины n. В случае мягких решений приемника совокупное воздействие передатчика, линии связи и приемника на сообщения назовем оператором внутреннего непомехоустойчивого полунепрерывного канала, который обозначим

$$\mathrm{chn}: \ \mathbb{F}_3^n \to \Xi_\varepsilon^n.$$

В случае жестких решений приемника на вход ПС помехоустойчивого канала поступают элементы из пространства $\mathbb{C}_3^n$. Соответствующий оператор внутреннего непомехоустойчивого дискретного канала обозначим

$$\mathrm{chn}_d: \ \mathbb{F}_3^n \to \mathbb{C}_3^n.$$

Оператор chn_d и породивший его дискретный помехоустойчивый канал будем называть *гладкими*, если зашумление вектора $C(f)$ $(\in \mathrm{RM}_3(2,\mathrm{m}))$ в канале тесно связано с зашумлением векторов $\mathrm{C}(D_{\bar b}f)$ $(\in \mathrm{RM}_3(1,\mathrm{m}))$ для всех $\bar b \in \mathbb{F}_3^m$, а именно, если

$$\Delta_{\bar b}(\mu_n(\mathrm{chn}_d(C(f)))) = \mu_n(\mathrm{chn}_\mathrm{d}(C(D_{\bar b}f))). \tag{10}$$

Разностный оператор $\Delta_{\bar b}$ является дискретной версией оператора дифференцирования $D_{\bar b}$, поэтому условие (10) — это некоторый аналог свойства преобразования касательных расслоений, индуцированных гладким отображением многообразий (см., например, [14, с. 29]).

Лемма 2. *Рассмотрим гладкий дискретный помехоустойчивый канал. Пусть* $f \in \mathbb{F}_3^{(2)}[x_1,\dots,x_m]$, $\bar b \in \mathbb{F}_3^m$,

$$\bar e = \mu_n(\mathrm{chn}_d(C(f))) - C(f), \quad \bar\varepsilon = \mu_n(\mathrm{chn}_d(\mathrm{C}(D_{\bar b}f))) - \mathrm{C}(D_{\bar b}f).$$

Тогда, если вес Хемминга ошибки $\bar e$ *не превосходит число ошибок, гарантированно исправляемых кодом* $\mathrm{RM}_3(2,m)$, *т. е.*

$$\mathrm{wt_h}(\bar e) \leqslant t_{RM_3(2,m)} = \frac{1}{2}\left(3^{m-1}-1\right),$$

то вес Хемминга ошибки $\bar\varepsilon$ *не превосходит число ошибок, гарантированно исправляемых кодом* $\mathrm{RM}_3(1,\mathrm{m})$, *т. е.*

$$\mathrm{wt_h}(\bar\varepsilon) \leqslant t_{RM_3(1,m)} = 3^{m-1}.$$

$\lhd$ Отметим, что значения $t_{RM_3(2,m)}$ и $t_{RM_3(1,m)}$ предъявлены в разделе **1**. Используя условие (10), линейность оператора $\Delta_{\bar b}$ и лемму 1 получаем

$$\begin{aligned}\mu_n(\mathrm{chn}_\mathrm{d}(\mathrm{C}(D_{\bar b}f))) &= \Delta_{\bar b}(\mu_n(\mathrm{chn}_d(C(f)))) = \Delta_{\bar b}(C(f)+\bar e)\\ &= \Delta_{\bar b}(C(f)) + \Delta_{\bar b}(\bar e) = C(D_{\bar b}f) + \tau_{\bar b}(\bar e) - \bar e.\end{aligned}$$

Таким образом,

$$\bar\varepsilon = \mathrm{chn}_d(\mathrm{C}(D_{\bar b}f)) - C(D_{\bar b}f) = \tau_{\bar b}(\bar e) - \bar e.$$

По условию леммы

$$\mathrm{wt_h}(\tau_{\bar b}(\bar e)) = \mathrm{wt_h}(\bar e) \leqslant \frac{1}{2}\left(3^{m-1}-1\right).$$

Следовательно,

$$\mathrm{wt_h}(\bar\varepsilon) = \mathrm{wt_h}(\tau_{\bar b}(\bar e) - \bar e) \leqslant \mathrm{wt_h}(\tau_{\bar b}(\bar e)) + \mathrm{wt_h}(\bar e) \leqslant \left(3^{m-1}-1\right). \rhd$$

3. Конструкция ДМР для кодов $RM_3(2,m)$

Опишем в усовершенствованном виде конструкцию ДМР для кодов $RM_3(2,m)$ из работы [6]. Для этого в пространстве Ξ_ε^n по аналогии с (2), (7) введем операторы

$$\xi_{\bar b}:\Xi_\varepsilon^n\to\Xi_\varepsilon^n,\quad \nabla_{\bar b}:\ \Xi_\varepsilon^n\to\Xi_\varepsilon^n,$$

которые действуют по правилам

$$\xi_{\bar b}(\overline{Y})=\left(y_{\bar b+\bar\alpha_1},\dots\ ,y_{\bar b+\bar\alpha_n}\right),\quad \nabla_{\bar b}(\overline{Y})=\left(\zeta\left(y_{\bar b+\bar\alpha_1}y_{\bar\alpha_1}^{-1}\right),\dots,\zeta\left(y_{\bar b+\bar\alpha_n}y_{\bar\alpha_n}^{-1}\right)\right)\qquad(11)$$

соответственно, где $\overline{Y}=(y_{\alpha_1},\dots,y_{\alpha_n})\in\Xi_\varepsilon^n$, ζ — фильтрующая функция (9).

Алгоритм. *Вход:* $[n,k,d]_3$-код $RM_3(2,m)$, полученный из канала зашумленный кодовый вектор $\overline{Y}=(Y_{\bar\alpha_1},\dots,Y_{\bar\alpha_n})\in\Xi_\varepsilon^n$ $(\subset\mathbb{C}^n)$.

Выход: восстановленный информационный вектор $\bar f$.

Шаг 1. Построим упорядоченный в соответствии с (1) набор векторов из Ξ_ε^n:

$$\left\{\nabla_{\bar\gamma}(\overline{Y})=\left(\zeta\left(Y_{\bar\gamma+\bar\alpha_1}Y_{\bar\alpha_1}^{-1}\right),\dots,\zeta\left(Y_{\bar\gamma+\bar\alpha_n}Y_{\bar\alpha_n}^{-1}\right)\right)\right\}_{\bar\gamma\in\mathbb{F}_3^m,\,\bar\gamma\neq\bar0},$$

где ζ — фильтрующая функция (9), $Y_{\bar\alpha_s}^{-1}$ — число, сопряженное к $Y_{\bar\alpha_s}$.

Шаг 2. Рассмотрим в соответствии с (1) все $\bar\gamma\in\mathbb{F}_3^m$, $\bar\gamma\neq\bar0$, и для фиксированного $\bar\gamma$ определим

$$\overline{P}=(P_{\bar\alpha_1},P_{\bar\alpha_2},\dots,P_{\bar\alpha_n})=\nabla_{\bar\gamma}(\overline{Y}).$$

Среди всех $\beta(\bar x)=\beta_0+\beta_1x_1+\ldots+\beta_mx_m$ из $\mathbb{F}_3^{(1)}[x_1,\dots,x_m]$ найдем полином, который минимизирует функционал:

$$\Psi(\overline{P},\bar\beta)=\sum_{s=1}^{n}\left|P_{\bar\alpha_s}-e^{i\frac{2}{3}\pi\beta(\bar\alpha_s)}\right|(\in\mathbb{R}).$$

Минимальное значение функционала для текущего значения $\bar\gamma$ обозначим через $\Psi_{\bar\gamma}$, а вектор, на котором достигается минимум — через $B_{\bar\gamma}=(\beta_1^{\bar\gamma},\dots,\beta_m^{\bar\gamma})$.

Найдем значения $\Psi_{\bar\gamma}$ и $B_{\bar\gamma}$ для каждого $\gamma\in\mathbb{F}_3^m$, $\bar\gamma\neq\bar0$. Сформируем упорядоченный в соответствии с (1) набор $\Psi=(\Psi_{\bar\alpha_1}=\bar0,\Psi_{\bar\alpha_2},\Psi_{\bar\alpha_3},\dots,\Psi_{\bar\alpha_n})$ и двумерный массив

$$B=\begin{pmatrix}\mathrm{B}_{\bar\alpha_1}\\ \mathrm{B}_{\bar\alpha_2}\\ \dots\\ \mathrm{B}_{\bar\alpha_n}\end{pmatrix}=\begin{pmatrix}0&\dots&0\\ \beta_1^{\bar\alpha_2}&\dots&\beta_m^{\bar\alpha_2}\\ \dots&\dots&\dots\\ \beta_1^{\bar\alpha_n}&\dots&\beta_m^{\bar\alpha_n}\end{pmatrix}.$$

Шаг 3. Пусть $\Theta=B$:

$$\Theta=\begin{pmatrix}\Theta_{\bar\alpha_1}\\ \dots\\ \Theta_{\bar\alpha_n}\end{pmatrix}=\begin{pmatrix}\theta_{11}&\cdots&\theta_{m1}\\ \vdots&\ddots&\vdots\\ \theta_{1n}&\cdots&\theta_{mn}\end{pmatrix}.$$

При необходимости j-й столбец полученного массива будем обозначать через Θ^j, $j=1,\dots,m$. Пусть $\mathrm{Maj}\{X\}$ — функция, возвращающая элемент, встречающийся наибольшее число раз в множестве X. Обновим строки массива Θ:

$$\Theta_{\bar\alpha_s}=\mathrm{Maj}\left\{\Theta_{\bar\alpha_s+\bar\beta_j}-\Theta_{\bar\beta_j}\right\}_{\bar\beta_j\in\mathbb{F}_3^m,\,\bar\beta_j\neq\bar\alpha_s}.$$

Шаг 4. Восстановим квадратичную часть $\psi(\bar{x})$ искомого информационного полинома $f(\bar{x})$, построив матрицу A (см. (4)).

Шаг 4.1. Для каждого $j \in \{1, \ldots, m\}$ на множестве всех линейных однородных полиномов вида

$$\delta(\bar{x}) = \sum_{q=1}^{m} \delta_q x_q, \quad \delta_q \in \mathbb{F}_3, \tag{12}$$

находим минимум функционала, определенного в соответствии с весовой L_1-нормой:

$$T_j(\delta) = \sum_{s=1}^{n} (\Psi_{\bar{\alpha}_s} + 1) \left| e^{i\frac{2\pi}{3}(2\delta(\bar{\alpha}_s) - \theta_{js})} - 1 \right| (\in \mathbb{R}). \tag{13}$$

Минимальное значение функционала для текущего фиксированного значения j обозначим через d_j, а полином, на котором достигается минимум — через

$$\omega^{(j)}(\bar{x}) = \sum_{q=1}^{m} \omega_q^{(j)} x_q.$$

Шаг 4.2. Симметрическую матрицу A построим в виде

$$A = (a_{qj})_{q,j \in [1,\ldots,m]},$$

где

$$a_{qj} = \begin{cases} \omega_j^{(q)}, & d_q < d_j, \\ \omega_q^{(j)}, & d_q \geqslant d_j. \end{cases}$$

Сформируем квадратичную часть $\psi(\bar{x})$ искомого полинома по формуле

$$\psi(\bar{x}) = \sum_{q \leqslant j} \varepsilon\, a_{qj}\, x_q\, x_j, \quad \bar{x} = (x_1, x_2, \ldots, x_m) \in \mathbb{F}_3^m, \quad a_{qj} \in \mathbb{F}_3, \quad q, j \in [1, \ldots, m]\,,$$

где $\varepsilon = 1$, если $q = j$, и $\varepsilon = 2$, если $q \neq j$.

Шаг 5. Среди множества всех полиномов $\zeta(\bar{x})(\in \mathbb{F}_3^{(1)}[x_1, \ldots, x_m])$ найдем полином, который минимизирует значение функционала

$$\Phi(Y, \zeta) = \sum_{s=1}^{n} \left| Y_{\bar{\alpha}_s} - e^{i\frac{2}{3}\pi(\zeta(\bar{\alpha}_s) + \psi(\bar{\alpha}_s))} \right| (\in \mathbb{R}),$$

который обозначим через $\phi(\bar{x}) = c_0 + \sum_{j=1}^{m} c_j x_j$. Результат декодирования строим в виде полинома $f(\bar{x}) = \psi(\bar{x}) + \phi(\bar{x})$, который определяет искомый информационный вектор $\bar{f}$.

4. Достаточное условие корректности работы ДМР

В следующей теореме показано, что алгоритм мягкого декодирования из раздела 3 корректен в случае применения его в гладком дискретном канале в ситуации, когда число ошибок не превышает половины кодового расстояния на одно кодовое слово. Но, проведенные в [8] эксперименты показали, что в действительности ДМР исправляет также и часть ошибок за пределами половины кодового расстояния. Таким образом, в целом, по корректирующей способности разработанный декодер превосходит декодер по минимальному расстоянию Хемминга. Из этого следует, что естественной областью применения

разработанного декодера являются каналы связи низкого качества, которые тем не менее приходится использовать на практике для легальной или нелегальной передачи важных сообщений.

Теорема. *Рассмотрим гладкий дискретный помехоустойчивый канал передачи данных, построенный на кодах Рида — Маллера $RM_3(2,m)$. Пусть $\bar f \in \mathbb{F}_3^k$ — информационный вектор, а $f \in \mathbb{F}_3^{(2)}[x_1,\dots,x_m]$ — соответствующий ему информационный полином. Предположим, что по каналу передано кодовое слово $C(f) \in RM_3(2,m)$, а приемником из канала получен вектор $\overline{Y} = \mathrm{chn}_d(C(f)) \in \mathbb{C}_3^n$, причем*

$$\mathrm{wt}_h(C(f) - \mu_n(\overline{Y})) \leqslant \frac{1}{2}\left(3^{m-1}-1\right).$$

Тогда результатом работы алгоритма декодирования является $\bar f$.

$\lhd$ Рассмотрим работу алгоритма декодирования по шагам.

На первом шаге по полученному из дискретного канала вектору $\overline{Y} = \mathrm{chn_d}(C(f)) \in \mathbf{C}_3^n (\subset \Xi_\varepsilon^n)$ для каждого $\bar\gamma \in \mathbb{F}_3^m$, $\bar\gamma \neq \bar 0$, строится $\nabla_{\bar\gamma}(\overline{Y}) = \nabla_{\bar\gamma}(\mathrm{chn_d}(C(f))) \in \Xi_\varepsilon^n$.

Для произвольного $\bar b \in \mathbb{F}_3^m$ обозначим через

$$\widetilde{\xi}_{\bar b} : \mathbb{C}_3^n \to \mathbb{C}_3^n, \quad \widetilde{\nabla}_{\bar b} : \mathbb{C}_3^n \to \mathbb{C}_3^n$$

ограничения на $\mathbb{C}_3^n$ отображений $\xi_{\bar b}$, $\nabla_{\bar b}$ соответственно. Непосредственно проверяется, что (см. (6)–(8), (11))

$$\tau_{\bar b}\cdot\mu_n = \mu_n\cdot\widetilde{\xi}_{\bar b}, \quad \Delta_{\bar b}\cdot\mu_n = \mu_n\cdot\widetilde{\nabla}_{\bar b}. \tag{14}$$

При определении дискретного канала пространство $\mathbb{C}_3^n$ отождествлялось с изоморфным ему пространством $\mathbb{F}_3^n$, поэтому для построенного на первом шаге алгоритма вектора $\nabla_{\bar\gamma}(\overline{Y})$ получаем, используя (14) и условие гладкости (10), что

$$\begin{aligned}\mu_n(\nabla_{\bar\gamma}(\overline{Y})) &= \mu_n(\tilde\nabla_{\bar\gamma}(\overline{Y})) = \mu_n(\tilde\nabla_{\bar\gamma}(\mathrm{chn_d}(C(f))))\\ &= \Delta_{\bar\gamma}(\mu_n(\mathrm{chn_d}(C(f)))) = \mu_n(\mathrm{chn_d}(C(D_{\bar\gamma}f))).\end{aligned}$$

Таким образом, на первом шаге по полученному из канала вектору $\overline{Y} = \mathrm{chn_d}(C(f)) \in \mathrm{C}_3^n$ фактически построено множество векторов $\mathrm{chn_d}(C(D_{\bar\gamma}f)) \in \mathbb{C}_3^n$, $\bar\gamma \in \mathbb{F}_3^m$, $\bar\gamma \neq \bar 0$. Согласно лемме 1 $C(D_{\bar\gamma}f) \in RM_3(1,m)$. В силу леммы 2 из условия теоремы получаем, что

$$\mathrm{wt_h}(C(D_{\bar\gamma}f) - \mathrm{chn_d}(C(D_{\bar\gamma}f)) \leqslant 3^{m-1}-1,$$

т. е. в построенных векторах $\mathrm{chn_d}(\mathrm{C}(\mathrm{D}_{\bar\gamma}\mathrm{f}))$ код $\mathrm{RM}_3(1,m)$ исправляет все ошибки.

На втором шаге для каждого из векторов $\nabla_{\bar\gamma}(\overline{Y}) = \mathrm{chn_d}(C(D_{\bar\gamma}f))$, $\bar\gamma \in \mathbb{F}_3^m$, $\bar\gamma \neq \bar 0$, с использованием функционала $\Psi(\overline{P},\bar\beta)$ отыскивается такой линейный полином $\beta^{\bar\gamma}(\bar x) = \beta_0 + \beta_1 x_1 + \ldots + \beta_m x_m$, который в закодированном виде $C(\beta^{\bar\gamma}(\bar x)) = \left(e^{i\frac{2}{3}\pi\beta^{\bar\gamma}(\bar\alpha_s)},\dots,e^{i\frac{2}{3}\pi\beta^{\bar\gamma}(\bar\alpha_s)}\right) (\in \mathbb{C}_3^n)$ близок к $\nabla_{\bar\gamma}(\overline{Y})$ по метрике L_1. Как было отмечено выше, код $RM_3(1,m)$ позволяет гарантированно исправить все ошибки в $\nabla_{\bar\gamma}(\overline{Y}) = \mathrm{chn_d}(C(D_{\bar\gamma}f))$. Метрика L_1 пропорциональна метрике Хемминга, поэтому на шаге 2 происходит декодирование производных по минимуму расстояния Хемминга и, следовательно,

$$\beta^{\bar\gamma}(\bar x) = \beta_0 + \beta_1^{\bar\gamma}x_1 + \ldots + \beta_m^{\bar\gamma}x_m = D_{\bar\gamma}f(\bar x). \tag{15}$$

В силу (5)

$$\beta^{\bar\gamma}(\bar x) = 2\bar x A\bar\gamma^T + f(\bar\gamma) - f_{00\ldots00},$$

поэтому

$$B_{\bar\gamma} = \left(\beta_1^{\bar\gamma}, \ldots, \beta_m^{\bar\gamma}\right) = \left(2A\bar\gamma^T\right)^T = 2\bar\gamma A. \tag{16}$$

Таким образом, в строках матрицы B находятся верные значения коэффициентов однородной части $L_{\bar\gamma}f$ производной $D_{\bar\gamma}f$, $\bar\gamma \in \mathbb{F}_3^m$. Иначе говоря,

$$B_{\bar\gamma} = \overline{L_{\bar\gamma}f}. \tag{17}$$

Элементы $\Psi_{\bar\gamma}$ набора Ψ можно назвать коэффициентами недоверия к найденному значению $B_{\bar\gamma}$: чем точнее найдено $B_{\bar\gamma}$, тем меньше параметр $\Psi_{\bar\gamma}$. При отсутствии ошибок в декодируемом кодовом слове элементы $\Psi_{\bar\gamma}$ принимают нулевые значения.

Третий шаг направлен на уточнение значений элементов B. Покажем, что при описанных в формулировке теоремы условиях на канал связи значения элементов B на этом шаге не изменяются. Именно, в основе уточняющих преобразований лежат следующие соображения: из (16) вытекает, что для произвольных $\bar\alpha_s$, $\bar\beta_j \in \mathbb{F}_3^m$ имеет место равенство

$$2\bar\alpha_s A + 2\bar\beta_j A = 2(\bar\alpha_s + \bar\beta_j)A,$$

следовательно, естественно требовать выполнение условия

$$B_{\bar\alpha_s} + B_{\bar\beta_j} = B_{\bar\alpha_s + \bar\beta_j}.$$

Однако выше было показано, что векторы $B_{\bar\gamma}$ найдены верно, следовательно, после процесса обновления строк матрицы $\Theta = B$, эта матрица не изменяется.

На вход четвертого шага поступает матрица $\Theta = B$, строки которой имеют вид (17). Воспользуемся равенством

$$L_{\bar\alpha_s}f = D_{\bar\alpha_s}(S(f)), \tag{18}$$

где $S(f)$ — однородная квадратичная часть f (см. (4)), и отметим, что матрица $\Theta = B$ в качестве строк содержит коэффициенты правильно найденных производных квадратичной части информационного полинома. Строки матрицы $\Theta = B$, соответствующие производным по базисным направлениям

$$\bar\nu_1 = (1,0,0,\ldots,0,0),\ \bar\nu_2 = (0,1,0,\ldots,0,0),\ \ldots,\ \bar\nu_m = (0,0,0,\ldots,0,1),$$

формируют симметрическую матрицу $2A$ (см. (4)). Действительно, воспользовавшись равенством (16), получаем

$$\left(\ B_{\bar\nu_1}^T|\ \ \ldots\ \ |\ B_{\bar\nu_m}^T\ \right) = \left(\ 2A\bar\nu_1^T|\ \ \ldots\ \ |2A\ \bar\nu_m^T\ \right) = 2A\left(\ \bar\nu_1^T|\ \ \ldots\ \ |\ \bar\nu_m^T\ \right) = 2A.$$

Итак, в случае гладкого дискретного помехоустойчивого канала передачи данных, в котором количество ошибок не превосходит половины кодового расстояния, матрица A уже построена, но декодер, спроектированный для более сложной ситуации, продолжает работать: на шаге 4.1 он строит вспомогательные полиномы $\delta_j(\bar x)$, а на шаге 4.2 формирует матрицу A из коэффициентов полиномов $\delta_j(\bar x)$, производя при этом ее симметризацию, которая может потребоваться в случае большого количества ошибок в канале связи. В заключение этого шага по матрице A определяется квадратичная часть $\pi(\bar x)$ искомого информационного полинома $f(\bar x)$. Теперь рассмотрим вспомогательные утверждения и покажем, что ни полиномы $\delta_j(\bar x)$, найденные на шаге 4.1, ни последующий процесс симметризации на шаге 4.2 не портят матрицу A.

Утверждение 1. *Пусть $\delta(\bar{x})$ — линейный однородный полином вида* (12). *Для каждого $j \in \{1,\dots,m\}$ функционал $T_j(\delta)$ принимает нулевое значение при*

$$2\delta(\bar{x}) = (L_{\bar{\nu}_j} f)(\bar{x}).$$

$\lhd$ Из (17) следует, что элементы θ_{js} матрицы $\Theta = B$ вычисляются по формуле $\theta_{js} = \overline{L_{\bar{\alpha}_s} f}\nu_j^T$. Тогда

$$\begin{aligned} 2\delta(\bar{\alpha}_s) = (L_{\bar{\nu}_j} f)(\bar{\alpha}_s) = \bar{\alpha}_s(\overline{L_{\bar{\nu}_j} f})^T = \bar{\alpha}_s(B_{\nu_j}^T) = \bar{\alpha}_s 2A\bar{\nu}_j^T \\ = 2\ \bar{\alpha}_s A\bar{\nu}_j^T = B_{\bar{\alpha}_s}\bar{\nu}_j^T = \overline{L_{\bar{\alpha}_s} f}\nu_j^T = \theta_{js}. \end{aligned}$$

В силу определения функционала $T_j(\delta)$ (см. (13)) это завершает доказательство. $\rhd$

Утверждение 2. *Рассмотрим базисные векторы $\bar{\nu}_j$, $j = 1,\dots,m$, пространства $\mathbb{F}_3^m$. Для столбца Θ^j матрицы Θ справедливо*

$$(\Theta^j)^T = C(L_{\bar{\nu}_j} f) = C(D_{\bar{\nu}_j}(S(f))),$$

где C — оператор кодирования (3).

$\lhd$ Сначала покажем, что (см. (1))

$$D_{\bar{\alpha}_s}(S(f))(\bar{\nu}_j) = D_{\bar{\nu}_j}(S(f))(\bar{\alpha}_s). \tag{19}$$

Используя (16), (18), преобразуем обе части равенства:

$$D_{\bar{\alpha}_s}(S(f))(\bar{\nu}_j) = (L_{\bar{\alpha}_s} f)(\bar{\nu}_j) = \langle B_{\bar{\alpha}_s}, \bar{\nu}_j\rangle = B_{\bar{\alpha}_s}\bar{\nu}_j^T = 2\bar{\alpha}_s A\bar{\nu}_j^T,$$

$$D_{\bar{\nu}_j}(S(f))(\bar{\alpha}_s) = (L_{\bar{\nu}_j} f)(\bar{\alpha}_s) = 2\bar{\nu}_j A\bar{\alpha}_s^T.$$

В силу симметричности матрицы A получаем (19).

Из (15) вытекает, что $\beta_j^{\bar{\gamma}} = D_{\bar{\gamma}}(S(f))(\bar{\nu}_j)$, где $\gamma \in \mathbb{F}_3^m$ (см. (1)). По определению матрица Θ, которая в условиях теоремы совпадает с матрицей B, формируется из n строк вида $B_{\bar{\gamma}} = (\beta_1^{\bar{\gamma}},\dots,\beta_m^{\bar{\gamma}})$. Воспользуемся (19), тогда j-й столбец матрицы Θ имеет вид

$$(\Theta^j)^T = \left(\beta_j^{\bar{\alpha}_1},\dots,\beta_j^{\bar{\alpha}_n}\right)^T = (D_{\bar{\nu}_j}(S(f))(\bar{\alpha}_1),\dots,D_{\bar{\nu}_j}(S(f))(\bar{\alpha}_n))^T = C(D_{\bar{\nu}_j}(S(f))).\ \rhd$$

Таким образом, с учетом условий теоремы, а также сформулированных утверждений, на шаге 4.1 найдены полиномы $\delta_j(\bar{x}) = 2D_{\bar{\nu}_j}(S(f))$, $j = 1,\dots,m$, которые после кодирования формируют столбцы уже найденной матрицы $\Theta = B$. Следовательно, на выходе шага 4.2 из коэффициентов этих полиномов формируется искомая матрица A квадратичной формы (см. (4)), для которой $A = 2(B_{\nu_1}^T|\dots|B_{\nu_m}^T)$.

Итак, на шаге 4.2 по правильно найденной матрице A восстанавливается квадратичная часть ψ искомого информационного полинома f кода $RM_3(2,m)$.

На вход пятого шага алгоритма подается полином ψ. В ходе выполнения этого шага перебором отыскивается линейная часть ϕ полинома $f = \phi + \psi$ таким образом, чтобы вектор $C(f)$ по L_1-метрике, пропорциональной метрике Хемминга, был ближайшим к полученному из канала вектору $\overline{Y}$. В силу условия теоремы, ограничивающего число ошибок в зашумленном кодовом векторе $\overline{Y}$ половиной минимального кодового расстояния кода Рида — Маллера $RM_3(2,m)$, такой полином ϕ, а, следовательно, и полином f находятся алгоритмом верно. $\rhd$

Литература

1. *Деундяк В. М., Маевский А. Э., Могилевская Н. С.* Методы помехоустойчивой защиты данных: Учеб.—Ростов н/Д.: Изд-во Южного федерального ун-та, 2014.—309 с.
2. *Прокис Дж.* Цифровая связь.—М.: Радио и связь, 2000.—800 с.
3. *Сидельников В. М., Першаков А. С.* Декодирование кодов Рида — Маллера при большом числе ошибок // Проблемы передачи информации.—1992.—Т. 28, № 3.—С. 80–94.
4. *Loidreau P., Sakkour B.* Modified version of Sidel'nikov–Pershakov decoding algorithm for binary second order Reed–Muller codes // Ninth International Workshop on Algebraic and Combinatorial Coding theory, ACCT-9, Kranevo.—2004.—P. 266–271.
5. *Могилевская Н. С., Скоробогат В. Р., Чудаков В. С.* Экспериментальное исследование декодеров кодов Рида — Маллера второго порядка // Вестн. Донского гос. тех. ун-та.—2008.—Т. 8, № 3.—С. 231–237.
6. *Деундяк В. М., Могилевская Н. С.* Модель троичного канала передачи данных с использованием декодера мягких решений кодов Рида — Маллера второго порядка // Изв. вузов. Сев.-Кавк. регион. Техн. науки.—2015.—№ 1 (182).—С. 3–10.
7. *Тейлор М.* Псевдодифференциальные операторы.—М.: Мир, 1985.—25 с.
8. *Могилевская Н. С.* Корректирующая способность декодера мягких решений троичных кодов Рида — Маллера второго порядка при большом числе ошибок // Вестн. Донского гос. тех. ун-та.—2015.—№ 1.—С. 121–130.
9. *Деундяк В. М., Косолапов Ю. В.* О стойкости кодового зашумления к статистическому анализу наблюдаемых данных многократного повторения // Модел. и анализ информ. систем.—2012.—Т. 19, № 4.—С. 110–127.
10. *Букашкин С. А.* Метод случайного кодирования // Радиотехника.—2014.—№ 4.—С. 30–36.
11. *Косолапов Ю. В.* Коды для обобщенной модели канала с подслушиванием // Проблемы передачи информации.—2015.—Т.51, № 1.—С. 23–28.
12. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии.—М.: МЦНМО, 2004.—470 с.
13. *Pellikaan R., Wu X.-W.* List decoding of q-ary Reed–Muller codes // IEEE. Trans. Infor. Theory.—2004.—Vol. 50 (4).—P. 679–682.
14. *Хирш М.* Дифференциальная топология.—М.: Мир, 1979.—280 с.

Статья поступила 11 октября 2015 г.

Деундяк Владимир Михайлович
Южный федеральный университет,
доцент кафедры алгебры и дискретной математики
РОССИЯ, 344090, Ростов-на-Дону, ул. Мильчакова, 8 а
E-mail: vl.deundyak@gmail.com

Могилевская Надежда Сергеевна
Донской государственный технический университет,
доцент кафедры кибербезопасности информационных систем
РОССИЯ, 344000, Ростов-на-Дону, пл. Гагарина, 1
E-mail: broshka@nm.com

ON CORRECTNESS CONDITIONS OF A SOFT-DECISIONS DECODER FOR TERNARY REED–MULLER CODES OF SECOND ORDER

Deundyak V. M., Mogilevskaya N. S.

We studied theoretically conditions of correct operation of a new soft decisions decoder of Reed–Muller second order codes over the field $\mathbb{F}_3$, whose experimental research showed that its corrective ability exceeds that of the decoder of the minimum Hamming's distance. For discrete data channel allocated we indicated the smoothness condition under which the decoder guarantees correction of all errors, the number of which does not exceed the permissible number of errors referred to the code design.

Key words: Reed–Muller codes, soft decoder, decoder correctness proof.