**УДК 519.876.5, 519.725** **DOI: 10.14529/cmse200204**

# О ДЕКОДЕРЕ МЯГКИХ РЕШЕНИЙ ДВОИЧНЫХ КОДОВ РИДА—МАЛЛЕРА ВТОРОГО ПОРЯДКА

**© 2020 В.М. Деундяк[1,2], Н.С. Могилевская[2]**

[1]*ФГНУ НИИ «Спецвузавтоматика»*

*(344002 Ростов-на-Дону, пер. Газетный, д. 51),*

[2]*Южный федеральный университет*

*(344090 Ростов-на-Дону, ул. Мильчакова, д. 8а)*

*E-mail: vl.deundyak@gmail.com, nadezhda.mogilevskaia@yandex.ru*

Поступила в редакцию: 22.11.2019

Построена общая модель помехоустойчивого двоичного канала передачи данных, предназначенная для использования с различными декодерами мягких решений. Линия связи, рассматриваемая в модели, является дискретной по входу и непрерывной по выходу. На ее вход подаются дискретные сигналы из мультипликативного двоичного алфавита, а в результате непреднамеренных помех, возникающих в линии связи, на выходе после фильтрации формируются символы из мультипликативной группы поля вещественных чисел, которые затем подаются на вход декодера помехоустойчивого кода. Мягкие и вероятностные декодеры позволяют исправлять большее количество ошибок в кодовых словах, чем гарантируется минимальным расстоянием используемого помехоустойчивого кода. В работе рассмотрен вероятностный декодер мягких решений Сидельникова—Першакова для кодов Рида—Маллера второго порядка в модификации, предложенной П. Лоидрю и Б. Саккуром. Ранее эффективность этих декодеров была подтверждена с помощью имитационных экспериментов, но теоретическое обоснование отсутствовало. В настоящей работе сформулировано требование к каналу связи, названное гладкостью канала, при выполнении которого теоретически доказана корректность этого декодера в случае, когда количество ошибок в каждом кодовом слове ограничено половиной кодового расстояния. В основе доказательства лежит использование теории квадратичных форм и методов дифференциального исчисления в кольце полиномов нескольких переменных над полями Галуа.

*Ключевые слова: коды Рида—Маллера, декодер, модель канала, доказательство корректности декодера.*

**ОБРАЗЕЦ ЦИТИРОВАНИЯ**

Деундяк В.М., Могилевская Н.С. О декодере мягких решений двоичных кодов Рида—Маллера второго порядка // Вестник ЮУрГУ. Серия: Вычислительная математика и информатика. 2020. Т. 9, № 2. С. 55–67. DOI: 10.14529/cmse200204.

## Введение

В.М. Сидельниковым и А.С. Першаковым в [10] предложен вероятностный мягкий декодер для двоичных кодов Рида—Маллера второго порядка (далее СП-декодер). Напомним, что по сравнению с классическими детерминированными декодерами вероятностные и мягкие декодеры исправляют бо́льшее количество ошибок, но при этом обладают большей сложностью. Вероятностные декодеры, как правило, гарантировано исправляют ошибки в пределах половины кодового расстояния, а при дальнейшем увеличении числа ошибок делают это с некоторой вероятностью. Декодеры мягких решений получают на вход данные из канала без демодуляции [9], за счет чего не накапливаются ошибки квантования, и в силу этого качество декодирования растет.

В [1] была предложена модификация СП-декодера (далее СПМ-декодер), авторы которой отказались от использования некоторых параметров СП-декодера, тем самым понизив его сложность, от $O(\log_2 n + hs^3)n^2$ до $O(n^2 \log_2 n)$, где $n$ — длина кода Рида—

Маллера, а $s$ и $h$ — параметры СП-декодера. СП и СПМ декодеры представлены их авторами без обоснования, однако корректирующая способность этих декодеров для дискретных ошибок подтверждена экспериментально (см., например, [1, 8]).

Декодеры СП и СПМ построены для линии связи, на выходе которой вместо входного бинарного алфавита появляются вещественные числа. В обоих декодерах на первом шаге фактически вычисляется производный вектор в мультипликативном виде, однако в соответствующих формулах вместо операции деления используется операция умножения, что, в конечном счете, способствует ухудшению процесса декодирования.

В настоящей работе построена модификация алгоритмов СП и СПМ, в которой производный вектор в мультипликативном виде вычисляется правильно с применением операции деления. Найдено условие для двоичного канала связи, названное гладкостью канала, при выполнении которого доказана корректность этого декодера кодов Рида—Маллера в случае, если число ошибок, повредившее кодовое слово, не превышает половины кодового расстояния.

Статья организована следующим образом. В разделе 1 построена общая модель помехоустойчивого двоичного канала передачи данных, предназначенная для использования с различными декодерами мягких решений, в которой оператор приемника фильтрует входные сигналы из $R$ таким образом, чтобы при вычислении производного вектора не возникало проблемы деления на ноль. Раздел 2 содержит необходимые сведения о кодах Рида—Маллера и описание некоторых их свойств. В разделе 3 разработана модификация СПМ-декодера, предназначенная для использования в канале, описываемом построенной моделью. В разделе 4 сформулировано условие для двоичного канала связи, названное гладкостью канала, при выполнении которого доказана корректность построенного декодера кодов Рида—Маллера в случае, если число ошибок, повредившее кодовое слово, не превышает половины кодового расстояния. В заключении приводится краткая сводка результатов, полученных в работе и указаны направления дальнейших исследований.

## 1. Модель бинарного канала передачи данных

Рассмотрим модель бинарного канала передачи данных (см. рис. 1). Источник сообщений генерирует информационные векторы $\bar{m} = (m_1, m_2, \ldots, m_k)$, $\bar{m} \in F_2^k$, где $F_2^k$ — линейное $k$-мерное пространство над полем Галуа $F_2$. Сгенерированные векторы поступают на вход кодера канала, где они кодируются с помощью некоторого двоичного линейного блочного кода длины $n$ размерности $k(< n)$, для которого известен декодер мягких решений. На выходе кодера канала вырабатываются кодовые векторы $\bar{c}$ из пространства $F_2^n$. В качестве оператора кодера канала рассмотрим отображение $Cod: F_2^k \to F_2^n$.

Из кодера данные попадают на вход передатчика, который трансформирует символы кодовых векторов в сигналы, пригодные для передачи в линии связи. Именно, с помощью изоморфизма аддитивной группы поля $F_2$ на мультипликативную группу $C_2 = \{e^{i\pi j)}\}_{j\in F_2} = \{1; -1\}$:

$$\phi: F_2 \to C_2,\ \phi(j) = e^{i\pi j} = (-1)^j,\ j \in F_2,$$

передатчик в модели преобразовывает кодовые векторы $\bar{c} \in F_2^n$ в векторы $\bar{z} = (z_1, z_2, \ldots, z_n)(\in C_2^n)$.

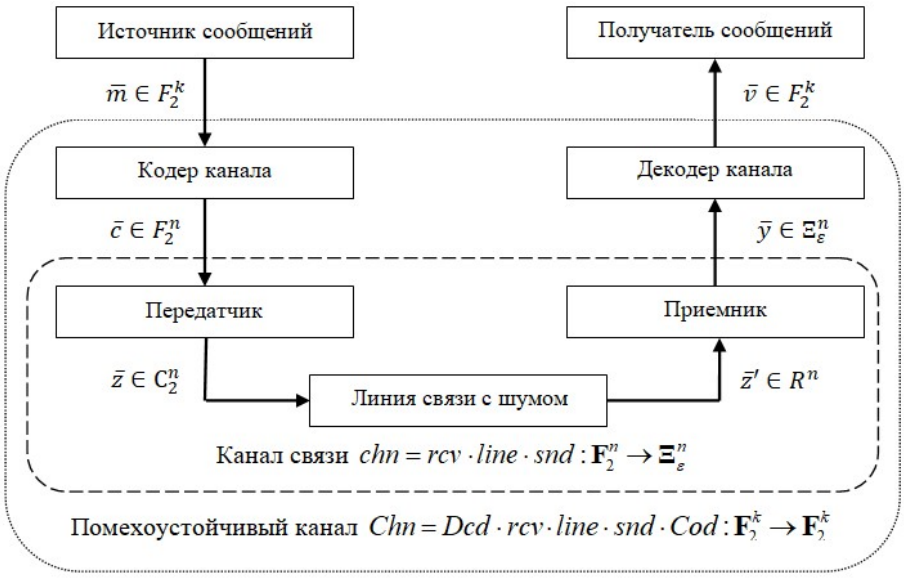


**Рис.1.** Схема моделируемого канала передачи данных

Введем оператор передатчика

$$snd: F_2^n \to C_2^n, \tag{1}$$

где $snd(\bar{a}) = (\phi(a_1), \ldots, \phi(a_n))$, $\bar{a} = (a_1, \ldots, a_n) \in F_2^n$, и рассмотрим отображение

$$\mu_n = (snd)^{-1}. \tag{2}$$

Полученные векторы $\bar{z} = (z_1, z_2, \ldots, z_n)$ направляются передатчиком в линию связи. Заметим, что физический аналог сигнала $z_j$ можно получить, например, применяя двоичную фазовую манипуляцию, в которой фаза несущего колебания смещается на одно из двух значений: ноль или $\pi$ [11].

На вход линии связи подаются дискретные сигналы из $C_2$, интерпретируемые как элементы $R$. В результате присутствующих в линии связи помех, на выходе вместо сигналов ±1 могут появиться произвольные вещественные числа из $R$. Отметим, что рассматриваемая линия связи является дискретной по входу и непрерывной по выходу. Таким образом, под воздействием шума координаты вектора $\bar{z}$ искажаются и формируется вектор $\bar{z}' = (z_1', z_2', \ldots, z_n') \in R^n$, и в результате получаем оператор линии связи $line: C_2^n \to R^n$.

Из линии связи вектор $\bar{z}' \in R^n$ поступает на вход приемника, который преобразует сигнал $z'_s$ в $y_s$ из допустимой области $\Xi_\varepsilon = \{\xi \in R | \varepsilon \le |\xi| \le 1/\varepsilon\}$, где $\varepsilon (\in (0;1])$ — параметр приемника. После такой фильтрации на выходе приемника появляется вектор $\bar{y} = (y_1, \ldots, y_n) \in \Xi_\varepsilon^n$. В результате, получаем оператор приемника с мягкими решениями:

$$rcv: R^n \to \Xi_\varepsilon^n. \tag{3}$$

Рассмотрим подробнее действие фильтра (см. рис. 2). Заштрихованные участки соответствуют допустимой области $\Xi_\varepsilon$, черные точки соответствуют корректным значениям сигнала из алфавита $C_2 = \{-1; 1\}$. Белые точки соответствуют искаженным, но оставшимся в допустимой области, сигналам. После фильтрации сигналы, принадлежащие области $\Xi_\varepsilon$, не изменяются. Если же искажение переводит сигнал за границы этой области (серые точки), то приемник смещает этот сигнал в область $\Xi_\varepsilon$ по кратчайшему пути.

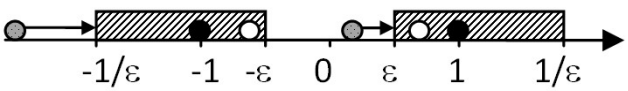


**Рис. 2.** Действие фильтра

Оператор непомехоустойчивого канала определим равенством

$$chn = rcv \cdot line \cdot snd\colon F_2^n \to \Xi_\varepsilon^n.$$

На вход декодера мягких решений поступает вектор $\bar{y}\,(\in \Xi_\varepsilon^n)$ с выхода приемника. Задача декодера состоит в восстановлении исходного информационного вектора $\bar{m} \in F_2^k$, через $Dcd$ обозначим оператор декодера $Dcd\colon \Xi_\varepsilon^n \to F_2^n$. Результат декодирования $\bar{v}$ передается получателю сообщения, при этом, если помеховая обстановка такова, что декодирование прошло успешно, то $\bar{m} = \bar{v}$.

Оператор помехоустойчивого канала определим формулой:

$$Chn = Dcd \cdot rcv \cdot line \cdot snd \cdot Cod\colon F_2^k \to F_2^k.$$

Из определений описанных операторов вытекает, что $Chn = Dcd \cdot chn \cdot Cod$.

Если в модели приемник принимает жесткие решение, т.е. формирует на своем выходе элементы из $C_2$, то реализуется дискретный непомехоустойчивый канал. Оператор этого канала имеет вид

$$chn_d = rcv \cdot line \cdot snd\colon F_2^n \to C_2^n, \tag{4}$$

и поэтому $Chn = Dcd \cdot chn_d \cdot Cod$.

Отметим, что для троичного канала связи подобная модель была ранее рассмотрена в [3–5], однако двоичная модель имеет отличие в геометрическом представлении сигнала и фильтрации.

## 2. Основные определения и свойства двоичных кодов Рида—Маллера

Над полем $F_2$ рассмотрим кольцо $F_2[x_1,\dots,x_m]$ полиномов от $m$ переменных. Далее будем полагать, что все мономы в полиномах этого кольца имеют вид $\phi = x_1^{\alpha_1}\dots x_m^{\alpha_m}$, $\alpha_i \in \{0;1\}$, $i = \overline{1,m}$.

Пусть $\rho(\bar{\alpha}) = \alpha_1 + \alpha_2 + \dots + \alpha_m$, где $\bar{\alpha} = (\alpha_1,\dots,\alpha_m) \in \{0;1\}^m$. Степень монома $\bar{x}^{\bar{\alpha}} = x_1^{\alpha_1}\dots x_m^{\alpha_m}$ определяется как $\deg(\bar{x}^{\bar{\alpha}}) = \rho(\bar{\alpha})$. Степень полинома $f \in F_2[x_1,x_2,\dots,x_m]$ определяется как максимум степеней его мономов с ненулевыми коэффициентами.

Зафиксируем упорядочение из $n = 2^m$ векторов

$$Order^m = \{\bar{\alpha}_1,\dots,\bar{\alpha}_n\}, \tag{5}$$

где $\bar{\alpha}_j = (\alpha_{j_1},\alpha_{j_2},\dots\alpha_{j_m})$, $\alpha_{j_i} \in \{0;1\}$, элементы которого расположены по возрастанию $\rho(\bar{\alpha})$, и упорядочены лексикографически при одинаковых $\rho(\bar{\alpha})$. Например,

$$Order^3 = \{(0,0,0);(0,0,1);(0,1,0);(1,0,0);(0,1,1);(1,0,1);(1,1,0);(1,1,1)\},$$

$$Order^2 = \{(0,0);\ (0,1);\ (1,0);\ (1,1)\ \}.$$

Далее полиномы $f \in F_2[x_1,\dots,x_m]$ будем записывать, располагая их слагаемые согласно упорядочению (5), и рассматривать их как сумму однородных полиномов со степенями от нуля до $\deg(f)$:

$$f(\bar{x}) = \sum\nolimits_{\rho(\bar{\alpha})\le\deg(f)} f_{\alpha_1\alpha_2\dots\alpha_m} x^{\alpha_1}x^{\alpha_2}\dots x^{\alpha_m} = f_{\bar{0}}x^{\bar{0}} + \sum\nolimits_{\rho(\bar{\alpha})=1} f_{\bar{\alpha}}\bar{x}^{\bar{\alpha}} + \sum\nolimits_{\rho(\bar{\alpha})=2} f_{\bar{\alpha}}\bar{x}^{\bar{\alpha}} + \dots + \sum\nolimits_{\rho(\bar{\alpha})=\deg(f)} f_{\bar{\alpha}}\bar{x}^{\bar{\alpha}} \tag{6}$$

Полиномы из $F_2[x_1,\dots,x_m]$, степени которых не превышают $r$, образуют линейное пространство $F_2^{(r)}[x_1,\dots,x_m]$:

$$F_2^{(r)}[x_1,\dots,x_m] = \{f(x_1,\dots,x_m) \in F_2\ [x_1,\dots,x_m] \mid \deg(f(x_1,\dots,x_m)) \le r\}.$$

Используя (5) для нумерации элементов кодового слова, определим двоичный код Рида—Маллера [2, 7] с параметрами $r$, $m$, где $m \ge r \ge 1$, $m \ge 2$, следующим образом:

$$RM(r,m) = \{(f(\bar{\alpha}_1),\dots,f(\bar{\alpha}_n)) | f \in F_2^{(r)}[x_1,\dots,x_m]\} \subset F_2^n. \tag{7}$$

Параметр $r$ называют порядком кода. Информационными полиномами кода $RM(r,m)$ являются полиномы из кольца $F_2^{(r)}[x_1,\ldots,x_m]$. Вектор $\bar{v} \in F_2^k$ коэффициентов информационного полинома $v(x_1,\ldots,x_m)$, называется информационным вектором. Основные параметры кода $RM(r,m)$ длина $n$, размерность $k$, минимальное кодовое расстояние $d$ и число исправляемых ошибок $t$ вычисляются по формулам:

$$n = 2^m,\ k = \sum_{i=0}^{r} C_m^i,\ d = 2^{m-r},\ t = 2^{m-r-1} - 1.$$

В случае кода $RM(1,m)$

$$n = 2^m,\ k = 1 + m,\ d = 2^{m-1},\ t = 2^{m-2} - 1, \tag{8}$$

а информационные полиномы записываются в виде

$$f(\bar{x}) = \sum\nolimits_{\rho(\bar{\alpha})\le 1} f_{\bar{\alpha}}\bar{x}^{\bar{\alpha}} = a_{\bar{0}}\bar{x}^{\bar{\alpha}} + \sum\nolimits_{\rho(\bar{\alpha})=1} a_{\bar{\alpha}}\bar{x}^{\bar{\alpha}}.$$

В случае кода $RM(2,m)$

$$n = 2^m,\ k = 1 + m + C_m^2\ ,\ d = 2^{m-2},\ t = 2^{m-3} - 1, \tag{9}$$

а информационные полиномы записываются в виде

$$f(\bar{x}) = \sum\nolimits_{\rho(\bar{\alpha})\le 2} f_{\bar{\alpha}}\bar{x}^{\bar{\alpha}} = a_{\bar{0}}\bar{x}^{\bar{\alpha}} + \sum\nolimits_{\rho(\bar{\alpha})=1} a_{\bar{\alpha}}\bar{x}^{\bar{\alpha}} + \sum\nolimits_{\rho(\bar{\alpha})=2} a_{\bar{\alpha}}\bar{x}^{\bar{\alpha}}.$$

Определим оператор кодирования

$$C: F_2^{(r)}[x_1,\ldots,x_m] \to F_2^n,$$

формулой

$$C(f) = (f(\bar{\alpha}_1),\ldots,f(\bar{\alpha}_n)), \tag{10}$$

где $f \in F_2^{(r)}[x_1,\ldots,x_m]$ информационный полином, $\alpha_i \in Order^m$.

Согласно [3, 6, 7] оператор дифференцирования полинома $f \in F_2^{(r)}[x_1,\ldots,x_m]$ по направлению $\bar{b} \in F_2^m$:

$$D_{\bar{b}}: F_2[x_1,\ldots,x_m] \to F_2[x_1,\ldots,x_m]$$

определяется правилом:

$$(D_{\bar{b}}f)(\bar{x}) = f_{\bar{b}}(\bar{x}) - f(\bar{x}),\quad \bar{x} \in F_2^m, \tag{11}$$

где

$$f_{\bar{b}}(\bar{x}) = f(\bar{x} + \bar{b}).$$

Полином $D_{\bar{b}}f$ называется производным полиномом для полинома $f \in F_2^{(r)}[x_1,\ldots,x_m]$ по направлению $\bar{b} \in F_q^m$.

Рассмотрим $f \in F_2^{(r)}[x_1,\ldots,x_m]$, $\bar{b} \in F_2^m$, тогда $D_{\bar{b}}f \in F_2^{(r-1)}[x_1,\ldots,x_m]$, а ограничение $D_{\bar{b}}$ на $F_2^{(r)}[x_1,\ldots,x_m]$ задает линейный оператор:

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

В работе [6] показано, что, если $f(\bar{x}) \in F_2^{(2)}[x_1,\ldots,x_m]$ — полином в виде (6), $\bar{b} = (b_1,\ldots,b_m) \in F_2^m$, тогда полиномы $f(\bar{x})$ и $(D_{\bar{b}}f)(\bar{x})$ могут быть записаны с использованием квадратичных форм:

$$f(\bar{x}) = f_{\bar{0}} + \bar{x}\hat{\bar{f}}^T + \bar{x}A\bar{x}^T, \tag{12}$$

где

$$\hat{\bar{f}} = (f_{10\ldots00}, f_{01\ldots00}, \ldots, f_{00\ldots01}),$$

$$A = \begin{pmatrix} 0 & f_{110..00} & f_{101..00} & \cdots & f_{100..10} & f_{100..01} \\ 0 & 0 & f_{011..00} & \cdots & f_{010..10} & f_{010..01} \\ 0 & 0 & 0 & \cdots & f_{001..10} & f_{001..01} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & f_{000..11} \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

$$(D_{\bar{b}}f)(\bar{x}) = \bar{x}(A + A^T)\bar{b}^T + f(\bar{b}) - f_{\bar{0}}. \tag{13}$$

Построим аналог оператора $D_{\bar{b}}$ (см. (11)) для линейного пространства $F_2^{\mathrm{n}}$, $n = 2^m$. Для нумерации элементов векторов из $F_2^{\mathrm{n}}$ будем использовать векторы из $\mathrm{F}_2^{\mathrm{m}}$, порядок которых определен в (5). Определим оператор сдвига $\tau_{\bar{b}}$, как перемешивающее биективное отображение

$$\tau_{\bar{b}}\colon F_2^{\mathrm{n}} \to F_2^{\mathrm{n}}, \quad \tau_{\bar{b}}(\bar{a}) = (a_{\bar{\alpha}_1+\bar{b}}, \ldots, a_{\bar{\alpha}_n+\bar{b}}),$$

где $\bar{a} = (a_{\bar{\alpha}_1}, \ldots, a_{\bar{\alpha}_n}) \in F_2^{\mathrm{n}}$, $\bar{b} = (b_1, \ldots, b_m) \in F_2^{\mathrm{m}}$. Разностный оператор $\Delta_{\bar{b}}$, являющийся аналогом $D_{\bar{b}}$, определим формулой:

$$\Delta_{\bar{b}}\colon F_2^{\mathrm{n}} \to F_2^{\mathrm{n}}, \Delta_{\bar{b}}(\bar{a}) = \tau_{\bar{b}}(\bar{a}) - \bar{a}, \bar{a} = (a_{\bar{\alpha}_1}, \ldots, a_{\bar{\alpha}_n}) \in F_2^{\mathrm{n}}. \tag{14}$$

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

В работе [6] показано, что, если $f \in F_q^{(2)}[x_1, x_2, \ldots, x_m]$, $\bar{b} = (b_1, \ldots, \mathrm{b_m}) \in F_q^m$, то

$$\tau_{\bar{b}}(C(f)) = C(f_{\bar{b}}),\ C(D_{\bar{b}}f) = \Delta_{\bar{b}}(C(f)), \tag{15}$$

где $\Delta_{\bar{b}}$, $D_{\bar{b}}$ и $C$ определены (10), (11) и (14) соответственно. Следовательно, если $C(w) \in RM(2,m)$, то и $\Delta_{\bar{b}}(C(w))) \in RM(1,m)$.

## 3. Декодер мягких решений для кодов $RM(2,m)$

Построим алгоритм декодирования мягких решений для кодов $RM(2,m)$, основываясь на модификации СПМ-декодера [1]. Напомним, что декодеры СП и СПМ построены для линии связи, на выходе которой появляются вещественные числа. При этом в обоих декодерах фактически вычисляется производный вектор в мультипликативном виде, хотя в соответствующих формулах вместо операции деления используется операция умножения. Ниже разработана модификация алгоритма СПМ, в которой производный вектор в мультипликативном виде вычисляется правильно с применением операции деления.

В пространстве $\Xi_\varepsilon^n$ подобно (14) введем операторы

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

формулами

$$\xi_{\bar{b}}(\bar{Y}) = (y_{\bar{\beta}+\bar{\alpha}_1}, \ldots, y_{\bar{\beta}+\bar{\alpha}_n}), \nabla_{\bar{b}}(\bar{Y}) = (\zeta(y_{\bar{\beta}+\bar{\alpha}_1} y_{\bar{\alpha}_1}^{-1}), \ldots, \zeta(y_{\bar{\beta}+\bar{\alpha}n} y_{\bar{\alpha}n}^{-1})),$$

где $\bar{Y} = (y_{\bar{\alpha}_1}, \ldots, y_{\bar{\alpha}_n}) \in \Xi_\varepsilon^n$, $\zeta$ — фильтрующая функция, выполняемая оператором приемника $rcv$ (см. (3)).

Вход: кодовый вектор $\bar{Y} = chn_d(C(f)) = (Y_{\bar{\alpha}_1}, \ldots, Y_{\bar{\alpha}_n}) \in C_2^n (\subset \Xi_\varepsilon^n)$, зашумленный в канале, а также параметры $m$, $n$, $k$ кода $RM(2,m)$.

Выход: информационный вектор $\bar{f}$.

Шаг 1. По вектору $\bar{Y} \in \Xi_\varepsilon^n$ построим упорядоченый согласно с (5) набор векторов из $R^n$:

$$\left\{\nabla_{\bar{\gamma}}(\bar{Y}) = \zeta\left(Y_{\bar{\gamma}+\bar{\alpha}_1} Y_{\bar{\alpha}_1}^{-1}, \ldots, Y_{\bar{\gamma}+\bar{\alpha}_n} Y_{\bar{\alpha}_n}^{-1}\right)\right\}_{\bar{\gamma} \in F_2^m, \bar{\gamma} \neq 0},$$

где $\zeta = rcv$ (см. (3)).

Шаг 2. Рассмотрим все векторы $\bar{\gamma} \in F_2^m$, $\bar{\gamma} \neq \bar{0}$, и $\bar{P}^{\bar{\gamma}} = (P_{\bar{\alpha}_1}, \ldots, P_{\bar{\alpha}_n}) = \nabla_{\bar{\gamma}}(\bar{Y})$. Для каждого $\bar{\beta} = (\beta_1, \ldots, \beta_m) \in F_2^m$ вычислим функционал

$$\Psi(\bar{P}^{\bar{\gamma}}, \bar{\beta}) = \sum\nolimits_{s=1}^{n} \left| P_{\bar{\alpha}_s} (-1)^{\langle \bar{\beta}, \bar{\alpha}_s \rangle} \right| (\in R),$$

где $\langle \bar{\beta}, \bar{\alpha}_s \rangle (\in F_2)$ — скалярное произведение. Обозначим через $\Psi_{\bar{\gamma}}$ максимальное значение функционала для фиксированного $\bar{\gamma}$, а через $B_{\bar{\gamma}} = (\beta_1^{\bar{\gamma}}, \beta_2^{\bar{\gamma}}, \ldots, \beta_m^{\bar{\gamma}})$ вектор $\bar{\beta}$, на котором достигается $\Psi_{\bar{\gamma}}$. Если функционал $\Psi(\bar{P}^{\bar{\gamma}}, \bar{\beta})$ принимает одинаковое наибольшее значение на нескольких векторах $\bar{\beta}$, то $B_{\bar{\gamma}}$ выбирается случайно из таких векторов.

Сгенерируем, используя (5), набор $\Psi = (\Psi_{\bar{\alpha}_1 = 0}, \Psi_{\bar{\alpha}_2}, \ldots, \Psi_{\bar{\alpha}_n})$ и массив

$$B = \begin{pmatrix} B_{\bar{\alpha}_1} \\ B_{\bar{\alpha}_2} \\ \dots \\ B_{\bar{\alpha}_n} \end{pmatrix} = \begin{pmatrix} 0 & \dots & 0 \\ \beta_1^{\bar{\alpha}_2} & \dots & \beta_m^{\bar{\alpha}_2} \\ \dots & \dots & \dots \\ \beta_1^{\bar{\alpha}_n} & \dots & \beta_m^{\bar{\alpha}_n} \end{pmatrix}.$$

Шаг 3. Положим

$$\Theta = \begin{pmatrix} \Theta_{\bar{\alpha}_1} \\ \dots \\ \Theta_{\bar{\alpha}_n} \end{pmatrix} = \begin{pmatrix} \theta_{1,1} & \dots & \theta_{m,1} \\ \dots & \dots & \dots \\ \theta_{1,n} & \dots & \theta_{m,n} \end{pmatrix} := B$$

и пересчитаем строки $\Theta$:

$$\Theta_{\bar{\alpha}_s} = Maj\left\{\Theta_{\bar{\alpha}_s+\bar{\beta}_j} - \Theta_{\bar{\beta}_j}\right\}_{\bar{\beta}_j \in F_2^m, \bar{\beta}_j \neq \bar{\alpha}_s, \bar{\beta}_j \neq \bar{0}},$$

где функция $Maj\{X\}$ находит элемент из конечного набора $X$, который встречается чаще остальных векторов в этом наборе.

Шаг 4. Для каждого $j = 1, \dots, m$ на множестве всех полиномов вида

$$\delta(\bar{x}) = \sum_{q=1}^{m} \delta_q x_q,\ \delta_q \in F_2,$$

находим максимум $d_j$ функционала

$$T_j(\delta) = \sum_{s=1}^{n} \Psi_{\bar{\alpha}_s} (-1)^{\delta(\bar{\alpha}_s) - \theta_{j,s}} (\in R),$$

и полином $\omega^{(j)}(\bar{x}) = \sum_{q=1}^{m} \omega_q^{(j)} x_q$, на котором он достигается.

Шаг 5. Сформируем матрицу $(A + A^T) = (a_{qi})_{q,j \in [1,..,m]}$, где

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

Шаг 6. Вычислим однородный полином второго порядка $\psi(\bar{x})$

$$\psi(\bar{x}) = \sum_{q<j} a_{qj} x_q x_j, \text{ где } \bar{x} = (x_1, x_2, \dots, x_m) \in F_2^m,\ a_{qj} \in F_2,\ q, j \in [1, \dots, m].$$

Шаг 7. (5.) На множестве всех полиномов $\bar{\zeta}(\bar{x})(\in F_2^{(1)}[x_1, x_2, \dots, x_m])$ найдем полином $\varphi(\bar{x})$, минимизирующий функционал

$$\Phi(Y, \zeta) = \sum_{s=1}^{n} \left| Y_{\bar{\alpha}_s} (-1)^{\bar{\zeta}(\bar{\alpha}_s) + \psi(\bar{\alpha}_s)} \right| (\in R).$$

Искомый информационный вектор $\bar{f}$ определяется полиномом $f(\bar{x}) = \psi(\bar{x}) + \varphi(\bar{x})$.

## 4. Обоснование корректности декодера мягких решений для гладкого канала

Рассмотрим построенную выше модель помехоустойчивого канала связи, использующую коды $RM(2, m)$. По аналогии с [5] дискретный помехоустойчивый канал, действие которого описывается оператором $chn_d$ (4), назовем *гладким*, если зашумленные в канале векторы $C(f)(\in RM(2, m))$ и $C(D_{\bar{b}}(w))(\in RM(1, m))$, где $\bar{b} \in F_2^m$, связаны равенством

$$\Delta_{\bar{b}}(\mu_n(chn_d(C(f)))) = \mu_n(chn_d(C(D_{\bar{b}} f))). \quad (16)$$

В [5] отмечено, что понятие гладкости канала возникло в связи с некоторой аналогией из теории гладких преобразований дифференцируемых многообразий [12].

**Лемма**. Рассмотрим дискретный помехоустойчивый канал, дейсвие которого описывается оператором $chn_d$ (4) и для которого выполняется условие гладкости (16). Пусть $f \in F_2^{(2)}[x_1, \dots, x_m]$, $\bar{b} \in F_2^m$,

$$\bar{e} = \mu_n(chn_d(C(f))) - C(f),\ \bar{\varepsilon} = \mu_n(chn_d(C(D_{\bar{b}} f))) - C(D_{\bar{b}} f).$$

Тогда, если вес Хемминга вектора ошибки $\bar{e}$ ограничен сверху числом ошибок, исправление которых гарантируется параметрами кода $RM_2(2,m)$, т.е.

$$wt_h(\bar{e}) \le t_{RM_2(2,m)} = 2^{m-3} - 1,$$

то вес Хемминга вектора ошибки $\bar{\varepsilon}$ ограничен сверху числом ошибок, исправление которых гарантируется параметрами кода $RM_2(1,m)$, т.е.

$$wt_h(\bar{\varepsilon}) \le t_{RM_2(1,m)} = 2^{m-2} - 1.$$

*Доказательство.* Количество ошибок $t_{RM_2(2,m)}$ и $t_{RM_2(1,m)}$, которые исправляются кодами $RM_2(2,m)$, $RM_2(1,m)$ подсчитаны в (8–9). Из (16), свойства линейности оператора $\Delta_{\bar{b}}$ и (15) получаем

$$\mu_n\left(chn_d\left(C(D_{\bar{b}}f)\right)\right) = \Delta_{\bar{b}}\left(\mu_n\left(chn_d\left(C(f)\right)\right)\right) = \Delta_{\bar{b}}(C(f) + \bar{e}) =$$
$$= \Delta_{\bar{b}}\left(C(f)\right) + \Delta_{\bar{b}}(\bar{e}) = C(D_{\bar{b}}f) + \tau_{\bar{b}}(\bar{e}) - \bar{e}.$$

Следовательно,

$$\bar{\varepsilon} = chn_d\left(C(D_{\bar{b}}f)\right) - C(D_{\bar{b}}f) = \tau_{\bar{b}}(\bar{e}) - \bar{e}.$$

Используя неравенство $wt_h(\bar{e}) \le 2^{m-3} - 1$, оценим сверху вес вектора $\bar{\varepsilon}$:

$$wt_h(\bar{\varepsilon}) = wt_h(\tau_{\bar{b}}(\bar{e}) - \bar{e}) \le wt_h(\tau_{\bar{b}}(\bar{e})) + wt_h(\bar{e}) \le 2(2^{m-3} - 1) = 2^{m-2} - 2.$$

Легко видеть, что выполняется условие леммы

$$wt_h(\bar{\varepsilon}) \le 2^{m-2} - 1.$$

В доказательстве леммы фактически показано, что если в передаваемом по каналу кодовому слову кода Рида—Маллера второго порядка произойдет ошибок не более чем $t_{RM_2(2,m)} = 2^{m-3} - 1$, то в производном векторе, построенном на основе зашумленного кодового слова, ошибок будет не более $2^{m-2} - 2$. Но производный вектор является кодовым словом кода Рида—Маллера первого порядка, следовательно, в нем может быть гарантировано исправлено не более чем $2^{m-2} - 1$ ошибок, т.е. есть некоторый «запас» по исправлению ошибок. Однако если увеличить на единицу число «разрешенных» ошибок в кодовом слове кода второго порядка, то исправление всех ошибок в производном векторе не гарантируется.

**Теорема.** Рассмотрим двоичный канал, помехоустойчивость которого обеспечивается применением кодов Рида—Маллера $RM(2,m)$, для которого выполняется условие гладкости (15). Пусть $\bar{f} \in F_2^k$ и $f \in F_2^{(2)}[x_1,\dots,x_m]$ — соответствующие друг другу информационные вектор и полином. Предположим, что кодовое слово $C(f) \in RM_2(2,m)$ было отправлено в канал, а из канала принят вектор $\bar{Y} = chn_d(C(f)) \in C_2(\subset \Xi_\varepsilon^n)$, такой, что

$$wt_h(C(f) - \mu_n(\bar{Y})) \le 2^{m-3} - 1.$$

Тогда алгоритм декодирования на выходе строит полином $f$.

*Доказательство. На первом шаге* по $\bar{Y} = chn_d(C(f)) \in C_2^n(\subset \Xi_\varepsilon^n)$ строятся векторы

$$\nabla_{\bar{\gamma}}(\bar{Y}) = \nabla_{\bar{\gamma}}(chn_d(C(f))),$$

где $\bar{\gamma} \in F_2^m$, $\bar{\gamma} \ne \bar{0}$.

Покажем, что на этом шаге фактически вычисляются векторы, которые могли быть получены, если бы по каналу передавалось бы не кодовое слово $C(f)$, а производные от этого слова во всех направлениях, т.е. $\nabla_{\bar{\gamma}}(\bar{Y}) = chn_d(C(D_{\bar{\gamma}}f))$, $\bar{\gamma} \in F_2^m, \bar{\gamma} \ne \bar{0}$.

Введем ограничения на $C_2^n$ отображений $\xi_{\bar{b}}$, $\Delta_{\bar{b}}$:

$$\tilde{\xi}_{\bar{b}}: C_2^n \to C_2^n,\ \tilde{\nabla}_{\bar{b}}: C_2^n \to C_2^n,$$

где $\bar{b} \in F_2^m$. Прямыми выкладками (см. (2), (14)) проверяется, что

$$\tau_{\bar{b}} \cdot \mu_n = \mu_n \cdot \tilde{\xi}_{\bar{b}}, \Delta_{\bar{b}} \cdot \mu_n = \mu_n \cdot \tilde{\nabla}_{\bar{b}}. \qquad (17)$$

Выше с использованием оператора $\mu_n$ пространство $C_2^n$ отождествлялось с $F_2^n$ (см. (1–2)), следовательно,

$$\mu_n(\nabla_{\bar{\gamma}}(\bar{Y})) = \mu_n(\tilde{\nabla}_{\bar{\gamma}}(\bar{Y})) = \mu_n(\tilde{\nabla}_{\bar{\gamma}}(chn_d(C(f)))),$$

используя (17), получаем

$$\mu_n(\tilde{\nabla}_{\bar{\gamma}}(chn_d(C(f)))) = \Delta_{\bar{\gamma}}(\mu_n(chn_d(C(f)))).$$

Из полученных равенств и условия гладкости (16) вытекает, что

$$\mu_n(\nabla_{\bar{\gamma}}(\bar{Y})) = \Delta_{\bar{\gamma}}(\mu_n(chn_d(C(f)))) = \mu_n(chn_d(C(D_{\bar{\gamma}}f))).$$

Вектор $C(D_{\bar{\gamma}}f)$ является кодовым словом $RM(1,m)$ и в силу леммы

$$wt_h(C(D_{\bar{\gamma}}f) - chn_d(C(D_{\bar{\gamma}}f))) < 2^{m-2} - 1.$$

*На втором шаге* из векторов $\nabla_{\bar{\gamma}}(\bar{Y}) = chn_d(C(D_{\bar{\gamma}}f)) = \tilde{\nabla}_{\bar{\gamma}}(\bar{Y})$, $\bar{\gamma} \in F_2^m$, $\bar{\gamma} \neq \bar{0}$, с помощью $\Psi(\bar{P},\bar{\beta})$, находится линейный однородный полином $\beta^{\bar{\gamma}}(\bar{x}) = \beta_1 x_1 + \ldots + \beta_m x_m$, который в закодированном виде $C(\beta^{\bar{\gamma}}(\bar{x})) = ((-1)^{\beta^{\bar{\gamma}}(\alpha_1)}, \ldots, (-1)^{\beta^{\bar{\gamma}}(\alpha_n)})(\in C_2^n)$ из всех подобных полиномов наиболее близок к $\nabla_{\bar{\gamma}}(\bar{Y})$. Как было показано в лемме, все ошибки в $\nabla_{\bar{\gamma}}(\bar{Y}) = chn_d(C(D_{\bar{\gamma}}f))$ исправляются кодом $RM(1,m)$. Фактически на шаге 2 производные полиномы декодируются по минимуму расстояния Хемминга, таким образом

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

Из (13)

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

следовательно,

$$B_{\bar{\gamma}} = (\beta_1^{\bar{\gamma}}, \ldots, \beta_m^{\bar{\gamma}}) = ((A + A^T)\bar{\gamma}^T)^T = \bar{\gamma}(A + A^T). \quad (18)$$

Получаем, что строки матрицы $B$ содержат верные значения коэффициентов однородной части $L_{\bar{\gamma}}f$ производной $D_{\bar{\gamma}}f$, $\bar{\gamma} \in F_2^m$. Тогда

$$B_{\bar{\gamma}} = \overline{L_{\bar{\gamma}}f}. \quad (19)$$

Обозначим s-тый столбец матрицы $(A + A^T)$ через $(A + A^T)^{(s)}$, тогда в силу (18)

$$B = \begin{pmatrix} B_{\bar{\alpha}_1} \\ B_{\bar{\alpha}_2} \\ \ldots \\ B_{\bar{\alpha}_n} \end{pmatrix} = \begin{pmatrix} \overline{L_{\bar{\alpha}_1}f} \\ \overline{L_{\bar{\alpha}_2}f} \\ \ldots \\ \overline{L_{\bar{\alpha}_n}f} \end{pmatrix} = \begin{pmatrix} \bar{\alpha}_1(A + A^T)^{(1)} & \ldots & \bar{\alpha}_1(A + A^T)^{(m)} \\ \bar{\alpha}_2(A + A^T)^{(1)} & \ldots & \bar{\alpha}_2(A + A^T)^{(m)} \\ \ldots & \ldots & \ldots \\ \bar{\alpha}_n(A + A^T)^{(1)} & \ldots & \bar{\alpha}_n(A + A^T)^{(m)} \end{pmatrix}.$$

В строках матрицы $B$, которые соответствуют векторам $\bar{\alpha}_i$ веса 1, т.е. $\bar{e}_1$=(1,0,...,0), $\bar{e}_2$=(0,1,...,0), ..., $\bar{e}_m$=(0,0,...,1), расположены неизменённые строки матрицы $(A + A^T)$. Согласно (19) в этих же строках расположены векторы коэффициентов однородной части $\overline{L_{\bar{e}_j}f}$ производной $D_{\bar{e}_j}f$. Тогда из симметричности матрицы $(A + A^T)$ вытекает, что ее столбцы так же содержат значения $\overline{L_{\bar{e}_j}f}$, $j = \overline{1,m}$.

В столбце $s$ матрицы $B$ расположены скалярные произведения вектора $(A + A^T)^s = \overline{L_{\bar{e}_s}f}$ на векторы $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ из (5). Другими словами, в столбце $s$ матрицы $B$ расположены закодированные значения однородной части производной $D_{\bar{e}_s}f$ (см. (19)).

Точность нахождения $B_{\bar{\gamma}}$ можно оценить по элементы $\Psi_{\bar{\gamma}}$ набора $\Psi$, а именно: чем больше параметр $\Psi_{\bar{\gamma}}$, тем точнее найдено $B_{\bar{\gamma}}$. Если декодируемое слов не содержит ошибок, то все элементы набора $\Psi$ равны $n$.

*На третьем шаге* уточняются значения элементов $B$. При описанных в формулировке теоремы условиях на канал связи значения элементов $B$ на этом шаге не изменяются. Покажем это. Согласно (17) для произвольных $\bar{\alpha}_s$, $\bar{\beta}_j \in F_2^m$ справедливо

$$\bar{\alpha}_s(A + A^T) + \bar{\beta}_j(A + A^T) = (\bar{\alpha}_s + \bar{\beta}_j)(A + A^T),$$

поэтому, должно выполняться

$$B_{\bar{\alpha}_s} + B_{\bar{\beta}_j} = B_{\bar{\alpha}_s + \bar{\beta}_j}.$$

Как уже было отмечено, векторы $B_{\bar{\gamma}}$ построены верно, следовательно, процедура пересчета строк не изменяет матрицу $\Theta = B$.

*На вход четвертого шага* поступает матрица $\Theta = B$. Выше было показано, что ее строки, соответствующие производным по базисным направлениям $\bar{e}_1$=(1,0,...,0), $\bar{e}_2$=(0,1,...,0), ..., $\bar{e}_m$=(0,0,...,1), формируют матрицу $(A + A^T)$ (см. (12)). Следовательно, в случае гладкого дискретного помехоустойчивого канала передачи данных, в котором количество ошибок не превосходит половины кодового расстояния, матрица $(A + A^T)$ уже построена. Но так как декодер разработан работы в ситуации с большим числом ошибок, то он продолжает работать и на 4, 5 и 6 шагах строит матрицу $(A + A^T)$. А именно, на четвертом шаге он строит вспомогательные полиномы $\delta(\bar{x}) = \sum_{q=1}^{m} \delta_q x_q$, $\delta(\bar{x}) \in F_2^m$, максимизирующие функционала $T_j(\delta)$.

*На пятом шаге* используя коэффициенты полиномов $\delta(\bar{x})$, декодер формирует матрицу $(A + A^T)$. При этом он учитывает ее симметричную структуру.

*На шестом шаге* из коэффициентов матрицы $(A + A^T)$ формируется полином $\pi(\bar{x})$, представляющий собой часть искомого полинома $f(\bar{x})$, содержащая квадратичные слагаемые. Обозначим эту часть полинома $\pi(\bar{x})$.

Покажем, что, с учетом условия теоремы, шаги 4, 5 и 6 не изменяют матрицу $(A + A^T)$. Функционал $T_j(\delta)$ для каждого $j \in \{1, \ldots, m\}$достигает максимального значения при $\delta(\bar{x}) = (L_{\bar{e}_j} f)(\bar{x})$:

$$\delta(\bar{\alpha}_s) = \left(L_{\bar{e}_j} f\right)(\bar{\alpha}_s) = \bar{\alpha}_s \left(\overline{L_{\bar{e}_j} f}\right)^T = \bar{\alpha}_s \left(B_{\bar{e}_j}^T\right) = \bar{\alpha}_s A \bar{e}_j^T = B_{\bar{\alpha}_s}^T \bar{e}_j^T = \overline{L_{\bar{\alpha}_s} f}\, \bar{e}_j^T = \theta_{js},$$

следовательно, найденные значения $\delta(\bar{x})$ совпадают со строками/столбцами матрицы $(A + A^T)$. Действия шага 5 направлены на симметризацию матрицы $(A + A^T)$, однако, при соблюдении условия теоремы построенная матрица $(A + A^T) = (a_{qi})_{q,j \in [1,..,m]}$ уже является симметричной. Следовательно, квадратичная часть $\psi$ искомого информационного полинома $f$ кода $RM(2, m)$ восстанавливается верно.

*На вход седьмого шага* алгоритма поступает полином $\psi$, который является квадратичной частью искомого информационного полинома $f$ кода $RM(2, m)$.

Затем перебираются все возможные значения линейной части $\phi$ полинома $f = \phi + \psi$. Каждый полином $f$ кодируется, и среди них всех полученных кодовых векторов $C(f)$ находится ближайший по $L_1$-метрике к вектору $\bar{Y}$.

Учитывая введенное в теореме ограничение на число ошибок в зашумленном кодовом векторе $\bar{Y}$, линейная часть $\phi$ и сам полином $f$ находятся алгоритмом верно.

## Заключение

В работе рассмотрен мягкий вероятностный декодер кодов Рида—Маллера, разработанный В.М. Сидельниковым и А.С. Першаковым, с изменениями, внесенными П. Лоидрю и Б. Саккуром, позволившими уменьшить вычислительную сложность декодирования. Для этого декодера известны результаты экспериментов, подтверждающие его высокую корректирующую способность [1, 8].

В разработанной общей модели канала предусматривается специальный фильтр, дающий возможность применять в декодере мультипликативный бинарный алфавит $C_2$ , что позволило построить такую модификацию алгоритма СПМ, в которой производный

вектор в мультипликативном виде вычисляется правильно. Получено теоретическое обоснование корректности этого декодера при выполнении условия гладкости канала.

Дальнейшие исследования могут быть связаны с использованием построенного декодера в кодовых криптосистемах и для распределенной передачи данных (см., например, [6]).

## Литература


1. 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'2004) (Kranevo, Bulgaria, 2004). 2004. P. 266–271.
2. Pellikaan R., Wu X.-W. List decoding of q-ary Reed—Muller Codes // IEEE Trans. On Information Theory. 2004. Vol. 50, no. 3. P. 679–682. DOI: 10.1109/tit.2004.825043.
3. Деундяк В.М., Могилевская Н.С. Дифференцирование полиномов нескольких переменных над полями Галуа нечетной мощности и приложения к кодам Рида-Маллера // Вестник Донского государственного технического университета. 2018. Т. 18, № 3. С. 339–348. DOI: 10.23947/1992-5980-2018-18-3-339-348.
4. Деундяк В.М., Могилевская Н.С. Модель троичного канала передачи данных с использованием декодера мягких решений кодов Рида—Маллера второго порядка // Известия высших учебных заведений. Северо-Кавказский регион. Серия: Технические науки. 2015. № 1(182). С. 3–10. DOI: 10.17213/0321-2653-2015-1-3-10.
5. Деундяк В.М., Могилевская Н.С. Об условиях корректности декодера мягких решений троичных кодов Рида—Маллера второго порядка // Владикавказский математический журнал. 2016. Т. 18, № 4. С. 23–33.
6. Деундяк В.М., Могилевская Н.С. Схема разделенной передачи конфиденциальных данных на основе дифференцирования полиномов нескольких переменных над простыми полями Галуа // Вопросы кибербезопасности. 2017. Т. 5, № 24. С. 64–71. DOI: 10.21681/2311-3456-2017-5-64-71.
7. Логачев О.А. Булевы функции в теории кодирования и криптологии. Москва: МЦНМО, 2004. 470 с.
8. Могилевская Н.С., Скоробогат В.Р., Чудаков В.С. Экспериментальное исследование декодеров кодов Рида—Маллера второго порядка // Вестник ДГТУ. 2008. Т. 8, № 3. С. 231–237.
9. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. Москва: Техносфера, 2005. 320 с.
10. Сидельников В.М., Першаков А.С. Декодирование кодов Рида—Маллера при большом числе ошибок // Пробл. передачи информ. 1992. Т. 28, № 3. С. 80–94.
11. Скляр Б. Цифровая связь. Теоретические основы и практическое применение, 2-е издание. Москва: Издательский дом «Вильямс», 2016. 1104 с.
12. Хирш М. Дифференциальная топология. Москва: Мир, 1979. 280 с.


Деундяк Владимир Михайлович, к.ф.-м.н., доцент, ФГНУ НИИ «Спецвузавтоматика», кафедра алгебры и дискретной математики, Южный федеральный университет (Ростов-на-Дону, Российская Федерация)

Могилевская Надежда Сергеевна, к.т.н., доцент, кафедра алгебры и дискретной математики, Южный федеральный университет (Ростов-на-Дону, Российская Федерация)

DOI: 10.14529/cmse200204

# ON SOFT SOLUTIONS DECODER FOR REED–MULLER BINARY CODES OF THE SECOND ORDER

© 2020 V.M. Deundyak[1,2], N.S. Mogilevskaya[2]
[1]*FGNU NII "Specvuzavtomatika"*
*(Gazetniy 51, Rostov-on-Don, 344002 Russia),*
[2]*Southern Federal University*
*(Milchakova 8a, Rostov-on-Don, 344090 Russia)*
*E-mail: vl.deundyak@gmail.com, nadezhda.mogilevskaia@yandex.ru*
Received: 22.11.2019

A general model of a noise-resistant binary data channel is constructed, intended for use with various soft decision decoders. The communication line considered in the model is discrete in input and continuous in output. Discrete signals from the multiplicative binary alphabet are received at its input, and due to distortions acting in the communication line, symbols from the multiplicative group of the field of real numbers are formed at the output after filtering, which are then fed to the input of the error-correcting code decoder. Soft and probabilistic decoders of error-correcting codes allow correcting more errors in code words than is guaranteed by the minimum distance of the code used. The paper considers a probabilistic Sidelnikov—Pershakov decoder of soft solutions for Reed—Muller codes of the second order in the modification proposed by P. Loidreau and B. Sakkour. Earlier, the effectiveness of these decoders was confirmed by simulation experiments, but there was no theoretical justification. In this paper, the requirement to the communication channel, called the smoothness of the channel, is formulated, in which the correctness of this decoder is theoretically proved in the case when the number of errors per code word does not exceed half the code distance. The proof is based on the use of the theory of quadratic forms and methods of differential calculus in the polynomial ring of several variables over Galois fields.

*Keywords: Reed–Muller codes, decoder, model of channel, proof of decoder correctness.*

**FOR CITATION**

Deundyak V.M., Mogilevskaya N.S. On Soft Solutions Decoder for Reed–Muller Binary Codes of the Second Order. *Bulletin of the South Ural State University. Series: Computational Mathematics and Software Engineering.* 2020. Vol. 9, no. 2. P. 55–67. (in Russian) DOI: 10.14529/cmse200204.



## References

1. 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'2004) (Kranevo, Bulgaria, 2004). 2004. P. 266–271.
2. Pellikaan R., Wu X.-W. List decoding of q-ary Reed–Muller Codes. IEEE Trans. On Information Theory. 2004. Vol. 50, no. 3. P. 679–682. DOI: 10.1109/tit.2004.825043.
3. Deundyak V.M., Mogilevskaya N.S. Differentiation of polynomials in several variables over Galois fields of odd cardinality and applications to Reed–Muller codes. Vestnik of Don

State Technical University. 2018. Vol. 18, no. 3. P. 339–348. (in Russian) DOI: 10.23947/1992-5980-2018-18-3-339-348.

4. Deundyak V.M., Mogilevskaya N.S. The model of the ternary communication channel with using the decoder of soft decision for Reed–Muller codes of the second order. University news. North-Caucasian region. Technical sciences series. 2015. Vol. 1, no. 182. P. 3–10. (in Russian) DOI: 10.17213/0321-2653-2015-1-3-10.
5. Deundyak V.M., Mogilevskaya N.S. On Correctness Conditions of a Soft-Decisions Decoder for Ternary Reed–Muller Codes of Second Order. Vladikavkaz Mathematical Journal. 2016. Vol. 18, no. 4. P. 23–33. (in Russian)
6. Deundyak V.M., Mogilevskaya N.S. The confidential data divided transmission scheme based on differential calculus of polynomials in several variables over prime Galois fields Voprosy kiberbezopasnosti. 2017. Vol. 5, no. 24. P. 64–71. (in Russian) DOI: 10.21681/2311-3456-2017-5-64-71.
7. Logachev O.A., Salnikov A.A., Iashchenko V.V. Boolean functions in coding theory and cryptology. MCCME, 2004. 470 p. (in Russian)
8. Mogilevskaya N.S., Skorobogat V.R., Chudakov V.S. Experimental research of second order Reed–Muller codes. Vestnik of Don State Technical University. 2008. Vol. 8, no. 3. P. 231–237. (in Russian)
9. Morelos-Saragosa R. The art of noiseless coding. Methods, Algorithms, Application. Tekhnosfera, 2005. 320 p. (in Russian)
10. Sidelnikov V.M., Pershakov A.S. Decoding of Reed–Muller codes with a large number of errors. Problems of Information Transmission. 1992. Vol. 28, no. 3. P. 80–94. (in Russian)
11. Skliar B. Digital communication. Theoretical foundations and practical application. Viliams Press, 2016. 1104 p. (in Russian)
12. Hirsch M. Differential topology. Mir Press, 1979. 280 p. (in Russian)