Вестник Донского государственного технического университета. 2018. Т. 18, № 3. С. 339–348. ISSN 1992-5980 eISSN 1992-6006
Vestnik of Don State Technical University. 2018. Vol. 18, no. 3, pp. 339–348. ISSN 1992-5980 eISSN 1992-6006

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT

УДК 512.6+519.725 https://doi.org/10.23947/1992-5980-2018-18-3-339-348

Дифференцирование полиномов нескольких переменных над полями Галуа нечетной мощности и приложения к кодам Рида-Маллера*

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

[1] НИИ «Спецвузавтоматика», г. Ростов-на-Дону, Российская Федерация.
[2] Южный федеральный университет, г. Ростов-на-Дону, Российская Федерация.

Differentiation of polynomials in several variables over Galois fields of fuzzy cardinality and applications to Reed-Muller codes***

V. M. Deundyak[1,2], N. S. Mogilevskaya[2]**

[1] Research Institute “Spetsvuzavtomatika”, Rostov-on-Don, Russian Federation.
[2] Southern Federal University, Rostov-on-Don, Russian Federation

Введение. Полиномы нескольких переменных над полями Галуа лежат в основе теории кодов Рида-Маллера, а также используются в ряде криптографических задач. В работе изучаются свойства таких полиномов, заданных над произвольными полями Галуа нечетной мощности. Для полученных результатов предложены два практических приложения: схема разделения данных и декодер кодов Рида-Маллера.

Материалы и методы. С использованием линейной алгебры, теории полей Галуа и общей теории полиномов нескольких переменных получены результаты, связанные с дифференцированием и интегрированием полиномов нескольких переменных над полями Галуа нечетной мощности. Для векторов построен и изучен аналог оператора дифференцирования.

Результаты исследования. На основе полученных результатов о дифференцировании и интегрировании полиномов предложен новый декодер для кодов Рида-Маллера второго порядка и предложена схема организации разделенной передачи конфиденциальных данных, т.е. такой системы связи, в которой исходные данные на стороне отправителя разделяются на несколько частей и, независимо друг от друга, передаются по различным каналам связи, а на стороне получателя из принятых частей восстанавливаются исходные данные. Особенностью предлагаемой схемы является то, что она позволяет защищать данные, как от нелегитимного доступа, так и от непреднамеренных ошибок, при этом в обоих случаях используется один и тот же математический аппарат. Разработанный декодер для кодов Рида-Маллера второго порядка, заданных над произвольным нечетным полем Галуа, может иметь некоторое ограничение по числу исправляемых ошибок, однако, его использование целесообразно для ряда

Introduction. Polynomials in several variables over Galois fields provide the basis for the Reed-Muller coding theory, and are also used in a number of cryptographic problems. The properties of such polynomials specified over the derived Galois fields of fuzzy cardinality are studied. For the results obtained, two real-world applications are proposed: partitioning scheme and Reed-Muller code decoder.

Materials and Methods. Using linear algebra, theory of Galois fields, and general theory of polynomials in several variables, we have obtained results related to the differentiation and integration of polynomials in several variables over Galois fields of fuzzy cardinality. An analog of the differentiation operator is constructed and studied for vectors.

Research Results. On the basis of the obtained results on the differentiation and integration of polynomials, a new decoder for Reed-Muller codes of the second order is given, and a scheme for organizing the partitioned transfer of confidential data is proposed. This is a communication system in which the source data on the sender is divided into several parts and, independently of one another, transmitted through different communication channels, and then, on the receiver, the initial data is restored of the parts retrieved. The proposed scheme feature is that it enables to protect data, both from the nonlegitimate access, and from unintentional errors; herewith, one and the same mathematical apparatus is used in both cases. The developed decoder for the second-order Reed-Muller codes prescribed over the derived odd Galois field may have a constraint to the recoverable error level; however, its

* Работа выполнена в рамках инициативной НИР.
** E-mail: vl.deundyak@gmail.com, nadezhda.mogilevskaia@yandex.ru
*** The research is done within the frame of independent R&D.

каналов связи.
Обсуждение и заключения. Предложенные практические приложения полученных результатов представляются полезными для организации надежных систем связи. В дальнейшем планируется исследование процесса восстановления исходного полинома по его производным, в случае их частичного искажения, и разработка соответствующих приложений.

use is advisable for a number of the communication channels.
Discussion and Conclusions. The proposed practical applications of the results obtained are useful for the organization of reliable communication systems. In future, it is planned to study the restoration process of the original polynomial by its derivatives, in case of their partial distortion, and the development of appropriate applications.

Ключевые слова: полиномы нескольких переменных, поля Галуа, производные полиномов, дифференцирование полиномов, коды Рида-Маллера, декодирование, разделенная передача данных.,

Keywords: polynomials in several variables, Galois fields, polynomial derivatives, differentiation of polynomials, Reed-Muller codes, decoding, partitioned data transmission.

Образец для цитирования: Деундяк, В. М. Дифференцирование полиномов нескольких переменных над полями Галуа нечетной мощности и приложения к кодам Рида-Маллера / В. М. Деундяк, Н. С. Могилевская // Вестник Дон. гос. техн. ун-та. — 2018. — Т. 18, № 3. — С. 339–348. https://doi.org/10.23947/1992-5980-2018-18-3-339-348

For citation: V. M. Deundyak, N. S. Mogilevskaya. Differentiation of polynomials in several variables over Galois fields of fuzzy cardinality and applications to Reed-Muller codes. Vestnik of DSTU, 2018, vol. 18, no.3, pp. 339–348. https://doi.org/10.23947/1992-5980-2018-18-3-339-348

Введение. Полиномы нескольких переменных над полями Галуа и их производные применяются в различных областях защиты информации. Некоторые вопросы, связанные с интегрированием и дифференцированием полиномов нескольких переменных, рассмотрены в ряде работ. Например, в [1] исследуются полиномы, заданные над простыми полями Галуа, в [2–4] получены результаты для булевых функций, а в [5–6] получены результаты для полиномов, заданных над троичными полями Галуа.

В работе рассматриваются полиномы нескольких переменных, заданные над произвольными полями Галуа нечетной мощности. Для таких полиномов получены результаты, связанные с вычислением производных по направлению, а также с восстановлением полинома по набору его производных, вычисленных в базисных направлениях. Для полученных результатов предложены два возможных практических приложения: схема разделения данных и декодер кодов Рида-Маллера (РМ-коды).

Предложенная схема разделения данных может быть использована для организации разделенной передачи конфиденциальных данных, т.е. такой системы связи, в которой исходные данные на стороне отправителя разделяются на несколько частей и, независимо друг от друга, передаются по различным каналам связи, а на стороне получателя из принятых частей восстанавливаются исходные данные. Особенностью предлагаемой схемы является то, что она позволяет защищать данные, как от нелегитимного доступа, так и от непреднамеренных ошибок. При этом в обоих случаях используется один и тот же математический аппарат, связанный с РМ-кодами и дифференцированием полиномов. Разделенная передача может быть использована как для повышения скорости связи, так и для обеспечения конфиденциальности данных за счет усложнения задачи перехвата из нескольких линий связи. Некоторые вопросы разделения данных рассмотрены в работах [7–11].

Для РМ-кодов второго порядка детерминированные декодеры известны только для некоторых значений мощности q полей Галуа. Например, довольно много известно декодеров для случая $q = 2$, например [12–13], для случая $q = 3$ и использования полунепрерывного канала связи сконструирован декодер [5]. В [14] предложен декодер кодов Рида-Маллера второго порядка, заданных над полями Галуа мощности 2, 4 и 8. Предлагаемый в данной работе декодер РМ-кодов второго порядка, заданных над произвольным нечетным полем Галуа, основан на редукции к кодам Рида-Маллера первого порядка, кодовые слова которых можно декодировать любым подходящим декодером. В случае РМ-кодов, заданных над полями мощности больше 3, предлагаемый декодер имеет некоторое ограничение по количеству исправляемых ошибок. Следует отметить, что использование предлагаемой схемы декодирования в случае полей мощности больше трех, несмотря на имеющееся ограничение, может быть целесообразным при невысоком уровне зашумления используемых каналов связи.

Дифференцирование полиномов нескольких переменных. Пусть $q = p^s$, p — простое нечетное число, $s \in \mathrm{N}$, F_q — поле Галуа мощности q. Рассмотрим кольцо полиномов от m переменных $\mathrm{F}_q[x_1,...,x_m]$ над

полем F_q. Линейное пространство полиномов из $\mathrm{F}_q[x_1,...,x_m]$ степени не выше r обозначим $\mathrm{F}_q^{(r)}[x_1,...,x_m]$. Пусть F_q^m — m-мерное линейное пространство над F_q.

Производной полинома $f \in \mathrm{F}_q^{(r)}[x_1,...,x_m]$ по направлению $\bar{b} \in \mathrm{F}_q^m$ называется результат действия оператора дифференцирования [3]:

$$(D_{\bar{b}} f)(\bar{x}) = f_{\bar{b}}(\bar{x}) - f(\bar{x}), \quad \bar{x} \in \mathrm{F}_q^m, \tag{1}$$

где $f_{\bar{b}}(\bar{x}) = f(\bar{x} + \bar{b})$. Легко показать, что $D_{\bar{b}} f \in \mathrm{F}_q^{(r-1)}[x_1,...,x_m]$, а оператор

$$D_{\bar{b}} f : \mathrm{F}_q^{(r)}[x_1,...,x_m] \to \mathrm{F}_q^{(r-1)}[x_1,...,x_m] \tag{2}$$

является линейным.

Сумму координат вектора $\bar{\alpha} \in \mathrm{F}_p^m$, где p — простое, как натуральных чисел обозначим $\rho(\bar{\alpha})$. Полиномы $f \in \mathrm{F}_q^{(2)}[x_1,...,x_m]$ будем записывать в каноническом виде

$$f(\bar{x}) = \sum_{\bar{\alpha} \in \mathrm{F}_q^m} f_{\bar{\alpha}} \bar{x}^{\bar{\alpha}} = a_{\bar{0}} \bar{x}^{\bar{0}} + \sum_{\rho(\bar{\alpha})=1} a_{\bar{\alpha}} \bar{x}^{\bar{\alpha}} + \sum_{\rho(\bar{\alpha})=2} a_{\bar{\alpha}} \bar{x}^{\bar{\alpha}}, \tag{3}$$

где при записи монома $\bar{x}^{\bar{\alpha}} = x_1^{\alpha_1} ... x_m^{\alpha_m}$ показатели α_i будем отождествлять с элементами поля F_p, а слагаемые в каждой сумме будем располагать в лексикографическом порядке по возрастанию. Если последняя сумма в (3) равна нулю, то получаем полином из $\mathrm{F}_q^{(1)}[x_1,...,x_m]$.

Лемма 1. Пусть $q = p^s$, p — простое нечетное число, $f(\bar{x}) \in \mathrm{F}_q^{(2)}[x_1,...,x_m]$ — полином в каноническом виде (3), $\bar{b} = (b_1,...,b_m) \in \mathrm{F}_q^m$. Тогда

$$f(\bar{x}) = f_{00...00} + \bar{x}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + \bar{x} A \bar{x}^T, \tag{4}$$

$$(D_{\bar{b}} f)(\bar{x}) = \bar{b}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + 2\bar{x} A \bar{b}^T + \bar{b} A \bar{b}^T = 2\bar{x} A \bar{b}^T + f(\bar{b}) - f_{00...00}, \tag{5}$$

где

$$A = \begin{pmatrix} f_{200..00} & f_{110..00}/2 & f_{101..00}/2 & \dots & f_{100..10}/2 & f_{100..01}/2 \\ f_{110..00}/2 & f_{020..00} & f_{011..00}/2 & \dots & f_{010..10}/2 & f_{010..01}/2 \\ f_{101..00}/2 & f_{011..00}/2 & f_{002..00} & \dots & f_{001..10}/2 & f_{001..01}/2 \\ \dots & \dots & \dots & \ddots & \dots & \dots \\ f_{100..10}/2 & f_{010..10}/2 & f_{001..10}/2 & \dots & f_{000..20} & f_{000..11}/2 \\ f_{100..01}/2 & f_{010..01}/2 & f_{001..01}/2 & \dots & f_{000..11}/2 & f_{000..02} \end{pmatrix},$$

Доказательство. В случае простого поля Галуа доказательство содержится в [1]. Используя (1), (4) и симметричность матрицы A получаем:

$$f_{\bar{b}}(\bar{x}) = f(\bar{x} + \bar{b}) = f_{00...00} + (\bar{x} + \bar{b})\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + (\bar{x} + \bar{b}) A (\bar{x} + \bar{b})^T,$$

$$(D_{\bar{b}} f)(\bar{x}) = f_{\bar{b}}(\bar{x}) - f(\bar{x}) = \bar{b}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + \bar{x} A \bar{b}^T + \bar{b} A \bar{x}^T + \bar{b} A \bar{b}^T,$$

$$(D_{\bar{b}} f)(\bar{x}) = \bar{b}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + 2\bar{x} A \bar{b}^T + \bar{b} A \bar{b}^T = 2\bar{x} A \bar{b}^T + f(\bar{b}) - f_{00...00}. \bullet$$

Докажем теорему, которая определяет способ восстановления с точностью до постоянного слагаемого полинома из $\mathrm{F}_q^{(2)}[x_1, x_2, ..., x_m]$ по набору его производных, вычисленных в базисных направлениях.

Теорема 1. Пусть $\beta = \{\bar{b}_i = (b_1^i, b_2^i, ..., b_m^i)\}_{i=1,...,m}$ — некоторый базис пространства F_q^m, где q — нечетное. Рассмотрим полином $f \in \mathrm{F}_q^{(2)}[x_1, x_2, ..., x_m]$ вида (4):

$$f(\bar{x}) = f_{00...00} + \bar{x}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + \bar{x} A \bar{x}^T.$$

Если

$$\left\{\left(D_{\bar{b}_i} f\right)(\bar{x}) = \alpha_1^i x_1 + \alpha_2^i x_2 + ... + \alpha_m^i x_m + \alpha_0^i\right\}_{i=1,...,m}, \tag{6}$$

то

$$A = \frac{1}{2} \begin{pmatrix} \alpha_1^1 & \alpha_1^2 & \dots & \alpha_1^m \\ \alpha_2^1 & \alpha_2^2 & \dots & \alpha_2^m \\ \vdots & \dots & \ddots & \vdots \\ \alpha_m^1 & \alpha_m^2 & \dots & \alpha_m^m \end{pmatrix} \begin{pmatrix} b_1^1 & b_1^2 & \dots & b_1^m \\ b_2^1 & b_2^2 & \dots & b_2^m \\ \vdots & \dots & \ddots & \vdots \\ b_m^1 & b_m^2 & \dots & b_m^m \end{pmatrix}^{-1}, \tag{7}$$

$$\begin{pmatrix} f_{10...00} \\ f_{01...00} \\ \vdots \\ f_{00...01} \end{pmatrix} = \begin{pmatrix} \alpha_0^1 - \bar{b}_1 A \bar{b}_1^T \\ \alpha_0^2 - \bar{b}_2 A \bar{b}_2^T \\ \vdots \\ \alpha_0^m - \bar{b}_m A \bar{b}_m^T \end{pmatrix} \begin{pmatrix} b_1^1 & b_2^1 & \cdots & b_m^1 \\ b_1^2 & b_2^2 & \cdots & b_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ b_1^m & b_2^m & \cdots & b_m^m \end{pmatrix}^{-1}. \quad (8)$$

Доказательство. Из (5), (6) получаем:

$$\forall\ i = 1, ..., m:\ 2A\bar{b}_i^T = (\alpha_1^i, \alpha_2^i, ..., \alpha_m^i)^T,\ f(\bar{b}_i) - f_{00..00} = \alpha_0^i. \quad (9)$$

Тогда

$$2A \begin{pmatrix} b_1^1 & b_1^2 & \cdots & b_1^m \\ b_2^1 & b_2^2 & \cdots & b_2^m \\ \vdots & \vdots & \ddots & \vdots \\ b_m^1 & b_m^2 & \cdots & b_m^m \end{pmatrix} = \begin{pmatrix} \alpha_1^1 & \alpha_1^2 & \ldots & \alpha_1^m \\ \alpha_2^1 & \alpha_2^2 & \ldots & \alpha_2^m \\ \vdots & \ldots & \ddots & \vdots \\ \alpha_m^1 & \alpha_m^2 & \cdots & \alpha_m^m \end{pmatrix}.$$

Следовательно, формула (7) верна.

Из (4) следует, что для любого $\bar{b} \in \mathrm{F}_q^m$:

$$f(\bar{b}) - f_{00..00} = \bar{b}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + \bar{b}A\bar{b}^T.$$

Возьмем в качестве $\bar{b}$ векторы $\bar{b}_i \in \beta$ и воспользуемся равенством $f(\bar{b}_i) - f_{00..00} = \alpha_0^i$ из (9). Тогда

$$\forall\ i = 1, ..., m:\ \alpha_0^i - \bar{b}_i A \bar{b}_i^T = \bar{b}_i \left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T.$$

Следовательно,

$$\begin{pmatrix} \alpha_0^1 - \bar{b}_1 A \bar{b}_1^T \\ \alpha_0^2 - \bar{b}_2 A \bar{b}_2^T \\ \vdots \\ \alpha_0^m - \bar{b}_m A \bar{b}_m^T \end{pmatrix} = \begin{pmatrix} b_1^1 & b_2^1 & \cdots & b_m^1 \\ b_1^2 & b_2^2 & \cdots & b_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ b_1^m & b_2^m & \cdots & b_m^m \end{pmatrix} \begin{pmatrix} f_{10...00} \\ f_{01...00} \\ \vdots \\ f_{00...01} \end{pmatrix}$$

и формула (8) доказана. •

q-ичные коды Рида-Маллера *$RM_q(r,m)$*. Рассмотрим РМ-коды над конечным полем F_q где $q = p^s$, p — простое нечетное число, $s \in \mathrm{N}$ [15–16]. Элементы $\mathrm{F}_q^{(r)}[x_1, ..., x_m]$ являются информационными полиномами кода $RM_q(r,m)$; будем полагать, что $m \geq r > 0$, $m \geq 2$. Вектор $\bar{f}$, составленный из коэффициентов информационного полинома $f(x_1, ..., x_m)$, называется информационным вектором.

В векторном пространстве F_q^m зафиксируем некоторое упорядочение

$$\{\bar{\alpha}_1, ..., \bar{\alpha}_n\}\ (\bar{\alpha}_j = (\alpha_{j1}, \alpha_{j2}, ..., \alpha_{jm})), \qquad n = q^m. \quad (10)$$

Произвольный информационный полином $f(\bar{x}) \in \mathrm{F}_q^{(r)}[x_1, ..., x_m]$ кодируется путем вычисления его значений в точках упорядоченного пространства F_q^m:

$$C(f) = (f(\bar{\alpha}_1), ..., f(\bar{\alpha}_n)), \quad (11)$$

и тем самым определяется оператор кодирования

$$C:\ \mathrm{F}_q^{(r)}[x_1, ..., x_m] \to \mathrm{F}_q^n.$$

Коды Рида-Маллера определяются натуральными параметрами r и m (r<m)

$$RM_q(r,m) = \{(f(\bar{\alpha}_1), ..., f(\bar{\alpha}_n)) \mid f(\bar{x}) \in \mathrm{F}_q[x_1, ..., x_m], \deg(f) \leq r\} \subset \mathrm{F}_q^n,$$

параметр r называется порядком кода. Они образуют семейство линейных $[n,k,d]q$-кодов, длина n и размерность k которых определяются по формулам

$$n = q^m,\ \ k = \sum_{i=0}^{r} \sum_{j=0}^{\lfloor i/q \rfloor} (-1)^j C_m^j C_{i-qj+m-1}^{m-1},$$

где $\lfloor\ \rfloor$ — округление до меньшего целого, а минимальное кодовое расстояние d кода $RM_q(r,m)$ удобно вычислять, используя параметры дуального кода $RM_q(r^\perp, m)$, где $r^\perp = m(q-1) - r - 1$. Пусть ρ — остаток от деления $r^\perp + 1$ на $q-1$: $r^\perp + 1 = \sigma(q-1) + \rho$, где $\rho < q-1$, тогда параметр d кода $RM_q(r,m)$ задается выражением

$$d = (\rho + 1)q^{\sigma}. \tag{12}$$

Отметим, что произвольный $[n,k,d]_q$-код позволяет исправить $t = \lfloor (d-1)/2 \rfloor$ ошибок в одном кодовом слове [17].

Далее будем рассматривать РМ-коды порядков 1 и 2, заданные над полями Галуа нечетной мощности, соответствующие им информационные полиномы записывать в виде (3), а для нумерации координат информационного вектора использовать упорядочение (10).

Лемма 2. Пусть $r \in \{1;2\}$, $q \geq 3$, тогда минимальное кодовое расстояние кода $RM_q(r,m)$ вычисляется по формуле:

$$d_r = (q-r)q^{m-1}, \tag{13}$$

а значения гарантировано исправляемых ошибок $t_r = \lfloor (d-1)/2 \rfloor$ кодами $RM_q(r,m)$, $r \in \{1;2\}$, связаны следующим образом:

$$t_1/2 \leq t_2. \tag{14}$$

Доказательство. Воспользуемся тем, что $r < q$, и вычислим σ и ρ — неполное частное и остаток от деления $r^{\perp}+1$ на $q-1$ соответственно:

$$\sigma = (m(q-1)-r)\operatorname{div}(q-1) = m-1;$$

$$\rho = (m(q-1)-r)\bmod(q-1) = q-1-r.$$

Тогда из формулы (12) получаем (13). Из равенств $d_1 = (q-1)q^{m-1}$, $d_2 = (q-2)q^{m-1}$ получаем, что искомое неравенство (14) имеет вид

$$\frac{1}{2}\cdot\left\lfloor \frac{(q-1)q^{m-1}-1}{2} \right\rfloor \leq \left\lfloor \frac{(q-2)q^{m-1}-1}{2} \right\rfloor.$$

Отметим, что d_2 — нечетное, а d_1 — четное, поэтому

$$\left\lfloor \frac{(q-2)q^{m-1}-1}{2} \right\rfloor = \frac{(q-2)q^{m-1}-1}{2},$$

$$\left\lfloor \frac{(q-1)q^{m-1}-1}{2} \right\rfloor = \frac{(q-1)q^{m-1}-2}{2},$$

Следовательно, неравенство (14) приобретает вид

$$\frac{1}{2}\left(\frac{(q-1)q^{m-1}-2}{2}\right) \leq \frac{(q-2)q^{m-1}-1}{2},$$

легко видеть, что оно эквивалентно неравенству $q \geq 3$. •

Следствие. Если q>3, то в (14) — строгое неравенство, то q=3, то в (14) — равенство.

В таблице 1 приведены параметры некоторых РМ-кодов. В трех верхних строках указаны такие параметры рассматриваемого кода $RM_q(r,m)$ как q, m, n. В следующих трех строках для кодов $RM_q(1,m)$ содержатся значения: k_1 — размерность кода, d_1 — минимальное кодовое расстояние и t_1 — число исправляемых ошибок. В следующих трех строках представлены аналогичные значения k_2, d_2, t_2 для кодов $RM_q(2,m)$.

Таблица 1

Значения параметров некоторых РМ-кодов

q		3				5				7			
m		2	3	5	7	2	3	5	7	2	3	4	5
n		9	27	243	2187	25	125	3125	78125	49	343	2401	16807
r=1	k_1	3	4	6	8	3	4	6	8	3	4	5	6
	d_1	6	18	162	1458	20	100	2500	62500	42	294	2058	14406
	t_1	2	8	80	728	9	49	1249	31249	20	146	1028	7202
r=2	k_2	6	10	21	36	6	10	21	36	6	10	15	21
	d_2	3	9	81	729	15	75	1875	46875	35	245	1725	12005
	t_2	1	4	40	364	7	37	937	23437	17	122	857	6002

Теперь введем аналог оператора дифференцирования $D_{\bar{b}}$, действующего в пространстве полиномов (2), для пространства F_q^n, где $n = q^m$. Координаты векторов из F_q^n будем нумеровать векторами из упорядоченного множества F_q^m (см.(10)). Рассмотрим оператор сдвига $\tau_{\bar{b}} : \mathrm{F}_q^n \to \mathrm{F}_q^n$, действующий по формуле

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

где $\bar{a} = (a_{\bar{\alpha}_1}, ..., a_{\bar{\alpha}_n}) \in \mathrm{F}_q^n$, $\bar{b} = (b_1, ..., b_m) \in \mathrm{F}_q^m$. Отметим, что оператор сдвига $\tau_{\bar{b}}$ является перемешивающим биективным отображением. Линейный оператор $\Delta_{\bar{b}} : \mathrm{F}_q^n \to \mathrm{F}_q^n$, являющийся аналогом $D_{\bar{b}}$, определим формулой:

$$\Delta_{\bar{b}}(\bar{a}) = \tau_{\bar{b}}(\bar{a}) - \bar{a},\ \bar{a} = (a_{\bar{\alpha}_1}, ..., a_{\bar{\alpha}_n}) \in \mathrm{F}_q^n. \quad (15)$$

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

Лемма 3. Рассмотрим полином $f \in \mathrm{F}_q^{(2)}[x_1, x_2, ..., x_m]$, вектор $\bar{b} = (b_1, ..., b_m) \in \mathrm{F}_q^m$, операторы $\Delta_{\bar{b}}$, $D_{\bar{b}}$ и C. Тогда

$$\tau_{\bar{b}}(C(f)) = C(f_{\bar{b}}),\ C(D_{\bar{b}} f) = \Delta_{\bar{b}}(C(f)). \quad (16)$$

Доказательство проводится прямыми выкладками и для $q = 3$ имеется в [6].•

Отметим, что из (2) и (16) вытекает, что если $C(w) \in RM_q(2, m)$, то $\Delta_{\bar{b}}(C(w)) \in RM_q(1, m)$.

Ниже рассмотрим примеры практических приложений полученных теоретических результатов.

Схема разделения данных. Для разделения и восстановления данных в предлагаемой схеме используем $[n, k_1, d_1]_q$-код $RM_q(1, m)$ и $[n, k_2, d_2]_q$-код $RM_q(2, m)$, заданные над произвольным полем Галуа F_q нечетной мощности. Значения q и m являются параметрами этой схемы.

Алгоритм разделения данных

Вход: информационный вектор $\bar{w} \in \mathrm{F}_q^{k_2}$ кода $RM_q(2, m)$ и упорядоченный набор базисных векторов

$$\beta = \{\bar{b}_i = (b_1^i, b_2^i, ..., b_m^i) \in \mathrm{F}_q^m\}_{i=1,...,m}, \quad (17)$$

который является секретным ключом рассматриваемой схемы.

Выход: векторы $\bar{S}_i \in \mathrm{F}_q^{n+1}$, $i = \overline{1, m}$.

Шаг 1. Сопоставим входному вектору $\bar{w}$ информационный полином $w = w(\bar{x})$ и закодируем его с использованием (11) в вектор $C(w) \in \mathrm{F}_q^n$ кода $RM_q(2, m)$.

Шаг 2. Сформируем m производных векторов (см. (15)):

$$\Delta_{\bar{b}_i}(C(w)) = C(D_{\bar{b}_i}(w)) \in \mathrm{F}_q^n,\ i = \overline{1, m},\ \bar{b}_i \in \beta.$$

Отметим, что $C(D_{\bar{b}_i}(w)) \in RM_q(1, m)$.

Шаг 3. Каждый вектор $C(D_{\bar{b}_i}(w)) \in \mathrm{F}_q^n$, $i = \overline{1, m}$ конкатенируем с коэффициентом $f_{00..00} := w(\bar{0})$ кодового вектора $C(w)$:

$$\bar{S}_i = C(D_{\bar{b}_i}(w)) \,||\, f_{00..00} \in \mathrm{F}_q^{n+1}.$$

Далее векторы $\overline{S}_i \in \mathrm{F}_q^{n+1}$, $i = \overline{1,m}$, передаются по m различным линиям связи. Очевидно, что во время передачи векторы $\overline{S}_i$, $i = \overline{1,m}$, могут быть искажены. Таким образом, из канала связи будут получены векторы $\overline{S}_i'$:

$$\overline{S}_i' = (C(D_{\overline{b}_i}(w)))' \| f'_{00..00} \in \mathrm{F}_p^{n+1},\ i = \overline{1,m}.$$

где $(C(D_{\overline{b}_i}(w)))'$ — возможно искаженный вектор $C(D_{\overline{b}_i}(w))$, а скаляр $f'_{00..00}$ — возможно искаженное значение $f_{00..00}$. Скаляр $f'_{00..00}$ соответствующий $\overline{S}_i'$ обозначим $f'_{00..00,i}$.

Алгоритм восстановления данных

Вход: векторы $\overline{S}_i'$, $i = \overline{1,m}$ и секретный ключ β (см. (17)).

Выход: вектор $\overline{w}' \in \mathrm{F}_q^{k_2}$.

Шаг 1. Из каждого вектора $\overline{S}_i'$, $i = \overline{1,m}$, выделяем две компоненты: $(C(D_{\overline{b}_i}(w)))' \in \mathrm{F}_q^n$ и $f'_{00..00,i}$, $i = \overline{1,m}$.

Шаг 2. Векторы $(C(D_{\overline{b}_i}(w)))'$ направляем в декодеры кода $RM_q(1,m)$. Отметим, что декодеры могут быть использованы произвольные, например, [16], [18]. На выходе рассматриваемых декодеров формируются полиномы $D'_{\overline{b}_i}(w) \subset \mathrm{F}_q^{(1)}[x_1, x_2, ..., x_m]$, $i = 1, ..., m$.

Шаг 3. Из коэффициентов $f'_{00..00,i}$ формируем вектор $(f'_{00..00,1}, f'_{00..00,2}, ..., f'_{00..00,m})$ и подаем на вход декодера кода $RM_q(0,m)$, фактически совпадающего с кодом m-кратного повторения. Результатом работы этого декодера является скаляр $f''_{00..00}$.

Шаг 4. Значения коэффициентов полиномов $D'_{\overline{b}_i}(w) \subset \mathrm{F}_q^{(1)}[x_1, x_2, ..., x_m]$, $i = \overline{1,m}$, и ключ β (см. (17)) подставляем в формулы (7) и (8) и из полученных результатов строим полином $f(\overline{x})$. Затем вычисляем искомый полином $w'(\overline{x}) = f(\overline{x}) + f''_{00..00}$.

Шаг 5. Получателю сообщений выдаем информационный вектор $\overline{w}' \in \mathrm{F}_q^k$, соответствующий полиному $w'(\overline{x})$.

Замечание 1. Корректность алгоритма восстановления данных зависит от числа ошибок, повредивших векторы $\overline{S}_i \in \mathrm{F}_q^{n+1}$ во время их передачи по линиям связи, а также от корректирующей способности используемых РМ-кодов первого порядка. Очевидно, что если используемые декодеры корректно восстановят векторы $C(D_{\overline{b}_i}(w))$ и значение $f_{00..00}$, то и восстановление исходных данных с использованием результатов теоремы 1 будет корректным, и, следовательно, вектор $w'(\overline{x})$, полученный на выходе алгоритма восстановления данных, совпадает с исходным информационным вектором $\overline{w} \in \mathrm{F}_q^{k_2}$. Отметим, что работа декодеров по восстановлению $C(D_{\overline{b}_i}(w))$ корректна, если

$$\forall i = \overline{1,m}:\ d_h(C(D_{\overline{b}_i}(w)), (C(D_{\overline{b}_i}(w)))') \le \lfloor (d_1 - 1)/2 \rfloor,$$

где $d_h(\overline{x}, \overline{y})$ — расстояние Хемминга между векторами $\overline{x}, \overline{y}$. Скаляр $f_{00..00}$ восстанавливается корректно, если вектор $(f'_{00..00,1}, f'_{00..00,2}, ..., f'_{00..00,m})$, сформированный на шаге 3 алгоритма, содержит менее m/2 координат, отличных от значения $f_{00..00} = w(\overline{0})$. Если в $\overline{S}_i \in \mathrm{F}_q^{n+1}$, $i = \overline{1,m}$, произошло ошибок больше, чем могут исправить используемые декодеры, то восстановление $\overline{w} \in \mathrm{F}_q^{k_2}$ не гарантируется.

Замечание 2. В предложенных алгоритмах разбиения и восстановления используются коды Рида-Маллера как первого, так и второго порядков, однако декодеры применяются только для кодов первого порядка.

Замечание 3. Конфиденциальность передаваемых данных обеспечивается не только необходимостью знания ключа, но и за счет использования нескольких линий связи, т.к. в этом случае перехват данных является более затруднительным для злоумышленника, чем нелегитимное получение данных из одной линии связи.

Декодер кодов Рида-Маллера второго порядка. Сначала рассмотрим идею организации алгоритма декодирования, а затем опишем алгоритм по шагам.

Зафиксируем некоторый базис $\beta = \{\overline{b}_i = (b_1^i, b_2^i, ..., b_m^i) \in \mathrm{F}_q^m\}_{i=1,...,m}$ в пространстве F_q^m, где $q = p^s$, p — простое нечетное число. Предположим, что на вход декодера поступает $\overline{Y} = C(w) + \overline{e}\ (\in \mathrm{F}_q^n)$, где w — информационный полином, $C(w)$ — кодовый вектор $[n, k_2, d_2]_q$-кода $RM_q(2,m)$, $\overline{e} \in F_q^n$ — вектор ошибок, для которого

$$wt_h(\bar{e}) \le t_2, \tag{18}$$

где $wt_h(.)$ — вес Хемминга, $t_2 = \lfloor (d_2 - 1)/2 \rfloor$. По вектору $\bar{Y}$ с помощью оператора $\Delta_{\bar{b}}$ построим m производных векторов, вычисленных в базисных направлениях:

$$\Delta_{\bar{b}_i}(\bar{Y}) = \Delta_{\bar{b}_i}(C(w) + \bar{e}) = \Delta_{\bar{b}_i}(C(w)) + \Delta_{\bar{b}_i}(\bar{e}),\ i = 1,...,m$$

каждый из которых представляет собой вектор $\Delta_{\bar{b}_i}(C(w)) \in RM_q(1,m)$, искаженный вектором ошибок $\Delta_{\bar{b}_i}(\bar{e}) \in \mathrm{F}_q^n$, и может быть безошибочно декодирован произвольным декодером $[n, k_1, d_1]_q$-кода $RM_q(1,m)$, работающим до половины кодового расстояния (см., напр., [16], [18]), в случае, если число ошибок не превосходит $t_1 = \lfloor (d_1 - 1)/2 \rfloor$, т.е. когда

$$wt_h(\Delta_{\bar{b}_i}(\bar{e})) \le t_1. \tag{19}$$

Если векторы $\Delta_{\bar{b}_i}(\bar{Y})$ декодируются правильно, то искомый информационный полином w кода $RM_q(2,m)$ может быть восстановлен с использованием теоремы 1 с точностью до одной координаты, которая затем может быть найдена, например, декодированием по максимуму правдоподобия. Таким образом, для правильного декодирования $\bar{Y}$ по предложенной схеме требуется выполнение условия (19).

Алгоритм декодирования кода $RM_q(2,m)$

Вход: параметры $[n, k_2, d_2]_q$-кода $RM_q(2,m)$, $\bar{Y} = (Y_{\alpha_1}, Y_{\alpha_2}, ...Y_{\alpha_n}) \in \mathrm{F}_q^n$.

Выход: восстановленный информационный вектор $\bar{w}$.

Шаг 1. Зафиксируем некоторый базис $\beta = \{\bar{b}_i = (b_1^i, b_2^i, ..., b_m^i) \in \mathrm{F_q^m}\}_{i=1,...,m}$ пространства $\mathrm{F_q^m}$ и вычислим производные векторы по всем направлениям $\bar{b}_i \in \beta$:

$$\Delta_{\bar{b}_i}(\bar{Y}) = \tau_{\bar{b}_i}(\bar{Y}) - \bar{Y}.$$

Шаг 2. Декодируем $\Delta_{\bar{b}_i}(\bar{Y})$, $i = 1,...,m$, используя произвольный декодер $RM_q(1,m)$-кодов, работающий до половины кодового расстояния, и в результате получаем векторы $\bar{p}_{\bar{b}_i}$ и их полиномиальные представления

$$p_{\bar{b}_i}(\bar{x}) = \alpha_1^i x_1 + \alpha_2^i x_2 + ... + \alpha_m^i x_m + \alpha_0^i \subset \mathrm{F}_p^{(1)}[x_1, x_2, ..., x_m],\ i = 1,...,m.$$

Шаг 3. Используя полиномы $p_{\bar{b}_i}(\bar{x})$, $i = 1,...,m$, по формулам (7) и (8) найдем полином $f(\bar{x})$ с нулевым свободным членом.

Шаг 4. Для всех $z \in \mathrm{F}_q$ вычислим

$$\Psi(z) = \sum_{i=1}^{n} \left| C(f(\bar{x}) + z)_{\alpha_i} - Y_{\alpha_i} \right|,$$

где $C(f(\bar{x}) + z)_{\alpha_i}$ — α_i-тая координата вектора $C(f(\bar{x}) + z)$ (см. (11)). Обозначим z_0 значение z на котором функция $\Psi(z)$ достигла своего минимума.

Шаг 5. Результатом декодирования является вектор $\bar{w}$ взаимно однозначно соответствующий информационному полиному $w(\bar{x}) = f(\bar{x}) + z_0$.•

Теорема 2. Для того, чтобы построенный алгоритм декодирования кода $RM_q(2,m)$ исправил все ошибки в $\bar{Y} = C(w) + \bar{e}$ достаточно, чтобы выполнялись условия (18) и

$$wt_h(\bar{e}) \le t_1/2, \tag{20}$$

где $t_1 = \lfloor (d_1 - 1)/2 \rfloor$, d_1 — минимальное кодовое расстояние кода $RM_q(1,m)$.

Доказательство. На шаге 2 на вход декодера поступают векторы

$$\Delta_{\bar{b}_i}(\bar{Y}) = \tau_{\bar{b}_i}(\bar{Y}) - \bar{Y} = \tau_{\bar{b}_i}(C(\bar{w})) + \tau_{\bar{b}_i}(\bar{e}) - C(\bar{w}) - \bar{e} = \Delta_{\bar{b}_i}(C(w)) + \Delta_{\bar{b}_i}(e).$$

Напомним, что $\Delta_{\bar{b}_i}(C(w)) \in RM_q(1,m)$, а декодеры кода $RM_q(1,m)$, работающие до половины кодового расстояния, исправляют до t_1 ошибок в кодовом слове. Из условия (20) вытекает, что

$$wt_h(\Delta_{\bar{b}_i}(\bar{e})) \le wt_h(\tau_{\bar{b}_i}(\bar{e})) + wt_h(\bar{e}) = 2wt_h(\bar{e}) \le t_1$$

Следовательно, векторы $\bar{p}_{\bar{b}_i}$, которые формируются на шаге 2, совпадают с $\Delta_{\bar{b}_i}(C(w))$. Из этого вытекает, что на шаге 3, в силу теоремы 1, формируется полином $f(\bar{x}) = w(\bar{x}) - w(\bar{0})$.

Из условия (18) вытекает, что вычисленная на шаге 4 величина z_0 равна свободному члену $w(\bar{0})$ искомого информационного полинома $w(\bar{x})$. Таким образом, на шаге 5 алгоритма получается искомый информационный вектор $\bar{w}$. •

Отметим, что для правильного декодирования по предложенной схеме требуется выполнение условия (20), из которого вытекает (19), хотя более естественным является условие (18). Рассмотрим связь между этими условиями.

Лемма 4. Для кодов $RM_q(2,m)$ в случае $q=3$ условия (18) и (20) равносильны, а в случае $q>3$ при выполнении условия (18) выполнение условия (20) не гарантируется.

Доказательство. Из следствия леммы 2 получаем, что при $q=3$ справедливо равенство $t_1/2=t_2$, т.е. правые части неравенств (18) и (20) совпадают, следовательно, из выполнения одного из них вытекает выполнение другого. При $q>3$ из следствия леммы 2 получаем, что $t_1/2<t_2$, т.е. из выполнения (18) не вытекает выполнение (20). •

Замечание 1. В [5–6] описан декодер $RM_3(2,m)$-кода, где, как и в предложенном алгоритме, для зашумленного кодового слова строятся производные векторы, которые декодируются по алгоритму максимального правдоподобия, а затем по полученным значениям восстанавливается искомое информационное слово. Однако, в декодере из [5–6] строятся производные векторы во всех 3^m возможных направлениях, а не только базисных, и используется иной механизм построения искомого информационного вектора.

Замечание 2. Для кодов $RM_q(2,m)$, $q=3$, предлагаемый декодер работает до половины кодового расстояния. Для кодов $RM_q(2,m)$, $q>3$, предлагаемый декодер не гарантирует исправление всех ошибок, число которых не превосходит t_2, но декодер будет работать корректно при соблюдении более слабого условия (20). Отметим, что использование предлагаемой схемы декодирования в случае полей мощности больше трех, несмотря на указанное ограничение, может быть целесообразно по следующим причинам. Во-первых, теория декодеров РМ-кодов второго порядка проработана недостаточно, но, если имеется декодер первого порядка, то предлагаемый декодер, являющийся надстройкой над ним, восполняет этот пробел. Во-вторых, при использовании каналов связи, вероятность ошибок в которых такова, что (20) выполняется, переход от РМ-кодов первого порядка к кодам второго порядка уменьшает избыточность (см. таблицу 1).

Заключение. Получены теоретические результаты, связанные с восстановлением полиномов нескольких переменных над полями Галуа нечетной мощности по их производным. В качестве практических приложений полученных результатов предложены схема разделения данных и декодер РМ-кодов второго порядка. В дальнейшем представляется полезным исследовать процесс восстановления полинома по искаженным производным и разработать соответствующие модификации предложенных в настоящей работе практических приложений.

Библиографический список

1. Деундяк, В. М. Интегрируемость систем полиномов нескольких переменных первой и второй степени над простыми полями Галуа / В. М. Деундяк, А. В. Кнутова // Известия вузов. Сев.-Кавк. регион. Естественные науки. — 2016. — №2. — С. 41–46.

2. Абросимов, А. С. Свойства бент-функций q-значной логики над конечными полями / А. С. Абросимов // Дискретная математика. — 1994. — № 3(6). — С. 50–60.

3. Логачев, О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. — Москва: МЦНМО, 2004. — 470 с.

4. Мазуренко, А. Способ восстановления булевой функции нескольких переменных по ее производной / А. Мазуренко, Н. С. Могилевская // Вестник Донского гос. техн. ун-та. — 2017. — № 1 (88). — С. 122–131.

5. Деундяк, В. М. Модель троичного канала передачи данных с использованием декодера мягких решений кодов Рида-Маллера второго порядка / В. М. Деундяк, Н. С. Могилевская // Известия вузов. Сев.-Кавк. регион. Технические науки. — 2015. — № 1 (182). — С. 3–10.

6. Деундяк, В. М. Об условиях корректности декодера мягких решений троичных кодов Рида-Маллера второго порядка / В. М. Деундяк, Н. С. Могилевская // Владикавказский математический журнал. — 2016, — Т. 18. Вып. 4. — С. 23–33.

7. Могилевская, Н. С. Пороговое разделение файлов на основе битовых масок: идея и возможное применение / Н. С. Могилевская, Р. В. Кульбикаян, Л. А. Журавлев / Вестник Дон. гос. техн. ун-та. — 2011. — Т.11. № 10. — С. 1749–1755.

8. Тормасов, А. Г. Обеспечение отказоустойчивости в распределенных средах / А. Г. Тормасов, М. А. Хасин, Ю. И. Пахомов // Программирование. — 2001. — Т.27, № 5. — С. 26.

9. Мищенко, В. А. Ущербные тексты и многоканальная криптография / В. А. Мищенко, Ю. В. Виланский. — Минск: Энциклопедикс, 2007. — 292 с.

10. Деундяк, В. М. Модель организации защищенного документооборота на базе распределенной передачи данных с аутентификацией / В. М. Деундяк, С. Б. Попова // Вестник Дон. гос. техн. ун-та. — 2015. — Т. 15, № 4. — С. 101–106.

11. Могилевская, Н. С. О применении порогового разделения данных для организации разделенной передачи на примере метода битовых масок [электронный ресурс] / Н. С. Могилевская // Инженерный вестник Дона. — 2017. — № 2. — Режим доступа: http://www.ivdon.ru/uploads/article/pdf/IVD_48_Mogilevskaya.pdf_492254b6f1.pdf (дата обращения :12.08.2017).

12. Сидельников, В. М. Декодирование кодов Рида-Маллера при большом числе ошибок / В. М. Сидельников, А. С. Першаков // Проблемы передачи информации. — 1992. — Т.28, №3. — С. 80–94.

13. Карякин, Ю. Д. Быстрое корреляционное декодирование кодов Рида—Маллера / Ю. Д. Карякин // Проблемы передачи информации. — 1987. — Том 23, № 2. — С. 40–49.

14. Paterson K. G., Jones A. E. Efficient decoding algorithms for generalized Reed-Muller codes // IEEE Transactions on Communications. 2000, Vol. 48. Issue 8. Pp. 1272 – 1285.

15. Pellikaan R., Wu X.-W. List decoding of q-ary Reed-Muller Codes // IEEE Trans. On Information Theory. 2004. Vol. 50. Issue 3. P. 679-682.

16. Santhi N. On Algebraic Decoding of q-ary Reed-Muller and Product Reed-Solomon Codes. - ISIT 2007 Conference, June 24 -29, Nice, France, 2007.

17. Деундяк, В. М. Методы помехоустойчивой защиты данных / В. М. Деундяк, А. Э. Маевский, Н. С. Могилевская. — Ростов-на-Дону: ЮФУ, 2014. — 309 с.

18. Ashikhmin A. E., Litsyn *S. N.* Fast Decoding of Non-Binary First Order Reed-Muller Codes // Applicable Algebra in Engineering, Communication and Computing. 1996. Vol. 7. Issue 4. pp. 299–308.

Поступила в редакцию 08.11 .2018
Сдана в редакцию 09.12.2018
Запланирована в номер 21.06.2018

Received 08.11 .2018
Submitted 09.12.2018
Scheduled in the issue 21.06.2018

Об авторах:

Деундяк Владимир Михайлович,
доцент Института математики, механики и компьютерных наук им. И.И. Воровича Южного федерального университета (РФ, 344090, г. Ростов-на-Дону, ул. Мильчакова 8А), старший научный сотрудник Южного регионального аттестационного центра (ЮРАЦ) ФГАНУ НИИ "Спецвузавтоматика"(РФ, 344002, г. Ростов-на-Дону, пер. Газетный, 51), кандидат физ.-мат. наук, доцент,
ORCID: http://orcid.org/0000-0001-8258-2419
vl.deundyak@gmail.com

Могилевская Надежда Сергеевна,
доцент Института математики, механики и компьютерных наук им. И.И. Воровича Южного федерального университета (РФ, 344090,. г. Ростов-на-Дону, ул. Мильчакова, 8-а), кандидат технических наук, доцент,
ORCID: http://orcid.org/0000-0003-1357-5869
nadezhda.mogilevskaia@yandex.ru

Authors:

Deundyak, Vladimir M.,
associate professor of the Algebra and Discrete Mathematics Department, Vorovich Institute for Mathematics, Mechanics, and Computer Science, Southern Federal University, Senior Research Scholar, Southern Regional Certification Centre, Research Institute “Spetsvuzavtomatika” (51, Gazetny per., Rostov-on-Don, 344002, RF), Cand(Phys-Math), associate professor,
ORCID: http://orcid.org/0000-0001-8258-2419
vl.deundyak@gmail.com

Mogilevskaya, Nadezhda S.,
associate professor of Vorovich Institute for Mathematics, Mechanics, and Computer Science, Southern Federal University (8-a, ul. Milchakova, Rostov-on-Don, 344090, RF), Cand(Eng), associate professor,
ORCID: http://orcid.org/0000-0003-1357-5869
nadezhda.mogilevskaia@yandex.ru