МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

DOI 10.17223/20710410/18/3

УДК 512.548.7, 512.554

КВАЗИГРУППЫ И КОЛЬЦА В КОДИРОВАНИИ И ПОСТРОЕНИИ КРИПТОСХЕМ

В. Т. Марков, А. В. Михалёв, А. В. Грибов, П. А. Золотых, С. С. Скаженик

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

E-mail: markov@mech.math.msu.su, alexey.gribov@yandex.ru, pzolotykh@gmail.com

Исследуются различные криптосхемы и коды над ассоциативными и неассоциативными структурами. Построены схема шифрования над градуированным кольцом, криптосхема над лупой Муфанг, протокол выработки общего ключа и линейно оптимальные коды.

Ключевые слова: *неассоциативные алгебраические структуры, градуированное кольцо, квазигрупповое кольцо, лупа Муфанг, коммутаторные квазигруппы, схема шифрования, линейно оптимальный код.*

Введение

В работе в п. 1 представлены необходимые теоретические сведения. В п. 2 построена криптосхема над градуированным кольцом с мультипликативным базисом. Это обобщает построение криптосхемы над групповым кольцом. При этом неоднозначность выбора градуировки и мультипликативного базиса расширяет множество подходящих алгебраических структур для шифрования. Похожая схема была построена в [1]. В п. 3 построен протокол выработки общего секретного ключа и сконструирована криптосхема, где все вычисления проводятся в лупе Муфанг.

В п. 4 с помощью квазигрупповых колец построены две цепочки линейно оптимальных $[n, n-3, 3]_q$-кодов для $n = 2q$ и $n = 2q-2$. Для построения $[2q, 2q-2, 3]_q$-кодов используется представление кодов Рида — Соломона как идеалов группового кольца $\mathbb{F}_{p^n}G$, где G — это p-элементарная абелева группа порядка p^n. В качестве иллюстрации приводятся линейно оптимальные коды, построенные с помощью коммутаторных квазигрупп для группы диэдра D_n.

1. Основные понятия

Приведём основные понятия и утверждения, необходимые для дальнейшего изложения (см., например, [2]).

Определение 1. *Группоид* — непустое множество с заданной бинарной операцией.

Пусть $(G, \cdot)$ — группоид и a — некоторый элемент из G. Рассмотрим отображения $L(a) : G \to G$, $R(a) : G \to G$ для любого $a \in G$. Определим их следующим образом: $xL(a) = x \cdot a$, $xR(a) = a \cdot x$ для любых $x \in G$.

Определение 2. *Квазигруппа* — такой группоид $(G, \cdot)$, что отображения $L(a)$, $R(a)$ являются биекциями для любого $a \in G$.

Это определение эквивалентно следующему: группоид $(G, \cdot)$ называется квазигруппой, если для любых $a, b \in G$ уравнения $x \cdot a = b$, $a \cdot y = b$ всегда разрешимы, причём однозначно.

Определение 3. Группоид $(G, \cdot)$ называется *лупой*, если $(G, \cdot)$ является квазигруппой с единицей. Для любого элемента a лупы $(G, \cdot)$ определим элементы a^λ и a^ρ условиями $a^\lambda \cdot a = 1$ и $a \cdot a^\rho = 1$

Определение 4. Лупа $(L, \cdot)$ с единичным элементом 1 называется *лупой Муфанг*, если выполняется тождество $(xy)(zx) = [x(yz)]x$ для любых $x, y, z \in L$.

Свойства элементов лупы Муфанг описывает

Теорема 1 [3]. Для элементов лупы Муфанг верны следующие тождества:

1) $y^\lambda = y^\rho$, что позволяет обозначить $y^\lambda = y^\rho = y^{-1}$;
2) $(xy)x = x(yx)$;
3) $(xy)(zx) = x[(yz)x]$;
4) $(xy)y^{-1} = x$;
5) $[(yx)z]x = y[x(zx)]$;
6) $[(xz)x]y = x[z(xy)]$;
7) $(xx)y = x(xy)$;
8) $(xy)y = x(yy)$.

Лемма 1 [4]. Пусть $(L, \cdot)$ — лупа Муфанг, тогда для любых $x, y \in L$

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Доказательство. Ясно, что $(xy)^{-1}(xy) = 1$. Тогда $[(xy)^{-1}(xy)]y^{-1} = y^{-1} = ((xy)^{-1})[(xy)y^{-1}] = (xy)^{-1}[x(yy^{-1})] = (xy)^{-1}x$, а следовательно, $(xy)^{-1} = y^{-1}x^{-1}$. ■

Одной из наиболее важных является следующая теорема.

Теорема 2 [3]. Пусть $(L, \cdot)$ — лупа Муфанг. Если для $x, y, z \in L$ выполняется $x(yz) = (xy)z$, то x, y, z порождают подгруппу в L.

Следствие 1. Любая лупа Муфанг $(M, \cdot)$ является ди-ассоциативной, т. е. любые два элемента порождают подгруппу в M.

Следствие 2. Любая лупа Муфанг $(M, \cdot)$ является лупой с ассоциативными степенями.

Рассмотрим класс луп, который называется лупами Пейджа.

Определение 5. Неассоциативная, конечная и простая лупа Муфанг M называется *лупой Пейджа*.

Следующее описание луп Пейджа представлено в работе [5]. Пусть $\mathbb{F}_q$ — конечное поле. Для $\alpha, \beta \in F_q^3$ определим операции $\cdot, \times$ следующим образом:

$$\alpha \cdot \beta = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3,$$
$$\alpha \times \beta = (\alpha_2\beta_3 - \alpha_3\beta_2, \alpha_3\beta_1 - \alpha_1\beta_3, \alpha_1\beta_2 - \alpha_2\beta_1).$$

Алгеброй Цорна $Z(q)$ называется множество (2×2)-матриц $\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$, где $a, b \in \mathbb{F}_q$ и $\alpha, \beta \in \mathbb{F}_q^3$, со следующей операцией:

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \cdot \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha\delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}.$$

Все элементы $Z(q)$ с определителем $M = ab - \alpha\beta = 1$ образуют лупу Пейджа $M^*(q)$ с нейтральным элементом $e = \begin{pmatrix} 1 & (0,0,0) \\ (0,0,0) & 1 \end{pmatrix}$.

Л. Пейдж в [6] показал, что $|M^*(q)| = q^3(q^4-1)$, когда q чётное, и $|M^*(q)| = q^3(q^4-1)/2$, если q нечётное.

Пусть $SL_2(q)$ — специальная линейная группа (2×2)-матриц с определителем, равным 1, над полем $\mathbb{F}_q$. Обозначим через $L_2(q)$ проективную группу $SL_2(q)/Z(SL_2(q))$.

П. Войтеховски [7] доказал следующую теорему.

Теорема 3. Пусть $S \subseteq Z$ — множество порядков всех элементов лупы $M^*(q)$ и T — множество порядков элементов $L_2(q)$. Тогда $S = T$ и порядок элемента $\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \in M^*(q)$ совпадает с порядком элемента $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in L_2(q)$ при $(\alpha,\beta) = (0,0)$ и с порядком элемента $\begin{pmatrix} a & 1 \\ \alpha\cdot\beta & b \end{pmatrix}$ из $L_2(q)$ при $\alpha \neq 0$.

Введём понятие *квазигруппового* (*лупового*) *кольца*. Пусть K — ассоциативное кольцо с единицей, L — лупа или квазигруппа. Рассмотрим множество KL, состоящее из всех формальных сумм вида $\sum\limits_{l\in L} \alpha_l \cdot l \ \ (\alpha_l \in K)$, в которых конечное число элементов α_l отлично от нуля. Два элемента $a, b \in KL$ считаются равными тогда и только тогда, когда $\alpha_l = \beta_l$ для всех $l \in L$.

На множестве KL определены операции сложения и умножения следующим образом: если $a = \sum\limits_{l\in L} \alpha_l \cdot l$ и $b = \sum\limits_{l\in L} \beta_l \cdot l$ — элементы KL, то $a + b = \sum\limits_{l\in L} (\alpha_l + \beta_l)\cdot l$, $ab = \sum\limits_{l\in L} \Big(\sum\limits_{\substack{m,h\in L: \\ mh=l}} \alpha_m\beta_h \Big) l$. Относительно этих операций множество KL является неассоциативным кольцом с единицей. Удобно отождествить $l \in L$ с элементом $1\cdot l \in KL$, а $\alpha \in K$ — с элементом $\alpha \cdot e$, где e — единица лупы, тогда K и L являются подмножествами в KL.

Пусть теперь R — ассоциативное кольцо с единицей $1 \in R$. Рассмотрим группу G в мультипликативной записи с нейтральным элементом $e \in G$.

Определение 6. Кольцо R называется *G-градуированным*, если существует такое семейство $\{R_\sigma : \sigma \in G\}$ аддитивных подгрупп R_σ аддитивной группы R, что $R = \bigoplus\limits_{\sigma\in G} R_\sigma$, $R_\sigma R_\tau \subseteq R_{\sigma\tau}$ для всех $\sigma, \tau \in G$. *Строго градуированным* называется G-градуированное кольцо R, для которого выполнено равенство $R_\sigma R_\tau = R_{\sigma\tau}$ для всех $\sigma, \tau \in G$. *Однородным степени* σ называется элемент $x \in R_\sigma$.

Будем обозначать множество обратимых по умножению элементов в кольце R символом $U(R)$.

Лемма 2. Пусть $R = \bigoplus\limits_{\sigma\in G} R_\sigma$ — G-градуированное кольцо. Тогда

1) $1 \in R_e$ и R_e является подкольцом кольца R;
2) обратный элемент r^{-1} к обратимому однородному элементу r также однородный;
3) G-градуированное кольцо R строго градуированно тогда и только тогда, когда $1 \in R_\sigma R_{\sigma^{-1}}$ для любого $\sigma \in G$.

Доказательство.

1. По определению $R_eR_e \subseteq R_e$; поэтому достаточно показать, что $1 \in R_e$. Пусть $1 = \sum\limits_{\sigma\in G} r_\sigma$, где $r_\sigma \in R_\sigma$. Для любого $h_\lambda \in R_\lambda$ получаем $h_\lambda = h_\lambda \cdot 1 = \sum\limits_{\sigma\in G} h_\lambda r_\sigma$ и

$h_\lambda r_\sigma \in R_{\lambda\sigma}$. Поэтому для любого $\sigma \neq e$ выполнено $h_\lambda r_\sigma = 0$. Итак, $1 \cdot r_\sigma = 0$, следовательно, $r_\sigma = 0$ для любого $\sigma \neq e$. Отсюда $1 = r_e \in R_e$.

2. Пусть $r \in U(R) \cap R_\lambda$. Если $r^{-1} = \sum\limits_{\sigma\in G} (r^{-1})_\sigma$, то $1 = rr^{-1} = \sum\limits_{\sigma\in G} r(r^{-1})_\sigma$. Так как $1 \in R_e$ и $r(r^{-1})_\sigma \in R_{\lambda\sigma}$, то $r(r^{-1})_\sigma = 0$ для любых $\sigma \neq \lambda^{-1}$. Но из того, что $r \in U(R)$ — обратимый элемент, следует соотношение $(r^{-1})_\sigma \neq 0$ для $\sigma \neq \lambda^{-1}$, и в итоге $r^{-1} = (r^{-1})_{\lambda^{-1}} \in R_{\lambda^{-1}}$ — тоже однородный элемент степени λ^{-1}.

3. Предположим, что $1 \in R_\sigma R_{\sigma^{-1}}$ для любого $\sigma \in G$, и докажем, что градуировка строгая. В самом деле, для любых $\sigma, \tau \in G$ имеем цепочку равенств

$$R_{\sigma\tau} = R_e R_{\sigma\tau} = (R_\sigma R_{\sigma^{-1}}) R_{\sigma\tau} = R_\sigma (R_{\sigma^{-1}} R_{\sigma\tau}) \subseteq R_\sigma R_\tau.$$

Это показывает, что $R_{\sigma\tau} = R_\sigma R_\tau$, что означает строгость градуировки.

Обратное утверждение очевидно: $1 \in R_e = R_\sigma R_{\sigma^{-1}}$. ■

Следствие 3. Справедливы равенства $R_e R_\sigma = R_\sigma R_e = R_\sigma$, т. е. R_σ есть R_e-бимодуль.

Пусть R — конечномерная некоммутативная алгебра над полем $\mathbb{F}$.

Определение 7. *Мультипликативным базисом* конечномерной алгебры R называется такой её базис B, что $B \cup \{0\}$ замкнуто относительно умножения.

Пример 1. Для алгебры $(n \times n)$-матриц $M_n(\mathbb{F})$ над полем $\mathbb{F}$ естественным мультипликативным базисом является стандартный базис, состоящий из матричных единиц E_{ij}, у которых на ij-й позиции стоит 1, а остальные элементы — нули.

Пример 2. Для любой конечномерной (полу)групповой алгебры $\mathbb{F}G$ моноида G в качестве мультипликативного базиса можно выбрать моноид G.

Для обобщения предыдущего примера рассмотрим обобщенные полугрупповые алгебры, обозначаемые $\Sigma(\Delta, R)$ и введённые в [8]. Здесь Δ — некоторое конечное множество, снабжённое частичным ассоциативным умножением. В свою очередь, $\Sigma(\Delta, R)$ — действительное векторное пространство функций из Δ в R. Мультипликативная структура на $\Sigma(\Delta, R)$ индуцируется умножением на Δ.

Пример 3. Любая конечномерная обобщённая полугрупповая алгебра $\Sigma(\Delta, R)$ имеет мультипликативный базис — так называемые характеристические функции χ_δ, $\delta \in \Delta$.

2. Криптосхемы над градуированными кольцами с мультипликативным базисом

2.1. Конструирование автоморфизмов градуированного кольца

В [9] рассматриваются автоморфизмы лупового кольца KL. Из автоморфизмов $\varphi \in \mathrm{Aut}(K)$ и $\psi \in \mathrm{Aut}(L)$ конструируется $\chi \in \mathrm{Aut}(KL)$ по следующему правилу: для любого $h = a_{l_1} l_1 + \ldots + a_{l_n} l_n$, $h \in KL$, по определению полагается $\chi(h) = \varphi(a_{l_1})\psi(l_1) + \ldots + \varphi(a_{l_n})\psi(l_n)$. Таким образом, если известна структура групп автоморфизмов $\mathrm{Aut}(K)$ и $\mathrm{Aut}(L)$ по отдельности, то есть возможность строить достаточно много автоморфизмов из $\mathrm{Aut}(KL)$. Заметим, что даже для произвольного группового кольца полного описания его группы автоморфизмов ещё не получено.

Пусть теперь R — кольцо, градуированное конечной группой G. По лемме 2 R_e — подкольцо в R, а по следствию 3 подгруппа R_σ есть R_e-бимодуль для любого $\sigma \in G$. Если описана группа автоморфизмов для подкольца R_e, то в общем случае, фиксируя

$\varphi \in \mathrm{Aut}(R_e)$, мы ещё не определяем однозначно автоморфизм для всего R. В самом деле, для этого необходимо распространить действие φ и на модули R_σ и таким образом получить $\chi \in \mathrm{Aut}(R)$. Для этого необходимо, чтобы $\chi(r_{\sigma_1} r_{\sigma_2}) = \chi(r_{\sigma_1})\chi(r_{\sigma_2})$ для $r_{\sigma_1} \in R_{\sigma_1}$, $r_{\sigma_2} \in R_{\sigma_2}$, $r_{\sigma_1} r_{\sigma_2} \in R_{\sigma_1\sigma_2}$.

Но если у кольца R существует мультипликативный базис B над R_e, то $R = R_e B$. Поэтому автоморфизм φ естественным образом продолжается до автоморфизма χ всего кольца R. В силу того, что B образует полугруппу по умножению, зададим $\psi \in \mathrm{Aut}(B)$ по аналогии с [9]. Этот автоморфизм будет перемешивать сам мультипликативный базис.

Заметим, что в случае (полу)группового кольца, рассматриваемого в естественной градуировке, такая конструкция в точности совпадает с построением его автоморфизма по отдельным автоморфизмам кольца и (полу)группы. Но даже для (полу)группового кольца, меняя градуировку или выбирая другой мультипликативный базис, получаем, вообще говоря, уже новые структуры для шифрования со своими автоморфизмами. Это расширяет множество подходящих для криптосхемы структур.

Пример 4. Рассмотрим $M_n(\mathbb{F})$, где $\mathbb{F} = R_n(K, J)$ — радикальное кольцо матриц. Пусть K — ассоциативное кольцо с единицей, J — идеал в K, $M_n(J)$ — кольцо $(n \times n)$-матриц над идеалом J. По определению из [10]

$$R_n(K, J) = NT_n(K) + M_n(J),$$

где $NT_n(K)$ — нижнетреугольные матрицы над кольцом K. Тогда $|\mathrm{Aut}(R_n(Z_{p^m}, (p^d)))| = (p^m - p^{m-1})^{n-1} \cdot p^{(2m-d)C_n^2 + d(n-2)}$, где $d|m$, $d < m$.

Автоморфизм $\psi \in \mathrm{Aut}(B)$ зададим по правилу $\psi(E_{ij}) = E_{\sigma(i)\sigma(j)}$, причём $\sigma \in S_n$. Так как $R_e = \mathbb{F}$, то $\mathrm{Aut}(R_e) = \mathrm{Aut}(\mathbb{F})$, а следовательно, количество индуцированных автоморфизмов равно

$$|\mathrm{Aut}(R_e)| \cdot |\mathrm{Aut}(B)| \geqslant |S_n| \cdot |\mathrm{Aut}(R_n(Z_{p^m}, (p^d)))| = n! \cdot (p^m - p^{m-1})^{n-1} \cdot p^{(2m-d)\cdot C_n^2 + d(n-2)}.$$

Таким образом, данная структура имеет достаточно богатую индуцированную группу автоморфизмов.

2.2. Построение криптосхемы

Участник A :

1) Выбирает градуированное кольцо R с мультипликативным базисом, такое, что группы автоморфизмов $\mathrm{Aut}(B)$ и $\mathrm{Aut}(R_e)$ некоммутативны. Предполагается, что группы $\mathrm{Aut}(B)$ и $\mathrm{Aut}(R_e)$ достаточно богаты некоммутирующими элементами большого порядка с нетривиальными централизаторами большого порядка. Положим $|\mathrm{Aut}(B)| \geqslant \geqslant t_1$, $|\mathrm{Aut}(R_e)| \geqslant t_2$. Здесь и далее t_i — параметры безопасности, которые по предположению экспоненциально зависят от порядка градуированного кольца R.

Фиксирует градуировку и этот базис (в случае, если кольцо допускает несколько различных базисов) с учётом вышеперечисленных условий. Эта информация объявляется по открытому каналу. Обозначим базис через B, а группу, по которой градуировано кольцо, — через G, тогда общеизвестны $\big(R, B, G\big)$.

2) Задает автоморфизм $\sigma \in \mathrm{Aut}(R_e)$ так, чтобы порядок $|\sigma| \geqslant t_3$, причём σ должен иметь нетривиальный централизатор и $|C(\sigma) \setminus \langle\sigma\rangle| \geqslant t_4$.

Конструирует автоморфизм $\eta \in \mathrm{Aut}(B)$ так, чтобы $|\eta| \geqslant t_5$, причём η должен иметь нетривиальный централизатор и $|C(\eta) \setminus \langle\eta\rangle| \geqslant t_6$.

3) Случайно выбирает автоморфизм $\tau \in C(\sigma) \setminus \langle\sigma\rangle$.

4) Случайно выбирает $\omega \in C(\eta) \setminus \langle\eta\rangle$.

5) По τ и ω строит секретный автоморфизм $\varphi \in \mathrm{Aut}(R)$ так: для любого $h \in R$ вида $h = a_{b_1}b_1 + \ldots + a_{b_n}b_n$, где $a_{b_1}, \ldots, a_{b_n} \in R_e$, полагает

$$\varphi(h) = \tau(a_{b_1})\omega(b_1) + \cdots + \tau(a_{b_n})\omega(b_n).$$

6) Выбирает элементы $a \in R$, $x \in R$ с нулевыми левыми аннуляторами. Это условие необходимо для последующей расшифровки.

7) Вычисляет $\varphi(x)$ и $\varphi(a)$.

Таким образом, открытым ключом участника A является

$$\Big(\sigma, \eta, x, \varphi(x), a, \varphi(a)\Big).$$

Отметим, что при должных параметрах безопасности t_3, t_4, t_5, t_6 автоморфизмов, подходящих для открытого ключа, достаточно много. Сформированный открытый ключ участник A передает участнику B по открытому каналу.

Участник B:

1) Выбирает натуральные числа i, j, k, l.

2) Используя открытый ключ участника A, получает пары автоморфизмов (σ^i, η^j), (σ^k, η^l) и по ним строит автоморфизмы $\psi, \chi \in \mathrm{Aut}(KL)$ таким же способом, как и участник A, т. е. для любого $h \in KL$ вида $h = a_{l_1}l_1 + \cdots + a_{l_n}l_n$ полагает $\psi(h) = \sigma^i(a_{l_1})\eta^j(l_1) + \cdots + \sigma^i(a_{l_n})\eta^j(l_n)$, $\chi(h) = \sigma^k(a_{l_1})\eta^l(l_1) + \cdots + \sigma^k(a_{l_n})\eta^l(l_n)$. Автоморфизмы ψ, χ будем называть сеансовыми.

3) Вычисляет $\chi(a) \cdot \psi(x)$.

4) Вычисляет $\chi(\varphi(a)) \cdot \psi(\varphi(x))$. Так как элементы a и x были выбраны с нулевым левым аннулятором, то и у этого произведения будет нулевой левый аннулятор.

5) Записывает исходный текст, который надо передать, в виде $m \in R$ и вычисляет $m \cdot [\chi(\varphi(a)) \cdot \psi(\varphi(x))]$. При необходимости исходный текст разбивается на блоки и каждый блок шифруется отдельно с разными секретными ключами.

6) Отправляет для A криптограмму

$$\Big(\chi(a) \cdot \psi(x),\ m \cdot \big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\big]\Big).$$

Получив криптограмму, участник A расшифровывает её:

1) Используя секретный автоморфизм φ, вычисляет $q = \varphi\big(\chi(a) \cdot \psi(x)\big)$.

2) Расшифровывает посланный текст, пользуясь тем, что χ, ψ и φ коммутируют. Таким образом, участник A знает $h = m \cdot [\chi(\varphi(a)) \cdot \psi(\varphi(x))]$ и $\varphi\big(\chi(a) \cdot \psi(x)\big)$. Для расшифровки сообщения m достаточно решить линейную систему $m \cdot q = h$ с коэффициентами из кольца R_e.

В самом деле, так как $\tau \in C(\sigma) \setminus \langle\sigma\rangle$ и $\omega \in C(\eta) \setminus \langle\eta\rangle$, то коммутируют между собой попарно автоморфизмы τ и σ, а также ω и η. Поэтому коммутируют и сконструированные на их основе автоморфизмы φ и ψ, φ и χ. Вследствие этого $\chi(\varphi(a)) \cdot \psi(\varphi(x)) = \varphi\big(\chi(a) \cdot \psi(x)\big) = q$. Кроме того, элемент $\chi(\varphi(a)) \cdot \psi(\varphi(x))$ выбран с нулевым левым аннулятором. Поэтому система уравнений $m \cdot q = h$ с коэффициентами из кольца R_e имеет единственное решение.

2.3. Анализ атак на криптосистему

Рассмотрим следующую задачу. Пусть R — некоторая алгебраическая структура, A — некоторое подмножество автоморфизмов в $\mathrm{Aut}\, R$, α — случайно выбранный

элемент из A. Предположим, что известно некоторое множество пар $(x_i, \alpha(x_i))$, $i = 1, \ldots, n$, где $x_i \in R$. Требуется найти автоморфизм $\alpha' \in A$, такой, что $\alpha'(x_i) = \alpha(x_i)$ для всех $i = 1, \ldots, n$. Обозначим эту задачу как $\Omega_n(A, R)$.

Заметим, что при отсутствии существенной информации о множествах A и R задача $\Omega_n(A, R)$ является вычислительно трудной, поскольку она разрешима только полным перебором всех элементов множества A и проверкой условия $\alpha'(x_i) = \alpha(x_i)$, $i = 1, \ldots, n$, для каждого выбранного $\alpha' \in A$.

Рассмотрим некоторые атаки на криптосистему.

Атака только с криптограммой

Пусть криптоаналитик располагает открытым ключом участника A и криптограммой. Перед ним стоит следующая задача: по известным парам $\big(a, \varphi(a)\big)$, $\big(x, \varphi(x)\big)$ найти такой $\alpha \in \mathrm{Aut}(R)$, индуцированный автоморфизмами (σ', η'), что $\varphi(a) = \alpha(a)$, $\varphi(x) = \alpha(x)$. К тому же необходимо, чтобы $\sigma' \in C(\sigma) \setminus \langle\sigma\rangle$, а $\eta' \in C(\eta) \setminus \langle\eta\rangle$.

Построим α. Положим $\alpha(a) := \varphi(a)$, $\alpha(x) := \varphi(x)$. Таким образом, определены $\alpha(ax) = \alpha(a) \cdot \alpha(x) := \varphi(a) \cdot \varphi(x)$ и $\alpha(xa) = \alpha(x) \cdot \alpha(a) := \varphi(x) \cdot \varphi(a)$. Но доопределить α на элемент $\chi(a) \cdot \psi(x)$ можно лишь перебором его образа с последующей проверкой того, что $\sigma' \in C(\sigma) \setminus \langle\sigma\rangle$, а $\eta' \in C(\eta) \setminus \langle\eta\rangle$. Это вычислительно не легче перебора всех автоморфизмов, индуцированных парами $(\sigma', \eta') \in \big(C(\sigma) \setminus \langle\sigma\rangle\big) \times \big(C(\eta) \setminus \langle\eta\rangle\big)$, удовлетворяющих начальным условиям $\alpha(a) = \varphi(a)$ и $\alpha(x) = \varphi(x)$. В итоге получаем задачу $\Omega_2(Y, R)$, где Y — это множество автоморфизмов R, полученных с помощью пар $(\sigma', \eta') \in \big[\big(C(\sigma) \setminus \langle\sigma\rangle\big) \times \big(C(\eta) \setminus \langle\eta\rangle\big)\big]$, что эквивалентно полному перебору секретных ключей.

Для оценки сложности вскрытия криптосистемы злоумышленником рассмотрим мощность множества, элементы которого необходимо перебрать. Тогда сложность данной атаки равна $t_4 \cdot t_6$. Поэтому при надлежащем выборе параметров безопасности задача является вычислительно трудной.

В случае, если криптоаналитик располагает несколькими криптограммами, даже при условии фиксированных автоморфизмов σ и η задача взлома всё равно сводится к полному перебору секретных ключей, так как предполагается, что они каждый раз выбираются разными.

Атака на сеансовые автоморфизмы ψ и χ

Другой способ атаки — найти автоморфизмы ψ и χ, а затем решить относительно m уравнение $m \cdot \big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\big] = h$, где h известен из криптограммы. Пусть ψ построен с помощью автоморфизмов (σ_1, η_1), а автоморфизм χ — с помощью (σ_2, η_2). Для того чтобы найти ψ и χ, криптоаналитику необходимо осуществить перебор образов $\psi(x)$, $\chi(a)$, таких, что $\chi(a)\psi(x) = h_1$, где h_1 известен из криптограммы, и проверить соотношения $(\sigma_1, \eta_1) \in (\langle\sigma\rangle, \langle\eta\rangle)$ и $(\sigma_2, \eta_2) \in (\langle\sigma\rangle, \langle\eta\rangle)$. Это вычислительно не легче, чем перебрать пары $(\sigma_1, \eta_1) \in (\langle\sigma\rangle, \langle\eta\rangle)$ и $(\sigma_2, \eta_2) \in (\langle\sigma\rangle, \langle\eta\rangle)$ (а это полный перебор соответствующих автоморфизмов) с последующей проверкой условия $\chi(a)\psi(x) = h_1$. Следовательно, определённая выше сложность атаки равна $t_3^2 \cdot t_5^2$. При правильном выборе соответствующих параметров безопасности эта задача является вычислительно трудной.

Атака с выбранным исходным текстом

Эта атака основана на попытке криптоаналитика получить $\chi(\varphi(a))\psi(\varphi(x)) \in R$ с последующим решением уравнения $m \cdot \chi(\varphi(a))\psi(\varphi(x)) = h$ относительно m посредством нового сеанса связи с участником B в качестве участника A. Даже если

участник B повторяет тот же исходный текст m, он должен сконструировать новые сеансовые автоморфизмы $\psi' \neq \psi$ и $\chi' \neq \chi$. Поэтому криптоаналитик получит не $m \cdot \chi(\varphi(a))\psi(\varphi(x))$, а $m \cdot \chi'(\varphi(a))\psi'(\varphi(x))$. И даже если он решит новое уравнение относительно $\chi'(\varphi(a))\psi'(\varphi(x))$, никакой новой информации относительно $\chi(\varphi(a))\psi(\varphi(x))$ он не получит.

3. Криптосхемы на основе луп

3.1. Протокол выработки общего секретного ключа

Рассмотрим протокол выработки общего ключа, построенный при помощи лупы Муфанг.

Пусть L — общеизвестная лупа Муфанг; $a, b, c \in L$ — общеизвестные элементы. Пусть M, K и N — порядки элементов a, b и c соответственно. Протокол выработки секретного ключа выглядит следующим образом:

1. Абонент A выбирает случайные натуральные числа $m < M$, $k < K$, $n < N$ и посылает абоненту B пару $(u_1, u_2) = (a^m b^k, b^k c^n)$.

2. Абонент B выбирает случайные натуральные числа $r < M$, $l < K$, $s < N$ и посылает сообщение $(v_1, v_2) = (a^r b^l, b^l c^s)$.

3. Абонент A вычисляет $(a^m v_1)b^k$ и $(b^k v_2)c^n$.

4. Абонент B вычисляет $(a^r u_1)b^l$ и $(b^l u_2)c^s$.

Общим ключом абонентов A и B является

$$K_{AB} = (a^{m+r}b^{k+l})(b^{k+l}c^{n+s}).$$

Непосредственно из теоремы 1 получаем

Утверждение 1. Если L — лупа Муфанг, $a, b \in L$, то

$$(a^n(a^r b^s))b^m = a^n((a^r b^s)b^m) = (a^s(a^n b^m))b^s = a^r((a^n b^m)b^s) = a^{r+n}b^{s+m}.$$

Таким образом, ключ абонента A: $K_A = ((a^m v_1)b^k)(b^k v_2)c^n) = (a^{m+r}b^{k+l})(b^{k+l}c^{n+s}) = = K_{AB}$; ключ абонента B: $K_B = ((a^r u_1)b^l)((b_l u_2)c^s) = K_{AB}$; $K_A = K_B$.

Отметим, что элементы a, b, c лупы L являются общеизвестными, а натуральные числа r, k, s, m, l, n — секретными.

Замечание 1. Покажем, что знание одного из секретных чисел достаточно для получения секретного ключа. Действительно, пусть злоумышленник каким-либо образом получил число m, тогда, сделав следующие вычисления: $(a^{-m}u_1) = b^k$, $b^{-k}u_2 = c^n$, $\left((a^m v_1)b^k\right)\left(b^k(v_2 c^n)\right) = K$, злоумышленник получает секретный ключ K.

Таким образом, стойкость протокола не превышает сложности нахождения одного секретного ключа.

Замечание 2. Злоумышленник для нахождения ключа может решить задачу дискретного логарифмирования в подгруппе $\langle a, b\rangle \subseteq L$ или $\langle b, c\rangle \subseteq L$, либо перебором найти элемент лупы, который является общим ключом.

Для примера рассмотрим класс луп Пейджа.

В качестве a, b, c можно выбрать элементы вида $\begin{pmatrix} \eta & e_1 \\ (0,0,0) & \eta^{-1} \end{pmatrix}$, $\begin{pmatrix} \theta & e_2 \\ (0,0,0) & \theta^{-1} \end{pmatrix}$, $\begin{pmatrix} \zeta & e_3 \\ (0,0,0) & \zeta^{-1} \end{pmatrix}$, где η, θ, ζ — примитивные элементы поля $\mathbb{F}_q$. Порядки данных элементов равны $(q-1)/2$.

3.2. Схема шифрования

Пусть L — конечная лупа и задана последовательность $\alpha = [A_1, \ldots, A_s]$, где $A_i \in L^r$ для некоторого натурального числа r, т. е. $A_i = (a_{i,1}, \ldots, a_{i,r})$, $a_{i,j} \in L$. Для каждого $i = 1, \ldots, s$ обозначим через A'_i элемент лупового кольца $\sum\limits_j a_{i,j} \in ZA$. Тогда $A'_1 \cdot \ldots \cdot A'_s = \sum a_l l$.

Определение 8. Последовательность $\alpha = [A_1, \ldots, A_s]$ называется $[s, r]$-покрытием для L, если для элемента лупового кольца $\sum a_l l = A'_1 \cdot \ldots \cdot A'_s$ выполняются условия: $a_l > 0$ для всех $l \in L$ и $|A_i| = r$, $i = 1, \ldots, s$.

Рассмотрим криптосхему, которая основана на $[s, r]$-покрытиях лупы Муфанг. Пусть L — конечная лупа Муфанг и $\alpha = (a_{i,j})$ — $[s, r]$-покрытие лупы L. В работе [11] показано, что сложность задачи разложения на множители $g = a_{1,j_1} \cdot a_{2,j_2} \cdot a_{3,j_3} \cdot \ldots \cdot a_{s,j_s}$ в конечной группе G эквивалентна сложности задачи дискретного логарифмирования в группе G. Тогда, в общем случае, задача разложения элемента лупы $l \in L$ на множители $l = (a_{1,j_1} \cdot (a_{2,j_2} \cdot (a_{3,j_3} \cdot \ldots \cdot a_{s,j_s})$ с неизвестной расстановкой скобок имеет не меньшую сложность, чем аналогичная задача в конечной группе.

Участник A:

1) Выбирает две лупы Муфанг L, M с достаточно большим количеством порождающих. Генерирует случайное $[s, r]$-покрытие $\alpha = (a_{i,j})$ для L.

2) Выбирает эпиморфизм $f : L \to M$, который он хранит в секрете, и вычисляет $\beta = (b_{i,j}) = f(\alpha) = f(a_{i,j})$. Заметим, что β является $[s, r]$-покрытием для лупы M.

Открытым ключом является

$$(\{\alpha\}, \{\beta\}).$$

Участник B:

1) Формирует сообщение $x \in M$.

2) Выбирает произвольное y_1 из покрытия α, причём расстановка скобок осуществляется произвольным способом. Таким образом, $y_1 = a_{1,j_1} \cdot (a_{2,j_2} \cdot (a_{3,j_3} \cdot \ldots \cdot a_{s,j_s})$.

3) Образует $y_2 \in \beta$ с аналогичной п. 2 расстановкой скобок.

4) Формирует $y_3 = xy_2$.

5) Посылает участнику A криптограмму (y_1, y_3).

Участник A, получив пару (y_1, y_3), вычисляет $f(y_1) = y_2$ и $y_3 y_2^{-1}$. Так как M — лупа Муфанг, то $y_3 y_2^{-1} = (xy_2)y_2^{-1} = x$.

Замечание 1. С практической точки зрения участнику А лучше заранее составить таблицу значений для эпиморфизма f.

Замечание 2. Конструкция легко может быть обобщена на произвольную квазигруппу, если умножение на y_2^{-1} справа в алгоритме расшифрования заменить на правое деление.

Замечание 3. Любое $[s, r]$-покрытие можно представить в виде матрицы $\alpha = (a_{i,j})$, где $a_{i,j} \in L$, $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant r$. Тогда с практической точки зрения $[s, r]$-покрытие удобно задавать случайной $(s \times r)$-матрицей с проверкой необходимых условий.

4. Линейно оптимальные коды в квазигрупповых кольцах

4.1. Предварительные сведения

Кодом длины n над алфавитом Ω называется подмножество $\mathcal{C} \subseteq \Omega^n$. Пусть $|\mathcal{C}| = q^k$, тогда $k = \log_q |\mathcal{C}|$ называется (*комбинаторной*) *размерностью* кода $\mathcal{C}$. На множестве $\mathcal{C}$

определим метрику (расстояние Хэмминга)

$$\mathrm{d}(a,b) = |\{i \in \{1,2,\ldots,n\} : a_i \neq b_i\}|,$$

где $a = (a_1,\ldots,a_n)$, $b = (b_1,\ldots,b_n)$.

Теперь определим расстояние кода:

$$d = \mathrm{d}(\mathcal{C}) = \min\{\mathrm{d}(a,b) : a,b \in \mathcal{C}, a \neq b\}.$$

Код с определёнными выше параметрами q,n,k,d называется $[n,k,d]_q$-*кодом* (подробнее см. [12, 13]).

Одной из задач алгебраической теории кодов является конструирование кодов, оптимизирующих один из параметров n,k,d при фиксированных значениях остальных двух и q.

Теорема 4 (граница Синглтона [12, 13]). Для любого $[n,k,d]_q$-кода выполнено неравенство $k \leqslant n-d+1$.

Определение 9. $[n,k,d]_q$-Код $\mathcal{C}$ называется *МДР-кодом*, если $k = n-d+1$.

Важный класс МДР-кодов исследуется в [14].

Если множество Ω снабжено алгебраической структурой (например, конечного поля, кольца или модуля) и код $\mathcal{C}$ согласован с этой структурой (например, если $\Omega = \mathbb{F}_q$ — конечное поле, то $\mathcal{C}$ должен быть подпространством в $\Omega = \mathbb{F}_q^n$), то код $\mathcal{C}$ называют *линейным кодом над* Ω.

Определение 10. Линейный $[n,k,d]_q$-код называется *линейно оптимальным*, если k — максимально возможная размерность линейного над полем $\Omega = \mathbb{F}_q$ кода длины n с расстоянием d.

Очевидно, что любой МДР-код оптимален. Сверх того, можно указать следующий признак линейной оптимальности.

Обозначим через $n(k,q)$ (соответственно, $m(k,q)$) максимальную длину МДР-кода комбинаторной размерности k над алфавитом из q элементов (соответственно, линейного МДР-кода над полем $\mathbb{F}_q$ для примарного числа q). Ясно, что $m(k,q) \leqslant n(k,q)$.

Утверждение 2. Пусть n,k — натуральные числа, q — такое примарное число, что $n > m(k+1,q)$. Тогда любой линейный $[n,n-k,k]_q$-код линейно оптимален.

Доказательство. Действительно, в противном случае существует линейный $[n,k+1,n-k]_q$-код. Но такой код является МДР-кодом, следовательно, $n \leqslant m(k+1,q)$. Получаем противоречие. ■

Одним из способом получения линейных над полем $\mathbb{F}_q$ кодов с экстремальными свойствами является следующая конструкция. Для конечной лупы $L = \{l_1,\ldots,l_n\}$ сформируем луповую алгебру $A = \mathbb{F}_q L$ и для каждого левого идеала $I \leqslant {}_A A$ определим код $\mathcal{C} = \mathcal{C}(I)$ как набор всех слов $(\alpha_1,\ldots,\alpha_n) \in \mathbb{F}_q^n$, таких, что $\sum \alpha_i l_i \in I$. Такие коды называются луповыми [15]. Каждая луповая алгебра (и даже квазигрупповая алгебра) содержит 2 *тривиальных МДР-кода*: $[n,1,n]$-код $\mathcal{C}(I_0)$, соответствующий левому идеалу $\mathbb{F}_q(\sum_{l\in L} l)$, и $[n,n-1,2]$-код $\mathcal{C}(\Delta)$, соответствующий фундаментальному идеалу

$$\Delta(A) = \left\{ \sum_{l\in L} \alpha(l) l : \sum_{l\in L} \alpha(l) = 0 \right\},$$

который является левым и правым аннулятором идеала I_0.

Компьютерные вычисления в [15] в случае луповых алгебр маленьких порядков ($q \leqslant 5$, $|L| \leqslant 7$) показали, что в большинстве случаев, когда лупа L неассоциативна, её решётка левых идеалов тривиальна, и поэтому она не содержит интересных луповых кодов. Исключение составляют линейно оптимальные $[6,2,4]_q$-коды для $q \in \{2,3\}$, а также $[6,3,3]_q$-коды для $q \in \{3,4\}$.

В данной работе строятся цепочки линейных $[n, n-3, 3]_q$-кодов над $\mathbb{F}_q$ для $n = 2q$ и $n = 2q-2$. Эти коды являются линейно оптимальными, что следует из утверждения 2, а также из того, что $n(k,q) = k+1$ при $q \leqslant k$ (см. [12, 13]).

Заметим, что линейный $[n, n-3, 3]_q$-код над $\mathbb{F}_q$ может быть легко построен с помощью укорочения $[N, N-3, 3]_q$-кода Хэмминга ([16, 17]), где $N = q^2+q+1$. Основной результат заключается в построении таких кодов как луповых кодов.

4.2. Коды Рида – Соломона как групповые коды

Пусть $q = p^l > 2$, $P = \mathbb{F}_q$, G — конечная группа. Единичный элемент поля P обозначим 1, единичный элемент группы G (он же единичный элемент группового кольца PG) обозначим e.

Следующее представление кодов Рида — Соломона как групповых кодов, впервые описанное в [18], играет ключевую роль в построении линейных луповых $[2q, 2q-3, 3]_q$-кодов.

Теорема 5. Пусть $(H, \cdot)$ — p-элементарная абелева группа порядка $q = p^l$. Фиксируем изоморфизм абелевых групп $\varphi : (H, \cdot) \to (P, +)$ и рассмотрим следующие элементы:

$$u_s = \sum_{h \in H} \varphi(h)^s h \in PH, \quad s = 0, \ldots, q-2. \tag{1}$$

Тогда для каждого i, $1 \leqslant i \leqslant q-1$, подпространство $\mathcal{R}_i = Pu_0 + \ldots + Pu_{i-1} \leqslant {}_P PH$ является $[q, i, q+1-i]_q$-МДР кодом Рида — Соломона и идеалом в PH. В частности,

$$\mathcal{R}_{q-1} = \Delta(PH). \tag{2}$$

Если $s = p^c$ для некоторого $1 \leqslant c \leqslant n-1$, то

$$\mathcal{R}_s = PHu_{s-1} \tag{3}$$

является главным идеалом.

Доказательство. Занумеруем элементы группы H: $H = \{h_1, \ldots, h_q\}$, и положим $w_r = \varphi(h_r)$, $1 \leqslant r \leqslant q$. Тогда $P = \{w_1, \ldots, w_q\}$ и элементы (1) имеют вид $u_s = \sum\limits_{r=1}^{q} w_r^s h_r$. Теперь легко видеть, что код $\mathcal{K}(\mathcal{R}_i) \leqslant {}_P PH$, соответствующий пространству $\mathcal{R}_i$, имеет порождающую матрицу

$$G_i = \begin{pmatrix} w_1^0 & w_2^0 & \ldots & w_q^0 \\ \ldots & \ldots & \ldots & \ldots \\ w_1^{i-1} & w_2^{i-1} & \ldots & w_q^{i-1} \end{pmatrix},$$

т. е. является $[q, i, q-i+1]_q$-кодом Рида — Соломона [12, 13]. Заметим, что пока использована только биективность φ.

С учётом того, что φ является изоморфизмом групп, докажем, что $\mathcal{R}_s$, $1 \leqslant s \leqslant q-1$, является идеалом в кольце $R = PH$. Достаточно показать, что $a\mathcal{R}_s \subseteq \mathcal{R}_s$ для любого $a \in H$. Докажем это индукцией по s. При $s = 1$ имеем

$$a\mathcal{R}_1 = Pau_0 = Pa \sum_{h \in H} \varphi(h)^0 h = P \sum_{h \in H} ah = P \sum_{h \in H} h = Pu_0 = \mathcal{R}_1.$$

При $s > 0$

$$au_s = \sum_{h\in H} \varphi(h)^s ah = \sum_{h\in H} \varphi(ha^{-1})^s h,$$

и, поскольку φ — гомоморфизм,

$$au_s = \sum_{h\in H} [\varphi(h) - \varphi(a)]^s h = \sum_{h\in H} \left[\varphi(h)^s + \sum_{t=1}^{s} (-1)^t \binom{s}{t} \varphi(h)^{s-t}\varphi(a)^t\right] h =$$

$$= \sum_{h\in H} \varphi(h)^s h + \sum_{t=1}^{s} (-1)^t \binom{s}{t} \varphi(a)^t \sum_{h\in H} \varphi(h)^{s-t} h.$$

Окончательно получаем

$$au_s = u_s + \sum_{t=1}^{s} (-1)^t \binom{s}{t} \varphi(a)^t u_{s-t} \in u_s + \mathcal{R}_s \subset \mathcal{R}_{s+1}. \tag{4}$$

Итак, $a\mathcal{R}_1 \subseteq \mathcal{R}_1$, и, учитывая, что по предположению индукции $a\mathcal{R}_s \subseteq \mathcal{R}_s$, получаем

$$a\mathcal{R}_{s+1} = Pau_s + a\mathcal{R}_s \subseteq Pu_s + \mathcal{R}_s + a\mathcal{R}_s = \mathcal{R}_{s+1},$$

что и требовалось.

Чтобы доказать равенство (2), покажем, что $\sum\limits_{\omega\in P} \omega^s = 0$ для $s = 0, \ldots, q-2$. Пусть $\alpha \in P : \langle\alpha\rangle = P^*$, тогда $\alpha^s \left(\sum\limits_{\omega\in P} \omega^s\right) = \sum\limits_{\omega\in P} \omega^s$, $s = 0, \ldots, q-2$, откуда получаем требуемое, так как $\alpha^s \neq 1$ при $s < q-1$. Таким образом, $\mathcal{R}_{q-1} \subseteq \Delta(PH)$. С другой стороны, $\dim_P \mathcal{R}_{q-1} = q-1 = \dim_P \Delta(PH)$, следовательно, $\mathcal{R}_{q-1} = \Delta(PH)$.

Доказательство равенства (3) основывается на хорошо известном результате Лукаса (см., например, [12]). Пусть r_{ts} — остаток по модулю p числа $(-1)^t \binom{s}{t}$ и $s = s_0 + ps_1 + \ldots + p^{l-1}s_{n-1}$, $t = t_0 + pt_1 + \ldots + p^{l-1}t_{n-1}$, где $p_i, t_j \in \{0, \ldots, p-1\}$, причём $s_i \leqslant t_i$. Тогда

$$r_{ts} \equiv (-1)^t \binom{s_0}{t_0}\binom{s_1}{t_1}\ldots\binom{s_{n-1}}{t_{n-1}} \pmod p.$$

Тем самым доказано следующее утверждение.

Лемма 3. Если $s = p^c$, то $r_{t,s-1} \in P^*$ для любого $1 \leqslant t \leqslant s-1$.

Теперь перепишем (4) в виде

$$\sum_{t=1}^{s-1} r_{t,s-1}\varphi(a)^t u_{s-1-t} = (a-e)u_{s-1}.$$

Выберем $s-1$ различных элементов $a_1, \ldots, a_{s-1} \in H \setminus \{e\}$ и положим $w_i = \varphi(a_i)$, $i = 1, \ldots, s-1$. Тогда, имея u_{s-1}, можем построить систему уравнений относительно неизвестных параметров $u_0, \ldots, u_{s-2}$:

$$\begin{pmatrix} r_{1,s-1}w_1 & r_{2,s-1}w_1^2 & \ldots & r_{s-1,s-1}w_1^{s-1} \\ r_{1,s-1}w_2 & r_{2,s-1}w_2^2 & \ldots & r_{s-1,s-1}w_2^{s-1} \\ \ldots & \ldots & \ldots & \ldots \\ r_{1,s-1}w_{s-1} & r_{2,s-1}w_{s-1}^2 & \ldots & r_{s-1,s-1}w_{s-1}^{s-1} \end{pmatrix} \begin{pmatrix} u_{s-2} \\ u_{s-3} \\ \ldots \\ u_o \end{pmatrix} = \begin{pmatrix} (a_1-e)u_{s-1} \\ (a_2-e)u_{s-1} \\ \ldots \\ (a_{s-1}-e)u_{s-1} \end{pmatrix}. \tag{5}$$

Если $s = p^c$, то по лемме 3 матрица в левой части системы (5) обратима (и, следовательно, система имеет единственное решение). Это означает, что $u_0, ..., u_{s-2} \in PHu_{s-1}$. Таким образом, (3) верно. ■

Близкие описания кодов Рида — Соломона получены в [19, 20].

4.3. Линейно оптимальные $[2q, 2q-3, 3]_q$-коды

Как и выше, p — простое, $q = p^n > 2$ и $P = \mathbb{F}_q$.

Сформулируем основной результат этого пункта.

Теорема 6. Пусть L — лупа порядка $2q$, содержащая p-элементарную абелеву группу H порядка q. Пусть также существует элемент $b \in L \setminus H$, обладающий следующими свойствами:

1) $\exists \dot{k} \in \{1, \ldots, p-1\} \quad \forall l \in L \setminus H \ \ \exists \dot{h}_l \in H \quad \forall h \in H \ \ lh = b(\dot{h}_l h^{\dot{k}})$;
2) $\exists \ddot{k} \in \{1, \ldots, p-1\} \quad \forall l \in L \setminus H \ \ \exists \ddot{h}_l \in H \quad \forall h \in H \ \ l(bh) = \ddot{h}_l h^{\ddot{k}}$;
3) $\forall \alpha \in H \ \ \exists h_\alpha \in H \quad \forall h \in H \ \ \alpha(bh) = b(h_\alpha h)$.

Тогда, если степень расширения n чётная или если $P = \mathbb{F}_p$ и

$$\exists k \in P \ k^2 = \dot{k}^{-1}\ddot{k}, \tag{6}$$

то в решётке левых идеалов PL содержится структура, изображенная на рис. 1.

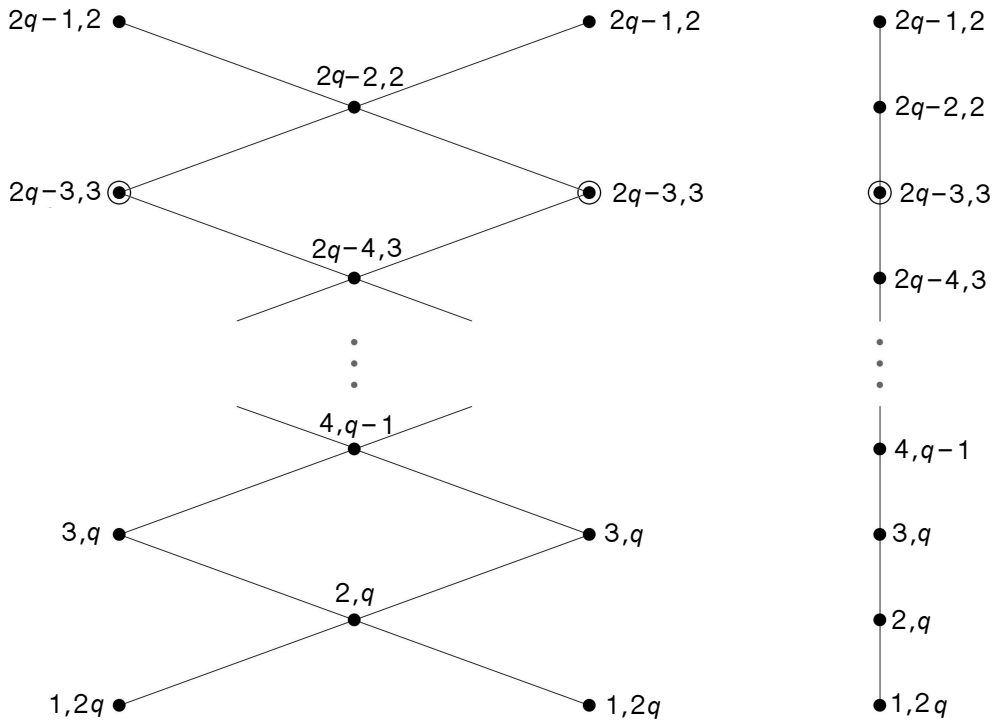

Рис. 1. Решётка идеалов PL при $\operatorname{char} P \neq 2$ (слева) и при $\operatorname{char} P = 2$ (справа). Каждый круг обозначает левый идеал PL, а k, d — сопровождающие числа, где k обозначает размерность, d — расстояние соответствующего кода. Любые два идеала соединены линией тогда и только тогда, когда нижний содержится в верхнем

Выделенные на рис. 1 идеалы соответствуют линейно оптимальным $[2q, 2q-3, 3]_q$-кодам.

Доказательство. Сохраним старые обозначения: пусть $\varphi : (H, \cdot) \to (P, +)$ — изоморфизм абелевых групп; $\mathcal{R}_i = Pu_0 + \ldots + Pu_{i-1} \leqslant {}_P PH$, $1 \leqslant i \leqslant q-1$.

Заметим, что если n чётное, то условие (6) выполнено, так как многочлен $x^2 - \dot{k}^{-1}\ddot{k} \in \mathbb{F}_p[x]$ раскладывается в $\mathbb{F}_{p^2}$ на линейные множители. Обозначим $\pm k_i$ квадратные корни из $(\dot{k}^{-1}\ddot{k})^i$.

С помощью $v_i \in \mathcal{R}_{i+1} \setminus \mathcal{R}_i$ построим

$$\sigma_i^+ = ev_i + b(k_i v_i), \quad \sigma_i^- = ev_i - b(k_i v_i),$$

если $\operatorname{char} P = 2$, то $\sigma_i^+ = \sigma_i^i$.

Тогда искомые идеалы имеют вид

$$\mathcal{L}_i = e\mathcal{R}_i + b\mathcal{R}_i \lhd PL,$$
$$\mathcal{M}_i^+ = e\mathcal{R}_i + b\mathcal{R}_i + P\sigma_i^+ \lhd PL, \qquad \mathcal{M}_i^- = e\mathcal{R}_i + b\mathcal{R}_i + P\sigma_i^- \lhd PL,$$

если $\operatorname{char} P = 2$, то $\mathcal{M}_i^+ = \mathcal{M}_i^i$.

Этим идеалам соответствуют луповые коды: $\mathcal{C}(\mathcal{L}_i)$ есть $[2q, 2i, q+1-i]_q$-код; $\mathcal{C}(\mathcal{M}_i^+)$ — $[2q, 2i+1, q+1-i]_q$-код; $\mathcal{C}(\mathcal{M}_i^-)$ — $[2q, 2i+1, q+1-i]_q$-код.

Так как $b \in L \setminus H$, то $L = H \cup bH$ и, следовательно, $PL = PH \dot{+} bPH$. Значит, $\mathcal{L}_i = e\mathcal{R}_i + b\mathcal{R}_i$ имеет размерность $2i$ и расстояние $q+1-i$.

Далее, так как $\mathcal{M}_i^+ = \mathcal{L}_i + P\sigma_i^+$, где $\sigma_i^+ = ev_i + b(k_i v_i)$ и $v_i \in \mathcal{R}_{i+1} \setminus \mathcal{R}_i$, то $\sigma_i^+ \notin \mathcal{L}_i$ и, следовательно, $\dim(\mathcal{L}_i) = 2i+1$. Аналогично для $\mathcal{M}_i^-$.

Теперь определим расстояние $\mathcal{M}_i^+$. Так как $\mathcal{M}_i^+ \supseteq e\mathcal{R}_i$, то $\mathrm{d}(\mathcal{M}_i^+) \leqslant \mathrm{d}(R_i) = q+1-i$. С другой стороны, включение $v_i \in \mathcal{R}_{i+1} \setminus \mathcal{R}_i$ влечёт неравенство

$$\mathrm{d}(v_i, \mathcal{R}_i) = \min\{\mathrm{d}(v_i, u) : u \in \mathcal{R}_i\} \geqslant q+1-(i+1) = q-i. \tag{7}$$

Рассмотрим произвольный элемент $x \in \mathcal{M}_i^+ \setminus \{0\}$, $x = ex_1 + bx_2 + \alpha\sigma_i^+$, где $x_1, x_2 \in \mathcal{R}_i$, $\alpha \in P$. Очевидно, что $||x|| = ||x_1 + \alpha v_i|| + ||b(x_2 + \alpha v_i)|| = ||x_1 + (\alpha k_i)v_i|| + ||x_2 + (\alpha k_i)v_i||$. Если $\alpha = 0$, то $x \in \mathcal{L}_i$ и $||x|| \geqslant q+1-i$. Иначе $||x_1 + \alpha v_1|| \geqslant q-i$ и $||x_2 + (\alpha k_i)v_2|| \geqslant q-i$ согласно (7). Таким образом, $||x|| \geqslant 2(q-i) \geqslant q+1-i$, если $i \leqslant q-1$. Окончательно, $\mathrm{d}(\mathcal{M}_i^+) = q+1-i$.

Аналогично доказывается, что $\mathrm{d}(\mathcal{M}_i^-) = q+1-i$.

Осталось показать, что $\mathcal{L}_i$, $\mathcal{M}_i^+$, $\mathcal{M}_i^+$ являются L-кодами, т. е. левыми иделами PL.

Сначала покажем, что $\mathcal{L}_i \lhd PL$. Достаточно проверить, что $\alpha\mathcal{L}_i \subseteq \mathcal{L}_i$, $\alpha \in H$, и $l\mathcal{L}_i \subseteq \mathcal{L}_i$, $l \in L \setminus H$. Учитывая свойство 3 из условия теоремы и то, что $\mathcal{R}_i \lhd PH$, получаем

$$\alpha\mathcal{L}_i = \alpha(e\mathcal{R}_i + b\mathcal{R}_i) = \alpha\mathcal{R}_i + \alpha(b\mathcal{R}_i) = \alpha\mathcal{R}_i + b(h_\alpha\mathcal{R}_i) \subseteq \mathcal{R}_i + b(\mathcal{R}_i) = \mathcal{L}_i.$$

Лемма 4. Пусть $v = \sum\limits_{h\in H} \alpha(h)h \in \mathcal{R}_i$. Определим $\psi_k(v) = \sum\limits_{h\in H} \alpha(h)h^k \in \mathcal{R}_i$, где $k \in \mathbb{Z}$, $p \nmid k$. Пусть μ таково, что $\mu p \equiv 1 \pmod p$. Тогда

$$\psi_k(v) \equiv \mu^{i-1} v \pmod{\mathcal{R}_{i-1}}. \tag{8}$$

В частности,

$$\psi_k(\mathcal{R}_i) \subseteq \mathcal{R}_i. \tag{9}$$

Доказательство. Напомним, что $\mathcal{R}_i = Pu_0 + \ldots + Pu_{i-1}$. Заметим, что отображение ψ_k линейное. Рассмотрим $\psi_k(u_s) = \psi_k\left(\sum\limits_{h\in H} \varphi(h)^s h\right) = \sum\limits_{h\in H} \varphi(h)^s h^k = \sum\limits_{h\in H} \varphi(h^\mu)^s h$ (это следует из того, что все элементы из $H \setminus \{e\}$ имеют порядок p). Так как φ — гомоморфизм, то $\psi_k(u_s) = \sum\limits_{h\in H} (\mu\varphi(h))^s h = \mu^s u_s$, откуда получаем (8) и (9). ■

Теперь можно показать, что $l\mathcal{L}_i \subseteq \mathcal{L}_i$:

$$l\mathcal{L}_i = l(e\mathcal{R}_i + b\mathcal{R}_i) = \ddot{h}_l\psi_{\ddot{k}}(\mathcal{R}_i) + b(\dot{h}_l\psi_{\dot{k}}(\mathcal{R}_i)) \subseteq \ddot{h}_l\mathcal{R}_i + b(\dot{h}_l\mathcal{R}_i) \subseteq \mathcal{R}_i + bR_i = \mathcal{L}_i.$$

Мы воспользовались свойством (9), свойствами 1, 2 из условия и тем, что $\mathcal{R}_i \lhd PH$.

Рассмотрим $\mathcal{M}_i^+ \leqslant {}_PPL$. Так как уже доказано, что $\mathcal{L}_i \lhd PL$, то достаточно проверить, что $\alpha\sigma_i^+ \subseteq \mathcal{M}_i^+$, $\alpha \in H$, и $l\sigma_i^+ \subseteq \mathcal{M}_i^+$, $l \in L \setminus H$. Справедливы равенства

$$\alpha\sigma_i^+ = \alpha(ev_i + b(k_iv_i)) = \alpha v_i + b(h_\alpha k_i v_i) =$$
$$= (\alpha - e)v_i + ev_i + b((h_\alpha - e)k_iv_i + e(k_iv_i)) = \sigma_i^+ + (\alpha - e)v_i + b((h_\alpha - e)k_iv_i).$$

Заметим, что из (4) следует соотношение $hv_i \equiv v_i \pmod{\mathcal{R}_{i-1}}$ для всех $v_i \in \mathcal{R}_i$, $h \in H$, значит, $(\alpha - e)v_i + b((h_\alpha - e)k_iv_i) \in \mathcal{L}_i$.

Далее, по свойствам 1, 2 и лемме 4 получим

$$l\sigma_i^+ = l(ev_i + b(k_iv_i)) = b(\dot{h}_l\psi_{\dot{k}}(v_i)) + \ddot{h}_l\psi_{\ddot{k}}(k_iv_i) =$$
$$= k_i\ddot{h}_l\psi_{\ddot{k}}(v_i) + b(\dot{h}_l\psi_{\dot{k}}(v_i)) \equiv k_i\ddot{\mu}^iv_i + b(\dot{\mu}^iv_i) \pmod{\mathcal{L}_i},$$

где $\dot{\mu}\dot{k} \equiv \ddot{\mu}\ddot{k} \equiv 1 \pmod p$. Остаётся заметить, что $k_i\ddot{\mu}^iv_i + b(\dot{\mu}^iv_i) = k_i\ddot{\mu}^i\sigma_i^+$, так как $k_i^2 \equiv (\dot{\mu}\ddot{\mu}^{-1})^i \pmod p$.

Доказательство для $\mathcal{M}_i^-$ аналогично.

Неравенство $\mathcal{M}_i^+ \neq \mathcal{M}_i^-$ следует из того, что $\mathcal{M}_i^+ + \mathcal{M}_i^- = \mathcal{L}_{i+1}$, а $\dim(\mathcal{L}_{i+1}) > \dim(\mathcal{M}_i^+) = \dim(\mathcal{M}_i^-)$.

Таким образом, мы построили всю решётку идеалов, за исключением идеалов размерности 1. Построим их:

$$\mathcal{M}_0^+ = P\left(\sum_{l\in L} l\right), \qquad \mathcal{M}_0^- = P\left(\sum_{h\in H} h - \sum_{l\in L\setminus H} l\right).$$

Теорема доказана. ■

Замечание. Если существует элемент $b \in L \setminus H$, удовлетворяющий условию теоремы 6, то и любой другой элемент из $L \setminus H$ тоже удовлетворяет этому условию.

4.4. Линейно оптимальные $[2q-2, 2q-5, 3]_q$-коды

Сохраним обозначения $P = \mathbb{F}_q$, $q = p^n$.

Теорема 7. Пусть L — лупа порядка $2q-2$, содержащая циклическую абелеву группу H порядка $q-1$. Пусть также существует элемент $b \in L \setminus H$, обладающий следующими тремя свойствами:

1) $\forall l \in L \setminus H \ \ \exists \dot{h}_l \in H \quad \forall h \in H \ \ lh = b(\dot{h}_l h)$;
2) $\forall l \in L \setminus H \ \ \exists \ddot{h}_l \in H \quad \forall h \in H \ \ l(bh) = \ddot{h}_l h$;
3) $\forall \alpha \in H \ \ \exists h_\alpha \in H \quad \forall h \in H \ \alpha(bh) = h_\alpha h$.

Тогда если $\operatorname{char} P \neq 2$, то в решётке левых идеалов PL содержится $\varphi(q-1)$ (φ — функция Эйлера) структур следующего вида (все идеалы, участвующие в структурах, попарно различны):

$$\mathcal{L}_i \subseteq \mathcal{M}_i^-, \quad \mathcal{M}_i^+ \subseteq \mathcal{N}_i, \quad i = 1, 2, \ldots, q-1,$$

причём $\mathcal{C}(\mathcal{M}_i^\pm)$ являются линейно оптимальными $[2q-5, 2q-3, 3]_q$-кодами.

Если $\operatorname{char} P = 2$, то в решётке левых идеалов PL содержится $\varphi(q-1)$ цепочек следующего вида (все идеалы, участвующие в цепочках, попарно различны):

$$\mathcal{L}_i \subseteq \mathcal{M}_i \subseteq \mathcal{N}_i, \quad i = 1, 2, \ldots, q-1,$$

причём $\mathcal{C}(\mathcal{M}_i)$ являются линейно оптимальными $[2q-5, 2q-3, 3]_q$-кодами.

Доказательство. По условию $H = \langle a \rangle_{q-1}$, поэтому $PH \cong \mathbb{F}_p[x]/(x^{q-1}-1)$ и все идеалы PH имеют вид $([g(x)])$, где $g(x) \mid x^{q-1}-1$. Заметим, что так как $|P^*| = q-1$, то многочлен $x^{q-1}-1$ раскладывается в P на (различные) линейные множители.

Для каждого примитивного $\alpha_i \in P$, $i = 1, \ldots, \varphi(q-1)$, определим

$$\mathcal{V}_i = ([(x-1)(x-\alpha_i)]) \lhd PH, \quad \mathcal{W}_i = ([(x-\alpha_i)]) \lhd PH.$$

Ясно, что $\dim(\mathcal{V}_i) = q-1-2 = q-3$, $\dim(\mathcal{W}_i) = q-1-1 = q-2$. Найдём теперь расстояния. Очевидно, что $\mathrm{d}(\mathcal{C}(\mathcal{W}_i)) = 2$. Чтобы определить расстояние $\mathcal{C}(\mathcal{V}_i)$, заметим, что вектор v принадлежит $\mathcal{C}(\mathcal{V}_i)$ тогда и только тогда, когда

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha_i & \alpha_i^2 & \ldots & \alpha_i^{q-2} \end{pmatrix} v = 0. \tag{10}$$

Так как $\mathrm{ord}\,(\alpha_i) = q-1$, то гарантированный ранг проверочной матрицы из (10) равен 2, следовательно, $\mathrm{d}(\mathcal{C}(\mathcal{V}_i)) = 3$.

С помощью $\mathcal{V}_i$ и $\mathcal{W}_i$ построим

$$\mathcal{L}_i = e\mathcal{V}_i + b\mathcal{V}_i, \quad \mathcal{N}_i = e\mathcal{W}_i + b\mathcal{W}_i.$$

По свойствам 1, 2, 3 легко проверяется, что $\mathcal{L}_i$ и $\mathcal{N}_i$ являются идеалами в PL. Далее, так как $b \in L \setminus H$, то $L = H \cup bH$, а значит, $PL = PH \dot{+} bPH$. Поэтому $\dim(\mathcal{L}_i) = 2(q-3) = 2q-6$, $\dim(\mathcal{N}_i) = 2(q-2) = 2q-4$, $\mathrm{d}(\mathcal{C}(\mathcal{L}_i)) = \mathrm{d}(\mathcal{C}(\mathcal{V}_i)) = 3$, $\mathrm{d}(\mathcal{C}(\mathcal{N}_i)) = \mathrm{d}(\mathcal{C}(\mathcal{W}_i)) = 2$.

Обозначим $\sigma_i^+ = ev_i + bv_i$, $\sigma_i^- = ev_i - bv_i$, где $v_i \in \mathcal{W}_i \setminus \mathcal{V}_i$ (если $\mathrm{char}\, P = 2$, то $\sigma_i^+ = \sigma_i^-$), и построим $\mathcal{M}_i^+, \mathcal{M}_i^- \leqslant {}_P PL$ (если $\mathrm{char}\, P = 2$, то $\mathcal{M}_i^+ = \mathcal{M}_i^- = \mathcal{M}$):

$$\mathcal{M}_i^+ = \mathcal{L}_i + P\sigma_i^+, \quad \mathcal{M}_i^- = \mathcal{L}_i + P\sigma_i^-.$$

Размерность $\mathcal{M}_i^\pm$ равна $2q-5$, так как $\sigma_i^\pm \neq \mathcal{L}_i$. Поскольку $\mathrm{d}(v_i, \mathcal{V}_i) \geqslant 2$, то $\mathrm{d}(\sigma_i^\pm, \mathcal{L}_i) \geqslant$ $\geqslant 4 > \mathrm{d}(\mathcal{C}(\mathcal{L}_i)) = 3$. Следовательно, $\mathrm{d}(\mathcal{C}(\mathcal{M}_i)) = \mathrm{d}(\mathcal{C}(\mathcal{L}_i)) = 3$. Далее нам понадобится следующее утверждение.

Лемма 5. Если $v_i \in \mathcal{W}_i$, то $(\alpha - e)v_i \in \mathcal{V}_i$ для всех $\alpha \in H$.

Доказательство. Вектору v_i соответствует $[v_i(x)] \in \mathbb{F}_q[x]/(x^{q-1}-1)$. Пусть $\alpha = a^k$, тогда $(\alpha - e)$ соответствует $[x^k - 1]$. Остаётся заметить, что $[v_i(x)(x^k-1)] \in$ $\in ([(x-1)(x-\alpha_i)]) = \mathcal{V}_i$, так как $(x-1) \mid (x^k-1)$. ■

Покажем, что $\mathcal{M}_i^+ \lhd PL$. Так как $\mathcal{L}_i \lhd PL$, то достаточно показать, что $\alpha\sigma_i^+ \in \mathcal{M}_i$, $l\sigma_i \in \mathcal{M}_i$ для всех $\alpha \in H$, $l \in L \setminus H$. Действительно, по лемме 5 и свойству 3 из условия получим

$$\alpha\sigma_i = \alpha(ev_i + bv_i) = \alpha v_i + b(h_\alpha v_i) =$$
$$= (\alpha - e)v_i + ev_i + b((h_\alpha - e)v_i + ev_i) = \sigma_i + (\alpha - e)v_i + b((h_\alpha - e)v_i) \equiv \sigma_i \pmod{\mathcal{L}_i},$$

а по лемме 5 и свойствам 1, 2

$$l\sigma_i = l(ev_i + bv_i) = \ddot{h}_l v_i + b(\dot{h}_l)v_i \equiv ev_i + bv_i \pmod{\mathcal{L}_i}.$$

При рассмотрении σ_i^- получим, что

$$\alpha\sigma_i^- \equiv \sigma_i^- \pmod{\mathcal{L}_i}, \quad l\sigma_i^- \equiv -\sigma_i^- \pmod{\mathcal{L}_i}, \quad \alpha \in H,\ l \in L \setminus H.$$

Покажем, что все идеалы $\mathcal{M}_i^\pm$ различны. Действительно, $\mathcal{M}_i^+ + \mathcal{M}_i^- = \mathcal{N}_i$, а $\mathcal{M}_i^\pm + \mathcal{M}_j^\pm \supseteq \mathcal{L}_i + \mathcal{L}_j = e\mathcal{S} \dot{+} b\mathcal{S}$, где $\mathcal{S} = (a-e) \lhd PH$, $\dim(\mathcal{S}) = q-2$. Таким образом, $\dim(\mathcal{N}_i) = \dim(\mathcal{L}_i + \mathcal{L}_j) = 2q-4 > \dim(\mathcal{M}_i^\pm)$, что доказывает требуемое. ■

4.5. Коммутаторные квазигруппы

Примеры неассоциативных луп, рассматриваемых в теоремах 6 и 7, можно построить с помощью коммутаторных квазигрупп, конструкция которых описывается ниже.

Конструкция и алгебраические свойства коммутаторных квазигрупп

Пусть G — конечная группа. Зафиксируем целые числа c, d и определим новое умножение на элементах G по следующему правилу:

$$x *_{c,d} y = x^{1-d} y^c x^d y^{1-c} = x[x^{-d}, y^c]y, \quad x, y \in G.$$

Получившийся группоид обозначается $(G)_{c,d}$ и называется *коммутаторным группоидом* (или *коммутаторной квазигруппой*, если он удовлетворяет определению квазигруппы) для группы G с параметрами c, d.

Утверждение 3. Обозначим через e единичный элемент G, $Z(G)$ — центр группы и $m = \exp(G/Z(G))$.

1) Если группа G удовлетворяет тождеству $[x^c, y^{d-1}] = e$ (соответственно, $[x^{c-1}, y^d] = e$), то операции в $(G)_{c,d}$ и $(G)_{c,1}$ (соответственно, в $(G)_{c,d}$ и $(G)_{1,d}$) совпадают.
2) $(G)_{0,d} = (G)_{c,0} = G \quad \forall c, d \in \mathbb{Z}$.
3) $(G)_{1,1} = G^{op}$, где G^{op} — инверсная группа.
4) $(G)_{c,d} \cong (G)^{op}_{c,d} \quad \forall c, d \in \mathbb{Z}$.
5) Если $[x, y] = e$ в G, то $x * y = xy$.
6) Если $u \equiv c \pmod m$, $v \equiv d \pmod m$, то $(G)_{u,v} = (G)_{c,d}$.
7) Пусть $m_1, \ldots, m_k$ — список всех различных порядков элементов группы G. Если $c \equiv i_k \pmod{m_k}$, $d \equiv j_k \pmod{m_k}$, где $i_k, j_k \in \{0, 1\}$, то группоид $G_{c,d}$ является лупой.

Доказательство. Пункты 1–5 доказываются простой проверкой. Докажем п. 6 и 7.

6. Пусть $u = c + kn$, $v = d + nm$. Тогда

$$[x^{-v}, y^u] = x^{-d} x^{-nm} y^c y^{km} x^d x^{nm} y^{-c} y^{-km} = x^{-d} y^c x^d x^{-nm} y^{km} x^{nm} y^{-km} = [x^{-d}, y^c],$$

так как $x^{nm}, y^{km} \in Z(G)$.

7. Покажем, что уравнения $x * a = b$, $a * y = b$ разрешимы при любых $a, b \in G$. Рассмотрим первое уравнение (второе рассматривается аналогично). Из условия следует, что $x * y \in \{xy, yx\}$, причём если $\operatorname{ord}(\tilde{x}) = \operatorname{ord}(x)$, $\operatorname{ord}(\tilde{y}) = \operatorname{ord}(y)$ и $x * y = xy$ (соответственно, $x * y = yx$), то и $\tilde{x} * \tilde{y} = \tilde{x}\tilde{y}$ (соответственно, $\tilde{x} * \tilde{y} = \tilde{y}\tilde{x}$). Если $ba^{-1} * a = b$, то положим $x = ba^{-1}$, иначе положим $x = a^{-1}b$. Получили, что $(G)_{c,d}$ является квазигруппой. Остаётся заметить, что e — её единица. ■

Пункт 6 показывает, что количество неизоморфных группоидов в множестве $(G)_{c,d}$, $c, d \in \mathbb{Z}$, есть мера некоммутативности группы G.

Группоид $(G)_{c,d}$ всегда содержит единичный элемент, но не всегда является лупой. В общем случае условия на G, c, d, которые гарантируют, что $(G)_{c,d}$ является лупой, неизвестны, но в некоторых случаях у нас есть ответ.

Коммутаторные квазигруппы для группы диэдра D_n

В табл. 1 приведены явные формулы умножения в $(D_n)_{c,d}$, которые зависят только от чётности c, d.

Таблица 1

Формулы умножения в $(D_n)_{c,d}$

Варианты	c – н, d – н	c – ч, d – н	c – н, d – ч
$a^k * a^l$	a^{k+l}	a^{k+l}	a^{k+l}
$a^k * ba^l$	$ba^{k(2d-1)+l}$	ba^{l-k}	$ba^{k(2d-1)+l}$
$ba^k * a^l$	$ba^{k+l(1-2c)}$	$ba^{k+l(1-2c)}$	ba^{k+l}
$ba^k * ba^l$	a^{k-l}	a^{l-k}	a^{l-k}

Утверждение 4. Табл. 2 показывает, при каких c и d группоид $(D_n)_{c,d}$ является лупой.

Таблица 2

$c \diagdown d$	ч, $2d-1 \in \mathbb{Z}_n^*$	ч, $2d-1 \notin \mathbb{Z}_n^*$	н, $2d-1 \in \mathbb{Z}_n^*$	н, $2d-1 \notin \mathbb{Z}_n^*$
ч, $2c-1 \in \mathbb{Z}_n^*$	+	+	+	+
ч, $2c-1 \notin \mathbb{Z}_n^*$	+	+	−	−
н, $2c-1 \in \mathbb{Z}_n^*$	+	−	+	−
н, $2c-1 \notin \mathbb{Z}_n^*$	+	−	−	−

Примечание. «+» – лупа, «−» – не лупа.

Утверждение 5. Если $c, d \in \{1, \ldots, \exp(D_n/Z(D_n)) - 1\}$, то $(D_n)_{c,d}$ — полугруппа тогда и только тогда, когда $c = d = 1$ (в этом случае $(D_n)_{c,d} = (D_n)^{op} \cong D_n$) или когда c и d оба чётные (в этом случае $(D_n)_{c,d} = D_n$).

Утверждение 6. При различных парах $c, d \in \{1, \ldots, \exp(D_n/Z(D_n)) - 1\}$, таких, что c, d оба нечётные и $2c-1, 2d-1 \in \mathbb{Z}_n^*$, соответствующие им лупы $(D_n)_{c,d}$ неизоморфны.

Доказательство. Пусть это не так и $(D_n)_{c_1,d_1} \cong (D_n)_{c_2,d_2}$, $(c_1, d_1) \neq (c_2, d_2)$, а φ — соответствующий изоморфизм. Пусть для определённости $c_1 \neq c_2$ (случай $d_1 \neq d_2$ рассматривается аналогично). Так как $(D_n)_{c_1,d_1}$, $(D_n)_{c_2,d_2}$ — лупы с ассоциативными степенями, то порядки элементов при изоморфизме сохраняются. Можно считать, что $n > 2$ (иначе группа D_n коммутативная и доказывать нечего). При $n > 2$ имеем

$$\varphi(a) = a^m,\ \varphi(a^k) = a^{mk},\ \varphi(b) = ba^l \quad (m, n) = 1.$$

Далее,

$$\varphi(ba^k) = \varphi(b *_{c_1,d_1} a^{k(1-2c_1)^{-1}}) = \varphi(b) *_{c_2,d_2} \varphi(a^{k(1-2c_1)^{-1}}) = ba^{l+m(1-2c_1)^{-1}(1-2c_2)k},$$

где $*_{c_1,d_1}$ ($*_{c_2,d_2}$) — умножение в группоиде $(D_n)_{c_1,d_1}$ ($(D_n)_{c_2,d_2}$), откуда

$$\varphi(ba^{k_1} *_{c_1,d_1} ba_2^k) = a^{m(1-2c_1)^{-1}(1-2c_2)(k_1-k_2)}.$$

С другой стороны,

$$ba^{k_1} *_{c_1,d_1} ba^{k_2} = a^{k_1-k_2},$$

поэтому

$$\forall k_1, k_2 \in \mathbb{Z}_n, m \in \mathbb{Z}_n^*\ \ a^{m(1-2c1)^{-1}(1-2c_2)(k_1-k_2)} = a^{m(k_1-k_2)},$$

значит, $1 - 2c_1 \equiv 1 - 2c_2 \pmod n$. Если n нечётное, то $c_1 \equiv c_2 \pmod n$, откуда $c_1 = c_2$, так как оба нечётные и не превосходят $2n - 1$. Если n чётное, но $4 \nmid n$, то

$c_1 = c_2 \pmod{n/2}$. Так как $n/2$ нечётное, а $\exp(D_n/Z(D_n)) - 1 = n - 1$, то $c_1 = c_2$. Наконец, если $4 \mid n$, то $c_1 \equiv c_2 \pmod{n/2}$, и так как $c_1, c_2 \leqslant n/2 - 1$, то $c_1 = c_2$. ■

Линейно оптимальные $(D_n)_{c,d}$-коды

Следующая лемма показывает, при каких значениях c и d группоид $(D_n)_{c,d}$ удовлетворяет условиям теорем 6 и 7.

Лемма 6. Пусть группоид $(D_n)_{c,d}$ является неассоциативной лупой и n — простое число. Тогда эта лупа удовлетворяет условиям 1, 2, 3 из теоремы 6.

Пусть группоид $(D_n)_{c,d} = (D_{p^l-1})_{c,d}$ является неассоциативной лупой и $n = p^l - 1$. Эта лупа удовлетворяет условиям 1, 2, 3 из теоремы 7, если и только если выполнено одно из следующих условий:

— c нечётное, d нечётное, $2c \equiv 2 \pmod{n}$;
— c чётное, d нечётное $2c \equiv 0 \pmod{n}$;
— c нечётное, d чётное.

Доказательство. Из утверждения 5 известно, что если c и d оба чётные, то группоид $(D_n)_{c,d}$ является полугруппой, поэтому такие c и d не подходят по условию.

Пользуясь формулами из табл. 1, рассмотрим оставшиеся три случая, в каждом из которых проверим выполнение условий 1, 2, 3.

1) c — нечётное, d — нечётное. По утверждению 4 имеем $2c - 1, 2d - 1 \in \mathbb{Z}_n^*$. Тогда
   а) $ba^k * a^l = ba^{k+l(1-2c)} = b * (a^{k(1-2c)^{-1}} * a^l)$;
   б) $ba^k * (b * a^l) = ba^k * ba^{l(1-2c)} = a^{k-l(1-2c)} = a^k * a^{l(2c-1)}$;
   в) $a^k * (b * a^l) = a^k * (ba^{l(1-2c)}) = ba^{k(2d-1)+l(1-2c)} = b * a^{k(2d-1)(1-2c)+l} = b * (a^{k(2d-1)(1-2c)} * a^l)$.
   Видно, что условия теоремы 7 выполнены тогда и только тогда, когда $2c - 1 \equiv 1 \pmod{n}$, а условия теоремы 6 выполнены всегда ($\dot{k} = 1$, $\ddot{k} = 2c - 1$).
2) c — чётное, d — нечётное. Согласно утверждению 4, $2c - 1 \in \mathbb{Z}_n^*$. Тогда
   а) $ba^k * a^l = ba^{k+l(1-2c)} = b * (a^{k(1-2c)^{-1}} * a^l)$;
   б) $ba^k * (b * a^l) = ba^k * ba^{l(1-2c)} = a^{l(1-2c)-k} = a^{-k} * a^{l(1-2c)}$;
   в) $a^k * (b * a^l) = a^k * (ba^{l(1-2c)}) = ba^{l(1-2c)-k} = b * a^{l-k(1-2c)^{-1}} = b * (a^{k(2c-1)} * a^l)$.
   Условия теоремы 7 выполнены тогда и только тогда, когда $1 - 2c \equiv 1 \pmod{n}$, а условия теоремы 6 выполнены всегда ($\dot{k} = 1$, $\ddot{k} = 1 - 2c$).
3) c — нечётное, d — чётное:
   а) $ba^k * a^l = ba^{k+l} = b * (a^k * a^l)$;
   б) $ba^k * (b * a^l) = ba^k * ba^l = a^{l-k} = a^{-k} * a^l$;
   в) $a^k * (b * a^l) = a^k * (ba^l) = ba^{k(2d-1)+l} = b * a^{k(2d-1)+l} = b * (a^{k(2d-1)} * a^l)$.

Лемма доказана. ■

Пусть p простое, $p > 2$, $P = \mathbb{F}_p$.

Теорема 8. Пусть $(D_p)_{c,d}$ является неассоциативной лупой и выполнено одно из следующих условий:

— c нечётное, d нечётное, существует $x \in \mathbb{Z}$, такой, что $x^2 \equiv 2c - 1 \pmod{p}$;
— c чётное, d нечётное, существует $x \in \mathbb{Z}$, такой, что $x^2 \equiv 1 - 2c \pmod{p}$;
— c нечётное, d чётное.

Тогда луповая алгебра $P(D_p)_{c,d}$ содержит по крайней мере два идеала, отвечающих линейно оптимальным $[2p, 2p - 3, 3]_p$-кодам.

Доказательство. Следует из леммы 6 и теоремы 6. ■

Пусть $q = p^l > 2$, $P = \mathbb{F}_q$.

Теорема 9. Пусть $(D_{q-1})_{c,d}$ является неассоциативной лупой и выполнено одно из следующих условий:

— c нечётное, d нечётное, $2c \equiv 2 \pmod{n}$;
— c чётное, d нечётное, $2c \equiv 0 \pmod{n}$;
— c нечётное, d чётное.

Тогда если $p > 2$ (соответственно, $p = 2$), то луповая алгебра $P(D_{q-1})_{c,d}$ содержит по крайней мере $2\varphi(q-1)$ (соответственно, $\varphi(q-1)$) идеалов, отвечающих линейно оптимальным $[2q-2, 2q-5, 3]_q$-кодам.

Доказательство. Следует из леммы 6 и теоремы 7. ■

В качестве иллюстрации к теореме 8 рассмотрим $\mathbb{F}_5(D_5)_{c,d},\ c,d \in \{1,\dots,9\}$. Табл. 3 показывает, при каких парах c и d группоиды $(D_n)_{c,d}$ являются лупами и когда эти лупы изоморфны.

Таблица 3

$c \diagdown d$	1	2	3	4	5	6	7	8	9
1	0	1	–	2	3	3	2	–	1
2	4	0	4	0	4	0	4	0	4
3	–	1	–	2	–	3	–	–	–
4	5	0	5	0	5	0	5	0	5
5	6	1	–	2	7	3	8	–	9
6	6	0	6	0	6	0	6	0	6
7	5	1	–	2	10	3	11	–	12
8	–	0	–	0	–	0	–	0	–
9	4	1	–	2	13	3	14	–	15

Примечание. «–» — не лупа; 0 — D_5;
1–15 — неассоциативные лупы.

Учитывая, что $x^2 = \pm 1$ при $x \in \mathbb{F}_5^*$, получаем, что условию теоремы 8 удовлетворяют только $\mathbb{F}_5(D_5)_{1,2},\ \mathbb{F}_5(D_5)_{1,4},\ \mathbb{F}_5(D_5)_{1,5},\ \mathbb{F}_5(D_5)_{5,1},\ \mathbb{F}_5(D_5)_{5,5},\ \mathbb{F}_5(D_5)_{5,7},\ \mathbb{F}_5(D_5)_{5,9}$.

Компьютерные вычисления показали, что среди $\mathbb{F}_5(D_5)_{c,d}$ *только* эти алгебры содержат линейно оптимальные коды. Более того, их решётка идеалов в точности совпадает с решёткой, представленной на рис. 1 (слева).

Отметим, что здесь не приведены примеры луп, порождающих $[2q, q-3, 3]_q$-коды, когда поле $\mathbb{F}_q$ не простое. Если $p = \operatorname{char}\mathbb{F}_q > 2$, то такие примеры легко построить с помощью $G_{c,d}$, где $G = \langle b\rangle_2 \leftthreetimes H$, а $H = \mathbb{Z}_p^l$ — p-элементарная группа, $bhb = h^{-1}$ для всех $h \in H$. Из того, что для всех $g_1, g_2 \in G$ либо $[g_1, g_2] = e$, либо $\langle g_1, g_2\rangle \cong D_p$, следует, что свойства таких группоидов полностью аналогичны $(D_p)_{c,d}$. В частности, для $\mathbb{F}_q G_{c,d}$ верен аналог теоремы 8.

В заключение заметим, что существуют лупы с неассоциативными степенями (а значит, не являющиеся коммутаторными квазигруппами), удовлетворяющие условиям теорем 6 или 7. Такие лупы можно построить с помощью следующей конструкции (рассматриваем теорему 6, для теоремы 7 всё аналогично). Пусть

$$H = \{e, h_1, \dots, h_{q-1}\} = Z_p^l, \quad q = p^l,$$

а $L = \{e, h_1, \dots, h_{q-1}, b, \dots, bh_{q-1}\}$ — расширение H, умножение $*$ в котором определено следующим образом:

$$h_i * h_j = h_i h_j, \quad b * h_i = bh_j, \quad be = e, \quad bh_i * hj = b * (h_i h_j),$$
$$bh_i * bh_j = \sigma(h_i)h_j, \quad h_i * bh_j = b * (\tau(h_i)h_j),$$

где σ, τ — произвольные перестановки на множестве H. При таком определении группоид $(L, *)$ является квазигруппой, а если ещё добавить условие $\tau(e) = e$, то он будет лупой, которая очевидно удовлетворяет теореме 6. Рассмотрим $(b * b) * b$ и $b * (b * b)$:

$$(b * b) * b = \sigma(e) * b = b * (\tau(\sigma(e))), \quad b * (b * b) = b * \sigma(e).$$

Если $\sigma(e) \neq e$ и $\tau(\sigma(e)) \neq \sigma(e)$, то $(b * b) * b \neq b * (b * b)$ и лупа L является лупой с неассоциативными степенями. Кроме того, поскольку $\dot{k} = \ddot{k} = 1$, в $\mathbb{F}_q L$ содержится идеал, отвечающий линейно оптимальному $[2q, 2q-3, 3]_q$-коду.

Интересно, что при $q = 3$ существуют четыре неассоциативные неизоморфные лупы, удовлетворяющие теореме 6, они же удовлетворяют и теореме 7, а следовательно, доставляют линейно оптимальные $[6, 3, 3]_3$- и $[6, 3, 3]_4$-коды. Согласно [15], этими четырьмя лупами исчерпываются все неассоциативные лупы порядка 6, доставляющие линейно оптимальные коды. Лишь одна из этих луп является коммутаторной квазигруппой, а именно $(D_3)_{1,3}$.

Авторы выражают благодарность М. М. Глухову за конструктивные предложения, а также А. М. Зубкову и А. А. Нечаеву за критические замечания, способствующие улучшению изложения.

ЛИТЕРАТУРА

1. *Росошек С. К.* Криптосистемы групповых колец // Вестник Томского госуниверситета. Приложение. 2003. № 6. С. 57–62.
2. *Белоусов В. Д.* Основы теории квазигрупп и луп. М.: Наука, 1967. 223 с.
3. *Pflugfelder H. O.* Quasigroups and Loops: Introduction. Berlin: Heldermann, 1990.
4. *Smith J. D. H.* An Introduction to Quasigroups and their Representations. Boca Raton: Chapman&Hall/CRC, 2007.
5. *Vojtechovsky P.* Generators for finite simple Moufang loops // J. Group Theory. 2003. No. 6. P. 169–174.
6. *Paige L. J.* A class of simple Moufang loops // Proc. Amer. Math. Soc. 1956. V. 7. No. 3. P. 471–482.
7. *Vojtechovsky P.* Finite simple Moufang loops // PhD thesis. Department of Mathematics, Iowa State University, Ames, 2001.
8. *Conrad P.* Generalized semigroup rings // J. Indian Math. Soc. 1957. V. 21. P. 73–95.
9. *Грибов А. В., Золотых П. А., Михалёв А. В.* Построение алгебраической криптосистемы над квазигрупповым кольцом // Математические вопросы криптографии. 2010. Т. 1. № 4. С. 23–33.
10. *Kuzucuoglu F. and Levchuk V. M.* The automorphism group of certain radical matrix rings // J. Algebra. 2001. V. 243. No. 2. P. 473–485.
11. *Magliveras S. S., Stinson D. R., and Tran van Trung.* New approaches to designing public key cryptosystem using one-way functions and trap-doors in finite groups // J. Cryptology. 2008. V. 15. No. 4. P. 285–297.
12. *МакВиллъямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
13. *Heise W. and Quattrocci P.* Informations und Codierungstheorie. Berlin; Heidelberg: Springer, 1995.
14. *Гонсалес С., Коусело Е., Марков В. Т., Нечаев А. А.* Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы // Дискретная математика. 1998. Т. 10. № 2. С. 3–29.
15. *Гонсалес С., Коусело Е., Марков В. Т., Нечаев А. А.* Групповые коды и их неассоциативные обобщения // Дискретная математика. 2004. Т. 14. № 1. С. 146–156.

16. *Brouwer A. E.* Bounds on linear codes // Handbook of Coding Theory. Amsterdam: Elsevier, 1998. P. 295–461.
17. *Grassl M.* Searching for linear codes with large minimum distance // Discovering Mathematics with Magma. Berlin; Heidelberg: Springer, 2006. V. 19. P. 287–313.
18. *Couselo E., Gonzalez S., Markov V., et al.* Some constructions of linearly optimal group codes // Linear Algebra and its Applications. 2010. No. 433. P. 356–364.
19. *Charpin P.* Les codes e Reed-Solomon en tant qu'idr̀eaux d'une alg‘ebre modulaire (French. English summary) // C. R. Acad. Sci. Paris. 1982. V. 294. No. 17. P. 597–600.
20. *Landrock P. and Manz O.* Classical codes as ideals in group algebras // Designs, Codes and Cryptography. 1992. No. 2. P. 273–285.