УДК 681.3

Э. М. Габидулин, А. А. Григорьев, Н. И. Пилипчук, И. Ю. Сысоев, А. В. Уривский, А. Л. Шишкин

Московский физико-технический институт (государственный университет)

Подпространственные коды на основе ранговой метрики – новое направление в теории кодирования

Представлен аналитический обзор работ нового направления теории кодирования, связанного с подпространственными и ранговыми кодами.

Ранговые коды были введены Э. М. Габидулиным в начале 80-х годов прошлого века [1] и к настоящему времени хорошо исследованы. Они приобрели широкую известность, дав начало новому принципу построения криптосистем с открытым ключом [2], и в связи с задачами пространственно-временного кодирования для радиоканалов с множественными антеннами [3]. В последние годы внимание привлек новый подход к организации трафика в сетях с коммутацией пакетов, эксплуатирующий идею формирования линейных комбинаций ретранслируемых пакетов в промежуточных узлах сети [4], [5], [6], [7]. Это привело к появлению новых схем сетевого кодирования и вызвало интерес к изучению подпространственных кодов, элементами которых являются конечномерные линейные пространства [8]. Была обнаружена тесная связь новых подпространственных кодов с изученными ранее ранговыми кодами, что стимулировало как определенный прорыв в теории подпространственных кодов, так и возрождение интереса к ранговым кодам.

Обзор построен следующим образом. В разделе 1 обсуждаются постановки задач кодирования для метрических пространств с хэмминговой, ранговой и подпространственной метриками. В разделе 2 приведены известные верхние границы для мощностей кодов. Здесь обсуждаются также новейшие оценки размеров списков при списочном декодировании ранговых кодов. Обзор конструкций кодов в ранговой и подпространственной метриках дан в разделе 3. Особенности алгоритмов декодирования обсуждаются в разделе 4. В разделе 5 обсуждается общее состояние дел и нерешённые проблемы.

1. Метрики и коды

Множество $\mathcal{S}$ с архимедовой метрикой $d(x,y) \geq 0$, $d(x,y) \leq d(x,z) + d(z,y)$ называется метрическим пространством. Задача построения (M,d)-кода состоит в выборе подмножества $\mathcal{C} \in \mathcal{S}$ максимальной мощности M с заданным ограничением на минимальное расстояние между его элементами:

$$d(x,y) \geq d; \quad x,y \in \mathcal{C};\, x \neq y.$$

Различные ветви теории кодирования отличаются природой обсуждаемых метрических пространств. В центре внимания любой из этих теорий находятся некоторые традиционные постановки. Прежде всего возникает задача *построения кода* максимальной мощности с заданным расстоянием или двойственная задача максимизации расстояния при заданной мощности. С позиций общей теории принципиальное значение имеют *верхние и нижние границы* для мощностей кодов, которые позволяют оценивать качество предлагаемых кодовых конструкций.

Практическое применение тех или иных кодов предполагает существование эффективных *алгоритмов* кодирования и декодирования. Под кодированием в широком смысле понимают алгоритм построения элемента кода по его номеру в некоторой заранее оговоренной нумерации. Задача декодирования ставится таким образом. Пусть предъявлен некоторый элемент $x \in \mathcal{S}$. Требуется найти элемент кода $c \in \mathcal{C}$, ближайший к x по метрике d, и указать его номер.

Если $d = 2r + 1$ и предъявленный элемент x находится на расстоянии $d \leq r$ от некоторой кодовой точки c, то есть лежит внутри шара $\mathcal{B}_r(c) = \{x : d(c, x) \leq r\}$ радиуса r, то он безошибочно декодируется по минимуму расстояния в точку c, поскольку r-шары, отвечающие разным точкам кода, заведомо не пересекаются. Величина $r = \frac{d-1}{2}$ известна как конструктивный радиус декодирования. За пределами этого радиуса, когда предъявленный элемент отстоит от всех точек кода на расстояние $d > r$, однозначное декодирование возможно не всегда. Фиксируем предъявленную точку x и будем рассматривать шары $\mathcal{B}_r(x)$ прогрессивно возрастающего радиуса $r = 0, 1, 2, \ldots$. При каком-то r в шаре впервые окажется хотя бы одна кодовая точка. Если конструктивная граница выполнена – $r \leq \frac{d-1}{2}$, то эта точка гарантированно окажется единственной. В противном случае в шаре может оказаться сразу несколько кодовых точек. Тогда потребителю выдается их полный список. О таком поведении говорят как о списочном декодировании. Перспективность списочного декодирования определяется зависимостью размера списка от радиуса r. Список имеет смысл, если его размер не слишком велик.

1.1. Коды в хэмминговой метрике

В классической теории помехоустойчивого кодирования для каналов связи с ошибками множество $\mathcal{S}_h$ – это n-мерное линейное пространство $V = F_q^n$ над полем F_q с q элементами (*q-степень простого числа*). Его элементами являются n-векторы (*кодовые слова*), которые в фиксированном базисе F_q^n над F_q представляются n-блоками $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ коэффициентов $x_j \in F_q$. Норма Хэмминга $||\mathbf{x}||_h$ блока $\mathbf{x}$ (*хэммингов вес*) вводится как число ненулевых коэффициентов в нём. Расстояние Хэмминга вводится через норму как $d_h(\mathbf{x}, \mathbf{y}) = ||\mathbf{x} - \mathbf{y}||_h$. Таким образом, введённые норма и расстояние зависят от выбора базиса.

1.2. Коды в ранговой метрике

Метрическое пространство $\mathcal{S}_r$, в котором строятся **ранговые** (n, m)-коды, — это множество F_q-линейных отображений $\varphi : F_q^n \to F_q^m$, которое является линейным пространством над F_q размерности nm. С каждым из таких отображений связаны ядро $\mathrm{Ker}(\varphi) = \{\mathrm{x} : \varphi(\mathrm{x}) = 0\}$ и образ $\mathrm{Im}(\varphi) = \{\mathrm{y} : \exists \mathrm{x}\, \varphi(\mathrm{x}) = \mathrm{y}\}$, являющиеся подпространствами в F_q^n и F_q^m. Отображение φ вполне определяет изоморфизм $F_q^n/\mathrm{Ker}(\varphi) \leftrightarrow \mathrm{Im}(\varphi)$. Норма (ранг) отображения φ вводится как размерность пространств, связанных этим изоморфизмом:

$$||\varphi||_r = \mathrm{rank}\, \varphi = \dim(\mathrm{Im}(\varphi)) = \dim(\mathrm{F_q^n}/\mathrm{Ker}(\varphi)) = \mathrm{n} - \dim(\mathrm{Ker}(\varphi)).$$

Эта норма задаёт ранговое расстояние между отображениями: $d_r(\varphi_1, \varphi_2) = \mathrm{rank}(\varphi_1 - \varphi_2)$. Ранговые норма и расстояние определены инвариантно – безотносительно к выбору какого-либо базиса.

Концепция ранговой метрики была введена Лу-Кенг Хуа (Loo-Keng Hua) [9] в 1951 году как «Арифметическое расстояние». Позднее, в 1978 году, Филипп Дельсарт (Philippe Delsarte) [10] дал эквивалентное определение рангового расстояния (q-расстояние) над множеством билинейных форм, эквивалентном множеству прямоугольных матриц.

Пусть в пространстве F_q^n зафиксирован базис $(e_1, e_2, \ldots, e_n)$. F_q-линейное отображение φ вполне определяется набором $(a_1, a_2, \ldots, a_n)$, $a_j = \varphi(e_j) \in F_q^m$ образов элементов базиса. Ранг отображения φ – это размерность линейной оболочки множества образов a_j, то есть число линейно независимых векторов из F_q^m в наборе $(a_1, a_2, \ldots, a_n)$.

Если зафиксировать базис также и в пространстве образов F_q^m, то каждый из образов a_j станет m-вектор-столбцом $a_{1,j}, a_{2,j}, \ldots, a_{m,j}$, и строка образов $(a_1, a_2, \ldots, a_n)$ окажется $n \times m$-матрицей над F_q:

$$\begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{1,2} & \dots & a_{1,n} \\ & & \dots & \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{vmatrix}.$$

Ранг отображения φ равен рангу этой матрицы, то есть числу линейно независимых столбцов в ней. При фиксированных базисах в F_q^n и F_q^m соответствие между F_q-линейными отображениями φ и $n \times m$-матрицами $\{a_{j,k}\}$ взаимно однозначно. Это приводит к матричному представлению линейного пространства, в котором конструируются ранговые коды. В этом представлении элементами кодов являются $n \times m$-матрицы над F_q. Ранг элемента равен рангу матрицы. Соответственно расстояние d_r между матрицами – это ранг их покомпонентной разности.

Пространство-образ F_q^m можно наделить структурой поля F_{q^m} – алгебраического расширения поля F_q степени m. Тогда строка образов $(a_1, a_2, \dots, a_n)$ станет элементом пространства $F_{q^m}^n$ n-векторов над расширенным полем F_{q^m}. Так формируется векторное представление пространства ранговых кодов. Ранг его элемента – это число координат, линейно независимых над расширенным полем. Расстояние между элементами – это ранг их разности. Впервые ранговое расстояние для векторных пространств над расширенными полями было введено Габидулиным в работе [1] 1985 года. Им же была выявлена связь между матричным и векторным представлениями.

Ранговый $(n, m, M, d)_r$-код – это подмножество $\mathcal{C}$ пространства $\mathcal{S}_r$ мощности M с минимальным расстоянием $d = d_r$ между элементами. Его можно рассматривать как в матричном, так и в вектором представлении. Код F_q линеен, если подмножество $\mathcal{C}$ является линейным F_q-подпространством в $\mathcal{S}_r$. Мощность линейного кода определяется размерностью этого подпространства $k < nm$ и составляет $M = q^k$.

Векторное представление позволяет рассматривать F_{q^m}-линейные коды как линейные подпространства в пространстве $F_{q^m}^n$. Мощность такого кода F_{q^m}-размерности k_m равна $M = (q^m)^{k_m} = q^{mk_m}$. Очевидно, что любой F_{q^m}-линейный код линеен также и над F_q. Однако обратное неверно. В матричном представлении F_{q^m}-линейность кода означает его инвариантность относительно умножения всех столбцов матрицы, рассматриваемых как базисные разложения элементов F_{q^m}, на произвольный элемент расширенного поля F_{q^m}, а не только на скаляр из F_q.

1.3. Подпространственные и грассмановы коды

Подпространственные коды строятся во множестве $\mathcal{S}_g$ всех конечномерных линейных пространств F_q^m, $0 \le m \le n$ над F_q, вложенных в n-мерное объемлющее пространство F_q^n. Элементы этих кодов – это конечномерные пространства размерностей от 0 до n.

Для любых двух пространств U и V из $\mathcal{S}_g$ существует нижняя грань $\inf(U, V) = U \cap V$ (*пересечение пространств*) и верхняя грань $\sup(U, V) = U \cup V$ (*линейная оболочка объединения*), которые наделяют множество пространств структурой решетки (*решетки Грассмана*). На решетке Грассмана существует архимедова метрика:

$$\begin{aligned} d_g(U, V) &= \dim(\sup(U, V)) - \dim(\inf(U, V)) = \dim(U \cup V) - \dim(U \cap V) = \\ &= \dim U + \dim V - 2\dim(U \cap V) = \\ &= 2\dim(U \cup V) - \dim U - \dim V. \end{aligned}$$

Подобно ранговой, эта метрика инвариантна, но в отличие от ранговой она не ассоциирована с какой-либо нормой на $\mathcal{S}_g$.

Пусть $(e_1, e_2, \dots, e_n)$ – фиксированный базис объемлющего пространства F_q^n. Рассмотрим некое m-подпространство $V \in F_q^n$. Пусть векторы $(v_1, v_2, \dots, v_m)$ образуют

его базис. Разложения $v_i = \sum_{j=1}^{n} a_{i,j} e_j$ приводят к представлению подпространства V линейной оболочкой строк F_q-матрицы:

$$\mathbf{V} = \begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \dots & a_{1,n} \\ a_{2,1} & a_{1,2} & a_{2,3} & \dots & a_{1,n} \\ & & \dots & & \\ a_{m,1} & a_{m,2} & a_{m,3} & \dots & a_{m,n} \end{vmatrix}.$$

Подобно элементу рангового кода, m-подпространство V представлено $m \times n$-матрицей V над F_q. Однако в отличие от ранговых кодов это представление не взаимно однозначно. То же самое пространство V можно задать линейной оболочкой иного базиса $(u_1, u_2, \dots, u_m)$, связанного с исходным линейным преобразованием с невырожденной $m \times m$-матрицей $\mathbf{O}$. Это означает, что матрицы $\mathbf{V}$ и $\mathbf{OV}$ представляют одно и то же подпространство. Иначе определяется и расстояние между подпространствами U, V по их матричным представлениям $\mathbf{U}$, $\mathbf{V}$:

$$d_g(U,V) = 2\dim(U \cup V) - \dim U - \dim V = 2\,\mathrm{rank} \begin{vmatrix} \mathbf{U} \\ \mathbf{V} \end{vmatrix} - \mathrm{rank}\mathbf{U} - \mathrm{rank}\mathbf{V}.$$

Подпространственный код $\mathcal{C}_g$ с параметрами (M, d) – это подмножество решётки $\mathcal{S}_g$ мощности M с минимальным расстоянием d.

Если в пространстве F_q^n прямые $\{\lambda x,\ \lambda \in F_q\}$ отождествить с точками, пользуясь эквивалентностью $x \sim \lambda x$, $\lambda \in F_q$, то это пространство становится проективной геометрией $PG_q(n-1)$. В проективной геометрии прямые из F_q^n становятся точками, а m-мерные подпространства F_q^m — $(m-1)$-мерными проективными плоскостями. Одномерные плоскости — образы пространств F_q^2 — называют проективными прямыми, нульмерные пространства — точками. Для проективных плоскостей U, V сохраняются понятия нижней грани $\inf(U,V)$ (*пересечение плоскостей*) и верхней грани $\sup(U,V)$ (*наименьшая плоскость, включающая объединение двух плоскостей*). Расстояние между плоскостями определяется так же, как и между пространствами:

$$d_P(U,V) = \dim(\sup(\mathrm{U},\mathrm{V})) - \dim(\inf(\mathrm{U},\mathrm{V})),$$

где dim – проективная размерность. Расстояние между подпространствами совпадает с расстоянием между отвечающими им проективными плоскостями.

Переход в проективное пространство позволяет сформулировать задачу пространственного кодирования как проблему проективной геометрии: нужно выбрать набор проективных плоскостей с заданным минимальным расстоянием между ними.

Какие-либо содержательные результаты относительно кодов на решётках Грассмана на данный момент практически отсутствуют. В центре внимания исследований находится более простая задача описания кодов, состоящих из пространств фиксированной размерности.

Подмножество грассмановой решетки, включающее все подпространства фиксированной размерности m, известно как грассманиан $\mathcal{G}_q(n,m)$. Решётка является объединением грассманианов $\mathcal{G}_q(n,m)$ с m от 0 до n. Число элементов грассманиана выражается гауссовским биномиальным коэффициентом:

$$|\mathcal{G}_q(n,m)| = W(n,m) = \begin{bmatrix} n \\ m \end{bmatrix} = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{m-1})}{(q^m-1)(q^m-q)\dots(q^m-q^{m-1})}.$$

Выражения для расстояний между подпространствами грассманиана $\mathcal{G}_q(n,m)$ упрощаются:

$$\begin{aligned} d_g(U,V) = 2\delta(U,V) &= 2\,(m - 2\,\dim(U \cap V)) = \\ &= 2\,(\dim(U \cup V) - m). \end{aligned}$$

Значения всех расстояний чётны ($d_g = 2\delta$) и лежат в диапазоне от 0 до $2n$ ($\delta \in [0, n]$).

Грассманов (n, m, M, δ)-код – это подмножество элементов $\mathcal{G}_q(n, m)$ мощности M с минимальным расстоянием $d = 2\delta$. В геометрической интерпретации это семейство $(m-1)$-плоскостей в $PG_q(n-1)$ с максимальной размерностью пересечения $\dim(U \cup V) = m - \delta$. Ограничение грассманианом переводит задачу кодирования в разряд типовых для проективной геометрии проблем инцидентности, то есть проблем оценивания размерностей пересечений геометрических объектов. Простейшая задача этого рода связана с изучением **спредов** – покрытий проективного пространства $PG_q(n-1)$ непересекающимися $(m-1)$-плоскостями. Каждое такое покрытие образует (n, m, M, m)-код с максимальным для грассманиана $\mathcal{G}_q(n, m)$ расстоянием $\delta = m$.

С каждым (n, m, M, δ)-кодом на грассманиане $\mathcal{G}_q(n, m)$ ассоциирован двойственный $(n, n-m, M, \delta)$-код на грассманиане $\mathcal{G}_q(n, n-m)$. Он образован дополнениями $U^\perp$ ко всем подпространствам U из кода (n, m, M, δ). Факт сохранения расстояния при переходе к дополнениям легко проверяется:

$$\begin{aligned}\delta(U^\perp, V^\perp) &= \dim(U^\perp \cup V^\perp) - (n-m) = \dim(U \cap V)^\perp - (n-m) = \\ &= n - \dim(U \cap V) - (n-m) = m - \dim(U \cap V) = \\ &= \delta(U, V).\end{aligned}$$

Возможность перехода к дополнениям позволяет ограничиться изучением кодов на грассманианах $\mathcal{G}_q(n, m)$ с $m \le \lceil (n+1)/2 \rceil$.

1.4. Связь грассмановых и ранговых кодов

В работе [11] 2008 года тремя авторами — Силвой (Silva), Кёттером (Koetter) и Кшишангом (Kshischang) — предложена лифтинговая конструкция, которая обеспечила прорыв в конструктивной теории пространственных кодов, установив их связь с ранговыми кодами. Это позволило построить широкий класс пространственных кодов, известных ныне как коды SKK (первые буквы фамилий авторов).

Пусть в пространстве F_q^n зафиксированы подпространство $V_m = F_q^m$ и его дополнение $V_{n-m} = F_q^{n-m}$, $(V_m \cap V_{n-m} = 0)$. Рассмотрим пространство $\mathcal{S} = \{\varphi : V_m \to V_{n-m}\}$ линейных отображений V_m в V_{n-m}. С каждым из этих отображений φ свяжем его график – пространство $U_\varphi = \{x + \varphi(x),\, x \in V_m\}$. Размерность графика U_φ равна m. Действительно, размерность не меньше m, поскольку размерность проекции U_φ на V_m, совпадающая с V_m, составляет m, но и не больше m, поскольку нулю в пространстве V_m отвечает нуль в U_φ.

Изучим размерность пересечения двух графиков U_{φ_1} и U_{φ_2}. Для всякого элемента u этого пересечения возможны два представления $u = x_1 + \varphi_1(x_1) = x_2 + \varphi_1(x_2)$. Проекция u на V_m с одной стороны равна x_1, а с другой – x_2. Поэтому $x_1 = x_2$. Таким образом,

$$U_{\varphi_1} \cap U_{\varphi_2} = \{x + \varphi_1(x) : \varphi_1(x) = \varphi_2(x)\} = \{x + \varphi_1(x) : x \in Ker(\varphi_1 - \varphi_2)\}$$

Следовательно,

$$\dim(U_{\varphi_1} \cap U_{\varphi_2}) = \dim \mathrm{Ker}(\varphi_1 - \varphi_2) = \mathrm{m} - \mathrm{rank}(\varphi_1 - \varphi_2),$$

а

$$\delta(U_{\varphi_1}, U_{\varphi_2}) = \mathrm{rank}(\varphi_1 - \varphi_2).$$

Таким образом, δ-расстояние между графиками двух отображений равно рангу разности этих отображений. Это сводит задачу построения пространственного кода на множестве графиков отображений к задаче построения рангового кода в линейном пространстве этих отображений.

Множество $\{U_\varphi\}$ графиков отображений $\varphi : V_m \to V_{n-m}$ не покрывает весь грассманиан $\mathcal{G}_q(n, m)$. В него входят только те подпространства из $\mathcal{G}_q(n, m)$, проекции которых

на выделенное подпространство V_m совпадают с V_m. На множество графиков можно перенести линейную структуру пространства отображений, объявив суммой пространств U_{φ_1}, U_{φ_2} пространство $U_{\varphi_1+\varphi_2}$. Это делает множества $\{U_\varphi\}$ аффинными картами q-размерности $n(n-m)$ и позволяет трактовать коды SKK как коды, заданные на аффинной карте грассманиана. Весь грассманиан покрывается с пересечениями аффинными картами, отвечающими разным подпространствам V_m.

2. Границы для мощностей кодов

Для мощности M рангового кода над F_q с параметрами (n, m, M, d) справедлива граница Синглтона [1]:

$$M \leq \min(q^{m(n-d+1)}, q^{n(m-d+1)}).$$

Известны конструкции оптимальных q-линейных ранговых кодов, достигающие этой границы. При $n \geq m$ асимптотическая по $m \to \infty$ форма этой границы имеет вид: $R \leq 1 - \delta$, где $R = \frac{\log_q M}{mn}$, $\delta = \frac{\delta}{m}$. Известна также и нижняя граница на относительное расстояние δ, условно называемая границей Варшамова–Гильберта [20] (далее — ВГ-граница): при $b \to \text{const}$ для любого $\delta \leqslant \min(1, b^{-1})$ существует код со скоростью $R \geqslant (1-\delta)(1-b\delta)$.

К этим границам имеют отношение новейшие результаты исследования размеров списков при списочном декодировании ранговых кодов. Пусть $L(\varrho)$ – число кодовых точек в шаре относительного рангового радиуса $\varrho = \frac{r}{m}$. В [22] получена оценка снизу на размер списка: $L \geqslant q^{Nn(R+\rho-1)}$. Она показывает, что при $R > 1 - \rho$, то есть когда радиус декодирования лежит выше границы Синглтона, списочное декодирование невозможно. Более точная оценка в той же работе показывает, что $L \geqslant q^{Nn(R-(1-\rho)(1-b\rho))}$. Таким образом, полиномиальное списочное декодирование *невозможно* при $R > (1-\rho)(1-b\rho)$, то есть в случае, если радиус декодирования лежит выше ВГ-границы.

Рассмотрим, что происходит ниже ВГ-границы. Оказывается [22], что для любого малого $0 < \varepsilon < 1$ случайно выбранный код со скоростью $R = (1-\rho)(1-b\rho) - \varepsilon$ декодируется в список размера $L = O(1/\varepsilon)$ с вероятностью, не меньшей значения $1 - q^{-Nn}$. Это означает, что *почти все* коды, радиус декодирования которых находится ниже ВГ-границы, могут декодироваться в список. Однако в этой области существуют и плохо декодируемые коды [21]: для $\frac{\delta}{2} < \rho < \delta$ и $\rho \leqslant 1/2$ *существует* код, для которого $L \geqslant q^{n^2(1-\rho)(\rho-\frac{\delta}{2})}$.

Верхняя граница мощности M грассманового кода над $\mathcal{G}_q(n, m)$ с параметрами $(n, m, M, d = 2\delta)$ получена в 2003 году в работе [12] (здесь и далее используем обозначение M_W):

$$M_W \leqslant \frac{|W(n, m-\delta+1)|}{|W(m, m-\delta+1)|} = \frac{\begin{bmatrix} n \\ m-\delta+1 \end{bmatrix}}{\begin{bmatrix} m \\ m-\delta+1 \end{bmatrix}}. \tag{1}$$

Это граница упаковки, построенная из простых соображений. Если расстояние между m-пространствами не меньше 2δ, то размерность их пересечения составляет как максимум $(m-\delta)$. Это означает, что всякое подпространство размерности $(m-\delta+1)$ не может быть вложено сразу в два кодовых подпространства. Число M_W кодовых подпространств оценивается тогда сверху делением общего числа $(m-\delta+1)$-пространств на число таких подпространств в подпространстве размерности m.

Две другие верхние границы, названные в работе [13] 2009 года Johnson I и Johnson II, здесь обозначим M_{JI} и M_{JII} соответственно. Граница M_{JI} устанавливает ограничения на длины кодовых слов в зависимости от кодового расстояния и размерности. Она определяет мощность для оптимальных подпространственных кодов и соответствующих им двойственных кодов. В случае двойственных кодов она является более точной, а для основных оптимальных кодов совпадает с границей M_W:

$$M_{JI} \leqslant \left\lfloor \frac{(q^m - q^{m-\delta})(q^n-1)}{(q^m-1)^2-(q^n-1)(q^{m-\delta}-1)} \right\rfloor \text{ при } (q^m-1)^2 - (q^n-1)(q^{m-\delta}-1) > 0\ . \tag{2}$$

Граница M_{JII} использует ограничения, связанные с целочисленностью значений кодовых слов, поэтому в некоторых неоптимальных случаях является более точной, чем M_W. При оптимальных параметрах $m = \delta$ все три границы совпадают.

$$M \leqslant \left\lfloor \frac{q^n-1}{q^m-1} \left\lfloor \frac{q^{n-1}-1}{q^{m-1}-1} \left\lfloor \dots \left\lfloor \frac{q^{n-m+\delta}-1}{q^\delta-1} \right\rfloor \dots \right\rfloor \right\rfloor \right\rfloor .$$

3. Конструкции кодов

3.1. Коды Габидулина

Широко известны оптимальные ранговые коды [1], именуемые кодами Габидулина. Их конструкция напоминает конструкцию кодов Рида–Соломона для хэммингова метрики. Рассматривается множество q-линейных отображений $\varphi : F_q^n \mapsto F_q^n$ n-мерного линейного пространства над F_q в себя. Это множество является линейным пространством и даже алгеброй, если умножение отображений определить как их композицию. Если в пространстве F_q^n введена структура расширенного поля F_{q^n}, то алгебра линейных отображений становится изоморфной алгебре линеаризованных многочленов:

$$\varphi_{\mathbf{a}}(x) = \sum_{j=0}^{n-1} a_j\, x^{q^j};\ \mathbf{a} = (a_0, \dots, a_{n-1}),\ a_j \in F_{q^n}$$

с композицией $\varphi_1\varphi_2(x) = \varphi_1(\varphi_2(x))$ в качестве умножения.

Множество корней линеаризованного многочлена, замкнутое относительно сложения, является линейным подпространством в F_{q^n}. Многочлен $\varphi_{\mathbf{a}}(x)$, $\mathbf{a} = (a_0, \dots, a_{k-1})$ q-степени $(k-1)$ (*степени* q^{k-1}) имеет q^{k-1} корней. То есть пространство его корней, являющееся ядром отображения $\varphi_{\mathbf{a}}(x)$, $(k-1)$-мерно. Следовательно, ранг отображения $\varphi_{\mathbf{a}}$ составляет $\mathrm{rank}(\varphi_{\mathbf{a}}) = \mathrm{n} - \dim(\varphi_{\mathbf{a}}) = \mathrm{n} - \mathrm{k} + 1$.

Ранговый код Габидулина – это множество отображений $\varphi_{\mathbf{a}}(x)$ q-степени не выше $(k-1)$. Его минимальное ранговое расстояние составляет $d_r = n - k + 1$, а мощность $M = q^{nk}$. Так что этот код оптимален, поскольку лежит на границе Синглтона.

Рассмотрим код Габидулина в векторном представлении. Зафиксируем базис $(e_1, e_2, \dots, e_n)$ в F_{q^n}. Множество образов этого базиса при отображениях $\varphi_{\mathbf{a}}$

$$(\varphi_{\mathbf{a}}(e_1), \dots, \varphi_{\mathbf{a}}(e_n)) = \mathbf{a}G = (a_0, a_1, \dots, a_{k-1}) \begin{vmatrix} e_1 & e_2 & e_3 & \dots & e_n \\ e_1^q & e_2^q & e_3^q & \dots & e_n^q \\ e_1^{q^2} & e_2^{q^2} & e_3^{q^2} & \dots & e_n^{q^2} \\ & & & \dots & \\ e_1^{q^{k-1}} & e_2^{q^{k-1}} & e_3^{q^{k-1}} & \dots & e_n^{q^{k-1}} \end{vmatrix}$$

оказывается линейным пространством, натянутым на строки $(k \times m)$-порождающей матрицы G. Матричную форму кода образует представление элементов кодовых блоков вектор-столбцами в базисе над F_q.

Кодирование кода Габидулина в этой форме – это умножение блока информационных символов $\mathbf{a} = (a_0, a_q, \dots, a_{k-1})$ на порождающей матрицу G с последующим представлением символов полученного кодового n-вектора в F_q-базисе.

Известна двойственная форма представления векторов этого кода как элементов $\mathbf{c} = (c_1, c_2, \dots, c_n)$ нулевого пространства проверочной $(n-k \times n)$ матрицы H:

$$\begin{vmatrix} h_1 & h_2 & h_3 & \dots & h_n \\ h_1^q & h_2^q & h_3^q & \dots & h_n^q \\ h_1^{q^2} & h_2^{q^2} & h_3^{q^2} & \dots & h_n^{q^2} \\ & & & \dots & \\ h_1^{q^{n-k-1}} & h_2^{q^{n-k-1}} & h_3^{q^{n-k-1}} & \dots & h_n^{q^{n-k-1}} \end{vmatrix} \begin{vmatrix} c_1 \\ c_2 \\ c_3 \\ \dots \\ c_n \end{vmatrix} = 0.$$

Строки порождающей матрицы лежат в нулевом пространстве проверочной: $HG^T = 0$.

Для заданных проверочной матрицей кодов используется систематическое кодирование. В матрице H выделяется невырожденная квадратная $(n-k \times n-k)$-матрица H_I и её $(n-k \times k)$-дополнение H_P: $H = H_I H_P$. Проверочная часть $\mathbf{c}$ кодового вектора $\mathbf{u} = \mathbf{ci}$ определяется по информационной части $\mathbf{i}$ как решение уравнения $H_I\mathbf{c} + H_P\mathbf{i} = 0$.

Первые конструкции матричных ранговых кодов были даны Дельсартом [10] еще в 1978 году в ходе исследования билинейных квадратичных форм. Матричная форма этих кодов имеет вид $\mathcal{M} = \left\{M(\mathbf{u}) = [M_{ij}(\mathbf{u})] : \mathbf{u} \in \mathbb{F}_{q^N}^{n-d+1}\right\}$, где

$$M_{ij}(\mathbf{u}) = \mathrm{Tr}\left(\sum_{s=0}^{n-d} u_s \omega_i \mu_j^{q^s}\right).$$

Здесь $(\omega_1, \ldots, \omega_n)$ — базис F_{q^n}, $(\mu_1, \ldots, \mu_m)$ — вектор из $m \le n$ линейно независимых элементов из F_{q^n}, $(u_0, \ldots, u_{m-d})$ – информационный вектор из $F_{q^n}^{m-d+1}$, а $\mathrm{Tr}(x) = \sum\limits_{l=0}^{n-1} x^{q^l}$ – след из F_{q^n} в F_q.

$\mathcal{M}$ — это ранговый код с расстоянием d на границе Синглтона $|\mathcal{M}| = q^{n(m-d+1)}$.

Пусть $A_r(n,d),\ r = 0, 1, \ldots, n,$ — число кодовых матриц ранга r. Тогда

$$A_r(n,d) = \begin{cases} 1, & \text{if } r = 0; \\ 0, & \text{if } r = 1, \ldots, d-1; \\ \begin{bmatrix} n \\ r \end{bmatrix} \sum\limits_{s=0}^{r-d} (-1)^s \begin{bmatrix} r \\ s \end{bmatrix} q^{\frac{s(s-1)}{2}} (q^{N(d-r+1-s)} - 1), & \text{if } r = d, \ldots, n. \end{cases}$$

где $\begin{bmatrix} n \\ r \end{bmatrix} = \prod\limits_{j=0}^{r-1} \frac{q^n - q^j}{q^r - q^j}$ – гауссов биномиальный коэффициент.

3.2. Грассмановы коды

Наиболее общие конструкции грассмановых кодов эксплуатируют заимствованное из алгебраической теории грассмановых многообразий разбиение $\mathcal{G}_q(n,m)$ на непересекающиеся подмножества, известные как ячейки Шуберта. Разбиение это зависит от выбора базиса $(e_1, e_2, \ldots, e_n)$ в объемлющем линейном пространстве F_q^n. Фиксация базиса задаёт флаг – набор вложенных подпространств

$$0 = V_0 \subset V_1 \subset V_2 \subset V_3 \subset \ldots \subset V_{n-1} \subset V_n = F_q^n; \quad \dim V_j = j$$

возрастающей размерности. Подпространство $V_j, j = [1,n]$ определяется как линейная оболочка базисных векторов $(e_1, \ldots, e_j)$.

Всякое m-мерное линейное подпространство $U \in \mathcal{G}_q(n,m)$ каким-то образом пересекается с подпространствами из флага. Целочисленная последовательность $s_j = \dim(U \cap V_j)$, $j = [0,n]$ размерностей этих пересечений не убывает, нарастая на отрезке $[0,n]$ от 0 до m на единицу на каждом этапе. Набор $\mathbf{j} = (j_{i_1}, j_{i_2}, \ldots, j_{i_m})$ значений индекса $j \in [1,n]$, при которых размерность пересечения возрастает на единицу, составляет мультииндекс $\mathbf{j}(U)$ подпространства U. Двоичный n-вектор $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ с единицами в позициях с номерами из мультииндекса $\mathbf{j}$ образует двоичный мультивектор $\mathbf{v}(U)$ хэммингового веса m. Соответствие между мультивекторами и мультииндексами взаимно однозначно. Множество мультивекторов — это множество двоичных n блоков фиксированного веса m. Его мощность равна $\begin{pmatrix} n \\ m \end{pmatrix}$. Всякому m-мерному подпространству $U \in \mathcal{G}_q(n,m)$ отвечает вполне определенный мультивектор $\mathbf{v}(U)$.

Ячейка Шуберта $\mathcal{S}_{\mathbf{b}} = \{U \in \mathcal{G}_q(n,m) : \mathbf{v}(U) = \mathbf{v}\}$ — это подмножество элементов грассманиана, обладающих мультивектором $\mathbf{v}$. Грассманиан расщепляется в объединение $\begin{pmatrix} n \\ m \end{pmatrix}$ непересекающихся ячеек Шуберта $\mathcal{S}_{\mathbf{v}}$ с различными мультивекторами.

Судить о мощностях ячеек Шуберта позволяет матричное представление элементов грассманиана. Пусть подпространству $U \in \mathcal{G}_q(n,m)$ отвечает мультивектор $\mathbf{v}$ с мультииндексом $\mathbf{j} = (j_{i_1}, j_{i_2}, \ldots, j_{i_m})$. Тогда $\dim(U \cap V_j) = 0$, $j < j_{i_1}$, $\dim U \cap V_{j_{i_1}} = 1$. Это значит, что первой из прямых λe_j, $\lambda \in F_q$ с направляющими векторами e_j, $j = 1, 2, \ldots$, которая пересекается с U, является прямая с вектором $e_{j_{i_1}}$. Таким образом, базисный вектор v_1 пространства U над F_q^n можно выбрать в виде $v_1 = (0, 0, 0, 1, *, *, \ldots, *)$ с лидирующей единицей в позиции j_{i_1} и произвольными элементами из F_q в позициях со «звездочками». Размерность пересечения $(U \cap V_j)$ возрастает до значения 2 при $j = j_{i_2}$. Следовательно, второй базисный вектор U можно выбрать в виде $v_1 = (0, 0, 0, 0, 0, 1, *, *, \ldots, *)$ с лидирующей единицей в позиции j_{i_2}. Действуя таким же образом далее, придем к матричному представлению U в форме

$$U = \begin{bmatrix} 0 & 1 & * & * & * & * & * & * & * & \ldots & * \\ 0 & 0 & 1 & * & * & * & * & * & * & \ldots & * \\ 0 & 0 & 0 & 0 & 0 & 1 & * & * & * & \ldots & * \\ & & & & & & & & & \ldots & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & \ldots & * \end{bmatrix}.$$

В каждой строке этой $(m \times n)$-матрицы имеется единственная лидирующая единица, слева от которой стоят нули, а справа — произвольные элементы F_q (звёздочки). Столбцы с лидирующими единицами составляют квадратную $(m \times m)$ верхнетреугольную матрицу. Операциями над строками, то есть умножением матрицы U слева на невырожденную квадратную матрицу, эта верхнетреугольная матрица преобразуется в единичную. Это дает представление пространства U с вектор-индексом $\mathbf{v}$ в канонической **привёденной ступенчатой** форме:

$$U = \begin{bmatrix} 0 & 1 & 0 & * & * & 0 & * & 0 & * & \ldots & * \\ 0 & 0 & 1 & * & * & 0 & * & 0 & * & \ldots & * \\ 0 & 0 & 0 & 0 & 0 & 1 & * & 0 & * & \ldots & * \\ & & & & & & & & & \ldots & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & \ldots & * \end{bmatrix}.$$

Соответствие между подпространствами $U \in \mathcal{G}_q(n,m)$ и $(m \times n)$-матрицами в приведённой ступенчатой форме взаимно однозначно. Положение лидирующих единиц (*и положение столбцов единичной подматрицы*) приведённой ступенчатой формы вполне определяется мультивектором $\mathbf{v}(U)$. Исключение столбцов единичной матрицы и лидирующих тождественно нулевых столбцов даёт представление приведённой ступенчатой формы таблицей (диаграммой) Феррера [15]:

$$\mathcal{F}(U) = \begin{bmatrix} * & * & * & * & \ldots & * \\ * & * & * & * & \ldots & * \\ 0 & 0 & * & * & \ldots & * \\ & & & & \ldots & * \\ 0 & 0 & 0 & * & \ldots & * \end{bmatrix}.$$

Структура таблицы Феррера однозначно определяет структуру приведённой ступенчатой формы – перед каждым столбцом таблицы, где число звездочек возрастает на l, вставляем l столбцов единичной матрицы, после чего увеличиваем горизонтальный размер матрицы до n вставкой нуль-столбцов слева.

Число подпространств в ячейке Шуберта $\mathcal{S}_{\mathbf{q}}$ составляет $q^{|\mathcal{F}|}$, где $|\mathcal{F}|$ – число звездочек в таблице Феррера. Наибольшей мощностью $q^{(m\times(n-m))}$ обладает ячейка с $\mathbf{v} = (1, \ldots, 1, 0, 0, \ldots, 0)$ (*все m единиц в начале*), наименьшей мощностью 1 – ячейка с $\mathbf{q} = (0, \ldots, 0, 0, 0, 1, \ldots, 1)$ (*все m единиц в конце*).

Коды SKK [11] строятся лифтингом – заменой $m \times (n-m)$-матрицы звёздочек в приведённой ступенчатой форме, отвечающей мультииндексу $\mathbf{v} = (1, \ldots, 1, 0, 0, \ldots, 0)$,

$(m \times n - m)$-матрицами рангового кода с ранговым расстоянием d_r. Это дает грассманов (n, m, M, δ)-код с $M = q^{\min[m(n-\delta), n(m-\delta)]}$ и подпространственным расстоянием $\delta = d_g/2 = d_r$. Все элементы SKK-кода лежат в одной аффинной карте на $\mathcal{G}_q(n, m)$. Поэтому они заведомо не оптимальны. Их мощности уступают верхним границам (1), (2).

Подпространства, лежащие на аффинной карте, выделены тем, что они имеют непустое пересечение с подпространством V_m, натянутым на базисные векторы $(e_1, \ldots, e_m)$. Подпространства, имеющие нулевое пересечение с V_m, целиком лежат в его дополнении – пространстве V_{n-m}. Их можно интерпретировать как элементы меньшего грассманиана $\mathcal{G}_q(n-m, m) \in \mathcal{G}_q(n, m)$, имеющего нулевое пересечение с аффинной картой, и применить к нему конструкцию SKK. Эту процедуру можно продолжать итеративно до тех пор, пока $n - lm \geq m$. Эта идея, принадлежащая Габидулину и Боссерту [14], дала начало многочисленным конструкциям многокомпонентных кодов. При $n = lm$ матрицы этих кодов имеют регулярную структуру

$$U = \Big| O_{m\times m} | \ldots | O_{m\times m} | I_{m\times m} | R_{m\times n-lm} \Big|,$$

где O – нуль матрицы в количестве $l > 0$, I – единичная матрица, а R – матрица рангового кода. При максимальном расстоянии $\delta = m$ мощность такого кода составляет $M = \frac{q^{lm}-1}{q^m-1}$, достигая границы (1). Эти коды эквиваленты спредам – покрытиям проективного пространства непересекающимися $(m-1)$-плоскостями. Если m – не делитель n, то горизонтальный размер последнего рангового кода составляет $n \mod m$. При максимальном расстоянии такая конструкция приводит к частичным покрытиям проективного пространства (частичным спредам).

Мощность такого кода вычисляется по формуле

$$M = q^{(l-1)m+s} + q^{(l-2)m+s} + \cdots + q^{m+s} + 1, \tag{3}$$

где $n = lm + s$, $s < m$.

Эффективность кода разумно оценить отношением его мощности к мощности, определяемой верхней границей (1). Эффективность кодов Габидулина–Боссерта достигает 1 при $\delta = m$ и $n = lm$, то есть когда они оказываются спредами, и превышает эффективность кодов SKK при всех параметрах.

Известна более изящная алгебраическая конструкция спредов. В поле F_{q^n} выделим подпространство $U = F_q^m = F_{q^m}$, являющееся подполем. Это возможно, только когда m – делитель n. Сдвиги $\alpha^j U$ этого подпространства вдоль циклической орбиты примитивного элемента α поля F_{q^n} над F_{q^m} не пересекаются, являются линейными m-пространствами и покрывают все пространство F_q^n. Набор этих сдвигов даёт спред — грассманов код мощности $M = (q^n - 1)/(q^m - 1)$ с $\delta = m$, лежащий на границе (1).

Развитие идеи многокомпонентного кодирования на вложенных подграссманианах приводит к кодированию на ячейках Шуберта. Переход к этим ячейкам связан с решением двух проблем. Во-первых, при построении таких кодов требуются оценки расстояний между элементами различных ячеек. Кроме того, таблицы Феррера ячеек Шуберта обычно не прямоугольны. Это требует обобщения конструкций ранговых кодов для таблиц произвольной структуры.

Проблема оценивания расстояний между ячейками Шуберта решается просто. Пусть $\mathbf{v}_1$, $\mathbf{v}_2$ – мультивекторы двух разных ячеек U_1, U_2 и пусть хэммингово расстояние между этими мультивекторами составляет $d_h = ||\mathbf{v}_1 - \mathbf{v}_2||_h$. Обозначим через s число позиций, в которых оба двоичные вектора $\mathbf{v}_1, \mathbf{v}_2$ веса m имеют единицы. Очевидно, что $2s = 2m - d_h$. Базисные векторы e_j, отвечающий этим позициям, лежат сразу в обоих пространствах U_1, U_2. Поэтому $\dim(U_1 \cap U_2) \geq s$. Имеем

$$d_g = 2\delta = 2m - 2\dim(U_1 \cap U_2) \geq 2m - 2s = d_h.$$

Таким образом, расстояние d_g между подпространствами из разных ячеек больше или равно хэммингову расстоянию между мультивекторами этих ячеек, а пространственное

δ-расстояние больше или равно половине хэммингова расстояния: $\delta \geq \delta_h = d_h/2$ (расстояние d_h между векторами одинакового веса всегда чётно). Граница $d_g \geq d_h$ остаётся справедливой и для пар подпространств разной размерности с мультивекторами неравного хэммингового веса.

Грассманов код Габидулина–Боссерта с расстоянием $\delta \neq m$ [14] строится на ячейках Шуберта с прямоугольными таблицами Феррера. Мультивекторы таких ячеек – это двоичные n-блоки, содержащие единственный пакет из m подряд идущих единиц. Пусть блоки единиц сдвинуты один относительно другого на δ. Тогда расстояние Хэмминга d_h между ними составляет 2δ, то есть $\delta_h \geq \delta$. В этом случае и пространственное δ-расстояние между элементами ячеек превышает δ.

Компоненты этого кода имеют вид

$$U_l = \Big| O_{m\times\delta} | \ldots | O_{m\times\delta} | I_{m\times m} | R_{m\times n-l\delta} \Big|,$$

где O – нуль матрицы в количестве $l > 0$, I – единичная матрица, а R – матрица рангового расстояния $\delta_r \geq \delta$. При $n - m = l\delta$ последняя кодовая компонента состоит из единственной матрицы

$$\Big| O_{m\times l\delta} \,|\, I_{m\times m} \Big|.$$

Если $n - m$ не делится на l, то такая компонента может быть добавлена в код. Мощность такого кода равна сумме мощностей ранговых кодов во всех компонентах. Известно, что они уступают границе (1) при всех параметрах, кроме случая $\delta = m$, $m = lm$, отвечающего проективному спреду.

Чтобы двигаться дальше, нужно подключать шубертовы ячейки с непрямоугольными таблицами Феррера. На этом пути возникают два вопроса. Какие именно из $\begin{pmatrix} n \\ m \end{pmatrix}$ ячеек отобрать? Как обобщить лифтинговую конструкцию для непрямоугольных таблиц?

Задача выбора ячеек отнюдь не проста. При заданном расстоянии грассманового кода δ речь идет о построении равновесного (с одинаковыми весами блоков m) двоичного n-кода с хэммингом расстоянием $d_h = 2\delta$. К тому же при построении этого кода должно отдаваться предпочтение словам со сдвинутыми влево единицами, поскольку при сдвиге единиц мультивектора вправо мощность отвечающей ему шубертовой ячейки быстро падает. Для мощности равновесного кода известна граница Элайеса–Бассалыго:

$$M \leqslant \left\lfloor \frac{n\delta}{m^2 - n(m-\delta)} \right\rfloor \text{ при } m^2 > n(m-\delta).$$

Первые подходы к решению этой задачи опирались на идею лексикографического упорядочения [15], [16]: мультивекторы $\mathbf{v}$ упорядочиваются в линейный список согласно естественному алфавитному порядку на множестве их мультииндексов $\mathbf{j}$. После этого применяется жадный алгоритм, который добавляет в конструируемый код с заданным расстоянием δ первый же элемент из списка, подходящий в смысле расстояния до всех слов, уже добавленных в код ранее. Далее в каждой из выбранных ячеек так или иначе строится код максимальной мощности. Конечно, мощность построенного жадным алгоритмом кода может зависеть от исходного линейного упорядочения мультивекторов. Более того, известны примеры, когда лексикографическое упорядочение не является наилучшим. Применённое в [17] упорядочение мультивекторов согласно некотором образом заданному порядку на множестве таблиц Феррера позволило достичь увеличения мощности кода при некоторых значениях параметров.

Конструирование кода жадным алгоритмом выдвигает вопросы сложности кодирования и декодирования. Обсуждение вопросов построения быстрых алгоритмов лексикографического кодирования содержится в [18]. Эффективные конструкции кодов с использованием неполных блок-схем приведены в работе [19].

Задача построения максимального пространственного кода в ячейке Шуберта с непрямоугольной таблицей Феррера требует определенного пересмотра классической теории ранговых кодов. В случае прямоугольной таблицы с размерами $(m\times k)$ задача состоит в выборе семейства F_q-линейных отображений $\varphi : F_q^m \to F_q^k$ с ограничением $d_r \geq \delta$ на ранговое расстояние. Для непрямоугольной таблицы класс допустимых отображений φ ограничивается дополнительным условием: образ $\mathrm{Im}(\varphi)$ любого из них должен быть определенным образом расположен относительно фиксированного флага в пространстве F_q^k. К примеру, таблице Феррера

$$\begin{vmatrix} * & * & * & * & * & * \\ * & * & * & * & * & * \\ 0 & 0 & 0 & * & * & * \end{vmatrix} \tag{4}$$

отвечают отображения $F_q^3 \to F_q^6$. Если в F_q^6 зафиксировать флаг

$$V_1 \subset V_2 \subset V_3 \subset V_4 \subset V_5 \subset V_6 \subset V_7,$$

то допустимыми оказываются те отображения φ, для которых последовательность размерностей пересечений $\mathrm{Im}(\varphi \cap \mathrm{V_j})$, $\mathrm{j} = [1,6]$ нарастает не быстрее, чем $1,2,\mathbf{2},3,3,3$. Прямоугольной 3×6-таблице отвечала бы последовательность $1,2,\mathbf{3},3,3,3$.

Ограничения, накладываемые формой таблицы Феррера, линейны. Множество удовлетворяющих им отображений, является линейным подпространством в пространстве всех F_q-линейных отображений $F_q^m \to F_q^k$. Конструкции ранговых кодов в пространствах с линейными ограничениями обсуждались в работе [19]. Один из подходов к их построению основывается на использовании систематического кодирования ранговых кодов.

Прямоугольную матрицу рангового кода можно построить в систематической форме, задав набор информационных столбцов (строк) волевым образом. Тогда компоненты проверочных столбцов (строк) вполне определяются по информационным столбцам (строкам). Переход к непрямоугольной таблице Феррера эквивалентен «отгрызанию» у прямоугольной кодовой матрицы левого нижнего угла. Важно, чтобы в этот угол не попали проверочные символы, которые не могут быть выбраны свободно. Потеря части информационных символов не является критичной: при кодировании значения потерянных символов объявляются нулевыми, что приводит к снижению размерности кода, но не уменьшает его расстояния. Предположим, что хотим построить код с $d_r = 3$ над таблицей (4). На прямоугольной (3×6)-матрице размерность такого кода $k = n - d + 1$ составляет 1. Он имеет два проверочных столбца и 1 информационный. Для вертикального размещения двух полных проверочных столбцов в таблице место находится:

$$\begin{vmatrix} * & * & * & i_1 & c_{11} & c_{12} \\ * & * & * & i_2 & c_{21} & c_{22} \\ 0 & 0 & 0 & i_3 & c_{31} & c_{32} \end{vmatrix}.$$

Получаем ранговый код мощности $M = q^3$. На прямоугольной (6×3)-матрице размерность кода с расстоянием 3 составляет $k = n - d + 1 = 4$, $n - k = 2$. Две полные проверочные строки удаётся разместить в таблице Феррера по горизонтали:

$$\begin{vmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} \\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} \\ 0 & 0 & 0 & i_1 & i_2 & i_3, \end{vmatrix},$$

что приводит к ранговому коду той же мощности $M = q^3$.

Подобная оптимизация в принципе открывает путь построения рангового d_r-кода по произвольной предъявленной таблице Феррера. В процессе построения можно ограничивать размеры таблицы по вертикали и/или горизонтали, что эквивалентно переходу в подпространство ранговых кодов меньшего размера. Неиспользованные позиции (звездочки)

можно заменять нулями (переход к подкоду) или произвольными элементами F_q (переход к смежному классу). Процедура не отличается регулярностью и не всегда приводит к результату. Может оказаться, что код с требуемым расстоянием в таблицу не вписывается.

А. Шишкин предложил новый подход к упорядочению мультивекторов для жадного алгоритма построения многокомпонентных грассмановых кодов. Пусть задано расстояние δ. Рассмотрим таблицы Феррера для всех ячеек Шуберта с мультивекторами $\mathbf{v}$ и для каждой из них определим мощность $M(\mathbf{v}, \delta)$ максимального рангового кода с расстоянием $d_r > \delta$. Затем упорядочим мультивекторы в порядке убывания $M(\mathbf{v}, \delta)$.

К примеру, для грассманового (n, m, δ)-кода с $m = 7$, $m = 3$, $\delta = 2$ лексикографически упорядоченный перечень мультивекторов всех ячеек Шуберта имеет вид

$$\{1110000, 1101000, 1100100, 1100010, 1100001, 1011000, 1010100,\\ 1010010, 1010001, 1001100, 1001010, 1001001, 1000110, 1000101,\\ 1000011, 0111000, 0110100, 0110010, 0110001, 0101100, 0101010,\\ 0101001, 0100110, 0100101, 0100011, 0011100, 0011010, 0011001,\\ 0010110, 0010101, 0010011, 0001110, 0001101, 0001011, 0000111\}.$$

Детальный анализ отвечающих этим мультивекторам мощностей максимального рангового кода даёт

$$\{(q^8, q^7, q^6, q^5, q^4, q^6, q^5), (q^4, q^3, q^4, q^3, q^2, q^2, q^1),\\ (q^0, q^6, q^5, q^4, q^3, q^4, q^3), (q^2, q^2, q^1, q^0, q^3, q^2, q^2),\\ (q^1, q^1, q^0, q^0, q^0, q^0, q^0)\}.$$

Упорядочение мультивекторов по убыванию мощности кода и применение жадного алгоритма с параметром $\delta = 2$ выделяет 7 ячеек Шуберта с мультииндексами: $\mathbf{j}_1 = (1, 2, 3)$, $\mathbf{j}_2 = (1, 4, 6)$, $\mathbf{j}_3 = (2, 4, 6)$, $\mathbf{j}_4 = (3, 4, 7)$, $\mathbf{j}_5 = (2, 5, 7)$, $\mathbf{j}_6 = (3, 5, 6)$, $\mathbf{j}_7 = (1, 6, 7)$. Мощность соответствующего многокомпонентного кода составляет $M = q^8 + q^4 + q^3 + q^2 + q + q + 1$, что совпадает с мощностью кода с теми же параметрами, построенного в [19] с использованием комбинаторных блок-схем.

Проведенные исследования показали, что упорядочение по мощности ранговых кодов даёт выигрыш в эффективности, где эффективность η определена в виде отношения мощности рассматриваемого кода к верхней границе M_W.

Таблица 1

Эффективности грассмановых (n, m, d)-кодов с $n = 16$ and $d = 3$

m	3	4	5	6	7	8
η_{SKK}	0,875	0,82	0,794	0,782	0,777	0,774
η_{GB}	1	0,823	0,796	0,782	0,777	0,774
η_{new}	1	0,835	0,798	0,785	0,778	0,775

Здесь использованы обозначения η_{SKK} — эффективность SKK-кода, η_{GB} — эффективность кода Габидулина–Боссерта, η_{new} — эффективность кода Шишкина.

4. Декодирование подпространственных и ранговых кодов

Подпространства из кода над грассманианом $\mathcal{G}_q(n, m)$ передаются в сеть в виде $(m \times n)$-матриц X, строки которых являются разложениями базисных векторов передаваемого подпространства по базису объемлющего n-мерного пространства. Получателю могут быть доставлены некоторые линейные комбинации этих строк. Это преобразование описывается умножением слева матрицы X на $(k \times m)$-матрицу A. Число строк k результирующей матрицы AX может отличаться от m. Если $k = m$ и матрица A невырождена, то переданное пространство доставлено получателю без искажений. Просто в нём выбран иной базис. При $\mathrm{rank\,A} < \mathrm{m}$ происходит пространственное стирание – получателю доставляется

подпространство переданного пространства размерности $\mathrm{rank\,A}$. Кроме того, в сети из-за ошибок или преднамеренных действий к строкам матрицы AX могут быть добавлены вектор-строки из «чужих» подпространств, упакованные в матрицу Z. В итоге получателю доставляются строки $(k \times n)$-матрицы

$$Y = AX + Z.$$

Если подпространственное расстояние используемого кода составляет d_g, то подпространство X может быть однозначно восстановлено по матрице Y, если $d(X,Y) = d(X, AX + Z) < d_g/2$. В [11] показано, что условие декодируемости выполняется, если

$$k - \mathrm{rank\,A} + 2\mathrm{rank\,Z} < \mathrm{d_g}/2.$$

Для многокомпонентных грассмановых кодов известен эффективный алгоритм декодирования [23]. На его первом этапе идентифицируется ячейка Шуберта, которой принадлежит переданное пространство. Для этого методом исключений Гаусса строится приведенная ступенчатая форма матрицы Z и определяется ее мультивектор $\mathbf{v}(Z)$. Поскольку $d_h(\mathbf{v}(X), \mathbf{v}(Y)) \geq d_g$, мультивектор $\mathbf{v}(X)$ переданного пространства однозначно восстанавливается по $\mathbf{v}(Y)$ декодированием двоичного кода в хэмминговой метрике. Тем самым ячейка Шуберта переданного пространства оказывается идентифицированной. Идентификация переданного пространства внутри ячейки осуществляется далее по стандартной процедуре декодирования рангового кода с ошибками и стираниями [19].

5. Эффективные алгоритмы декодирования ранговых кодов

При передаче информации по каналу связи с использованием ранговых кодов информационный вектор i умножается на порождающую матрицу G [1], что даст кодовый вектор $c = iG$. При передаче к кодовому вектору добавляется вектор ошибки e: $y = c + e$. Если ранг ошибки меньше половины кодового расстояния d рангового кода, то существует алгоритм декодирования, гарантированно определяющий вектор ошибки.

Первый этап декодирования состоит в том, что по принятому вектору y с использованием проверочной матрицы вычисляют синдром s: $s = yH^T$. В работе [25] дан эффективный алгоритм вычисления синдрома с использованием слабого самоортогонального базиса [24]. Он позволяет вычислить синдром со сложностью $\mathcal{C}^s \approx \mathcal{O}\left(\log N\right)^2 N) + \mathcal{O}\left(N^{\log_2 3}\right)$, где N — степень расширения конечного поля. Если синдром равен нулю, то приёмник делает вывод, что ошибки при передаче отсутствовали и завершает работу алгоритма.

В противном случае приёмник переходит ко *второму этапу* декодирования. На данном этапе декодеру необходимо решить ключевое уравнение:

$$F(x) = \Delta(z) \times S(z) \mod z^{[d-1]}, \tag{5}$$

где $S(z) = \sum_{j=0}^{d-2} s_j z^{[j]}$ — линеаризованный многочлен, коэффициенты которого являются элементами синдрома, $\Delta(z) = \sum_{p=0}^{m} \Delta_p z^{[p]}$ — линеаризованный многочлен, корнями которого являются всевозможные линейные комбинации элементов базиса ошибок, $F(z) = \sum_{i=0}^{m-1} F_i z^{[i]}, F_i = \sum_{p=0}^{i} \Delta_p s_{i-p}^{[p]}$. Существуют эффективные алгоритмы решения ключевого уравнения (нахождения $\Delta(z)$). Они разделяются на две группы. К первой относятся алгоритмы на основе алгоритма Евклида для линеаризованных многочленов, ко второй группе относятся алгоритмы, основанные на процедуре восстановления полинома. К ним относятся алгоритмы Берлекампа–Мэсси и Велча–Берлекампа. Идеи алгоритмов второй группы опираются на результаты, полученные при изучении кодов Рида–Соломона. Алгоритмы первой группы подходят для аппаратной реализации, в то время как алгоритмы второй группы — к программной реализации.

Один из эффективных алгоритмов первой группы был предложен тремя авторами Вахтер, Сидоренко, Боссерт в 2010 году в работе [27]. Основная идея этого алгоритма

заключается в том, что для решения ключевого уравнения нет необходимости выполнять вычисления до полного выполнения алгоритма. Достаточно выполнить вычисления до того момента, когда результат итерации будет меньше, чем $(d-1)/2$. Таким образом, нет необходимости использовать в вычислении коэффициенты, относящиеся к степеням меньше $(d-1)/2$. Сложность выполнения алгоритма в этом случае оценивается как $\mathcal{C}_{LEEA}(d,N) = \mathcal{O}(d^{1.69}\log dC^K_{mult}(N)) = \mathcal{O}(N^{3.275}\log N)$.

В 2014 году [28] Сысоев предложил эффективный алгоритм Евклида для линеаризованного многочлена, относящийся к первой группе алгоритмов декодирования. Он основан на использовании слабого самоортогонального базиса. Идея алгоритма заключается в том, что операции поиска умножения и обратного элемента реализуются рекурсивным способом и заменяются на набор операций меньшей размерности. Здесь используется известный принцип «разделяй и властвуй». Сложность алгоритма в этом случае оценивается как $\mathcal{C} = \mathcal{O}(N^{3.585})$.

Ко второй группе эффективных алгоритмов относится алгоритм, предложенный Рихтером и Плассом [26]. Идея алгоритма основана на результате, полученном Берлекампом и Мэсси. С помощью сдвигового регистра восстанавливается многочлен, корнями которого являются суперпозиции элементов базиса ошибок. В работе [29] Луадро предложил алгоритм восстановления многочлена с использованием идеи построения линеаризованного многочлена методом Велча–Берлекампа. Сложность этого алгоритма оценивается как $\mathcal{C}_{WB}(N) = \mathcal{O}(N^{3.585})$

Остальные этапы декодирования ранговых кодов заключаются в нахождении базиса ошибок, нахождении локаторов ошибок, вычислении вектора ошибки, восстановлении кодового вектора и нахождении информационного вектора. Данные этапы не являются трудоёмкими по сравнению с первыми двумя этапами [31], [30]. Подробнее эти этапы описаны в работах [1] и [30].

6. Заключение

Здесь представлен аналитический обзор основных работ по подпространственным кодам, построенным на основе ранговых кодов Габидулина. Приведены верхние границы мощности этих кодов, позволяющие оценить их потенциальные возможности. Показаны конкретные коды, достигающие максимально возможной мощности при определённых параметрах, а также коды, мощности которых в принципе не могут достичь верхней границы. Приведены различные алгоритмы кодирования и декодирования и отмечены оценки сложности декодирования.

Подпространственные коды являются относительно новой областью исследований, интерес к которой проявился в начале 2000 годов и усилился с появлением кодов SKK, то есть с 2007–2008 годов. От хэмминговых и ранговых кодов подпространственные коды отличаются тем, что метрическое пространство, в котором они строятся, не является линейным, а его метрика не связана к какой-либо нормой. Это означает, что такого объекта, как линейный пространственный код, не существует. Особое значение это обстоятельство приобретает в свете того, что основные успехи в кодировании для хэмминговой и ранговой метрик связаны именно с линейными кодами. Поэтому быстрый успех Силвы, Кёттера, Кшишанга в построении SKK-кодов обусловлен тем, что им удалось ограничить задачу аффинными картами на грассманианах, на которых индуцируется линейная структура. Что же до нелинейных кодов на грассманианах или решетках Грассмана, то проблема их построения на данный момент только слегка намечена, но не решена.

В новую область исследований переносятся некоторые результаты из теории алгебраических многообразий, связанные с покрытиями и свойствами инцедентности. Однако они, как правило, оказываются слишком частными. На сегодняшний день существует единственный подход, позволяющий достичь достаточной общности конструкций – это многокомпонентное кодирование, связанное с разбиением грассманиана на непересекающиеся ячейки Шуберта. Но и его разработка далека от завершения. Предложенные методы конструирова-

ния пригодны для кодов малой мощности, но оказываются вычислительно несостоятельными при больших мощностях, когда количество ячеек Шуберта становится экспоненциально большим. В этой связи представляют интерес эффективные алгоритмы построения оптимальных наборов ячеек Шуберта с заданным расстоянием и простые конструкции хороших ранговых кодов на таблицах Феррера произвольной формы.

Имеются некоторые результаты, представленные в работе [32], которые показывают, что максимизация мощности кода в каждой из ячеек Шуберта – это не всегда наилучший путь. Предложена конструкция оптимального $(n, m, M, \delta) = (6, 3, 77, 2)$ двоичного грассманового кода, в которой для достижения максимальной мощности $M = 77$ в одной из ячеек приходится сознательно выбирать заведомо не максимальный код. Этот факт создаёт почву для размышлений о качественно иных подходах к построению кодов на грассманианах.

Приведённые здесь результаты указывают на то, что в настоящее время подпространственное кодирование является быстро и успешно развивающимся новым направлением в теории алгебраического кодирования. Известные открытые темы добавляют интерес к исследованиям в этом направлении.

Литература

1. *Габидулин Э.М.* Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации. — 1985. — Т. 21, № 1. — С. 1–12.
2. *Gabidulin E.M., Paramonov A.V., Tretjakov O.V.* Rank errors and rank erasurs correction // Proc. Fourth Int. Colloquium on Coding Theory. — 1992. — P. 11–19.
3. *El Gamal H., Damen M.O.* Universal Space-Time Coding // IEEE Transactions on Information Theory. — 2003. — V.49, N 5. — P. 1097–1119.
4. *Li S.-Y.R., Yeung R.W., Sai N.* Coding for errors and erasures in random network coding // IEEE Transaction on Information Theory. — 2008. — V. 49, N 3. — P. 371–381.
5. *Alswede R., Cai N., Li S.-Y.R., Yeung R.W.* Network information flow // IEEE Transaction on Informational Theory. — 2004. — V. 46, N 4. — P. 1203–1216.
6. *Колыбельников А.И.* Обзор технологий беспроводных сетей // Труды МФТИ. — 2012. — Т. 4, № 2. — С. 3–29.
7. *Владимиров С.М.* Улучшение алгоритма декодирования МППЧ-кодов в сетевом кодировании для канала со стиранием // Труды МФТИ. — 2010. — Т. 2, № 3. — С. 100–107.
8. *Koetter R., Kschischang F.R.* A rank metric approach in random network coding // IEEE Transaction on Informational Theory. — 2008. — V. 54, N 8. — P. 3579–3591.
9. *Loo-Keng Hua* A theorem on matrices over a field and its applications // Chinese mathematical society. — 1951. — V. 1, N 2. — P. 109–163.
10. *Delsarte P.* Bilinear Forms over a Finite Field, with Applications to Coding Theory // Journal of Combinatorial Theory, Series A. — 1978. — V. 25. — P. 226–241.
11. *Silva D., Kschischang F.R., Koetter R.* A Rank-Metric Approach to Error Control in Random Network Coding // IEEE Transaction on Informational Theory. — 2008. — V. 54, N 9. — P. 3951–3967.
12. *Wang H., Xing C., Safavi-Naini R.* Linear Autentication Codes: Bounds and Constructions // IEEE Transaction on Informational Theory. — 2003. — V. 49, N 4. — P. 866–873.
13. *Xia T., Fu F.W.* Johnson type bounds on constant dimension codes // Designs, Codes and Cryptography. — 2009. — V. 50, N 2. — P. 163–172.
14. *Gabidulin E.M., Bossert M.* Algebraic codes for network coding // Probl. Inform. Transm. — 2009. — V. 45, N 4. — P. 3–38.
15. *Silberstein N., Etzion T.* Enumerative Encoding in the Grassmannian Space // IEEE Information Theory Workshop. — 2009. — P. 544–548.

16. *Etzion T., Silberstein N.* Error-Correcting Codes in Projective Spaces via Rank-Metric Codes and Ferrers Diagrams // IEEE Transactions on Information Theory. — 2011. — V. 55, N 7. — P. 2909–2919.

17. *Etzion T., Silberstein N.* Large Constant Dimension Codes and Lexicodes // Advances in Mathematics of Communications. — 2011. — V. 5, N 2. — P. 177–189.

18. *Medvedeva Yu.S., Ryabko B.Y.* Fast enumeration algorithm for words with given constraints on run ltngths of ones // Probl. Inform. Transm. — 2010. — V. 45, I. 4. — P. 130–139.

19. *Gabidulin E.M., Pilipchuk N.I.* Rank subcodes in multicomponent network coding // Probl. Inform. Transm. — 2013. — V. 49, N 1. — P. 46–60.

20. *Gadouleau M., Yan Z.* Packing and Covering Properties of Rank Metric Codes // IEEE Trans. on Information Theory. — 2008. — V. 54, N 9. — P. 3873–3883.

21. *Wachter-Zeh A.* Bounds on List Decoding of Rank-Metric Codes // IEEE Trans. on Information Theory. — 2013. — V. 59, N 11. — P. 7268–7277.

22. *Ding Y.* On List-Decodability of Random Rank Metric Codes and Subspace Subcodes // IEEE Trans. on Information Theory. — 2015. — V. 61, N 1. — P. 51–59.

23. *Gabidulin E.M, Pilipchuk N.I., Bossert M.* Decoding of random network codes // Probl. Inform. Transm. — 2010. — V. 46, N 4. — P. 33–55.

24. *Gabidulin E.M., Pilipchuk N.I.* Symmetric matrices and codes correcting rank errors beyond the $\lfloor (d-1)/2 \rfloor$ bound // Discrete Applied Mathematics. — 2006. — V. 154, I. 2. — P. 305–312.

25. *Сысоев И.Ю., Габидулин Э.М.* Декодирование ранговых кодов с использованием слабоортогонального базиса // Труды МФТИ. — 2014. — Т. 6, № 4. — С. 126–138.

26. *Richter G., Plass S.* Error and Erasure Decoding of Rank-Codes with a Modified Berlekamp-Massey Algorithm // In 5th International ITG Conference on Source and Channel Coding (SCC). — 2004.

27. *Wachter A., Afanassiev V.B., Sidorenko V.R.* A Fast Linearized Euclidean Algorithm for Decoding Gabidulin Codes // Proc. of Twelfth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2010). — 2010. — P. 298–303.

28. *Sysoev I.Y.* Euclidean algorithm for linearized polynomials // The Fourtheenth Workshop on Algebraic and Combinatorial Coding Theory — ACCT 2014. — 2014. — P. 307–312.

29. *Loidreau P.* A Welch-Berlekamp Like Algorithm for Decoding Gabidulin Codes // Coding and Cryptography. — 2005. — V. 3969. — P. 36–45.

30. *Сысоев И.Ю., Габидулин Э.М.* Аппаратная реализация кодека ранговых кодов // Проблемы разработки перспективных микро- и наноэлектронных систем: сборник трудов под ред. академика РАН А.Л. Стемпковского. — 2014. — Т. 4. — С. 61–66.

31. *Gabidulin E.M., Sysoev I.Y.* Hardware implementation of rank codec // Mathematics of Distances and Applications. — 2012. — P. 181–189.

32. *Honold T., Kiermaier M., Kurz S.* Optimal binary subspace codecs of length 6, constand dimension 3 and minimum subspace distance 4 // to bee published (arXiv:1311.0464v2 [math.CO] 26 Nov 2014).

References

1. *Gabidulin, E.M.* Theory of codes with maximal rank distance. Probl. Inform. Transm. 1985. T. 21., № 1. C. 1–12. (in Russian).

2. *Gabidulin, E.M., Paramonov, A.V., Tretjakov O.V.* Rank errors and rank erasurs correction. Proc. Fourth Int. Colloquium on Coding Theory. 1992. P. 11–19.

3. *El Gamal, H., Damen, M.O.* Universal Space-Time Coding. IEEE Transactions on Information Theory. 2003. V.49, N 5. P. 1097–1119.

4. *Li, S.-Y.R., Yeung, R.W., Sai, N.* Coding for errors and erasures in random network coding. IEEE Transaction on Information Theory. 2008. V. 49, N 3. P. 371–381.

5. *Alswede, R., Cai, N., Li, S.-Y.R., Yeung, R.W.* Network information flow. IEEE Transaction on Informational Theory. 2004. V. 46, N 4. P. 1203–1216.

6. *Kolybelnikov, A.I.* Overview of Wireless Technology. Proceedings of MIPT. 2012. V. 4, N 2. P. 3–29. (in Russian).

7. *Vladimirov, S.M.* Improved algorithm for decoding LDPC codes for network coding of the binary erasure channel. Proceedings of MIPT. 2010. V. 2, N 3. P. 100–107.

8. *Koetter, R., Kschischang, F.R.* A rank metric approach in random network coding. IEEE Transaction on Informational Theory. 2008. V. 54, N 8. P. 3579–3591.

9. *Loo-Keng, Hua* A theorem on matrices over a field and its applications. Chinese mathematical society. 1951. V. 1, N 2. P. 109–163.

10. *Delsarte, P.* Bilinear Forms over a Finite Field, with Applications to Coding Theory. Journal of Combinatorial Theory, Series A. 1978. V. 25. P. 226–241.

11. *Silva, D., Kschischang, F.R., Koetter, R.* A Rank-Metric Approach to Error Control in Random Network Coding. IEEE Transaction on Informational Theory. 2008. V. 54, N 9. P. 3951–3967.

12. *Wang, H., Xing, C., Safavi-Naini, R.* Linear Autentication Codes: Bounds and Constructions. IEEE Transaction on Informational Theory. 2003. V. 49, N 4. P. 866–873.

13. *Xia, T., Fu, F.W.* Johnson type bounds on constant dimension codes. Designs, Codes and Cryptography. 2009. V. 50, N 2. P. 163–172.

14. *Gabidulin, E.M., Bossert, M.* Algebraic codes for network coding. Probl. Inform. Transm. 2009. V. 45, N 4. P. 3–38.

15. *Silberstein, N. Etzion, T.*Enumerative Encoding in the Grassmannian Space. IEEE Information Theory Workshop. 2009. P. 544–548.

16. *Etzion, T., Silberstein, N.* Error-Correcting Codes in Projective Spaces via Rank-Metric Codes and Ferrers Diagrams. IEEE Transactions on Information Theory. 2011. V. 55, N 7. P. 2909–2919.

17. *Etzion, T., Silberstein, N.* Large Constant Dimension Codes and Lexicodes. Advances in Mathematics of Communications. 2011. V. 5, N 2. P. 177–189.

18. *Medvedeva, Yu.S., Ryabko, B.Y.* Fast enumeration algorithm for words with given constraints on run ltngths of ones. Probl. Inform. Transm. 2010. — V. 45, I. 4. — P. 130–139.

19. *Gabidulin, E.M., Pilipchuk, N.I.* Rank subcodes in multicomponent network coding. Probl. Inform. Transm. 2013. V. 49, N 1. P. 46-60.

20. *Gadouleau, M., Yan, Z.* Packing and Covering Properties of Rank Metric Codes. IEEE Transactions on Information Theory. 2008. V. 54, N 9. P. 3873–3883.

21. *Wachter-Zeh, A.* Bounds on List Decoding of Rank-Metric Codes. IEEE Trans. on Information Theory. 2013. V. 59, N 11. P. 7268–7277.

22. *Ding, Y.* On List-Decodability of Random Rank Metric Codes and Subspace Subcodes. IEEE Trans. on Information Theory. 2015. V. 61, N 1. P. 51–59.

23. *Gabidulin, E.M, Pilipchuk, N.I., Bossert, M.* Decoding of random network codes. Probl. Inform. Transm. 2010. V. 46, N 4. P. 33–55.

24. *Gabidulin, E.M., Pilipchuk, N.I.* Symmetric matrices and codes correcting rank errors beyond the $\lfloor (d-1)/2 \rfloor$ bound. Discrete Applied Mathematics. 2006. V. 154, I. 2. P. 305–312.

25. *Sysoev, I.Y., Gabudulin, E.M.* Decoding od rank codes in week orthogonal basis. Proccedings of MIPT. 2014. T. 6, № 4. C. 126–138. (in Russian).

26. *Richter, G., Plass, S.* Error and Erasure Decoding of Rank-Codes with a Modified Berlekamp-Massey Algorithm. In 5th International ITG Conference on Source and Channel Coding (SCC). 2004.

27. *Wachter, A., Afanassiev, V.B., Sidorenko V.R.* A Fast Linearized Euclidean Algorithm for Decoding Gabidulin Codes. Proc. of Twelfth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2010). 2010. P. 298–303.

28. *Sysoev, I.Y.* Euclidean algorithm for linearized polynomials. The Fourtheenth Workshop on Algebraic and Combinatorial Coding Theory – ACCT 2014. 2014. P. 307–312.

29. *Loidreau, P.* A Welch-Berlekamp Like Algorithm for Decoding Gabidulin Codes. Coding and Cryptography. 2005. V. 3969. P. 36–45.

30. *Sysoev, I.Y, Gabidulin, E.M.* Hardware realisation of codec for rank codes. Problems of micro- and nanoelecnronic devices development. 2014. T. 4. C. 61–66. (in Russian).

31. *Gabidulin, E.M., Sysoev, I.Y.* Hardware implementation of rank codec. Mathematics of Distances and Applications. 2012. P. 181–189.

32. *Honold, T., Kiermaier, M., Kurz, S.* Optimal binary subspace codecs of length 6, constand dimension 3 and minimum subspace distance 4. to be published (arXiv:1311.0464v2 [math.CO] 26 Nov 2014).

Поступила в редакцию 15.04.2015.