РОССИЙСКАЯ АКАДЕМИЯ НАУК

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Журнал основан в январе 1965 г. **ISSN: 0555-2923** **Выходит 4 раза в год**

Том 58, 2022 **Вып. 1**

Январь–Февраль–Март

М о с к в а

С О Д Е Р Ж А Н И Е

Теория кодирования

Большие системы

CONTENTS

Coding Theory

Large Systems

EDN: FBTQIT
ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 1**

УДК 621.391.1 : 519.725

© 2022 г. **Л.А. Бассалыго, В.А. Зиновьев, В.С. Лебедев**

СЛАБО РАЗРЕШИМЫЕ БЛОК-СХЕМЫ И НЕДВОИЧНЫЕ КОДЫ, ЛЕЖАЩИЕ НА ГРАНИЦЕ ДЖОНСОНА[1]

Указаны два новых семейства разрешимых блок-схем. Дано определение слабо разрешимой блок-схемы и доказана эквивалентность такой схемы и недвоичных кодов, лежащих на границе Джонсона. Построено новое семейство таких кодов.

Ключевые слова: разрешимая блок-схема, слабо разрешимая блок-схема, недвоичный код, граница Джонсона.

DOI: 10.31857/S0555292322010016

1. Блок-схемой $B(v,k,\lambda)$ называется такое размещение v различных элементов $a_1,\dots,a_v$ по b блокам $B_1,\dots,B_b$, при котором каждый блок содержит ровно k различных элементов, каждый элемент принадлежит ровно r блокам, и каждая пара различных элементов a_i,a_j, $i\neq j$, принадлежит ровно λ блокам. Параметры v,k,λ блок-схемы однозначно определяют параметры b и r (см. [1]):

$$b=\frac{\lambda v(v-1)}{k(k-1)},\quad r=\frac{\lambda(v-1)}{k-1}.$$

Блок-схема полностью описывается своей матрицей инцидентности $A=[a_{ij}]$, где

$$a_{ij}=\begin{cases}1, & \text{если } a_i\in B_j,\\ 0, & \text{если } a_i\notin B_j,\end{cases}$$

$i=1,\dots,v$, $j=1,\dots,b$.

Блок-схема $B(v,k,\lambda)$ называется разрешимой и обозначается через $RB(v,k,\lambda)$, если ее матрица инцидентности может быть приведена перестановкой строк (что соответствует перенумерации элементов блок-схемы) и столбцов (что соответствует перенумерации блоков) к следующему виду:

$$A=[A_1\,|\,A_2\,|\,\dots\,|\,A_r], \tag{1}$$

где каждая подматрица A_j размера $v\times\dfrac{v}{k}$ состоит из строк веса 1. Построение новых разрешимых блок-схем зиждется на следующем результате из [2].

Теорема 1. *Существование $RB(v,k,\lambda)$-схемы эквивалентно существованию q-ичного эквидистантного кода мощности N длины n с расстоянием d, лежащего*

[1] Работа выполнена в ИППИ РАН при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 19-01-00364) и Национального научного фонда Болгарии (номер гранта 20-51-18002).

на границе Плоткина

$$N \leqslant \frac{qd}{qd-(q-1)n},$$

где

$$q=\frac{v}{k},\quad N=v,\quad n=r=\frac{\lambda(v-1)}{k-1},\quad d=r-\lambda=\frac{\lambda(v-k)}{k-1}.$$

Доказательство этой теоремы в [2] использует естественное преобразование матрицы инцидентности схемы в q-ичный код и столь же естественное обратное преобразование. Поэтому построение новых разрешимых схем эквивалентно построению новых q-ичных кодов, лежащих на границе Плоткина. Здесь мы предложим процедуру построения нового класса таких четверичных кодов из $B(v,k,\lambda)$-схем, являющуюся обобщением процедуры из работы [3].

Утверждение 1. *Любая блок-схема $B(v,k,\lambda)$ порождает четверичный равновесный эквидистантный код с параметрами*

$$N=v,\quad n=\binom{b}{3},\quad w=\frac{r(b-2)(b-r)}{2},\quad d=(b-2)(r-\lambda)(b-2(r-\lambda)). \qquad (2)$$

Доказательство. Построение кода весьма просто: выбираются любые три столбца матрицы инцидентности блок-схемы (таковых $\binom{b}{3}$) и заменяются на один столбец q-ичного кода по следующему правилу:

$$(0,0,0),(1,1,1)\to 0,\quad (0,0,1),(1,1,0)\to 1,$$
$$(0,1,0),(1,0,1)\to 2,\quad (1,0,0),(0,1,1)\to 3,$$

так что в результате получаем четверичный код. Очевидно, что построенный код имеет дину $n=\binom{b}{3}$ и число слов $N=v$. Нетрудно проверить, что расстояние между любыми двумя кодовыми словами равно

$$\binom{b-2(r-\lambda)}{2}\binom{2(r-\lambda)}{1}+\binom{b-2(r-\lambda)}{1}\binom{2(r-\lambda)}{2}=$$
$$=(b-2)(r-\lambda)(b-2(r-\lambda),$$

а вес кодовых слов равен

$$\binom{b}{3}-\binom{r}{3}-\binom{b-r}{3}=\frac{r(b-2)(b-r)}{2}. \quad \blacktriangle$$

Если в качестве схемы $B(v,k,\lambda)$ выбрать симметричную (т.е. такую, в которой $b=v$ и $r=k$) схему $B(4t-1,2t,t)$ (полученную из $(0,1)$-матрицы Адамара с нулевой строкой и нулевым столбцом выкидыванием этой строки и этого столбца), то получим четверичный код с параметрами

$$N=4t-1,\quad n=\frac{(4t-1)(2t-1)(4t-3)}{3},\quad w=d=t(2t-1)(4t-3). \qquad (3)$$

Присоединив к коду нулевое слово, получим эквидистантный код, лежащий на границе Плоткина:

$$4t=\frac{4t(2t-1)(4t-3)}{4t(2t-1)(4t-3)-(4t-1)(2t-1)(4t-3)}.$$

В [3], а еще ранее в [4] с помощью выбора любых двух столбцов матрицы инцидентности из схемы $B(4t-1,2t,t)$ был построен другой четверичный код, лежащий на границе Плоткина, с параметрами

$$N=4t,\quad n=(4t-1)(2t-1),\quad d=3t(2t-1).$$

Воспользовавшись теоремой 1 из [2], получаем следующее

Утверждение 2. *Любая блок-схема $B(4t-1,2t,t)$ порождает две разрешимые блок-схемы*:

$$RB(4t,t,(t-1)(2t-1))\quad и\quad RB(4t,t,(t-1)(2t-1)(4t-3)/3).$$

Замечание 1. Казалось естественным продолжить такую конструкцию, выбирая любые четыре (или даже больше) столбца матрицы инцидентности симметричной схемы $B(4t-1,2t,t)$, но уже выбор четырех столбцов не привел к кодам, лежащим на границе Плоткина, а следовательно, и к новым разрешимым схемам.

2. Теорема 1 указывает на взаимосвязь разрешимой схемы и недвоичных кодов, лежащих на границе Плоткина. Теперь мы хотим слегка обобщить понятие разрешимой схемы, чтобы установить аналогичную взаимосвязь между этим обобщением и недвоичными равновесными кодами, лежащими на границе Джонсона [5]

$$N\leqslant\frac{(q-1)dn}{qw^2-(q-1)(2w-d)n},\tag{4}$$

где N – мощность кода, n – его длина, d – кодовое расстояние, w – вес кодового слова.

Предлагаемое обобщение отличается от разрешимой схемы $RB(v,k,\lambda)$ только в одном: в разрешимой схеме каждый столбец подматриц A_j, $j=1,2,\ldots,r$, содержит ровно k единиц, а в слабо разрешимой $WRB_m(v,k,\lambda)$-схеме один столбец подматрицы A_j, $j=1,2,\ldots,r$, содержит m единиц, $m\geqslant 1$. Очевидно, что при $m=k$ слабо разрешимая схема превращается в разрешимую. В слабо разрешимой схеме каждая подматрица A_j, $j=1,2,\ldots,r$, имеет размер $v\times\dfrac{v-m+k}{k}$, а параметр r (число блоков, которым принадлежит каждый элемент, что для разрешимых схем совпадает с числом подматриц A_j или, что то же самое, с весом каждой строки матрицы A) определяется следующим соотношением:

$$\lambda\binom{v}{2}=r\left(\binom{m}{2}+\frac{v-m}{k}\binom{k}{2}\right).\tag{5}$$

Это соотношение доказывается стандартным образом: скалярное произведение любых двух различных строк матрицы A по определению равно λ, а число пар строк равно $\binom{v}{2}$. С другой стороны, сумма скалярных произведений попарных строк в любой подматрице A_j равна

$$\binom{m}{2}+\frac{v-m}{k}\binom{k}{2},$$

а число матриц A_j равно r. Следовательно,

$$r=\frac{\lambda\binom{v}{2}}{\binom{m}{2}+\frac{v-m}{k}\binom{k}{2}}.\tag{6}$$

Теперь мы уже можем сформулировать аналог теоремы 1.

Теорема 2. *Существование слабо разрешимой $WRB_m(v,k,\lambda)$-схемы эквивалентно существованию q-ичного эквидистантного кода мощности N длины n с расстоянием d, лежащего на границе Джонсона* (4), *где параметры схемы и кода связаны следующими равенствами*:

$$q=\frac{v-m+k}{k},\quad n=r=\frac{\lambda v(v-1)}{m(m-1)+(v-m)(k-1)},$$
$$N=v,\quad d=r-\lambda,\quad w=\frac{r(v-m)}{v}. \tag{7}$$

Доказательство. Доказательство теоремы очевидно. Без ограничения общности можно считать, что в каждой подматрице A_j столбец с m единицами стоит на первом месте. Установим следующее взаимно-однозначное соответствие между строками подматриц (их длина равна $(v-m+k)/k$) и символами алфавита $0,1,\ldots,q-1=(v-m)/k$: строке $(1,0,\ldots,0)$ поставим в соответствие 0, а строке с единицей на i-м месте – символ $i-1$, где $i>1$. При таком соответствии каждый ненулевой символ встретится в столбце кода k раз, а нуль – m раз (такой код мы назвали посимвольно равномерным [3]). Очевидно, что полученный код эквидистантен и $d=r-\lambda$. Согласно [3, утверждение 1] код лежит на границе Джонсона тогда и только тогда, когда он посимвольно равномерен и эквидистантен, а при $m\neq k$ он к тому же равновесен (см. [3, утверждение 2]). Это же соответствие переводит каждый столбец q-ичного кода в подматрицу слабо разрешимой $WRB_m(v,k,\lambda)$-схемы. ▲

Следствие. *Так как четверичный код с параметрами* (3) *лежит на границе Джонсона, то существует слабо разрешимая $WRB_{t-1}(4t-1,t,(t-1)(2t-1)\times\times(4t-3)/3)$-схема. Параметры схемы легко вычисляются по параметрам кода*:

$$v=N,\quad \lambda=n-d,\quad m=\frac{N(n-w)}{n},\quad k=\frac{Nw}{n(q-1)}.$$

Замечание 2. Теорема 1 является частным случаем теоремы 2 при $m=k$. Надо только помнить, что при $m=k$ код не является равновесным, а величина $\dfrac{r(v-m)}{v}$ является средним весом $\bar{w}$ кодовых слов, при котором также верна граница Джонсона (см. [3]).

Замечание 3. Введенная в [6] m-квазиразрешимая $NRB_m(v,k,\lambda)$-схема эквивалентна слабо разрешимой $WRB_m(v,k,\lambda')$-схеме, столбцы которой с m единицами образуют $B(v,m,\xi)$-схему, где

$$\xi=\frac{\lambda m(m-1)}{(v-m)(k-1)}.$$

Эквивалентность здесь такова: квазиразрешимая схема получается из слабо разрешимой удалением из каждой матрицы A_j (см. (1)) столбца с m единицами, а слабо разрешимая из квазиразрешимой – вставкой в каждую матрицу A_j столбца с m единицами на позициях, соответствующих нулевым строкам матрицы A_j. При этом, очевидно, $\lambda'=\lambda+\xi$.

3. Рассмотрим теперь другой частный случай слабо разрешимой схемы: $k=2$, $\lambda=1$. Так как вес кодовых слов (см. (7)) является целым числом

$$w=\frac{n(N-m)}{N}=\frac{r(v-m)}{v}=r-m+\frac{m(m-1)^2}{v+m(m-2)},$$

то целочисленной является дробь

$$\frac{m(m-1)^2}{v+m(m-2)}. \tag{8}$$

Таким образом, целочисленность дроби (8) является необходимым условием для существования слабо разрешимой $WRB_m(v,2,1)$-схемы, и следовательно, для существования кода, лежащего на границе Джонсона, параметры которого определены в теореме 2. Впрочем, иногда это необходимое условие является и достаточным, примеры чему будут приведены ниже.

Нетрудно проверить, что если мы ищем знаменатель дроби (8) в виде произведения сомножителей ее числителя, то единственным таким решением (при $m \geqslant 3$) является

$$v = m(m-1)^2 - m(m-2) = m(m^2-3m+3) = (m-1)^3 + 1. \tag{9}$$

Конечно, существует много других значений параметра v, при которых дробь (8) является целым числом. Мы приведем только два таких примера – по одному для нечетного и четного m:

$$v = \begin{cases} 2m(m-1) - m(m-2) = m^2, & m \text{ – нечетное}, \\ 2(m-1)^2 - m(m-2) = m^2 - 2m + 2, & m \text{ – четное}. \end{cases} \tag{10}$$

Выпишем для всех трех случаев допустимые значения параметров кодов, лежащих на границе Джонсона:

(I) $N = m(m^2-3m+3)$, $n = (m-1)(m^2-3m+3)$, $d = n-1$, $w = n-m+1$, $q = \dfrac{N-m}{2} + 1$;

(II) $N = m^2$, $n = \dfrac{m(m+1)}{2}$, $d = n-1$, $w = \dfrac{N-1}{2}$, $q = \dfrac{N-m}{2} + 1$, m – нечетное;

(III) $N = m^2 - 2m + 2$, $n = \dfrac{m^2-2m+2}{2}$, $d = n-1$, $w = \dfrac{N-m}{2}$, $q = \dfrac{N-m}{2} + 1$, m – четное.

Во всех трех случаях удалось для некоторых значений m построить коды с такими параметрами.

4. Начнем со случая (II), для которого удалось построить семейства кодов с указанными параметрами.

Предложение 1. *Для любого нечетного простого m существует код со значениями параметров* (II).

Доказательство. Представим код C в виде матрицы размера $m^2 \times \dfrac{m(m+1)}{2}$:

$$C = \begin{bmatrix} B_1 & A_{1,1} & \dots & A_{1,(m-1)/2} \\ B_2 & A_{2,1} & \dots & A_{2,(m-1)/2} \\ \dots & \dots & \dots & \dots \\ B_m & A_{m,1} & \dots & A_{m,(m-1)/2} \end{bmatrix},$$

где каждая из матриц B_r, $r = 1, \dots, m$, и $A_{r,s}$, $r = 1, \dots, m$, $s = 1, \dots, (m-1)/2$, является циркулянтной (по модулю m) матрицей размера $m \times m$ (строки и столбцы любой квадратной матрицы размера $p \times p$ всюду далее будем нумеровать от 0 до $p-1$). Следовательно, каждая из этих матриц определяется своей первой строкой. Сначала зададим первые строки матриц B_r:

$$b_{0,0}(r) = 0, \quad b_{0,t}(r) = (r-1)(m-1)/2 + \min\{t, m-t\}, \quad t = 1, 2, \dots, m-1. \tag{11}$$

Для пояснения приведем простой пример при $m = 7$, а именно выпишем первые строки матриц B_1, B_2 и B_7 ($q = 22$, символы алфавита обозначаем числами от 0 до 21):

$$(0\ 1\ 2\ 3\ 3\ 2\ 1), \quad (0\ 4\ 5\ 6\ 6\ 5\ 4), \quad (0\ 19\ 20\ 21\ 21\ 20\ 19).$$

Так как в каждой первой строке матриц B_r используется $\dfrac{m-1}{2}$ различных ненулевых символов, в двух разных строках используются различные ненулевые символы алфавита, а число первых строк равно m, то мощности алфавита, равной $m(m-1)/2+1$, достаточно для первых строк всех матриц. Нетрудно видеть, что расстояние между словами матрицы B_r равно $m-1$ при любом r, $r = 1, 2, \ldots, m$. Обозначим через P_B матрицу первых строк матриц B_r, $r = 1, \ldots, m$.

Далее требуется построить первые строки матриц $A_{r,s}$, $r = 1, \ldots, m$, $s = 1, \ldots, (m-1)/2$. Обозначим через P_s, $s = 1, \ldots, (m-1)/2$, матрицу, образованную первыми строками матриц $A_{r,s}$, $r = 1, \ldots, m$, и укажем способ ее построения (координаты в матрице на пересечении i-й строки и ℓ-го столбца будем обозначать через (i, ℓ)). Сначала определим расположение нулей в матрице P_s: в каждой строке и каждом столбце матрицы встретится ровно один 0 в позиции $(i, is \bmod m)$, $i = 0, 1, \ldots, m-1$, (напомним, что m – простое число и $s \leqslant (m-1)/2$). Всего в матрице P_s имеется $\binom{m}{2}$ пар нулей. Каждая такая пара нулей с координатами $(i, is \bmod m)$ и $(j, js \bmod m)$ определяет координаты $(i, js \bmod m)$ и $(j, is \bmod m)$, $i \neq j$, и на этих позициях располагается некоторый ненулевой символ, причем различным парам нулей соответствуют различные ненулевые символы (это возможно, так как число ненулевых символов алфавита и число пар нулей одно и то же: $m(m-1)/2$).

Приведем в качестве примера такого построения матрицы P_1 и P_2 при $m = 5$:

$$P_1 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 5 & 6 & 7 \\ 2 & 5 & 0 & 8 & 9 \\ 3 & 6 & 7 & 0 & 10 \\ 4 & 8 & 9 & 10 & 0 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 0 & 3 & 1 & 4 & 2 \\ 1 & 6 & 0 & 7 & 5 \\ 2 & 8 & 5 & 9 & 0 \\ 3 & 0 & 6 & 10 & 8 \\ 4 & 10 & 7 & 0 & 9 \end{bmatrix}.$$

Так как все символы в первой строке матриц $A_{r,s}$, $r = 1, \ldots, m$, $s = 1, \ldots, (m-1)/2$, различны, а сами матрицы циркулянтны, то расстояние между строками каждой матрицы равно m, и следовательно, расстояние между кодовыми словами внутри r-го слоя кода C равно $n-1$. Осталось доказать, что расстояние между любыми двумя кодовыми словами матрицы C из разных слоев равно $n-1$. Определим следующую матрицу $P(C)$ размера $m \times m(m+1)/2$:

$$P(C) = [P_B \,|\, P_1 \,|\, \ldots \,|\, P_s | \ldots | \, P_{(m-1)/2}].$$

Нетрудно видеть, что расстояние между кодовыми словами матрицы C из разных слоев в силу циркулянтности матриц B_r и $A_{r,s}$ совпадает с расстоянием между некоторыми фиксированными сдвигами соответствующих строк матрицы $P(C)$. Естественно, эти сдвиги определяются выбранными кодовыми словами, а сами сдвиги (по модулю m) происходят в каждой из матриц P_B, P_s, $s = 1, \ldots, (m-1)/2$, размера $m \times m$. Опять же в силу циркулянтности матриц B_r и $A_{r,s}$ можно зафиксировать одну строку матрицы $P(C)$ и сдвигать лишь другую. Отметим прежде всего, что по построению в любых двух строках каждой матрицы P_s, $s = 1, \ldots, (m-1)/2$, имеется ровно два одинаковых символа алфавита: один нулевой, а другой ненулевой, причем никакой сдвиг одной строки матрицы P_s, $s = 1, \ldots, (m-1)/2$, относительно другой не может привести к совпадению этих двух символов на соответствующих позициях этих двух строк.

Зафиксируем теперь две строки матрицы $P(C)$ с номерами i и j и рассмотрим эти строки в матрицах P_s и $P_{s'}$, $s \neq s'$. По построению нули в этих строках находятся в позициях $(i, si \bmod m)$ и $(j, sj \bmod m)$ в матрице P_s и в позициях $(i, s'i \bmod m)$ и $(j, s'j \bmod m)$ в матрице $P_{s'}$, а позиции одинаковых ненулевых символов – $(i, sj \bmod m)$ и $(j, si \bmod m)$ в матрице P_s и $(i, s'j \bmod m)$ и $(j, s'i \bmod m)$ в матрице $P_{s'}$.

Чтобы при сдвиге j-й строки совпали позиции нулей в обеих матрицах, должно выполняться следующее условие:

$$(i-j)s \equiv (i-j)s' \pmod m,$$

т.е.

$$(i-j)(s-s') \equiv 0 \pmod m,$$

что невозможно, так как m – простое число, а $i \neq j$ и $s \neq s'$. Напомним, что

$$i < m, \quad j < m, \quad s \leqslant (m-1)/2, \quad s' \leqslant (m-1)/2.$$

Чтобы при сдвиге j-й строки совпали позиции нулей в одной матрице (например, в P_s) и позиции одинаковых ненулевых символов в другой матрице, должно выполняться следующее условие:

$$(i-j)s \equiv (j-i)s' \pmod m,$$

т.е.

$$(i-j)(s+s') \equiv 0 \pmod m,$$

что невозможно, так как m – простое число, а $i \neq j$ и $s + s' \leqslant (m-1)$. Совпадение при сдвиге j-й строки позиций одинаковых ненулевых символов в одной матрице и одинаковых ненулевых символов в другой матрице невозможно по той же причине, что и совпадение двух нулевых символов.

Так как число различных матриц P_s равно $(m-1)/2$, в каждой матрице P_s всего для двух сдвигов j-й строки относительно i-й происходит совпадение символов в i-й и j-й строках (одного нулевого и одного ненулевого), а число различных ненулевых сдвигов j-й строки относительно i-й равно $m-1$, то при каждом сдвиге происходит совпадение символов этих двух строк ровно в одной позиции. При нулевом сдвиге, т.е. при отсутствии сдвига, совпадают нулевые символы в i-й и j-й строках матрицы P_B. Следовательно, расстояние между любыми кодовыми словами матрицы C равно $n-1$. ▲.

Приведенное доказательство не применимо к случаю, когда m – не простое число. Однако в теории кодирования редко бывает, чтобы некоторое утверждение было верным только для простого поля, а не любого конечного поля (в нашем случае для m, являющегося степенью простого). И действительно, справедливо

Предложение 2. *Для любого нечетного m, являющегося степенью простого числа, существует код со значениями параметров* (II).

Доказательство. Известно [7], что для любого m, являющегося степенью простого, существует МДР-код с параметрами

$$N' = m^2, \quad n' = m+1, \quad d' = m, \quad q = m. \tag{12}$$

Так как размерность этого МДР-кода равна 2, то любые две позиции кода являются информационными, т.е. любые два столбца кода содержат каждую пару символов алфавита ровно один раз (символы алфавита обозначим через $0, 1, \ldots, m-1$). Обратимся теперь к матрицам B_r, введенным в предложении 1 (заметим, что их

определение не зависит от простоты числа m). Это циркулянтные матрицы, первая строка которых определяется равенствами (11). Обозначим j-ю строку матрицы B_r через $b_j(r)$ и зададим отображение

$$f(j,r) = b_j(r),$$

переводящее каждую пару символов МДР-кода (j,r), $j = 0,1,\ldots,m-1$, $r = 0,1,\ldots,m-1$, в j-ю строку $b_j(r)$ длины m матрицы B_r. Разобьем теперь столбцы МДР-кода на пары и, используя отображение $f(j,r)$, поставим в соответствие каждой паре столбцов матрицу размера $m^2 \times m$. В результате получим матрицу кода с параметрами (II). Действительно, число кодовых слов равно числу кодовых слов МДР-кода, т.е. $N = m^2$, длина кода равна числу пар столбцов $(m+1)/2$, умноженному на m, т.е. $n = m(m+1)/2$, алфавит кода равен объединению алфавитов, используемых во всех матрицах B_r в предложении 1, т.е. $q = 1 + m(m-1)/2 = 1 + (N-m)/2$, а вес кодовых слов равен числу пар столбцов $(m+1)/2$, умноженному на вес строки матриц B_r, равный $m-1$, т.е. $(N-1)/2$. Осталось вычислить кодовое расстояние. Очевидно, что для $(j,r) \neq (j',r')$

$$d\big(f(j,r), f(j',r')\big) = \begin{cases} m, & \text{если } j \neq j' \text{ и } r \neq r', \\ m-1, & \text{если } j = j' \text{ или } r = r'. \end{cases} \tag{13}$$

Так как у любых двух слов МДР-кода символы совпадают лишь в одной позиции (и эти символы, естественно, принадлежат лишь одной паре столбцов разбиения МДР-кода), то согласно (13) расстояние между соответствующими словами построенного нами кода равно $m(m-1)/2 + m - 1 = n - 1$. ▲

Замечание 4. Конечно, предложение 1 представляет собой частный случай предложения 2, но авторам показалась достаточно своеобразной и заслуживающей изложения конструкция кода в предложении 1.

5. При рассмотрении случая (II) в предыдущем пункте мы ограничились нечетными m, так как при четных m слабо разрешимая схема $WRB_m(m^2,2,1)$ не существует, ибо не выполнено необходимое условие, что $w = \dfrac{N-1}{2}$ – целое число. Поэтому, если мы хотим оставить первые два параметра схемы неизменными ($v = m^2$, $k = 2$), то мы должны перейти к схеме $WRB_m(m^2,2,2)$. При этом согласно теореме 2 параметры кода должны быть следующими:

$$\begin{aligned} &N = m^2, \quad n = m(m+1), \quad d = n-2, \quad w = N-1, \\ &q = \frac{N-m}{2} + 1, \quad m \text{ – четное.} \end{aligned} \tag{14}$$

И при m, равном степени числа 2, такие коды удается построить.

Предложение 3. *Для любого m, являющегося степенью числа* 2, *существует код со значениями параметров* (14).

Доказательство. Построение таких кодов, по существу, весьма близко к тому, которое использовалось в предложении 2 для m, равного степени нечетного простого числа. Отличие связано с тем, что при четных m длина МДР-кода с параметрами (12) нечетна, и следовательно, он не может быть разбит на пары столбцов. Поэтому в строки матриц, весьма схожих с матрицами B_r из предложения 1, отображается каждый столбец МДР-кода.

Сначала для любого элемента a алфавита нашего будущего кода ($a = 0,1,\ldots,m(m-1)/2$) определим циркулянтную матрицу $D(a)$ размера $(m-1) \times (m-1)$, первая строка которой имеет вид

$$a, a+1, a+2, \ldots, a+(m-2)/2, a+(m-2)/2, a+(m-2)/2-1, \ldots, a+2, a+1.$$

Затем превратим эту матрицу в матрицу $D(a,\ell)$ размера $m\times m$, присоединив к ней сначала снизу строку $a,a,\ldots,a$ длины $m-1$, а затем вставив нулевой столбец в ℓ-й позиции, $\ell=0,1,\ldots,m-1$. Приведем пример такого построения при $m=8$:

$$D(a)=\begin{bmatrix} a & a+1 & a+2 & a+3 & a+3 & a+2 & a+1\\ a+1 & a & a+1 & a+2 & a+3 & a+3 & a+2\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ a+2 & a+3 & a+3 & a+2 & a+1 & a & a+1\\ a+1 & a+2 & a+3 & a+3 & a+2 & a+1 & a \end{bmatrix}$$

и

$$D(a,3)=\begin{bmatrix} a & a+1 & a+2 & 0 & a+3 & a+3 & a+2 & a+1\\ a+1 & a & a+1 & 0 & a+2 & a+3 & a+3 & a+2\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ a+2 & a+3 & a+3 & 0 & a+2 & a+1 & a & a+1\\ a+1 & a+2 & a+3 & 0 & a+3 & a+2 & a+1 & a\\ a & a & a & 0 & a & a & a & a \end{bmatrix}.$$

Нетрудно видеть, что расстояние между строками матрицы $D(a,\ell)$ равно $m-2$. Положим $A=\{1+rm/2:\ r=0,1,\ldots,m-2\}$. Очевидно, что для любых $a,a'\in A$, $a\ne a'$, расстояние между строками матриц $D(a,\ell)$ и $D(a',\ell')$ равно m, если $\ell\ne\ell'$. Теперь уже мы можем определить матрицы D_r: $D_r=D(1+rm/2,r)$, $r=0,1,\ldots,m-2$. Матрицу D_{m-1} определим несколько иным способом: положим ее r-й столбец равным $(r+1)$-му столбцу матрицы D_r, $r=0,1,\ldots,m-2$, а последний ($(m-1)$-й) столбец положим нулевым.

Нетрудно видеть, что расстояние между строками матрицы D_r, $r=0,1,\ldots,m-1$, равно $m-2$, а между строками матриц D_r и $D_{r'}$, $r\ne r'$, равно m.

Проиллюстрируем построение матриц D_r на примере $m=4$. Первые три матрицы имеют вид

$$D_0=\begin{bmatrix}0&1&2&2\\0&2&1&2\\0&2&2&1\\0&1&1&1\end{bmatrix},\quad D_1=\begin{bmatrix}3&0&4&4\\4&0&3&4\\4&0&4&3\\3&0&3&3\end{bmatrix},\quad D_2=\begin{bmatrix}5&6&0&6\\6&5&0&6\\6&6&0&5\\5&5&0&5\end{bmatrix},$$

а последняя –

$$D_3=\begin{bmatrix}1&4&6&0\\2&3&6&0\\2&4&5&0\\1&3&5&0\end{bmatrix}.$$

Отображение МДР-кода (12) в код с параметрами (14) совсем просто: каждый символ r этого кода, $r=0,1,\ldots,m-1$, заменяется на строку матрицы D_r с выполнением единственного требования – два одинаковых символа в одном столбце МДР-кода должны заменяться на разные строки соответствующей матрицы (напомним, что каждый символ МДР-кода (12) в каждом столбце встречается m раз, а каждая матрица D_r состоит из m строк). Формально такое отображение можно задать, например, следующим образом. Обозначим j-ю строку матрицы D_r через $d_j(r)$ и зададим отображение

$$\varphi(j,r)=d_j(r),$$

переводящее каждую пару (j,r), $j=0,1,\ldots,m-1$, $r=0,1,\ldots,m-1$, в j-ю строку $d_j(r)$ длины m матрицы D_r. Перенумеруем строки матрицы МДР-кода числами от 1 до m^2. В каждом столбце матрицы МДР-кода каждый из его m символов

$\{0,1,\ldots,m-1\}$ встречается m раз. Пусть $i_0(r) < i_1(r) < \ldots < i_{m-1}(r)$ – номера строк МДР-кода, в которых встречается фиксированный символ r этого кода. Если этот символ стоит в строке с номером $i_j(r)$, то применим к этому символу отображение $\varphi(j,r)$, т.е. поставим в соответствие этому символу j-ю строку матрицы D_r. Тем самым, каждый столбец матрицы МДР-кода отобразится в некоторую матрицу размера $m^2 \times m$, состоящую из строк матриц $D_0,\ldots,D_{m-1}$. Матрица размера $m^2 \times m(m+1)$, полученная в результате такого отображения всех $m+1$ столбцов МДР-кода, представляет собой код с параметрами (14). Вычисление параметров полученного кода аналогично соответствующему вычислению в предложении 2. ▲

Продолжим иллюстрацию примера при $m = 4$:

$$\begin{bmatrix}
0&0&0&0&0\\0&1&1&1&1\\0&2&2&2&2\\0&3&3&3&3\\1&0&1&2&3\\1&1&0&3&2\\1&2&3&0&1\\1&3&2&1&0\\2&0&2&3&1\\2&1&3&2&0\\2&2&0&1&3\\2&3&1&0&2\\3&0&3&1&2\\3&1&2&0&3\\3&2&1&3&0\\3&3&0&2&1
\end{bmatrix},\quad
\begin{bmatrix}
0&1&2&2&0&1&2&2&0&1&2&2&0&1&2&2&0&1&2&2\\
0&2&1&2&3&0&4&4&3&0&4&4&3&0&4&4&3&0&4&4\\
0&2&2&1&5&6&0&6&5&6&0&6&5&6&0&6&5&6&0&6\\
0&1&1&1&1&4&6&0&1&4&6&0&1&4&6&0&1&4&6&0\\
3&0&4&4&0&2&1&2&4&0&3&4&6&5&0&6&2&3&6&0\\
4&0&3&4&4&0&3&4&0&2&1&2&2&3&6&0&6&5&0&6\\
4&0&4&3&6&5&0&6&2&3&6&0&0&2&1&2&4&0&3&4\\
3&0&3&3&2&3&6&0&6&5&0&6&4&0&3&4&0&2&1&2\\
5&6&0&6&0&2&2&1&6&6&0&5&2&4&5&0&4&0&4&3\\
6&5&0&6&4&0&4&3&2&4&5&0&6&6&0&5&0&2&2&1\\
6&6&0&5&6&6&0&5&0&2&2&1&4&0&4&3&2&4&5&0\\
5&5&0&5&2&4&5&0&4&0&4&3&0&2&2&1&6&6&0&5\\
1&4&6&0&0&1&1&1&1&3&5&0&3&0&3&3&5&5&0&5\\
2&3&6&0&3&0&3&3&5&5&0&5&0&1&1&1&1&3&5&0\\
2&4&5&0&5&5&0&5&3&0&3&3&1&3&5&0&0&1&1&1\\
1&3&5&0&1&3&5&0&0&1&1&1&5&5&0&5&3&0&3&3
\end{bmatrix}.$$

Левая матрица представляет собой исходный $[5,2,4]_4$-МДР-код, а правая – семеричный код мощности 16 с длиной 20, расстоянием 18 и весом 15, полученный при описанном выше отображении МДР-кода с помощью матриц D_0, D_1, D_2, D_3.

6. Перейдем теперь к случаю (I), где удалось построить соответствующий код лишь при $m = 4$ и $m = 5$; при $m = 3$ соответствующий код совпадает с кодом, построенным в случае (II), и давно известен (см., например, [8]) – это четверичный код мощности 9 с длиной 6, расстоянием 5 и весом кодовых слов 4. Построение обоих кодов основано, как и в предыдущем пункте, на использовании циркулянтных матриц, но само построение циркулянтных матриц произведено "вручную", так что нам не удалось распространить его на бóльшие значения m.

При $m = 4$ это код C_1 над алфавитом из 13 символов мощности 28 с длиной 21, расстоянием 20 и весом кодовых слов 18. Матрица размера 28×21 кодовых слов кода C_1 строится по тому же правилу, что и матрицы в случае (II):

$$C_1 = \begin{bmatrix} B_1 & A_{1,1} & A_{1,2} \\ B_2 & A_{2,1} & A_{2,2} \\ B_3 & A_{3,1} & A_{3,2} \\ B_4 & A_{4,1} & A_{4,2} \end{bmatrix},$$

где каждая из квадратных матриц размера 7×7 циркулянтна и поэтому, как и в случае (II), можно определить матрицу $P(C_1)$ размера 4×7, состоящую из первых строк всех матриц B_r, A_{rs}, $r = 1,2,3,4$, $s = 1,2$:

$$P(C_1) = [P_B \,|\, P_1 \,|\, P_2].$$

Здесь матрица P_B строится так же, как и в случае (II):

$$P_B = \begin{bmatrix} 0 & 1 & 2 & 3 & 3 & 2 & 1 \\ 0 & 4 & 5 & 6 & 6 & 5 & 4 \\ 0 & 7 & 8 & 9 & 9 & 8 & 7 \\ 0 & 10 & 11 & 12 & 12 & 11 & 10 \end{bmatrix}.$$

Матрица P_1 задается в следующем виде:

$$P_1 = \begin{bmatrix} 0 & 1 & 2 & 5 & 6 & 3 & 4 \\ 1 & 9 & 0 & 7 & 8 & 10 & 2 \\ 4 & 8 & 7 & 3 & 0 & 11 & 12 \\ 10 & 6 & 9 & 12 & 11 & 5 & 0 \end{bmatrix},$$

а строками матрицы P_2 являются строки матрицы P_1, записанные в обратном порядке. Нетрудно проверить непосредственно, что расстояние кода C_1 равно 20.

При $m = 5$ это код C_2 над алфавитом из 31 символа мощности 65 с длиной 52, расстоянием 51 и весом кодовых слов 48. Матрица кодовых слов C_2 размера 65×52 выглядит так:

$$C_2 = \begin{bmatrix} A_{1,1} & A_{1,2} & A_{1,3} & A_{1,4} \\ A_{2,1} & A_{2,2} & A_{2,3} & A_{2,4} \\ A_{3,1} & A_{3,2} & A_{3,3} & A_{3,4} \\ A_{4,1} & A_{4,2} & A_{4,3} & A_{4,4} \\ A_{5,1} & A_{5,2} & A_{5,3} & A_{5,4} \end{bmatrix},$$

где каждая из квадратных матриц размера 13×13 циркулянтна. Поэтому можно определить матрицу $P(C_2)$ размера 5×13, состоящую из первых строк всех матриц A_{rs}, $r = 1, 2, 3, 4, 5$, $s = 1, 2, 3, 4$:

$$P(C_2) = [P_1 \,|\, P_2 \,|\, P_3 \,|\, P_4].$$

Матрицы P_s задаются в следующем виде:

$$P_1 = \begin{bmatrix} 1 & 6 & 11 & 16 & 0 & 21 & 22 & 23 & 24 & 16 & 11 & 6 & 1 \\ 2 & 7 & 12 & 17 & 21 & 0 & 25 & 26 & 27 & 17 & 12 & 7 & 2 \\ 3 & 8 & 13 & 18 & 22 & 25 & 0 & 28 & 29 & 18 & 13 & 8 & 3 \\ 4 & 9 & 14 & 19 & 23 & 26 & 28 & 0 & 30 & 19 & 14 & 9 & 4 \\ 5 & 10 & 15 & 20 & 24 & 27 & 29 & 30 & 0 & 20 & 15 & 10 & 5 \end{bmatrix},$$

$$P_2 = \begin{bmatrix} 1 & 21 & 6 & 22 & 11 & 16 & 23 & 16 & 11 & 0 & 9 & 24 & 4 \\ 2 & 0 & 7 & 25 & 12 & 17 & 26 & 17 & 12 & 21 & 10 & 27 & 5 \\ 3 & 26 & 8 & 28 & 13 & 18 & 0 & 18 & 13 & 23 & 6 & 29 & 1 \\ 4 & 27 & 9 & 29 & 14 & 19 & 30 & 19 & 14 & 24 & 7 & 0 & 2 \\ 5 & 25 & 10 & 0 & 15 & 20 & 28 & 20 & 15 & 22 & 8 & 30 & 3 \end{bmatrix},$$

$$P_3 = \begin{bmatrix} 0 & 1 & 6 & 21 & 5 & 16 & 22 & 20 & 11 & 23 & 8 & 12 & 24 \\ 21 & 2 & 7 & 0 & 12 & 16 & 25 & 18 & 1 & 26 & 9 & 13 & 27 \\ 22 & 3 & 8 & 25 & 13 & 17 & 0 & 18 & 2 & 28 & 10 & 14 & 29 \\ 23 & 4 & 9 & 26 & 14 & 17 & 28 & 19 & 3 & 0 & 6 & 15 & 30 \\ 24 & 5 & 10 & 27 & 15 & 20 & 29 & 19 & 4 & 30 & 7 & 11 & 0 \end{bmatrix},$$

$$P_4 = \begin{bmatrix} 1 & 6 & 0 & 11 & 21 & 10 & 22 & 12 & 23 & 17 & 24 & 20 & 3 \\ 2 & 7 & 21 & 12 & 0 & 6 & 25 & 15 & 26 & 18 & 27 & 16 & 4 \\ 3 & 8 & 22 & 11 & 25 & 9 & 0 & 16 & 28 & 19 & 29 & 15 & 5 \\ 4 & 9 & 23 & 13 & 26 & 8 & 28 & 14 & 0 & 18 & 30 & 20 & 1 \\ 5 & 7 & 24 & 14 & 27 & 10 & 29 & 13 & 30 & 19 & 0 & 17 & 2 \end{bmatrix}.$$

Непосредственная, но достаточно утомительная проверка показывает, что расстояние кода C_2 равно 51.

Хотя нам и не удалось для случая (I) построить бесконечное семейство кодов с заданными параметрами, но три указанных кода оставляют надежду на то, что такое семейство существует.

7. Осталось рассмотреть случай (III). Вначале отметим, что если в транспонированной матрице кодовых слов заменить все ненулевые символы на 0, а нулевой символ на 1, то эта матрица будет представлять собой двоичный код, лежащий на границе Джонсона, с параметрами

$$N = \frac{m^2 - 2m + 2}{2}, \quad n = m^2 - 2m + 2, \quad d = 2(m-1), \quad w = m,$$

или, что то же самое, блок-схему $B(v = 2k^2 - 2k + 1, k, 1)$, где $k = m/2$. Следовательно, существование таких блок-схем является необходимым условием существования кода с параметрами (III), но далеко не достаточным. Ведь наличие блок-схемы позволяет лишь правильно расположить нулевые символы в кодовой матрице, а правильное расположение пар ненулевых символов в каждом столбце – это отдельная нелегкая задача. Мы знаем, например, что указанные блок-схемы построены при $k = 2, 3, 4, 5$ (т.е. при $m = 4, 6, 8, 10$), но лишь при $m = 4$ соответствующий равновесный четверичный код длины 5 мощности 10 с расстоянием 4 давно известен (см., например, [8]).

8. В [3] была поставлена задача построения посимвольно равномерных эквидистантных кодов минимальной длины при заданных параметрах q, k, m (напомним, что каждый ненулевой символ встретится в столбце кодовой матрицы k раз, а нулевой символ – m раз; очевидно, что число кодовых слов $N = (q-1)k + m$). Согласно теореме 2 длина такого кода равна

$$n = \frac{\lambda N(N-1)}{m(m-1) + (N-m)(k-1)}, \tag{15}$$

где через $\lambda = n - d$ обозначена разность между длиной кода и его расстоянием. Так как n – целое число, то очевидно, что минимальная длина достигается при наименьшем λ, таком что правая дробь в (15) становится целым числом. Обозначим через (a, b) наибольший общий делитель чисел a и b. Ясно, что минимальное λ, при котором дробь $\dfrac{\lambda a}{b}$ становится целым числом, равно $\dfrac{b}{(a,b)}$. Следовательно, имеет место

Предложение 4. *Минимальная длина n посимвольно равномерного эквидистантного кода с параметрами q, k, m удовлетворяет неравенству*

$$n \geqslant \frac{N(N-1)}{(N(N-1), m(m-k) + N(k-1))}, \tag{16}$$

где $N = (q-1)k + m$.

Нетрудно непосредственно проверить, что все коды, приведенные в пп. 3, 4, 6, 7, имеют минимальную длину.

СПИСОК ЛИТЕРАТУРЫ

1. *Beth T., Jungnickel D., Lenz B.* Design Theory. Cambridge: Cambridge Univ. Press, 1999.
2. *Семаков Н.В., Зиновьев В.А.* Эквидистантные q-ичные коды с максимальным расстоянием и разрешимые уравновешенные неполные блок-схемы // Пробл. передачи информ. 1968. Т. 4. № 2. С. 3–10. `http://mi.mathnet.ru/ppi1845`

3. *Бассалыго Л.А., Зиновьев В.А., Лебедев В.С.* Симметричные блок-схемы и оптимальные эквидистантные коды // Пробл. передачи информ. 2020. Т. 56. № 3. С. 50–58. https://doi.org/10.31857/S055529232003002X
4. *Sinha K., Sinha N.* A Class of Optimal Quaternary Codes // Ars Combin. 2010. V. 94. P. 61–64.
5. *Бассалыго Л.А.* Новые верхние границы для кодов, исправляющих ошибки // Пробл. передачи информ. 1965. Т. 1. № 4. С. 41–44. http://mi.mathnet.ru/ppi762
6. *Бассалыго Л.А., Зиновьев В.А., Лебедев В.С.* Об m-квазиразрешимых блок-схемах и q-ичных равновесных кодах // Пробл. передачи информ. 2018. Т. 54. № 3. С. 54–61. http://mi.mathnet.ru/ppi2272
7. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
8. *Todorov T., Bogdanova G., Yorgova T.* Lexicographic Constant-Weight Equidistant Codes over the Alphabet of Three, Four and Five Elements // Intell. Inf. Manag. 2010. V. 2. № 3. P. 183–187. https://doi.org/10.4236/iim.2012.23021

Бассалыго Леонид Александрович
Зиновьев Виктор Александрович
Лебедев Владимир Сергеевич
Институт проблем передачи информации
им. А.А. Харкевича РАН
bass@iitp.ru
vazinov@iitp.ru
lebedev37@mail.ru

Поступила в редакцию
16.04.2021
После доработки
11.09.2021
Принята к публикации
01.10.2021

EDN: YSXKJZ
ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 1**

УДК 621.391 : 519.725.3

© 2022 г. **А.Ю. Баринов**

ПРИВЕДЕНИЕ РЕКУРСИВНЫХ ФИЛЬТРОВ К ПРЕДСТАВЛЕНИЮ РАЗРЕЖЕННЫМИ МАТРИЦАМИ

Рекурсивный фильтр как часть рекурсивного сверточного кодера имеет практическую значимость в схемах составных кодов с перемежением. В статье рассматривается матричное описание рекурсивных фильтров во временной области над конечным полем $\mathbb{F}_2$. Исследовано и формализовано приведение матриц, описывающих рекурсивные фильтры (с перфорацией), к разреженным матрицам специального вида. Основное внимание направлено на исследование двоичных последовательностей рекурсивных фильтров с перфорацией каждого второго бита. Дается приложение полученных разреженных матриц к нахождению перфорированных передаточных функций для таких фильтров. Предложен подход к минимальной схемной реализации перфорированных передаточных функций. Приведены примеры схемной реализации перфорированных турбокодов как двойных турбокодов.

Ключевые слова: рекурсивный фильтр, импульсная характеристика, перфорация, разреженная матрица, сверточный код, усечение сверточного кода, рекурсивный систематический сверточный кодер, минимальный кодер, двойной турбокод, идентификация перемежителя.

DOI: 10.31857/S0555292322010028

§ 1. Введение

Начиная с появления турбокодов [1], рекурсивные сверточные кодеры (кодеры с обратной связью) стали привлекать к себе повышенный интерес. Сегодня данные кодеры находят применение во многих передовых схемах помехоустойчивого кодирования, включая: классические (сверточные) турбокоды [1,2], двойные (duo-binary) турбокоды [3, 4], коды повторения-накопления (repeat accumulate (RA) codes) [5, 6]. Перечисленные коды часто называют турбоподобными [7].

Рекурсивный сверточный кодер по сути является сверточным кодером общего вида и описывается рациональной матричной передаточной функцией (рациональной порождающей матрицей)

$$G(D) = \big\{g_{ij}(D) = f_{ij}(D)/q_{ij}(D),\ i = 0, \ldots, k-1,\ j = 0, \ldots, n-1\big\},$$

элементы которой – рациональные передаточные функции соответствующих рекурсивных фильтров, где формальная переменная D имеет смысл задержки на один такт.

На практике, как правило, используют рекурсивные систематические сверточные кодеры (recursive systematic convolutional (RSC) encoders). Для достижения высоких скоростей передачи проверочная часть RSC-кодера подвергается перфорации (выкалыванию) [8], часто удаляют каждый второй символ проверочной части [1, 9].

Известно, что кодеры, порождающие один и тот же код, называются эквивалентными. В [10] показано, что для любого рекурсивного сверточного кодера $G_1(D)$ можно найти эквивалентный сверточный кодер $G_2(D)$ как

$$G_2(D) = Q(D)G_1(D),$$

где $Q(D) = \text{НОК}(\{q_{ij}(D)\})$.

Следовательно, исследование свойств сверточных кодов можно проводить на основе рассмотрения полиномиальных передаточных функций нерекурсивных фильтров. Например, рекурсивный фильтр $\frac{f(D)}{q(D)}$ можно привести к нерекурсивному фильтру $f(D) = q(D)\frac{f(D)}{q(D)}$.

В случае перфорации выходной последовательности рекурсивного фильтра вид его перфорированной рациональной передаточной функции не очевиден. С другой стороны, возможно представление рекурсивного фильтра с перфорацией во временной форме в виде матрицы бесконечного порядка, строки которой – перфорированные сдвиги импульсной характеристики фильтра.

В работе [11] предложено применять произведение матрицы рекурсивного фильтра (с перфорацией) $\frac{f(D)}{q(D)}$ на матрицу фильтра $q(D)$ справа к идентификации перемежителя турбоподобного кода. Это преобразование приводит к разреженной матрице со структурой и показало практическую ценность при идентификации перемежителя в условиях помех.

Основная цель настоящей статьи – исследование свойств (перфорированной) последовательности рекурсивного фильтра $\frac{f(D)}{q(D)}$ на основе анализа произведения матрицы данного фильтра на матрицу фильтра $q(D)$ во временной форме. В настоящей статье обобщается и доказывается теоретический результат, полученный в [11], а также рассматривается его приложение к нахождению полиномиального представления и схемной реализации RSC-кодера с перфорацией.

Статья организована следующим образом. В § 2 даются основные определения и обозначения, рассматривается матричное описание рекурсивных фильтров во временной области. В § 3 представлены результаты о разреженных матрицах, полученных из (перфорированных) матриц рекурсивных фильтров, в частности, с перфорацией каждого второго бита на выходе. В § 4 рассмотрено приложение представленных результатов к нахождению перфорированных передаточных функций для рекурсивных фильтров с перфорацией, предложен подход к минимальной схемной реализации данных функций, обсуждаются возможные схемные реализации некоторых турбокодов. Заключение дано в § 5.

§ 2. Предварительные сведения

О п р е д е л е н и е 1. Множество всевозможных последовательностей на выходе линейной схемы, приведенной на рис. 1, назовем сверточным кодом со скоростью $R = k/n$.

На практике в основном используются двоичные сверточные коды, поэтому далее в статье рассматриваются последовательности битов (логических 0 (нулей) и 1 (единиц)) и операции в конечном поле $\mathbb{F}_2$.

На каждом такте работы кодера ($i = 0, 1, \ldots$) на его вход поступает блок из k входных информационных битов $\boldsymbol{u}_i = (u_{i,1}, \ldots, u_{i,k})$, тогда как с выхода схемы считывается очередной кодовый блок из n кодовых битов $\boldsymbol{v}_i = (v_{i,1}, \ldots, v_{i,n})$. Таким образом, любой полубесконечной информационной последовательности $\boldsymbol{u} = (\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots)$ сопоставляется полубесконечное кодовое слово $\boldsymbol{v} = (\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots)$.

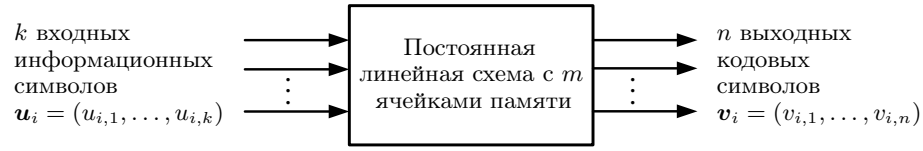

Рис. 1. Сверточный кодер со скоростью $R = k/n$

Кодирование сверточным кодом в полиномиальном виде представляет собой произведение

$$\boldsymbol{v}(D) = \boldsymbol{u}(D)G(D),$$

где $G(D)$ – матричная передаточная функция сверточного кодера.

Перфорированные сверточные коды были введены в [12] для получения высокоскоростных кодов. Перфорация кода состоит в систематическом удалении из процесса передачи в канал проверочных битов с выхода кодера. Матрица перфорации **Perf** задает правило удаления выходных битов. Обычно правило перфорации является периодическим [13].

Определение 2. Для сверточного кодера со скоростью $R = k/n$ матрица перфорации **Perf** – это двоичная $(n \times n_p)$-матрица, элементы которой perf_{ij} указывают, что соответствующий выходной бит будет передан ($\mathrm{perf}_{ij} = 1$) или нет ($\mathrm{perf}_{ij} = 0$), где n – количество выходов кодера, n_p – период перфорации, i – номер выхода, j – номер такта. Каждая строка данной матрицы представляет собой вектор перфорации $\mathbf{perf}_i$ для i-го выхода кодера.

Следует заметить, что множество последовательностей одного и того же сверточного кода может быть сгенерировано различными кодерами, причем некоторые кодеры могут быть предпочтительнее других. Для составных кодов часто выбирают компонентные рекурсивные сверточные кодеры, в том числе с перфорацией. Например, классический турбокод обычно основан на параллельном соединении RSC-кодеров вида $(1 \quad f(D)/q(D))$, тогда как в двойных турбокодах могут использовать RSC-кодеры вида $\begin{pmatrix} 1 & 0 & f(D)/q(D) \\ 0 & 1 & g(D)/q(D) \end{pmatrix}$. Неотъемлемой частью систематических кодов повторения-накопления, а также их модификаций, является RSC-кодер конкретного вида – $(1 \quad 1/(1+D))$ [6].

Рассмотрим RSC-кодер $(1 \quad f(D)/q(D))$. Данный RSC-кодер можно описать порождающей матрицей бесконечного порядка

$$\boldsymbol{G} = (\boldsymbol{I} \quad \boldsymbol{P}),$$

где $\boldsymbol{I}$ – полубесконечная единичная матрица, $\boldsymbol{P}$ – полубесконечная матрица, генерирующая проверочные биты кода.

Матрица $\boldsymbol{P}$ представляет рекурсивный фильтр $f(D)/q(D)$ из состава RSC-кодера во временной области.

Рекурсивные сверточные кодеры строятся на основе рекурсивных фильтров $f(D)/q(D)$ с реализуемой (т.е. $q_0 = 1$) передаточной функцией

$$P(D) = \frac{f(D)}{q(D)} = \frac{f_0 + f_1 D + \ldots + f_m D^m}{1 + q_1 D + \ldots + q_m D^m},$$

где m – память фильтра.

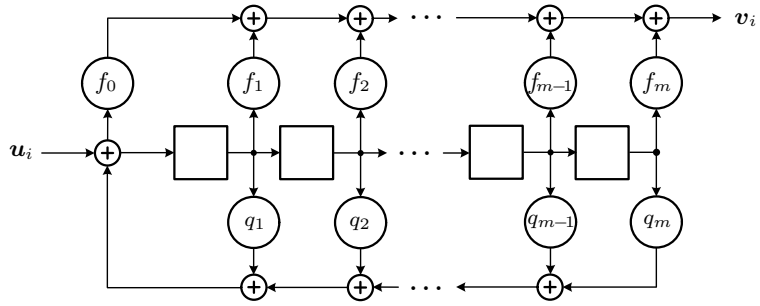

Рис. 2. Каноническая форма цифрового фильтра с вынесенными сумматорами (controller canonical form)

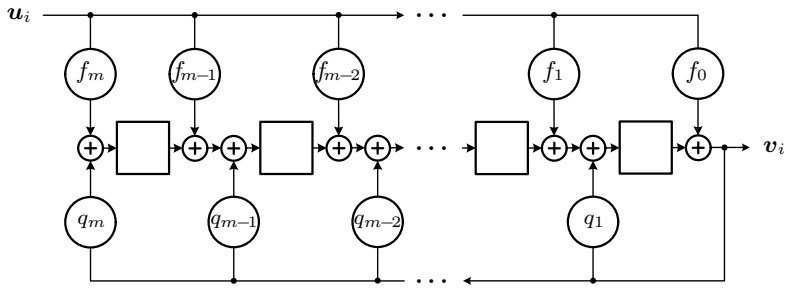

Рис. 3. Каноническая форма цифрового фильтра со встроенными сумматорами (observer canonical form)

Данные на входе и выходе фильтра представим в виде полиномов

$$u(D) = u_0 + u_1 D + u_2 D + \dots,$$
$$v(D) = v_0 + v_1 D + v_2 D + \dots,$$

тогда

$$v(D) = u(D)\frac{f(D)}{q(D)} = u(D)\frac{f_0 + f_1 D + \dots + f_m D^m}{1 + q_1 D + \dots + q_m D^m}.$$

С другой стороны, это равенство можно переписать как

$$v(D) = u(D)(f_0 + f_1 D + \dots + f_m D^m) + v(D)(q_1 D + \dots + q_m D^m).$$

Две канонические реализации фильтра с передаточной функцией $P(D) = f(D)/q(D)$ показаны на рис. 2, 3.

Рекурсивный фильтр использует элементы памяти и выполняет операции в $\mathbb{F}_2$ (т.е. с использованием логики “исключающее ИЛИ”) над содержимым памяти и информационными битами на своем входе. Во временной области рекурсивный фильтр можно описать разностным уравнением

$$v_i = \sum_{j=0}^{m} u_{i-j} f_j + \sum_{j=1}^{m} v_{i-j} q_j, \quad i = 0, 1, \dots, \tag{1}$$

где здесь и далее в статье $x_{\text{ind}} = 0$ для всех $\text{ind} < 0$.

Саму операцию фильтрации можно записать как

$$v_i = \sum_{j=0}^{m} u_{i-j} p_i, \quad i = 0, 1, \ldots,$$

где здесь и далее $\{p_i\} = (p_0, p_1, \ldots)$ – биты бесконечной импульсной характеристики (БИХ) рекурсивного фильтра $P(D) = f(D)/q(D)$.

Данную операцию в матричном виде можно представить как

$$\boldsymbol{v} = \boldsymbol{u}\boldsymbol{P},$$

где $\boldsymbol{P}$ – полубесконечная матрица, строки которой – сдвиги БИХ рекурсивного фильтра.

В реальности сеансы связи конечны, информацию передают блоками конечной длины (например, несколько тысяч бит) [13]. Самый простой способ получения блочного кода из сверточного кода – прямое усечение (direct truncation) [14]. Для RSC-кодера $(1 \quad f(D)/q(D))$ конструкция с прямым усечением кодовых последовательностей приводит к блочному $(2K, K, d_{DT})$-коду C_{DT} с матрицей $\boldsymbol{P}^{(DT)}$, генерирующей проверочные биты данного кода

$$\boldsymbol{P}^{(DT)} = \begin{pmatrix} p_0 & p_1 & \cdots & & p_{K-1} \\ & p_0 & p_1 & \cdots & p_{K-2} \\ & & \ddots & \ddots & \vdots \\ & & & p_0 & p_1 \\ & & & & p_0 \end{pmatrix},$$

здесь и далее пустые области матриц считаются заполненными нулями.

Усечение с обнулением состояния (zero-tail termination) предусматривает добавление "хвоста" из m нулей к каждому информационному блоку длины K, при этом на период заполнения памяти m нулями обратную связь кодера отключают [15]. В случае RSC-кодера $(1 \quad f(D)/q(D))$ данная конструкция приводит к блочному $(2K + 2m, K, d_{ZT})$-коду C_{ZT} с матрицей $\boldsymbol{P}^{(ZT)}$, генерирующей проверочные биты данного кода

$$\boldsymbol{P}^{(ZT)} = \begin{pmatrix} p_0 & p_1 & \cdots & & p_{K-1} & & & \\ & p_0 & p_1 & \cdots & p_{K-2} & & & \\ & & \ddots & \ddots & \vdots & f_m & & \\ & & & & & \vdots & \ddots & \\ & & & p_0 & p_1 & \vdots & & \\ & & & & p_0 & f_1 & \cdots & f_m \end{pmatrix}.$$

При циклическом усечении (tail-biting) [10,14] для RSC-кодера $(1 \quad f(D)/q(D))$ на длине K получаем блочный $(2K, K, d_{TB})$-код C_{TB} с матрицей $\boldsymbol{P}^{(TB)}$, генерирующей проверочные биты данного кода

$$\boldsymbol{P}^{(TB)} = \begin{pmatrix} p_0 & p_1 & \cdots & p_{K-2} & p_{K-1} \\ p_{K-1} & p_0 & \cdots & p_{K-3} & p_{K-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ p_2 & p_3 & \cdots & p_0 & p_1 \\ p_1 & p_2 & \cdots & p_{K-1} & p_0 \end{pmatrix}.$$

§ 3. Приведение рекурсивных фильтров к представлению разреженными матрицами

В этом параграфе проанализируем приведение матриц, описывающих рекурсивные фильтры $f(D)/q(D)$ (с перфорацией) во временной форме, к разреженным матрицам специального вида. Данное приведение выражается в умножении на матрицу $\boldsymbol{Q}$, соответствующую полиному $q(D)$ в знаменателе рекурсивного фильтра.

Определение 3. Матрица, имеющая небольшой процент ненулевых элементов, называется разреженной.

В настоящей статье матрица размера $M \times K$, содержащая τ единиц, будет считаться разреженной, если $\tau \ll MK$, причем $MK > 10^3$.

Определение 4. Разреженная матрица $\boldsymbol{G}$ называется ленточной матрицей с шириной ленты β, если для всех ее ненулевых элементов g_{ij} выполняется условие $|i-j| \leqslant \beta$.

Рассмотрим рекурсивный фильтр $P(D) = f(D)/q(D)$, которому во временной области соответствует полубесконечная матрица $\boldsymbol{P}$.

Теорема 1. *Пусть $\boldsymbol{P}$ – матрица, строки которой являются сдвигами импульсного отклика фильтра $f(D)/q(D)$, $\boldsymbol{Q}$ – матрица, строки которой являются сдвигами импульсного отклика фильтра $q(D)$. Тогда $\boldsymbol{F} = \boldsymbol{QP} = \boldsymbol{PQ}$ – матрица, строки которой являются сдвигами импульсного отклика фильтра $f(D)$ и представляет собой ленточную матрицу с шириной ленты $\beta \leqslant m+1$.*

Доказательство. В полиномиальном представлении матрице $\boldsymbol{P}$ соответствует передаточная функция $P(D) = f(D)/q(D)$, тогда передаточная функция $q(D)P(D) = f(D)$ во временной области может быть представлена в виде

$$\boldsymbol{F} = \boldsymbol{QP} = \boldsymbol{PQ} = \begin{pmatrix} f_0 & f_1 & \dots & f_m & & \\ & f_0 & f_1 & \dots & f_m & \\ & & \ddots & \ddots & \ddots & \ddots \end{pmatrix},$$

где

$$f_i = \sum_{j=0}^{m} q_j p_{i-j}, \quad i = 0, 1, \dots, m. \quad \blacktriangle$$

Последнее уравнение можно использовать для построения рекурсивного фильтра $f(D)/q(D)$ по первым битам его БИХ при известном $q(D)$.

Если определенные биты на выходе рекурсивного фильтра удаляются, то данному фильтру с перфорацией соответствует матрица $\boldsymbol{P}_{\text{perf}}$.

Обычно правило перфорации является периодическим. Например, при удалении каждого второго бита на выходе рекурсивного фильтра согласно вектору перфорации $\mathbf{perf} = (0 \;\; 1)$ получим матрицу

$$\boldsymbol{P}_{(0\ 1)} = \begin{pmatrix} p_1 & p_3 & p_5 & \dots & & \\ p_0 & p_2 & p_4 & \dots & & \\ & p_1 & p_3 & p_5 & \dots & \\ & p_0 & p_2 & p_4 & \dots & \\ & & \ddots & \ddots & \ddots & \ddots \end{pmatrix},$$

согласно вектору перфорации $\mathbf{perf} = (1 \quad 0)$ соответственно получим

$$\boldsymbol{P}_{(1\ 0)} = \begin{pmatrix} p_0 & p_2 & p_4 & \dots & & \\ & p_1 & p_3 & p_5 & \dots & \\ & p_0 & p_2 & p_4 & \dots & \\ & & p_1 & p_3 & p_5 & \dots \\ & & p_0 & p_2 & p_4 & \dots \\ & & & \ddots & \ddots & \ddots & \ddots \end{pmatrix}.$$

Далее в статье перфорация каждого второго бита преимущественно рассматривается на примере вектора перфорации $\mathbf{perf} = (0 \quad 1)$, что соответствует перфорации нечетных битов. Рассуждения для перфорации четных битов, т.е. согласно вектору перфорации $\mathbf{perf} = (1 \quad 0)$, аналогичны.

Из теоремы 1 получаем

Следствие 1. *Матрицу* $\boldsymbol{F}_{\text{perf}}$, *описывающую фильтр* $f(D)$ *с перфорацией, можно получить в результате умножения матрицы* $\boldsymbol{P}_{\text{perf}}$ *на соответствующую полиному обратной связи* $q(D)$ *ленточную матрицу* $\boldsymbol{Q}$ *слева*:

$$\boldsymbol{F}_{\text{perf}} = \boldsymbol{Q}\boldsymbol{P}_{\text{perf}},$$

альтернативным образом матрицу $\boldsymbol{F}_{\text{perf}}$ *можно получить удалением определенных столбцов соответствующей матрицы* $\boldsymbol{F}$.

С другой стороны, для решения задачи идентификации перемежителя в работе [11] предложено умножать матрицу $\boldsymbol{P}_{(0\ 1)}$, описывающую рекурсивный фильтр $f(D)/q(D)$ с перфорацией, на соответствующую полиному обратной связи $q(D)$ ленточную матрицу $\boldsymbol{Q}$ справа. При этом получим следующую матрицу:

$$\boldsymbol{Y}_{(0\ 1)} = \boldsymbol{P}_{(0\ 1)}\boldsymbol{Q}. \tag{2}$$

В работе [11] утверждается, что матрица $\boldsymbol{Y}_{(0\ 1)}$ генерирует модифицированную перфорированную последовательность рекурсивного фильтра, каждый член которой зависит от ограниченного количества $\leqslant 2m$ входных информационных битов. Докажем данное утверждение, которое имеет значение для идентификации перемежителя турбоподобного кода в условиях априорной неопределенности при наличии помех.

Теорема 2. *Пусть матрица* $\boldsymbol{P}_{(0\ 1)}$ *описывает рекурсивный фильтр* $\dfrac{f(D)}{q(D)} = \dfrac{f_0 + f_1 D + \ldots + f_m D^m}{1 + q_1 D + \ldots + q_m D^m}$ *с перфорацией. Тогда матрица* $\boldsymbol{Y}_{(0\ 1)} = \boldsymbol{P}_{(0\ 1)}\boldsymbol{Q}$ *является разреженной.*

Доказательство. Матрица $\boldsymbol{Y}_{(0\ 1)}$ является результатом произведения матриц специального вида, следовательно, может быть представлена в виде

$$\boldsymbol{Y}_{(0\ 1)} = \begin{pmatrix} y_1 & y_3 & y_5 & \dots & \\ y_0 & y_2 & y_4 & \dots & \\ & y_1 & y_3 & y_5 & \dots \\ & y_0 & y_2 & y_4 & \dots \\ & & \ddots & \ddots & \ddots & \ddots \end{pmatrix},$$

где

$$y_i = \sum_{j=0}^{m} q_j p_{i-2j}, \quad i = 0, 1, \ldots \tag{3}$$

Если в уравнении (1) информационная последовательность является импульсным (единичным) воздействием $\{u_i\} = (1, 0, 0, 0, \ldots)$, то получим уравнение импульсной характеристики рекурсивного фильтра $f(D)/q(D)$

$$p_i = f_i + \sum_{j=1}^{m} q_j p_{i-j}, \quad i = 0, 1, \ldots, \tag{4}$$

где $f_i \stackrel{\text{def}}{=} 0$ для всех $i > m$.

Уравнение (3) с учетом (4) и $q_0 = 1$ примет вид

$$y_i = p_i + \sum_{j=1}^{m} q_j p_{i-2j} = f_i + \sum_{j=1}^{m} q_j p_{i-j} + \sum_{j=1}^{m} q_j p_{i-2j} =$$
$$= f_i + \sum_{j=1}^{m} q_j f_{i-j} + \left(\sum_{j=1}^{m} q_j \sum_{l=1}^{m} q_l p_{i-j-l} + \sum_{j=1}^{m} q_j p_{i-2j} \right),$$

в поле $\mathbb{F}_2$ выражение в скобках равно нулю, следовательно,

$$y_i = \sum_{j=0}^{m} q_j f_{i-j}, \quad i = 0, 1, \ldots,$$

где $f_{i-j} \stackrel{\text{def}}{=} 0$ для всех $i - j > m$.

Тогда понятно, что $y_i = 0$ для всех $i > 2m$, и матрицу $\boldsymbol{Y}_{(0\ 1)}$ можно переписать в виде

$$\boldsymbol{Y}_{(0\ 1)} = \begin{pmatrix} y_1 & y_3 & \cdots & y_{2m-1} & & & \\ y_0 & y_2 & \cdots & y_{2m-2} & y_{2m} & & \\ & y_1 & \cdots & y_{2m-3} & y_{2m-1} & & \\ & y_0 & \cdots & y_{2m-4} & y_{2m-2} & y_{2m} & \\ & & \ddots & \vdots & y_{2m-3} & y_{2m-1} & \\ & & & y_1 & \vdots & y_{2m-2} & \ddots \\ & & & y_0 & y_2 & \vdots & \ddots \\ & & & & y_1 & y_3 & \ddots \\ & & & & y_0 & y_2 & \ddots \\ & & & & & y_1 & \ddots \\ & & & & & y_0 & \ddots \\ & & & & & & \ddots \end{pmatrix}, \tag{5}$$

где

$$y_i = \sum_{j=0}^{m} q_j f_{i-j}, \quad i = 0, 1, \ldots, 2m, \tag{6}$$

где $f_{i-j} \stackrel{\text{def}}{=} 0$ для всех $i - j > m$.

Таким образом, матрица $\boldsymbol{Y}_{(0\ 1)}$ является разреженной. ▲

Пусть матрица $\boldsymbol{P'}_{(0\ 1)}$ описывает рекурсивный фильтр $q(D)/f(D)$, тогда для матрицы (5) справедливо свойство

$$\boldsymbol{Y}_{(0\ 1)} = \boldsymbol{P}_{(0\ 1)}\boldsymbol{Q} = \boldsymbol{P'}_{(0\ 1)}\boldsymbol{F}.$$

Данное свойство следует из теоремы 2 и проверяется вычислением согласно уравнению (6), которое симметрично относительно своих членов.

Особый случай представляют RA-коды, а также их модификации, где одной из ключевых компонент является фильтр с передаточной функцией $1/(1+D)$ с разными правилами перфорации.

Следующий пример иллюстрирует приведение матрицы $\boldsymbol{P}_{\text{perf}}$, соответствующей фильтру $1/(1+D)$ с произвольной перфорацией, к разреженному виду.

Пример 1. Для матрицы $\boldsymbol{P}_{\text{perf}}$, описывающей рекурсивный фильтр $1/(1+D)$, получим вид матрицы $\boldsymbol{Y}_{\text{perf}} = \boldsymbol{P}_{\text{perf}}\boldsymbol{Q}$, где матрица $\boldsymbol{Q}$ соответствует полиному $q(D) = 1 + D$.

БИХ рекурсивного фильтра $1/(1+D)$ во временной области представляет собой последовательность единиц $\{p_i\} = (1111111\ldots)$, которая инвариантна к перфорации. Следовательно, матрица $\boldsymbol{P}_{\text{perf}}$, порождающая перфорированную последовательность рекурсивного фильтра $1/(1+D)$, имеет перфорированную ступенчатую структуру, заполненную единицами, при этом высота каждой ступени зависит от правила перфорации.

Тогда с учетом структур матриц $\boldsymbol{P}_{\text{perf}}$ и $\boldsymbol{Q}$ получим

$$\boldsymbol{Y}_{\text{perf}} = \begin{pmatrix} 1 & & & & \\ \vdots & & & & \\ 1 & & & & \\ & 1 & & & \\ & \vdots & & & \\ & 1 & \ddots & & \\ & & & 1 & \\ & & & \vdots & \\ & & & 1 & \ddots \end{pmatrix}.$$

Таким образом, матрица $\boldsymbol{Y}_{\text{perf}}$ представляет собой разреженную матрицу со ступенчатой структурой, где длина серии единиц в каждом блоке-столбце зависит от правила перфорации.

В связи с тем, что в практических приложениях данные передают блоками конечной длины, рассмотрим разреженные матрицы, соотносящиеся с матрицами, генерирующими проверочные биты блочных кодов.

Очевидно, что при прямом усечении выполнены равенства $\boldsymbol{F}^{(DT)} = \boldsymbol{P}^{(DT)}\boldsymbol{Q}^{(DT)}$ и $\boldsymbol{Y}^{(DT)}_{(0\ 1)} = \boldsymbol{P}^{(DT)}_{(0\ 1)}\boldsymbol{Q}^{(DT)}$, где $\boldsymbol{Q}^{(DT)}$ – квадратная матрица соответствующего размера, полученная из матрицы $\boldsymbol{Q}$ прямым усечением.

Также понятно, что в случае усечения с обнулением состояния имеем $\boldsymbol{F}^{(ZT)} = \boldsymbol{P}^{(ZT)}\boldsymbol{Q}^{(ZT)}$, где $\boldsymbol{Q}^{(ZT)}$ – матрица размера $(K+m)\times(K+m)$

$$\boldsymbol{Q}^{(ZT)} = \begin{pmatrix} q_0 & q_1 & \cdots & & q_{K-1} & & & \\ & q_0 & q_1 & \cdots & q_{K-2} & & & \\ & & \ddots & \ddots & \vdots & & & \\ & & & q_0 & q_1 & & & \\ & & & & q_0 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix},$$

и $\boldsymbol{Y}^{(ZT)}_{(0\ 1)} = \boldsymbol{P}^{(ZT)}_{(0\ 1)}\boldsymbol{Q}^{(ZT)}$, где $\boldsymbol{Q}^{(ZT)}$ – матрица соответствующего размера.

Теорема 3. *Пусть матрица $\boldsymbol{P}^{(TB)}$ описывает рекурсивный фильтр при циклическом усечении. Тогда матрица $\boldsymbol{A}^{(TB)} = \boldsymbol{P}^{(TB)}\boldsymbol{Q}^{(TB)}$ является разреженной циркулянтной матрицей.*

Доказательство. $\boldsymbol{Q}^{(TB)}$ – циркулянтная матрица, полученная из матрицы $\boldsymbol{Q}$ циклическим усечением на длине K. Из структур матриц $\boldsymbol{P}^{(TB)}$ и $\boldsymbol{Q}^{(TB)}$ видно, что $\boldsymbol{A}^{(TB)} = \boldsymbol{P}^{(TB)}\boldsymbol{Q}^{(TB)} = \boldsymbol{Q}^{(TB)}\boldsymbol{P}^{(TB)}$, где

$$\boldsymbol{A}^{(TB)} = \begin{pmatrix} a_0 & a_1 & \dots & a_{K-2} & a_{K-1} \\ a_{K-1} & a_0 & \dots & a_{K-3} & a_{K-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_3 & \dots & a_0 & a_1 \\ a_1 & a_2 & \dots & a_{K-1} & a_0 \end{pmatrix},$$

$$a_i = \sum_{j=0}^{m} q_j p_{(i-j+K) \bmod K}, \quad i = 0, 1, \dots, K-1.$$

Данное уравнение с учетом (4) и равенства $q_0 = 1$ примет вид

$$a_i = f_i + \sum_{j=1}^{m} q_j p_{i-j} + \sum_{j=1}^{m} q_j p_{(i-j+K) \bmod K},$$

где $f_i \stackrel{\text{def}}{=} 0$ для всех $i > m$.

Понятно, что при $i > m$ имеем $a_i = 0$. Тогда матрицу $\boldsymbol{A}^{(TB)}$ можно представить в виде

$$\boldsymbol{A}^{(TB)} = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_m & & & \\ & a_0 & a_1 & a_2 & \dots & a_m & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & a_0 & a_1 & a_2 & \dots & a_m \\ a_m & & & & a_0 & a_1 & \dots & a_{m-1} \\ \vdots & \ddots & & & & \ddots & \ddots & \vdots \\ a_1 & \dots & a_m & & & & & a_0 \end{pmatrix},$$

где

$$a_i = \sum_{j=0}^{m} q_j p_{(i-j+K) \bmod K}, \quad i = 0, 1, \dots, m. \quad \blacktriangle$$

Теорема 4. *Пусть $\boldsymbol{P}^{(TB)}_{(0\ 1)}$ – циркулянтная матрица, описывающая рекурсивный фильтр с перфорацией. Тогда матрица $\boldsymbol{B}^{(TB)}_{(0\ 1)} = \boldsymbol{P}^{(TB)}_{(0\ 1)}\boldsymbol{Q}^{(TB)}$ является разреженной циркулянтной матрицей.*

Доказательство. Рассмотрим матрицу

$$\boldsymbol{B}^{(TB)}_{(0\ 1)} = \begin{pmatrix} b_1 & b_3 & \dots & b_{K-3} & b_{K-1} \\ b_0 & b_2 & \dots & b_{K-4} & b_{K-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_3 & b_5 & \dots & b_{K-1} & b_1 \\ b_2 & b_4 & \dots & b_{K-2} & b_0 \end{pmatrix},$$

где

$$b_i = \sum_{j=0}^{m} q_j p_{(i-2j+K) \bmod K}, \quad i = 0, 1, \ldots, K-1.$$

Данное уравнение с учетом (4) и $q_0 = 1$ примет вид

$$b_i = f_i + \sum_{j=1}^{m} q_j f_{i-j} + \left(\sum_{j=1}^{m} q_j \sum_{l=1}^{m} q_l p_{i-j-l} + \sum_{j=1}^{m} q_j p_{(i-2j+K) \bmod K} \right),$$

где $f_i \stackrel{\text{def}}{=} 0$ для всех $i > m$, $f_{i-j} \stackrel{\text{def}}{=} 0$ для всех $i - j > m$.

В поле $\mathbb{F}_2$ при $i \geqslant 2m$ выражение в скобках равно нулю, следовательно, при $i > 2m$ имеем $b_i = 0$. Тогда матрицу $\boldsymbol{B}^{(TB)}_{(0\ 1)}$ можно представить в виде

$$\boldsymbol{B}^{(TB)}_{(0\ 1)} = \begin{pmatrix}
b_1 & b_3 & \ldots & b_{2m-1} & & & & & & & \\
b_0 & b_2 & \ldots & b_{2m-2} & b_{2m} & & & & & & \\
 & b_1 & \ldots & b_{2m-3} & b_{2m-1} & & & & & & \\
 & b_0 & \ldots & b_{2m-4} & b_{2m-2} & \ddots & & & & & \\
 & & \ddots & \vdots & \vdots & \ddots & b_{2m} & & & & \\
 & & & b_1 & b_3 & \ddots & b_{2m-1} & & & & \\
 & & & b_0 & b_2 & \ddots & b_{2m-2} & b_{2m} & & & \\
 & & & & b_1 & \ddots & b_{2m-3} & b_{2m-1} & & & \\
 & & & & b_0 & \ddots & b_{2m-4} & b_{2m-2} & b_{2m} & & \\
 & & & & & \ddots & \vdots & \vdots & \vdots & \ddots & b_{2m} \\
 & & & & & & b_1 & b_3 & b_5 & \ldots & b_{2m-1} \\
b_{2m} & & & & & & b_0 & b_2 & b_4 & \ldots & b_{2m-2} \\
b_{2m-1} & & & & & & & b_1 & b_3 & \ldots & b_{2m-3} \\
b_{2m-2} & b_{2m} & & & & & & b_0 & b_2 & \ldots & b_{2m-4} \\
b_{2m-3} & b_{2m-1} & & & & & & & b_1 & \ldots & b_{2m-5} \\
\vdots & \vdots & & & & & & & & \ddots & \vdots \\
b_3 & b_5 & \ddots & & & & & & & & b_1 \\
b_2 & b_4 & \ldots & b_{2m} & & & & & & & b_0
\end{pmatrix},$$

где

$$b_i = \sum_{j=0}^{m} q_j p_{(i-2j+K) \bmod K}, \quad i = 0, 1, \ldots, 2m. \quad \blacktriangle$$

§ 4. Варианты реализации рекурсивных фильтров с перфорацией

В этом параграфе для некоторых рекурсивных фильтров с перфорацией, воспользовавшись равенством (2), получим перфорированные передаточные функции. Рассмотрим новый подход к минимальной реализации полученных функций и их связь с двойными RSC-кодерами.

Теорема 5. *Перфорация каждого второго бита на выходе рекурсивного фильтра* $P(D) = f(D)/q(D) = \dfrac{f_0 + f_1 D + \ldots + f_m D^m}{1 + q_1 D + \ldots + q_m D^m}$ *приводит к рекурсивному фильтру*

с перфорированной рациональной передаточной функцией

$$P_{(0\ 1)}(D) = \begin{pmatrix} y_1(D)/q(D) \\ y_0(D)/q(D) \end{pmatrix}$$

в случае перфорации нечетных битов, и

$$P_{(1\ 0)}(D) = \begin{pmatrix} y_0(D)/q(D) \\ Dy_1(D)/q(D) \end{pmatrix}$$

в случае перфорации четных битов, где

$$y_0(D) = y_0 + y_2 D + y_4 D^2 + \ldots + y_{2m} D^m,$$
$$y_1(D) = y_1 + y_3 D + y_5 D^2 + \ldots + y_{2m-1} D^{m-1},$$

а коэффициенты $(y_0, y_1, \ldots, y_{2m})$ *определяются формулой* (6) *по коэффициентам* $(f_0, f_1, \ldots, f_m)$ *и* $(q_0 = 1, q_1, \ldots, q_m)$ *фильтра* $f(D)/q(D)$.

Доказательство. В соответствии с теоремой 2 и структурой матрицы (5) равенство (2) можно записать в полиномиальном виде как

$$Y_{(0\ 1)}(D) = P_{(0\ 1)}(D) q(D),$$

где

$$P_{(0\ 1)}(D) = \begin{pmatrix} p_1(D) \\ p_0(D) \end{pmatrix},$$
$$p_0(D) = p_0 + p_2 D + p_4 D^2 + \ldots,$$
$$p_1(D) = p_1 + p_3 D + p_5 D^2 + \ldots,$$

$\{p_i\} = (p_0, p_1, \ldots)$ – БИХ рекурсивного фильтра $P(D) = f(D)/q(D)$,

$$Y_{(0\ 1)}(D) = \begin{pmatrix} y_1(D) \\ y_0(D) \end{pmatrix}.$$

В силу этого

$$P_{(0\ 1)}(D) = \begin{pmatrix} y_1(D)/q(D) \\ y_0(D)/q(D) \end{pmatrix}.$$

Вид функции $P_{(1\ 0)}(D)$ доказывается аналогично. ▲

В качестве следствия теоремы 5 получаем

Следствие 2. *Для рекурсивного фильтра* $P(D) = f(D)/q(D)$ *с* t*-кратной перфорацией каждого второго бита, определяемой вектором* $\mathbf{perf} = (0\ \ 1)$, *перфорированная рациональная передаточная функция имеет вид*

$$P_{\mathrm{perf}^{(t)}}(D) = \begin{pmatrix} y_{2^t-1}(D)/q(D) \\ \cdots\cdots\cdots\cdots \\ y_1(D)/q(D) \\ y_0(D)/q(D) \end{pmatrix},$$

где каждый из полиномов $y_0(D), y_1(D), \ldots, y_{2^t-1}(D)$ *имеет степень* $\leqslant m$.

Рассмотрим следующий

Пример 2. В RA-кодах, а также в их модификациях, одной из ключевых компонент является фильтр с передаточной функцией $1/(1 + D)$ с разными правилами перфорации. Для случая перфорации каждого второго бита на выходе данного

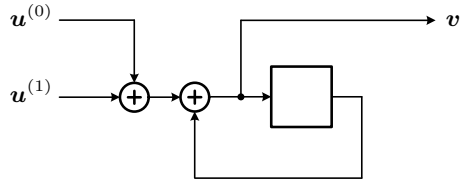

Рис. 4. Двойной рекурсивный фильтр для примера 2

фильтра, применив теорему 5, получим перфорированную рациональную передаточную функцию

$$P_{(0\ 1)}(D) = \begin{pmatrix} 1/(1+D) \\ 1/(1+D) \end{pmatrix}.$$

Легко заметить, что полученную функцию можно оптимально реализовать как двойной рекурсивный фильтр, изображенный на рис. 4.

Однако схемная реализация функции $P_{(0\ 1)}(D)$ общего вида с минимальным количеством элементов памяти далеко не очевидна. Можно воспользоваться стандартным методом минимизации последовательных схем (см., например, [16, 17]).

Представим оригинальный подход к минимальной схемной реализации функции вида $P_{(0\ 1)}(D)$ на основе анализа импульсных характеристик, которые являются полной характеристикой системы.

Сперва сформулируем свойство импульсной характеристики фильтра $f(D)/q(D)$ в виде следующей леммы.

Лемма 1. *Предположим, что полином обратной связи $q(D)$ для рекурсивного фильтра $f(D)/q(D)$ памяти m является примитивным, а это означает, что в состав фильтра входит регистр сдвига с линейной обратной связью (РСЛОС), генерирующий повторяющуюся последовательность максимальной длины $N = 2^m - 1$: $\{\boldsymbol{h}, \boldsymbol{h}, \ldots, \boldsymbol{h}, \ldots\}$, где $\boldsymbol{h} = (h_1, h_2, \ldots, h_N)$. Тогда импульсная характеристика данного фильтра имеет вид $\boldsymbol{p} = \{f_0, \boldsymbol{h}(i), \boldsymbol{h}(i), \ldots, \boldsymbol{h}(i), \ldots\}$, где $\boldsymbol{h}(i)$ – i-кратный циклический сдвиг вектора $\boldsymbol{h}$, т.е. $\boldsymbol{h}(i) = (h_{N-i+1}, h_{N-i+2}, \ldots, h_N, h_1, h_2, \ldots, h_{N-i})$, $i \in [1, \ldots, N]$.*

Доказательство. Рассмотрим отклик рекурсивного фильтра $f(D)/q(D)$, реализованного в канонической форме со встроенными сумматорами (см. рис. 3), на единичный проходящий бит при нулевых начальных условиях S_0. Видно, что на первом такте в ячейки памяти фильтра производится запись некоторого ненулевого состояния S_1, а первый бит импульсной характеристики $p_0 = f_0$. При этом состояние S_1 зависит от мест подсоединения отводов фильтра. Поскольку в состав рекурсивного фильтра входит РСЛОС, генерирующий последовательность максимальной длины, то последующие состояния фильтра имеют вид $\{S_1, S_2, \ldots, S_N, S_1, \ldots\}$, т.е. повторяются через каждые N тактов. Следовательно, со второго такта импульсная характеристика рекурсивного фильтра определяется последовательностью максимальной длины, сгенерированной РСЛОС из некоторого состояния S_1. ▲

Суть предлагаемого подхода к минимальной реализации фильтра изложена в следующей теореме.

Теорема 6. *Рациональную передаточную функцию вида*

$$P_{(0\ 1)}(D) = \begin{pmatrix} f(D)/q(D) = \dfrac{f_0 + f_1 D + \ldots + f_m D^m}{1 + q_1 D + \ldots + q_m D^m} \\ \\ g(D)/q(D) = \dfrac{g_0 + g_1 D + \ldots + g_m D^m}{1 + q_1 D + \ldots + q_m D^m} \end{pmatrix},$$

где $q(D)$ – примитивный полином степени m, можно реализовать на основе только схемы фильтра $f(D)/q(D)$ или фильтра $g(D)/q(D)$ с использованием дополнительных сумматоров.

Доказательство. Возьмем фильтр $f(D)/q(D)$ в канонической форме с вынесенными сумматорами (см. рис. 2). Изначально все разряды данного фильтра заполнены нулями и находятся в состоянии S_0. При импульсном воздействии последующие состояния и соответствующие им биты импульсной характеристики фильтра $f(D)/q(D)$ имеют вид

$$\begin{array}{cccccccc} S_0 & S_1 & S_2 & \dots & S_N & S_1 & S_2 & \dots \\ p_0 = f_0 & p_1 & p_2 & \dots & p_N & p_1 & p_2 & \dots \end{array}$$

Теперь возьмем фильтр $g(D)/q(D)$ в канонической форме с вынесенными сумматорами. Применяя лемму 1, импульсную характеристику фильтра $g(D)/q(D)$ выразим через биты $(p_1, p_2, \dots, p_N, \dots)$ импульсной характеристики фильтра $f(D)/q(D)$ как

$$g_0 \quad p_{N-i+1} \quad p_{N-i+2} \quad \dots \quad p_N \quad p_1 \quad p_2 \quad \dots \quad p_{N-i} \quad p_{N-i+1} \quad p_{N-i+2} \quad \dots$$

Тогда соответствие между состояниями и импульсной характеристикой фильтра $g(D)/q(D)$ в терминах фильтра $f(D)/q(D)$ имеет вид

$$\begin{array}{cccccccccccc} S_0 & S^* = S_{N-i+1} & S_{N-i+2} & \dots & S_N & S_1 & S_2 & \dots & S_{N-i} & S_{N-i+1} & S_{N-i+2} & \dots \\ g_0 & p_{N-i+1} & p_{N-i+2} & \dots & p_N & p_1 & p_2 & \dots & p_{N-i} & p_{N-i+1} & p_{N-i+2} & \dots \end{array}$$

Из этого соответствия следует, что фильтр $g(D)/q(D)$ можно реализовать на основе фильтра $f(D)/q(D)$ в канонической форме с вынесенными сумматорами (см. рис. 2), если на первом такте работы (отклика на единичное воздействие) фильтра на рис. 2:

– записать в ячейки памяти фильтра $d_1\ d_2\ \dots\ d_m$ состояние $S^* = S_{N-i+1}$;

– обеспечить начальный бит импульсной характеристики фильтра g_0.

Указанные требования можно выполнить, подав входную последовательность на встроенные в соответствующих местах схемы на рис. 2 сумматоры.

Таким образом, возможный вариант реализации функции $P_{(0\ 1)}(D)$ – это схема фильтра $f(D)/q(D)$ на рис. 2, в которую добавлен второй вход через встроенные в соответствующих местах дополнительные сумматоры.

Реализация функции $P_{(0\ 1)}(D)$ на основе фильтра $g(D)/q(D)$ доказывается аналогично. ▲

С учетом вышеизложенного представим алгоритм минимальной реализации рекурсивного фильтра $f(D)/q(D)$ с перфорацией каждого второго бита как двойного рекурсивного фильтра, где $q(D)$ – примитивный полином.

Шаг 1: Для фильтра $f(D)/q(D) = \dfrac{f_0 + f_1 D + \ldots + f_m D^m}{1 + q_1 D + \ldots + q_m D^m}$ получить перфорированную рациональную передаточную функцию

$$P_{(0\ 1)}(D) = \begin{pmatrix} y_1(D)/q(D) = \dfrac{y_1 + y_3 D + y_5 D^2 + \ldots + y_{2m-1} D^{m-1}}{1 + q_1 D + \ldots + q_m D^m} \\ \\ y_0(D)/q(D) = \dfrac{y_0 + y_2 D + y_4 D^2 + \ldots + y_{2m} D^m}{1 + q_1 D + \ldots + q_m D^m} \end{pmatrix},$$

где

$$y_i = \sum_{j=0}^{m} q_j f_{i-j}, \quad i = 0, 1, \ldots, 2m,$$

$q_0 = 1$, $f_{i-j} \stackrel{\text{def}}{=} 0$ для всех $i - j > m$.

Шаг 2: Взять фильтр $y_1(D)/q(D)$ в канонической форме с вынесенными сумматорами и записать его $N + 1 = 2^m$ состояний при импульсном воздействии, начиная с начального нулевого состояния S_0:

$$S_0, S_1, S_2, \ldots, S_N. \tag{7}$$

Шаг 3: Первые 2^m битов импульсной характеристики фильтра $y_1(D)/q(D)$

$$\{y_1, p_1, p_2, \ldots, p_N\}$$

сравнить с первыми 2^m битами импульсной характеристики фильтра $y_0(D)/q(D)$

$$\{y_0, p_{N-i+1}, p_{N-i+2}, \ldots, p_{N-i}\}.$$

Найти сдвиг i.

Определить состояние $S^* = S_{N-i+1}$ из (7).

Шаг 4: На схеме фильтра $y_1(D)/q(D)$ в канонической форме с вынесенными сумматорами организовать второй вход через встроенные в схему дополнительные сумматоры. Данный вход организовать таким образом, чтобы при поданном на него импульсном воздействии на первом такте работы фильтра выполнялись условия:

– запись в ячейки памяти фильтра $d_1\ d_2\ \ldots\ d_m$ состояния S^*;
– обеспечение начального бита импульсной характеристики фильтра $p_0 = y_0$.

Заметим, что возможна альтернативная реализация на основе схемы фильтра $y_0(D)/q(D)$. Лучше выбрать вариант, требующий меньшего количества сумматоров.

Рассмотрим применение алгоритма на примерах для кодеров турбокодов с перфорацией.

Пример 3. В составе кодера турбокода системы спутниковой связи Inmarsat нашел применение RSC-кодер

$$G(D) = \left(1 \quad (1 + D + D^2 + D^4)/(1 + D^3 + D^4)\right)$$

с перфорацией каждого второго проверочного бита [18], т.е. на выходе первого компонентного RSC-кодера удаляется каждый четный проверочный бит, на выходе второго компонентного RSC-кодера удаляется каждый нечетный проверочный бит (см. рис. 5, где π – перемежитель).

Отметим, что полином обратной связи $q(D) = 1 + D^3 + D^4$ является примитивным.

Возможная реализация показана на рис. 6 и не является ни одной из канонических форм представления (со встроенными сумматорами, с вынесенными сумматорами).

Для рекурсивного фильтра $(1 + D + D^2 + D^4)/(1 + D^3 + D^4)$ вычислим перфорированные рациональные передаточные функции

$$P_{(0\ 1)}(D) = \begin{pmatrix} p_1(D) \\ p_0(D) \end{pmatrix} = \begin{pmatrix} \dfrac{1 + D + D^3}{1 + D^3 + D^4} \\ \dfrac{1 + D + D^2 + D^3 + D^4}{1 + D^3 + D^4} \end{pmatrix},$$

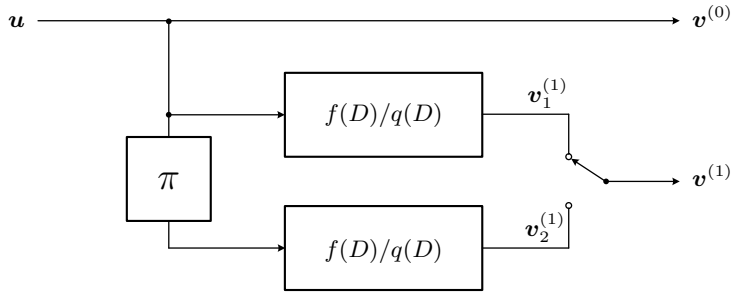

Рис. 5. Кодер систематического турбокода скорости $1/2$

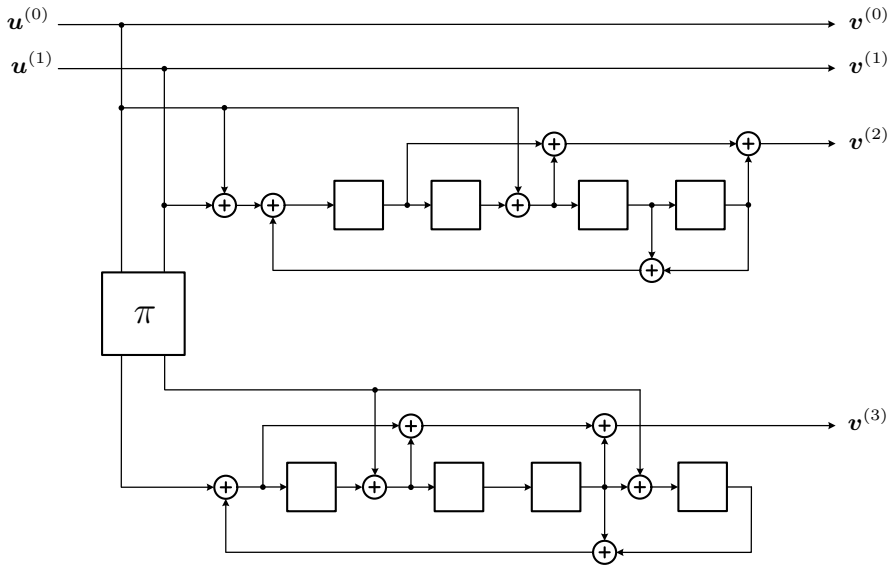

Рис. 6. Реализация кодера на рис. 5 при $\dfrac{f(D)}{q(D)} = \dfrac{1+D+D^2+D^4}{1+D^3+D^4}$ как кодера двойного турбокода

$$P_{(1\ 0)}(D) = \begin{pmatrix} p_0(D) \\ Dp_1(D) \end{pmatrix} = \begin{pmatrix} \dfrac{1+D+D^2+D^3+D^4}{1+D^3+D^4} \\ \dfrac{D+D^2+D^4}{1+D^3+D^4} \end{pmatrix}.$$

Рассмотрим минимизацию схемной реализации передаточной функции

$$P_{(1\ 0)}(D) = \begin{pmatrix} \dfrac{1+D+D^2+D^3+D^4}{1+D^3+D^4} \\ \dfrac{D+D^2+D^4}{1+D^3+D^4} \end{pmatrix}.$$

За основу такой схемы можно взять фильтр $\dfrac{1+D+D^2+D^3+D^4}{1+D^3+D^4}$ или же фильтр $\dfrac{D+D^2+D^4}{1+D^3+D^4}$ в канонической форме с вынесенными сумматорами. Возьмем фильтр

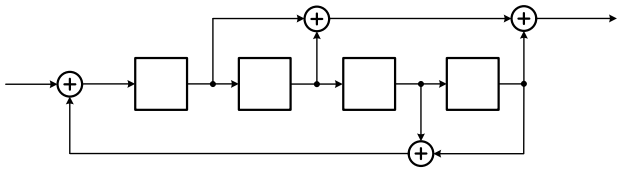

Рис. 7. Фильтр $\dfrac{D+D^2+D^4}{1+D^3+D^4}$ в канонической форме с вынесенными сумматорами

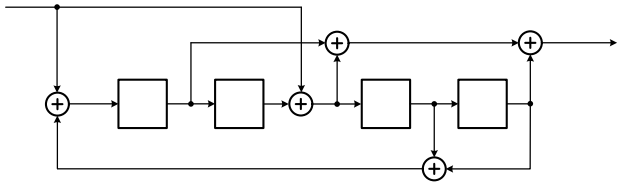

Рис. 8. Реализация фильтра $\dfrac{1+D+D^2+D^3+D^4}{1+D^3+D^4}$ на основе схемы на рис. 7

$\dfrac{D+D^2+D^4}{1+D^3+D^4}$, изображенный на рис. 7, так как для его реализации необходимо меньшее количество сумматоров (логики "исключающее ИЛИ").

Изначально все разряды данного фильтра находятся в состоянии $S_0 = 0000$. Тогда при импульсном воздействии последующие состояния имеют вид

$$\begin{array}{cccccc} S_0=0000 & S_1=1000 & S_2=0100 & S_3=0010 & S_4=1001 & S_5=1100 \\ S_6=0110 & S_7=1011 & S_8=0101 & S_9=1010 & S_{10}=1101 & S_{11}=1110 \\ S_{12}=1111 & S_{13}=0111 & S_{14}=0011 & S_{15}=0001 & S_1=1000 & S_2=0100. \end{array}$$

Сравнив первые 16 битов импульсной характеристики фильтра $\dfrac{D+D^2+D^4}{1+D^3+D^4}$

$$\{y_1, p_1, p_2, \ldots, p_N\} = 0,1,1,0,0,0,1,0,0,1,1,0,1,0,1,1$$

с первыми 16 битами импульсной характеристики фильтра $\dfrac{1+D+D^2+D^3+D^4}{1+D^3+D^4}$

$$\{y_0, p_{N-i+1}, p_{N-i+2}, \ldots, p_{N-i}\} = 1,1,1,0,1,0,1,1,1,1,0,0,0,1,0,0,$$

найдем $i = 7$, тогда $S^* = S_9 = 1010$.

Теперь на основе схемы фильтра $\dfrac{D+D^2+D^4}{1+D^3+D^4}$, представленного на рис. 7, реализуем фильтр $\dfrac{1+D+D^2+D^3+D^4}{1+D^3+D^4}$. В схеме на рис. 7 организуем вход таким образом, чтобы на первом такте работы (реакции на импульсное воздействие) фильтра на рис. 7:

– записать в ячейки памяти фильтра состояние $S^* = 1010$;

– обеспечить первый бит импульсной характеристики фильтра $y_0 = 1$.

Указанные условия можно выполнить, подав входную последовательность на встроенные в соответствующих местах схемы на рис. 7 сумматоры, как показано на рис. 8.

Таким образом, возможный вариант минимальной реализации $P_{(1\ 0)}(D)$ – это вычислитель проверочных битов $v^{(2)}$ на рис. 6.

Аналогично рассмотрим основные этапы минимизации схемной реализации для функции

$$P_{(0\ 1)}(D) = \begin{pmatrix} \dfrac{1+D+D^3}{1+D^3+D^4} \\ \dfrac{1+D+D^2+D^3+D^4}{1+D^3+D^4} \end{pmatrix}.$$

За основу схемы возьмем фильтр $\dfrac{1+D+D^3}{1+D^3+D^4}$ в форме с вынесенными сумматорами. Сравнив первые 16 битов импульсной характеристики данного фильтра

$$\{y_1, p_1, p_2, \ldots, p_N\} = 1,1,0,0,0,1,0,0,1,1,0,1,0,1,1,1$$

с первыми 16 битами импульсной характеристикой фильтра $\dfrac{1+D+D^2+D^3+D^4}{1+D^3+D^4}$

$$\{y_0, p_{N-i+1}, p_{N-i+2}, \ldots, p_{N-i}\} = 1,1,1,0,1,0,1,1,1,1,0,0,0,1,0,0,$$

найдем $i = 8$, тогда $S^* = S_8 = 0101$.

Тогда фильтр $\dfrac{1+D+D^2+D^3+D^4}{1+D^3+D^4}$ может быть реализован на основе фильтра $\dfrac{1+D+D^3}{1+D^3+D^4}$, если на первом такте работы (реакции на импульсное воздействие) данного фильтра:

– записать в ячейки памяти фильтра состояние $S^* = 0101$;
– обеспечить начальный бит импульсной характеристики фильтра $y_0 = 1$.

Таким образом, схемная реализация $P_{(0\ 1)}(D)$ – это вычислитель проверочных битов $v^{(3)}$ на рис. 6.

Пример 4. В системах спутниковой телеметрии CCSDS рекомендует кодер турбокода на рис. 5 при $f(D)/q(D) = (1+D+D^3+D^4)/(1+D^3+D^4)$ [9]. Применив предложенный алгоритм, получим возможную реализацию на рис. 9.

Отметим, что реализация фильтров с перфорацией в представленном виде может иметь преимущества. Например, использование в турбокодах двойных RSC-кодеров в сравнении с традиционными RSC-кодерами показывает меньшую задержку.

§ 5. Заключение

В статье получены следующие результаты.

Исследовано приведение рекурсивных фильтров (с перфорацией) к представлению разреженными матрицами, обладающими структурой. Найдены явные формулы расчета элементов приведенных разреженных матриц для рекурсивных фильтров с перфорацией каждого второго бита на выходе.

Рассмотрено приложение полученных разреженных матриц к нахождению перфорированных передаточных функций для рекурсивных фильтров с перфорацией каждого второго бита. Предложен подход к минимальной схемной реализации данных функций. Представлены возможные варианты схемной реализации некоторых турбокодов с перфорацией.

Приложение приведенных в статье разреженных матриц к задаче идентификации турбоподобных кодов в условиях априорной неопределенности при наличии помех предложено в [11], обсуждается в работах [19,20] и является направлением дальнейших исследований.

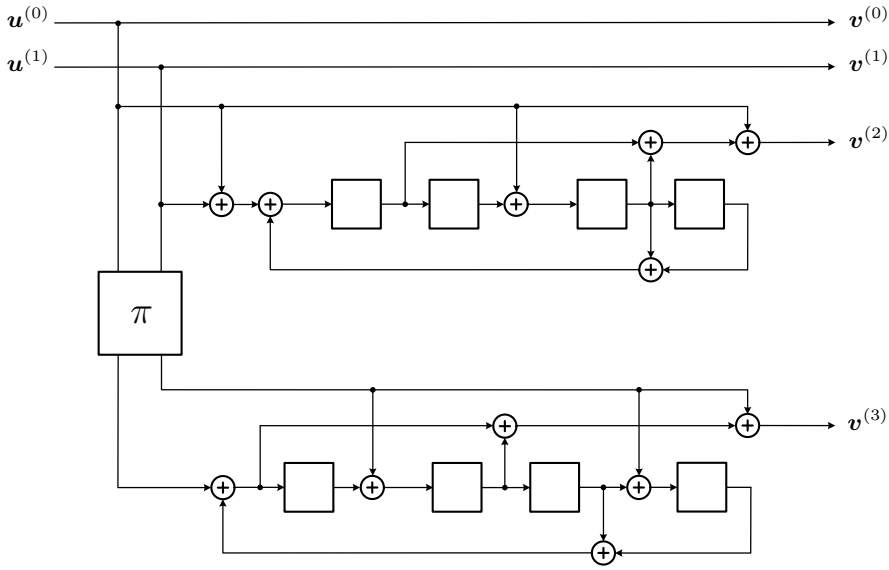

Рис. 9. Реализация кодера на рис. 5 при $\dfrac{f(D)}{q(D)} = \dfrac{1 + D + D^3 + D^4}{1 + D^3 + D^4}$ как кодера двойного турбокода

Автор благодарит рецензента за полезные замечания и предложения, позволившие значительно улучшить первоначальный вариант статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Berrou C., Glavieux A., Thitimajshima P.* Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes. 1 // Proc. IEEE Int. Conf. on Communications (ICC'93). Geneva, Switzerland. May 23–26, 1993. V. 2. P. 1064–1070. https://doi.org/10.1109/ICC.1993.397441
2. *Berrou C., Glavieux A.* Near Optimum Error Correcting Coding and Decoding // IEEE Trans. Commun. 1996. V. 44. № 10. P. 1261–1271. https://doi.org/10.1109/26.539767
3. *Douillard C., Berrou C.* Turbo Codes with Rate-$m/(m + 1)$ Constituent Convolutional Codes // IEEE Trans. Commun. 2005. V. 53. № 10. P. 1630–1638. https://doi.org/10.1109/TCOMM.2005.857165
4. Channel Coding in Communication Networks: From Theory to Turbocodes. London; Newport Beach, CA: ISTE, 2007.
5. *Jin H., Khandecar A., McEliece R.* Irregular Repeat-Accumulate Codes // Proc. 2nd Int. Symp. on Turbo Codes and Related Topics. Brest, France. Sept. 4–7, 2000. P. 1–8.
6. *Johnson S.J.* Iterative Error Correction: Turbo, Low-Density Parity-Check and Repeat-Accumulate Codes. Cambridge, UK; New York: Cambridge Univ. Press, 2010.
7. *Abbasfar A.* Turbo-like Codes: Design for High Speed Decoding. Dordrecht: Springer, 2007.
8. *Deshmukh R.M., Ladhake S.A.* Analysis of Various Puncturing Patterns and Code Rates: Turbo Code // Int. J. Electron. Eng. Res. 2009. V. 1. № 2. P. 79–88.
9. TM Synchronization and Channel Coding: Recommended Standard, Issue 3. CCSDS 131.0-B-3 (Blue Book, September 2017). Washington, DC: CCSDS, 2017.
10. *Johannesson R., Zigangirov K.Sh.* Fundamentals of Convolutional Coding. Pisacataway, NJ: IEEE Press; Hoboken, NJ: Wiley, 2015.
11. *Баринов А.Ю.* Методы анализа турбоподобных кодов с учетом идентификации их компонентных перемежителей // Наукоемкие технологии. 2016. Т. 17. № 12. С. 4–11.
12. *Clark G., Cain J.* Error-Correction Coding for Digital Communications. New York: Plenum, 1981.

13. *Morelos-Zaragoza R.H.* The Art of Error Correcting Coding. Chichester, UK: Wiley, 2002.
14. *Бочарова И.Е., Хуг Ф., Йоханнессон Р., Кудряшов Б.Д.* Дуальные сверточные коды и тождества Мак-Вильямс // Пробл. передачи информ. 2012. Т. 48. № 1. С. 26–36. http://mi.mathnet.ru/ppi2066
15. *Richardson T., Urbanke R.* Modern Coding Theory. Cambridge, UK: Cambridge Univ. Press, 2008.
16. *Gill A.* Linear Sequential Circuits; Analysis, Synthesis and Applications. New York: McGraw-Hill, 1966.
17. *Lee S.C.* Modern Switching Theory and Digital Design. Englewood Cliffs, NJ: Prentice-Hall, 1978.
18. *Costello D.J., Forney G.D.* Channel Coding: The Road to Channel Capacity // Proc. IEEE. 2007. V. 95. № 6. P. 1150–1177. https://doi.org/10.1109/JPROC.2007.895188
19. *Баринов А.Ю., Асеев А.Ю.* Модифицированная математическая модель системы генерирования перемеженной дискретной последовательности турбоподобного кода // Вестн. ЧерГУ. 2017. № 6 (81). С. 9–18. https://doi.org/10.23859/1994-0637-2017-6-81-1
20. *Баринов А.Ю.* Идентификация перемежителей турбокодов на основе их полиномиального и матричного представления // Информация и космос. 2018. № 2. С. 61–66.

Баринов Антон Юрьевич
Военный университет радиоэлектроники, Череповец
aybarinov@mail.ru

Поступила в редакцию
12.05.2021
После доработки
15.12.2021
Принята к публикации
03.02.2022

EDN: DTCBVT
ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 1**

УДК 621.391.1 : 519.725 : 512.647.2

© 2022 г. **С. Шарма**[1], **А. Шарма**[2]

МУЛЬТИСКРУЧЕННЫЕ АДДИТИВНЫЕ КОДЫ С ДОПОЛНИТЕЛЬНЫМИ ДВОЙСТВЕННЫМИ НАД КОНЕЧНЫМИ ПОЛЯМИ

Мультискрученные (МС) аддитивные коды над конечными полями образуют важный класс аддитивных кодов, обобщающий констациклические аддитивные коды. Изучается специальный класс аддитивных МС-кодов над конечными полями, а именно аддитивные МС-коды с дополнительными двойственными кодами относительно обычной билинейной, эрмитовой и $*$-формы следа. Также выводится необходимое и достаточное условие, при котором аддитивный МС-код над конечным полем имеет дополнительный двойственный. Затем приводятся явные формулы для числа всех аддитивных МС-кодов с дополнительными двойственными над конечными полями относительно вышеупомянутых билинейных форм следа. Результаты проиллюстрированы несколькими примерами.

Ключевые слова: констациклические аддитивные коды, разложение Витта, индекс Витта.

DOI: 10.31857/S055529232201003X

§ 1. Введение

Линейные коды над конечными полями – наиболее хорошо изученный класс кодов, исправляющих ошибки. Линейный код, имеющий тривиальное пересечение со своим двойственным кодом, называется линейным кодом с дополнительным двойственным (или LCD-кодом – linear complementary-dual code). LCD-коды над конечными полями были введены в [1], где была дана алгебраическая характеризация LCD-кодов над конечными полями и показано, что существуют асимптотически хорошие LCD-коды. Там же было показано, что LCD-коды дают оптимальное решение задачи линейного кодирования для двоичного суммирующего канала с двумя пользователями. Позже в [2] было получено необходимое и достаточное условие, при котором циклический код над конечным полем является LCD-кодом. В [3], используя спектры размерностей остовов (hulls) линейных кодов, было показано, что LCD-коды над конечными полями лежат на асимптотической границе Варшамова–Гилберта. В [4] были построены LCD-коды с помощью ортогональных матриц, комбинаторных дизайнов, самодвойственных кодов и отображений Грея из кодов над семейством колец $\mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2, u_iu_j - u_ju_i\rangle$. Там же была получена граница линейного программирования на наибольший размер LCD-кода заданной длины с заданным минимальным расстоянием и представлена таблица нижних границ для этой комбинаторной функции для умеренных значений параметров. Помимо применения LCD-кодов в системах связи и хранения данных, LCD-коды недавно нашли

[1] Работа выполнена при финансовой поддержке Комиссии по университетским грантам (UGC) Индии.

[2] Работа выполнена при финансовой поддержке фонда iHub-Anubhuti-IIITD в рамках программы NM-ICPS Министерства науки и технологии Индии (номер гранта IHUB Anubhuti/Project Grant/12).

применение в криптографии. В [5] было показано, что LCD-коды могут быть полезны для защиты конфиденциальной информации от атак по сторонним каналам (SCA) и по привнесенным помехам (FIA). Также там было представлено несколько конструкций LCD-кодов над конечными полями, основанных на расширении кодов Рида–Соломона.

Как естественное обобщение линейных кодов в другом направлении в [6] были введены и изучены аддитивные коды над конечным полем $\mathbb{F}_4$. Там же были рассмотрены их двойственные коды относительно скалярного произведения, заданного функцией следа, и предложен метод построения квантовых кодов, исправляющих ошибки, из самоортогональных аддитивных кодов над $\mathbb{F}_4$. Затем в [7, 8] изучались аддитивные коды над произвольными конечными полями. Позднее в [9, 10] были исследованы циклические аддитивные коды длины n над $\mathbb{F}_4$ и найдено каноническое разложение для таких кодов. Также в [9, 10] изучались их двойственные коды относительно скалярного произведения с функцией следа на $\mathbb{F}_4^n$ и было найдено число всех самоортогональных и самодвойственных циклических аддитивных кодов над $\mathbb{F}_4$. Обобщением этой работы явилась работа [11], в которой изучались циклические аддитивные коды длины n над $\mathbb{F}_{q^t}$, где $t \geqslant 2$ – целое число, q – степень простого, $\mathbb{F}_{q^t}$ – конечное поле порядка q^t, а n – положительное целое число, такое что НОД$(n, q) = 1$. Число всех таких кодов было найдено с помощью полученного канонического разложения для этих кодов. Там же были изучены их двойственные коды и найдено число всех самоортогональных и самодвойственных циклических аддитивных кодов над $\mathbb{F}_{q^t}$ относительно обыкновенной и эрмитовой билинейных форм следа на $\mathbb{F}_{q^t}^n$. Позже в [12] была введена и изучена новая билинейная форма следа на $\mathbb{F}_{q^t}^n$, названная $*$-формой следа, а также исследованы двойственные коды циклических аддитивных кодов и найдено число всех самоортогональных и самодвойственных циклических аддитивных кодов над $\mathbb{F}_{q^t}$ относительно билинейной $*$-формы следа. В другой работе тех же авторов [13] были изучены циклические аддитивные коды длины n с дополнительными двойственными над $\mathbb{F}_{q^t}$ относительно обычной билинейной, эрмитовой и $*$-формы следа и приведены явные формулы для числа кодов этих трех классов. В последующей работе [14] циклические аддитивные коды над $\mathbb{F}_{q^t}$ были обобщены далее – изучались констациклические аддитивные коды длины n над $\mathbb{F}_{q^t}$, где t – простое число и НОД$(n, q) = 1$. Были также изучены их двойственные коды относительно обычной билинейной формы следа на $\mathbb{F}_{q^t}^n$. В той же работе были получены необходимые и достаточные условия для того, чтобы негациклический аддитивный код длины n над $\mathbb{F}_{q^2}$ был самодвойственным или самоортогональным. Далее, для любого целого числа $t \geqslant 2$ (не обязательно степени простого) в [15] была тщательно исследована алгебраическая структура констациклических аддитивных кодов длины n над $\mathbb{F}_{q^t}$, и число всех таких кодов было найдено с помощью полученного там канонического разложения. Кроме того, были изучены их двойственные коды и даны явные формулы для числа всех констациклических аддитивных самоортогональных, самодвойственных кодов и кодов с дополнительными двойственными длины n над $\mathbb{F}_{q^t}$ относительно обычной билинейной, эрмитовой и $*$-формы следа на $\mathbb{F}_{q^t}^n$. Как обобщение констациклических аддитивных кодов в недавней работе [16] были введены и исследованы аддитивные мультискрученные (multi-twisted) коды (MC-коды) над конечными полями. Были также изучены их двойственные коды и получены явные выражения для числа всех самоортогональных и самодвойственных аддитивных MC-кодов длины n над $\mathbb{F}_{q^t}$ относительно обычной билинейной, эрмитовой и $*$-формы следа на $\mathbb{F}_{q^t}^n$.

Основной целью настоящей статьи является изучение аддитивных MC-кодов с дополнительными двойственными над конечными полями относительно следующих билинейных форм следа: обычной, эрмитовой и $*$-формы. Более точно, будет выведено необходимое и достаточное условие, при котором аддитивный MC-код над конечным полем имеет дополнительный двойственный. Будут также получены яв-

ные формулы для числа всех аддитивных МС-кодов над конечными полями с дополнительными двойственными относительно вышеуказанных билинейных форм следа.

Статья имеет следующую структуру. В § 2 приведены некоторые предварительные сведения, необходимые для вывода основных результатов. В § 3 выведено необходимое и достаточное условие, при котором аддитивный МС-код над конечным полем имеет дополнительный двойственный (теорема 3). В § 4 получены явные формулы для числа всех аддитивных МС-кодов над конечными полями относительно обычной билинейной, эрмитовой и $*$-формы следа (теорема 4), а также приведены примеры, иллюстрирующие эти результаты. В § 5 вкратце подведены итоги и сформулирован интересный открытый вопрос в данном направлении.

§ 2. Предварительные сведения

В этом параграфе вводятся обозначения и приводятся некоторые базовые определения и факты, необходимые для вывода основных результатов. Всюду далее $t \geqslant 2$ – целое число, q – степень простого числа p, а через $\mathbb{F}_q$ и $\mathbb{F}_{q^t}$ обозначаются конечные поля порядков q и q^t соответственно. Пусть $m_1, m_2, \ldots, m_\ell$ – натуральные числа, взаимно простые с q, и пусть $n = m_1 + m_2 + \ldots + m_\ell$. Зафиксируем множество $\Omega = (\omega_1, \omega_2, \ldots, \omega_\ell)$, где $\omega_1, \omega_2, \ldots, \omega_\ell$ – ненулевые элементы поля $\mathbb{F}_q$. Для каждого $1 \leqslant i \leqslant \ell$ определим факторкольцо $\mathcal{V}_i = \mathbb{F}_{q^t}[x]/\langle x^{m_i} - \omega_i \rangle$. Тогда множество $\mathcal{V} = \prod_{i=1}^{\ell} \mathcal{V}_i$ можно рассматривать как $\mathbb{F}_q[x]$-модуль относительно операций покомпонентного сложения и покомпонентного умножения на скаляры, который будем называть Ω-мультискрученным модулем (Ω-МС-модулем). Тогда Ω-мультискрученный аддитивный код (аддитивный Ω-МС-код) $\mathcal{C}$ длины n с длинами блоков $(m_1, m_2, \ldots, m_\ell)$ над $\mathbb{F}_{q^t}$ определяется [16] как $\mathbb{F}_q[x]$-подмодуль модуля $\mathcal{V}$.

Всюду далее в качестве элементов факторкольца $\mathbb{F}_{\mathfrak{Q}}[x]/\langle F(x) \rangle$ будут рассматриваться их представители в $\mathbb{F}_{\mathfrak{Q}}[x]$ степени строго меньшей, чем степень $F(x)$, и их сложение и умножение будет выполняться по модулю $F(x)$, где $\mathbb{F}_{\mathfrak{Q}}$ – конечное поле порядка $\mathfrak{Q}$, а $F(x)$ – непостоянный многочлен из $\mathbb{F}_{\mathfrak{Q}}[x]$. При этом вектор $\alpha \in \mathbb{F}_{q^t}^n$ будем записывать в виде $(\alpha_{1,0}, \alpha_{1,1}, \ldots, \alpha_{1,m_1-1}; \ldots; \alpha_{\ell,0}, \alpha_{\ell,1}, \ldots, \alpha_{\ell,m_\ell-1})$ и будем отождествлять его с элементом $\alpha(x) = (\alpha_1(x), \alpha_2(x), \ldots, \alpha_\ell(x)) \in \mathcal{V}$, где $\alpha_i(x) = \alpha_{i,0} + \alpha_{i,1}x + \ldots + \alpha_{i,m_i-1}x^{m_i-1} \in \mathcal{V}_i$ для $1 \leqslant i \leqslant \ell$. Это отображение из $\mathbb{F}_{q^t}^n$ в $\mathcal{V}$ является изоморфизмом векторных пространств. При таком отождествлении Ω-аддитивный МС-код $\mathcal{C}$ можно рассматривать как $\mathbb{F}_q$-линейное подпространство пространства $\mathbb{F}_{q^t}^n$ (или аддитивный код длины n над $\mathbb{F}_{q^t}$), удовлетворяющее следующему свойству: если $c = (c_{1,0}, c_{1,1}, \ldots, c_{1,m_1-1}; c_{2,0}, c_{2,1}, \ldots, c_{2,m_2-1}; \ldots; c_{\ell,0}, c_{\ell,1}, \ldots, c_{\ell,m_\ell-1})$ – кодовое слово кода $\mathcal{C}$, то его Ω-мультискрученный сдвиг (Ω-МС-сдвиг)

$$T_\Omega(c) = (\omega_1 c_{1,m_1-1}, c_{1,0}, \ldots, c_{1,m_1-2}; \omega_2 c_{2,m_2-1}, c_{2,0}, \ldots, c_{2,m_2-2}; \ldots; \omega_\ell c_{\ell,m_\ell-1}, c_{\ell,0}, \ldots, c_{\ell,m_\ell-2})$$

также является кодовым словом кода $\mathcal{C}$. Следует отметить, что аддитивные Ω-МС-коды над $\mathbb{F}_{q^t}$ совпадают с

- ω_1-констациклическими аддитивными кодами над $\mathbb{F}_{q^t}$ при $\ell = 1$ (см. [14, 15]);
- циклическими аддитивными кодами над $\mathbb{F}_{q^t}$ при $\ell = 1$ и $\omega_1 = 1$ (см. [11–13]);
- негациклическими аддитивными кодами над $\mathbb{F}_{q^t}$ при $\ell = 1$ и $\omega_1 = -1$ (см. [15]).

Для дальнейшего изучения алгебраической структуры аддитивных Ω-МС-кодов длины n над $\mathbb{F}_{q^t}$ обозначим через $g_1(x), g_2(x), \ldots, g_r(x)$ все различные неприводимые множители многочленов $x^{m_1} - \omega_1, x^{m_2} - \omega_2, \ldots, x^{m_\ell} - \omega_\ell$ в кольце $\mathbb{F}_q[x]$. Для $1 \leqslant u \leqslant r$

и $1 \leqslant i \leqslant \ell$ положим

$$\varepsilon_{u,i} = \begin{cases} 1, & \text{если } g_u(x) \text{ делит } x^{m_i} - \omega_i \text{ в } \mathbb{F}_q[x], \\ 0 & \text{в противном случае.} \end{cases}$$

Из китайской теоремы об остатках получаем, что $\mathbb{F}_q[x]/\langle x^{m_i} - \omega_i\rangle \simeq \bigoplus\limits_{u=1}^{r} \varepsilon_{u,i}\mathcal{F}_u$ для $1 \leqslant i \leqslant \ell$, где $\mathcal{F}_u = \mathbb{F}_q[x]/\langle g_u(x)\rangle \simeq \mathbb{F}_{q^{d_u}}$, $d_u = \deg g_u(x)$ для $1 \leqslant u \leqslant r$. Согласно [11, лемма 1] можно далее разложить многочлен $g_u(x)$ на неприводимые многочлены над $\mathbb{F}_{q^t}$ в виде $g_u(x) = g_{u,0}(x)g_{u,1}(x)\dots g_{u,a_u-1}(x)$, где $a_u = \text{НОД}(t, d_u)$, а $g_{u,j}(x)$ – неприводимый многочлен над $\mathbb{F}_{q^t}$ степени $\deg g_{u,j}(x) = d_u/a_u = D_u$ для $0 \leqslant j \leqslant a_u - 1$. Снова применяя китайскую теорему об остатках, получаем, что $\mathcal{V}_i \simeq \bigoplus\limits_{u=1}^{r}\bigoplus\limits_{j=0}^{a_u-1} \varepsilon_{u,i}\mathcal{F}_{u,j}$ для каждого i, где $\mathcal{F}_{u,j} = \mathbb{F}_{q^t}[x]/\langle g_{u,j}(x)\rangle \simeq \mathbb{F}_{q^{tD_u}}$ для $1 \leqslant u \leqslant r$ и $0 \leqslant j \leqslant a_u - 1$. В действительности для $1 \leqslant i \leqslant \ell$ соответствующий изоморфизм колец $\psi_i\colon \mathcal{V}_i \to \bigoplus\limits_{u=1}^{r}\bigoplus\limits_{j=0}^{a_u-1} \varepsilon_{u,i}\mathcal{F}_{u,j}$ задается как

$$\psi_i(\alpha_i(x)) = \big(\varepsilon_{1,i}\alpha_i(x) + \langle g_{1,0}(x)\rangle, \varepsilon_{1,i}\alpha_i(x) + \langle g_{1,1}(x)\rangle, \dots, \varepsilon_{1,i}\alpha_i(x) + \langle g_{1,a_1-1}(x)\rangle,$$
$$\dots, \varepsilon_{r,i}\alpha_i(x) + \langle g_{r,0}(x)\rangle, \varepsilon_{r,i}\alpha_i(x) + \langle g_{r,1}(x)\rangle, \dots, \varepsilon_{r,i}\alpha_i(x) + \langle g_{r,a_r-1}(x)\rangle\big)$$
для любого $\alpha_i(x) \in \mathcal{V}_i$.

Из этого следует, что

$$\mathcal{V} \simeq \bigoplus_{u=1}^{r}\bigoplus_{j=0}^{a_u-1} \underbrace{(\varepsilon_{u,1}\mathcal{F}_{u,j}, \varepsilon_{u,2}\mathcal{F}_{u,j}, \dots, \varepsilon_{u,\ell}\mathcal{F}_{u,j})}_{\mathcal{G}_{u,j}}.$$

Положим $\mathcal{G} = \bigoplus\limits_{u=1}^{r} \mathcal{G}_u$, где $\mathcal{G}_u = \bigoplus\limits_{j=0}^{a_u-1} \mathcal{G}_{u,j}$ для $1 \leqslant u \leqslant r$. Тогда соответствующий изоморфизм колец $\psi\colon \mathcal{V} \to \mathcal{G}$ задается как

$$\psi(\alpha_1(x), \alpha_2(x), \dots, \alpha_\ell(x)) = \mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_r)$$
для любого $(\alpha_1(x), \alpha_2(x), \dots, \alpha_\ell(x)) \in \mathcal{V}$,

где $\mathcal{A}_u = (\mathcal{A}_{u,0}, \mathcal{A}_{u,1}, \dots, \mathcal{A}_{u,a_u-1}) \in \mathcal{G}_u$, а $\mathcal{A}_{u,j} \in \mathcal{G}_{u,j}$ имеет вид $\mathcal{A}_{u,j} = (\mathcal{A}_{u,j}^{(1)}, \mathcal{A}_{u,j}^{(2)}, \dots, \mathcal{A}_{u,j}^{(\ell)})$, где $\mathcal{A}_{u,j}^{(i)} := \varepsilon_{u,i}\alpha_i(x) + \langle g_{u,j}(x)\rangle \in \varepsilon_{u,i}\mathcal{F}_{u,j}$ для любых i, u и j. Далее, для $1 \leqslant u \leqslant r$ положим $\varepsilon_u = \sum\limits_{i=1}^{\ell} \varepsilon_{u,i}$. Заметим, что множество $\mathcal{G}_u$ является $(\varepsilon_u t)$-мерным векторным пространством над $\mathcal{F}_u$ относительно покомпонентного сложения и покомпонентного умножения на скаляры. Теперь приведем теорему 2.2 из работы [16], описывающую каноническое разложение всякого Ω-аддитивного МС-кода длины n над $\mathbb{F}_{q^t}$.

Теорема 1 [16]. *Справедливы следующие утверждения.*

(a) *Пусть $\mathcal{C}$ – Ω-аддитивный МС-код длины n над $\mathbb{F}_{q^t}$. Для $1 \leqslant u \leqslant r$ положим $\mathcal{C}_u = \mathcal{C} \cap \mathcal{G}_u$. Тогда для каждого u множество $\mathcal{C}_u$ является $\mathcal{F}_u$-линейным подпространством пространства $\mathcal{G}_u$, а код $\mathcal{C}$ имеет единственное разложение в прямую сумму $\mathcal{C} = \bigoplus\limits_{u=1}^{r} \mathcal{C}_u$. (Подпространства $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_r$ называются компонентами кода $\mathcal{C}$.)*

(b) *И наоборот, если* $\mathcal{D}_u$ *–* $\mathcal{F}_u$*-линейное подпространство пространства* $\mathcal{G}_u$ *для* $1 \leqslant u \leqslant r$ *и* $\mathcal{D} = \sum_{u=1}^{r} \mathcal{D}_u$*, то* $\mathcal{D} = \bigoplus_{u=1}^{r} \mathcal{D}_u$ *и множество* $\mathcal{D}$ *является* Ω*-аддитивным МС-кодом длины* n *над* $\mathbb{F}_{q^t}$.

В [16, §§ 2, 3] изучались двойственные коды аддитивных Ω-МС-кодов длины n над $\mathbb{F}_{q^t}$ относительно следующих билинейных форм следа: обычной, эрмитовой и $*$-формы следа на $\mathbb{F}_{q^t}^n$, которые определяются следующим образом.

Обычная билинейная форма следа – это отображение $\langle \cdot\,, \cdot \rangle_0 \colon \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \to \mathbb{F}_q$, задаваемое формулой

$$\langle \alpha, \beta \rangle_0 = \sum_{i=1}^{\ell} \sum_{h=0}^{m_i - 1} \mathrm{Tr}_{q^t,q}(\alpha_{i,h} \beta_{i,h})$$

для любых $\alpha, \beta \in \mathbb{F}_{q^t}^n$, где $\mathrm{Tr}_{q^t,q}$ – отображение следа из $\mathbb{F}_{q^t}$ в $\mathbb{F}_q$. Как указано в [11, лемма 5], эта билинейная форма следа $\langle \cdot\,, \cdot \rangle_0$ является невырожденной симметрической билинейной формой на $\mathbb{F}_{q^t}^n$.

Для определения эрмитовой билинейной форм следа пусть $t \geqslant 2$ – четное целое, и пусть $t = 2^a U$, где $a \geqslant 1$, а U – нечетное целое. Нетрудно видеть, что существует ненулевой элемент $\gamma \in \mathbb{F}_{q^{2^a}}$, такой что $\gamma + \gamma^{q^{2^{a-1}}} = 0$. Тогда эрмитова билинейная форма следа – это отображение $\langle \cdot\,, \cdot \rangle_\gamma \colon \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \to \mathbb{F}_q$, задаваемое формулой

$$\langle \alpha, \beta \rangle_\gamma = \sum_{i=1}^{\ell} \sum_{h=0}^{m_i - 1} \mathrm{Tr}_{q^t,q}(\gamma \alpha_{i,h} \beta_{i,h}^{q^{t/2}})$$

для любых $\alpha, \beta \in \mathbb{F}_{q^t}^n$. Как указано в [11, лемма 5], эрмитова билинейная форма следа $\langle \cdot\,, \cdot \rangle_\gamma$ является невырожденной рефлексивной неопределенной билинейной формой на $\mathbb{F}_{q^t}^n$.

Наконец, для определения билинейной $*$-формы следа пусть $t \geqslant 2$ – целое число, такое что $t \not\equiv 1 \pmod p$. Тогда отображение $\varphi \colon \mathbb{F}_{q^t} \to \mathbb{F}_{q^t}$, задаваемое формулой $\varphi(a) = \sum_{\lambda=1}^{t-1} a^{q^\lambda} = \mathrm{Tr}_{q^t,q}(a) - a$ для всех $a \in \mathbb{F}_{q^t}$, является $\mathbb{F}_q$-линейным изоморфизмом векторных пространств. Билинейная $*$-форма следа – это отображение $\langle \cdot\,, \cdot \rangle_* \colon \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \to \mathbb{F}_q$, задаваемое формулой

$$\langle \alpha, \beta \rangle_* = \sum_{i=1}^{\ell} \sum_{h=0}^{m_i - 1} \mathrm{Tr}_{q^t,q}(\alpha_{i,h} \varphi(\beta_{i,h}))$$

для любых $\alpha, \beta \in \mathbb{F}_{q^t}^n$. Согласно [12, лемма 3.2] билинейная $*$-форма следа $\langle \cdot\,, \cdot \rangle_*$ является невырожденной симметрической билинейной формой на $\mathbb{F}_{q^t}^n$, причем неопределенной в случае четного q.

Всюду далее будем использовать обозначение $\delta \in \{0, *, \gamma\}$ и определим $\mathbb{T}_\delta$ как множество (i) всех целых чисел $t \geqslant 2$, если $\delta = 0$, (ii) всех целых $t \geqslant 2$, таких что $t \not\equiv 1 \pmod p$, если $\delta = *$, и (iii) всех четных целых $t \geqslant 2$, если $\delta = \gamma$. Далее, если $\mathcal{C}$ $(\subseteq \mathbb{F}_{q^t}^n)$ – Ω-аддитивный МС-код длины n над $\mathbb{F}_{q^t}$, то его δ-двойственный код $\mathcal{C}^{\perp_\delta}$ определяется как $\mathcal{C}^{\perp_\delta} = \{v \in \mathbb{F}_{q^t}^n : \langle v, c \rangle_\delta = 0 \text{ для всех } c \in \mathcal{C}\}$. Можно показать, что δ-двойственный код $\mathcal{C}^{\perp_\delta}$ является Ω'-аддитивным МС-кодом длины n над $\mathbb{F}_{q^t}$, где $\Omega' = (\omega_1^{-1}, \omega_2^{-1}, \ldots, \omega_\ell^{-1})$. При этом Ω-аддитивный МС-код $\mathcal{C}$ называется кодом, имеющим дополнительный δ-двойственный, где $\delta \in \{0, *, \gamma\}$, если он удовлетворяет соотношению $\mathcal{C} \cap \mathcal{C}^{\perp_\delta} = \{0\}$. Рассуждая как и выше, нетрудно пока-

зать, что δ-двойственный код $\mathcal{C}^{\perp_\delta}$ можно также рассматривать как $\mathbb{F}_q[x]$-подмодуль Ω'-МС-модуля $\mathcal{V}' = \prod_{i=1}^{\ell} \mathcal{V}'_i$, где $\mathcal{V}'_i = \mathbb{F}_{q^t}[x]/\langle x^{m_i} - \omega_i^{-1}\rangle$ для $1 \leqslant i \leqslant \ell$.

Для дальнейшего изучения алгебраической структуры δ-двойственных кодов для аддитивных Ω-МС-кодов над $\mathbb{F}_{q^t}$ заметим, что число $m = \mathrm{НОК}[m_1 O(\omega_1), m_2 O(\omega_2), \ldots, m_\ell O(\omega_\ell)]$ является наименьшим натуральным числом, таким что $\mathrm{НОК}[x^{m_1} - \omega_1, x^{m_2} - \omega_2, \ldots, x^{m_\ell} - \omega_\ell]$ делит $x^m - 1$ в $\mathbb{F}_q[x]$, где через $O(\omega_i)$ обозначается мультипликативный порядок элемента ω_i, $1 \leqslant i \leqslant \ell$. Отметим, что $T_\Omega^m = I$, где I – тождественный оператор на $\mathbb{F}_{q^t}^n$. Теперь пусть $\mathfrak{Q} = q^e$, где $e \geqslant 1$, $\pi \in \{1, -1\}$, и пусть θ – целое число, такое что $0 \leqslant \theta \leqslant e-1$. Далее, пусть $F(x) = \sum_{h=0}^{d-1} a_h x^h + x^d$ – нормированный делитель многочлена $x^m - 1$ в $\mathbb{F}_{\mathfrak{Q}}[x]$. Тогда многочлен, взаимный с $F(x)$, определяется как $F^\dagger(x) = a_0^{-1} \sum_{h=0}^{d-1} a_h x^{d-h} + a_0^{-1}$. Кроме того, определим $\widehat{F}(x) = \sum_{h=0}^{d-1} a_h^{q^\theta} x^h + x^d$, если $\pi = 1$, и $\widehat{F}(x) = a_0^{-q^\theta} \sum_{h=0}^{d-1} a_h^{q^\theta} x^{d-h} + a_0^{-q^\theta}$, если $\pi = -1$. Тогда отображение $\tau_{q^\theta,\pi}\colon \mathbb{F}_{\mathfrak{Q}}[x]/\langle F(x)\rangle \to \mathbb{F}_{\mathfrak{Q}}[x]/\langle \widehat{F}(x)\rangle$, определяемое как

$$\tau_{q^\theta,\pi}\left(\sum_{h=0}^{d-1} f_h x^h\right) = \sum_{h=0}^{d-1} f_h^{q^\theta} x^{\pi h} \quad \text{для любого } \sum_{h=0}^{d-1} f_h x^h \in \mathbb{F}_{\mathfrak{Q}}[x]/\langle F(x)\rangle,$$

является изоморфизмом колец, где $x^{-1} = x^{m-1}$ в $\mathbb{F}_{\mathfrak{Q}}[x]/\langle \widehat{F}(x)\rangle$, если $\pi = -1$. Более того, изоморфизм $\tau_{q^{e-\theta},\pi}$ является обратным к $\tau_{q^\theta,\pi}$. В частности, если $F(x) = x^{m_i} - \omega_i^{-1} \in \mathbb{F}_{q^t}[x]$, то $\widehat{F}(x) = x^{m_i} - \omega_i$, где $1 \leqslant i \leqslant \ell$. Кроме того, для $1 \leqslant i \leqslant \ell$ изоморфизм $\tau_{1,-1}\colon \mathcal{V}'_i \to \mathcal{V}_i$ задается равенством $\tau_{1,-1}(\beta_i(x)) = \beta_i(x^{-1})$ для любого $\beta_i(x) \in \mathcal{V}'_i$, где $x^{-1} = \omega_i^{-1} x^{m_i - 1} \in \mathcal{V}_i$. Отображение $\tau_{1,-1}$ можно далее продолжить до отображения $\tau_{1,-1}\colon \mathcal{V}' \to \mathcal{V}$ как $\tau_{1,-1}(\beta(x)) = \big(\tau_{1,-1}(\beta_1(x)), \tau_{1,-1}(\beta_2(x)), \ldots, \tau_{1,-1}(\beta_\ell(x))\big)$ для любого $\beta(x) = (\beta_1(x), \beta_2(x), \ldots, \beta_\ell(x)) \in \mathcal{V}'$. С другой стороны, если $F(x) = x^m - 1$, то $\widehat{F}(x) = x^m - 1$, и поэтому отображение $\tau_{1,-1}\colon \mathbb{F}_q[x]/\langle x^m - 1\rangle \to \mathbb{F}_q[x]/\langle x^m - 1\rangle$ задается как

$$\tau_{1,-1}\left(\sum_{h=0}^{m-1} a_h x^h\right) = \sum_{h=0}^{m-1} a_h x^{-h} \quad \text{для любого } \sum_{h=0}^{m-1} a_h x^h \in \mathbb{F}_q[x]/\langle x^m - 1\rangle,$$

где $x^{-1} = x^{m-1}$ в $\mathbb{F}_q[x]/\langle x^m - 1\rangle$. Теперь для $\delta \in \{0, *, \gamma\}$ определим отображение $(\cdot\,,\cdot)_\delta\colon \mathcal{V} \times \mathcal{V}' \to \mathbb{F}_q[x]/\langle x^m - 1\rangle$ следующим образом.

Для $\alpha(x) \in \mathcal{V}$ и $\beta(x) \in \mathcal{V}'$ положим

$$(\alpha(x), \beta(x))_\delta = \begin{cases} \sum\limits_{i=1}^{\ell} \sum\limits_{\mu=0}^{t-1} \omega_i \Big(\dfrac{x^m - 1}{x^{m_i} - \omega_i}\Big) \tau_{q^\mu,1}\big(\alpha_i(x) \tau_{1,-1}(\beta_i(x))\big) & \text{для } \delta = 0, \\ \sum\limits_{i=1}^{\ell} \sum\limits_{\mu=0}^{t-1} \omega_i \Big(\dfrac{x^m - 1}{x^{m_i} - \omega_i}\Big) \tau_{q^\mu,1}\Big(\alpha_i(x) \sum\limits_{\lambda=1}^{t-1} \tau_{q^\lambda,-1}(\beta_i(x))\Big) & \text{для } \delta = *, \\ \sum\limits_{i=1}^{\ell} \sum\limits_{\mu=0}^{t-1} \omega_i \Big(\dfrac{x^m - 1}{x^{m_i} - \omega_i}\Big) \tau_{q^\mu,1}\big(\gamma \alpha_i(x) \tau_{q^{t/2},-1}(\beta_i(x))\big) & \text{для } \delta = \gamma. \end{cases}$$

Здесь факторкольцо $\mathbb{F}_q[x]/\langle x^m - 1\rangle$ рассматривается как $\mathbb{F}_q[x]$-модуль. Согласно [16, лемма 2.2] для $\delta \in \{0, *, \gamma\}$ имеем $(\alpha(x), \beta(x))_\delta = \sum_{k=0}^{m-1} \langle \alpha, T_{\Omega'}^k(\beta)\rangle_\delta x^k$ для $\alpha(x) \in \mathcal{V}$ и

$\beta(x) \in \mathcal{V}'$, где через $T^k_{\Omega'}(\beta)$ обозначен k-кратный Ω'-МС-сдвиг вектора $\beta \in \mathbb{F}^n_{q^t}$. При этом отображение $(\cdot\,,\cdot)_\delta$ является рефлексивной невырожденной $\tau_{1,-1}$-полуторалинейной формой на $\mathcal{V} \times \mathcal{V}'$ для $\delta \in \{0, *, \gamma\}$. Отображение $(\cdot\,,\cdot)_\delta$ эрмитово, когда $\delta \in \{0, *\}$, и антиэрмитово, когда $\delta = \gamma$. Кроме того, согласно [16, теорема 2.4], если $\mathcal{C}\ (\subseteq \mathcal{V})$ – Ω-аддитивный МС-код длины n над $\mathbb{F}_{q^t}$, то для $\delta \in \{0, *, \gamma\}$ соответствующий δ-двойственный код $\mathcal{C}^{\perp_\delta}(\subseteq \mathcal{V}')$ кода $\mathcal{C}$ является $\mathbb{F}_q[x]$-подмодулем $\mathcal{V}'$ и имеет вид $\mathcal{C}^{\perp_\delta} = \{\beta(x) \in \mathcal{V}' :\ (\alpha(x), \beta(x))_\delta = 0$ для всех $\alpha(x) \in \mathcal{C}\}$.

Снова применяя китайскую теорему об остатках и рассуждая как выше, получаем, что $\mathcal{V}' \simeq \mathcal{G}' = \bigoplus\limits_{u=1}^{r} \mathcal{G}'_u$, где $\mathcal{G}'_u = \bigoplus\limits_{j=0}^{a_u-1} \mathcal{G}'_{u,j}$, а $\mathcal{G}'_{u,j} = \big(\varepsilon_{u,1}\mathcal{F}^\dagger_{u,j}, \varepsilon_{u,2}\mathcal{F}^\dagger_{u,j}, \ldots, \varepsilon_{u,\ell}\mathcal{F}^\dagger_{u,j}\big)$, где $\mathcal{F}^\dagger_{u,j} = \mathbb{F}_{q^t}[x]/\langle g^\dagger_{u,j}(x)\rangle$ для $1 \leqslant u \leqslant r$ и $0 \leqslant j \leqslant a_u - 1$. Поэтому всякий элемент $(\beta_1(x), \beta_2(x), \ldots, \beta_\ell(x)) \in \mathcal{V}'$ отождествляется с элементом $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_r) \in \mathcal{G}'$, где $\mathcal{B}_u = (\mathcal{B}_{u,0}, \mathcal{B}_{u,1}, \ldots, \mathcal{B}_{u,a_u-1}) \in \mathcal{G}'_u$, а элемент $\mathcal{B}_{u,j} \in \mathcal{G}'_{u,j}$ имеет вид $\mathcal{B}_{u,j} = (\mathcal{B}^{(1)}_{u,j}, \mathcal{B}^{(2)}_{u,j}, \ldots, \mathcal{B}^{(\ell)}_{u,j})$, где $\mathcal{B}^{(i)}_{u,j} := \varepsilon_{u,i}\beta_i(x) + \langle g^\dagger_{u,j}(x)\rangle \in \varepsilon_{u,i}\mathcal{F}^\dagger_{u,j}$ для $1 \leqslant i \leqslant \ell$, $1 \leqslant u \leqslant r$ и $0 \leqslant j \leqslant a_u - 1$. При таких отождествлениях $\mathcal{V}$ с $\mathcal{G}$ и $\mathcal{V}'$ с $\mathcal{G}'$ пусть $[\cdot\,,\cdot]_\delta \colon \mathcal{G} \times \mathcal{G}' \to \to \bigoplus\limits_{u=1}^{r} \mathcal{F}_u$ – отображение, соответствующее $\tau_{1,-1}$-полуторалинейной форме $(\cdot\,,\cdot)_\delta$ для $\delta \in \{0, \gamma, *\}$, имеющее в трех случаях следующий вид соответственно:

$$[\mathcal{A}, \mathcal{B}]_0 = \Bigg(\sum_{i=1}^{\ell} \frac{m}{m_i}\varepsilon_{1,i} \sum_{j=0}^{a_1-1} \sum_{\mu=0}^{(t/a_1)-1} \tau_{q^{\mu a_1+j},1}(\mathcal{A}^{(i)}_{1,a_1-j}\tau_{1,-1}(\mathcal{B}^{(i)}_{1,a_1-j})), \ldots$$
$$\ldots, \sum_{i=1}^{\ell} \frac{m}{m_i}\varepsilon_{r,i} \sum_{j=0}^{a_r-1} \sum_{\mu=0}^{(t/a_r)-1} \tau_{q^{\mu a_r+j},1}(\mathcal{A}^{(i)}_{r,a_r-j}\tau_{1,-1}(\mathcal{B}^{(i)}_{r,a_r-j}))\Bigg),$$
$$[\mathcal{A}, \mathcal{B}]_\gamma = \Bigg(\sum_{i=1}^{\ell} \frac{m}{m_i}\varepsilon_{1,i} \sum_{j=0}^{a_1-1} \sum_{\mu=0}^{(t/a_1)-1} \tau_{q^{\mu a_1+j},1}(\gamma\mathcal{A}^{(i)}_{1,a_1-j}\tau_{q^{\frac{t}{2}},-1}(\mathcal{B}^{(i)}_{1,\frac{t}{2}-j})), \ldots$$
$$\ldots, \sum_{i=1}^{\ell} \frac{m}{m_i}\varepsilon_{r,i} \sum_{j=0}^{a_r-1} \sum_{\mu=0}^{(t/a_r)-1} \tau_{q^{\mu a_r+j},1}(\gamma\mathcal{A}^{(i)}_{r,a_r-j}\tau_{q^{\frac{t}{2}},-1}(\mathcal{B}^{(i)}_{r,\frac{t}{2}-j}))\Bigg)$$

и

$$[\mathcal{A}, \mathcal{B}]_* = -[\mathcal{A}, \mathcal{B}]_0 + \Bigg(\sum_{i=1}^{\ell} \frac{m}{m_i}\varepsilon_{1,i}\Bigg(\Bigg(\sum_{j=0}^{a_1-1} \sum_{\mu=0}^{(t/a_1)-1} \tau_{q^{\mu a_1+j},1}(\mathcal{A}^{(i)}_{1,a_1-j})\Bigg) \times$$
$$\times \Bigg(\sum_{j=0}^{a_1-1} \sum_{\sigma=0}^{(t/a_1)-1} \tau_{q^{\sigma a_1+j},1}(\tau_{1,-1}(\mathcal{B}^{(i)}_{1,a_1-j}))\Bigg)\Bigg), \ldots$$
$$\ldots, \sum_{i=1}^{\ell} \frac{m}{m_i}\varepsilon_{r,i}\Bigg(\Bigg(\sum_{j=0}^{a_r-1} \sum_{\mu=0}^{(t/a_r)-1} \tau_{q^{\mu a_r+j},1}(\mathcal{A}^{(i)}_{r,a_r-j})\Bigg) \times$$
$$\times \Bigg(\sum_{j=0}^{a_r-1} \sum_{\sigma=0}^{(t/a_r)-1} \tau_{q^{\sigma a_r+j},1}(\tau_{1,-1}(\mathcal{B}^{(i)}_{r,a_r-j}))\Bigg)\Bigg)\Bigg)$$

для любых $\mathcal{A} \in \mathcal{G}$ и $\mathcal{B} \in \mathcal{G}'$. Согласно [16, леммы 2.3, 2.4] отображение $[\cdot\,,\cdot]_\delta$ является рефлексивной невырожденной эрмитовой $\tau_{1,-1}$-полуторалинейной формой на $\mathcal{G} \times \mathcal{G}'$ при $\delta \in \{0, *\}$, а отображение $[\cdot\,,\cdot]_\gamma$ – рефлексивной невырожденной антиэрмитовой

$\tau_{1,-1}$-полуторалинейной формой на $\mathcal{G}\times\mathcal{G}'$. Ввиду вышесказанного δ-двойственный код $\mathcal{C}^{\perp_\delta}$ для Ω-аддитивного МС-кода $\mathcal{C}(\subseteq\mathcal{G})$ длины n над $\mathbb{F}_{q^t}$ задается как

$$\mathcal{C}^{\perp_\delta}=\{\mathcal{B}\in\mathcal{G}':\ [\mathcal{A},\mathcal{B}]_\delta=0 \text{ для всех } \mathcal{A}\in\mathcal{C}\}.$$

Теперь без ограничения общности пусть $g_{1,0}(x), g_{1,1}(x),\dots,g_{1,a_1-1}(x),\dots,g_{e_1,0}(x)$, $g_{e_1,1}(x),\dots,g_{e_1,a_{e_1}-1}(x)$ – все различные возвратные (взаимные самим себе) неприводимые множители многочленов $x^{m_1}-\omega_1, x^{m_2}-\omega_2,\dots,x^{m_\ell}-\omega_\ell$ в кольце $\mathbb{F}_{q^t}[x]$, $g_{e_1+1,0}(x), g^\dagger_{e_1+1,0}(x),\ g_{e_1+1,1}(x), g^\dagger_{e_1+1,1}(x),\ \dots,\ g_{e_1+1,a_{e_1+1}-1}(x), g^\dagger_{e_1+1,a_{e_1+1}-1}(x),\ \dots,$ $g_{e_2,0}(x), g^\dagger_{e_2,0}(x),\ g_{e_2,1}(x), g^\dagger_{e_2,1}(x),\ \dots,\ g_{e_2,a_{e_2}-1}(x), g^\dagger_{e_2,a_{e_2}-1}(x)$ – неприводимые множители, образующие взаимные пары, а $g_{e_2+1,0}(x), g_{e_2+1,1}(x),\dots,g_{e_2+1,a_{e_2+1}-1}(x),\dots,$ $g_{e_3,0}(x), g_{e_3,1}(x),\dots,g_{e_3,a_{e_3}-1}(x)$ – все остальные неприводимые множители этих многочленов. Заметим, что $r=e_2+e_3-e_1$.

Далее, для $e_1+1\leqslant w\leqslant e_2$ и $1\leqslant i\leqslant\ell$ положим

$$\varepsilon^\dagger_{w,i}=\begin{cases}1, & \text{если } g^\dagger_{w,j}(x)\mid(x^{m_i}-\omega_i) \text{ в } \mathbb{F}_{q^t}[x] \text{ для некоторого } j,\\ 0 & \text{в противном случае.}\end{cases}$$

Пусть $\mathcal{I}_w=\{i:\ 1\leqslant i\leqslant\ell,\ \varepsilon_{w,i}=\varepsilon^\dagger_{w,i}\}$ и $\mathcal{I}'_w=\{i:\ 1\leqslant i\leqslant\ell,\ \varepsilon_{w,i}\neq\varepsilon^\dagger_{w,i}\}$. Заметим, что тогда $\{1,2,\dots,\ell\}=\mathcal{I}_w\cup\mathcal{I}'_w$ (несвязное объединение). Положим $\eta_w=\sum\limits_{i\in\mathcal{I}_w}\varepsilon_{w,i}$, $\varrho_w=\sum\limits_{i\in\mathcal{I}'_w}\varepsilon_{w,i}$ и $\tau_w=\sum\limits_{i\in\mathcal{I}'_w}\varepsilon^\dagger_{w,i}$ для $e_1+1\leqslant w\leqslant e_2$. Тогда

$$\mathcal{G}=\left(\bigoplus_{\nu=1}^{e_1}\mathcal{G}_\nu\right)\oplus\left(\bigoplus_{w=e_1+1}^{e_2}(\mathcal{G}_w\oplus\mathcal{G}^\dagger_w)\right)\oplus\left(\bigoplus_{s=e_2+1}^{e_3}\mathcal{G}_s\right),$$

где $\mathcal{G}_\nu$ (соответственно, $\mathcal{G}_w$, $\mathcal{G}^\dagger_w$ и $\mathcal{G}_s$) – векторное пространство над $\mathcal{F}_\nu$ (соответственно, $\mathcal{F}_w$, $\mathcal{F}^\dagger_w$ и $\mathcal{F}_s$) для каждого ν (соответственно, w и s). Заметим также, что

$$\mathcal{G}'=\left(\bigoplus_{\nu=1}^{e_1}\mathcal{G}_\nu\right)\oplus\left(\bigoplus_{w=e_1+1}^{e_2}(\mathcal{H}_w\oplus\mathcal{H}^\dagger_w)\right)\oplus\left(\bigoplus_{s=e_2+1}^{e_3}\mathcal{G}^\dagger_s\right),$$

где $\mathcal{G}_\nu$ (соответственно, $\mathcal{H}_w$, $\mathcal{H}^\dagger_w$ и $\mathcal{G}^\dagger_s$) – векторное пространство над $\mathcal{F}_\nu$ (соответственно, $\mathcal{F}_w$, $\mathcal{F}^\dagger_w$ и $\mathcal{F}^\dagger_s$) для каждого ν (соответственно, w и s). Таким образом, справедлива следующая

Теорема 2 [16]. *Пусть $\mathcal{C}$ – Ω-аддитивный МС-код длины n над $\mathbb{F}_{q^t}$. Тогда имеют место следующие разложения*:

(a) $\mathcal{C}=\left(\bigoplus\limits_{\nu=1}^{e_1}\mathcal{C}_\nu\right)\oplus\left(\bigoplus\limits_{w=e_1+1}^{e_2}(\mathcal{C}_w\oplus\mathcal{C}^\dagger_w)\right)\oplus\left(\bigoplus\limits_{s=e_2+1}^{e_3}\mathcal{C}_s\right)$, *где $\mathcal{C}_\nu$ (соответственно, $\mathcal{C}_w$, $\mathcal{C}^\dagger_w$ и $\mathcal{C}_s$) – подпространство пространства $\mathcal{G}_\nu$ (соответственно, $\mathcal{G}_w$, $\mathcal{G}^\dagger_w$ и $\mathcal{G}_s$) над $\mathcal{F}_\nu$ (соответственно, $\mathcal{F}_w$, $\mathcal{F}^\dagger_w$ и $\mathcal{F}_s$) для каждого ν (соответственно, w и s)*;

(b) $\mathcal{C}^{\perp_\delta}=\left(\bigoplus\limits_{\nu=1}^{e_1}\mathcal{C}^{\perp_\delta}_\nu\right)\oplus\left(\bigoplus\limits_{w=e_1+1}^{e_2}(\mathcal{C}^{\dagger\perp_\delta}_w\oplus\mathcal{C}^{\perp_\delta}_w)\right)\oplus\left(\bigoplus\limits_{s=e_2+1}^{e_3}\mathcal{C}^{\perp_\delta}_s\right)$, *где $\mathcal{C}^{\perp_\delta}_\nu$ (соответственно, $\mathcal{C}^{\perp_\delta}_w$, $\mathcal{C}^{\dagger\perp_\delta}_w$ и $\mathcal{C}^{\perp_\delta}_s$) – ортогональное дополнение к $\mathcal{C}_\nu$ (соответственно, $\mathcal{C}_w$, $\mathcal{C}^\dagger_w$ и $\mathcal{C}_s$) относительно полуторалинейной формы $[\cdot\,,\cdot]_\delta$, ограниченной на $\mathcal{G}_\nu\times\mathcal{G}_\nu$ (соответственно, $\mathcal{H}^\dagger_w\times\mathcal{G}_w$, $\mathcal{H}_w\times\mathcal{G}^\dagger_w$ и $\mathcal{G}^\dagger_s\times\mathcal{G}_s$) для каждого ν (соответственно, w и s).*

Подробнее об алгебраических структурах аддитивных Ω-МС-кодов над $\mathbb{F}_{q^t}$ и их δ-двойственных кодов см. в [16, §§ 2, 3].

§ 3. Необходимое и достаточное условие, при котором Ω-аддитивный МС-код над $\mathbb{F}_{q^t}$ имеет дополнительный δ-двойственный

В следующей теореме выводится необходимое и достаточное условие, при котором Ω-аддитивный МС-код длины n над $\mathbb{F}_{q^t}$ имеет дополнительный δ-двойственный, где $\delta \in \{0, *, \gamma\}$.

Теорема 3. *Пусть $\Omega = (\omega_1, \omega_2, \ldots, \omega_\ell)$ фиксировано. Рассмотрим Ω-аддитивный МС-код*

$$\mathcal{C} = \left(\bigoplus_{\nu=1}^{e_1} \mathcal{C}_\nu\right) \oplus \left(\bigoplus_{w=e_1+1}^{e_2} (\mathcal{C}_w \oplus \mathcal{C}_w^\dagger)\right) \oplus \left(\bigoplus_{s=e_2+1}^{e_3} \mathcal{C}_s\right)$$

длины n над $\mathbb{F}_{q^t}$. Для $\delta \in \{0, *, \gamma\}$ код $\mathcal{C}$ имеет дополнительный δ-двойственный тогда и только тогда, когда выполнены следующие два условия:

- *Для $1 \leqslant \nu \leqslant e_1$ пространство $\mathcal{C}_\nu$ является $\mathcal{F}_\nu$-подпространством $\mathcal{G}_\nu$, таким что $\mathcal{C}_\nu \cap \mathcal{C}_\nu^{\perp_\delta} = \{0\}$ (т.е. $\mathcal{C}_\nu$ – невырожденное $\mathcal{F}_\nu$-подпространство $\mathcal{G}_\nu$)*;
- *Для $e_1+1 \leqslant w \leqslant e_2$ пространство $\mathcal{C}_w$ является $\mathcal{F}_w$-подпространством $\mathcal{G}_w$, а $\mathcal{C}_w^\dagger$ – $\mathcal{F}_w^\dagger$-подпространством $\mathcal{G}_w^\dagger$, и при этом $\mathcal{C}_w \cap \mathcal{C}_w^{\dagger\perp_\delta} = \{0\}$ и $\mathcal{C}_w^\dagger \cap \mathcal{C}_w^{\perp_\delta} = \{0\}$.*

Как следствие, общее число $\mathfrak{D}$ различных аддитивных Ω-МС-кодов длины n над $\mathbb{F}_{q^t}$, имеющих дополнительные δ-двойственные, равно

$$\mathfrak{D} = \prod_{\nu=1}^{e_1} \mathfrak{D}_\nu \prod_{w=e_1+1}^{e_2} \mathfrak{D}_w \prod_{s=e_2+1}^{e_3} \mathfrak{D}_s, \tag{1}$$

где $\mathfrak{D}_\nu$, $1 \leqslant \nu \leqslant e_1$, – число различных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$, $\mathfrak{D}_w$, $e_1+1 \leqslant w \leqslant e_2$, – число различных пар $(\mathcal{C}_w, \mathcal{C}_w^\dagger)$, где $\mathcal{C}_w$ – $\mathcal{F}_w$-подпространство в $\mathcal{G}_w$, а $\mathcal{C}_w^\dagger$ – $\mathcal{F}_w^\dagger$-подпространство в $\mathcal{G}_w^\dagger$, таких что $\mathcal{C}_w \cap \mathcal{C}_w^{\dagger\perp_\delta} = \{0\}$ и $\mathcal{C}_w^\dagger \cap \mathcal{C}_w^{\perp_\delta} = \{0\}$, а $\mathfrak{D}_s$, $e_2+1 \leqslant s \leqslant e_3$, – число различных $\mathcal{F}_s$-подпространств в $\mathcal{G}_s$.

Доказательство непосредственно вытекает из теорем 1 и 2. ▲

Теперь применим эту теорему и теорию разложений Витта для подсчета количества всех аддитивных Ω-МС-кодов длины n над $\mathbb{F}_{q^t}$, имеющих дополнительные δ-двойственные, где $\delta \in \{0, *, \gamma\}$. Для этого вначале напомним некоторые определения из геометрии и теории групп. Если V – конечномерное векторное пространство над полем $\mathbb{F}_\mathfrak{Q}$, а B – полуторалинейная форма на V, то пара (V, B) называется полуторалинейным пространством (formed space) над $\mathbb{F}_\mathfrak{Q}$. Размерностью полуторалинейного пространства (V, B) называется размерность V как векторного пространства над $\mathbb{F}_\mathfrak{Q}$ и обозначается через $\dim_{\mathbb{F}_\mathfrak{Q}} V$. Пусть теперь (V, B) – n-мерное рефлексивное невырожденное полуторалинейное пространство над $\mathbb{F}_\mathfrak{Q}$. Индексом Витта m пространства (V, B) называется размерность максимального самоортогонального (или, что то же самое, максимального вполне изотропного) подпространства V. Отметим, что $n \geqslant 2m$. Ненулевой вектор $v \in V$ называется изотропным, если $B(v, v) = 0$. Гиперболической парой называется пара (v, w) изотропных векторов $v, w \in V$, таких что $B(v, w) = 1$. Всюду далее через $I_{m,n-2m}$ и $H_{m,n-2m}$ будем обозначать, соответственно, число изотропных векторов и гиперболических пар в n-мерном полуторалинейном пространстве (V, B) с индексом Витта m. Подробнее см. в [17, 18].

Напомним также следующий хорошо известный факт.

Лемма 1. *Для любого числа $\mathfrak{Q}$, равного степени простого, и любых натуральных чисел B, K, таких что $B \leqslant K$, число различных B-мерных подпространств K-мерного векторного пространств над $\mathbb{F}_\mathfrak{Q}$ равно $\mathfrak{Q}$-ичному гауссовскому биномиальному коэффициенту* $\begin{bmatrix} K \\ B \end{bmatrix}_\mathfrak{Q} = \prod_{b=0}^{B-1} \frac{(\mathfrak{Q}^{K-b} - 1)}{(\mathfrak{Q}^{b+1} - 1)}$ *(напомним, что $\mathfrak{Q}$-ичный биномиа-*

альный коэффициент $\begin{bmatrix} K \\ 0 \end{bmatrix}_{\mathfrak{Q}}$ *по определению равен* 1). *Как следствие, общее число различных подпространств* K*-мерного векторного пространства над* $\mathbb{F}_{\mathfrak{Q}}$ *равно*

$$N(K,\mathfrak{Q}) = \sum_{B=0}^{K} \begin{bmatrix} K \\ B \end{bmatrix}_{\mathfrak{Q}} = 1 + \sum_{B=1}^{K} \begin{bmatrix} K \\ B \end{bmatrix}_{\mathfrak{Q}}.$$

Теперь приступим к подсчету количества всех аддитивных Ω-МС-кодов длины n с длинами блоков $(m_1, m_2, \ldots, m_\ell)$ над $\mathbb{F}_{q^t}$, имеющих дополнительные δ-двойственные, для $\delta \in \{0, *, \gamma\}$.

§ 4. Число аддитивных Ω-МС-кодов над $\mathbb{F}_{q^t}$, имеющих дополнительные δ-двойственные

В следующей теореме получены явные формулы для числа всех аддитивных Ω-МС-кодов длины n над $\mathbb{F}_{q^t}$, имеющих дополнительные δ-двойственные, для $\delta \in \in \{0, *, \gamma\}$.

Теорема 4. *Пусть* $\Omega = (\omega_1, \omega_2, \ldots, \omega_\ell)$ *фиксировано. Тогда для* $\delta \in \{0, *, \gamma\}$ *общее число* $\mathfrak{D}$ *различных аддитивных* Ω*-МС-кодов длины* n *над* $\mathbb{F}_{q^t}$, *имеющих дополнительные* δ*-двойственные, равно*

$$\mathfrak{D} = \prod_{\nu=1}^{e_1} \mathfrak{D}_\nu \prod_{w=e_1+1}^{e_2} \left(\sum_{k=0}^{\eta_w t} \sum_{k_1=0}^{\varrho_w t} \sum_{k_2=0}^{\tau_w t} q^{k d_w (\eta_w t - k)} \begin{bmatrix} \eta_w t \\ k \end{bmatrix}_{q^{d_w}} \begin{bmatrix} \varrho_w t \\ k_1 \end{bmatrix}_{q^{d_w}} \begin{bmatrix} \tau_w t \\ k_2 \end{bmatrix}_{q^{d_w}} \right) \times$$
$$\times \prod_{s=e_2+1}^{e_3} \left(\sum_{a=0}^{\varepsilon_s t} \begin{bmatrix} \varepsilon_s t \\ a \end{bmatrix}_{q^{d_s}} \right),$$

где число $\mathfrak{D}_\nu$, $1 \leqslant \nu \leqslant e_1$, *равно следующему*:

- $2 + \sum\limits_{\substack{k=1 \\ k \text{ четно}}}^{\varepsilon_\nu t - 1} q^{\frac{k(\varepsilon_\nu t - k)}{2}} \begin{bmatrix} \varepsilon_\nu t/2 \\ k/2 \end{bmatrix}_{q^2}$, *если* $\nu \in \mathcal{J}_1$ *и либо* $\delta = \gamma$ *и* $\varepsilon_\nu t$ *четно, либо* $\delta = *$ *и оба числа* $\varepsilon_\nu t, q$ *четны*;
- $2 + \sum\limits_{\substack{k=1 \\ k \text{ четно}}}^{\varepsilon_\nu t - 1} q^{\frac{k(\varepsilon_\nu t - k + 1)}{2}} \begin{bmatrix} (\varepsilon_\nu t - 1)/2 \\ k/2 \end{bmatrix}_{q^2} + \sum\limits_{\substack{k=1 \\ k \text{ нечетно}}}^{\varepsilon_\nu t - 1} q^{\frac{(\varepsilon_\nu t - k)(k+1)}{2}} \begin{bmatrix} (\varepsilon_\nu t - 1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}$, *если* $\nu \in \mathcal{J}_1$, $\delta \in \{0, *\}$ *и оба числа* $\varepsilon_\nu t, q$ *нечетны*;
- $2 + \sum\limits_{\substack{k=1 \\ k \text{ четно}}}^{\varepsilon_\nu t - 1} q^{\frac{k(\varepsilon_\nu t - k)}{2}} \begin{bmatrix} \varepsilon_\nu t/2 \\ k/2 \end{bmatrix}_{q^2} + \sum\limits_{\substack{k=1 \\ k \text{ нечетно}}}^{\varepsilon_\nu t - 1} q^{\frac{(k\varepsilon_\nu t - k^2 - 1)}{2}} (q^{\frac{\varepsilon_\nu t}{2}} + 1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}$, *если* $\nu \in \mathcal{J}_1$, $\delta \in \{0, *\}$ *и либо* $\varepsilon_\nu t$ *четно и* $q \equiv 1 \pmod 4$, *либо* $\varepsilon_\nu t \equiv 0 \pmod 4$ *и* $q \equiv 3 \pmod 4$;
- $2 + \sum\limits_{\substack{k=1 \\ k \text{ четно}}}^{\varepsilon_\nu t - 1} q^{\frac{k(\varepsilon_\nu t - k)}{2}} \begin{bmatrix} \varepsilon_\nu t/2 \\ k/2 \end{bmatrix}_{q^2} + \sum\limits_{\substack{k=1 \\ k \text{ нечетно}}}^{\varepsilon_\nu t - 1} q^{\frac{(k\varepsilon_\nu t - k^2 - 1)}{2}} (q^{\frac{\varepsilon_\nu t}{2}} - 1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}$, *если* $\nu \in \mathcal{J}_1$, $\delta \in \{0, *\}$, $\varepsilon_\nu t \equiv 2 \pmod 4$ *и* $q \equiv 3 \pmod 4$;
- $2 + \sum\limits_{\substack{k=1 \\ k \text{ четно}}}^{\varepsilon_\nu t - 1} q^{\frac{k(\varepsilon_\nu t - k + 1)}{2}} \begin{bmatrix} (\varepsilon_\nu t - 1)/2 \\ k/2 \end{bmatrix}_{q^2} + \sum\limits_{\substack{k=1 \\ k \text{ нечетно}}}^{\varepsilon_\nu t - 1} q^{\frac{(\varepsilon_\nu t - k)(k+1)}{2}} \begin{bmatrix} (\varepsilon_\nu t - 1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}$, *если* $\nu \in \mathcal{J}_1$, $\delta = 0$, q *четно и* $\varepsilon_\nu t$ *нечетно*;

- $2+\sum\limits_{\substack{k=1\\ k\text{ четно}}}^{\varepsilon_\nu t-1} q^{\frac{(k\varepsilon_\nu t-k^2-2)}{2}}\left\{(q^k+q-1)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\ k/2\end{bmatrix}_{q^2}+(q^{\varepsilon_\nu t-k+1}-q^{\varepsilon_\nu t-k}+1)\times\right.$
$\left.\times\begin{bmatrix}(\varepsilon_\nu t-2)/2\\ (k-2)/2\end{bmatrix}_{q^2}\right\}+\sum\limits_{\substack{k=1\\ k\text{ нечетно}}}^{\varepsilon_\nu t-1} q^{\frac{(k+1)\varepsilon_\nu t-(k^2+1)}{2}}\begin{bmatrix}(\varepsilon_\nu t-2)/2\\ (k-1)/2\end{bmatrix}_{q^2}$, *если* $\nu\in\mathcal{J}_1$, $\delta=0$ *и оба числа* $\varepsilon_\nu t, q$ *четны*;
- $2+\sum\limits_{k=1}^{\varepsilon_\nu t-1} q^{\frac{k(\varepsilon_\nu t-k)d_\nu}{2}}\prod\limits_{a=0}^{k-1}\left(\dfrac{q^{\frac{(\varepsilon_\nu t-a)d_\nu}{2}}-(-1)^{\varepsilon_\nu t-a}}{q^{\frac{(k-a)d_\nu}{2}}-(-1)^{k-a}}\right)$, *если* $\nu\in\mathcal{J}_2$.

Для доказательства теоремы напомним, что согласно (1) общее число $\mathfrak{D}$ различных аддитивных Ω-МС-кодов длины n над $\mathbb{F}_{q^t}$, имеющих дополнительные δ-двойственные, равно $\mathfrak{D}=\prod\limits_{\nu=1}^{e_1}\mathfrak{D}_\nu\prod\limits_{w=e_1+1}^{e_2}\mathfrak{D}_w\prod\limits_{s=e_2+1}^{e_3}\mathfrak{D}_s$, где

- $\mathfrak{D}_\nu$, $1\leqslant\nu\leqslant e_1$, равно числу различных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$;
- $\mathfrak{D}_w$, $e_1+1\leqslant w\leqslant e_2$, равно числу различных пар $(\mathcal{C}_w,\mathcal{C}_w^\dagger)$, где $\mathcal{C}_w$ – $\mathcal{F}_w$-подпространство в $\mathcal{G}_w$, а $\mathcal{C}_w^\dagger$ – $\mathcal{F}_w^\dagger$-подпространство в $\mathcal{G}_w^\dagger$, таких что $\mathcal{C}_w\cap\mathcal{C}_w^{\dagger\perp_\delta}=\{0\}$ и $\mathcal{C}_w^\dagger\cap\mathcal{C}_w^{\perp_\delta}=\{0\}$;
- $\mathfrak{D}_s$, $e_2+1\leqslant s\leqslant e_3$, равно числу различных $\mathcal{F}_s$-подпространств в $\mathcal{G}_s$.

Ввиду этого для доказательства теоремы 4 достаточно определить числа $\mathfrak{D}_\nu$ для $1\leqslant\nu\leqslant e_1$, $\mathfrak{D}_w$ для $e_1+1\leqslant w\leqslant e_2$ и $\mathfrak{D}_s$ для $e_2+1\leqslant s\leqslant e_3$. С этой целью введем множества $\mathcal{J}_1=\{\nu:\,1\leqslant\nu\leqslant e_1,\,d_\nu=1\}$ и $\mathcal{J}_2=\{\nu:\,1\leqslant\nu\leqslant e_1,\,d_\nu>1\}$. Отметим, что $\{1,2,\ldots,e_1\}=\mathcal{J}_1\cup\mathcal{J}_2$ (несвязное объединение). Теперь приведем лемму 3.4 из работы [16], полезную для определения чисел $\mathfrak{D}_\nu$, $1\leqslant\nu\leqslant e_1$.

Лемма 2 [16]. *Зафиксируем* $\nu\in\mathcal{J}_1\cup\mathcal{J}_2=\{1,2,\ldots,e_1\}$. *Для* $\delta\in\{0,*,\gamma\}$ *обозначим через* $[\cdot\,,\cdot]_\delta\restriction_{\mathcal{G}_\nu\times\mathcal{G}_\nu}$ *ограничение* $\tau_{1,-1}$*-полуторалинейной формы* $[\cdot\,,\cdot]_\delta$ *на* $\mathcal{G}_\nu\times\mathcal{G}_\nu$. *Тогда справедливы следующие утверждения*:

(a) *Для* $\delta\in\{0,*,\gamma\}$ *ограничение* $[\cdot\,,\cdot]_\delta\restriction_{\mathcal{G}_\nu\times\mathcal{G}_\nu}$ *является рефлексивной невырожденной* $\tau_{1,-1}$*-полуторалинейной формой на* $\mathcal{G}_\nu$;

(b) *Для* $\nu\in\mathcal{J}_1$ *форма* $[\cdot\,,\cdot]_\delta\restriction_{\mathcal{G}_\nu\times\mathcal{G}_\nu}$ *является симметрической при* $\delta\in\{0,*\}$, *а форма* $[\cdot\,,\cdot]_\gamma\restriction_{\mathcal{G}_\nu\times\mathcal{G}_\nu}$ – *неопределенная*;

(c) *Для* $\nu\in\mathcal{J}_2$ *форма* $[\cdot\,,\cdot]_\delta\restriction_{\mathcal{G}_\nu\times\mathcal{G}_\nu}$ *является эрмитовой при* $\delta\in\{0,*\}$, *а форма* $[\cdot\,,\cdot]_\gamma\restriction_{\mathcal{G}_\nu\times\mathcal{G}_\nu}$ – *антиэрмитова.*

Для доказательства теоремы 4 вначале найдем значения $\mathfrak{D}_\nu$ для $\nu\in\mathcal{J}_1\cup\mathcal{J}_2=\{1,2,\ldots,e_1\}$. Для этого сперва заметим, что если обозначить через $\mathcal{N}_{\nu,k}$ число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$ для $0\leqslant k\leqslant\varepsilon_\nu t$, то $\mathfrak{D}_\nu=\sum\limits_{k=0}^{\varepsilon_\nu t}\mathcal{N}_{\nu,k}$. Так как $\tau_{1,-1}$-полуторалинейная форма $[\cdot\,,\cdot]_\delta\restriction_{\mathcal{G}_\nu\times\mathcal{G}_\nu}$ рефлексивна и невырождена, то $\mathcal{N}_{\nu,0}=\mathcal{N}_{\nu,\varepsilon_\nu t}=1$, откуда получаем

$$\mathfrak{D}_\nu=2+\sum_{k=1}^{\varepsilon_\nu t-1}\mathcal{N}_{\nu,k}\quad\text{для }\nu\in\mathcal{J}_1\cup\mathcal{J}_2=\{1,2,\ldots,e_1\}.\tag{2}$$

4.1. Определение числа $\mathfrak{D}_\nu$ для $\nu\in\mathcal{J}_1$. В этом пункте рассмотрим случай $\nu\in\mathcal{J}_1$ и найдем значения $\mathfrak{D}_\nu$ для $\delta\in\{0,*,\gamma\}$. Здесь $d_\nu=1$, и поэтому $\mathcal{F}_\nu\simeq\mathbb{F}_q$. В следующем предложении вычисляются значения $\mathfrak{D}_\nu$, когда либо $\delta=\gamma$, либо $\delta=*$ и q четно.

Предложение 1. *Пусть $\nu \in \mathcal{J}_1$ фиксировано. Если либо $\delta = \gamma$, либо $\delta = *$ и q четно, то*

$$\mathfrak{D}_\nu = 2 + \sum_{\substack{k=1 \\ k \text{ четно}}}^{\varepsilon_\nu t - 1} q^{\frac{k(\varepsilon_\nu t - k)}{2}} \begin{bmatrix} \varepsilon_\nu t/2 \\ k/2 \end{bmatrix}_{q^2}.$$

Доказательство. Согласно формуле (2) для доказательства достаточно найти числа $\mathcal{N}_{\nu,k}$ для $1 \leqslant k \leqslant \varepsilon_\nu t - 1$. Для этого заметим, что по утверждениям (a), (b) леммы 2 $(\mathcal{G}_\nu, [\cdot\,,\cdot]_\delta \restriction_{\mathcal{G}_\nu \times \mathcal{G}_\nu})$ является симплектическим пространством над $\mathcal{F}_\nu$, когда $\delta = \gamma$. Кроме того, когда $\delta = *$ и q четно, $[\mathcal{A}_\nu, \mathcal{A}_\nu]_* = 0$ для всех $\mathcal{A}_\nu \in \mathcal{G}_\nu$. Отсюда по лемме 2(a) следует, что $(\mathcal{G}_\nu, [\cdot\,,\cdot]_* \restriction_{\mathcal{G}_\nu \times \mathcal{G}_\nu})$ также является симплектическим пространством над $\mathcal{F}_\nu$, когда q четно. Далее, любое k-мерное невырожденное $\mathcal{F}_\nu$-подпространство W в $\mathcal{G}_\nu$ также является симплектическим пространством. Согласно [18, с. 69] размерность k такого подпространства W должна быть четной. Значит, $\mathcal{N}_{\nu,k} = 0$, если k нечетно.

Пусть k четно. В этом случае k-мерное подпространство W в $\mathcal{G}_\nu$ имеет разложение Витта $W = \langle \mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)} \rangle \perp \langle \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)} \rangle \perp \ldots \perp \langle \mathcal{A}_\nu^{(\frac{k}{2})}, \mathcal{B}_\nu^{(\frac{k}{2})} \rangle$, где $(\mathcal{A}_\nu^{(h)}, \mathcal{B}_\nu^{(h)})$ – гиперболическая пара в $\mathcal{G}_\nu$ для $1 \leqslant h \leqslant \dfrac{k}{2}$; множество $\{\mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(\frac{k}{2})}, \mathcal{B}_\nu^{(\frac{k}{2})}\}$ называется базисом Витта пространства W над $\mathcal{F}_\nu$ (см. [18, с. 69]). Применяя [17, предложение 2.9] и теорему Витта о сокращении, получаем, что число базисов Витта типа $\{\mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(\frac{k}{2})}, \mathcal{B}_\nu^{(\frac{k}{2})}\}$ в $\mathcal{G}_\nu$ равно

$$U_{k,\varepsilon_\nu t} = H_{\frac{\varepsilon_\nu t}{2},0} H_{\frac{\varepsilon_\nu t - 2}{2},0} \ldots H_{\frac{\varepsilon_\nu t - k + 2}{2},0}.$$

Аналогично выводится, что число базисов Витта k-мерного $\mathcal{F}_\nu$-подпространства в $\mathcal{G}_\nu$ равно

$$U_k = H_{\frac{k}{2},0} H_{\frac{k-2}{2},0} \ldots H_{1,0}.$$

Тогда согласно [18, с. 70] получаем

$$\mathcal{N}_{\nu,k} = \frac{U_{k,\varepsilon_\nu t}}{U_k} = q^{\frac{k(\varepsilon_\nu t - k)}{2}} \begin{bmatrix} \varepsilon_\nu t/2 \\ k/2 \end{bmatrix}_{q^2}.$$

Из этого с учетом (2) немедленно вытекает требуемое. ▲

В следующем предложении найдены числа $\mathfrak{D}_\nu$ в случае нечетного q и $\delta \in \{0, *\}$.

Предложение 2. *Пусть $\nu \in \mathcal{J}_1$ фиксировано. Если $\delta \in \{0, *\}$, а нечетное q – степень простого числа, то*

$$\mathfrak{D}_\nu = \begin{cases} 2 + \sum\limits_{\substack{k=1 \\ k \text{ четно}}}^{\varepsilon_\nu t - 1} q^{\frac{k(\varepsilon_\nu t - k + 1)}{2}} \begin{bmatrix} (\varepsilon_\nu t - 1)/2 \\ k/2 \end{bmatrix}_{q^2} + \sum\limits_{\substack{k=1 \\ k \text{ нечетно}}}^{\varepsilon_\nu t - 1} q^{\frac{(\varepsilon_\nu t - k)(k+1)}{2}} \begin{bmatrix} (\varepsilon_\nu t - 1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}, \\ \quad \textit{если } \varepsilon_\nu t \textit{ нечетно}, \\ 2 + \sum\limits_{\substack{k=1 \\ k \text{ четно}}}^{\varepsilon_\nu t - 1} q^{\frac{k(\varepsilon_\nu t - k)}{2}} \begin{bmatrix} \varepsilon_\nu t/2 \\ k/2 \end{bmatrix}_{q^2} + \sum\limits_{\substack{k=1 \\ k \text{ нечетно}}}^{\varepsilon_\nu t - 1} q^{\frac{(\varepsilon_\nu t k - k^2 - 1)}{2}} (q^{\frac{\varepsilon_\nu t}{2}} + 1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}, \\ \quad \textit{если либо } \varepsilon_\nu t \textit{ четно и } q \equiv 1 \pmod 4, \\ \quad \textit{либо } \varepsilon_\nu t \equiv 0 \pmod 4 \textit{ и } q \equiv 3 \pmod 4, \\ 2 + \sum\limits_{\substack{k=1 \\ k \text{ четно}}}^{\varepsilon_\nu t - 1} q^{\frac{k(\varepsilon_\nu t - k)}{2}} \begin{bmatrix} \varepsilon_\nu t/2 \\ k/2 \end{bmatrix}_{q^2} + \sum\limits_{\substack{k=1 \\ k \text{ нечетно}}}^{\varepsilon_\nu t - 1} q^{\frac{(\varepsilon_\nu t k - k^2 - 1)}{2}} (q^{\frac{\varepsilon_\nu t}{2}} - 1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}, \\ \quad \textit{если } \varepsilon_\nu t \equiv 2 \pmod 4 \textit{ и } q \equiv 3 \pmod 4. \end{cases}$$

Доказательство. В случае $\delta \in \{0, *\}$ согласно утверждениям (a), (b) леммы 2 $(\mathcal{G}_\nu, [\cdot,\cdot]_\delta \restriction_{\mathcal{G}_\nu \times \mathcal{G}_\nu})$ является $(\varepsilon_\nu t)$-мерным ортогональным пространством над $\mathcal{F}_\nu$. Далее, поскольку q нечетно, ортогональное пространство $(\mathcal{G}_\nu, [\cdot,\cdot]_\delta \restriction_{\mathcal{G}_\nu \times \mathcal{G}_\nu})$ может рассматриваться как невырожденное квадратичное пространство $(\mathcal{G}_\nu, \mathcal{Q}_\nu)$ относительно квадратичной формы $\mathcal{Q}_\nu \colon \mathcal{G}_\nu \to \mathcal{F}_\nu$, определяемой как $\mathcal{Q}_\nu(\mathcal{A}_\nu) = \frac{1}{2}[\mathcal{A}_\nu, \mathcal{A}_\nu]_\delta$ для всех $\mathcal{A}_\nu \in \mathcal{G}_\nu$. Далее, индекс Витта θ для $\mathcal{G}_\nu$ (см. [11, с. 279]) имеет вид

$$\theta = \begin{cases} (\varepsilon_\nu t - 1)/2, & \text{если } \varepsilon_\nu t \text{ нечетно,} \\ \varepsilon_\nu t/2, & \text{если } \varepsilon_\nu t \equiv 2 \pmod 4 \text{ и } q \equiv 3 \pmod 4, \\ (\varepsilon_\nu t - 2)/2, & \text{если либо } \varepsilon_\nu t \text{ четно и } q \equiv 1 \pmod 4, \\ & \text{либо } \varepsilon_\nu t \equiv 0 \pmod 4 \text{ и } q \equiv 3 \pmod 4. \end{cases} \tag{3}$$

Для вычисления $\mathfrak{D}_\nu$ согласно (2) достаточно определить числа $\mathcal{N}_{\nu,k}$ для $1 \leqslant k \leqslant \varepsilon_\nu t - 1$. Поэтому далее будем считать, что $1 \leqslant k \leqslant \varepsilon_\nu t - 1$ фиксировано. Из [18, с. 138] известно, что k-мерное невырожденное квадратичное $\mathcal{F}_\nu$-подпространство W в $\mathcal{G}_\nu$ имеет разложение Витта вида $W = \langle \mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)} \rangle \perp \langle \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)} \rangle \perp \ldots \perp \perp \langle \mathcal{A}_\nu^{(\theta_k)}, \mathcal{B}_\nu^{(\theta_k)} \rangle \perp \mathcal{W}_k$, где θ_k – индекс Витта пространства W, $(\mathcal{A}_\nu^{(h)}, \mathcal{B}_\nu^{(h)})$ – гиперболическая пара в $\mathcal{G}_\nu$ для $1 \leqslant h \leqslant \theta_k$, а $\mathcal{W}_k$ – анизотропное $\mathcal{F}_\nu$-подпространство в $\mathcal{G}_\nu$, такое что $\dim_{\mathcal{F}_\nu} \mathcal{W}_k = k - 2\theta_k \leqslant 2$. Рассмотрим отдельно следующие два случая: (i) k нечетно и (ii) k четно.

(i) Вначале пусть k нечетно. Тогда согласно [18, с. 138] имеем $\theta_k = (k-1)/2$, откуда $\dim_{\mathcal{F}_\nu} \mathcal{W}_k = 1$. Из этого, в свою очередь, следует, что k-мерное $\mathcal{F}_\nu$-подпространство W в $\mathcal{G}_\nu$ имеет разложение Витта $W = \langle \mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)} \rangle \perp \langle \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)} \rangle \perp \ldots \perp \perp \langle \mathcal{A}_\nu^{(\frac{k-1}{2})}, \mathcal{B}_\nu^{(\frac{k-1}{2})} \rangle \perp \langle Z_\nu \rangle$, где $(\mathcal{A}_\nu^{(h)}, \mathcal{B}_\nu^{(h)})$ – гиперболическая пара в $\mathcal{G}_\nu$ для $1 \leqslant h \leqslant \frac{k-1}{2}$, а Z_ν – несингулярный вектор в $\mathcal{G}_\nu$; множество $\{\mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(\frac{k-1}{2})}, \mathcal{B}_\nu^{(\frac{k-1}{2})}, Z_\nu\}$ называется базисом Витта пространства W над $\mathcal{F}_\nu$. Применяя [17, предложение 2.9] и теорему Витта о сокращении, получаем, что число базисов Витта типа $\{\mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(\frac{k-1}{2})}, \mathcal{B}_\nu^{(\frac{k-1}{2})}, Z_\nu\}$ в $\mathcal{G}_\nu$ равно

$$U_{\frac{k-1}{2},\theta} = H_{\theta,\varepsilon_\nu t-2\theta} H_{\theta-1,\varepsilon_\nu t-2\theta} \ldots H_{\theta-\frac{(k-3)}{2},\varepsilon_\nu t-2\theta} \Big(q^{\varepsilon_\nu t-k+1} - 1 - I_{\theta-\frac{(k-1)}{2},\varepsilon_\nu t-2\theta} \Big).$$

Аналогично выводится, что число базисов Витта для k-мерного $\mathcal{F}_\nu$-подпространства в $\mathcal{G}_\nu$ равно

$$U_{\frac{k-1}{2}} = H_{\frac{k-1}{2},1} H_{\frac{k-3}{2},1} \ldots H_{1,1}(q-1).$$

Тогда в силу [18, с. 140–141] имеем

$$\mathcal{N}_{\nu,k} = \frac{U_{\frac{k-1}{2},\theta}}{U_{\frac{k-1}{2}}} = \begin{cases} q^{\frac{(k\varepsilon_\nu t - k^2 - 1)}{2}} (q^{\frac{\varepsilon_\nu t}{2}} - 1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}, & \text{если } \theta = \varepsilon_\nu t/2, \\ q^{\frac{(\varepsilon_\nu t - k)(k+1)}{2}} \begin{bmatrix} (\varepsilon_\nu t - 1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}, & \text{если } \theta = (\varepsilon_\nu t - 1)/2, \\ q^{\frac{(k\varepsilon_\nu t - k^2 - 1)}{2}} (q^{\frac{\varepsilon_\nu t}{2}} + 1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}, & \text{если } \theta = (\varepsilon_\nu t - 2)/2. \end{cases} \tag{4}$$

(ii) Теперь пусть k четно. Согласно [18, с. 138] имеем либо $\theta_k = k/2$, либо $\theta_k = (k-2)/2$. Обозначим через $R_{\nu,k}$ и $S_{\nu,k}$ число k-мерных невырожденных квадратичных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$, имеющих индексы Витта $k/2$ и $(k-2)/2$ соответственно. Отметим, что $\mathcal{N}_{\nu,k} = R_{\nu,k} + S_{\nu,k}$.

Если $\theta_k = k/2$, то $\dim_{\mathcal{F}_\nu} \mathcal{W}_k = 0$. Тогда k-мерное $\mathcal{F}_\nu$-подпространство W в $\mathcal{G}_\nu$ имеет разложение Витта $W = \langle \mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)} \rangle \perp \langle \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)} \rangle \perp \ldots \perp \langle \mathcal{A}_\nu^{(\frac{k}{2})}, \mathcal{B}_\nu^{(\frac{k}{2})} \rangle$, где $(\mathcal{A}_\nu^{(h)}, \mathcal{B}_\nu^{(h)})$ – гиперболическая пара в $\mathcal{G}_\nu$ для $1 \leqslant h \leqslant \dfrac{k}{2}$; множество $\{\mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(\frac{k}{2})}, \mathcal{B}_\nu^{(\frac{k}{2})}\}$ называется базисом Витта пространства W над $\mathcal{F}_\nu$. Применяя [17, предложение 2.9] и теорему Витта о сокращении, получаем, что число базисов Витта типа $\{\mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(\frac{k}{2})}, \mathcal{B}_\nu^{(\frac{k}{2})}\}$ в $\mathcal{G}_\nu$ равно

$$U_{\frac{k}{2},\theta} = H_{\theta,\varepsilon_\nu t-2\theta} H_{\theta-1,\varepsilon_\nu t-2\theta} \ldots H_{\theta-\frac{k-2}{2},\varepsilon_\nu t-2\theta},$$

а число базисов Витта k-мерного $\mathcal{F}_\nu$-подпространства в $\mathcal{G}_\nu$, имеющего индекс Витта $\dfrac{k}{2}$, равно $U_{\frac{k}{2}} = H_{\frac{k}{2},0} H_{\frac{k-2}{2},0} \ldots H_{1,0}$. Тогда из [18, с. 140–141] получаем

$$R_{\nu,k} = \frac{U_{\frac{k}{2},\theta}}{U_{\frac{k}{2}}} = \begin{cases} \dfrac{q^{\frac{k(\varepsilon_\nu t-k)}{2}}(q^{\frac{k}{2}}+1)(q^{\frac{\varepsilon_\nu t-k}{2}}+1)}{2(q^{\frac{\varepsilon_\nu t}{2}}+1)} \begin{bmatrix} \varepsilon_\nu t/2 \\ k/2 \end{bmatrix}_{q^2}, & \text{если } \theta = \varepsilon_\nu t/2, \\ \dfrac{q^{\frac{k(\varepsilon_\nu t-k)}{2}}(q^{\frac{k}{2}}+1)}{2} \begin{bmatrix} (\varepsilon_\nu t-1)/2 \\ k/2 \end{bmatrix}_{q^2}, & \text{если } \theta = (\varepsilon_\nu t-1)/2, \\ \dfrac{q^{\frac{k(\varepsilon_\nu t-k)}{2}}(q^{\frac{k}{2}}+1)(q^{\frac{\varepsilon_\nu t-k}{2}}-1)}{2(q^{\frac{\varepsilon_\nu t}{2}}-1)} \begin{bmatrix} \varepsilon_\nu t/2 \\ k/2 \end{bmatrix}_{q^2}, & \text{если } \theta = (\varepsilon_\nu t-2)/2. \end{cases}$$

Если $\theta_k = (k-2)/2$, то $\dim_{\mathcal{F}_\nu} \mathcal{W}_k = 2$. В этом случае, рассуждая так же, как и в [13, леммы 3.2, 3.3], получаем что каждое двумерное анизотропное $\mathcal{F}_\nu$-подпространство в W имеет ортогональный базис и что число различных ортогональных базисов двумерного анизотропного $\mathcal{F}_\nu$-подпространства в W равно

$$X_{k,\theta} = \begin{cases} \dfrac{q^{\varepsilon_\nu t-k}(q-1)^2(q^{\frac{\varepsilon_\nu t-k}{2}}-1)(q^{\frac{\varepsilon_\nu t-k+2}{2}}-1)}{2}, & \text{если } \theta = \varepsilon_\nu t/2, \\ \dfrac{q^{\varepsilon_\nu t-k}(q-1)^2(q^{\varepsilon_\nu t-k+1}-1)}{2}, & \text{если } \theta = (\varepsilon_\nu t-1)/2, \\ \dfrac{q^{\varepsilon_\nu t-k}(q-1)^2(q^{\frac{\varepsilon_\nu t-k}{2}}+1)(q^{\frac{\varepsilon_\nu t-k+2}{2}}+1)}{2}, & \text{если } \theta = (\varepsilon_\nu t-2)/2. \end{cases}$$

Таким образом, k-мерное $\mathcal{F}_\nu$-подпространство W пространства $\mathcal{G}_\nu$ имеет разложение Витта $W = \langle \mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)} \rangle \perp \langle \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)} \rangle \perp \ldots \perp \langle \mathcal{A}_\nu^{(\frac{k-2}{2})}, \mathcal{B}_\nu^{(\frac{k-2}{2})} \rangle \perp \langle Z_\nu^{(1)}, Z_\nu^{(2)} \rangle$, где $(\mathcal{A}_\nu^{(h)}, \mathcal{B}_\nu^{(h)})$ – гиперболическая пара в $\mathcal{G}_\nu$ для $1 \leqslant h \leqslant \dfrac{k-2}{2}$, а $\{Z_\nu^{(1)}, Z_\nu^{(2)}\}$ – ортогональный базис двумерного анизотропного $\mathcal{F}_\nu$-подпространства $\mathcal{W}_k$ пространства W; множество $\{\mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(\frac{k-2}{2})}, \mathcal{B}_\nu^{(\frac{k-2}{2})}, Z_\nu^{(1)}, Z_\nu^{(2)}\}$ называется базисом Витта пространства W над $\mathcal{F}_\nu$. Применяя [17, предложение 2.9] и теорему Витта о сокращении, получаем, что число базисов Витта типа $\{\mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(\frac{k-2}{2})}, \mathcal{B}_\nu^{(\frac{k-2}{2})}, Z_\nu^{(1)}, Z_\nu^{(2)}\}$ в $\mathcal{G}_\nu$ равно

$$U_{\frac{k-2}{2},\theta} = H_{\theta,\varepsilon_\nu t-2\theta} H_{\theta-1,\varepsilon_\nu t-2\theta} \ldots H_{\theta-\frac{(k-4)}{2},\varepsilon_\nu t-2\theta} X_{k,\theta}.$$

Аналогично выводится, что число базисов Витта k-мерного $\mathcal{F}_\nu$-подпространства в $\mathcal{G}_\nu$, имеющих индекс Витта $\dfrac{k-2}{2}$, равно

$$U_{\frac{k-2}{2}} = H_{\frac{k-2}{2},2} H_{\frac{k-4}{2},2} \ldots H_{1,2}(q^2-1)(q-1).$$

Тогда согласно [18, с. 140–141] получаем

$$S_{\nu,k}=\frac{U_{\frac{k-2}{2},\theta}}{U_{\frac{k-2}{2}}}=\begin{cases}\dfrac{q^{\frac{k(\varepsilon_\nu t-k)}{2}}(q^{\frac{k}{2}}-1)(q^{\frac{\varepsilon_\nu t-k}{2}}-1)}{2(q^{\frac{\varepsilon_\nu t}{2}}+1)}\begin{bmatrix}\varepsilon_\nu t/2\\ k/2\end{bmatrix}_{q^2}, & \text{если } \theta=\varepsilon_\nu t/2,\\ \dfrac{q^{\frac{k(\varepsilon_\nu t-k)}{2}}(q^{\frac{k}{2}}-1)}{2}\begin{bmatrix}(\varepsilon_\nu t-1)/2\\ k/2\end{bmatrix}_{q^2}, & \text{если } \theta=(\varepsilon_\nu t-1)/2,\\ \dfrac{q^{\frac{k(\varepsilon_\nu t-k)}{2}}(q^{\frac{k}{2}}-1)(q^{\frac{\varepsilon_\nu t-k}{2}}+1)}{2(q^{\frac{\varepsilon_\nu t}{2}}-1)}\begin{bmatrix}\varepsilon_\nu t/2\\ k/2\end{bmatrix}_{q^2}, & \text{если } \theta=(\varepsilon_\nu t-2)/2.\end{cases}$$

Отсюда следует, что

$$\mathcal{N}_{\nu,k}=R_{\nu,k}+S_{\nu,k}=\begin{cases}q^{\frac{k(\varepsilon_\nu t-k)}{2}}\begin{bmatrix}\varepsilon_\nu t/2\\ k/2\end{bmatrix}_{q^2}, & \text{если } \theta=\varepsilon_\nu t/2,\\ q^{\frac{k(\varepsilon_\nu t-k+1)}{2}}\begin{bmatrix}(\varepsilon_\nu t-1)/2\\ k/2\end{bmatrix}_{q^2}, & \text{если } \theta=(\varepsilon_\nu t-1)/2,\\ q^{\frac{k(\varepsilon_\nu t-k)}{2}}\begin{bmatrix}\varepsilon_\nu t/2\\ k/2\end{bmatrix}_{q^2}, & \text{если } \theta=(\varepsilon_\nu t-2)/2.\end{cases}\tag{5}$$

Наконец, подставляя значения $\mathcal{N}_{\nu,k}$ из (4), (5) в (2), получаем требуемый результат. ▲

В следующем предложении найдены числа $\mathfrak{D}_\nu$ в случае, когда q четно и $\delta=0$.

Предложение 3. *Пусть $\nu\in\mathcal{J}_1$ фиксировано. Если $\delta=0$, а четное q – степень простого числа, то*

$$\mathfrak{D}_\nu=\begin{cases}2+\sum\limits_{\substack{k=1\\ k\text{ четно}}}^{\varepsilon_\nu t-1}q^{\frac{k(\varepsilon_\nu t-k+1)}{2}}\begin{bmatrix}(\varepsilon_\nu t-1)/2\\ k/2\end{bmatrix}_{q^2}+\\ \quad+\sum\limits_{\substack{k=1\\ k\text{ нечетно}}}^{\varepsilon_\nu t-1}q^{\frac{(\varepsilon_\nu t-k)(k+1)}{2}}\begin{bmatrix}(\varepsilon_\nu t-1)/2\\ (k-1)/2\end{bmatrix}_{q^2}, & \text{если } \varepsilon_\nu t \text{ нечетно},\\ 2+\sum\limits_{\substack{k=1\\ k\text{ четно}}}^{\varepsilon_\nu t-1}q^{\frac{(k\varepsilon_\nu t-k^2-2)}{2}}\Bigg((q^k+q-1)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\ k/2\end{bmatrix}_{q^2}+\\ \quad+(q^{\varepsilon_\nu t-k+1}-q^{\varepsilon_\nu t-k}+1)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\ (k-2)/2\end{bmatrix}_{q^2}\Bigg)+\\ \quad+\sum\limits_{\substack{k=1\\ k\text{ нечетно}}}^{\varepsilon_\nu t-1}q^{\frac{(k+1)\varepsilon_\nu t-(k^2+1)}{2}}\begin{bmatrix}(\varepsilon_\nu t-2)/2\\ (k-1)/2\end{bmatrix}_{q^2}, & \text{если } \varepsilon_\nu t \text{ четно}.\end{cases}$$

Доказательство. Чтобы вычислить $\mathfrak{D}_\nu$, в силу (2) достаточно найти числа $\mathcal{N}_{\nu,k}$ для $1\leqslant k\leqslant\varepsilon_\nu t-1$. Для этого зафиксируем $1\leqslant k\leqslant\varepsilon_\nu t-1$. Заметим, что поскольку q здесь четно, все m_i – нечетные целые числа. Следовательно, m нечетно, откуда, в свою очередь, вытекает, что $\dfrac{m}{m_i}=1$ в $\mathcal{F}_\nu$. Так как $\nu\in\mathcal{J}_1$, то $d_\nu=1$, откуда $a_\nu=\text{НОД}(t,d_\nu)=1$. Поэтому каждый $\mathcal{A}_\nu\in\mathcal{G}_\nu$ можно представить в виде $\mathcal{A}_\nu=\mathcal{A}_{\nu,0}=(\mathcal{A}_{\nu,0}^{(1)},\mathcal{A}_{\nu,0}^{(2)},\dots,\mathcal{A}_{\nu,0}^{(\ell)})$, где $\mathcal{A}_{\nu,0}^{(i)}\in\varepsilon_{\nu,i}\mathcal{F}_{\nu,0}$ для $1\leqslant i\leqslant\ell$. Теперь положим

$$\mathcal{M}_\nu=\left\{(\mathcal{A}_{\nu,0}^{(1)},\mathcal{A}_{\nu,0}^{(2)},\dots,\mathcal{A}_{\nu,0}^{(\ell)})\in\mathcal{G}_\nu:\sum_{i=1}^{\ell}\varepsilon_{\nu,i}\big(\mathcal{A}_{\nu,0}^{(i)}+\tau_{q,1}(\mathcal{A}_{\nu,0}^{(i)})+\ldots+\tau_{q^{t-1},1}(\mathcal{A}_{\nu,0}^{(i)})\big)=0\right\}.$$

Заметим, что множество $\mathcal{M}_\nu$ является $(\varepsilon_\nu t-1)$-мерным $\mathcal{F}_\nu$-подпространством в $\mathcal{G}_\nu$. Положим также $\Theta_\nu=(\varepsilon_{\nu,1},\varepsilon_{\nu,2},\dots,\varepsilon_{\nu,\ell})\in\mathcal{G}_\nu$. Легко видеть, что $\Theta_\nu\in\mathcal{M}_\nu$ тогда и только тогда, когда $\varepsilon_\nu t$ четно. Соответственно возникают следующие случаи: (i) $\varepsilon_\nu t$ нечетно и (ii) $\varepsilon_\nu t$ четно.

(i) Пусть $\varepsilon_\nu t$ нечетно. Тогда $\Theta_\nu \notin \mathcal{M}_\nu$ и $\dim_{\mathcal{F}_\nu}\langle \Theta_\nu\rangle = 1$. Кроме того, $[\mathcal{A}_\nu, \Theta_\nu]_0 = 0$ для всех $\mathcal{A}_\nu \in \mathcal{M}_\nu$, и при этом $\mathcal{M}_\nu \cap \langle \Theta_\nu\rangle = \{0\}$. Отсюда следует, что пространство $\mathcal{G}_\nu$ является ортогональной прямой суммой своих $\mathcal{F}_\nu$-подпространств $\mathcal{M}_\nu$ и $\langle \Theta_\nu\rangle$, т.е. $\mathcal{G}_\nu = \mathcal{M}_\nu \perp \langle \Theta_\nu\rangle$. Далее, $(\mathcal{M}_\nu, [\cdot\,,\cdot]_0\restriction_{\mathcal{M}_\nu\times\mathcal{M}_\nu})$ – симплектическое пространство над $\mathcal{F}_\nu$. При этом любое $\mathcal{F}_\nu$-подпространство в $\mathcal{G}_\nu$ либо содержится в $\mathcal{M}_\nu$, либо не содержится в $\mathcal{M}_\nu$.

Для вычисления $\mathcal{N}_{\nu,k}$ вначале определим число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств пространства $\mathcal{G}_\nu$, содержащихся в $\mathcal{M}_\nu$. Для этого, рассуждая так же, как и в предложении 1, получаем, что для нечетного k в $\mathcal{M}_\nu$ не существует k-мерных невырожденных $\mathcal{F}_\nu$-подпространств, а для четного k в $\mathcal{M}_\nu$ содержится ровно

$$\mathfrak{N}^{(e)}_{\nu,k} = q^{\frac{k(\varepsilon_\nu t-k-1)}{2}} \begin{bmatrix} (\varepsilon_\nu t-1)/2 \\ k/2 \end{bmatrix}_{q^2}$$

различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств.

Далее, нетрудно видеть, что любое k-мерное $\mathcal{F}_\nu$-подпространство W в $\mathcal{G}_\nu$, не содержащееся в $\mathcal{M}_\nu$, имеет тип $W = \langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k-1)}_\nu, \mathcal{A}^{(k)}_\nu + \Theta_\nu\rangle$, где $\mathcal{A}^{(h)}_\nu \in \in \mathcal{M}_\nu \setminus \{0\}$ для $1 \leqslant h \leqslant k-1$ и $\mathcal{A}^{(k)}_\nu \in \mathcal{M}_\nu$. Теперь отдельно рассмотрим следующие два случая: k нечетно и k четно.

Вначале пусть k нечетно. Тогда, применяя [19, теорема 5.1.1] и [20, гл. 6, упражнение 21], получаем, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k-1)}_\nu, \mathcal{A}^{(k)}_\nu + \Theta_\nu\rangle$ пространства $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда $\langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k-1)}_\nu\rangle$ является $(k-1)$-мерным невырожденным $\mathcal{F}_\nu$-подпространством в $\mathcal{M}_\nu$. Далее заметим, что все $\mathcal{A}^{(k)}_\nu \in \langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k-1)}_\nu\rangle^{\perp_0}$ порождают различные k-мерные невырожденные $\mathcal{F}_\nu$-подпространства $\langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k-1)}_\nu, \mathcal{A}^{(k)}_\nu + \Theta_\nu\rangle$ в $\mathcal{G}_\nu$ и что есть ровно $q^{\varepsilon_\nu t-k}$ способов выбрать $\mathcal{A}^{(k)}_\nu$. Отсюда, рассуждая так же, как в предложении 1, получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств типа $\langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k-1)}_\nu, \mathcal{A}^{(k)}_\nu + \Theta_\nu\rangle$ в $\mathcal{G}_\nu$ равно

$$\mathfrak{M}^{(o)}_{\nu,k} = q^{\varepsilon_\nu t-k} q^{\frac{(k-1)(\varepsilon_\nu t-k)}{2}} \begin{bmatrix} (\varepsilon_\nu t-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}.$$

Теперь пусть k четно. Если $\mathcal{A}^{(k)}_\nu = 0$, то в силу [19, теорема 5.1.1] и [20, гл. 6, упражнение 21] получаем, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k-1)}_\nu, \Theta_\nu\rangle$ пространства $\mathcal{G}_\nu$ вырождено.

Если $\mathcal{A}^{(k)}_\nu \neq 0$, то снова применяя [19, теорема 5.1.1] и [20, гл. 6, упражнение 21], находим, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k-1)}_\nu, \mathcal{A}^{(k)}_\nu + \Theta_\nu\rangle$ в $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда $\langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k)}_\nu\rangle$ является k-мерным невырожденным $\mathcal{F}_\nu$-подпространством в $\mathcal{M}_\nu$. Далее, каждое k-мерное невырожденное $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k)}_\nu\rangle$ в $\mathcal{M}_\nu$ порождает ровно (q^k-1) различных $\mathcal{F}_\nu$-подпространств $\langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k-1)}_\nu, \mathcal{A}^{(k)}_\nu + \Theta_\nu\rangle$ в $\mathcal{G}_\nu$. Отсюда, рассуждая так же, как и в предложении 1, заключаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств типа $\langle \mathcal{A}^{(1)}_\nu, \mathcal{A}^{(2)}_\nu, \ldots, \mathcal{A}^{(k-1)}_\nu, \mathcal{A}^{(k)}_\nu + \Theta_\nu\rangle$ в $\mathcal{G}_\nu$, где $\mathcal{A}^{(h)}_\nu \in \mathcal{M}_\nu \setminus \{0\}$ для $1 \leqslant h \leqslant k$, равно

$$\mathfrak{M}^{(e)}_{\nu,k} = q^{\frac{k(\varepsilon_\nu t-k-1)}{2}}(q^k-1) \begin{bmatrix} (\varepsilon_\nu t-1)/2 \\ k/2 \end{bmatrix}_{q^2}.$$

Объединяя эти случаи, получаем

$$\mathcal{N}_{\nu,k} = \mathfrak{M}^{(o)}_{\nu,k} = q^{\frac{(k+1)(\varepsilon_\nu t-k)}{2}} \begin{bmatrix} (\varepsilon_\nu t-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}, \quad \text{если } k \text{ нечетно,}$$

и

$$\mathcal{N}_{\nu,k} = \mathfrak{N}^{(e)}_{\nu,k} + \mathfrak{M}^{(e)}_{\nu,k} = q^{\frac{k(\varepsilon_\nu t-k+1)}{2}} \begin{bmatrix} (\varepsilon_\nu t-1)/2 \\ k/2 \end{bmatrix}_{q^2}, \quad \text{если } k \text{ четно.}$$

(ii) Пусть $\varepsilon_\nu t$ четно. Тогда $\Theta_\nu \in \mathcal{M}_\nu \cap \mathcal{M}_\nu^{\perp_0}$. Пусть теперь $\widehat{\mathcal{M}}_\nu$ – $(\varepsilon_\nu t-2)$-мерное $\mathcal{F}_\nu$-подпространство в $\mathcal{M}_\nu$, такое что $\Theta_\nu \notin \widehat{\mathcal{M}}_\nu$, так что $\mathcal{M}_\nu = \widehat{\mathcal{M}}_\nu \oplus \langle \Theta_\nu \rangle$. Далее, заметим, что существует $y_\nu \in \widehat{\mathcal{M}}_\nu^{\perp_0} \setminus \mathcal{M}_\nu$, такой что $\mathcal{G}_\nu = \widehat{\mathcal{M}}_\nu \oplus \langle \Theta_\nu \rangle \oplus \langle y_\nu \rangle$. При этом $(\widehat{\mathcal{M}}_\nu, [\cdot\,,\cdot]_0 \restriction_{\widehat{\mathcal{M}}_\nu \times \widehat{\mathcal{M}}_\nu})$ является $(\varepsilon_\nu t-2)$-мерным симплектическим $\mathcal{F}_\nu$-подпространством в $\mathcal{G}_\nu$. Далее заметим, что каждое k-мерное $\mathcal{F}_\nu$-подпространство в $\mathcal{G}_\nu$ либо содержится в $\widehat{\mathcal{M}}_\nu$, либо содержится в $\widehat{\mathcal{M}}_\nu \oplus \langle \Theta_\nu \rangle$, но не содержится в $\widehat{\mathcal{M}}_\nu$, либо содержится в $\widehat{\mathcal{M}}_\nu \oplus \langle y_\nu \rangle$, но не содержится в $\widehat{\mathcal{M}}_\nu$, либо содержится в $\mathcal{G}_\nu = \widehat{\mathcal{M}}_\nu \oplus \oplus \langle \Theta_\nu \rangle \oplus \langle y_\nu \rangle$, но не содержится ни в одном из подпространств $\widehat{\mathcal{M}}_\nu$, $\widehat{\mathcal{M}}_\nu \oplus \langle \Theta_\nu \rangle$ и $\widehat{\mathcal{M}}_\nu \oplus \langle y_\nu \rangle$. В соответствии с этим рассмотрим следующие четыре случая по отдельности.

A. Вначале подсчитаем число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\widehat{\mathcal{M}}_\nu$. Для этого, рассуждая так же, как и в предложении 1, заметим, что для нечетного k в $\widehat{\mathcal{M}}_\nu$ не существует k-мерных невырожденных $\mathcal{F}_\nu$-подпространств, а для четного k в $\widehat{\mathcal{M}}_\nu$ есть ровно

$$\mathfrak{N}^{(e)}_{\nu,k} = q^{\frac{k(\varepsilon_\nu t-k-2)}{2}\left[\begin{smallmatrix}(\varepsilon_\nu t-2)/2 \\ k/2\end{smallmatrix}\right]_{q^2}}$$

различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств.

B. Теперь подсчитаем все различные k-мерные невырожденные $\mathcal{F}_\nu$-подпространства пространства $\mathcal{G}_\nu$, содержащиеся в $\widehat{\mathcal{M}}_\nu \oplus \langle \Theta_\nu \rangle$, но не содержащиеся в $\widehat{\mathcal{M}}_\nu$. Рассуждая, как и в случае (i), получаем, что если k нечетно, то в $\mathcal{G}_\nu$ не существует таких k-мерных невырожденных $\mathcal{F}_\nu$-подпространств, а если k четно, то в $\mathcal{G}_\nu$ есть ровно

$$\mathfrak{S}^{(e)}_{\nu,k} = (q^k-1)q^{\frac{k(\varepsilon_\nu t-k-2)}{2}\left[\begin{smallmatrix}(\varepsilon_\nu t-2)/2 \\ k/2\end{smallmatrix}\right]_{q^2}}$$

таких k-мерных невырожденных $\mathcal{F}_\nu$-подпространств.

C. Теперь подсчитаем все различные k-мерные невырожденные $\mathcal{F}_\nu$-подпространства пространства $\mathcal{G}_\nu$, содержащиеся в $\widehat{\mathcal{M}}_\nu \oplus \langle y_\nu \rangle$, но не содержащиеся в $\widehat{\mathcal{M}}_\nu$. Снова рассуждая, как в случае (i), получаем, что если k нечетно, то в $\mathcal{G}_\nu$ есть ровно

$$\mathfrak{T}^{(o)}_{\nu,k} = q^{\frac{(k+1)(\varepsilon_\nu t-k-1)}{2}} \begin{bmatrix} (\varepsilon_\nu t-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}$$

таких k-мерных невырожденных $\mathcal{F}_\nu$-подпространств, а если k четно, то ровно

$$\mathfrak{T}^{(e)}_{\nu,k} = (q^k-1)q^{\frac{k(\varepsilon_\nu t-k-2)}{2}\left[\begin{smallmatrix}(\varepsilon_\nu t-2)/2 \\ k/2\end{smallmatrix}\right]_{q^2}}$$

таких k-мерных невырожденных $\mathcal{F}_\nu$-подпространств.

D. Теперь заметим, что любое k-мерное $\mathcal{F}_\nu$-подпространство W пространства $\mathcal{G}_\nu$, содержащееся в $\mathcal{G}_\nu = \widehat{\mathcal{M}}_\nu \oplus \langle \Theta_\nu \rangle \oplus \langle y_\nu \rangle$, но не содержащееся ни в одном из его

подпространств $\widehat{\mathcal{M}}_\nu$, $\widehat{\mathcal{M}}_\nu \oplus \langle \Theta_\nu \rangle$ и $\widehat{\mathcal{M}}_\nu \oplus \langle y_\nu \rangle$, относится к одному из следующих двух типов:

I. $W = \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} + \Theta_\nu + \lambda_\nu y_\nu \rangle$, где $\lambda_\nu \in \mathcal{F}_\nu \setminus \{0\}$, $\mathcal{A}_\nu^{(h)} \in \widehat{\mathcal{M}}_\nu \setminus \{0\}$ для $1 \leqslant h \leqslant k-1$ и $\mathcal{A}_\nu^{(k)} \in \widehat{\mathcal{M}}_\nu$.

II. $W = \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$, где $k \geqslant 2$, $\mathcal{A}_\nu^{(h)} \in \widehat{\mathcal{M}}_\nu \setminus \{0\}$ для $1 \leqslant h \leqslant k-2$ и $\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} \in \widehat{\mathcal{M}}_\nu$.

Чтобы вычислить $\mathcal{N}_{\nu,k}$, вначале определим число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств типа $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} + \Theta_\nu + \lambda_\nu y_\nu \rangle$ в $\mathcal{G}_\nu$, где $\lambda_\nu \in \mathcal{F}_\nu \setminus \{0\}$, $\mathcal{A}_\nu^{(h)} \in \widehat{\mathcal{M}}_\nu \setminus \{0\}$ для $1 \leqslant h \leqslant k-1$ и $\mathcal{A}_\nu^{(k)} \in \widehat{\mathcal{M}}_\nu$. Для этого рассмотрим следующие два случая: k четно и k нечетно.

Сперва пусть k четно. Если $\mathcal{A}_\nu^{(k)} = 0$, то в силу [19, теорема 5.1.1] и [20, гл. 6, упражнение 21] получаем, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \Theta_\nu + \lambda_\nu y_\nu \rangle$ пространства $\mathcal{G}_\nu$ вырождено.

Если же $\mathcal{A}_\nu^{(k)} \neq 0$, то снова применяя [19, теорема 5.1.1] и [20, гл. 6, упражнение 21], получаем, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} + \Theta_\nu + \lambda_\nu y_\nu \rangle$ пространства $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} \rangle$ является k-мерным невырожденным $\mathcal{F}_\nu$-подпространством в $\widehat{\mathcal{M}}_\nu$. Далее, каждое k-мерное невырожденное $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} \rangle$ в $\widehat{\mathcal{M}}_\nu$ порождает ровно $(q^k-1)(q-1)$ различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} + \Theta_\nu + \lambda_\nu y_\nu \rangle$ пространства $\mathcal{G}_\nu$.

Отсюда, рассуждая, как в предложении 1, получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств пространства $\mathcal{G}_\nu$, имеющих тип $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} + \Theta_\nu + \lambda_\nu y_\nu \rangle$, равно

$$\mathfrak{U}_{\nu,k}^{(e)} = q^{\frac{k(\varepsilon_\nu t - k - 2)}{2}} (q^k - 1)(q-1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ k/2 \end{bmatrix}_{q^2}.$$

Теперь предположим, что k нечетно. Тогда в силу [19, теорема 5.1.1] и [20, гл. 6, упражнение 21] получаем, что подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} + \Theta_\nu + {} + \lambda_\nu y_\nu \rangle$ в $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)} \rangle$ является $(k-1)$-мерным невырожденным $\mathcal{F}_\nu$-подпространством в $\widehat{\mathcal{M}}_\nu$. Далее, заметим, что все элементы $\lambda_\nu \in \mathcal{F}_\nu \setminus \{0\}$ и все элементы $\mathcal{A}_\nu^{(k)} \in \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)} \rangle^{\perp_0}$ порождают различные k-мерные невырожденные $\mathcal{F}_\nu$-подпространства $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} + \Theta_\nu + \lambda_\nu y_\nu \rangle$ в $\mathcal{G}_\nu$. Отсюда, рассуждая, как в предложении 1, получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$, имеющих тип $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} + \Theta_\nu + \lambda_\nu y_\nu \rangle$, где $\lambda_\nu \in \mathcal{F}_\nu \setminus \{0\}$ и $\mathcal{A}_\nu^{(h)} \in \widehat{\mathcal{M}}_\nu \setminus \{0\}$ для $1 \leqslant h \leqslant k-1$ и $\mathcal{A}_\nu^{(k)} \in \widehat{\mathcal{M}}_\nu$, равно

$$\mathfrak{U}_{\nu,k}^{(o)} = q^{\frac{(k+1)(\varepsilon_\nu t - k - 1)}{2}} (q-1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}.$$

Теперь подсчитаем количество различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$, имеющих тип $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$, где $k \geqslant 2$, $\mathcal{A}_\nu^{(h)} \in \widehat{\mathcal{M}}_\nu \setminus \{0\}$ для $1 \leqslant h \leqslant k-2$ и $\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} \in \widehat{\mathcal{M}}_\nu$. Для этого снова отдельно рассмотрим два случая: k нечетно и k четно.

Сперва пусть k нечетно. Если $\mathcal{A}_\nu^{(k-1)}=0$, то в силу [19, теорема 5.1.1] и [20, гл. 6, упражнение 21] получаем, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \Theta_\nu, \mathcal{A}_\nu^{(k)} + {} + y_\nu\rangle$ пространства $\mathcal{G}_\nu$ вырождено.

Если $\mathcal{A}_\nu^{(k-1)}\neq 0$, а $\mathcal{A}_\nu^{(k)}=0$, то в силу [19, теорема 5.1.1] и [20, гл. 6, упражнение 21] получаем, что подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu, y_\nu\rangle$ в $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}\rangle$ является $(k-1)$-мерным невырожденным $\mathcal{F}_\nu$-подпространством в $\widehat{\mathcal{M}}_\nu$. Тогда, рассуждая, как и в случае (i), получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$, имеющих тип $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu, y_\nu\rangle$, равно

$$\mathfrak{W}_{\nu,k}^{(o_1)} = q^{\frac{(k-1)(\varepsilon_\nu t-k-1)}{2}}(q^{k-1}-1)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\ (k-1)/2\end{bmatrix}_{q^2}.$$

Теперь пусть оба вектора $\mathcal{A}_\nu^{(k-1)}$ и $\mathcal{A}_\nu^{(k)}$ ненулевые. Тогда отдельно рассмотрим следующие два случая: $\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)}$ линейно зависимы или $\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)}$ линейно независимы над $\mathcal{F}_\nu$.

Сперва пусть $\mathcal{A}_\nu^{(k-1)}$ и $\mathcal{A}_\nu^{(k)}$ линейно зависимы над $\mathcal{F}_\nu$. Тогда $\mathcal{A}_\nu^{(k)}=\alpha_\nu\mathcal{A}_\nu^{(k-1)}$ для некоторого $\alpha_\nu\in\mathcal{F}_\nu\setminus\{0\}$. Нетрудно заметить, что $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu, \mathcal{A}_\nu^{(k)}+y_\nu\rangle = \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu, \lambda_\nu y_\nu+\Theta_\nu\rangle$, где $\lambda_\nu\in\mathcal{F}_\nu\setminus\{0\}$ и $\mathcal{A}_\nu^{(h)}\in\widehat{\mathcal{M}}_\nu\setminus\{0\}$ для $1\leqslant h\leqslant k-1$. Применяя [19, теорема 5.1.1] и [20, гл. 6, упражнение 21], получаем, что подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu, \lambda_\nu y_\nu+\Theta_\nu\rangle$ в $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда $(k-1)$-мерное $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-1)}\rangle$ пространства $\widehat{\mathcal{M}}_\nu$ невырождено. Снова рассуждая, как в случае (i), получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$, имеющих тип $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu, \mathcal{A}_\nu^{(k)}+y_\nu\rangle$, в случае, когда $\mathcal{A}_\nu^{(k-1)}$ и $\mathcal{A}_\nu^{(k)}$ линейно зависимы над $\mathcal{F}_\nu$, равно

$$\mathfrak{W}_{\nu,k}^{(o_2)} = q^{\frac{(k-1)(\varepsilon_\nu t-k-1)}{2}}(q^{k-1}-1)(q-1)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\ (k-1)/2\end{bmatrix}_{q^2}.$$

Теперь предположим, что $\mathcal{A}_\nu^{(k-1)}$ и $\mathcal{A}_\nu^{(k)}$ линейно независимы над $\mathcal{F}_\nu$. Тогда, снова применяя [19, теорема 5.1.1] и [20, гл. 6, упражнение 21], получаем, что подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu, \mathcal{A}_\nu^{(k)}+y_\nu\rangle$ в $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-1)}\rangle$ является $(k-1)$-мерным невырожденным $\mathcal{F}_\nu$-подпространством в $\widehat{\mathcal{M}}_\nu$. Далее, заметим, что каждое $(k-1)$-мерное невырожденное $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-1)}\rangle$ в $\widehat{\mathcal{M}}_\nu$ порождает ровно $(q^{k-1}-1)$ различных $(k-1)$-мерных невырожденных $\mathcal{F}_\nu$-подпространств $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu\rangle$ в $\mathcal{G}_\nu$. Кроме того, в силу [17, предложение 2.9] можно представить $\mathcal{A}_\nu^{(k)}\in\widehat{\mathcal{M}}_\nu$ в виде $\mathcal{A}_\nu^{(k)}=\sum\limits_{h=1}^{k-1}\alpha_\nu^{(h)}\mathcal{A}_\nu^{(h)}+\widetilde{\mathcal{W}}_\nu^{(k)}$, где $\alpha_\nu^{(h)}\in\mathcal{F}_\nu$ для $1\leqslant h\leqslant k-1$ и $\widetilde{\mathcal{W}}_\nu^{(k)}\in {}\in\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-1)}\rangle^{\perp_0}$. Теперь заметим, что $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu, \mathcal{A}_\nu^{(k)}+y_\nu\rangle = \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu, \alpha_\nu^{(k-1)}\mathcal{A}_\nu^{(k-1)}+\widetilde{\mathcal{W}}_\nu^{(k)}+y_\nu\rangle$. Нетрудно видеть, что все ненулевые элементы $\mathcal{A}_\nu^{(k)}=\alpha_\nu^{(k-1)}\mathcal{A}_\nu^{(k-1)}+\widetilde{\mathcal{W}}_\nu^{(k)}$ порождают различные k-мерные невырожденные $\mathcal{F}_\nu$-подпространства $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)}+\Theta_\nu, \mathcal{A}_\nu^{(k)}+y_\nu\rangle$ в $\mathcal{G}_\nu$. Отсюда, рассуждая, как в предложении 1, получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$, имеющих тип

$\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$, в случае, когда $\mathcal{A}_\nu^{(k-1)}$ и $\mathcal{A}_\nu^{(k)}$ линейно независимы над $\mathcal{F}_\nu$, равно

$$\mathfrak{W}_{\nu,k}^{(o_3)} = (q^{\varepsilon_\nu t-k} - q)(q^{k-1} - 1) q^{\frac{(k-1)(\varepsilon_\nu t-k-1)}{2}} \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}.$$

Объединяя рассмотренные выше случаи, получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$, имеющих тип $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$, где $\mathcal{A}_\nu^{(h)} \in \widehat{\mathcal{M}}_\nu \setminus \{0\}$ для $1 \leqslant h \leqslant k-2$ и $\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} \in \widehat{\mathcal{M}}_\nu$, равно

$$\mathfrak{W}_{\nu,k}^{(o)} = \mathfrak{W}_{\nu,k}^{(o_1)} + \mathfrak{W}_{\nu,k}^{(o_2)} + \mathfrak{W}_{\nu,k}^{(o_3)} = q^{\frac{k(\varepsilon_\nu t-k)+(\varepsilon_\nu t-2k+1)}{2}} (q^{k-1} - 1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}.$$

Пусть теперь k четно. Если $\mathcal{A}_\nu^{(k-1)} = \mathcal{A}_\nu^{(k)} = 0$, то в силу [19, теорема 5.1.1] и [20, гл. 6, упражнение 21] получаем, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \Theta_\nu, y_\nu \rangle$ в $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle$ является $(k-2)$-мерным невырожденным $\mathcal{F}_\nu$-подпространством в $\widehat{\mathcal{M}}_\nu$. Рассуждая, как и в предложении 1, получаем, что число таких подпространств равно

$$\mathfrak{W}_{\nu,k}^{(e_1)} = q^{\frac{(k-2)(\varepsilon_\nu t-k)}{2}} \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-2)/2 \end{bmatrix}_{q^2}.$$

Далее, если $\mathcal{A}_\nu^{(k-1)} = 0$, а $\mathcal{A}_\nu^{(k)} \neq 0$, то снова применяя [19, теорема 5.1.1] и [20, гл. 6, упражнение 21], получаем, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$ в $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда $(k-2)$-мерное $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle$ пространства $\widehat{\mathcal{M}}_\nu$ невырождено. Заметим также, что все элементы $\mathcal{A}_\nu^{(k)} \in \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0} \setminus \{0\}$ порождают различные k-мерные невырожденные $\mathcal{F}_\nu$-подпространства $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$ в $\mathcal{G}_\nu$ и что есть ровно $(q^{\varepsilon_\nu t-k} - 1)$ способов выбрать $\mathcal{A}_\nu^{(k)}$. Отсюда, рассуждая, как в предложении 1, получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств пространства $\mathcal{G}_\nu$, имеющих тип $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$, равно

$$\mathfrak{W}_{\nu,k}^{(e_2)} = q^{\frac{(k-2)(\varepsilon_\nu t-k)}{2}} (q^{\varepsilon_\nu t-k} - 1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-2)/2 \end{bmatrix}_{q^2}.$$

Далее, если $\mathcal{A}_\nu^{(k)} = 0$, а $\mathcal{A}_\nu^{(k-1)} \neq 0$, то рассуждая, как и выше, получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$, имеющих тип $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, y_\nu \rangle$, равно

$$\mathfrak{W}_{\nu,k}^{(e_3)} = q^{\frac{(k-2)(\varepsilon_\nu t-k)}{2}} (q^{\varepsilon_\nu t-k} - 1) \begin{bmatrix} (\varepsilon_\nu t - 2)/2 \\ (k-2)/2 \end{bmatrix}_{q^2}.$$

Наконец, пусть оба вектора $\mathcal{A}_\nu^{(k-1)}$ и $\mathcal{A}_\nu^{(k)}$ ненулевые. Тогда выделяются следующие случаи: $\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)}$ линейно зависимы или $\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)}$ линейно независимы над $\mathcal{F}_\nu$.

Сперва пусть $\mathcal{A}_\nu^{(k-1)}$ и $\mathcal{A}_\nu^{(k)}$ линейно зависимы над $\mathcal{F}_\nu$. Тогда $\mathcal{A}_\nu^{(k)} = \beta_\nu \mathcal{A}_\nu^{(k-1)}$ для некоторого $\beta_\nu \in \mathcal{F}_\nu \setminus \{0\}$. Нетрудно видеть, что $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle = \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \beta_\nu y_\nu + \Theta_\nu \rangle$, где $\beta_\nu \in \mathcal{F}_\nu \setminus \{0\}$ и $\mathcal{A}_\nu^{(h)} \in \widehat{\mathcal{M}}_\nu \setminus \{0\}$

для $1 \leqslant h \leqslant k-1$. В силу [19, теорема 5.1.1] и [20, гл. 6, упражнение 21] получаем, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \beta_\nu y_\nu + \Theta_\nu \rangle$ в $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle$ является $(k-2)$-мерным невырожденным $\mathcal{F}_\nu$-подпространством в $\widehat{\mathcal{M}}_\nu$. Далее, заметим, что все $\beta_\nu \in \mathcal{F}_\nu \setminus \{0\}$ и все $\mathcal{A}_\nu^{(k-1)} \in \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0}$ порождают различные k-мерные невырожденные $\mathcal{F}_\nu$-подпространства $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \beta_\nu y_\nu + \Theta_\nu \rangle$ в $\mathcal{G}_\nu$. Отсюда, рассуждая, как в предложении 1, получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$, имеющих тип $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$, в случае, когда $\mathcal{A}_\nu^{(k-1)}$ и $\mathcal{A}_\nu^{(k)}$ линейно зависимы над $\mathcal{F}_\nu$, равно

$$\mathfrak{W}_{\nu,k}^{(e_4)} = q^{\frac{(k-2)(\varepsilon_\nu t-k)}{2}}(q^{\varepsilon_\nu t-k}-1)(q-1)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\ (k-2)/2\end{bmatrix}_{q^2}.$$

Пусть теперь $\mathcal{A}_\nu^{(k-1)}$ и $\mathcal{A}_\nu^{(k)}$ линейно независимы над $\mathcal{F}_\nu$. Тогда, снова применяя [19, теорема 5.1.1] и [20, гл. 6, упражнение 21], получаем, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$ пространства $\mathcal{G}_\nu$ невырождено тогда и только тогда, когда либо

($\star$) k-мерное $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k)} \rangle$ пространства $\widehat{\mathcal{M}}_\nu$ вырождено, а $(k-2)$-мерное $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle$ пространства $\widehat{\mathcal{M}}_\nu$ невырождено, либо

($\diamond$) k-мерное $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k)} \rangle$ пространства $\widehat{\mathcal{M}}_\nu$ невырождено, а $(k-2)$-мерное $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle$ пространства $\widehat{\mathcal{M}}_\nu$ вырождено, либо

($\ddagger$) оба $\mathcal{F}_\nu$-подпространства $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k)} \rangle$ и $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle$ пространства $\widehat{\mathcal{M}}_\nu$ невырождены и $\det \mathfrak{G}(\mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k)}) \neq \det \mathfrak{G}(\mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)})$, где $\det \mathfrak{G}(\mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k)})$ и $\det \mathfrak{G}(\mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)})$ – определители матриц Грама $\mathcal{F}_\nu$-подпространств $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k)} \rangle$ и $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle$ в $\widehat{\mathcal{M}}_\nu$ относительно базисов $\{\mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k)}\}$ и $\{\mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}\}$ соответственно.

Вначале найдем число k-мерных $\mathcal{F}_\nu$-подпространств типа $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$ в $\mathcal{G}_\nu$, удовлетворяющих условию ($\star$). Для этого заметим, что $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle$ – невырожденное $\mathcal{F}_\nu$-подпространство в $\widehat{\mathcal{M}}_\nu$. Следовательно, в силу [17, предложение 2.9] имеем $\widehat{\mathcal{M}}_\nu = \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle \perp \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0}$, где $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0}$ – $(\varepsilon_\nu t - k)$-мерное невырожденное $\mathcal{F}_\nu$-подпространство в $\widehat{\mathcal{M}}_\nu$. Далее, все пары $(\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)})$ линейно независимых векторов в $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0}$ порождают различные k-мерные невырожденные $\mathcal{F}_\nu$-подпространства $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$ в $\mathcal{G}_\nu$. Нетрудно видеть, что $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k)} \rangle = \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle \perp \langle \mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)} \rangle$, откуда следует, что $\det \mathfrak{G}(\mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k)}) = \det \mathfrak{G}(\mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)}) \det \mathfrak{G}(\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)})$. Поэтому $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k)} \rangle$ в $\widehat{\mathcal{M}}_\nu$ вырождено тогда и только тогда, когда $\det \mathfrak{G}(\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)}) = 0$, что имеет место тогда и только тогда, когда $\mathcal{A}_\nu^{(k)} \in \in \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-1)} \rangle^{\perp_0}$. Кроме того, заметим, что $\mathcal{A}_\nu^{(k-1)} \in \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0} \setminus \{0\}$, поэтому его можно выбрать $(q^{\varepsilon_\nu t-k}-1)$ способами. Далее, заметим, что есть $(q^{\varepsilon_\nu t-k}-1)(q^{\varepsilon_\nu t-k-1}-q)$ способов выбрать пару $(\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)})$. Отсюда, рассуждая так же, как и в предложении 1, получаем, что число различных k-мерных

невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$ типа $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$, удовлетворяющих условию $(\star)$, равно

$$\mathfrak{W}_{\nu,k}^{(e_5)} = q^{\frac{(k-2)(\varepsilon_\nu t-k)}{2}}(q^{\varepsilon_\nu t-k}-1)(q^{\varepsilon_\nu t-k-1}-q)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\(k-2)/2\end{bmatrix}_{q^2}.$$

Теперь подсчитаем количество k-мерных $\mathcal{F}_\nu$-подпространств типа $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$ в $\mathcal{G}_\nu$, удовлетворяющих условию $(\diamond)$. Рассуждая, как в предложении 1, получаем, что число k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\widehat{\mathcal{M}}_\nu$ равно $q^{\frac{k(\varepsilon_\nu t-k-2)}{2}}\begin{bmatrix}(\varepsilon_\nu t-2)/2\\k/2\end{bmatrix}_{q^2}$. Отметим, что каждое k-мерное невырожденное $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k)} \rangle$ в $\widehat{\mathcal{M}}_\nu$ имеет ровно $q^{k-2}\begin{bmatrix}k/2\\(k-2)/2\end{bmatrix}_{q^2}$ различных $(k-2)$-мерных невырожденных $\mathcal{F}_\nu$-подпространств. Отсюда с учетом леммы 1 получаем, что в $\widehat{\mathcal{M}}_\nu$ есть ровно $\begin{bmatrix}k\\k-2\end{bmatrix}_q - q^{k-2}\begin{bmatrix}k/2\\(k-2)/2\end{bmatrix}_{q^2}$ различных $(k-2)$-мерных вырожденных $\mathcal{F}_\nu$-подпространств $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k)} \rangle$. Пусть $\langle \mathcal{B}_\nu^{(1)}, \mathcal{B}_\nu^{(2)}, \ldots, \mathcal{B}_\nu^{(k-2)} \rangle$ – фиксированное $(k-2)$-мерное вырожденное $\mathcal{F}_\nu$-подпространство в $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k)} \rangle$. Выберем два линейно независимых вектора $\mathcal{B}_\nu^{(k-1)}, \mathcal{B}_\nu^{(k)}$, принадлежащих $\mathcal{F}_\nu$-подпространству $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k)} \rangle$ пространства $\widehat{\mathcal{M}}_\nu$, таких что $\langle \mathcal{B}_\nu^{(1)}, \mathcal{B}_\nu^{(2)}, \ldots, \mathcal{B}_\nu^{(k)} \rangle = \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k)} \rangle$. Заметим, что пару $(\mathcal{B}_\nu^{(k-1)}, \mathcal{B}_\nu^{(k)})$ можно выбрать $(q^2-1)(q^2-q)$ различными способами. Отсюда, рассуждая так же, как и в предложении 1, получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств типа $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$ в $\mathcal{G}_\nu$, удовлетворяющих условию $(\diamond)$, равно

$$\mathfrak{W}_{\nu,k}^{(e_6)} = q^{\frac{k(\varepsilon_\nu t-k-2)}{2}}(q^2-1)(q^2-q)\times$$
$$\times\begin{bmatrix}(\varepsilon_\nu t-2)/2\\k/2\end{bmatrix}_{q^2}\left(\begin{bmatrix}k\\k-2\end{bmatrix}q - q^{k-2}\begin{bmatrix}k/2\\(k-2)/2\end{bmatrix}_{q^2}\right).$$

Наконец, подсчитаем число k-мерных $\mathcal{F}_\nu$-подпространств типа $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)}, \mathcal{A}_\nu^{(k-1)} + \Theta_\nu, \mathcal{A}_\nu^{(k)} + y_\nu \rangle$ в $\mathcal{G}_\nu$, удовлетворяющих условию $(\ddagger)$. Рассуждая, как и в предложении 1, получаем, что в $\widehat{\mathcal{M}}_\nu$ есть ровно $q^{\frac{(k-2)(\varepsilon_\nu t-k)}{2}}\begin{bmatrix}(\varepsilon_\nu t-2)/2\\(k-2)/2\end{bmatrix}_{q^2}$ различных $(k-2)$-мерных невырожденных $\mathcal{F}_\nu$-подпространств. Применяя [17, предложение 2.9], получаем $\widehat{\mathcal{M}}_\nu = \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)} \rangle \perp \langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0}$, где $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0}$ – $(\varepsilon_\nu t-k)$-мерное невырожденное $\mathcal{F}_\nu$-подпространство в $\widehat{\mathcal{M}}_\nu$. Отсюда получаем $\det \mathfrak{G}(\mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k)}) = \det \mathfrak{G}(\mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)}) \times$ $\times \det \mathfrak{G}(\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)})$, откуда в свою очередь следует, что $\mathcal{F}_\nu$-подпространство $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k)} \rangle$ в $\widehat{\mathcal{M}}_\nu$ невырождено тогда и только тогда, когда $\det \mathfrak{G}(\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)}) \neq$ $\neq 0$, т.е. тогда и только тогда, когда $\mathcal{A}_\nu^{(k)} \notin \langle \mathcal{A}_\nu^{(k-1)} \rangle^{\perp_0}$ и $(\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)})$ не является гиперболической парой в $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0}$. Таким образом, есть ровно $q^{\varepsilon_\nu t-k-1}(q-1)(q^{\varepsilon_\nu t-k}-1)$ различных способов выбрать пару $(\mathcal{A}_\nu^{(k-1)}, \mathcal{A}_\nu^{(k)})$ так, чтобы $\mathcal{F}_\nu$-подпространства $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)} \rangle$ и $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k)} \rangle$ в $\widehat{\mathcal{M}}_\nu$ были невырожденными. Далее, согласно [18, с. 69–70] получаем, что индекс Витта пространства $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0}$ равен $(\varepsilon_\nu t-k)/2$, а число гиперболических пар в $\langle \mathcal{A}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \ldots, \mathcal{A}_\nu^{(k-2)} \rangle^{\perp_0}$ равно $H_{\frac{\varepsilon_\nu t-k}{2},0} = q^{\varepsilon_\nu t-k-1}(q^{\varepsilon_\nu t-k}-1)$. Итак, есть ровно

$q^{\varepsilon_\nu t-k-1}(q-1)(q^{\varepsilon_\nu t-k}-1)-q^{\varepsilon_\nu t-k-1}(q^{\varepsilon_\nu t-k}-1)=q^{\varepsilon_\nu t-k-1}(q-2)(q^{\varepsilon_\nu t-k}-1)$ способов выбрать пару $(\mathcal{A}_\nu^{(k-1)},\mathcal{A}_\nu^{(k)})$. Отсюда получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств типа $\langle\mathcal{A}_\nu^{(1)},\mathcal{A}_\nu^{(2)},\dots,\mathcal{A}_\nu^{(k-2)},\mathcal{A}_\nu^{(k-1)}+\Theta_\nu,\mathcal{A}_\nu^{(k)}+y_\nu\rangle$ в $\mathcal{G}_\nu$, удовлетворяющих условию ($\ddagger$), равно

$$\mathfrak{W}_{\nu,k}^{(e_7)}=q^{\frac{(k-2)(\varepsilon_\nu t-k)}{2}}q^{\varepsilon_\nu t-k-1}(q-2)(q^{\varepsilon_\nu t-k}-1)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\(k-2)/2\end{bmatrix}_{q^2}.$$

Объединяя эти случаи, получаем, что число различных k-мерных невырожденных $\mathcal{F}_\nu$-подпространств типа $\langle\mathcal{A}_\nu^{(1)},\mathcal{A}_\nu^{(2)},\dots,\mathcal{A}_\nu^{(k-2)},\mathcal{A}_\nu^{(k-1)}+\Theta_\nu,\mathcal{A}_\nu^{(k)}+y_\nu\rangle$ в $\mathcal{G}_\nu$ в случае, когда $\mathcal{A}_\nu^{(h)}\in\widehat{\mathcal{M}}_\nu\setminus\{0\}$ для $1\leqslant h\leqslant k-2$ и $\mathcal{A}_\nu^{(k-1)},\mathcal{A}_\nu^{(k)}\in\widehat{\mathcal{M}}_\nu$, равно

$$\begin{aligned}&\mathfrak{W}_{\nu,k}^{(e)}=\mathfrak{W}_{\nu,k}^{(e_1)}+\mathfrak{W}_{\nu,k}^{(e_2)}+\mathfrak{W}_{\nu,k}^{(e_3)}+\mathfrak{W}_{\nu,k}^{(e_4)}+\mathfrak{W}_{\nu,k}^{(e_5)}+\mathfrak{W}_{\nu,k}^{(e_6)}+\mathfrak{W}_{\nu,k}^{(e_7)}=\\&=q^{\frac{k\varepsilon_\nu t-k^2-2}{2}}(q^{\varepsilon_\nu t-k+1}-q^{\varepsilon_\nu t-k}+1)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\(k-2)/2\end{bmatrix}_{q^2}+\\&+q^{\frac{k(\varepsilon_\nu t-k-2)}{2}}(q^{k+1}-q)(q^{k-2}-1)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\k/2\end{bmatrix}_{q^2}.\end{aligned}$$

Объединяя все рассмотренные случаи, получаем

$$\mathcal{N}_{\nu,k}=\mathfrak{T}_{\nu,k}^{(o)}+\mathfrak{U}_{\nu,k}^{(o)}+\mathfrak{W}_{\nu,k}^{(o)}=q^{\frac{(k+1)\varepsilon_\nu t-(k^2+1)}{2}}\begin{bmatrix}(\varepsilon_\nu t-2)/2\\(k-1)/2\end{bmatrix}_{q^2},\quad\text{если } k \text{ нечетно,}$$

и

$$\begin{aligned}&\mathcal{N}_{\nu,k}=\mathfrak{R}_{\nu,k}^{(e)}+\mathfrak{S}_{\nu,k}^{(e)}+\mathfrak{T}_{\nu,k}^{(e)}+\mathfrak{U}_{\nu,k}^{(e)}+\mathfrak{W}_{\nu,k}^{(e)}=q^{\frac{k\varepsilon_\nu t-k^2-2}{2}}\Bigg((q^k+q-1)\times\\&\times\begin{bmatrix}(\varepsilon_\nu t-2)/2\\k/2\end{bmatrix}_{q^2}+(q^{\varepsilon_\nu t-k+1}-q^{\varepsilon_\nu t-k}+1)\begin{bmatrix}(\varepsilon_\nu t-2)/2\\(k-2)/2\end{bmatrix}_{q^2}\Bigg),\quad\text{если } k \text{ четно.}\end{aligned}$$

Наконец, подставляя найденные значения $\mathcal{N}_{\nu,k}$ в уравнение (2) в соответствующих случаях, получаем требуемый результат. ▲

4.2. Определение числа $\mathfrak{D}_\nu$ для $\nu\in\mathcal{J}_2$. В следующем предложении определяется число $\mathfrak{D}_\nu$ в случае, когда $\nu\in\mathcal{J}_2$ и $\delta\in\{0,*,\gamma\}$.

Предложение 4. *Пусть $\nu\in\mathcal{J}_2$ фиксировано. Для $\delta\in\{0,*,\gamma\}$ имеем*

$$\mathfrak{D}_\nu=2+\sum_{k=1}^{\varepsilon_\nu t-1}q^{\frac{k(\varepsilon_\nu t-k)d_\nu}{2}}\prod_{a=0}^{k-1}\left(\frac{q^{\frac{(\varepsilon_\nu t-a)d_\nu}{2}}-(-1)^{\varepsilon_\nu t-a}}{q^{\frac{(k-a)d_\nu}{2}}-(-1)^{k-a}}\right).$$

Доказательство. Чтобы вычислить $\mathfrak{D}_\nu$, в силу (2) достаточно найти числа $\mathcal{N}_{\nu,k}$ для $1\leqslant k\leqslant\varepsilon_\nu t-1$. Для этого рассмотрим следующие два случая: I. $\delta\in\{0,*\}$ и II. $\delta=\gamma$.

I. Пусть $\delta\in\{0,*\}$. Тогда в силу утверждений (a), (c) леммы 2 $(\mathcal{G}_\nu,[\cdot,\cdot]_\delta\restriction_{\mathcal{G}_\nu\times\mathcal{G}_\nu})$ является унитарным пространством над $\mathcal{F}_\nu$. Тогда всякое k-мерное невырожденное $\mathcal{F}_\nu$-подпространство пространства $\mathcal{G}_\nu$ также является унитарным пространством. Рассмотрим отдельно следующие случаи: (i) k нечетно и (ii) k четно.

(i) Вначале пусть k нечетно. Тогда k-мерное $\mathcal{F}_\nu$-подпространство W в $\mathcal{G}_\nu$ имеет разложение Витта $W=\langle\mathcal{A}_\nu^{(1)},\mathcal{B}_\nu^{(1)}\rangle\perp\langle\mathcal{A}_\nu^{(2)},\mathcal{B}_\nu^{(2)}\rangle\perp\ldots\perp\langle\mathcal{A}_\nu^{(\frac{k-1}{2})},\mathcal{B}_\nu^{(\frac{k-1}{2})}\rangle\perp\langle Z_\nu\rangle$, где

$(\mathcal{A}_\nu^{(h)}, \mathcal{B}_\nu^{(h)})$ – гиперболическая пара в $\mathcal{G}_\nu$ для $1 \leqslant h \leqslant \dfrac{k-1}{2}$, а Z_ν – анизотропный вектор в $\mathcal{G}_\nu$; множество $\{\mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(\frac{k-1}{2})}, \mathcal{B}_\nu^{(\frac{k-1}{2})}, Z_\nu\}$ называется базисом Витта пространства W над $\mathcal{F}_\nu$ (см. [18, с. 116]). Через ϑ_h обозначим индекс Витта пространства $\langle \mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(h-1)}, \mathcal{B}_\nu^{(h-1)} \rangle^{\perp_\delta} \subseteq \mathcal{G}_\nu$ для $1 \leqslant h \leqslant \dfrac{k+1}{2}$. Применяя [17, предложение 2.9] и теорему Витта о сокращении, получаем, что число базисов Витта типа $\{\mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)}, \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)}, \dots, \mathcal{A}_\nu^{(\frac{k-1}{2})}, \mathcal{B}_\nu^{(\frac{k-1}{2})}, Z_\nu\}$ в $\mathcal{G}_\nu$ равно

$$U_{k,\varepsilon_\nu t} = H_{\vartheta_1, \varepsilon_\nu t - 2\vartheta_1} H_{\vartheta_2, \varepsilon_\nu t - 2 - 2\vartheta_2} \dots H_{\vartheta_{\frac{k-1}{2}}, \varepsilon_\nu t - k + 3 - 2\vartheta_{\frac{k-1}{2}}} \times$$
$$\times \left(q^{(\varepsilon_\nu t - k + 1)d_\nu} - 1 - I_{\vartheta_{\frac{k+1}{2}}, \varepsilon_\nu t - k + 1 - 2\vartheta_{\frac{k+1}{2}}} \right).$$

Аналогичными рассуждениями получаем, что число базисов Витта k-мерного унитарного $\mathcal{F}_\nu$-подпространства в $\mathcal{G}_\nu$ равно

$$U_k = H_{\frac{k-1}{2}, 1} H_{\frac{k-3}{2}, 1} \dots H_{1,1}(q^{d_\nu} - 1).$$

Применяя теперь [18, лемма 10.4 и следствие 10.6], получаем

$$\mathcal{N}_{\nu,k} = \frac{U_{k,\varepsilon_\nu t}}{U_k} = q^{\frac{k(\varepsilon_\nu t - k)d_\nu}{2}} \prod_{a=0}^{k-1} \left(\frac{q^{\frac{(\varepsilon_\nu t - a)d_\nu}{2}} - (-1)^{\varepsilon_\nu t - a}}{q^{\frac{(k-a)d_\nu}{2}} - (-1)^{k-a}} \right), \quad 1 \leqslant k \leqslant \varepsilon_\nu t - 1.$$

(ii) Пусть теперь k четно. Тогда получаем, что k-мерное $\mathcal{F}_\nu$-подпространство W в $\mathcal{G}_\nu$ имеет разложение Витта $W = \langle \mathcal{A}_\nu^{(1)}, \mathcal{B}_\nu^{(1)} \rangle \perp \langle \mathcal{A}_\nu^{(2)}, \mathcal{B}_\nu^{(2)} \rangle \perp \dots \perp \langle \mathcal{A}_\nu^{(\frac{k}{2})}, \mathcal{B}_\nu^{(\frac{k}{2})} \rangle$, где $(\mathcal{A}_\nu^{(h)}, \mathcal{B}_\nu^{(h)})$ – гиперболическая пара в $\mathcal{G}_\nu$ для $1 \leqslant h \leqslant \dfrac{k}{2}$. Рассуждая так же, как в случае (i), и снова применяя [18, лемма 10.4 и следствие 10.6], получаем

$$\mathcal{N}_{\nu,k} = q^{\frac{k(\varepsilon_\nu t - k)d_\nu}{2}} \prod_{a=0}^{k-1} \left(\frac{q^{\frac{(\varepsilon_\nu t - a)d_\nu}{2}} - (-1)^{\varepsilon_\nu t - a}}{q^{\frac{(k-a)d_\nu}{2}} - (-1)^{k-a}} \right), \quad 1 \leqslant k \leqslant \varepsilon_\nu t - 1.$$

II. Пусть $\delta = \gamma$. В этом случае согласно утверждениям (a) и (c) леммы 2 получаем, что $[\cdot\,,\cdot]_\gamma \restriction_{\mathcal{G}_\nu \times \mathcal{G}_\nu}$ является рефлексивной невырожденной антиэрмитовой $\tau_{1,-1}$-полуторалинейной формой. Вначале приведем антиэрмитову форму $[\cdot\,,\cdot]_\gamma \restriction_{\mathcal{G}_\nu \times \mathcal{G}_\nu}$ к сохраняющей ортогональность эрмитовой $\tau_{1,-1}$-полуторалинейной форме $[\cdot\,,\cdot]_{\gamma^{(H)}} \restriction_{\mathcal{G}_\nu \times \mathcal{G}_\nu}$. Для этого, применяя [16, лемма 3.1(b)], заметим, что $\tau_{1,-1}$ – автоморфизм $\mathcal{F}_\nu$ порядка два. Поэтому существует элемент $\xi_\nu \in \mathcal{F}_\nu$, такой что $\tau_{1,-1}(\xi_\nu) \neq \xi_\nu$. Теперь возьмем $\zeta_\nu = \xi_\nu - \tau_{1,-1}(\xi_\nu) (\neq 0) \in \mathcal{F}_\nu$. Отметим, что $\tau_{1,-1}(\zeta_\nu) = -\zeta_\nu$. Теперь определим отображение $[\cdot\,,\cdot]_{\gamma^{(H)}} \colon \mathcal{G}_\nu \times \mathcal{G}_\nu \to \mathcal{F}_\nu$ как $[\mathcal{A}_\nu, \mathcal{B}_\nu]_{\gamma^{(H)}} = \zeta_\nu [\mathcal{A}_\nu, \mathcal{B}_\nu]_\gamma$ для всех $\mathcal{A}_\nu, \mathcal{B}_\nu \in \mathcal{G}_\nu$. Заметим, что отображение $[\cdot\,,\cdot]_{\gamma^{(H)}}$ является невырожденной эрмитовой $\tau_{1,-1}$-полуторалинейной формой на $\mathcal{G}_\nu$, так что $(\mathcal{G}_\nu, [\cdot\,,\cdot]_{\gamma^{(H)}} \restriction_{\mathcal{G}_\nu \times \mathcal{G}_\nu})$ – унитарное пространство размерности $\varepsilon_\nu t$ над $\mathcal{F}_\nu \simeq \mathbb{F}_{q^{d_\nu}}$. Поскольку $\zeta_\nu \in \mathcal{F}_\nu \setminus \{0\}$, получаем, что число k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$ относительно $[\cdot\,,\cdot]_\gamma$ равно числу k-мерных невырожденных $\mathcal{F}_\nu$-подпространств в $\mathcal{G}_\nu$ относительно $[\cdot\,,\cdot]_{\gamma^{(H)}}$. Рассуждая далее, как в случае I, получаем

$$\mathcal{N}_{\nu,k} = q^{\frac{k(\varepsilon_\nu t - k)d_\nu}{2}} \prod_{a=0}^{k-1} \left(\frac{q^{\frac{(\varepsilon_\nu t - a)d_\nu}{2}} - (-1)^{\varepsilon_\nu t - a}}{q^{\frac{(k-a)d_\nu}{2}} - (-1)^{k-a}} \right), \quad 1 \leqslant k \leqslant \varepsilon_\nu t - 1.$$

От сюда с учетом (2) немедленно вытекает требуемый результат. ▲

4.3. Определение числа $\mathfrak{D}_w$ для $e_1+1 \leqslant w \leqslant e_2$. В этом пункте определим число $\mathfrak{D}_w$ различных пар $(\mathcal{C}_w, \mathcal{C}_w^\dagger)$, где $\mathcal{C}_w$ – $\mathcal{F}_w$-подпространство в $\mathcal{G}_w$, а $\mathcal{C}_w^\dagger$ – $\mathcal{F}_w^\dagger$-подпространство в $\mathcal{G}_w^\dagger$, такие что $\mathcal{C}_w \cap \mathcal{C}_w^{\dagger\perp_\delta} = \{0\}$ и $\mathcal{C}_w^\dagger \cap \mathcal{C}_w^{\perp_\delta} = \{0\}$ для $e_1+1 \leqslant w \leqslant e_2$, где $\delta \in \{0, *, \gamma\}$. С этой целью зафиксируем $e_1+1 \leqslant w \leqslant e_2$. Напомним, что $\mathcal{I}_w = \{i : 1 \leqslant i \leqslant \ell,\ \varepsilon_{w,i} = \varepsilon_{w,i}^\dagger\}$ и $\mathcal{I}'_w = \{i : 1 \leqslant i \leqslant \ell,\ \varepsilon_{w,i} \neq \varepsilon_{w,i}^\dagger\}$, а также что $\{1, 2, \ldots, \ell\} = \mathcal{I}_w \cup \mathcal{I}'_w$ (несвязное объединение). Кроме того, напомним, что $\eta_w = \sum\limits_{i \in \mathcal{I}_w} \varepsilon_{w,i}$, $\varrho_w = \sum\limits_{i \in \mathcal{I}'_w} \varepsilon_{w,i}$ и $\tau_w = \sum\limits_{i \in \mathcal{I}'_w} \varepsilon_{w,i}^\dagger$.

Без ограничения общности можно считать, что существует целое h, удовлетворяющее $1 \leqslant h \leqslant \ell$, такое что $\varepsilon_{w,i} = \varepsilon_{w,i}^\dagger$ для $1 \leqslant i \leqslant h$ и $\varepsilon_{w,i} \neq \varepsilon_{w,i}^\dagger$ для $h+1 \leqslant i \leqslant \ell$, т.е. $\mathcal{I}_w = \{1, 2, \ldots, h\}$ и $\mathcal{I}'_w = \{h+1, h+2, \ldots, \ell\}$. Тогда $\eta_w = \sum\limits_{i=1}^{h} \varepsilon_{w,i}$, $\varrho_w = \sum\limits_{i=h+1}^{\ell} \varepsilon_{w,i}$ и $\tau_w = \sum\limits_{i=h+1}^{\ell} \varepsilon_{w,i}^\dagger$. Поэтому можно записать $\mathcal{G}_w = \mathcal{K}_w \oplus \mathcal{K}'_w$ и $\mathcal{G}_w^\dagger = \mathcal{K}_w^\dagger \oplus \mathcal{K}_w^{\dagger\prime}$, где

$$\mathcal{K}_w = \bigoplus_{j=0}^{a_w-1} \Big(\underbrace{\varepsilon_{w,1}\mathcal{F}_{w,j}, \varepsilon_{w,2}\mathcal{F}_{w,j}, \ldots, \varepsilon_{w,h}\mathcal{F}_{w,j}, 0, \ldots, 0}_{\mathcal{K}_{w,j}} \Big),$$

$$\mathcal{K}'_w = \bigoplus_{j=0}^{a_w-1} \Big(\underbrace{0, \ldots, 0, \varepsilon_{w,h+1}\mathcal{F}_{w,j}, \varepsilon_{w,h+2}\mathcal{F}_{w,j}, \ldots, \varepsilon_{w,\ell}\mathcal{F}_{w,j}}_{\mathcal{K}'_{w,j}} \Big),$$

$$\mathcal{K}_w^\dagger = \bigoplus_{j=0}^{a_w-1} \Big(\underbrace{\varepsilon_{w,1}\mathcal{F}_{w,j}^\dagger, \varepsilon_{w,2}\mathcal{F}_{w,j}^\dagger, \ldots, \varepsilon_{w,h}\mathcal{F}_{w,j}^\dagger, 0, \ldots, 0}_{\mathcal{K}_{w,j}^\dagger} \Big),$$

$$\mathcal{K}_w^{\dagger\prime} = \bigoplus_{j=0}^{a_w-1} \Big(\underbrace{0, \ldots, 0, \varepsilon_{w,h+1}^\dagger\mathcal{F}_{w,j}^\dagger, \varepsilon_{w,h+2}^\dagger\mathcal{F}_{w,j}^\dagger, \ldots, \varepsilon_{w,\ell}^\dagger\mathcal{F}_{w,j}^\dagger}_{\mathcal{K}_{w,j}^{\dagger\prime}} \Big).$$

Тогда каждое $\mathcal{F}_w$-подпространство $\mathcal{C}_w$ в $\mathcal{G}_w$ и каждое $\mathcal{F}_w^\dagger$-подпространство $\mathcal{C}_w^\dagger$ в $\mathcal{G}_w^\dagger$ можно единственным образом представить в виде $\mathcal{C}_w = \mathcal{D}_w \oplus \mathcal{D}'_w$ и $\mathcal{C}_w^\dagger = \mathcal{D}_w^\dagger \oplus \mathcal{D}_w^{\dagger\prime}$, где $\mathcal{D}_w$ и $\mathcal{D}'_w$ (соответственно, $\mathcal{D}_w^\dagger$ и $\mathcal{D}_w^{\dagger\prime}$) – подпространства пространств $\mathcal{K}_w$ и $\mathcal{K}'_w$ (соответственно, $\mathcal{K}_w^\dagger$ и $\mathcal{K}_w^{\dagger\prime}$) над $\mathcal{F}_w$ (соответственно, над $\mathcal{F}_w^\dagger$) соответственно. Теперь заметим, что $\mathcal{K}_w$ (соответственно, $\mathcal{K}_w^\dagger$) – $(\eta_w t)$-мерное векторное пространство над $\mathcal{F}_w$ (соответственно, над $\mathcal{F}_w^\dagger$). Кроме того, заметим, что $\mathcal{K}'_w$ и $\mathcal{K}_w^{\dagger\prime}$ – $(\varrho_w t)$-мерное и $(\tau_w t)$-мерное пространства над $\mathcal{F}_w$ и $\mathcal{F}_w^\dagger$ соответственно.

Всюду далее в этом пункте элементы прямой суммы $\mathcal{K}_w \oplus \mathcal{K}_w^\dagger$ будем представлять в виде $\mathcal{A}_w + \mathcal{A}_w^\dagger$, где $\mathcal{A}_w \in \mathcal{K}_w$, а $\mathcal{A}_w^\dagger \in \mathcal{K}_w^\dagger$. Аналогично будем представлять элементы прямой суммы $\mathcal{F}_w \oplus \mathcal{F}_w^\dagger$ в виде $\alpha_w + \alpha_w^\dagger$, где $\alpha_w \in \mathcal{F}_w$, а $\alpha_w^\dagger \in \mathcal{F}_w^\dagger$. При этом множество $\mathcal{K}_w \oplus \mathcal{K}_w^\dagger$ будем рассматривать как $\big(\mathcal{F}_w \oplus \mathcal{F}_w^\dagger\big)$-модуль относительно следующих операций:

$$(\mathcal{A}_w + \mathcal{A}_w^\dagger) + (\mathcal{B}_w + \mathcal{B}_w^\dagger) = (\mathcal{A}_w + \mathcal{B}_w) + (\mathcal{A}_w^\dagger + \mathcal{B}_w^\dagger) \qquad \text{(сложение)} \quad (6)$$

$$(\alpha_w + \alpha_w^\dagger)(\mathcal{A}_w + \mathcal{A}_w^\dagger) = \alpha_w\mathcal{A}_w + \alpha_w^\dagger\mathcal{A}_w^\dagger \qquad \text{(умножение на скаляры)} \quad (7)$$

для любых $\mathcal{A}_w + \mathcal{A}_w^\dagger,\ \mathcal{B}_w + \mathcal{B}_w^\dagger \in \mathcal{K}_w \oplus \mathcal{K}_w^\dagger$ и $\alpha_w + \alpha_w^\dagger \in \mathcal{F}_w \oplus \mathcal{F}_w^\dagger$. Далее, для $\delta \in \{0, *, \gamma\}$ заметим, что $[\mathcal{A}_w + \mathcal{A}_w^\dagger, \mathcal{B}_w + \mathcal{B}_w^\dagger]_\delta = [\mathcal{A}_w, \mathcal{B}_w^\dagger]_\delta + [\mathcal{A}_w^\dagger, \mathcal{B}_w]_\delta \in \mathcal{F}_w \oplus \mathcal{F}_w^\dagger$ для любых $\mathcal{A}_w + \mathcal{A}_w^\dagger, \mathcal{B}_w + \mathcal{B}_w^\dagger \in \mathcal{K}_w \oplus \mathcal{K}_w^\dagger$. Теперь для $\delta \in \{0, *, \gamma\}$ обозначим через $[\cdot\,,\cdot]_\delta \restriction_{(\mathcal{K}_w \oplus \mathcal{K}_w^\dagger) \times (\mathcal{K}_w \oplus \mathcal{K}_w^\dagger)}$ ограничение полуторалинейной формы $[\cdot\,,\cdot]_\delta$ на $\big(\mathcal{K}_w \oplus \mathcal{K}_w^\dagger\big) \times \times \big(\mathcal{K}_w \oplus \mathcal{K}_w^\dagger\big)$. Тогда имеет место следующая

Лемма 3. *Пусть $e_1+1\leqslant w\leqslant e_2$ фиксировано. Для $\delta\in\{0,*,\gamma\}$ справедливы следующие утверждения*:

(a) $\mathcal{K}_w\oplus\mathcal{K}_w^\dagger$ *является свободным* $\big(\mathcal{F}_w\oplus\mathcal{F}_w^\dagger\big)$*-модулем ранга* $\eta_w t$;

(b) *Форма* $[\cdot\,,\cdot]_\delta\restriction_{(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)\times(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)}$ *рефлексивна и невырождена*;

(c) *Форма* $[\cdot\,,\cdot]_\delta\restriction_{(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)\times(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)}$ *эрмитова при* $\delta\in\{0,*\}$ *и антиэрмитова при* $\delta=\gamma$.

Если $\mathcal{L}_w$ – $\mathcal{F}_w$-подпространство в $\mathcal{K}_w$, а $\mathcal{L}_w^\dagger$ – $\mathcal{F}_w^\dagger$-подпространство в $\mathcal{K}_w^\dagger$, то их прямая сумма $\mathcal{L}_w\oplus\mathcal{L}_w^\dagger$ является $\big(\mathcal{F}_w\oplus\mathcal{F}_w^\dagger\big)$-подмодулем модуля $\mathcal{K}_w\oplus\mathcal{K}_w^\dagger$ относительно операций (6), (7). Для $\delta\in\{0,*,\gamma\}$ ортогональное дополнение к $\mathcal{L}_w\oplus\mathcal{L}_w^\dagger$ относительно формы $[\cdot\,,\cdot]_\delta\restriction_{(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)\times(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)}$ определяется как

$$\big(\mathcal{L}_w\oplus\mathcal{L}_w^\dagger\big)^{\perp_\delta}=\big\{\mathcal{A}_w+\mathcal{A}_w^\dagger\in\mathcal{K}_w\oplus\mathcal{K}_w^\dagger:\,[\mathcal{A}_w+\mathcal{A}_w^\dagger,\mathcal{B}_w+\mathcal{B}_w^\dagger]_\delta=0$$
$$\text{для всех }\mathcal{B}_w+\mathcal{B}_w^\dagger\in\mathcal{L}_w\oplus\mathcal{L}_w^\dagger\big\}.$$

Легко видеть, что $\big(\mathcal{L}_w\oplus\mathcal{L}_w^\dagger\big)^{\perp_\delta}$ является $\big(\mathcal{F}_w\oplus\mathcal{F}_w^\dagger\big)$-подмодулем $\mathcal{K}_w\oplus\mathcal{K}_w^\dagger$ и что $\big(\mathcal{L}_w\oplus\mathcal{L}_w^\dagger\big)^{\perp_\delta}=\mathcal{L}_w^{\dagger\perp_\delta}\oplus\mathcal{L}_w^{\perp_\delta}$. Для $\delta\in\{0,*,\gamma\}$ говорят, что $\big(\mathcal{F}_w\oplus\mathcal{F}_w^\dagger\big)$-подмодуль $\mathcal{L}_w\oplus\mathcal{L}_w^\dagger$ модуля $\mathcal{K}_w\oplus\mathcal{K}_w^\dagger$ невырожден, если он удовлетворяет условию $\big(\mathcal{L}_w\oplus\mathcal{L}_w^\dagger\big)\cap\big(\mathcal{L}_w\oplus\mathcal{L}_w^\dagger\big)^{\perp_\delta}=\{0\}$, т.е. $\big(\mathcal{L}_w\oplus\mathcal{L}_w^\dagger\big)\cap\big(\mathcal{L}_w^{\dagger\perp_\delta}\oplus\mathcal{L}_w^{\perp_\delta}\big)=\{0\}$.

Из леммы 3(c) получаем, что $[\cdot\,,\cdot]_\gamma\restriction_{(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)\times(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)}$ является антиэрмитовой формой. Вначале приведем ее к эрмитовой форме $[\cdot\,,\cdot]_{\gamma^{(H)}}\restriction_{(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)\times(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)}$. С этой целью заметим для $e_1+1\leqslant w\leqslant e_2$, что $\tau_{1,-1}$ является автоморфизмом $\mathcal{F}_w$ порядка два, так что существует элемент $\varkappa_w(\neq 0)\in\mathcal{F}_w$, такой что $\varkappa_w\neq\tau_{1,-1}(\varkappa_w)$. Тогда $\zeta_w=\varkappa_w-\tau_{1,-1}(\varkappa_w)(\neq 0)\in\mathcal{F}_w\oplus\mathcal{F}_w^\dagger$ удовлетворяет соотношению $\tau_{1,-1}(\zeta_w)=-\zeta_w$. Теперь определим отображение $[\cdot\,,\cdot]_{\gamma^{(H)}}\colon\big(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger\big)\times\big(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger\big)\to\mathcal{F}_w\oplus\mathcal{F}_w^\dagger$ как $[\mathcal{A}_w+\mathcal{A}_w^\dagger,\mathcal{B}_w+\mathcal{B}_w^\dagger]_{\gamma^{(H)}}=\zeta_w[\mathcal{A}_w+\mathcal{A}_w^\dagger,\mathcal{B}_w+\mathcal{B}_w^\dagger]_\gamma$ для всех $\mathcal{A}_w+\mathcal{A}_w^\dagger,\mathcal{B}_w+\mathcal{B}_w^\dagger\in\mathcal{K}_w\oplus\mathcal{K}_w^\dagger$. Легко видеть, что отображение $[\cdot\,,\cdot]_{\gamma^{(H)}}$ является невырожденной эрмитовой формой на $\big(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger\big)\times\big(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger\big)$. Далее, заметим, что $\big(\mathcal{F}_w\oplus\mathcal{F}_w^\dagger\big)$-подмодуль модуля $\mathcal{K}_w\oplus\mathcal{K}_w^\dagger$ невырожден относительно формы $[\cdot\,,\cdot]_{\gamma^{(H)}}\restriction_{(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)\times(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)}$ тогда и только тогда, когда он невырожден относительно формы $[\cdot\,,\cdot]_\gamma\restriction_{(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)\times(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)}$. Поэтому всюду далее вместо антиэрмитовой невырожденной формы $[\cdot\,,\cdot]_\gamma\restriction_{(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)\times(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)}$ будем рассматривать эрмитову невырожденную форму $[\cdot\,,\cdot]_{\gamma^{(H)}}\restriction_{(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)\times(\mathcal{K}_w\oplus\mathcal{K}_w^\dagger)}$.

В следующем предложении определяется число $\mathfrak{D}_w$ в случае, когда $e_1+1\leqslant w\leqslant e_2$, а $\delta\in\{0,*,\gamma^{(H)}\}$, и тем самым, $\delta\in\{0,*,\gamma\}$.

Предложение 5. *Пусть $e_1+1\leqslant w\leqslant e_2$ фиксировано. Для $\delta\in\{0,*,\gamma^{(H)}\}$ имеем*

$$\mathfrak{D}_w=\sum_{k=0}^{\eta_w t}\sum_{k_1=0}^{\varrho_w t}\sum_{k_2=0}^{\tau_w t}q^{kd_w(\eta_w t-k)}\begin{bmatrix}\eta_w t\\ k\end{bmatrix}_{q^{d_w}}\begin{bmatrix}\varrho_w t\\ k_1\end{bmatrix}_{q^{d_w}}\begin{bmatrix}\tau_w t\\ k_2\end{bmatrix}_{q^{d_w}}.$$

Доказательство. Заметим, что согласно теореме 3 число $\mathfrak{D}_w$ равно числу различных пар $(\mathcal{C}_w,\mathcal{C}_w^\dagger)$, где $\mathcal{C}_w$ – $\mathcal{F}_w$-подпространство в $\mathcal{G}_w$, а $\mathcal{C}_w^\dagger$ – $\mathcal{F}_w^\dagger$-подпространство в $\mathcal{G}_w^\dagger$, такие что $\mathcal{C}_w\cap\mathcal{C}_w^{\dagger\perp_\delta}=\{0\}$ и $\mathcal{C}_w^\dagger\cap\mathcal{C}_w^{\perp_\delta}=\{0\}$. Далее, заметим, что каждое $\mathcal{F}_w$-подпространство $\mathcal{C}_w$ в $\mathcal{G}_w$ и каждое $\mathcal{F}_w^\dagger$-подпространство $\mathcal{C}_w^\dagger$ в $\mathcal{G}_w^\dagger$ можно единственным образом представить в виде $\mathcal{C}_w=\mathcal{D}_w\oplus\mathcal{D}'_w$ и $\mathcal{C}_w^\dagger=\mathcal{D}_w^\dagger\oplus\mathcal{D}_w^{\dagger\prime}$, где $\mathcal{D}_w$ и $\mathcal{D}'_w$ (соответственно, $\mathcal{D}_w^\dagger$ и $\mathcal{D}_w^{\dagger\prime}$) – подпространства пространств $\mathcal{K}_w$ и $\mathcal{K}'_w$ (соответственно, $\mathcal{K}_w^\dagger$ и $\mathcal{K}_w^{\dagger\prime}$) над $\mathcal{F}_w$ (соответственно, над $\mathcal{F}_w^\dagger$) соответственно. Теперь для каждой пары $(\mathcal{D}'_w,\mathcal{D}_w^{\dagger\prime})$ заметим, что $\big(\mathcal{C}_w\oplus\mathcal{C}_w^\dagger\big)\cap\big(\mathcal{C}_w^{\dagger\perp_\delta}\oplus\mathcal{C}_w^{\perp_\delta}\big)=\{0\}$ тогда и только тогда, когда $\big(\mathcal{D}_w\oplus\mathcal{D}_w^\dagger\big)\cap\big(\mathcal{D}_w^{\dagger\perp_\delta}\oplus\mathcal{D}_w^{\perp_\delta}\big)=\{0\}$. Кроме того, заметим, что $\big(\mathcal{D}_w\oplus\mathcal{D}_w^\dagger\big)\cap\big(\mathcal{D}_w^{\dagger\perp_\delta}\oplus\mathcal{D}_w^{\perp_\delta}\big)=$

$= \{0\}$ тогда и только тогда, когда $\mathcal{D}_w \cap \mathcal{D}_w^{\dagger\perp_\delta} = \{0\}$ и $\mathcal{D}_w^\dagger \cap \mathcal{D}_w^{\perp_\delta} = \{0\}$. Из леммы 1 получаем, что есть ровно

$$\mathfrak{E}_w = \sum_{k_1=0}^{\varrho_w t} \sum_{k_2=0}^{\tau_w t} \begin{bmatrix} \varrho_w t \\ k_1 \end{bmatrix}_{q^{d_w}} \begin{bmatrix} \tau_w t \\ k_2 \end{bmatrix}_{q^{d_w}}$$

различных способов выбрать пару $(\mathcal{D}'_w, \mathcal{D}_w^{\dagger\prime})$. Таким образом, чтобы вычислить $\mathfrak{D}_w$, достаточно определить число $\mathfrak{F}_w$ различных способов выбрать пару $(\mathcal{D}_w, \mathcal{D}_w^\dagger)$, где $\mathcal{D}_w$ – $\mathcal{F}_w$-подпространство в $\mathcal{K}_w$, а $\mathcal{D}_w^\dagger$ – $\mathcal{F}_w^\dagger$-подпространство в $\mathcal{K}_w^\dagger$, такие что $\mathcal{D}_w \cap \cap \mathcal{D}_w^{\dagger\perp_\delta} = \{0\}$ и $\mathcal{D}_w^\dagger \cap \mathcal{D}_w^{\perp_\delta} = \{0\}$. Из этих рассуждений заключаем, что $\mathfrak{F}_w$ равно числу различных невырожденных $\big(\mathcal{F}_w \oplus \mathcal{F}_w^\dagger\big)$-подмодулей $\mathcal{D}_w \oplus \mathcal{D}_w^\dagger$ модуля $\mathcal{K}_w \oplus \mathcal{K}_w^\dagger$, где $\mathcal{D}_w$ – $\mathcal{F}_w$-подпространство в $\mathcal{K}_w$, а $\mathcal{D}_w^\dagger$ – $\mathcal{F}_w^\dagger$-подпространство в $\mathcal{K}_w^\dagger$. Тогда, рассуждая, как в [13, предложение 3.5], получаем

$$\mathfrak{F}_w = 2 + \sum_{k=1}^{\eta_w t - 1} q^{k(\eta_w t - k) d_w} \begin{bmatrix} \eta_w t \\ k \end{bmatrix}_{q^{d_w}}.$$

Отсюда

$$\mathfrak{D}_w = \mathfrak{E}_w \mathfrak{F}_w = \sum_{k=0}^{\eta_w t} \sum_{k_1=0}^{\varrho_w t} \sum_{k_2=0}^{\tau_w t} q^{k d_w (\eta_w t - k)} \begin{bmatrix} \eta_w t \\ k \end{bmatrix}_{q^{d_w}} \begin{bmatrix} \varrho_w t \\ k_1 \end{bmatrix}_{q^{d_w}} \begin{bmatrix} \tau_w t \\ k_2 \end{bmatrix}_{q^{d_w}}. \quad \blacktriangle$$

4.4. Определение числа $\mathfrak{D}_s$ для $e_2 + 1 \leqslant s \leqslant e_3$. В следующем предложении определяется число $\mathfrak{D}_s$ в случае $e_2 + 1 \leqslant s \leqslant e_3$ и $\delta \in \{0, *, \gamma\}$.

Предложение 6. *Пусть $e_2 + 1 \leqslant s \leqslant e_3$ фиксировано. Для $\delta \in \{0, *, \gamma\}$ имеем*

$$\mathfrak{D}_s = \sum_{a=0}^{\varepsilon_s t} \begin{bmatrix} \varepsilon_s t \\ a \end{bmatrix}_{q^{d_s}}.$$

Доказательство. Из теоремы 3 получаем, что число $\mathfrak{D}_s$ равно числу различных $\mathcal{F}_s$-подпространств в $\mathcal{G}_s$ для $e_2 + 1 \leqslant s \leqslant e_3$. Так как $\dim_{\mathcal{F}_s} \mathcal{G}_s = \varepsilon_s t$, то применяя лемму 1, получаем $\mathfrak{D}_s = \sum\limits_{a=0}^{\varepsilon_s t} \begin{bmatrix} \varepsilon_s t \\ a \end{bmatrix}_{q^{d_s}}$. $\blacktriangle$

Доказательство теоремы 4. Подставляя значения $\mathfrak{D}_\nu$ $(1 \leqslant \nu \leqslant e_1)$ из предложений 1–4, значения $\mathfrak{D}_w$ $(e_1 + 1 \leqslant w \leqslant e_2)$ из предложения 5 и значения $\mathfrak{D}_s$ $(e_2 + 1 \leqslant s \leqslant e_3)$ из предложения 6 в формулу (1), получаем требуемый результат. $\blacktriangle$

Следующие примеры иллюстрируют теорему 4.

Пример 1. Пусть $q = 5$, $t = 2$, $m_1 = m_2 = 3$, $\omega_1 = 1$ и $\omega_2 = 2$, так что $n = m_1 + m_2 = 6$ и $\Omega = (\omega_1, \omega_2) = (1, 2)$. Тогда $x^{m_1} - \omega_1 = x^3 - 1 = (x + 4)(x^2 + x + 1)$ и $x^{m_2} - \omega_2 = x^3 - 2 = (x + 2)(x^2 + 3x + 4)$ – неприводимые разложения многочленов $x^{m_1} - \omega_1$ и $x^{m_2} - \omega_2$ над $\mathbb{F}_5$ соответственно. Возьмем $g_1(x) = x + 4$, $g_2(x) = x^2 + x + 1$, $g_3(x) = x + 2$ и $g_4(x) = x^2 + 3x + 4$. Тогда получаем, что $g_u^\dagger(x) = g_u(x)$ для $1 \leqslant u \leqslant 2$, $g_3^\dagger(x) \neq g_3(x)$, $g_4^\dagger(x) \neq g_4(x)$ и $g_3^\dagger(x) \neq g_4(x)$, откуда $d_1 = d_3 = 1$, $d_2 = d_4 = 2$, $\varepsilon_{1,1} = \varepsilon_{2,1} = \varepsilon_{3,2} = \varepsilon_{4,2} = 1$ и $\varepsilon_{1,2} = \varepsilon_{2,2} = \varepsilon_{3,1} = \varepsilon_{4,1} = 0$. Отсюда вытекает, что $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon_4 = 1$. Вычисления с помощью системы компьютерной алгебры Magma показывают, что существует ровно 39424 различных аддитивных Ω-MC-кодов длины 6 над $\mathbb{F}_{5^2}$, имеющих дополнительные 0-двойственные, что согласуется с теоремой 4.

Пример 2. Пусть $q = 5$, $t = 2$, $m_1 = 2$, $m_2 = 4$, $\omega_1 = 3$ и $\omega_2 = 4$, так что $n = m_1 + m_2 = 6$ и $\Omega = (\omega_1, \omega_2) = (3, 4)$. Тогда $x^{m_1} - \omega_1 = x^2 - 3 = x^2 + 2$ и $x^{m_2} - \omega_2 =$

$= x^4-4 = (x^2+2)(x^2+3)$ – неприводимые разложения многочленов $x^{m_1}-\omega_1$ и $x^{m_2}-\omega_2$ над $\mathbb{F}_5$ соответственно. Возьмем $g_1(x) = x^2+2$ и $g_2(x) = x^2+3$. Тогда получаем, что $g_1^\dagger(x) = g_2(x)$, откуда $d_1 = d_2 = 2$, $\varepsilon_{1,1} = \varepsilon_{1,2} = \varepsilon_{1,2}^\dagger = 1$, $\varepsilon_{1,1}^\dagger = 0$, $\mathcal{I}_1 = \{2\}$ и $\mathcal{I}_1' = \{1\}$. Отсюда вытекает, что $\eta_1 = \varrho_1 = 1$ и $\tau_1 = 0$. Вычисления с помощью системы компьютерной алгебры Magma показывают, что существует ровно 18256 различных аддитивных Ω-МС-кодов длины 6 над $\mathbb{F}_{5^2}$, имеющих дополнительные $*$-двойственные, что согласуется с теоремой 4.

Пример 3. Пусть $q = 7$, $t = 2$, $m_1 = 2$, $m_2 = 4$, $m_3 = 6$, $\omega_1 = 5$, $\omega_2 = 2$ и $\omega_3 = 6$, так что $n = m_1 + m_2 + m_3 = 12$ и $\Omega = (\omega_1, \omega_2, \omega_3) = (5, 2, 6)$. Тогда $x^{m_1} - \omega_1 = x^2 - 5 = x^2 + 2$, $x^{m_2} - \omega_2 = x^4 - 2 = (x+2)(x+5)(x^2+4)$ и $x^{m_3} - \omega_3 = x^6 - 6 = (x^2+1)(x^2+2)(x^2+4)$ – неприводимые разложения многочленов $x^{m_1} - \omega_1$, $x^{m_2} - \omega_2$ и $x^{m_3} - \omega_3$ над $\mathbb{F}_7$ соответственно. Возьмем $g_1(x) = x^2+1$, $g_2(x) = x^2+2$, $g_3(x) = x^2+4$, $g_4(x) = x+2$ и $g_5(x) = x+5$. Тогда получаем, что $g_1^\dagger(x) = g_1(x)$, $g_2^\dagger(x) = g_3(x)$, $g_4^\dagger(x) \neq g_4(x)$, $g_5^\dagger(x) \neq g_5(x)$ и $g_4^\dagger(x) \neq g_5(x)$, откуда $d_1 = d_2 = d_3 = 2$, $d_4 = d_5 = 1$, $\varepsilon_{1,3} = \varepsilon_{2,1} = \varepsilon_{2,3} = \varepsilon_{4,2} = \varepsilon_{5,2} = \varepsilon_{2,2}^\dagger = \varepsilon_{2,3}^\dagger = 1$, $\varepsilon_{1,1} = \varepsilon_{1,2} = \varepsilon_{2,2} = \varepsilon_{4,1} = \varepsilon_{4,3} = \varepsilon_{5,1} = \varepsilon_{5,3} = \varepsilon_{2,1}^\dagger = 0$, $\mathcal{I}_2 = \{3\}$ и $\mathcal{I}_2' = \{1, 2\}$. Отсюда вытекает, что $\varepsilon_1 = \varepsilon_4 = \varepsilon_5 = \eta_2 = \varrho_2 = \tau_2 = 1$ и $\varepsilon_2 = 2$.

Вычисления с помощью системы компьютерной алгебры Magma показывают, что существует ровно 29172915200 различных аддитивных Ω-МС-кодов длины 12 над $\mathbb{F}_{7^2}$, имеющих дополнительные γ-двойственные, что согласуется с теоремой 4.

Замечание 1. Заметим, что теорема 3.1 работы [13] вытекает из теоремы 4 при выборе $\ell = 1$ и $\omega_1 = 1$, а теорема 5.6 работы [15] – при выборе $\ell = 1$ и $\omega_1 = -1$.

§ 5. Заключение и направления дальнейшей работы

В статье исследованы аддитивные МС-коды с дополнительными двойственными над конечными полями относительно обычной билинейной, эрмитовой и $*$-формы следа. Выведено необходимое и достаточное условие, при котором аддитивный МС-код имеет дополнительный двойственный. Также получены явные формулы для числа аддитивных МС-кодов с дополнительными двойственными. Эти формулы полезны для классификации аддитивных МС-кодов с дополнительными двойственными над конечными полями с точностью до эквивалентности. Результаты, полученные в [13, 15], вытекают из наших результатов как частные случаи (см. замечание 1). В последующей работе мы покажем, что класс аддитивных МС-кодов с дополнительными двойственными над конечными полями является асимптотически хорошим. Было бы интересно получить классификацию аддитивных МС-кодов с дополнительными двойственными над конечными полями с точностью до эквивалентности с помощью полученных формул.

Авторы заявляют об отсутствии конфликта интересов в отношении содержания настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Massey, J.L.* Linear Codes with Complementary Duals // Discrete Math. 1992. V. 106–107. P. 337–342. https://doi.org/10.1016/0012-365X(92)90563-U
2. *Yang X., Massey J.L.* The Condition for a Cyclic Code to Have a Complementary Dual // Discrete Math. 1994. V. 126. № 1–3. P. 391–393. https://doi.org/10.1016/0012-365X(94)90283-6
3. *Sendrier N.* Linear Codes with Complementary Duals Meet the Gilbert–Varshamov Bound // Discrete Math. 2004. V. 285. № 1–3. P. 345–347. https://doi.org/10.1016/j.disc.2004.05.005

4. *Dougherty S.T., Kim J.L., Özkaya B., Sok L., Solé P.* The Combinatorics of LCD Codes: Linear Programming Bound and Orthogonal Matrices // Int. J. Inform. Coding Theory. 2017. V. 4. № 2–3. P. 116–128. https://doi.org/10.1504/IJICOT.2017.083827
5. *Carlet C., Guilley S.* Complementary Dual Codes for Counter-measures to Side-Channel Attacks // Adv. Math. Commun. 2016. V. 10. № 1. P. 131–150. http://dx.doi.org/10.3934/amc.2016.10.131
6. *Calderbank A.R., Rains E.M., Shor P.W., Sloane N.J.A.* Quantum Error Correction via Codes over GF(4) // IEEE Trans. Inform. Theory. 1998. V. 44. № 4. P. 1369–1387. https://doi.org/10.1109/18.681315
7. *Bierbrauer J., Edel Y.* Quantum Twisted Codes // J. Combin. Des. 2000. V. 8. № 3. P. 174–188. https://doi.org/10.1002/(SICI)1520-6610(2000)8:3<174::AID-JCD3>3.0.CO;2-T
8. *Rains E.M.* Nonbinary Quantum Codes // IEEE Trans. Inform. Theory. 1999. V. 45. № 6. P. 1827–1832. https://doi.org/10.1109/18.782103
9. *Huffman W.C.* Additive Cyclic Codes over $\mathbb{F}_4$ // Adv. Math. Commun. 2007. V. 1. № 4. P. 427–459. http://doi.org/10.3934/amc.2007.1.427
10. *Huffman W.C.* Additive Cyclic Codes over $\mathbb{F}_4$ of Even Length // Adv. Math. Commun. 2008. V. 2. № 3. P. 309–343. http://doi.org/10.3934/amc.2008.2.309
11. *Huffman W.C.* Cyclic $\mathbb{F}_q$-Linear $\mathbb{F}_{q^t}$-Codes // Int. J. Inf. Coding Theory. 2010. V. 1. № 3. P. 249–284. http://doi.org/10.1504/IJICOT.2010.032543
12. *Sharma A., Kaur T.* On Cyclic $\mathbb{F}_q$-Linear $\mathbb{F}_{q^t}$-Codes // Int. J. Inform. Coding Theory. 2017. V. 4. № 1. P. 19–46. https://doi.org/10.1504/IJICOT.2017.081457
13. *Sharma A., Kaur T.* Enumeration of Complementary-Dual Cyclic $\mathbb{F}_q$-Linear $\mathbb{F}_{q^t}$-Codes // Discrete Math. 2018. V. 341. № 4. P. 965–980. https://doi.org/10.1016/j.disc.2017.12.006
14. *Cao Y., Chang X., Cao Y.* Constacyclic $\mathbb{F}_q$-Linear $\mathbb{F}_{q^\ell}$-Codes // Appl. Algebra Engrg. Comm. Comput. 2015. V. 26. № 4. P. 369–388. https://doi.org/10.1007/s00200-015-0257-4
15. *Kaur T., Sharma A.* Constacyclic Additive Codes over Finite Fields // Discrete Math. Algorithms Appl. 2017. V. 9. № 3. Article no. 1750037 (35 pp.). https://doi.org/10.1142/S1793830917500379
16. *Sharma S., Sharma A.* Multi-twisted Additive Codes over Finite Fields // Beitr. Algebra Geom. 2021. Online First article (34 pp.). https://doi.org/10.1007/s13366-021-00576-1
17. *Grove L.C.* Classical Groups and Geometric Algebra. Providence, RI: Amer. Math. Soc., 2002.
18. *Taylor D.E.* The Geometry of the Classical Groups. Berlin: Heldermann, 1992.
19. *Szymiczek K.* Bilinear Algebra: An Introduction to the Algebraic Theory of Quadratic Forms. Amsterdam: Gordon & Breach, 1997.
20. *Brualdi R.A.* Introductory Combinatorics. Upper Saddle River, NJ: Pearson/Prentice Hall, 2010.

Шарма Сандип
Шарма Анурадха✉
Отделение математики, Институт информационных технологий Индрапрастха (IIIT-Delhi), Нью-Дели, Индия
✉anuradha@iiitd.ac.in

Поступила в редакцию
05.08.2021
После доработки
05.08.2021
Принята к публикации
23.01.2022

EDN: BIWIBU
ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 1**

УДК 621.391.1 : 519.725

© 2022 г. **И.Ю. Могильных**

О q-ИЧНЫХ ПРОПЕЛИНЕЙНЫХ СОВЕРШЕННЫХ КОДАХ НА ОСНОВЕ РЕГУЛЯРНЫХ ПОДГРУПП ОБЩЕЙ АФФИННОЙ ГРУППЫ[1]

Код называется пропелинейным, если его группа автоморфизмов содержит подгруппу, действующую регулярно на кодовых словах кода. Подгруппа группы аффинных преобразований $GA(r,q)$ называется регулярной, если она действует регулярно на векторах $\mathbb{F}_q^r$. Всякий автоморфизм регулярной подгруппы общей линейной группы $GA(r,q)$ индуцирует перестановку на смежных классах по коду Хэмминга длины $\frac{q^r-1}{q-1}$. На основе этой перестановки в статье предложена конструкция q-ичных пропелинейных совершенных кодов длины $\frac{q^{r+1}-1}{q-1}$. В частности, для любого простого q получена бесконечная серия q-ичных пропелинейных совершенных кодов предполного ранга.

Ключевые слова: пропелинейный код, совершенный код, регулярное действие, аффинная группа, ранг.

DOI: 10.31857/S0555292322010041

§ 1. Введение

Понятие пропелинейного кода было введено в [1]. Эти коды обобщают такие классы кодов как линейные, $\mathbb{Z}_4$-линейные и пр. Отметим, что многие известные конструкции двоичных совершенных кодов позволяют строить пропелинейные коды. В частности, к таким относятся пропелинейные коды из оригинальных конструкций Васильева [2] и Соловьевой [3], предложенные в работах [4–6]. Помимо пропелинейных двоичных совершенных кодов известны также конструкции других оптимальных кодов. Например, все известные на сегодняшний день конструкции кодов Препараты являются пропелинейными [7–9].

В отличие от двоичного случая, работ, посвященных q-ичным, $q \geqslant 3$, оптимальным пропелинейным кодам относительно немного. Транзитивные и пропелинейные МДР-коды исследовались в работе [10]. В работе [5] была предложена конструкция совершенных q-ичных кодов ранга на единицу больше размерности кода Хэмминга на основе конструкции Шонхейма.

В данной статье рассмотрена конструкция q-ичных совершенных кодов, использующая автоморфизмы регулярных подгрупп группы $GA(r,q)$ и конструкцию Моллара [11] (см. также [12]). При $q = 2$ эта конструкция является частным случаем конструкции Соловьевой для двоичных совершенных кодов и расширенных совершенных из [3] и была рассмотрена в работах [6, 13].

Двоичные пропелинейные коды из работы [6] имеют относительно большое ядро, ранги этих кодов принимают все значения от размерности кода Хэмминга до предполного ранга. В работе [13] показано существование бесконечной серии двоичных

[1] Исследование выполнено за счет гранта Российского научного фонда № 22-21-00135, https://rscf.ru/en/project/22-21-00135/

расширенных совершенных кодов, чья группа автоморфизмов действует транзитивно на коде, а также транзитивно на множестве векторов на расстоянии 1 от кода. Коды с таким свойством известны как транзитивные на соседях (neighbor transitive), см. [14]. В [13] установлено, что эквивалентность расширенных совершенных пропелинейных кодов из [6] равносильна изоморфизму их систем четверок Штейнера, что позволяет решать проблему эквивалентности этих кодов, имеющих длину 32, с помощью персонального компьютера.

Опишем содержание данной статьи, которое идейно восходит к [6]. В § 2 приводятся определения и обозначения. Конструкция пропелинейных кодов дана в § 3. В исходной конструкции Моллара [11] для построения совершенного кода длины $\frac{q^{r+1}-1}{q-1}$ используются смежные классы двух кодов – кода Хэмминга длины $\frac{q^r-1}{q-1}$ и кода, проверочная матрица которого состоит из всех векторов длины r, а также перестановка τ на векторах $\mathbb{F}_q^r$. Каждый автоморфизм всякой регулярной подгруппы $GA(r,q)$ – это перестановка на множестве векторов $\mathbb{F}_q^r$. В § 3 показано, что если τ – такая перестановка, то соответствующий код Моллара пропелинеен. Заметим, что эта конструкция, помимо кодов Хэмминга и кодов из работы [5], является единственным методом построения q-ичных пропелинейных совершенных кодов для $q \geqslant 3$, известным на сегодняшний день.

В § 4 рассматривается проблема рангов q-ичных пропелинейных кодов, полученных в § 3. Для всякого простого q показано существование перестановки τ, такой что код S_τ длины q^2+q+1 является пропелинейным и имеет предполный ранг. С использованием конструкции прямого произведения для регулярных подгрупп $GA(r,q)$ (см. [15]) этот результат обобщается следующим образом: для всякого простого q и любых ℓ, r, $0 \leqslant \ell \leqslant r/2$, $r \geqslant 2$, существует q-ичный совершенный пропелинейный код длины $\frac{q^{r+1}-1}{q-1}$ ранга $\frac{q^{r+1}-1}{q-1} - r - 1 + 2\ell$. В частности, этот класс содержит бесконечную серию кодов предполного ранга растущей длины. Так как при $q = 3$ ранг является инвариантом класса эквивалентности кодов, то имеется $\left\lfloor \frac{r}{2} \right\rfloor + 1$ троичных кодов попарно различных рангов длины $\frac{3^{r+1}-1}{2}$, не эквивалентных кодам из [5], так как последние имеют ранг, на единицу превосходящий ранг кода Хэмминга.

Результаты, изложенные в этой статье, были анонсированы в препринте [16] без доказательств.

§ 2. Определения и обозначения

Через $\mathbb{F}_q^n$ обозначим пространство всех векторов над полем $\mathbb{F}_q$. Нулевой элемент векторного пространства и вектор из одних единиц будем обозначать через $\mathbf{0}$ и $\mathbf{1}$, и их длина будет очевидна из контекста. Конкатенацию векторов x и y обозначаем через $x\,|\,y$. Если C и D – q-ичные коды, то

$$C \times D = \{(x\,|\,y) :\ x \in C,\ y \in D\}.$$

Совершенным называется q-ичный код с кодовым расстоянием 3, мощность которого достигает границы Хэмминга.

Пусть f, f' – перестановки векторов в пространствах $\mathbb{F}_q^n$ и $\mathbb{F}_q^{n'}$ соответственно. Обозначим через $(f\,|\,f')$ перестановку, которая действует на конкатенациях векторов x из $\mathbb{F}_q^n$ и y из $\mathbb{F}_q^{n'}$ следующим образом:

$$(f\,|\,f')(x\,|\,y) = (f(x)\,|\,f'(y)). \tag{1}$$

Отметим, что в § 3 в частном случае, когда f, f' являются автоморфизмами (например, перестановками позиций) $\mathbb{F}_q^n$ и $\mathbb{F}_q^{n'}$, определенное в (1) обозначение трактуется как автоморфизм $\mathbb{F}_q^{n+n'}$.

Перестановка π координатных позиций $\{1, 2, \ldots, n\}$ действует следующим образом:

$$\pi(x) = \pi(x_1, \ldots, x_n) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)}).$$

Рассмотрим n перестановок σ_i, $i \in \{1, \ldots, n\}$, элементов поля $\mathbb{F}_q$. *Посимвольной перестановкой* пространства $\mathbb{F}_q^n$ называется отображение $\sigma = (\sigma_1, \ldots, \sigma_n)$, переставляющее символы в каждой из позиций:

$$(\sigma_1, \ldots, \sigma_n)(x_1, \ldots, x_n) = (\sigma_1(x_1), \ldots, \sigma_n(x_n)).$$

Композиция $\sigma\sigma'$ двух перестановок σ и σ' такого типа – это посимвольная перестановка $(\sigma_1\sigma'_1, \ldots, \sigma_n\sigma'_n)$, где $\sigma_i\sigma'_i$ – композиция $\sigma_i\sigma'_i(\cdot) = \sigma_i(\sigma'_i(\cdot))$ для любого $i \in \{1, 2, \ldots, n\}$.

Под *автоморфизмом* $\mathbb{F}_q^n$ будем понимать изометрию пространства, т.е. биективное отображение на себя, сохраняющее попарное расстояние между векторами. Всякий автоморфизм $\mathbb{F}_q^n$ можно описать парой $(\sigma; \pi)$, где π – перестановка позиций $\{1, \ldots, n\}$, σ – посимвольная перестановка, а образ вектора x определяется следующим образом:

$$(\sigma; \pi)(x) = \sigma(\pi(x)).$$

Композиция двух изометрий $(\sigma; \pi)$ и $(\delta; \pi')$ определяется как

$$(\sigma; \pi)(\delta; \pi') = (\sigma\delta'; \pi\pi'), \tag{2}$$

где $\delta' = \left(\delta_{\pi^{-1}(1)}, \ldots, \delta_{\pi^{-1}(n)}\right)$. Совокупность всех автоморфизмов $\mathbb{F}_q^n$ относительно операции композиции образует группу, обозначаемую $\mathrm{Aut}(\mathbb{F}_q^n)$.

Для всякой перестановки позиций π автоморфизм $(\sigma; \pi)$ называется *мономиальным*, если для каждого $i \in \{1, \ldots, n\}$ найдется ненулевой элемент α_i поля $\mathbb{F}_q$, такой что $\sigma_i(\gamma) = \alpha_i * \gamma$ для всякого $\gamma \in \mathbb{F}_q$, где через $*$ обозначено умножение в $\mathbb{F}_q$. Отметим, что всякий мономиальный автоморфизм является линейным. Пусть u – вектор из $\mathbb{F}_q^n$. Через σ_u обозначим посимвольную перестановку, такую что для всякого $x \in \mathbb{F}_q^n$

$$\sigma_u(x) = u + x, \tag{3}$$

где через $+$ обозначено сложение векторов в $\mathbb{F}_q^n$. Такие перестановки будем называть *трансляциями*.

Утверждение 1. *Для мономиального автоморфизма m пространства $\mathbb{F}_q^n$ и любого вектора и пространства $\mathbb{F}_q^n$ имеет место равенство*

$$m\sigma_u = \sigma_{m(u)}m.$$

Доказательство. В силу определения (3) трансляции σ_u и линейности мономиального автоморфизма m образ всякого вектора $x \in \mathbb{F}_q^n$ под действием автоморфизма $m\sigma_u$ равен

$$m\sigma_u(x) = m(u + x) = m(u) + m(x).$$

Вектор $m(u) + m(x)$ можно записать как $\sigma_{m(u)}m(x)$, откуда получаем требуемое. ▲

Группой автоморфизмов кода C называется стабилизатор кода C как множества в группе $\mathrm{Aut}(\mathbb{F}_q^n)$. Напомним, что действие группы на множестве M называется *регулярным*, если оно транзитивно и порядок группы совпадает с мощностью M. *Пропелинейным* (см. [17]; оригинальное определение было дано в [1]) называется q-ичный код, чья группа автоморфизмов содержит подгруппу, действующую регулярно на его кодовых словах. Два кода длины n называются *эквивалентными*, если найдется автоморфизм (изометрия) пространства $\mathbb{F}_q^n$, переводящий один код в другой.

Общей линейной группой $GL(r,q)$ называется группа невырожденных $(r \times r)$-матриц над $\mathbb{F}_q$. *Общей аффинной группой* $GA(r,q)$ называется группа преобразований (a,M), где a – вектор-столбец из $\mathbb{F}_q^r$, $M \in GL(r,q)$, действующих на векторах-столбцах $b \in \mathbb{F}_q^r$ следующим образом:

$$(a,M)(b) = a + Mb,$$

относительно композиции

$$(a,M)(b,M') = (a + Mb, MM'). \tag{4}$$

Подгруппа G группы $GA(r,q)$ называется *регулярной*, если она действует транзитивно на векторах из $\mathbb{F}_q^r$ и имеет порядок q^r. Другими словами, для всякого вектора $a \in \mathbb{F}_q^r$ найдется единственное аффинное преобразование g из G, такое что $g = (a,M)$ для некоторой матрицы $M \in GL(r,q)$. Очевидно, что группа трансляций на векторы из $\mathbb{F}_q^r$ является регулярной подгруппой $GA(r,q)$. Существует также большое число других регулярных подгрупп $GA(r,q)$ с разнообразными свойствами. В п. 4.2 рассмотрена регулярная подгруппа $GA(2,q)$, при простых q изоморфная группе трансляций, но не сопряженная с ней.

Через $\langle C \rangle$ обозначим линейную оболочку, натянутую на векторы кода C. Через $\dim(C)$ обозначим размерность линейного пространства C. Через $\mathrm{rank}(M)$ обозначим ранг матрицы M. *Рангом* кода C называется $\dim(\langle C \rangle)$, т.е. ранг его кодовой матрицы. Ранг кода длины n называется *полным* (*предполным*), если он равен n ($n-1$ соответственно).

В силу того, что при $q = 2, 3$ всякий автоморфизм является композицией мономиального автоморфизма и трансляции, имеем следующее (см., например, [18]):

Утверждение 2. *Если q равно 2 или 3, то ранг любого кода, содержащего нулевой вектор, является инвариантом класса эквивалентности этого кода.*

Замечание 1. Ситуацию при $q \geqslant 4$ проиллюстрируем на следующем примере. Пусть C – код Хэмминга с проверочной матрицей $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \alpha & \alpha^2 \end{pmatrix}$, где α – примитивный элемент поля $\mathbb{F}_4$. Векторы $(00\alpha\alpha^2 1)$, $(00\alpha^2 1\alpha)$ принадлежат коду C. Рассмотрим посимвольную перестановку $\sigma = (\mathrm{Id}, \mathrm{Id}, \mathrm{Id}, \mathrm{Id}, (1\alpha))$. Заметим, что код $\sigma(C)$ содержит векторы $(00\alpha\alpha^2\alpha)$, $(00\alpha^2 11)$. Отсюда заключаем, что в линейной оболочке $\sigma(C)$ содержится вектор (00001) веса 1.

Таким образом, $\sigma(C)$ и C имеют ранги 4 и 3 соответственно. Отметим, что применяя подобные перестановки к q-ичному коду Хэмминга любой длины, можно строить коды, эквивалентные кодам Хэмминга, произвольных рангов от размерности кода до полного при любом $q \geqslant 4$. Таким образом, в случае $q \geqslant 4$ ранг кода, содержащего нулевой вектор, не является инвариантом класса эквивалентности.

§ 3. Пропелинейные совершенные коды из автоморфизмов регулярных подгрупп $GA(r,q)$

В данном параграфе приводится основная конструкция кодов. Построение базируется на методе Моллара, однако будет использовано более подходящее для нас из-

ложение Романова из [12], чему посвящен п. 3.1. Конструкция использует разбиение пространства предыдущей кодовой длины на коды Хэмминга. В п. 3.2 приводятся известные факты о действии общей линейной группы на смежных классах этого разбиения. Конструкция пропелинейных кодов приведена в п. 3.3, где мы воспользуемся автоморфизмами регулярных подгрупп $GA(r,q)$ для построения пропелинейных кодов.

3.1. Каскадная конструкция q-ичных совершенных кодов. Пусть H_C – проверочная матрица q-ичного кода Хэмминга C с r проверочными символами, H' – матрица размера $r \times q^r$, столбцами которой являются все векторы из $\mathbb{F}_q^r$. Построим проверочную матрицу q-ичного кода Хэмминга с $r+1$ проверками. Пусть в ее первой строке первые $\dfrac{q^r-1}{q-1}$ элементов являются нулевыми, а оставшиеся q^r элементов – единицы поля $\mathbb{F}_q$. Несложно видеть, что матрица

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} \\ H_C & H' \end{pmatrix} \tag{5}$$

является проверочной для q-ичного кода Хэмминга длины $\dfrac{q^{r+1}-1}{q-1}$.

Для $a \in \mathbb{F}_q^r$ через C_a обозначим смежный класс по коду C, синдром которого равен a:

$$C_a = \{x : \, x \in \mathbb{F}_q^{\frac{q^r-1}{q-1}}, \, H_C x^T = a\}. \tag{6}$$

Обозначим через D линейный код длины q^r с проверочной матрицей

$$H_D = \begin{pmatrix} \mathbf{1} \\ H' \end{pmatrix}, \tag{7}$$

где H', как и ранее, – матрица размера $r \times q^r$, столбцами которой являются все векторы из $\mathbb{F}_q^r$. Позиции кода D пронумеруем столбцами проверочной матрицы H_D: позиция имеет номер $a \in \mathbb{F}_q^r$, если $\begin{pmatrix} 1 \\ a \end{pmatrix}$ – соответствующий столбец проверочной матрицы H_D. Для $a \in \mathbb{F}_q^r$ через D_a обозначим смежный класс $D + e_{\mathbf{0}} - e_a$, где e_a – вектор с единицей только в позиции, занумерованной вектором a, в остальных позициях e_a равен нулю. Для перестановки τ на множестве векторов $\mathbb{F}_q^r$ рассмотрим следующий код:

$$S_\tau = \bigcup_{a \in \mathbb{F}_q^r} C_a \times D_{\tau(a)}.$$

Теорема 1 [11, 12]. *Для любой степени простого числа q и произвольной перестановки τ векторов $\mathbb{F}_q^r$ код S_τ является q-ичным совершенным кодом длины* $\dfrac{q^{r+1}-1}{q-1}$.

Заметим, что в силу определения C_a и D_a код Хэмминга $\bigcup\limits_{a \in \mathbb{F}_q^r} C_a \times D_a$ имеет проверочную матрицу (5), поэтому является частным случаем этой конструкции.

3.2. Действие $GL(r,q)$ на смежных классах по C и D. Следующие свойства кодов Хэмминга являются широко известными (см., например, [19, теорема 7.1]) или напрямую вытекают из обозначения для смежного класса C_a.

Утверждение 3. *Пусть C – код Хэмминга длины $\dfrac{q^r-1}{q-1}$ с проверочной матрицей H_C, и пусть C_a – смежный класс* (6). *Тогда*

1. *Для любых двух векторов a и b из $\mathbb{F}_q^r$ выполнено $C_a + C_b = C_{a+b}$;*
2. [19, теорема 7.1] *Для всякой матрицы $M \in GL(r,q)$ найдется мономиальный автоморфизм $m_M \in \mathrm{Aut}(C)$, такой что для любого вектора x выполнено*

$$H_C(m_M(x))^T = MH_Cx^T.$$

Отображение $M \to m_M$ является инъективным гомоморфизмом $GL(r,q)$ в группу $\mathrm{Aut}(C)$;
3. *Для всякого $a \in \mathbb{F}_q^r$ имеет место равенство $m_M(C_a) = C_{Ma}$.*

Рассмотрим гомоморфизм $GL(r,q)$ в группу автоморфизмов кода D. Если M – невырожденная $(r \times r)$-матрица над $\mathbb{F}_q$, то через π_M обозначим перестановку координатных позиций D, действующую следующим образом:

$$\pi_M(e_a) = e_{Ma}. \tag{8}$$

Очевидно, π_M является автоморфизмом кода D, проверочная матрица которого состоит из всех векторов из $\mathbb{F}_q^r$. Отметим также, что группа $\{\pi_M : M \in GL(r,q)\}$ также действует на множестве смежных классов D_a, $a \in \mathbb{F}_q^r$.

Утверждение 4. *Справедливо следующее*:
1. *Для любых векторов $a, b \in \mathbb{F}_q^r$ имеем $D_a + D_b = D_{a+b}$;*
2. *Отображение $M \to \pi_M$ является инъективным гомоморфизмом $GL(r,q)$ в группу* $\mathrm{Aut}(D)$. *Для любого $b \in \mathbb{F}_q^r$ имеет место*

$$\pi_M(D_b) = D_{Mb}.$$

Доказательство. 1. Заметим, что $D_a + D_b = D + 2e_{\mathbf{0}} - e_a - e_b$. Для доказательства равенства $D_a + D_b = D + e_{\mathbf{0}} - e_{a+b}$ достаточно показать, что вектор $2e_{\mathbf{0}} - e_a - e_b - (e_{\mathbf{0}} - e_{a+b}) = e_{\mathbf{0}} + e_{a+b} - e_a - e_b$ принадлежит коду D. В свою очередь, это вытекает из нумерации столбцов проверочной матрицы H_D кода D векторами из $\mathbb{F}_q^r$, а именно

$$H_D(e_{\mathbf{0}} + e_{a+b} - e_a - e_b)^T = \begin{pmatrix}1\\ \mathbf{0}\end{pmatrix} + \begin{pmatrix}1\\ a+b\end{pmatrix} - \begin{pmatrix}1\\ a\end{pmatrix} - \begin{pmatrix}1\\ b\end{pmatrix} = \begin{pmatrix}0\\ \mathbf{0}\end{pmatrix}.$$

2. Из того, что π_M – автоморфизм кода D, и из (8) имеем

$$\pi_M(D_b) = \pi_M(D + e_{\mathbf{0}} - e_b) = D + e_0 - e_{Mb} = D_{Mb}. \quad \blacktriangle$$

3.3. Пропелинейные коды из регулярных подгрупп $GA(r,q)$. Пусть G – регулярная подгруппа общей аффинной группы $GA(r,q)$. Тогда в силу определения регулярного действия для любого $a \in \mathbb{F}_q^r$ найдется единственное аффинное преобразование из группы G, обозначаемое везде далее через g_a, которое отображает вектор $\mathbf{0}$ в вектор a. Заметим, что так как $g_a(\mathbf{0}) = a$, то аффинное преобразование g_a принимает вид

$$g_a = (a, M_a) \tag{9}$$

для некоторой невырожденной матрицы M_a. Таким образом, q^r элементов всякой регулярной подгруппы группы $GA(r,q)$ занумерованы векторами из $\mathbb{F}_q^r$.

Используя введенную нумерацию, получим несколько равенств. Рассмотрим композицию преобразований g_a и g_b:

$$g_ag_b = (a, M_a)(b, M_b) = (a + M_ab, M_aM_b).$$

Аффинное преобразование $g_a g_b$ принадлежит группе G и отображает $\mathbf{0}$ в $a+M_a b$, что вытекает из приведенного выше выражения для $g_a g_b$. В силу регулярности действия G на векторах из $\mathbb{F}_q^r$ найдется единственное аффинное преобразование, переводящее $\mathbf{0}$ в вектор $g_a(b) = a+M_a b$. Используя введенную в (9) нумерацию элементов G через векторы $\mathbb{F}_q^r$, это преобразование обозначается $g_{g_a(b)}$.

Итак,

$$g_a g_b = (a + M_a b, M_a M_b) = g_{g_a(b)} = (a + M_a b, M_{g_a(b)}), \tag{10}$$

откуда

$$M_a M_b = M_{g_a(b)} = M_{a+M_a b}. \tag{11}$$

Пусть T – автоморфизм группы G, тогда перестановка τ векторов $\mathbb{F}_q^r$ вида $g_{\tau(a)} = T(g_a)$ для всякого $a \in \mathbb{F}_q^r$ называется перестановкой, *индуцированной автоморфизмом* T. Заметим, что всякий автоморфизм оставляет на месте нейтральный элемент группы, поэтому для всякой перестановки τ, индуцированной автоморфизмом, имеет место $\tau(\mathbf{0}) = \mathbf{0}$.

В силу определения индуцированной перестановки, а также учитывая преобразование $g_{g_a(b)} = g_a g_b$ (см. (10)), имеем

$$g_{\tau(g_a(b))} = (\tau(g_a(b)), M_{\tau(g_a(b))}) = T(g_{g_a(b)}) = T(g_a g_b).$$

Так как T автоморфизм, то $T(g_a g_b) = T(g_a)T(g_b)$, и следовательно,

$$T(g_a g_b) = T(g_a)T(g_b) = g_{\tau(a)} g_{\tau(b)} = (g_{\tau(a)}(\tau(b)), M_{\tau(a)} M_{\tau(b)}).$$

Отсюда можно заключить, что преобразования $(\tau(g_a(b)), M_{\tau(g_a(b))})$ и $(g_{\tau(a)}(\tau(b)), M_{\tau(a)} M_{\tau(b)})$ равны, а следовательно,

$$\tau(g_a(b)) = g_{\tau(a)}(\tau(b)), \tag{12}$$

$$M_{\tau(g_a(b))} = M_{\tau(a)} M_{\tau(b)}. \tag{13}$$

Т е о р е м а 2. *Пусть τ – перестановка векторов $\mathbb{F}_q^r$, индуцированная автоморфизмом регулярной подгруппы $GA(r,q)$. Тогда S_τ – пропелинейный q-ичный совершенный код длины $\dfrac{q^{r+1}-1}{q-1}$.*

Д о к а з а т е л ь с т в о. Пусть τ – перестановка, индуцированная автоморфизмом регулярной подгруппы G группы $GA(r,q)$. Напомним, что для всякого $a \in \mathbb{F}_q^r$ преобразование g_a – преобразование вида (9) из группы G.

Покажем, что следующее множество автоморфизмов $\mathbb{F}_q^r$ является группой:

$$\Gamma = \bigcup_{a \in \mathbb{F}_q^r} \big\{ (\sigma_x \,|\, \sigma_y)(m_{M_a} \,|\, \pi_{M_{\tau(a)}}) : (x \,|\, y) \in C_a \times D_{M_{\tau(a)}} \big\},$$

где σ_x, σ_y – трансляции, отвечающие векторам x и y (см. (3)), M_a – матричная часть преобразования $g_a \in G$ (см. (9)), m_{M_a} – мономиальный автоморфизм кода Хэмминга C, отвечающий матрице M_a, а $\pi_{M_{\tau(a)}}$ – перестановочный автоморфизм кода D, отвечающий матрице $M_{\tau(a)}$ (см. п. 3.2). Напомним, что $(x \,|\, y)$ – конкатенация векторов, на которой действует автоморфизм $(m_{M_a} \,|\, \pi_{M_{\tau(a)}})$, где операция $\cdot\,|\,\cdot$ определена в (1). Заметим, что для каждого фиксированного a в выражении для Γ, приведенном выше, $(x \,|\, y)$ пробегает код $C_a \times D_{\tau(a)}$, однозначно задавая трансляции $(\sigma_x \,|\, \sigma_y)$. При этом автоморфизм $(m_{M_a} \,|\, \pi_{M_{\tau(a)}})$ зависит лишь от a, поэтому $|\Gamma| = |S_\tau|$.

Рассмотрим композицию двух автоморфизмов из Γ и покажем, что автоморфизм

$$(\sigma_x \,|\, \sigma_y)(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(\sigma_u \,|\, \sigma_v)(m_{M_b} \,|\, \pi_{M_{\tau(b)}}) \tag{14}$$

принадлежит Γ, где $x \in C_a$, $y \in D_{\tau(a)}$ и $u \in C_b$, $v \in D_{\tau(b)}$ для некоторых векторов a и b из $\mathbb{F}_q^r$. Преобразуем

$$(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(\sigma_u \,|\, \sigma_v). \tag{15}$$

Так как $(m_{M_a} \,|\, \pi_{M_{\tau(a)}})$ – мономиальный автоморфизм, а $(\sigma_u \,|\, \sigma_v)$ – трансляция, то в силу утверждения 1 имеем

$$(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(\sigma_u \,|\, \sigma_v) = (m_{M_a}\sigma_u \,|\, \pi_{M_{\tau(a)}}\sigma_v) = (\sigma_{m_{M_a}(u)} \,|\, \sigma_{\pi_{M_{\tau(a)}}(v)})(m_{M_a} \,|\, \pi_{M_{\tau(a)}}).$$

Обозначим векторы $m_{M_a}(u)$ и $\pi_{M_{\tau(a)}}(v)$ через u' и v' соответственно. Выражение (14) преобразуется в

$$(\sigma_x \,|\, \sigma_y)(\sigma_{u'} \,|\, \sigma_{v'})(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(m_{M_b} \,|\, \pi_{M_{\tau(b)}}). \tag{16}$$

Вектор u принадлежит C_b, поэтому в силу п. 3 утверждения 3 имеем $m_{M_a}(u) \in$ $\in C_{M_a b}$, т.е.

$$u' \in C_{M_a b}. \tag{17}$$

В свою очередь, вектор v принадлежит $D_{\tau(b)}$, откуда в силу п. 2 утверждения 4 для $v' = \pi_{M_{\tau(a)}}(v)$ выполняется

$$v' \in D_{M_{\tau(a)}\tau(b)}. \tag{18}$$

Очевидно, что трансляции (перестановки вида (3)) коммутируют, поэтому для трансляций автоморфизма (16) выполнены следующие равенства: $\sigma_x\sigma_{u'} = \sigma_{x+u'}$ и $\sigma_y\sigma_{v'} = \sigma_{y+v'}$. Напомним, что $x \in C_a$, а также согласно (17) вектор $u' \in C_{M_a b}$, поэтому в силу п. 1 утверждения 3 вектор $x + u'$ принадлежит $C_{a+M_a(b)}$. Отсюда, учитывая, что аффинное преобразование g_a равно (a, M_a), имеем $g_a(b) = a + M_a(b)$. Следовательно, $C_{a+M_a(b)} = C_{g_a(b)}$ и

$$x + u' \in C_{g_a(b)}. \tag{19}$$

Имеем $y \in D_{\tau(a)}$, и в силу (18) $v' \in D_{M_{\tau(a)}\tau(b)}$. Тогда согласно п. 1 утверждения 4 получаем следующее:

$$y + v' \in D_{\tau(a)} + D_{M_{\tau(a)}\tau(b)} = D_{\tau(a)+M_{\tau(a)}\tau(b)}.$$

Заметим, что аффинное преобразование $g_{\tau(a)}$ равно $(\tau(a), M_{\tau(a)})$, и так как согласно (12) выполняется $g_{\tau(a)}(\tau(b)) = \tau(g_a(b))$, то

$$y + v' \in D_{\tau(a)+M_{\tau(a)}\tau(b)} = D_{g_{\tau(a)}(\tau(b))} = D_{\tau(g_a(b))}. \tag{20}$$

Итак, (16) преобразуется в

$$(\sigma_{x+u'} \,|\, \sigma_{y+v'})(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(m_{M_b} \,|\, \pi_{M_{\tau(b)}}), \tag{21}$$

где $(x + u' \,|\, y + v') \in C_{g_a(b)} \times D_{\tau(g_a(b))}$ в силу (19) и (20).

Рассмотрим мономиальную часть $(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(m_{M_b} \,|\, \pi_{M_{\tau(b)}})$ автоморфизма (21). Согласно п. 2 утверждения 3 отображение $M \to m_M$ является гомоморфизмом

$GL(r,q)$ в $\mathrm{Aut}(C)$, поэтому выполнено следующее:

$$m_{M_a} m_{M_b} = m_{M_a M_b}.$$

В свою очередь, в силу (11) выполняется $m_{M_a M_b} = m_{g_a(b)}$, поэтому

$$m_{M_a} m_{M_b} = m_{g_a(b)}. \tag{22}$$

Так как в силу п. 2 утверждения 4 отображение $M \to \pi_M$ является гомоморфизмом $GL(r,q)$ в $\mathrm{Aut}(D)$, то

$$\pi_{M_{\tau(a)}} \pi_{M_{\tau(b)}} = \pi_{M_{\tau(a)} M_{\tau(b)}}.$$

Согласно (13) справедливо $M_{\tau(a)} M_{\tau(b)} = M_{\tau(g_a(b))}$, и следовательно,

$$\pi_{M_{\tau(a)}} \pi_{M_{\tau(b)}} = \pi_{M_{\tau(g_a(b))}}. \tag{23}$$

Итак, автоморфизм (21) и, соответственно, исходная композиция автоморфизмов (14) преобразуется в

$$(\sigma_{x+u'} \,|\, \sigma_{y+v'})(m_{g_a(b)} \,|\, \pi_{M_{\tau(g_a(b))}}),$$

где $(x + u' \,|\, y + v') \in C_{g_a(b)} \times D_{\tau(g_a(b))}$, т.е. принадлежит Γ. Отсюда заключаем, что Γ является группой. Отметим, что трансляции $(\sigma_x \,|\, \sigma_y)$ в выражении для Γ таковы, что $(x \,|\, y)$ пробегают весь код S_τ, поэтому орбита нулевого вектора под действием Γ совпадает с кодом S_τ. Другими словами, группа Γ – подгруппа группы автоморфизмов кода S_τ, действующая транзитивно на его кодовых словах. Более того, так как порядок Γ совпадает с мощностью кода S_τ, то Γ также регулярна, а код S_τ пропелинеен. ▲

§ 4. Ранги кодов, полученных каскадной конструкцией

Пусть τ – перестановка векторов $\mathbb{F}_q^r$, оставляющая на месте $\mathbf{0}$. Так как позиции кода D занумерованы векторами $\mathbb{F}_q^r$, то τ также будем трактовать как перестановку позиций кода D. *Дефектом* перестановки τ будем называть разность $\dim(D) - \dim(D \cap \tau(D))$. Через $D^\perp$ обозначим код, дуальный к D. Заметим, что

$$\dim(D) - \dim(D \cap \tau(D)) = \dim((D \cap \tau(D))^\perp) - \dim(D^\perp).$$

В силу выражения для размерности суммы и пересечения подпространств имеем

$$\dim((D \cap \tau(D))^\perp) - \dim(D^\perp) = \dim(\langle D^\perp \cup (\tau(D))^\perp \rangle) - \dim(D^\perp) =$$
$$= \dim(\langle D^\perp \cup (\tau(D))^\perp \rangle) - r - 1.$$

Лемма 1. *Пусть $\mathbf{0}, a^2, \ldots, a^{q^r}$ – все векторы пространства $\mathbb{F}_q^r$, τ – любая перестановка этих векторов, $\tau(\mathbf{0}) = \mathbf{0}$, D – код с проверочной матрицей $H_D = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \mathbf{0} & a^2 & \ldots & a^{q^r} \end{pmatrix}$. Тогда дефект τ равен*

$$\mathrm{rank} \begin{pmatrix} a^2 & \ldots & a^{q^r} \\ \tau(a^2) & \ldots & \tau(a^{q^r}) \end{pmatrix} - r.$$

Доказательство. По определению дефект τ равен $\dim(\langle D^\perp \cup (\tau(D))^\perp \rangle) - r - 1$.

Размерность кода $\langle D^\perp \cup (\tau(D))^\perp \rangle$ можно выразить как $\mathrm{rank} \begin{pmatrix} H_D \\ \tau(H_D) \end{pmatrix}$, где $\tau(H_D)$ – проверочная матрица кода $\tau(D)$.

Подействовав перестановкой τ^{-1} на столбцы матрицы $\begin{pmatrix} H_D \\ \tau(H_D) \end{pmatrix}$, получим равенство $\operatorname{rank}\begin{pmatrix} H_D \\ \tau(H_D) \end{pmatrix} = \operatorname{rank}\begin{pmatrix} H_D \\ \tau^{-1}(H_D) \end{pmatrix}$. Матрица $\begin{pmatrix} H_D \\ \tau^{-1}(H_D) \end{pmatrix}$ равна

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \mathbf{0} & a^2 & \dots & a^{q^r} \\ 1 & 1 & \dots & 1 \\ \mathbf{0} & \tau(a^2) & \dots & \tau(a^{q^r}) \end{pmatrix},$$

и пространство ее строк раскладывается в прямую сумму ее первой строки и подматрицы $\begin{pmatrix} \mathbf{0} & a^2 & \dots & a^{q^r} \\ \mathbf{0} & \tau(a^2) & \dots & \tau(a^{q^r}) \end{pmatrix}$, откуда имеем требуемое выражение для дефекта. ▲

Отметим, что в следующей теореме код S_τ не обязательно является пропелинейным.

Теорема 3 [16]. *Пусть τ – перестановка векторов $\mathbb{F}_q^r$ с дефектом ℓ, такая что $\tau(\mathbf{0}) = \mathbf{0}$. Тогда ранг кода S_τ длины $\dfrac{q^{r+1}-1}{q-1}$ равен $\dfrac{q^{r+1}-1}{q-1} - r - 1 + \ell$.*

В п. 4.1 введем подход, позволяющий строить перестановки векторов пространства $\mathbb{F}_q^r$ с увеличивающимся дефектом из существующих перестановок пространств $\mathbb{F}_q^{r'}$ и $\mathbb{F}_q^{r-r'}$. Этот подход позволяет строить коды с растущей прибавкой ранга по отношению к размерности кода Хэмминга. В п. 4.2 рассмотрим конструкцию перестановки τ, индуцированной автоморфизмом регулярной подгруппы, дающую бесконечную серию пропелинейных совершенных кодов S_τ растущей длины.

4.1. Дефект итерации перестановок. Пусть τ и σ – биекции (перестановки) на себя множеств векторов из $\mathbb{F}_q^{r_1}$ и $\mathbb{F}_q^{r_2}$ соответственно, $\tau(\mathbf{0}) = \mathbf{0}$, $\sigma(\mathbf{0}) = \mathbf{0}$. Всякий вектор-столбец из $\mathbb{F}_q^{r_1+r_2}$ представляет собой конкатенацию $\begin{pmatrix} a \\ b \end{pmatrix}$ некоторых векторов-столбцов $a \in \mathbb{F}_q^{r_1}$ и $b \in \mathbb{F}_q^{r_2}$. В соответствии с (1) определим *итерацию перестановок* τ и σ как перестановку $\tau \,|\, \sigma$, которая отображает вектор-столбец $\begin{pmatrix} a \\ b \end{pmatrix}$ пространства $\mathbb{F}_q^{r_1+r_2}$, где a и b – векторы-столбцы из $\mathbb{F}_q^{r_1}$ и $\mathbb{F}_q^{r_2}$, следующим образом:

$$(\tau \,|\, \sigma)\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \tau(a) \\ \sigma(b) \end{pmatrix}. \tag{24}$$

Утверждение 5. *Пусть τ и σ – перестановки множеств векторов из $\mathbb{F}_q^{r_1}$ и $\mathbb{F}_q^{r_2}$ соответственно, индуцированные автоморфизмами некоторых регулярных подгрупп $GA(r_1, q)$ и $GA(r_2, q)$ соответственно. Тогда $\tau \,|\, \sigma$ – подстановка, индуцированная автоморфизмом некоторой регулярной подгруппы $GA(r_1 + r_2, q)$.*

Доказательство. Пусть G_1 и G_2 – регулярные подгруппы групп $GA(r_1, q)$ и $GA(r_2, q)$. Для элементов $(a, M) \in G_1$ и $(b, M') \in G_2$ рассмотрим следующее аффинное преобразование из $GA(r_1 + r_2, q)$, которое обозначим через $(a, M) \times (b, M')$:

$$\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} M & 0 \\ 0 & M' \end{pmatrix}\right).$$

Заметим, что $\{(a, M) \times (b, M') : (a, M) \in G_1,\ (b, M') \in G_2\}$ является прямым произведением групп G_1 и G_2 и, более того, является регулярной подгруппой $GA(r_1 + r_2, q)$ (см., например, [15, § 6]). Обозначим эту группу через $G_1 \times G_2$.

Пусть T и S – автоморфизмы групп G_1 и G_2 с индуцированными перестановками τ и σ соответственно. Автоморфизмы T и S являются перестановками элементов

групп G_1 и G_2 соответственно. Определим перестановку $T \times S$ элементов группы $G_1 \times G_2$, действующую на аффинных преобразованиях из $G_1 \times G_2$ следующим образом: $(T \times S)(g_1 \times g_2) = T(g_1) \times S(g_2)$. Очевидно, что $T \times S$ является автоморфизмом группы $G_1 \times G_2$ и индуцированная перестановка автоморфизма $T \times S$ есть $\tau \,|\, \sigma$, определенная ранее в (24). ▲

Теорема 4. *Пусть τ и φ – перестановки векторов пространств $\mathbb{F}_q^{r_1}$ и $\mathbb{F}_q^{r_2}$, $q \geqslant 2$, с дефектами ℓ_1 и ℓ_2 соответственно, $\tau(\mathbf{0}) = \mathbf{0}$, $\varphi(\mathbf{0}) = \mathbf{0}$. Тогда дефект перестановки $\tau \,|\, \varphi$ равен $\ell_1 + \ell_2$.*

Доказательство. Рассмотрим следующую нумерацию всех q-ичных векторов длины $r_1 + r_2$. Всякий вектор-столбец длины $r_1 + r_2$ является конкатенацией двух векторов длин r_1 и r_2. Пусть векторы длин r_1 и и r_2 занумерованы в некотором порядке, начиная с нулевых векторов: $\mathbf{0}, a^2, \ldots, a^{q^{r_1}}$ и $\mathbf{0}, b^2, \ldots, b^{q^{r_2}}$. Перечислим $q^{r_1+r_2}$ векторов длины $r_1 + r_2$ в следующем порядке: вначале перечислим все векторы (q^{r_2} штук), первые r_1 позиций которых равны нулевому вектору $\mathbf{0}$, потом все векторы, первые r_1 позиций которых равны a^2, и т.д.

Применяя лемму 1 для указанной нумерации векторов из $\mathbb{F}_q^{r_1+r_2}$, получаем, что дефект перестановки $(\tau \,|\, \varphi)$ равен

$$\operatorname{rank}(M) - r_1 - r_2, \tag{25}$$

где M – матрица

$$\begin{pmatrix}
\mathbf{0} & \ldots & \mathbf{0} & a^2 & a^2 & \ldots & a^2 & \ldots & a^{q^{r_1}} & a^{q^{r_1}} & \ldots & a^{q^{r_1}} \\
b^2 & \ldots & b^{q^{r_2}} & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} & \ldots & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} \\
\mathbf{0} & \ldots & \mathbf{0} & \tau(a^2) & \tau(a^2) & \ldots & \tau(a^2) & \ldots & \tau(a^{q^{r_1}}) & \tau(a^{q^{r_1}}) & \ldots & \tau(a^{q^{r_1}}) \\
\varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \ldots & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}})
\end{pmatrix}.$$

Ранг матрицы M равен рангу следующей матрицы:

$$\begin{pmatrix}
\mathbf{0} & \ldots & \mathbf{0} & a^2 & a^2 & \ldots & a^2 & \ldots & a^{q^{r_1}} & a^{q^{r_1}} & \ldots & a^{q^{r_1}} \\
\mathbf{0} & \ldots & \mathbf{0} & \tau(a^2) & \tau(a^2) & \ldots & \tau(a^2) & \ldots & \tau(a^{q^{r_1}}) & \tau(a^{q^{r_1}}) & \ldots & \tau(a^{q^{r_1}}) \\
b^2 & \ldots & b^{q^{r_2}} & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} & \ldots & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} \\
\varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \ldots & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}})
\end{pmatrix}.$$

В силу расположения нулевых векторов в этой матрице, пространство ее строк раскладывается в прямую сумму пространств строк следующих двух ее подматриц:

$$\begin{pmatrix}
\mathbf{0} & \ldots & \mathbf{0} & a^2 & a^2 & \ldots & a^2 & \ldots & a^{q^{r_1}} & a^{q^{r_1}} & \ldots & a^{q^{r_1}} \\
\mathbf{0} & \ldots & \mathbf{0} & \tau(a^2) & \tau(a^2) & \ldots & \tau(a^2) & \ldots & \tau(a^{q^{r_1}}) & \tau(a^{q^{r_1}}) & \ldots & \tau(a^{q^{r_1}})
\end{pmatrix},$$
$$\begin{pmatrix}
b^2 & \ldots & b^{q^{r_2}} & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} & \ldots & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} \\
\varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \ldots & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}})
\end{pmatrix}.$$

Удалив повторяющиеся и нулевые столбцы из матриц, получаем следующее:

$$\operatorname{rank}(M) = \operatorname{rank}\begin{pmatrix} a^2 & \ldots & a^{q^{r_1}} \\ \tau(a^2) & \ldots & \tau(a^{q^{r_1}}) \end{pmatrix} + \operatorname{rank}\begin{pmatrix} b^2 & \ldots & b^{q^{r_2}} \\ \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) \end{pmatrix}.$$

По лемме 1 ранги матриц $\begin{pmatrix} a^2 & \ldots & a^{q^{r_1}} \\ \tau(a^2) & \ldots & \tau(a^{q^{r_1}}) \end{pmatrix}$ и $\begin{pmatrix} b^2 & \ldots & b^{q^{r_2}} \\ \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) \end{pmatrix}$ равны $\ell_1 + r_1$ и $\ell_2 + r_2$ соответственно, где ℓ_1 и ℓ_2 –дефекты перестановок τ и φ соответственно, поэтому $\operatorname{rank}(M) = r_1 + r_2 - \ell_1 - \ell_2$. Отсюда из (25) получаем, что дефект $(\tau \,|\, \varphi)$ равен $\ell_1 + \ell_2$. ▲

Замечание 2. Отметим, что частный случай теоремы 4 при $q = 2$ был доказан в [6, лемма 3], однако доказательство содержит ошибку.

4.2. Бесконечная серия пропелинейных совершенных кодов различных рангов над простым алфавитом.

Пример 1. Пусть q – простое число, $q > 2$. Ниже мы рассмотрим регулярную подгруппу $GA(2, q)$, изоморфную $\mathbb{Z}_q^2$, но не сопряженную с подгруппой трансляций на векторы из $\mathbb{F}_q^2$ в группе $GA(2, q)$. Покажем, что существует автоморфизм этой группы, такой что дефект индуцированной им перестановки равен 2.

Рассмотрим следующие аффинные преобразования:

$$g = \left(\begin{pmatrix}1\\0\end{pmatrix}, \mathrm{Id}\right), \quad h = \left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right).$$

По индукции покажем, что для любого i имеет место

$$h^i = \left(\begin{pmatrix}i(i-1)\\ i\end{pmatrix}, \begin{pmatrix}1 & 2i\\0 & 1\end{pmatrix}\right). \tag{26}$$

Предположим, что для некоторого i выполнено равенство (26), тогда по определению композиции (4) имеем

$$\begin{aligned}
h^{i+1} &= \left(\begin{pmatrix}i(i-1)\\ i\end{pmatrix}, \begin{pmatrix}1 & 2i\\0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right) = \\
&= \left(\begin{pmatrix}i(i-1)\\ i\end{pmatrix} + \begin{pmatrix}1 & 2i\\0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1 & 2i\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right) = \\
&= \left(\begin{pmatrix}i(i-1)+2i\\ i+1\end{pmatrix}, \begin{pmatrix}1 & 2i+2\\0 & 1\end{pmatrix}\right) = \left(\begin{pmatrix}i(i+1)\\ i+1\end{pmatrix}, \begin{pmatrix}1 & 2i+2\\0 & 1\end{pmatrix}\right).
\end{aligned}$$

Таким образом, формула (26) выполнена для любого i. Из (26) вытекает, что h имеет порядок q.

Заметим, что $gh = \left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right)$. Более того,

$$\begin{aligned}
hg &= \left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1\\0\end{pmatrix}, \mathrm{Id}\right) = \left(\begin{pmatrix}0\\1\end{pmatrix} + \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right) = \\
&= \left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right).
\end{aligned}$$

Таким образом, g и h коммутируют и имеют порядок q, поэтому группа, порожденная этими элементами, изоморфна $\mathbb{Z}_q^2$. Покажем, что эта группа является регулярной подгруппой $GA(2, q)$. Учитывая формулу (26), имеем

$$g^i h^j = \left(\begin{pmatrix}i\\0\end{pmatrix}, \mathrm{Id}\right)\left(\begin{pmatrix}j(j-1)\\ j\end{pmatrix}, \begin{pmatrix}1 & 2j\\0 & 1\end{pmatrix}\right) = \left(\begin{pmatrix}i+j(j-1)\\ j\end{pmatrix}, \begin{pmatrix}1 & 2j\\0 & 1\end{pmatrix}\right). \tag{27}$$

Если упорядоченная пара (i, j) не равна паре (i', j'), то векторы $\begin{pmatrix}i+j(j-1)\\ j\end{pmatrix}$ и $\begin{pmatrix}i'+j'(j'-1)\\ j'\end{pmatrix}$ различны. Поэтому группа, порожденная g и h, является регулярной подгруппой $GA(2, q)$.

Так как группа, порожденная g и h, изоморфна $\mathbb{Z}_q^2$, то перестановка T ее элементов, такая что

$$T(g^i h^j) = h^i g^j$$

для всех $i, j \in \{0, \ldots, q-1\}$, является автоморфизмом этой группы порядка 2. Заметим, что в силу формулы (27) выполняется

$$g^i h^j = \left(\begin{pmatrix} i + j(j-1) \\ j \end{pmatrix}, \begin{pmatrix} 1 & 2j \\ 0 & 1 \end{pmatrix} \right)$$

и, так как g и h коммутируют,

$$h^i g^j = \left(\begin{pmatrix} j + i(i-1) \\ i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 0 & 1 \end{pmatrix} \right).$$

Рассмотрим перестановку τ, индуцированную автоморфизмом T. По определению перестановки τ, индуцированной автоморфизмом T, имеем $T((a, M)) = (\tau(a), M')$, где (a, M) – элемент рассматриваемой регулярной группы. Поэтому, учитывая данные выше выражения для $g^i h^j$ и $h^i g^j$, для произвольных $i, j \in \{0, \ldots, q-1\}$ справедливо

$$\tau \begin{pmatrix} i + j(j-1) \\ j \end{pmatrix} = \begin{pmatrix} j + i(i-1) \\ i \end{pmatrix}.$$

В частности, когда пары (i, j) равны $(1, 0)$, $(0, 1)$, $(-1, -2)$, $(0, 2)$, имеем

$$\tau \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \tau \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \tau \begin{pmatrix} 5 \\ -2 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \quad \tau \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}. \tag{28}$$

Покажем, что дефект перестановки τ равен 2. Так как $r = 2$, то по лемме 1 дефект τ равен $\operatorname{rank} \begin{pmatrix} a^2 & \ldots & a^{q^2} \\ \tau(a^2) & \ldots & \tau(a^{q^2}) \end{pmatrix} - 2$, где $a^2, \ldots, a^{q^2}$ – ненулевые векторы $\mathbb{F}_q^2$. Покажем, что $\operatorname{rank} \begin{pmatrix} a^2 & \ldots & a^{q^2} \\ \tau(a^2) & \ldots & \tau(a^{q^2}) \end{pmatrix} = 4$, т.е. перестановка τ имеет дефект 2.

Возьмем следующие векторы $a^2, \ldots, a^5$: $a^2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $a^3 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $a^4 = \begin{pmatrix} 5 \\ -2 \end{pmatrix}$, $a^5 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$. Учитывая равенства (28), производя невырожденные линейные преобразования со строками матрицы, убеждаемся, что ее строки линейно независимы:

$$\operatorname{rank} \begin{pmatrix} a^2 & \ldots & a^{q^2} \\ \tau(b^2) & \ldots & \tau(a^{q^2}) \end{pmatrix} =$$

$$= \operatorname{rank} \begin{pmatrix} 1 & 0 & 5 & 2 & \ldots \\ 0 & 1 & -2 & 2 & \ldots \\ 0 & 1 & 0 & 2 & \ldots \\ 1 & 0 & -1 & 0 & \ldots \end{pmatrix} = \operatorname{rank} \begin{pmatrix} 1 & 0 & 5 & 2 & \ldots \\ 0 & 1 & -2 & 2 & \ldots \\ 0 & 0 & 2 & 0 & \ldots \\ 0 & 0 & 6 & 2 & \ldots \end{pmatrix} = 4.$$

Следовательно, τ имеет дефект 2.

Т е о р е м а 5. *Для всякого простого q, $q \geqslant 3$, и любых $r \geqslant 2$, $i \in \{0, \ldots, \lfloor r/2 \rfloor\}$ существует пропелинейный q-ичный совершенный код S_φ длины $\dfrac{q^{r+1}-1}{q-1}$ ранга $\dfrac{q^{r+1}-1}{q-1} - r - 1 + 2i$.*

Д о к а з а т е л ь с т в о. Пусть τ – перестановка векторов $\mathbb{F}_q^2$ с дефектом 2, индуцированная автоморфизмом регулярной подгруппы из примера 1. Рассмотрим пере-

становку

$$\varphi = \tau \,|\, \ldots \,|\, \tau \,|\, \mathrm{id} \,|\, \ldots \,|\, \mathrm{id}$$

векторов $\mathbb{F}_q^r$, где τ взята i раз, а тождественная перестановка взята $r - 2i$ раз. По утверждению 5 эта перестановка индуцирована автоморфизмом, поэтому по теореме 2 код S_φ – пропелинейный. По теореме 4 дефект перестановки φ равен $2i$, откуда в силу теоремы 3 имеем требуемое значение для ранга S_φ. ▲

Замечание 3. Отметим, что при $q = 3$ ранг является инвариантом, поэтому все $\lfloor r/2 \rfloor + 1$ кодов, описанных в теореме 5, попарно неэквивалентны. Следовательно, все из них, кроме линейного, отличаются от кодов, построенных в работе [5], так как последние либо линейные, либо имеют ранг, на единицу превосходящий размерность кода Хэмминга той же длины. При $q \geqslant 4$ коды из классов эквивалентности кодов из доказательства теоремы 5, скорее всего, также не могут иметь ранг, на единицу превосходящий размерность кода Хэмминга той же длины. Однако показать это представляется технически трудным.

Автор выражает благодарность Ф.И. Соловьевой, в дискуссиях с которой появилась часть утверждений и подходов данной статьи, а также рецензенту за ценные замечания и предложения, позволившие улучшить изложение материала.

СПИСОК ЛИТЕРАТУРЫ

1. *Rifà J., Basart J.M., Huguet L.* On Completely Regular Propelinear Codes // Proc. 6th Int. Conf. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-6). Rome, Italy. July 4–8, 1988. Lect. Notes Comp. Sci. V. 357. Berlin: Springer, 1989. P. 341–355. https://doi.org/10.1007/3-540-51083-4_71
2. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. Т. 8. М.: Физматлит, 1962. С. 337–339.
3. *Соловьева Ф.И.* О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. Вып. 37. Новосибирск: Ин-т матем. СО АН СССР, 1981. С. 65–76.
4. *Borges J., Mogilnykh I.Yu., Rifà J., Solov'eva F.I.* Structural Properties of Binary Propelinear Codes // Adv. Math. Commun. 2012. V. 6. № 3. P. 329–346. https://doi.org/10.3934/amc.2012.6.329
5. *Krotov D.S., Potapov V.N.* Propelinear 1-Perfect Codes from Quadratic Functions // IEEE Trans. Inform. Theory. 2014. V. 60. № 4. P. 2065–2068. https://doi.org/10.1109/TIT.2014.2303158
6. *Mogilnykh I.Yu., Solov'eva F.I.* A Concatenation Construction for Propelinear Perfect Codes from Regular Subgroups of $GA(r, 2)$ // Сиб. электрон. матем. изв. 2019. Т. 16. С. 1689–1702. https://doi.org/10.33048/semi.2019.16.119
7. *Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.* The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 301–319. https://doi.org/10.1109/18.312154
8. *Borges J., Phelps K.P., Rifà J., Zinoviev V.A.* On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like Codes // IEEE Trans. Inform. Theory. 2003. V. 49. № 11. P. 2834–2843. https://doi.org/10.1109/TIT.2003.819329
9. *Зиновьев В.А., Зиновьев Д.В.* Обобщенные коды Препараты и 2-разрешимые системы четверок Штейнера // Пробл. передачи информ. 2016. V. 52. № 2. С. 15–36. http://mi.mathnet.ru/ppi2201
10. *Krotov D.S., Potapov V.N.* Constructions of Transitive Latin Hypercubes // European J. Combin. 2016. V. 54. P. 51–64. https://doi.org/10.1016/j.ejc.2015.12.001
11. *Mollard M.* Une novelle famille de 3-codes parfaits sur $GF(q)$ // Discrete Math. 1984. V. 49. № 2. P. 209–212. https://doi.org/10.1016/0012-365X(84)90121-3
12. *Romanov A.M.* On Non-Full-Rank Perfect Codes over Finite Fields // Des. Codes Cryptogr. 2019. V. 87. № 5. P. 995–1003. https://doi.org/10.1007/s10623-018-0506-1

13. *Mogilnykh I.Yu., Solov'eva F.I.* Coordinate Transitivity of a Class of Extended Perfect Codes and Their SQS // Сиб. электрон. матем. изв. 2020. Т. 17. С. 1451–1462. https://doi.org/10.33048/semi.2020.17.101
14. *Gillespie N.I., Praeger C.E.* New Characterisations of the Nordstrom–Robinson Codes // Bull. London Math. Soc. 2017. V. 49. № 2. P. 320–330. https://doi.org/10.1112/blms.12016
15. *Pellegrini M.A., Tamburini Bellani M.C.* More on Regular Subgroups of the Affine Group // Linear Algebra Appl. 2016. V. 505. P. 126–151. https://doi.org/10.1016/j.laa.2016.04.031
16. *Mogilnykh I.Yu.* q-ary Propelinear Perfect Codes from the Regular Subgroups of the $GA(r, q)$ and Their Ranks, https://arXiv.org/abs/2112.08659 [math.CO], 2021.
17. *Phelps K.T., Rifà J.* On Binary 1-Perfect Additive Codes: Some Structural Properties // IEEE Trans. Inform. Theory. 2002. V. 48. № 9. P. 2587–2592. https://doi.org/10.1109/TIT.2002.801474
18. *Горкунов Е.В.* Группы автоморфизмов кодов Хэмминга и их компонент: Дис. ... канд. физ.-мат. наук: 01.01.09. Новосибирск: НГУ, 2010.
19. *Huffman W.C.* Codes and Groups // Handbook of Coding Theory. Amsterdam: Elsevier, 1998. Ch. 6. P. 1345–1440.

Могильных Иван Юрьевич
Институт математики им. С.Л. Соболева
СО РАН, Новосибирск
ivmog@math.nsc.ru

Поступила в редакцию
17.12.2021
После доработки
10.02.2022
Принята к публикации
12.02.2022

EDN: KMRFVL
ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 1**

УДК 621.391 : 519.174 : 519.179.1

© 2022 г. **А.С. Семенов**[1], **Д.А. Шабанов**[2]

ОЦЕНКИ ПОРОГОВЫХ ВЕРОЯТНОСТЕЙ ДЛЯ СВОЙСТВ РАСКРАСОК СЛУЧАЙНЫХ ГИПЕРГРАФОВ

Статья посвящена изучению пороговой вероятности для свойства наличия раскраски в r цветов специального вида у случайного k-однородного гиперграфа в биномиальной модели $H(n,k,p)$. Рассматривается параметрическое множество j-хроматических чисел случайного гиперграфа. Раскраска множества вершин гиперграфа называется j-правильной, если в ней каждое ребро содержит не более j вершин каждого цвета. Исследуется вопрос о нахождении точной пороговой вероятности наличия j-правильной раскраски в r цветов у $H(n,k,p)$. С помощью метода второго момента получены весьма точные оценки этой величины при условии, что k и j велики по отношению к r.

Ключевые слова: случайный гиперграф, раскраски гиперграфов, j-хроматическое число, метод второго момента.

DOI: 10.31857/S0555292322010053

§ 1. Введение

В данной статье рассматривается одна из центральных задач в теории случайных графов и гиперграфов о нахождении предельного распределения хроматических чисел случайных гиперграфов. Рассматриваются хроматические числа общего вида, напомним их определения.

1.1. Определения. Пусть $H = (V, E)$ – гиперграф с множеством вершин V и множеством ребер E, а $j \geqslant 1$ – некоторое натуральное число. Подмножество вершин $W \subset V$ называется *j-независимым*, если каждое ребро H имеет не более j общих вершин с W, т.е. $|W \cap A| \leqslant j$ для любого $A \in E$. Отметим, что для k-однородного гиперграфа имеет смысл рассматривать только $j \leqslant k-1$, иначе любое подмножество вершин гиперграфа будет j-независимыми. Экстремальные и вероятностные задачи, касающиеся j-независимых множеств в гиперграфах, изучались, например, в [1–4].

Раскраской вершин гиперграфа $H = (V, E)$ в r цветов является отображение $\tau\colon V \to \{1, \ldots, r\}$. Множества $V_i = \tau^{-1}(i)$, $i = 1, \ldots, r$, принято называть *цветовыми классами* раскраски τ. Если каждый цветовой класс τ является j-независимым множеством в H, то τ называется *j-правильной* раскраской гиперграфа H. Тем самым, каждое ребро в j-правильной раскраске имеет не более j вершин каждого из цветов. Минимальное количество цветов r, необходимое для j-правильной раскраски вершин H, называется *j-хроматическим числом* гиперграфа H и обозначается

[1] Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта № 18-31-00348.

[2] Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта № 20-31-70039 и частичной поддержке гранта Президента РФ № МД-1562.2020.1.

через $\chi_j(H)$. В случае k-однородного гиперграфа существует специальная классификация j-хроматических чисел. Для $j \geqslant k/2$ эти числа называются *слабыми*, а для $j < k/2$ – *сильными*. Суть разделения понятна: в случае $j \geqslant k/2$ неправильно раскрашенное ребро содержит лишь одно большое одноцветное подмножество вершин. Наиболее распространен случай $j = k-1$, который соответствует классическому понятию *хроматического числа гиперграфа* $\chi(H)$.

В данной статье рассматривается проблема нахождения точной пороговой вероятности наличия j-правильной раскраски в заданное число цветов у случайного k-однородного гиперграфа в биномиальной модели $H(n,k,p)$, $n > k \geqslant 2$, $p \in (0,1)$. Напомним, что случайный гиперграф $H(n,k,p)$ образуется в виде схемы Бернулли на ребрах полного k-однородного гиперграфа $K_n^{(k)}$ на n вершинах: каждое ребро $K_n^{(k)}$ включается в $H(n,k,p)$ в качестве ребра независимо и с вероятностью p. Для $k=2$ модель $H(n,2,p)$ очень хорошо известна как $G(n,p)$, биномиальная модель случайного графа, еще называемая моделью Эрдеша–Реньи. Все эти модели являются классическим и центральным объектом изучения в вероятностной комбинаторике. Везде в статье мы предполагаем, что $r \geqslant 2$, $k \geqslant 2$ и $1 \leqslant j \leqslant k-1$ фиксированы, n стремится к бесконечности и $p = p(n) \in (0,1)$ – функция от n.

1.2. Известные результаты. Асимптотическое поведение хроматического числа случайного графа $G(n,p)$ изучается еще с 70-х годов прошлого века. Лучшие текущие результаты описаны, например, в [5,6]. Отметим лишь, что точное предельное распределение можно найти только в *разреженном случае*, когда математическое ожидание числа ребер является линейным по числу вершин n, т.е. $p = p(n) = c/n$ для некоторого фиксированного параметра $c > 0$. В этом случае известно, что хроматическое число имеет фиксированное предельное значение $r = r(c)$ для почти всех значений c, а для оставшихся небольших интервалов значений c существует двухточечная концентрация в двух последовательных натуральных числах. Основные понятия и теоремы относительно сходимости по распределению в теории вероятностей могут быть найдены читателем в главе 3 книги [7].

Гораздо труднее дело обстоит с j-хроматическим числом $H(n,k,p)$. Асимптотическое поведение $\chi_j(H(n,k,p))$ изучалось в работах [8–10], а также [11]. Перечисленные результаты можно кратко описать следующим образом.

1. Если для $p = p(n)$ выполнено $p\binom{n-j-1}{k-j-1} / \ln n \to \infty$, тогда с вероятностью, стремящейся к 1 при $n \to \infty$, j-хроматическое число случайного гиперграфа сравнимо с j-хроматическим числом полного гиперграфа $\chi_j(K_n^{(k)}) = \lceil n/j \rceil$, т.е.

   $$\mathbf{P}(\chi_j(H(n,k,p)) = \lceil n/j \rceil) \to 1 \quad \text{при } n \to \infty.$$

   Например, это соотношение будет выполнено при любом фиксированном $p \in (0,1)$ и любом $j < k-1$. Отметим, что случай $j = k-1$ является особым. При фиксированном $p \in (0,1)$ хроматическое число $\chi_{k-1}(H(n,k,p)$ будет иметь порядок $o(n)$ (см., например, [8]).

2. Обозначим через $d = p\binom{n-1}{k-1}$ математическое ожидание степени вершины в $H(n,k,p)$, и пусть $d_j = j\binom{k-1}{j} d$. Если для $d = d(n)$ выполнено $d \to \infty$ и $dn^{-j} \to 0$ при $n \to \infty$ (т.е. $pn^{k-1} \to \infty$ и $pn^{k-1-j} \to 0$), тогда (см. [11]) для $\chi_j(H(n,k,p))$ выполнен закон больших чисел:

   $$\chi_j(H(n,k,p)) \left(\frac{d_j}{(j+1)\ln d_j} \right)^{-1/j} \xrightarrow{\mathbf{P}} 1 \quad \text{при } n \to \infty.$$

3. Если d_j фиксировано, но больше некоторой абсолютной константы d_0, то имеет место следующая концентрация для значения j-хроматического числа (см. [11]): с вероятностью, стремящейся к 1 при $n \to \infty$, выполнено

$$\left(\frac{d_j}{(j+1)\ln d_j}\right)^{1/j} \leqslant \chi_j(H(n,k,p)) \leqslant \left(\frac{d_j}{(j+1)\ln d_j}\left(1+\frac{1}{\ln^{0,1} d_j}\right)\right)^{1/j}.$$

Для разреженного случая, т.е. для фиксированного $d = d(n)$, в классическом варианте $j = k-1$ более точные оценки были получены в работах [6,12,13]. Обозначим $u_{r,k} = r^{k-1}\ln r - \frac{1}{2}\ln r$ для $r, k \geqslant 2$, и пусть $p = cn/\binom{n}{k}$, где $c > 0$ – некоторый положительный параметр.

1. Если $c > u_{r,k}$, тогда (см. [12])

$$\mathbf{P}(\chi(H(n,k,p)) > r) \to 1 \quad \text{при } n \to \infty; \tag{1}$$

2. Если $c < u_{r,k} - \dfrac{r-1}{r} + O(k^2 r^{1-k/3}\ln r)$ и $k \geqslant 4$, тогда (см. [6])

$$\mathbf{P}(\chi(H(n,k,p)) \leqslant r) \to 1 \quad \text{при } n \to \infty; \tag{2}$$

3. Если $r > r_0(k)$ велико относительно $k \geqslant 3$ и $c < u_{r,k} - \ln 2 - 1{,}01\dfrac{\ln r}{r}$, тогда (см. [13])

$$\mathbf{P}(\chi(H(n,k,p)) \leqslant r) \to 1 \quad \text{при } n \to \infty. \tag{3}$$

Грубо говоря, значение $u_{r,k}$ почти является пороговым значением параметра c для свойства наличия раскраски в r цветов. На интервале $(u_{r,k}, u_{r+1,k})$ хроматическое число сконцентрировано в точке $r+1$ почти везде, кроме небольшого интервала фиксированной величины. В зависимости от отношения r и k длина этого интервала равна либо $\dfrac{r-1}{r} + o(1)$, либо $\ln 2 + o(1)$.

Особый интерес представляет поиск пороговой вероятности для свойств раскраски в два цвета. Поиску пороговой вероятности для свойства "*хроматическое число не превосходит двух*" у случайного гиперграфа $H(n,k,p)$ посвящены работы [14–16]. Наилучший результат был получен в [17], где авторы показали, что существует такая функция $\varepsilon_k = 2^{-k(1+o_k(1))}$, что при $p = cn/\binom{n}{k}$ и

$$c < 2^{k-1}\ln 2 - \frac{\ln 2}{2} - \frac{1}{4} - \varepsilon_k$$

выполнено $\mathbf{P}(\chi(H(n,k,p)) \leqslant 2) \to 1$ с ростом n, а для

$$c > 2^{k-1}\ln 2 - \frac{\ln 2}{2} - \frac{1}{4} + \varepsilon_k$$

выполнено $\mathbf{P}(\chi(H(n,k,p)) > 2) \to 1$ при $n \to \infty$. Тем самым, пороговое значение параметра c удалось локализовать с точностью до интервала, длина которого стремится к нулю с ростом k. Подобный эффект был также обнаружен в статье [18], где для свойства "*j-хроматическое число $H(n,k,p)$ не превосходит двух*" при $k - j < \sqrt{k}$ были получены такие верхняя и нижняя оценки порогового значения параметра c, что разность между ними стремится к нулю с ростом k.

Однако для раскрасок в большее число цветов похожих результатов в общем случае пока добиться не удалось. Даже для классического хроматического числа остается зазор порядка $O(1)$ для свойства наличия правильной раскраски в $r \geqslant 3$ цветов (см. вышеперечисленные результаты 1–3 из работ [6,12,13]).

1.3. Новый результат. Основной результат данный статьи дополняет ранее известные результаты и дает очень точные оценки пороговой вероятности для свойства наличия j-правильной раскраски в r цветов у случайного гиперграфа $H(n,k,p)$ при $j<k-1$, $j\sim k$ и $r\ll k$. Точная формулировка выглядит следующим образом.

Теорема 1. *Пусть $H(n,k,p)$ – случайный k-однородный гиперграф на n вершинах, где $p=cn/\binom{n}{k}$ и $c=c(k,j,r)>0$ не зависит от n. Для любого $r>2$ существуют такие положительные числа $C_\ell=C_\ell(r)$, $C_u=C_u(r)$ и $k_0=k_0(r)$, что при $k>k_0$ и $1<k-j<k^{1/4}$ выполнено следующее*:

1) *Если*

$$c>\frac{r^{k-1}\ln r}{\sum\limits_{s=0}^{k-j-1}\binom{k}{s}(r-1)^s}-\frac{\ln r}{2}+C_u\binom{k}{j+1}r^{-j}, \tag{4}$$

то с вероятностью, стремящейся к 1 при $n\to\infty$, $\chi_j\left(H\left(n,k,p\right)\right)>r$;

2) *Если*

$$c<\frac{r^{k-1}\ln r}{\sum\limits_{s=0}^{k-j-1}\binom{k}{s}(r-1)^s}-\frac{\ln r}{2}-C_\ell k^{(j-k+1)/2}, \tag{5}$$

то с вероятностью, стремящейся к 1 при $n\to\infty$, $\chi_j\left(H\left(n,k,p\right)\right)\leqslant r$.

Прокомментируем результаты теоремы.

1. При фиксированном r и $k-j<k^{1/4}$ (а значит, $j\sim k$) разность между полученными оценками порогового значения c стремится к нулю с ростом k. Это замечательный эффект, который, как видно из полученных выражений, не получается в классическом случае $j=k-1$. Данный феномен мы пока можем объяснить лишь техническими особенностями применения метода второго момента, который мы используем для доказательства теоремы 1, хотя вполне может оказаться, что имеет место некоторая особенность множества j-правильных раскрасок случайного гиперграфа при $j<k-1$.
2. Ограничение $k-j<k^{1/4}$, по-видимому, не является оптимальным даже в рамках применяемого метода. Например, как будет видно из доказательства в § 2, оценка (4) верна и при $k-j=o(k/\ln k)$. Однако учитывая техническую сложность вычислений, нам было важно показать, что теорема верна в достаточно широком диапазоне значений параметров.
3. С точки зрения изучения собственно распределения j-хроматического числа $H(n,k,p)$ представляет интерес обратная ситуация, когда $r\gg k$. Здесь были исследованы некоторые частные случаи. Случай $j=1$, $k=3$ можно найти в работе [19], а случай $j=k-2$ – в работе [20]. В обеих работах полученные оценки пороговой вероятности имеют зазор, стремящийся к положительной константе при $r\to\infty$.

§ 2. Доказательство верхней оценки

Для доказательства верхней оценки обратимся к другой модели случайного гиперграфа $H'(n,k,m)$, где $m=\lceil cn\rceil$ и выполнено неравенство (4). В этой модели независимо, равномерно и с возвращением набираются m ребер из всевозможных k-подмножеств вершин. Обозначим через Z_n число различных ребер в $H'(n,k,m)$. Нужно отметить, что Z_n может быть меньше m, если некоторые случайные ребра совпадут.

Пусть $p' = c'n/\binom{n}{k}$, причем $c' > c$. Тогда покажем, что

$$\mathbf{P}\Big(\chi_j(H'(n,k,m)) > r\Big) \leqslant \mathbf{P}\Big(\chi_j(H(n,k,p')) > r\Big) + o_n(1).$$

Действительно, возьмем случайную перестановку σ ребер полного гиперграфа $K_n^{(k)}$. Далее рассмотрим две независимые с σ случайные величины: ξ_1 с распределением $\mathrm{Bin}\Big(\binom{n}{k}, p'\Big)$ и ξ_2, имеющую то же распределение, что и Z_n. Тогда с точки зрения распределения

- гиперграф H_1, образованный первыми ξ_1 ребрами согласно σ, есть $H\,(n,k,p')$;
- гиперграф H_2, образованный первыми ξ_2 ребрами согласно σ, есть $H'\,(n,k,m)$.

Случайные величины ξ_1 и ξ_2 сильно сконцентрированы вокруг своих средних: $\mathbf{E}\,\xi_1 = = c'n$, $\mathbf{E}\,\xi_2 \sim cn$, $\mathbf{D}\,\xi_1 = O(n)$, $\mathbf{D}\,\xi_2 = O(n)$, и значит, из неравенства Чебышева следует, что $\mathbf{P}(\xi_1 > \xi_2) \to 1$ при $n \to \infty$. Следовательно, с вероятностью, стремящейся к 1, гиперграф H_1 содержит H_2, и нам остается показать, что

$$\mathbf{P}\Big(\chi_j(H'(n,k,m)) > r\Big) \to 1, \quad n \to \infty.$$

Пусть τ – произвольная раскраска вершин гиперграфа $H'(n,k,m)$ в r цветов. Обозначим через $v_1, \ldots, v_r$ мощности ее цветовых классов ($\sum\limits_{i=1}^{r} v_i = n$). Тогда вероятность того, что τ является j-правильной раскраской $H'(n,k,m)$, равна

$$\left(1 - \sum_{i=1}^{r} \sum_{s=0}^{k-j-1} \binom{v_i}{k-s}\binom{n-v_i}{s}\Big/\binom{n}{k}\right)^m. \tag{6}$$

Поясним выражение (6). В силу условия теоремы $k - j < k^{1/4} < k/2$. Значит, если ребро неправильно покрашено в раскраске τ, то в нем существует единственный блок из хотя бы $j+1 > k/2$ одинаково покрашенных вершин. Остальные вершины могут быть раскрашены произвольным образом. Следовательно, в раскраске τ есть в точности $\sum\limits_{i=1}^{r} \sum\limits_{s=0}^{k-j-1} \binom{v_i}{k-s}\binom{n-v_i}{s}$ неправильно раскрашенных k-подмножеств, и ни одно из них не должно войти в случайных гиперграф в качестве ребра.

Для оценивания выражения (6) понадобится следующая

Лемма 1. *Пусть $k, j, r, v_1, \ldots, v_r \in \mathbb{N}$ таковы, что $r > 2$ и $2 < k - j < k^{1/4}$. Существует $k_0 = k_0(r)$, такое что при $k \geqslant k_0$ и любых $v_1, \ldots, v_r$ с условием $\sum\limits_{i=1}^{r} v_i = n$ выполнено*

$$\sum_{i=1}^{r} \sum_{s=0}^{k-j-1} \binom{v_i}{k-s}\binom{n-v_i}{s} \geqslant r \sum_{s=0}^{k-j-1} \binom{n/r}{k-s}\binom{n-n/r}{s} + o(n^k), \quad n \to \infty. \tag{7}$$

Доказательство. Правую часть неравенства можно оценить следующим образом:

$$r \sum_{s=0}^{k-j-1} \binom{n/r}{k-s}\binom{n-n/r}{s} \leqslant \frac{r}{k!} \sum_{s=0}^{k-j-1} \binom{k}{s} \Big(\frac{n}{r}\Big)^{k-s} \left(\frac{n(r-1)}{r}\right)^s.$$

Оценим левую часть

$$\sum_{i=1}^{r} \sum_{s=0}^{k-j-1} \binom{v_i}{k-s}\binom{n-v_i}{s} = \frac{1}{k!} \sum_{i=1}^{r} \sum_{s=0}^{k-j-1} \binom{k}{s} v_i^{k-s}(n-v_i)^s + o(n^k).$$

Рассмотрим функцию $f(x) = \sum\limits_{s=0}^{k-j-1} \binom{k}{s} x^{k-s}(n-x)^s$. Для нее выполнено

$$f'(x) = kx^{k-1} + \sum_{s=1}^{k-j-1} \binom{k}{s} x^{k-s-1}(n-x)^{s-1}(n(k-s)-kx),$$
$$f''(x) = k(k-1)x^{k-3}((1-k)x + n(k-2)) + \sum_{s=2}^{k-j-1} \binom{k}{s} x^{k-s-2}(n-x)^{s-2} \times$$
$$\times \left[k(k-1)x^2 - 2n(k-1)(k-s)x + n^2(k-s)(k-s-1)\right].$$

Наименьший корень квадратного трехчлена в скобках можно найти явно и оценить следующим образом:

$$x_{\min} = n\frac{(k-1)(k-s) - \sqrt{s(k-1)(k-s)}}{k(k-1)} \geqslant$$

(при $s \leqslant k/2$ минимум данного выражения достигается при $s = k/2$)

$$\geqslant n\frac{k-1-\sqrt{k-1}}{2(k-1)} = \frac{n}{2} - \frac{n}{2\sqrt{k-1}} \geqslant \frac{3n}{8},$$

начиная с $k = 17$. Следовательно, на отрезке $[0, 3n/8]$ функция $f(x)$ возрастает и выпукла вниз. Значит, если все $v_i \in [0, 3n/8]$, то из неравенства Йенсена ($\mathbf{E}\, f(\xi) \geqslant \geqslant f(\mathbf{E}\,\xi)$ для выпуклой вниз функции $f(x)$ и случайной величины ξ) следует искомое соотношение

$$\frac{1}{k!}\sum_{i=1}^{r}\sum_{s=0}^{k-j-1} \binom{k}{s} v_i^{k-s}(n-v_i)^s \geqslant \frac{r}{k!}\sum_{s=0}^{k-j-1} \binom{k}{s} \left(\frac{n}{r}\right)^{k-s} \left(\frac{n(r-1)}{r}\right)^s.$$

Пусть теперь, например, $v_1 > 3n/8$, тогда левая часть в выражении (7) заведомо больше, чем

$$\sum_{s=0}^{k-j-1} \binom{v_1}{k-s}\binom{n-v_1}{s} \geqslant \frac{(v_1-k)^k}{k!} \geqslant \frac{1}{k!}\left(\frac{n}{r}\right)^k \left(\frac{3r}{8} - \frac{kr}{n}\right)^k,$$

в то время как

$$\frac{r}{k!}\sum_{s=0}^{k-j-1} \binom{k}{s} \left(\frac{n}{r}\right)^{k-s} \left(\frac{n(r-1)}{r}\right)^s = \frac{1}{k!}\left(\frac{n}{r}\right)^k r \sum_{s=0}^{k-j-1} \binom{k}{s}(r-1)^s \leqslant$$
$$\leqslant \frac{1}{k!}\left(\frac{n}{r}\right)^k r k^{k-j-1} r^{k-j-1} \sum_{s=0}^{k-j-1} \frac{1}{s!} \leqslant \frac{1}{k!}\left(\frac{n}{r}\right)^k k^{k-j-1} r^{k-j} e.$$

Следовательно, при $r \geqslant 3$ и $k - j < k^{1/4}$, начиная с некоторого $k_0(r)$, неравенство (7) также будет выполнено. ▲

Замечание. Отметим, что доказательство леммы 1 работает и при более слабых ограничениях на разность $k - j$. Например, достаточно потребовать, чтобы $k - j = = o(k/\ln k)$.

Из леммы следует, что выражение в скобках в (6) максимально при почти равных значениях $v_1, \ldots, v_r$, а значит, математическое ожидание числа искомых раскрасок

$H'(n,k,m)$ не превосходит

$$r^n\left(1-\frac{r\sum\limits_{s=0}^{k-j-1}\binom{n/r}{k-s}\binom{n-n/r}{s}}{\binom{n}{k}}+o_n(1)\right)^m\leqslant$$

$$\leqslant r^n\left(1-r^{1-k}\sum_{s=0}^{k-j-1}\binom{k}{s}(r-1)^s+o_n(1)\right)^{\lceil cn\rceil}=$$

$$=\exp\left(n\left[\ln r+c\ln\left(1-r^{1-k}\sum_{s=0}^{k-j-1}\binom{k}{s}(r-1)^s\right)+o_n(1)\right]\right).$$

Заметим, что последнее выражение стремится к нулю с ростом n (а значит, то же самое происходит с вероятностью того, что $\chi_j(H'(n,k,m))\leqslant r$) при $c>\dfrac{-\ln r}{\ln(1-q)}$, где $q=r^{1-k}\sum\limits_{s=0}^{k-j-1}\binom{k}{s}(r-1)^s$. При этом верно, что

$$\frac{-\ln r}{\ln(1-q)}\leqslant\frac{\ln r}{q+q^2/2+q^3/3}\leqslant\frac{\ln r}{q}(1-q/2+q^2/3)=$$

$$=\frac{r^{k-1}\ln r}{\sum\limits_{s=0}^{k-j-1}\binom{k}{s}(r-1)^s}-\frac{\ln r}{2}+\frac{q\ln r}{3}.$$

Учитывая, что $q=O\Big(\binom{k}{j+1}r^{-j}\Big)$, верхняя оценка (4) доказана.

§ 3. Доказательство нижней оценки

Доказательство нижней оценки основывается на методе второго момента. Доказательство будет проведено в несколько шагов и следует идеям из работы [6].

3.1. Точная пороговая вероятность. Необходимым условием для нашего применения метода второго момента является наличие точной пороговой вероятности для свойства $\chi_j(H)\leqslant r$. Напомним, что наличие точной пороговой вероятности означает, что для любых фиксированных r,j,k существует некоторая функция $\widehat{p}=\widehat{p}(n)$, такая что для любого $\varepsilon>0$

$$\mathbf{P}\big(\chi_j(H(n,k,p))\leqslant r\big)\to\begin{cases}1, & \text{если } p<(1-\varepsilon)\widehat{p},\\ 0, & \text{если } p>(1+\varepsilon)\widehat{p}.\end{cases}$$

Для обоснования ее существования воспользуемся следующим результатом из [21].

Теорема 2 [21, теорема 5]. *Пусть $k\geqslant 3$. Пусть $F=(V',E')$ – фиксированный связный k-однородный гиперграф, в котором ребрами выступают произвольные упорядоченные наборы из k вершин (т.е. вершины в ребрах могут повторяться) и который не содержит петель (ребер, в котором все вершины совпадают). Тогда свойство наличие гомоморфизма из случайного гиперграфа $H(n,k,p)$ в F имеет точную пороговую вероятность.*

В нашем случае гиперграф $H(n,k,p)$ обладает свойством $\chi_j(H(n,k,p))\leqslant r$ тогда и только тогда, когда существует гомоморфизм из $H(n,k,p)$ в гиперграф $F=$

$= (V', E')$, где

$$V' = \{1, \dots, r\}, \quad E' = \big\{(a_1, \dots, a_k) : \operatorname{maxcount}(a_1, \dots, a_k) < j + 1\big\},$$

а $\operatorname{maxcount}(a_1, \dots, a_k)$ обозначает максимальное количество одинаковых значений среди $a_1, \dots, a_k$.

В силу существования точной пороговой вероятности достаточно показать, что вероятность наличия рассматриваемого свойства отделена от нуля. Действительно, если для некоторого $c > 0$ мы покажем, что

$$\liminf_{n\to\infty} \mathbf{P}\left(\chi_j\left(H\left(n, k, cn\Big/\binom{n}{k}\right)\right) \leqslant r\right) > 0, \tag{8}$$

то для любого $c' < c$ вероятность $\mathbf{P}\left(\chi_j\left(H\left(n, k, c'n\Big/\binom{n}{k}\right)\right) \leqslant r\right)$ уже будет стремиться к 1, так как величина $c'n\Big/\binom{n}{k}$ будет заведомо меньше пороговой вероятности.

3.2. Снова равномерная модель. При доказательстве нижних оценок мы также будем использовать другую модель случайного гиперграфа. Рассмотрим случайный гиперграф $H''(n, k, m)$, где $m = \lceil cn \rceil$, состоящий из m независимых случайных k-подмножеств множества вершин, причем и в каждом таком k-подмножестве все k вершин выбираются случайно, независимо и равновероятно. В таком гиперграфе ребра могут не только повторяться, но и иметь размер меньше, чем k, т.е. иметь повторяющиеся вершины. Легко убедиться с помощью неравенства Чебышева, что число полных ребер (из k различных вершин) $H''(n, k, m)$ с вероятностью, стремящейся к 1, будет лежать в $O(n^{1/2} \ln n)$-окрестности числа cn. Действительно, эта случайная величина имеет биномиальное распределение $\operatorname{Bin}(m, 1 + O(1/n))$, а потому сильно сконцентрирована вокруг своего среднего значения, равного $cn + O(1)$. Значит, при $c' < c$, вновь используя обозначение $p' = c'n\Big/\binom{n}{k}$,

$$\mathbf{P}\Big(\chi_j(H(n, k, p')) \leqslant r\Big) \geqslant \mathbf{P}\Big(\chi_j(H''(n, k, m)) \leqslant r\Big) + o_n(1).$$

Следовательно, вместо (8) достаточно показать, что выполнено

$$\liminf_{n\to\infty} \mathbf{P}\big(\chi_j(H''(n, k, m)) \leqslant r\big) > 0. \tag{9}$$

Отметим, что при поиске j-правильной раскраски гиперграфа $H''(n, k, m)$ для его неправильных ребер мы также будем требовать отсутствия одноцветного набора из $j + 1$ вершин.

3.3. Подсчет числа раскрасок. Заметим, что с вероятностью, стремящейся к 1 при $n \to \infty$, в рассматриваемом гиперграфе будет много изолированных вершин. С помощью этого факта несложно проверить, что достаточно установить (9) только для подпоследовательности n, кратных r (см. [12, лемма 1.4]). С учетом этого для доказательства неравенства (9) рассмотрим так называемые *сбалансированные* раскраски. Раскраска называется сбалансированной, если все ее цветовые классы имеют одинаковую мощность. Пусть X_n – количество j-правильных сбалансированных раскрасок случайного гиперграфа $H''(n, k, m)$ в r цветов, тогда

$$\mathbf{P}\big(\chi_j(H''(n, k, m)) \leqslant r\big) \geqslant \mathbf{P}(X_n > 0),$$

а в силу неравенства Пэли – Зигмунда

$$\mathbf{P}(X_n > 0) \geqslant \frac{(\mathbf{E}\, X_n)^2}{\mathbf{E}\, X_n^2}.$$

Таким образом, остается показать, что

$$\mathbf{E}\, X_n^2 = O_{k,j,r}((\mathbf{E}\, X_n)^2). \tag{10}$$

3.4. Подсчет моментов. Найдем первый момент числа j-правильных сбалансированных раскрасок

$$\mathbf{E}\, X_n = \frac{n!}{((n/r)!)^r}(1-q)^{\lceil cn\rceil} = \Theta_{k,j,r}\big(n^{-(r-1)/2}\exp(n[\ln r + c\ln(1-q)])\big), \tag{11}$$

где величина q означает вероятность того, что при фиксированной сбалансированной раскраске хотя бы $j+1$ вершин случайного ребра будут покрашены в один и тот же цвет. Эту вероятность нетрудно вычислить аналитически. По условию теоремы $k - j < k^{1/4} < k/2$, и значит, подобный одноцветный набор вершин может быть только один. Так как раскраска сбалансированная, то вероятность того, что случайно выбранная вершина окажется окрашенной в какой-либо конкретный цвет, равна $1/r$. Тогда вероятность того, что при случайном независимом равновероятном выборе k вершин ребра ровно s вершин окажутся именно этого цвета, равна $r^{-k}\binom{k}{s}(r-1)^{k-s}$. Учитывая все цвета и суммируя по всем s, не меньшим чем $j+1$, получим

$$q = r^{1-k}\sum_{s=j+1}^{k}\binom{k}{s}(r-1)^{k-s} = r^{1-k}\sum_{s=0}^{k-j-1}\binom{k}{s}(r-1)^{s}.$$

Мы уже вводили это обозначение в конце § 2. Множитель $\dfrac{n!}{((n/r)!)^r}$ соответствует числу всех сбалансированных раскрасок в r цветов. Величина $1-q$ означает вероятность того, что в сбалансированной раскраске никакие $j+1$ вершин случайного ребра не будут покрашены в один цвет. Так как ребра выбираются независимо, то данную величину необходимо возвести в степень, равную количеству ребер, т.е. $\lceil cn\rceil$.

Второй момент вычисляется несколько сложнее. Для краткости будем называть ребро *плохим* в некоторой раскраске, если оно имеет хотя бы $j+1$ вершин одного и того же цвета. Пусть τ_1, τ_2 – две сбалансированные раскраски, а e – случайное ребро гиперграфа $H''(n,k,m)$. Найдем вероятность того, что в обеих раскрасках никакой набор e из $j+1$ вершин не покрашен в один и тот же цвет. Для этого рассмотрим класс $\mathcal{A}$ матриц размера $r\times r$, у которых все элементы являются целыми неотрицательными числами, а сумма в каждой строке и в каждом столбце равна n/r. Матрицы такого вида отлично представляют собой пары r-цветных сбалансированных раскрасок вершин гиперграфа $H''(n,k,m)$. Если $A\in\mathcal{A}$, $A=(a_{iu}, i,u=1,\dots,r)$, то будем считать что a_{iu} – это число вершин, имеющих цвет i в раскраске τ_1 и цвет u в раскраске τ_2. Для раскрасок τ_1,τ_2 вероятность того, что e будет раскрашено плохо хотя бы в одной из них, зависит лишь от матрицы A. Обозначим эту вероятность через $\mathcal{Q}(A)$. Далее, матрица $A\in\mathcal{A}$ представляет

$$\frac{n!}{\prod\limits_{i,u=1}^{r} a_{iu}!}$$

пар сбалансированных раскрасок. Вероятность того, что и τ_1, и τ_2 являются j-правильными раскрасками $H''(n,k,m)$, равна $(1-\mathcal{Q}(A))^{\lceil cn\rceil}$. Стало быть, второй момент случайной величины X_n будет равен

$$\mathbf{E}\, X_n^2 = n!\sum_{A\in\mathcal{A}}\left(\prod_{i,u=1}^{r} a_{iu}!\right)^{-1}(1-\mathcal{Q}(A))^{\lceil cn\rceil}. \tag{12}$$

Осталось найти $\mathcal{Q}(A)$. Напомним, что вероятность того, что случайное ребро является плохим в раскраске τ_i, $i = 1, 2$, равна q. Теперь рассмотрим событие, при котором ребро будет плохим в обеих раскрасках, а именно событие, состоящее в том, что ребро содержит хотя бы $j + 1$ вершин цвета i в первой раскраске и хотя бы $j + 1$ вершин цвета u во второй раскраске. Пусть s – число вершин ребра, покрашенных в цвет i в первой раскраске, t – число вершин ребра, покрашенных в первой раскраске в цвет i, а во второй – в любой цвет, кроме u, и наконец, h – число вершин ребра, покрашенных во второй раскраске в цвет u, а в первой – в любой цвет, кроме цвета i. Тогда в ребре во второй раскраске будет ровно $h + s - t$ вершин цвета u. Интересующее нас событие имеет место быть, если и только если

$$j + 1 \leqslant s \leqslant k, \quad 0 \leqslant h \leqslant k - s, \quad h + s - t \geqslant j + 1. \tag{13}$$

Последнее вытекает из того, что во второй раскраске должно быть не менее $j + 1$ вершин цвета u. Далее, в силу свойств матрицы A

- каждая вершина цвета i в первой раскраске и цвета u во второй может быть выбрана a_{iu} способами, всего таких вершин $s - t$;
- каждая вершина цвета i в первой раскраске и не цвета u во второй может быть выбрана $n/r - a_{iu}$ способами, всего таких вершин t;
- каждая вершина не цвета i в первой раскраске и цвета u во второй может быть выбрана $n/r - a_{iu}$ способами, всего таких вершин h;
- наконец, вершина не цвета i в первой раскраске и не цвета u во второй может быть выбрана по формуле включений и исключений $\dfrac{n(r-2)}{r} + a_{iu}$ способами, всего таких вершин $k - h - s$.

Тогда вероятность искомого события будет равна

$$\sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} \times$$
$$\times \left(\frac{\frac{n}{r} - a_{iu}}{n} \right)^{h+t} \left(\frac{a_{iu}}{n} \right)^{s-t} \left(\frac{\frac{n(r-2)}{r} + a_{iu}}{n} \right)^{k-h-s}.$$

Осталось просуммировать по всем i и u. Таким образом, вероятность $\mathcal{Q}(A)$ того, что ребро будет плохим хотя бы в одной из раскрасок, будет равна

$$\mathcal{Q}(A) = 2q - \sum_{i,u=1}^{r} \sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} \times$$
$$\times \left(\frac{\frac{n}{r} - a_{iu}}{n} \right)^{h+t} \left(\frac{a_{iu}}{n} \right)^{s-t} \left(\frac{\frac{n(r-2)}{r} + a_{iu}}{n} \right)^{k-h-s}. \tag{14}$$

Теперь, применяя оценки Стирлинга вида $x! = \Theta((x/e)^x \sqrt{x+1})$ к выражению в (12), получим

$$\mathbf{E}\, X_n^2 = \Theta_{k,j,r} \left(n^{1/2} \sum_{A \in \mathcal{A}} \left(\prod_{i,u=1}^{r} \sqrt{a_{iu} + 1} \right)^{-1} \times \right.$$
$$\left. \times \exp\left(n \left[- \sum_{i,u=1}^{r} \left(\frac{a_{iu}}{n} \right) \ln \left(\frac{a_{iu}}{n} \right) + c \ln\left(1 - \mathcal{Q}(A)\right) \right] \right) \right). \tag{15}$$

Введем следующие обозначения: для $A \in \mathcal{A}$

$$\mathcal{H}(A) = -\sum_{i,u=1}^{r} \frac{a_{iu}}{n} \ln \frac{r a_{iu}}{n},$$
$$\mathcal{E}(A) = \ln(1 - \mathcal{Q}(A)).$$

Для $c > 0$ обозначим $\mathcal{G}_c(A) = \mathcal{H}(A) + c\mathcal{E}(A)$. Дальнейшая наша цель будет состоять в обосновании того факта, что в условиях теоремы функция $\mathcal{G}_c(A)$ достигает своего максимума при $A = J_r$, где J_r – матрица, все элементы которой равны n/r^2. Для этого сначала вычислим $\mathcal{G}_c(J_r)$.

Утверждение 1. *Для любых $r, k, j \in \mathbb{N}$, таких что $k/2 < j < k$, выполнено*

$$\mathcal{G}_c(J_r) = \ln r + c \ln(1 - q)^2.$$

Кроме того, имеет место тождество

$$\sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} \left(\frac{1}{r} - \frac{1}{r^2}\right)^{h+t} \left(\frac{1}{r^2}\right)^{s-t} \left(\frac{(r-1)^2}{r^2}\right)^{k-h-s} = \frac{q^2}{r^2}.$$

Доказательство утверждения 1 сугубо техническое, мы приведем его в § 6, а пока продолжим рассуждения.

Из (11), (12) и утверждения 1 получаем следующую оценку $\mathbf{E}\, X_n^2$:

$$\mathbf{E}\, X_n^2 = \Theta_{k,j,r}\left((\mathbf{E}\, X_n)^2 n^{r-1/2} \sum_{A \in \mathcal{A}} \left(\prod_{i,u=1}^{r} \sqrt{a_{iu}+1} \right)^{-1} \times \right.$$
$$\left. \times \exp\left(n \left[-\sum_{i,u=1}^{r} \frac{a_{iu}}{n} \ln \frac{a_{iu}}{n} + c \ln(1 - \mathcal{Q}(A)) - \ln r^2 - c \ln(1-q)^2 \right] \right) \right) =$$
$$= \exp\left(n \left[-\sum_{i,u=1}^{r} \frac{a_{iu}}{n} \ln \frac{r a_{iu}}{n} + c \ln(1 - \mathcal{Q}(A)) - \mathcal{G}_c(J_r) \right] \right) \Bigg) =$$
$$= \Theta_{k,j,r}\left((\mathbf{E}\, X_n)^2 n^{r-1/2} \sum_{A \in \mathcal{A}} \left(\prod_{i,u=1}^{r} \sqrt{a_{iu}+1} \right)^{-1} \exp\Big(n \big[\mathcal{G}_c(A) - \mathcal{G}_c(J_r) \big] \Big) \right).$$

Для завершения доказательства нам понадобится следующая

Лемма 2. *Если выполнено условие* (5), *то существует функция $b = b(k, r) > 0$, такая что для любой матрицы $A = (a_{iu},\ i, u = 1, \ldots, r)$ из $\mathcal{A}$ выполнено*

$$\mathcal{G}_c(J_r) - \mathcal{G}_c(A) \geqslant b \sum_{i,u=1}^{r} \left(\frac{a_{iu}}{n} - \frac{1}{r^2} \right)^2. \tag{16}$$

Иными словами, на матрицах класса $\mathcal{A}$ максимальное значение $\mathcal{G}_c$ достигается именно на матрице J_r. Доказательство леммы будет приведено в следующем параграфе, а здесь заметим, что для любого $a_{iu} = 0, \ldots, n/r$ выполнено

$$\big(\sqrt{a_{iu}+1}\big)^{-1} e^{-nb\left(\frac{a_{iu}}{n} - \frac{1}{r^2}\right)^2} = O_{k,j,r}\big(n^{-1/2}\big).$$

Применяя эту оценку ко всем парам i, u, таким что $\max(i,u) = r$, а также лемму 2, можно оценить второй момент случайной величины X_n следующим образом:

$$\mathbf{E}\, X_n^2 = O_{k,j,r}\left((\mathbf{E}\, X_n)^2 \sum_{A\in\mathcal{A}} \prod_{i,u=1}^{r-1} \left(\sqrt{a_{iu}+1}\right)^{-1} e^{-nb\left(\frac{a_{iu}}{n}-\frac{1}{r^2}\right)^2} \right).$$

Учитывая, что числа $(a_{iu},\ i,u = 1,\ldots,r-1)$ однозначно определяют матрицу A, полученная сумма по матрицам не превосходит полной суммы по всем значениям a_{iu}, $i,u = 1,\ldots,r-1$, от 0 до n/r. Стало быть,

$$\mathbf{E}\, X_n^2 = O_{k,j,r}\left((\mathbf{E}\, X_n)^2 \left(\sum_{a=0}^{n/r} \frac{1}{\sqrt{a+1}} e^{-nb\left(\frac{a}{n}-\frac{1}{r^2}\right)^2} \right)^{(r-1)^2} \right).$$

Следовательно,

$$\mathbf{E}\, X_n^2 \leqslant O_{k,j,r}\left((\mathbf{E}\, X_n)^2 \left(\int_0^{\infty} \frac{1}{\sqrt{x+1}} e^{-nb\left(\frac{x}{n}-\frac{1}{r^2}\right)^2} dx \right)^{(r-1)^2} \right) = O_{k,j,r}\left((\mathbf{E}\, X_n)^2 \right)$$

в силу того, что $\int\limits_0^{\infty} \frac{1}{\sqrt{x+1}} e^{-nb(x/n-1/r^2)^2} dx = O_{k,r}(1)$. Значит, неравенство (10) выполнено и нижняя оценка доказана. Осталось лишь доказать лемму 2, чему и будет посвящен следующий параграф.

§ 4. Доказательство леммы 2

В этом параграфе мы покажем справедливость неравенства (16). Из формулировки видно, что нам будет удобно также пользоваться "заменой" $\varepsilon_{iu} = \dfrac{a_{iu}}{n} - \dfrac{1}{r^2}$, $i,u = 1,\ldots,r$. В данных обозначениях (16) можно переформулировать следующим образом:

$$\begin{aligned}
&\mathcal{G}_c(J_r) - \mathcal{G}_c(A) = \ln r + c(1-q)^2 + \sum_{i,u=1}^{r} \frac{a_{iu}}{n} \ln \frac{r a_{iu}}{n} - c\ln(1-\mathcal{Q}(A)) = \\
&= \sum_{i,u=1}^{r} \frac{a_{iu}}{n} \ln \frac{r^2 a_{iu}}{n} - c\ln\left(\frac{1-\mathcal{Q}(A)}{(1-q)^2}\right) = \\
&= \sum_{i,u=1}^{r} \left(\frac{1}{r^2} + \varepsilon_{iu}\right) \ln(1+r^2\varepsilon_{iu}) - c\ln\left(1 + \frac{-\mathcal{Q}(A) + 2q - q^2}{(1-q)^2}\right). \qquad (17)
\end{aligned}$$

В силу (14) величина $\mathcal{Q}(A) - 2q + q^2$ будет равна

$$\begin{aligned}
&-\mathcal{Q}(A) + 2q - q^2 = \sum_{i,u=1}^{r} \sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} \times \\
&\times \left(\frac{1}{r} - \frac{1}{r^2} - \varepsilon_{iu}\right)^{h+t} \left(\frac{1}{r^2} + \varepsilon_{iu}\right)^{s-t} \left(\frac{(r-1)^2}{r^2} + \varepsilon_{iu}\right)^{k-h-s} - q^2. \qquad (18)
\end{aligned}$$

Введем матрицу $\Upsilon = (\varepsilon_{iu},\ i,u = 1,\ldots,r)$ и отметим ее свойства: все элементы принадлежат отрезку $[-1/r^2, 1/r - 1/r^2]$, а также суммы элементов по всем строкам

и столбцам равны нулю, т.е. формально – для любых $i, u = 1, \ldots, r$

$$\varepsilon_{iu} \in \left[-\frac{1}{r^2}, \frac{1}{r} - \frac{1}{r^2}\right], \quad \sum_{i'=1}^{r} \varepsilon_{i'u} = 0, \quad \sum_{u'=1}^{r} \varepsilon_{iu'} = 0. \tag{19}$$

Неравенство (16) можно переформулировать так: существует такая $b = b(k, r)$, что для любой матрицы $\Upsilon = (\varepsilon_{iu},\ i, u = 1, \ldots, r)$ со свойствами (19) выполнено

$$\mathcal{G}_c(J_r) - \mathcal{G}_c(A) \geqslant b \sum_{i,u=1}^{r} \varepsilon_{iu}^2.$$

Рассмотрим следующие функции строк для каждого $i = 1, \ldots, r$:

$$\mathcal{H}_i(\Upsilon) = \sum_{u=1}^{r} \left(\frac{1}{r^2} + \varepsilon_{iu}\right) \ln\left(1 + r^2 \varepsilon_{iu}\right),$$

$$\mathcal{E}_i(\Upsilon) = \frac{1}{(1-q)^2} \left[\sum_{u=1}^{r} \sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} \times \right.$$

$$\left. \times \left(\frac{1}{r} - \frac{1}{r^2} - \varepsilon_{iu}\right)^{h+t} \left(\frac{1}{r^2} + \varepsilon_{iu}\right)^{s-t} \left(\frac{(r-1)^2}{r^2} + \varepsilon_{iu}\right)^{k-h-s} - q^2/r \right].$$

Из (17), (18) получаем, что

$$\mathcal{G}_c(J_r) - \mathcal{G}_c(A) = \sum_{i=1}^{r} \mathcal{H}_i(\Upsilon) - c \ln\left(1 + \sum_{i=1}^{r} \mathcal{E}_i(\Upsilon)\right) \geqslant \sum_{i=1}^{r} \big(\mathcal{H}_i(\Upsilon) - c\mathcal{E}_i(\Upsilon)\big). \tag{20}$$

Далее будем исследовать разность $\mathcal{H}_i(\Upsilon) - c\mathcal{E}_i(\Upsilon)$. Будем классифицировать строки матрицы Υ на центральные, хорошие и плохие в зависимости от максимального значения элементов следующим образом:

- строка с номером i – *центральная*, если

$$0 \leqslant \max_{u=1,\ldots,r} \varepsilon_{iu} < \frac{1}{r} - \frac{1}{r^2} - \frac{1}{rk^{2/3}};$$

- строка с номером i – *хорошая*, если

$$\max_{u=1,\ldots,r} \varepsilon_{iu} \in \left[\frac{1}{r} - \frac{1}{r^2} - \frac{1}{rk^{2/3}}, \frac{1}{r} - \frac{1}{r^2} - r^{-2k/3}\right];$$

- строка с номером i – *плохая*, если

$$\max_{u=1,\ldots,r} \varepsilon_{iu} \in \left(\frac{1}{r} - \frac{1}{r^2} - r^{-2k/3}, \frac{1}{r} - \frac{1}{r^2}\right].$$

Начнем с анализа центральных строк.

4.1. Центральные строки.

Утверждение 2. *Для центральной строки с номером i выполнено*

$$\mathcal{H}_i(\Upsilon) - c\mathcal{E}_i(\Upsilon) \geqslant \frac{r^2}{4} \sum_{u:\, \varepsilon_{iu} < 0} \varepsilon_{iu}^2 + a(r) \sum_{u:\, \varepsilon_{iu} \geqslant 0} \varepsilon_{iu}^2, \tag{21}$$

где $a(r) > 0$ – некоторая положительная функция от r.

Доказательство. Вначале оценим $\mathcal{H}_i(\Upsilon)$. В сумме $\mathcal{H}_i(\Upsilon)$ оценим слагаемые $(1/r^2+\varepsilon_{iu})\ln(1+r^2\varepsilon_{iu})$ по-разному в зависимости от ε_{iu}.

Случай 1. Если $\varepsilon_{iu}<0$, то используем оценки функции $\varphi(x)=(1+x)\ln(1+x)$ при $x>-1$, про которую известно, что

$$\varphi(x)>x+\frac{x^2}{2}\quad\text{для } x<0.$$

Тогда для $x=r^2\varepsilon_{iu}$

$$(1/r^2+\varepsilon_{iu})\ln(1+r^2\varepsilon_{iu})\geqslant\varepsilon_{iu}+\frac{r^2}{2}\varepsilon_{iu}^2. \tag{22}$$

Отметим, что неравенство (22) верно и при $\varepsilon_{iu}=-1/r^2$.

Случай 2. Если $\varepsilon_{iu}>0$, но $\varepsilon_{iu}\leqslant 1/(r\ln r)-1/r^2$, то снова используем оценки функции $\varphi(x)=(1+x)\ln(1+x)$, про которую известно, что

$$\varphi(x)>x+\frac{x^2}{2(1+x/3)}\quad\text{для } x>0.$$

Тогда при $x=r^2\varepsilon_{iu}$

$$(1/r^2+\varepsilon_{iu})\ln(1+r^2\varepsilon_{iu})\geqslant\varepsilon_{iu}+\frac{r^2\varepsilon_{iu}^2}{2(1+r^2\varepsilon_{iu}/3)}\geqslant$$

(оценим знаменатель $1+r^2\varepsilon_{iu}/3<1+r/(3\ln r)-1/3<2r/(3\ln r)$)

$$\geqslant\varepsilon_{iu}+\frac{3r\ln r}{4}\varepsilon_{iu}^2.$$

Случай 3. Наконец, если же $\varepsilon_{iu}>1/(r\ln r)-1/r^2$, то оценим слагаемое следующим образом:

$$(1/r^2+\varepsilon_{iu})\ln(1+r^2\varepsilon_{iu})\geqslant(1/r^2+\varepsilon_{iu})\ln\Big(\frac{r}{\ln r}\Big)\geqslant$$
$$\geqslant\varepsilon_{iu}+\varepsilon_{iu}(\ln r-\ln\ln r-1)\geqslant$$

(воспользуемся тем, что $1\geqslant r\varepsilon_{iu}\left(1-\frac{1}{r}-\frac{1}{k^{2/3}}\right)^{-1}$)

$$\geqslant\varepsilon_{iu}+r\varepsilon_{iu}^2\left(1-\frac{1}{r}-\frac{1}{k^{2/3}}\right)^{-1}(\ln r-\ln\ln r-1).$$

Тем самым, в силу (19)

$$\mathcal{H}_i(\Upsilon)=\sum_{u=1}^{r}(1/r^2+\varepsilon_{iu})\ln(1+r^2\varepsilon_{iu})\geqslant\sum_{u=1}^{r}\varepsilon_{iu}+\frac{r^2}{2}\sum_{u:\,\varepsilon_{iu}<0}\varepsilon_{iu}^2+$$
$$+\min\left(\frac{3r\ln r}{4},r\left(1-\frac{1}{r}-\frac{1}{k^{2/3}}\right)^{-1}(\ln r-\ln\ln r-1)\right)\sum_{u:\,\varepsilon_{iu}>0}\varepsilon_{iu}^2=$$
$$=\frac{r^2}{2}\sum_{u:\,\varepsilon_{iu}<0}\varepsilon_{iu}^2+\min\left(\frac{3r\ln r}{4},r\left(1-\frac{1}{r}-\frac{1}{k^{2/3}}\right)^{-1}(\ln r-\ln\ln r-1)\right)\sum_{u:\,\varepsilon_{iu}>0}\varepsilon_{iu}^2.$$

Далее оценим $c\mathcal{E}_i(\Upsilon)$ сверху. Данная величина является полиномом относительно ε_{iu}, причем в силу утверждения 1 свободный член в этом многочлене равен нулю.

Заметим также, что данный полином симметричен относительно ε_{iu} по u при фиксированном i в силу инвариантности задачи при переобозначении цветовых классов. Из свойств (19) матрицы Υ следует, что $\sum\limits_{u=1}^{r} \varepsilon_{iu} = 0$, поэтому остается рассматривать лишь коэффициенты при степенях ε_{iu} от второй и выше. Тогда $\mathcal{E}_i(\Upsilon)$ можно оценить следующим образом:

$$\mathcal{E}_i(\Upsilon) \leqslant \frac{1}{(1-q)^2} \sum_{u=1}^{r} \sum_{v=2}^{k} \binom{k}{v} r^{2v} |\varepsilon_{iu}|^v \times$$
$$\times \left[\sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} \left(\frac{1}{r} - \frac{1}{r^2}\right)^{h+t} \left(\frac{1}{r^2}\right)^{s-t} \left(\frac{(r-1)^2}{r^2}\right)^{k-h-s} \right].$$

Прокомментируем неравенство. Коэффициент $\binom{k}{v}$ получен исходя из того, что из всех множителей вида $\left(\frac{1}{r} - \frac{1}{r^2} - \varepsilon_{iu}\right)$, $\left(\frac{1}{r^2} + \varepsilon_{iu}\right)$ и $\left(\frac{(r-1)^2}{r^2} + \varepsilon_{iu}\right)$ в выражении для $\mathcal{E}_i(\Upsilon)$ ровно в v случаях из k нужно взять ε_{iu} или $-\varepsilon_{iu}$. При этом мы получим коэффициент вида

$$\left(\frac{1}{r} - \frac{1}{r^2}\right)^{h+t-\alpha} \left(\frac{1}{r^2}\right)^{s-t-\beta} \left(\frac{(r-1)^2}{r^2}\right)^{k-h-s-\gamma},$$

где $\alpha + \beta + \gamma = v$. Ясно, что каждый подобный коэффициент не превосходит

$$r^{2v} \left(\frac{1}{r} - \frac{1}{r^2}\right)^{h+t} \left(\frac{1}{r^2}\right)^{s-t} \left(\frac{(r-1)^2}{r^2}\right)^{k-h-s}.$$

Так как мы оцениваем сверху, то не берем в расчет знак ε_{iu} и рассматриваем только абсолютное значение $|\varepsilon_{iu}|$. Далее, используя утверждение 1, получаем оценку

$$\mathcal{E}_i(\Upsilon) \leqslant \frac{1}{(1-q)^2} \sum_{u=1}^{r} \sum_{v=2}^{k} \binom{k}{v} r^{2v-2} q^2 |\varepsilon_{iu}|^v.$$

Если $\varepsilon_{iu} < 0$, то его модуль в силу (19) не превосходит $1/r^2$, а в противном случае $\varepsilon_{iu} < \frac{1}{r} - \frac{1}{r^2} - \frac{1}{rk^{2/3}}$. Следовательно,

$$c\mathcal{E}_i(\Upsilon) \leqslant \frac{c}{(1-q)^2} \left[\sum_{u:\, \varepsilon_{iu}<0} \varepsilon_{iu}^2 \sum_{v=2}^{k} \binom{k}{v} r^2 q^2 + \right.$$
$$\left. + \sum_{u:\, \varepsilon_{iu}>0} \varepsilon_{iu}^2 \sum_{v=2}^{k} \binom{k}{v} r^{2v-2} \left(\frac{1}{r} - \frac{1}{r^2} - \frac{1}{rk^{2/3}}\right)^{v-2} q^2 \right] \leqslant$$
$$\leqslant \frac{cq^2}{(1-q)^2} \left[\sum_{u:\, \varepsilon_{iu}<0} \varepsilon_{iu}^2 \sum_{v=2}^{k} \binom{k}{v} r^2 + \right.$$
$$\left. + \sum_{u:\, \varepsilon_{iu}>0} \varepsilon_{iu}^2 r^{2k-2} \left(\frac{1}{r} - \frac{1}{r^2} - \frac{1}{rk^{2/3}}\right)^{-2} \left(\frac{1}{r} - \frac{1}{rk^{2/3}}\right)^{k} \right] \leqslant$$

(пользуясь тем, что $c < \ln r/q$ по условию (5))

$$\leqslant \frac{q\ln r}{(1-q)^2}\left[\sum_{u\colon \varepsilon_{iu}<0}\varepsilon_{iu}^2 2^k r^2 + r^k \sum_{u\colon \varepsilon_{iu}>0}\varepsilon_{iu}^2\left(1-\frac{1}{r}-\frac{1}{k^{2/3}}\right)^{-2}\left(1-\frac{1}{k^{2/3}}\right)^k\right]\leqslant$$

(так как начиная с некоторого k выполнено $\left(1-\frac{1}{k^{2/3}}\right)^k \leqslant e^{-k^{1/3}}$)

$$\leqslant \frac{qr^2 2^k \ln r}{(1-q)^2}\sum_{u\colon \varepsilon_{iu}<0}\varepsilon_{iu}^2 + \frac{qr^k \ln r\left(1-\frac{1}{r}-\frac{1}{k^{2/3}}\right)^{-2} e^{-k^{1/3}}}{(1-q)^2}\sum_{u\colon \varepsilon_{iu}>0}\varepsilon_{iu}^2.$$

Остается оценить коэффициенты при $\sum\limits_{u\colon \varepsilon_{iu}<0}\varepsilon_{iu}^2$ и $\sum\limits_{u\colon \varepsilon_{iu}>0}\varepsilon_{iu}^2$ с помощью следующего технического утверждения, доказательство которого вынесено в § 6.

Утверждение 3. *Для любого $r>3$ существует такое $k_0=k_0(r)$, что для всех $k,j\in\mathbb{N}$, таких что $k-j<k^{1/4}$ и $k>k_0$, выполнены следующие неравенства*:

$$\frac{qr^2 2^k \ln r}{(1-q)^2}\leqslant\frac{r^2}{4},\quad \frac{qr^k \ln r\left(1-\frac{1}{r}-\frac{1}{k^{2/3}}\right)^{-2} e^{-k^{1/3}}}{(1-q)^2} < e^{-10} r\ln r.$$

Из вышеприведенного утверждения следует, что коэффициент при $\sum\limits_{u\colon \varepsilon_{iu}>0}\varepsilon_{iu}^2$ не превосходит $e^{-10}r\ln r$, что сильно меньше $\frac{3r\ln r}{8}$. Кроме того, выполнено

$$e^{-10}r\ln r < \frac{1}{2}r(\ln r-\ln\ln r-1).$$

В итоге из оценок $\mathcal{H}_i(\Upsilon)$ и $c\mathcal{E}_i(\Upsilon)$ следует, что при достаточно большом k

$$\mathcal{H}_i(\Upsilon)-c\mathcal{E}_i(\Upsilon)\geqslant\frac{r^2}{4}\sum_{u\colon \varepsilon_{iu}<0}\varepsilon_{iu}^2 +$$
$$+\min\left(\frac{3r\ln r}{8},\frac{1}{2}r\left(1-\frac{1}{r}-\frac{1}{k^{2/3}}\right)^{-1}(\ln r-\ln\ln r-1)\right)\sum_{u\colon \varepsilon_{iu}>0}\varepsilon_{iu}^2.$$

4.2. Хорошие строки. Строку с номером i мы называем хорошей, если нашелся такой u_0, что

$$\varepsilon_{iu_0}=\max_{u=1,\dots,r}\varepsilon_{iu}\in\left[\frac{1}{r}-\frac{1}{r^2}-\frac{1}{rk^{2/3}},\frac{1}{r}-\frac{1}{r^2}-r^{-2k/3}\right].$$

Для простоты будем считать, что $u_0=1$. Введем параметр $\delta_i=\frac{1}{r}-\frac{1}{r^2}-\varepsilon_{i1}$. Тогда $\delta_i\in[r^{-2k/3},\frac{1}{rk^{2/3}}]$. Далее, обозначим $\delta_{iu}=\frac{1}{r^2}+\varepsilon_{iu}$, $u>1$. Отметим, что $\delta_{iu}\geqslant 0$ и $\sum\limits_{u=2}^{r}\delta_{iu}=\delta_i$ в силу (19).

Рассмотрим $\mathcal{H}_i(\Upsilon)$ и $\mathcal{E}_i(\Upsilon)$ как функции от δ_i,δ_{iu}. Нам достаточно показать, что $\mathcal{H}_i(\Upsilon)$ и $c\mathcal{E}_i(\Upsilon)$ отличаются на некоторую величину $a=a(k,r)>0$. Имеем

$$\mathcal{H}_i(A)=(1/r-\delta_i)\ln(r-r^2\delta_i)+\sum_{u=2}^{r}\delta_{iu}\ln(r^2\delta_{iu})=$$
$$=\frac{\ln r}{r}-\delta_i\ln r+(1/r-\delta_i)\ln(1-r\delta_i)+2\sum_{u=2}^{r}\delta_{iu}\ln r+\sum_{u=2}^{r}\delta_{iu}\ln\delta_{iu}\geqslant$$

(вспомним, что $\sum\limits_{u=2}^{r}\delta_{iu}=\delta_i$, поэтому последняя сумма в силу неравенства Йенсена для функции $f(x)=x\ln x$ не меньше $-\ln(r-1)\delta_i+\delta_i\ln\delta_i$)

$$\geqslant \frac{\ln r}{r}+\delta_i\ln r+(1/r-\delta_i)\ln(1-r\delta_i)-\delta_i\ln(r-1)+\delta_i\ln\delta_i\geqslant$$

(воспользуемся тем, что $\ln(1-r\delta_i)>(-r\delta_i)/(1-r\delta_i)$)

$$\geqslant \frac{\ln r}{r}+\delta_i\ln\delta_i+\delta_i\ln\left(\frac{r}{r-1}\right)-\delta_i. \tag{23}$$

Оценим величину $c\mathcal{E}_i(\Upsilon)$ сверху. Выпишем сперва ее как функцию от величин δ_{iu}, $u=1,\dots,r$:

$$\begin{aligned}
c\mathcal{E}_i(\Upsilon)&=\frac{c}{(1-q)^2}\left[\sum_{u=1}^{r}\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}\sum_{t=0}^{s-j-1+h}k-sh\binom{s}{t}\times\right.\\
&\left.\times\left(\frac{1}{r}-\frac{1}{r^2}-\varepsilon_{iu}\right)^{h+t}\left(\frac{1}{r^2}+\varepsilon_{iu}\right)^{s-t}\left(\frac{(r-1)^2}{r^2}+\varepsilon_{iu}\right)^{k-h-s}-q^2/r\right]=\\
&=\frac{c}{(1-q)^2}\left[\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}\sum_{t=0}^{s-j-1+h}\binom{k-s}{h}\binom{s}{t}\delta_i^{h+t}\left(\frac{1}{r}-\delta_i\right)^{s-t}\times\right.\\
&\times\left(\frac{r-1}{r}-\delta_i\right)^{k-h-s}+\sum_{u=2}^{r}\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}\sum_{t=0}^{s-j-1+h}\binom{k-s}{h}\binom{s}{t}\times\\
&\left.\times\left(\frac{1}{r}-\delta_{iu}\right)^{h+t}\delta_{iu}^{s-t}\left(\frac{r-2}{r}+\delta_{iu}\right)^{k-h-s}-q^2/r\right].
\end{aligned}\tag{24}$$

Выражение в правой части (24) содержит две группы вложенных сумм. Их можно оценить следующим образом. Сразу отметим, что приведенные оценки пригодятся и для случая плохих строк.

Утверждение 4. *Если $r,k,j\in\mathbb{N}$ таковы, что $1<k-j<k^{1/4}$, $r>2$ и k достаточно велико по отношению к r, то для любой хорошей или плохой строки с номером i выполнено следующее неравенство*:

$$\begin{aligned}
&\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}\sum_{t=0}^{s-j-1+h}\binom{k-s}{h}\binom{s}{t}\delta_i^{h+t}\left(\frac{1}{r}-\delta_i\right)^{s-t}\left(\frac{r-1}{r}-\delta_i\right)^{k-h-s}\leqslant\\
&\leqslant q(1-r\delta_i)^{2j+2-k}\bigl(1+\delta_i O(k^{7/12})\bigr)/r.
\end{aligned}$$

Утверждение 5. *Если $r,k,j\in\mathbb{N}$ таковы, что $1<k-j<k^{1/4}$, $r>2$ и k достаточно велико по отношению к r, то для любой хорошей или плохой строки с номером i выполнено следующее неравенство*:

$$\begin{aligned}
&\sum_{u=2}^{r}\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}\sum_{t=0}^{s-j-1+h}\binom{k-s}{h}\binom{s}{t}\left(\frac{1}{r}-\delta_{iu}\right)^{h+t}\delta_{iu}^{s-t}\left(\frac{r-2}{r}+\delta_{iu}\right)^{k-h-s}\leqslant\\
&\leqslant q(r\delta_i)^{2j+2-k}k^{9(k-j-1)/4}(1+2/k)^2/r.
\end{aligned}$$

Доказательства утверждений 4 и 5 мы приведем в § 6. А сейчас воспользуемся ими и продолжим анализ хороших строк.

С помощью утверждений 4 и 5, а также неравенства $c < \ln r/q$ (см. условие (5)) получаем из (24) следующую оценку величины $c\mathcal{E}_i(\Upsilon)$:

$$c\mathcal{E}_i(\Upsilon) \leqslant \frac{\ln r}{r(1-q)^2}\Big[(1-r\delta_i)^{2j+2-k}\big(1+\delta_i O(k^{7/12})\big) + \\ + (r\delta_i)^{2j+2-k}k^{9(k-j-1)/4}(1+2/k)^2\Big]. \tag{25}$$

Теперь оценим разность $\mathcal{H}_i(\Upsilon) - c\mathcal{E}_i(\Upsilon)$.

Случай 1. Пусть сначала $r\delta_i > \frac{1}{3k}$. Так как $\delta_i = O\Big(\frac{1}{rk^{2/3}}\Big)$, то $\delta_i \ln \delta_i = O\Big(\frac{\ln k}{rk^{2/3}}\Big)$. Значит, в силу (23) при достаточно большом k выполнено $\mathcal{H}_i(\Upsilon) \geqslant 0{,}85\frac{\ln r}{r}$.

Далее, раз $r\delta_i \leqslant k^{-2/3}$, то для всех достаточно больших k выполнено $r\delta_i < \frac{1}{40}$. Оценим сразу остаточные члены в (25):

$$\delta_i k^{7/12} \leqslant k^{-1/12},$$
$$(r\delta_i)^{2j+2-k}k^{9(k-j-1)/4}(1+2/k)^2 = O\big(k^{-2/3(2j+2-k)}k^{9(k-j-1)/4}\big) = \\ = k^{-4/3k+O(k^{1/4})} < 0{,}0001$$

для всех достаточно больших k. Следовательно, верна следующая оценка:

$$c\mathcal{E}_i(\Upsilon) \leqslant \frac{\ln r}{r(1-q)^2}\Big[(1-r\delta_i)^{2j+2-k}(1+O(k^{-1/12})) + 0{,}0001\Big].$$

Далее, заметим, что $(1-r\delta_i)^{2j+2-k} \leqslant (1-1/(3k))^{2j+2-k} \leqslant e^{-(1/3)(2j+2-k)/k}$. С учетом того, что $(2j+2-k)/k = 1+O(k^{-3/4})$, для всех достаточно больших k можно считать, что $(1-r\delta_i)^{2j+2-k} \leqslant 1{,}05e^{-1/3}$. Наконец, для всех достаточно больших k выполнено $(1-q)^2 < 0{,}9$. В итоге получаем, что

$$c\mathcal{E}_i(\Upsilon) \leqslant \frac{10\ln r}{9r}\big[1{,}05e^{-1/3} + 0{,}0001\big] \leqslant 0{,}84\frac{\ln r}{r}.$$

Итак, верна оценка

$$\mathcal{H}_i(\Upsilon) - c\mathcal{E}_i(\Upsilon) \geqslant \frac{\ln r}{100r}. \tag{26}$$

Случай 2. Пусть теперь $r\delta_i \leqslant \frac{1}{3k}$. Опять начнем с оценивания $\mathcal{H}_i(\Upsilon)$. С учетом неравенства $\delta_i \geqslant r^{-2k/3}$ и (23) выполнено

$$\mathcal{H}_i(\Upsilon) \geqslant \frac{\ln r}{r} - \left(\frac{2k}{3}\ln r - \ln\Big(\frac{r}{r-1}\Big) + 1\right)\delta_i.$$

Теперь оценим $c\mathcal{E}_i(\Upsilon)$. Воспользуемся тем, что для $m \in \mathbb{N}$ и $x \in [0, \frac{1}{3m}]$ выполнено неравенство

$$(1-x)^m \leqslant 1 - \frac{mx}{1+mx} \leqslant 1 - \frac{3}{4}mx.$$

Тогда

$$(1-r\delta_i)^{2j+2-k} \leqslant 1 - \frac{3}{4}(2j+2-k)r\delta_i.$$

Далее, $2j+1-k > 9(k-j-1)/4 > 2$, и мы знаем, что $r\delta_i \leqslant 1/(3k)$. Значит,

$$(r\delta_i)^{2j+2-k}k^{9(k-j-1)/4} \leqslant r\delta_i(r\delta_i k)^{2j+1-k} \leqslant r\delta_i(1/3)^{9(k-j-1)/4} < \frac{1}{2}r\delta_i. \tag{27}$$

Кроме того, для всех достаточно больших k выполнено $(1+2/k)^2 \leqslant 2$. Стало быть, в силу (25)

$$c\mathcal{E}_i(\Upsilon) \leqslant \frac{\ln r}{r(1-q)^2}\left[\Big(1-\frac{3}{4}(2j+2-k)r\delta_i\Big)\big(1+\delta_i O(k^{7/12})\big)+r\delta_i\right].$$

Остается оценить величину q, участвующую в знаменателе. По определению имеем

$$q = r^{1-k}\sum_{s=j+1}^{k}\binom{k}{s}(r-1)^{k-s} \leqslant 2\binom{k}{j+1}r^{1-k}(r-1)^{k-j+1} \leqslant$$
$$\leqslant 2\binom{k}{j+1}r^{2-j} \leqslant 2k^{k-j-1}r^{2-j} \leqslant k^{k^{1/4}}r^{2-k+k^{1/4}} \leqslant r^{-k/6}r\delta_i. \tag{28}$$

Здесь мы воспользовались доминированием слагаемого при $s=j+1$ в сумме, а также тем, что $k-j<k^{1/4}$, а $\delta_i \geqslant r^{-3k/4}$. Следовательно,

$$(1-q)^{-2} \leqslant 1+8q \leqslant 1+8r^{-k/6}r\delta_i,$$

и значит,

$$c\mathcal{E}_i(\Upsilon) \leqslant \frac{\ln r}{r}\left[\Big(1-\frac{3}{4}(2j+2-k)r\delta_i\Big)\big(1+\delta_i O(k^{7/12})\big)+r\delta_i\right](1+8r^{-k/6}r\delta_i) =$$
$$= \frac{\ln r}{r}\left[1-\frac{3}{4}(2j+2-k)r\delta_i + r\delta_i + 8r^{-k/6}r\delta_i + \delta_i O(k^{7/12})\right] =$$
$$= \frac{\ln r}{r} - \left[\frac{3}{4}(2j+2-k)\ln r - \ln r - 8r^{-k/6}\ln r + O(k^{7/12})\ln r/r\right]\delta_i.$$

Таким образом,

$$\mathcal{H}_i(\Upsilon) - c\mathcal{E}_i(\Upsilon) \geqslant \frac{\ln r}{r} - \left(\frac{2k}{3}\ln r - \ln\Big(\frac{r}{r-1}\Big)+1\right)\delta_i -$$
$$- \frac{\ln r}{r} + \left[\frac{3}{4}(2j+2-k)\ln r - \ln r - 8r^{-k/6}\ln r + O(k^{7/12})\ln r/r\right]\delta_i =$$
$$= \left(\frac{3}{4}(2j+2-k)\ln r + O(k^{7/12})\ln r/r - \frac{2k}{3}\ln r\right)\delta_i.$$

В силу того, что $k-j<k^{1/4}$ и k достаточно велико, выполнено соотношение

$$\frac{3}{4}(2j+2-k)\ln r + O(k^{7/12})\ln r/r - \frac{2k}{3}\ln r = \frac{1}{12}k\ln r + O(k^{7/12})\frac{\ln r}{r} > \frac{1}{20}k\ln r.$$

В итоге для каждой хорошей строки получаем

$$\mathcal{H}_i(\Upsilon) - c\mathcal{E}_i(\Upsilon) \geqslant \frac{1}{20}k(\ln r)\delta_i \geqslant \frac{1}{20}k(\ln r)r^{-2k/3}. \tag{29}$$

Отметим, что данная оценка также верна и для предыдущего случая, когда выполнено $r\delta_i > 1/(3k)$.

4.3. Плохие строки. Будем называть строку с номером i плохой, если нашелся u_0 с условием $\varepsilon_{iu_0} > \frac{1}{r} - \frac{1}{r^2} - r^{-2k/3}$ и это максимальный элемент среди ε_{iu}. Вновь для простоты будем считать, что $u_0 = 1$. Тогда, пользуясь уже введенными обозначениями δ_i, δ_{iu}, получаем, что $\delta_i < r^{-2k/3}$. Значит, можно считать, что $kr\delta_i < 1/3$.

Оценим $\mathcal{H}_i$ снизу так же, как и для хороших строк; полученная оценка (23) верна всегда:

$$\mathcal{H}_i(\Upsilon) \geqslant \frac{\ln r}{r} + \delta_i \ln \delta_i + \ln\Big(\frac{r}{r-1}\Big)\delta_i - \delta_i.$$

Оценим $c\mathcal{E}_i(A)$ сверху. Пользуясь (25), имеем

$$c\mathcal{E}_i(A) \leqslant \frac{\ln r}{r(1-q)^2}\Big[(1-r\delta_i)^{2j+2-k}\big(1+\delta_i O(k^{7/12})\big) +$$
$$+ (r\delta_i)^{2j+2-k} k^{9(k-j-1)/4}(1+2/k)^3\Big] =$$

(пользуемся тем, что $(1-r\delta_i)^{2j+2-k} = 1 - r(2j+2-k)\delta_i + O(k^2r^2\delta_i^2)$, а также (27) для оценки последнего слагаемого)

$$= \frac{\ln r}{r(1-q)^2}\Big[1 - r(2j+2-k)\delta_i + O(k^{7/12}\delta_i)\Big] =$$

(используем оценки $\delta_i < r^{-2k/3}$ и $(1-q)^{-2} = (1+O(q))$, а также $q = O(k^{7/12}r^{-2k/3})$ в силу (28))

$$= \frac{\ln r}{r}\Big[1 - r(2j+2-k)\delta_i + O(k^{7/12}r^{-2k/3})\Big](1+O(q)) =$$
$$= \frac{\ln r}{r} - (2j+2-k)(\ln r)\delta_i + O(k^{7/12}r^{-2k/3}).$$

Получим

$$\mathcal{H}_i(\Upsilon) - c\mathcal{E}_i(\Upsilon) \geqslant \delta_i \ln \delta_i + \ln\Big(\frac{r}{r-1}\Big)\delta_i - \delta_i + (2j+2-k)(\ln r)\delta_i + O(k^{7/12}r^{-2k/3}).$$

Минимум данного выражения достигается при $\delta_i = \frac{r-1}{r^{2j-k+3}}$, а само выражение при таком δ_i равно

$$-\frac{r-1}{r^{2j-k+3}} + O(k^{7/12}r^{-2k/3}).$$

Значит, либо $\mathcal{H}_i(\Upsilon) - c\mathcal{E}_i(\Upsilon) \geqslant 0$, либо $|\mathcal{H}_i(\Upsilon) - c\mathcal{E}_i(\Upsilon)| = O(k^{7/12}r^{-2k/3})$.

§ 5. Перебор случаев

Мы уже показали в (21), (29), что если плохих строк нет, то найдется такая функция $b = b(k,r)$, что выполняется искомое неравенство:

$$\mathcal{G}_c(J_r) - \mathcal{G}_c(A) \geqslant \sum_{i=1}^{r} \mathcal{H}_i(\Upsilon) - c\sum_{i=1}^{r} \mathcal{E}_i(\Upsilon) \geqslant b\|\varepsilon\|^2.$$

5.1. Не только плохие строки. Пусть теперь имеется некоторое количество плохих строк, но есть дополнительно либо хорошие, либо центральные. Предположим для удобства, что при $i = 1, \ldots, s$ у нас получились плохие строки, а остальные не являются плохими. Пусть также максимальные элементы плохих строк лежат по

диагонали, они обязаны находиться в разных столбцах в силу свойств матрицы A. Тогда согласно результатам предыдущего параграфа

$$\sum_{i=1}^{s} \mathcal{H}_i(A) \geqslant c \sum_{i=1}^{s} \mathcal{E}_i(A) - O(sk^{7/12}r^{-2k/3}).$$

Случай 1. Пусть имеется центральная строка с номером $i_0 > s$. Тогда все элементы нормированной матрицы A/n в первых s столбцах будут меньше $r^{-2k/3} \leqslant r^{-2}3^{-2/3}$, ведь они лежат в одном столбце с $1/r - \delta_u$, $u = 1, \ldots, s$. Но эти элементы равны $\dfrac{1}{r^2} + \varepsilon_{i_0 u}$, $u = 1, \ldots, s$. Значит, $\varepsilon_{i_0 u}$ отрицательны и, более того, $\varepsilon_{i_0 u} < (3^{-2/3} - 1)r^{-2}$. Но тогда согласно (21)

$$\mathcal{H}_{i_0}(\Upsilon) - c\mathcal{E}_{i_0}(\Upsilon) \geqslant \frac{r^2}{4} \sum_{u:\, \varepsilon_{i_0 u} < 0} \varepsilon_{i_0 u}^2 \geqslant \frac{r^2}{4} s(3^{-2/3} - 1)^2 r^{-4} \geqslant \frac{s}{16} r^{-2}.$$

Полученная оценка значительно больше, чем $O(sk^{7/12}r^{-2k/3})$, при достаточно большом k. Значит, при наличии центральной строки имеем $\mathcal{G}_c(A) - \mathcal{G}_c(J_r) \geqslant \dfrac{1}{32} r^{-2}$, и этого более чем достаточно в наших условиях.

Случай 2. Если же центральных строк нет, но среди оставшихся есть хорошая с номером i_0, то запаса разницы между $\mathcal{H}_{i_0}(A)$ и $c\mathcal{E}_{i_0}(A)$ снова более чем достаточно, чтобы компенсировать плохие строки. Согласно (29) данная разность не меньше $\dfrac{1}{20} k(\ln r) r^{-2k/3}$, что при $k \geqslant k_0(r)$ значительно больше, чем $O(sk^{7/12}r^{-2k/3}) = O(rk^{7/12}r^{-2k/3})$.

Тем самым, остается только один неразобранный случай, а именно случай, когда все строки матрицы A являются плохими.

5.2. Только плохие строки. Наконец, пусть в каждой строке нормированной матрицы A/n имеется элемент, лежащий в пределах $[1/r - r^{-2k/3}, 1/r]$. Подобные элементы обязаны лежать в разных столбцах. Будем считать, что они лежат по диагонали. Обозначим их, как и раньше, через $1/r - \delta_i$, $i = 1, \ldots, r$. Тогда для $\sum\limits_{i=1}^{r} \mathcal{H}_i(\Upsilon)$ снова используем оценку (23). А вот величину $c \ln\Bigl(1 + \sum\limits_{i=1}^{r} \mathcal{E}_i(\Upsilon)\Bigr)$ в (20) будем оценивать целиком, чтобы получить более точные оценки. Обозначим

$$\psi = (1-q)^2 \sum_{i=1}^{r} \mathcal{E}_i(\Upsilon).$$

Из (24) имеем

$$\psi = \sum_{i=1}^{r} \Biggl[\sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} \delta_i^{h+t} \left(\frac{1}{r} - \delta_i\right)^{s-t} \times$$
$$\times \left(\frac{r-1}{r} - \delta_i\right)^{k-h-s} + \sum_{u \neq i} \sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} \times$$
$$\times \left(\frac{1}{r} - \delta_{iu}\right)^{h+t} \delta_{iu}^{s-t} \left(\frac{r-2}{r} + \delta_{iu}\right)^{k-h-s} - q^2/r \Biggr].$$

Будем рассматривать коэффициенты при степенях δ_i и δ_{iu} до второй. Сразу отметим, что минимальная степень при δ_{iu} равна $2j+2-k$, а это сильно больше двух. Свободный член (коэффициент при нулевой степени δ_i) равен

$$\sum_{i=1}^{r}\left(\sum_{s=j+1}^{k}\binom{k}{s}\left(\frac{1}{r}\right)^s\left(\frac{r-1}{r}\right)^{k-s}-q^2/r\right)=$$
$$=\sum_{i=1}^{r}\left(r^{-k}\sum_{s=j+1}^{k}\binom{k}{s}(r-1)^s-q^2/r\right)=\sum_{i=1}^{r}(q/r-q^2/r)=q-q^2.$$

Коэффициент при первой степени равен

$$\frac{1}{r^{k-1}}\sum_{i=1}^{r}\left[-\sum_{s=j+1}^{k}\binom{k}{s}\left(s(r-1)^{k-s}+(k-s)(r-1)^{k-s-1}\right)+\right.$$
$$\left.+\sum_{s=j+2}^{k}\binom{k}{s}s(r-1)^{k-s}+\sum_{s=j+1}^{k-1}\binom{k}{s}(k-s)(r-1)^{k-1-s}\right]\delta_i=$$
$$=-r^{1-k}\binom{k}{j+1}(j+1)(r-1)^{k-j-1}\sum_{i=1}^{r}\delta_i.$$

С учетом ограничений на $\delta_i\in[0,r^{-2k/3}]$ степени по δ_i и δ_{iu} выше первой (с учетом коэффициентов) будут составлять $O(qk^2\delta_i^2)=O(qk^2r^{-4k/3})$ (см. утверждения 4 и 5), а значит, будет выполнено соотношение

$$\psi=q-r^{1-k}\binom{k}{j+1}(j+1)(r-1)^{k-j-1}\sum_{i=1}^{r}\delta_i-q^2+O(qk^2r^{-4k/3}).$$

Доминирующим слагаемым здесь будет $q=O(k^{k-j-1}r^{2-j})$ (см. (28)). Отсюда получаем, что

$$c\ln\left(1+\sum_{i=1}^{r}\mathcal{E}(\Upsilon)\right)=c\ln\left(1+\frac{\psi}{(1-q)^2}\right)=$$
$$=c\left(\frac{\psi}{(1-q)^2}-\frac{1}{2}\left(\frac{\psi}{(1-q)^2}\right)^2+O(q^3)\right).$$

Далее, заметим, что

$$\psi(1-q)^{-2}=\psi(1+2q+O(q^2))=$$
$$=q-r^{1-k}\binom{k}{j+1}(j+1)(r-1)^{k-j-1}\sum_{i=1}^{r}\delta_i+q^2+O(qk^2r^{-4k/3}).$$

В свою очередь,

$$\psi^2(1-q)^{-4}=q^2+O\left(qr^{1-k}\binom{k}{j+1}(j+1)(r-1)^{k-j-1}\sum_{i=1}^{r}\delta_i\right)=$$
$$=q^2+O(qk^{k-j}r^{1-j-2k/3}).$$

Стало быть,

$$c\ln\Big(\sum_{i=1}^{r}\mathcal{E}_i(\Upsilon)\Big) =$$
$$= c\Big(q - r^{1-k}\binom{k}{j+1}(j+1)(r-1)^{k-j-1}\sum_{i=1}^{r}\delta_i + q^2/2 + O(qk^2r^{-4k/3})\Big).$$

С учетом нижней оценки (23) для $\sum\limits_{i=1}^{r}\mathcal{H}_i(\Upsilon)$ нам достаточно взять такое c, что

$$c < \frac{\ln r}{q}\min_{\delta_i\in[0,r^{-2k/3}]}\Bigg[\Big(1 - r^{1-k}\binom{k}{j+1}(j+1)(r-1)^{k-j-1}\sum_{i=1}^{r}\delta_i/q + \frac{q}{2} +$$
$$+ O(k^2r^{-4k/3})\Big)^{-1}\Big(1 + \sum_{i=1}^{r}\Big[\delta_i\log_r\delta_i + \log_r\Big(\frac{r}{r-1}\Big)\delta_i - \frac{\delta_i}{\ln r}\Big]\Big)\Bigg].$$

Нам важен порядок этого минимума с точностью до $o(q/\ln r)$. Снова используя оценки на δ_i, получаем, что

$$\Big(1 - r^{1-k}\binom{k}{j+1}(j+1)(r-1)^{k-j-1}\sum_{i=1}^{r}\delta_i/q + \frac{q}{2} + O(k^2r^{-4k/3})\Big)^{-1}\times$$
$$\times\Big(1 + \sum_{i=1}^{r}\Big[\delta_i\log_r\delta_i + \log_r\Big(\frac{r}{r-1}\Big)\delta_i - \frac{\delta_i}{\ln r}\Big]\Big) =$$

(пользуемся тем, что $|\delta_i\log_r\delta_i| = O(kr^{-2k/3})$)

$$= 1 + \sum_{i=1}^{r}\Big[(j+1)\frac{r^{1-k}\binom{k}{j+1}(r-1)^{k-j-1}}{q}\delta_i + \delta_i\log_r\delta_i + \log_r\Big(\frac{r}{r-1}\Big)\delta_i - \frac{\delta_i}{\ln r}\Big] -$$
$$- \frac{q}{2} + O(k^2r^{-4k/3}).$$

Обозначим через $f(x)$ следующую функцию:

$$f(x) = (j+1)\frac{r^{1-k}\binom{k}{j+1}(r-1)^{k-j-1}}{q}x + x\log_r x + \log_r\Big(\frac{r}{r-1}\Big)x - \frac{x}{\ln r}.$$

Минимум значения $f(x)$ достигается при $x = x_0 = \dfrac{r-1}{r^{t+1}}$, где

$$t = (j+1)\frac{r^{1-k}\binom{k}{j+1}(r-1)^{k-j-1}}{q}.$$

Подставляя его, получаем значение $f(x_0) = -\dfrac{r-1}{r^{t+1}\ln r}$. В итоге нам достаточно взять

$$c < \frac{\ln r}{q} - \frac{\ln r}{2} - \frac{r-1}{r^{t+1}q} + O\big(q^{-1}(\ln r)k^2r^{-4k/3}\big).$$

Осталось заметить, что

$$q = r^{1-k}\binom{k}{j+1}(r-1)^{k-j-1}\left(1 + O\Big(\frac{k-j}{k(r-1)}\Big)\right).$$

Откуда следует, что

$$t = (j+1)\frac{r^{1-k}\binom{k}{j+1}(r-1)^{k-j-1}}{q} = (j+1)\left(1+O\left(\frac{k-j}{k(r-1)}\right)\right) =$$
$$= j+1+O((k-j)/r),$$

а также что

$$\frac{1}{q} = O\left(r^{k-1}(r-1)^{j+1-k}\frac{1}{\binom{k}{j+1}}\right) = O\left(r^{k-1}\left(\frac{k-j}{(r-1)k}\right)^{k-j-1}\right).$$

Значит, величину $\dfrac{r-1}{r^t q}$ можно оценить сверху следующим образом: при всех достаточно больших $k > k_0(r)$ выполнено

$$\frac{r-1}{r^{t+1}q} = O\left(r^{k-1}\left(\frac{k-j}{(r-1)k}\right)^{k-j-1}\right)\frac{r-1}{r^{t+1}} =$$
$$= O\left(r^{k-1}\left(\frac{k-j}{(r-1)k}\right)^{k-j-1}\right)\frac{r-1}{r^{j+1+O((k-j)/r)}} =$$
$$= O\left(\left(\frac{(k-j)r^{1+}O(1/r)}{(r-1)k}\right)^{k-j-1}\right) =$$
$$= O\left(\left(\frac{r^{1+O(1/r)}}{k^{3/4}}\right)^{k-j-1}\right) = k^{\frac{3}{4}(j-k+1)(1+o(1))} \leqslant k^{(j-k+1)/2}.$$

Тем самым, лемма 2 полностью доказана.

§ 6. Доказательства вспомогательных утверждений

В данном параграфе приводятся доказательства вспомогательных утверждений, использованных в статье.

6.1. Доказательство утверждения 1. Рассмотрим по определению

$$\mathcal{G}_c(J_r) = \mathcal{H}(J_r) + c\mathcal{E}(J_r) = -r^2\frac{1}{r^2}\ln\frac{1}{r} + c\ln(1-\mathcal{Q}(J_r)) = \ln r + c\ln(1-\mathcal{Q}(J_r)).$$

Теперь вычислим $\mathcal{Q}(J_r)$. В силу (14)

$$\mathcal{Q}(J_r) = 2q - \sum_{i,u=1}^{r}\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}\sum_{t=0}^{s-j-1+h}\binom{k-s}{h}\binom{s}{t}\times$$
$$\times\left(\frac{1}{r}-\frac{1}{r^2}\right)^{h+t}\left(\frac{1}{r^2}\right)^{s-t}\left(\frac{r-2}{r}+\frac{1}{r^2}\right)^{k-h-s}.$$

Проверим, что кратная сумма в правой части равна q^2. Действительно, простыми преобразованиями получаем

$$\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}\sum_{t=0}^{s-j-1+h}\binom{k-s}{h}\binom{s}{t}\left(\frac{1}{r}-\frac{1}{r^2}\right)^{h+t}\left(\frac{1}{r^2}\right)^{s-t}\left(\frac{(r-1)^2}{r^2}\right)^{k-h-s} =$$

$$= r^{-2k} \sum_{s=j+1}^{k} \binom{k}{s} (r-1)^{k-s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} (r-1)^{k-s-h+t} =$$

(сделаем замену $s' = s + h - t$ вместо t)

$$= r^{-2k} \sum_{s=j+1}^{k} \binom{k}{s} (r-1)^{k-s} \sum_{h=0}^{k-s} \sum_{s'=j+1}^{s+h} \binom{k-s}{h} \binom{s}{s'-h} (r-1)^{k-s'} =$$

$$= r^{-2k} \sum_{s=j+1}^{k} \binom{k}{s} (r-1)^{k-s} \sum_{s'=j+1}^{k} (r-1)^{k-s'} \sum_{h=\max(0,s'-s)}^{k-s} \binom{k-s}{h} \binom{s}{s'-h} =$$

$$= r^{-2k} \sum_{s=j+1}^{k} \binom{k}{s} (r-1)^{k-s} \sum_{s'=j+1}^{k} \binom{k}{s'} (r-1)^{k-s'} = \frac{q^2}{r^2}.$$

Суммирование по i, u дает недостающий множитель r^2. В итоге $\mathcal{Q}(J_r) = 2q - q^2$ и $\mathcal{G}_c(J_r) = \ln r + c \ln(1-q)^2$. Утверждение 1 доказано.

6.2. Доказательство утверждения 3. Сначала оценим величину q. Напомним, что $q = r^{1-k} \sum\limits_{s=j+1}^{k} \binom{k}{s} (r-1)^{k-s}$. В силу условия $s \geqslant j+1 > k/2$ максимальное слагаемое соответствует значению $s = j+1$, поэтому

$$q \leqslant r^{1-k} k \binom{k}{k-j-1} (r-1)^{k-j-1} \leqslant r^{1-k} k (kr)^{k-j-1} =$$

$$= r^{-k} (kr)^{k-j} \leqslant r^{-k} e^{k^{1/4}(\ln k + \ln r)}. \tag{30}$$

Видно, что при всех достаточно больших k данная величина очень мала. В частности, можно считать, что $q < 1/2$.

Докажем первое неравенство. В силу вышеприведенной оценки q получаем

$$\frac{qr^2 2^k \ln r}{(1-q)^2} \leqslant 4qr^2 2^k \ln r \leqslant 4r^2 2^k \ln r r^{-k} e^{k^{1/4}(\ln k + \ln r)} \leqslant$$

(пользуемся тем, что $r > 2$)

$$\leqslant 4r^2 2^k \ln r 3^{-k} e^{k^{1/4}(\ln k + \ln r)} = r^2 (2/3)^{k + O(k^{1/4} \ln k)} < \frac{r^2}{4}.$$

Последнее неравенство верно при всех достаточно больших k по отношению к r.

Докажем второе неравенство. Пользуясь оценкой (30), имеем

$$\frac{qr^k \ln r \left(1 - \frac{1}{r} - \frac{1}{k^{2/3}}\right)^{-2} e^{-k^{1/3}}}{(1-q)^2} \leqslant 4qr^k \ln r \left(1 - \frac{1}{r} - \frac{1}{k^{2/3}}\right)^{-2} e^{-k^{1/3}} \leqslant$$

$$\leqslant 4e^{k^{1/4}(\ln k + \ln r)} \ln r \left(1 - \frac{1}{r} - \frac{1}{k^{2/3}}\right)^{-2} e^{-k^{1/3}} = e^{-k^{1/3} + O(k^{1/4} \ln k)} \ln r < e^{-10} r \ln r$$

для всех k, достаточно больших по отношению к r. Утверждение 3 доказано.

6.3. Доказательство утверждения 4. Рассмотрим цепочку преобразований

$$\sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} \delta_i^{h+t} \left(\frac{1}{r} - \delta_i\right)^{s-t} \left(\frac{r-1}{r} - \delta_i\right)^{k-h-s} =$$

$$= r^{-k} \sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=0}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} (r\delta_i)^{h+t} (1-r\delta_i)^{s-t} (r-1-r\delta_i)^{k-h-s} \leqslant$$

(выделим отдельно члены суммы при $t = h = 0$ и $t > h = 0$ и оценим грубо множитель $(1 - r\delta_i)^{s-t}$, учитывая, что $s - t \geqslant 2j + 2 - k$ в силу (13))

$$\leqslant r^{-k}(1-r\delta_i)^{2j+2-k} \Bigg[\sum_{s=j+1}^{k} \binom{k}{s} (r-1-r\delta_i)^{k-s} +$$
$$+ \sum_{s=j+2}^{k} \binom{k}{s} \sum_{t=1}^{s-j-1} \binom{s}{t} (r\delta_i)^t (r-1-r\delta_i)^{k-s} +$$
$$+ \sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=1}^{k-s} \sum_{t=0}^{s-j-1+h} \binom{k-s}{h} \binom{s}{t} (r\delta_i)^{h+t} (r-1-r\delta_i)^{k-h-s} \Bigg]. \tag{31}$$

Во всех суммах множитель вида $(r - 1 - r\delta_i)^\alpha$ оценим сверху выражением $(r-1)^\alpha$. Тогда первая сумма оценится величиной $\sum\limits_{s=j+1}^{k} \binom{k}{s} (r-1)^{k-s} = r^{k-1}q$. Далее, во второй и третьей суммах $\binom{s}{t}$ оценим сверху через k^t, а $\binom{k-s}{h} \leqslant (k-s)^h \leqslant k^{h/4}$. В итоге выражение (31) не превосходит

$$r^{-k}(1-r\delta_i)^{2j+2-k} \Bigg[r^{k-1}q + \sum_{s=j+2}^{k} \binom{k}{s} \sum_{t=1}^{s-j-1} k^t (r\delta_i)^t (r-1)^{k-s} +$$
$$+ \sum_{s=j+1}^{k} \binom{k}{s} \sum_{h=1}^{k-s} \sum_{t=0}^{s-j-1+h} k^{t+h/4} (r\delta_i)^{h+t} (r-1)^{k-h-s} \Bigg]. \tag{32}$$

Далее мы рассмотрим два случая в зависимости от того, насколько велико значение $kr\delta_i$.

Случай 1. Пусть $kr\delta_i > 2$. Оценим сначала первую сумму в скобках в (32). В ней воспользуемся тем, что $\sum\limits_{t=1}^{s-j-1} k^t (r\delta_i)^t \leqslant 2(kr\delta_i)^{s-j-1}$. Тогда

$$\sum_{s=j+2}^{k} \binom{k}{s} \sum_{t=1}^{s-j-1} k^t (r\delta_i)^t (r-1)^{k-s} \leqslant 2 \sum_{s=j+2}^{k} \binom{k}{s} (r-1)^{k-s} (kr\delta_i)^{s-j-1} =$$
$$= 2kr\delta_i \sum_{s=j+2}^{k} \binom{k}{s} (r-1)^{k-s} (kr\delta_i)^{s-j-2} \leqslant$$

(воспользуемся тем, что для хорошей или плохой строки выполнено $r\delta_i \leqslant k^{-2/3}$)

$$\leqslant 2kr\delta_i \sum_{s=j+2}^{k} \binom{k}{s} (r-1)^{k-s} k^{(s-j-2)/3}.$$

Оценим отношение последовательных слагаемых в получившейся сумме:

$$\frac{\binom{k}{s}(r-1)^{k-s}k^{(s-j-2)/3}}{\binom{k}{s-1}(r-1)^{k-s+1}k^{(s-j-3)/3}} = \frac{k^{1/3}(k-s+1)}{s(r-1)} \leqslant \frac{k^{7/12}}{(k-k^{1/4})(r-1)} \leqslant k^{-5/12},$$

начиная с некоторого k. Здесь мы воспользовались тем, что $s \geqslant j+1 > k - k^{1/4}$ и $r > 2$. В итоге, сворачивая геометрическую прогрессию и пользуясь неравенством $(1-x)^{-1} \leqslant 1 + 2x$ при $x = k^{-5/12}$, получаем, что первая сумма в скобках (32) не превосходит

$$2kr\delta_i(r-1)^{k-j-2}\binom{k}{j+2}(1+2k^{-5/12}) =$$
$$= 2kr\delta_i(r-1)^{-1}\frac{\binom{k}{j+2}}{\binom{k}{j+1}}\binom{k}{j+1}(r-1)^{k-j-1}(1+2k^{-5/12}) =$$
$$= 2kr\delta_i(r-1)^{-1}\frac{k-j-1}{j+2}\binom{k}{j+1}(r-1)^{k-j-1}(1+2k^{-5/12}) \leqslant$$

(воспользуемся тем, что $\binom{k}{j+1}(r-1)^{k-j-1} < qr^{k-1}$)

$$\leqslant 2qr^k\delta_i\frac{(k-j)k}{(j+2)(r-1)}(1+2k^{-5/12})(1+2k^{-5/12}) = O(qr^k\delta_i k^{1/4}r^{-1}) \tag{33}$$

в силу условия $j \sim k$ и $k - j < k^{1/4}$.

Аналогично оценим вторую сумму в скобках в (32). Сумму $\sum\limits_{t=0}^{s-j-1+h}(kr\delta_i)^t$ по t оценим как удвоенное максимальное слагаемое, т.е. как $2(kr\delta_i)^{s-j-1+h}$. В итоге искомая сумма не превосходит

$$\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=1}^{k-s}k^{h/4}(r\delta_i)^h(r-1)^{k-h-s}2(kr\delta_i)^{s-j-1+h} =$$
$$= 2\sum_{s=j+1}^{k}\binom{k}{s}(r-1)^{k-s}(kr\delta_i)^{s-j-1}\sum_{h=1}^{k-s}(k^{5/4}r^2\delta_i^2(r-1)^{-1})^h.$$

Заметим, что $k^{5/4}r^2\delta_i^2(r-1)^{-1} < k^{5/4-4/3} = k^{-1/12}$, а потому сумма по h оценивается сверху своим максимальным слагаемым (при $h=1$), умноженным на $1 + 2k^{-1/12}$. Стало быть, получаем оценку

$$2\sum_{s=j+1}^{k}\binom{k}{s}k^{s-j-1+5/4}(r\delta_i)^{s-j+1}(r-1)^{k-s-1}(1+2k^{-1/12}).$$

Снова рассмотрим отношение соседних слагаемых в оставшейся сумме по s:

$$\frac{\binom{k}{s}k^{s-j-1+5/4}(r\delta_i)^{s-j+1}(r-1)^{k-s-1}}{\binom{k}{s-1}k^{s-j-2+5/4}(r\delta_i)^{s-j}(r-1)^{k-s}} = \frac{(k-s+1)kr\delta_i}{s(r-1)} \leqslant$$
$$\leqslant \frac{k^{1/4+1-2/3}}{(k-k^{1/4})(r-1)} \leqslant k^{-5/12}.$$

Следовательно, сумма по s оценивается сверху своим максимальным слагаемым (при $s = j+1$), умноженным на $1 + 2k^{-5/12}$. В итоге получаем оценку

$$2(r\delta_i)^2\binom{k}{j+1}k^{5/4}(r-1)^{k-j-2}(1+2k^{-1/12})(1+2k^{-5/12}) \leqslant$$

(снова воспользуемся тем, что $r\delta_i \leqslant k^{-2/3}$)

$$\leqslant 2r\delta_i\binom{k}{j+1}k^{7/12}(r-1)^{k-j-2}(1+2k^{-1/12})(1+2k^{-5/12}) \leqslant$$

(применим очевидное неравенство $\binom{k}{j+1}(r-1)^{k-j-1} < qr^{k-1}$)

$$\leqslant 2r^k q\delta_i k^{7/12}(r-1)^{-1}(1+2k^{-1/12})(1+2k^{-5/12}) = O(r^k q\delta_i k^{7/12} r^{-1}). \tag{34}$$

В итоге из (33) и (34) получаем, что в рассматриваемом случае выражение (32) не превосходит

$$r^{-k}(1-r\delta_i)^{2j+2-k}\left[r^{k-1}q + O(r^{k-1}q\delta_i k^{1/4}) + O(r^{k-1}q\delta_i k^{7/12})\right] =$$
$$= q(1-r\delta_i)^{2j+2-k}r^{-1}\left(1+O(\delta_i k^{7/12})\right).$$

Случай 2. Пусть теперь $kr\delta_i \leqslant 2$. Вновь отдельно оценим суммы, входящие в (32). Начнем с первой. Внутреннюю сумму по t оценим тривиальным образом, пользуясь ограничением второго случая: $\sum\limits_{t=1}^{s-j-1}(kr\delta_i)^t \leqslant kr\delta_i 2^{s-j-1}$. Стало быть,

$$\sum_{s=j+2}^{k}\binom{k}{s}\sum_{t=1}^{s-j-1}(kr\delta_i)^t(r-1)^{k-s} \leqslant kr\delta_i\sum_{s=j+2}^{k}\binom{k}{s}(r-1)^{k-s}2^{s-j-1}.$$

Покажем, что в получившейся сумме максимальному слагаемому отвечает $s = j+2$. Рассмотрим отношение последовательных слагаемых в сумме:

$$\frac{\binom{k}{s}(r-1)^{k-s}2^{s-j-1}}{\binom{k}{s-1}(r-1)^{k-s+1}2^{s-j-2}} = \frac{2(k-s+1)}{s(r-1)} \leqslant \frac{2k^{1/4}}{(r-1)(k-k^{1/4})} \leqslant 2k^{-3/4},$$

начиная с некоторого k, где переход в неравенстве выполнен с учетом убывания выражения по s и ограничения $k-s < k^{1/4}$. Значит, вся сумма оценивается своим максимальным слагаемым, умноженным на $1+4k^{-3/4}$:

$$kr\delta_i\sum_{s=j+2}^{k}\binom{k}{s}(r-1)^{k-s}2^{s-j-1} \leqslant 2\binom{k}{j+2}kr\delta_i(r-1)^{k-j-2}(1+4k^{-3/4}) =$$
$$= 2kr\delta_i(r-1)^{-1}(1+4k^{-3/4})\frac{\binom{k}{j+2}}{\binom{k}{j+1}}\binom{k}{j+1}(r-1)^{k-j-1} \leqslant$$

(пользуемся тем, что $\binom{k}{j+1}(r-1)^{k-j-1} \leqslant qr^{k-1}$)

$$\leqslant 2qr^k\delta_i(1+4k^{-3/4})\frac{(k-j-1)k}{(j+2)(r-1)} = O\left(qr^{k-1}\delta_i k^{1/4}\right). \tag{35}$$

Здесь мы снова пользовались тем, что $j \sim k$ и $k-j < k^{1/4}$.

Остается оценить вторую сумму в (32). Здесь все полностью аналогично. Внутренняя сумма по t оценивается с помощью ограничения $kr\delta_i \leqslant 2$:

$$\sum_{t=0}^{s-j-1+h}(kr\delta_i)^t \leqslant 2^{s-j+h}.$$

Следовательно,

$$\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=1}^{k-s}\sum_{t=0}^{s-j-1+h}k^{t+h/4}(r\delta_i)^{h+t}(r-1)^{k-h-s}\leqslant$$
$$\leqslant\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=1}^{k-s}k^{h/4}(r\delta_i)^{h}(r-1)^{k-h-s}2^{s-j+h}=$$
$$=\sum_{s=j+1}^{k}\binom{k}{s}(r-1)^{k-s}2^{s-j}\sum_{h=1}^{k-s}\left(\frac{2k^{1/4}r\delta_i}{r-1}\right)^{h}.$$

Сумма по h – это снова геометрическая прогрессия, причем ее знаменатель мал: из условия $r\delta_i\leqslant k^{-1}$ получаем, что

$$\frac{2k^{1/4}r\delta_i}{r-1}\leqslant k^{-3/4}.$$

Значит, вся сумма оценивается сверху своим первым слагаемым, умноженным на $1+2k^{-3/4}$. В итоге имеем оценку

$$\frac{2k^{1/4}r}{r-1}\delta_i(1+2k^{-3/4})\sum_{s=j+1}^{k}\binom{k}{s}2^{s-j}(r-1)^{k-s-1}.$$

Проверим, что в оставшейся сумме максимальному слагаемому отвечает $s=j+1$. Вновь выпишем отношение последовательных членов суммы:

$$\frac{\binom{k}{s}2^{s-j}(r-1)^{k-s-1}}{\binom{k}{s-1}2^{s-j-1}(r-1)^{k-s}}=\frac{2(k-s+1)}{s(r-1)}\leqslant 2k^{-3/4},$$

тогда вся сумма оценивается своим максимальным слагаемым, умноженным на $1+4k^{-3/4}$. Получаем итоговую оценку:

$$\frac{2k^{1/4}r}{r-1}\delta_i(1+2k^{-3/4})\sum_{s=j+1}^{k}\binom{k}{s}2^{s-j}(r-1)^{k-s-1}\leqslant$$
$$\leqslant\frac{2k^{1/4}r}{r-1}\delta_i(1+2k^{-3/4})\binom{k}{j+1}2(r-1)^{k-j-2}(1+4k^{-3/4})\leqslant$$

(пользуемся тем, что $\binom{k}{j+1}(r-1)^{k-j-1}\leqslant qr^{k-1}$)

$$\leqslant 4k^{1/4}qr^k(r-1)^{-2}\delta_i(1+2k^{-3/4})(1+4k^{-3/4})=O(qr^kk^{1/4}r^{-2}\delta_i).\qquad(36)$$

В итоге, из (35) и (36) получаем, что выражение (32) не превосходит

$$r^{-k}(1-r\delta_i)^{2j+2-k}\Big[r^{k-1}q+O(qr^{k-1}\delta_ik^{1/4})+O(qr^kk^{1/4}r^{-2}\delta_i)\Big]=$$
$$=q(1-r\delta_i)^{2j+2-k}r^{-1}\big(1+O(k^{1/4}\delta_i)\big).$$

Утверждение 4 доказано.

6.4. Доказательство утверждения 5. Преобразуем оцениваемое выражение:

$$\sum_{u=2}^{r}\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}\sum_{t=0}^{s-j-1+h}\binom{k-s}{h}\binom{s}{t}\left(\frac{1}{r}-\delta_{iu}\right)^{h+t}\delta_{iu}^{s-t}\left(\frac{r-2}{r}+\delta_{iu}\right)^{k-h-s}=$$

$$=r^{-k}\sum_{u=2}^{r}\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}\sum_{t=0}^{s-j-1+h}\binom{k-s}{h}\binom{s}{t}\times$$

$$\times\left(1-r\delta_{iu}\right)^{h+t}\left(r\delta_{iu}\right)^{s-t}\left(r-2+r\delta_{iu}\right)^{k-h-s}.$$

Здесь достаточно совсем грубых оценок. Оценим биномиальные коэффициенты следующим образом:

$$\binom{s}{t}\leqslant k^t,\quad \binom{k-s}{h}\leqslant(k-s)^h\leqslant(k^{1/4})^h.$$

В последнем неравенстве мы пользуемся тем, что $k-s<k-j<k^{1/4}$. Отметим также, что раз $r\delta_i<k^{-2/3}<1$, то $r-2+r\delta_{iu}<r-1$. Далее, в силу (13) выполнено $s-t\geqslant 2j+2-k$, а потому $(r\delta_{iu})^{s-t}\leqslant(r\delta_{iu})^{2j+2-k}$. Стало быть, искомое выражение не превосходит величины

$$r^{-k}\sum_{u=2}^{r}(r\delta_{iu})^{2j+2-k}\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}(r-1)^{k-h-s}\sum_{t=0}^{s-j-1+h}k^{k-s+t+h/4}.$$

Внутренняя сумма по t – это геометрическая прогрессия с растущим знаменателем k, потому она не превосходит своего последнего слагаемого, умноженного на $1+2/k$. Получаем оценку

$$r^{-k}\sum_{u=2}^{r}(r\delta_{iu})^{2j+2-k}\sum_{s=j+1}^{k}\binom{k}{s}\sum_{h=0}^{k-s}(r-1)^{k-h-s}k^{k-j-1+5h/4}(1+2/k)\leqslant$$

$$\leqslant r^{-k}k^{k-j-1}\sum_{u=2}^{r}(r\delta_{iu})^{2j+2-k}\sum_{s=j+1}^{k}\binom{k}{s}(r-1)^{k-s}\sum_{h=0}^{k-s}k^{5h/4}(1+2/k)\leqslant$$

$$\leqslant r^{-k}k^{k-j-1}\sum_{u=2}^{r}(r\delta_{iu})^{2j+2-k}\sum_{s=j+1}^{k}\binom{k}{s}(r-1)^{k-s}k^{5(k-s)/4}(1+2/k)^2.$$

Здесь мы снова воспользовались оценкой геометрической прогрессии. Применим оценку $k^{5(k-s)/4}\leqslant k^{5(k-j-1)/4}$, тогда оставшаяся сумма по s станет равна qr^{k-1}. В итоге получаем оценку

$$qr^{-1}k^{9(k-j-1)/4}(1+2/k)^2\sum_{u=2}^{r}(r\delta_{iu})^{2j+2-k}.$$

Осталось заметить, что в силу условий $\delta_{iu}\geqslant 0$ и $\sum\limits_{u=2}^{r}\delta_{iu}=\delta_i$ выполнено простое неравенство для норм:

$$\sum_{u=2}^{r}\delta_{iu}^{2j+2-k}\leqslant\left(\sum_{u=2}^{r}\delta_{iu}\right)^{2j+2-k}=\delta_i^{2j+2-k}.$$

Утверждение 5 доказано.

СПИСОК ЛИТЕРАТУРЫ

1. *Cutler J., Radcliffe A.J.* Hypergraph Independent Sets // Combin. Probab. Comput. 2013. V. 22. № 1. P. 9–20. https://doi.org/10.1017/S0963548312000454
2. *Ordentlich E., Roth R.M.* Independent Sets in Regular Hypergraphs and Multidimensional Runlength-Limited Constraints // SIAM J. Discrete Math. 2004. V. 17. № 4. P. 615–623. https://doi.org/10.1137/S0895480102419767
3. *Балобанов А.Е., Шабанов Д.А.* О числе независимых множеств в простых гиперграфах // Матем. заметки. 2018. Т. 103. № 1. С. 38–48 https://doi.org/10.4213/mzm11508
4. *Семенов А.С., Шабанов Д.А.* Независимые множества общего вида в случайных сильно разреженных гиперграфах // Пробл. передачи информ. 2018. Т. 54. № 1. С. 63–77. http://mi.mathnet.ru/ppi2260
5. *Heckel A.* The Chromatic Number of Dense Random Graphs // Random Structures Algorithms. 2018. V. 53. № 1. P. 140–182. https://doi.org/10.1002/rsa.20757
6. *Shabanov D.A.* Estimating the r-Colorability Threshold for a Random Hypergraph // Discrete Appl. Math. 2020. V. 282. P. 168–183. https://doi.org/10.1016/j.dam.2019.10.031
7. *Ширяев А.Н.* Вероятность. В 2-х кн., 6-е изд. испр. М: МЦНМО, 2017.
8. *Schmidt-Pruzan J., Shamir E., Upfal E.* Random Hypergraph Coloring Algorithms and the Weak Chromatic Number // J. Graph Theory. 1985. V. 9. № 3. P. 347–362. https://doi.org/10.1002/jgt.3190090307
9. *Schmidt J.P.* Probabilistic Analysis of Strong Hypergraph Coloring Algorithms and the Strong Chromatic Number // Discrete Math. 1987. V. 66. № 3. P. 259–277. https://doi.org/10.1016/0012-365X(87)90101-4
10. *Shamir E.* Chromatic Number of Random Hypergraphs and Associated Graphs // Randomness and Computation. Adv. Comput. Res. V. 5. Greenwich, CT: JAI Press, 1989. P. 127–142.
11. *Krivelevich M., Sudakov B.* The Chromatic Numbers of Random Hypergraphs // Random Structures Algorithms. 1998. V. 12. № 4. P. 381–403. https://doi.org/10.1002/(SICI)1098-2418(199807)12:4<381::AID-RSA5>3.0.CO;2-P
12. *Dyer M., Frieze A., Greenhill C.* On the Chromatic Number of a Random Hypergraph // J. Combin. Theory Ser. B. 2015. V. 113. P. 68–122. https://doi.org/10.1016/j.jctb.2015.01.002
13. *Ayre P., Coja-Oghlan A., Greenhill C.* Hypergraph Coloring up to Condensation // Random Structures Algorithms. 2019. V. 54. № 4. P. 615–652. https://doi.org/10.1002/rsa.20824
14. *Achlioptas D., Kim J.H., Krivelevich M., Tetali P.* Two-Colorings Random Hypergraphs // Random Structures Algorithms. 2002. V. 20. № 2. P. 249–259. https://doi.org/10.1002/rsa.997
15. *Achlioptas D., Moore C.* On the 2-Colorability of Random Hypergraphs // Randomization and Approximation Techniques in Computer Science (Proc. 6th Int. Workshop RANDOM'2002. Cambridge, MA, USA. Sept. 13–15, 2002). Lect. Notes Comput. Sci. V. 2483. Berlin: Springer, 2002. P. 78–90. https://doi.org/10.1007/3-540-45726-7_7
16. *Coja-Oghlan A., Zdeborová L.* The Condensation Transition in Random Hypergraph 2-Coloring // Proc. 23rd Annu. ACM–SIAM Symp. on Discrete Algorithms (SODA'12). Kyoto, Japan. Jan. 17–19, 2012. P. 241–250. https://doi.org/10.1137/1.9781611973099.22
17. *Coja-Oghlan A., Panagiotou K.* Catching the k-NAESAT Threshold // Proc. 44th Annu. ACM Symp. on Theory of Computing (STOC'12). New York, USA. May 19–22, 2012. P. 899–908. https://doi.org/10.1145/2213977.2214058
18. *Семенов А.С.* Двухцветные раскраски случайного гиперграфа // Теория вероятн. и ее примен. 2019. Т. 64. № 1. С. 75–97. https://doi.org/10.4213/tvp5165
19. *Balobanov A.E., Shabanov D.A.* On the Strong Chromatic Number of a Random 3-Uniform Hypergraph // Discrete Math. 2021. V. 344. № 3. Paper No. 112231 (16 pp.). https://doi.org/10.1016/j.disc.2020.112231

20. *Semenov A.S., Shabanov D.A.* On the Weak Chromatic Number of Random Hypergraphs // Discrete Appl. Math. 2020. V. 276. P. 134–154. https://doi.org/10.1016/j.dam.2019.03.025
21. *Hatami H., Molloy M.* Sharp Thresholds for Constraint Satisfaction Problems and Homomorphisms // Random Structures Algorithms. 2008. V. 33. № 3. P. 310–332. https://doi.org/10.1002/rsa.20225

Семенов Александр Сергеевич
Московский физико-технический институт
(государственный университет),
факультет инноваций и высоких технологий,
кафедра дискретной математики
alexsemenov1992@mail.ru
Шабанов Дмитрий Александрович
Московский физико-технический институт
(государственный университет),
лаборатория комбинаторных и геометрических структур
Московский государственный университет
им. М.В. Ломоносова, механико-математический факультет,
кафедра теории вероятностей
Национальный исследовательский университет
«Высшая школа экономики»,
факультет компьютерных наук
dmitry.shabanov@phystech.edu

Поступила в редакцию
09.03.2020
После доработки
18.02.2022
Принята к публикации
18.02.2022

Адрес редакции: 127051, Москва, Б. Каретный пер., 19, стр. 1, тел. (495) 650-47-39

Оригинал-макет подготовил *Д.Ю. Ногин*
по контракту с ООО «Тематическая редакция»

Москва
ООО «Тематическая редакция»