Дискретная математика

том 35 выпуск 3 * 2023

УДК 519.725 DOI https://doi.org/10.4213/dm1763

Квадрат Адамара последовательно соединенных линейных кодов

© 2023 г. И. В. Чижов*

Последовательно соединенные коды порождаются матрицами, которые получаются последовательным соединением порождающих матриц других линейных кодов. В работе получена оценка вероятности того, что квадрат Адамара последовательно соединенных случайных линейных кодов равен декартову произведению квадратов Адамара линейных кодов, участвующих в соединении.

Ключевые слова: квадрат Адамара, квадрат Шура, произведение Адамара линейных кодов, произведение Шура линейных кодов, последовательно соединенные линейные коды

1. Введение

Произведение Адамара (Шура) или просто покоординатное произведение линейных кодов изучается довольно давно. Вначале оно применялось для построения алгебраических декодеров для ряда линейных кодов, исправляющих ошибки [1]. В последнее время оно все чаще применяется в криптографии. Например, с помощью произведений Адамара строятся схемы разделения секрета и протоколы многосторонних безопасных вычислений [2].

Одним из главных приложений этой операции над кодами в криптоанализе являются атаки на кодовые постквантовые криптографические механизмы. Стоит отметить построенную на двоичных кодах Рида – Маллера атаку [3] на криптосистему Мак-Элиса или атаку [4] на ту же криптосистему, но основанную на подкодах кода Рида – Соломона. Также многочисленные примеры применения произведений Адамара для построения атак на различные кодовые криптосистемы дают работы [5–9]. Кроме того, впервые с помощью этой операции в статье [10] построен эффективный алгоритм, отличающий коды Гоппы от случайных кодов.

Для практических приложений оказывается важным описание квадрата Адамара кода и установление его свойств как линейного кода. Например, в [11] доказано, что с вероятностью, близкой к единице, квадрат Адамара линейного кода заполняет все пространство. Это свойство часто используется для построения атак на постквантовые криптосистемы с открытым ключом, см., например, [5, 8, 9, 12]. В ряде криптографических механизмов применяются коды, квадрат Адамара которых не равен

*Место работы: МГУ им. М. В. Ломоносова; Федеральный исследовательский центр «Информатика и управление» РАН; НПК «Криптонит», e-mail: ichizhov@cs.msu.ru

всему пространству, и тогда оказывается важной алгебраическая или комбинаторная структура квадрата Адамара кода.

В последнее время построен ряд атак [9, 13–15] на постквантовые криптографические механизмы, основанные на кодах, которые получаются последовательным соединением других линейных кодов. Такие коды состоят из кодовых слов, которые можно представить как конкатенацию некоторых кодовых слов других кодов. В работе такие коды называются комбинированными. Причем для корректной работы этих атак требуется, чтобы квадрат Адамара комбинированного кода был равен декартову произведению квадратов Адамара кодов, использованных в соединении. В экспериментах исследователи отмечали, что это свойство выполняется почти всегда, однако теоретического обоснования этого факта не приводилось.

В настоящей работе изучается вероятность того, что квадрат Адамара кода, полученного последовательным соединением случайных кодов, равен декартову произведению квадратов Адамара кодов, которые стоят в соединении.

2. Основные термины и определения

Для произвольного натурального n через $V_n(q)$ будем обозначать множество векторов-строк длины n над конечным полем $\mathrm{GF}(q)$, а через $V_n^\top(q)$ множество векторов-столбцов длины n над $\mathrm{GF}(q)$. Здесь $q = p^\ell$ — некоторая степень простого числа. При $q = 2$ вместо $V_n(2)$ и $V_n^\top(2)$ будем использовать обозначения V_n и $V_n^\top$ соответственно.

Определение 1. *Линейным блоковым $[n]_q$-кодом $\mathcal{C}$* называется произвольное линейное подпространство пространства $V_n(q)$. При этом число n называется *длиной* кода $\mathcal{C}$. Векторы, лежащие в коде $\mathcal{C}$, будем называть *кодовыми словами*.

Определение 2. *Линейным блоковым $[n, k]_q$-кодом $\mathcal{C}$* называется линейное подпространство пространства $V_n(q)$ размерности k. При этом число k называется *размерностью* кода $\mathcal{C}$.

Определение 3. *Порождающей матрицей* $[n, k]_q$-кода $\mathcal{C}$ называется $(k \times n)$-матрица G, строками которой являются базисные векторы $[n, k]_q$-кода $\mathcal{C}$ как подпространства $V_n(q)$.

Утверждение 1. *Справедливо равенство*

$$\mathcal{C} = \{a \cdot G \mid a \in V_k(q)\}.$$

Утверждение 2. *Две $(k \times n)$-матрицы G_1 и G_2 порождают один и тот же $[n, k]_q$-код $\mathcal{C}$, если и только если существует такая невырожденная $(k \times k)$-матрица A над полем* $\mathrm{GF}(q)$, *что $AG_1 = G_2$.*

Определение 4 ([16, с. 33])**.** *Охватывающей матрицей линейного $[n]_q$-кода $\mathcal{C}$* называется такая $(\ell \times n)$-матрица D, что линейная оболочка ее строк совпадает с $[n]_q$-кодом $\mathcal{C}$, т. е. $\mathcal{C} = \{a \cdot D \mid a \in V_\ell(q)\}$.

Ясно, что если $(\ell \times n)$-матрица D охватывает некоторый $[n, k]_q$-код, то верно неравенство $\ell \geqslant k$. Кроме того, порождающая матрица G кода $\mathcal{C}$ получается из охватывающей матрицы D удалением линейно зависимых строк.

Определение 5. *Произведением Адамара* (или *произведением Шура*) *векторов* $c = (c_1, \ldots, c_n) \in V_n(q)$ и $b = (b_1, \ldots, b_n) \in V_n(q)$ называется покомпонентное произведение векторов c и b, т. е. вектор

$$c \circ b = (c_1 \cdot b_1, \ldots, c_n \cdot b_n),$$

здесь «$\cdot$» — операция умножения элементов поля $\mathrm{GF}(q)$.

Определение 6. *Произведением Адамара* (или *произведением Шура*) $[n]_q$-кодов $\mathcal{C}$ и $\mathcal{B}$ называется код $\mathcal{C} \circ \mathcal{B}$, который совпадает с линейной оболочкой множества $\{c \circ b \mid c \in \mathcal{C},\ b \in \mathcal{B}\}$. Здесь $c \circ b$ — произведение Адамара векторов c и b.

Определение 7. *Квадратом Адамара* кода $\mathcal{C}$ называется код $\mathcal{C}^{\circ 2} = \mathcal{C} \circ \mathcal{C}$.

Утверждение 3. *Если* $\mathcal{B} \subseteq \mathcal{C}$, *то* $\mathcal{B}^{\circ 2} \subseteq \mathcal{C}^{\circ 2}$.

Определение 8. *Декартовым произведением линейных кодов* $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_u$ называется линейный код $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_u$, состоящий из всех возможных кодовых слов вида $c = (c_1 \| c_2 \| \ldots \| c_u)$, здесь c_i — кодовое слово кода $\mathcal{C}_i$ для всех $i = 1, 2, \ldots, u$, т. е.

$$\mathcal{C} = \{c = (c_1 \| c_2 \| \ldots \| c_u) \mid c_1 \in \mathcal{C}_1, c_2 \in \mathcal{C}_2, \ldots, c_u \in \mathcal{C}_u\}.$$

Утверждение 4. *Если код* $\mathcal{C}_i$ *является* $[n_i, k_i]_q$*-кодом для некоторых натуральных чисел* n_i *и* k_i, $i = 1, 2, \ldots, u$, *то код* $\mathcal{C}$ *является* $[\sum_{i=1}^{u} n_i, \sum_{i=1}^{u} k_i\,]$*-кодом.*

Утверждение 5. *Пусть линейные коды* $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_u, \mathcal{B}_1, \ldots, \mathcal{B}_u$ *таковы, что пары кодов* $\mathcal{C}_i, \mathcal{B}_i$ *имеют одну и ту же длину* n_i, $i = 1, 2, \ldots, u$. *Тогда верно равенство*

$$(\mathcal{C}_1 \times \cdots \times \mathcal{C}_u) \circ (\mathcal{B}_1 \times \cdots \times \mathcal{B}_u) = (\mathcal{C}_1 \circ \mathcal{B}_1) \times \cdots \times (\mathcal{C}_u \circ \mathcal{B}_u).$$

Следствие 1. *Для любого линейного кода* $\mathcal{C}$ *верно равенство*

$$(\mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_u)^{\circ 2} = \mathcal{C}_1^{\circ 2} \times \mathcal{C}_2^{\circ 2} \times \cdots \times \mathcal{C}_u^{\circ 2}.$$

Пусть $G'=(g'_1 g'_2 \ldots g'_{n_1})$ — $(k \times n_1)$-матрица, состоящая из столбцов $g'_1, \ldots, g'_{n_1} \in V_k^{\top}(q)$, а $G'' = (g''_1 g''_2 \ldots g''_{n_2})$ — $(k \times n_2)$-матрица, состоящая из столбцов $g''_1, \ldots, g''_{n_2} \in V_k^{\top}(q)$, тогда через $(G' \| G'')$ обозначим $(k \times (n_1 + n_2))$-матрицу $(g'_1 g'_2 \ldots g'_{n_1} g''_1 g''_2 \ldots g''_{n_2})$.

Определение 9. *Кодом, полученным последовательным соединением линейных кодов*, или просто *комбинацией линейных кодов* $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_u$, называется линейный код $\mathcal{C}$, который охватывается матрицей $G = (G_1 \| \ldots \| G_u)$, здесь G_i – некоторая $(\ell \times n_i)$-матрица, которая охватывает код $\mathcal{C}_i$, $i = 1, 2, \ldots, u$. Заметим, что код $\mathcal{C}$ является $[\sum_{i=1}^{u} n_i\,]_q$-кодом. В общем случае комбинация кодов не определена однозначно, так как возможно для построения кода $\mathcal{C}$ выбирать разные охватывающие матрицы. Множество всех кодов $\mathcal{C}$, являющихся комбинацией некоторых кодов $\mathcal{C}_1, \ldots, \mathcal{C}_u$, будем обозначать $\mathcal{C}_1 \| \ldots \| \mathcal{C}_u$.

Утверждение 6. *Для любого* $\mathcal{C} \in \mathcal{C}_1 \| \mathcal{C}_2 \| \ldots \| \mathcal{C}_u$ *верно включение* $\mathcal{C} \subseteq \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_u$.

2.1. Постановка проблемы. Сформулируем центральный вопрос статьи.

Для единообразия обозначений в рамках данной статьи через $V_{k \times n}(q)$ будем обозначать множество всех $(k \times n)$-матриц над полем $\mathrm{GF}(q)$. Пусть $G_i \in V_{k \times n_i}$ — некоторые $(k \times n_i)$-матрицы над полем $\mathrm{GF}(q)$, $i = 1, 2, \ldots, u$, выбранные в соответствии с заданным вероятностным распределением на декартовом произведении $\prod_{i=1}^{u} V_{k \times n_i}(q)$. Это распределение будет конкретизировано в формулировках основных результатов статьи — теоремах 1 и 2.

Положим $n = n_1 + n_2 + \cdots + n_u$. Рассмотрим $(k \times n)$-матрицу

$$G = (G_1 \| G_2 \| \dots \| G_u).$$

Она охватывает некоторый код $\mathcal{C} \in \mathcal{C}_1 \| \mathcal{C}_2 \| \dots \| \mathcal{C}_u$, где $\mathcal{C}_i$ — $[n_i]_q$-код, охватываемый матрицей G_i, $i = 1, 2, \dots, u$. В силу утверждений 6, 3 и следствия 1 верно включение

$$\mathcal{C}^{\circ 2} \subseteq \mathcal{C}_1^{\circ 2} \times \mathcal{C}_2^{\circ 2} \times \cdots \times \mathcal{C}_u^{\circ 2}. \tag{1}$$

Вопрос 1. *С какой вероятностью при случайном выборе матриц $G_1, G_2, \dots, G_u$ в соответствии с заданным распределением на $\prod_{i=1}^{u} V_{k \times n_i}(q)$ квадрат Адамара комбинированного кода $\mathcal{C}$ совпадает с декартовым произведением квадратов Адамара кодов $\mathcal{C}_i$, входящих в комбинацию? Т. е. с какой вероятностью включение* (1) *становится равенством?*

3. Квадрат Адамара кода и квадратичные формы

Определение 10. *Квадратичной формой* $Q(x_1, \dots, x_k)$ над полем $\mathrm{GF}(q)$ называется однородный квадратный многочлен $Q(x_1, \dots, x_k)$ над полем $\mathrm{GF}(q)$, т. е.

$$Q(x_1, \dots, x_k) = \sum_{1 \leqslant i < j \leqslant k} a_{i,j} x_i x_j + \sum_{i=1}^{k} b_i x_i^2,$$

где $a_{i,j} \in \mathrm{GF}(q), 1 \leqslant i < j \leqslant k$, и $b_i \in \mathrm{GF}(q), 1 \leqslant i \leqslant k$. *Множество квадратичных форм* над полем $\mathrm{GF}(q)$ от k переменных будем обозначать $\mathcal{Q}_k(q)$.

Для простоты далее предположим, что q — простое число. В случае, когда q является степенью p^a, $a > 1$, некоторого простого числа p, все описанные ниже рассуждения остаются верными за тем лишь исключением, что вместо чисел $0, 1, \dots, q-1$ везде нужно использовать элементы поля $\mathrm{GF}(q)$, которые упорядочены в соответствии с некоторым правилом. Само это правило для целей настоящей работы не важно, поэтому его выбор остается за читателем. Далее имеется в виду лексикографический порядок векторов длины k над полем $\mathrm{GF}(q)$.

Итак, пусть $Q(x_1, \dots, x_k) \in \mathcal{Q}_k(q)$ — некоторая квадратичная форма. Обозначим через $\Omega_Q \in V_{q^k}(q)$ вектор ее значений на всех наборах $(x_1, \dots, x_k) \in V_k(q)$, упорядоченных в лексикографическом порядке, т. е.

$$\Omega_Q = (Q(0, \dots, 0), Q(0, \dots, 1), Q(0, \dots, 2), \dots, Q(q-1, \dots, q-1)) \in V_{q^k}(q).$$

Через R обозначим $\left(\frac{k(k+1)}{2} \times q^k\right)$-матрицу

$$R = \begin{pmatrix} \Omega_{x_k^2} \\ \Omega_{x_{k-1}^2} \\ \vdots \\ \Omega_{x_1^2} \\ \Omega_{x_k x_{k-1}} \\ \vdots \\ \Omega_{x_2 x_1} \end{pmatrix}. \tag{2}$$

Она является порождающей матрицей однородного кода Рида – Маллера $\mathcal{HRM}_q(2,k)$, который состоит из векторов значений Ω_Q всех квадратичных форм $Q \in \mathcal{Q}_k(q)$.

Заметим, что код $\mathcal{HRM}_q(2,k)$ имеет длину $N = 2^k$ и размерность $K = k\cdot(k+1)/2$.

Все столбцы матрицы R занумеруем q-ичными вектор-столбцами длины k

$$0 = (0,\dots,0)^\top, 1 = (0,\dots,1)^\top, \dots, q^k - 1 = (q-1,\dots,q-1)^\top.$$

Пусть $g \in V_q^\top(k)$ — вектор-столбец длины k, тогда через R_g будем обозначать столбец матрицы R с номером g. Подматрицу размера $\left(\frac{k(k+1)}{2} \times n\right)$ матрицы R, содержащую столбцы с номерами $g_1, g_2, \dots, g_n$, $g_i \in V_k^\top(q)$ для всех $i = 1,2,\dots,n$, будем обозначать $R_{\{g_1 g_2 \dots g_n\}}$. Заметим, что если $G = (g_1 g_2 \dots g_n)$ — $(k \times n)$-матрица, составленная из столбцов $g_1, g_2, \dots, g_n \in V_k^\top(q)$, то R_G обозначает матрицу $R_{\{g_1 \dots g_n\}}$.

Таким образом, квадратичную форму $Q \in \mathcal{Q}_k(q)$ можно однозначно задать двумя способами: либо вектором коэффициентов ω_Q=$(b_k,b_{k-1},\dots,b_1,a_{k-1,k},a_{k-2,k},\dots,a_{1,2})$, упорядоченных в соответствии с порядком строк матрицы R, либо вектором значений Ω_Q. При этом верно равенство

$$\Omega_Q = \omega_Q \cdot R.$$

К тому же для любых $g_1, g_2 \dots, g_n \in V_k^\top(q)$ и любого $Q \in \mathcal{Q}_q(k)$

$$(Q(g_1), Q(g_2), \dots, Q(g_n)) = \omega_Q \cdot R_{\{g_1 g_2 \dots g_n\}}. \tag{3}$$

Утверждение 7 ([17]). *Пусть $G = (g_1 g_2 \dots g_k)$ — порождающая $(k \times n)$-матрица $[n,k]_q$-кода $\mathcal{C}$, здесь $g_i \in V_k^\top(q)$ — столбец матрицы G с номером $i = 1,2,\dots,n$. Рассмотрим отображение $\ell_G\colon \mathcal{Q}_k(q) \to V_n(q)$ из множества $\mathcal{Q}_k(q)$ квадратичных форм над полем $\mathrm{GF}(q)$ от k переменных в множество $V_n(q)$ векторов длины n над полем $\mathrm{GF}(q)$, которое ставит в соответствие квадратичной форме $Q(x_1, x_2, \dots, x_k)$ вектор*

$$(Q(g_1), Q(g_2), \dots, Q(g_n)),$$

т. е.

$$\ell_G(Q) = (Q(g_1), Q(g_2), \dots, Q(g_n)), \quad \forall\, Q \in \mathcal{Q}_k(q). \tag{4}$$

Тогда $\mathcal{C}^{\circ 2} = \operatorname{Im} \ell_G$.

Следствие 2 ([17]). *Пусть $G = (g_1 g_2 \dots g_n)$ — порождающая $(k \times n)$-матрица $[n,k]_q$-кода $\mathcal{C}$. Тогда $\dim \mathcal{C}^{\circ 2} = \operatorname{rank} R_{\{g_1 g_2 \dots g_n\}}$.*

Следствие 2 можно обобщить на случай, когда код задан не порождающей матрицей, а охватывающей.

Следствие 3. *Пусть D — охватывающая $(\kappa \times n)$-матрица $[n,k]_q$-кода $\mathcal{C}$. Тогда $\dim \mathcal{C}^{\circ 2} = \operatorname{rank} R_D$.*

Доказательство. Фактически достаточно доказать, что если G — некоторая порождающая матрица $\mathcal{C}$, то $\operatorname{Im} \ell_D = \operatorname{Im} \ell_G$.

Действительно, так как $\operatorname{Im} \ell_D = \operatorname{rank} R_D$, то в силу утверждения 7 верна цепочка равенств

$$\mathcal{C}^{\circ 2} = \operatorname{Im} \ell_G = \operatorname{Im} \ell_D = \operatorname{rank} R_D.$$

Охватывающая матрица в каких-то строках содержит порождающую матрицу кода. Будем считать для определенности, что это первые k строк. Пусть G — порождающая матрица, стоящая в первых k строках матрицы D. Итак, докажем, что $\operatorname{Im}\ell_G = \operatorname{Im}\ell_D$.

Рассмотрим произвольную квадратичную форму $Q \in \mathcal{Q}_\kappa(q)$. Пусть $L_i(x_1,\dots,x_k) = a_1x_1 + \dots + a_{i,k}x_k$, $i = k+1,\dots,\kappa$, — некоторые линейные функции над полем $\mathrm{GF}(q)$, т. е. $a_{i,j} \in \mathrm{GF}(q)$ для всех $i = k+1,\dots,\kappa$, $j = 1,2,\dots,k$.

Подставим в квадратичную форму $Q(x_1,\dots,x_\kappa)$ вместо переменной x_i функцию L_i, $i = k+1,\dots,\kappa$. Раскрывая скобки и приводя подобные слагаемые, несложно убедиться, что $Q_0 = Q(x_1,\dots,x_k,L_{k+1},\dots,L_\kappa)$ является квадратичной формой от переменных $x_1,\dots,x_k$, т. е. $Q_0 \in \mathcal{Q}_k(q)$. Поэтому если вектор $u \in V_\kappa^\top(q)$ таков, что

$$u = (u_1,u_2,\dots,u_k,L_{k+1}(u_1,\dots,u_k),\dots,L_\kappa(u_1,\dots,u_k))^\top,$$

то

$$\ell_u(Q) \stackrel{def}{=} Q(u) = Q_0(u_1,\dots,u_k) \stackrel{def}{=} \ell_{\widehat{u}}(Q_0), \tag{5}$$

здесь $\widehat{u} = (u_1,\dots,u_k)^\top \in V_k^\top(q)$.

Строки с номерами $k+1,\dots,\kappa$ матрицы D являются линейными комбинациями строк с номерами $1,2,\dots,k$, поэтому из соотношения (5) следует равенство

$$\ell_D(Q) = \ell_G(Q_0),$$

из которого следует включение $\operatorname{Im}\ell_D \subseteq \operatorname{Im}\ell_G$.

Докажем обратное включение $\operatorname{Im}\ell_G \subseteq \operatorname{Im}\ell_D$.

Рассмотрим квадратичную форму $Q_0(x_1,\dots,x_k) \in \mathcal{Q}_k(q)$. Добавлением к Q_0 мономов, зависящих от переменных $x_{k+1},\dots,x_\kappa$, можно получить квадратичную форму $Q(x_1,\dots,x_k,x_{k+1},\dots,x_\kappa) \in \mathcal{Q}_\kappa(q)$, зависящую от последних $\kappa - k$ переменных фиктивно. При этом по построению Q_0 для любого вектора $(u_1,\dots,u_k,u_{k+1},\dots,u_\kappa) \in V_\kappa(q)$ выполняется равенство

$$Q_0(u_1\dots,u_k) = Q(u_1,\dots,u_k,u_{k+1},\dots,u_\kappa).$$

Из него очевидно следует, что для любого $\widehat{u} = (u_{k+1},\dots,u_\kappa)^\top \in V_{\kappa-k}^\top(q)$ и любого $u = (u_1,\dots,u_k)^\top \in V_k^\top(q)$ справедливо равенство

$$\ell_u(Q) = \ell_{\binom{u}{\widehat{u}}}(Q_0). \tag{6}$$

Но из (6) получается равенство $\ell_G(Q_0) = \ell_D(Q)$, поэтому $\operatorname{Im}\ell_G \subseteq \operatorname{Im}\ell_D$. □

Утверждение 8. *Пусть G_i — некоторые $(k \times n_i)$-матрицы над полем* $\mathrm{GF}(q)$, $i = 1,2,\dots,u$. *Положим $n = n_1 + n_2 + \dots + n_u$. Матрица размера $(k \times n)$*

$$G = (G_1\|G_2\|\dots\|G_u)$$

охватывает некоторый код $\mathcal{C} \in \mathcal{C}_1\|\mathcal{C}_2\|\dots\|\mathcal{C}_u$, где $\mathcal{C}_i$ — $[n_i]_q$-код, охватываемый матрицей G_i, $i = 1,2,\dots,u$. Тогда

$$\mathcal{C}^{\circ 2} = \mathcal{C}_1^{\circ 2} \times \mathcal{C}_2^{\circ 2} \times \dots \times \mathcal{C}_u^{\circ 2}, \tag{7}$$

если и только если выполнено равенство

$$\operatorname{rank}(R_{G_1}\|R_{G_2}\|\dots\|R_{G_u}) = \sum_{i=1}^{u} \operatorname{rank} R_{G_i}. \tag{8}$$

Доказательство. Необходимость.

Пусть выполнено равенство (7), тогда

$$\dim \mathcal{C}^{\circ 2} = \sum_{i=1}^{u} \dim \mathcal{C}_i^{\circ 2}. \tag{9}$$

Но согласно следствию 3

$$\dim \mathcal{C}^{\circ 2} = \operatorname{rank}(R_{G_1}\|R_{G_2}\|\dots\|R_{G_u}),$$

и для любого $i = 1, 2, \dots, u$

$$\dim \mathcal{C}_i^{\circ 2} = \operatorname{rank} R_{G_i}.$$

Поэтому верно равенство (8).

Достаточность.

Пусть выполняется равенство (8), но тогда из следствия 3 получаем равенство (9), поэтому

$$\dim \mathcal{C}^{\circ 2} = \dim(\mathcal{C}_1^{\circ 2} \times \mathcal{C}_2^{\circ 2} \times \dots \times \mathcal{C}_u^{\circ 2}).$$

Откуда с учетом включения (1) получаем равенство (7). □

Таким образом, решение вопроса 1 сводится к определению вероятности того, что ранг матрицы, полученной объединением некоторых подматриц порождающей матрицы R кода $\mathcal{HRM}_q(2, k)$, равен сумме рангов этих подматриц.

4. Оценка вероятности того, что ранг матрицы равен сумме рангов ее подматриц

Для любого натурального $0 \leqslant s \leqslant n$ обозначим через $\mathbf{A}_n^s$ множество, которое содержит все подмножества $\alpha = \{i_1, i_2, \dots, i_s\} \subseteq \{0, 1, \dots, n-1\}$ из s элементов. Заметим, что $\mathbf{A}_n^0$ содержит только пустое подмножество $\varnothing$. Пусть также $S \subseteq \{0, 1, \dots, n-1\}$; через $\mathbf{A}_n^S$ обозначим объединение множеств $\mathbf{A}_n^i$, $i \in S$, т. е.

$$\mathbf{A}_n^S = \bigcup_{i \in S} \mathbf{A}_n^i,$$

при этом, если $S = \varnothing$, то и $\mathbf{A}_n^S = \varnothing$. Важные частные случаи S: «$\leqslant s = \{i : 1 \leqslant i \leqslant s\}$», «$< s = \{i : 1 \leqslant i < s\}$», «$\geqslant s = \{i : s \leqslant i \leqslant n\}$», «$> s = \{i : s < i \leqslant n\}$».

Далее, для каждого $\alpha \in \mathbf{A}_n^s$ через $\overline{\alpha}$ обозначим дополнение подмножества α до множества $\{0, 1, \dots, n-1\}$, т. е. $\overline{\alpha} = \{0, 1, \dots, n-1\} \setminus \alpha \in \mathbf{A}_n^{n-s}$. Заметим, что из определения следует равенство $\overline{\overline{\alpha}} = \alpha$.

И, наконец, для каждого $S \subseteq \{0, 1, \dots, n-1\}$ ($S \subseteq \{1, \dots, n\}$) определим множества $\widetilde{\mathbf{A}}_n^S$, которые отличаются от множеств $\mathbf{A}_n^S$ только тем, что каждый элемент $\widetilde{\alpha}$ этих множеств может быть мультимножеством с элементами из $\{0, 1, \dots, n-1\}$.

Рассмотрим произвольную $(k\times n)$-матрицу G. Тогда для $\alpha \in \widetilde{\mathbf{A}}_n^s$ через G_α обозначим $(k \times s)$-подматрицу матрицы G, составленную из столбцов матрицы G с номерами из множества α. Будем предполагать для определенности, что столбцы в G_α упорядочены по возрастанию номеров в множестве α.

Пусть $\varepsilon(\cdot)\colon \mathbb{R} \to \mathbb{R}$ и $b(\cdot)\colon \mathbb{R} \to \mathbb{R}$ — некоторые функции, заданные на множестве действительных чисел $\mathbb{R}$, пусть также $t \in \mathbb{N}$. Следуя работе [17], обозначим через $\mathbf{P}_{\varepsilon,b}(t)$ класс таких матриц G над полем $\mathrm{GF}(q)$, что для любого $\alpha \in \mathbf{A}_n^{>\varepsilon(t)\cdot\frac{n}{k}}$ подматрица G_α имеет ранг больше, чем $b(t)$, здесь k — число строк матрицы G, а n — число ее столбцов.

Более того, для произвольного $T \subseteq \mathbb{N}$ через $\mathbf{P}_{\varepsilon,b}(T)$ обозначим пересечение классов $\mathbf{P}_{\varepsilon,b}(t)$, $t \in T$,

$$\mathbf{P}_{\varepsilon,b}(T) = \bigcap_{t\in T} \mathbf{P}_{\varepsilon,b}(t),$$

т. е. $(k\times n)$-матрица G лежит в $\mathbf{P}_{\varepsilon,b}(T)$, если и только если для любого $t \in T$, любого $\alpha \in \mathbf{A}_n^{>\varepsilon(t)\cdot\frac{n}{k}}$ подматрица G_α имеет ранг больше, чем $b(t)$.

В [17] доказано следующее утверждение.

Утверждение 9. *Пусть $(K\times N)$-матрица $X \in \mathbf{P}_{\varepsilon,b}(t)$. Тогда если для некоторого $\beta \in \mathbf{A}_N^{\leqslant N}$ выполнено неравенство $\operatorname{rank} X_\beta \leqslant b(t)$, то $|\operatorname{span}_X(\beta)| \leqslant \varepsilon(t)\cdot\frac{N}{K}$. Здесь через $\operatorname{span}_X(\beta)$ обозначается множество номеров столбцов матрицы X, которые лежат в линейной оболочке столбцов подматрицы X_β.*

Пусть $\widetilde{\beta} \in \widetilde{\mathbf{A}}_N^{\leqslant N}$. Рассмотрим $\beta \in \mathbf{A}_N^{\leqslant N}$, получающееся из мультимножества $\widetilde{\beta}$ удалением повторяющихся элементов. Тогда для любой $(K\times N)$-матрицы X верны очевидные равенства $\operatorname{rank} X_{\widetilde{\beta}} = \operatorname{rank} X_\beta$ и $\operatorname{span}_X(\widetilde{\beta}) = \operatorname{span}_X(\beta)$, поэтому из утверждения 9 получаем следующее утверждение.

Утверждение 10. *Пусть $(K\times N)$-матрица $X \in \mathbf{P}_{\varepsilon,b}(t)$. Тогда если для некоторого $\widetilde{\beta} \in \widetilde{\mathbf{A}}_N^{\leqslant N}$ выполнено неравенство $\operatorname{rank} X_{\widetilde{\beta}} \leqslant b(t)$, то $|\operatorname{span}_X(\widetilde{\beta})| \leqslant \varepsilon(t)\cdot\frac{N}{K}$.*

В этом разделе доказаны два центральных утверждения. В утверждении 14 получена оценка вероятности того, что ранг матрицы равен сумме рангов подматриц, при условии, что столбцы матрицы выбираются из некоторой другой матрицы X, которая лежит в классе $\mathbf{P}_{\varepsilon,b}(t)$. Оказывается, что в этом случае вероятность можно оценить снизу через значение функции $\varepsilon(t)$ и параметры матрицы.

Утверждение 15 позволяет распространить оценку утверждения 14 на случай, когда подматрицы образуются из некоторой фиксированной подматрицы X_α матрицы X применением к номерам α случайных подстановок σ из группы подстановок, заданной на множестве номеров столбцов матрицы X.

4.1. Критерий того, что ранг матрицы равен сумме рангов подматриц.

Сперва установим удобный для дальнейшего критерий того, что ранг матрицы равен сумме рангов подматриц.

Пусть k и N — некоторые натуральные числа. Для любых векторов $x_1, \ldots, x_n \in V_K^\top(q)$ обозначим через $L(x_1, \ldots, x_n)$ линейную оболочку этих векторов над полем $\mathrm{GF}(q)$, т. е.

$$L(x_1, \ldots, x_n) = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n \mid a_1, a_2, \ldots, a_n \in \mathrm{GF}(q)\}.$$

Для краткости линейную оболочку столбцов произвольной $(K \times n)$-матрицы $X = (x_1 \dots x_n)$, $x_i \in V_K^{\top}(q)$, $i = 1, 2, \dots, n$, будем обозначать $L(X)$.

Как и раньше, через $\operatorname{span}_X(\alpha) \in \mathbf{A}_n^{\leqslant n}$ для любого $\alpha = \{\alpha_1, \dots, \alpha_s\} \in \widetilde{\mathbf{A}}_n^s$ обозначим множество, состоящее из номеров тех столбцов $(K \times n)$-матрицы X, которые лежат в линейной оболочке столбцов $x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_s}$:

$$\operatorname{span}_X(\alpha) = \{0 \leqslant i \leqslant n-1 \mid x_i \in L(X_\alpha)\}.$$

Заметим, что для любой матрицы X, состоящей из n столбцов, span_X является отображением из множества $\widetilde{\mathbf{A}}_n^{\leqslant n}$ в множество $\mathbf{A}_n^{\leqslant n}$, т. е.

$$\operatorname{span}_X \colon \widetilde{\mathbf{A}}_n^{\leqslant n} \to \mathbf{A}_n^{\leqslant n}.$$

Стандартными рассуждениями из линейной алгебры несложно доказать следующее утверждение.

Утверждение 11. *Пусть $X = (X_1 \| X_2)$ для некоторых $(K \times n_1)$-матрицы X_1 и $(K \times n_2)$-матрицы X_2. Будем считать, что столбцы матрицы X занумерованы числами от 1 до n_1+n_2 таким образом, что $X_{\{1,\dots,n_1\}} = X_1$ и $X_{\{n_1+1,\dots,n_1+n_2\}} = X_2$. Тогда $\operatorname{rank} X = \operatorname{rank} X_1 + \operatorname{rank} X_2$, если и только если для любого $j = 1, 2, \dots, n_2$ выполняется условие: если $x_{n_1+j} \notin L(x_{n_1+1}, \dots, x_{n_1+j-1})$, то $x_{n_1+j} \notin L(X_1, x_{n_1+1}, \dots, x_{n_1+j-1})$.*

В качестве следствия из утверждения 11 установим теперь необходимое и достаточное условие того, что ранг матрицы равен сумме рангов подматриц, при условии, что сама матрица сформирована из столбцов некоторой большой матрицы.

Утверждение 12. *Рассмотрим некоторую $(K \times N)$-матрицу X. Пусть $\beta \in \widetilde{\mathbf{A}}_n^{n_1}$ и $\gamma \in \widetilde{\mathbf{A}}_n^{n_2}$, $n_1 + n_2 = n$. Тогда $\operatorname{rank} X_{\beta\cup\gamma} = \operatorname{rank} X_\beta + \operatorname{rank} X_\gamma$, если и только если для любого $j = 1, 2, \dots, n_2$ выполняется условие: если $\gamma_j \notin \operatorname{span}_X(\{\gamma_1, \dots, \gamma_{j-1}\})$, то $\gamma_j \notin \operatorname{span}_X(\beta \cup \{\gamma_1, \dots, \gamma_{j-1}\})$.*

Утверждение 13. *Ранг матрицы $X = (X_1 \| X_2 \| \dots \| X_u)$ равен сумме рангов матриц $X_1, X_2, \dots, X_u$, если и только если $\operatorname{rank} X = \operatorname{rank} X_u + \operatorname{rank}(X_1 \| X_2 \| \dots \| X_{u-1})$ и $\operatorname{rank}(X_1 \| X_2 \| \dots \| X_{u-1}) = \sum_{i=1}^{u-1} \operatorname{rank} X_i$.*

Доказательство. Достаточность очевидна. Докажем необходимость.

Пусть $\operatorname{rank} X = \sum_{i=1}^{u} \operatorname{rank} X_i$. Но $\operatorname{rank} X \leqslant \operatorname{rank} X_u + \operatorname{rank}(X_1 \| X_2 \| \dots X_{u-1})$. Поэтому

$$\sum_{i=1}^{u} \operatorname{rank} X_i = \operatorname{rank} X \leqslant \operatorname{rank} X_u + \operatorname{rank}(X_1 \| X_2 \| \dots \| X_{u-1})$$
$$\Rightarrow \sum_{i=1}^{u-1} \operatorname{rank} X_i \leqslant \operatorname{rank}(X_1 \| X_2 \| \dots \| X_{u-1}).$$

Но так как $\operatorname{rank}(X_1 \| X_2 \| \dots \| X_{u-1}) \leqslant \sum_{i=1}^{u-1} \operatorname{rank} X_i$, то выполняется точное равенство

$$\operatorname{rank}(X_1 \| X_2 \| \dots \| X_{u-1}) = \sum_{i=1}^{u-1} \operatorname{rank} X_i. \tag{10}$$

Если же $\operatorname{rank} X < \operatorname{rank} X_u + \operatorname{rank}(X_1 \| X_2 \| \dots \| X_{u-1})$, то с учетом (10) получим строгое неравенство

$$\sum_{i=1}^{u} \operatorname{rank} X_i < \sum_{i=1}^{u} \operatorname{rank} X_i.$$

Противоречие. □

4.2. Оценка вероятности. Рассмотрим следующую вероятностную схему. Будем последовательно из множества $\{0, 1, \ldots, N-1\}$ выбирать случайно с одинаковыми вероятностями номера $\alpha_1, \alpha_2, \ldots, \alpha_s$, используя выборку с возвращением. В итоге получится $\widetilde{\alpha} = \{\alpha_1, \ldots, \alpha_s\}$ — мультимножество, т. е. множество, содержащее, возможно, повторяющиеся элементы. Описанный процесс построения $\widetilde{\alpha}$ будем обозначать $\widetilde{\alpha} \xleftarrow{\$} \widetilde{\mathbf{A}}_N^s$.

Рассмотрим некоторую $(K \times N)$-матрицу X. Выберем некоторое $\widetilde{\beta} \in \widetilde{\mathbf{A}}_N^{n_0}$. Далее случайно выберем $\widetilde{\gamma} \xleftarrow{\$} \widetilde{\mathbf{A}}_N^{n_1}$. Найдем вероятность того, что $\operatorname{rank} X_{\widetilde{\beta}\cup\widetilde{\gamma}} = \operatorname{rank} X_{\widetilde{\beta}} + \operatorname{rank} X_{\widetilde{\gamma}}$.

Лемма 1. *Пусть* $X \in \mathbf{P}_{\varepsilon,b}(t)$. *Зафиксируем некоторое* $\widetilde{\beta} \in \widetilde{\mathbf{A}}_N^{n_0}$. *Выберем* $\widetilde{\gamma} \xleftarrow{\$} \widetilde{\mathbf{A}}_N^{n_1}$. *Тогда если* $1 \leqslant n = n_0 + n_1 \leqslant b(t) < K$, *то*

$$\mathbf{P}\big\{\operatorname{rank} X_{\widetilde{\beta}\cup\widetilde{\gamma}} = \operatorname{rank} X_{\widetilde{\beta}} + \operatorname{rank} X_{\widetilde{\gamma}}\big\} \geqslant 1 - \varepsilon(t) \cdot \frac{n_1}{K}.$$

Доказательство. Пусть Γ — событие, которое состоит в том, что $\operatorname{rank} X_{\widetilde{\beta}\cup\widetilde{\gamma}} = \operatorname{rank} X_{\widetilde{\beta}} + \operatorname{rank} X_{\widetilde{\gamma}}$. Тогда дополнительное к Γ — это событие $\overline{\Gamma}$, которое состоит в том, что $\operatorname{rank} X_{\widetilde{\beta}\cup\widetilde{\gamma}} \neq \operatorname{rank} X_{\widetilde{\beta}} + \operatorname{rank} X_{\widetilde{\gamma}}$.

Согласно утверждению 12 событие $\overline{\Gamma}$ происходит, если реализуется хотя бы одно из событий $\delta_1, \ldots, \delta_{n_1}$. Событие $\delta_j, j = 1, 2, \ldots, n_1$, состоит в том, что случайно выбранный столбец $\gamma_j \notin \operatorname{span}_X(\{\gamma_1, \ldots, \gamma_{j-1}\})$ и при этом $\gamma_j \in \operatorname{span}_X(\widetilde{\beta} \cup \{\gamma_1, \ldots, \gamma_{j-1}\})$, т. е.

$$\delta_j = \{\gamma_j \notin \operatorname{span}_X(\{\gamma_1, \ldots, \gamma_{j-1}\})\} \cap \big\{\gamma_j \in \operatorname{span}_X\big(\widetilde{\beta} \cup \{\gamma_1, \ldots, \gamma_{j-1}\}\big)\big\}.$$

Значит,

$$\mathbf{P}\{\overline{\Gamma}\} \leqslant \sum_{j=1}^{n_1} \mathbf{P}\{\delta_j\}. \tag{11}$$

Теперь оценим $\mathbf{P}\{\delta_j\}$. Так как δ_j при любом $j = 1, 2, \ldots, n_1$ является пересечением двух событий, одно из которых $\Delta_j = \{\gamma_j \in \operatorname{span}_X(\widetilde{\beta} \cup \{\gamma_1, \ldots, \gamma_{j-1}\})\}$, то верно неравенство $\mathbf{P}\{\delta_j\} \leqslant \mathbf{P}\{\Delta_j\}$.

Рассмотрим теперь событие Δ_j. Для всех $j = 1, 2, \ldots, n_1$ выполняется равенство

$$\mathbf{P}\{\Delta_j\} = \sum_{\gamma_1'=0}^{N-1} \sum_{\gamma_2'=0}^{N-1} \cdots \sum_{\gamma_{j-1}'=0}^{N-1} \mathbf{P}\{\Delta_j', \gamma_1 = \gamma_1', \ldots, \gamma_{j-1} = \gamma_{j-1}'\}, \tag{12}$$

здесь $\Delta_j' = \{\gamma_j \in \operatorname{span}_X(\widetilde{\beta} \cup \{\gamma_1', \ldots, \gamma_{j-1}'\})\}$ — событие, которое рассматривается при фиксированных значениях $\gamma_1', \ldots, \gamma_{j-1}'$. Таким образом, Δ_j' зависит только от случайной величины γ_j и не зависит от случайных величин $\gamma_1, \gamma_2, \ldots, \gamma_{j-1}$.

Так как все $\gamma_1, \ldots, \gamma_{j-1}, \gamma_j$ выбираются независимо друг от друга, то все события Δ_j', $\{\gamma_1 = \gamma_1'\}, \ldots, \{\gamma_{j-1} = \gamma_{j-1}'\}$, независимы, а значит,

$$\mathbf{P}\{\Delta_j', \gamma_1 = \gamma_1', \ldots, \gamma_{j-1} = \gamma_{j-1}'\} = \mathbf{P}\{\Delta_j'\} \cdot \prod_{i=1}^{j-1} \mathbf{P}\{\gamma_i = \gamma_i'\}. \tag{13}$$

Далее, все $\gamma_1, \ldots, \gamma_{j-1}$ выбираются равновероятно, поэтому $\mathbf{P}\{\gamma_i = \gamma'_i\} = 1/N$ для всех $i = 1, 2, \ldots, j-1$. Но тогда из (13) получим, что

$$\mathbf{P}\{\Delta'_j, \gamma_1 = \gamma'_1, \gamma_2 = \gamma'_2, \ldots, \gamma_{j-1} = \gamma'_{j-1}\} = \frac{1}{N^{j-1}} \mathbf{P}\{\Delta'_j\}. \tag{14}$$

Так как $\gamma'_1, \ldots, \gamma'_{j-1}$ — некоторые произвольные, но фиксированные элементы множества $\{0, 1, \ldots, N-1\}$, то для всех $j = 1, 2, \ldots, n_1$, выполнено равенство

$$\mathbf{P}\{\Delta'_j\} = \frac{\left|\operatorname{span}_X(\widetilde{\beta} \cup \{\gamma'_1, \ldots, \gamma'_{j-1}\})\right|}{N}. \tag{15}$$

Но тогда из условий леммы и утверждения 10 следует, что

$$\mathbf{P}\{\Delta'_j\} \leqslant \frac{\varepsilon(t)}{K}.$$

Подставляя эту оценку в равенство (14), получаем

$$\mathbf{P}\{\Delta'_j, \gamma_1 = \gamma'_1, \gamma_2 = \gamma'_2, \ldots, \gamma_{j-1} = \gamma'_{j-1}\} \leqslant \frac{1}{N^{j-1}} \frac{\varepsilon(t)}{K}.$$

Но тогда из равенства (12) следует, что для любого $j = 1, 2, \ldots, n_1$

$$\mathbf{P}\{\Delta_j\} \leqslant \frac{\varepsilon(t)}{K} \cdot \sum_{\gamma'_1=0}^{N-1} \sum_{\gamma'_2=0}^{N-1} \cdots \sum_{\gamma'_{j-1}=0}^{N-1} \frac{1}{N^{j-1}} = \frac{\varepsilon(t)}{K}.$$

Поэтому из (11) с учетом того, что $\mathbf{P}\{\delta_j\} \leqslant \mathbf{P}\{\Delta_j\}$, $j = 1, 2, \ldots, n_1$, следует неравенство

$$\mathbf{P}\{\overline{\Gamma}\} \leqslant \varepsilon(t) \cdot \frac{n_1}{K}.$$

Получается, что вероятность события Γ не меньше $1 - \varepsilon(t) \cdot \frac{n_1}{K}$. □

Утверждение 14. *Пусть $X \in \mathbf{P}_{\varepsilon,\beta}(t)$. Зафиксируем некоторое $\widetilde{\gamma}_0 \in \widetilde{\mathbf{A}}_N^{n_0}$. Выберем последовательно $\widetilde{\gamma}_1 \xleftarrow{\$} \widetilde{\mathbf{A}}_N^{n_1}, \widetilde{\gamma}_2 \xleftarrow{\$} \widetilde{\mathbf{A}}_N^{n_2}, \ldots, \widetilde{\gamma}_u \xleftarrow{\$} \widetilde{\mathbf{A}}_N^{n_u}$.*

Тогда если $1 \leqslant n = \sum_{i=0}^{u} n_i \leqslant b(t) < K$, то верно неравенство

$$\mathbf{P}\left\{\operatorname{rank} X_{\widetilde{\gamma}_0 \cup \widetilde{\gamma}_1 \cup \cdots \cup \widetilde{\gamma}_u} = \sum_{i=0}^{u} \operatorname{rank} X_{\widetilde{\gamma}_i}\right\} \geqslant 1 - \varepsilon(t) \frac{\sum_{i=1}^{u} n_i}{K}.$$

Доказательство. Проведем доказательство по индукции. При $u = 1$ утверждение следует из леммы 1.

Пусть утверждение верно для всех значений, меньших u. Докажем, что оно верно для u.

Оценим сверху вероятность события

$$\Gamma = \left\{\operatorname{rank} X_{\widetilde{\gamma}_0 \cup \widetilde{\gamma}_1 \cup \cdots \cup \widetilde{\gamma}_u} \neq \sum_{i=0}^{u} \operatorname{rank} X_{\widetilde{\gamma}_i}\right\}.$$

Тогда из равенства

$$\mathbf{P}\left\{\operatorname{rank} X_{\widetilde{\gamma}_0\cup\widetilde{\gamma}_1\cup\cdots\cup\widetilde{\gamma}_u} = \sum_{i=0}^{u}\operatorname{rank} X_{\widetilde{\gamma}_i}\right\} = 1 - \mathbf{P}\{\Gamma\}$$

получим оценку снизу для нужного нам события.
По утверждению 13 событие Γ происходит при реализации любого из двух событий

$$\Gamma_1 = \left\{\operatorname{rank} X_{\widetilde{\gamma}_0\cup\widetilde{\gamma}_1\cup\cdots\cup\widetilde{\gamma}_{u-1}} \neq \sum_{i=0}^{u-1}\operatorname{rank} X_{\widetilde{\gamma}_i}\right\}$$

или

$$\Gamma_2 = \{\operatorname{rank}(X_{\widetilde{\gamma}_0\cup\widetilde{\gamma}_1\cup\cdots\cup\widetilde{\gamma}_{u-1}}\|X_{\widetilde{\gamma}_u}) \neq \operatorname{rank} X_{\widetilde{\gamma}_0\cup\widetilde{\gamma}_1\cup\cdots\cup\widetilde{\gamma}_{u-1}} + \operatorname{rank} X_{\widetilde{\gamma}_u}\}.$$

Поэтому

$$\mathbf{P}\{\Gamma\} \leqslant \mathbf{P}\{\Gamma_1\} + \mathbf{P}\{\Gamma_2\}. \tag{16}$$

По предположению индукции

$$\mathbf{P}\{\Gamma_1\} \leqslant \varepsilon(t)\frac{\sum_{i=1}^{u-1} n_i}{K}. \tag{17}$$

Теперь, используя формулу полной вероятности, можно записать, что

$$\mathbf{P}\{\Gamma_2\} = \sum_{\gamma'_1=0}^{N-1}\sum_{\gamma'_2=0}^{N-1}\cdots\sum_{\gamma'_{u-1}=0}^{N-1}\mathbf{P}\{\Gamma'_2, \gamma_1=\gamma'_1,\ldots,\gamma_{u-1}=\gamma'_{u-1}\}, \tag{18}$$

здесь

$$\Gamma'_2 = \{\operatorname{rank}(X_{\widetilde{\gamma}_0\cup\widetilde{\gamma}'_1\cup\cdots\cup\widetilde{\gamma}'_{u-1}}\|X_{\widetilde{\gamma}_u}) \neq \operatorname{rank} X_{\widetilde{\gamma}_0\cup\widetilde{\gamma}'_1\cup\cdots\cup\widetilde{\gamma}'_{u-1}} + \operatorname{rank} X_{\widetilde{\gamma}_u}\}.$$

Если положить $\widetilde{\beta} = \widetilde{\gamma}_0\cup\widetilde{\gamma}'_1\cup\cdots\cup\widetilde{\gamma}'_{u-1}$, $\widetilde{\gamma} = \widetilde{\gamma}_u$, то из леммы 1 следует неравенство

$$\mathbf{P}\{\Gamma'_2\} \leqslant \varepsilon(t)\cdot\frac{n_u}{K}.$$

С учетом этого неравенства, пользуясь независимостью в совокупности событий $\Gamma'_2, \{\gamma_1=\gamma'_1\},\ldots,\{\gamma_{u-1}=\gamma'_{u-1}\}$, из (18) получим

$$\mathbf{P}\{\Gamma_2\} \leqslant \varepsilon(t)\cdot\frac{n_u}{K}\sum_{\gamma'_1=0}^{N-1}\sum_{\gamma'_2=0}^{N-1}\cdots\sum_{\gamma'_{u-1}=0}^{N-1}\mathbf{P}\{\gamma_1=\gamma'_1,\ldots,\gamma_{u-1}=\gamma'_{u-1}\}.$$

Отсюда следует, что

$$\mathbf{P}\{\Gamma_2\} \leqslant \varepsilon(t)\cdot\frac{n_u}{K} \tag{19}$$

Теперь, объединяя неравенства (16), (17) и (19), окончательно получим

$$\mathbf{P}\{\Gamma\} \leqslant \varepsilon(t)\frac{\sum_{i=1}^{u-1} n_i}{K} + \varepsilon(t)\cdot\frac{n_u}{K} = \varepsilon(t)\frac{\sum_{i=1}^{u} n_i}{K}. \qquad \square$$

4.3. Случай подматриц, которые получаются отображением, заданным на номерах столбцов. Пусть $\mathcal{S}_N$ — группа подстановок на множестве $\{0, 1, \ldots, N-1\}$. Для любого мультиподмножества $\widetilde{\gamma} = \{\gamma_1, \ldots, \gamma_s\} \in \widetilde{\mathbf{A}}_N^s$ и подстановки $\sigma \in \mathcal{S}_N$ обозначим через $\sigma(\widetilde{\gamma})$ мультиподмножество

$$\sigma(\widetilde{\gamma}) = \{\sigma(\gamma_1), \ldots, \sigma(\gamma_s)\} \in \widetilde{\mathbf{A}}_N^s.$$

Зададим на любом подмножестве $\mathcal{S}$ группы $\mathcal{S}_N$ следующую вероятностную схему. Будем равновероятно из множества $\mathcal{S}$ выбирать подстановку σ. Тот факт, что σ получена с помощью описанной схемы, будем записывать формулой $\sigma \overset{\$}{\leftarrow} \mathcal{S}$.

Лемма 2. *Рассмотрим $(K \times N)$-матрицу $X \in \mathbf{P}_{\varepsilon,b}(t)$. Зафиксируем $\widetilde{\beta}_0 \in \widetilde{\mathbf{A}}_N^{n_0}$ и $\widetilde{\beta}_1 \in \widetilde{\mathbf{A}}_N^{n_1}$. Выберем $\sigma \overset{\$}{\leftarrow} \mathcal{S}_N$. Тогда если $1 \leqslant n = n_0 + n_1 \leqslant b(t) \leqslant K$, то вероятность того, что* $\operatorname{rank} X_{\widetilde{\beta}_1 \cup \sigma(\widetilde{\beta}_0)} = \operatorname{rank} X_{\widetilde{\beta}_1} + \operatorname{rank} X_{\sigma(\widetilde{\beta}_0)}$, *не меньше* $1 - \varepsilon(t)\frac{n_0 N}{K(N-n_0)}$, *т. е.*

$$\mathbf{P}\big\{\operatorname{rank} X_{\widetilde{\beta}_1 \cup \sigma(\widetilde{\beta}_0)} = \operatorname{rank} X_{\widetilde{\beta}_1} + \operatorname{rank} X_{\sigma(\widetilde{\beta}_0)}\big\} \geqslant 1 - \varepsilon(t) \cdot \frac{n_0 \cdot N}{K(N - n_0)}.$$

Доказательство. Пусть Γ — событие, которое состоит в том, что $\operatorname{rank} X_{\widetilde{\beta}_1 \cup \sigma(\widetilde{\beta}_0)} = \operatorname{rank} X_{\widetilde{\beta}_1} + \operatorname{rank} X_{\sigma(\widetilde{\beta}_0)}$.

Тогда дополнительное к Γ — это событие $\overline{\Gamma}$, которое состоит в том, что $\operatorname{rank} X_{\widetilde{\beta}_1 \cup \sigma(\widetilde{\beta}_0)} \neq \operatorname{rank} X_{\widetilde{\beta}_1} + \operatorname{rank} X_{\sigma(\widetilde{\beta}_0)}$.

Пусть $\widetilde{\beta}_0 = (\beta_1, \ldots, \beta_{n_0})$. Согласно утверждению 12, событие $\overline{\Gamma}$ возникает при реализации хотя бы одного из событий $\Delta_1, \ldots, \Delta_{n_0}$. Событие Δ_j, $j = 1, 2, \ldots, n_0$, состоит в том, что столбец $\sigma(\beta_j) \notin \operatorname{span}_X(\{\sigma(\beta_1), \ldots, \sigma(\beta_{j-1})\})$ и при этом $\sigma(\beta_j) \in \operatorname{span}_X(\widetilde{\beta}_1 \cup \{\sigma(\beta_1), \ldots, \sigma(\beta_{j-1})\})$, т. е.

$$\Delta_j = \big\{\sigma(\beta_j) \notin \operatorname{span}_X(\{\sigma(\beta_1), \ldots, \sigma(\beta_{j-1})\})\big\} \cap \big\{\sigma(\beta_j) \in \operatorname{span}_X(\widetilde{\beta}_1 \cup \{\sigma(\beta_1), \ldots, \sigma(\beta_{j-1})\})\big\}.$$

Значит,

$$\mathbf{P}\{\overline{\Gamma}\} \leqslant \sum_{j=1}^{n_0} \mathbf{P}\{\Delta_j\}. \tag{20}$$

Теперь оценим $\mathbf{P}\{\Delta_j\}$.

Для любых $\gamma_1, \ldots, \gamma_s \in \widetilde{\mathbf{A}}_N$ через $D(\gamma_1, \ldots, \gamma_s)$ обозначим множество

$$D(\gamma_1, \ldots, \gamma_s) = \operatorname{span}_X(\widetilde{\beta}_1 \cup \{\gamma_1, \ldots, \gamma_s\}) \setminus \operatorname{span}_X(\{\gamma_1, \ldots, \gamma_s\}).$$

Тогда для любого $j = 1, 2, \ldots, n_0$ можно записать

$$\Delta_j = \{\sigma(\beta_j) \in D(\sigma(\beta_1), \ldots, \sigma(\beta_{j-1}))\}.$$

Зафиксируем некоторые числа $0 \leqslant i_1, i_2, \ldots, i_{j-1} \leqslant N-1$. Рассмотрим множества $\mathcal{S}(i_1, \ldots, i_{j-1})$, состоящие из таких подстановок $\sigma \in \mathcal{S}_N$, что $\sigma(\beta_1) = i_1, \sigma(\beta_2) = i_2, \ldots, \sigma(\beta_{j-1}) = i_{j-1}$. Ясно, что если векторы $(i'_1, \ldots, i'_{j-1})$ и $(i''_1, \ldots, i''_{j-1})$ различны, то $\mathcal{S}(i'_1, \ldots, i'_{j-1})$ и $\mathcal{S}(i''_1, \ldots, i''_{j-1})$ не пересекаются.

Но тогда по формуле полной вероятности получим, что

$$\mathbf{P}\{\Delta_j\} = \sum_{i_1, \ldots, i_{j-1}} \mathbf{P}\{\sigma(\beta_j) \in D(i_1, \ldots, i_{j-1}) \,|\, \sigma \in \mathcal{S}(i_1, \ldots, i_{j-1}))\} \cdot \mathbf{P}\{\sigma \in S(i_1, \ldots, i_{j-1})\}. \tag{21}$$

При этом в (21) сумма берется только по таким наборам $(i_1, \ldots, i_{j-1})$, что $\mathcal{S}(i_1, \ldots, i_{j-1})$ не пусто, т. е. $\mathbf{P}\{\sigma \in S(i_1, \ldots, i_{j-1})\} > 0$.

Оценим условную вероятность

$$P_j = P_j(i_1, \ldots, i_{j-1}) = \mathbf{P}\{\sigma(\beta_j) \in D(i_1, \ldots, i_{j-1}) \mid \sigma \in \mathcal{S}(i_1, \ldots, i_{j-1})\}.$$

Так как событие $\{\sigma(\beta_j) \in D(i_1, \ldots, i_{j-1})\}$ реализуется в случаях, когда существует такое $i_j \in D(i_1, \ldots, i_{j-1})$, что $\sigma(\beta_j) = i_j$, то

$$P_j = \sum_{i_j \in D(i_1, \ldots, i_{j-1})} \mathbf{P}\{\sigma(\beta_j) = i_j \mid \sigma \in \mathcal{S}(i_1, \ldots, i_{j-1})\}.$$

Для начала заметим, что если среди подстановок $\sigma \in \mathcal{S}(i_1, \ldots, i_{j-1})$ не существует таких, что $\sigma(\beta_j) = i_j$, то вероятность $\mathbf{P}\{\sigma(\beta_j) = i_j \mid \sigma \in \mathcal{S}(i_1, \ldots, i_{j-1}))\}$ равна 0, и в этом случае она будет оцениваться сверху любым неотрицательным числом.

Оценим долю подстановок σ из $\mathcal{S}(i_1, \ldots, i_{j-1})$, для которых выполняется равенство $\sigma(\beta_j) = i_j$, при условии, что такие подстановки там существуют.

Множество $D(i_1, \ldots, i_{j-1})$ не содержит чисел $i_1, \ldots, i_{j-1}$, так как они лежат в множестве $\operatorname{span}_X(\{i_1, \ldots, i_{j-1}\})$, которое не содержится в $D(i_1, \ldots, i_{j-1})$ по построению. Значит, можно, считать, что i_j отличается от чисел $i_1, i_2, \ldots, i_{j-1}$.

Поэтому если $\beta_j \in \{\beta_1, \ldots, \beta_{j-1}\}$, то $\mathbf{P}\{\sigma(\beta_j) = i_j \mid \sigma \in \mathcal{S}(i_1, \ldots, i_{j-1})\}$ равна нулю.

Осталось рассмотреть случай, когда $\beta_j \notin \{\beta_1, \ldots, \beta_{j-1}\}$. Пусть среди элементов $\beta_1, \ldots, \beta_{j-1}$ ровно $t < j$ различных, не ограничивая общности, будем считать, что это первые t: $\beta_1, \ldots, \beta_t$. Тогда общее количество подстановок из $\sigma \in \mathcal{S}_N$, для которых $\sigma(\beta_1) = i_1, \ldots, \sigma(\beta_t) = i_t$, равно $(N-t)!$ Общее же число подстановок из $\sigma \in \mathcal{S}_N$, для которых $\sigma(\beta_1) = i_1, \ldots, \sigma(\beta_t) = i_t, \sigma(\beta_j) = i_j$, равно $(N-t-1)!$ Значит, в этом случае

$$\mathbf{P}\{\sigma(\beta_j) = i_j \mid \sigma \in \mathcal{S}(i_1, \ldots, i_{j-1}))\} = \frac{(N-t-1)!}{(N-t)!} = \frac{1}{N-t} < \frac{1}{N-j}.$$

Заметив, что $j \leqslant n_0$, получим неравенство

$$\mathbf{P}\{\sigma(\beta_j) = i_j \mid \sigma \in \mathcal{S}(i_1, \ldots, i_{j-1}))\} = \frac{(N-t-1)!}{(N-t)!} = \frac{1}{N-t} \leqslant \frac{1}{N-n_0},$$

верное для всех j, $1 \leqslant j \leqslant n_0$, и всех $\beta_j, i_1, i_2, \ldots, i_{j-1}$, для которых $\mathcal{S}(i_1, \ldots, i_{j-1})$ непусто.

Но тогда выполняется неравенство

$$P_j \leqslant \frac{|D(i_1, \ldots, i_{j-1})|}{N-n_0}.$$

Далее, $|D(i_1, \ldots, i_{j-1})| \leqslant |\operatorname{span}_X(\widetilde{\beta}_1 \cup \{i_1, \ldots, i_{j-1}\})|$, поэтому

$$P_j \leqslant \frac{|\operatorname{span}_X(\widetilde{\beta}_1 \cup \{i_1, \ldots, i_{j-1}\})|}{N-n_0}.$$

Так как $n_1 + j - 1 \leqslant n_0 + n_1 - 1 = n - 1 < b(t) \leqslant K$, то для всех $1 \leqslant j \leqslant n_0$ число столбцов в матрице $X_{\widetilde{\beta}_1 \cup \{i_1,\ldots,i_{j-1}\}}$ строго меньше $b(t)$. Но тогда верно неравенство $\operatorname{rank} X_{\widetilde{\beta}_1 \cup \{i_1,\ldots,i_{j-1}\}} < b(t)$. Значит, из утверждения 10 следует, что

$$\left|\operatorname{span}_X\left(\widetilde{\beta}_1 \cup \{i_1, \ldots, i_{j-1}\}\right)\right| \leqslant \varepsilon(t) \cdot \frac{N}{K}.$$

Тогда для любых $0 \leqslant i_1, \ldots, i_{j-1} \leqslant N - 1$ верно неравенство

$$P_j \leqslant \varepsilon(t) \cdot \frac{N}{K(N - n_0)}.$$

Поэтому из соотношения (21) следует неравенство

$$\mathbf{P}\{\Delta_j\} \leqslant \varepsilon(t) \cdot \frac{N}{K(N - n_0)} \cdot \sum_{(i_1,\ldots,i_{j-1})} \mathbf{P}\{\sigma \in S(i_1, \ldots, i_{j-1})\}.$$

Учитывая, что $\sum_{(i_1,\ldots,i_{j-1})} \mathbf{P}\{\sigma \in S(i_1, \ldots, i_{j-1})\} = 1$, приходим к оценке вероятности события Δ_j

$$\mathbf{P}\{\Delta_j\} \leqslant \varepsilon(t) \cdot \frac{N}{K(N - n_0)}.$$

Из этой оценки с учетом неравенств (20) получим, что

$$\mathbf{P}\{\overline{\Gamma}\} \leqslant \varepsilon(t) \cdot \frac{n_0 N}{K(N - n_0)}. \qquad \square$$

Утверждение 15. *Рассмотрим $(K \times N)$-матрицу $X \in \mathbf{P}_{\varepsilon,b}(t)$. Для $i = 0, 1, \ldots, u$ зафиксируем $\widetilde{\gamma}_i \in \widetilde{\mathbf{A}}_N^{n_i}$. Выберем независимо друг от друга $\sigma_1, \sigma_2, \ldots, \sigma_u \overset{\$}{\leftarrow} \mathcal{S}_N$. Пусть также σ_0 — тождественная подстановка. Тогда если $1 \leqslant \sum_{i=0}^{u} n_i \leqslant b(t) \leqslant K$, то вероятность того, что $\operatorname{rank} X_{\widetilde{\gamma}_0 \cup \sigma_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma_u(\widetilde{\gamma}_u)} = \sum_{i=0}^{u} \operatorname{rank} X_{\sigma_i(\widetilde{\gamma}_i)}$, не меньше $1 - \varepsilon(t) \sum_{i=1}^{u} \frac{n_i N}{K(N-n_i)}$, т. е.*

$$\mathbf{P}\left\{\operatorname{rank} X_{\widetilde{\gamma}_0 \cup \sigma_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma_u(\widetilde{\gamma}_u)} = \sum_{i=0}^{u} \operatorname{rank} X_{\sigma_i(\widetilde{\gamma}_i)}\right\} \geqslant 1 - \varepsilon(t) \sum_{i=1}^{u} \frac{n_i N}{K(N - n_i)}.$$

Доказательство. Докажем утверждение по индукции так же, как утверждение 14.

При $u = 1$ утверждение следует из леммы 2.

Пусть утверждение верно для всех значений, меньших u. Докажем, что оно верно для u. Оценим сверху вероятность события

$$\Gamma = \left\{\operatorname{rank} X_{\widetilde{\gamma}_0 \cup \sigma_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma_u(\widetilde{\gamma}_u)} \neq \sum_{i=0}^{u} \operatorname{rank} X_{\sigma_i(\widetilde{\gamma}_i)}\right\}.$$

Тогда из равенства

$$\mathbf{P}\left\{\operatorname{rank} X_{\widetilde{\gamma}_0 \cup \sigma_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma_u(\widetilde{\gamma}_u)} = \sum_{i=0}^{u} \operatorname{rank} X_{\sigma_i(\widetilde{\gamma}_i)}\right\} = 1 - \mathbf{P}\{\Gamma\}$$

получим оценку снизу для нужного нам события.

По утверждению 13 событие Γ возникает при реализации любого из двух событий

$$\Gamma_1 = \left\{ \operatorname{rank} X_{\widetilde{\gamma}_0 \cup \sigma_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma_{u-1}(\widetilde{\gamma}_{u-1})} \neq \sum_{i=0}^{u-1} \operatorname{rank} X_{\sigma_i(\widetilde{\gamma}_i)} \right\}$$

или

$$\Gamma_2 = \big\{ \operatorname{rank}\big(X_{\widetilde{\gamma}_0 \cup \sigma_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma_{u-1}(\widetilde{\gamma}_{u-1})} \| X_{\sigma_u(\widetilde{\gamma}_u)} \big) \neq \operatorname{rank} X_{\widetilde{\gamma}_0 \cup \sigma_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma_{u-1}(\widetilde{\gamma}_{u-1})} + \operatorname{rank} X_{\sigma_u(\widetilde{\gamma}_u)} \big\}.$$

Поэтому

$$\mathbf{P}\{\Gamma\} \leqslant \mathbf{P}\{\Gamma_1\} + \mathbf{P}\{\Gamma_2\}. \tag{22}$$

По предположению индукции

$$\mathbf{P}\{\Gamma_1\} \leqslant \varepsilon(t) \sum_{i=1}^{u-1} \frac{N n_i}{K(N-n_i)}. \tag{23}$$

Теперь, используя формулу полной вероятности, можно записать, что

$$\mathbf{P}\{\Gamma_2\} = \sum_{\sigma'_1 \in \mathcal{S}_N} \sum_{\sigma'_2 \in \mathcal{S}_N} \cdots \sum_{\sigma'_{u-1} \in \mathcal{S}_N} \mathbf{P}\{\Gamma'_2, \sigma_1 = \sigma'_1, \ldots, \sigma_{u-1} = \sigma'_{u-1}\}, \tag{24}$$

здесь

$$\Gamma'_2 = \big\{ \operatorname{rank}\big(X_{\widetilde{\gamma}_0 \cup \sigma'_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma'_{u-1}(\widetilde{\gamma}_{u-1})} \| X_{\sigma_u(\widetilde{\gamma}_u)} \big) \neq \operatorname{rank} X_{\widetilde{\gamma}_0 \cup \sigma'_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma'_{u-1}(\widetilde{\gamma}_{u-1})} + \operatorname{rank} X_{\sigma_u(\widetilde{\gamma}_u)} \big\}.$$

Если положить $\widetilde{\beta}_1 = \widetilde{\gamma}_0 \cup \sigma'_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma'_{u-1}(\widetilde{\gamma}_{u-1})$, $\widetilde{\beta}_0 = \widetilde{\gamma}_u$, то согласно утверждению 14

$$\mathbf{P}\{\Gamma'_2\} \leqslant \varepsilon(t) \cdot \frac{n_u N}{K(N-n_u)}.$$

С учетом этого неравенства, используя тот факт, что события $\Gamma'_2, \{\sigma_1 = \sigma'_1\}, \ldots, \{\sigma_{u-1} = \sigma'_{u-1}\}$ независимы в совокупности, из (24) получим

$$\mathbf{P}\{\Gamma_2\} \leqslant \varepsilon(t) \cdot \frac{n_u N}{K(N-n_u)} \sum_{\sigma'_1 \in \mathcal{S}_N} \cdots \sum_{\sigma'_{u-1} \in \mathcal{S}_N} \mathbf{P}\{\sigma_1 = \sigma'_1, \ldots, \sigma_{u-1} = \sigma'_{u-1}\}.$$

Поэтому

$$\mathbf{P}\{\Gamma_2\} \leqslant \varepsilon(t) \cdot \frac{n_u N}{K(N-n_u)}. \tag{25}$$

Теперь, объединяя неравенства (22), (23) и (25), окончательно получим

$$\mathbf{P}\{\Gamma\} \leqslant \varepsilon(t) \sum_{i=1}^{u-1} \frac{n_i N}{K(N-n_i)} + \varepsilon(t) \cdot \frac{n_u N}{K(N-n_u)} = \varepsilon(t) \sum_{i=1}^{u} \frac{n_i N}{K(N-n_i)}. \qquad \square$$

В качестве следствия из утверждения 15 несложно доказать следующее утверждение.

Утверждение 16. *Рассмотрим $(K \times N)$-матрицу $X \in \mathbf{P}_{\varepsilon,b}(t)$. Для $i = 0, 1, \ldots, u$ зафиксируем $\widetilde{\gamma}_i \in \widetilde{\mathbf{A}}_N^{n_i}$. Выберем независимо друг от друга $\sigma_1, \sigma_2, \ldots, \sigma_u \xleftarrow{\$} \mathcal{S}_N$. Пусть также σ_0 — тождественная подстановка. Тогда если $1 \leqslant \sum_{i=0}^{u} n_i \leqslant b(t) \leqslant K$, то вероятность того, что $\operatorname{rank} X_{\widetilde{\gamma}_0 \cup \sigma_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma_u(\widetilde{\gamma}_u)} = \sum_{i=0}^{u} \operatorname{rank} X_{\sigma_i(\widetilde{\gamma}_i)}$, не меньше $1 - \varepsilon(t)\frac{u \cdot n^\star N}{K(N-n^\star)}$, т. е.*

$$\mathbf{P}\left\{\operatorname{rank} X_{\widetilde{\gamma}_0 \cup \sigma_1(\widetilde{\gamma}_1) \cup \cdots \cup \sigma_u(\widetilde{\gamma}_u)} = \sum_{i=0}^{u} \operatorname{rank} X_{\sigma_i(\widetilde{\gamma}_i)}\right\} \geqslant 1 - \varepsilon(t)\frac{u \cdot n^\star N}{K(N-n^\star)},$$

здесь $n^\star = \max\{n_1, \ldots, n_u\}$.

5. Квадрат Адамара комбинированного кода с большой вероятностью равен декартову произведению квадратов Адамара

В [17] доказано следующее утверждение.

Утверждение 17. *Пусть R — порождающая $\left(\frac{k(k+1)}{2} \times q^k\right)$-матрица кода $\mathcal{HRM}_q(2,k)$. Тогда $R \in \mathbf{P}_{\varepsilon,b}([1,T])$ для $\varepsilon(t) = \frac{k(k+1)}{2q^t}$ и $b(t) = \frac{k(k+1)}{2} + \frac{t(t-\mu)}{2} - kt$. Здесь*

$$T = \begin{cases} k, & \text{если } q = 2, \\ k + 1 - \left\lceil \frac{1}{2}(\sqrt{8k+9} - 1) \right\rceil, & \text{если } q > 2, \end{cases} \qquad \mu = \begin{cases} 1, & \text{если } q = 2, \\ 3, & \text{если } q > 2. \end{cases}$$

Используя утверждение 17, установим вероятность с которой ранг матрицы, составленной из подматриц порождающей матрицы кода $\mathcal{HRM}_q(2,k)$, равен сумме рангов этих подматриц.

Утверждение 18. *Пусть R — порождающая матрица кода $\mathcal{HRM}_q(2,k)$. Зафиксируем некоторое $\widetilde{\gamma}_0 \in \widetilde{\mathbf{A}}_N^{n_0}$. Выберем последовательно $\widetilde{\gamma}_1 \xleftarrow{\$} \widetilde{\mathbf{A}}_N^{n_1}, \widetilde{\gamma}_2 \xleftarrow{\$} \widetilde{\mathbf{A}}_N^{n_2}, \ldots, \widetilde{\gamma}_u \xleftarrow{\$} \widetilde{\mathbf{A}}_N^{n_u}$. Обозначим $n = n_0 + n_1 + \cdots + n_u$. Тогда*

$$\mathbf{P}\left\{\operatorname{rank} R_{\widetilde{\gamma}_0 \cup \widetilde{\gamma}_1 \cup \cdots \cup \widetilde{\gamma}_u} = \sum_{i=0}^{u} \operatorname{rank} R_{\widetilde{\gamma}_i}\right\} \geqslant 1 - \frac{1}{q^{k - \log_q(n-n_0) - \delta_q(n,k)}},$$

где

$$\delta_q(n,k) = \begin{cases} \left\lceil \dfrac{\sqrt{8n+1}-1}{2} \right\rceil, & \text{если } q = 2, \\ \left\lceil \dfrac{\sqrt{8(n+k+1)+1}-1}{2} \right\rceil - 1, & \text{если } q > 2. \end{cases}$$

Доказательство. Из утверждения 17 следует, что $R \in \mathbf{P}_{\varepsilon,b}([1,T])$ для $\varepsilon(t) = \frac{k(k+1)}{2q^t}$ и $b(t) = \frac{k(k+1)}{2} + \frac{t(t-\mu)}{2} - kt$. Здесь

$$T = \begin{cases} k, & \text{если } q = 2, \\ k + 1 - \left\lceil \frac{1}{2}\left(\sqrt{8k+9} - 1\right) \right\rceil, & \text{если } q > 2, \end{cases} \qquad \mu = \begin{cases} 1, & \text{если } q = 2, \\ 3, & \text{если } q > 2. \end{cases}$$

Поэтому при $1 \leqslant n \leqslant b(t) = \frac{k(k+1)}{2} - kt + \frac{t(t-\mu)}{2}$ и $1 \leqslant t \leqslant T$, то из утверждения 14 следует, что

$$\mathbf{P}\left\{\operatorname{rank} R_{\widetilde{\gamma}_0 \cup \widetilde{\gamma}_1 \cup \ldots \cup \widetilde{\gamma}_u} = \sum_{i=0}^{u} \operatorname{rank} R_{\widetilde{\gamma}_i}\right\} \geqslant 1 - \frac{n-n_0}{q^t} = 1 - \frac{1}{q^{t-\log_q(n-n_0)}}. \tag{26}$$

Осталось выбрать t так чтобы эта вероятность была максимальной. Для этого нужно подобрать максимальное допустимое t.

Найдем сначала t, удовлетворяющие условию

$$n \leqslant \frac{k(k+1)}{2} - kt + \frac{t(t-\mu)}{2}. \tag{27}$$

Перепишем неравенство в виде

$$2n \leqslant k(k+1) - 2kt + t^2 - \mu t = t^2 - (2k+\mu)t + k(k+1).$$

Отсюда получаем неравенство

$$t^2 - (2k+\mu)t + k(k+1) - 2n \geqslant 0. \tag{28}$$

Далее,

$$t^2 - (2k+\mu)t + k(k+1) - 2n = \left(t - k - \frac{\mu}{2}\right)^2 + k(k+1) - 2n - \left(k + \frac{\mu}{2}\right)^2$$
$$= \left(t - k - \frac{\mu}{2}\right)^2 + k^2 + k - 2n - k^2 - \mu k - \frac{\mu^2}{4} = \left(t - k - \frac{\mu}{2}\right)^2 - \left(2n + (\mu-1)k + \frac{\mu^2}{4}\right).$$

Тогда из (28) следует неравенство

$$\left(t - k - \frac{\mu}{2}\right)^2 \geqslant 2n + (\mu-1)k + \frac{\mu^2}{4}. \tag{29}$$

Извлекая из левой и правой частей квадратный корень, получим систему неравенств

$$\begin{cases} t - k - \dfrac{\mu}{2} & \geqslant \sqrt{2n + (\mu-1)k + \dfrac{\mu^2}{4}}, \\ -\left(t - k - \dfrac{\mu}{2}\right) & \geqslant \sqrt{2n + (\mu-1)k + \dfrac{\mu^2}{4}}, \end{cases}$$

которая эквивалентна системе

$$\begin{cases} t & \geqslant k + \dfrac{\mu}{2} + \sqrt{2n + (\mu-1)k + \dfrac{\mu^2}{4}}, \\ t & \leqslant k + \dfrac{\mu}{2} - \sqrt{2n + (\mu-1)k + \dfrac{\mu^2}{4}}. \end{cases}$$

Так как $1 \leqslant t \leqslant T \leqslant k$, то допустимы только t, удовлетворяющие условию

$$1 \leqslant t \leqslant k + \frac{\mu}{2} - \sqrt{2n + (\mu-1)k + \frac{\mu^2}{4}}.$$

Заметим, что для всех $n, k \geqslant 0$ и $\mu \geqslant 1$ выполняется неравенство

$$k + \frac{\mu}{2} - \sqrt{2n + (\mu - 1)k + \frac{\mu^2}{4}} \leqslant k. \tag{30}$$

Действительно, так как для всех $n, k \geqslant 0$ и $\mu \geqslant 1$

$$2n + (\mu - 1)k \geqslant 0,$$

то

$$2n + (\mu - 1)k + \frac{\mu^2}{4} \geqslant \frac{\mu^2}{4}. \tag{31}$$

Извлекая из левой и правой частей неравенства (31) корень, получим

$$\sqrt{2n + (\mu - 1)k + \frac{\mu^2}{4}} \geqslant \frac{\mu}{2}.$$

Отсюда

$$-\sqrt{2n + (\mu - 1)k + \frac{\mu^2}{4}} \leqslant -\frac{\mu}{2}.$$

И, наконец, получим неравенство (30).

Из (30) следует, что допустимые t, удовлетворяющие неравенству (27), лежат на отрезке

$$1 \leqslant t \leqslant k + \frac{\mu}{2} - \sqrt{2n + (\mu - 1)k + \frac{\mu^2}{4}}.$$

Теперь рассмотрим возможные случаи.

Пусть $q = 2$. Тогда $1 \leqslant t \leqslant k$ и $\mu = 1$. Поэтому с учетом неравенства (30) максимально возможное допустимое t равно

$$t = k - \left\lceil \frac{\sqrt{8n + 1} - 1}{2} \right\rceil.$$

Пусть $q > 2$. Тогда $1 \leqslant t \leqslant k + 1 - \left\lceil \frac{1}{2}(\sqrt{8k + 9} - 1) \right\rceil$ и $\mu = 3$, поэтому

$$1 \leqslant t \leqslant \min\left\{ k + 1 - \left\lceil \frac{1}{2}\left(\sqrt{8k + 9} - 1\right) \right\rceil, k + 1 - \left\lceil \frac{1}{2}\left(\sqrt{8n + 8k + 9} - 1\right) \right\rceil \right\}.$$

Очевидно, что верно неравенство $(\sqrt{8k + 9} - 1)/2 < (\sqrt{8k + 9 + 8n} - 1)/2$, поэтому

$$1 \leqslant t \leqslant k + 1 - \left\lceil \frac{1}{2}\left(\sqrt{8n + 8k + 9} - 1\right) \right\rceil.$$

Значит, в этом случае максимально возможное допустимое t будет равно

$$t = k + 1 - \left\lceil \frac{\sqrt{8(n + k + 1) + 1} - 1}{2} \right\rceil.$$

Полагая

$$\delta_q(n, k) = \begin{cases} \left\lceil \dfrac{\sqrt{8n + 1} - 1}{2} \right\rceil, & \text{если } q = 2, \\ \left\lceil \dfrac{\sqrt{8(n + k + 1) + 1} - 1}{2} \right\rceil - 1, & \text{если } q > 2, \end{cases}$$

из (26) получаем нужное неравенство. □

Опишем вероятностную схему случайного выбора $(k \times n)$-матрицы. Будем случайно и равновероятно из множества столбцов $V_k^\top(q)$ выбирать векторы-столбцы $g_1, \dots, g_n$, используя выборку с возвращением. Сформируем матрицу

$$G = (g_1 \dots g_n).$$

Этот процесс будем кратко обозначать $G \xleftarrow{\$} V_{k\times n}(q)$.

Теорема 1. *Пусть $k, n_0, n_1, \dots, n_u$ — натуральные числа и $n = n_0 + n_1 + \dots + n_u$. Зафиксируем некоторую $(k \times n_0)$-матрицу G_0 над полем $\mathrm{GF}(q)$. Выберем последовательно $G_i \xleftarrow{\$} V_{k\times n_i}(q)$, $i = 1, 2, \dots, u$. Рассмотрим $(k \times n)$-матрицу*

$$G = (G_0 \| G_1 \| \dots \| G_u).$$

Матрица G охватывает некоторый $[n]_q$-код $\mathcal{C}$, который является последовательным соединением кодов $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_u$, где $\mathcal{C}_i$ — $[n_i]_q$-код, охватываемый матрицей G_i, $i = 0, 1, \dots, u$.

Тогда

$$\mathbf{P}\{\mathcal{C}^{\circ 2} = \mathcal{C}_0^{\circ 2} \times \mathcal{C}_1^{\circ 2} \times \dots \times \mathcal{C}_u^{\circ 2}\} \geqslant 1 - \frac{1}{q^{k - \log_q(n-n_0) - \delta_q(n,k)}},$$

где

$$\delta_q(n,k) = \begin{cases} \left\lceil \dfrac{\sqrt{8n+1}-1}{2} \right\rceil, & \text{если } q = 2, \\ \left\lceil \dfrac{\sqrt{8(n+k+1)+1}-1}{2} \right\rceil - 1, & \text{если } q > 2. \end{cases}$$

Доказательство. Пусть $\widetilde{\gamma}_i$ — множество, составленное из столбцов матрицы G_i, $i = 0, 1, \dots, u$. Напомним, что мы не делаем различий между векторами из $V_k^\top(q)$ и их представлениями в виде чисел от 0 до $N - 1 = q^k - 1$. Таким образом, можно считать, что $\widetilde{\gamma}_i \in \widetilde{\mathbf{A}}_N^k$, $i = 0, 1, \dots, u$.

Случайный выбор матриц $G_1, \dots, G_u$ эквивалентен случайному выбору номеров столбцов матрицы R, поэтому если $G_i \xleftarrow{\$} V_{k\times n_i}$, то фактически $\widetilde{\gamma}_i \xleftarrow{\$} \widetilde{\mathbf{A}}_N^{n_i}$, $i = 1, 2, \dots, u$.

Если заметить, что и матрице G_0 будет соответствовать некоторое $\widetilde{\gamma}_0 \in \widetilde{\mathbf{A}}_N^{n_0}$, то можно считать, что для каждого $i = 0, 1, \dots, u$ код $\mathcal{C}_i$ будет порождаться матрицей $R_{\widetilde{\gamma}_i}$, а код $\mathcal{C}$ — матрицей $(R_{\widetilde{\gamma}_0} \| R_{\widetilde{\gamma}_1} \| \dots \| R_{\widetilde{\gamma}_u}) = R_{\widetilde{\gamma}_0 \cup \widetilde{\gamma}_1 \cup \dots \cup \widetilde{\gamma}_u}$.

Согласно утверждению 8 равенство $\mathcal{C}^{\circ 2} = \mathcal{C}_0^{\circ 2} \times \mathcal{C}_1^{\circ 2} \times \dots \times \mathcal{C}_u^{\circ 2}$ эквивалентно равенству

$$\operatorname{rank} R_{\widetilde{\gamma}_0 \cup \widetilde{\gamma}_1 \cup \dots \cup \widetilde{\gamma}_u} = \operatorname{rank} R_{\widetilde{\gamma}_0} + \operatorname{rank} R_{\widetilde{\gamma}_1} + \dots + \operatorname{rank} R_{\widetilde{\gamma}_u}.$$

А значит, справедливость теоремы следует из утверждения 18. □

Утверждение 19. *Пусть R — порождающая матрица кода $\mathcal{HRM}_q(2,k)$. Выберем $u \in \mathbb{N}$. Для каждого $i = 1, 2, \dots, u$ зафиксируем некоторые $\widetilde{\gamma}_i \in \widetilde{\mathbf{A}}_{q^k}^{n_i}$. Выберем $\sigma_1, \sigma_2, \dots, \sigma_u \xleftarrow{\$} \mathcal{S}_{q^k}$. Пусть также σ_0 — тождественная подстановка, $n = n_0 + n_1 + \dots + n_u$ и $n^\star = \max(n_1, \dots, n_u)$. Тогда*

$$\mathbf{P}\left\{ \operatorname{rank} R_{\widetilde{\gamma}_0 \cup \sigma_1(\widetilde{\gamma}_1) \cup \dots \cup \sigma_u(\widetilde{\gamma}_u)} = \sum_{i=0}^{u} \operatorname{rank} R_{\sigma_i(\widetilde{\gamma}_i)} \right\} \geqslant 1 - \frac{1}{q^{\log_q(q^k - n^\star) - \delta_q(n,k) - \log_q(u \cdot n^\star)}},$$

где

$$\delta_q(n,k) = \begin{cases} \left\lceil \dfrac{\sqrt{8n+1}-1}{2} \right\rceil, & \text{если } q = 2, \\ \left\lceil \dfrac{\sqrt{8(n+k+1)+1}-1}{2} \right\rceil - 1, & \text{если } q > 2. \end{cases}$$

Доказательство. Доказывается с помощью утверждения 16 аналогично утверждению 18. □

Аналогично выводу теоремы 1 в качестве следствия из утверждения 18, из утверждения 19 получим следующую теорему.

Теорема 2. *Пусть u — натуральное число. Для каждого $i = 0, 1, \ldots, u$ зафиксируем некоторую $(k \times n_i)$-матрицу G_i над полем* $\mathrm{GF}(q)$. *Выберем последовательно $\sigma_i \xleftarrow{\$} \mathcal{S}_{q^k}$, $i = 1, 2, \ldots, u$. Пусть $n = \sum_{i=0}^{u} n_i$ и $n^\star = \max(n_1, \ldots, n_u)$. Рассмотрим $(k \times n)$-матрицу*

$$G = (G_0 \| \sigma_1(G_1) \| \ldots \| \sigma_u(G_u)).$$

Матрица G охватывает некоторый $[n]_q$-код $\mathcal{C}$, который является последовательным соединением кодов $\mathcal{C}_i$, $i = 0, \ldots, u$, охватываемых матрицами $\sigma_i(G_i)$, здесь σ_0 — тождественная подстановка.

Тогда

$$\mathbf{P}\{\mathcal{C}^{\circ 2} = \mathcal{C}_0^{\circ 2} \times \mathcal{C}_1^{\circ 2} \times \cdots \times \mathcal{C}_u^{\circ 2}\} \geqslant 1 - \frac{1}{q^{\log_q(q^k - n^\star) - \delta_q(n,k) - \log_q(u \cdot n^\star)}},$$

где

$$\delta_q(n,k) = \begin{cases} \left\lceil \dfrac{\sqrt{8n+1}-1}{2} \right\rceil, & q = 2, \\ \left\lceil \dfrac{\sqrt{8(n+k+1)+1}-1}{2} \right\rceil - 1, & q > 2. \end{cases}$$

6. Некоторые приложения

Коды, которые получаются последовательным соединением других кодов, иногда используются для построения постквантовых криптографических механизмов, основанных на кодах, исправляющих ошибки.

Однако благодаря теоремам 1 и 2 криптографический анализ подобных конструкций может быть во многих случаях сведен к криптоанализу механизмов, построенных на отдельных кодах, участвующих в соединении. Поэтому подобные модификации кодовых криптосистем, вообще говоря, не увеличивают надежность криптомеханизма. Рассмотрим несколько примеров.

6.1. Криптосистема Мак-Элиса на основе соединения кодов Рида–Маллера. В [18] предлагается для построения криптосистемы Мак-Элиса использовать коды, которые порождаются матрицей вида

$$G = (R \| A_1 R \| \ldots \| A_u R),$$

здесь R — порождающая матрица двоичного $[n,k]$-кода Рида–Маллера $\mathcal{RM}(r,m)$, а $A_i \in \mathrm{GL}_k(2)$, $i = 1,\ldots,u$. При этом в процессе создания ключей матрицы $A_1, A_2, \ldots, A_u$ выбираются случайно и равновероятно из множества всех двоичных $(k \times k)$-матриц.

В [13] предлагается эффективная структурная атака на такую криптосистему Мак-Элиса. При этом для успеха атаки необходимо, чтобы для кода $\mathcal{C}$ с порождающей матрицей G выполнялось условие

$$\mathcal{C}^{\circ 2} = \underbrace{\mathcal{RM}^{\circ 2}(r,m) \times \cdots \times \mathcal{RM}^{\circ 2}(r,m)}_{u+1}. \tag{32}$$

Авторы атаки смогли только экспериментально проверить, что равенство (32) выполняется почти всегда. Теорема 2 косвенно подтверждает, что например, для оригинальных параметров $r = 3, m = 10, u = 3$, предложенных в [18], равенство (32), скорее всего, выполняется с большой вероятностью.

Впрямую теорема 2 не применима к рассматриваемой конструкции. Однако если заменить матрицы $A_1,\ldots,A_u$ некоторыми случайными подстановками $\sigma_1,\ldots,\sigma_u$, которые действуют на двоичных векторах длины k, то вероятность выполнения равенства

$$\mathcal{C}^{\circ 2} = \mathcal{RM}^{\circ 2}(3,10) \times \sigma_1(\mathcal{RM}(3,10))^{\circ 2} \times \sigma_2(\mathcal{RM}(3,10))^{\circ 2} \times \sigma_3(\mathcal{RM}(3,10))^{\circ 2}$$

можно оценить следующим образом. Так как в данном случае $n^\star = 1024$, $k = 176$ и $u = 3$, то она не меньше

$$1 - 2^{-(\log_2(2^{176}-1024)-\delta_2(1024,176)-\log_2(3\cdot 1024))}.$$

При этом $\delta_2(1024,176,3) = \left\lceil \frac{\sqrt{32\cdot 1024+1}-1}{2} \right\rceil = 91$ и $\log_2(3\cdot 1024) \leqslant 11.6$ Значит, вероятность не меньше

$$1 - 2^{-(\log_2(2^{176}-1024)-102.6)} > 1 - 2^{102.6-175} = 1 - 2^{-72.4}.$$

Та же самая вероятность для кода $\mathcal{RM}(4,10)$ уже будет не меньше $1 - 2^{-273.4}$.

6.2. Криптосистема Мак-Элиса на основе соединения кодов Рида–Маллера и случайных кодов. В [19] авторы предлагают строить криптосистему на основе кода $\mathcal{C}$ из семейства $\mathcal{RM}(r,m)\|\Gamma$, где Γ — двоичный код Гоппы. В процессе генерации ключей для построения двоичной порождающей матрицы случайного кода Гоппы выбираются случайный многочлен $g(z)$ над конечным полем $\mathrm{GF}(2^m)$ и случайное подмножество $L \subseteq \mathrm{GF}(2^m)$. По $g(z)$ и L строится порождающая матрица $G(g(z),L)$ кода Гоппы. Обозначим множество всех таких матриц $G(g(z),L)$ через M. Также через $M_{k,n}$ обозначим множество матриц из M размера $(k \times n)$.

В [14] и [15] построена атака на эту криптосистему в некоторых моделях противника. Помимо прочего в атаках используется факт выполнения равенства $\mathcal{C}^{\circ 2} = \mathcal{RM}^{\circ 2}(r,m) \times \Gamma^{\circ 2}$. Если считать, что при случайном выборе G из множества $V_{k\times n}$ выполняется условие $\mathbf{P}\{G \in M_{k,n}\} \approx 1$, то для конкретных параметров кодов можно установить, что это равенство выполняется почти всегда.

Так, например, рассматривая $r = 3$ и $m = 10$, и ограничив длину кода Γ числом $2^{10} = 1024$, получим, что $\mathcal{C}^{\circ 2} = \mathcal{RM}^{\circ 2}(3, 10) \times \Gamma^{\circ 2}$ с вероятностью не меньше

$$1-2^{-\left(176-\log_2 1024-\left\lceil \frac{\sqrt{8\cdot 2048+1}-1}{2}\right\rceil\right)}=1-2^{-\left(166-\left\lceil \frac{\sqrt{8\cdot 2048+1}-1}{2}\right\rceil\right)} = 1-2^{-(166-64)} = 1-2^{-102}.$$

В завершение рассмотрим атаку из [9]. В ней рассматривается криптосистема Мак-Элиса, построенная на коде Рида – Маллера $\mathcal{RM}(r, m)$, у которого к каждому кодовому слову добавлены случайные координаты так, чтобы сохранилось свойство линейности кода. В п. 5.2 в замечании 1 авторы отмечают, что они экспериментально установили следующий факт. Если к коду $\mathcal{RM}(r, m)$ добавить t случайных координат, то квадрат Адамара нового кода $\mathcal{B}$ будет иметь размерность

$$\dim \mathcal{B}^{\circ 2} = \dim \mathcal{RM}(2r, m) + t. \tag{33}$$

Фактически код $\mathcal{B}$ порождается матрицей $(R(r, m)\|G(t))$, где $R(r, m)$ — порождающая матрица $[n, k]$-кода $\mathcal{RM}(r, m)$, а $G(t)$ — $(k \times t)$-матрица, которая выбирается случайно и равновероятно из множества $V_{k\times t}$. С учетом того, что квадрат Адамара кода $\mathcal{RM}(r, m)$ равен коду $\mathcal{RM}(2r, m)$ (мы считаем, что $2r < m$), то в силу включения (1) выполняется неравенство $\dim \mathcal{B}^{\circ 2} \leqslant \dim \mathcal{RM}(2r, m) + \dim \mathcal{C}^{\circ 2}(t)$, здесь $\mathcal{C}^{\circ 2}(t)$ — код, охватываемый матрицей $G(t)$. Тогда если выполнено равенство (33), то из него следует, что $\dim \mathcal{RM}(2r, m) + t \leqslant \dim \mathcal{RM}(2r, m) + \dim \mathcal{C}^{\circ 2}(t)$, т. е. $t \leqslant \dim \mathcal{C}^{\circ 2}(t)$. Но длина кода $\mathcal{C}^{\circ 2}(t)$ равна t, поэтому $\dim \mathcal{C}^{\circ 2}(t) \leqslant t$ и из (33) следует равенство $\dim \mathcal{C}^{\circ 2}(t) = t$, которое эквивалентно равенству $\mathcal{C}^{\circ 2}(t) = V_t$. Далее, так как $t = \dim \mathcal{C}^{\circ 2}(t)$, то из равенства (33) также следует равенство

$$\dim \mathcal{B}^{\circ 2} = \dim \mathcal{RM}^{\circ 2}(r, m) + \dim \mathcal{C}^{\circ 2}(t).$$

С помощью утверждения 8 было доказано, что равенство (33) выполняется, если и только если

$$\mathcal{B}^{\circ 2} = \mathcal{RM}^{\circ 2}(r, m) \times \mathcal{C}^{\circ 2} \tag{34}$$

и $\mathcal{C}^{\circ 2} = V_t$.

Таким образом, вероятность того, что условие (33) не выполняется, не больше суммы вероятностей

$$\mathbf{P}\{\mathcal{B}^{\circ 2} \neq \mathcal{RM}^{\circ 2}(r, m) \times \mathcal{C}^{\circ 2}\} + \mathbf{P}\{\mathcal{C}^{\circ 2} \neq V_t\}.$$

Из теоремы 1 следует, что

$$\mathbf{P}\{\mathcal{B}^{\circ 2} \neq \mathcal{RM}^{\circ 2}(r, m) \times \mathcal{C}^{\circ 2}\} \leqslant 2^{-(k-\log_2(t)-\delta_2(n,k))}.$$

Осталось оценить вероятность второго события. Из теоремы 2 работы [17] следует, что

$$\mathbf{P}\{\mathcal{C}^{\circ 2} \neq V_t\} \leqslant 2^{-(k-\log_2(t)-\delta_2(t,k))}.$$

Поэтому вероятность выполнения условия (33) не меньше

$$1 - 2^{-(k-\log_2(t)-\delta_2(n,k))} - 2^{-(k-\log_2(t)-\delta_2(t,k))} \geqslant 1 - 2^{-(k-\log_2(t)-\delta_2(n,k)-1)}.$$

Рассмотрим для примера код Рида – Маллера $\mathcal{RM}(3, 10)$. Для него $k = 176$. Выберем $t = 2k = 352$. Так как длина кода $\mathcal{RM}(3, 10)$ равна 1024, то в этом случае $n = 1024 + t = 1024 + 352 = 1376$. Тогда несложно вычислить, что вероятность выполнения условия (33) будет не меньше $1 - 2^{-114}$. Кроме того, если ограничить t величиной n, то в этом случае для всех таких t вероятность выполнения условия (33) будет не меньше $1 - 2^{-101}$.

Таким образом, экспериментально установленный для конкретных параметров факт можно строго доказать, используя основной результат статьи.

7. Благодарности

Автор выражает глубокую признательность Григорию Анатольевичу Карпунину за ценные замечания, которые помогли сделать текст работы намного лучше, за интерес к статье, за полезное обсуждение полученных результатов и за титанический труд по поиску опечаток, ошибок и неточностей в доказательствах.

Список литературы

1. Pellikaan R., “On decoding by error location and dependent sets of error positions”, *Discrete Math.*, **106–107** (1992), 369–381.
2. Chen H., Cramer R., “Algebraic geometric secret sharing schemes and secure multi-party computations over small fields”, CRYPTO 2006, Lect. Notes Comput. Sci., **4117**, 2006, 521–536.
3. Бородин М. А., Чижов И. В., “Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера”, *Дискретная математика*, **26**:1 (2014), 10–20.
4. Wieschebrink C., “Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes”, PQCrypto 2010, Lect. Notes Comput. Sci., **6061**, 2010, 61–72.
5. Couvreur C., Gaborit P., Gauthier-Umaña V., Otmani A., Tillich J.-P., “Distinguisher-based attacks on public-key cryptosystems using Reed – Solomon codes”, *Des., Codes Cryptogr.*, **73**:2 (2014), 641–666.
6. Couvreur A., Márquez-Corbella I., Pellikaan R., “Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes”, Coding Theory and Applications, CIM Ser. Math. Sci., **3**, 2015, 133–140.
7. Couvreur A., Otmani A., Tillich J.-P., “Polynomial time attack on wild McEliece over quadratic extensions”, *IEEE Trans. Inf. Theory*, **63**:1 (2017), 404–427.
8. Couvreur A., Otmani A., Tillich J.-P., Gauthier-Umaña V., “A polynomial-time attack on the BBCRS scheme”, PKC 2015, Lect. Notes Comput. Sci., **9020**, 2015, 175–193.
9. Otmani A., Kalachi H. T., “Square code attack on a modified Sidelnikov cryptosystem”, C2SI 2015, Lect. Notes Comput. Sci., **9084**, 2015, 173–183.
10. Faugére J.-C., Gauthier-Umaña V., Otmani A., Perret L., Tillich J.-P., “A distinguisher for high-rate McEliece cryptosystems”, *IEEE Trans. Inf. Theory*, **59**:10 (2013), 6830–6844.
11. Cascudo I., Cramer R., Mirandola D., Zémor G., “Squares of random linear codes”, *IEEE Trans. Inf. Theory*, **61**:3 (2015), 1159–1173.
12. Bardet M., Bertin M., Couvreur A., Otmani A., “Practical algebraic attack on DAGS”, CBC 2019, Lect. Notes Comput. Sci., **11666**, 2019, 86–101.
13. Чижов И. В., Конюхов С. А., Давлетшина А. М., “Эффективная структурная атака на криптосистему Мак-Элиса – Сидельникова”, *Int. J. Open Inf. Technol.*, **8**:7 (2020), 1–10.

14. Чижов И. В., Попова Е. А., “Структурная атака на криптосистемы типа Мак-Элиса – Сидельникова, построенная на основе комбинирования случайных кодов с кодами Рида – Маллера”, *Int. J. Open Inf. Technol.*, **8**:6 (2020), 24–33.
15. Deundyak V. M., Kosolapov Y. V., “On the strength of asymmetric code cryptosystems based on the merging of generating matrices of linear codes”, XVI Int. Symp. “Problems of Redundancy in Information and Control Systems” (REDUNDANCY), 2019, 143–148.
16. Hall J. I., *Notes on Coding Theory. Chapter* 3: *Linear Codes*, Dept. Mathematics, Michigan State Univ., 2015, `users.math.msu.edu/users/halljo/classes/CODENOTES/Linear.pdf`.
17. Чижов И. В., “Квадрат Адамара и обобщенное минимальное расстояние кода Рида – Маллера порядка 2”, *Дискретная математика*, **35**:1 (2023), 128–152.
18. Сидельников В. М., “Открытое шифрование на основе двоичных кодов Рида – Маллера”, *Дискретная математика*, **6**:2, 3–20.
19. Egorova E., Kabatiansky G., Krouk E., Tavernier C., “A new code-based public-key cryptosystem resistant to quantum computer attacks”, *J. Phys. Conf. Ser.*, **1163**:012061 (2019).

Статья поступила 23.01.2023.