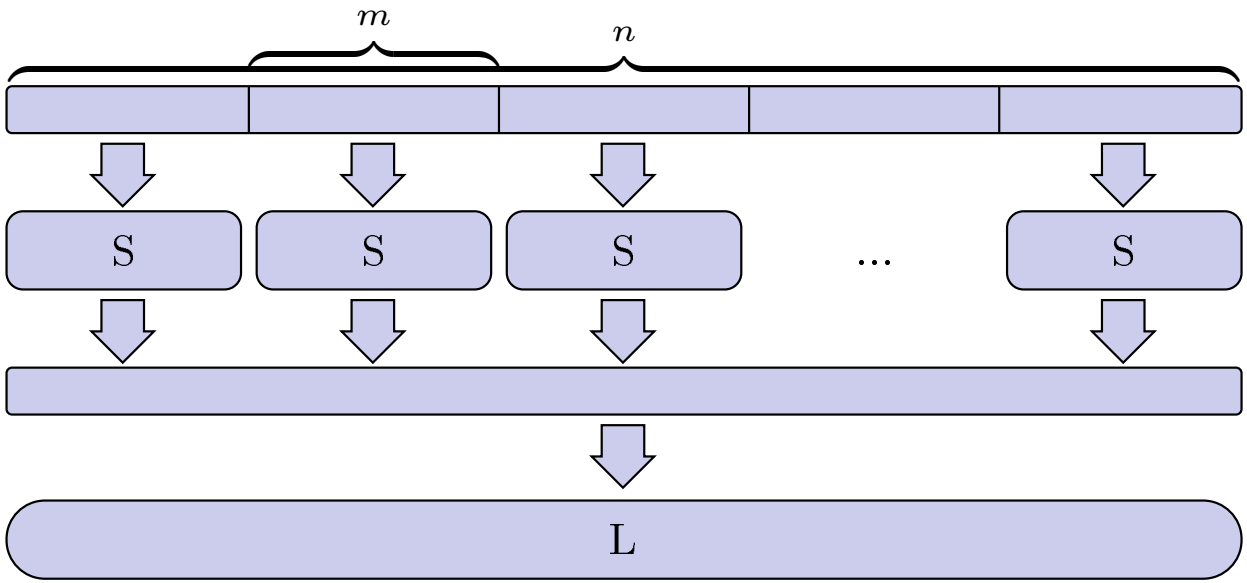
АДАПТИРОВАННЫЙ СПЕКТРАЛЬНО-РАССЕИВАЮЩИЙ МЕТОД ПОСТРОЕНИЯ МАТРИЦ СПЕЦИАЛЬНОГО ВИДА С ВЫСОКИМИ ЗНАЧЕНИЯМИ КОЭФФИЦИЕНТОВ РАССЕИВАНИЯ

Менячихин Андрей

Принципы Шеннона[1]

1. наложение ключа,
2. нелинейное перемешивающее отображение,
3. рассеивающее преобразование.



Замечание

Рассеивающее преобразование в современных блочных шифрсистемах чаще всего может быть представлено в виде некторой матрицы, преобразующей двоичные векторы достаточно большой размерности n (как правило, $n = 32, 64, 128, ...$).

Рассеивающие свойства такой матрицы принято оценивать с помощью коэффициентов рассеивания ρ и ρ'.

[1] Шеннон К. Работы по теории информации и кибернетике.— М.:ИЛ, 1963.— 829с.

Пусть $(e_0, e_1, ..., e_{n-1})$ – стандартный базис векторного пространства V_n. Обозначим через $H_{(s)}$ подпространство векторного пространства V_n, порожденное векторами $e_0, ..., e_{s-1}$:

$$H_{(s)} = \langle e_0, ..., e_{s-1} \rangle < V_n, \dim H_{(s)} = s.$$

Через $L_{H_{(s)}} : H_{(s)} \to V_n$ обозначим *ограничение* преобразования $L \in GL(n, 2)$ на множество $H_{(s)} \subseteq V_n$.

Символом «$*$» обозначим произвольный (не определенный) элемент поля $\mathbb{F}_2$. С учетом естественного равенства $0 \cdot * = 0$ в поле $\mathbb{F}_2$, введем следующее определение.

Определение 1

Матрицей линейного отображения $L_{H_{(s)}}$ будем называть $n \times n$-матрицу, первые s строк которой заданы элементами $\mathbb{F}_2$, остальные строки не определены.

Пример

Ниже приведен пример 4×4-матрицы некоторого линейного преобразования $L_{H_{(2)}} : H_{(2)} \to V_4$:

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ * & * & * & * \\ * & * & * & * \end{pmatrix}.$$

Ввиду взаимно однозначного соответствия между множеством $s \times n$-матриц над $\mathbb{F}_2$ и множеством линейных отображений $L_{H_{(s)}} : H_{(s)} \to V_n$ (при фиксированном базисе), будем через $L_{H_{(s)}}$ обозначать как матрицу, так и соответствующее ей отображение.

Для вектора $v = (v_0, ..., v_{n-1}) \in V_n$, преобразуемого матрицей $L \in GL(n, 2)$ по правилу $v \to vL$, определим разбиение на подвекторы $v = \left(v_{(0)}, ..., v_{(d-1)}\right)$, $v_{(i)} \in V_m$, $i = \overline{0, d-1}$, $n = m \cdot d$.

Определение 2

Коэффициентами рассеивания $\rho_m\left(L_{H_{(s)}}\right)$ и $\rho'_m\left(L_{H_{(s)}}\right)$ отображения $L_{H_{(s)}}$ относительно разностного и линейного методов криптографического анализа соответственно называются числа

$$\rho_m\left(L_{H_{(s)}}\right) = \min_{v \in H^{\times}_{(s)}} \left([v] + \left[vL_{H_{(s)}}\right]\right) \text{ и}$$

$$\rho'_m\left(L_{H_{(s)}}\right) = \rho_m\left(\left(L^T\right)_{H_{(s)}}\right) = \min_{v \in H^{\times}_{(s)}} \left([v] + \left[v\left(L^T\right)_{H_{(s)}}\right]\right),$$

где через $[v]$ обозначен обобщенный вес вектора $v \in V_n$,

$$[v] = \left|\left\{i \in \overline{0, d-1} \,\middle|\, v_{(i)} \neq 0\right\}\right|.$$

В случае, когда $s < n$ (то есть в случае, когда $H_{(s)}$ собственное подмножество множества V_n), величины $\rho_m\left(L_{H_{(s)}}\right)$ и $\rho'_m\left(L_{H_{(s)}}\right)$ будем также называть *частичными коэффициентами рассеивания* преобразования L на множестве $H_{(s)}$.

Замечание

Для цепочки подмножеств $H_{(1)} \subset ... \subset H_{(s)} \subset ... \subset H_{(n)} = V_n$ справедлива цепочка неравенств

$$d+1 \geq \rho_m\left(L_{H_{(1)}}\right) \geq ... \geq \rho_m\left(L_{H_{(s)}}\right) \geq ... \geq \rho_m\left(L_{H_{(n)}}\right) \geq 2.$$

Определение 3

Преобразование $L \in GL(n,2)$ называется *максимально рассеивающим*, если

$$\rho_m(L) = \rho'_m(L) = d+1.$$

Для отображения $L_{H_{(s)}} : H_{(s)} \to V_n$ и числа $\rho \in \{2, ..., d+1\}$ определим множества

$$P\left(L_{H_{(s)}}, \rho\right) = \left\{ v \in H_{(s)} \,\middle|\, [v] + \left[vL_{H_{(s)}}\right] = \rho \right\} \text{ и}$$

$$P'\left(L_{H_{(s)}}, \rho\right) = \left\{ v \in H_{(s)} \,\middle|\, [v] + \left[v\left(L^T\right)_{H_{(s)}}\right] = \rho \right\}.$$

Определение 4

$\rho_m\left(L_{H_{(s)}}\right)$ и $\rho'_m\left(L_{H_{(s)}}\right)$ - *спектрами рассеивания* отображения $L_{H_{(s)}} : H_{(s)} \to V_n$ называются соответственно упорядоченные множества

$$P\left(L_{H_{(s)}}\right) = \left\{ \left(\rho, \left|P\left(L_{H_{(s)}}, \rho\right)\right| \,|\rho \in \{2,3,...,d+1\}\right) \right\} \text{ и}$$

$$P'\left(L_{H_{(s)}}\right) = \left\{ \left(\rho, \left|P'\left(L_{H_{(s)}}, \rho\right)\right| \,|\rho \in \{2,3,...,d+1\}\right) \right\}.$$

Паре отображений $L_{H_{(s)}}$ и $\left(L^T\right)_{H_{(s)}}$ поставим во взаимно однозначное соответствие *частично заданную* $n \times n$*-матрицу* $\overline{L}_{H_{(s)}}$, первые s строк которой совпадают с первыми s строками матрицы линейного отображения $L_{H_{(s)}}$, первые s столбцов которой совпадают с первыми s столбцами транспонированной матрицы линейного преобразования $\left(L^T\right)_{H_{(s)}}$, а оставшиеся $(n-s)^2$ элементов матрицы $\overline{L}_{H_{(s)}}$ не определены.

Пример

Ниже приведена частично заданная 4×4-матрица $\overline{L}_{H_{(2)}}$, составленная из 2 первых строк матрицы линейного преобразования $L_{H_{(2)}}$, $L_{H_{(2)}} \begin{pmatrix} 0, & 1 \\ 0, & 1, \quad 2, \quad 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$, и 2 первых столбцов транспонированной матрицы линейного преобразования $\left(L^T\right)_{H_{(2)}}$, $\left(\left(L^T\right)_{H_{(2)}} \begin{pmatrix} 0, & 1 \\ 0, & 1, \quad 2, \quad 3 \end{pmatrix}\right)^T = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$:

$$\overline{L}_{H_{(2)}} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & * & * \\ 0 & 1 & * & * \end{pmatrix},$$

где символом «$*$» обозначены не определенные элементы матрицы $\overline{L}_{H_{(2)}}$.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

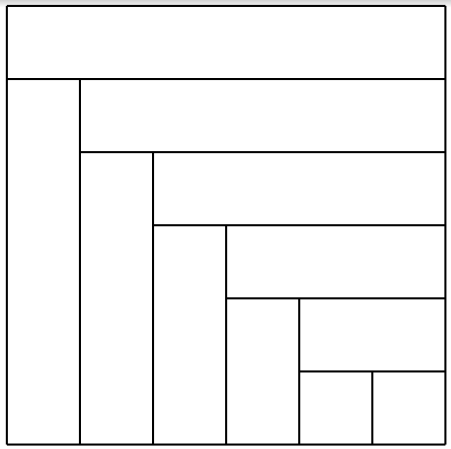


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

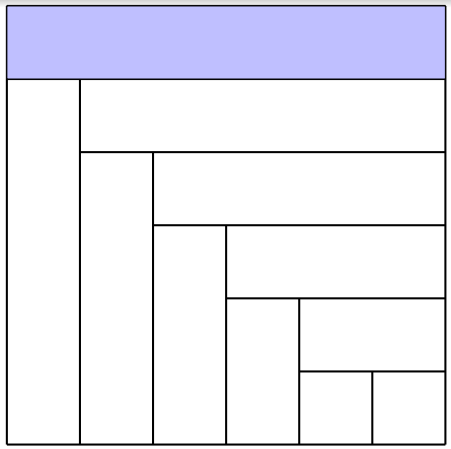


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

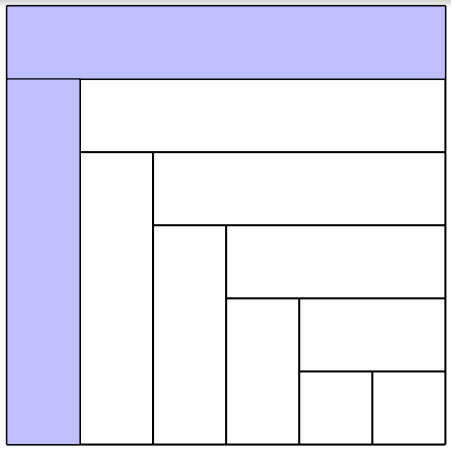


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

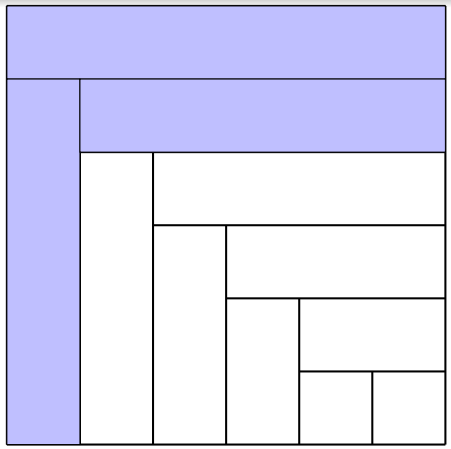


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

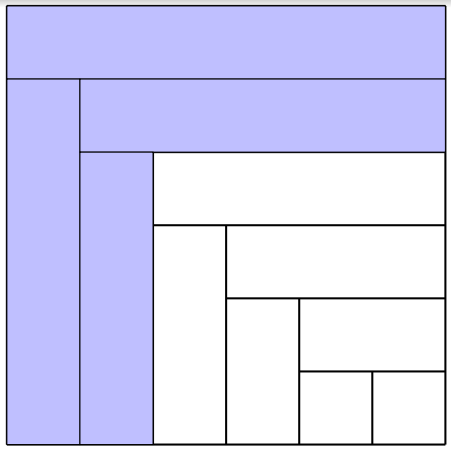


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

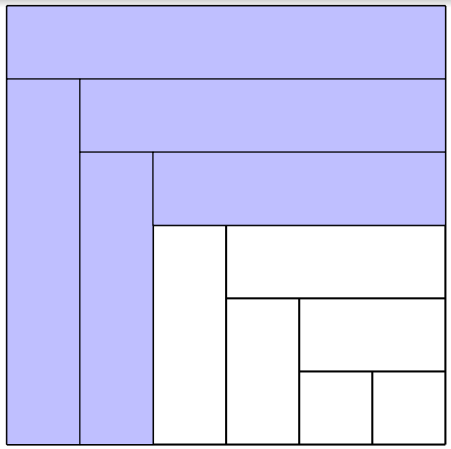


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

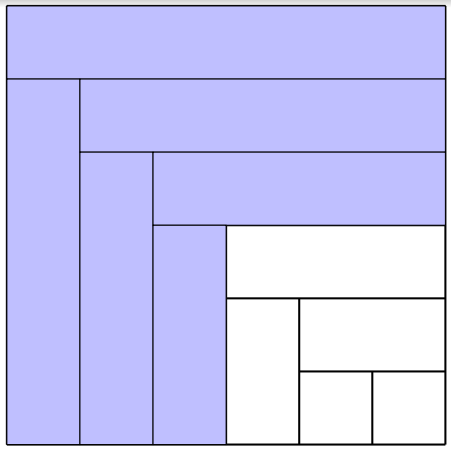


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

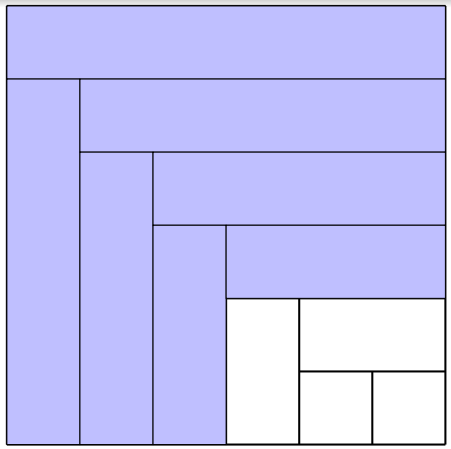


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

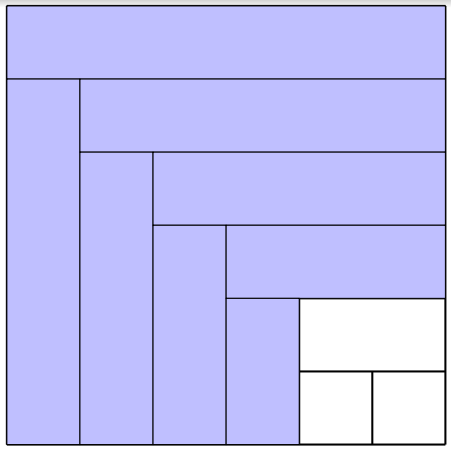


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

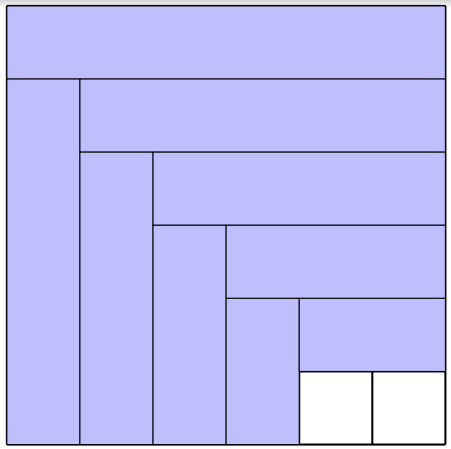


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

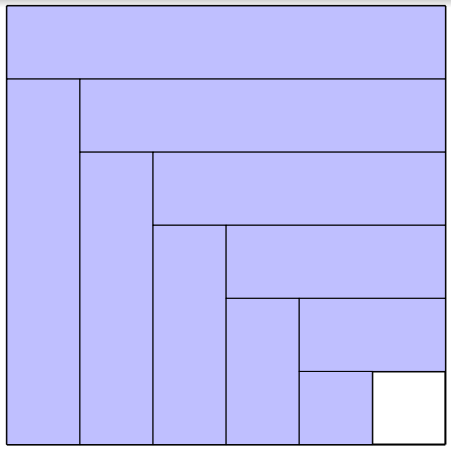


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Основная идея адаптированного спектрально-рассеивающего метода

Идея построения матрицы $L \in GL(n,2)$ состоит в последовательном определении действия преобразований L и L^T на элементах каждого из множеств $H_{(s)}$, $s = 1, ..., n$, путем фиксации строк матриц L и L^T (строк и столбцов матрицы L) с помощью специальным образом выбираемых векторов $v \in V_{n-s+1}$ и $v' \in V_{n-s}$ (см. Рис. 1). В конечном счете, как правило, это приводит к матрицам с требуемыми значениями коэффициентов рассеивания.

Замечания

1. Предлагаемый в настоящей работе подход наследует идею предложенную в работе[1].
2. Проблема дополнения частично заданной матрицы является одной из классических проблем линейной алгебры[2].

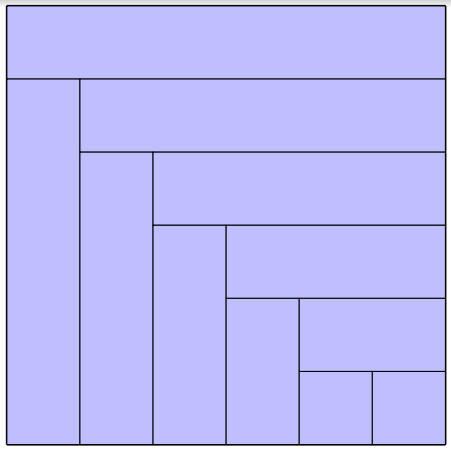


Рис. 1.

[1] Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$, Дискретная математика, 35:2(2023), С. 42-77.

[2] Paulsen V.I., Power S. and Smith R.R. Schur products and matrix completions, J. Funct. Anal., 85(1989), P. 151-178.

Классические подходы к вычислению частичных коэффициентов рассеивания $\rho_m\left(L_{H_{(s)}}\right)$ и $\rho'_m\left(L_{H_{(s)}}\right)$

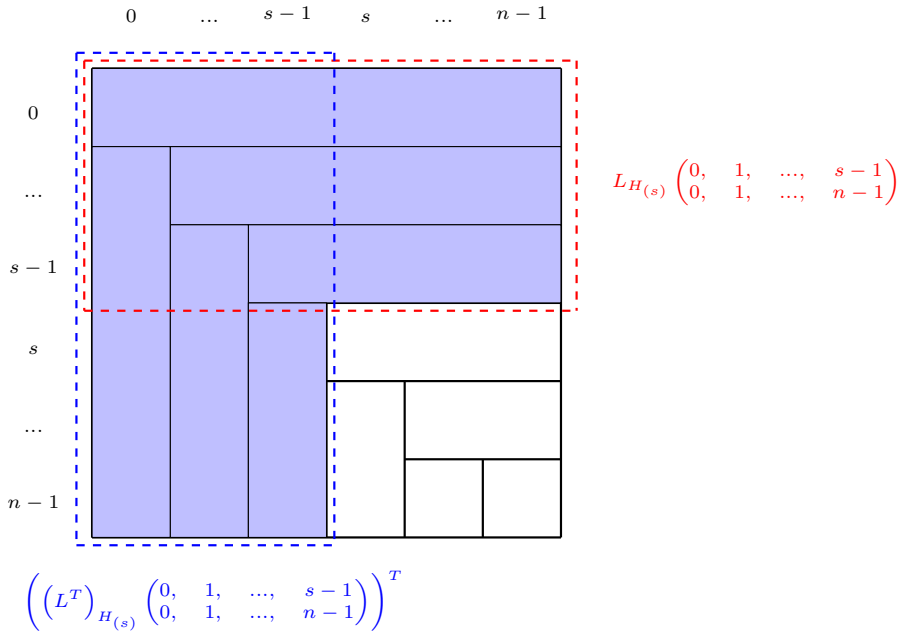


Рис. 2.

Обозначим через t_1 трудоемкость вычисления элементов $\rho_m\left(L_{H_{(s)}}\right)$ и $\left|P\left(L_{H_{(s)}}, \rho_m\left(L_{H_{(s)}}\right)\right)\right|$ линейного отображения $L_{H_{(s)}}: H_{(s)} \to V_n$, $s, n \in \mathbb{N}$, $s < n$, по определению 2.

Утверждение 1

Пусть $L_{H_{(s)}}$ – матрица линейного отображения $L_{H_{(s)}}: H_{(s)} \to V_n$, $s, n \in \mathbb{N}$, $1 \le s \le n$, тогда

$$t_1 \le c_1 2^s sn, \text{ где } c_1 = const. \quad (1)$$

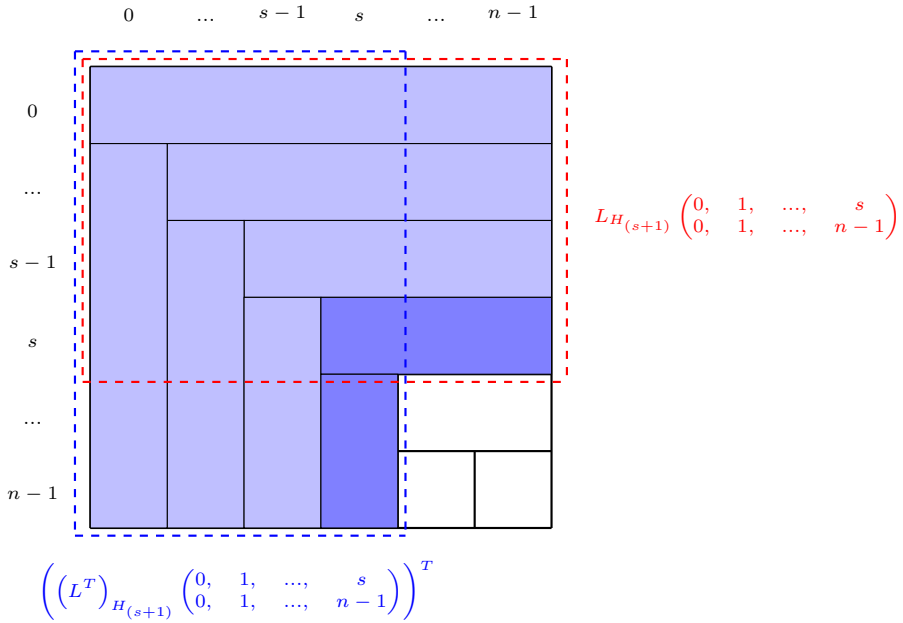


Рис. 3.

Если по известным значениям $\rho_m\left(L_{H_{(s)}}\right)$ и $\left|P\left(L_{H_{(s)}}, \rho_m\left(L_{H_{(s)}}\right)\right)\right|$ требуется вычислить элементы $\rho_m\left(L_{H_{(s+1)}}\right)$ и $\left|P\left(L_{H_{(s+1)}}, \rho_m\left(L_{H_{(s+1)}}\right)\right)\right|$ линейного отображения $L_{H_{(s+1)}}: H_{(s+1)} \to V_n, s, n \in \mathbb{N}$, $s \leq n-1$, то сделать это можно с некоторой трудоемкостью t_2.

Утверждение 2

Пусть $L_{H_{(s+1)}}$ – матрица линейного отображения $L_{H_{(s+1)}}: H_{(s+1)} \to V_n$, $s, n \in \mathbb{N}$, $1 \leq s \leq n-1$, тогда

$$t_2 \leq c_2 2^s (s+1) n, \text{ где } c_2 = const. \quad (2)$$

Алгоритм, реализующий адаптированный спектрально-рассеивающий метод

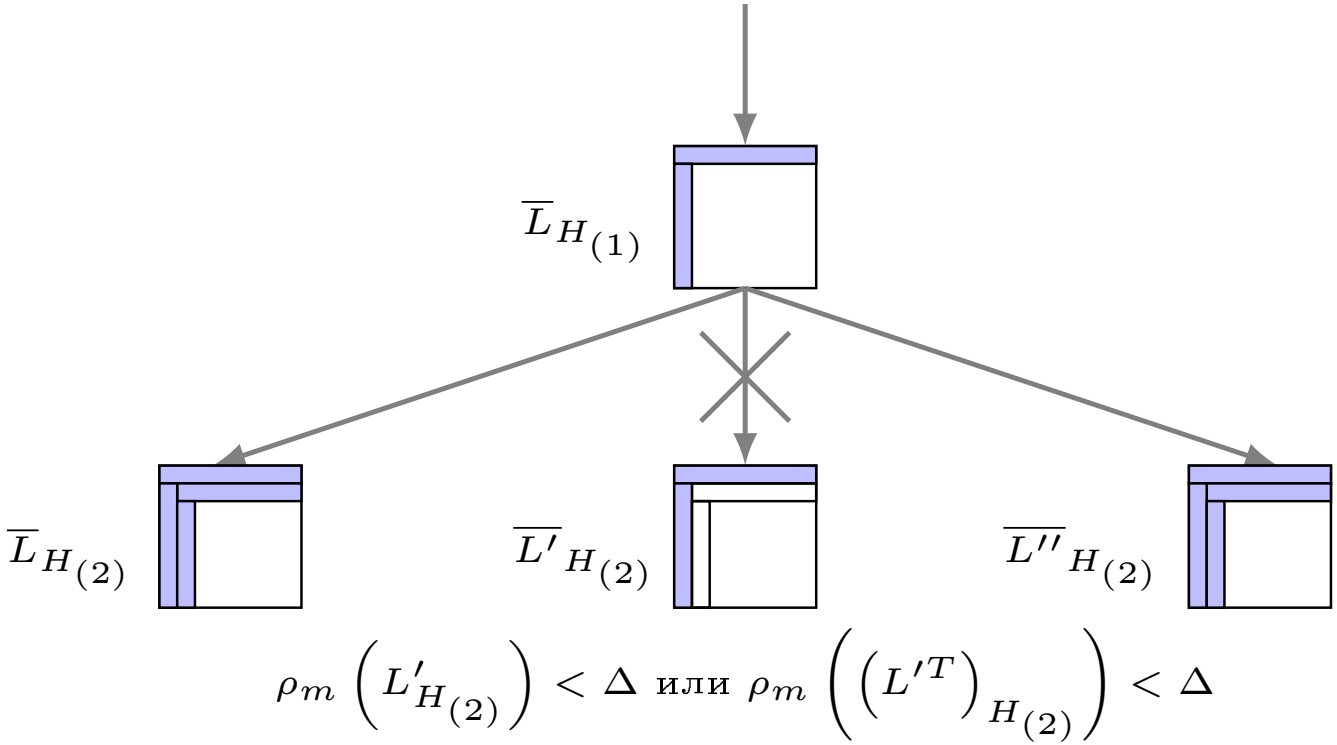


Рис. 4

Трудоемкость t построения матриц $L \in GL(n,2)$ с помощью алгоритма, реализующего адаптированный спектрально-рассеивающий метод характеризует следующее утверждение.

Утверждение 3

Если $L \in GL(n,2)$, $n, w \in \mathbb{N}$, $n \geq 2$, то для величины t справедлива оценка

$$t \leq cwn2^{2n}\left(\log w + 2n + 5\right), \text{ где } c = const. \quad (3)$$

Определение 5

Матрица $L \in GL(\nu, 2)$, каждая строка и каждый столбец которой содержат ровно k единиц, называется *k-регулярной*.

Замечание

Целесообразность использования k - регулярных матриц L в сетях Фейстеля обусловлена тем, что матрица L^{-1}, обратная к L, может никак не использоваться в процессах зашифрования и расшифрования. В таком случае, не нужно обеспечивать эффективную реализацию матрицы L^{-1}.

Определение 6

Если $L \in GL(\nu, 2)$, и каждая строка и каждый столбец матриц L и L^{-1} содержат ровно k единиц, то L называется *(ν, k)-матрицей*[1,2,3,4].

Замечание

Прямая реализация линейного рассеивающего преобразования $L \in GL(n, 2)$ в XSL-шифрсистемах предполагает минимизацию числа ненулевых элементов как в матрице L, используемой при зашифровании, так и в обратной матрице L^{-1}, используемой при расшифровании.

[1] Малышев Ф.М., Тараканов В.Е. О (v, k)-конфигурациях, Математический сборник, 192:9(2001), С.85-108.

[2] Тришин А.Е. Классификация циркулянтных $(v, 5)$-матриц, Обозрение прикладной и промышленной математики, 11:2(2004), С.258-259.

[3] Фролов А.А. Классификация неразложимых абелевых $(v, 5)$-групп, Дискретная математика, 20:1(2008), С.94-108.

[4] Комягин М.М. Классификация $(v, 5)$-конфигураций для $v \leq 11$, Дискретная математика, 36:1(2024), С.46-66.

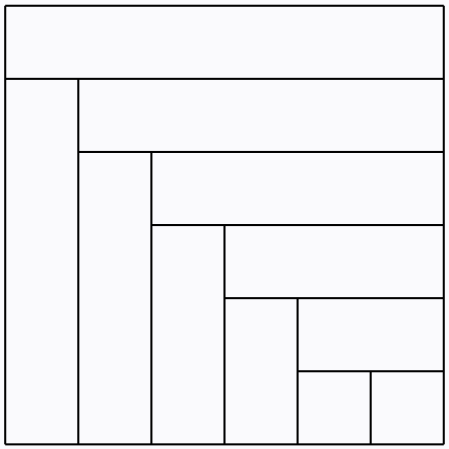
Замечание

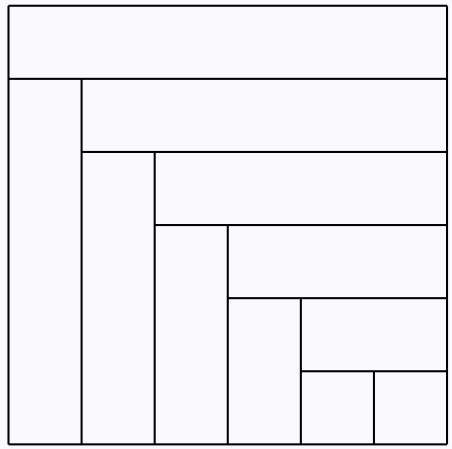
Полученные в утверждении 3 оценки трудоемкости не позволяют напрямую применять предложенный алгоритм для построения матриц $L \in GL(n, 2)$ при $n \geq 20$. Сделать это можно установив связь между коэффициентом рассеивания $\rho_m(L)$ матрицы $L \in GL(n, 2)$ и кодовым расстоянием χ_C линейного кода C, задаваемого порождающей матрицей $(E_{n\times n}, L_{n\times n})$:

$$\chi_C = \min_{\alpha \in C \setminus 0} [\alpha] = \min_{\beta \in V_n^{\times}(2)} [\beta \cdot (E_{n\times n}, L_{n\times n})] = \min_{\beta \in V_n^{\times}(2)} ([\beta] + [\beta \cdot L_{n\times n}]) = \rho_m(L)$$

Кодовое расстояние χ_C может быть вычислено, как *гарантируемый ранг* проверочной матрицы $\left(L^T_{n\times n}, E_{n\times n},\right)$ кода C, т.е. как минимальное число столбцов, являющихся линейно независимыми[1].

Проверка инволютивности





[1] Нечаев А.А. Конечные фробениусовы бимодули в теории линейных кодов, Тр. по дискр. матем., 8(2004), С.187-215.

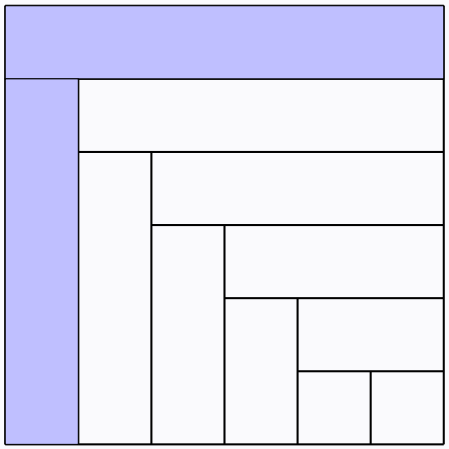
Замечание

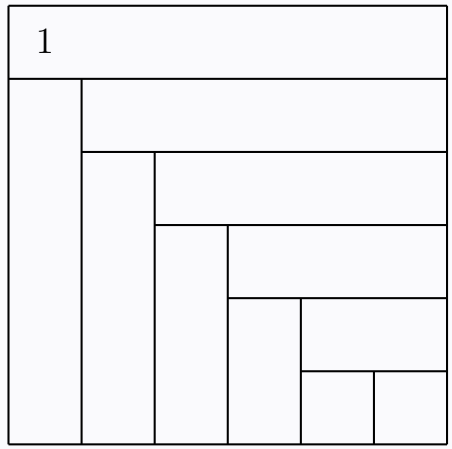
Полученные в утверждении 3 оценки трудоемкости не позволяют напрямую применять предложенный алгоритм для построения матриц $L \in GL(n, 2)$ при $n \geq 20$. Сделать это можно установив связь между коэффициентом рассеивания $\rho_m(L)$ матрицы $L \in GL(n, 2)$ и кодовым расстоянием χ_C линейного кода C, задаваемого порождающей матрицей $(E_{n\times n}, L_{n\times n})$:

$$\chi_C = \min_{\alpha \in C \setminus 0} [\alpha] = \min_{\beta \in V_n^{\times}(2)} [\beta \cdot (E_{n\times n}, L_{n\times n})] = \min_{\beta \in V_n^{\times}(2)} ([\beta] + [\beta \cdot L_{n\times n}]) = \rho_m(L)$$

Кодовое расстояние χ_C может быть вычислено, как *гарантируемый ранг* проверочной матрицы $\left(L^T_{n\times n}, E_{n\times n},\right)$ кода C, т.е. как минимальное число столбцов, являющихся линейно независимыми[1].

Проверка инволютивности





[1] Нечаев А.А. Конечные фробениусовы бимодули в теории линейных кодов, Тр. по дискр. матем., 8(2004), С.187-215.

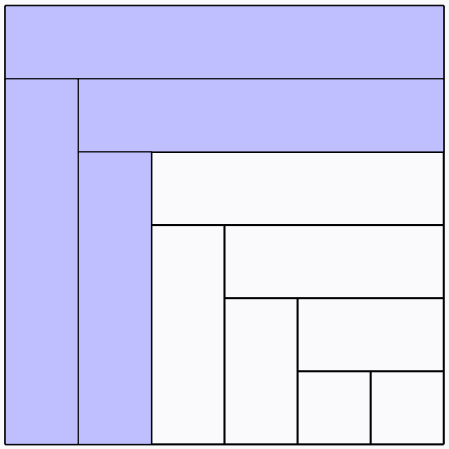
Замечание

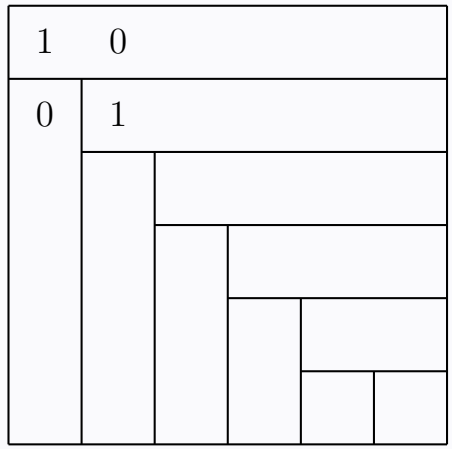
Полученные в утверждении 3 оценки трудоемкости не позволяют напрямую применять предложенный алгоритм для построения матриц $L \in GL(n, 2)$ при $n \geq 20$. Сделать это можно установив связь между коэффициентом рассеивания $\rho_m(L)$ матрицы $L \in GL(n, 2)$ и кодовым расстоянием χ_C линейного кода C, задаваемого порождающей матрицей $(E_{n\times n}, L_{n\times n})$:

$$\chi_C = \min_{\alpha \in C \setminus 0} [\alpha] = \min_{\beta \in V_n^{\times}(2)} [\beta \cdot (E_{n\times n}, L_{n\times n})] = \min_{\beta \in V_n^{\times}(2)} ([\beta] + [\beta \cdot L_{n\times n}]) = \rho_m(L)$$

Кодовое расстояние χ_C может быть вычислено, как *гарантируемый ранг* проверочной матрицы $\left(L^T_{n\times n}, E_{n\times n},\right)$ кода C, т.е. как минимальное число столбцов, являющихся линейно независимыми[1].

Проверка инволютивности





[1] Нечаев А.А. Конечные фробениусовы бимодули в теории линейных кодов, Тр. по дискр. матем., 8(2004), С.187-215.

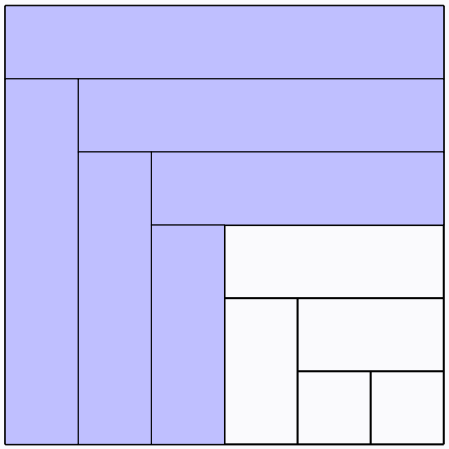
Замечание

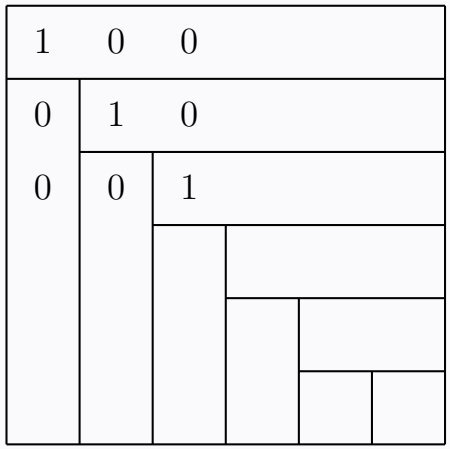
Полученные в утверждении 3 оценки трудоемкости не позволяют напрямую применять предложенный алгоритм для построения матриц $L \in GL(n, 2)$ при $n \geq 20$. Сделать это можно установив связь между коэффициентом рассеивания $\rho_m(L)$ матрицы $L \in GL(n, 2)$ и кодовым расстоянием χ_C линейного кода C, задаваемого порождающей матрицей $(E_{n\times n}, L_{n\times n})$:

$$\chi_C = \min_{\alpha \in C \setminus 0} [\alpha] = \min_{\beta \in V_n^{\times}(2)} [\beta \cdot (E_{n\times n}, L_{n\times n})] = \min_{\beta \in V_n^{\times}(2)} ([\beta] + [\beta \cdot L_{n\times n}]) = \rho_m(L)$$

Кодовое расстояние χ_C может быть вычислено, как *гарантируемый ранг* проверочной матрицы $\left(L^T_{n\times n}, E_{n\times n},\right)$ кода C, т.е. как минимальное число столбцов, являющихся линейно независимыми[1].

Проверка инволютивности





[1] Нечаев А.А. Конечные фробениусовы бимодули в теории линейных кодов, Тр. по дискр. матем., 8(2004), С.187-215.

Полученные результаты. Примеры инволютивных $(16, 3)$-матриц

$L \in GL(16, 2)$	$\rho_1(L)$	$\lvert P(L, \rho_1(L))\rvert$	$\rho'_1(L)$	$\lvert P'(L, \rho'_1(L))\rvert$	$\lvert F_L\rvert$
$\begin{pmatrix} 0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0 \\ 0&1&0&0&0&0&1&1&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&1 \\ 0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1 \\ 0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0 \\ 0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0 \\ 0&1&0&0&0&0&0&1&0&0&0&1&0&0&0&0 \\ 1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0 \\ 0&0&0&0&0&0&1&1&0&0&0&1&0&0&0&0 \\ 0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0 \\ 0&0&0&1&0&1&0&0&0&1&0&0&0&0&0&0 \\ 0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0 \end{pmatrix}$	4	56	4	56	256
	$\rho_4(L)$	$\lvert P(L, \rho_4(L))\rvert$	$\rho'_4(L)$	$\lvert P'(L, \rho'_4(L))\rvert$	$\lvert F_L\rvert$
$\begin{pmatrix} 0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0&0&1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&0&0&1&0&0&1&0&0&0&0&0 \\ 0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1 \\ 0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&0 \\ 1&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0 \\ 0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&1&0&0&0&0&0&0&1&0 \\ 1&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0 \\ 1&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0&0&1&0&0&0&1&0&0&0 \\ 0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0 \end{pmatrix}$	4	60	4	60	256

Полученные результаты. Примеры инволютивных симметричных $(16, 5)$-матриц

$L \in GL(16, 2)$	$\rho_1(L)$	$\lvert P(L, \rho_1(L))\rvert$	$\rho_1'(L)$	$\lvert P'(L, \rho_1'(L))\rvert$	$\lvert F_L\rvert$
$\begin{pmatrix} 0&1&0&0&1&1&0&0&0&0&0&1&0&1&0&0 \\ 1&0&0&0&0&1&0&0&0&1&0&0&1&1&0&0 \\ 0&0&0&0&0&0&0&1&0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&0&1&0&1&1&0&1&0&1&0 \\ 1&0&0&0&0&0&1&0&1&0&1&0&1&0&0&0 \\ 1&1&0&0&0&0&1&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&1&1&0&0&1&0&0&0&1&0&1&0 \\ 0&0&1&1&0&0&0&0&1&0&1&0&0&0&1&0 \\ 0&0&0&0&1&0&1&1&0&0&0&0&1&1&0&0 \\ 0&1&1&1&0&0&0&0&0&0&0&1&0&0&0&1 \\ 0&0&0&1&1&0&0&1&0&0&0&1&0&0&1&0 \\ 1&0&1&0&0&0&0&0&0&1&1&0&0&0&0&1 \\ 0&1&0&1&1&0&1&0&1&0&0&0&0&0&0&0 \\ 1&1&1&0&0&1&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&1&1&0&0&1&0&0&0&0&1 \\ 0&0&1&0&0&1&0&0&0&1&0&1&0&0&1&0 \end{pmatrix}$	6	32	6	32	256
	$\rho_2(L)$	$\lvert P(L, \rho_2(L))\rvert$	$\rho_2'(L)$	$\lvert P'(L, \rho_2'(L))\rvert$	$\lvert F_L\rvert$
$\begin{pmatrix} 0&0&0&1&1&0&0&0&1&0&1&0&0&0&1&0 \\ 0&0&1&0&0&0&0&1&0&1&0&0&0&1&0&1 \\ 0&1&1&0&0&0&1&0&0&0&0&1&0&0&0&1 \\ 1&0&0&1&0&1&0&0&1&0&0&0&1&0&0&0 \\ 1&0&0&0&0&1&1&0&0&0&0&0&0&1&0&1 \\ 0&0&0&1&1&0&0&1&0&1&0&0&1&0&0&0 \\ 0&0&1&0&1&0&0&1&0&0&0&1&0&0&1&0 \\ 0&1&0&0&0&1&1&0&1&0&1&0&0&0&0&0 \\ 1&0&0&1&0&0&0&1&0&0&0&0&0&1&1&0 \\ 0&1&0&0&0&1&0&0&0&1&0&0&1&0&0&1 \\ 1&0&0&0&0&0&0&1&0&0&0&1&1&0&0&1 \\ 0&0&1&0&0&0&1&0&0&0&1&0&0&1&1&0 \\ 0&0&0&1&0&1&0&0&0&1&1&0&0&1&0&0 \\ 0&1&0&0&1&0&0&0&1&0&0&1&1&0&0&0 \\ 1&0&0&0&0&0&1&0&1&0&0&1&0&0&1&0 \\ 0&1&1&0&1&0&0&0&0&1&1&0&0&0&0&0 \end{pmatrix}$	6	112	6	112	256

Полученные результаты. Примеры инволютивных симметричных $(16, 7)$-матриц

$L \in GL(16, 2)$	$\rho_1(L)$	$\lvert P(L, \rho_1(L))\rvert$	$\rho'_1(L)$	$\lvert P'(L, \rho'_1(L))\rvert$	$\lvert F_L\rvert$
$\begin{pmatrix} 0&0&1&0&1&0&0&1&1&0&0&1&0&1&1&0 \\ 0&1&0&1&1&1&1&0&0&0&0&0&1&0&1&0 \\ 1&0&1&1&0&0&1&0&0&0&1&1&0&0&0&1 \\ 0&1&1&0&0&0&1&0&0&1&1&0&0&1&0&1 \\ 1&1&0&0&0&0&0&0&1&1&0&0&1&1&0&1 \\ 0&1&0&0&0&1&0&1&1&0&0&0&1&1&1&0 \\ 0&1&1&1&0&0&0&1&1&1&0&0&0&1&0&0 \\ 1&0&0&0&0&1&1&0&0&1&0&1&0&1&0&1 \\ 1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0 \\ 0&0&0&1&1&0&1&1&0&0&1&1&0&0&1&0 \\ 0&0&1&1&0&0&0&0&1&1&1&0&1&0&0&1 \\ 1&0&1&0&0&0&0&1&1&1&0&0&1&0&1&0 \\ 0&1&0&0&1&1&0&0&1&0&1&1&0&0&1&0 \\ 1&0&0&1&1&1&1&1&0&0&0&0&0&0&0&1 \\ 1&1&0&0&0&1&0&0&0&1&0&1&1&0&1&0 \\ 0&0&1&1&1&0&0&1&0&0&1&0&0&1&0&1 \end{pmatrix}$	8	620	8	620	256
$\begin{pmatrix} 0&0&1&0&1&0&0&1&1&0&0&1&0&1&1&0 \\ 0&1&0&0&1&0&1&0&1&1&0&0&1&0&0&1 \\ 1&0&0&1&0&0&1&0&0&1&1&1&0&1&0&0 \\ 0&0&1&1&0&1&0&0&1&0&0&0&0&1&1&1 \\ 1&1&0&0&0&0&1&1&0&0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&0&1&0&0&1&0&1&0&1&1 \\ 0&1&1&0&1&0&1&1&0&0&0&0&1&1&0&0 \\ 1&0&0&0&1&1&1&0&1&1&0&0&0&0&0&0 \\ 1&1&0&1&0&0&0&1&0&0&1&1&0&0&0&1 \\ 0&1&1&0&0&0&0&1&0&1&1&1&0&1&0&0 \\ 0&0&1&0&0&1&0&1&1&1&1&0&0&0&1&0 \\ 1&0&1&0&1&0&0&0&1&1&0&0&0&0&1&1 \\ 0&1&0&0&0&1&1&0&0&0&0&0&1&1&1&1 \\ 1&0&1&1&1&0&1&0&0&1&0&0&1&0&0&0 \\ 1&0&0&1&1&1&1&0&0&0&0&1&1&1&0&0 \\ 0&1&0&1&0&1&0&0&1&0&0&1&1&0&0&1 \end{pmatrix}$	8	620	8	620	512

Замечание

Первая матрица в приведенной таблице имеет аналогичные с матрицей алгоритма ARIA[1] значения параметров $\rho_1(L)$, $\lvert P(L, \rho_1(L))\rvert$, $\rho'_1(L)$, $\left\lvert P'\left(L, \rho'_1(L)\right)\right\rvert$ и вдвое меньшее число неподвижный точек (256 против 512 в матрице алгоритма ARIA[1])

[1] Kwon D., Kim J., Park S., Sung S.H. et al. New block cipher: Aria, Information Security and Cryptology – ICISC 2003: 6th International Conference, LNCS, 2971(2004), C.432-445.

Полученные результаты. Примеры симметричных 3-регулярных 16×16 матриц

$L \in GL(16,2)$	$\rho_1(L)$	$\lvert P(L,\rho_1(L))\rvert$	$\rho'_1(L)$	$\lvert P'(L,\rho'_1(L))\rvert$	$\lvert F_L\rvert$
$\begin{pmatrix} 0&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0\\ 0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0\\ 0&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0\\ 1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1\\ 0&0&1&0&0&1&0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&1&0&1&1&0&0&0\\ 1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&0\\ 0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&1\\ 0&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1&0&1&0&0&0&0&1&0\\ 1&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0\\ 0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0\\ 0&1&0&0&0&1&0&0&0&0&1&0&0&0&0&0 \end{pmatrix}$	4	16	4	16	2
	$\rho_2(L)$	$\lvert P(L,\rho_2(L))\rvert$	$\rho'_2(L)$	$\lvert P'(L,\rho'_2(L))\rvert$	$\lvert F_L\rvert$
$\begin{pmatrix} 1&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0\\ 0&0&0&0&0&1&0&0&1&0&0&0&0&0&1&0\\ 0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0\\ 1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1\\ 0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0\\ 0&1&0&0&0&0&0&0&0&0&0&1&0&0&1&0\\ 0&0&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&1\\ 0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\ 1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&1\\ 0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&0\\ 0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0 \end{pmatrix}$	4	16	4	16	2

Замечание

Матрицы в приведенной таблице имеют максимально возможные в данном классе матриц значения $\rho_m(L)$, $\rho'_m(L)$ и минимально возможные значения $\lvert P(L,\rho_m(L))\rvert$, $\lvert P'(L,\rho'_m(L))\rvert$.

Полученные результаты.
Пример симметричной 3-регулярной 32×32 матрицы

$L \in GL(32, 2)$	$\rho_8(L)$	$\lvert P(L, \rho_8(L))\rvert$	$\rho'_8(L)$	$\lvert P'(L, \rho'_8(L))\rvert$	$\lvert F_L\rvert$
$\begin{pmatrix} 1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&1&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{pmatrix}$	4	88	4	88	4

Выводы

Выводы

1. Метод эффективен при построении k-регулярных матриц размера $\nu \times \nu$ ($\nu \in \{16, 32, 64\}$, $k \in \{3, 5\}$) и инволютивных (ν, k)-матриц ($\nu \leq 32$, $k \in \{3, 5, 7\}$) с максимально возможными значениями коэффициентов рассеивания.

Выводы

1. Метод эффективен при построении k-регулярных матриц размера $\nu \times \nu$ ($\nu \in \{16, 32, 64\}$, $k \in \{3, 5\}$) и инволютивных (ν, k)-матриц ($\nu \leq 32$, $k \in \{3, 5, 7\}$) с максимально возможными значениями коэффициентов рассеивания.

2. Метод позволяет строить k-регулярные и (ν, k)-матрицы с максимально возможными значениями коэффициентов рассеивания из различных классов комбинаторной эквивалентности.

Выводы

1. Метод эффективен при построении k-регулярных матриц размера $\nu \times \nu$ ($\nu \in \{16, 32, 64\}$, $k \in \{3, 5\}$) и инволютивных (ν, k)-матриц ($\nu \leq 32$, $k \in \{3, 5, 7\}$) с максимально возможными значениями коэффициентов рассеивания.

2. Метод позволяет строить k-регулярные и (ν, k)-матрицы с максимально возможными значениями коэффициентов рассеивания из различных классов комбинаторной эквивалентности.

3. В ряде случаев метод позволяет строить k-регулярные матрицы с максимально возможными значениями коэффициентов рассеивания $\rho_m(L)$, $\rho'_m(L)$ и минимально возможными значениями $|P(L, \rho_m(L))|$, $|P'(L, \rho'_m(L))|$.

Спасибо за внимание