ЛЕКЦИЯ 5. МЕТОД ГАУССА.

Мы разобрали выше два различных способа задания линейных подпространств $V \subset \mathbb{F}_2^n$ – при помощи образующих и как множество решений системы линейных уравнений. Для различных приложений нам совершенно необходимы оба описания, которые можно рассматривать как `двойственные`. Используя оба подхода, мы хотим дать, по возможности, более простое описание подпространства, найти его размерность, базис и простейшую систему уравнений, которые его задают. Начнем исследование с *описания подпространств, порожденных векторами*, т.е. с задачи, которая появилась в пункте 3 из Приложения в Лекции 4.

Лемма Гаусса. *Пусть $V = \langle v_1, \ldots, v_m \rangle$ подпространство в $\mathbb{F}_2^n$, порожденное m векторами $v_1, \ldots, v_m \in \mathbb{F}_2^n$. Подпространство V не меняется при следующих преобразованиях:*

1) при любой перестановке векторов $v_1, \ldots v_m$;

2) при замене вектора v_2 на вектор $v_2 + v_1$ (или, после перестановок, при замене v_j на вектор $v_j + v_i$, $i \neq j$).

Преобразования типа 1) и 2) называются **элементарными**.

Иными словами, пусть $i_1, \ldots, i_m$ перестановка индексов $1, \ldots, m$. Тогда

1) $\langle v_1, \ldots, v_m \rangle = \langle v_{i_1}, \ldots, v_{i_m} \rangle$;

2) $\langle v_1, v_2, v_3, \ldots, v_m \rangle = \langle v_1, v_2 + v_1, v_3, \ldots, v_m \rangle$.

Доказательство. Свойство 1) верно, т.к. сложение векторов коммутативно. Включение

$$\langle v_1, v_2, \ldots, v_m \rangle \supset \langle v_1, v_2 + v_1, \ldots, v_m \rangle$$

справедливо, т.к. $v_2 + v_1 \in \langle v_1, v_2, \ldots, v_m \rangle$. Имеем $v_2 = (v_2 + v_1) + v_2$, поэтому

$$\langle v_1, v_2 + v_1, \ldots, v_m \rangle \supset \langle v_1, v_2, \ldots, v_m \rangle.$$

□

Основная идея метода Гаусса состоит в том, чтобы упростить систему образующих подпространства $\langle v_1, v_2, \ldots, v_m \rangle$, последовательно применяя элементарные преобразования к *координатной матрице* образующих. Пусть $V = \langle v_1, \ldots, v_m \rangle \subset \mathbb{F}_2^n$, и известны координаты векторов $v_i = (a_{i1}, a_{i2}, \ldots, a_{in}) \in \mathbb{F}_2^n$ в каноническом базисе. Построим координатную матрицу размера m на n, состоящую из m строк-координат всех векторов v_i $(1 \leq i \leq m)$

$$A_V = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

К какой форме координатной матрицы мы будем стремиться, выполняя элементарные преобразования?

Пример 1. Пусть даны три вектора $u_1, u_2, u_3 \in \mathbb{F}_2^3$ с координатной матрицей *верхне-треугольной* формы

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 0 \end{pmatrix}.$$

Заметим, что сама форма координатной матрицы показывает, что вектора u_1, u_2, u_3 линейно независимы. Действительно, рассмотрим произвольную линейную комбинацию $t_1u_1 + t_2u_2 + t_3u_3$ данных векторов, где $t_i \in \mathbb{F}_2$:

$$\begin{array}{rcl} + \left\{ \begin{array}{l} t_1u_1 \\ t_2u_2 \\ t_3u_3 \end{array} \right. & = & + \left\{ \begin{array}{l} t_1(1,a,b) \\ t_2(0,1,c) \\ t_3(0,0,1) \end{array} \right. \\ \hline t_1u_1 + t_2u_2 + t_3u_3 & = & (t_1, t_2 + at_1, t_3 + t_2c + t_1b). \end{array}$$

Если $t_1u_1 + t_2u_2 + t_3u_3 = \bar{0} = (0,0,0)$, то из формулы справа получаем

$$(t_1 = 0) \Rightarrow (t_2 = 0) \Rightarrow (t_3 = 0).$$

Рассмотрим теперь *Метод Гаусса* на примере, в котором применяя элементарные преобразования к координатной матрице образующих V, мы найдем размерность подпространства V, его базис и уравнения, задающие это подпространство.

Пример 2. Пусть $V = \langle u_1, u_2, u_3, u_4 \rangle \subset \mathbb{F}_2^5$. Координаты образующих u_i заданы строчками следующей матрицы A_V размера 4 на 5 (на матрицу после вертикальной черты пока внимания не обращаем)

$$A_V = \left(\begin{array}{ccccc} \boxed{1} & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{array} \right| \left. \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right).$$

Напомним, что первую (слева) ненулевую координату вектора-строчки v называем **осевым элементом** или **осью** вектора (см. Предложение 3.1 из Лекции 3). Будем заключать его в квадрат. Используя ось первой строчки, мы можем обнулить все элементы первого столбца. Для матрицы A_V это можно сделать элементарными преобразованиями $u_2 + u_1$, $u_3 + u_1$ и $u_4 + u_1$. Чтобы запомнить эти преобразования, мы добавим справа к матрице A_V квадратную матрицу порядка 4 (по числу строк!) с единицами на главной диагонали, *единичную матрицу порядка* 4, и будем выполнять с ее строчками соответствующие линейные операции,

кодирующие выполняемые элементарные операции. Назовем эту дополнительную матрицу **матрицей линейных комбинаций**. После первых преобразований $u_2 \mapsto u_2 + u_1$, $u_3 \mapsto u_3 + u_1$ и $u_4 \mapsto u_4 + u_1$ получаем матрицы

$$\left(\begin{array}{ccccc} \boxed{1} & 1 & 1 & 0 & 1 \\ 0 & 0 & \boxed{1} & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right) \left| \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right).$$

В силу Леммы Гаусса четыре строчки новой матрицы u'_1, u'_2, u'_3 и u'_4 порождают исходное подпространство V. Следующим осевым элементом будет третий элемент второй строчки. Продолжим элементарные преобразования и сделаем нулями элементы под вторым осевым элементом $u'_3 \mapsto u'_3 + u'_2$)

$$\left(\begin{array}{ccccc} \boxed{1} & 1 & 1 & 0 & 1 \\ 0 & 0 & \boxed{1} & 1 & 1 \\ 0 & 0 & 0 & 0 & \boxed{1} \\ 0 & 0 & 0 & 0 & 1 \end{array}\right) \left| \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right).$$

Следующим осевым элементом будет последний элемент третьей строчки. Выполним преобразование $u''_4 \mapsto u''_4 + u''_3 = \bar{0}$, получим

$$A_V^{(2)} = \left(\begin{array}{ccccc} \boxed{1} & 1 & 1 & 0 & 1 \\ 0 & 0 & \boxed{1} & 1 & 1 \\ 0 & 0 & 0 & 0 & \boxed{1} \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \left| \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{array}\right) .$$

В матрице $A_V^{(2)}$ нет других осевых элементов. Переменные x_1, x_3 и x_5 называем осевыми, а x_2 x_4 – неосевыми. Следовательно, используя элементарные преобразования, мы привели матрицу A_V к **ступенчатой** матрице $A_V^{(2)}$. В силу полной аналогии с Примером 1, можете показать, что три строчки этой матрицы *линейно независимые.*

Первые выводы.

1) **Базис и размерность.** У последней матрицы три осевых элемента. Они указывают на три линейно независимые строчки

$$v_1 = (\boxed{1}, 1, 1, 0, 1), \quad v_2 = (0, 0, \boxed{1}, 1, 1), \quad v_3 = (0, 0, 0, 0, \boxed{1})$$

и три линейно независимые столбца с номерами 1, 3 и 5. В силу Леммы Гаусса

$$V = \langle u_1, u_2, u_3, u_4 \rangle = \langle v_1, v_2, v_3, \bar{0} \rangle = \langle v_1, v_2, v_3 \rangle$$

и

$$\dim V = 3.$$

Линейно независимые векторы v_1, v_2, v_3 образуют **базис** исходного подпространства $V \subset \mathbb{F}_2^5$.

2) **Линейные соотношения между образующими.** Кроме того, мы нашли линейное соотношение между исходными образующими $V = \langle u_1, u_2, u_3, u_4 \rangle$, которое соответствует последней нулевой строчке матрицы $A_V^{(2)}$. Соответствующие коэффициенты стоят в последней строчке матрицы линейных комбинаций

$$u_1 + u_2 + u_3 + u_4 = 0.$$

3) **Расширение базиса V до базиса $\mathbb{F}_2^5$.** У ступенчатой матрицы $A_V^{(2)}$ имеются три осевых элемента, отвечающих первой, третьей и пятой координатам. Чтобы достроить базис V до базиса $\mathbb{F}_2^n$ достаточно добавить вектора $e_2 = (0,1,0,0,0)$ и $e_4 = (0,0,0,1,0)$ соответствующие неосевым координатам x_2 и x_4

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

Можно ли продолжить Метод Гаусса и найти более простую систему образующих подпространства V? Да, мы можем продолжить элементарные преобразования, начиная с последнего осевого элемента, и добиться того, чтобы все элементы координатной матрицы **над осевыми элементами** были равны 0.

Используем последний столбец и получим матрицу

$$\left(\begin{array}{ccccc} \boxed{1} & 1 & 1 & 0 & 0 \\ 0 & 0 & \boxed{1} & 1 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} \end{array}\right) \left| \begin{array}{cccc} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right).$$

В дополнительной матрице линейных соотношений указаны соответствующие преобразования со строками. Потом упрощаем третий столбец

$$A_V^{(3)} = \left(\begin{array}{ccccc} \boxed{1} & 1 & 0 & 1 & 0 \\ 0 & 0 & \boxed{1} & 1 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} \end{array}\right) \left| \begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right).$$

Получилась матрица $A_V^{(3)}$, у которой ниже и выше всех осевых элементов стоят нули. Строки $A_V^{(3)}$ содержат новый базис (w_1, w_2, w_3) исходного подпространства V. Правая дополнительная матрица дает выражения этих векторов через исходные образующие

$$w_1 = (1,1,0,1,0), \quad w_2 = (0,0,1,1,0), \quad w_3 = (0,0,0,0,1),$$

$$w_1 = u_2, \qquad w_2 = u_1 + u_3, \qquad w_3 = u_2 + u_3.$$

4) Задание подпространства V уравнениями. *Матрица $A_V^{(3)}$ позволяет нам найти уравнения, задающие подпространство V.* В координатной матрице есть три осевые координаты x_1, x_2, x_3. Над осевыми элементами нет ненулевых элементов. Мы можем найти неосевые координаты x_2 и x_4 через осевые. Чтобы убедиться в этом, рассмотрим все линейные комбинации базиса w_1, w_2, w_3 подпространства V

$$\begin{array}{rcl} + \left\{ \begin{array}{l} t_1 w_1 \\ t_2 w_2 \\ t_3 w_3 \end{array} \right. & = & + \left\{ \begin{array}{l} t_1(\boxed{1},\ 1,\ 0,\ \ 1,\ \ 0) \\ t_2(\ 0,\ \ 0,\ \boxed{1},\ 1,\ \ 0) \\ t_3(\ 0,\ \ 0,\ \ 0,\ \ 0,\ \boxed{1}) \end{array} \right. \\ \hline t_1 w_1 + t_2 w_2 + t_3 w_3 & = & (t_1,\ t_1,\ t_2, t_1 + t_2, t_3). \end{array}$$

Следовательно, для всех векторов $(x_1, x_2, x_3, x_4, x_5) \in V$ выполняется

$$(x_1, x_2, x_3, x_4, x_5) = (t_1, t_1, t_2, t_1 + t_2, t_3),$$

откуда мы получаем два уравнения, задающие подпространство V

$$x_2 = x_1 \quad \text{и} \quad x_4 = x_1 + x_3.$$

Другими словами эти два уравнения, задающие подпространство V, определяются неосевыми столбцами расширенной матрицы $A_V^{(2)}$

$$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \qquad \tilde{A}_V^{(2)} = \begin{pmatrix} \boxed{1} & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & \boxed{1} & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} \end{pmatrix}.$$

Системы линейных уравнений и линейные отображения.

Для развития Метода Гаусса нам потребуются концепция линейных отображений. Рассмотрим неоднородную систему из $m \geq 1$ уравнений с $n \geq 1$ неизвестными над полем $\mathbb{F}_2$

$$(A|b) = \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n & = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n & = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n & = b_m, \end{cases}$$

где $a_{ij} \in \mathbb{F}_2$ для $1 \leq i \leq m$, $1 \leq j \leq n$ и $b_i \in \mathbb{F}_2$ для $1 \leq i \leq m$.

Заметим, что левая часть i-го уравнения может быть записана с помощью билинейной формы $(\cdot,\cdot) : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$

$$a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = (\bar{a}_i, \bar{x}),$$

где $\bar{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in})$ и $\bar{x} = (x_1, x_2, \ldots, x_n)$. Тогда левая часть системы уравнений перепишется в форме столбца, зависящего от вектора $\bar{x}$, который мы обозначим $A \cdot \underline{x}$

$$A \cdot \underline{x} = A \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} (\bar{a}_1, \bar{x}) \\ (\bar{a}_2, \bar{x}) \\ \vdots \\ (\bar{a}_m, \bar{x}) \end{pmatrix},$$

где $\underline{x}$ обозначает вектор-столбец из $\mathbb{F}_2^n$. Эта новая операция $A \cdot \underline{x}$, – *умножение матрицы A размера m на n на вектор-столбец $\underline{x}$ высоты n*, – линейна по векторному аргументу

$$A \cdot (\underline{x} + \underline{x'}) = (A \cdot \underline{x}) + (A \cdot \underline{x'}).$$

Это непосредственно следует из линейности спаривания $(\cdot,\cdot)$.

Мы будем использовать обе модели линейного векторного пространства $\mathbb{F}_2^n$ в форме векторов-строк длины n и в форме векторов-столбцов высоты n. Иными словами мы рассматриваем эти модели как реализацию одного и того же пространства. (Отметим, что спаривание $(\cdot,\cdot)$ фиксирует двойственность между этими пространствами. Мы обсудим этот вопрос позднее.)

Итак, левую часть системы линейных уравнений можно рассматривать как **линейное отображение**

$$\mathcal{A} : \mathbb{F}_2^n \to \mathbb{F}_2^m, \qquad \mathcal{A}(x) = A \cdot \underline{x} \in \mathbb{F}_2^m.$$

В этих функциональных терминах мы можем легко переформулировать вопрос о существовании решения у системы неоднородных линейных уравнений $(A|b)$ для любого вектора $b \in \mathbb{F}_2^m$ и описать все такие решения. Решение существует тогда и только тогда, когда вектор b лежит в образе линейного отображение $\mathcal{A}$, т.е. $b \in \mathrm{Im}(\mathcal{A})$.

Предложение 1. *Пусть $V_A \subset \mathbb{F}_2^n$ есть подпространство решений однородной системы линейных уравнений $(A|\underline{0})$ с нулевой правой частью. Предположим, что существует решение $\underline{x_b} \in \mathbb{F}_2^n$ системы уравнений $(A|b)$: $A \cdot \underline{x_b} = \underline{b}$. Тогда множество всех решений системы $(A|b)$ совпадает с* **аффинным подпространством**

$$x_b + V_A = \{x_b + u \,|\, u \in V_A\}.$$

Доказательство. 1) Пусть $v \in x_b + V_A$, т.е. $v = x_b + u$, где $A \cdot \underline{u} = \underline{0}$. Докажем, что это решение системы $(A|b)$

$$A \cdot \underline{v} = A \cdot (\underline{x_b} + \underline{v}) = A \cdot \underline{x_b} + A \cdot \underline{v} = \underline{b} + \underline{0} = \underline{b}.$$

2) Пусть v какое-то решение. Тогда $A \cdot \underline{v} = A \cdot \underline{x_b} = \underline{b}$, поэтому

$$A \cdot \underline{v} - A \cdot \underline{x_b} = A \cdot (\underline{v} - \underline{x_b}) = \underline{0}.$$

Следовательно, $v - x_b \in V_A$ и $v \in x_b + V_A$.

□

В предыдущих лекция мы описали пространство решений V_A однородной системы уравнений $(A|\underline{0})$. Это линейное подпространство в $\mathbb{F}_2^n$ размерности $n - k$, где k ранг матрицы коэффициентов A. Техника линейных пространств, которую мы изучили, позволяет нам дать качественный ответ на вопрос о существовании решений системы $(A|b)$.

Теорема 9. Теорема Кронекера-Капелли. *Неоднородная система линейных уравненений $(A|\underline{b})$ совместима тогда и только тогда, когда ранг матрицы коэффициентов системы $A \in M_{m\times n}(\mathbb{F}_2)$ равен рангу расширенной матрицы $(A|\underline{b}) \in M_{m\times(n+1)}(\mathbb{F}_2)$.*

Доказательство. Запишем систему уравнений в форме векторного уравнения в пространстве $\mathbb{F}_2^m$ (см. Лекцию 3)

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} x_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} x_2 + \cdots + \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} x_n = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix},$$

где мы используем вектора-столбцы A_j высоты m матрицы коэффициентов A и вектор-столбец $\underline{b}$

$$A_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}, \quad \underline{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{F}_2^m \qquad \text{для } j = 1, \ldots, n.$$

Вектор $\underline{b}$ представим в виде линейной комбинации столбцов A_j тогда и только тогда, когда

$$\underline{b} \in \langle A_1, \ldots A_n \rangle \subset \mathbb{F}_2^m.$$

Это эквивалентно тому, что

$$\langle A_1, \ldots A_n, \underline{b} \rangle \subset \langle A_1, \ldots A_n \rangle.$$

Но второе подпространство является подпространством первого, поэтому включение выполняется тогда и только тогда, когда

$$\dim \langle A_1, \ldots A_n \rangle = \dim \langle A_1, \ldots A_n, \underline{b} \rangle.$$

Это эквивалентно утверждению доказываемой теоремы в силу результата Теоремы 8 о том, что ранг матрицы по строкам равен рангу по столбцам.

□