ЛЕКЦИЯ 4. Задание подпространств уравнениями, системы линейных уравнений, ранг матрицы.

Основные результаты Лекции 4.

1) Любое подпространство $V_k \subset \mathbb{F}_2^n$ размерности k задается некоторой системой из $n-k$ линейных однородных уравнений.

2) Пространство решений m линейных однородных уравнений с n неизвестными есть подпространство в $\mathbb{F}_2^n$ размерности $n-k$, где k размерность подпространства в $\mathbb{F}_2^n$, порожденного векторами коэффициентов уравнений системы.

3) Ранг любой $m \times n$-матрицы по m векторам-строчкам равен рангу этой матрицы по n векторам-столбцам.

4) Задача к Лемме 1 этой Лекции (в реале не была сформулирована). Биекция между подпространствами размерности k и $n-k$.

В этой лекции мы покажем, как можно использовать существование двойственного базиса для исследования систем линейных уравнений. В Лекции 3 мы доказали следующий результат.

Теорема 5. (**О существовании двойственного базиса.**) *Пусть* $(u_1, \dots, u_n)$ *произвольный базис* n*-мерного пространства* $\mathbb{F}_2^n$. *Тогда существует другой базис* $(u_1^*, \dots, u_n^*)$ *пространства* $\mathbb{F}_2^n$ *такой, что*

$$\forall\, 1 \le i, j \le n: \ (u_i, u_j^*) = \begin{cases} 1 & i = j, \\ 0 & i \ne j. \end{cases}$$

Базис $(u_1^*, \dots, u_n^*)$ *называется* **двойственным** *к базису* $(u_1, \dots, u_n)$.

Двойственный базис позволяет находить координаты вектора v в базисе $(u_1, \dots, u_n)$, используя билинейную форму (u, v). Если

$$v = x_1 u_1 + x_2 u_2 + \dots + x_n u_n, \quad \text{тогда} \quad x_i = (v, u_i^*) \quad \forall\, 1 \le i \le n.$$

Аналогично, можно найти координаты *того же самого вектора* v в двойственном базисе. Если

$$v = y_1 u_1^* + y_2 u_2^* + \dots + y_n u_n^*, \quad \text{тогда} \quad y_i = (v, u_i) \quad \forall\, 1 \le i \le n.$$

Теорема 6. (О возможности задания подпространства линейными уравнениями.) *Любое подпространство* $V_k \subset \mathbb{F}_2^n$ *размерности* k *задается системой из* $n-k$ *линейных однородных уравнений.*

Доказательство. Пусть $(u_1, \dots, u_k)$ какой-нибудь базис подпространства V_k. Дополним его до базиса $(u_1, \dots, u_k; u_{k+1}, \dots, u_n)$ пространства $\mathbb{F}_2^n$ (см. Следствие 2 Теоремы 1, Лекция 1). Рассмотрим двойственный к

нему базис $(u_1^*, \ldots, u_k^*, u_{k+1}^*, \ldots, u_n^*)$. Получаем

$$\begin{aligned} V_k &= \{v = x_1u_1 + \ldots x_ku_k + 0 \cdot u_{k+1} + \cdots + 0 \cdot u_n \,|\, x_i \in \mathbb{F}_2 \text{ для } 1 \le i \le k\} \\ &= \{v \in \mathbb{F}_2^n \,|\, (v, u_{k+1}^*) = \cdots = (v, u_n^*) = 0\} \\ &= H_{u_{k+1}^*} \cap \ldots \cap H_{u_n^*}. \end{aligned}$$

Следовательно, V_k совпадает со множеством решений системы из $n-k$ однородных линейных уравнений или, другими словами, с пересечением $n-k$ попарно различных гиперплоскостей.

□

ПРИЛОЖЕНИЕ. Описание пространства решений системы однородных линейных уравнений от n переменных.

Рассмотрим систему из $m \ge 1$ уравнений с $n \ge 1$ неизвестными над полем $\mathbb{F}_2$ из двух элементов 0 и 1

$$(A) = \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n & = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n & = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n & = 0, \end{cases}$$

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

Обозначим через $V_A \subset \mathbb{F}_2^n$ множество решений этой системы, т.е. множество векторов $\bar{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, координаты $x_1, \ldots, x_n$ которых удовлетворяют указанной выше системы линейных уравнений (A). Отметим, что V_A содержит нулевой вектор для любой системы (A).

1. *Множество решений V_A является линейным подпространством в $\mathbb{F}_2^n$.*

Каждое уравнение системы может быть переписано в форме $(\bar{a}_i, \bar{x}) = 0$, где вектор $\bar{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in}) \in \mathbb{F}_2^n$ образован коэффициентами уравнения с номером i, а $\bar{x} = (x_1, x_2, \ldots, x_n)$. Уравнение $(\bar{a}_i, \bar{x}) = 0$ с ненулевые вектором $\bar{a_i}$ определяет гиперплоскость $H_{\bar{a_i}}$ размерности $n-1$, а нулевое уравнение $0 \cdot x_1 + 0 \cdot x_2 + \ldots + 0 \cdot x_n = 0$ определяет все пространство $\mathbb{F}_2^n$. Получаем, что V_A есть пересечение m подпространств. Следовательно, V_A является подпространством по Теореме 2 (Лекция 2).

□

2. *Как найти размерность пространства решений V_A и его базис?*

ПЕРВЫЙ МЕТОД, использующий вектора коэффициентов уравнений, т.е. **строки** системы (A).

Рассмотрим подпространство $L_A = \langle \bar{a}_1, \ldots, \bar{a}_m \rangle \subset \mathbb{F}_2^n$, порожденное m векторами, построенными по коэффициентам уравнений. Размерность

$k = \dim L_A$ этого подпространства называется **рангом системы векторов** $(\bar{a}_1, \ldots, \bar{a}_m)$. Мы дадим новое описание пространства решений V_A, используя подпространство L_A.

Лемма 1. Определим подпространство

$$(L_A)^\perp = \{\bar{x} \in \mathbb{F}_2^n : \forall\ l \in L_A :\ (l, \bar{x}) = 0\}.$$

Тогда $V_A = (L_A)^\perp$.

Доказательство. По определению,

$$V_A = \{\bar{x} \in \mathbb{F}_2^n : \forall\, 1 \leq i \leq n : (\bar{a}_i, \bar{x}) = 0\}.$$

Все a_i лежат в L_A, поэтому в определении подпространства $(L_A)^\perp$ имеется *больше* линейных уравнений. Следовательно, $V_A \supset (L_A)^\perp$.

Докажем обратное. Любой вектор $l \in L_A$ есть линейная комбинация образующих $l = y_1\bar{a}_1 + \ldots + y_m\bar{a}_m$. Следовательно, для любого решения $\bar{x} \in V_A$ исходной системы (A) имеем

$$(l, \bar{x}) = (y_1 a_1 + \ldots + y_m a_m, \bar{x}) = y_1(\bar{a}_1, \bar{x}) + \ldots + y_m(\bar{a}_m, \bar{x}) = 0.$$

(Напомним, что спаривание $(\cdot, \cdot)$ линейно по каждому аргументу.) Мы доказали включение $V_A \subset (L_A)^\perp$.

□

Положим, что пространство, порожденное векторами уравнений, имеет размерность $k = \dim L_A$. Ясно, что $k \leq m$. Рассмотрим какой-нибудь базис $(b_1, \ldots, b_k)$ подпространства L_A, который можно построить, используя алгоритм из доказательства Теоремы 1. (Другой алгоритм, алгоритм Гаусса, мы рассмотрим в Лекции 5.)

Применим Лемму 1 к этим новым образующим подпространства $L_A = \langle \bar{b}_1 \ldots, \bar{b}_k \rangle$. Получаем третье описание пространства решений исходной системы уравнений (A), использующее только k уравнений

$$V_A = (L_A)^\perp = \{\bar{x} \in \mathbb{F}_2^n \mid (\bar{b}_i, \bar{x}) = 0 \text{ для } 1 \leq i \leq k\}.$$

Вектора базиса $(\bar{b}_1 \ldots, \bar{b}_k)$ являются линейно независимыми, а между векторами $(\bar{a}_1, \ldots, \bar{a}_m)$ коэффициентов исходных уравнений могли быть линейные соотношения.

Теперь мы можем описание подпространства решений, используя метод доказательства Теоремы 6. Достроим выбранный базис до базиса $(\bar{b}_1, \ldots, \bar{b}_k; \bar{b}_{k+1}, \ldots, \bar{b}_n)$ пространства $\mathbb{F}_2^n$ и возьмем двойственный к нему базис $(\bar{b}_1^*, \ldots, \bar{b}_n^*)$. Тогда, как и в Теореме 6, получаем явное описание пространства решений. Возьмем произвольный вектор $\bar{x} \in \mathbb{F}_2^n$ и **запишем его в базисе** $(\bar{b}_1^*, \ldots, \bar{b}_n^*)$ пространства $\mathbb{F}_2^n$

$$\bar{x} = x_1\bar{b}_1^* + \cdots + x_k\bar{b}_n^*$$

Этот вектор будет решением системы уравнений (A) тогда и только тогда, когда

$$(\bar{x}, \bar{b}_i) = 0 \qquad \text{для любого} \quad 1 \le i \le k.$$

Это эквивалентно тому, что все координаты x_i в представлении решения $\bar{x}$ в двойственном базисе равны 0. Следовательно, мы получаем следующее описание пространства решений

$$V_A = \{v = x_{k+1}\bar{b}^*_{k+1} + \cdots + x_n\bar{b}^*_n \,|\, x_{k+1}, \ldots, x_n \in \mathbb{F}_2^n\}.$$

Вектора $(\bar{b}^*_{k+1}, \ldots, \bar{b}^*_n)$ линейно независимы как вектора двойственного базиса. Они дают базис пространства решений V_A исходной системы линейных уравнений (A). Размерность V_A равна $n - k$. Тем самым мы доказали следующую теорему.

Теорема 7. (Размерность пространства решений системы линейных уравнений.) *Пространство решений системы линейных однородных уравнений (A) является подпространством размерности $n - k$ в $\mathbb{F}_2^n$, где k ранг системы векторов $(\bar{a}_1, \ldots, \bar{a}_m)$, образованных коэффициентами всех m уравнений системы (или размерность подпространства $L_A = \langle \bar{a}_1, \ldots, \bar{a}_m \rangle \subset \mathbb{F}_2^n$, порожденного этими векторами).*

ВТОРОЙ МЕТОД, описания решений системы (A), использующий одно векторное уравнение, построенное по **столбцам** системы уравнений (A). Перепишем исходную систему уравнений

$$(A) = \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n & = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n & = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n & = 0, \end{cases}$$

в форме векторного уравнения в пространстве $\mathbb{F}_2^m$ размерности m:

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} x_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} x_2 + \cdots + \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} x_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

где мы ввели n векторов-столбцов высоты m

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

Рассмотрим подпространство, порожденное векторами A_j в $\mathbb{F}_2^m$

$$C_A = \langle A_1, \ldots A_n \rangle \subset \mathbb{F}_2^m.$$

Пусть $l = \dim C_A$. Выберем базис $(A_{i_1}, \ldots, A_{i_l})$ ($1 \le i_s \le n$ для $1 \le s \le l$) подпространства C_A из столбцов-векторов $A_1, \ldots, A_n$. Такой базис можно найти, используя алгоритм из доказательства Теоремы 1 Лекции 1. (Проверьте!) Теперь мы можем описать множество решений, используя этот базис. По свойству базиса для любых $x_j \in \mathbb{F}_2$ ($1 \le j \le n$ и $j \ne i_s$ с $1 \le s \le l$) *всегда существует единственный набор* $(x_{i_1}, \ldots x_{i_l})$ коэффициентов из $\mathbb{F}_2$ такой, что

$$\sum_{1 \le j \le m \text{ и } j \ne i_1, \ldots, i_l} A_j x_j = A_{i_1} x_{i_1} + \cdots + A_{i_l} x_{i_l}.$$

Каждая из $n - l$ переменных x_j в левой части последнего уравнения принимает два значения 0 и 1 независимо от остальных переменных в левой части. Следовательно, векторное уравнение в $\mathbb{F}_2^m$ (а значит и исходная система уравнений (A)!) имеет 2^{n-l} решений. Иными словами, пространство решений системы (A) имеет размерность $n - l$, где $l = \dim \langle A_1, A_2, \ldots, A_n \rangle$.

Выше, используя первый метод, мы доказали, что пространство решений системы однородных линейных уравнений (A) имеет размерность $n-k$, где $k = \dim L_A = \dim \langle \bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n \rangle$ размерность подпространства, порожденного векторами, составленными из коэффициентов уравнений, т.е. из строк системы (A). Следовательно, $k = l$ и мы доказали следующую важную теорему.

Теорема 8. *Пусть дана* **матрица** A *размера* m *на* n *с элементами в поле* $\mathbb{F}_2$

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \in M_{m \times n}(\mathbb{F}_2).$$

(m– число строк, а n – число столбцов.) Тогда размерность подпространства

$$L_A = \langle \bar{a}_1, \bar{a}_2, \ldots, \bar{a}_m \rangle \subset \mathbb{F}_2^n,$$

порожденного m *строками матрицы* A

$$\bar{a}_i = (a_{i1}, a_{i2}, \ldots a_{in}) \in \mathbb{F}_2^n, \qquad 1 \le i \le m,$$

совпадает с размерностью подпространства

$$C_A = \langle A_1, A_2, \ldots, A_n \rangle \subset \mathbb{F}_2^m,$$

порожденного n *столбцами матрицы* A

$$A_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix} \in \mathbb{F}_2^m, \qquad 1 \le j \le n.$$

Эта размерность

$$k = \dim L_A = \dim C_A$$

называется **рангом матрицы** A.

Какие вопросы мы должны прояснить?

1) Как "быстро" найти базис подпространства $\langle \bar{a}_1, \ldots, \bar{a}_m \rangle \subset \mathbb{F}_2^n$ или подпространства $\langle A_1, \ldots \bar{A}_n \rangle \subset \mathbb{F}_2^m$?

2) Как найти все линейные соотношения между векторами $(\bar{a}_1, \ldots, \bar{a}_m)$ в пространстве $\mathbb{F}_2^n$?

3) Как "быстро" расширить базис подпространства до базиса всего линейного пространства $\mathbb{F}_2^n$?

4) Можно ли найти базис пространства решений в Теореме 7 без расширения базиса подпространства L_A до базиса всего пространства и нахождения двойственного базиса пространства $\mathbb{F}_2^n$?

5) Как найти $n - k$ уравнения, задающие подпространство V_k в Теореме 6, без расширения базиса и нахождения двойственного базиса всего пространства $\mathbb{F}_2^n$?

6) Дать алгоритм построения двойственного базиса по данному базису в n-мерном пространстве $\mathbb{F}_2^n$.

Правильная и полная реализация **Метода Гаусса** дает нам единый эффективный алгоритм и новый теоретических метод для **одновременного** решения всех поставленных выше вопросов. Мы сделаем это в следующей лекции,

Задача к Лемме 1. По любому подпространству $U \subset \mathbb{F}_2^n$ мы можем определить "дуальное" к нему подпространство, используя результат Леммы 1:

$$U^\perp = \{v \in \mathbb{F}_2^n \,|\, \forall\, u \in U \;\; (u, v) = 0\}.$$

Например, $\{\bar{0}\}^\perp = \mathbb{F}_2^n$ и $(\mathbb{F}_2^n)^\perp = \{\bar{0}\}$. (Проверьте!)

1. Показать, что $U^\perp$ подпространство.

2. Найти размерность подпространства $U^\perp$.

3. Найти подпространство $(U^\perp)^\perp$.

4. Доказать, что отображение $U \mapsto U^\perp$ является биективным отображением множества всех подпространств $\mathbb{F}_2^n$ на себя.

5. Число подпространств в $\mathbb{F}_2^n$ размерности k равно числу подпространств в $\mathbb{F}_2^n$ размерности $n - k$.

6*. Найти примеры подпространств в $\mathbb{F}_2^n$ (с $n > 0$) таких, что $U = U^\perp$.

7**. Дать какое-нибудь разумное описание всех таких подпространств в пространствах размерности 4 и 8 над полем $\mathbb{F}_2$.