ЛЕКЦИЯ 2. Операции с подпространствами, число базисов число базисов и число подпространств размерности k.

`Основные результаты Лекции 2.`

1) $U \cap V$, $U + V$, $\dim(U + V)$.
2) Подсчет числа плоскостей в $\mathbb{F}_2^4$.
3) Число различных базисов.
4) Число подпространств размерности k в $\mathbb{F}_2^n$.
5) Число ненулевых векторов совпадает с число гиперплоскостей.

ОПЕРАЦИИ С ПОДПРОСТРАНСТВАМИ

Теорема 2. *Пусть U и V два подпространства в $\mathbb{F}_2^n$.*

1) Подмножества $U \cap V$ и $U + V = \{u + v \,|\, u \in U, v \in V\}$ являются подпространствами в $\mathbb{F}_2^n$. $U + V$ называется **суммой** *двух подпространств.*

2) $\dim(U + V) = \dim U + \dim V - \dim (U \cap V)$.

Доказательство. 1) Пусть $u, v \in U \cap V$. Тогда $u, v \in U$ и $u, v \in V$, поэтому $u + v \in U$ и $u + v \in V$. Следовательно $u + v \in U \cap V$.

Пусть $w_1, w_2 \in U+V$. Тогда $w_i = u_i+v_i$, где $u_i \in U$ и $v_i \in V$, поэтому $w_1 + w_2 = (u_1 + v_1) + (u_2 + v_2) = (u_1 + u_2) + (v_1 + v_2) \in U + V$.

2) Пусть $\dim U = k$ и $\dim V = m$. Имеем $U \cap V \subset U$ и $U \cap V \subset V$. Возьмем какой-нибудь базис $(w_1, \ldots, w_l)$ подпространства $U \cap V$. Дополним его векторами $(u_{l+1}, \ldots, u_k)$ до базиса подпространства U и векторами $(v_{l+1}, \ldots, v_m)$ до базиса подпространства V.

а) Векторы $(w_1, \ldots, w_l, u_{l+1}, \ldots, u_k, v_{l+1}, \ldots, v_m)$ порождают подпространство $U+V$. Для любых $u \in U$ и $v \in V$ существуют $a_1, \ldots, a_k, b_1, \ldots, b_m \in \mathbb{F}_2$ такие, что

$$u = a_1 w_1 + \cdots + a_l w_l + a_{l+1} u_{l+1} + \cdots + a_k u_k,$$
$$v = b_1 w_1 + \cdots + b_l w_l + b_{l+1} v_{l+1} + \cdots + b_m v_m.$$

Получаем

$$u+v = (a_1+b_1)w_1+\ldots+(a_l+b_l)w_l+a_{l+1}u_{l+1}+\ldots+a_l u_k+b_{l+1}v_{l+1}+\ldots+b_m v_m.$$

б) Докажем, что эта система из $k + (l - k) + (m - k) = l + m - k$ векторов линейно независима. Пусть

$$a_1 w_1 + \ldots + a_l w_l + b_{l+1} u_{l+1} + \ldots + b_k u_k + c_{l+1} v_{l+1} + \ldots + c_m v_m = \bar{0}.$$

Тогда

$$c_{l+1} v_{l+1} + \ldots + c_m v_m = a_1 w_1 + \ldots + a_l w_l + b_{l+1} u_{l+1} + \ldots + b_k u_k \in U \cap V.$$

По построению базиса $(w_1, \ldots, w_l, v_{l+1}, \ldots v_m)$ любая ненулевая линейная комбинация векторов $(v_{l+1}, \ldots, v_m)$ не принадлежит подпространству $U \cap V$, т.к. в противном случае получилось бы нетривиальное линейное соотношение между векторами базиса U. Следовательно, все коэффициенты c_j равны 0. Но тогда и все a_s, и все b_t равны 0, так как $(w_1, \ldots, w_l, u_{l+1}, \ldots, u_k)$ базис подпространства V.

ПРИМЕРЫ 2.1–2.5. Плоскости в $\mathbb{F}_2^4$.

1) *Пространство $\mathbb{F}_2^4$ содержит 35 плоскостей.*

В качества базиса плоскости $V_2 \subset \mathbb{F}_2^4$ выбираем пару векторов (u, v), где $u \in \mathbb{F}_2^4 \setminus \{\bar{0}\}$ (15 вариантов) и $v \in \mathbb{F}_2^4 \setminus \langle u \rangle$ $(16 - 2 = 14$ вариантов). Следовательно существует $15 \cdot 14$ базисов плоскостей в $\mathbb{F}_2^4$. Каждая плоскость имеет ровно 6 базисов, поэтому существует ровно $\frac{15 \cdot 14}{6} = 35$ различных плоскостей в $\mathbb{F}_2^4$.

2) *Пусть V_2 некоторая плоскость в $\mathbb{F}_2^4$. Сколько плоскостей (из 35!) пересекаются с ней только по нулевому вектору $\{\bar{0}\}$?*

Пусть $\{u, w\}$ такая плоскость U_2. Тогда $u \notin V_2$ и имеется $16 - 4 = 12$ таких векторов. Далее $w \notin V_2 \cup (V_2 + u) = \langle V_2, u \rangle = V_3$ (трехмерное подпространство!). Следовательно, мы имеем $2^4 - 2^3 = 8$ вариантов для w и $12 \cdot 8$ вариантов выбора базиса плоскости U. Но каждая плоскость имеет 6 различных базисов, поэтому существует 16 плоскостей U_2 таких, что $V_2 \cap U_2 = \{\bar{0}\}$. Отметим, что в этом случае $V_2 + U_2 = \mathbb{F}_2^4$ по формуле размерности.

3) *Пусть $V_2 = \langle v_1, v_2 \rangle$. Сколько плоскостей U_2 в $\mathbb{F}_2^4$ пересекают V_2 по прямой $\langle v_1 \rangle$?*

U_2 содержит v_1 и еще один вектор w, не лежащий в V_2 (имеется $16 - 4 = 12$ вариантов). Отметим, что w и $w + v_1$ задают одну плоскость. Следовательно, имеется $12/2 = 6$ плоскостей.

4) Всего имеется $6 \times 3 = 18$ плоскостей пересекающих V_2 нетривиально, т.е. не по $\{\bar{0}\}$. (Отметим, что $18 + 16 + 1 = 35$!)

5) **Творческий вопрос.** Представить графически 15 "прямых"и 35 "плоскостей"пространства $\mathbb{F}_2^4$.

Теорема 3. 1) *m-мерное подпространство V_m имеет ровно*

$$B_m = (2^m - 1)(2^m - 2)(2^m - 2^2) \cdot \ldots \cdot (2^m - 2^{m-1})$$

различных базисов.

2) *Бинарное n-мерное пространство $\mathbb{F}_2^n$ имеет ровно*

$$B_n^k = \frac{(2^n - 1)(2^n - 2) \cdot \ldots \cdot (2^n - 2^{k-1})}{(2^k - 1)(2^k - 2) \cdot \ldots \cdot (2^k - 2^{k-1})}$$

различных подпространств размерности k для $k > 0$.

Доказательство. 1) Воспользуемся алгоритмом из док-ва Теоремы 1 (см. Следствие 1 из этой теоремы). За первый элемент базиса возьмем произвольный ненулевой элемент $u_1 \neq \bar{0}$ в V_m. Имеется $2^m - 1$ таких элементов. В качестве u_2 возьмем любой вектор, не принадлежащий подпространству $\langle u_1 \rangle = \{a_1 u_1, a_1 \in \mathbb{F}_2\}$, порожденному выбранным вектором u_1. Имеем $2^m - 2$ таких элементов. За u_3 возьмем любой элемент, не принадлежащий подпространству $\langle u_1, u_2 \rangle = \{a_1 u_1 + a_2 u_2, a_1, a_2 \in \mathbb{F}_2\}$. Имеется $2^m - 2^2$ таких векторов. Продолжим подобным образом до выбора последнего вектора базиса

$$u_m \in V_m \setminus \langle u_1, \ldots, u_{m-1} \rangle = V_m \setminus \{a_1 u_1 + \ldots + a_{n-1} u_{n-1}, a_i \in \mathbb{F}_2\}.$$

Следовательно, вектор u_m можно выбрать $2^m - 2^{m-1}$ различными способами. В итоге, получаем формулу для числа различных базисов m-мерного подпространства V_m.

2) Любое подпространство V_k размерности k задается каким-то своим базисом $(u_1, \ldots, u_k)$.

$$\begin{aligned}
u_1 &\in \mathbb{F}_2^n \setminus \{\bar{0}\} \quad (2^n - 1 \text{ вариантов}),\\
u_2 &\in \mathbb{F}_2^n \setminus \langle u_1 \rangle \quad (2^n - 2^1 \text{ вариантов}),\\
u_3 &\in \mathbb{F}_2^n \setminus \langle u_1, u_2 \rangle \quad (2^n - 2^2 \text{ вариантов}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
u_k &\in \mathbb{F}_2^n \setminus \langle u_1, u_2, \ldots, u_{m-1} \rangle \quad (2^n - 2^{k-1} \text{ вариантов}).
\end{aligned}$$

Это дает число выборов базиса подпространства V_k и совпадает с числителем формулы для B_n^k. Но любое подпространство размерности k имеет B_k базисов. Это число стоит в знаменателе формулы для B_n^k.

□

Следствие. *Число гиперплоскостей равно числу прямых в* $\mathbb{F}_2^n$:

$$B_n^1 = B_n^{n-1} = 2^{n-1}.$$

Доказательство.

$$\begin{aligned}
B_n^{n-1} &= \frac{(2^n - 1)}{1} \frac{(2^n - 2)(2^n - 2^2) \ldots (2^n - 2^{n-2})}{(2^{n-1} - 1)(2^{n-1} - 2) \ldots (2^{n-1} - 2^{n-3})} \frac{1}{(2^{n-1} - 2^{n-2})}\\
&= (2^n - 1) \frac{2^{n-2}}{2^{n-2}} = 2^n - 1.
\end{aligned}$$

□

В следующей лекции увидим, что последнее равенство отражает важные структурные взаимосвязи между линейными подпространствами и линейными уравнениями. В частности, мы докажем, что *любая гиперплоскость в* $\mathbb{F}_2^n$ *задается ровно одним ненулевым линейным уравнением.* Это ключевой результат Лекции 3.

ЛЕКЦИЯ 3. Линейные подпространства и системы линейных уравнений.

`Основные результаты Лекции 3.`

1) *Любая гиперплоскость в $\mathbb{F}_2^n$, т.е. подпространство размерности $n-1$, задается ровно одним ненулевым линейным уравнением.* Для доказательства требуется применить один шаг метода Гаусса для двух уравнений, чтобы найти число элементов пересечения двух гиперплоскостей.

2) Из 1) следует существование двойственного базиса!

3) Из 2) получаем, что любое подпространство V_k в $\mathbb{F}_2^n$ размерности k совпадает со множеством решений некоторой системы из $n-k$ линейных уравнений.

Вопрос: *Как можно задать линейное подпространство V в $\mathbb{F}_2^n$?*

В Лекции 1 мы показали, что V можно задать некоторым базисом $(u_1, \ldots, u_k)$

$$V = \langle u_1, \ldots, u_k \rangle = \{v = a_1u_1 + \ldots + a_ku_k,\ a_i \in \mathbb{F}_2\}, \quad |V| = 2^k$$

Все линейные комбинации $a_1u_1 + \ldots + a_ku_k$ попарно различные и дают нам все элементы подпространства V. Различных базисов у V достаточно много (см. Теорему 2). Для задания гиперплоскости в $\mathbb{F}_2^n$, т.е. подпространства размерности $n-1$, надо найти $n-1$ линейно независимых векторов. Сейчас мы рассмотрим другой способ задания подпространств *линейными уравнениями.*

Теорема 4. *Любая гиперповерхность в $\mathbb{F}_2^n$ может быть задана ровно одним линейным уравнением. Точнее, пусть $V_{n-1} \subset \mathbb{F}_2^n$ произвольное линейное подпространство размерности $n-1$. Тогда существует (единственный) ненулевой вектор $\bar{a} = (a_1, \ldots, a_n)$ в F_2^n такой, что*

$$V_{n-1} = H_{\bar{a}} = \{v = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n \,|\, a_1x_1 + \ldots + a_nx_n = 0\}.$$

Предложение 3.1. *Возьмем произвольный ненулевой вектор $\bar{a} = (a_1, \ldots, a_n)$ в $\mathbb{F}_2^n$. Тогда множество решений $H_{\bar{a}}$ является гиперплоскостью в $\mathbb{F}_2^n$, т.е. линейным подпространством $\mathbb{F}_2^n$ размерности $n-1$.*

Доказательство. Введем спаривание

$$(\cdot, \cdot) : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2,$$

т.е. отображение упорядоченных пар векторов из $\mathbb{F}_2^n$ в $\mathbb{F}_2$. Для любых $u = (a_1, \ldots, a_n)$ и $v = (b_1, \ldots, b_n)$ в $\mathbb{F}_2^n$ положим

$$(u, v) = a_1b_1 + \cdots + a_nb_n.$$

Это спаривание симметрично и линейно по каждому аргументу:

$$(u, v) = (v, u), \qquad (u_1 + u_2, v) = (u_1, v) + (u_2, v).$$

Говорят, что это спаривание является симметричной билинейной формой.

Множество

$$H_{\bar{a}} = \{v \in \mathbb{F}_2^n \mid (\bar{a}, v) = 0\}$$

непусто ($\bar{0} \in H_{\bar{a}}$) и замкнуто относительно сложения векторов. Если $(\bar{a}, u) = 0$ и $(\bar{a}, v) = 0$, то $(\bar{a}, u + v) = (\bar{a}, u) + (\bar{a}, v) = 0$ и $u + v \in H_{\bar{a}}$. Следовательно, $H_{\bar{a}}$ подпространство.

Найдем его размерность. Пусть a_k первая ненулевая координата вектора $\bar{a} = (0, \ldots, 0, a_k, \ldots a_n)$, $a_k \neq 0$, т.е. $a_k = 1$. Будем называть этот элемент **осью** (или **осевым элементом**) вектора $\bar{a}$. Тогда координаты x_i любого вектора $v = (x_1, \ldots, x_n) \in H_{\bar{a}}$ могут быть описаны следующим образом. Мы полагаем все $x_i \in \mathbb{F}_2$ для $i \neq k$ произвольными, а координату x_k находим однозначно из уравнения $(\bar{a}, v) = 0$. Точнее, $x_k = a_{k+1}x_{k+1} + \ldots + a_n x_n$. Получаем, что любой элемент $v \in H_{\bar{a}}$ записывается в виде

$$v = (x_1, \ldots, x_{k-1}, (a_{k+1}x_{k+1} + \ldots + a_n x_n), x_{k+1}, \ldots, x_n).$$

Следовательно, $H_{\bar{a}}$ содержит ровно 2^{n-1} векторов, т.е. $\dim H_{\bar{a}} = n - 1$.

□

Вопрос. Найти базис линейного подпространства $H_{\bar{a}}$.

Для нахождения базиса в $H_{\bar{a}}$ мы можем использовать стандартный базис $(e_1, \ldots, e_n)$ пространства $\mathbb{F}_2^n$ (см. Лекцию 1). Тогда произвольный вектор $v \in H_{\bar{a}}$ запишется как линейная комбинация

$$v = x_1 e_1 + \cdots + x_{k-1}e_{k-1} + (a_{k+1}x_{k+1} + \ldots + a_n x_n)e_k + \\ x_{k+1}e_{k+1} + \ldots + x_n e_n$$

или

$$v = x_1 e_1 + \cdots + x_{k-1}e_{k-1} + x_{k+1}(e_{k+1} + a_{k+1}e_k) + \ldots + x_n(e_n + a_n e_k).$$

Отметим, что

$$e_1, \ldots, e_{k-1},\ e_{k+1} + a_{k+1}e_k, \ldots,\ e_n + a_n e_k$$

линейно независимые. (Проверьте!) Это и есть один из базисов $H_{\bar{a}}$.

□

Предложение 3.2. *Для двух различных ненулевых векторов $\bar{a} = (a_1, \ldots, a_n)$ и $\bar{b} = (b_1, \ldots, b_n)$ пересечение гиперплоскостей $H_{\bar{a}} \cap H_{\bar{b}}$ есть подпространство размерности $n - 2$. В частности, гиперплоскости $H_{\bar{a}}$ и $H_{\bar{b}}$ различные.*

Доказательство. 1) $H_{\bar{a}} \cap H_{\bar{b}}$ подпространство, как пересечение двух подпространств.

2) Пересечение гиперплоскостей совпадает со множеством решений системы уравнений

$$\begin{cases} (\bar{a}, v) & = 0, \\ (\bar{b}, v) & = 0. \end{cases}$$

Заметим, что **заменяя второе уравнение на сумму первых двух, мы получаем систему эквивалентную исходной**. Действительно

$$\begin{cases} (\bar{a}, v) & = 0 \\ (\bar{b}, v) & = 0 \end{cases} \Rightarrow \begin{cases} (\bar{a}, v) & = 0 \\ (\bar{b} + \bar{a}, v) & = 0 \end{cases} \Rightarrow \begin{cases} (\bar{a}, v) & = 0 \\ ((\bar{b} + \bar{a}) + \bar{a}, v) & = 0 \end{cases} \Rightarrow \begin{cases} (\bar{a}, v) & = 0 \\ (\bar{b}, v) & = 0. \end{cases}$$

Пусть a_k и b_l осевые элементы векторов $\bar{a}$ и $\bar{b}$. Иными словами это первые ненулевые координаты векторов. Переставляя уравнения, можно добиться того, что $l \geq k$. Если $l > k$, то система уже имеет ступенчатый вид (см. ниже). Если $k = l$, то

$$(S) = \begin{cases} a_k x_k + \ldots + a_n x_n & = 0 \\ b_k x_k + \ldots + b_n x_n & = 0, \end{cases}$$

где $a_k \neq 0$ и $b_k \neq 0$ (т.е. $a_k = b_k = 1$). Заменяем второе уравнение на линейную комбинацию двух уравнений

$$(b_k + a_k)x_k + \ldots + (b_n + a_n)x_n = 0,$$

где полагаем $c_i = b_i + a_i$. Тогда $c_k = 0$ и найдется $c_m = a_m + b_m \neq 0$ с некоторым $m > k$, так как векторы $\bar{a}$ и $\bar{b}$ различные. Следовательно, мы доказали, что система двух линейных уравнений (S) эквивалентно системе уравнений, имеющей **ступенчатый вид**

$$(S) \Leftrightarrow (S') = \begin{cases} a_k x_k + \ldots\ldots\ldots\ldots + a_n x_n & = 0 \\ c_m x_m + \ldots + c_n x_n & = 0, \end{cases}$$

где $a_k \neq 0$, $b_m \neq 0$ и $k < m$. Такую системы уже легко решить! Возьмем произвольные $x_i \in \mathbb{F}_2^n$ для $i \neq k$ и $i \neq m$ ($n - 2$ переменных). Найдем x_m из второго уравнения, а x_k из первого. Следовательно, система уравнений имеет ровно 2^{n-2} решений и

$$|H_{\bar{a}} \cap H_{\bar{b}}| = 2^{n-2}.$$

□

Замечание. Преобразование системы уравнений, сделанное выше, является основным шагом в **методе Гаусса** решения систем линейных уравнений.

Доказательство Теоремы 4. Мы доказали, что $2^n - 1$ ненулевых векторов $\bar{a}$ в $\mathbb{F}_2^n$ определяют $2^n - 1$ попарно различных гиперплоскостей в

$\mathbb{F}_2^n$. Но число различных гиперплоскостей равно $2^n - 1$. Следовательно мы нашли все гиперплоскости!

Следствием этой теоремы является следующий важный результат.

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

$$(u_i, u_j^*) = \begin{cases} 1 & i = j, \\ 0 & i \neq j. \end{cases}$$

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

Доказательство. Зафиксируем индекс $1 \leq i \leq n$ и рассмотрим гиперплоскость $H_i = \langle u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n \rangle$. Эта гиперплоскость задается одним уравнением в силу Теоремы 2. Следовательно, существует ненулевой вектор $u_i^* \in \mathbb{F}_2^n$ такой, что $H_i = H_{u_i^*}$. Следовательно $\forall\, v \in H_i$: $(v, u_i^*) = 0$. В частности, $(u_j, u_i^*) = 0$ для всех $j \neq i$.

Если бы выполнялось равенство $(u_i, u_i^*) = 0$, тогда гиперплоскость $H_{u_i^*}$ содержала бы все пространство $\langle u_1, \ldots, u_n \rangle = \mathbb{F}_2^n$, что противоречит тому, что $\dim H_i = n - 1$. Следовательно, $(u_i, u_i^*) = 1$.

Таким образом мы построим u_1^*, u_2^*, $\ldots$, u_n^*. Докажем, что они линейно независимы.

Предположим, что $a_1 u_1^* + \ldots + a_n u_n^* = \bar{0}$. Тогда для любого $1 \leq i \leq n$ получаем $0 = (a_1 u_1^* + \ldots + a_n u_n^*, u_i) = a_i$. Для завершения доказательства отметим, что любые n линейно независимых векторов в $\mathbb{F}_2^n$ образуют базис этого пространства.

□

Замечание. *Важное свойство двойственного базиса.* Двойственный базис позволяет находить координаты вектора в базисе $(u_1, \ldots, u_n)$ через спаривание векторов. Пусть

$$v = a_1 u_1 + \ldots a_n u_n.$$

Тогда $(v, u_i^*) = (a_1 u_1 + \ldots a_n u_n, u_i^*) = a_i$.

Теперь мы можем обобщить Теорему 4. (*Будет доказано в Лекции 4.*)

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 уравнений.*

Доказательство. Пусть $(u_1, \ldots, u_k)$ какой-нибудь базис подпространства V_k. Дополним его до базиса $(u_1, \ldots, u_k, u_{k+1}, \ldots, u_n)$ пространства $\mathbb{F}_2^n$ (см. Следствие 2 Темы 1). Рассмотрим двойственный к нему базис $(u_1^*, \ldots, u_k^*, u_{k+1}^*, \ldots, u_n^*)$. Заметим, что для любого $v = x_1 u_1 + \ldots x_n u_n \in \mathbb{F}_2^n$ имеем $(v, u_i^*) = x_i$. Получаем

$$V_k = \{x_1 u_1 + \ldots x_k u_k \,|\, x_i \in \mathbb{F}_2\} = \{v \in \mathbb{F}_2^n \,|\, (v, u_{k+1}^*) = \cdots = (v, u_n^*) = 0\}.$$

Следовательно, V_k совпадает со множеством решений системы $n-k$ однородных линейных уравнений.