КУРС АЛГЕБРЫ-1 в НИУ ВШЭ (осень 2017)

Валерий Алексеевич Гриценко

ЛЕКЦИЯ 1. Линейные подпространства в $\mathbb{F}_2^n$.

`Основные результаты Лекции 1.`

Каждое подпространство F_2^n содержит 2^k векторов, где $0 \le k \le n$. Доказательство этой теоремы дает алгоритм построения базиса подпространства, алгоритм расширения базиса подпространства до базиса всего пространства (и формулу для $\dim(V+U)$, доказанную в Лекции 2).

1) Метод удвоения пространства: $V' = V \cup (u+V)$ (Предложение 1.3).

2) Алгоритм построения базиса.

3) Конечная плоскость Фано, т.е. "граф" $\mathbb{P}(\mathbb{F}_2^3)$.

Введение: поле $\mathbb{F}_2$ из двух элементов и векторное пространство $\mathbb{F}_2^n$ бинарных векторов длины n.

1) Рассмотрим поле $\mathbb{F}_2 = \{0, 1\}$ со следующими операциями сложения $+$ и умножения $\cdot$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Отметим, что $\forall\, b \in \mathbb{F}_2$ имеем $b+b=0$, поэтому $b = -b$ в $\mathbb{F}_2$. В поле $\mathbb{F}_2$ можно решать уравнения $ax + b = c$, как и в поле рациональных чисел $\mathbb{Q}$. Например, $x + b = c \Leftrightarrow x = c + b$.

2) Для любого $n \ge 1$ определим множество бинарных векторов длины n

$$\mathbb{F}_2^n = \{(a_1, a_2, \dots, a_n) \,|\, a_i \in \mathbb{F}_2\},$$

содержащее 2^n элементов.

3) В $\mathbb{F}_2^n$ есть операция $+$, обладающая обычными свойствами сложения. Для любых $u, v, w \in \mathbb{F}_2$ и нулевого вектора $\bar{0} = (0, 0, \dots, 0)$ имеем

$$u + v = v + u, \quad (u + v) + w = u + (v + w), \quad u + \bar{0} = u.$$

У каждого бинарного вектора v есть обратный относительно сложения векторов $v + v = \bar{0}$, т.е. $-v = v$ для любого бинарного вектора $v \in \mathbb{F}_2^n$.

Векторные уравнения: как найти решение уравнения $v + \bar{x} = u$?

$$v + \bar{x} = u \Leftrightarrow \bar{x} = u - v = u + v.$$

В $\mathbb{F}_2^n$ есть вторая операция – *умножение векторов на элементы из* $\mathbb{F}_2$. По определению, полагаем $1 \cdot v = v$ и $0 \cdot v = \bar{0}$. Эта операция удовлетворяет обычным свойствам линейности

$$a \cdot (u + v) = a \cdot u + a \cdot v, \quad (a + b) \cdot v = a \cdot v + b \cdot v, \quad a \cdot (b \cdot v) = (ab) \cdot v.$$

Определение 1. *Непустое подмножество $V \subset \mathbb{F}_2^n$ называется линейным подпространством в $\mathbb{F}_2^n$, если $\forall\, u, v \in V:\ u+v \in V$.* (Линейное подпространство — это ненулевое подмножество в $\mathbb{F}_2^n$ замкнутое относительно операции $+$ (и умножения на элементы поля $\mathbb{F}_2$).)

Свойства: 1) нулевой вектор $\bar{0} \in V$ лежит в любом подпространстве. ($\exists\, u \in V$, тогда $u + u = \bar{0} \in V$).

2) $\{\bar{0}\}$ и $\mathbb{F}_2^n$ – подпространства в $\mathbb{F}_2^n$.

3) Для любого ненулевого вектора $u \in \mathbb{F}_2^n$ множество $V_1 = \{\bar{0}, u\} = \{0 \cdot u,\ 1 \cdot u\} = \{au, a \in \mathbb{F}_2\}$ является линейным подпространством.

4) Пусть u и w два `различных ненулевых` вектора в $\mathbb{F}_2^n$, тогда $V_2 = \{\bar{0}, u, w, u+w\}$ является линейный подпространством. Отметим, что $u \neq (u+w)$ и $w \neq (u+w)$. Множество замкнуто относительно сложения, так как $u + (u+w) = w$ и $w + (u+w) = u$. Другая форма записи этого подпространства:

$$V_2 = \{\, \bar{0} = 0 \cdot u + 0 \cdot w,\ u = 1 \cdot u + 0 \cdot w,\ w = 0 \cdot u + 1 \cdot w, u + w = 1 \cdot u + 1 \cdot w\}$$
$$= \{au + bw,\ a, b \in \mathbb{F}_2\}.$$

5) *Первое обобщение предыдущего свойства.*

Предложение 1.1 *Пусть $\{u_1, \ldots, u_m\}$ произвольный набор векторов из $\mathbb{F}_2^n$. Тогда множество всех их* **линейных комбинаций** $a_1u_1 + \cdots + a_mu_m$ *с коэффициентами в $\mathbb{F}_2$*

$$V = \langle u_1, \ldots, u_m\rangle_{\mathbb{F}_2} = \langle u_1, \ldots, u_m\rangle = \{\, a_1u_1 + \cdots + a_mu_m, a_i \in \mathbb{F}_2\}$$

является линейным подпространством в $\mathbb{F}_2^n$. В этом случае говорят, что подпространство V **порождается** векторами $u_1, \ldots, u_m$, или что V является **линейной оболочкой** векторов $(u_1, \ldots, u_m)$. Векторы $(u_1, \ldots, u_m)$ называется **образующими** подпространства V.

Доказательство. Надо показать, что $\langle u_1, \ldots, u_m\rangle$ замкнуто относительно сложения. Сумма двух линейных комбинаций есть линейная комбинация

$$(a_1u_1 + \ldots + a_mu_m) + (b_1u_1 + \ldots + b_mu_m) = (a_1 + b_1)u_1 + \ldots + (a_m + b_m)u_m.$$

□

Отметим, что линейные комбинации не обязаны быть попарно различными! Пусть есть две *различные* линейные комбинации, которые дают один и то же результат

$$a_1u_1 + \ldots + a_mu_m = b_1u_1 + \ldots + b_mu_m \quad \text{и} \quad \exists\, i\ :\ a_i \neq b_i.$$

Тогда мы имеем нетривиальное представление нулевого вектора $\bar{0}$ в виде линейной комбинации исходных векторов

$$(a_1 - b_1)u_1 + \ldots + (a_m - b_m)u_m = \bar{0} \quad \exists\ i\ :\ a_i - b_i \neq 0.$$

(Напомним, что $b_i = -b_i$.) В таком случае вектора $(u_1, \ldots, u_m)$ называются **линейно зависимыми**.

Вектора $(u_1, \ldots, u_m)$ называются **линейно независимыми**, если равенство

$$c_1 u_1 + \ldots + c_m u_m = \bar{0}$$

влечет $c_1 = c_2 = \cdots = c_m = 0$. Рассуждения, приведенные выше дают нам следующее утверждение

Предложение 1.2. *Если вектора $(u_1, \ldots, u_m)$ линейно независимы, то все их различные линейные комбинации определяют попарно различные вектора. Иначе говоря, все элементы в линейно оболочке*

$$V = \{a_1 u_1 + \ldots + a_m u_m \,|\, a_i \in \mathbb{F}_2\}$$

попарно различные и $|V| = 2^m$. В этом случае говорят, что упорядоченный набор векторов $(u_1, \ldots, u_m)$ является **базисом** *подпространства V, а $m = \log_2 |V|$ называется размерностью подпространства V. Коэффициенты $(a_1, \ldots, a_k)$ называются* **координатами вектора v в базисе** $(u_1, \ldots, u_k)$.

Замечание. Базис $(u_1, \ldots, u_m)$ это *упорядоченная* последовательность векторов!

ПРИМЕРЫ 1.1 – 1.3.

1) **Канонический базис** $\mathbb{F}_2^n$. Положим $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{F}_2^n$ $(1 \le i \le n)$ с единицей на i-том месте. Тогда n векторов $(e_1, e_2, \ldots, e_n)$ составляют базис пространства $\mathbb{F}_2^n$, который называют `стандартным` или `каноническим`. В частности,

$$a_1 e_1 + \cdots + a_n e_n = (a_1, \ldots, a_n) \in \mathbb{F}_2^n.$$

2) **Число базисов плоскости в $\mathbb{F}_2^n$.** Будем называть двумерное подпространство **плоскостью**. Любая плоскость $V_2 = \langle u, v \rangle = \{\bar{0}, u, v, u+v\}$ порождена двумя различными ненулевыми элементами u, v. Все три ненулевые вектора $\{u, v, u+v\}$ совершенно равноправны. Например, любой из них равен сумме двух других. (Проверьте!) За базис мы можем выбрать любую пару ненулевых векторов. Следовательно, любая плоскость в $\mathbb{F}_2^n$ имеет 6 различных базисов

$$(u, v),\ (v, u),\ (u, u+v),\ (u+v, u),\ (v, u+v),\ (u+v, v).$$

3) **Базис тривиального подпространства.** Является ли система из одного нулевого вектора линейно независимой?

Нет. Из равенства $a \cdot \bar{0} = \bar{0}$ не следует, что $a = 0$, так как $1 \cdot \bar{0} = \bar{0}$. Следовательно, *тривиальное подпространство $\{\bar{0}\}$ не имеет базиса.* Иначе говоря, его базис содержит 0 элементов, $\dim\{\bar{0}\} = 0$ и $|\{\bar{0}\}| = 2^0 = 1$.

В следующем предложении мы дадим другое содержательное обобщение свойств 3) и 4).

Предложение 1.3. (**Метод удвоения линейного подпространства**). *Пусть даны линейное подпространство $V \subset \mathbb{F}_2^n$ и вектор $u \notin V$, не принадлежащий ему. Положим $V + u = \{v + u, v \in V\}$. Тогда объединение множеств $V \cup (V + u)$ является линейным подпространством, содержащим $2|V|$ элементов.*

Доказательство. Проверим, что множество $V \cup (V + u)$ замкнуто относительно сложения векторов. $\forall\, v_1, v_2 \in V : v_1 + v_2 \in V$, $v_1 + (v_2 + u) = (v_1 + v_2) + u \in u + V$, $(v_1 + u) + (v_2 + u) = v_1 + v_2 \in V$.

Почему объединение содержит $2|V|$ элементов? Если $v_1 + u = v_2 + u$, то добавляя u справа, получаем $(v_1 + u) + u = (v_2 + u) + u$ или $v_1 = v_2$. Если $v_1 = v_2 + u$, то $v_1 + v_2 = (v_2 + u) + v_2 = u + (v_2 + v_2) = u + \bar{0} = u \in V$, что противоречит выбору u.

□

Теорема 1. *Любое линейное подпространство V в $\mathbb{F}_2^n$ содержит ровно 2^k векторов, где $0 \leq k \leq n$.*

Доказательство. Если $V = \{\bar{0}\}$, то $|V| = 1 = 2^0$. Пусть $V \neq \{\bar{0}\}$. Тогда существует ненулевой u_1 в V. В силу 3)

$$V_1 = \{\bar{0}, u_1\} = \{a_1 u_1,\ a_1 \in \mathbb{F}_2\} = \langle u_1 \rangle \subset V$$

является подпространством в V. Если $V = V_1$, то $|V| = 2$. Если $\{\bar{0}, u_1\} \neq V$, то существует $u_2 \in V$ такой, что $u_2 \notin V_1 = \{\bar{0}, u_1\}$. Тогда

$$\begin{aligned} V_2 = V_1 \cup (V_1 + u_2) &= \{au_1 \,|\, a \in \mathbb{F}_2\} \cup (\{au_1 \,|\, a \in \mathbb{F}_2\} + u_2) \\ &= \{a_1 u_1 + a_2 u_2 \,|\, a_1, a_2 \in \mathbb{F}_2\} = \langle u_1, u_2 \rangle \subset V \end{aligned}$$

является линейным подпространством в силу 4) или в силу Предложения 2.

Если $V = V_2$, то $|V| = 2^2$. Если $V \neq V_2$, то существует $u_3 \in V \setminus V_2$. Тогда в силу Предложения 2, V содержит подпространство $V_3 = V_2 \cup (V_2 + u_3)$, имеющее 2^3 элементов. Более того

$$\begin{aligned} V_3 = V_2 \cup (V_2 + u_2) &= \{au_1 + a_2 u_2 \,|\, a \in \mathbb{F}_2\} \cup (\{au_1 + a_2 u_2 \,|\, a \in \mathbb{F}_2\} + u_3) \\ &= \{a_1 u_1 + a_2 u_2 + a_3 u_3 \,|\, a_1, a_2, a_3 \in \mathbb{F}_2\} = \langle u_1, u_2, u_3 \rangle \subset V. \end{aligned}$$

Продолжим этот процесс, который оборвется на итерации с номером k, где $0 \leq k \leq n$:

$$\begin{aligned} V = V_{k-1} \cup (V_{k-1} + u_k) &= \langle u_1, \ldots, u_{k-1} \rangle \cup (\langle u_1, \ldots, u_{k-1} \rangle + u_k) \\ &= \langle u_1, \ldots, u_{k-1}, u_k \rangle. \end{aligned}$$

Получаем, что $|V| = 2|V_{k-1}| = 2 \cdot 2^{k-1} = 2^k$.

□

Следствие 1. (**Существование базиса.**) *Мы доказали выше, что в любом ненулевом (!) подпространстве $V \subset \mathbb{F}_2^n$ существует базис и что V совпадает со множеством всех 2^k* **попарно различных** *линейных комбинаций базисных векторов $\{a_1u_1 + \cdots + a_ku_k,\ a_1, \ldots, a_k \in \mathbb{F}_2\}$.*

Доказательство. В доказательстве Теоремы 1 мы описали **алгоритм построения некоторого базиса** произвольного подпространства $V \subset \mathbb{F}_2^n$. Мы последовательно выбираем вектора, которые дают нам "башню" (или "флаг") строго вложенных друг в друга подпространств

$$\{\bar{0}\} \subsetneq \langle u_1\rangle \subsetneq \langle u_1, u_2\rangle \subsetneq \langle u_1, u_2, u_3\rangle \subsetneq \ldots \subsetneq \langle u_1, \ldots, u_k\rangle = V_k.$$

На каждом этапе мы выбираем вектор $u_j \notin \langle u_1, \ldots, u_{j-1}\rangle$.

□

Этот алгоритм дает второе важное Следствие 2.

Следствие 2. (**О расширении базиса подпространства до базиса $\mathbb{F}_2^n$.**) *Любой базис $(u_1, u_2, \ldots, u_k)$ k-мерного подпространства V_k в $\mathbb{F}_2^n$ может быть расширен некоторыми векторами $(u_{k+1}, \ldots, u_n)$ до базиса всего пространства $\mathbb{F}_2^n$.*

Доказательство. Если $V_k \neq \mathbb{F}_2^n$, то возьмем произвольный вектор $u_{k+1} \in \mathbb{F}_2^n \setminus V_k$. Как и в доказательстве Теоремы 1 получим подпространство $V_{k+1} = V_k \cup (V_k + u_{k+1})$ размерности $k+1$. Затем выберем $u_{k+2} \in \mathbb{F}_2^n \setminus V_{k+1}$ и т.д.

□

ПРИМЕР 1.4

Ненулевые линейные подпространства в $\mathbb{F}_2^3$ или конечная проективная плоскость Фано.

1) Каждая плоскость $U = \langle u, v\rangle = \{\bar{0}, u, v, u+v\}$ содержит ровно **три** прямых $\langle u\rangle$, $\langle v\rangle$, $\langle u+v\rangle$, т.е. подпространств размерности 1.

2) Трехмерное пространство $\mathbb{F}_2^3$ имеет $2^3 - 1$ одномерных подпространств, т.е. прямых $\langle u\rangle = \{\bar{0}, u\}$, $u \in \mathbb{F}_2^3$. Сосчитаем количество плоскостей в $\mathbb{F}_2^3$. Два различных ненулевых вектора (u, v) в $\mathbb{F}_2^3$ можно выбрать $(2^3 - 1)(2^3 - 2)$ различными способами. Каждая плоскость будет сосчитана 6 раз, т.к. она обладает 6 базисами. Следовательно имеется $(7 \cdot 6)/6 = 7$ различных плоскостей. Отметим, что число плоскостей в $\mathbb{F}_2^3$ совпадает с числом прямых.

3) Докажем, что любые две плоскости в $\mathbb{F}_2^3$ пересекаются по некоторой прямой. Для этого мы используем свойство линейности. Предположим, что две плоскости пересекаются только по нулевому вектору $U, V \subset \mathbb{F}_2^3$ и $U \cap V = \{\bar{0}\}$. Рассмотрим базисы $U = \langle u_1, u_2\rangle$ и $V = \langle v_1, v_2\rangle$. Тогда $U \cup V$ содержит по крайней мере 7 попарно различных элементов

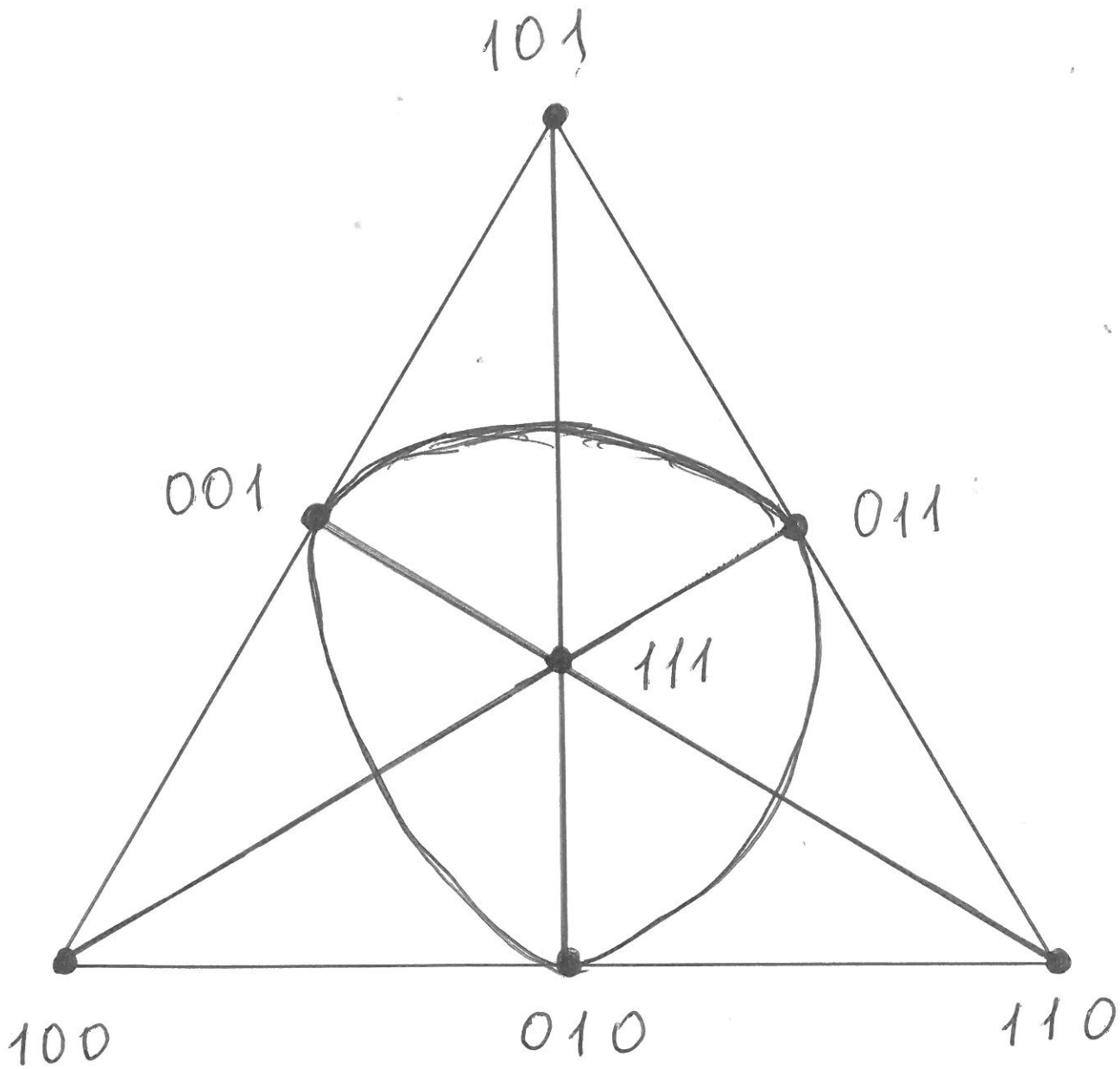
$$\{\bar{0}, u_1, u_2, u_1 + u_2, v_1, v_2, v_1 + v_2\} \subset U \cup V \subset \mathbb{F}_2^3.$$

Построим новые элементы в $\mathbb{F}_2^3$. Например, два различных элемента $u_1 + v_1 \neq u_1 + v_2$ из $\mathbb{F}_2^3$ не лежат в $U \cup V$. Если $u_1 + v_1 \in U$, то $v_1 \in U$?! Если $u_1 + v_1 \in V$, то $u_1 \in V$?! Следовательно, мы получили 9 различных элементов в $\mathbb{F}_2^3$?!

4) Если две плоскости пересекаются по двум ненулевым векторам, то они совпадают. (См. замечание о ненулевых векторах в Примере 1.2). Следовательно, любые две плоскости пересекаются ровно по одной прямой.

5) Докажем, что через каждую прямую проходят ровно три плоскости. Надо дополнить базис $\langle u \rangle$ до базиса плоскости $\langle u, v \rangle$. Для v имеется $2^3 - 2 = 6$ вариантов. Но $\langle u, v \rangle = \langle u, v + u \rangle$. Следовательно, через каждую прямую проходят ровно **три** плоскости.

6) Дадим условный рисунок прямых и плоскостей в $\mathbb{F}_2^3$. Вектор $\bar{0}$ лежит в каждой прямой и плоскости, поэтому мы его не изображаем. Прямая без нулевого вектора $\{u\} = \langle u \rangle \setminus \{\bar{0}\}$ называется `проективной точкой`, а плоскость без нулевого вектора $\{u, v, u + v\} = \langle u, v \rangle \setminus \{\bar{0}\}$ называется `проективной прямой`.


101
001
011
111
100
010
110