Линейные пространства над конечным полем

5 января 2023 г. 1:32

Конечные поля

Конечное множество X называется *конечным полем* (или полем Галуа) если имеют место следующие свойства:

- На множестве определены операции сложения и умножения, результат этих операций принадлежит множеству.
- Для любых элементов $x_i, x_j, x_k \in X$ выполняются следующие равенства:

$$(x_i + x_j) + x_k = x_i + (x_k + x_j),$$
$$(x_i \cdot x_j) \cdot x_k = x_i \cdot (x_k \cdot x_j),$$
$$x_i + x_j = x_j + x_i,$$
$$x_i \cdot x_j = x_j \cdot x_i,$$
$$(x_i + x_j) \cdot x_k = x_i \cdot x_k + x_j \cdot x_k.$$

- Существует нулевой элемент для сложения $x_0 \in X$ и единичный элемент для умножения $x_1 \in X$:

$$x_i + x_0 = x_0 + x_i = x_i,$$
$$x_i \cdot x_1 = x_1 \cdot x_i = x_i.$$

- Для каждого элемента $x_i \in X$ существует единственный элемент $x_j \in X$, обратный для сложения

$$x_i + x_j = 0,$$

- Для каждого элемента $x_i \in X$, кроме x_0, существует единственный элемент $x_j \in X$, обратный для умножения

$$x_i \cdot x_j = 1.$$

В литературе, конечное поле обозначается как $GF(q)$, где q – число элементов в поле.

Пример

Рассмотрим конечное поле $GF(5) = \{0, 1, 2, 3, 4\}$, которое включает в себя все вычеты по модулю 5. Здесь $x_0 = 0$, $x_1 = 1$.

Таблица: Таблица сложения (слева) и умножения (справа) в поле $GF(5)$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Пусть X – конечное поле и $\mathbf{x} = (x_1, x_2, ..., x_n) \in X^n$ – вектор, каждая компонента которого принадлежит X. Тогда *сумма векторов* $\mathbf{x} \in X^n$ and $\mathbf{y} \in X^n$ определяется как

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n). \quad (1)$$

Если $c \in X$, тогда умножение вектора $\mathbf{x}$ на скаляр c определяется как

$$c \cdot \mathbf{x} = (c \cdot x_1, c \cdot x_2, ..., c \cdot x_n). \quad (2)$$

Пример. Рассмотрим два вектора $\mathbf{x} = (1, 2, 3, 4)$ и $\mathbf{y} = (4, 2, 3, 1)$, каждый элемент которого принадлежит $GF(5)$. Тогда $\mathbf{x} + \mathbf{y} = (0, 4, 1, 0)$. Пусть $c = 2$, тогда $c \cdot \mathbf{x} = (2, 4, 1, 3)$.

Линейные пространства над конечным полем

Множество векторов $\mathbf{V}$ формируют *линейное пространство*, если это множество является замкнутым по отношению к операциям сложения и умножения на скаляр. Это означает, что для любого $k = \{1, 2, 3, ...\}$, вектор

$$\mathbf{z} = \sum_{i=1}^{k} c_i \cdot \mathbf{x}_i \quad (3)$$

принадлежит $\mathbf{V}$ для любого $c_i \in X$ и $\mathbf{x}_i \in X^n$. Правая часть (3) называется *линейной комбинацией* векторов $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k$.

Пример. Рассмотрим два множества векторов V_1 и V_2 над полем $GF(2) = \{0, 1\}$.

$$\mathbf{V}_1 = \left\{ \begin{array}{c} 000 \\ 110 \\ 011 \\ 101 \end{array} \right\}, \mathbf{V}_2 = \left\{ \begin{array}{c} 000 \\ 100 \\ 010 \\ 001 \end{array} \right\}.$$

Множество $\mathbf{V}_1$ является линейным пространством, потому что сумма любой пары векторов из $\mathbf{V}_1$ принадлежит $\mathbf{V}_1$. Множество $\mathbf{V}_2$ не является линейным пространством.

Подмножество линейного пространства, для которого выполняются все

Подмножество линейного пространства, для которого выполняются все свойства линейного пространства, называется *линейным подпространством.*

Пример. Рассмотрим два множества векторов V_1 и V_2 в поле $GF(2) = \{0, 1\}$.

$$\mathbf{V}_1 = \left\{ \begin{array}{c} 000 \\ 001 \\ 010 \\ 100 \\ 101 \\ 110 \\ 111 \end{array} \right\}, \mathbf{V}_2 = \left\{ \begin{array}{c} 000 \\ 110 \\ 011 \\ 101 \end{array} \right\}.$$

Множество $\mathbf{V}_2$ является линейным подпространством пространства $\mathbf{V}_1$.

Векторы $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k$ называются *линейно независимыми*, если равенство

$$c_1 \cdot \mathbf{x}_1 + c_2 \cdot \mathbf{x}_2 + ... + c_k \cdot \mathbf{x}_k = \mathbf{0}, \quad (4)$$

где $\mathbf{0}$ – нулевой вектор, выполняется, если

$$c_1 = c_2 = ... = c_k = 0. \quad (5)$$

Жирный ноль - множество нулевых векторов

Пример. Векторы $(0, 1, 1, 1)$ и $(0, 2, 2, 2)$ над полем $GF(5)$ являются линейно зависимыми, поскольку $2 \cdot (0, 2, 2, 2) + (0, 1, 1, 1) = (0, 0, 0, 0)$.

В каждом линейном пространстве существуют линейно независимые векторы $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k$, такие что каждый вектор

$$\mathbf{x}_i = c_1 \cdot \mathbf{x}_1 + c_2 \cdot \mathbf{x}_2 + c_k \cdot \mathbf{x}_k. \quad (6)$$

Такие векторы называются *базисными векторами* линейного пространства.

Пример. Рассмотрим два множества векторов $\mathbf{V}_1$ и $\mathbf{V}_2$ над полем $GF(2) = \{0, 1\}$.

$$\mathbf{V}_1 = \left\{ \begin{array}{c} 000 \\ 001 \\ 010 \\ 100 \\ 101 \\ 110 \\ 111 \end{array} \right\}, \mathbf{V}_2 = \left\{ \begin{array}{c} 100 \\ 010 \\ 001 \end{array} \right\}.$$

Векторы, принадлежащие $\mathbf{V}_2$ являются базисными векторами для линейного пространства $\mathbf{V}_1$.