

01204211 Discrete Mathematics

Lecture 9a: Spans and Vector Spaces

Jittat Fakcharoenphol

October 15, 2024

Review: Linear combinations

Definition

For any scalars

$$\alpha_1, \alpha_2, \dots, \alpha_m$$

and vectors

$$\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m,$$

we say that

$$\alpha_1 \mathbf{u}_1 + \alpha_2 \mathbf{u}_2 + \dots + \alpha_m \mathbf{u}_m$$

is a **linear combination** of $\mathbf{u}_1, \dots, \mathbf{u}_m$.

Review: Span

Definition

A set of all linear combination of vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$ is called the **span** of that set of vectors.

It is denoted by $\text{Span}\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m\}$.

Exercise

The following vectors represent the amount of nutritions for 100ml of the healthy drink ingredients

$$\mathbf{v} = \begin{bmatrix} 100 \\ 50 \\ 0 \\ 0 \end{bmatrix} \quad \mathbf{c} = \begin{bmatrix} 0 \\ 0 \\ 300 \\ 0 \end{bmatrix} \quad \mathbf{w} = \begin{bmatrix} 50 \\ 0 \\ 50 \\ 10 \end{bmatrix}$$

Exercise

The following vectors represent the amount of nutritions for 100ml of the healthy drink ingredients

$$\boldsymbol{v} = \begin{bmatrix} 100 \\ 50 \\ 0 \\ 0 \end{bmatrix} \quad \boldsymbol{c} = \begin{bmatrix} 0 \\ 0 \\ 300 \\ 0 \end{bmatrix} \quad \boldsymbol{w} = \begin{bmatrix} 50 \\ 0 \\ 50 \\ 10 \end{bmatrix}$$

Write down the nutritions for a mixed drink that consists of 50ml of \boldsymbol{v} , 200ml of \boldsymbol{c} and 10ml of \boldsymbol{w} .

Exercise

$$0,5 \begin{bmatrix} 100 \\ 50 \\ 0 \\ 0 \end{bmatrix} + 2 \cdot \begin{bmatrix} 6 \\ 6 \\ 300 \\ 0 \end{bmatrix} + 0,1 \begin{bmatrix} 50 \\ 0 \\ 50 \\ 10 \end{bmatrix}$$

The following vectors represent the amount of nutritions for 100ml of the healthy drink ingredients

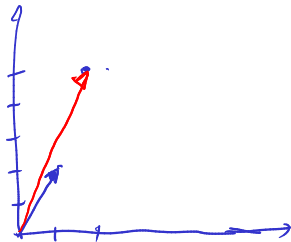
$$v = \begin{bmatrix} 100 \\ 50 \\ 0 \\ 0 \end{bmatrix} \quad c = \begin{bmatrix} 0 \\ 0 \\ 300 \\ 0 \end{bmatrix} \quad w = \begin{bmatrix} 50 \\ 0 \\ 50 \\ 10 \end{bmatrix}$$

- ① Write down the nutritions for a mixed drink that consists of 50ml of v , 200ml of c and 10ml of w . *(as a linear combination of v , c , & w)*
- ② Write that result as a matrix-vector product. (The matrix should be a 4×3 matrix.)

$$\begin{bmatrix} 100 & 0 & 50 \\ 50 & 0 & 0 \\ 0 & 300 & 50 \\ 0 & 0 & 10 \end{bmatrix} \begin{bmatrix} 0,5 \\ 2 \\ 0,1 \end{bmatrix} = \begin{bmatrix} 100 & 0 & 50 \\ 50 & 0 & 0 \\ 0 & 300 & 50 \\ 0 & 0 & 10 \end{bmatrix} \begin{bmatrix} 0,5 \\ 2 \\ 0,1 \end{bmatrix} = \begin{bmatrix} 100 \\ 50 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 300 \\ 0 \end{bmatrix} \begin{bmatrix} 50 \\ 0 \\ 50 \\ 10 \end{bmatrix} \begin{bmatrix} 0,5 \\ 2 \\ 0,1 \end{bmatrix}$$

Example 1

Is $\text{Span} \{[1, 2], [2, 5]\} = \mathbb{R}^2$?



Example 2

Is $\text{Span} \{[1, 0, 1], [1, 1, 0], [2, 3, 4]\} = \mathbb{R}^3$?

Example 3

Is $\text{Span} \{[1, 0, 1], [1, 1, 0], [4, 2, 2]\} = \mathbb{R}^3$?

Elements in a vector

- ▶ We see examples of vectors over \mathbb{R} .
- ▶ However, elements in a vector can be from other sets with appropriate property. (I.e., they should behave a real numbers.)
- ▶ What do we want from an element in a vector?
 - ▶ We should be able to perform addition, subtraction, multiplication, and division.
 - ▶ Operations should be commutative and associative.
 - ▶ Additive and multiplicative identity should exist.
 - ▶ Addition and multiplication should have inverses.
- ▶ We refer to a set with these properties as a **field**.

$$(ab)c = a(bc)$$

A field

Definition

A set \mathbb{F} with two operations $+$ and \times (or \cdot) is a **field** iff these operations satisfy the following properties:

- ▶ (Associativity): $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- ▶ (Commutativity): $a + b = b + a$ and $a \cdot b = b \cdot a$
- ▶ (Identities): There exist two elements $0 \in \mathbb{F}$ and $1 \in \mathbb{F}$ such that $a + 0 = a$ and $a \cdot 1 = a$
- ▶ (Additive inverse): For every element $a \in \mathbb{F}$, there is an element $-a \in \mathbb{F}$ such that $a + (-a) = 0$
- ▶ (Multiplicative inverse): For every element $a \in \mathbb{F} \setminus \{0\}$, there is an element a^{-1} such that $a \cdot a^{-1} = 1$
- ▶ (Distributive): $a \cdot (b + c) = a \cdot b + a \cdot c$

Another useful field: $GF(2)$

$GF(2) = \{0, 1\}$. I.e., it is a “bit” field.

What are $+$ and \cdot in $GF(2)$?

Another useful field: $GF(2)$

$GF(2) = \{0, 1\}$. I.e., it is a “bit” field.

What are $+$ and \cdot in $GF(2)$?

► We define $b_1 + b_2$ to be XOR.

$$0 + 0 = 0$$

$$0 + 1 = 1 + 0 = 1$$

$$1 + 1 = 0$$

Another useful field: $GF(2)$

$GF(2) = \{0, 1\}$. I.e., it is a “bit” field.

What are $+$ and \cdot in $GF(2)$?

- We define $b_1 + b_2$ to be XOR.

$$\begin{aligned}0 + 0 &= 0 \\0 + 1 &= 1 + 0 = 1 \\1 + 1 &= 0\end{aligned}$$

- We define $b_1 \cdot b_2$ to be standard multiplication.

$$\begin{aligned}0 \cdot 0 &= 0 \cdot 1 = 1 \cdot 0 = 0 \\1 \cdot 1 &= 1\end{aligned}$$

You can check that $GF(2)$ satisfies the axioms of fields.

3 x 3 Lights out

1	2	3
6	6	6
4	5	6
7	8	9

$b_1 =$

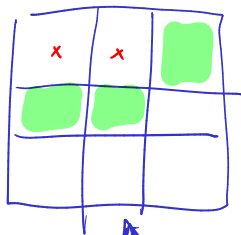
$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$b_2 =$

$$\begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$b_5 =$

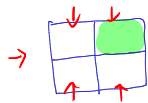
$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$



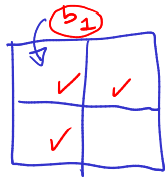
$$b_1 + b_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

b_1, b_2, \dots, b_9

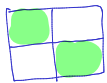
2 x 2 Lights out 4-vector



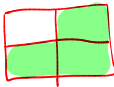
$$[0, 1, 0, 0] + b_1 =$$



$$= [1, 1, 1, 0]$$



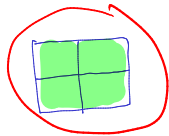
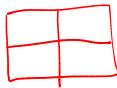
$$[1, 0, 0, 1]$$



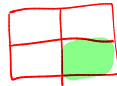
b_1	b_2
b_3	b_4



$$[1, 1, 1, 0]$$



$$[1, 1, 1, 1]$$



$$b_1 = [1, 1, 1, 0]$$

$$b_2 = [1, 1, 0, 1]$$

$$b_3 = [1, 0, 1, 1]$$

$$b_4 = [0, 1, 1, 1]$$

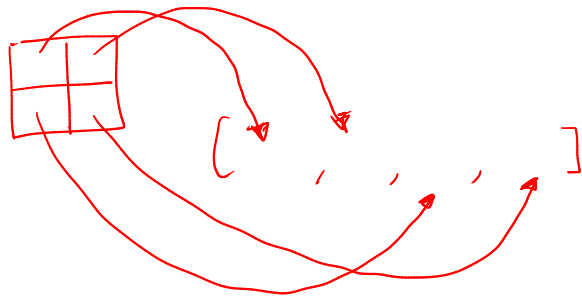
2×2 Lights out

$$b_1 = [1, 1, 1, 0]$$

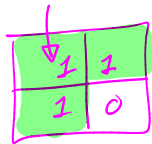
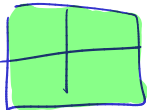
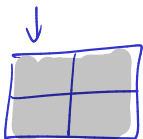
$$b_2 = [1, 1, 0, 1]$$

$$b_3 = [1, 0, 1, 1]$$

$$b_4 = [0, 1, 1, 1]$$



$$[0, 0, 0, 0]$$



$$[1, 1, 1, 0]$$

Press b_1 for x_1 time
 b_2 for x_2 time
 b_3 for x_3 time
 b_4 for x_4 time.

$$[1, 1, 1, 1] = x_1 b_1 + x_2 b_2 + x_3 b_3 + x_4 b_4$$

2×2 Lights out

$$x_1 \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} + x_3 \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + x_4 \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$



$$\begin{array}{rcl} x_1 + x_2 + x_3 & = & 1 \\ x_1 + x_2 & + x_4 & = 1 \\ x_1 & + x_3 + x_4 & = 1 \\ & x_2 + x_3 + \cancel{x_4} & = 1 \end{array}$$

$$b_1 = [1, 1, 1, 0]$$

$$b_2 = [1, 1, 0, 1]$$

$$b_3 = [1, 0, 1, 1]$$

$$b_4 = [0, 1, 1, 1]$$

2×2 Lights out

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

3×3 Lights out

g -vector

b_1	b_2	b_3
	b_3	

$$b_1 = \begin{bmatrix} 1, 1, 0 \\ 1, 0, 0 \\ 0, 0, 0 \end{bmatrix}$$

$$b_3 = \begin{bmatrix} 0, 0, 0 \\ 0, 1, 0 \\ 1, 1, 1 \end{bmatrix}$$

Parity-check code

Parity-check code

From message $\mathbf{a} = [a_1, a_2, a_3, a_4]$, we compute (in $GF(2)$) the parity check bit

$$b = a_1 + a_2 + a_3 + a_4.$$

Parity-check code

From message $\mathbf{a} = [a_1, a_2, a_3, a_4]$, we compute (in $GF(2)$) the parity check bit

$$\underline{b} = a_1 + a_2 + a_3 + a_4.$$

$$\boxed{1011 \textcircled{1}}$$

Now our encoded message becomes

$$1 + 0 + 1 + 1 = 1$$

$$[a_1, a_2, a_3, a_4, \textcircled{a_5}]$$

where $a_5 = b = a_1 + a_2 + a_3 + a_4$. It can detect a single-bit error.

$$\textcircled{6}$$
$$\underline{0011 \textcircled{1}}$$

Parity-check code

From message $\mathbf{a} = [a_1, a_2, a_3, a_4]$, we compute (in $GF(2)$) the parity check bit

$$b = a_1 + a_2 + a_3 + a_4.$$

Now our encoded message becomes

$$[a_1, a_2, a_3, a_4, a_5],$$

where $a_5 = b = a_1 + a_2 + a_3 + a_4$. It can detect a single-bit error.

What can we say about the condition on a_5 ?

Parity-check code

From message $\mathbf{a} = [a_1, a_2, a_3, a_4]$, we compute (in $GF(2)$) the parity check bit

$$b = a_1 + a_2 + a_3 + a_4.$$

Now our encoded message becomes

$$[a_1, a_2, a_3, a_4, a_5],$$

where $a_5 = b = a_1 + a_2 + a_3 + a_4$. It can detect a single-bit error.

What can we say about the condition on a_5 ?

It is in fact a homogeneous linear equation (in $GF(2)$):

$$a_1 + a_2 + a_3 + a_4 + a_5 = 0$$

Parity-check code

From message $\mathbf{a} = [a_1, a_2, a_3, a_4]$, we compute (in $GF(2)$) the parity check bit

$$b = a_1 + a_2 + a_3 + a_4.$$

Now our encoded message becomes

$$[a_1, a_2, a_3, a_4, a_5],$$

where $a_5 = b = a_1 + a_2 + a_3 + a_4$. It can detect a single-bit error.

What can we say about the condition on a_5 ?

It is in fact a homogeneous linear equation (in $GF(2)$):

$$a_1 + a_2 + a_3 + a_4 + a_5 = 0$$

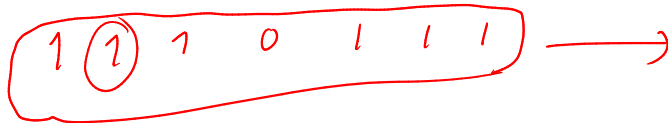
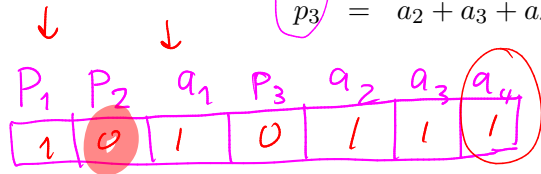
Now, what is the set of all possible codewords?

Hamming code

You can detect and correct more errors with Hamming codes. In this version called a $[7, 4]$ Hamming code, you encode 4-bit data $[a_1, a_2, a_3, a_4]$ into a 7-bit codeword $[p_1, p_2, a_1, p_3, a_2, a_3, a_4]$. Using the formula:

$$\begin{aligned} p_1 &= a_1 + a_2 + a_4 = 0 \\ p_2 &= a_1 + a_3 + a_4 = 0 \\ p_3 &= a_2 + a_3 + a_4 = 0 \end{aligned}$$

$$\begin{array}{c} 1110 \\ \hline a_1 \ a_2 \ a_3 \ a_4 \end{array}$$



s_3	s_2	s_1
0	0	1
0	1	1
1	1	1

Hamming code

You can detect and correct more errors with Hamming codes. In this version called a $[7, 4]$ Hamming code, you encode 4-bit data $[a_1, a_2, a_3, a_4]$ into a 7-bit codeword $[p_1, p_2, a_1, p_3, a_2, a_3, a_4]$. Using the formula:

$$p_1 = a_1 + a_2 + a_4$$

$$p_2 = a_1 + a_3 + a_4$$

$$p_3 = a_2 + a_3 + a_4$$

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}$$

Let's see how this works.

7×4

1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	1

A

m

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \\ a_1 \\ p_3 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}$$

w

Hamming code (encoding as matrix multiplication)

Parity check

Suppose that we are given $[d_1, d_2, d_3, d_4, d_5, d_6, d_7]$ Let

$$s_1 = d_1 + d_3 + d_5 + d_7 = 1$$

$$s_2 = d_2 + d_3 + d_6 + d_7 = 0 + 1 + 1 + 1 = 1$$

$$s_3 = d_4 + d_5 + d_6 + d_7 = 1 + 0 + 1 + 1 = 1$$

Given a codeword $w = [c_1, c_2, \dots, c_7]$, if we compute s_1, s_2, s_3 , we would get all zeros.

1	2	3	4	5	6	7
1	0	1	0	1	0	1
0	0	0	1	1	1	1
0	0	0	1	1	1	1

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$\begin{bmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \\ d_5 \\ d_6 \\ d_7 \end{bmatrix}$

$\begin{bmatrix} 0 \\ 0 \end{bmatrix}$

$\begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix}$

$\begin{matrix} s_3 & s_2 & s_1 \\ \hline 1 & 1 & 1 \end{matrix}$

Parity check

Suppose that we are given $[d_1, d_2, d_3, d_4, d_5, d_6, d_7]$ Let

$$0 = s_1 = d_1 + d_3 + d_5 + d_7$$

$$0 = s_2 = d_2 + d_3 + d_6 + d_7$$

$$0 = s_3 = d_4 + d_5 + d_6 + d_7$$

Given a codewords $\mathbf{w} = [c_1, c_2, \dots, c_7]$, if we compute s_1, s_2, s_3 , we would get all zero's.

What if there is an error? Let's try.

Hamming code (parity check as matrix multiplication)

$$\begin{bmatrix} \textcircled{1} & \textcircled{1} & 0 & \textcircled{1} \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}$$

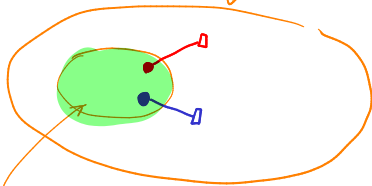
=

$$\begin{bmatrix} P_1 \\ P_2 \\ a_1 \\ P_3 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}$$

codeword \leftarrow 7 bits

2^7 possible strings

128



16 possible codewords

$2^4 = 16$ possible messages



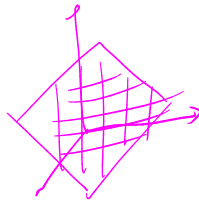
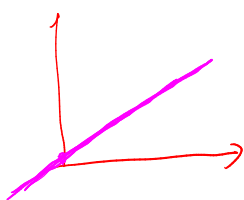
Codewords from Hamming code

$$[d_1, d_2, d_3, d_4, d_5, d_6, d_7]$$

Turning the formula for p_1, p_2, p_3 around, we have 3 homogeneous linear equations:

$$\begin{aligned} d_1 + d_3 + d_5 + d_7 &= 0 \\ d_2 + d_3 + d_6 + d_7 &= 0 \\ d_4 + d_5 + d_6 + d_7 &= 0 \end{aligned}$$

and again the set of all possible codewords \mathcal{W} forms a vector space over $GF(2)$.



Can you solve 2×2 Lights out?

(skipped)

Let $\mathbf{u}_1 = [1, 1, 1, 0]$, $\mathbf{u}_2 = [1, 1, 0, 1]$, $\mathbf{u}_3 = [1, 0, 1, 1]$, and $\mathbf{u}_4 = [0, 1, 1, 1]$.

Given $\mathbf{b} = [b_1, b_2, b_3, b_4]$, can you always find $a_1, a_2, a_3, a_4 \in GF(2)$ such that

$$a_1 \cdot \mathbf{u}_1 + a_2 \cdot \mathbf{u}_2 + a_3 \cdot \mathbf{u}_3 + a_4 \cdot \mathbf{u}_4 = \mathbf{b}?$$

Can you solve 2×2 Lights out?

Let $\mathbf{u}_1 = [1, 1, 1, 0]$, $\mathbf{u}_2 = [1, 1, 0, 1]$, $\mathbf{u}_3 = [1, 0, 1, 1]$, and $\mathbf{u}_4 = [0, 1, 1, 1]$.

Given $\mathbf{b} = [b_1, b_2, b_3, b_4]$, can you always find $a_1, a_2, a_3, a_4 \in GF(2)$ such that

$$a_1 \cdot \mathbf{u}_1 + a_2 \cdot \mathbf{u}_2 + a_3 \cdot \mathbf{u}_3 + a_4 \cdot \mathbf{u}_4 = \mathbf{b}?$$

Same question: Is $\text{Span} \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4\} = GF(2)^4$?

Can you solve 2×2 Lights out?

Let's try with an example. Let $\mathbf{b} = [1, 0, 0, 0]$. Can you find $a_1, a_2, a_3, a_4 \in GF(2)$ such that

$$a_1 \cdot \mathbf{u}_1 + a_2 \cdot \mathbf{u}_2 + a_3 \cdot \mathbf{u}_3 + a_4 \cdot \mathbf{u}_4 = \mathbf{b}?$$

Can you solve 2×2 Lights out?

Since

$$[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 1, 0], [0, 0, 0, 1] \in \text{Span} \{ \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4 \},$$

and

Can you solve 2×2 Lights out?

Since

$$[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 1, 0], [0, 0, 0, 1] \in \text{Span} \{ \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4 \},$$

and

$$\text{Span} \{ [1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 1, 0], [0, 0, 0, 1] \} = GF(2)^4,$$

Can you solve 2×2 Lights out?

Since

$$[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 1, 0], [0, 0, 0, 1] \in \text{Span} \{ \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4 \},$$

and

$$\text{Span} \{ [1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 1, 0], [0, 0, 0, 1] \} = GF(2)^4,$$

what can we say about $\text{Span} \{ \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4 \}$?

Generators

Definition

Let \mathcal{V} be a set of vectors. Consider vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$.

If $\text{Span} \{ \mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n \} = \mathcal{V}$, we say that

- ▶ $\{ \mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n \}$ is a **generating set** for \mathcal{V}
- ▶ vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$ are **generators** for \mathcal{V}

Generators

Definition

Let \mathcal{V} be a set of vectors. Consider vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$.

If $\text{Span} \{ \mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n \} = \mathcal{V}$, we say that

- ▶ $\{ \mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n \}$ is a **generating set** for \mathcal{V}
- ▶ vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$ are **generators** for \mathcal{V}

Examples

Standard generators

Note that $\{[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 1, 0], [0, 0, 0, 1]\}$ are generators for $GF(2)^4$.
Why?

Standard generators

Note that $\{[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 1, 0], [0, 0, 0, 1]\}$ are generators for $GF(2)^4$.
Why?

They are called **standard generators** for $GF(2)^4$, written as e_1, e_2, e_3, e_4 .

Standard generators

Note that $\{[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 1, 0], [0, 0, 0, 1]\}$ are generators for $GF(2)^4$.
Why?

They are called **standard generators** for $GF(2)^4$, written as e_1, e_2, e_3, e_4 .

For \mathbb{R}^n , we also have $[1, 0, 0, \dots, 0], [0, 1, 0, \dots, 0], [0, 0, 1, \dots, 0], \dots, [0, 0, 0, \dots, 1]$ as standard generators.

Generators and spans

Lemma 1

Consider vectors u_1, u_2, \dots, u_n . If v_1, v_2, \dots, v_k are generators for \mathcal{V} , and for each i ,

$$v_i \in \text{Span} \{u_1, u_2, \dots, u_n\},$$

we have that $\mathcal{V} \subseteq \text{Span} \{u_1, u_2, \dots, u_n\}$.

Adding a vector into a span

Lemma 2

Consider vectors u_1, u_2, \dots, u_n . If $v \in \text{Span} \{u_1, u_2, \dots, u_n\}$, then

$$\text{Span} \{u_1, u_2, \dots, u_n, v\} = \text{Span} \{u_1, u_2, \dots, u_n\}$$

Geometry of spans: in \mathbb{R}^2

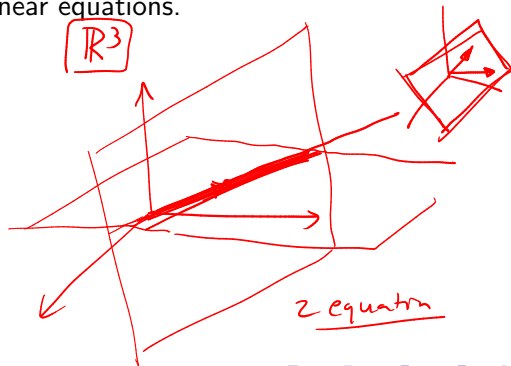
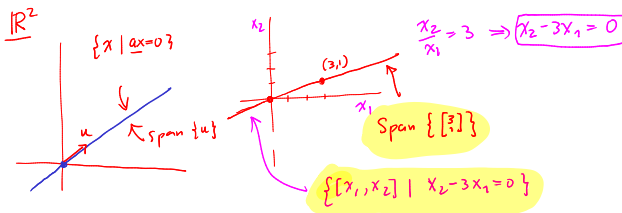
Geometry of spans: in \mathbb{R}^3

Two representations

Vector space

There are two ways to represent a line, a plane, and a (hyper)plane, passing through the origin:

- ▶ as a span of vectors
- ▶ as solutions of a system of homogeneous linear equations.



Two representations

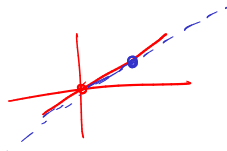
$$\underline{Ax} = \underline{b}^0$$

There are two ways to represent a line, a plane, and a (hyper)plane, passing through the origin:

- ▶ as a span of vectors
- ▶ as solutions of a system of homogeneous linear equations.

What are common properties of these geometric objects?

Two representations



There are two ways to represent a line, a plane, and a (hyper)plane, passing through the origin:

- ▶ as a span of vectors
- ▶ as solutions of a system of homogeneous linear equations.

What are common properties of these geometric objects?

- ▶ they pass through the origin,
- ▶ if vector u is in the objects, αu for any scalar α is also in the objects, and
- ▶ if u and v are in the objects, $u + v$ is also in the objects.

closed
under
scalar
multiplication

closed under addition

Vector space

Vector spaces

Definition

A set \mathcal{V} of vectors over \mathbb{F} is a **vector space** iff

- ▶ (V1) $\mathbf{0} \in \mathcal{V}$,
- ▶ (V2) for any $\mathbf{u} \in \mathcal{V}$,

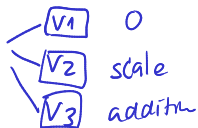
$$\alpha \cdot \mathbf{u} \in \mathcal{V}$$

for any $\alpha \in \mathbb{F}$, and

- ▶ (V3) for any $\mathbf{u}, \mathbf{v} \in \mathcal{V}$,

$$\mathbf{u} + \mathbf{v} \in \mathcal{V}.$$

Span of vectors is a vector space



Consider n -vectors u_1, u_2, \dots, u_m ,

$\text{Span} \{u_1, u_2, \dots, u_m\}$

is a vector space.

Span of vectors is a vector space

Consider n -vectors u_1, u_2, \dots, u_m ,

$$\text{Span} \{u_1, u_2, \dots, u_m\}$$

is a vector space.

Let's check if properties V1, V2, and V3 are satisfied.

$$(V1) \quad 0 \in \text{Span} \{u_1, u_2, \dots, u_m\} \quad \checkmark$$

$$(V2) \quad \text{If } u \in \text{Span} \{u_1, \dots, u_m\}, \text{ any } \alpha$$

Proof: there exist $\alpha_1, \alpha_2, \dots, \alpha_m$ s.t.

$$u = \alpha_1 u_1 + \alpha_2 u_2 + \dots + \alpha_m u_m$$

$$\beta u = \beta$$

$$= (\beta \alpha_1 u_1 + \beta \alpha_2 u_2 + \dots)$$

$\in \text{Span} \{ \dots \}$

$$(V3) \quad \begin{array}{l} \text{if} \\ x \in \text{Span} \\ y \in \text{Span} \end{array}$$

Solutions to homogeneous linear equations is a vector space



Consider a set \mathcal{S} of all n -vectors in the form $[x_1, x_2, \dots, x_n]$ where

homogeneous

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

m equation

Let's check if properties V1, V2, and V3 are satisfied.

V1

Dot product

Definition

For n -vectors $\mathbf{u} = [u_1, u_2, \dots, u_n]$ and $\mathbf{v} = [v_1, v_2, \dots, v_n]$, the **dot product** of \mathbf{u} and \mathbf{v} , denoted by $\mathbf{u} \cdot \mathbf{v}$, is

$$u_1 \cdot v_1 + u_2 \cdot v_2 + \dots + u_n \cdot v_n$$

Dot product

Definition

For n -vectors $\mathbf{u} = [u_1, u_2, \dots, u_n]$ and $\mathbf{v} = [v_1, v_2, \dots, v_n]$, the **dot product** of \mathbf{u} and \mathbf{v} , denoted by $\mathbf{u} \cdot \mathbf{v}$, is

$$u_1 \cdot v_1 + u_2 \cdot v_2 + \dots + u_n \cdot v_n$$

Using dot products, the previous set \mathcal{S} can be written as

$$\{\mathbf{x} \in \mathbb{R}^n : \mathbf{a}_1 \cdot \mathbf{x} = 0, \mathbf{a}_2 \cdot \mathbf{x} = 0, \dots, \mathbf{a}_m \cdot \mathbf{x} = 0\}$$

and we know that \mathcal{S} is a vector space.

An object not passing through the origin: 2 dimensions

An object not passing through the origin: 3 dimensions

Translation

If we have a line or a plane passing through a vector \mathbf{a} , but not through the origin, how can we represent it?

Translation

If we have a line or a plane passing through a vector \mathbf{a} , but not through the origin, how can we represent it?

- Translate the object so that it passes through the origin.

Translation

If we have a line or a plane passing through a vector \mathbf{a} , but not through the origin, how can we represent it?

- ▶ Translate the object so that it passes through the origin.
- ▶ We obtain a vector space \mathcal{V} .

Translation

If we have a line or a plane passing through a vector \mathbf{a} , but not through the origin, how can we represent it?

- ▶ Translate the object so that it passes through the origin.
- ▶ We obtain a vector space \mathcal{V} .
- ▶ Then we translate it back so that it passes through \mathbf{a} .

Translation

If we have a line or a plane passing through a vector \mathbf{a} , but not through the origin, how can we represent it?

- ▶ Translate the object so that it passes through the origin.
- ▶ We obtain a vector space \mathcal{V} .
- ▶ Then we translate it back so that it passes through \mathbf{a} .
- ▶ We get the set

$$\mathcal{A} = \{\mathbf{a} + \mathbf{u} : \mathbf{u} \in \mathcal{V}\}$$

Translation

If we have a line or a plane passing through a vector \mathbf{a} , but not through the origin, how can we represent it?

- ▶ Translate the object so that it passes through the origin.
- ▶ We obtain a vector space \mathcal{V} .
- ▶ Then we translate it back so that it passes through \mathbf{a} .
- ▶ We get the set

$$\mathcal{A} = \{\mathbf{a} + \mathbf{u} : \mathbf{u} \in \mathcal{V}\}$$

- ▶ *Question:* Is \mathcal{A} a vector space?

Translation

If we have a line or a plane passing through a vector \mathbf{a} , but not through the origin, how can we represent it?

- ▶ Translate the object so that it passes through the origin.
- ▶ We obtain a vector space \mathcal{V} .
- ▶ Then we translate it back so that it passes through \mathbf{a} .
- ▶ We get the set

$$\mathcal{A} = \{\mathbf{a} + \mathbf{u} : \mathbf{u} \in \mathcal{V}\}$$

- ▶ *Question:* Is \mathcal{A} a vector space?
- ▶ We also write it as $\mathbf{a} + \mathcal{V}$.

Affine spaces

Definition

If \mathbf{a} is a vector and \mathcal{V} is a vector space, then

$$\mathbf{a} + \mathcal{V}$$

is an **affine space**.

An affine space and convex combination: 2 dimensions

An affine space and convex combination: 3 dimensions

Affine combination

Definition

For any scalars $\alpha_1, \alpha_2, \dots, \alpha_m$ such that

$$\alpha_1 + \alpha_2 + \dots + \alpha_m = 1$$

and vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$, we say that a linear combination

$$\alpha_1 \mathbf{u}_1 + \alpha_2 \mathbf{u}_2 + \dots + \alpha_m \mathbf{u}_m$$

is an **affine combination** of $\mathbf{u}_1, \dots, \mathbf{u}_m$.

Affine combination

Definition

For any scalars $\alpha_1, \alpha_2, \dots, \alpha_m$ such that

$$\alpha_1 + \alpha_2 + \dots + \alpha_m = 1$$

and vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$, we say that a linear combination

$$\alpha_1 \mathbf{u}_1 + \alpha_2 \mathbf{u}_2 + \dots + \alpha_m \mathbf{u}_m$$

is an **affine combination** of $\mathbf{u}_1, \dots, \mathbf{u}_m$.

Definition

The set of all affine combinations of vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$ is called the **affine hull** of $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$.

Convex combination: review

Definition

For any scalars $\alpha_1, \alpha_2, \dots, \alpha_m \geq 0$ such that

$$\alpha_1 + \alpha_2 + \dots + \alpha_m = 1$$

and vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$, we say that a linear combination

$$\alpha_1 \mathbf{u}_1 + \alpha_2 \mathbf{u}_2 + \dots + \alpha_m \mathbf{u}_m$$

is a **convex combination** of $\mathbf{u}_1, \dots, \mathbf{u}_m$.

Definition

The set of all convex combinations of vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$ is called the **convex hull** of $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$.

Writing an affine space using a span

Writing an affine space using a span

An affine space

An affine space passing through $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$ is

$$\mathbf{u}_1 + \text{Span} \{ \mathbf{u}_2 - \mathbf{u}_1, \mathbf{u}_3 - \mathbf{u}_1, \dots, \mathbf{u}_n - \mathbf{u}_1 \}.$$

Non-homogeneous linear system

Two linear systems:

$$\begin{aligned} \mathbf{a}_1 \cdot \mathbf{x} &= b_1 \\ \mathbf{a}_2 \cdot \mathbf{x} &= b_2 \\ &\vdots \\ \mathbf{a}_m \cdot \mathbf{x} &= b_m \end{aligned}$$

$$\begin{aligned} \mathbf{a}_1 \cdot \mathbf{x} &= 0 \\ \mathbf{a}_2 \cdot \mathbf{x} &= 0 \\ &\vdots \\ \mathbf{a}_m \cdot \mathbf{x} &= 0 \end{aligned}$$

What can you say about the solution sets of these two related linear systems?

Non-homogeneous linear system

Two linear systems:

$$\begin{array}{rcl} \mathbf{a}_1 \cdot \mathbf{x} & = & b_1 \\ \mathbf{a}_2 \cdot \mathbf{x} & = & b_2 \\ & \vdots & \\ \mathbf{a}_m \cdot \mathbf{x} & = & b_m \end{array}$$

$$\begin{array}{rcl} \mathbf{a}_1 \cdot \mathbf{x} & = & 0 \\ \mathbf{a}_2 \cdot \mathbf{x} & = & 0 \\ & \vdots & \\ \mathbf{a}_m \cdot \mathbf{x} & = & 0 \end{array}$$

What can you say about the solution sets of these two related linear systems?

$\mathbf{0}$ is always a solution to the linear system on the right.

Note: A linear equation whose right-hand-side is zero is called a **homogeneous linear equation**. A system of linear homogeneous equations is called a **homogeneous linear system**.

Solutions of the two systems

Recall that if \mathbf{u}_1 and \mathbf{u}_2 are both solutions to the non-homogeneous linear system, we have that for any i

$$\mathbf{a}_i \mathbf{u}_1 - \mathbf{a}_i \mathbf{u}_2 = b_i - b_i = 0 = \mathbf{a}_i (\mathbf{u}_1 - \mathbf{u}_2).$$

Solutions of the two systems

Recall that if \mathbf{u}_1 and \mathbf{u}_2 are both solutions to the non-homogeneous linear system, we have that for any i

$$\mathbf{a}_i \mathbf{u}_1 - \mathbf{a}_i \mathbf{u}_2 = b_i - b_i = 0 = \mathbf{a}_i (\mathbf{u}_1 - \mathbf{u}_2).$$

This implies that $\mathbf{u}_1 - \mathbf{u}_2$ is a solution to the homogeneous linear system.

Suppose that \mathcal{W} is the set of all solution to the non-homogeneous linear system, i.e.,

$$\mathcal{W} = \{\boldsymbol{x} : \boldsymbol{a}_i \boldsymbol{x} = b_i, \text{ for } 1 \leq i \leq m\},$$

and let $\boldsymbol{u} \in \mathcal{W}$ be one of the solutions, we have that

$$\{\boldsymbol{v} - \boldsymbol{u} : \boldsymbol{v} \in \mathcal{W}\}$$

Suppose that \mathcal{W} is the set of all solution to the non-homogeneous linear system, i.e.,

$$\mathcal{W} = \{\mathbf{x} : \mathbf{a}_i \mathbf{x} = b_i, \text{ for } 1 \leq i \leq m\},$$

and let $\mathbf{u} \in \mathcal{W}$ be one of the solutions, we have that

$$\{\mathbf{v} - \mathbf{u} : \mathbf{v} \in \mathcal{W}\}$$

is a vector space, because

Suppose that \mathcal{W} is the set of all solution to the non-homogeneous linear system, i.e.,

$$\mathcal{W} = \{\mathbf{x} : \mathbf{a}_i \mathbf{x} = b_i, \text{ for } 1 \leq i \leq m\},$$

and let $\mathbf{u} \in \mathcal{W}$ be one of the solutions, we have that

$$\{\mathbf{v} - \mathbf{u} : \mathbf{v} \in \mathcal{W}\}$$

is a vector space, because

$$\{\mathbf{v} - \mathbf{u} : \mathbf{v} \in \mathcal{W}\} = \{\mathbf{x} : \mathbf{a}_i \mathbf{x} = 0, \text{ for } 1 \leq i \leq m\}$$

Suppose that \mathcal{W} is the set of all solution to the non-homogeneous linear system, i.e.,

$$\mathcal{W} = \{\mathbf{x} : \mathbf{a}_i \mathbf{x} = b_i, \text{ for } 1 \leq i \leq m\},$$

and let $\mathbf{u} \in \mathcal{W}$ be one of the solutions, we have that

$$\{\mathbf{v} - \mathbf{u} : \mathbf{v} \in \mathcal{W}\}$$

is a vector space, because

$$\{\mathbf{v} - \mathbf{u} : \mathbf{v} \in \mathcal{W}\} = \{\mathbf{x} : \mathbf{a}_i \mathbf{x} = 0, \text{ for } 1 \leq i \leq m\}$$

In other words,

$$\begin{aligned} \mathcal{W} &= \mathbf{u} + \{\mathbf{v} - \mathbf{u} : \mathbf{v} \in \mathcal{W}\} \\ &= \mathbf{u} + \{\mathbf{x} : \mathbf{a}_i \mathbf{x} = 0, \text{ for } 1 \leq i \leq m\}, \end{aligned}$$

Suppose that \mathcal{W} is the set of all solution to the non-homogeneous linear system, i.e.,

$$\mathcal{W} = \{\mathbf{x} : \mathbf{a}_i \mathbf{x} = b_i, \text{ for } 1 \leq i \leq m\},$$

and let $\mathbf{u} \in \mathcal{W}$ be one of the solutions, we have that

$$\{\mathbf{v} - \mathbf{u} : \mathbf{v} \in \mathcal{W}\}$$

is a vector space, because

$$\{\mathbf{v} - \mathbf{u} : \mathbf{v} \in \mathcal{W}\} = \{\mathbf{x} : \mathbf{a}_i \mathbf{x} = 0, \text{ for } 1 \leq i \leq m\}$$

In other words,

$$\begin{aligned}\mathcal{W} &= \mathbf{u} + \{\mathbf{v} - \mathbf{u} : \mathbf{v} \in \mathcal{W}\} \\ &= \mathbf{u} + \{\mathbf{x} : \mathbf{a}_i \mathbf{x} = 0, \text{ for } 1 \leq i \leq m\},\end{aligned}$$

i.e., \mathcal{W} is an affine space.

Solutions to a non-homogeneous linear system

Lemma 3

If the solution set of a linear system is not empty, it is an affine space.