01204211 Discrete Mathematics
Lecture 9a: Spans and Vector Spaces

Jittat Fakcharoenphol

August 30, 2022

Review: Linear combinations

Definition

For any scalars

$$\alpha_1, \alpha_2, \ldots, \alpha_m$$

and vectors

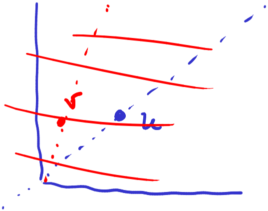
$$\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m,$$

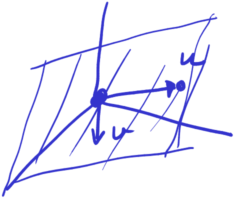
we say that

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_m \boldsymbol{u}_m$$

is a **linear combination** of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$.

Review: Span





Definition

A set of all linear combination of vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$ is called the **span** of that set of vectors.
It is denoted by $\mathrm{Span}\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m\}$.

Example 1

$\boxed{[1,2] \quad [0,5]}$ $-$ $\underline{\mathrm{Span}\{[1,0],[0,1]\}} = \mathbb{R}^2$

$(x,y) \in \mathrm{Span}\{\_\_\_\}$

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

บอกว่า สำหรับ $\forall\,(x,y) \in \mathbb{R}^2$

มี $\alpha_1 \in \mathbb{R}$, $\alpha_2 \in \mathbb{R}$ ที่

$$\alpha_1 [1,2] + \alpha_2 [2,5] = [x,y]$$

$$\underline{[1,0]} = -0.5\big([2,5] - 2.5[1,2]\big)$$

$\underline{[0,1]}$ ...... ———

Example 2

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

$2, 1, 1$

Example 3

Span $\{[1,0,1], [1,1,0]\}$

$\mathbin{/\!/}$

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

No! มี vector $\underline{[x,y,z] \in \mathbb{R}^3}$
แต่ $[x,y,z] \notin \text{Span}\,(\;)$

พิจารณา $[4,\underset{=}{2},3]$ แสดงว่า $[4,2,3] \notin \text{Span}\ldots$

$\vdots$

Elements in a vector

$\mathbb{R}$ $\mathbb{C}$

- 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**.

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 alement 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(p)

$GF(2) = \{0, 1\}$. I.e., it is a "bit" field.
What are $+$ and $\cdot$ in $GF(2)$?

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

$$
\begin{gathered}
0 + 0 = 0 \\
0 + 1 = 1 + 0 = 1 \\
1 + 1 = 0
\end{gathered}
$$

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.

$$\begin{gathered} 0 + 0 = 0 \\ 0 + 1 = 1 + 0 = 1 \\ 1 + 1 = 0 \end{gathered}$$

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

$$\begin{gathered} 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 \\ 1 \cdot 1 = 1 \end{gathered}$$

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

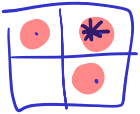
2×2 Lights out

$\boxed{GF(2)}$

ไฟติด — 1

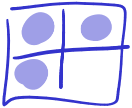
ดับ 0

a_1	a_2
a_3	a_4



init $[0, 1, 0, 0] = a$

$u_1 = [1, 1, 0, 1]$



$u_2 = [1, 1, 1, 0]$

$u_3 = [0, 1, 1, 1]$

$u_4 = [1, 0, 1, 1]$

จาก a

เอา $\underline{u_1, u_2 \ldots, u_4}$ ไปบวกเข้ากับ a จนกระทั่งได้ 0

Can you solve 2×2 Lights out?

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

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

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

Can you solve 2×2 Lights out?

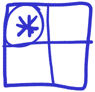
Let $\boldsymbol{u}_1 = [1,1,1,0]$, $\boldsymbol{u}_2 = [1,1,0,1]$, $\boldsymbol{u}_3 = [1,0,1,1]$, and $\boldsymbol{u}_4 = [0,1,1,1]$.

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

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

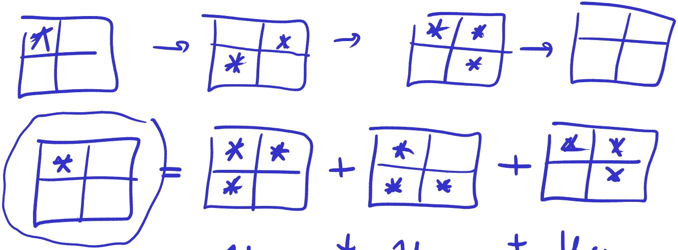
Same question: Is $\mathrm{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4\} = GF(2)^4$?

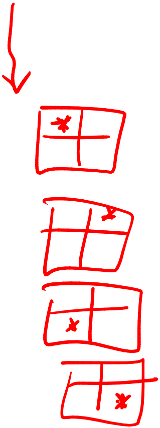
Can you solve 2×2 Lights out?



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

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





$u_1 + u_3 + u_4$

Can you solve 2×2 Lights out?

Since

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

and

Can you solve 2×2 Lights out?

Since

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

and

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

$[a_1, a_2, a_3, a_4]$

$= a_1 [1, \_\_]$

Can you solve 2×2 Lights out?

Since

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

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 Span $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4\}$? $=$ $GF(2)^4$

Generators

Definition

Let $\mathcal{V}$ be a set of vectors. Consider vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$.
If $\text{Span}\ \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\} = \mathcal{V}$, we say that

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

Generators

Definition

Let $\mathcal{V}$ be a set of vectors. Consider vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$.
If $\text{Span}\ \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\} = \mathcal{V}$, we say that

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

Examples

$[0,1], [1,0]$ are generators for $\mathbb{R}^2$

$[1,2], [2,5]$ are generators for $\mathbb{R}^2$

u_1, u_2, u_3, u_4 for $GF(2)^4$

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?

Standard generators

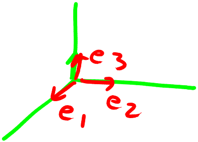
Note that $\{[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 1, 0], [0, 0, 0, 1]\}$ are generators for $GF(2)^4$. Why?

They are called **standard generators** for $GF(2)^4$, written as $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4$.

Standard generators

(x, y, z)

$= e_1 x + e_2 y + e_3 z.$



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 $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4$.

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

e_1 $\quad$ e_2 $\quad$ e_n

Generators and spans

Lemma 1

Consider vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$. *If* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ *are generators for* $\mathcal{V}$, *and for each* i,

$$\boldsymbol{v}_i \in \operatorname{Span}\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\},$$

we have that $\mathcal{V} \subseteq \operatorname{Span}\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$.

Goal $\forall x \in \mathcal{V}$, $x \in \operatorname{Span}\{u_1, u_2, \ldots, u_n\}$

มี $\alpha_1, \alpha_2, \ldots, \alpha_n$ ที่
$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n = x$

(sketch)
Proof เพราะ: $x \in \mathcal{V}$, x เป็น linear comb ของ $v_1, v_2, \ldots, v_k$
นั่นคือ มี $\alpha_1, \ldots, \alpha_k$ ที่ $x = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k$
$\forall i$ เพราะว่า $v_i \in \operatorname{Span}\{\ldots\}$ มี $\beta_{i1}, \beta_{i2}, \ldots, \beta_{in}$ ที่ $v_i = \beta_{i1} \cdot u_1 + \beta_{i2} \cdot u_2 + \cdots + \beta_{in} u_n$
ดังนั้น จะได้ว่า $x = \alpha_1(\beta_{11} u_1 + \beta_{12} u_2 + \cdots + \beta_{1n} u_n) + \alpha_2(\ \_\_\_\_\_\_$
$= (\alpha_1 \beta_{11} + \alpha_2 \beta_{12} + \alpha_3 \beta_{13} + \cdots + \alpha_k \beta_{1k}) u_1 + \ldots$

Adding a vector into a span

Lemma 2

Consider vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$. *If* $\boldsymbol{v} \in \overbrace{\mathrm{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}}^{A}$, *then*

เพิ่ม v

$$\mathrm{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n, \boldsymbol{v}\} = \mathrm{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$$

จะแสดงว่า $x \in \mathrm{Span}\{u_1, \ldots, u_n, v\}$ แล้ว $x \in \mathrm{Span}\{u_1, \ldots, u_n\}$

เนื่องจาก มี $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha'$ ที่

$$x = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n + \alpha' v \qquad (1)$$

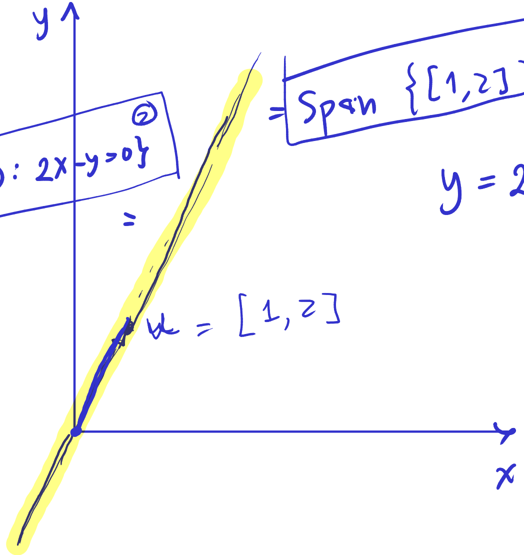
แต่ $v \in \mathrm{Span}\, A$ นั่นคือ มี $\beta_1, \beta_2, \ldots, \beta_n$ ที่

$$v = \beta_1 u_1 + \beta_2 u_2 + \cdots \beta_n u_n$$ — แทนค่าลงใน (1) ได้

$$x = \alpha_1 u_1 + \cdots + \alpha_n u_n + \alpha'(\beta_1 u_1 + \cdots + \beta_n u_n) = (\alpha_1 + \alpha'\beta_1)u_1 + (\alpha_2 + \alpha'\beta_2)u_2 + \cdots + (\alpha_n + \alpha'\beta_n)u_n$$

นั่นคือ x เป็น lin. comb. ของ $u_1, \ldots, u_n \Rightarrow x \in \mathrm{Span}\, A$

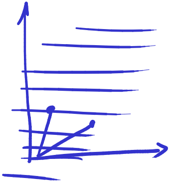
Geometry of spans: in $\mathbb{R}^2$



$$\boxed{\{(x,y) : 2x - y = 0\}} \quad ② \quad = \quad \boxed{\operatorname{Span}\{[1,2]\}} \quad ①$$

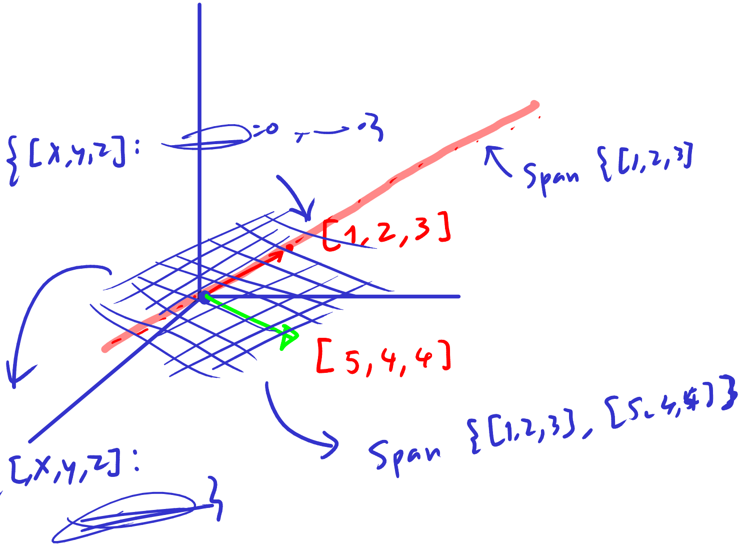
$u = [1, 2]$

$$y = 2x \iff 2x - y = 0$$



$\{(x,y) :$

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



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

= 0

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?

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 $\boldsymbol{u}$ is in the objects, $\alpha \boldsymbol{u}$ for any scalar α is also in the objects, and
- if $\boldsymbol{u}$ and $\boldsymbol{v}$ are in the objects, $\boldsymbol{u} + \boldsymbol{v}$ is also in the objects.

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 $\boldsymbol{u} \in \mathcal{V}$,
$$\alpha \cdot \boldsymbol{u} \in \mathcal{V}$$
  for any $\alpha \in \mathbb{F}$, and
- (V3) for any $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{V}$,
$$\boldsymbol{u} + \boldsymbol{v} \in \mathcal{V}.$$

Span of vectors is a vector space

Consider n-vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$,

$$\mathrm{Span}\ \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m\}$$

is a vector space.

Span of vectors is a vector space

$x+y = (\alpha_1+\beta_1)u_1 + (\alpha_2+\beta_2) \cdots$

Consider n-vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$,

$$\text{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m\}$$

is a vector space.

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

(V1) $0 \in \text{Sp}\ldots$?

(V2) เนื่องจาก $x \in \text{Span}\{u_1, \ldots, u_m\}$, มี $\alpha_1, \alpha_2, \ldots, \alpha_m$

ที่ $x = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_m u_m$

พิจารณา scalar β ได้ว่า $\beta x = \beta\alpha_1 u_1 + \beta\alpha_2 u_2 + \cdots + \beta\alpha_m u_m$

นั่นคือ $\beta x \in \text{Span}\{u_1, \ldots, u_m\}$ ตามต้องการ

(V3)

Solutions to homogeneous linear equations is a vector space

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

$$\left.\begin{array}{rcl}
a_{11} \cdot x_1 + a_{12} \cdot x_2 + \cdots + a_{1n} \cdot x_n & = & 0 \\
a_{21} \cdot x_1 + a_{22} \cdot x_2 + \cdots + a_{2n} \cdot x_n & = & 0 \\
\vdots & = & \vdots \\
a_{m1} x \cdot_1 + a_{m2} \cdot x_2 + \cdots + a_{mn} \cdot x_n & = & 0
\end{array}\right\} \text{m homo-gen equations}$$

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

(V1) $x_1 = x_2 = \cdots = x_n = 0$ ✓

(V2) $a_{i1} \alpha x_1 + a_{i2} \alpha x_2 + a_{i3} \cdot \alpha x_3 + \cdots = \alpha (\_\_\_\_) = \alpha \cdot 0 = 0$

(V3) ✓

Dot product

element-wise

Definition

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

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

Dot product

$a_1 = [a_{11}, a_{12}, \cdot \cdot, a_{1n}]$

Definition

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

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

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

$$\{\boldsymbol{x} \in \mathbb{R}^n : \underbrace{\boldsymbol{a}_1 \cdot \boldsymbol{x} = 0}, \underbrace{\boldsymbol{a}_2 \cdot \boldsymbol{x} = 0}, \ldots, \underbrace{\boldsymbol{a}_m \cdot \boldsymbol{x} = 0}\}$$

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

Parity-check code

GF(2)

error detection

110 $\boxed{0}$

1000

Parity-check code

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

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

Parity-check code

From message $\boldsymbol{a} = [a_1, a_2, a_3, a_4]$, 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 detects a single-bit error.

Parity-check code

From message $\boldsymbol{a} = [a_1, a_2, a_3, a_4]$, 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 detects a single-bit error.

What can we say about the condition on a_5?

Parity-check code

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

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

Now our encoded message becomes

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

where $a_5 = b = a_1 + a_2 + a_3 + a_4$. It can detects 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 $\boldsymbol{a} = [a_1, a_2, a_3, a_4]$, 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 detects a single-bit error.

What can we say about the condition on a_5?
It is in fact a homogeneous linear equation (in $GF(2)$):

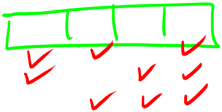
$$a_1 + a_2 + a_3 + a_4 + a_5 = 0$$

Now, what is the set of all possible codewords?

เปน vector space

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 $[a_1, a_2, a_3, a_4, a_5, a_6, a_7]$. Using the formula:



$$
\begin{aligned}
a_5 &= a_1 + a_2 + a_4 \\
a_6 &= a_1 + a_3 + a_4 \\
a_7 &= a_2 + a_3 + a_4
\end{aligned}
$$

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 $[a_1, a_2, a_3, a_4, a_5, a_6, a_7]$. Using the formula:

$$\begin{aligned} a_5 &= a_1 + a_2 + a_4 \\ a_6 &= a_1 + a_3 + a_4 \\ a_7 &= a_2 + a_3 + a_4 \end{aligned}$$

Let's see how this works.

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

Parity check

1 1 1 0 0 0 0

1 0 1 0 0 0 0

$\boxed{1\,0\,1}$

Let

$$
\begin{aligned}
s_1 &= a_1 + a_2 + a_4 + a_5 \\
s_2 &= a_1 + a_3 + a_4 + a_6 \\
s_3 &= a_2 + a_3 + a_4 + a_7
\end{aligned}
$$

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

Parity check

Let

$$
\begin{aligned}
s_1 &= a_1 + a_2 + a_4 + a_5 \\
s_2 &= a_1 + a_3 + a_4 + a_6 \\
s_3 &= a_2 + a_3 + a_4 + a_7
\end{aligned}
$$

Given a codewords $\boldsymbol{w} = [c_1, c_2, \ldots, c_7]$, if we compute s_1, s_2, s_3, we would get all zero's.
What if there is an error? Let's try.

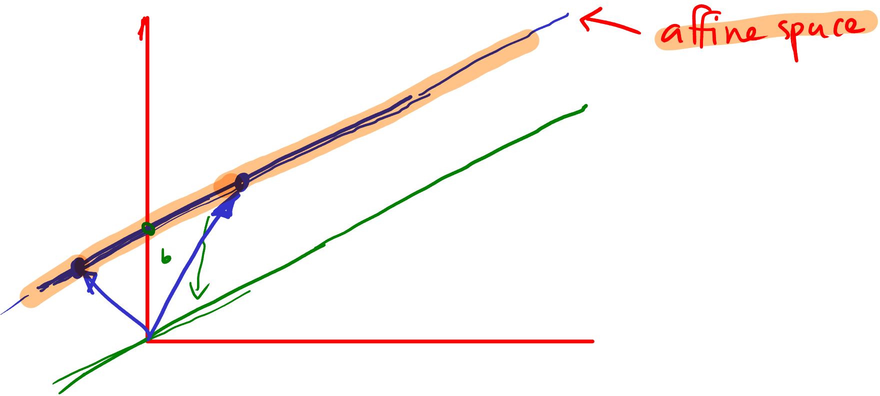
Codewords from Hamming code

Turning the formula for a_5, a_6, a_7 around, we have 3 homogeneous linear equations:

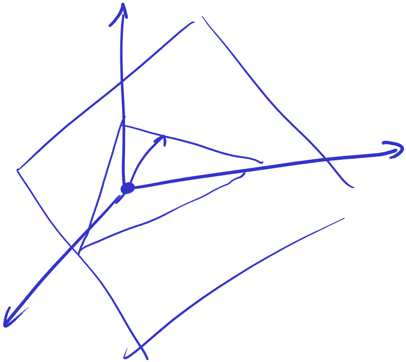
$$\boxed{\begin{array}{rcl} a_1 + a_2 + a_4 + a_5 & = & 0 \\ a_1 + a_3 + a_4 + a_6 & = & 0 \\ a_2 + a_3 + a_4 + a_7 & = & 0 \end{array}}$$

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

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 $\boldsymbol{a}$, but not through the origin, how can we represent it?

Translation

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

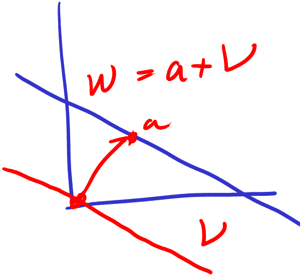
- Translate the object so that it passes through the origin.
- We obtain a vector space $\mathcal{V}$.
- Then we translate it back so that it passes through $\boldsymbol{a}$.

Translation

If we have a line or a plane passing through a vector $\boldsymbol{a}$, 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 $\boldsymbol{a}$.
- We get the set

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



Translation

If we have a line or a plane passing through a vector $\boldsymbol{a}$, 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 $\boldsymbol{a}$.
- We get the set
$$\mathcal{A} = \{\boldsymbol{a} + \boldsymbol{u} : \boldsymbol{u} \in \mathcal{V}\}$$
- *Question:* Is $\mathcal{A}$ a vector space?

Translation

If we have a line or a plane passing through a vector $\boldsymbol{a}$, 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 $\boldsymbol{a}$.
- We get the set
$$\mathcal{A} = \{\boldsymbol{a} + \boldsymbol{u} : \boldsymbol{u} \in \mathcal{V}\}$$
- *Question:* Is $\mathcal{A}$ a vector space?
- We also write it as $\boldsymbol{a} + \mathcal{V}$.

Affine spaces

Definition

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

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

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 $\alpha_1, \alpha_2, \ldots, \alpha_m$ such that

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

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

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_m \boldsymbol{u}_m$$

is an **affine combination** of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$.

Affine combination

Definition

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

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

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

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_m \boldsymbol{u}_m$$

is an **affine combination** of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$.

Definition

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

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

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_m \boldsymbol{u}_m$$

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

Definition

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

Writing an affine space using a span

Writing an affine space using a span

An affine space

An affine space passing through $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ is

$$\boldsymbol{u}_1 + \mathrm{Span}\,\{\boldsymbol{u}_2 - \boldsymbol{u}_1, \boldsymbol{u}_3 - \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n - \boldsymbol{u}_1\}.$$

Non-homogeneous linear system

Two linear systems:

$$\begin{aligned} \boldsymbol{a_1} \cdot \boldsymbol{x} &= b_1 \\ \boldsymbol{a_2} \cdot \boldsymbol{x} &= b_2 \\ &\vdots \\ \boldsymbol{a_m} \cdot \boldsymbol{x} &= b_m \end{aligned} \qquad\qquad \begin{aligned} \boldsymbol{a_1} \cdot \boldsymbol{x} &= 0 \\ \boldsymbol{a_2} \cdot \boldsymbol{x} &= 0 \\ &\vdots \\ \boldsymbol{a_m} \cdot \boldsymbol{x} &= 0 \end{aligned}$$

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

Non-homogeneous linear system

Two linear systems:

$$\begin{array}{rcl} \boldsymbol{a_1} \cdot \boldsymbol{x} & = & b_1 \\ \boldsymbol{a_2} \cdot \boldsymbol{x} & = & b_2 \\ & \vdots & \\ \boldsymbol{a_m} \cdot \boldsymbol{x} & = & b_m \end{array} \qquad\qquad \begin{array}{rcl} \boldsymbol{a_1} \cdot \boldsymbol{x} & = & 0 \\ \boldsymbol{a_2} \cdot \boldsymbol{x} & = & 0 \\ & \vdots & \\ \boldsymbol{a_m} \cdot \boldsymbol{x} & = & 0 \end{array}$$

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

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

Solutions of the two systems

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

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

This implies that $\boldsymbol{u}_1 - \boldsymbol{u}_2$ 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.,

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

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

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

is a vector space, because

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

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

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

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

is a vector space, because

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

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

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

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

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

is a vector space, because

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

In other words,

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

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

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

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

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

is a vector space, because

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

In other words,

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

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.