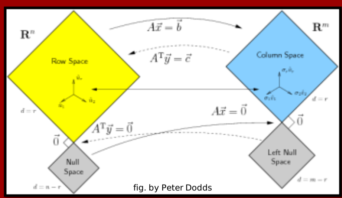
15-251: Great Theoretical Ideas in Computer Science
Lecture 23

Linear Algebra



Linear algebra is about vectors.

Concretely, vectors look like this:

$$\begin{bmatrix} 7 \\ 5 \\ 2 \end{bmatrix}$$

They are arrays of numbers.

\# of numbers, n, is called the *dimension*.

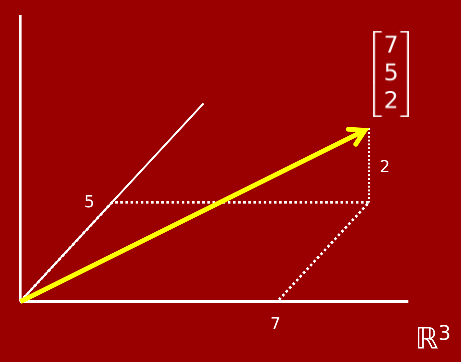
In linear algebra, 'numbers' are called *scalars*.

They can actually be from any *field*.

$$\begin{bmatrix} 7 \\ 5 \\ 2 \end{bmatrix}$$

F^n = {all vectors of dimension n over field F}

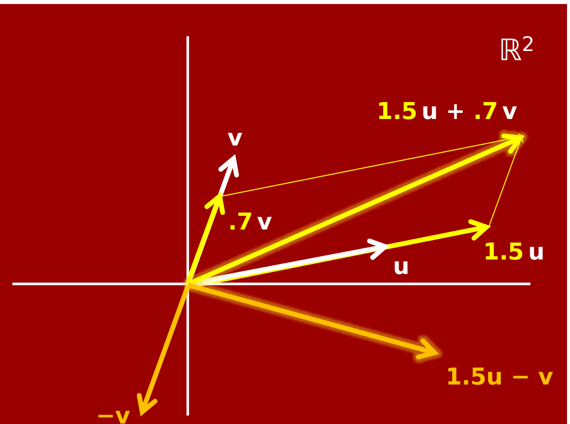
If the field is $\mathbb{R}$ and the dimension is ≤ 3, you can draw pictures.



The key operation on vectors:
taking linear combinations

= multiplying them by scalars and adding them

$$2\begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} + 1\begin{bmatrix} 4 \\ 3 \\ 1 \end{bmatrix} + 2\begin{bmatrix} -1.5 \\ -1 \\ -.5 \end{bmatrix} = \begin{bmatrix} 7 \\ 5 \\ 2 \end{bmatrix}$$



Remark: Even in, say, $\mathbb{F}_{11}^3$ when the scalars are from a finite field, geometric intuition can be helpful.

To take linear combinations of vectors,

say, $\begin{bmatrix}3\\2\\1\end{bmatrix}$ and $\begin{bmatrix}4\\3\\1\end{bmatrix}$,

make them the columns of a *matrix*: $\begin{bmatrix}3&4\\2&3\\1&1\end{bmatrix}$

Linear combination with scalars a,b is:

$$\begin{bmatrix}3&4\\2&3\\1&1\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix}=a\begin{bmatrix}3\\2\\1\end{bmatrix}+b\begin{bmatrix}4\\3\\1\end{bmatrix}$$

$$\begin{bmatrix}3&4\\2&3\\1&1\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix}=a\begin{bmatrix}3\\2\\1\end{bmatrix}+b\begin{bmatrix}4\\3\\1\end{bmatrix}$$

This is the definition of Matrix × Vector multiplication.

If you stack several linear combinations horizontally, you get the definition of Matrix × Matrix multiplication:

$$\begin{bmatrix}3&4\\2&3\\1&1\end{bmatrix}\begin{bmatrix}1&0&1&100\\0&1&1&-2\end{bmatrix}=\begin{bmatrix}3&4&7&292\\2&3&5&194\\1&1&2&98\end{bmatrix}$$

Matrix mult is associative, but **not** commutative!

$$\begin{bmatrix}3&4\\2&3\\1&1\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix}=a\begin{bmatrix}3\\2\\1\end{bmatrix}+b\begin{bmatrix}4\\3\\1\end{bmatrix}$$

You can also think of $\begin{bmatrix}3&4\\2&3\\1&1\end{bmatrix}$ as a map, $\mathbb{R}^2 \to \mathbb{R}^3$

$$\begin{bmatrix}1\\0\end{bmatrix}\mapsto\begin{bmatrix}3\\2\\1\end{bmatrix} \qquad \begin{bmatrix}0\\1\end{bmatrix}\mapsto\begin{bmatrix}4\\3\\1\end{bmatrix} \qquad \begin{bmatrix}1\\1\end{bmatrix}\mapsto\begin{bmatrix}7\\5\\2\end{bmatrix}$$

Application: Fun with Fibonacci

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...

Fibonacci sequence:

$F_0 = 0, \quad F_1 = 1, \quad F_k = F_{k-1} + F_{k-2}.$

There's a direct formula for F_k:

$$F_k = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k$$

You could prove that by induction.
But how would you come up with it?!

Fibonacci via Linear Algebra

Fibonacci sequence:

$F_0 = 0, \quad F_1 = 1, \quad F_k = F_{k-1} + F_{k-2}.$

To get the next, you only need to know last two.

Let's stack the the last two into a vector:

$$\begin{bmatrix}F_{k-1}\\F_{k-2}\end{bmatrix}\overset{?}{\mapsto}\begin{bmatrix}F_k\\F_{k-1}\end{bmatrix}$$

$$\begin{bmatrix}F_k\\F_{k-1}\end{bmatrix}=\begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}F_{k-1}\\F_{k-2}\end{bmatrix}$$

Fibonacci via Linear Algebra

$$\begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}1\\1\end{bmatrix} \qquad \begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}=\begin{bmatrix}2\\1\end{bmatrix}$$

$$\begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}2\\1\end{bmatrix}=\begin{bmatrix}3\\2\end{bmatrix} \qquad \begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}3\\2\end{bmatrix}=\begin{bmatrix}5\\3\end{bmatrix}$$

$$\begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}5\\3\end{bmatrix}=\begin{bmatrix}8\\5\end{bmatrix}$$

$$\begin{bmatrix}1&1\\1&0\end{bmatrix}^5\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}8\\5\end{bmatrix}$$

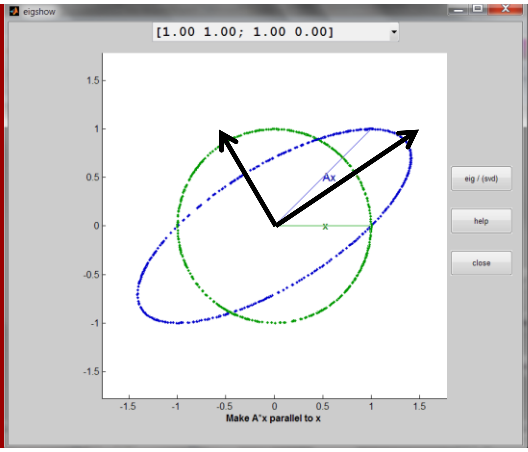
$$\begin{bmatrix}1&1\\1&0\end{bmatrix}^k\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}F_{k+1}\\F_k\end{bmatrix}$$

Fibonacci via Linear Algebra

We can think of $A=\begin{bmatrix}1&1\\1&0\end{bmatrix}$ as a map, $\mathbb{R}^2 \to \mathbb{R}^2$.

What does this map look like?

To the computer!



Fibonacci via Linear Algebra

Two 'interesting' directions, which A just scales.

They satisfy $\begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}=\lambda\begin{bmatrix}x\\y\end{bmatrix}$

(from the picture, $\lambda \approx 1.6, -0.6$)

How can we solve for x, y, λ?
(2 equations, 3 unknowns)

If (x,y) is a solution, so is (2x,2y), (3x,3y), (¼x,¼y)…

WLOG, fix y = 1.

Fibonacci via Linear Algebra

Two 'interesting' directions, which A just scales.

They satisfy $\begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}x\\1\end{bmatrix}=\lambda\begin{bmatrix}x\\1\end{bmatrix}$

WLOG, fix y = 1. $\Leftrightarrow \begin{array}{c}x+1=\lambda x\\ x=\lambda\end{array}$

$\Leftrightarrow$ x=λ solves $x^2-x-1=0$

$\Leftrightarrow x=\lambda=\dfrac{1\pm\sqrt{5}}{2}$

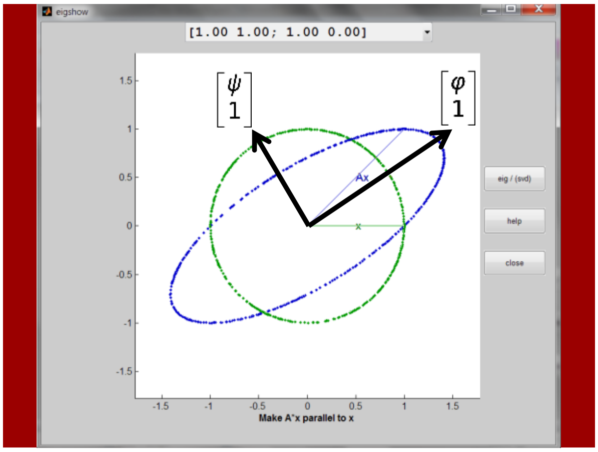
Fibonacci via Linear Algebra

Define: $\varphi=\frac{1+\sqrt{5}}{2}\approx 1.618$, $\psi=\frac{1-\sqrt{5}}{2}\approx -.618$

We just showed: $\begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}\varphi\\1\end{bmatrix}=\varphi\cdot\begin{bmatrix}\varphi\\1\end{bmatrix}$

$\begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}\psi\\1\end{bmatrix}=\psi\cdot\begin{bmatrix}\psi\\1\end{bmatrix}$

(The 'interesting' directions are called *eigenvectors* and the scaling factors are called *eigenvalues*.)



Fibonacci via Linear Algebra

Define: $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618, \quad \psi = \frac{1-\sqrt{5}}{2} \approx -.618$

We just showed: $\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\varphi\\1\end{bmatrix} = \varphi \cdot \begin{bmatrix}\varphi\\1\end{bmatrix}$

$\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\psi\\1\end{bmatrix} = \psi \cdot \begin{bmatrix}\psi\\1\end{bmatrix}$

Hence: $\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}^k\begin{bmatrix}\varphi\\1\end{bmatrix} = \varphi^k \cdot \begin{bmatrix}\varphi\\1\end{bmatrix}$

$$\begin{bmatrix}1.618\\1\end{bmatrix} \mapsto \begin{bmatrix}2.618\\1.618\end{bmatrix} \mapsto \begin{bmatrix}4.236\\2.618\end{bmatrix} \mapsto \begin{bmatrix}6.854\\4.236\end{bmatrix} \mapsto \begin{bmatrix}11.090\\6.854\end{bmatrix}$$

Fibonacci via Linear Algebra

Define: $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618, \quad \psi = \frac{1-\sqrt{5}}{2} \approx -.618$

We just showed: $\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\varphi\\1\end{bmatrix} = \varphi \cdot \begin{bmatrix}\varphi\\1\end{bmatrix}$

$\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\psi\\1\end{bmatrix} = \psi \cdot \begin{bmatrix}\psi\\1\end{bmatrix}$

Hence: $\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}^k\begin{bmatrix}\psi\\1\end{bmatrix} = \psi^k \cdot \begin{bmatrix}\psi\\1\end{bmatrix}$

$$\begin{bmatrix}-0.618\\1\end{bmatrix} \mapsto \begin{bmatrix}0.382\\-0.618\end{bmatrix} \mapsto \begin{bmatrix}-0.236\\0.382\end{bmatrix} \mapsto \begin{bmatrix}0.146\\-0.236\end{bmatrix}$$

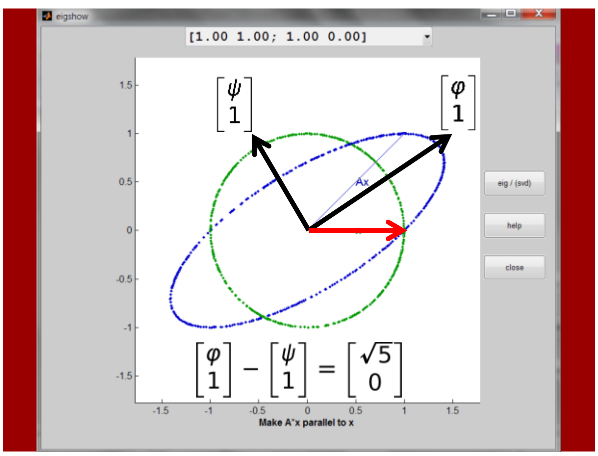
Fibonacci via Linear Algebra

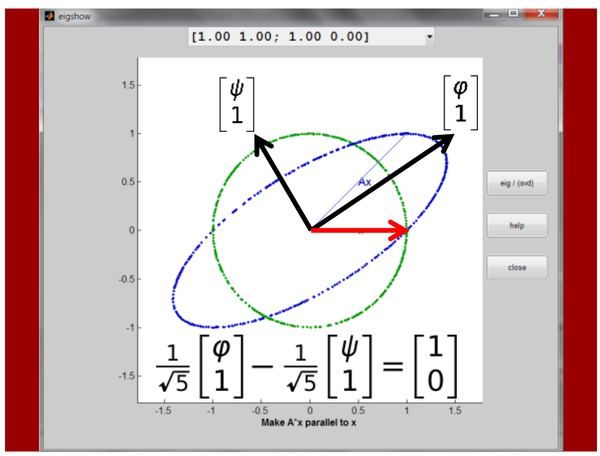
Define: $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618, \quad \psi = \frac{1-\sqrt{5}}{2} \approx -.618$

We just showed: $\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\varphi\\1\end{bmatrix} = \varphi \cdot \begin{bmatrix}\varphi\\1\end{bmatrix}$

$\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\psi\\1\end{bmatrix} = \psi \cdot \begin{bmatrix}\psi\\1\end{bmatrix}$

Hence: $\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}^k\begin{bmatrix}1\\0\end{bmatrix} = ??$





Fibonacci via Linear Algebra

Define: $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618$, $\psi = \frac{1-\sqrt{5}}{2} \approx -.618$

$$\begin{bmatrix}1&1\\1&0\end{bmatrix}^k \begin{bmatrix}\varphi\\1\end{bmatrix} = \varphi^k \cdot \begin{bmatrix}\varphi\\1\end{bmatrix} \qquad \begin{bmatrix}1&1\\1&0\end{bmatrix}^k \begin{bmatrix}\psi\\1\end{bmatrix} = \psi^k \cdot \begin{bmatrix}\psi\\1\end{bmatrix}$$

$$\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{5}}\begin{bmatrix}\varphi\\1\end{bmatrix} - \frac{1}{\sqrt{5}}\begin{bmatrix}\psi\\1\end{bmatrix}$$

$$\begin{bmatrix}F_{k+1}\\F_k\end{bmatrix} = \begin{bmatrix}1&1\\1&0\end{bmatrix}^k \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1&1\\1&0\end{bmatrix}^k \left(\frac{1}{\sqrt{5}}\begin{bmatrix}\varphi\\1\end{bmatrix} - \frac{1}{\sqrt{5}}\begin{bmatrix}\psi\\1\end{bmatrix}\right)$$
$$= \frac{1}{\sqrt{5}} \cdot \varphi^k \begin{bmatrix}\varphi\\1\end{bmatrix} - \frac{1}{\sqrt{5}} \cdot \psi^k \begin{bmatrix}\psi\\1\end{bmatrix}$$

Fibonacci via Linear Algebra

Define: $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618$, $\psi = \frac{1-\sqrt{5}}{2} \approx -.618$

$$\therefore \quad \boxed{F_k = \frac{1}{\sqrt{5}}\varphi^k - \frac{1}{\sqrt{5}}\psi^k}$$

$$\begin{bmatrix}F_{k+1}\\F_k\end{bmatrix} = \begin{bmatrix}1&1\\1&0\end{bmatrix}^k \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1&1\\1&0\end{bmatrix}^k \left(\frac{1}{\sqrt{5}}\begin{bmatrix}\varphi\\1\end{bmatrix} - \frac{1}{\sqrt{5}}\begin{bmatrix}\psi\\1\end{bmatrix}\right)$$
$$= \frac{1}{\sqrt{5}} \cdot \varphi^k \begin{bmatrix}\varphi\\1\end{bmatrix} - \frac{1}{\sqrt{5}} \cdot \psi^k \begin{bmatrix}\psi\\1\end{bmatrix}$$

More on linear combinations

A key step: expressing $\begin{bmatrix}1\\0\end{bmatrix}$ as a linear combination of $\begin{bmatrix}\varphi\\1\end{bmatrix}$ and $\begin{bmatrix}\psi\\1\end{bmatrix}$

More generally:

We often fix a small number of vectors and ask:

What can we get by taking linear combinations?

Definition:

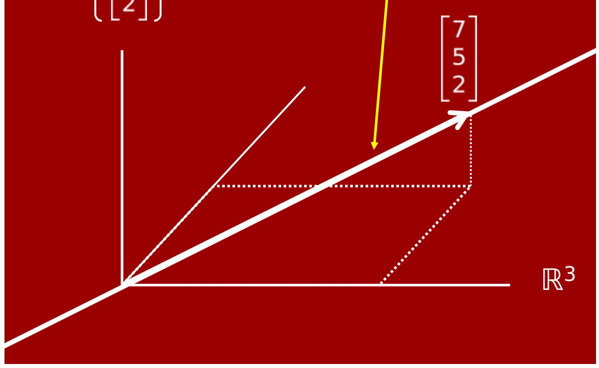
The **span** of a set of vectors $S=\{v_1, \ldots, v_k\}$, is the set of all linear combinations of them.

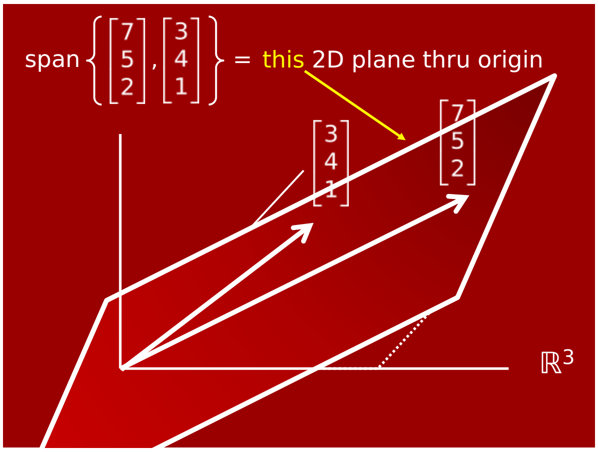
$$\text{span}(\{v_1,v_2,v_3\}) = \left\{ \begin{bmatrix} \vdots & \vdots & \vdots \\ v_1 & v_2 & v_3 \\ \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix}c_1\\c_2\\c_3\end{bmatrix} : c_1,c_2,c_3 \in F \right\}$$

k = 0 technicality: span(∅) = {the 0 vector}

Let's do some examples in $\mathbb{R}^3$.

$\text{span}\left\{\begin{bmatrix}7\\5\\2\end{bmatrix}\right\}$ = all vectors on this line thru origin





A span example in $\mathbb{F}_2^n$

Remember:

$\mathbb{F}_2$ is the 2-element field (integers mod 2).
$\mathbb{F}_2^n$ is all length-n vectors over this field.

E.g., $\mathbb{F}_2^7$ has 128 vectors. Here's a linear combination:

$$1\cdot\begin{bmatrix}0\\1\\1\\0\\0\\0\\1\end{bmatrix}+1\cdot\begin{bmatrix}1\\1\\0\\1\\1\\0\\1\end{bmatrix}=\begin{bmatrix}1\\0\\1\\1\\1\\0\\0\end{bmatrix}$$

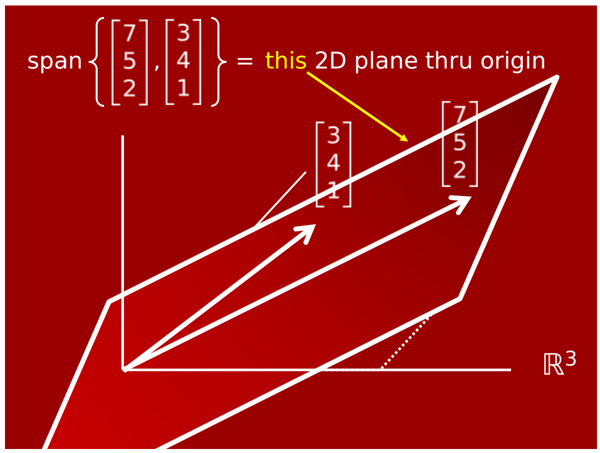
(Note: only two possible scalars, 0 and 1.)

A span example in $\mathbb{F}_2^n$

Here are n−1 vectors in $\mathbb{F}_2^n$:

$$E = \text{span}\left\{\begin{bmatrix}1\\0\\0\\\cdots\\0\\0\\1\end{bmatrix},\begin{bmatrix}0\\1\\0\\\cdots\\0\\0\\1\end{bmatrix},\begin{bmatrix}0\\0\\1\\\cdots\\0\\0\\1\end{bmatrix},\ldots,\begin{bmatrix}0\\0\\0\\\cdots\\0\\1\\1\end{bmatrix}\right\} = ??$$

Claim: E = {all vectors with an **even** # of 1's}.



Vector spaces/subspaces

In $\mathbb{R}^3$, a span of 2 vectors (not on the same line) is a 2D plane through the origin.

A 2D plane is kind of 'like' a copy of $\mathbb{R}^2$.

It's a closed space where vectors can hang out.

Let's make this a bit more formal.

Vector spaces/subspaces

Definition:

Let S be a set of vectors in F^n.
The set V = span(S) is called a *subspace* of F^n.
We may also just call it a *vector space*.

Equivalently:

$V \subseteq F^n$ is a subspace if and only if it is "closed under linear combinations".

(I.e., the linear combination of vectors in V is always also in V.)

Vector subspace example #1

$$E = \text{span}\left\{ \begin{bmatrix}1\\0\\0\\\cdots\\0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\0\\\cdots\\0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\0\\1\\\cdots\\0\\0\\1\end{bmatrix}, \ldots, \begin{bmatrix}0\\0\\0\\\cdots\\0\\1\\1\end{bmatrix} \right\}$$

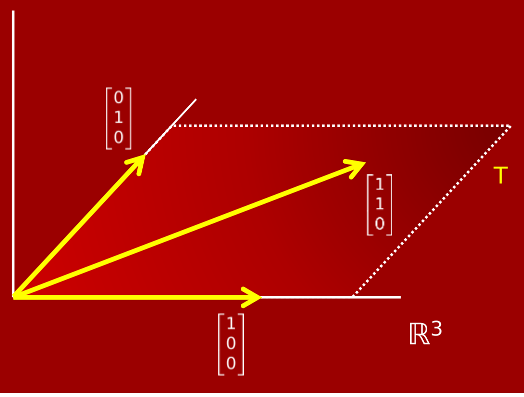
$= \{$all vectors in $\mathbb{F}_2^n$ with an **even** # of 1's$\}$.

This is a vector space.
It's closed under linear combinations:
the sum of any set of vectors in E is in E.

Vector subspace example #2

Let $u = \begin{bmatrix}1\\0\\0\end{bmatrix}$, $v = \begin{bmatrix}0\\1\\0\end{bmatrix}$, $w = \begin{bmatrix}1\\1\\0\end{bmatrix} \in \mathbb{R}^3$

$T = \text{span}(\{u,v,w\}) = \{x \in \mathbb{R}^3 : x_3 = 0\}$



Vector subspace example #2

Let $u = \begin{bmatrix}1\\0\\0\end{bmatrix}$, $v = \begin{bmatrix}0\\1\\0\end{bmatrix}$, $w = \begin{bmatrix}1\\1\\0\end{bmatrix} \in \mathbb{R}^3$

$T = \text{span}(\{u,v,w\}) = \{x \in \mathbb{R}^3 : x_3 = 0\}$

Subspace T is also the span of any 2 of $\{u,v,w\}$.

The spanning set $\{u,v,w\}$ is a bit redundant.

We would prefer an 'irredundant' set.

Linear independence

$S \subseteq V$ is linearly independent if no $v \in S$ is in the span of $S \setminus \{v\}$.

$\mathbb{R}^3$ example: Let $u = \begin{bmatrix}1\\0\\0\end{bmatrix}$, $v = \begin{bmatrix}0\\1\\0\end{bmatrix}$, $w = \begin{bmatrix}1\\1\\0\end{bmatrix}$.

- $\{u,v,w\}$: not linearly independent ('linearly dependent')
- $\{u,v\}$: linearly independent. As are $\{u,w\}$, $\{v,w\}$
- $\{u\}$: linearly independent
- $\{0\}$: not linearly independent } edge cases
- $\varnothing$: linearly independent } edge cases

Linear independence

Let $S = \{s_1, \ldots, s_d\} \subseteq F^n$ be linearly independent.
Let W be the subspace span(S).

Theorem: Every $v \in W$ is a *unique* linear combination of vectors in S.

Proof:

Suppose $v = a_1 s_1 + \cdots + a_d s_d$ & $v = b_1 s_1 + \cdots + b_d s_d$.

Want to prove $a_i = b_i$ $\forall i$. Suppose otherwise; say $a_k \neq b_k$.

WLOG, $k = 1$. Now subtract the two representations of v:

$0 = (a_1 - b_1) s_1 + (a_2 - b_2) s_2 + \cdots + (a_d - b_d) s_d$

$\Rightarrow s_1 = -\frac{a_2 - b_2}{a_1 - b_1} s_2 - \cdots - \frac{a_d - b_d}{a_1 - b_1} s_d$, contradicting S lin. indep.

Linear independence

Let $S = \{s_1, \dots, s_d\} \subseteq F^n$ be linearly independent.
Let W be the subspace span(S).

Theorem: Every $v \in W$ is a *unique* linear combination of vectors in S.

We say that S is a **basis** for W.

A basis for a vector space is a **spanning** and **linearly independent** set.

A nontrivial Linear Algebra theorem

Theorem:
Let V be a vector (sub)space.
Every basis of V has the same # of vectors.

Definition: We call this V's **dimension**, dim(V).

Proof: Suppose $L \subseteq V$ is linearly independent
and $S \subseteq V$ is spanning for V.
We will prove $|L| \le |S|$.

Then if T_1, T_2 are bases (lin. indep. & spanning), we have $|T_1| \le |T_2|$ and $|T_2| \le |T_1|$; i.e., $|T_1|=|T_2|$.

Claim: Suppose $L \subseteq V$ is linearly independent
and $S = \{s_1, \dots, s_d\} \subseteq V$ is spanning for V.
Then $|L| \le |S| = d$.

Proof:
Take $\ell_1 \in L$ and delete it from L.
ℓ_1 is a nonzero (why?) linear combo of vectors from S:

$$\ell_1 = a_1 s_1 + a_2 s_2 + \cdots + a_d s_d$$

WLOG, $a_1 \ne 0$. So s_1 is a linear combo of $\ell_1, s_2, \dots, s_d$.
Now redefine $S = \{\ell_1, s_2, \dots, s_d\}$, still spans V.

Claim: Suppose $L \subseteq V$ is linearly independent
and $S = \{s_1, \dots, s_d\} \subseteq V$ is spanning for V.
Then $|L| \le |S| = d$.

Proof:
Take $\ell_2 \in L$ and delete it from L.
ℓ_2 is a linear combo of vectors from S:

$$\ell_2 = b_1 \ell_1 + b_2 s_2 + \cdots + b_n s_d$$

Some $b_i \ne 0$ for $i \ge 2$ (else L not linearly independent).
WLOG, assume $b_2 \ne 0$.
So s_2 is a linear combo of $\ell_1, \ell_2, s_3, \dots, s_d$.

$S = \{\ell_1, s_2, \dots, s_d\}$ still spans V.

Claim: Suppose $L \subseteq V$ is linearly independent
and $S = \{s_1, \dots, s_d\} \subseteq V$ is spanning for V.
Then $|L| \le |S| = d$.

Proof:
Take $\ell_2 \in L$ and delete it from L.
ℓ_2 is a linear combo of vectors from S:

$$\ell_2 = b_1 \ell_1 + b_2 s_2 + \cdots + b_n s_d$$

Some $b_i \ne 0$ for $i \ge 2$ (else L not linearly independent).
WLOG, assume $b_2 \ne 0$.
So s_2 is a linear combo of $\ell_1, \ell_2, s_3, \dots, s_d$.
Now redefine $S = \{\ell_1, \ell_2, s_3, \dots, s_d\}$, still spans V.

Repeat, until all of L is deleted.
But S always has d vectors. $\therefore$ initially, $|L| \le d$. □

Enough linear algebra theory.

Let's see another application.

Sending messages on a noisy channel

Alice

Um, what if $d+2k+1 > 257$?

Message: $d+1$ symbols from $\mathbb{F}_{257}$

Reed–Solomon: To guard against k corruptions, treat message as coeffs of poly P, send P(1), P(2), …, P(d+2k+1)

Sending messages on a noisy channel

Alice

Um, what if $d+2k+1 > 257$?

What if the noisy channel corrupts **bits**, not bytes?

from $\mathbb{F}_{257}$

against k corruptions, essage as coeffs of poly P, send P(1), P(2), …, P(d+2k+1)

Sending messages on a noisy channel

Alice wants to send an n-bit message to Bob.

The channel may flip up to k bits.

How can Alice get the message across?

Sending messages on a noisy channel

Alice wants to send an $(n-1)$-bit message to Bob.

The channel may flip up to 1 bit.

How can Alice get the message across?

Q1: How can Bob detect if there's been a bit-flip?

Parity-check solution

Alice tacks on a bit, equal to the parity (sum mod 2) of the message's $n-1$ bits.

Alice's n-bit 'encoding' always has an even number of 1's.

Bob can detect if the channel flips a bit: if he receives a string with an odd # of 1's.

1-bit error-detection for 2^{n-1} messages by sending n bits: optimal! (exercise)

Linear Algebra perspective

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{n-1} \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_{n-1} \\ y_n \end{bmatrix}$$

G: an $n\times(n-1)$ 'generator' matrix

Alice's message $x \in \mathbb{F}_2^{n-1}$

Alice transmits

Linear Algebra perspective

Let C be the set of strings Alice may transmit.

C is the span of the columns of G.

I.e., C is an $(n-1)$-dimensional subspace of $\mathbb{F}_2^n$.

Linear Algebra perspective

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ \vdots \\ z_{n-1} \\ z_n \end{bmatrix} \stackrel{?}{=} 0$$

H: a 1×n 'parity check' matrix

Bob receives

Bob checks this to detect if no errors

Solves 1-bit error detection, but not correction

If Bob sees $z = (1, 0, 0, 0, 0, 0, 0)$,

did Alice send $y = (0, 0, 0, 0, 0, 0, 0)$,
or $y = (1, 1, 0, 0, 0, 0, 0)$,
or $y = (1, 0, 1, 0, 0, 0, 0)$,
or… ?

The Hamming(7,4) Code

Alice sends 4-bit messages using 7 bits.

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

Alice encodes $x \in \mathbb{F}_2^4$ by Gx,

which looks like x followed by 3 extra bits.

The Hamming(7,4) Code

Alice sends 4-bit messages using 7 bits.

Any 'codeword' $y = Gx$ satisfies some 'parity checks':

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

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

$Hy = 0$, because $HG = 0$.

The Hamming(7,4) Code

Alice sends 4-bit messages using 7 bits.

Columns are 1…7 in binary!

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

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

$Hy = 0$, because $HG = 0$.

The Hamming(7,4) Code

On receiving $z \in \mathbb{F}_2^7$, Bob computes Hz.

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

If no errors, $z = Gx$, so $Hz = HGx = 0$.

If jth coordinate corrupted, $z = Gx+e_j$.

(vector with 1 in j^{th} coordinate, 0's else)

Then $Hz = H(Gx+e_j) = HGx + He_j$

$= He_j$ = (jth col. of H) = bin. rep. of j

Bob knows where the error is, can recover msg!

The General Hamming Code

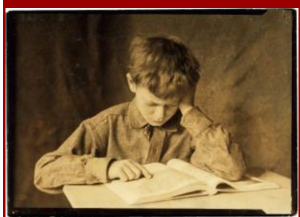
By sending $n = 7$ bits, Alice can communicate one of 16 messages, guarding against 1 error.

This scheme generalizes: Let $n = 2^r-1$,
take H to be the $r\times(2^r-1)$ matrix whose columns are the numbers $1\ldots2^r$ in binary.

The appropriate G has $2^r-1-r = n-\log_2(n+1)$ columns, meaning Alice can communicate one of $2^n/(n+1)$ messages (using n bits).

Fact: This is optimal for guarding against 1 error!

Study Guide



Definitions:
- Span
- Vector (sub)space
- Linear independence
- Basis
- Subspace
- Dimension

Ideas:
- Solving Fibonacci recurrence.
- Hamming Code.