Math 127, Mon Mar 01

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: 5.1, 5.2, 5.3 (reload book).
- Reading for Wed: 5.4, 5.5 (to be rewritten; reload again).
- PS04 outline due Wed, full version due Mon Mar 08.
- Problem session Fri Mar 05, 10am–noon.

A data compression problem

bitstrings of length 5

Consider $\mathcal{C} = \{a, b, c, d, e, f, g, h\}$:

$$a = 00000 \quad b = 00111 \quad c = 01011 \quad d = 01100$$
$$e = 10010 \quad f = 10101 \quad g = 11001 \quad h = 11110$$

closure prop

Notable property of $\mathcal{C}$: Closed under bitwise addition (mod 2).

Example:

$$\begin{array}{r} e = 10010 \\ g = 11001 \\ \hline 01011 \end{array} = c$$

$1+1=0 \pmod 2$

(aka XOR)

Same works for any pair of bitstrings in C.

Note: If we just want to remember all bitstrings in C, we didn't need to write down bitstring c -- can recover from e,g and closure.

Motivating Problem

What is the *smallest* number of bitstrings of $\mathcal{C}$ from which we could recover all of $\mathcal{C}$, just by knowing that $\mathcal{C}$ has the closure property?

Turns out:

{d,e,g} works
{d,e} doesn't work - only get {a,d,e,h}
{d,e,h} doesn't work, same result

Some questions that arise

Call a set of bitstrings $\mathcal{B}$ a **minimal recovery set** if we can recover $\mathcal{C}$ from $\mathcal{B}$ and the closure property, but if you remove any element of $\mathcal{B}$, this is no longer true.

Example: $\{b, c, g\}$ is a minimal recovery set; $\{b, c, g, h\}$ isn't minimal; can't recover from $\{b, c\}$ or $\{b, c, d\}$.

Motivating Problem

How can you tell if you can recover $\mathcal{C}$ from a given set of bitstrings? Better than adding until we can't? span

method

Motivating Problem

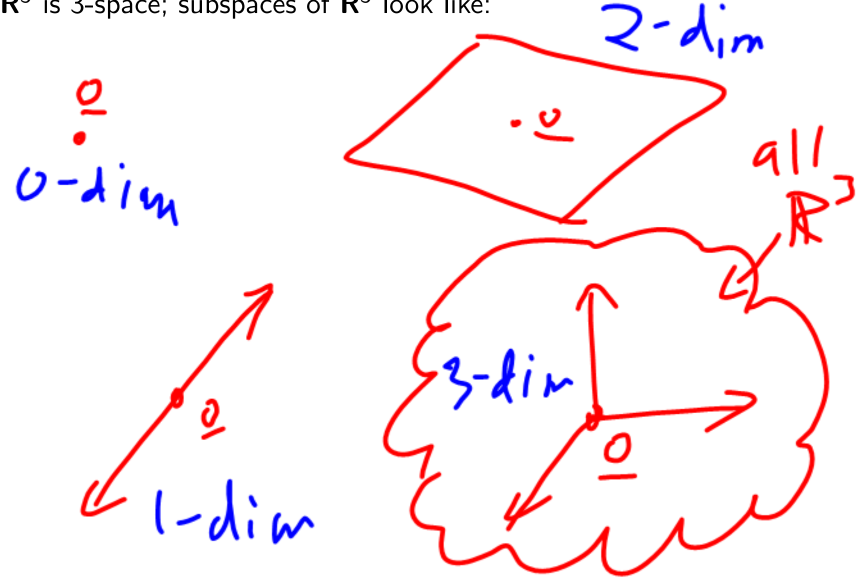
What's an efficient way to tell if $\mathcal{B}$ is minimal? lin ind

Motivating Problem

Are all minimal recovery sets the same size, or are some minimal recovery sets size 3 and others (say) size 2? dim?

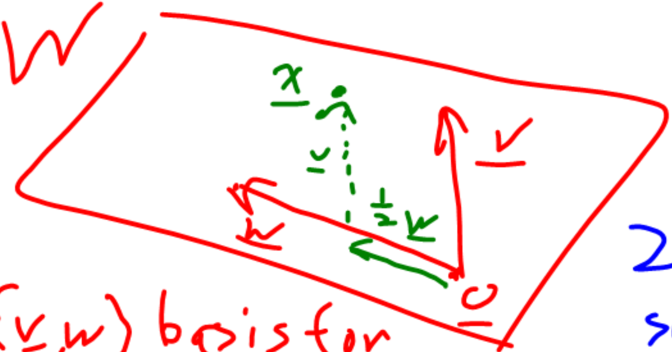
Subspaces of $\mathbf{R}^3$

$\mathbf{R}^3$ is 3-space; subspaces of $\mathbf{R}^3$ look like:



Bases define coordinates

If a subspace W has dimension d, then you can find d vectors that define unique coordinates for each point of W:



2-d subsp

$\{\underline{v}, \underline{w}\}$ basis for W

$\underline{x} = 1\underline{v} + \frac{1}{2}\underline{w}$ coords: $(1, \frac{1}{2})$

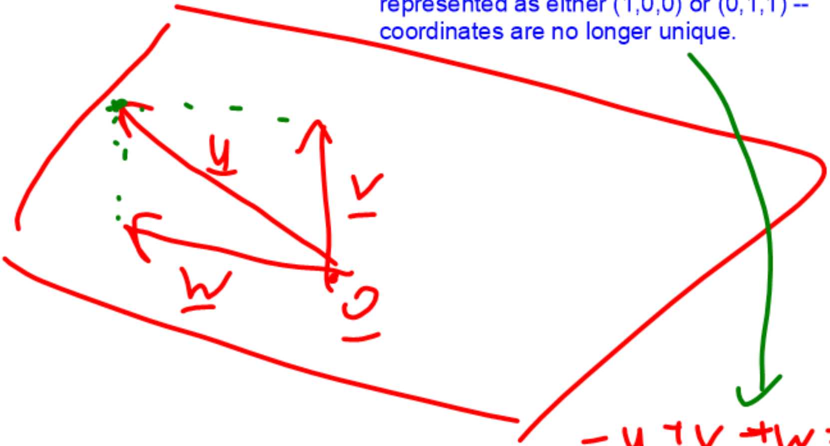
We can think of a basis as being infinite data compression: We can represent the infinitely many points of W using just the two vectors v and w.

A linearly dependent set doesn't define coordinates

efficient

If you have too many vectors, the coordinates you define won't be unique anymore:

So in {u,v,w} coordinates, the point u can be represented as either (1,0,0) or (0,1,1) -- coordinates are no longer unique.



$-\underline{u} + \underline{v} + \underline{w} = \underline{0}$

Problem is that these vectors are **linearly dependent**.

Idea (almost defn-thm) of a basis

Upshot:

> A basis for a subspace W is a linearly independent set that also spans W. You can use a basis for W to describe exactly which vectors are contained in W in terms of coordinates.
>
> Infinite data compression!

And that's linear algebra! (Or at least the money-making parts.) But we'll consider a more abstract version, replacing $\mathbf{R}$ with an arbitrary field F, that allows us to solve today's first batch of problems (minimal recovery sets) as well.

$F = \mathbb{F}_2 = \{0, 1\}$

The space F^n

For ($F = \mathbb{R}$, $F^n = \mathbb{R}^n$)

Let F be a field and $n \in \mathbf{N}$. We define

$F = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p$

$$F^n = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \middle| x_i \in F \right\},$$

Elements of F^n called **vectors**. Vector addition:

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix}.$$

Scalar multiplication:

$a \in F$

$$a \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} ax_1 \\ \vdots \\ ax_n \end{bmatrix}.$$

Subspaces of F^n

Definition

For $n \in \mathbf{N}$, a **subspace** of F^n is $W \subseteq F^n$ s.t.:

1. W contains the zero vector $\mathbf{0}$;
2. (Closed under $+$) For any $\mathbf{v}, \mathbf{w} \in W$, we have $\mathbf{v} + \mathbf{w} \in W$; and
3. (Closed under scalar multiplication) For any $\mathbf{v} \in W$ and $a \in F$, we have $a\mathbf{v} \in W$.

Not super-interesting examples: $\{\mathbf{0}\}$, F^n.

Special case: $F = \mathbf{F}_2$

$\mathcal{C} = \left\{ \begin{array}{llll} a = 00000 & b = 00111 & c = 01011 & d = 01100 \\ e = 10010 & f = 10101 & g = 11001 & h = 11110 \end{array} \right\}$

$\mathcal{C}$ in $\mathbb{F}_2^5$

In $\mathbf{F}_2^n$:

- Vectors are **bitstrings** of length n.
- Vector addition is bitwise addition (mod 2), just like at the beginning of class.
- The only scalars in $\mathbf{F}_2$ are $0, 1$, so scalar mult not very interesting.
- So W is a subspace of $\mathbf{F}_2^n$ if and only if W contains 0 and is closed under vector addition, e.g., the set $\mathcal{C}$ we saw at the beginning of class.

Minimal recovery sets?

F-linear combinations

Let $\mathbf{v}_1, \ldots, \mathbf{v}_k$ be vectors in F^n. A **linear combination** of $\mathbf{v}_1, \ldots, \mathbf{v}_k$ is a vector of the form

$$a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k$$

for $a_i \in F$.

- a_i are **coefficients** of lin comb.
- If all $a_i = 0$, **trivial** lin comb.
- Otherwise, **nontrivial** lin comb.

(at least one $a_i \neq 0$)

What it means for a set to span W

$\mathbf{v}_1, \ldots, \mathbf{v}_k$ vectors in F^n, W a subspace of F^n.
Span of $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is

all possible lin combs of {v_1,...,v_k}

noun

$$\operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\} = \{a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k \mid a_i \in F\}.$$

To say that $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ **spans** W means both of the following hold:

verb

1. Each of the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ is contained in W.
2. Every $\mathbf{x} \in W$ is a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_k$.

(Ie, $W = \operatorname{span}\{\underline{v}_1, \ldots, \underline{v}_k\}$)

What it means for a set to be linearly independent

$\mathbf{v}_1, \ldots, \mathbf{v}_k$ vectors in F^n.

To say $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is **linearly dependent** means that

$$a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k = \mathbf{0} \tag{1}$$

for some choice of coefficients $a_1, \ldots, a_k \in F$, not all of which are 0. (nontriv l.c. $= \underline{0}$)

Opposite: To say that $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ **linearly independent** means that the only time that (1) holds is when all of the a_i are equal to 0. I.e., lin ind means:

$$\textbf{If } (1), \textbf{ then } \text{all } a_i = 0.$$

Only l.c. of v_1,...,v_k that is equal to 0 is the trivial l.c.

<u>Ex</u>. $\mathbb{F}_2^5$ has 2^5 vecs:

all 00000,
00001,
... (30 more)

$\mathcal{E} = \{00000, 00111,$
$\ldots\}$ has 8 vecs

$b, c, g \in \mathcal{E}$.

Can check (brute force):

$\to \{b, c, g\}$ span $\mathcal{E}$

$\to \{b, c, g\}$ lin ind.

$\boxed{\beta b + \gamma c + \eta g \text{ 8 l.c.s.}}$

Basis, dimension, coordinates

W subspace of F^n.

A **basis** for W is a linearly independent subset $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ of W that also spans W.

$\dim W = k$ means that W has a basis with k vectors in it.

Theorem

$\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a basis for W. Then for every $\mathbf{w} \in W$, there exists unique $a_1, \ldots, a_k \in F$ s.t.

$$\mathbf{w} = a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k.$$

Proof:

What could possibly go wrong?

- Is it possible for a subspace W to have one basis with 5 vectors and another basis with 7 vectors? In other words, is it possible for the dimension of W to be both 5 and 7?
- Is it possible for F^8 to contain a subspace of dimension 10? In other words, is it possible for a smaller space to have a larger dimension?
- Can we find a subspace of F^n that doesn't have a basis at all?

What do we need to compute?

- Given a subspace W of F^n and vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ that span W, how can we check that $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is a basis for W?
- Given a subspace W of F^n, how can we find a basis for W?
- Given a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ for a subspace W of F^n, and a vector $\mathbf{v}$ in F^n, how can we determine if $\mathbf{v}$ is in W?