RSA

- In Diffie-Hellman, two parties agree on a shared key. RSA keys are <u>asymmetric</u>.

First some prereqs.

<u>Def</u> a and b are <u>coprime</u> if they have no common factors other than 1.

e.g. 7 and 15 coprime ✓

12 and 15 not coprime: both mults of 3.

<u>Def</u> the Euler φ function (also called <u>totient</u>) is

$$\varphi(n) = \#\{k \text{ such that } k \text{ is coprime to } n\}, \quad 1 \le k \le n$$

<u>ex</u> $\varphi(12)$

1 ~~2~~ ~~3~~ ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~

$\varphi(12) = 4$

$\varphi(10) = 4$

1 2 3 4 5 6 7 8 9 10

$\varphi(13) = 12$

1 2 3 4 5 6 7 8 9 10 11 12 ~~13~~

everything coprime to it, since 13 is prime!

$\varphi(p) = p - 1$

Same reason

Only things not coprime to pq are mults of p, mults of q

$$\varphi(pq) = \underbrace{pq}_{\text{all numbers}} - \underbrace{p}_{\substack{\text{mults of } q \\ q, 2q, 3q, 4q, \ldots pq}} - \underbrace{q}_{\text{mults of } p} + \underbrace{1}_{\substack{pq \text{ itself was} \\ \text{double-counted}}}$$

$$= (p-1)(q-1)$$

One fact.

Suppose b and n are coprime. Then there exists a unique $1 \le a \le n$ such that $ab \equiv 1 \bmod n$.

a is the "inverse of b modulo n"

Ex $n=25$, $b=12$

Looking for a so $ab \equiv 1 \bmod 25$

a	1	2	3	4	5	6	7	8 ...
$12a$:	12,	24,	36,	48,	60, ...			
$12a \bmod 25$		$-1 \bmod 25$.						

$a=-2$ works! But $-2 \equiv 23 \bmod 25$,

so $a=23$ works.

Check: $23 \times 12 = 276 \equiv 275 + 1 \equiv 1 \bmod 25$

Ex $n=7$, $b=3$.

Find a so $ab \equiv 1 \bmod n$.

Sol: Check multiples of 3 until you get $1 \bmod 7$

$3, 6, 9, 12, \underline{15}, 18$

$15 \equiv 1 \bmod 7$.

$\underline{a=5}$

Fermat's Little Theorem

Suppose b and n are positive and coprime, then $b^{\varphi(n)} \equiv 1 \bmod n$.

---

e.g. n is prime: $b^{n-1} \equiv 1 \bmod n$

$n=10$ $\quad b^4 \equiv 1 \bmod 10$

b coprime to 10 means last digit $1, 3, 7, 9$

Proof warm-up:

$n=10, \quad b=3.$

Make a list of all numbers less than 10, coprime to 10

$$1 \quad 3 \quad 7 \quad 9 \xrightarrow[\text{mod } 10]{\text{product is}} 9$$

multiply all by b, take result mod 10

$$\begin{array}{cccc} 3\cdot 1 & 3\cdot 3 & 3\cdot 7 & 3\cdot 9 \\ \| & \| & \| & \| \\ 3 & 9 & 1 & 7 \end{array} \longrightarrow 3^4 \cdot 9$$

$$3 \; 9 \; 1 \; 7 \longrightarrow \text{also } 9 \text{ (same list!)}$$

same as original list, scrambled

$3^4 \cdot 9 \equiv 9 \mod 10.$ Multiply by inverse of 9 mod 10

$3^4 \equiv 1 \mod 10$

"Official" proof $\quad b^{\varphi(n)} \equiv 1 \mod n$

Make a list of all numbers less than n, coprime to n:

$$a_1, a_2, a_3, \ldots, a_{\varphi(n)}.$$

Multiply everything in list by $b \pmod n$.

$r_i = ba_i \mod n$. New list:

$$r_1, r_2, r_3, \ldots, r_{\varphi(n)}.$$

I claim this is just original list, scrambled.

Why no duplicates in new list?

If $r_1 = r_2$ (for example)

Then $ba_1 \equiv ba_2 \mod n$. Let c inverse of $b \mod n$.

$$\underbrace{cb}_{1}a_1 \equiv \underbrace{cb}_{1}a_2 \mod n$$

$$a_1 \equiv a_2 \mod n.$$

So

$$a_1 \cdots a_{\varphi(n)} = r_1 \cdots r_{\varphi(n)}$$

$$a_1 \cdots a_{\varphi(n)} = (ba_1) \cdots (ba_{\varphi(n)})$$

$$\prod a_i \equiv b^{\varphi(n)} \left(\prod a_i\right) \mod n$$

$$b^{\varphi(n)} \equiv 1 \mod n.$$

RSA

The person receiving encrypted messages chooses two really big prime numbers, p and q.

~150 digits.

computes product $n = pq$.

Picks an encyption key "e"

(in real life, $e = 65537$) often

Compute $\varphi(n) = (p-1)(q-1)$

Compute inverse of e mod $\varphi(n)$.

This is d so $de \equiv 1 \bmod \varphi(n)$.

Publicly announce: n, e

Keep secret: p, q, d.

How to check if p prime?

Compute $2^{p-1} \bmod p$.

If not $1 \bmod p$, not prime!

"Pseudoprime test"

Nemesis

~~They~~ could try to factor n and find p, q.

But n is so big this is impractical!

If you want to send a message:

- Represent it as a number M.
- Compute $E = M^e \bmod n$. (fast!)

E is the encrypted message!

To decrypt:

Just compute $E^d \overset{M}{\overset{\shortparallel}{\bmod n}}$ (the decrypter knows d and can do this)

Why? Secretly

$$E^d \equiv (M^e)^d \equiv M^{de} = M^{k\varphi(n)+1} \bmod n.$$

$de = k\varphi(n)+1$

$$= (M^{\varphi(n)})^k \cdot M \bmod n$$

$$= M \bmod n,$$

by Fermat's little theorem!

After this we did the example on the worksheet, using CoCalc.

Today: Some linear algebra.

personal.psu.edu/jdl249/courses/topics2f21/

1) formula for Fibonacci: $1, \overset{F_n}{\overset{\shortparallel}{1}}, 2, 3, 5, 8, 13, 21, 34, \ldots$

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

2) formula for substition in double integrals ("Jacobian determinant").

<u>Def</u> A function $T: \mathbb{R}^n \to \mathbb{R}^m$ ← vectors of length m.

↑ vector of length n

is called a <u>linear transformation</u> if

1) $T(v+w) = T(v) + T(w)$ any two vectors $v, w \in \mathbb{R}^n$

2) $T(cv) = c \cdot T(v)$

<u>Ex</u> $T: \mathbb{R}^2 \to \mathbb{R}^3$

defined by

$$T\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} x - 7y \\ 2x + 5y \\ x + y \end{pmatrix}$$

linear equations

check:

$$T\left(\overset{v}{\begin{pmatrix} 1 \\ 2 \end{pmatrix}}\right) = \begin{pmatrix} -13 \\ 12 \\ 3 \end{pmatrix}$$

$$T\left(\overset{w}{\begin{pmatrix} 2 \\ -3 \end{pmatrix}}\right) = \begin{pmatrix} 23 \\ -11 \\ -1 \end{pmatrix}$$

$$T\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} + \begin{pmatrix} 2 \\ -3 \end{pmatrix}\right) = T\left(\underset{v+w}{\begin{pmatrix} 3 \\ -1 \end{pmatrix}}\right) = \begin{pmatrix} 10 \\ 1 \\ 2 \end{pmatrix}$$

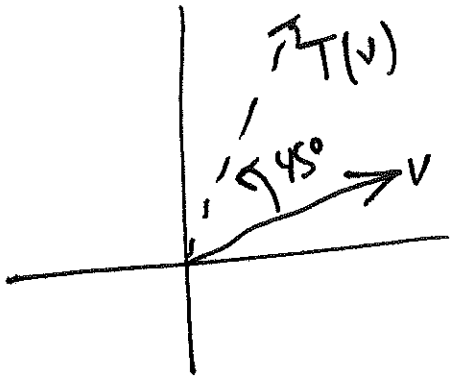
Did it work?

$$T(v) + T(w) = T(v+w) \ ?$$

$$\begin{pmatrix} -13 \\ 12 \\ 3 \end{pmatrix} + \begin{pmatrix} 23 \\ -11 \\ -1 \end{pmatrix} = \begin{pmatrix} 10 \\ 1 \\ 2 \end{pmatrix} \quad \checkmark$$

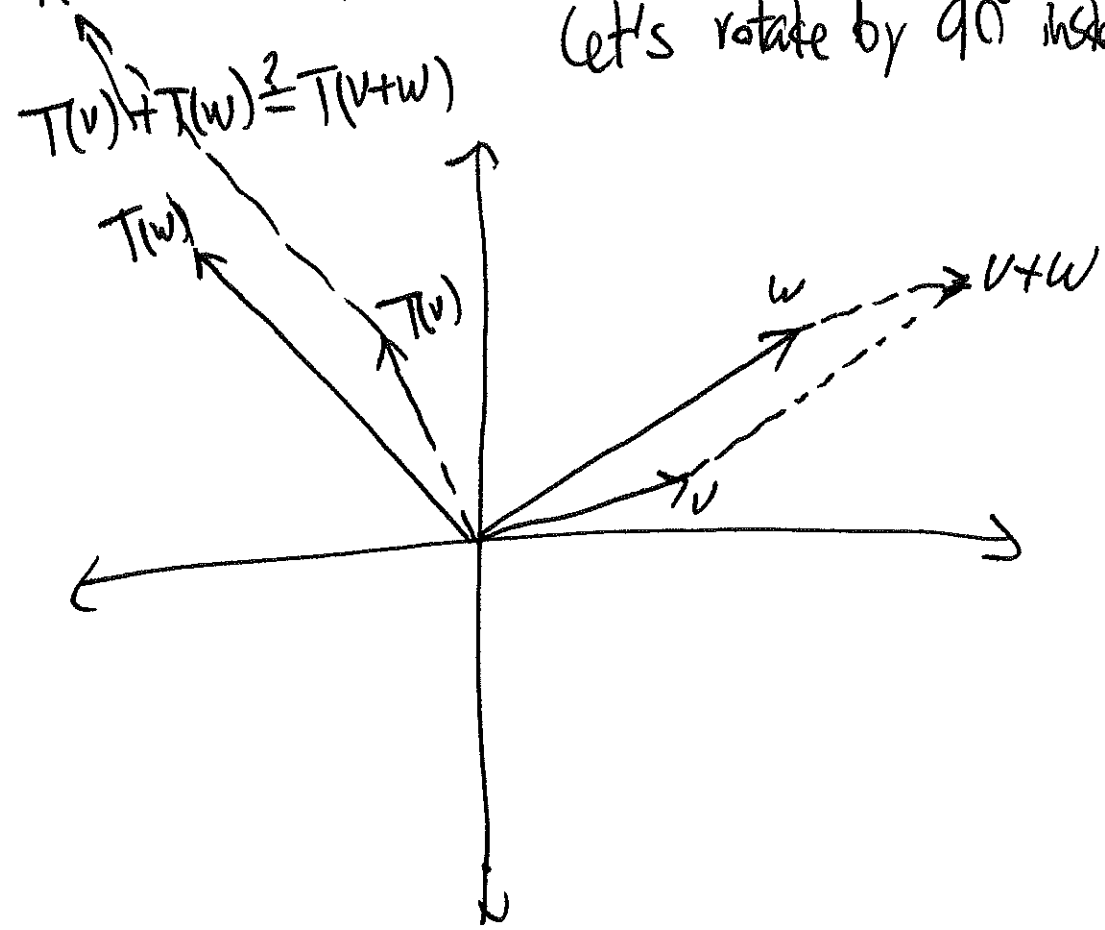
Ex $T : \mathbb{R}^2 \to \mathbb{R}^2$

$T(v) =$ v rotated counterclockwise by $45°$.



Let's rotate by $90°$ instead

$T(v) + T(w) \overset{?}{=} T(v+w)$



↑

We can rewrite this using matrices.

$$\begin{pmatrix} x-7y \\ 2x+5y \\ x+y \end{pmatrix} = \begin{array}{c} (x\ \ y)\ x \\ \begin{pmatrix} 1 & -7 \\ 2 & 5 \\ 1 & 1 \end{pmatrix} \end{array} \begin{pmatrix} x \\ y \end{pmatrix}$$

Our first map can be written as:

$T(v) = Mv$ where M is matrix $\begin{pmatrix} 1 & -7 \\ 2 & 5 \\ 1 & 1 \end{pmatrix}$

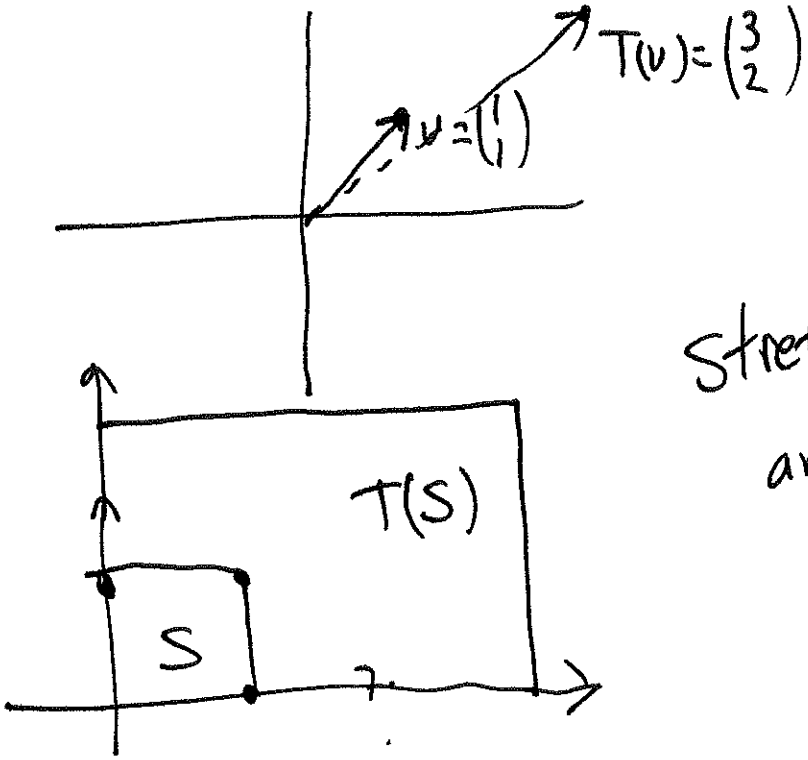
$$T\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} 1 & -7 \\ 2 & 5 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

In fact, <u>every</u> linear map is determined by a matrix: if $T: \mathbb{R}^n \to \mathbb{R}^m$ satisfies the axioms, then there's a $m \times n$ matrix M so $T(v) = Mv$ for any $v \in \mathbb{R}^n$.

1a. $M = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}$.

Gives us a map $T : \mathbb{R}^2 \to \mathbb{R}^2$.

$$T\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3x \\ 2y \end{pmatrix}$$



Stretches horizontally 3x and vertically 2x.

Adv Topics 2 (Lesieutre)
August 31, 2021

$T(v)$

Problem 1. For each of the following matrices T, choose a couple sample vectors $\mathbf{v} = \begin{pmatrix} x \\ y \end{pmatrix}$ and compute $T\mathbf{v}$. What does the matrix do to a vector, geometrically? What does it do to the unit square?

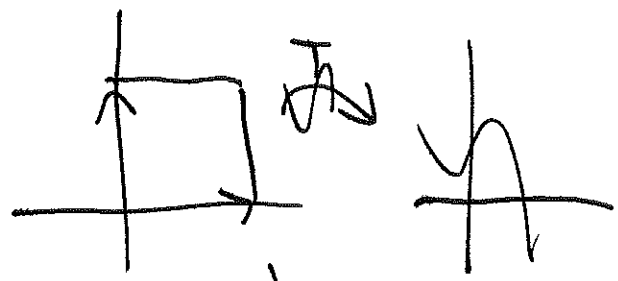
a) $\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}$

$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+3y \\ y \end{pmatrix}$

$T\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $T\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix}$

$T\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$



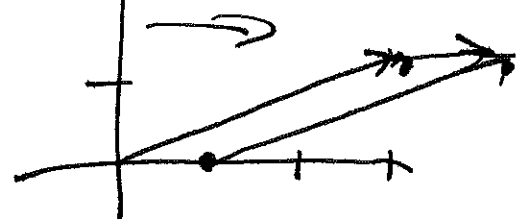
c) $\begin{pmatrix} 1 & 6 \\ 0 & 2 \end{pmatrix}$

"Shear transformation"

T_b

d) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

linearity means squares turn into rectangles →



e) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

f) $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$T: \mathbb{R}^3 \to \mathbb{R}^2$

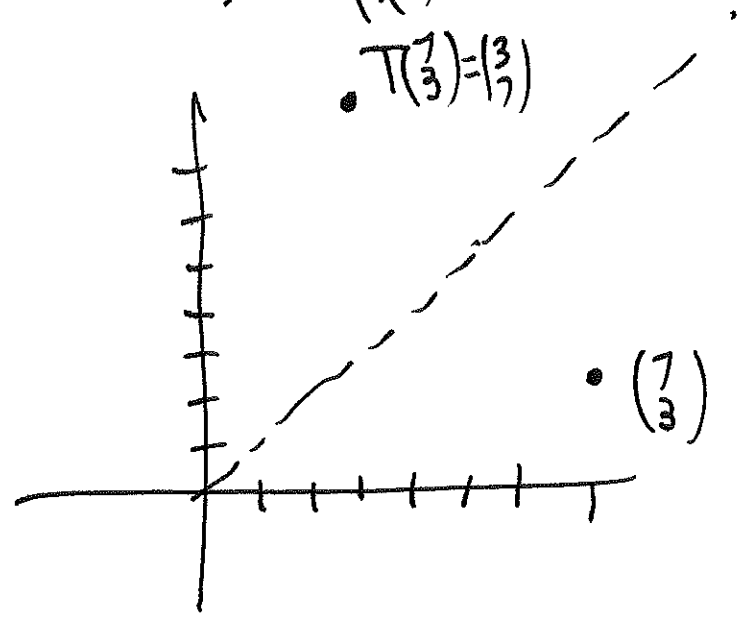
g) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}$

c) yuck

h) $\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

i) $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

d) $T\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}y\\x\end{pmatrix}$

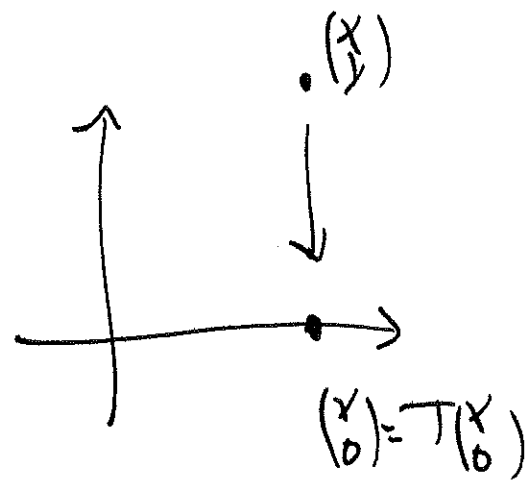


e) $T\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x\\-y\end{pmatrix}$

reflect over x-axis

f) $T\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x\\0\end{pmatrix}$

project onto x-axis



g) $T\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}x\\y\end{pmatrix}$ project onto xy-plane.

Strategy for finding a matrix. (given a description of map)

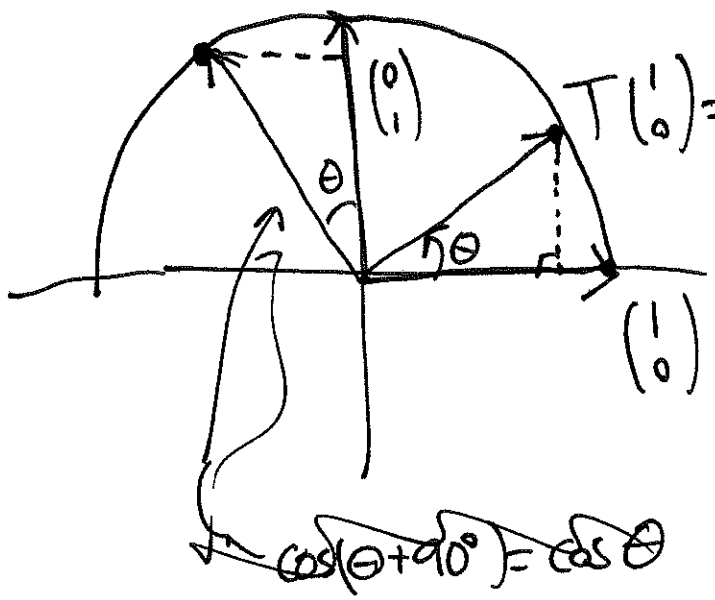
By definition: the first column of M is where $\begin{pmatrix}1\\0\end{pmatrix}$ goes.

the second column is where $\begin{pmatrix}0\\1\end{pmatrix}$ goes.

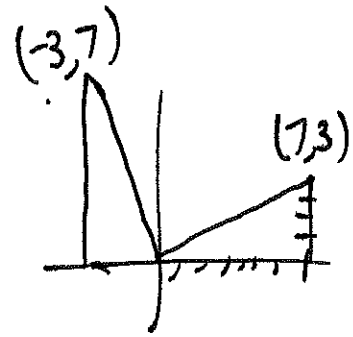
$$\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}a\\c\end{pmatrix} \qquad \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}b\\d\end{pmatrix}.$$

ex

Rotate θ counterclockwise. What's the matrix?



$$T\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix}$$

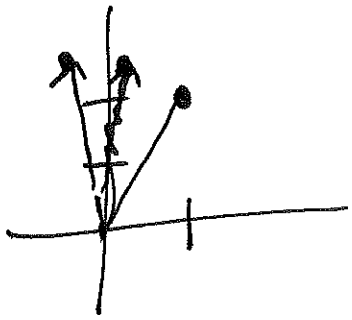


$$T\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}-\sin\theta\\ \cos\theta\end{pmatrix}$$

matrix for rotation:

$$\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$$

What's $\begin{pmatrix}1\\2\end{pmatrix}$ rotated 30° counterclockwise?



$$M = \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}^{\theta=30^\circ} = \begin{pmatrix}\sqrt{3}/2 & -1/2\\ 1/2 & \sqrt{3}/2\end{pmatrix}$$

$$\begin{pmatrix}\sqrt{3}/2 & -1/2\\ 1/2 & \sqrt{3}/2\end{pmatrix}\begin{pmatrix}1\\2\end{pmatrix} = \begin{pmatrix}\frac{\sqrt{3}}{2} - 1\\ \frac{1}{2} + \sqrt{3}\end{pmatrix}$$

$$\begin{pmatrix}3 & 0\\ 0 & 2\end{pmatrix}\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix} = \begin{pmatrix}3 & 9\\ 0 & 2\end{pmatrix}.$$

$$\begin{pmatrix}3 & 0\\ 0 & 2\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}3\\0\end{pmatrix} \qquad \begin{pmatrix}3 & 0\\ 0 & 2\end{pmatrix}\begin{pmatrix}3\\1\end{pmatrix} = \begin{pmatrix}9\\2\end{pmatrix}$$

$$\begin{array}{cc} 3 & 0 \end{array}$$
$$\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}\begin{pmatrix}3 & 0\\ 0 & 2\end{pmatrix} = \begin{pmatrix}3 & 6\\ 0 & 2\end{pmatrix}$$

Why is this the formula?

$\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}$ gives the function $T_1 : \mathbb{R}^2 \to \mathbb{R}^2$

$$T_1\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3x \\ 2y \end{pmatrix}$$

$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$ gives the function $T_2 : \mathbb{R}^2 \to \mathbb{R}^2$.

$$T_2\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+3y \\ y \end{pmatrix}$$

What's $T_1 \circ T_2$? (composition)

$$(T_1 \circ T_2)\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = T_1\left(T_2\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)\right)$$

$$= T_1\begin{pmatrix} x+3y \\ y \end{pmatrix} = \begin{pmatrix} 3x+9y \\ 2y \end{pmatrix}$$

This is just $\begin{pmatrix} 3 & 9 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$!

If $S: \mathbb{R}^2 \to \mathbb{R}^2$ ~~to~~

and $T: \mathbb{R}^2 \to \mathbb{R}^2$ are linear transformations:

~~matrix~~ $(\text{matrix for } \underbrace{T \circ S}_{\text{composition}}) = (\text{matrix for } T)(\text{matrix for } S)$

Matrix multiplication is not commutative!

$$M_2 M_1 \neq M_1 M_2.$$

This just reflects the fact that function composition not commutative.

$f(x) = \log x$

$g(x) = \sqrt{x}$

$f(g(x)) = \log(\sqrt{x})$

$g(f(x)) = \sqrt{\log(x)}$

Today: Linear maps, determinants

Let $M = \begin{pmatrix} 2 & 3 \\ -1 & 4 \end{pmatrix}$ $\quad N = \begin{pmatrix} -2 & 0 \\ 3 & 1 \end{pmatrix}$.

What are the linear transformations $f : \mathbb{R}^2 \to \mathbb{R}^2$ $\quad N$

$M \rightsquigarrow f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = ?$ $\quad g : \mathbb{R}^2 \to \mathbb{R}^2$

What's the composite function $(f \circ g)\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)$? $= f\left(g\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)\right)$

What's MN?

$$M \quad f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \overset{M}{\begin{pmatrix} 2 & 3 \\ -1 & 4 \end{pmatrix}} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x+3y \\ -x+4y \end{pmatrix}$$

$$g\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} -2 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -2x \\ 3x+y \end{pmatrix}$$

$(f \circ g)\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)$? Take $g\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} -2x + 0y \\ 3x + y \end{pmatrix}$

Plug in to $f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)$:

$$\begin{pmatrix} 2(-2x+0y)+3(3x+y) \\ -1(-2x+0y)+4(3x+y) \end{pmatrix} = \begin{pmatrix} 5x + 3y \\ 14x + 4y \end{pmatrix}$$

$$\begin{pmatrix} 2 & 3 \\ -1 & 4 \end{pmatrix}\begin{pmatrix} -2 & 0 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 14 & 4 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 5 & 3 \\ 14 & 4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

Matrix for composition is product of matrices!

Adv Topics 2 (Lesieutre)
September 2, 2021

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

Problem 1. For each of the following matrices T, choose a couple sample vectors $\mathbf{v} = \begin{pmatrix} x \\ y \end{pmatrix}$ and compute $T\mathbf{v}$. What does the matrix do to a vector, geometrically? What does it do to the unit square?

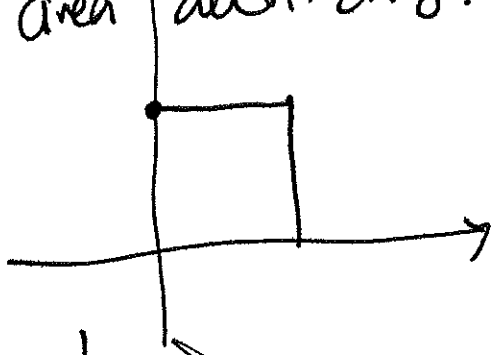
6 a) $\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}$

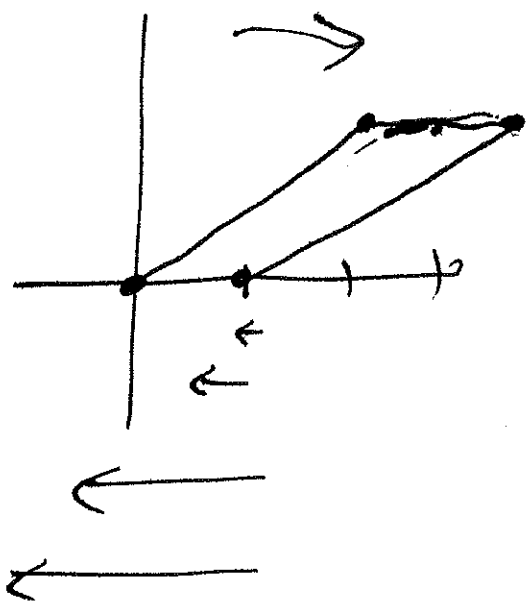
a) Stretch horizontally by 3 vertically by 2. | area multiplies by 6

1 b) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$

b) area doesn't change!

2 c) $\begin{pmatrix} 1 & 6 \\ 0 & 2 \end{pmatrix}$





-1 d) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

-1 e) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

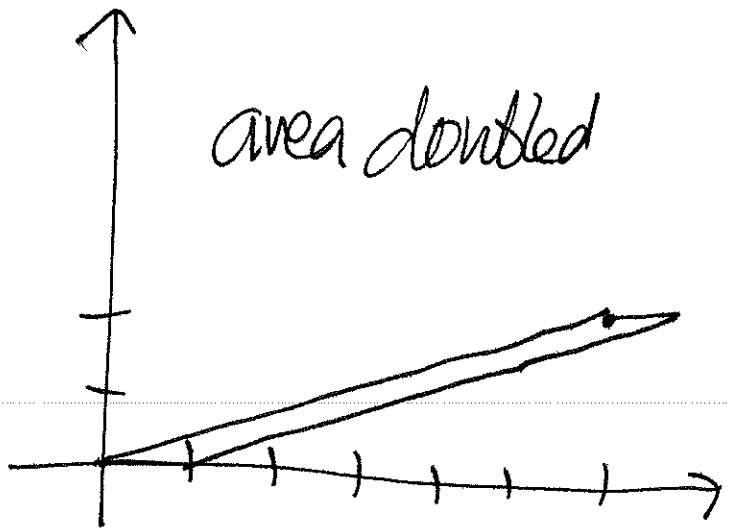
0 f) $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

g) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

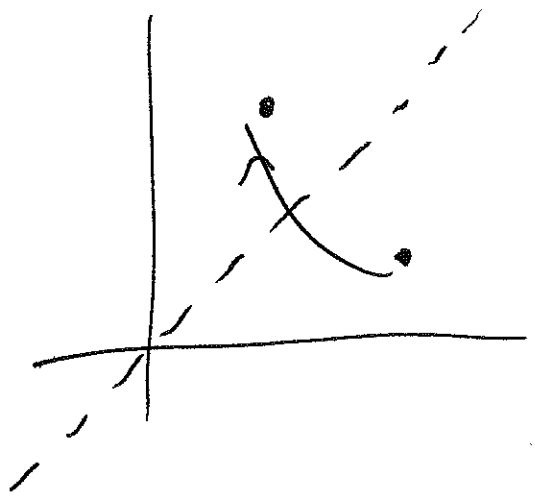
c) area doubled

h) $\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

i) $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$



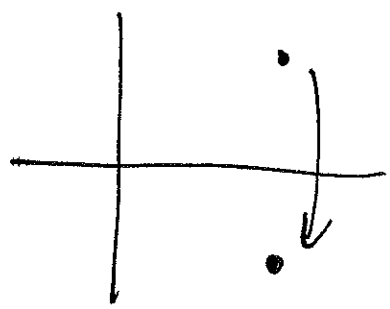
d) Reflects over $y=x$



area doesn't change!

but reverses orientation

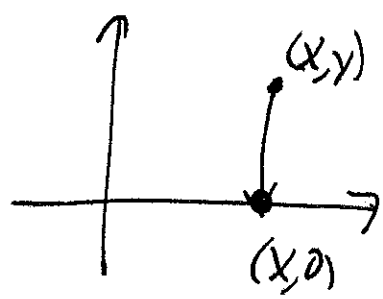
e



flip over x-axis.

Same area, orientation reversed

f) $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$



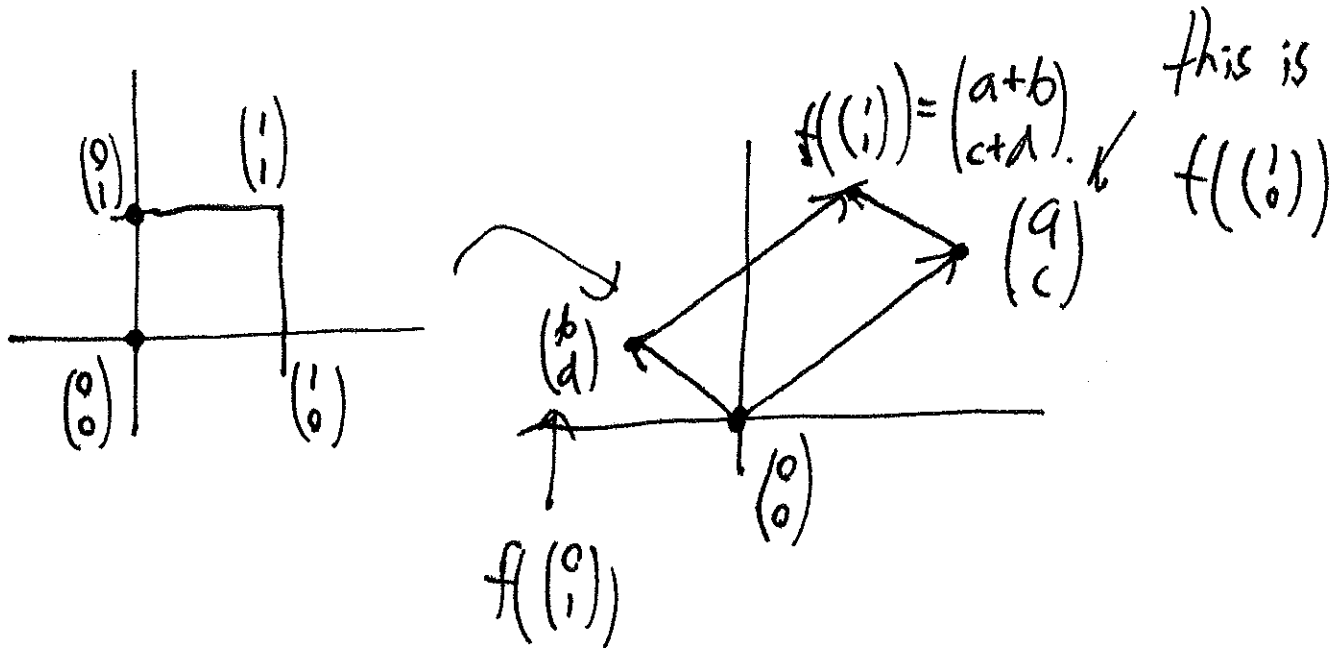
multiplies area by 0.

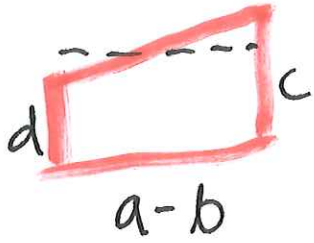
If $f: \mathbb{R}^2 \to \mathbb{R}^2$ is a linear transformation, corresponding to a 2×2 matrix M, then f rescales areas by a factor of $\det(M) = ad - bc$

(If this is negative, it means f reverses orientations).

Why does $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ scale areas by $ad-bc$?

What happens to unit square?

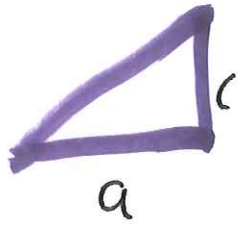


area of 

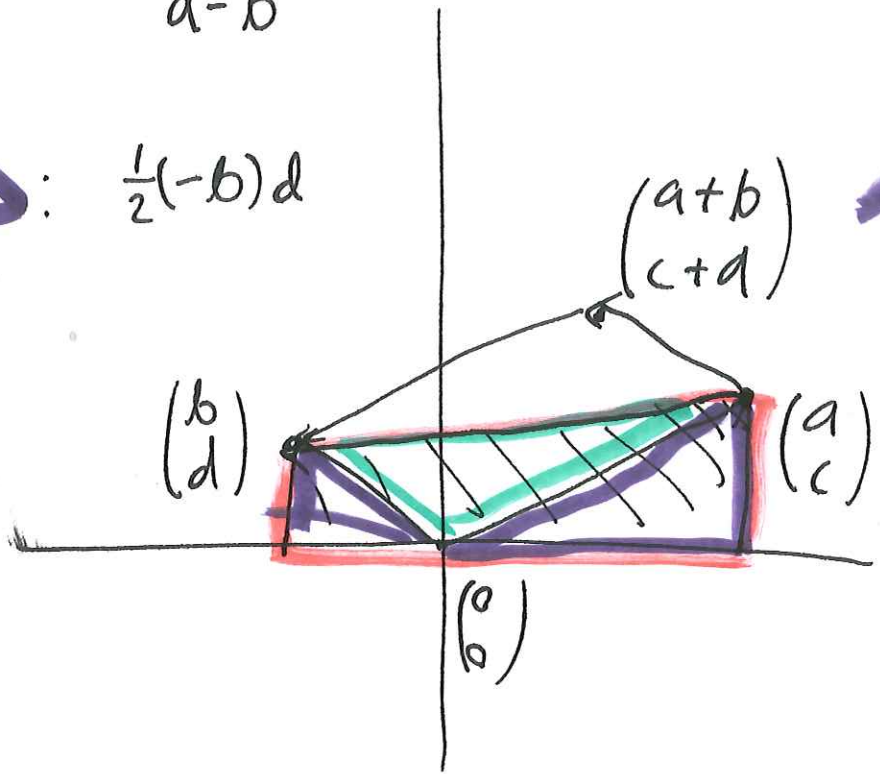
$\rightsquigarrow (a-b)\left(\frac{c+d}{2}\right)$

area of

: $\frac{1}{2}(-b)d$



$A = \frac{1}{2}ac$



Area of

$$= (a-b)\left(\frac{c+d}{2}\right) - \frac{1}{2}(-bd) - \frac{1}{2}ac$$

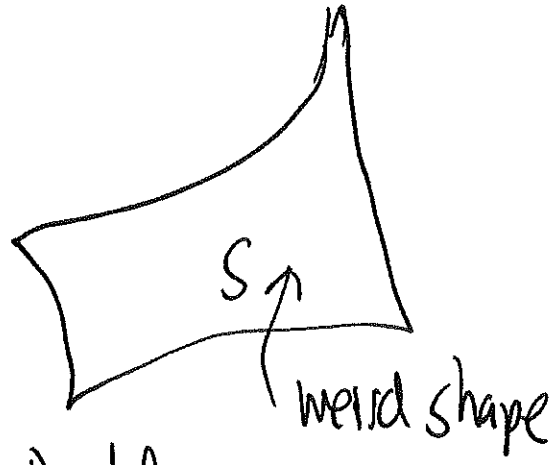
$$= \frac{1}{2}\left[(ac+ad-bc-bd)+bd-ac\right]$$

$$= \frac{1}{2}(ad-bc).$$

Area of
is $\boxed{ad-bc}$

Jacobian determinant

To compute



$$\iint_S f(x,y)\, dA$$

use multivariable coordinate change!

Imagine you can parametrize the region:

new variables s, t $\quad a \le s \le b$
$\quad c \le t \le d$

and functions ~~x(s)~~
$x(s,t)$ and $y(s,t)$ such that $x(s,t)$, $y(s,t)$

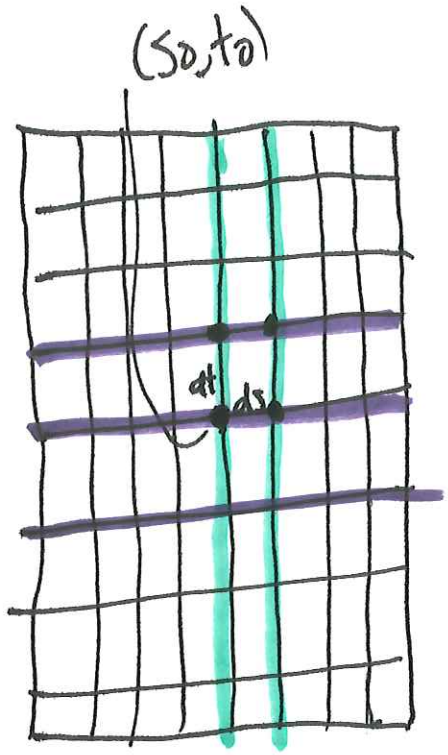
covers our region S when we vary s and t.

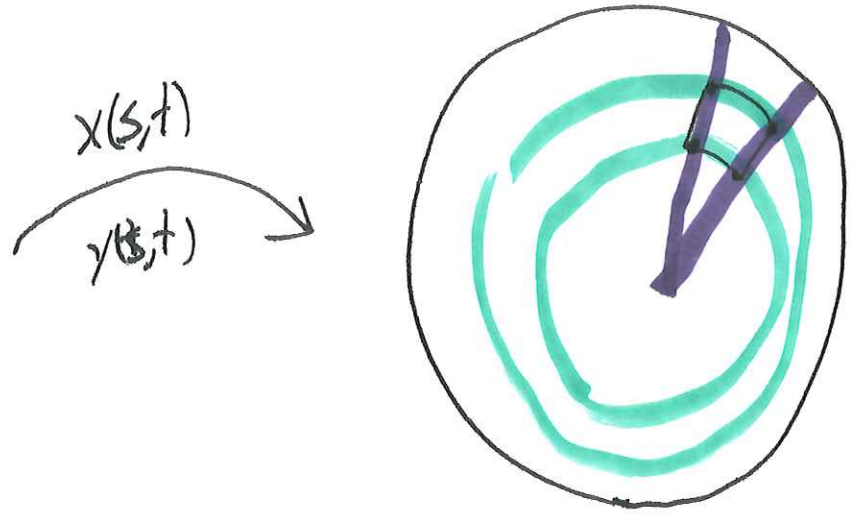
What if S is unit disk? How to parametrize S?

Think of s,t as being new coordinates, and $x(s,t)$ $y(s,t)$ tell you how to convert those new coords into regular old x,y values.

$0 \le s \le 1$ ← (polar "r") $\qquad x(s,t) = s\cos t$

$0 \le t \le 2\pi$ ← (polar "θ") $\qquad y(s,t) = s\sin t$





$0 \le s \le 1$

$0 \le t \le 2\pi$

Vertices of image of our rectangle:

$$(s_0,t_0) \mapsto (x(s_0,t_0),\ y(s_0,t_0))$$

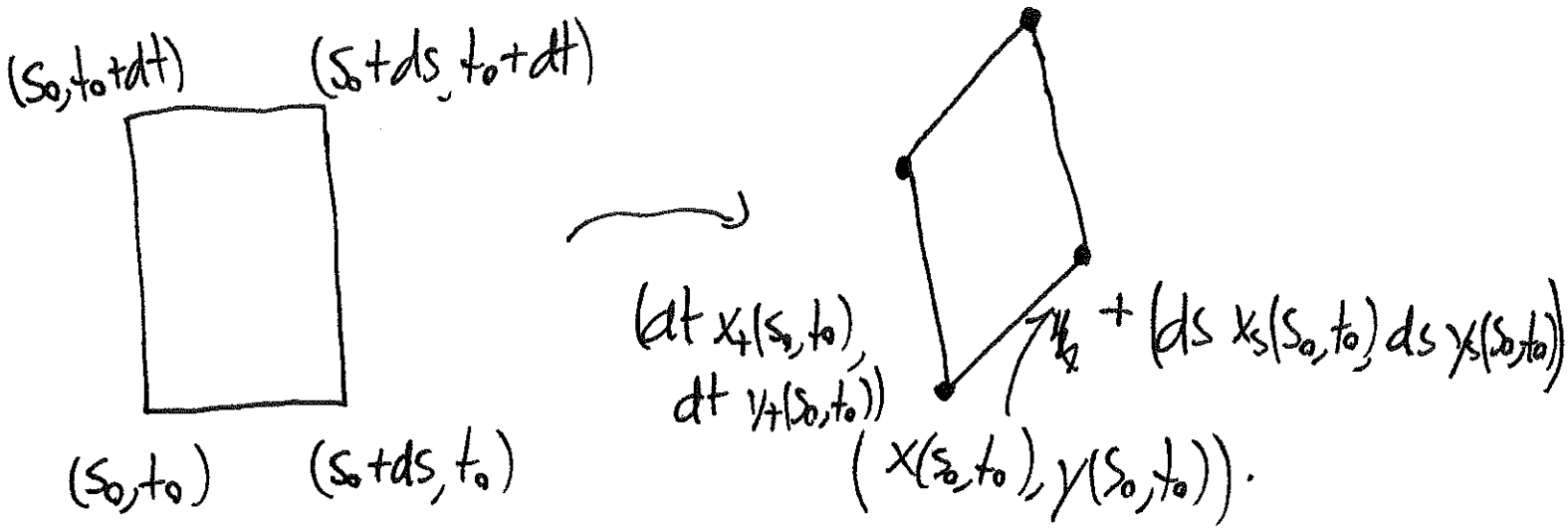
$$(s_0+ds,t_0) \mapsto (x(s_0+ds,t_0),\ y(s_0+ds,t_0))$$

$$\approx (x(s_0,t_0) + ds \cdot x_s(s_0,t_0),\ \frac{\partial x}{\partial s}$$

$$y(s_0,t_0) + ds \cdot y_s(s_0,t_0)$$

$$(s_0,t_0+dt) \mapsto (x(s_0,t_0+dt),\ y(s_0,t_0+dt))$$

$$\approx (x(s_0,t_0) + dt\, x_t(s_0,t_0),\ y(s_0,t_0) + dt\, y_t(s_0,t_0))$$



$$\begin{array}{cc} 1^{st}\text{ leg} & 2^{nd}\text{ leg} \\ \end{array}$$

$$\begin{pmatrix} ds\, x_s(s_0,t_0) & dt\, x_t(s_0,t_0) \\ ds\, y_s(s_0,t_0) & dt\, y_t(s_0,t_0) \end{pmatrix}$$

$$= \begin{pmatrix} x_s(s_0,t_0) & x_t(s_0,t_0) \\ y_s(s_0,t_0) & y_t(s_0,t_0) \end{pmatrix} \begin{pmatrix} ds \\ dt \end{pmatrix}$$

area of image mesh is:

$$\underbrace{(x_s y_t - x_t y_s)}_{\text{Jacobian determinant}}(s_0,t_0) \cdot ds \cdot dt$$

To integrate over weird shape.

$$\iint_S f(x,y)\,dx\,dy = \int_{s=a}^{b}\int_{t=c}^{d} f(x(s,t), y(s,t))\,(x_s y_t - x_t y_s)\,ds\,dt$$

<u>Area of circle</u> New coords: $0 \le s \le 1$
$0 \le t \le 2\pi$

$x(s,t) = s\cos t$
$y(s,t) = s\sin t$

$x_s = \cos t$
$x_t = -s\sin t$
$y_s = \sin t$
$y_t = s\cos t$

$$x_s y_t - x_t y_s = (\cos t)(s\cos t) - (-s\sin t)(\sin t)$$
$$= s.$$

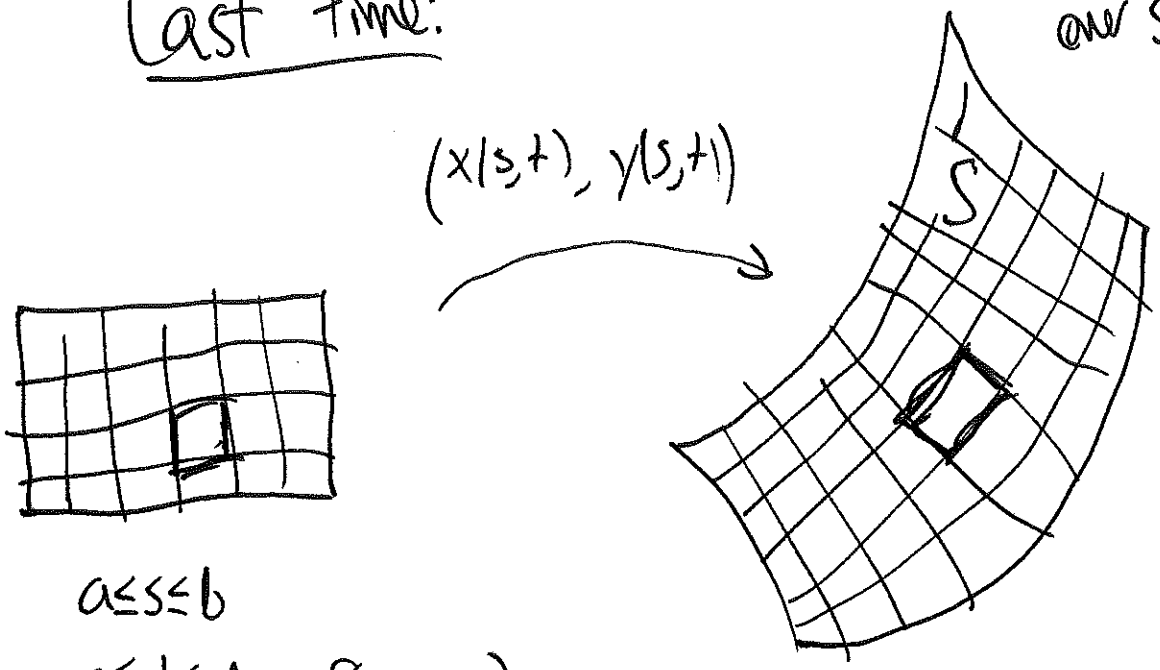
(that's $r\,dr\,d\theta$!)

$$A = \iint_{\text{circle}} 1\,dx\,dy = \int_{s=0}^{1} \int_{t=0}^{2\pi} 1 \; s \; \cancel{ds/dt}\; dt\, ds$$

$$= \int_{s=0}^{1} 2\pi s\, ds = \pi s^2 \Big|_0^1 = \boxed{\pi}$$

Last time:

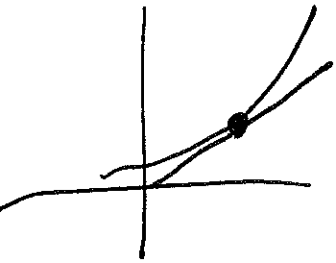
Want to integrate over S:



$a \le s \le b$

$c \le t \le d$

$$f(x+\Delta x) \approx f(x) + \Delta x f'(x)$$



2x2 matrix "Jacobian"

$$\begin{pmatrix} x(s+ds, t+dt) \\ y(s+ds, t+dt) \end{pmatrix} \approx \begin{pmatrix} x(s,t) \\ y(s,t) \end{pmatrix} + \begin{pmatrix} x_s & x_t \\ y_s & y_t \end{pmatrix} \begin{pmatrix} ds \\ dt \end{pmatrix}$$

$$\iint_S f(x,y)\,dx\,dy = \int_{s=a}^{b} \int_{t=c}^{d} f(x(s,t), y(s,t))\,(x_s y_t - x_t y_s)\,ds\,dt$$

Example:

Let $f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} x^2y + x \\ xy^3 - 7y \end{pmatrix}$.

Approximate $f\left(\begin{pmatrix} 2.01 \\ 2.99 \end{pmatrix}\right)$?

Renamed:

$$f\left(\begin{pmatrix} s \\ t \end{pmatrix}\right) = \begin{pmatrix} s^2t + s \\ st^3 - 7t \end{pmatrix} \begin{matrix} \leftarrow x(s,t) \\ \leftarrow y(s,t) \end{matrix}$$

$$f\left(\begin{pmatrix} 2.01 \\ 2.99 \end{pmatrix}\right)$$

$x_s(2,3)$

$x_s = 2st + 1 \quad y_s = t^3$

$x_t = s^2 \quad y_t = 3st^2 - 7$

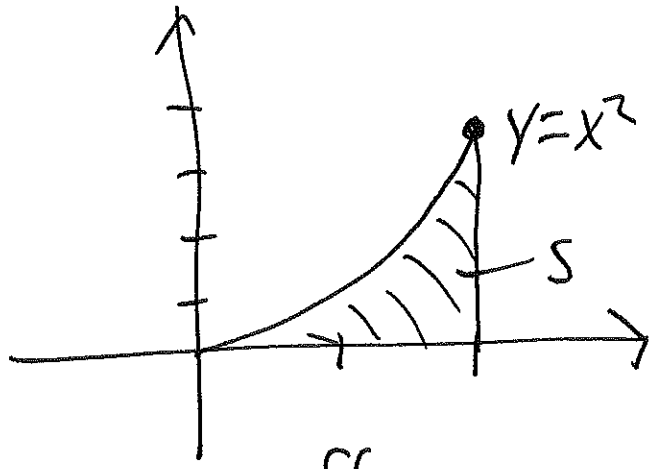
$x_s(2,3) = 13 \quad y_s(2,3) = 27$

$x_t(2,3) = 4 \quad y_t(2,3) = 47$ (?)

$$f\left(\begin{pmatrix} 2.01 \\ 2.99 \end{pmatrix}\right) = \cancel{f\left(\begin{pmatrix} 2 \\ 3 \end{pmatrix}\right) + \begin{pmatrix} x_s(2,3) & y_s(2 \\ x_t(2,3) & \end{pmatrix}}$$

$$\approx f\left(\begin{pmatrix} 2 \\ 3 \end{pmatrix}\right) + \begin{pmatrix} x_s(2,3) & x_t(2,3) \\ y_s(2,3) & y_t(2,3) \end{pmatrix} \begin{pmatrix} 0.01 \\ -0.01 \end{pmatrix}$$

$$= \begin{pmatrix} 14 \\ 33 \end{pmatrix} + \begin{pmatrix} 13 & 4 \\ 27 & 47 \end{pmatrix} \begin{pmatrix} 0.01 \\ -0.01 \end{pmatrix} = \begin{pmatrix} 14.09 \\ 32.80 \end{pmatrix}$$



$f(x,y)=xy$

$0\le x\le 2$

$$\iint_S xy\,dx\,dy$$

$$\left(\frac{y^2}{2}\right)\Big|_0^{x^2}=\frac{x^4}{2}$$

$$\int_{x=0}^{2}\int_{y=0}^{x^2} xy\,dy\,dx=\int_{x=0}^{2} x\cdot\left(\int_{y=0}^{x^2} y\,dy\right)dx$$

$$=\int_{x=0}^{2}\frac{x^5}{2}\,dx=\frac{x^6}{12}\Big|_0^2=\frac{64}{12}=\frac{32}{6}=\frac{16}{3}.$$

$x \to 0\le s\le 2$ (coord)

$x(s,t)=s$ $\quad y(s,t)=s^2t$

$0\le t\le 1$

proportion of the way you are from $y=0$ to $y=x^2$

$x_s=1 \quad x_t=0$

$y_s=2st \quad y_t=s^2$

$x_s y_t - x_t y_s = s^2$

$$\int_{s=0}^{2}\int_{t=0}^{1}(s\cdot s^2t)\cdot(s^2)\,dt\,ds$$

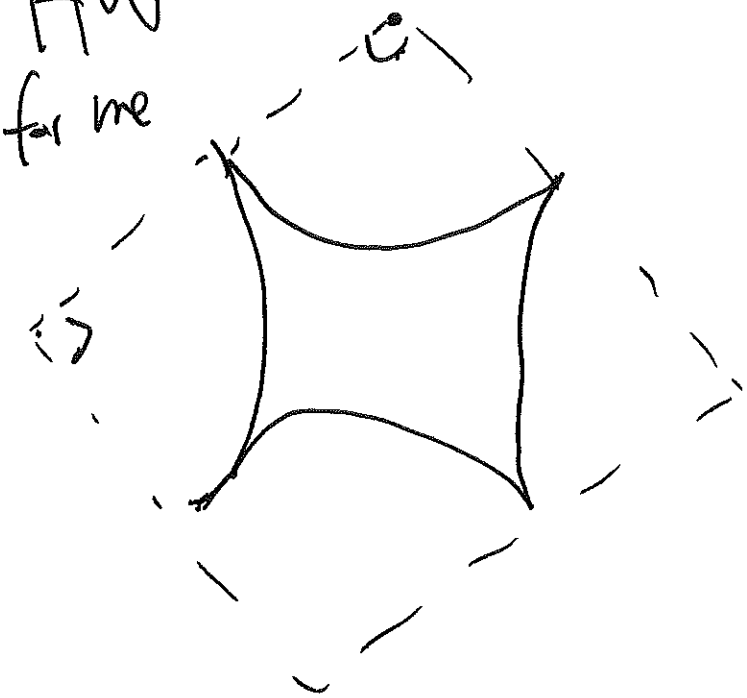
Jacobian

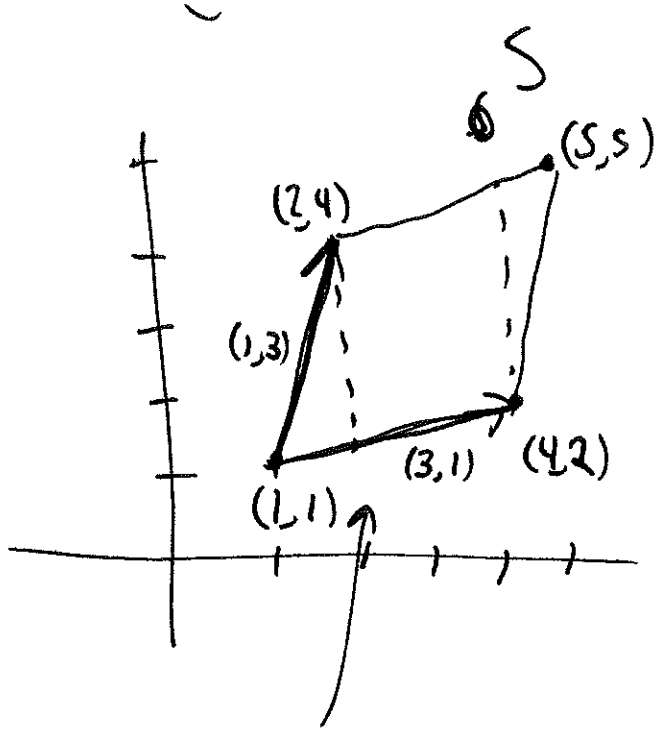
$=xy$, our function

$$\cancel{= \int_{s=0}^{2} s^5\, ds \cdot \int_{t=0}^{1} t\, dt}$$

$$= \int_{s=0}^{2} \int_{t=0}^{1} s^5\, t\, dt\, ds = \int_{s=0}^{2} \frac{1}{2} s^5\, ds = \frac{s^6}{12}\Big|_0^2 = \frac{64}{12} = \frac{16}{3}$$

HW for me





$$\begin{pmatrix} x \\ y \end{pmatrix}(s,t) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} + s\begin{pmatrix} 3 \\ 1 \end{pmatrix} + t\begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

$x(s,t) = 1 + 3s + t \quad 0 \le s \le 1$

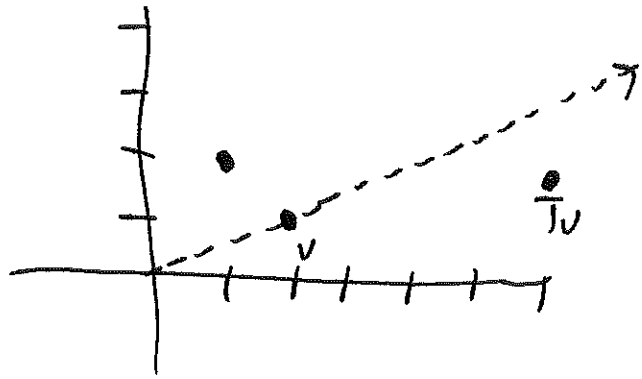
$y(s,t) = 1 + s + 3t \quad 0 \le t \le 1$

area is

$$\det\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix} = 8.$$

$\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}$

$T\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} 3x \\ 2y \end{pmatrix}$



$T(v)$ <u>not</u> parallel to v!

e.g. $v = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ $T(v) = \begin{pmatrix} 6 \\ 2 \end{pmatrix}$ not an eigenvector.

$\cancel{w = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \quad T(w) = \begin{pmatrix} 3 \\ 4 \end{pmatrix}}$ $\begin{pmatrix} 3 \\ 0 \end{pmatrix}$ is an eigenvector!

In fact, any vector $\begin{pmatrix} x \\ 0 \end{pmatrix}$! Turns into $\begin{pmatrix} 3x \\ 0 \end{pmatrix}$, so $\lambda = 3$.

$T\begin{pmatrix} 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 9 \\ 0 \end{pmatrix} = 3 \cdot \begin{pmatrix} 3 \\ 0 \end{pmatrix}$.

The number λ is called the <u>eigenvalue</u>.

$\begin{pmatrix} 0 \\ y \end{pmatrix}$ is also eigenvector: $T\begin{pmatrix} 0 \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 2y \end{pmatrix}$, so $\lambda = 2$ for these.

Eigenvectors:

If $T\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)$ is a linear transformation

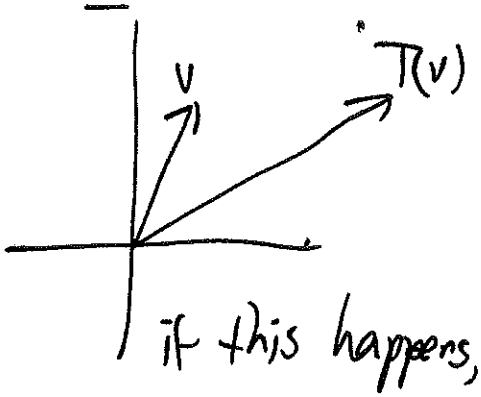
ex $T\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} 3x+2y \\ -x-7y \end{pmatrix}$.

a vector v is called an <u>eigenvector</u> for T if $T(v) = \lambda v$ for some scalar λ.

scalar mult

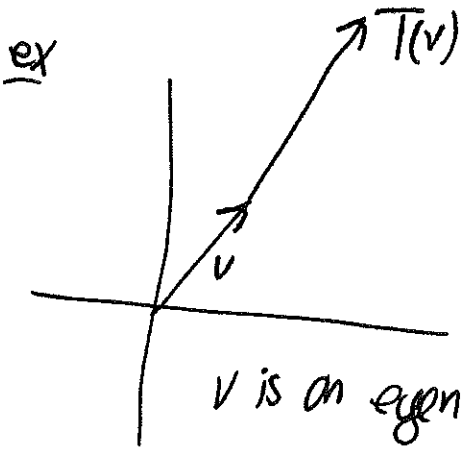
"$T(v)$ is parallel to v"

ex



if this happens, v is <u>not</u> an eigenvector!

ex



v is an eigenvector.

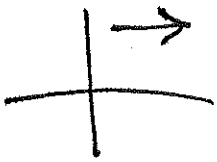
A13B

Adv Topics 2 (Lesieutre)
September 1, 2021

Problem 1. *For each of the following matrices T, choose a couple sample vectors* $\mathbf{v} = \begin{pmatrix} x \\ y \end{pmatrix}$ *and compute $T\mathbf{v}$. What does the matrix do to a vector, geometrically? What does it do to the unit square?*

a) $\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}$

* b) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$



$T\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} x \\ y \end{pmatrix}$

~~c) $\begin{pmatrix} 1 & 6 \\ 0 & 2 \end{pmatrix}$~~

* d) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ reflects on $y=x$ (x,x) $\lambda=1$ $(x,-x)$ $\lambda=-1$.

* e) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ reflection on x-axis $T(x,y)=(x,-y)$ $(x,0)$ $\lambda=1$ $(0,y)$ $\lambda=-1$

* f) $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ projections $(x,0)$ $\lambda=1$ $(0,x)$ $\lambda=0$.

~~g) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$~~

~~h) $\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$~~

i) $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$???

Problem 2. *For each of the linear maps described, write down the matrix for the corresponding transformation.*

a) *Reflection about the y-axis.*

b) *Rotation by $45°$ clockwise. What about other angles θ?*

c) *In 3D: rotation by an angle θ around the z-axis.*

b) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$

$(x,0)$ $\lambda = 1$.

that's the only option!

c) $\begin{pmatrix} 1 & 6 \\ 0 & 2 \end{pmatrix}$

Suppose (a,b) is eigenvector

$T(v) = \lambda v$

$\begin{pmatrix} a+3b \\ b \end{pmatrix} = \lambda \begin{pmatrix} a \\ b \end{pmatrix}$

$a+3b = \lambda a$

$b = \lambda b.$ $\Rightarrow$ $b(\lambda - 1) = 0$

Either: $\lambda = 1$ or $b = 0$

$a+3b = a$

$3b = 0$

$b = 0$ works!

$\begin{pmatrix} a \\ 0 \end{pmatrix}$ eigenvector

$\lambda = 1$.

$a = \lambda a$

either $a = 0$ and $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

or $\lambda = 1$ and we get same again.

$$\begin{pmatrix} 1 & 6 \\ 0 & 2 \end{pmatrix}$$

$$T\begin{pmatrix} a \\ b \end{pmatrix} = \lambda \begin{pmatrix} a \\ b \end{pmatrix}$$

$$\begin{pmatrix} a+6b \\ 2b \end{pmatrix} = \begin{pmatrix} \lambda a \\ \lambda b \end{pmatrix}$$

$a+6b=\lambda a$

$2b=\lambda b$

$(\lambda-2)b=0$

So... $\lambda=2$ or $b=0$

$\lambda=2$

$a+6b=2a$

$a=6b$

eigenvector is $\begin{pmatrix} 6 \\ 1 \end{pmatrix}$ (or a mult of that)

$$\begin{pmatrix} 1 & 6 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 6 \\ 1 \end{pmatrix} = \begin{pmatrix} 12 \\ 2 \end{pmatrix} = 2 \cdot \begin{pmatrix} 6 \\ 1 \end{pmatrix}$$

✓

$b=0$

$\begin{pmatrix} a \\ 0 \end{pmatrix}$ is eigenvector, $\lambda=1$.

Eigenstuff

$T: \mathbb{R}^2 \to \mathbb{R}^2$ linear transformation
(or matrix)

A vector v is an <u>eigenvector</u> if $T(v) = \lambda v$ for some scalar λ. This means $T(v)$ points in same direction as v (or opposite if $\lambda < 0$).

If T given by $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ so

$T\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} 2x \\ 3y \end{pmatrix}$ then $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are eigenvectors.

$T\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 0 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$T\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 3 \end{pmatrix} = 3 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

$T\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$, not parallel to $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$!

Consider the matrix $M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

Compute $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \boxed{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \boxed{\begin{pmatrix} 1 \\ 2 \end{pmatrix}}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \end{pmatrix} = \boxed{\begin{pmatrix} 2 \\ 3 \end{pmatrix}} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^3 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$\cdots$

What's this, in terms of n?

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 2 \\ 3 \end{pmatrix} = \boxed{\begin{pmatrix} 3 \\ 5 \end{pmatrix}} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Can you prove it?

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

Claim: $M^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix}$

Where $F_1 = 1$, $F_2 = 1$, $\ldots$ $F_{n+1} = F_{n-1} + F_n$

Fibonacci

<u>Pf.</u> Induction. $n=1$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} F_1 \\ F_2 \end{pmatrix} \quad \checkmark$$

Inductive step:

Assume $M^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix}$

Then $M^{n+1} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = M \left(M^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \overset{M}{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}} \begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix}$

$$= \begin{pmatrix} F_{n+1} \\ F_n + F_{n+1} \end{pmatrix} = \begin{pmatrix} F_{n+1} \\ F_{n+2} \end{pmatrix} \quad \checkmark$$

Idea: Let's try to get an exact formula for F_n by computing $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ using linear algebra.

Suppose v and w are two eigenvectors of M:

$Mv = \lambda v$ some λ, $Mw = \mu w$ some μ.

Suppose too we can write $\begin{pmatrix}0\\1\end{pmatrix}$ as a combination of v and w:

a, b constants

$$\begin{pmatrix}0\\1\end{pmatrix} = av + bw$$

$$M^n \begin{pmatrix}0\\1\end{pmatrix} = M^n((av+bw))$$

$$\begin{pmatrix}F_n\\F_{n+1}\end{pmatrix} = aM^n v + bM^n w$$

$$= \underbrace{a\lambda^n v + b\mu^n w}_{\text{(a vector)}}.$$

F_n is top entry of the vector!

What's

$M^n v ? = \lambda^n v$

$Mv = \lambda v$

$M^2 v = M(Mv)$

$= M(\lambda v) = \lambda \cdot Mv$

$= \lambda^2 v$

$M^3 v = M(M^2 v)$

$= M(\lambda^2 v) = \lambda^3 v$

$= \lambda^3$

Let's try it!

$M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. First: find eigenvectors. (and eigenvalues)

want $v = \begin{pmatrix} x \\ y \end{pmatrix}$ $\quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix}$

so $\begin{pmatrix} y \\ x+y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}$

$y = \lambda x, \quad x + y = \lambda y \Rightarrow x + \lambda x = \lambda(\lambda x) = \lambda^2 x$

$(\lambda^2 - \lambda - 1)x = 0$

so $\lambda^2 - \lambda - 1 = 0$

If $x = 0$, $y = 0$ too, boring.

$$\lambda = \frac{1 \pm \sqrt{1+4}}{2} = \underbrace{\frac{1+\sqrt{5}}{2}}_{\lambda} \text{ or } \underbrace{\frac{1-\sqrt{5}}{2}}_{\mu}$$

What are the eigenvectors?

We can use any number for x, and solve for y! $x=1$ for simplicity. Then $y=\lambda x$.

So: eigenvectors are $v=\begin{pmatrix}1\\ \lambda\end{pmatrix}$ with eigenvalue $\lambda=\frac{1+\sqrt{5}}{2}$

$M\begin{pmatrix}1\\ \lambda\end{pmatrix}=\lambda\begin{pmatrix}1\\ \lambda\end{pmatrix}$

$w=\begin{pmatrix}1\\ \mu\end{pmatrix}$ with eigenvalue $\mu=\frac{1-\sqrt{5}}{2}$

$M\begin{pmatrix}1\\ \mu\end{pmatrix}=\mu\begin{pmatrix}1\\ \mu\end{pmatrix}$.

Want: $M^n\begin{pmatrix}0\\ 1\end{pmatrix}$. How to write $\begin{pmatrix}0\\ 1\end{pmatrix}$ as combo of v, w?

Find a & b so

$$a\underbrace{\begin{pmatrix}1\\ \lambda\end{pmatrix}}_{v}+b\underbrace{\begin{pmatrix}1\\ \mu\end{pmatrix}}_{w}=\begin{pmatrix}0\\ 1\end{pmatrix}$$

$a+b=0$

$\lambda a+\mu b=1$

$b = -a$ so

$$\lambda a + \mu(-a) = 1$$

$$a(\lambda - \mu) = 1 \qquad a = \frac{1}{\lambda - \mu} = \frac{1}{\left(\frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)} = \frac{1}{\sqrt{5}} = \frac{\sqrt{5}}{5}$$

$$b = -\frac{1}{\sqrt{5}}$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{5}} v - \frac{1}{\sqrt{5}} w \qquad \left(\begin{array}{c} v \text{ \& } w \text{ are the} \\ \text{eigenvectors} \end{array}\right).$$

So...

$$Mv = \lambda v \qquad Mw = \mu w$$
$$M^n v = \lambda^n v \qquad M^n w = \mu^n w$$

$$M^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = M^n \left(\frac{1}{\sqrt{5}} v - \frac{1}{\sqrt{5}} w \right) \qquad \left(\begin{array}{c} \text{only really} \\ \text{care about top} \\ \text{entry} \end{array}\right)$$

$$= \frac{1}{\sqrt{5}} M^n v - \frac{1}{\sqrt{5}} M^n w = \frac{1}{\sqrt{5}} \lambda^n v - \frac{1}{\sqrt{5}} \mu^n w$$

$$= \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n \begin{pmatrix} 1 \\ \lambda \end{pmatrix} - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n \begin{pmatrix} 1 \\ w \end{pmatrix}.$$

Top entry:

$$\cancel{F_n} \boxed{F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.}$$

this term goes to 0 as $n \to \infty$ since $\left|\frac{1-\sqrt{5}}{2}\right| \sim 0.6 < 1$.

so $F_n \approx \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n$

Linear Recurrence sequence.

<u>Ex</u> <u>Def</u> Define a sequence by

$S_0 = 1$

$S_1 = 2$ and $S_{n+1} = 3S_n - 4S_{n-1} + 5S_{n-2}$

$S_2 = 3$

$3\cdot 3 - 4\cdot 2 + 5\cdot 1$

$1, 2, 3, 6, 26, \ldots$

$3\cdot 6 - 4\cdot 3 + 5\cdot 2$

"Fibonacci-like sequence"

You can always analyze it in the same way!

For that one, consider the matrix:

remember the two terms

top is "oldest term"

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 5 & -4 & 3 \end{pmatrix}$$

then

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 5 & -4 & 3 \end{pmatrix}\begin{pmatrix} S_{n-2} \\ S_{n-1} \\ S_n \end{pmatrix} = \begin{pmatrix} S_{n-1} \\ S_n \\ 5S_{n-2} - 4S_{n-1} + 3S_n \end{pmatrix}$$

$$= \begin{pmatrix} S_{n-1} \\ S_n \\ S_{n+1} \end{pmatrix}.$$

to find S_n:

compute:

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 5 & -4 & 3 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

find eigenvalues & eigenvectors!

This week: knot theory

What is a knot?

- A closed loop in $\mathbb{R}^3$

- A function $f: \mathbb{R} \to \mathbb{R}^3$ periodic.

$\cancel{f: \mathbb{R} \to}$

$0 \le t \le 1$

- $f: [0,1] \longrightarrow \mathbb{R}^3$

$f(t) = (x(t), y(t), z(t))$

f must be <u>continuous</u> (infinitely differentiable)

(you can draw without lifting pen)

$f(0) = f(1)$

(so it joins up)

otherwise $f(a) \neq f(b)$

for any a and b.

(so it doesn't cross itself)

Definition

A <u>knot</u> is an infinitely differentiable function $f: [0,1] \to \mathbb{R}^3$ given by $f(t) = (x(t), y(t), z(t))$ satisfying:

1) $f(0) = f(1)$
2) $f(a) \neq f(b)$ unless $a = b$ (with exeption of $[0,1]$).

Two knots are <u>isotopic</u> if:
(think: the same)

Say $f:[0,1]\to\mathbb{R}^3$

$g:[0,1]\to\mathbb{R}^3$

there exists a family of knots

$\cancel{f_s:[0,1]\to}$ $f_s:[0,1]\to\mathbb{R}^3$ $(0\le s\le 1)$

~~such~~ smoothly varying as s varies and with

$f_0=f$, $f_1=g$.

<u>Question</u> - How can we tell if two knots are isotopic?

- How can we tell if a knot can be untied? (I.e. isotopic to the unknot)

From playing with knots:

- The trefoil is <u>not</u> isotopic to its reverse.
  overhand knot — mirror image
  "chiral"
- The figure eight knot <u>is</u> isotopic to its reverse.
  "amphichiral"

It's hard to tell whether two knots are isotopic!

It's hard to tell whether a knot is isotopic to the unknot!

Those are the "Perko pair": for 75 years thought to be different knots.

How to prove left-handed trefoil is different from right-handed and both are different from unknot?

Idea: Assign numbers to a knot.

If two knots give different answers, they must be different knots.

→ But: need a number that doesn't depend on the exact way the knot is presented.

The <u>crossing number</u> of a knot is the minimum number of times the rope crosses itself in a 2D picture

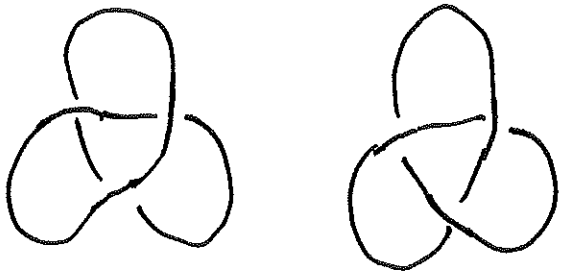
<u>Ex</u> Crossing number of (left- or right-) trefoil is 3.

↳ a) How can you prove it's 3? (⇒ not unknot, or figure eight) which has crossing number 4.

b) This can't distinguish handedness.

"Knot invariants"

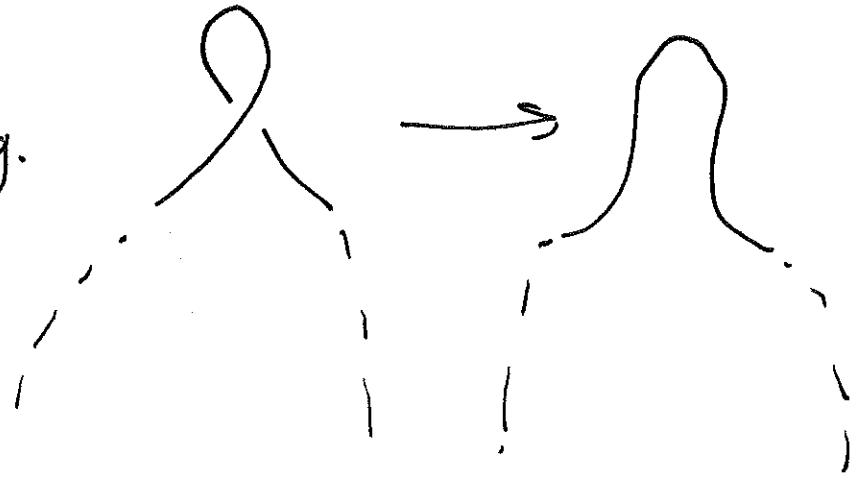
A <u>knot diagram</u> is a 2D picture of a knot, showing which strand goes on top at every crossing:



unknot trefoil

How can we draw isotopies in knot diagrams? What moves can we perform of a knot diagram without changing the knot?

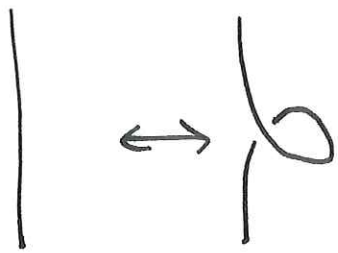
e.g.



Any isotopy can be made as a combination of three basic moves:

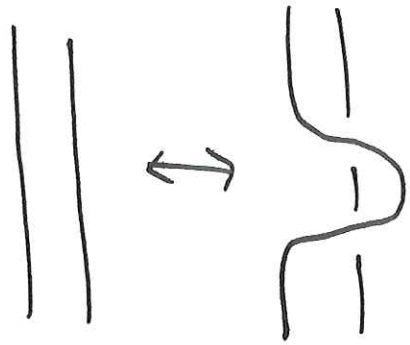
("Reidemeister moves")

1)



untwist

2)



cross over

3)

pass over a crossing
(or under)

Every isotopy can be broken down into these steps! (Annoying to prove, though.)

Def A knot is <u>tricolorable</u> if (True/False invariant, not a number)

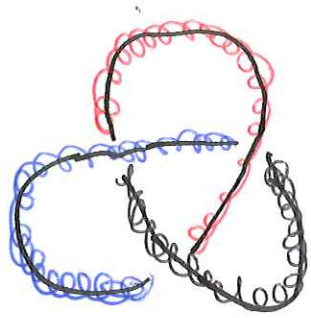
in a knot diagram for the knot,

we can color each arc of the knot

with one of three colors, such that:

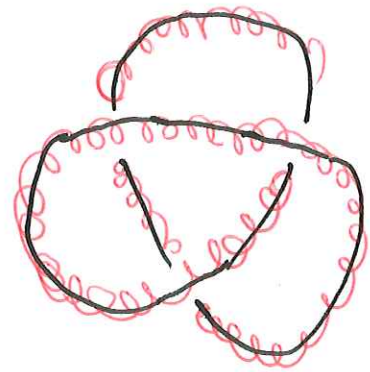
1) At each crossing, either only one color, or all three colors appear.

2) At least two colors are used.



trefoil

tricolorable

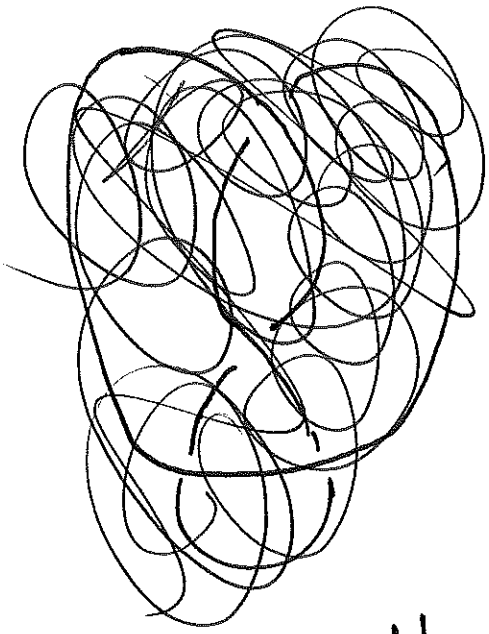


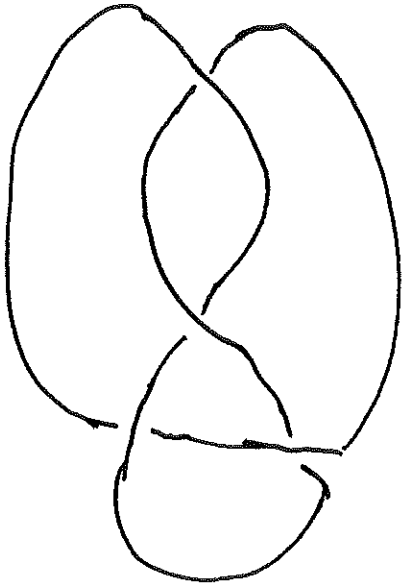
unknot

not tricolorable

(we still need to check that Reidemeister moves don't affect tricolorability!)

Is figure eight tricolorable?





No

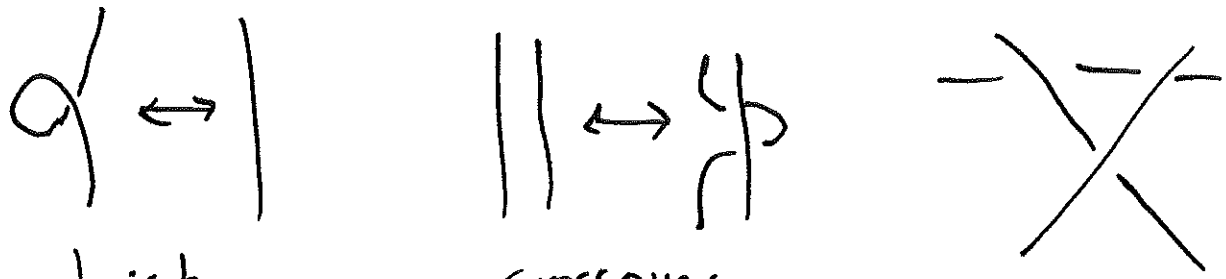
→ not the same as trefoil

→ but maybe the same as unknot?

Recap

→ We defined a knot and a knot diagram.

→ We defined three Reidemeister moves:



twist
I

crossover
II

passover
III

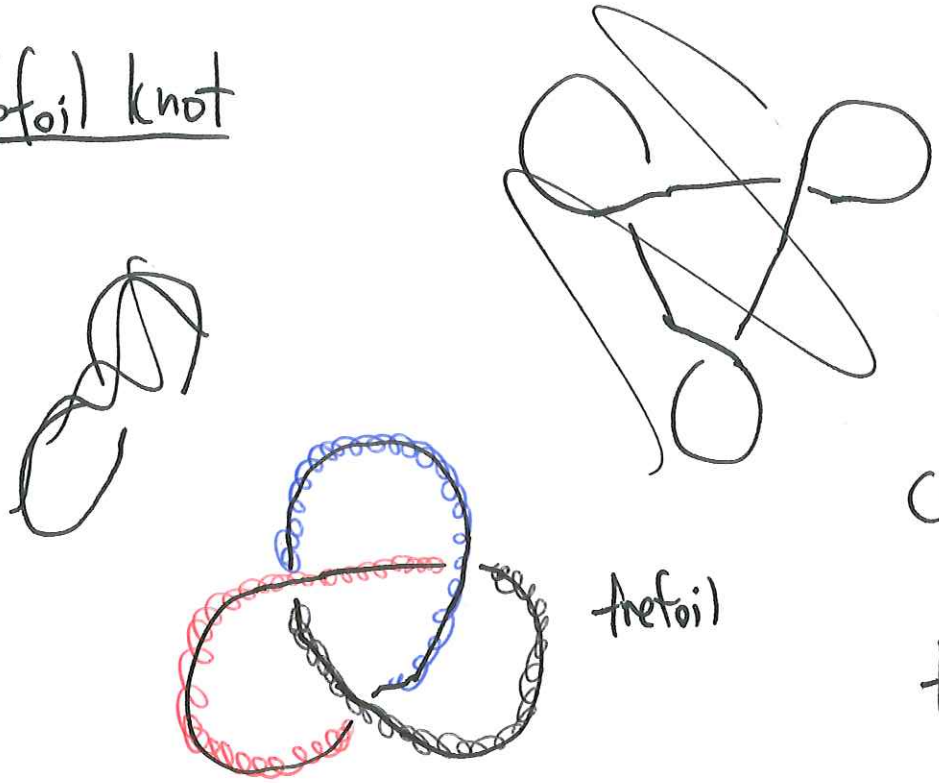
Properties of knots:

- crossing number (minimal number of crossings in a diagram)
- tricolorability
- chirality (is knot same as reverse?)

...

Today:
- bridge number
- Alexander polynomial

Trefoil knot



trefoil

tricolorable:

Crossing number?

3

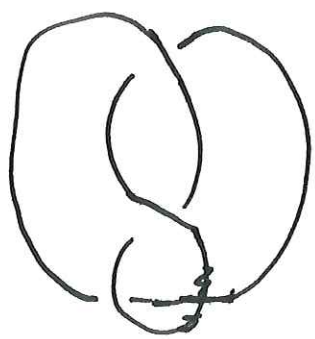
tricolorable?

yes

chiral? (different from reverse, or same)

yes (different)

Figure eight



crossing number?

4

tricolorable?

no

chiral?

no (amphichiral/achiral)

Unknot

crossing number?

0

tricolorable?

no

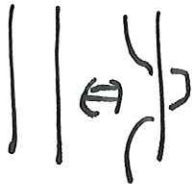
chiral?

amphichiral

- Tricolorability unaffected by Reidemeister moves
- Proofs for crossing numbers.

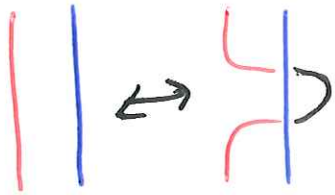
Suppose K is tricolorable. If we perform any Reidemeister moves, it stays that way. (needs checked for all three moves)

ex. <u>Type II</u>. existing tricolor could be either.



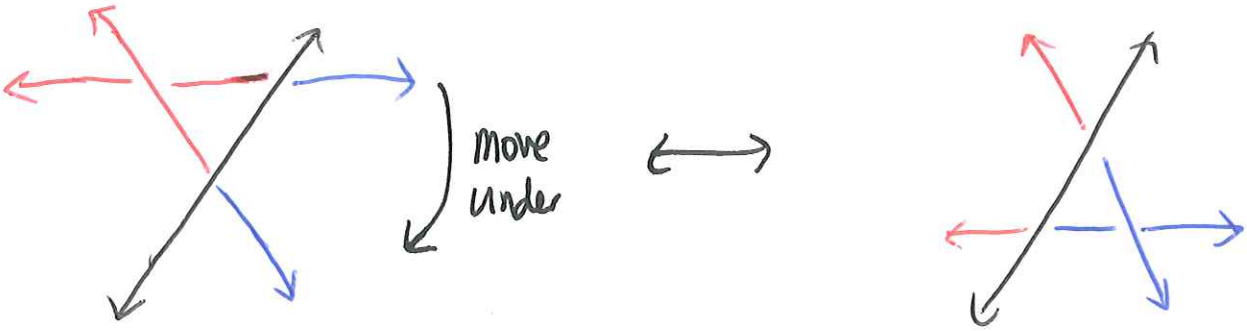
a)

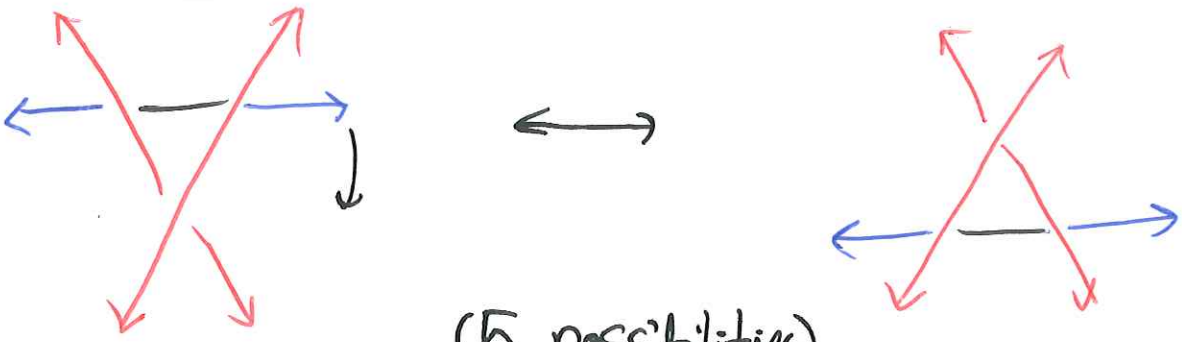
all reversible!

b) 

we need to get a tricoloring on new diagram without changing colors of "outbound" strands.

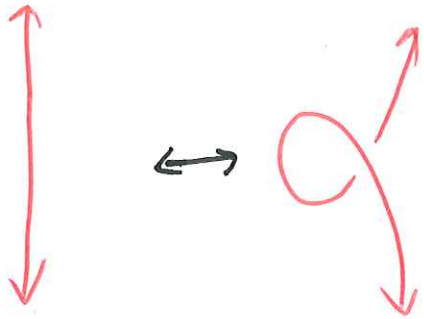
Type III





(5 possibilities)

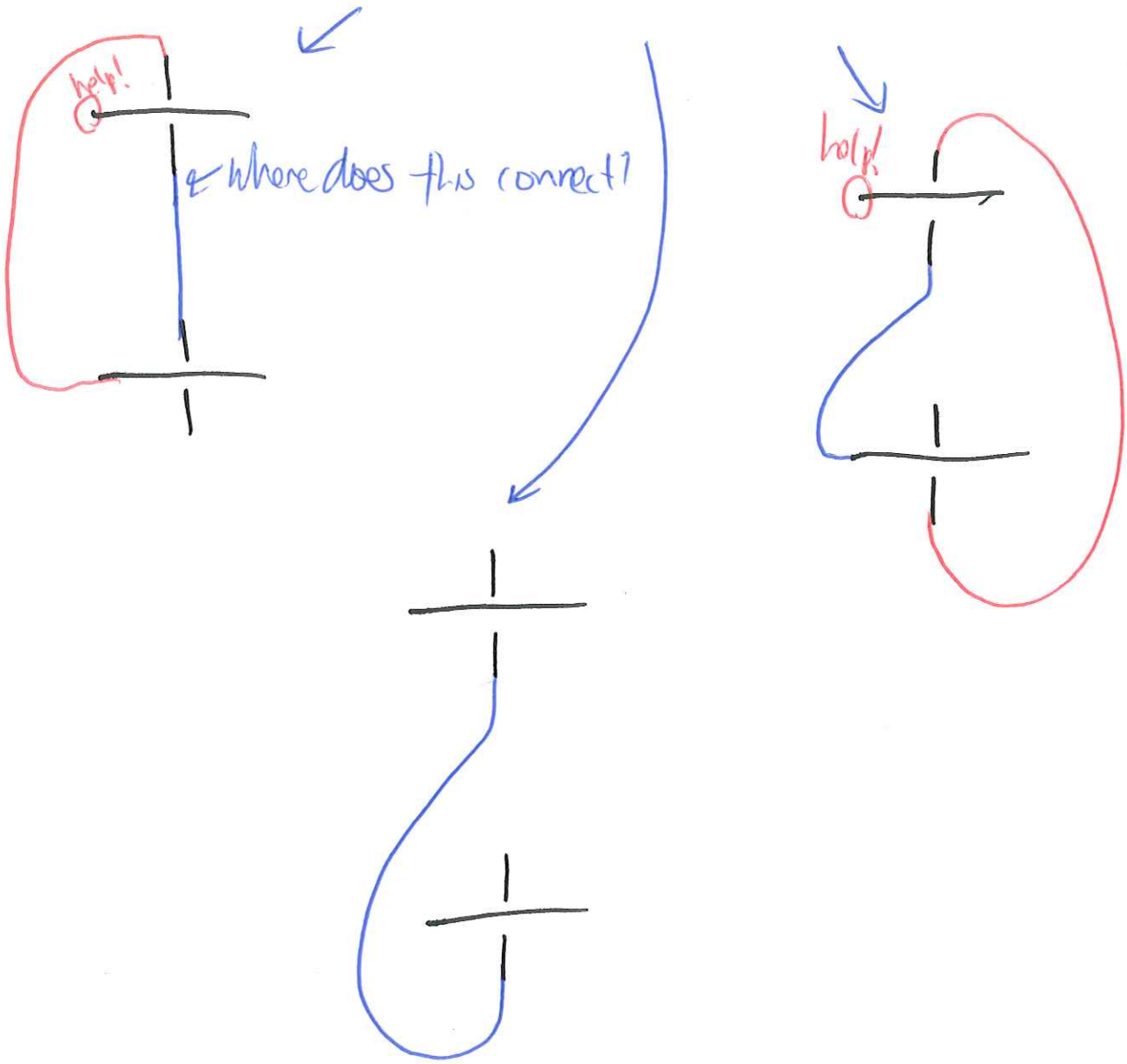
Type I



Two-crossing knots

/ first step

Is there a knot with crossing number two? / 2nd



No! All are unknots.

→ Crossing numbe

<u>Theorem</u> Trefoil is ~~actually~~ not isotopic to the unknot, and $cr(\text{trefoil}) = 3$.

<u>Pf.</u> It's tricolorable, and the unknot isn't.
(and tricolorability is isotopy invariant)

$cr(K) \leq 3$ because we can draw it with 3 crossings.

$cr(K) \neq 2$ because any knot with crossing number 2 is unknot (but trefoil is not unknot)

$cr(K) \neq 1, 0$ for same reason.

How to prove crossing number of fig 8 is 4?

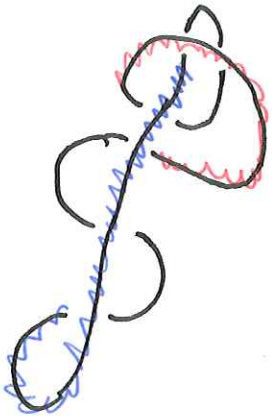
(Prove anything with 3 is trefoil or unknot
and prove figure eight is not unknot)

Crossing number too hard to compute!! Useless invarient. Tricolorability not precise enough.

We need more invariants!

(these have same defect as crossing #; hard to compute)

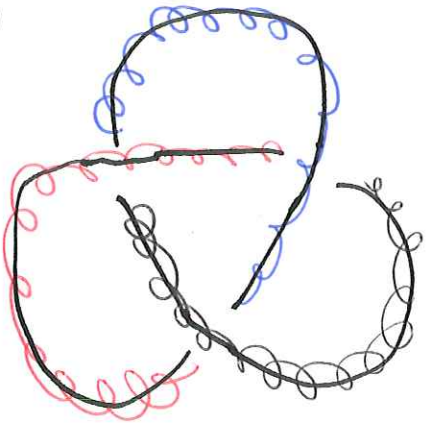
Bridge number



a <u>bridge</u> in a knot diagram is an arc that makes 1 or more overcrossings

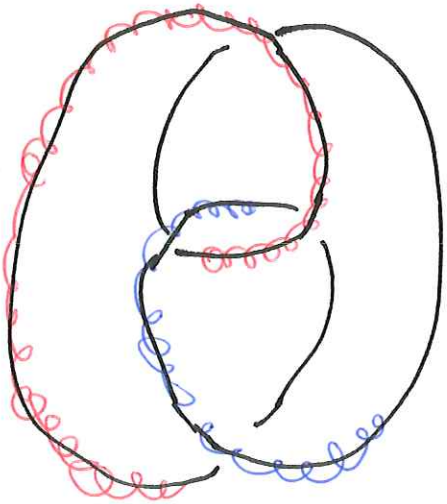
the bridge number of a knot is the minimum number of bridges in a diagram for the knot.

Trefoil?



at most 3...

it's actually just 2!



Next time:

Come up with more invariants that aren't changed by Reidemeister moves, since much easier to calculate

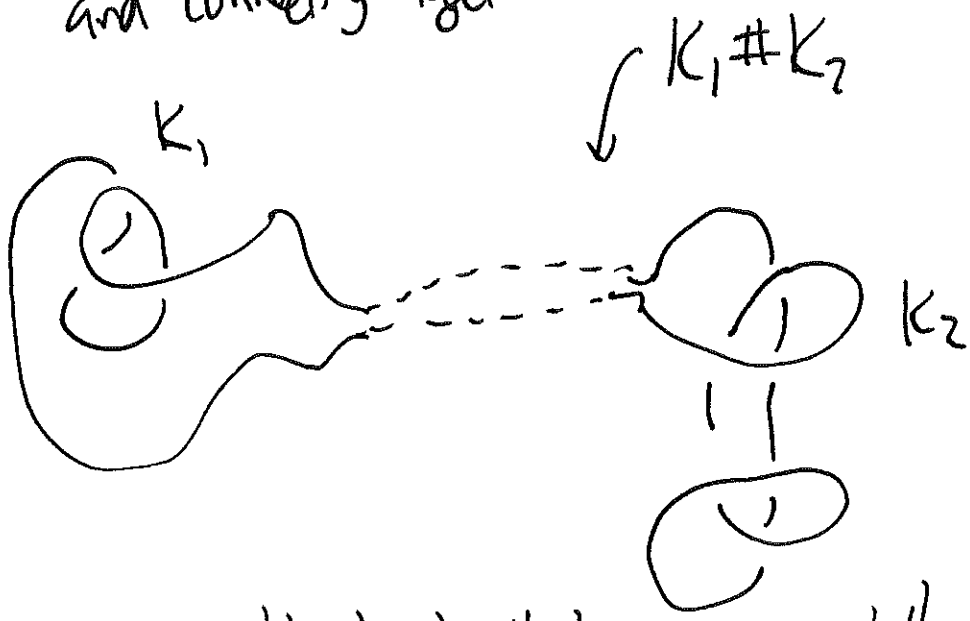
Mostly associate a polynomial to a knot: Alexander poly
Jones poly
HOMFLY poly
...

("Skein relations")

Connected Sum

If K_1, K_2 are two knots,

$K_1 \# K_2$ is obtained by cutting both open and connecting together.



Seems like it shouldn't depend on where we cut it.

this does depend on having an <u>orientation</u> on the knot: a chosen direction to walk along the knot.

1) Is (right-handed trefoil) # (left-handed trefoil)

$\parallel$ "square knot"

(right-hand trefoil) # (right-handed trefoil)

"granny knot"

2) What's $cr(K_1 \# K_2)$ in terms of $cr(K_1)$ and $cr(K_2)$

3) Could $K_1 \# K_2$ be the unknot even if neither knot is?

i) A knot is a <u>prime knot</u> if it can't be written as a sum of two other nontrivial knots.

→ square/granny knots are <u>not</u> prime.

→ figure 8/trefoil <u>are</u> prime.

Every knot can be broken down into prime knots in a unique way. (a bit hard to prove.)

2) $cr(K_1 \# K_2) \leq cr(K_1) + cr(K_2)$

<u>Open problem</u>: Is it always equal?

(probably yes)

3) Could $K_1 \# K_2 = \bigcirc$?

If 2) true, couldn't happen.

Let's prove it's impossible.

Classic wrong proof.

$$1 = 1 + 0 + 0 + 0 + \cdots$$

$$= 1 + (-1 + 1) + (-1 + 1) + (-1 + 1) + \cdots$$

$$= (1 + -1) + (1 + -1) + (1 + -1) + (1 + -1) + \cdots$$

$$= 0 + 0 + 0 + 0 + \cdots = 0$$

rebracketing non-convergent infinite series doesn't work.

Another warning:

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \cdots$$ converges to $\log 2$. AKA $\ln 2$

But! You can reorder terms and make it convergen to anything you want.

For knots, this proof is correct(able)!

"Mazur's swindle"

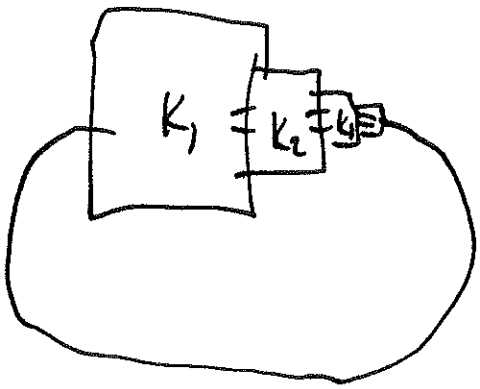
Suppose $K_1 \# K_2 = 0$

$$K_1 = K_1 \# (K_2 \# K_1) \# (K_2 \# K_1) \# (K_2 \# K_1) \# \cdots$$

$$= (K_1 \# K_2) \# (K_1 \# K_2) \# (K_1 \# K_2) \# \cdots$$

$$= 0 \# 0 \# 0 \# 0 = 0 \quad \text{so } K_1 = 0. \ (\text{ditto } K_2)$$

You can always take an infinite sum of knots by making them smaller and smaller and smaller

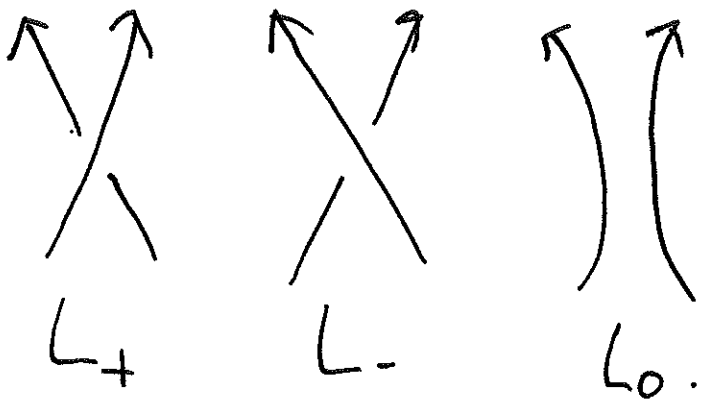


size of $K_n = 1/2^n$

Alexander polynomial

Definition using "Skein relations".

Suppose we have three oriented knots, that only differ in one crossing:



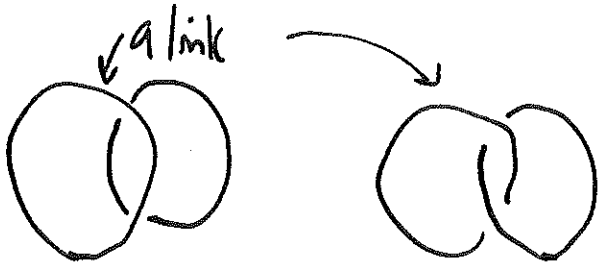
The <u>Alexander polynomial</u> $\Delta_K(t)$ is defined recursively by two rules:

1) $\Delta_K(\text{unknot}) = 1$

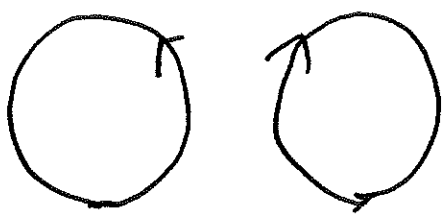
2) $\Delta_{L_+} - \Delta_{L_-} + (t^{+1/2} - t^{-1/2})\Delta_{L_0} = 0$

(so if you know Δ for two, you can get the third)

This is defined not just for knots, but also links:



Warm-up: Δ for two disjoint unknots



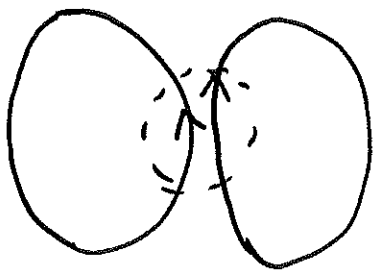
$$\Delta_{L_+} - \Delta_{L_-} + (t^{1/2} - t^{-1/2})\Delta_{L_0} = 0$$

$$1 - 1 + (t^{1/2} - t^{-1/2})\Delta_{L_0} = 0$$

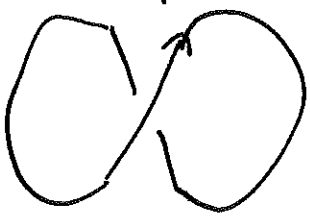
$$\boxed{\Delta_{L_0} = 0}$$

(really $\Delta_{L_0}(t) = 0$)

L_0

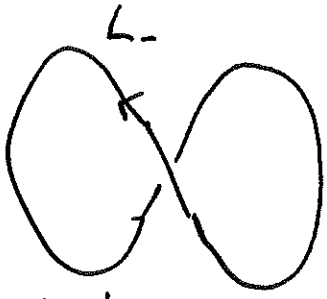


L_+

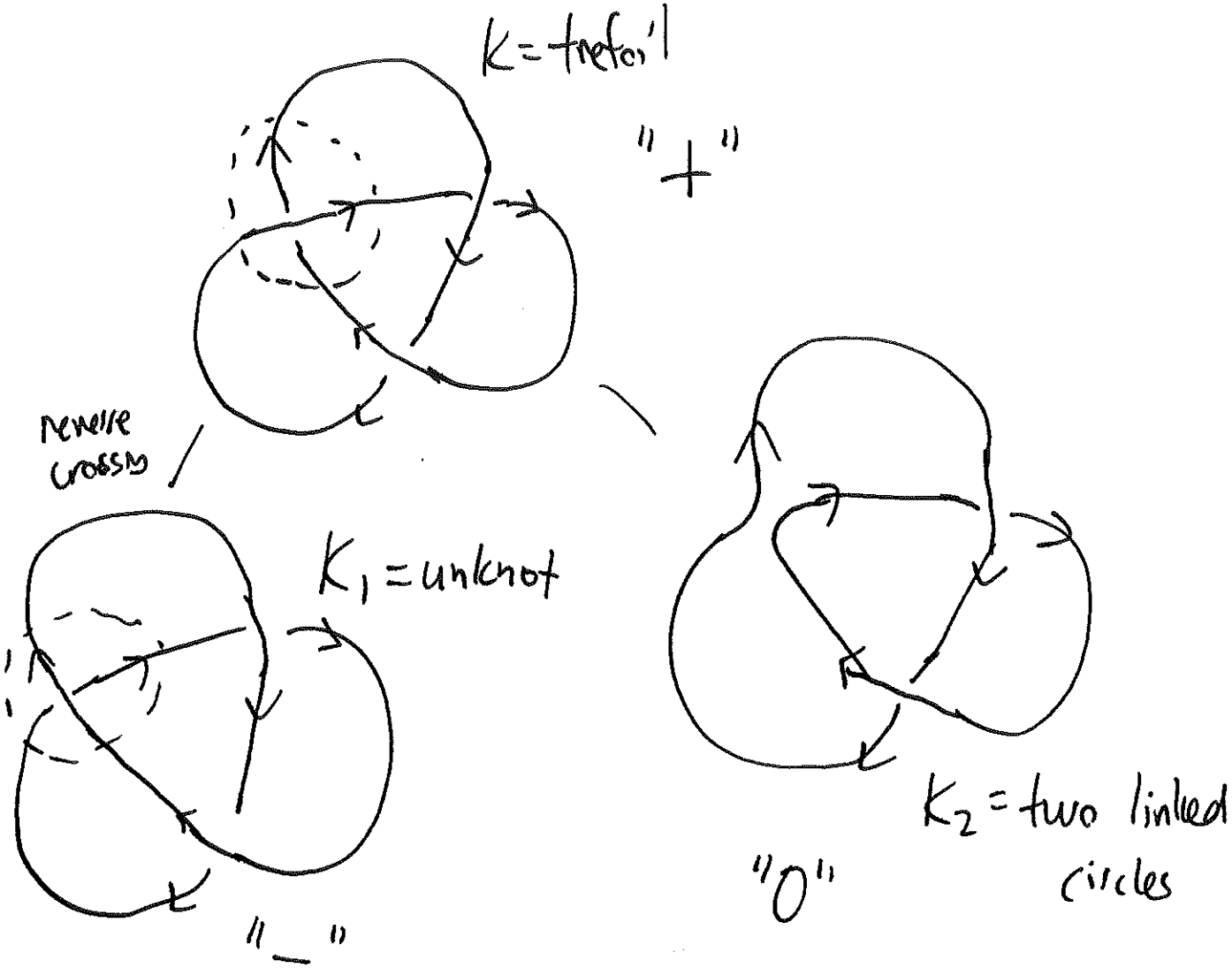


unknot

L_-



unknot



$$\overset{+}{\Delta_K} - \overset{-}{\Delta_{K_1}} + (t^{1/2} - t^{-1/2})\overset{0}{\Delta_{K_2}} = 0$$

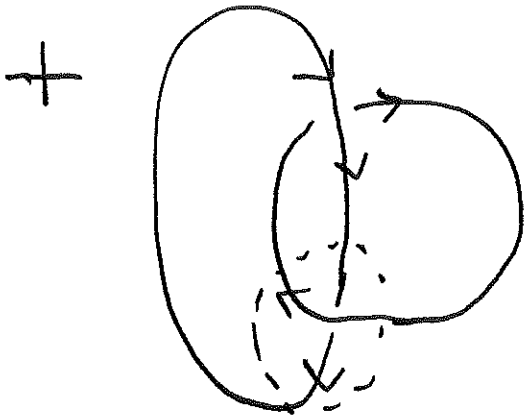
Δ_{K_2} on next page

$$\Delta_K - 1 + (t^{1/2} - t^{-1/2})\left(-(t^{1/2} - t^{-1/2})\right) = 0$$

$$\Delta_K = 1 + (t^{1/2} - t^{-1/2})^2 = 1 + (t - 2 + t^{-1})$$

(negative powers of t and half-int) $\longrightarrow$ $\boxed{= t - 1 + t^{-1}}$

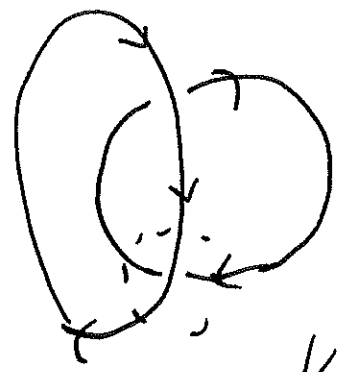
K_2 = two linked circles



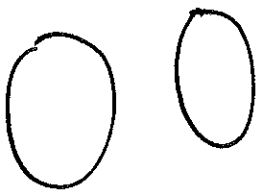
$$\Delta_{K_2} - \Delta_{K_3} + (t^{1/2} - t^{-1/2})\Delta_{K_4} = 0$$

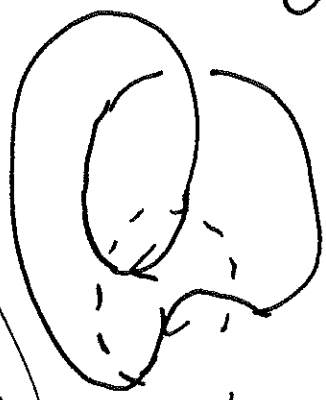
$$\Delta_{K_2} - 0 + (t^{1/2} - t^{-1/2})1 = 0$$

$$\Delta_{K_2} = -(t^{1/2} - t^{-1/2})$$



K_3 = disjoint circles





K_4 = unknot

Things to check

- not affected by Reidemeister
- these rules actually define it for any knot

HW Calculate $\Delta_{\text{figure 8}}$.

(you should get $3 - t - t^{-1}$)

$\longrightarrow$ not trefoil

$\longrightarrow$ not unknot!

But:

$$\Delta_K = \Delta_{\text{reverse}(K)}$$

(e.g. left- and right-handed trefoil give same answer)

$$\Delta_{K_1 \# K_2} = \Delta_{K_1} \Delta_{K_2} \quad \text{(HW!)}$$

So

$$\Delta_{\text{square knot}} = \Delta_{\text{right trefoil}} \cdot \Delta_{\text{left trefoil}}$$

$$= (t - 1 + t^{-1})(t - 1 + t^{-1})$$

$$= (t - 1 + t^{-1})^2$$

$$\Delta_{\text{granny knot}} = \Delta_{\text{right trefoil}} \cdot \Delta_{\text{right trefoil}}$$

$$= (t - 1 + t^{-1})^2$$

Δ can't tell the difference between square and granny knots!

Enter the Jones polynomial:

$$\frac{1}{t}\Delta_{K_+} - t\Delta_{K_-} = \left(\sqrt{t} - \frac{1}{\sqrt{t}}\right)\Delta_{K_0}.$$

Calculate in the same way!

→ Jones polynomial <u>can</u> tell difference between square + granny knots.

→ and between left and right trefoils!

but even this can't tell all knots apart...

Need new invariants... Khovanov homology...

Real analysis (the definitions and proofs behind calculus)

What do we mean when we say "The sequence x or $\{x_n\}_{n\geq 1}$ or $\langle x_n \rangle$ or $x_1, x_2, x_3, x_4, \ldots$ has limit L"?

→ the values of the terms are all getting close to L.

$\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \ldots$ converges to 2?
(of course not!)

distance from x_n to L.

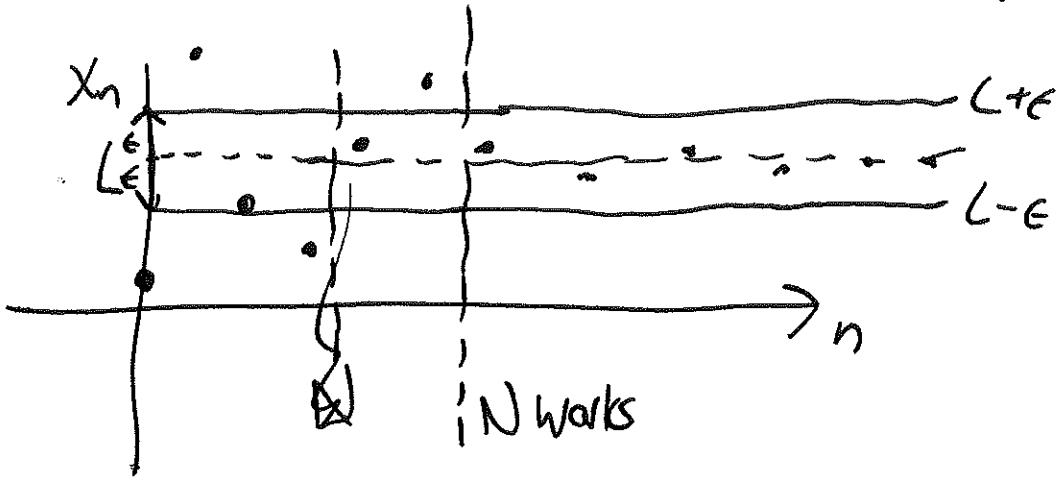
so $|x_n - L|$ approaches 0. ← what does that mean?

get infinitely close...

Does $\frac{1}{2}, \frac{2}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{2}{4}, \frac{1}{5}, \frac{2}{5}, \ldots$

approach 0? (Yes!)

Def $x_1, x_2, x_3, x_4, \ldots$ converges to L if for every $\epsilon > 0$, there exists an N (depends on ϵ), so that if $n > N$ then $|x_n - L| < \epsilon$.



Theorem The sequence defined by $x_n = 3 + 2/n$ converges to the limit $L = 3$.

Pf. Suppose that $\epsilon > 0$ is given. Take $N = 2/\epsilon$.

If $n > N$, then $n > 2/\epsilon$ and so $\epsilon > 2/n$.

Then if $n > N$,

$$|x_n - L| = |(3 + 2/n) - 3| = \left|\frac{2}{n}\right| = \frac{2}{n} < \epsilon.$$

Where did $N = 2/\epsilon$ come from?

I wanted $|(3+2/n)-3| < \epsilon$, so how big does n need to be the guarantee this?

Needed $\left|\frac{2}{n}\right| < \epsilon$ so $\frac{2}{n} < \epsilon$ i.e. ~~$n > \epsilon/2$~~

$n > \underline{\underline{2/\epsilon}}$. So I used $N = 2/\epsilon$.

usually do this before sitting down to write proof.

<u>Ex</u> a) $x_n = 2 + 1/\sqrt{n}$

b) $y_n = \frac{n+1}{n-1}$

find limit, and prove it using definition.

c) Prove that if $x_n \to L$ and $y_n \to M$ then $x_n + y_n \to L + M$.

a) $x_n = 2 + 1/\sqrt{n}$.

$L = 2$.

Pf. Suppose $\epsilon > 0$. Let $N = 1/\epsilon^2$. If $n > N$,

then $n > 1/\epsilon^2$, and so $\epsilon^2 > \frac{1}{n}$, and $\epsilon > \frac{1}{\sqrt{n}}$.

Then $|x_n - L| = \left|\left(2 + \frac{1}{\sqrt{n}}\right) - 2\right| = \left|\frac{1}{\sqrt{n}}\right| = \frac{1}{\sqrt{n}} < \epsilon$.

---

b) $y_n = \frac{n+1}{n-1}$ Scratch work: limit is 1. We want

$\left|\frac{n+1}{n-1} - 1\right| < \epsilon$; how big does n need to be?

$\frac{n+1}{n-1} - 1 = \frac{n+1}{n-1} - \frac{n-1}{n-1} = \frac{2}{n-1}$, want $< \epsilon$.

$\frac{2}{n-1} < \epsilon$. $\frac{2}{\epsilon} < n - 1$, so $n > \boxed{\frac{2}{\epsilon} + 1}$

that's N

c) Suppose x_n converges to L

and y_n converges to M.

Then $x_n + y_n \to L + M$.

<u>Pf.</u> Suppose $\epsilon > 0$. We know there's a value N_1 so that if $n > N_1$, $|x_n - L| < \epsilon/2$. There's another cutoff N_2 so that if $n > N_2$ then $|y_n - M| < \epsilon/2$. Take $N = \max(N_1, N_2)$.

If $n > N$, then both $n > N_1$ and $n > N_2$. This means

$$|(x_n + y_n) - (L + M)| = |(x_n - L) + (y_n - M)| \leq |x_n - L| + |y_n - M|$$
$$< \epsilon/2 + \epsilon/2 = \epsilon.$$

Similar rules for product, quotient, ...

Product formula

Suppose $x_n \to L$, $y_n \to M$. Then $x_n y_n \to LM$.

Pf We'll use some inequality tricks:

$$|x_n y_n - LM| = |(x_n - L)y_n + L(y_n - M)|$$

$$\leq |(x_n - L)y_n| + |L(y_n - M)|$$

$$= |x_n - L|\,|y_n| + |L|\,|y_n - M|$$

want: $< \epsilon$.

Need: $|x_n - L||y_n| < \epsilon/2$ and $|L|\,|y_n - M| < \epsilon/2$.

to get this, pick N_2 so if $n > N_2$ then $|y_n - M| < \frac{\epsilon}{2|L|}$. If $L = 0$ any N_2 works.

y_n converges to M, so $|y_n| \leq |M| + 1$ for $n > N_0$.
(since $|y_n - M| < 1$)

then take N_1 so $|x_n - L| < \frac{\epsilon}{2(|M|+1)}$.

Let $N = \max(N_0, N_1, N_2)$

Limit points

If $x_1, x_2, x_3, x_4, x_5, \ldots$ is a sequence, a <u>subsequence</u> is a new sequence obtained by removing terms.

$$1, -1, 1, -1, 1, -1, 1, -1, 1, -1$$

sequence has no limit

One subsequence:

$$1, 1, 1, 1, 1, 1, \ldots$$

$$-1, -1, -1, -1, -1, \ldots$$

but subsequences do!

$$1, 1, -1, -1, 1, 1, -1, -1, 1, 1, \ldots$$

(not this one)

A <u>limit point</u> of a sequence is a number R that's a limit of some subsequence.

Q Can you find a sequence with two limit points?

- 10 limit points?
- Infinitely many?
- All positive integers?
- All numbers $0 \le R \le 1$?

Integers:

$1, 1, 2, 1, 2, 3, 1, 2, 3, 4, 1, 2, 3, 4, 5, \ldots$

k is limit of subsequence $k, k, k, k, k, k, \ldots$

$0 \le R \le 1$: almost the "Farey sequence"

$\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \ldots$

Why is $\pi/4$ a limit point?

$\pi/4 \approx 0.785398\ldots$ $\quad \frac{7}{10}, \frac{78}{100}, \frac{785}{1000}, \frac{78539}{100000}, \ldots$ converges to $\pi/4$.

<u>Theorem</u> (Bolzano-Weierstrass)

Suppose $x_1, x_2, x_3, \ldots$ is a bounded sequence.

(There are A, B so $A < x_n < B$ for every n).

Then it has a subsequence that converges.

This doesn't work if your sequence isn't bounded:

$1, 2, 3, 4, 5, 6, 7, 8, \ldots$

<u>Series</u> What does it mean that $\sum_{n=1}^{\infty} a_n$ converges?

Define a sequence:

$$S_i = \sum_{n=1}^{i} a_n \quad \text{the "sequence of partial sums"}$$

If sequence S_i converges, we say series converges.

Ex $a_n = \frac{1}{2^n}$ $\quad \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \ldots$

$\sum_{n=1}^{\infty} a_n$ converges.

$S_1 = \frac{1}{2}$

$S_2 = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}$

$S_3 = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} = \frac{7}{8}$

$S_4 = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} = \frac{15}{16}.$

$S_i = 1 - \frac{1}{2^i}.$

converges to 1 ✓

Continuity

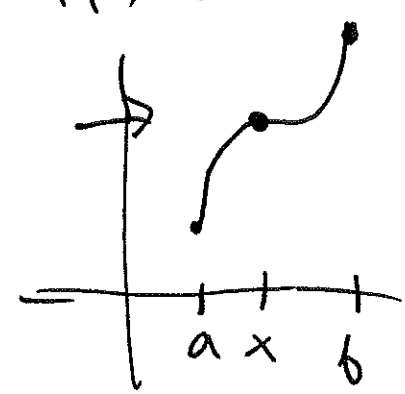
Intuition: a continuous function is a function you can graph without lifting your pen.

How to make this a precise definition?

We want a definition of "continuous" that guarantees all the important theorems are true:

- Intermediate Value Theorem:

  If $f(x)$ is continuous, and $a < b$, then c is between $f(a)$ and $f(b)$, there exists an x with $a \le x \le b$ so $f(x) = c$.



- $\frac{d}{dx} \int_a^x \cancel{f(t)\,dt}\ f(t)\,dt = f(x)$ FTC:

can you even integrate every continuous fct?

Old, defunct def of continuous:

$f(x)$ is continuous if it satisfies the intermediate value theorem: given c with $f(a) \le c \le f(b)$, there exists x so $f(x) = c$.

A crazy function: Conway's Base-13 function.

(it satisfies above definition, but shouldn't count as continuous.)

Given x to compute $f(x)$:

1) Write x in base 13, using 0–9, A, B, C.
2) Turn A into "+", B into "−", C into ".".
3) If ends with:

   + or − (some numbers) . (some numbers, maybe infinite)

   then $f(x)$ = that.

4) If it doesn't end like that, $f(x) = 0$.

If

numbers

$x_{13} = 1AB.32CA9134C1347\ldots$

$\rightarrow 1+-.32.+9134.1347\ldots$

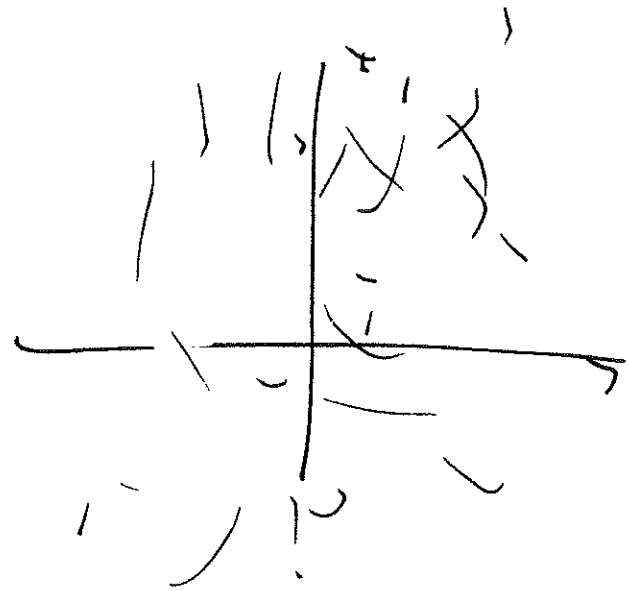
then $f(x) = +9134.1347\ldots$

$x_{13} = AB.12A12A12A12A\ldots$

$\rightarrow +-.12+12+12+12+\ldots$

$f(x) = 0$

No way to graph it!



Why does it satisfy IVT?

→ Given any a & b, and any target value c whatsoever (doesn't have to be between a and b), there's $x \in [a,b]$ so $f(x) = c$.

Challenge: $a = \pi = 3.141592$

$b = 2\sqrt{2} = 4.2\ldots$ $\quad c = e = 2.71828\ldots$

can put anything here and be $\in [a,b]$

$$x_{13} = 4.0000\overbrace{A2C}71828\,182845\ldots$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ + & & . \end{array}$$

then $f(x) = e$!

Modern definition (Cauchy, 1880s?)

First need to define limit of a function.

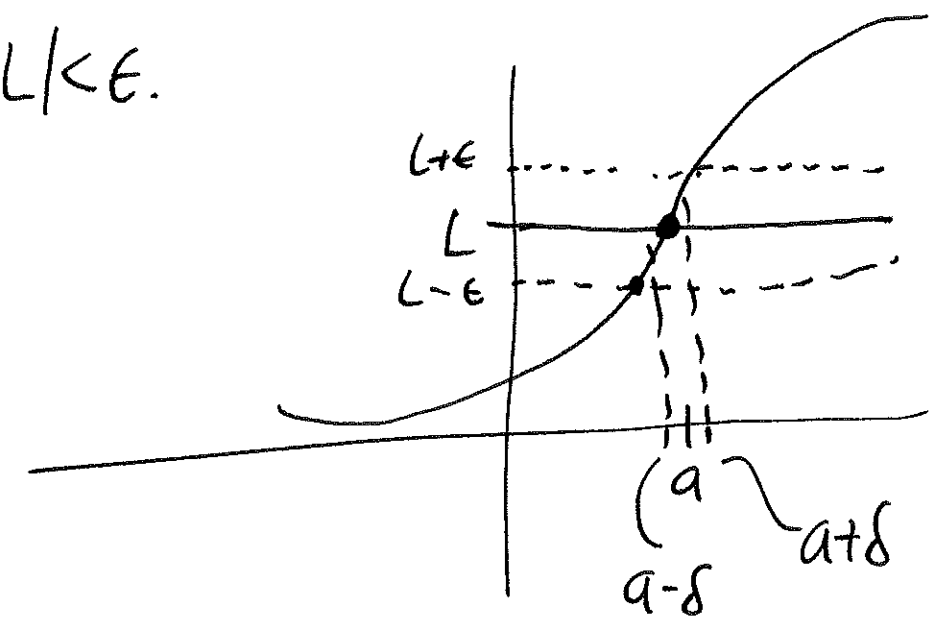
Suppose $f(x)$ is a function. We say

$\lim_{x \to a} f(x) = L$ if... for any $\epsilon > 0$,

x is within δ of a

there exists a $\delta > 0$ such that if $|x - a| < \delta$

then $|f(x) - L| < \epsilon$.



Prove that $\lim_{x \to 2} x^2 = 4$.

Suppose $\epsilon > 0$. You need to find δ so that if $|x-2| < \delta$, then $|x^2 - 4| < \epsilon$.

---

want:

$|x^2 - 4| < \epsilon$

$\underbrace{|x-2|}\ \underbrace{|x+2|} < \epsilon$.

We can make this as small as we want! by picking δ.

As long as we pick a δ that's ≤ 1, x will be between 3 and 5, so $|x+2| \leq 5$.

Suppose $\epsilon > 0$.

<u>Pf.</u> Take $\delta = \min(1, \epsilon/5)$.

This means $\delta \leq 1$ and $\delta \leq \epsilon/5$.

Then if $|x-2| < \delta$

$$|x^2 - 4| = \underbrace{|x-2|}\,\underbrace{|x+2|}$$
$$\leq (\epsilon/5)\cdot(5) = \epsilon.$$

we know $|x-2| < \delta$ so $|x-2| < 1$. This means $1 < x < 3$, so $3 < |x+2| < 5$

Another: Prove $\lim_{x \to 1} 3x = 3$

Suppose $\epsilon > 0$. You need a δ so that

if $|x-1| < \delta$ then $|3x-3| < \epsilon$.

<u>Pf.</u> Suppose $\epsilon > 0$. Let $\delta = \epsilon/3$. If $|x-1| < \delta = \epsilon/3$, then $3|x-1| < \epsilon$ so $|3x-3| < \epsilon$, which is what we wanted.

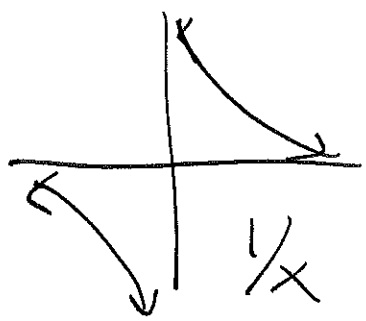
$\leftarrow |f(x) - L|$

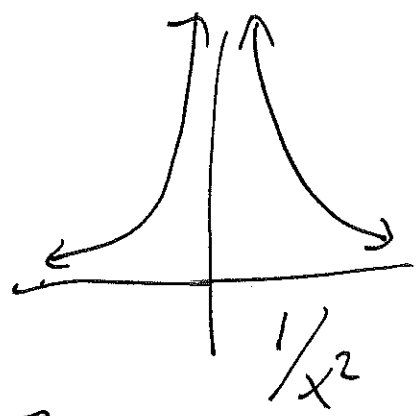
Def $f(x)$ is <u>continuous</u> if for any value of a,

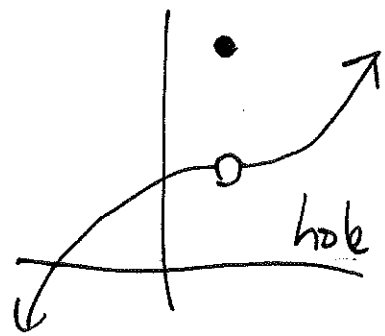
$\lim_{x \to a} f(x)$ exists (and is equal to $f(a)$.)

automatic if it exists

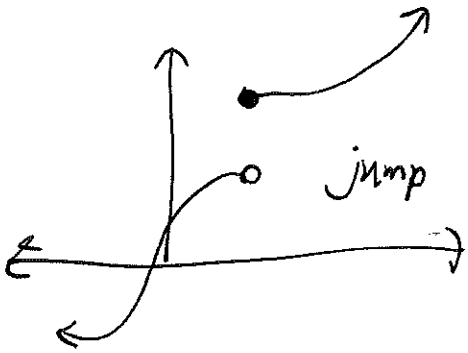
Some non-continuous functions.

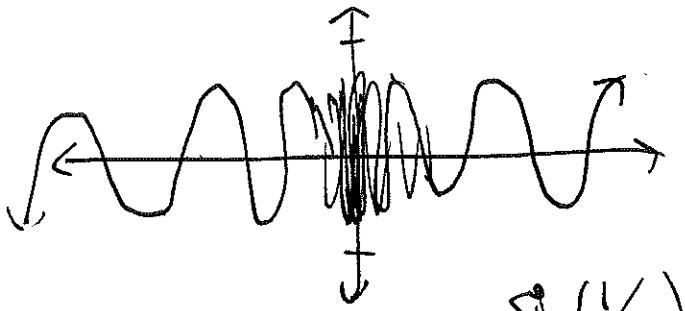






by our def limit doesn't exist





$\sin(1/x)$

$\lim_{x \to 0} \sin(1/x)$ doesn't exist.

Raindrop function

$$f(x) = \begin{cases} 1/q & \text{if } x \text{ is rational and } x = p/q. \\ 0 & \text{if } x \text{ is irrational} \end{cases}$$

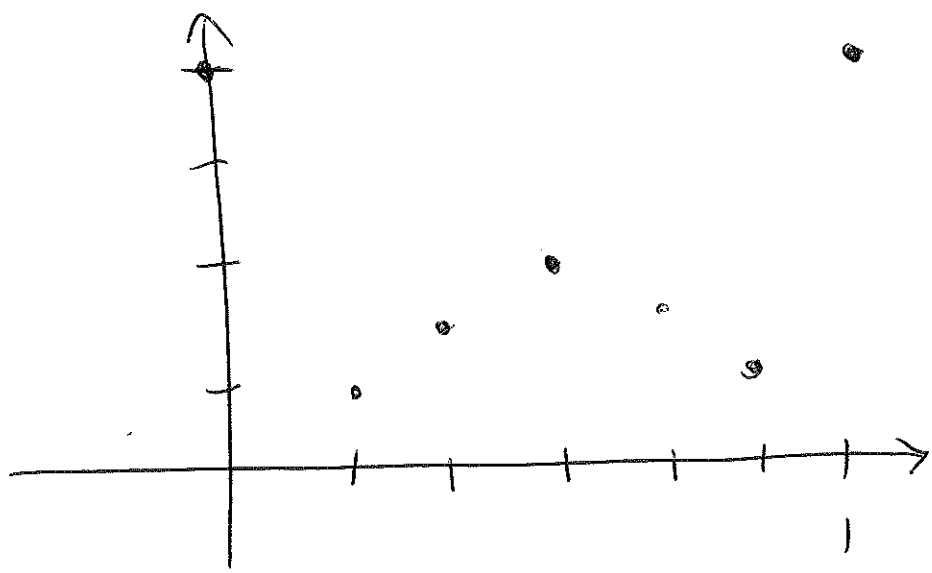
reduced

and $f(0) = 1$

e.g. $f(6/7) = 1/7$

are there a values where it is continuous at $x = a$?

$\lim_{x \to a} f(x)$ exists?



Is it continuous at $x = 1/2$? $f(x) = 1/2$

No! Take $\epsilon = 1/4$?

Can we find a δ so every x between

$(1/2 - \delta, 1/2 + \delta)$ has $|f(x) - f(1/2)| < \epsilon$

i.e. $1/4 < f(x) < 3/4$?

no! no matter how small δ is,

there's an irrational x is $(1/2 - \delta, 1/2 + \delta)$,

which has $f(x) = 0$.

I claim that if a is irrational then $f(x)$ is continuous at a.

e.g. $a = \frac{1}{\pi} = 0.318309\ldots$

Suppose we have $\epsilon = \frac{1}{10}$.

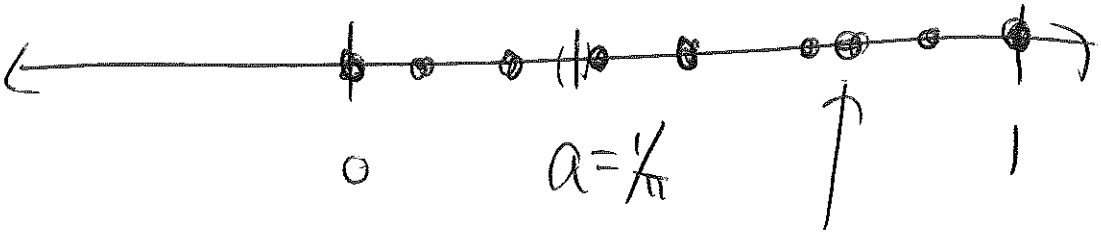
Trying to come up with δ so that if

$|x - \frac{1}{\pi}| < \delta$, then $|f(x) - f(1/\pi)| < \epsilon = \frac{1}{10}$.

so $|f(x)| < \frac{1}{10}$

But there are only finitely many x's for which $|f(x)| \geq \frac{1}{10}$!

$x = \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \ldots, \frac{1}{10}, \ldots, \frac{9}{10}$.



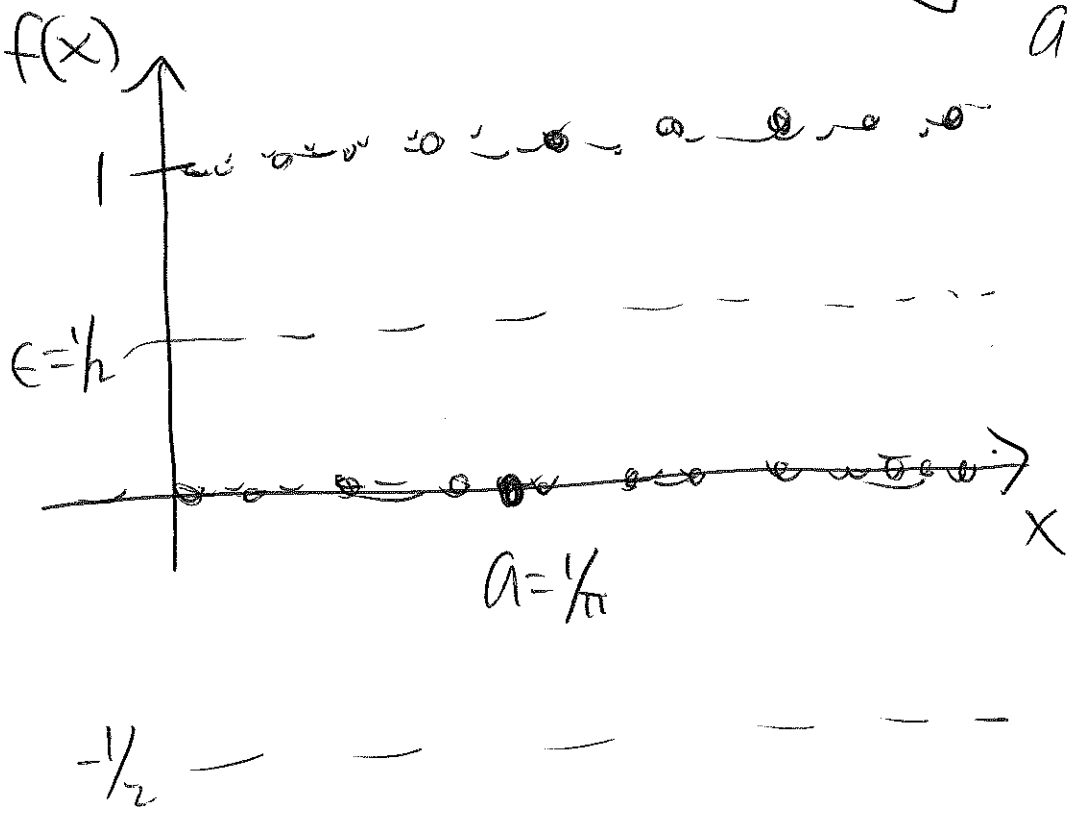
finitely many x values where $f(x) \geq \frac{1}{10}$

pick δ so

$(a-\delta, a+\delta)$ avoids these numbers!

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is rational} \\ 0 & \text{otherwise} \end{cases}$$

not continuous anywhere!



One more day of pathological functions

Last time:

- limits of functions: $\lim_{x \to a} f(x) = L$ for any $\epsilon > 0$, there exists δ so that if $|x-a| < \delta$, then $|f(x) - L| < \epsilon$.

- continuous functions:

  $\lim_{x \to a} f(x)$ exists at every a value.

Examples from last time	
Raindrop function $f(x) = \begin{cases} \frac{1}{q} & \text{where } x = \frac{p}{q} \text{ if } x \in \mathbb{Q} \\ 0 & \text{if } x \notin \mathbb{Q}. \end{cases}$	continuous at all irrational numbers! but not rational
Conway Base-13 function.	Satisfies IVT despite not continuous. On any interval $[a,b]$ obtains every real value.

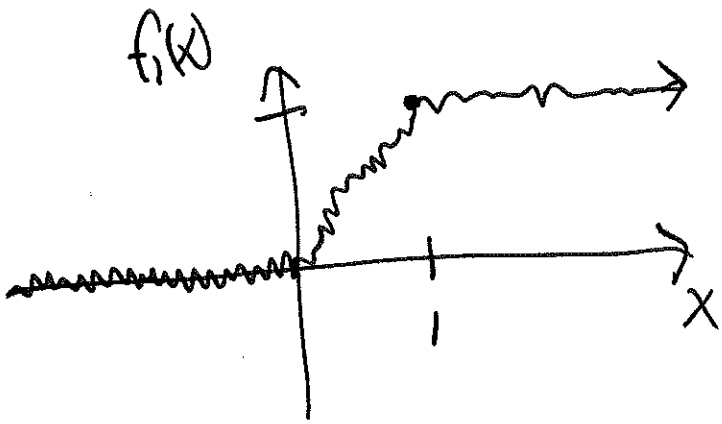
Suppose we have a sequence of continuous functions:

$$f_1(x),\ f_2(x),\ f_3(x),\ f_4(x),\ \ldots$$

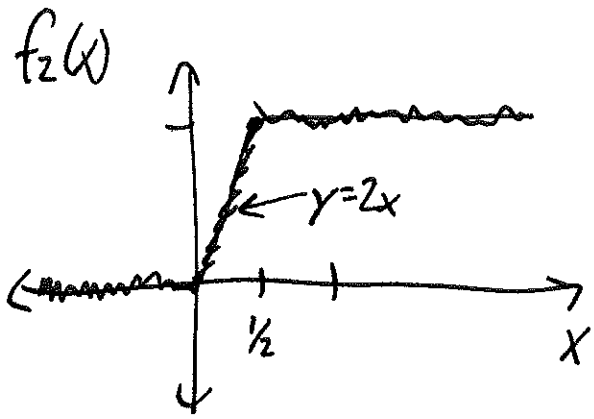
Define $f(x) = \lim_{n\to\infty} f_n(x)$, and assume limit exists for every x.

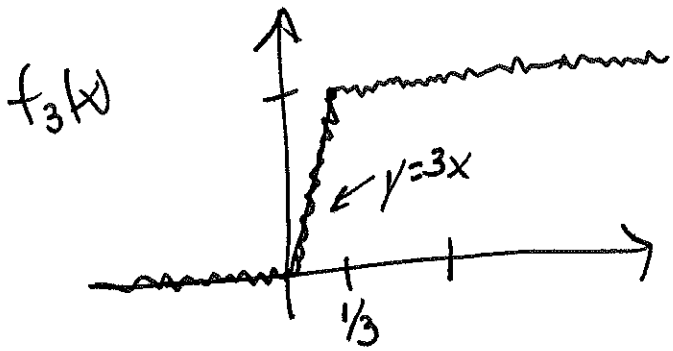
$\boxed{\text{Is } f(x) \text{ continuous?}}$ Maybe, maybe not!

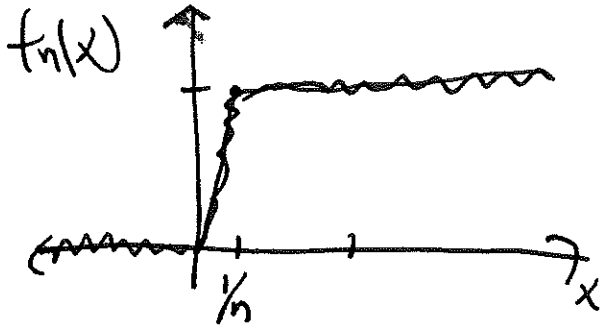
$f_1(x)$



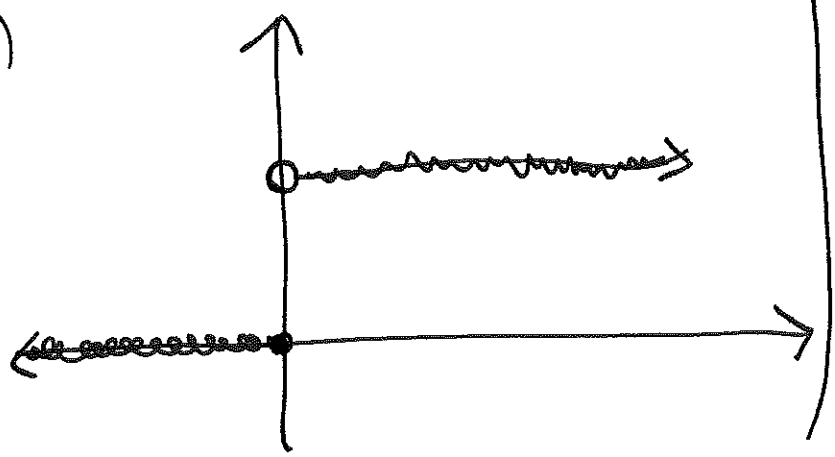
$f_2(x)$







$f(x) = \lim_{n\to\infty} f_n(x)$



Even though each $f_n(x)$ is continuous, the limit is not!

$f_1\left(\frac{1}{4}\right) = \frac{1}{4}$, $f_2\left(\frac{1}{4}\right) = \frac{1}{2}$, $f_3\left(\frac{1}{4}\right) = \frac{3}{4}$, $f_4\left(\frac{1}{4}\right) = 1$,

$f_5\left(\frac{1}{4}\right) = 1$, $f_6\left(\frac{1}{4}\right) = 1$, $f_7\left(\frac{1}{4}\right) = 1$

$\lim_{n\to\infty} f_n\left(\frac{1}{4}\right) = 1.$

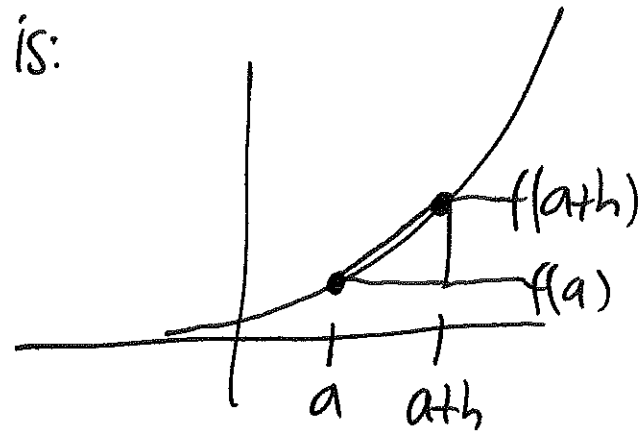
$\lim_{n\to\infty} f_n\left(\frac{1}{100}\right) = 1$

$\lim_{n\to\infty} f_n(0) = 0$

Derivatives

Suppose $f(x)$ is a function. The derivative of $f(x)$ at the value $x=a$ is:

$$\lim_{h\to 0} \frac{f(a+h)-f(a)}{h}$$



<u>Example</u> Compute the derivative of $f(x)=x^2$ at $a=2$. Use the definition, but you can assume basic facts about limits.

$$\lim_{h\to 0} \frac{\overbrace{(2+h)^2}^{f(a+h)} - \overbrace{2^2}^{f(a)}}{h} = \frac{(4+4h+h^2)-4}{h} = \frac{4h+h^2}{h} = 4+h$$

$$\lim_{h\to 0} 4+h = 4.$$

The devil's staircase

Domain is $0 \le x \le 1$

Define $f(x)$ as follows:

1) Write x in base 3
2) If there's a "1" in the expansion, turn every digit after the 1 into 0.
3) Turn all the 2's into 1's.
4) Interpret the result as a binary number.

base 3

$$f\left(\frac{1}{2}\right) = f(0.1111111\ldots_3)$$

$$\rightsquigarrow 0.10000000\ldots_2 = \frac{1}{2}$$

$$f\left(\tfrac{4}{5}\right) = f(0.210121012\ldots_3)$$

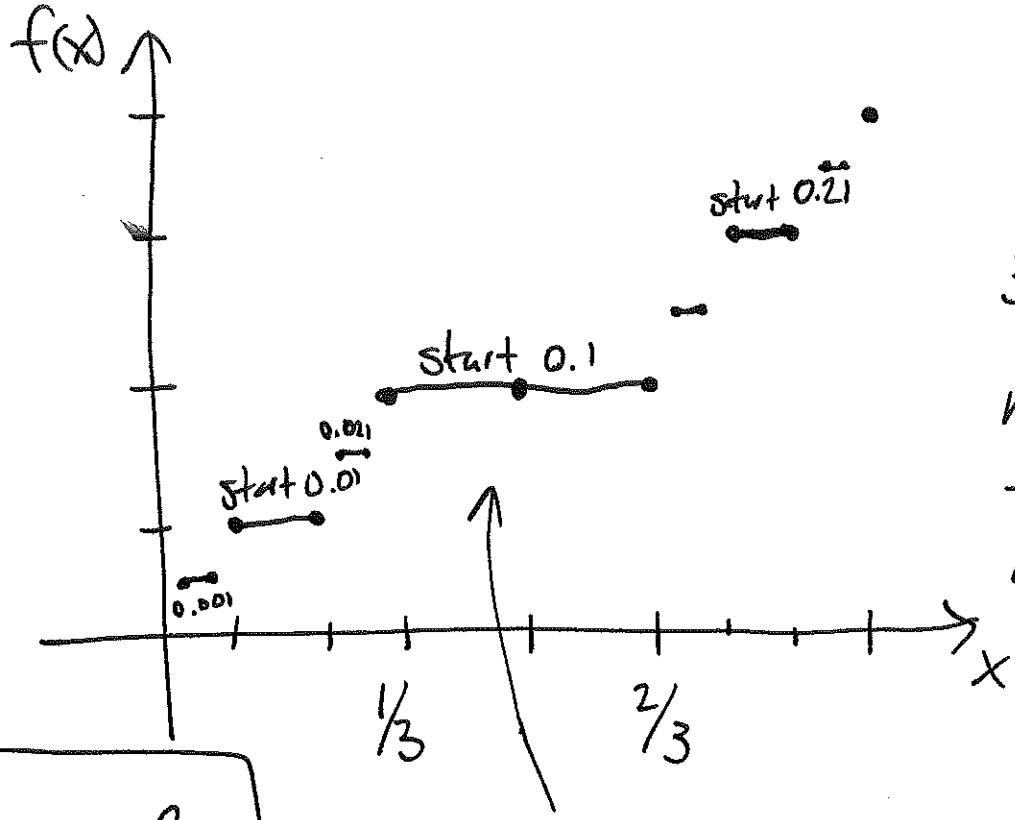
$$\rightsquigarrow 0.210000000$$

$$\rightsquigarrow 0.110000000$$

$$= \frac{3}{4}.$$

Try to plot the function:

(Hint: constant in many places)



3/4 is missing from domain!

anything in this range starts as $0.1\ldots_3$ in base 3.

$\rightsquigarrow f(x) = \frac{1}{2}$.

Value at 3/4 is:

$0.202020\ldots$

$0.10101010\ldots_2$

$$\frac{1}{2} + \frac{1}{8} + \frac{1}{32} + \cdots = \frac{1/2}{1 - 1/4} = \frac{1/2}{3/4} = \boxed{\frac{2}{3}}$$

continuous?

What number has no 1's?

$0.20202020\ldots_3$

that's

$$\frac{2}{3} + \frac{2}{27} + \frac{2}{243} + \cdots$$

$$\frac{2/3}{1 - 1/9} = \frac{2}{3} \Big/ \frac{8}{9} = \frac{2}{3} \cdot \frac{9}{8} = \boxed{\frac{3}{4}}$$

How much of the domain is "in a stair" so the function is constant nearby?

$$\underbrace{\frac{1}{3}}_{\text{one big stair}} + \underbrace{\frac{2}{9}}_{\text{two stairs of size } 1/9} + \underbrace{\frac{4}{27}}_{\text{four of size } 1/27} + \frac{8}{81} + \frac{16}{243} + \cdots = \frac{1/3}{1-2/3} = \boxed{1}$$

$\boxed{\text{Total width is } 1!}$

This function is constant (and has derivative 0) on a bunch of intervals whose length adds up to 1!

It <u>is</u> continuous for all x.

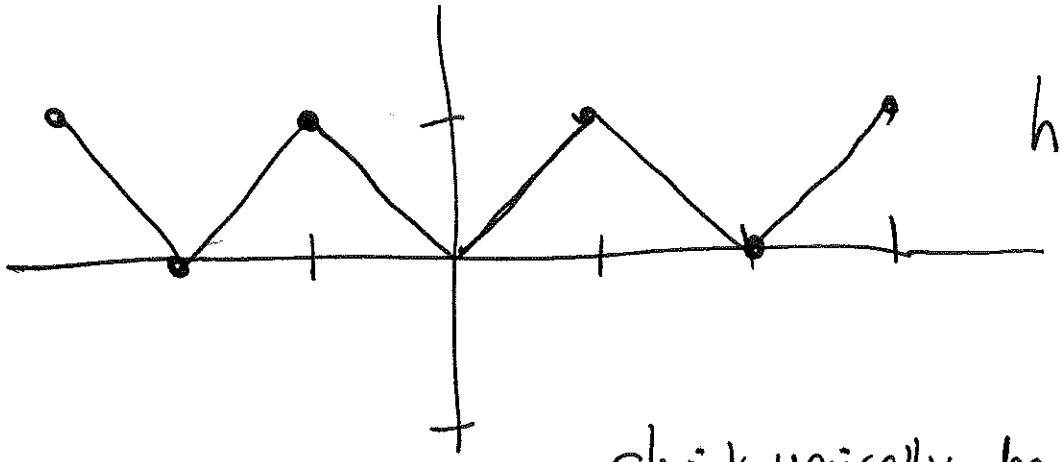
It's not differentiable at points with no 1's in the base-3 expansion (the "Cantor set").
(Otherwise it would violate FTC)

The Weierstrass function.

Let $h(x) = |x|$ if $-1 \le x \le 1$

and h has period 2.

HW #2:
Check Staircase
not differentiable at
$x = 2/3$.



$h(x)$

shrink vertically by $1/2^n$

Let

$$h_n(x) = \frac{1}{2^n} h(2^n x).$$ Plot me!

squish horizontally by 2^n

Set. $$g(x) = \sum_{n=0}^{\infty} h_n(x)$$ Definitely converges for any x.

What does this look like?

Solving systems of linear equations in many variables (Gaussian elimination).

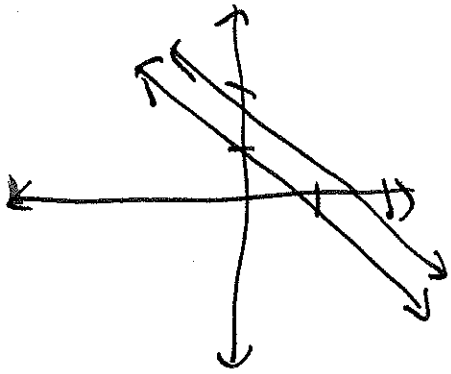
2 linear equations in two variables.

$$3x+5y=-2, \quad 6x-7y=1$$

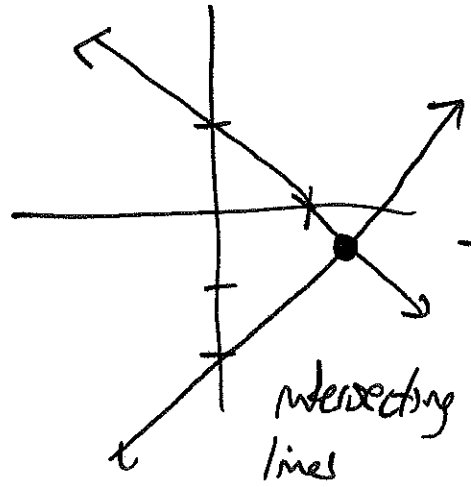
~~Usually only~~ How many solutions?

Three options

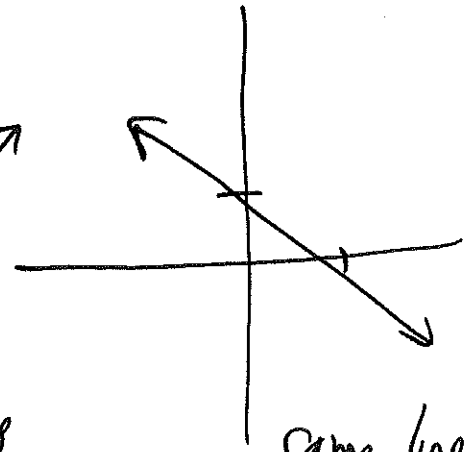
No solutions:	Just one: (common)	Infinitely many:
$x+y=1$	$x+y=1$	$x+y=1$
$2x+2y=3$	$x-y=2$	$2x+2y=2$



parallel lines



intersecting lines



same line twice

3 variables, 2 equations.

How many solutions?

$x+2y+3z=7$

(intersections of two planes)

<u>No solutions</u>

$x+y+z=1$

$x+y+z=3$

parallel planes!

<u>Infinitely many solutions</u>

$x=0$
$y=0$ $\longrightarrow$ $(0,0,z)$ solution

(two planes intersecting in a line)

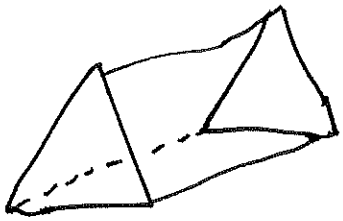
Can't have just one solution!

3 variables, 3 equations.

(three intersecting planes)

zero solutions	one solution (meet in a pt)	infinitely many

possible now even if they're not parallel!



---

m equations, n variables? ← Goal: find a foolproof method.

$m=n$: 0, 1, or ∞ solutions ("usually" 1)

$m>n$: 0, 1, or ∞ solution (usually 0)

$m<n$: 0, or ∞ (usually ∞)

Solve this:

$$\begin{aligned} 2x+y&=1 \\ -x+y&=3 \end{aligned} \rightsquigarrow \begin{aligned} x&=-2/3 \\ y&=7/3 \end{aligned}$$

First step: represent equations as a matrix ("augmented matrix")

$$\begin{array}{l} 2x+y=1 \rightarrow \\ -x+y=3 \rightarrow \end{array} \left(\begin{array}{cc|c} 2 & 1 & 1 \\ -1 & 1 & 3 \end{array}\right) \xrightarrow{R1 \mathrel{+}= (-1)*R2} \left(\begin{array}{cc|c} 3 & 0 & -2 \\ -1 & 1 & 3 \end{array}\right) \xrightarrow{\text{mult by } 1/3,\ R1 \mathrel{*}= 1/3} \left(\begin{array}{cc|c} 1 & 0 & -2/3 \\ -1 & 1 & 3 \end{array}\right)$$

subtract second from first

$$\begin{aligned} 2x+y&=1 \\ -x+y&=3 \end{aligned} \rightsquigarrow \begin{aligned} 3x&=-2 \\ -x+y&=3 \end{aligned} \xrightarrow{\text{divide first by } 3} \begin{aligned} x&=-2/3 \\ -x+y&=3 \end{aligned}$$

add first equation to second

$$\xrightarrow{R2 \mathrel{+}= 1 \cdot R1} \left(\begin{array}{cc|c} 1 & 0 & -2/3 \\ 0 & 1 & 7/3 \end{array}\right).$$

$x=-2/3$

$y=7/3$

Solved!

If you have a matrix M, there are three "elementary row operations":

1) add a multiple of one row to another row $\longleftrightarrow$ add a multiple of one equation to another

2) multiply a row by a nonzero real number $\longleftrightarrow$ multiply an equation by a number

3) swap two rows $\longleftrightarrow$ reordering the equations.

Given a system of linear equations:*

1) Write the augmented matrix.

2) Perform row operations to make left side the identity matrix. (Then you've solved it!)

*for n equations in n variables.

Try it!

$$2x+4y=-4$$
$$5x+7y=11$$

$$\left(\begin{array}{cc|c} 2 & 4 & -4 \\ 5 & 7 & 11 \end{array}\right) \xrightarrow{R1 \mathrel{+}= -4/2\, R2} \left(\quad\quad\quad\quad\right)$$

many ways to start!

"official" way: 1) make everything in left column below the top one 0. ("eliminate x")

$$\left(\begin{array}{cc|c} 2 & 4 & -4 \\ 5 & 7 & 11 \end{array}\right) \xrightarrow{R2 \mathrel{+}= -5/2\, R1} \left(\begin{array}{cc|c} 2 & 4 & -4 \\ 0 & -3 & 21 \end{array}\right) \xrightarrow{R1 \mathrel{+}= 4/3\, R2} \left(\begin{array}{cc|c} 2 & 0 & 24 \\ 0 & -3 & 21 \end{array}\right)$$

$$\xrightarrow{R1 \mathrel{*}= 1/2} \left(\begin{array}{cc|c} 1 & 0 & 12 \\ 0 & -3 & 21 \end{array}\right) \xrightarrow{R2 \mathrel{*}= -1/3} \left(\begin{array}{cc|c} 1 & 0 & 12 \\ 0 & 1 & -7 \end{array}\right)$$

3 equations, 3 variables

$$x - 3z = 8$$

$$2x + 2y + 9z = 7$$

$$y + 5z = -2$$

$$\begin{array}{c} \begin{array}{cccc} & 5^{th} & 5^{th} & 4^{th} \end{array} \\ \left(\begin{array}{ccc|c} 1 & 0 & -3 & 8 \\ 2 & 2 & 9 & 7 \\ 0 & 1 & 5 & -2 \end{array}\right) \end{array}$$

make 0 first!

make 0 second

this is third

1) make first col 0 below diagonal

2) make second col 0 below diagonal

...

3) have an upper triangular matrix!

4) make last col 0 above diagonal

5) then next-to-last

...

6) done!

$$\left(\begin{array}{ccc|c} 1 & 0 & -3 & 8 \\ 2 & 2 & 9 & 7 \\ 0 & 1 & 5 & -2 \end{array}\right) \xrightarrow{R2 \mathrel{+}= (-2)\cdot R1} \left(\begin{array}{ccc|c} 1 & 0 & -3 & 8 \\ 0 & 2 & 15 & -9 \\ 0 & 1 & 5 & -2 \end{array}\right)$$

$$\Big\downarrow R3 \mathrel{+}= (-\tfrac{1}{2})\, R2$$

$$\left(\begin{array}{ccc|c} 1 & 0 & -3 & 8 \\ 0 & 2 & 15 & -9 \\ 0 & 0 & 1 & -1 \end{array}\right) \xleftarrow{R3 \mathrel{*}= -2/5} \left(\begin{array}{ccc|c} 1 & 0 & -3 & 8 \\ 0 & 2 & 15 & -9 \\ 0 & 0 & -5/2 & 5/2 \end{array}\right)$$

$$\Big\downarrow \begin{array}{l} R1 \mathrel{+}= 3\cdot R3 \\ R2 \mathrel{+}= -15\cdot R3 \end{array}$$

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 5 \\ 0 & 2 & 0 & 6 \\ 0 & 0 & 1 & -1 \end{array}\right) \xrightarrow{R2 \mathrel{*}= 1/2} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 5 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & -1 \end{array}\right)$$

Try this one:

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 1 & 3 & 7 & 3 \\ 2 & 4 & 8 & 6 \end{array}\right) \xrightarrow[\substack{R2 += (-1)R1 \\ R3 += (-2)R1}]{} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 0 & 2 & 6 & 1 \\ 0 & 2 & 6 & 2 \end{array}\right)$$

$$\xrightarrow{R3 += (-1)R2} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 0 & 2 & 6 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

this says $0=1$!

<u>no solutions</u>

We're never going to reach the identity matrix!

But: you can always get to "echelon form", which means you've simplified your equations as much as possible.

You can't always row reduce and make left the identity matrix.

<u>But!</u>

You can always row reduce so matrix is rref.

This corresponds to reducing the linear equations as much as possible. Once you have rref, you can find the solutions.

Ex.

A matrix is in "echelon form" if

1) all rows of 0's are at the bottom

2) the leading entry (first nonzero number) of each row is to the right of leading entry in row above.

3) all entries in a column <u>below</u> the leading entry of any row are 0.

It's in "row reduced echelon form" (rref) if

4) leading entry of any row is 1

5) each leading 1 is the only nonzero thing in its column.

Echelon:

$$\left(\begin{array}{ccccc|c} 1 & 2 & 2 & 3 & 4 & 1 \\ 0 & 0 & 4 & 7 & 1 & 2 \\ 0 & 0 & 0 & 5 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Rref:

$$\left(\begin{array}{ccccc|c} 1 & 2 & 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 4 \\ 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

rref.

$$\left(\begin{array}{ccccc|c} 1 & 2 & 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 4 \\ 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Say variables are

v, w, x, y, z

$$v + 2w + z = 3$$
$$x + 3z = 4$$
$$y + z = 2$$

v, x, y only in one equation! can't eliminate anything.

---

w & z could have any value whatsoever!

once you pick values for those, the other variable are determined.

$w =$ anything
$z =$ anything $\rightarrow$

$$v = 3 - 2w - z$$
$$x = 4 - 3z$$
$$y = 2 - z$$

Solving a system of linear equations

1. Convert our equations into an augmented matrix

$$\begin{aligned} 3x-2y+z&=7 \\ 2x+y-2z&=3 \end{aligned} \rightsquigarrow \left(\begin{array}{ccc|c} 3 & -2 & 1 & 7 \\ 2 & 1 & -2 & 3 \end{array}\right)$$

2. Do row operations on the matrix to put it into RREF. (row reduced echelon form)
   (this corresponds to eliminating variables)

   a) Add a multiple of a row to another

   b) Multiply a row by a number

   c) Swap two rows.

$$\left(\begin{array}{ccc|c} 3 & -2 & 1 & 7 \\ 2 & 1 & -2 & 3 \end{array}\right) \xrightarrow[R2 \mathrel{+}= -\frac{2}{3} \cdot R1]{} \left(\begin{array}{ccc|c} 3 & -2 & 1 & 7 \\ 0 & 7/3 & -8/3 & -5/3 \end{array}\right)$$

$$\Big\downarrow R2 \times = 3$$

$$\left(\begin{array}{ccc|c} 3 & 0 & -9/7 & 39/7 \\ 0 & 7 & -8 & -5 \end{array}\right) \xleftarrow{R1 \mathrel{+}= \frac{2}{7} R2} \left(\begin{array}{ccc|c} 3 & -2 & 1 & 7 \\ 0 & 7 & -8 & -5 \end{array}\right)$$

$$\Big\downarrow \begin{array}{l} R1 \times = \frac{1}{3} \\ R2 \times = \frac{1}{7} \end{array}$$

$$\begin{array}{c} \left(\begin{array}{ccc|c} 1 & 0 & -3/7 & 13/7 \\ 0 & 1 & -8/7 & -5/7 \end{array}\right) \\ \begin{array}{ccc} x & y & \end{array} \end{array}$$

RREF!

$$x - \tfrac{3}{7} z = \tfrac{13}{7}$$
$$y - \tfrac{8}{7} z = -\tfrac{5}{7}$$

3) Read off all solutions from rref.

Identify <u>pivot</u> variables (correspond to leading entries of some row)	Identify <u>free</u> variables (not <u>pivot</u> variables)
x and y	z

Solve for ~~free~~ pivot variables in terms of free variables.

$$\left.\begin{aligned} z &= \text{anything} \\ x &= 13/7 + 3/7\, z \\ y &= -5/7 + 8/7\, z \end{aligned}\right] \quad \text{"general solution"}$$

A matrix is in "echelon form" if

1) all rows of 0s at bottom
2) the leading entry is to the right of the leading entry above it
3) all entries <u>below</u> a leading entry are 0

" "row reduced echelon form"

4) every leading entry is 1
5) each leading 1 is only nonzero thing in column.

Find general solution of

$$x+3y+4z=7$$
$$3x+9y+7z=6$$

$$\left(\begin{array}{ccc|c} 1 & 3 & 4 & 7 \\ 3 & 9 & 7 & 6 \end{array}\right) \xrightarrow{R2 += (-3)R1} \left(\begin{array}{ccc|c} 1 & 3 & 4 & 7 \\ 0 & 0 & -5 & -15 \end{array}\right)$$

$$\Big\downarrow R2 \times = \left(-\tfrac{1}{5}\right)$$

$$\left(\begin{array}{ccc|c} 1 & 3 & 0 & -5 \\ 0 & 0 & 1 & 3 \end{array}\right) \xleftarrow{R1 += (-4)R2} \left(\begin{array}{ccc|c} 1 & 3 & 4 & 7 \\ 0 & 0 & 1 & 3 \end{array}\right)$$

Solution? Pivots: x, z $\quad$ y can be anything.

Free: y $\quad$ Solve for x, z in terms of y.

$$\begin{array}{l} x+3y=-5 \\ z=3 \end{array} \Longrightarrow \begin{cases} y \text{ is anything} \\ x=-5-3y \\ z=3 \end{cases}$$

e.g. plug in $y=-2$

$\downarrow$

$x=1$
$y=-2$
$z=3$

Balance the reaction:

$$\underline{x_1}\, Na_3PO_4 + \underline{x_2}\, Ba(NO_3)_2 \rightarrow \underline{x_3}\, Ba_3(PO_4)_2 + \underline{x_4}\, NaNO_3$$

Fill in the blanks!

Na: $3x_1 = x_4$

Ba: $x_2 = 3x_3$

PO_4: $x_1 = 2x_3$

NO_3: $2x_2 = x_4$

$\longrightarrow$

$x_1 - x_4 = 0$

$x_2 - 3x_3 = 0$

$x_1 - 2x_3 = 0$

$2x_2 - x_4 = 0$

$$\left(\begin{array}{cccc|c} 3 & 0 & 0 & -1 & 0 \\ 0 & 1 & -3 & 0 & 0 \\ 1 & 0 & -2 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 \end{array}\right) \xrightarrow{\text{rref}} \begin{array}{c} \begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \end{array} \\ \left(\begin{array}{cccc|c} 1 & 0 & 0 & -1/3 & 0 \\ 0 & 1 & 0 & -1/2 & 0 \\ 0 & 0 & 1 & -1/6 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \end{array}$$

Pivot: x_1, x_2, x_3

Free: x_4

$x_1 = +\frac{1}{3}x_4$

$x_2 = +\frac{1}{2}x_4$

$x_3 = +\frac{1}{6}x_4$

$x_4 = 6$ $\quad x_2 = 3$

$x_1 = 2$ $\quad x_3 = 1$

$$2\,Na_3PO_4 + 3\,Ba(NO_3)_2 \rightarrow Ba_3(PO_4)_2 + 6\,NaNO_3.$$

One more:

$$\underline{x_1}\,CH_3NH_2 + \underline{x_2}\,O_2 \rightarrow \underline{x_3}\,CO_2 + \underline{x_4}\,H_2O + \underline{x_5}\,N_2$$

C: $x_1 = x_3$	$x_1 - x_3 = 0$
H: $5x_1 = 2x_4$	$5x_1 - 2x_4 = 0$
N: $x_1 = 2x_5$	$x_1 - 2x_5 = 0$
O: $2x_2 = 2x_3 + x_4$	$2x_2 - 2x_3 - x_4 = 0$

$$\left(\begin{array}{ccccc|c} 1 & 0 & -1 & 0 & 0 & 0 \\ 5 & 0 & 0 & -2 & 0 & 0 \\ 1 & 0 & 0 & 0 & -2 & 0 \\ 0 & 2 & -2 & -1 & 0 & 0 \end{array}\right) \xrightarrow{\text{rref}} \begin{array}{c} \begin{array}{ccccc} x_1 & x_2 & x_3 & x_4 & x_5 \end{array} \\ \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & -2 & 0 \\ 0 & 1 & 0 & 0 & -9/2 & 0 \\ 0 & 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 0 & 1 & -5 & 0 \end{array}\right) \end{array}$$

x_5 free!

$$\begin{aligned} x_1 &= 2x_5 \\ x_2 &= 9/2\,x_5 \\ x_3 &= 2x_5 \\ x_4 &= 5x_5 \end{aligned} \quad \xrightarrow{\text{use 2}} \quad \begin{aligned} x_1 &= 4 \\ x_2 &= 9 \\ x_3 &= 4 \\ x_4 &= 10 \end{aligned}$$

What happens to systems with no solution?

$$x+y+z=2$$
$$2x+2y+2z=5$$

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 5 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{array}\right).$$ rref ✓

<u>How many solutions to a linear system of eqns?</u>

- Write down matrix, compute rref.

- If there's a row $(0\ 0\ 0\ 0 \mid b)$ where $b \neq 0$, no solutions!

- If there's a free variable (but no $(0\ 0\ 0 \mid b)$ row), then infinitely many solutions.

- If there's no free variable and no $(0\ 0\ 0 \mid b)$ row, then <u>one</u> solution.

Also notice:

If you have more variables than equations, and there is a solution, then there are infinitely many solutions.

Why? e.g. 4 variables, 2 eqns.

There is at most one pivot variable per equation! (At most 2 in this case)

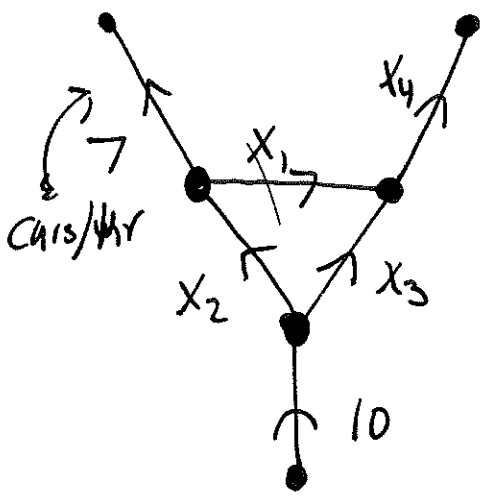
So there must be free variable.

Applications to networks

A "network" is:

- a set of "nodes"
- a set of "branches" connecting nodes

<u>Ex</u> network of roads: nodes are intersections, branches are roads (one-way) connecting the intersections.



to get linear equations:

1) at any intersections, (cars in) = (cars out)

2) (total cars in) = (total cars out)

① $x_2 + x_3 = 10$

② $x_2 = 7 + x_1$

③ $x_1 + x_3 = x_4$

④ $10 = 7 + x_4$

Augmented matrix:

$$\left(\begin{array}{cccc|c} -1 & 1 & 0 & 0 & 7 \\ 0 & 1 & 1 & 0 & 10 \\ 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right)$$

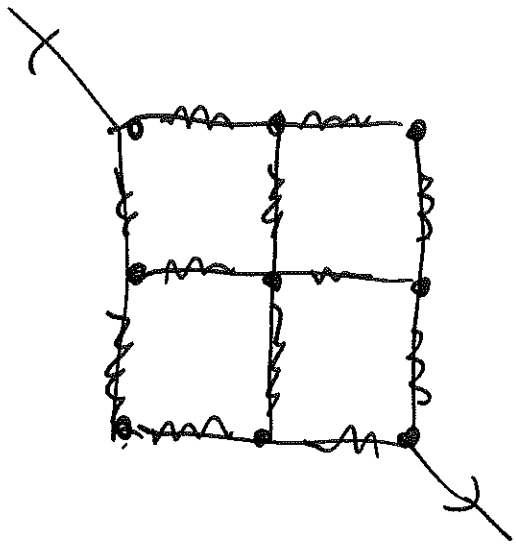
$$\Big\downarrow \text{rref}$$

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 3 \\ 0 & 1 & 1 & 0 & 10 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Multiple solutions! We need one more equation. Send out somebody else to watch the road, maybe measure value of x_1.

This works for circuits too!

(use Kirkhoff's junction rule at each point)



equivalent resistance?

To invert this

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 2 & 3 & -4 & 0 & 1 & 0 \\ 7 & 5 & -12 & 0 & 0 & 1 \end{array}\right)$$

$$\Big\downarrow \text{rref}$$

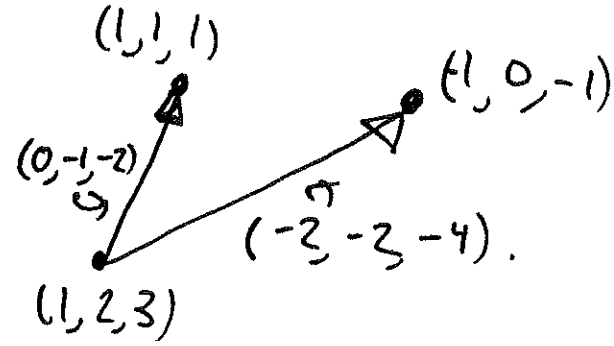
$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & 1 & 0 & \text{inverse of the matrix you started with} \\ 0 & 0 & 1 & \end{array}\right)$$

A couple other forms of linear equations.

Consider the plane through $(1,2,3)$, $(1,1,1)$ and $(1,0,-1)$. Is $(2,1,2)$ on the plane?

→ one method:

1) find eqn of plane



2) cross product $(0,-1,-2)\times(-2,-2,-4)$

$$\begin{vmatrix} \hat{i} & \hat{j} & \hat{k} \\ 0 & -1 & -2 \\ -2 & -2 & -4 \end{vmatrix} = 0\hat{i} + 4\hat{j} - 2\hat{k}$$

that's the normal vector!

Plane is: $0x + 4y - 2z = C$ some constant C.

$(1,1,1)$ on plane $\Rightarrow C = 2$.

Plane is $4y - 2z = 2$.

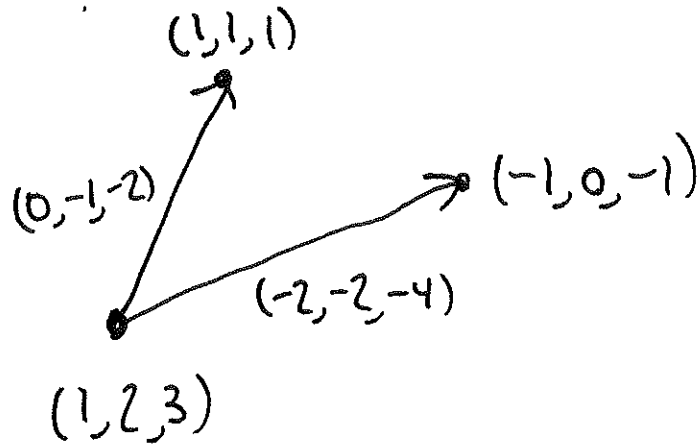
Is $(2,1,2)$ there?

$4y - 2z = 0$

$\boxed{\text{NO}}$

Other method!

Plane through $(1,2,3)$, $(1,1,1)$, $(-1,0,-1)$.



Some other pts:

$$\begin{pmatrix}1\\2\\3\end{pmatrix}+2\begin{pmatrix}-2\\-2\\-4\end{pmatrix} \qquad \begin{pmatrix}1\\2\\3\end{pmatrix}+3\begin{pmatrix}0\\-1\\-2\end{pmatrix}.$$

Every pt is:

$$\begin{pmatrix}1\\2\\3\end{pmatrix}+s\begin{pmatrix}-2\\-2\\-4\end{pmatrix}+t\begin{pmatrix}0\\-1\\-2\end{pmatrix}.$$

Is $\begin{pmatrix}2\\1\\2\end{pmatrix}$ on the plane? Try to solve for s & t

$$\begin{pmatrix}1\\2\\3\end{pmatrix} + s\begin{pmatrix}-2\\-2\\-4\end{pmatrix} + t\begin{pmatrix}0\\-1\\2\end{pmatrix} = \begin{pmatrix}2\\1\\2\end{pmatrix}$$

Solve for s & t!

(oops, I switched a sign! Let's use this plane.)

$$\begin{pmatrix}1-2s+0t\\2-2s-t\\3-4s+2t\end{pmatrix} = \begin{pmatrix}2\\1\\2\end{pmatrix}$$

$$\left.\begin{aligned}1-2s+0t&=2\\2-2s-t&=1\\3-4s+2t&=2\end{aligned}\right\} \longrightarrow \begin{aligned}-2s+0t&=1\\-2s-t&=-1\\-4s+2t&=-1\end{aligned}$$

Augmented:

$$\left(\begin{array}{cc|c}-2&0&1\\-2&-1&-1\\-4&2&-1\end{array}\right)$$

$$\left(\begin{array}{cc|c}-2&0&1\\-2&-1&-1\\-4&2&-1\end{array}\right) \xrightarrow[R3-=2R1]{R2-=R1} \left(\begin{array}{cc|c}-2&0&1\\0&-1&-2\\0&2&-3\end{array}\right) \xrightarrow{R3+=2R2} \left(\begin{array}{cc|c}-2&0&1\\0&-1&-2\\0&0&-7\end{array}\right)$$

not rref, but I can already see no solutions!

~~Algorithm~~

~~To find~~

<u>Fun fact</u> The determinant of a diagonal matrix

$$\begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix} \text{ is } \lambda_1 \lambda_2 \lambda_3.$$

In fact, the determinant of an ~~ap~~ upper triangular matrix is the product of the diagonal entries:

$$\det \begin{pmatrix} 4 & 1 & 191 \\ 0 & 7 & -95 \\ 0 & 0 & 2 \end{pmatrix} = 4 \cdot 7 \cdot 2 = 56.$$

To find det(M):

Use row reduction to make M upper triangular.

Try to only use $R_i += c \cdot R_j$. (no swaps, no mult by constants)

Then det(M) = det(upper triangular)

$$\det\begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 7 \\ 1 & 2 & -1 \end{pmatrix} ?$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 7 \\ 1 & 2 & -1 \end{pmatrix} \xrightarrow{R2 += -R1} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 6 \\ 1 & 2 & -1 \end{pmatrix} \xrightarrow{R3 += R1} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 6 \\ 0 & 1 & -2 \end{pmatrix}$$

$$\xrightarrow{R3 += -\frac{1}{2}R2} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 6 \\ 0 & 0 & -5 \end{pmatrix}$$

$$\boxed{\begin{aligned} \det &= (1)(2)(-5) \\ &= -10 \end{aligned}}$$

Other applications of row reduction

- How does applying each row operation change the determinant of a matrix?

Try it: use $M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. How does each of the three row operations change determinant? (why does the same thing work for other matrices?)

Reminder: $\det = ad - bc$
= area of parallelogram with legs the rows (or cols) of the matrix.

How to find determinant of $\begin{pmatrix} 3 & 5 \\ 1 & 3 \end{pmatrix}$ using row reduction?

Try algebraically:

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ determinant $= 1$

a) Multiply a row by constant λ: $\Longrightarrow$ det multiplied by λ.

$\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$ $\det = \lambda$.

b) Add c times a row to another row: $\Rightarrow$ no change

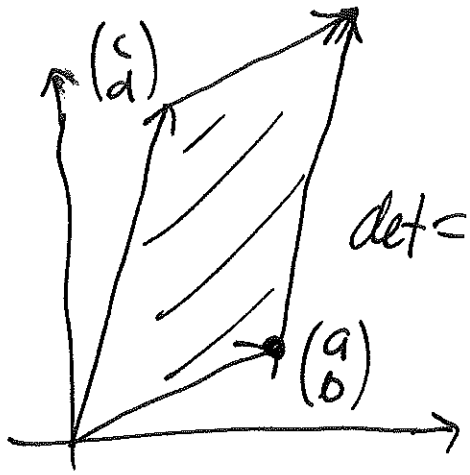
$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$ $\det = 1$

c) Swap rows $\Longrightarrow$ determinant mult by -1.

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\det = -1$

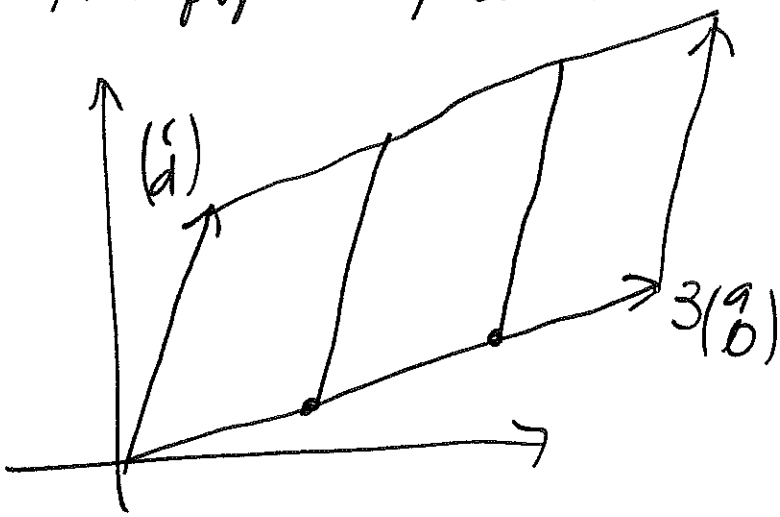
Or geometrically:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$



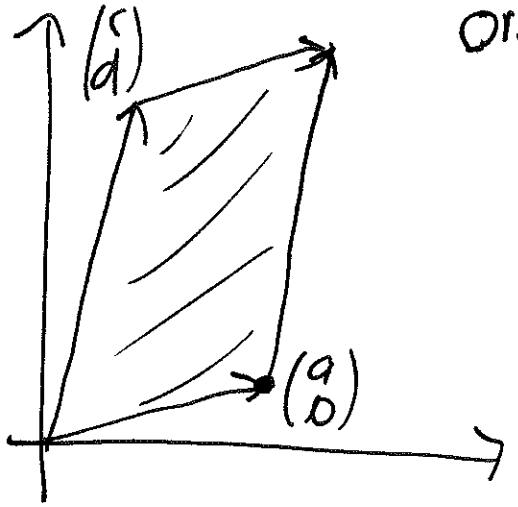
det = area

a) Multiply row by constant



determinant multiplied by c!

b) Row swap



orientation, det mult by -1.

c) Add $c \cdot row_i$ to row_j:

Apply shear transform $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$, no change.

$$\begin{pmatrix} 3 & 5 \\ 1 & 3 \end{pmatrix} \qquad \det = d$$

$$\Big\downarrow \text{swap}$$

$$\begin{pmatrix} 1 & 3 \\ 3 & 5 \end{pmatrix} \qquad \det = -d$$

$$\Big\downarrow R1 \mathrel{+}= -3R2$$

$$\begin{pmatrix} 1 & 3 \\ 0 & -4 \end{pmatrix} \qquad \det = -d$$

$$\Big\downarrow R2 \mathrel{+}= \tfrac{3}{4}R1$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -4 \end{pmatrix} \qquad \det = -d$$

$$\Big\downarrow R2 \mathrel{*}= -\tfrac{1}{4}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \det = \tfrac{1}{4}d$$

so $\frac{1}{4}d = 1$

$d = 4$

Imagine you want to solve

$$\begin{aligned} x+2y+3z&=5 \\ y+4z&=4 \\ 5x+6y \quad &= -1 \end{aligned} \qquad \Bigg\| \qquad \begin{aligned} x+2y+3z&=6 \\ y+4z&=-2 \\ 5x+6y \quad &= 4 \end{aligned}$$

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 5 \\ 0 & 1 & 4 & 4 \\ 5 & 6 & 0 & -1 \end{array}\right) \text{ row reduce ... } \left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & 1 & 0 & ?? \\ 0 & 0 & 1 & \end{array}\right)$$

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 6 \\ 0 & 1 & 4 & -2 \\ 5 & 6 & 0 & 4 \end{array}\right) \text{ row reduce ... } \left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & 1 & 0 & ?? \\ 0 & 0 & 1 & \end{array}\right)$$

Only the left side matters! we do the same steps both ways. just use two augmented columns, and row reduce that.

$$\left(\begin{array}{ccc|cc} 1 & 2 & 3 & 5 & 6 \\ 0 & 1 & 4 & 4 & -2 \\ 5 & 6 & 0 & -1 & 4 \end{array}\right) \xrightarrow{\text{row red}} \left(\begin{array}{ccc|cc} 1 & 0 & 0 & -53 & -160 \\ 0 & 1 & 0 & 44 & 134 \\ 0 & 0 & 1 & -10 & -34 \end{array}\right)$$

First system. $x=-53$, $y=44$, $z=-10$

Second: $x=-160$, $y=134$, $z=-34$

Related problem:

Say you want to find the inverse of a matrix.

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{pmatrix}\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

How to find all the letters? How to find a, d, g?

(top left

$$\begin{aligned} 1a+2d+3g &= 1 \\ 0a+1d+4g &= 0 \\ 5a+6d+0g &= 0 \end{aligned}$$

b, e, h

$$\begin{aligned} 1b+2e+3h &= 0 \\ 0b+1e+4h &= 1 \\ 5b+6e+0h &= 0 \end{aligned}$$

$$\Downarrow \qquad \Downarrow \qquad \Downarrow$$

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 4 & 0 \\ 5 & 6 & 0 & 0 \end{array}\right) \qquad \left(\begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 0 & 1 & 4 & 1 \\ 5 & 6 & 0 & 0 \end{array}\right) \qquad \left(\begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 0 & 1 & 4 & 0 \\ 5 & 6 & 0 & 1 \end{array}\right)$$

Row reduce together!

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 \\ 5 & 6 & 0 & 0 & 0 & 1 \end{array}\right) \xrightarrow{R3 \mathrel{+}= (-5)R1} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 \\ 0 & -4 & -15 & -5 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{R1 \mathrel{+}= (-2)R2} \left(\begin{array}{ccc|ccc} 1 & 0 & -5 & 1 & -2 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 \\ 0 & -4 & -15 & -5 & 0 & 1 \end{array}\right) \xrightarrow{R3 \mathrel{+}= 4R2} \left(\begin{array}{ccc|ccc} 1 & 0 & -5 & 1 & -2 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 \\ 0 & 0 & 1 & -5 & 4 & 1 \end{array}\right)$$

$$\xrightarrow{\cdots} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -24 & 18 & 5 \\ 0 & 1 & 0 & 20 & -15 & -4 \\ 0 & 0 & 1 & -5 & 4 & 1 \end{array}\right)$$

tell us a,d,g

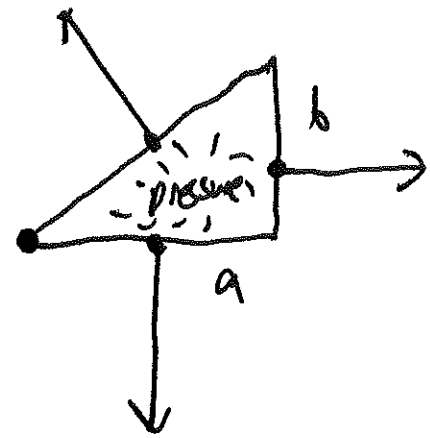
b,h,e

this is the inverse!

Today: one more day of linear algebra (LU decomposition, invertibility, Markov processes)

Next: something fun (requests?)

- Fourier (after a break)
- Game theory?
- Physics proofs?
- Algebraic geometry!



Recap last time: determinants of any size matrix

to find det(M): - use row operation of add cR_i to R_j until we get upper triangular. don't change determinant!

- then determinant is product of diagonal entries.

Inverse of an $n \times n$ matrix.

$$\left(\begin{array}{ccc|ccc} 0 & 3 & 2 & 1 & 0 & 0 \\ -1 & 4 & 2 & 0 & 1 & 0 \\ 3 & -4 & -1 & 0 & 0 & 1 \end{array}\right)$$

$$\Big\downarrow \text{rref}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -4 & 5 & 2 \\ 0 & 1 & 0 & -5 & 6 & 2 \\ 0 & 0 & 1 & 8 & -9 & -3 \end{array}\right)$$

this is the inverse!

takes n^3 steps.

$$\begin{pmatrix} 0 & 3 & 2 \\ -1 & 4 & 2 \\ 3 & -4 & -1 \end{pmatrix} \xrightarrow{R1 -= R2} \begin{pmatrix} 1 & -1 & 0 \\ -1 & 4 & 2 \\ 3 & -4 & -1 \end{pmatrix} \xrightarrow{R2 += R1} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 3 & 2 \\ 3 & -4 & -1 \end{pmatrix}$$

$$\xrightarrow{R3 += (-3)R1} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 3 & 2 \\ 0 & -1 & -1 \end{pmatrix} \xrightarrow{R3 += (+1/3)R2} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 3 & 2 \\ 0 & 0 & -1/3 \end{pmatrix}$$

upper triangular! det is -1.

Why is this faster? (What is the other way anyway?)

$n \times n$ matrix! (must be square!)

$$M = \begin{pmatrix} 1 & 2 & 3 & 4 & -1 \\ 7 & 1 & 2 & 9 & 1 \\ 3 & 1 & 7 & 0 & 1 \\ 5 & 0 & -6 & 1 & 25 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Look at every possible way to pick n things, one from each row and each column.

There are $n!$ ways to do it.

For each way, multiply circled numbers, add up, half with a +, half with a −.

Takes $(n+1)!$ steps! Yuck! row red takes n^3 steps.

LU decomposition

Imagine you want to solve

$$Ax=b_1,\ Ax=b_2,\ \dots\ Ax=b_6,\ Ax=b_{100},$$

$$Ax=b_{1000000},\ \dots$$ many b's, same A, different x for each b.

Given a matrix A, dimensions $m \times n$.

We will find: $A=LU$

where L is an $m \times m$ lower triangular matrix

U is an $m \times n$ ~~upper tri~~ echelon form matrix (upper triangular, basically)

How does this help solve $Ax=b$?

To solve $Ax=b$:

1) Solve $Ly=b$ for y. (easy! L is lower-triangular)
2) Solve $Ux=y$, for the y you just found.

   x is solution:

$$Ax=(LU)x=L(Ux)=Ly=x.$$

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

The decomposition is:

$$L = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix}$$

$$LU = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad \checkmark$$

$Ax = b$ where $b = \begin{pmatrix} 12 \\ 17 \end{pmatrix}$

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1 \\ 2 & 1 & 0 & 0 & 7 \\ 3 & -1 & 1 & 0 & -3 \\ 4 & 5 & 6 & 1 & 4 \end{array}\right)$$

$Ly = b$ for y: $\left(\begin{array}{cc|c} 1 & 0 & 12 \\ 3 & 1 & 17 \end{array}\right)$

$x_1 = 12 \qquad 3x_1 + x_2 = 17$

$x_2 = 17 - 3x_1 = 17 - 36 = -19$

$y = \begin{pmatrix} 12 \\ -19 \end{pmatrix}$

$Ux = y$ for x $\left(\begin{array}{cc|c} 1 & 2 & 12 \\ 0 & -2 & -19 \end{array}\right)$ $\quad x_2 = \frac{19}{2} \qquad x = \begin{pmatrix} -7 \\ 19/2 \end{pmatrix}$

$x_1 = 12 - 2x_2 = -7.$

How to find L&U

0) Use a computer!

if you must:

1) Row reduce A, using only operation $R_i \mathrel{+}= c \cdot R_j$.*

2) Get to echelon form (not reduced)
(if you must row swap, read about it)

3) LU decomposition records steps of row reduction.

U = final echelon matrix you got

L = lower triangular, with L_{ij} = what multiple of row j did you subtract from row i?

row i
col j

*do in order: first fix first col, then the second, ...

diagonal entries = 1

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \xrightarrow{R2 -= 3R1} \begin{pmatrix} 1 & 2 \\ 0 & -2 \\ 5 & 6 \end{pmatrix} \xrightarrow{R3 -= 5 \cdot R1} \begin{pmatrix} 1 & 2 \\ 0 & -2 \\ 0 & -4 \end{pmatrix}$$

$$\xrightarrow{R3 -= 2R2} \begin{pmatrix} 1 & 2 \\ 0 & -2 \\ 0 & 0 \end{pmatrix}$$

that's U!

What about L?

$$L_{21} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 5 & 2 & 1 \end{pmatrix}$$

L_{31} $\quad$ L_{32}

L_{ij} = what multiple of row j did you subtract from row i?

row i
col j

$$\cancel{\begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 5 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix}}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 5 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & -2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$$

Try one!

$$\begin{pmatrix} 3 & -7 & -2 \\ -3 & 5 & 1 \\ 6 & -4 & 0 \end{pmatrix}$$

<u>Find $LU=A$</u>

One last topic: (Markov processes)

Suppose that every year:

5% of people in State College move to Bellefonte

95% stay put

3% in Bellefonte move to State College

97% stay put.

Suppose in year 0: 40000 in SC
10000 in Bellefonte.

How many in each place in 1 year?
2 years?
100 years?
1000000 years?

SC in a year:

$0.95 \cdot 40000 + 0.03 \cdot 10000$

Bfte in a year:

$0.05 \cdot 40000 + 0.97 \cdot 10000$

$$x_{n+1} = \begin{pmatrix} 0.95 & 0.03 \\ 0.05 & 0.97 \end{pmatrix} x_n$$

columns sum to 1

"Markov matrix"!

stabilizes:

$$Ax = x$$ ← you eigenvector with eigenvalue 1.

$$Ax = Ix$$

$$(A - I)x = 0.$$

$$\left(\begin{array}{cc|c} -0.05 & 0.03 & 0 \\ 0.05 & -0.03 & 0 \end{array}\right) \longrightarrow \left(\begin{array}{cc|c} -0.05 & 0.03 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

$$-0.05x + 0.03y = 0 \qquad x + y = 50000$$

$$-5x + 3y = 0 \qquad x + y = 50000$$

$$x = 18750$$

$$y = 31250$$

Today: Primality testing and factorization.

Next time: Game theory

Who cares? → For RSA, you need to figure out if big numbers are prime.

→ To be sure RSA is secure, need a good understanding of how fast factorization can go.

Warm-up: is 123456789 prime?

no! checked divibility be 2, 3. it is divisible.

$$123456789 = 9 \cdot \underbrace{13717421}_{\text{how about that?}}$$

You could check all the possible factors:

divide by everything up to $\sqrt{13717421}$.

If don't find a factor, it's prime.

This is "trial division". Pretty slow, but it works.

(it will find a factor of 13717421 eventually.)

<u>Better algorithm for primality testing.</u> (no help factoring!)

<u>Fermat's Little Theorem:</u>

$$n^{p-1} \equiv 1 \bmod p$$ (if n is not a multiple of p, p prime)

To check if 13717421 is prime:

Find $\underbrace{2^{13717420}}_{\text{really big. but we have a fast algorithm! "repeated squaring"}} \bmod 13717421.$ If it's not 1 not prime!

$= 7682470$

<u>not prime!</u>

Try: is 341 prime?

$2^{340} \bmod 341$

$(2^0 \equiv 1 \bmod 341)$

$2^1 \equiv 2 \bmod 341$

$2^2 \equiv 4 \bmod 341$

$2^4 \equiv 16 \bmod 341$

$2^8 \equiv 256 \bmod 341$

...

$2^{256} \equiv 64 \bmod 341$ (comp)

binary expansion

those we know

$$2^{340} = 2^{256+64+16+4} = 2^{256} \cdot 2^{64} \cdot 2^{16} \cdot 2^4 = \underline{\underline{1}}$$

What does that tell us? It <u>might</u> be prime.

Try $n=3$!

$3^{340} \bmod 341 = 56.$ <u>not prime!</u>

($34 = 11 \times 31$, I checked seperately.)

This test is very fast, but not 100% reliable.

→ If $n^{p-1} \equiv 1 \bmod p$, then p is probably prime. (no guarantees)

→ If $n^{p-1} \not\equiv 1 \bmod p$, definitely not prime.

Algorithm: to determine if m is prime.

- Compute $2^{m-1} \bmod m$.
  - → if $\neq 1$, ~~keep going~~ definitely not prime
  - → if $= 1$, try another base.
- keep going until you are bored. the more bases, the surer you are it's prime, but never 100% certainty.

<u>DANGER</u>: There are numbers that pass the test for every base but aren't prime: "Carmichael numbers".
Smallest one is $561 = 3 \times 11 \times 17$.

How fast is this?

- To check if n is prime using bases 2, 3, 5, 7, 11: takes time $O(\log n)$. "about" big-Oh
- Compare to trial division: $O(\sqrt{n})$.

test is much faster, but very rarely gives false positives.

Factorization Pollard ρ algorithm.

Birthday problem: If 25 people are in a room, what's the chance that 2 of them have the same birthday?

$$\frac{365!}{340!} = {}_{365}P_{25} = \frac{\binom{365}{25}\cdot 25!}{365^{25}}$$

$\mathbb{P}$(no two have the same birthday)

$$= \underset{1^{st}}{\frac{365}{365}} \cdot \underset{2^{nd}}{\frac{364}{365}} \cdot \underset{3^{rd}}{\frac{363}{365}} \cdot \cdots \cdot \underset{25^{th}}{\frac{341}{365}}$$

$$\overset{\text{calc.}}{=} 0.43$$

$$\mathbb{P}\left(\begin{matrix}\text{two people have the}\\ \text{same}\end{matrix}\right) = 1 - \text{that} \approx 57\%$$

To generalize this:

~~If we have~~

If we pick k random numbers from N options,

- What is the chance 2 are the same? $\left(\begin{matrix}N=365\\ k=25\end{matrix}\right)$ done
- If we fix N, how big does k need to be to guarantee at least a 50% chance that 2 are the same? $\left(\begin{matrix}N=365\\ k=23 \text{ is enough}\end{matrix}\right)$

$$1 - \frac{N}{N} \cdot \frac{N-1}{N} \cdot \dots \cdot \frac{N+1-k}{N}$$

$$= 1 - \frac{\frac{N!}{(N-k)!}}{N^k} = 1 - \frac{N!}{N^k (N-k)!}$$

For second problem, we want the k that makes that $> 50\%$.

if $N=1000$, when is $1 - \frac{1000!}{1000^k (1000-k)!} \approx 50\%$

Hard! One idea: we need

$$(1)\left(1-\frac{1}{N}\right)\left(1-\frac{2}{N}\right)\cdots\left(1-\frac{k-1}{N}\right) < \frac{1}{2}$$

$$\approx 1 - \frac{(1+2+\cdots+(k-1))}{N} + \left(\frac{1}{N^2}\text{ stuff}\right)$$

let's ignore.

so we need $\frac{1+2+\cdots+(k-1)}{N} > \frac{1}{2}$

so $\frac{\frac{k^2-k}{2}}{N} > \frac{1}{2}$ roughly $\frac{\frac{k^2}{2}}{N} > \frac{1}{2}$

$\frac{k^2}{N} > 1$. so $\boxed{k > \sqrt{N}}$ this is right when N is really big!

Factoring

Suppose you want to factor N.

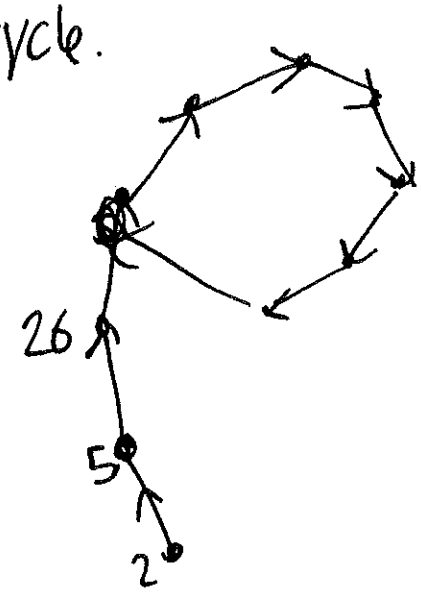
Here's what we do.

Set $X_0 = 2$ (or another favorite number)

$X_{i+1} = X_i^2 + 1 \mod N.$

this is basically a sequence of random numbers mod N.

eventually (probably after $\sim\sqrt{N}$ steps), you hit a number you already saw, and enter a cycle.



looks like "ρ", vaguely.

$N = 120$

$2, 5, 26, 77, 50, 101,$

$N = 500$

$2, 5, \underline{26}, 177, 330, 401, 302, 205, \underline{26}, 177, 330, \ldots$

repeat after 9 numbers!

Suppose N is a multiple of p. What happens to our sequence x_i if we look mod p instead of mod n?

It will probably repeat faster mod p than mod N!

$\sqrt{p}$ vs $\sqrt{N}$

eg $N = 500$ is a multiple of 10!

repeats mod 10 faster than mod 500. ✓

Idea: if x_i and x_j agree mod p

(which is likely to happen pretty quickly),

then $x_i - x_j$ is a multiple of p.

To try to find a factor of N:

- Compute "random" sequence x_i
- Check $\gcd(N, x_i - x_j)$ for various i, j.

  Hope that finds a factor!

Game theory

(I will follow Math 486 lecture notes from PSU, Christopher Griffin)

Conditional probability

"$\mathbb{P}(A)$" means the probability that A happens.
it's a number between 0 and 1 (inclusive)

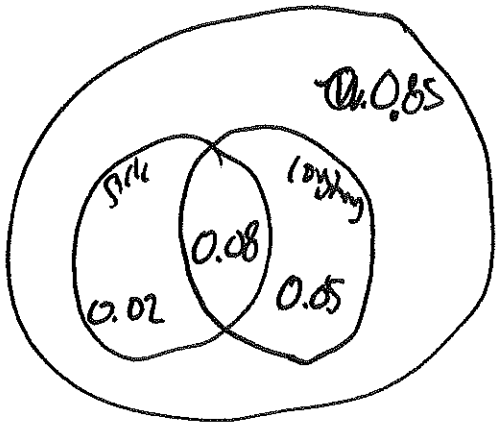
"$\mathbb{P}(B)$"

"$\mathbb{P}(B|A)$" is the probability that B happens, given that A happens.

Ex A = person is sick
B = person is coughing

Suppose:

sick + coughing	0.08
sick + not coughing	0.02
not sick + coughing	0.05
not sick + not coughing	0.85
Σ	1



$\mathbb{P}(A) = 0.08 + 0.02 = 0.10$

$\mathbb{P}(B) = 0.08 + 0.05 = 0.13$

$$\mathbb{P}(\text{sick} \mid \text{coughing}) = \frac{0.08}{0.08 + 0.05} = \frac{8}{13}$$

in general, the rule is:

$$\mathbb{P}(A \mid B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$$

Challenge: Come up with a formula relating $\mathbb{P}(B \mid A)$ and $\mathbb{P}(A \mid B)$ using that definition?

$$\mathbb{P}(A \mid B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} \qquad \mathbb{P}(B \mid A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(A)}$$

$$\frac{\mathbb{P}(A \mid B)}{\mathbb{P}(B \mid A)} = \frac{\mathbb{P}(A)}{\mathbb{P}(B)} \quad \text{or} \quad \boxed{\text{Bayes' rule}} \quad \mathbb{P}(A \mid B) = \frac{\mathbb{P}(B \mid A)\,\mathbb{P}(A)}{\mathbb{P}(B)}$$

The Monty Hall Problem

The host of a game show hides a prize behind one of three doors.

First, you pick a door. (but don't open it)

The host ~~reveals~~ opens one of the other empty doors, showing there's nothing there.

You can stick with your choice, or switch doors.

What should you do?

What's $\mathbb{P}(\text{win} \mid \text{switch})$?

$\mathbb{P}(\text{win} \mid \text{don't switch})$?

P(you picked wrong to start) is $2/3$.

in this case, if you switch, you win.

So if your strategy is to always switch, you'll win $2/3$ of the time!

$$P(\text{win} \mid \text{switch}) = 2/3$$

$$P(\text{win} \mid \text{don't switch}) = P\left(\begin{array}{l}\text{you picked right in} \\ \text{the first place}\end{array}\right) = 1/3.$$

Let's try to define a game using a <u>game tree</u>.

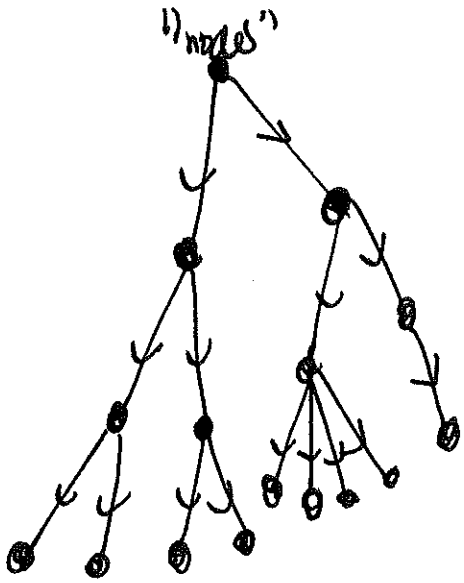
Simplest kind of game: - Complete information
- No chance

We start with a "directed tree" (V, E)

set of vertices

set of edges

no loops



- node for every possible game position
- edge between two nodes if there's a legal move taking you from one to other.

"player vertex assignment": $v: V \setminus \text{terminal} \to P$

every node is assigned to a player.

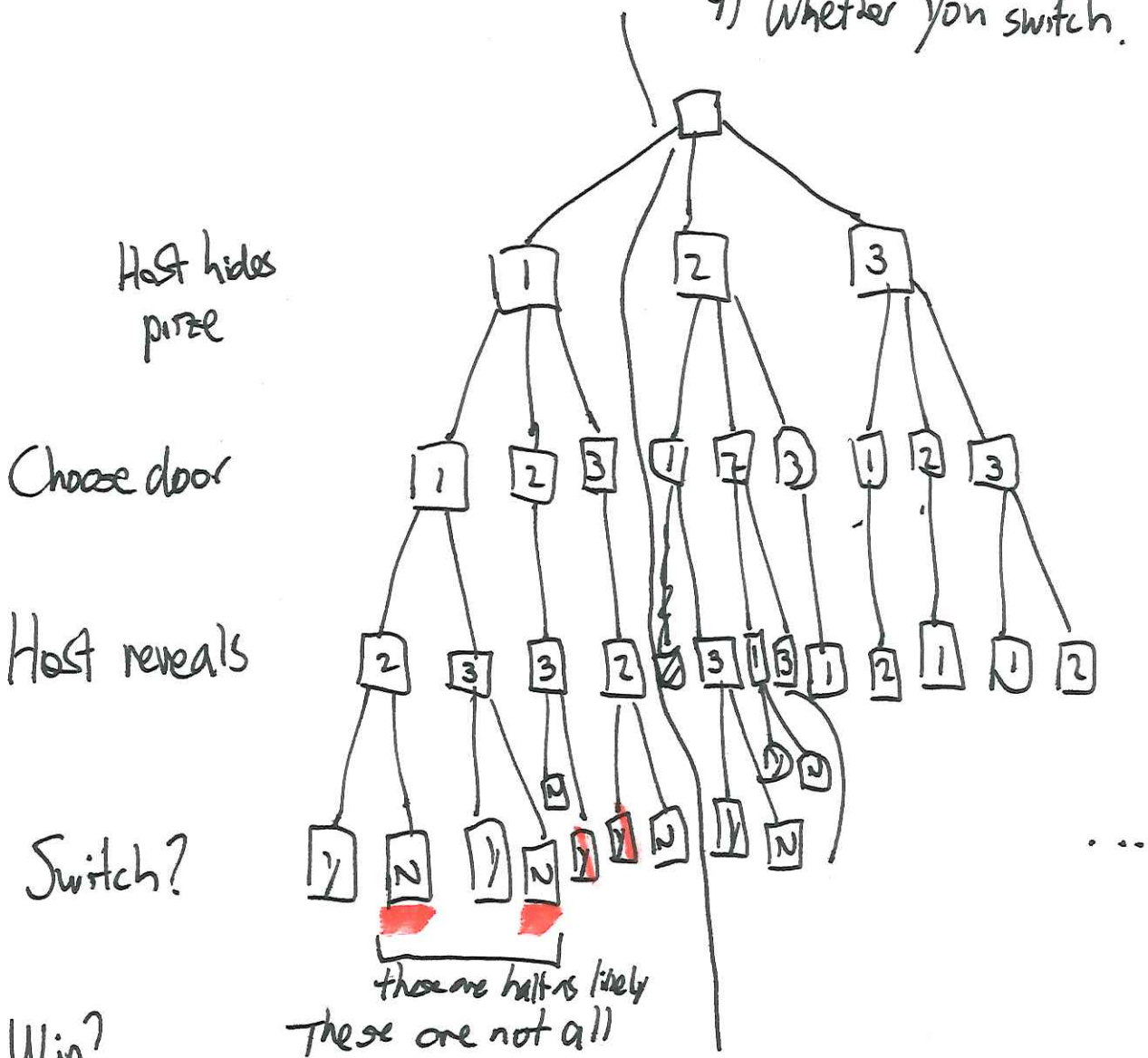
"payoff function"

at every terminal node (final position), assign a numerical outcome to each player. $F: \{\text{terminal nodes}\} \to \mathbb{R}^N$

a vector with an entry for each player

Represent the game as a tree.

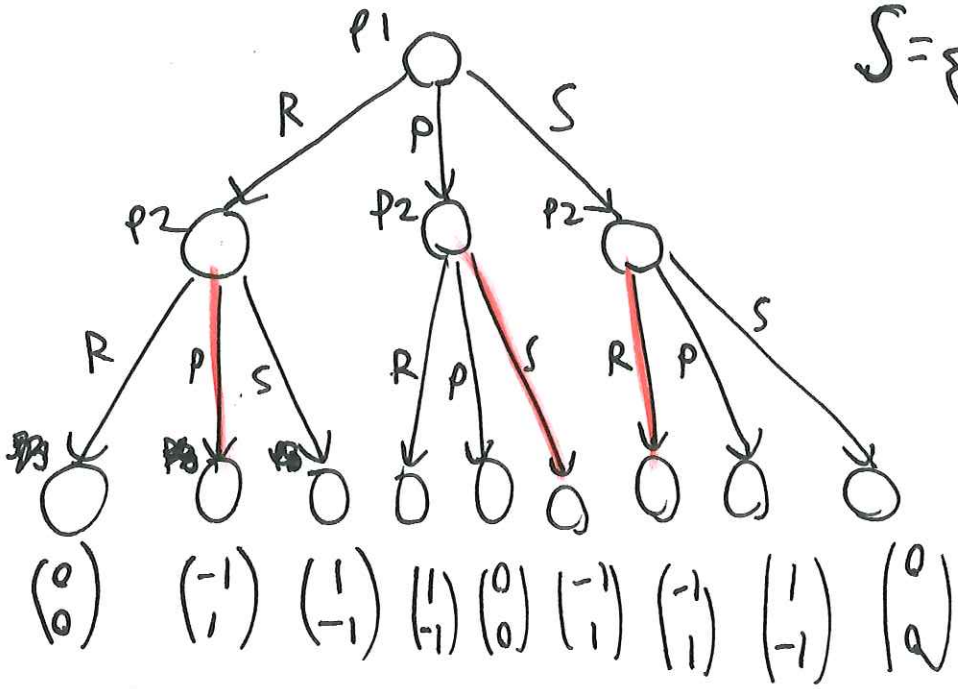
1) Which door it's hidden
2) Which door you choose
3) Which door host reveals
4) Whether you switch.



"move assignment": give a set of "moves" S, and every edge should be assigned to one element of S.

<u>Problem</u> Unfair rock paper scissors

$S = \{R, P, S\}$



✓ everything is defined.

A <u>strategy</u> for Player i in a game like this is: a choice of move at every vertex ~~owned~~ controlled by player.

~~vertices where it's your turn~~

$G_i : V_i$

Imperfect information

Now we want to describe games where the player doesn't have complete information (i.e. player doesn't know which vertex they're at)

Ex Rock paper scissors, blackjack, poker, kriegspiel, ... Monty Hall, ...

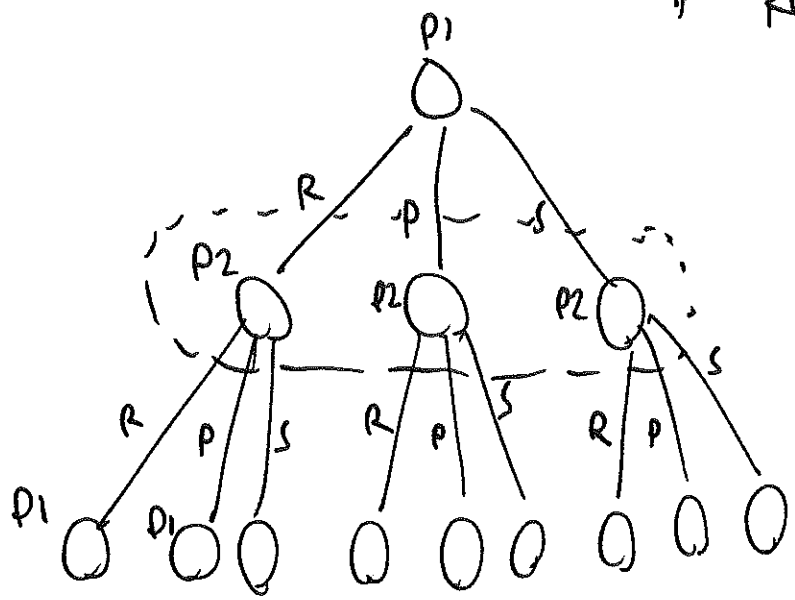
(some of these have an element of chance)

How to formalize this?

Divide the vertices into "information sets":

- all vertices in an information set must have same player's turn.
- all vertices in an information set must have the same "~~xxxx~~ moves types" available to a player.

Real RPS:



How to incorporate chance into a game?

Add player 0, "Fate"! ~~Now some~~

At every "fate" vertex, assign probability to each edge leaving the vertex.

Types of games:

- number of players
- turn-taking vs simultaneous moves
- complete information (both players know where on the game tree they are)
- randomness ("nature"/"fate" player?)

...

(check Wiki!)

Tic-tac-toe: 2-player, complete information, not randomness.

Prisoner's dilemma/RPS, 2-player, not complete information

BattleShip

Yahtzee!

Sorry! Incomplete + random

[...]

Theorem (Zermelo's theorem)

In a 2-player game with complete information, no randomness, only win/loss outcomes, then either Player 1 or Player 2 has a forced win strategy.

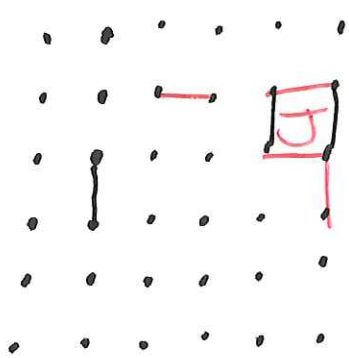
(a choice of move at every node on the game tree)

~~Example~~

If game also allows draws, there's a third possibility: either player can force a draw.

What does this apply to?

- Chomp
- Dots & Boxes



- Nim
- Hex

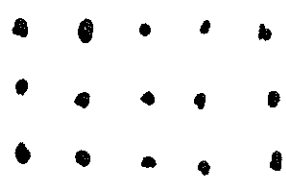
Nim (one version):

2 player

→ Put N rocks in middle of table
(maybe N=15?)

→ Each player picks up 1, 2, or 3 rocks as a turn.

→ Whoever takes last rock loses.



Zermelo: either first or second player has a forced win!
But which is it?

Who wins? N=15. First player should pick up 2.
1st!

13 left.

If second player picks up j, first player picks 4-j.] total is 4

9 left.

repeat. 2x

5 left, 1 left, and 2nd player picks it up and loses.

First player loses if $N \equiv 1 \bmod 4$.

Hex (see board on next page)

- draws are impossible! so forced win for either 1st or 2nd player

(John Nash proved in 1949)

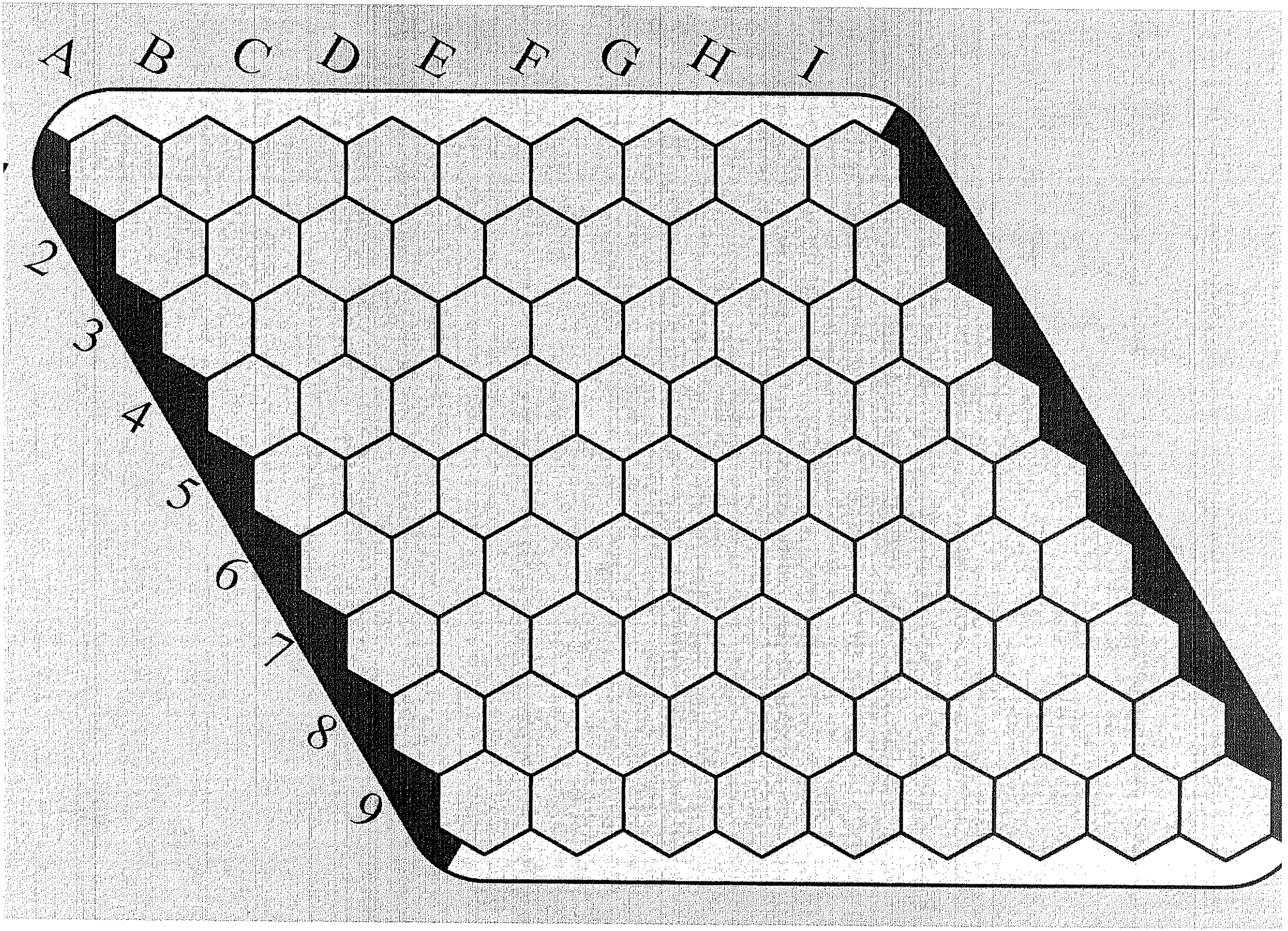
"Brouwer fixed point theorem"

Zermelo: Either 1st or 2nd player has a winning strategy.

Which is it? It's a forced win for first player!
(But nobody actually knows the winning strategy.)

"Strategy stealing": if there were a forced win for 2nd player, first player could just make a random move and then adopt that strategy.

doesn't apply to chess, dots & boxes, because taking turn can hurt you in those games.


A B C D E F G H I
2
3
4
5
6
7
8
9

Review of last week:

A new game: Battle of the Bismarck Sea

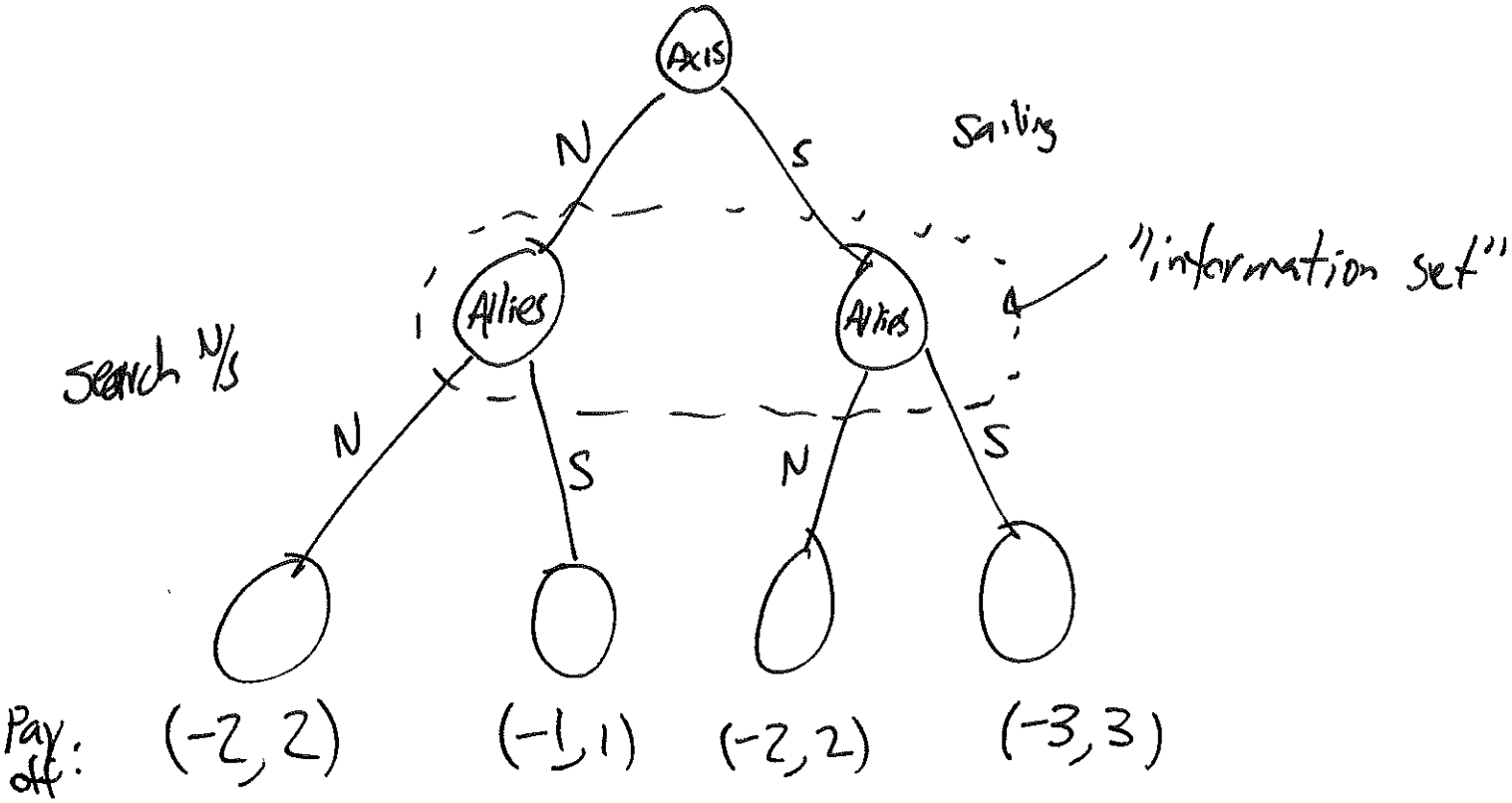
Axis: Must choose to sail either N or S of New Britain.

Allies: Must search either N or S.

<u>Payoff functions:</u>

Sail north, search south: bomb for 1 day.
Sail north, search north: bombed for 2 days.
Sail south, search south: bomb for 3 days.
Sail south, search north: bombed for 2 days.

Challenge: Draw game tree for battle (+payoff functions)



"extensive form" of the game.

"Sail north" <u>weakly dominates</u> "sail south"

(no matter what the other player does, outcome is no worse)

Strategic form of a game.

For a two-player game, let $\Sigma_1 = \left\{ \begin{array}{c} \text{Strategies for} \\ \text{player } 1 \end{array} \right\}$

$\Sigma_2 = \left\{ \begin{array}{c} \text{strategies for} \\ \text{player } 2 \end{array} \right\}$.

number of strategies

Suppose $\#\Sigma_1 = N_1$, $\#\Sigma_2 = N_2$.

$|\Sigma_1|$

$\text{card}(\Sigma_1)$

make an $N_1 \times N_2$ matrix, and in each (i,j) entry put the payoff for player 1 is case ~~of~~ ~~strat~~ player 1 uses i^{th} strategy and player 2 uses j^{th} strategy.

Then do same for player 2.

Ex Battle of Bismarck sea.

Player 1 (Axis)

	search N	search S
sail N	-2	-1
sail S	-2	-3

Player 2 (Allies)

	search N	search S
sail N	2	1
sail S	2	3

$$A_1 = \begin{pmatrix} -2 & -1 \\ -2 & -3 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}$$

$A_1 = -A_2$ (a "zero-sum game")

Chicken

Player 1

	swerve	don't swerve
swerve	0	-1
don't swerve	1	-100

$$\begin{pmatrix} 0 & -1 \\ 1 & -100 \end{pmatrix}$$

Player 2

	swerve	don't
swerve	0	1
don't	-1	-100

$$\begin{pmatrix} 0 & +1 \\ -1 & -100 \end{pmatrix}$$

not zero-sum!

For complex games, strategic form is too large, but for simple games, it helps the analysis a lot!

Another example: 2 players, three strategies each

$$A = \begin{pmatrix} -15 & -35 & 10 \\ \boxed{-5} & 8 & 0 \\ -12 & -36 & 20 \end{pmatrix}$$

zero-sum game: payoff for P2 is opposite.

Player 1: "Minimax strategy": Pick option whose worst possible outcome is least painful.

(that's option 2)

Player 2: analogous option 1

Player 1 doing strategy 2, Player 2 doing strategy 1 is "equilibrium"

Nash Equilibrium

Two player game.
Two Strategy

	a	b
	c	d

Mixed strategy: [Player 1 does Strategy 1 with prob x
Strategy 2 with prob $1-x$

[Player 2 does Strategy 2 with prob y
strategy 2 with prob $1-y$.

---

e.g.

$$\begin{array}{c} \\ x \rightarrow \\ 1-x \rightarrow \end{array} \begin{array}{c} \begin{array}{cc} y & 1-y \end{array} \\ \begin{pmatrix} 1 & 5 \\ 6 & 4 \end{pmatrix} \end{array}$$

Player 1's matrix

Expected payoff for P1:

$$xy(1) + x(1-y)(5) + (1-x)y(6) + (1-x)(1-y)(4)$$

$$= -6xy + 2y + x + 4$$

$$= \begin{pmatrix} x & 1-x \end{pmatrix} \begin{pmatrix} 1 & 5 \\ 6 & 4 \end{pmatrix} \begin{pmatrix} y \\ 1-y \end{pmatrix}$$

Nash equilibrium occurs at saddle point!

$$f(x,y) = -6xy + 2y + x + 4$$

$$f_x = -6y + 1 \qquad f_y = -6x + 2.$$

Saddle point: $\left(\frac{1}{3}, \frac{1}{6}\right)$ is the equilibrium!

A catch: Sometimes the equilibrium isn't at a saddle pt; it could be on the "edge" of region ($x=0$ or 1, $y=0,1$).

Here's a game:

Imagine $f(x,y) = x + y$. What's Nash equilibrium?

$x=1$ (otherwise increasing x improves player 1)

$y=0$ (otherwise decreasing y would improve player 2)

Try another: chicken.

		y	$1-y$
		DS	S
x	DS	-10	1
$1-x$	S	-1	0

	DS	S
DS	-10	-1
S	1	0

Nash equilibria?

$$f_1(x,y) = -10xy + x(1-y) - y(1-x) = -10xy + x - y$$

$$f_2(x,y) = -10xy + (1-x)y - x(1-y) = -10xy - x + y$$

---

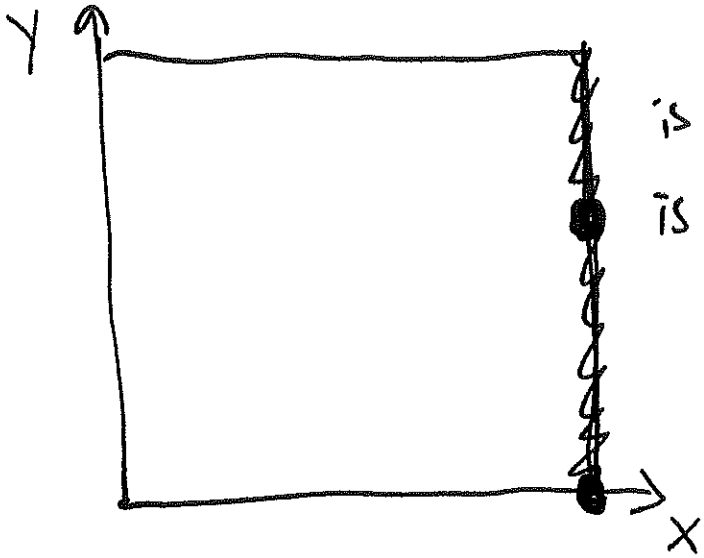
is there one in the "middle"?

$$\frac{\partial}{\partial x} f_1 = 0 \quad \text{and} \quad \frac{\partial}{\partial y} f_2 = 0$$

$$-10y + 1 = 0 \qquad -10x + 1. \rightsquigarrow \left(\frac{1}{10}, \frac{1}{10}\right)$$

Nash equilibrium

On "edges"



is there an equilibrium here?

is $(1, y_0)$ an equilibrium for some y?

if $\left(\frac{\partial}{\partial x} f_1\right)(1, y_0) > 0$ then P1 ok.

$\left(\frac{\partial}{\partial y} f_2\right)(1, y_0) = 0$ then P2 ok.

$$(-10x + 1)\Big|_{(1, y_0)} = 0 \qquad x \in \cancel{[0}$$

No way!

No equilibrium in the middle of an edge!

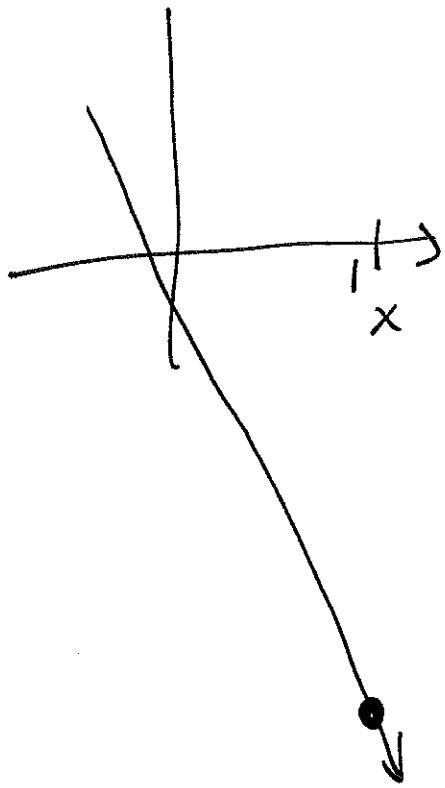
What about $(1,1)$?

$(1,1)$? If P1 decreases x a little bit, does f_1 increase or decrease?

$f_1(x,y) = -10xy + x - y.$

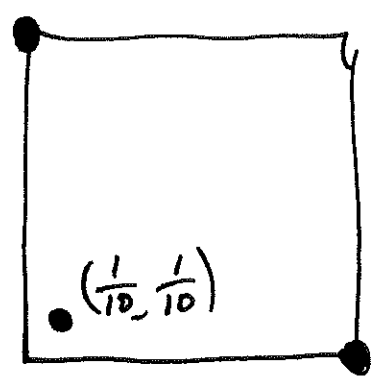
If $y=1$: ∇_x

$-9x - 1.$



<u>Not</u> a Nash equilibrium!

Player 1 can change strategy and do better.



3 equilibria!

Main part of proof

Brouwer Fixed Point Thm

If you have a continuous function

$f: K \to K$ where K is a <u>convex</u> closed subset of $\mathbb{R}^n$,

then there exists an x with $f(x) = x$

ex: $f: [0,1] \times [0,1] \to [0,1] \times [0,1]$

"If you crumple up a sheet of paper map and set

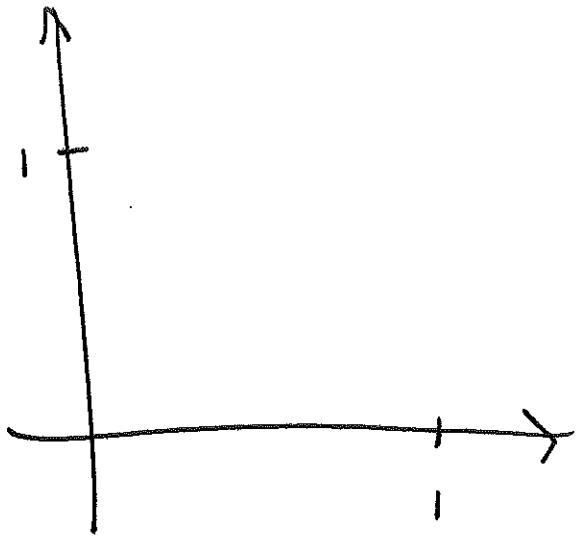
- If you crumple a sheet of paper and place it on top of another sheet of paper, some point ends up directly above corresponding point on other paper.

- If you place a map of USA on the ground inside USA, some point on map is directly above the corresponding real-life point.

(Why: Let K be the map, maybe $0 \le x \le 2$, $0 \le y \le 1$

$$f((x,y)) = \begin{pmatrix} \text{the new } (x,y) \text{ on map where} \\ \text{original pt ended map} \end{pmatrix}$$

- If you stir a cup of coffee, some coffee particle ends up in the same place it was before you stirred!



This doesn't work if we relax the requirements!

→ If not closed, $x^2 : (0,1) \to (0,1)$.

→ If not continuous, $f(x) = x + 0.1 \mod 1$

→ If not convex, rotate

"algebraic topology"

Borsuk-Ulam thm

Suppose $f: S^2 \to \mathbb{R}^2$ is continuous.

sphere (no cutting!)

opposite pt.

There exists an x so $f(x) = f(-x)$.

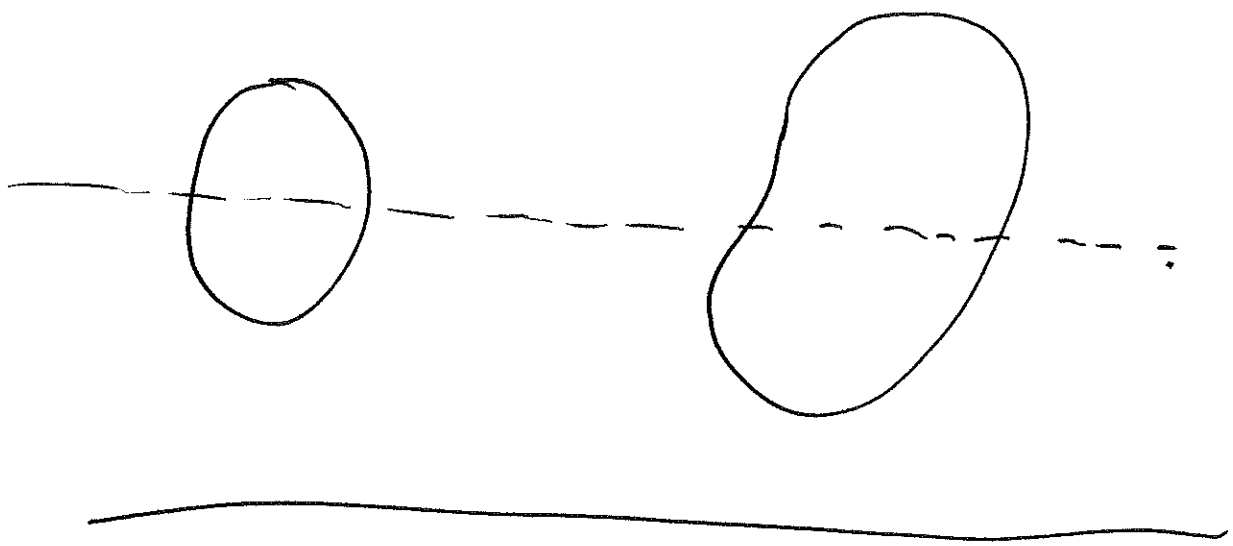
"There are always two opposite points on earth with the same temperature and the same humidity."

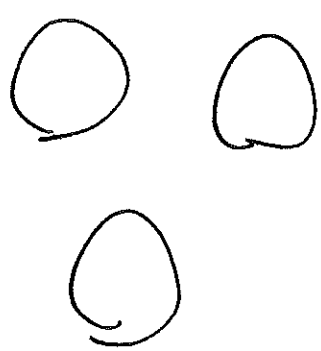
$$f(\text{pt on earth}) = \begin{pmatrix} \text{temp at pt}, & \text{humidity at pt} \end{pmatrix}$$

Ham Sandwich Theorem

Suppose you have n regions in $\mathbb{R}^n$.

There exists an $(n-1)$-dimensional plane which cuts all your regions in half.





Hairy ball theorem: ("you can't comb a tennis ball")

Let $f: S^2 \to \mathbb{R}^3$ is a function such that

sphere

$f(x)$ is ~~perpendicular~~ parallel to sphere

tangent

at every point.

Then $f(x) = 0$ for some x.

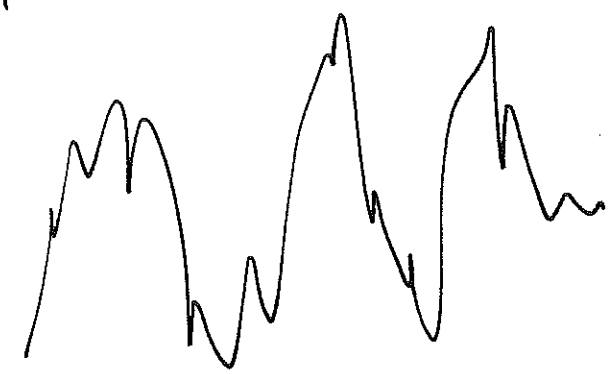
"There's always a point on Earth where the wind isn't blowing."

Optimization

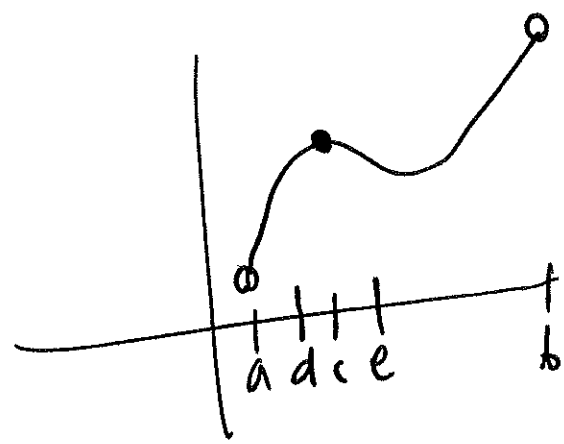
Suppose f is a function defined on an interval (a,b).

$x=c$ is a <u>local maximum</u> of f if:

"decreasing on both sides"



There's a smaller interval (d,e) with $d \le c \le e$ and if $x \in (d,e)$ then $f(x) \le f(c)$.



$x=c$ is a <u>global maximum</u> of f: for any $x \in (a,b)$,

$f(x) \le f(c)$.

Theorem

Suppose f is a differentiable function defined on (a,b). If c is a local max/min of f, then $f'(c)=0$.

Pf. We know that $\lim_{x\to c} \underbrace{\frac{f(x)-f(c)}{x-c}} = f'(c)$.

Suppose $f'(c)>0$ for contradiction.

This means there is an interval (d,e) containing c so that if $x\in(d,e)$ then

$$\frac{f(x)-f(c)}{x-c}>0.$$

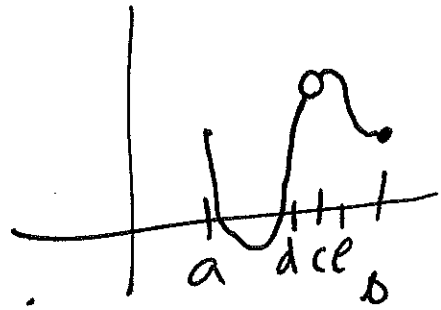
~~I claim~~ Suppose if $x\in(d,c)$

then $x-c<0$ so $f(x)-f(c)<0$.

So $f(x)<f(c)$, so ~~the~~ c not a local min.

If $x\in(c,e)$ then $f(x)>f(c)$, so c not local max.

draw a picture of this as a function of x

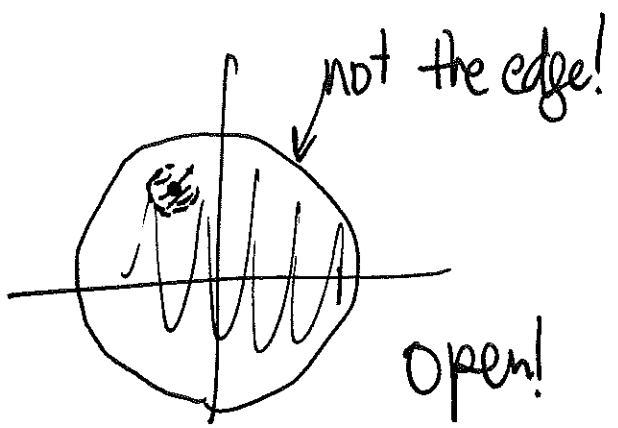


A set $S \subset \mathbb{R}^2$ is <u>open</u>

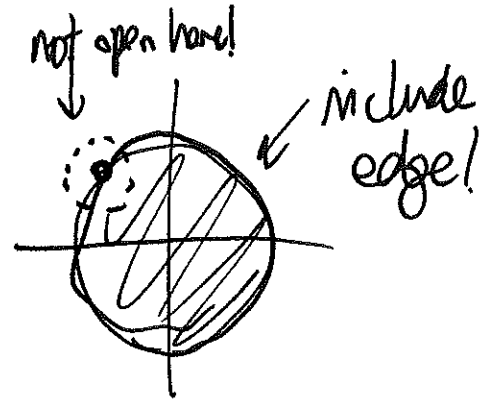
if for ~~any~~ every point $x \in S$, there's a small disk around x that's entirely contained in S.

<u>Ex</u>

$S = \{(x,y) : x^2 + y^2 < 1\}$



$S = \{(x,y) : x^2 + y^2 \leq 1\}$



S is <u>closed</u> if its complement is open.

- for any $p \notin S$, there's a disk around p entirely not in S.

Quiz: Open, closed, both, neither.

a) $\{(x,y): 0 < x < 1\}$

open but not closed

b) $\{(x,y): 0 \leq x < 1\}$

neither open nor closed

c) $\{(x,y)$: x and y are both integers$\}$

closed

g) $\{(x,y)$: x and y are both rational$\}$

neither

d) $S = \mathbb{R}^2$

both!

"clopen"; "sets are not doors"

e) $S = \phi$.

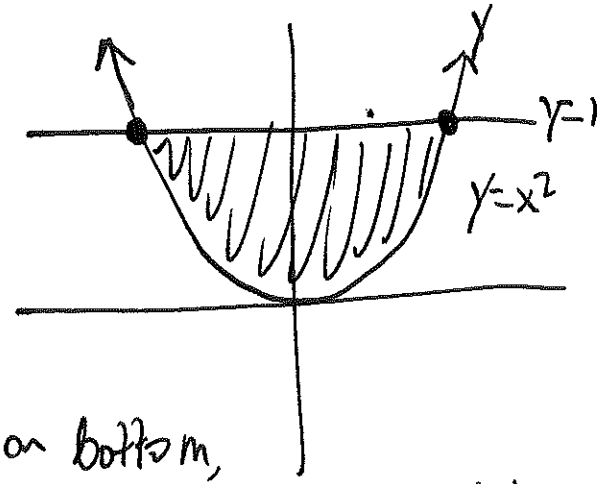
both!

f) All of $\mathbb{R}^2$ except $(0,0)$

open but not closed.

Find global max+min

$$f(x,y)=5x-7y$$



Max/min either in middle, on top, on bottom, or at corner.

Critical pts:

$f_x=5$ $f_y=-7$, none!

top edge: plug in $y=1$, find x $(-1\le x\le 1)$ to max/min $5x-7$.

bottom edge: plug in x^2. max/min $5x-7y=5x-7x^2$ for $-1\le x\le 1$.

$$\frac{d}{dx}(5x-7x^2)=5-14x \rightsquigarrow x=\frac{5}{14},\ y=\frac{25}{196}$$

Candidates:

(x,y)	$f(x,y)$	
$(1,1)$	-2	
$(-1,+1)$	-12	MIN
$\left(\frac{5}{14},\frac{25}{196}\right)$	$\frac{175}{196}$	MAX

Who cares?

- Suppose $f(x,y)$ has a local max/min at c on an <u>open</u> set S. Then c is a critical pt:

$$\frac{\partial f}{\partial x}(c) = \frac{\partial f}{\partial y}(c) = 0.$$

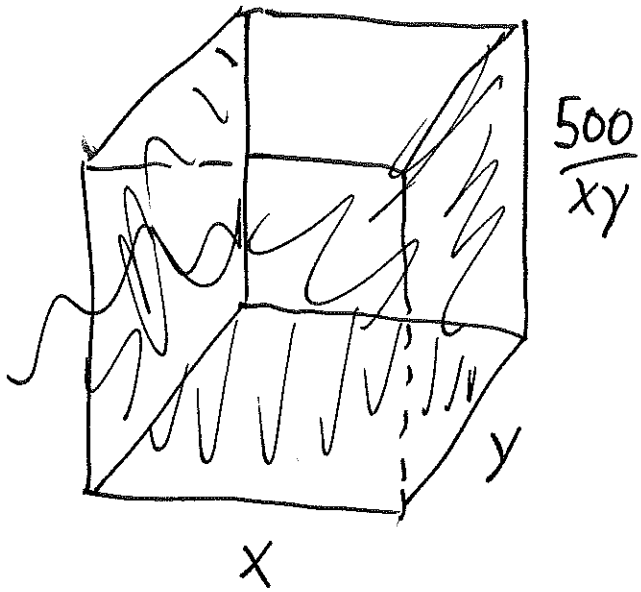
(You already know this from Calc I: a max/min on non-open set might be at an endpt)

↳ Suppose you want to maximize f on a set T that isn't open! Split T into

$$T = S \cup B \text{ where } S \text{ is open, } B \text{ is "boundary"}$$

Find candidate max/min in S using critical points, then worry about B.

Find dimensions of a box with no top such that volume = 500 and surface area is minimized.

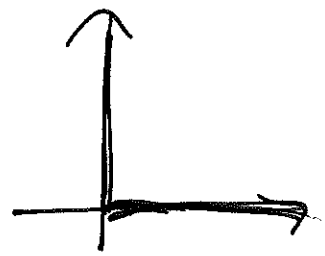


Find x, y to minimize:

$$f(x,y) = xy + \frac{1000}{x} + \frac{1000}{y}$$

constraints:

$x, y \geq 0$



$$f_x = y - \frac{1000}{x^2} = 0, \quad f_y = x - \frac{1000}{y^2} = 0$$

$x = 10, \; y = 10, \; z = 5$

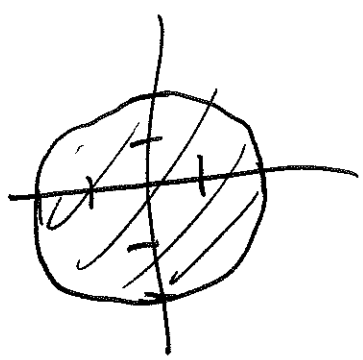
~~Maximize~~

<u>Fact:</u> If T is a set that's closed & bounded, then f has a global maximum/minimum on T.

<u>Problem:</u>

Minimize $x^2 - 2x + 3y^2 + 2$ on a closed disk of radius 2.

$\{(x,y) : x^2 + y^2 \leq 4\}$



If there's a minimum inside the circle, it will be at a critical pt.

How to check for min on the edge?

Critical pts

$f_x = 2x - 2$ $\qquad x = 1$

$f_y = 6y$ $\qquad y = 0$

$(1,0)$ could be minimum!

on the edge?

Parametrize it!

$x = 2\cos\theta$

$y = 2\sin\theta$

$0 \le \theta \le 2\pi.$

Find the θ that minimizes it:

Possible minima

(x,y)	$f(x,y)$
$(1,0)$	1
$\theta=0$: $(2,0)$	2
$\theta=\pi$: $(-2,0)$	10
$(-1/2, \frac{\sqrt{15}}{2})$	$\cancel{\frac{29}{2}}$ $\cancel{\frac{25}{2}}$ $\frac{29}{2}$
$(-1/2, -\frac{\sqrt{15}}{2})$	$\frac{29}{2}$

global min

$$4\cos^2\theta - 4\cos\theta + 12\sin^2\theta + 2$$

$$= 6 - 4\cos\theta + 8\sin^2\theta.$$ ← want to minimize single var minimization!

derivative $\frac{d}{d\theta}$ is: $4\sin\theta + 16\sin\theta\cos\theta = 0$

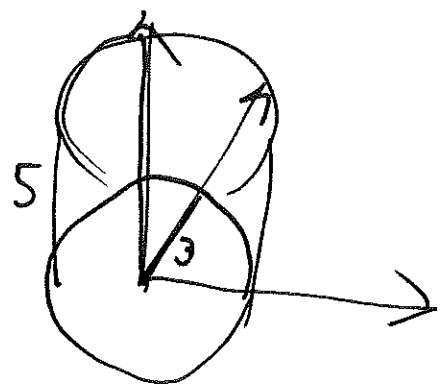
$4(\sin\theta)(1 + 4\cos\theta) = 0 \qquad \theta = 0, \pi, \cos^{-1}\left(-\frac{1}{4}\right)$ all of them

Let's say ~~so~~ you want to maximize/minimize

$f(x,y,z) = x^2 - y^2 + 2x + z$

on a cylindrical region:

$$\left\{ \begin{array}{l} x^2+y^2 \le 9 \\ 0 \le z \le 5 \end{array} \right\}$$



Regions to search:

- inside
  (find critical pts)
- top
  (parametrize, solve 2-var max/min)
- bottom
- circular rims (top, bottom)

Candidate pts:

(x,y,z)	$f(x,y,z)$

Optimization

1) One more problem like last time

2) "Constrained optimization": Lagrange multipliers

   maximize $x^2+3xy+7$

   subject to constraint: $x^2+y^2=25$

3) Linear programming

4) Gradient descent

Example:

Max/min $f(x,y,z)=2x^2+y^2+z^2-2z+xz$

on a cylinder of radius 3 and height 5

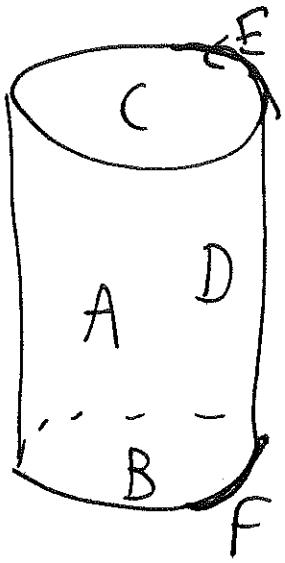
~~centered on (0,0,0)~~

with base in xy-plane around origin

Things to check:

A - Inside cylinder

critical points: $f_x = f_y = f_z$



B - Bottom face

parametrize in polar

or: plug in $z=0$

C - Top face

D - Outer ~~edge~~ face

parametrize

E - Top edge

parametrize with one variable

F - Bottom edge

parametrize with one variable

$x^2+y^2 \le 9$

$0 \le z \le 5$

$\boxed{\text{Inside the cylinder:}}$

Look for critical points

$f_x = 4x + z \rightarrow z = -4x$

$f_y = 2y$

$f_z = 2z - 2 + x \qquad -8x - 2 + x = 0$

$7x = 2$

$x = 2/7,\ y = 0,\ z = -8/7$

Candidate points.

(x,y,z)	$f(x,y,z)$
$(-2/7, 0, 8/7)$	$-8/7$

Bottom face Parametrize it!

$$\left.\begin{aligned} x &= r\cos\theta \\ y &= r\sin\theta \\ z &= 0 \end{aligned}\right] \quad \begin{aligned} &0 \le \theta \le 2\pi \\ &0 \le r \le 3 \end{aligned}$$

$f(x,y,z) =$

$2x^2 + y^2 + z^2 - 2z + xz$

$= 2r^2\cos^2\theta + r^2\sin^2\theta + 0 - 0 + 0$

$= r^2 + r^2\cos^2\theta = (r^2+1)\cos^2\theta$

Max on outside face of cylinder.

Parametrize it by θ, z:

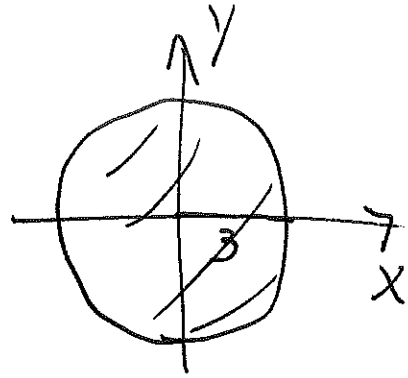
$$\left.\begin{aligned} x &= 3\cos\theta \\ y &= 3\sin\theta \\ z &= z \end{aligned}\right] \rightarrow \text{plug in as } x, y, z.$$

find θ, z to max/min function.

$f(x,y,z) = 2x^2 + y^2 + z^2 - 2z + xz$

Bottom face:

Plug in $z=0$



what x, y make max/min?

$f(x,y) = 2x^2 + y^2$.

$f_x = 4x \Rightarrow x=0,\ y=0,\ z=0.$

$f_y = 2y$

<u>Edge of bottom face:</u>

$(0,0,0)$

$x^2+y^2=9$, substitute in:

$x=-3 \Rightarrow (-3,0,0)$

$f(x,y) = 9 + x^2$. max at $x=3 \Rightarrow (3,0,0)$

min at $x=0 \Rightarrow (0,3,0)$

$(0,-3,0)$

Lagrange multipliers

Suppose you want to maximize/minimize $f(x,y)$ subject to a constraint $g(x,y)=c$.

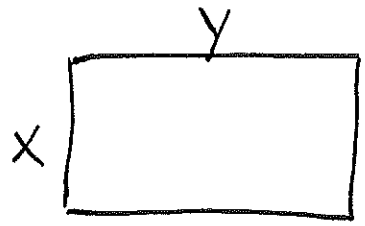
Then the max&min satisfy

$$\nabla f(x,y) = \lambda \nabla g(x,y).$$

scalar

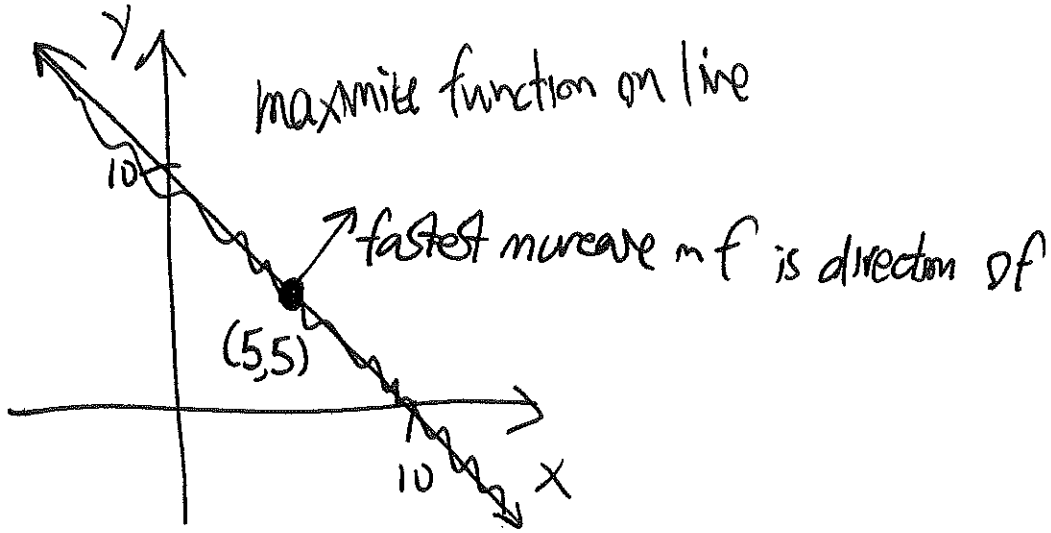
∇f parallel to ∇g!

Ex. Find a rectangle of perimeter 20 with maximize area.



maximize $f(x,y) = xy$

constraint: $g(x,y) = 2x + 2y = 20$.



Solve: $\nabla f = \lambda \nabla g$ and $g(x,y)=c$.

$$\langle y, x\rangle = \lambda\langle 2, 2\rangle \qquad 2x+2y=20.$$

Three equations:

$$\left.\begin{aligned} y &= 2\lambda \\ x &= 2\lambda \\ 2x+2y &= 20 \end{aligned}\right]$$

solve:

$x=y$ so

$4x=20$ so

$\boxed{x=5}$ $\boxed{y=5}$

$\boxed{\lambda=5/2}$

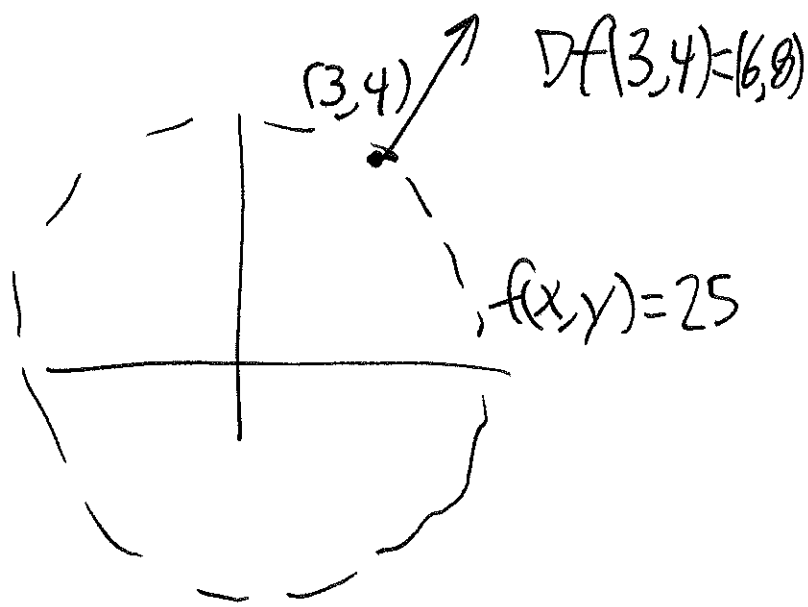
Two ways to think about ∇f:

1) Direction of fastest increase of f

2) Perpendicular to level curves of f:

$f(x,y) = x^2 + y^2$

$\nabla f = (2x, 2y)$



Maximize:

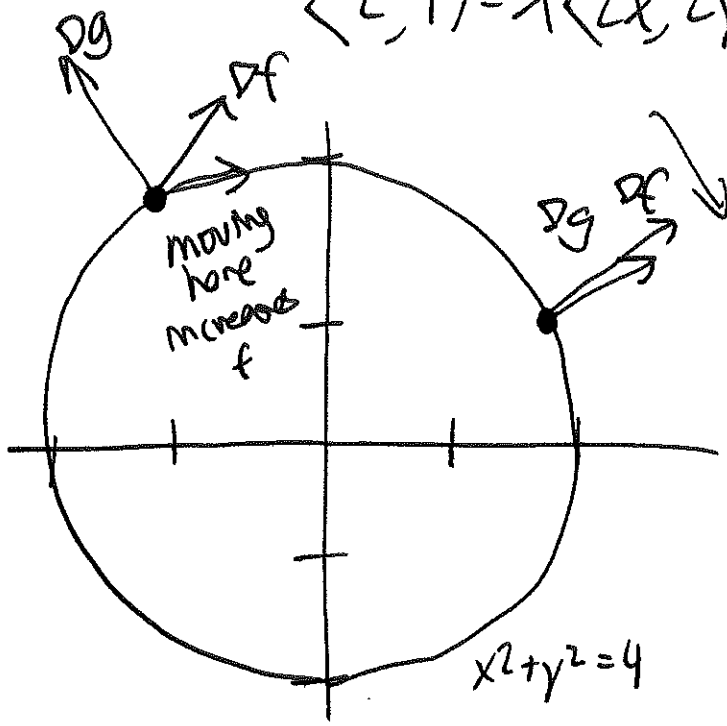
$f(x,y) = 2x + y$

Subject to:

$\underbrace{x^2 + y^2}_{g(x,y)} = 4$

$\nabla f = \lambda \nabla g$

$\langle 2, 1 \rangle = \lambda \langle 2x, 2y \rangle$



$$\left.\begin{aligned} 2 &= 2\lambda x \\ 1 &= 2\lambda y \\ x^2 + y^2 &= 4 \end{aligned}\right]$$

$\frac{2}{x} = \frac{1}{y}$ $\quad 2y = x$

$(2y)^2 + y^2 = 4$

$y^2 = 4/5 \quad y = \pm 2/\sqrt{5}$

$x = \pm 4/\sqrt{5}$

$$2^{2+i} = ?$$

$$x = 2^{2+i}$$

$$\log x = \log 2^{2+i}$$

$$= (2+i)\log 2$$

$$e^{ix} = \text{cis } x$$
$$= \cos x + i \sin x$$

$$\cancel{x = e^{2+i} \cdot e^{\log 2}}$$

$$x = e^{(2+i)\log 2}$$

$$\cancel{= e^{2\log 2}}$$

$$e^{2\log 2} \cdot e^{i\log 2} = (e^{\log 2})^2 e^{i\log 2}$$

$$= 4 \cdot \cos(\log 2) + 4i \sin(\log 2)$$

$$i^i = x$$

$$\left((-1)^{1/2}\right)^i = x$$

$$x = (-1)^{1/2 i}$$

$$\ln x = \ln (-1)^{1/2 i}$$

$$= \frac{1}{2} i \ln(-1).$$

$e^{i\pi} = -1$ so $\ln(-1) = i\pi$

$$= -\frac{1}{2}\pi$$

$$= e^{-1/2 \pi} = 1/\sqrt{e^{\pi}}$$

$$\boxed{i^i = \frac{1}{\sqrt{e^{\pi}}}.}$$

Disclamer: $e^{(2k+1)i\pi} = -1$ so "$\ln(-1)$" isn't really defined. "multi-valued function"

$$\ln x = \frac{1}{2} i \left(e^{(2k+1)i\pi}\right)$$

$$\ln x = \frac{1}{2}\left(-(2k+1)\pi\right)$$

$$x = \sqrt{e^{-(2k+1)\pi}}$$

Why? TI says

$0.5! = 0.866$

$$\int u\,dv = uv - \int v\,du$$

$$\int_0^\infty e^{-t}\,dt = 1$$

$$\int_0^\infty te^{-t}\,dt = 1$$

$$\int_0^\infty t^2 e^{-t}\,dt$$

$$\int te^{-t}\,dt$$

$u = t \qquad v = -e^{-t}$

$du = dt \qquad dv = e^{-t}\,dt$

$$\int u\,dv = uv - \int v\,du$$

$$= (-te^{-t}) - \int (-e^{-t})\,dt$$

$$= -te^{-t} - e^{-t}$$

$$-(t+1)e^{-t}$$

$$\left(-(t+1)e^{-t}\right)\Big|_0^\infty = (0 - -1) = 1$$

Let

$$C_n = \int_0^\infty t^n e^{-t}\,dt$$

The Γ function:

$$\cancel{\Gamma(z) = \int_0^\infty x^{z-1} e^{-x}\,dx}$$

$$\boxed{\Gamma(z) = \int_0^\infty t^{z-1} e^{-t}\,dt}$$

$\Gamma(n) = (n-1)!$

$C_0 = 1,\ C_1 = 1,\ C_2 = 2,\ C_3 = 6,\ C_4 = 24$

Guess (prove by induction + integration by parts)

$C_n = n!$

I checked

So $\left(\frac{1}{2}\right)! = \int_0^\infty t^{1/2} e^{-t}\,dt = \frac{\sqrt{\pi}}{2}$

What you missed:

Plan: Today: Linear programming.

Next: ", Gradient descent

Linear programming:

Chocolate company produces two chocolates:
dark/milk

dark: ~~used~~ uses 1 unit milk + 3 units cocoa

milk: uses 1 unit milk + 2 units cocoa.

Sell dark for \$6, sell milk for \$5

In stock they have 50 milk
120 cocoa

What should they produce to maximize income?

x dark chocolate

y milk chocolate

Linear programming

$x + y \le 50$ (milk constraint)

$3x + 2y \le 120$ (cocoa)

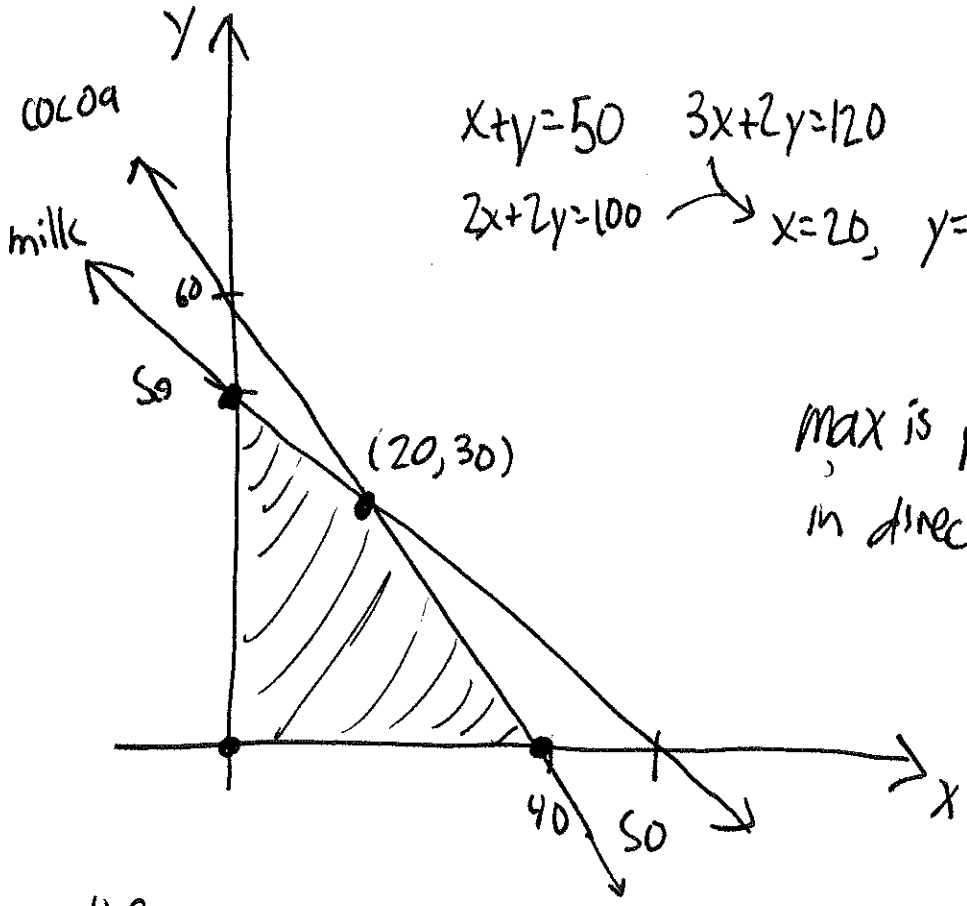
$x \ge 0$

$y \ge 0$

linear constraints

maximize. $6x + 5y$

linear thing to maximize



$x+y=50$ $3x+2y=120$

$2x+2y=100$ → $x=20,\ y=30$

max is point furthest in directed (6,5).

must be at corner!

(0,50) → 200

(40,0) → 240

* (20,30) → 270

(0,0) → 0

"feasible region"

1000 variables, 2000 inequalities:

How many corners?

$$\sim \binom{2000}{1000}. \text{ huge!}$$

$$\frac{200 \times 199 \times 198 \times \cdots}{100 \times 99 \times \cdots}$$

Optimization

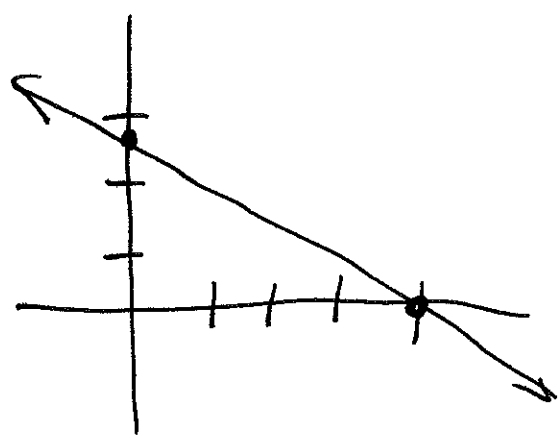
- finding critical pts, etc
- Lagrange multipliers
- Linear programming
- Gradient descent (+ Newton's method)

Maximize/minimize $f(x,y)$

subject to $g(x,y)=c$.

occurs where $Df = \lambda Dg$.

Ex Find the point on $2x+3y=8$ closest to $(0,0)$.



$g(x,y)=2x+3y=8$

Want to minimize!

$\sqrt{x^2+y^2}$ use $f(x,y)=x^2+y^2$ instead.

$Df = \lambda Dg$

$\langle 2x, 2y \rangle = \lambda \langle 2, 3 \rangle$

3 eqns, 3 variables.

$2x = 2\lambda$

$2y = 3\lambda$

$2x + 3y = 8$

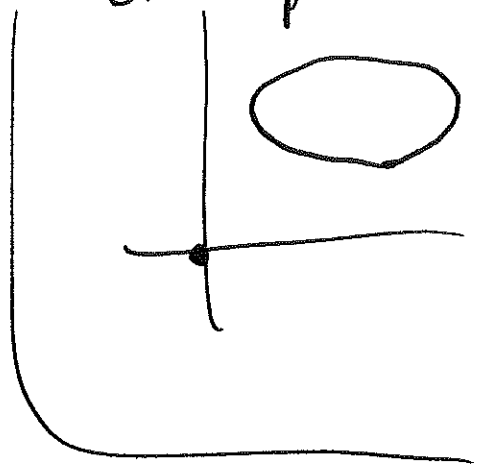
$3y = \frac{9}{2}\lambda$

$2x + 3y = \frac{13}{2}\lambda = 8$

$\lambda = \frac{16}{13}$

$$\boxed{x = \frac{16}{13}, \quad y = \frac{24}{13}}$$

Can solve similar problems!



Linear programming

3 variable problem

3 foods available:

	cost	Vit A	Calories
Corn	18¢	107	72
milk	23¢	500	121
bread	5¢	0	65

Requirements: ~~Budget: L$~~

Vit A: 5000-50000

Calories: 2000-2250

Minimize Budget while satisfying both requirements.

With two variables, we can draw a plot!

With ≥ 3, better to use an algorithm: the simplex method

Use variables c, m, b.

$$107c + 500m + 0b \le 50000$$

$$c, m, b \ge 0$$

$$107c + 500m + 0b \ge 5000$$

$$72c + 121m + 65b \ge 2000$$

$$72c + 121m + 65 \le 2250.$$

objective function:

minimize $18c + 23\cancel{b}m + 5b$

maximize: $-18c - 23m - 5b$

Simplex Method

(we solved it on the computer)

Knapsack problem

Suppose you're packing your backpack.

You have list of possible items, each with a weight + usefulness score.

	Item	Weight	Useful
x_1	Lunch	2	10
x_2	Books	10	1
x_3	Water	1	6
x_4	Computer	5	11
x_5	Spare coat	2	2
x_6	Pencils	0.5	5

all variables must be binary! Either 0 or 1. Simplex alg can handle that

Max weight: 7 lbs

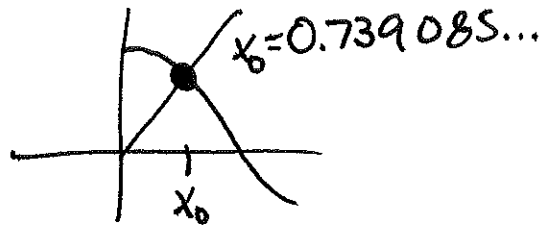
Maximize: $10x_1 + 1x_2 + 6x_3 + 11x_4 + 2x_5 + 5x_6$

Subject to: $2x_1 + 10x_2 + 1x_3 + 5x_4 + 2x_5 + 0.5x_6 \leq 7$

Newton's method (root-finding, not optimization)

Suppose you want to find a root of a function $f(x)$ but can't solve algebraically.

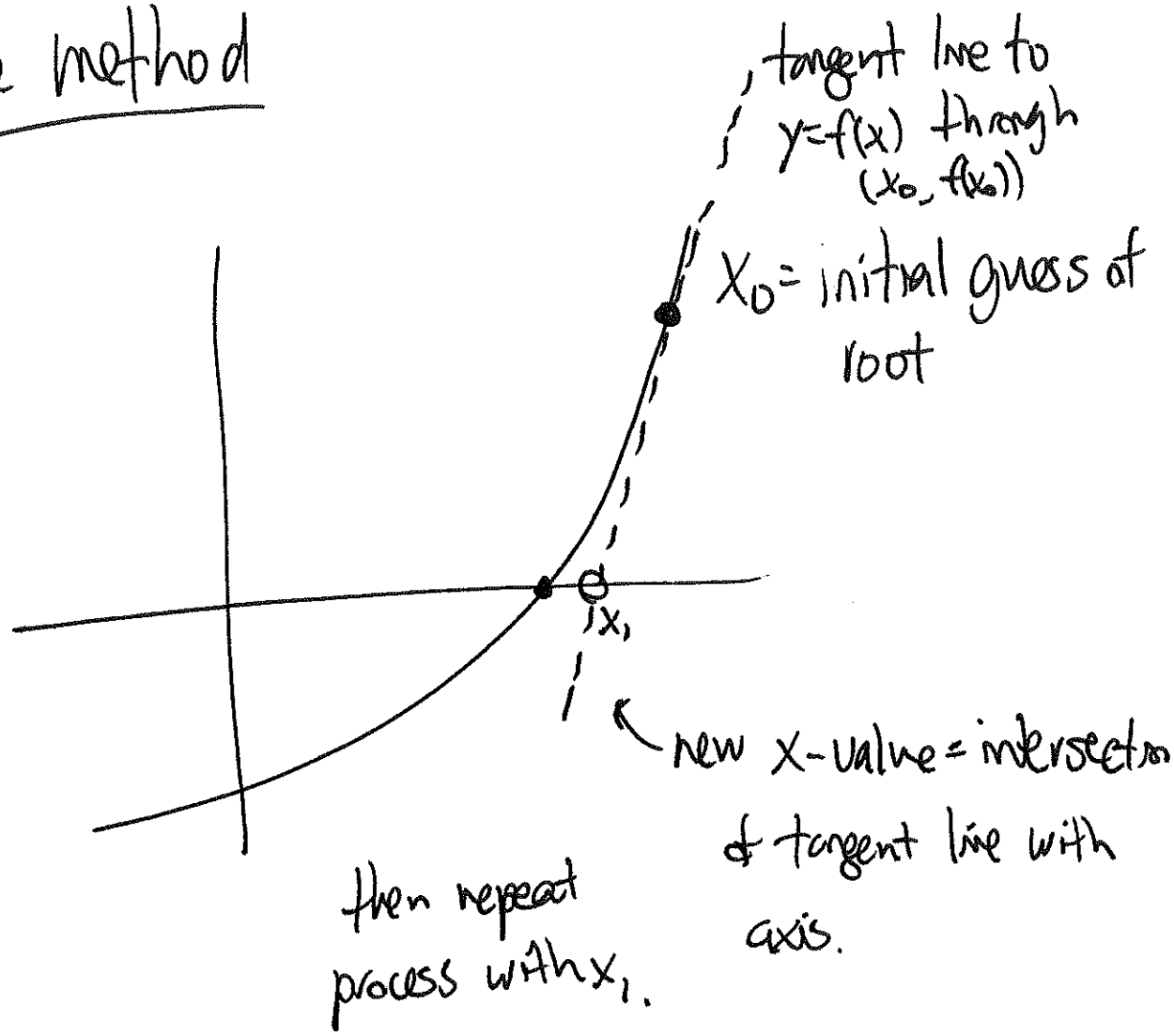
e.g. $x - \cos x = 0$



Newton's method lets you find a numerically accurate approximation of the root (many digits)

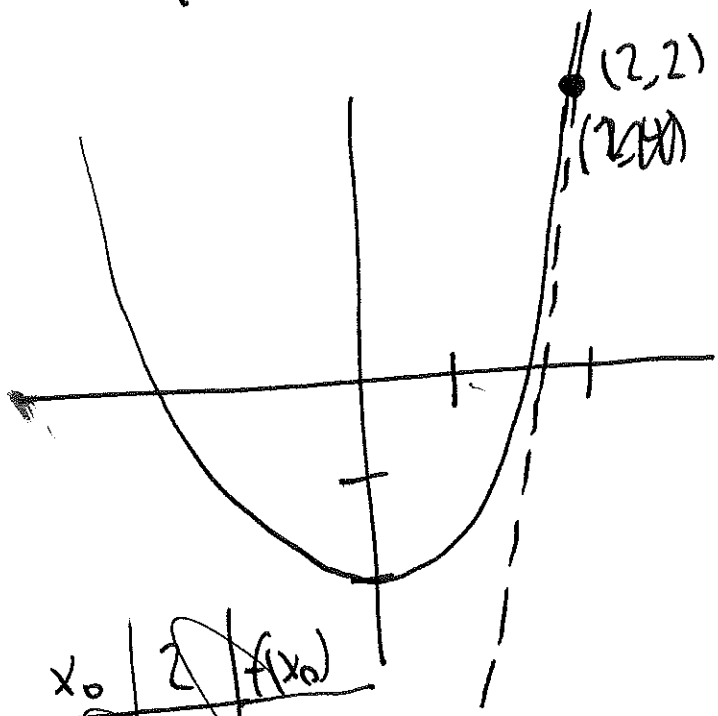
Easier

The method


tangent line to $y=f(x)$ through $(x_0, f(x_0))$
x_0 = initial guess of root
x_1
new x-value = intersection of tangent line with axis.
then repeat process with x_1.

Example

Find a root of, $x^2-2=0$



Initial guess: $x_0=2$

Tangent line to x^2-2 at $x=2$?

$y=4x-6$

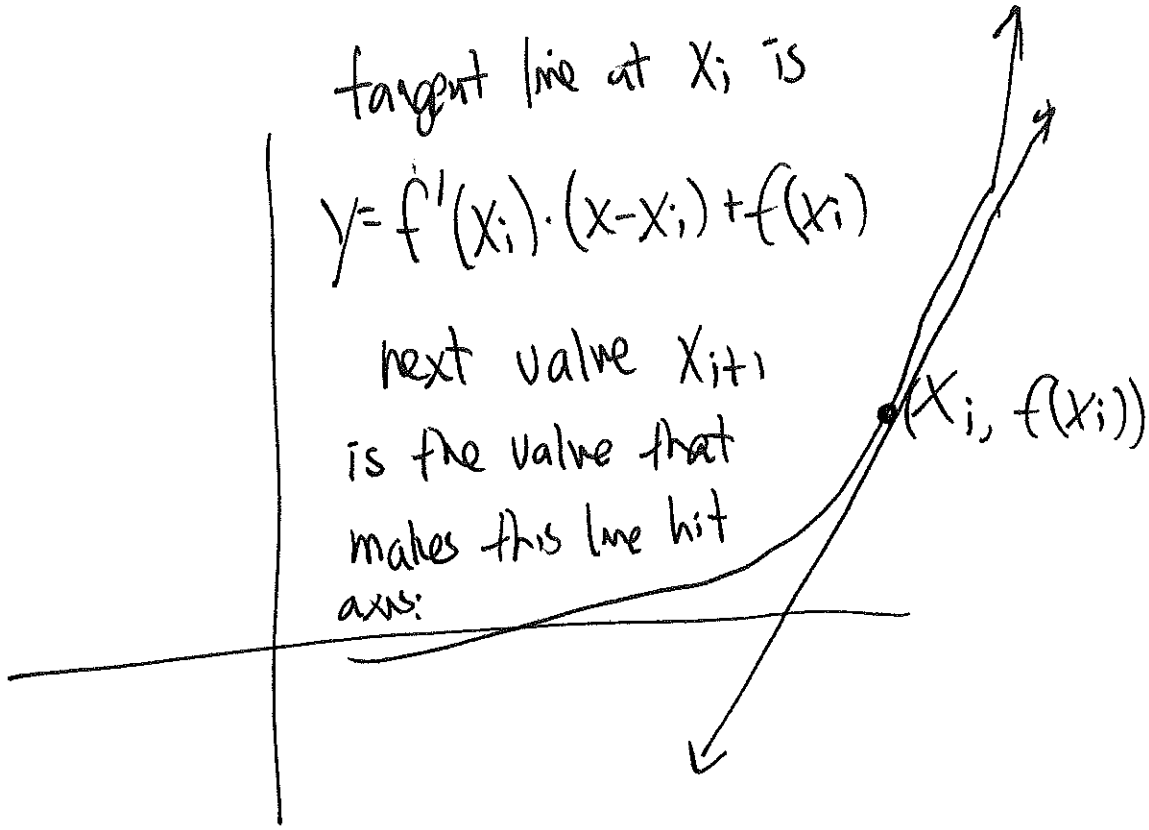
$y=0$ when $x=3/2$

x_0	2	$f(x_0)$
x_1	$3/2$	

i	x_i	$f(x_i)$
0	2	2
1	$3/2$	$1/4$
2	$17/12$	$1/144$

Keep going: ...

General formula



tangent line at x_i is

$$y = f'(x_i)\cdot(x - x_i) + f(x_i)$$

next value x_{i+1} is the value that makes this line hit axis:

$$f'(x_i)\cdot(x - x_i) + f(x_i) = 0$$

$$x - x_i = -\frac{f(x_i)}{f'(x_i)}$$

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

Newton examples

$f(x) = x^2 - 2 \rightsquigarrow$ approximations of $\sqrt{2}$

$2, 3/2, 17/12, 577/408, 665857/470832$

or $1, 1/2, 9/4, 113/72, 23137/16272, \ldots$

$f(x) = x - \cos x$

$1.000, 0.75036, 0.73911,$

$0.7390851333, 0.7390851332151 61, \ldots$

Doubles the number of correct digits every iterations!

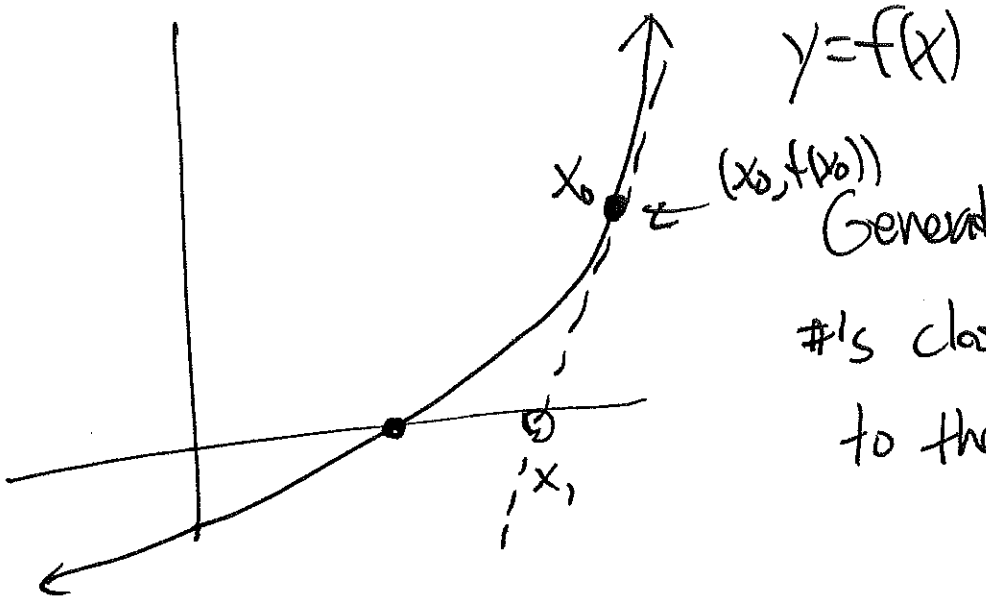
$f(x) = \sin x \longrightarrow$ approximate π

$3, 3.142546\ldots, 3.14159265330048, \ldots$

$3.141592653589 79, \ldots$

Newton's method

"numerical root finding"



Generate a sequence of #'s closer and closer to the actual root.

Tangent line: $y = f'(x_0)(x-x_0) + f(x_0)$

where does it hit axis?

$$0 = f'(x_0)(x-x_0) + f(x_0)$$

$$\Rightarrow x - x_0 = -\frac{f(x_0)}{f'(x_0)}$$

$$x = x_0 - \frac{f(x_0)}{f'(x_0)}$$

Adv Topics 2 (Lesieutre)
Newton's method
November 11, 2021

Problem 1. Use Newton's method to approximate the cube root of 3. For the first five values of x_i, compute the error $\left|\sqrt{3} - x_i\right|$. How fast is the error decreasing?

it seems to be squared every time!

Problem 2. Repeat the first problem, this time to approximate the value of π.

use $\sin x = f(x)$.

Problem 3. Try Newton's method with $f(x) = x^3 - 1$ starting with $x_0 = 0$. What happens? What if you try other starting values?

horizontal tg line → failure

Problem 4. How about $f(x) = x^3 - 2x + 2$, starting with $x_0 = 0$? What about other starting values?

bounces $0 \to 1 \to 0 \to 1 \to 0$

Problem 5. What happens if you try Newton's method for $f(x) = x^2 + 1$? Why?

there's no root

Problem 6. What happens if you try Newton's method for $f(x) = \sqrt[3]{x}$? Why?

gets further and further away!

Problem 7. Consider $f(x) = \frac{1}{1+x^2} - \frac{1}{2}$. Try a few values of x_0. Which root of f do you find? Is there a pattern?

Problem 8. Now we want to derive the steepest descent algorithm for minimization. We use a similar idea to Newton's method: start with a guess x_0, and keep improving it one step at a time.

Do you have a guess? How should we choose a next x-value?

Problem 9. What is your proposal for the step size?

Problem 10. Write down a function with multiple maxima and minima. Apply the algorithm, with a couple options for step size. What do you find?

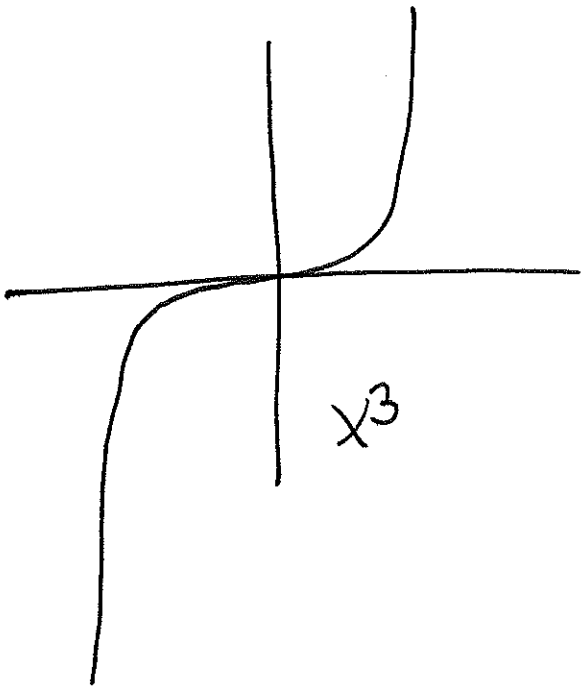
Problem 2: to get π, solve for a root of $\sin(x)$.

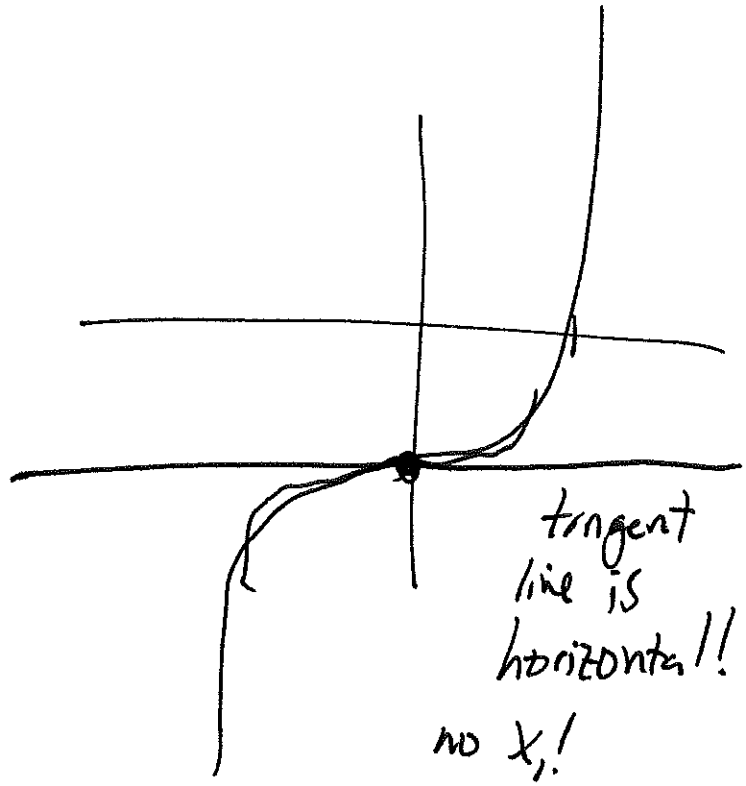
start with $x_0 = 3$ (this is to avoid getting $x=0$).

or: look $\sin(x) - 1$, and still converge to $\pi/2$.

(or $5\pi/2$, etc)

Problem 3: $f(x) = x^3 - 1$ with $x_0 = 0$

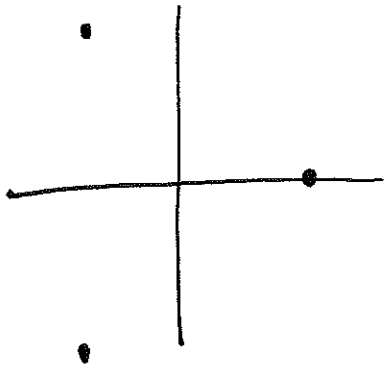




Question:

for $f(x)=x^3-1$, this has 3 complex roots:

If $$1,\ e^{\frac{4\pi}{3}i},\ e^{\frac{8\pi}{3}i}.$$



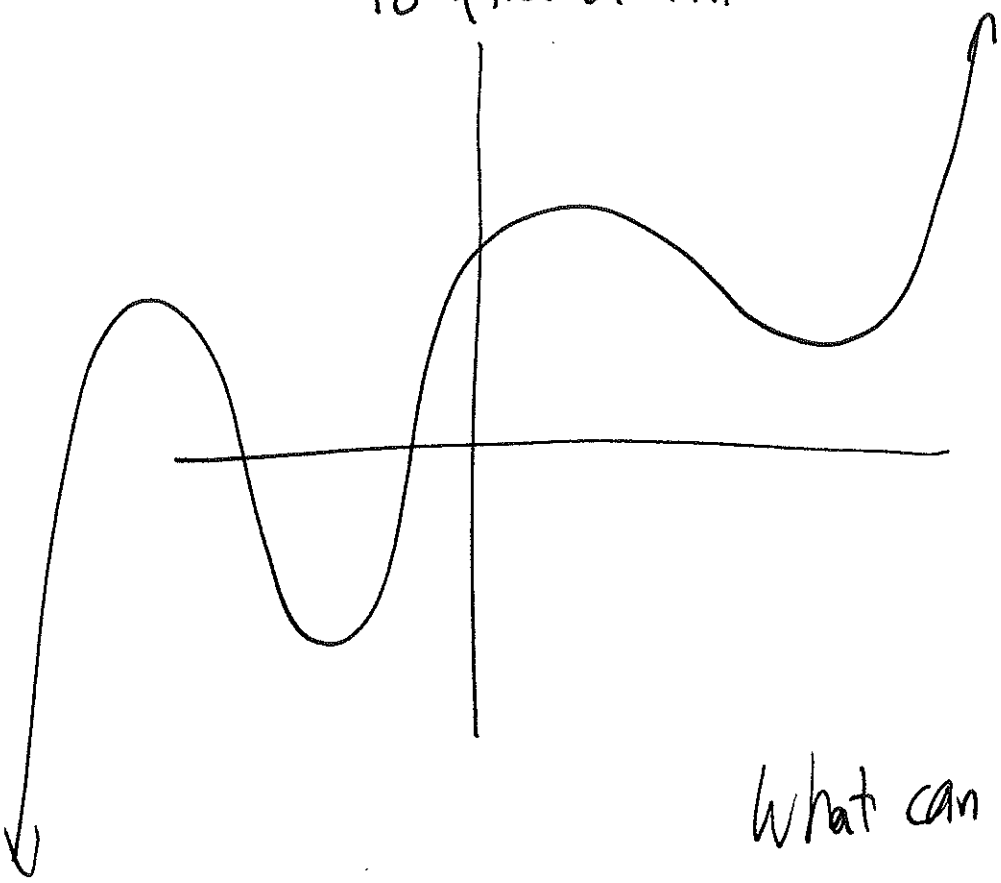
$$\left(e^{\frac{4\pi}{3}i}\right)^3 = e^{4\pi i} = 1.$$

$\cos(4\pi) + i\sin(4\pi)$

Challenge: which complex x_0 find which of the three roots?

Newton's method for optimization.

To find a min:



$y=f(x)$.

You can compute f', f'', but not solve for max/min exactly.

What can we do?

a) Use Newton's method to find a root of f', that's the critical pt

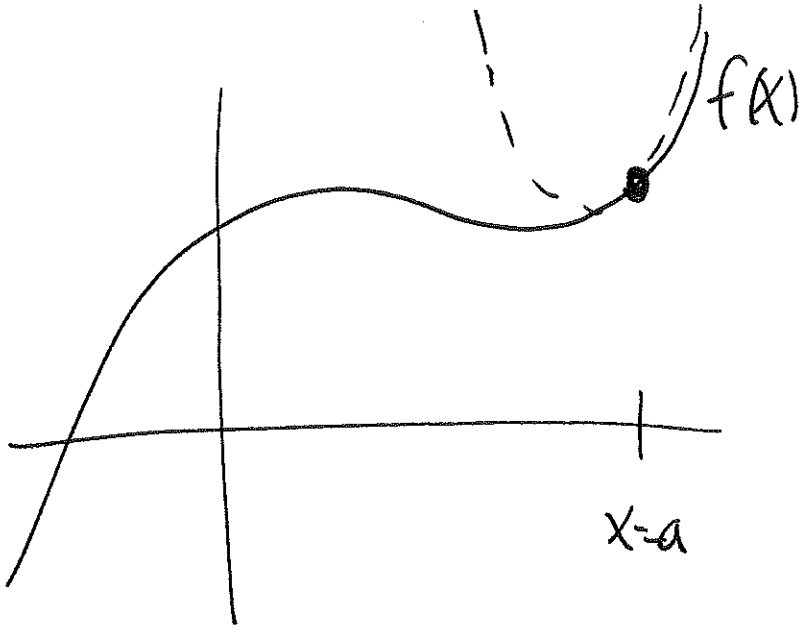
OR

b) Check $f'(x_0)$. If $f'(x_0)<0$, let $x_1=x_0+0.0000$1

OR

if $f'(x_0)>0$, let $x_1=x_0-0.0000$1

* c) Approximate function by a parabola, let x_1 = min of parabola.



<u>Parabola approximation:</u>

$p(x) =$ ~~p~~ 2nd order Taylor series!

(next time)

Taylor Series

Reminder:

Find a cubic polynomial $g(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$ that agrees with $f(x) = \sin x$ "as closely as possible":

1) $g(0) = f(0)$

2) $g'(0) = f'(0)$ $\qquad g'(x) = a_1 + 2a_2 x + 3a_3 x^2$

3) $g''(0) = f''(0)$ $\qquad f'(x) = \cos x$

4) $g'''(0) = f'''(0)$ $\qquad g''(x) = 2a_2 + 6a_3 x$

$f''(x) = -\sin x$

1) gives us $a_0 = 0$ $\qquad g'''(x) = 6a_3$, $f'''(x) = -\cos x$

2) gives $a_1 = 1$ $\qquad$ 4) gives $a_3 = -\frac{1}{6}$

3) gives $a_2 = 0$

$$\boxed{g(x) = x - \frac{x^3}{6}}$$

Deriving the general formula

We have a function $f(x)$

We want to a power series ("infinite degree polynomial") that has $g(0), g'(0), g''(0), g'''(0), g^{(4)}(0), \ldots$ all the same as f does.

This should be a good approximation of f, at least near 0.

Let's just solve for it, one coefficient at a time:

Suppose $g(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \ldots$

We want $f^{(i)}(0) = g^{(i)}(0)$ for every i.

Well, $g^{(4)}(x) = 4 \cdot 3 \cdot 2 \cdot 1 a_4 x^0 + 5 \cdot 4 \cdot 3 \cdot 2 a_5 x^1 + \ldots$

$$g^{(i)}(x) = (i!) a_i x^0 + (\text{terms with } x \text{ in them})$$

$$g^{(i)}(0) = (i!) a_i$$

We want $g^{(i)}(0) = f^{(i)}(0)$

so $(i!)a_i = f^{(i)}(0)$

$$a_i = \frac{f^{(i)}(0)}{i!}$$

So:

$$g(x) = \underbrace{f(0) + f'(0)\cdot x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \frac{f''''(0)}{4!}x^4 + \dots}_{\text{Taylor series for } f(x)}$$

$$\boxed{g(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n}$$

As you include more and more terms, you get a better and better approximation of your function.

Maclaurin series:

$$g(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n$$

Examples

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots$$

$$\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \dots$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \dots$$

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots$$

$$* \quad \frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + x^8 - \dots$$

plug in "$-x^2$"

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \dots$$

$\cos(x) + i\sin(x)$

$\arctan(x)$ / $\tan^{-1}(x)$

$f(x) =$

$$1 + x + 2x^2 + 3x^3 + 5x^4 + 8x^5 + 13x^6 + 21x^7 + 34x^8 + \dots$$

What is it?

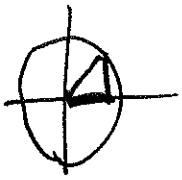
$\tan^{-1}(x)$?

$$\frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + x^8 - x^{10} + \cdots$$

$$\tan^{-1}(x) = C + x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \frac{x^9}{9} - \cdots$$

plug in $x=0 \longrightarrow C=0.$

$$\tan^{-1}(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \frac{x^9}{9} - \cdots$$



$$= \tan^{-1}(1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} = \pi/4$$

$$\pi = 4 - \frac{4}{3} + \frac{4}{5} - \frac{4}{7} + \frac{4}{9} - \frac{4}{13} + \frac{4}{13} - \cdots$$

very slow formula for π!

$\cos(x) + i\sin(x)$

$=$

$$\left(1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots\right) + \cancel{i\left(1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} - \cdots\right)}$$

$$\times\, i\left(x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots\right)$$

$\overline{\text{or}}$

$$= 1 + ix - \frac{x^2}{2!} - \frac{i}{3!}x^3 + \frac{1}{4!}x^4 + \frac{i}{5!}x^5 - \frac{1}{6!}x^6 - \frac{i}{7!}x^7 + \cdots$$

$$= 1 + (ix) + \frac{(ix)^2}{2!} + \frac{(ix)^3}{3!} + \frac{(ix)^4}{4!} + \frac{(ix)^5}{5!} + \frac{(ix)^6}{6!} + \frac{(ix)^7}{7!}$$

$$= e^{ix}$$

$$\boxed{e^{ix} = \cos x + i\sin x}$$

$$f(x) = 1 + x + 2x^2 + 3x^3 + 5x^4 + 8x^5 + 13x^6 + 21x^7 + \cdots$$

"generating function of Fibonacci numbers"

$$x f(x) = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + 13x^7 + 21x^8 + \cdots$$

$$f(x) + x f(x) = 1 + 2x + 3x^2 + 5x^3 + 8x^4 + 13x^5 + 21x^6 + \cdots$$

$$= \frac{f(x) - 1}{x}$$

$$f(x) + x f(x) = \frac{f(x) - 1}{x}$$

$$x f(x) + x^2 f(x) = f(x) - 1$$

$$1 = (1 - x - x^2) f(x)$$

$$\boxed{f(x) = \frac{1}{1 - x - x^2}}$$

"generating function for Fibonacci numbers"

Warning! Those series don't converge for all x values.

<u>ex</u>

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + x^5 + \dots$$

This gives a good approximation of f only in the range where the series converges!

converges for $-1 < x < 1$.

What about

$$\cancel{\ln(x)} = \ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \frac{x^6}{6} + \dots$$

Ratio test:

If $a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + \cdots$

is an infinite series and

$$\lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right|$$ exists and is less than 1,

then the series converges.

$$x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \frac{x^6}{6} + \cdots$$ for what values of x does this converge?

<u>use ratio:</u>

$$a_n = (-1)^{n+1}\frac{x^n}{n}$$

$$\lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right| = \left|\frac{(-1)^{n+2}\frac{x^{n+1}}{n+1}}{(-1)^{n+1}\frac{x^n}{n}}\right| = \frac{n}{n+1}|x|.$$

$1 - \frac{1}{n+1}$

$$= \lim_{n\to\infty}\frac{n}{n+1}|x| = |x|.$$

So $|x| < 1$ it converges.

One more use for Taylor series.

Suppose you wanted to solve a differential equation. Often (usually!) you can't really solve for $f(x)$ exactly. But you <u>can</u> find a Taylor series:

$$y'' - x^2 y = e^x \quad (\text{find } y(x))$$

Easier example: $y' = 2y$ (you know the answer: e^{2x})

$y(0) = 1$

Suppose $y = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + \cdots$

$$y' = a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + 5a_5 x^4 + \cdots$$

$$2y = 2a_0 + 2a_1 x + 2a_2 x^2 + 2a_3 x^3 + 2a_4 x^4 + \cdots$$

$y(0) = 1 \rightsquigarrow a_0 = 1$

$a_1 = 2a_0$, so $a_1 = 2$.

$2a_2 = 2a_1$, so $a_2 = 2$

$3a_3 = 2a_2$, so $a_3 = 4/3$

$4a_4 = 2a_3$, so $a_4 = 2/3$

$5a_5 = 2a_4$, so $a_5 = 4/15$

$a_0 = 1$

$a_1 = 2$

$a_2 = 2$

$a_3 = 4/3$

$a_4 = 2/3$

$a_5 = 4/15$

$$\rightsquigarrow \quad y = 1 + 2x + 2x^2 + \tfrac{4}{3}x^3 + \tfrac{2}{3}x^4 + \tfrac{4}{15}x^5 + \cdots$$

(Taylor for e^{2x})

Recap: Optimization.

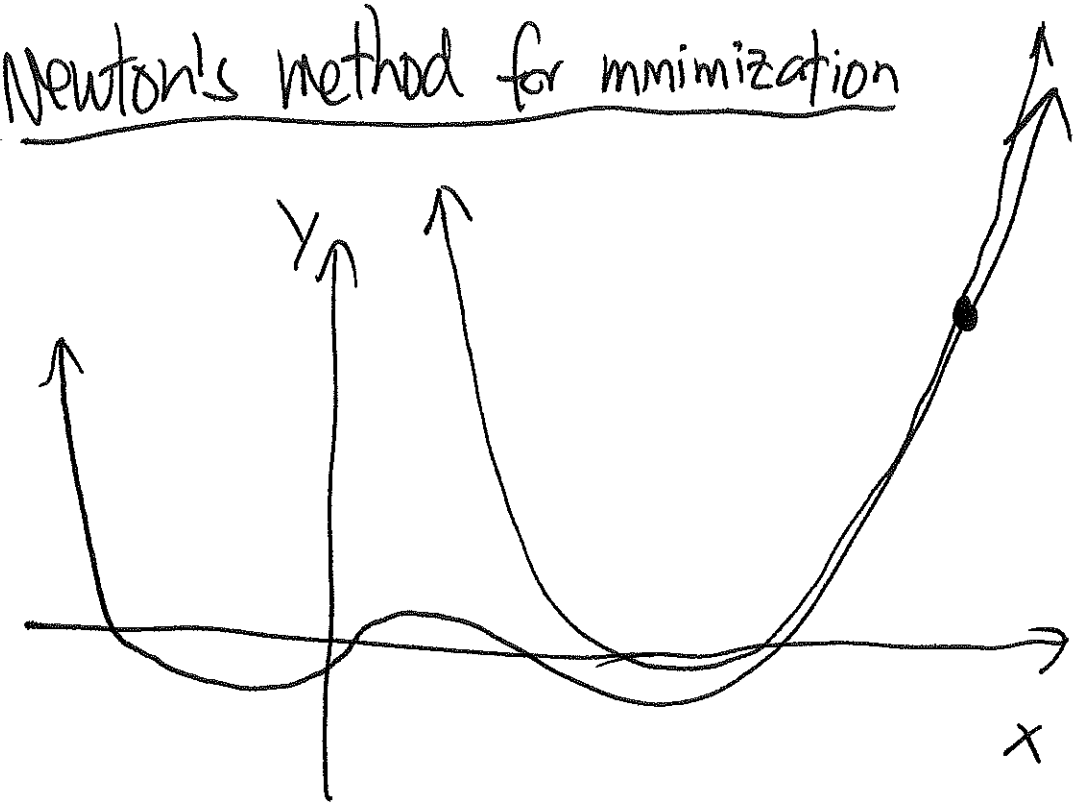
1) Critical pts, max/min on boundary
   (find max/min of easy function on a region)
2) Lagrange multipliers
   (max/min a easy function with a constraint)

3) Linear programming
   (max/min of linear function with many linear constraints: there's an algorithm)
   simplex method
4) Newton's method (for roots)
   (for max/min)

   (complicated functions: decimal approx of max/min without finding it exactly)

5) Gradient descent: solves similar problems to Newton's method.

Newton's method for minimization



To find minimum of $f(x)$:

1) Make an initial guess x_0

2) Find parabola $g(x)$ through $(x_0, f(x_0))$

that has $f(x_0) = g(x_0)$, $f'(x_0) = g'(x_0)$, $f''(x_0) = g''(x_0)$

$$g(x) = f(x_0) + f'(x_0)(x - x_0) + \frac{f''(x_0)}{2}(x - x_0)^2$$

Guess: minimum of f is near minimum of g:

To find minimum of $g(x)$:

$$g'(x) = f'(x_0) + f''(x_0)(x - x_0) = 0.$$

$$x - x_0 = -\frac{f'(x_0)}{f''(x_0)}$$

$$x = x_0 - \frac{f'(x_0)}{f''(x_0)}$$

our next guess for minimum!

$$\boxed{x_{n+1} = x_n - \frac{f'(x_n)}{f''(x_n)}}$$

this is the same as Newton's method for a root of f'!

(probably finds a local minimum only)

To find absolute: find all local minimal by trying different x_0, then compare them.

What about optimizing functions of two (or more) variables?

<u>Newton's method for optimization:</u>

Given $f(x,y)$:

want a point (x,y) so $f_x(x,y)=f_y(x,y)=0$

1) Make a guess (x_0,y_0)

2) Find a paraboloid

$$g(x,y)=ax^2+bxy+cy^2+dx+ey+f$$

that has maximum to $f(x,y)$ at (x_0,y_0):

$$g(x_0,y_0)=f(x_0,y_0) \qquad g_{xx}=f_{xx}$$

$$g_x(x_0,y_0)=f_x(x_0,y_0) \qquad g_{xy}=f_{xy}$$

$$g_y(x_0,y_0)=f_y(x_0,y_0) \qquad g_{yy}=f_{yy}$$

~~"osculati~~ "Osculating paraboloid"

3) Take (x_1,y_1) to be minimum, and iterate

Gradient descent.

To find minimum of $f(x,y)$.

1) Make an initial guess (x_0, y_0)

2) Then move in direction of fastest decrease, which is

$$-\nabla f(x_0, y_0).$$

γ_n = step size: how far do you in that direction?

$$(x_{n+1}, y_{n+1}) = (x_n, y_n) - \gamma_n \nabla f(x_n, y_n)$$

If γ_n is small, you'll frequently update direction, but you'll have to compute gradient many times!

Picking correct γ_n is tricky.

Dynamical systems & chaos

Consider the function

$$f(x) = r \cdot x \cdot (1-x)$$ where r is a parameter.

What happens when we start iterating?

$$x_0$$
$$f(x_0)$$
$$f(f(x_0))$$
$$f(f(f(x_0)))$$
$$f(f(f(f(x_0))))$$
$$\cdots ?$$

We saw that if you do

$$\cos(\cos(\cos(\cos(\cos(\cos(\cos(1)))))))$$

it got closer and closer to some specific number. Why?

Try some r-values:

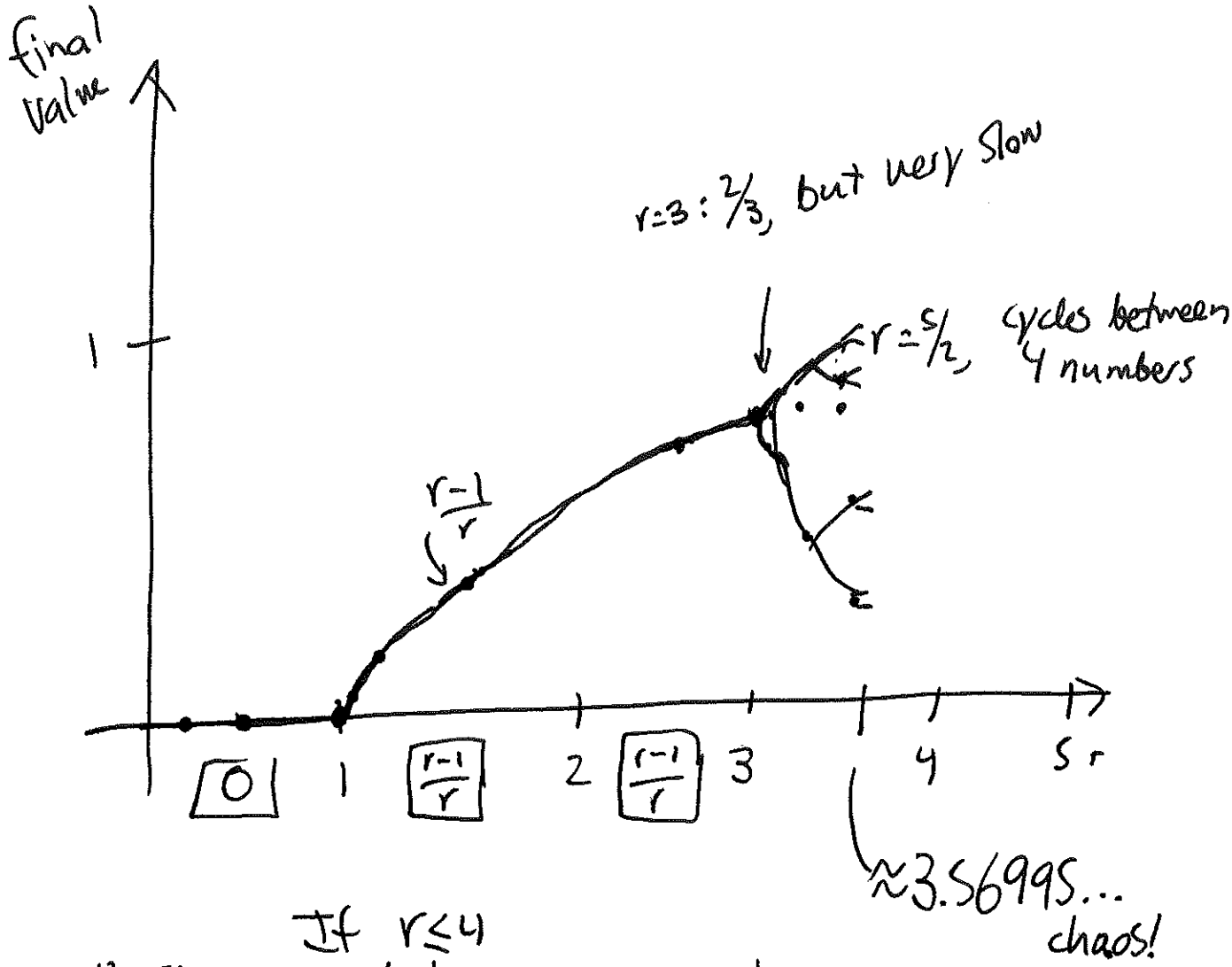
$r = 1/2$ || $r = 3/2$ || $r = 7/2$ || $r = 4.$

Start with $x_0 = 0.1$. $f(x) = rx(1-x)$

Compute $f(f(f(f(f\cdots(x_0)))))$

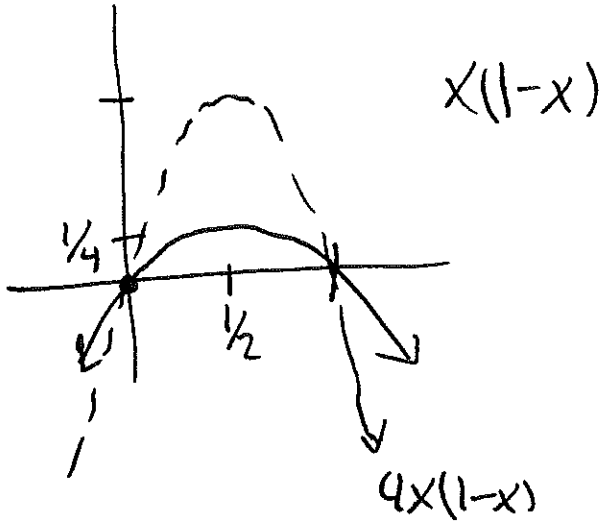
and see what happens.

Can you explain why?



If $r \leq 4$

If x_0 is between 0 and 1, all x's will be:



For $0<r<2$ it converges to a point where $f(x)=x$

$$x = rx(1-x)$$

$$1 = r(1-x) = r - rx$$

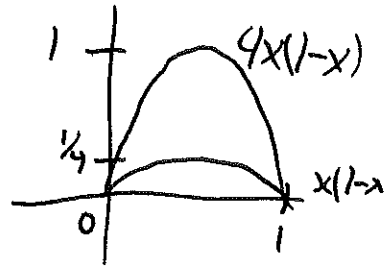
$$rx = r-1$$

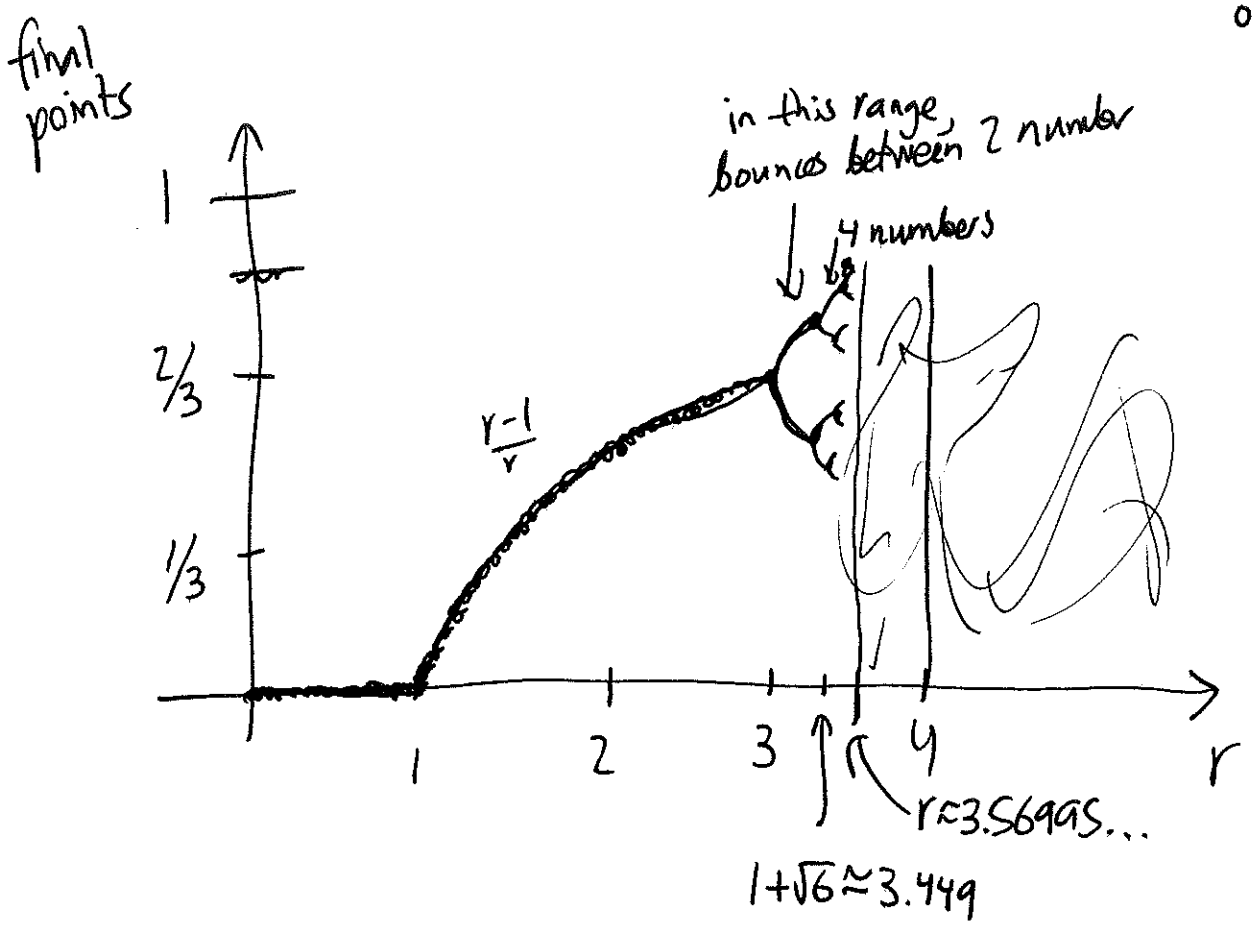
$$x = \frac{r-1}{r}$$

Today: More dynamical systems

$0 < r < 4$ and $x_0 \in [0,1]$

$f(x) = rx(1-x)$ "logistic map"





Past $r = 3.5699s\ldots$ the map devolves into chaos: typically it doesn't repeat any trajectory at all.

There a handful of special r values where not chaotic: $r = 1+\sqrt{8}$: $\rightarrow$ period 3 cycle.

Warm-up

$f(x) = \frac{1}{2}x(1-x)$

Suppose $r = 1/2$, $x_0 = 1/2$.

$\underbrace{f(f(f(f(f(f(x)))))}_{n \text{ times}}$

Can you prove $\lim_{n\to\infty} f^n(x_0) = 0$? "$n^{th}$ iterate"

(Hint: use calculus theorems about limits)

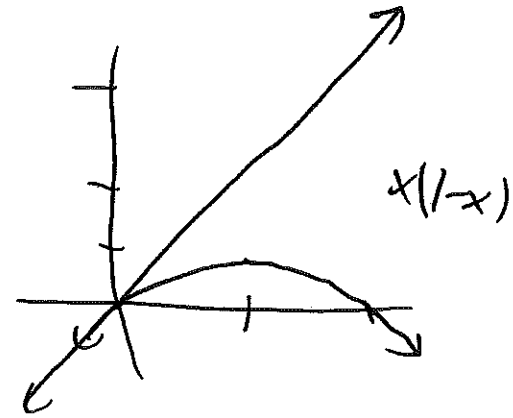
$r = 3$

Suppose $r = 3/2$. $x_0 = 1/2$.

Can you prove $\lim_{n\to\infty} f^n(x_0) = \frac{r-1}{r} = \frac{1}{3}$?

If r is in $[3, 1+\sqrt{6}]$: what are the repeating values?

Pf. for $r = 1/2$



$$x_{n+1} = f(x_n) = \frac{1}{2} x_n (1 - x_n)$$

$$\lim_{n \to \infty} x_n = 0.$$

$$x_{n+1} = \frac{1}{2} x_n (1 - x_n) = \frac{1}{2} x_n - \frac{1}{2} x_n^2 \leq \frac{1}{2} x_n$$

so $x_1 \leq \frac{1}{2} x_0$

$x_2 \leq \frac{1}{2} x_1 \leq \frac{1}{4} x_0$

$\cdots$

$\cancel{x_{n+1}}$ $\boxed{x_n \leq \frac{1}{2^n} x_0}$

Since

Let $y_n = \frac{1}{2^n} x_0$

$z_n = 0$

$f^n(x_0)$

$$z_n \leq x_n \leq y_n$$

$$\begin{array}{ccc} \downarrow & \downarrow & \downarrow \\ 0 & 0 & 0 \end{array}$$

by sandwich thm.

This works for $0 < r < 1$

What about $r=1$?

$x_0 = 1/2.$

$f(x) = x(1-x)$

$\lim_{n\to\infty} f^n(x_0) = 0$

$\boxed{\text{Homework!}}$ for me

0.5, 0.25, 0.1875, 0.152343,

0.129135, ...

What about $r = 3/2$?

$$x_{n+1} = \frac{3}{2} x_n (1 - x_n) \qquad x_0 = 1/2$$

Question: $\lim_{n \to \infty} f(x_n) = 1/3$.

Let $e_n = x_n - \frac{1}{3}$.

Try to prove $\lim_{n \to \infty} e_n = 0$.

What is e_{n+1} in terms of e_n?

$$e_{n+1} = x_{n+1} - \frac{1}{3} = \frac{3}{2} x_n (1 - x_n) - \frac{1}{3}$$

$$= \frac{3}{2}\left(e_n + \frac{1}{3}\right)\left(1 - \left(e_n + \frac{1}{3}\right)\right) - \frac{1}{3}$$

$$= \frac{1}{2} e_n - \frac{3}{2} e_n^2$$

goes to $\quad \text{"}\frac{1}{2} e_n (1 - 3e_n)$

this means $x_n < 2/3$

automatic for e_1!

if $e_n < \frac{1}{3}$ then $0 < e_{n+1} < \frac{1}{2} e_n$

use sandwich thm.

For $r=3$:

$$e_{n+1} = -e_n - 3e_n^2$$

$$\Downarrow$$

$$e_{n+2} = e_n - 18e_n^3 - 27e_n^4$$

if $e_n = \frac{1}{100}$

then $e_{n+2} = \frac{1}{100} - \frac{18}{1000000}$

$$e_n \sim \frac{1}{\sqrt{n}}$$

One more thing: what about period 2 pts?

$3 < r < 1+\sqrt{6}$.

How to find the numbers a & b it oscilbates between?

$\searrow$ $ra(1-a)=b$ and $rb(1-b)=a$

two eqns, two variables.

$\downarrow$

$\cancel{r(r(b-1)}$.

$$a = \frac{(r+1) - \sqrt{r^2-2r+3}}{2r}$$

$$b = \frac{(r+1) + \sqrt{r^2-2r+3}}{2r}$$

Julia & Mandlebrot sets

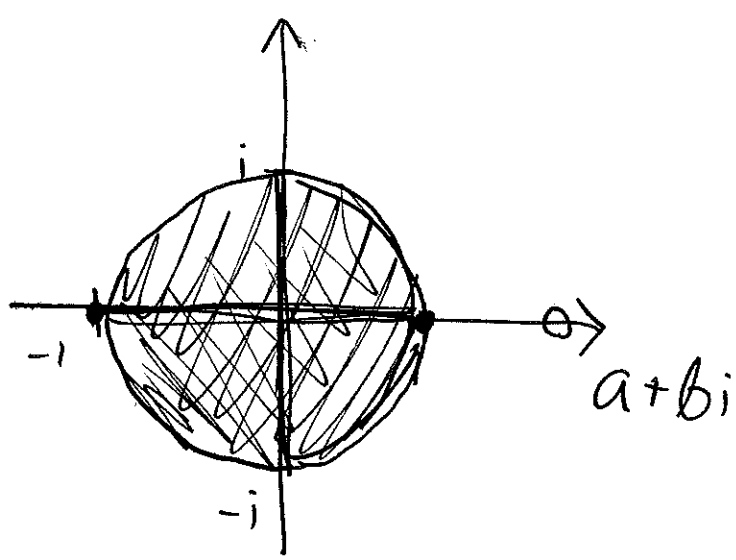
Fix a complex number c. Let $f_c(x) = x^2 + c$

Look at $J(c) = \{ z : f_c^n(z)$ stays bounded, doesn't go to $\infty \}$.

Simplest case $c = 0$.

$f_0(z) = z^2$

$J(0) = \{ z : f_0^n(z)$ stays bounded$\}$



$$(re^{i\theta})^2$$
$$\shortparallel$$
$$r^2 e^{2i\theta}$$
$$\downarrow$$
$$r^4 e^{4i\theta}$$
$$\downarrow$$
$$r^8 e^{8i\theta} \rightarrow$$

Today: More dynamical systems, more fractals.

HW $r=1$ logistic map

$f(x)=x(1-x)$.

call x_n : so $x_{n+1}=x_n(1-x_n)$

Prove $\lim_{n\to\infty} f^n(x_0)=0$.

Let $y_n = 1/x_n$, Let's prove $y_n \to \infty$

$$y_{n+1} = \frac{1}{x_{n+1}} = \frac{1}{x_n(1-x_n)} = \frac{1}{1/y_n(1-1/y_n)}$$

$$= \frac{1}{\frac{1}{y_n} - \frac{1}{y_n^2}} = \frac{1}{\frac{y_n}{y_n^2} - \frac{1}{y_n^2}} = \frac{1}{\frac{y_n-1}{y_n^2}}$$

$0<x_n<1$ so $y_n>1$ so $y_n-1>0$

$$= \frac{y_n^2}{y_n-1} = \frac{y_n^2-1}{y_n-1} + \frac{1}{y_n-1} = y_n+1+\frac{1}{y_n-1}$$

$$> y_n+1$$

So $\boxed{y_{n+1} > y_n + 1}$

this means $y_n \to \infty$, so $x_n \to 0$.

Julia sets.

If c is a complex number, get $f_c(z) = z^2 + c$.

there exists R so $|f^n(z)| < R$ all n.

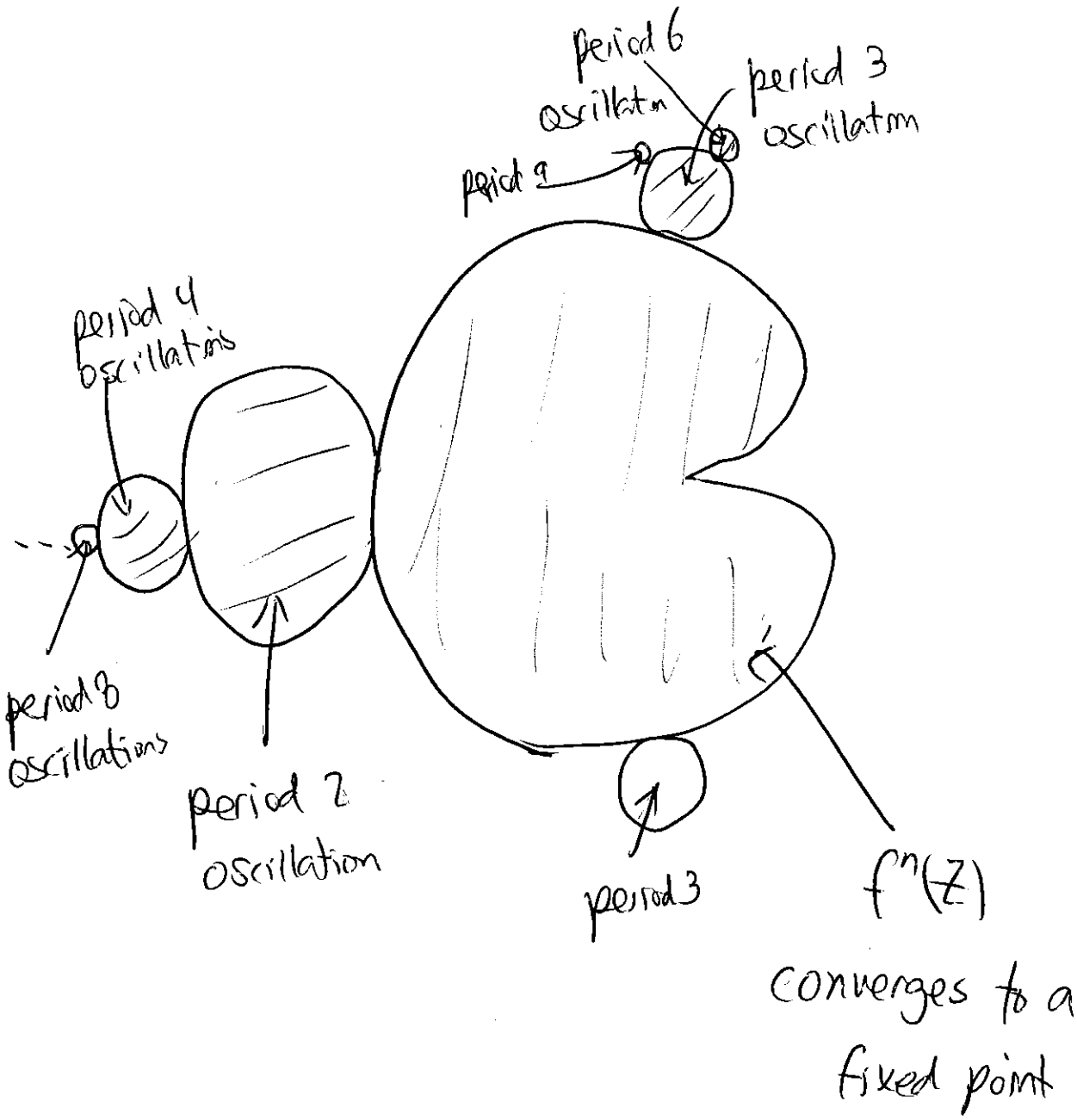
$$J(c) = \{ z : f_c^n(z) \text{ stays bounded as } n \to \infty \}$$

<u>Mandlebrot set</u>

"one piece"

$$M = \{ c : J(c) \text{ is connected} \}$$

$$= \{ c : 0 \text{ has bounded orbit under } f_c \}$$


period 6
oscillation
period 3
oscillation
period 9
period 4
oscillations
period 8
oscillations
period 2
oscillation
period 3
$f^n(z)$
converges to a
fixed point

We've seen some examples of "chaos":

- never goes to ∞, not bounded
- never repeats
- unpredictable: can't guess anything about $f^{1000}(z)$ without calculating it.

  (unlike $r=1/2$ logistic map: then $f^{1000}(z) \approx 0$)
- nearby starting pt have different behavior.

  ("butterfly effect")

How can we define chaos more precisely?

<u>Warm-up</u> How do we define <u>dimension</u>?

(of a fractal, or a non-fractal)

What is dimension of a geometric object?

- How many "independent" directions can we go?

- Number of orthogonal lines/segments you can draw?

Another way:

If we double S in every direction, how much does the size $\mu(S)$ change?

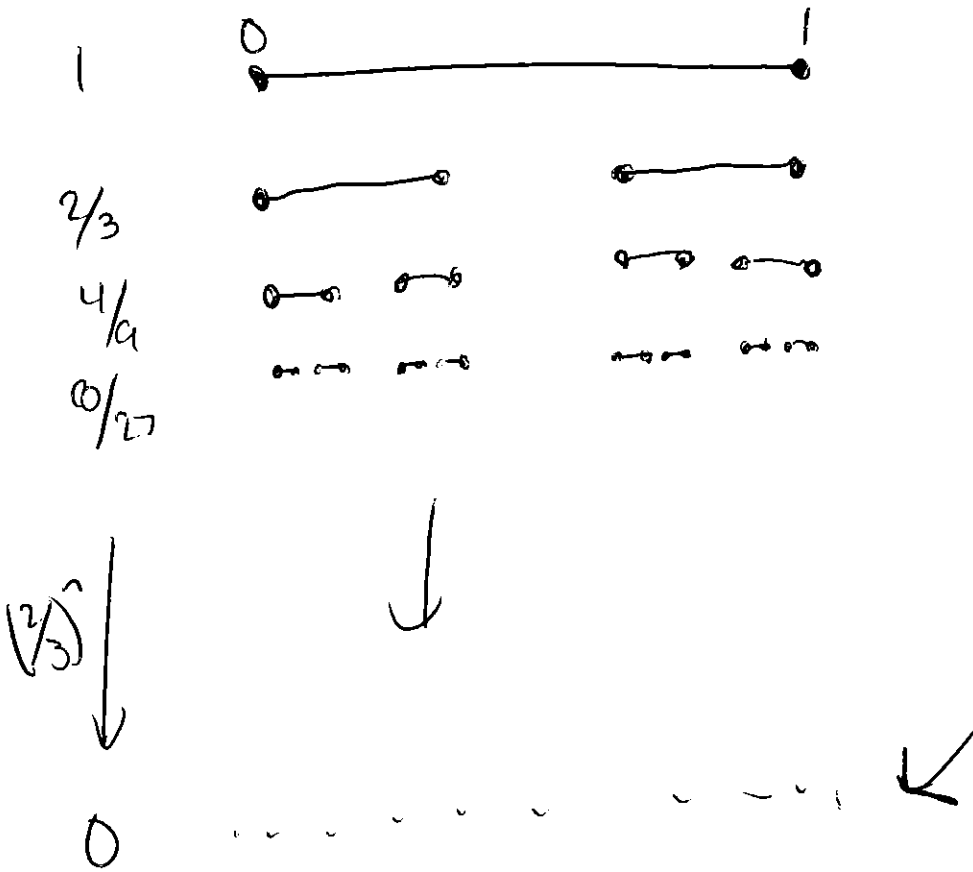
S stretched by factor of 2.

Square: $\mu(2 \cdot S) = \mu(S) \cdot 2^{2}$

Cube: $\mu(2 \cdot S) = \mu(S) \cdot 2^{3}$

the dimension

Cantor set

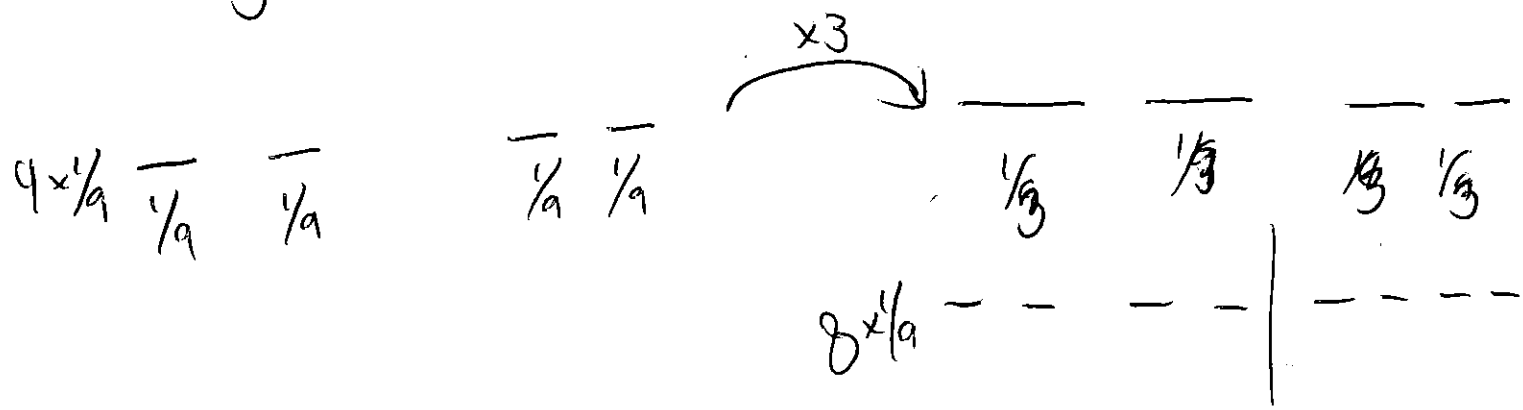


Cantor set is what's left over.

Dimension? If we stretch by a factor of 3, we get:

$3\times$ Cantor set

original



$=2$ Cantor sets!

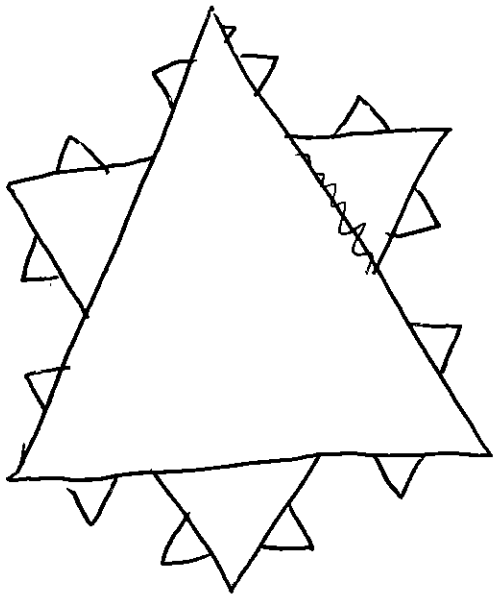
So $\rightarrow \mu(3\cdot S)=\mu(S)\cdot 2$

but $\mu(3\cdot S)=\mu(S)\cdot 3^d$

$$d=\log_3 2\approx 0.630929\ldots$$

"fractal" since not an integer.

Koch snowflake



perimeter of nth iterate: ?

$P_0 = 3$

area enclosed

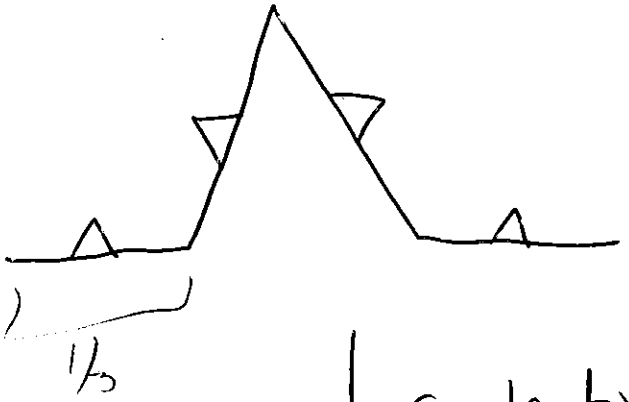
$P_0 = \frac{\sqrt{3}}{4}$

perimeter of $P_n = \left(\frac{4}{3}\right)^n \cdot 3$

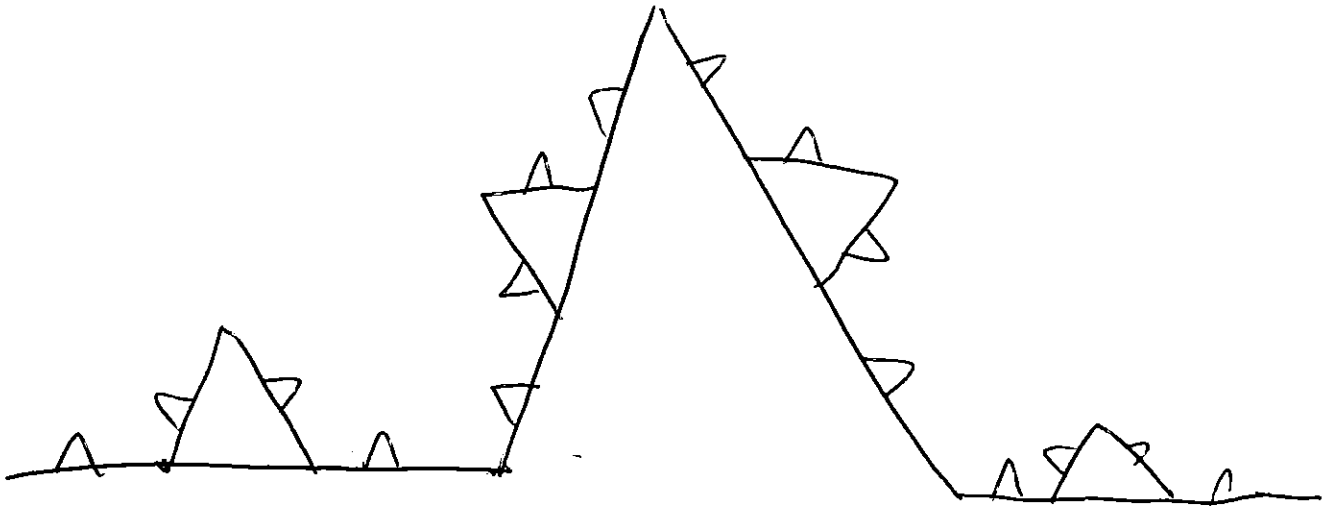
perimeter(snowflake) $= \infty$

area of P_n = stays finite

dimension = 1? 2? other?



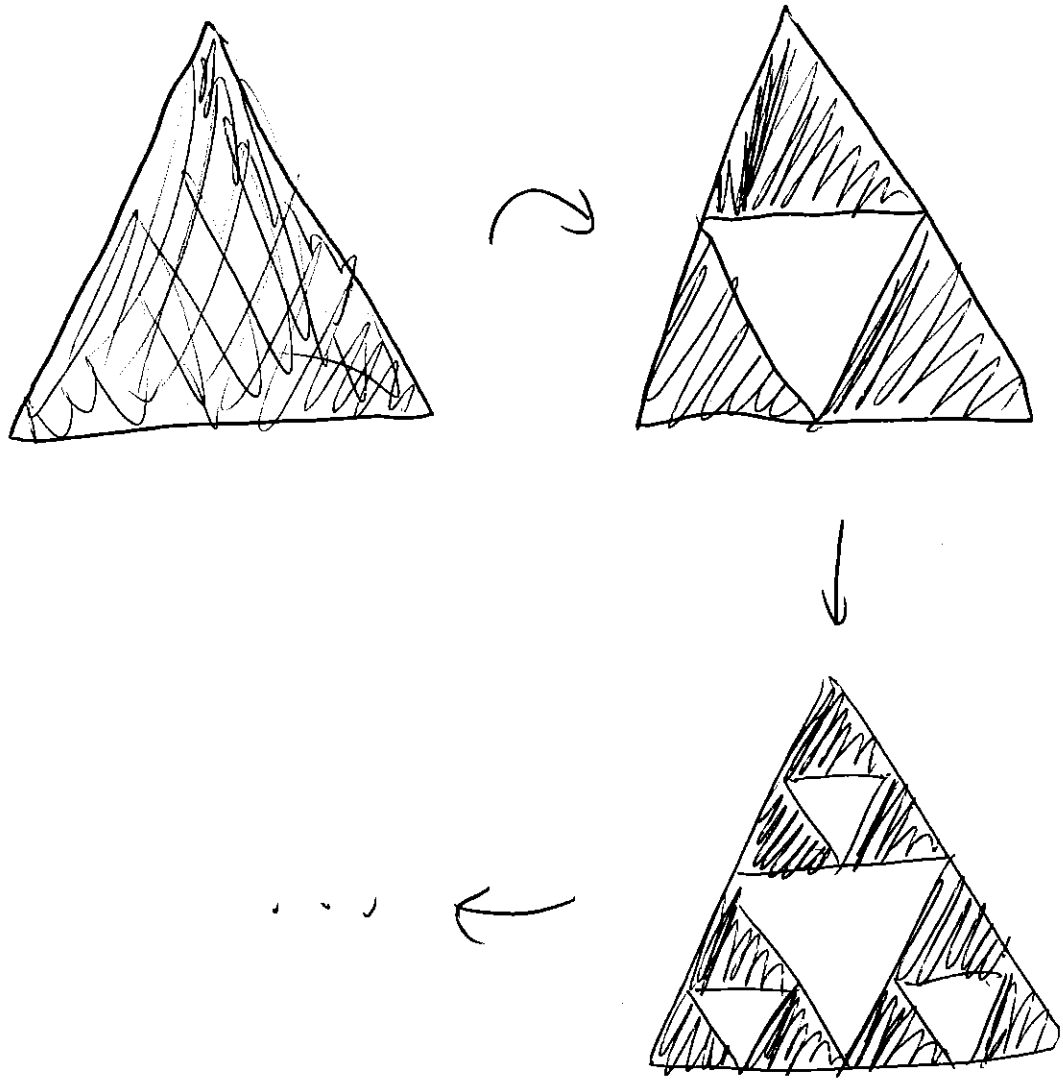
scale by 3



$$\mu(3\cdot S) = 4\,\mu(S)$$

but $\mu(3\cdot S) = \mu(S)\cdot 3^d \Rightarrow d = \log_3 4 = 1.2618\ldots$

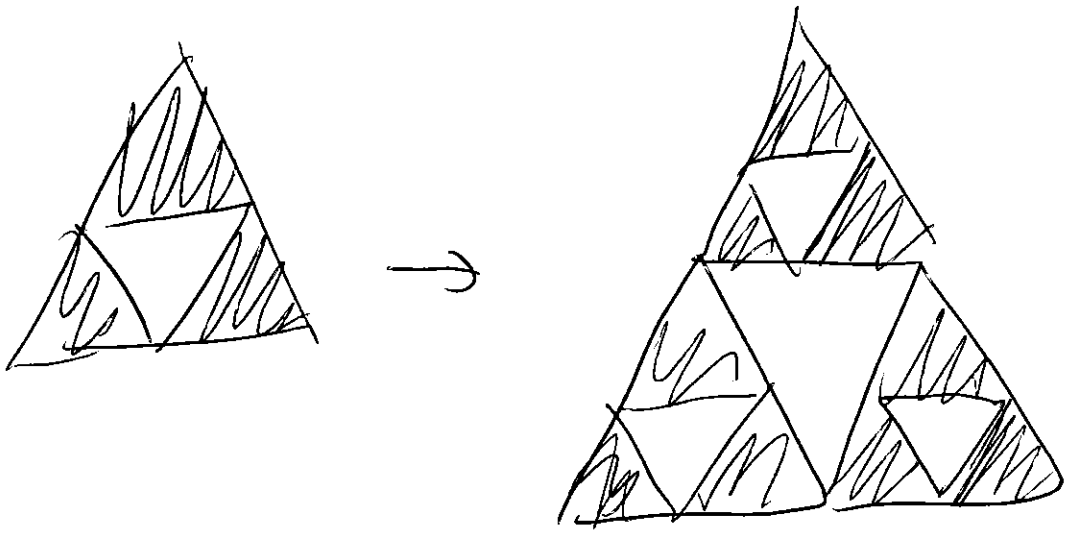
Sierpinski triangle



$\text{area}(P_n) \approx \left(\frac{3}{4}\right)^n$ final area is 0!

Dimension = ?

Stretch by 2 $\rightsquigarrow$ 3 copies of original!



$$\mu(2 \cdot S) = 3\,\mu(S)$$

$$\mu(2 \cdot S) = \mu(S) \cdot 2^d \qquad d = \log_2 3$$

Today: Last day of dynamical systems

+ chaos

Next:
- Inequalities, least-squares regressions
- Abstract algebra (Galois theory...)
- Topology
- Calculus of variations
- Probability

Dimension of fractals.

→ Suppose S is a shape (any dimension)

→ How to define $\dim(S)$?

"size of"

$$\mu(\underbrace{k \cdot S}) = k^{d} \cdot \mu(S)$$

d is the dimension

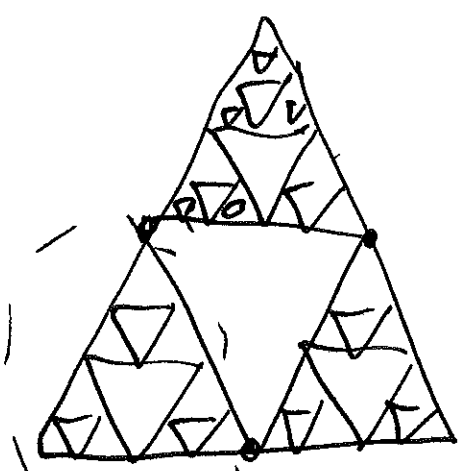
S scaled by factor of k in every direction

$\mu(2 \cdot S) = 3 \cdot \mu(S)$

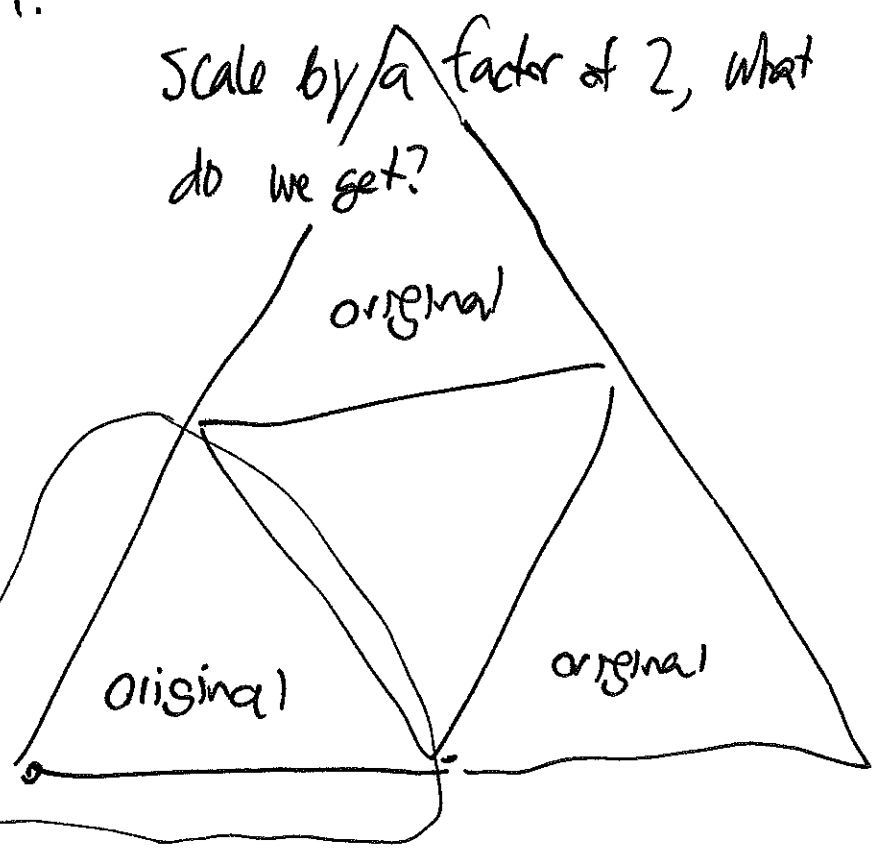
$2^{d} = 3 \rightsquigarrow d = \log_2 3$

$1 < d < 2.$

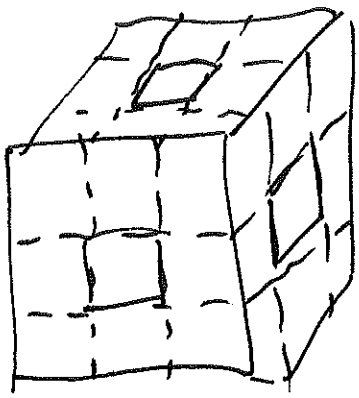
ex Sierpinski gasket:



Scale by a factor of 2, what do we get?



Menger sponge



dimension?

scale by factor of 3:

$20 = 8+4+8$ copies of original.

$$\mu(3\cdot S) = 3^d \cdot \mu(S)$$

$$\parallel$$

$$20 \cdot \mu(S)$$

$$3^d = 20$$

$$d = \log_3 20$$

"Hausdorff dimension"

Hausdorff dimension

Two problems with what we've done:

1) Doesn't work if not perfectly self-similar (e.g. Mandlebrot)

2) What is "μ" anyway? (hard!)

size

The official definition (avoids these problems)

Suppose we have a set S.

"the d-dimensional size of S"

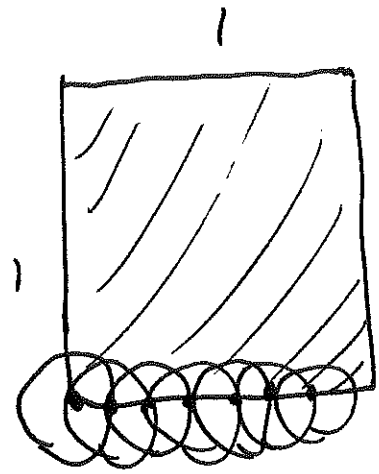
"what would be the size of S if we think of S as being d-dimensional?"

$$\mu_d(S) = \lim_{\epsilon \to 0} \min_{\substack{\text{covers} \\ U_i}} \sum (\text{diam}(U_i))^d$$

where U_i are balls that cover S and have diameter at most ϵ. (they can overlap)

ex

$S =$



square

U_i = {put balls of radius 0.1 in a 0.1×0.1 grid, it will cover S}

here we have 11×11 grid

$\downarrow$

121 balls U_i

$\epsilon = 0.2$

$\cancel{\mu_2(S) = 121}$

$$\sum (\mathrm{diam}(U_i))^d = 121 \cdot (0.2)^d.$$

What about a different ϵ?

Cover U_i could be grid of balls of radius $\epsilon/2$ spaced every $\epsilon/2$. There are $\sim \left(\frac{2}{\epsilon}\right) \cdot \left(\frac{2}{\epsilon}\right) = \frac{4}{\epsilon^2}$ balls.

$$\mu_d(\text{square}) = \lim_{\epsilon \to 0} \sum_{\text{balls } U_i} \text{diam}(U_i)^d$$

$$= \lim_{\epsilon \to 0} \frac{4}{\epsilon^2} \cdot \left(\frac{\epsilon}{2}\right)^d$$

$$= \lim_{\epsilon \to 0} \frac{4}{\epsilon^2} \left(\frac{\epsilon}{2}\right)^d$$

try:

$d=3$

$$\lim_{\epsilon \to 0} \frac{4}{\epsilon^2}\left(\frac{\epsilon}{2}\right)^3 = \lim_{\epsilon \to 0} \frac{1}{2}\epsilon = 0$$

$d=1$

$$\lim_{\epsilon \to 0} \frac{4}{\epsilon^2}\left(\frac{\epsilon}{2}\right)^1 = \lim_{\epsilon \to 0} \frac{2}{\epsilon} = \infty.$$

$$\longrightarrow \mu_d(S) = \begin{cases} 0 & \text{if } d>2 \\ 1 & \text{if } d=2 \\ \infty & \text{if } d<2 \end{cases}$$

Def

If S is any shape, there is a value ~~of~~ d_0 so that

$$\mu_d(S) = 0 \quad \text{if } d > d_0$$

$$\mu_d(S) = \infty \quad \text{if } d < d_0$$

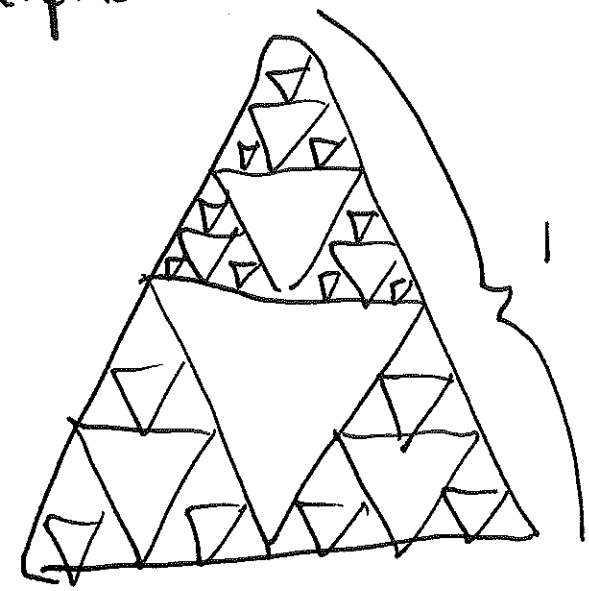
<u>d_0 is the Hausdorff dimension of S.</u>

(looked at pictures of the coast of Britain, pictures of Broccoli, ...)

up next... topological entropy

one to try.

Sierpinski



2 circles of diameter δ

cover a triangle of side δ

		U_i:
$\epsilon = 1/2$	$\rightsquigarrow 3$ tri	$\rightsquigarrow 6$
$\epsilon = 1/4$	$\rightsquigarrow 9$ tri	$\rightsquigarrow 18$
$\epsilon = 1/8$	$\rightsquigarrow 27$ tri	$\rightsquigarrow 54$

$$\mu_d(S) = \sum \operatorname{diam}(U_i)^d$$

$\epsilon = 1/2^n \rightsquigarrow 3^n$ tri $\rightsquigarrow 2 \cdot 3^n$

to cover it with balls of diameter $\frac{1}{2^n} = \epsilon$

~~we need:~~

$$\mu_d(S) = \lim_{\epsilon \to 0} \sum \operatorname{diam}(U_i)^d = \lim_{n \to \infty} \left(\frac{1}{2^n}\right)^d \cdot (2 \cdot 3^n)$$

$$= \lim_{n \to \infty} \left(\frac{3}{2^d}\right)^n \cdot 2 = \begin{cases} 0 & \text{if } d > \log_2 3 \\ \infty & \text{if } d < \log_2 3 \end{cases} \Rightarrow$$

Hausdorff is $\log_2 3$.

Today: Inequalities.

I'm going to follow: notes by Charles Martin "A ~~Power~~ Primer on Inequalities"

Four important inequalities:

also more notes by Kiran Kedlaya

0) $x^2 \geq 0$ for any x

1) Triangle inequality

2) AM / GM inequality

3) Cauchy-Schwarz inequality

4) Jensen's inequality

---

1) Problem: Prove that for any real a, b,

$$\frac{a^2+b^2}{2} \geq ab.$$

Sol:

$$(a-b)^2 \geq 0$$

$$a^2 - 2ab + b^2 \geq 0$$

$$a^2 + b^2 \geq 2ab$$

$$\frac{a^2+b^2}{2} \geq ab \quad \checkmark.$$

Try this:

Prove that $a^2+b^2+c^2 \geq ab+bc+ca$ any a, b, c.

Sol:

$$(a-b)^2+(b-c)^2+(c-a)^2 \geq 0$$

$$2a^2+2b^2+2c^2-2ab-2bc-2ca \geq 0$$

$$a^2+b^2+c^2 \geq ab+bc+ca.$$

AM / GM / HM inequality: arithmetic mean / geometric mean.

Suppose $a_1, \dots, a_n$ are positive.

arithmetic mean: $\dfrac{a_1+a_2+\cdots+a_n}{n}$

geometric mean: $\sqrt[n]{a_1 a_2 \cdots a_n}$

harmonic mean: $\left(\dfrac{\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_n}}{n}\right)^{-1}$

AM/GM $\dfrac{a_1+\cdots+a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n} \geq$

Harmonic mean

You have to paint 1000 ft of fence.

You can paint ~~40~~ it in 4 hours

Your friend can do it in 5 hours.

How long if you work together?

You: $250 \text{ ft/hr} = \frac{1000}{4}$

Friend: $200 \text{ ft/hr} = \frac{1000}{5}$

Together: $450 = 1000\left(\frac{1}{4} + \frac{1}{5}\right)$

Total: $\frac{1000}{1000\left(\frac{1}{4} + \frac{1}{5}\right)} = \left(\frac{1}{4} + \frac{1}{5}\right)^{-1}$

↑

like the harmonic mean.

Proof of ~~AM~~ AM/GM.

Induction. Base case. $n=1$:

$$\frac{a_1}{1} \geq (a_1)^{1/1} \quad \checkmark$$

Base case $n=2$:

$$\frac{a_1+a_2}{2} \geq \sqrt{a_1 a_2}$$

Pf. Let $a=\sqrt{a_1}$, $b=\sqrt{a_2}$. By first inequality we did:

$$\frac{a^2+b^2}{2} \geq ab$$

$$\frac{a_1+a_2}{2} \geq \sqrt{a_1 a_2} \quad \checkmark$$

$\ddots$

Crazy induction:

Let's prove that AMGM with n things implies it with $2n$ things. Assume it works with n things.

Let $a_1, \dots, a_{2n}$ be positive.

n^{th} root

$$\frac{a_1 + \cdots + a_n}{n} \geq (a_1 \cdots a_n)^{1/n}$$

$$\frac{a_{n+1} + \cdots + a_{2n}}{n} \geq (a_{n+1} \cdots a_{2n})^{1/n}$$

by inductive hypothesis.

$$a_1 + \cdots + a_n + a_{n+1} + \cdots + a_{2n} \geq n(a_1 \cdots a_n)^{1/n} + n(a_{n+1} \cdots a_{2n})^{1/n}$$

$$= 2n \frac{(a_1 \cdots a_n)^{1/n} + (a_{n+1} \cdots a_{2n})^{1/n}}{2}$$

$$\geq 2n \sqrt{(a_1 \cdots a_n)^{1/n} (a_{n+1} \cdots a_{2n})^{1/n}}$$

$$= 2n (a_1 \cdots a_{2n})^{1/2n}$$

so

$$\frac{a_1 + \cdots + a_{2n}}{2n} \geq (a_1 \cdots a_{2n})^{1/2n}.$$

This proves AM/GM, but only when n is a power of 2!

Next: Prove that AM/GM for n things implies AM/GM for $n-1$ things!

This will cover all cases:

Suppose we have $a_1, \dots, a_{n-1}$.

Let $b = (a_1 \cdots a_{n-1})^{1/n-1}$

Use AMGM for these n things!

$$\frac{a_1 + a_2 + \cdots + a_{n-1} + b}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_{n-1} b} = b$$

$$a_1 + a_2 + \cdots + a_{n-1} + b \geq nb$$

$$a_1 + \cdots + a_{n-1} \geq (n-1) b$$

$$\frac{a_1 + \cdots + a_{n-1}}{n-1} \geq \overbrace{(a_1 \cdots a_{n-1})^{1/n-1}}^{=b}$$

0 →			1				
1 →		1		1			
2 →	1		2		1		
3 →	1	3		3		1	
4 →	1	4	6		4		1
5 →	1	5	10	10		5	1
6 →	1	6	15	20	15	6	1
	a_1	a_2	...			a_{n+1}	

Question:

If we multiply together everything in n^{th} row, how big could it be?

(Give me an upper bound with no factorials!)

trivia:

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}.$$

"Stirling's formula"

Problem: a, b, c positive, prove

$$\frac{ab}{c} + \frac{bc}{a} + \frac{ca}{b} \geq a + b + c$$

$$\underbrace{\binom{n}{1}\binom{n}{2}\cdots\binom{n}{n-1}}_{\text{product of things in row } n\text{, leaving out the 1's}} \le \left(\frac{\binom{n}{1}+\cdots+\binom{n}{n-1}}{n-1}\right)^{n-1}$$

$$\shortparallel$$

$$\left(\frac{2^n-2}{n-1}\right)^{n-1}$$

Why is sum 2^n?

$\rightarrow$ number of ways to choose a subset of $\{1,\dots,n\}$ is 2^n

$\rightarrow$ $= \binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n} = 2^n.$

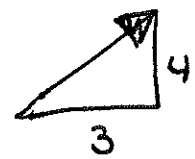
$$2^n = (1+1)^n = \sum_{j=0}^{n} 1^j \cdot 1^{n-j}\binom{n}{j} = \sum_{j=0}^{n}\binom{n}{j}.$$

Cauchy - Schwarz - Bunyakovsky inequality

a) Say $V=(v_1,\dots,v_n)$
$W=(w_1,\dots,w_n)$ are vectors (allowed negative numbers)

$$(v_1w_1+v_2w_2+\cdots+v_nw_n)^2 \le (v_1^2+\cdots+v_n^2)(w_1^2+\cdots+w_n^2)$$

b) If f, g are two functions



$|v|=\sqrt{3^2+4^2}$

$$\int_{-\infty}^{\infty} |fg|\,dx \le \left(\int_{-\infty}^{\infty} |f|^2\,dx\right)^{1/2} \left(\int_{-\infty}^{\infty} |g|^2\,dx\right)^{1/2}$$

(These are actually both cases of the same general theorem! We'll do it when we cover inner product space.)

<u>Pf.</u> of a) at least when $n=2$.

It's saying $(V\cdot W)^2 \le |V|^2|W|^2$.

So we need to prove $\underbrace{|V\cdot W|}_{\text{absolute val}} \le \underbrace{|V|}_{\text{length}}\cdot\underbrace{|W|}_{\text{length}}$

Why is

$|v \cdot w| \leq |v| \cdot |w|$?

Well, $v \cdot w = |v| \cdot |w| \cos \theta$

since $-1 \leq \cos \theta \leq 1$

we get $|v \cdot w| \leq |v| \cdot |w|$ as needed.

Let $a_1, \dots, a_n$ be positive. Prove that

$$(a_1 + \cdots + a_n)\left(\frac{1}{a_1} + \cdots + \frac{1}{a_n}\right) \geq n^2$$

Let $v_i = \sqrt{a_i}$
$w_i = 1/\sqrt{a_i}$

CS:

$$\left(\sqrt{a_1}\frac{1}{\sqrt{a_1}} + \cdots + \sqrt{a_n}\frac{1}{\sqrt{a_n}}\right)^2 \leq \left(\sqrt{a_i}^2 + \cdots \sqrt{a_n}^2\right)\left(\frac{1}{\sqrt{a_1}^2} + \cdots + \frac{1}{\sqrt{a_n}^2}\right)$$

If all a_i are 1, then both sides are equal!

$$n^2 \leq (a_1 + \cdots + a_n)\left(\frac{1}{a_1} + \cdots + \frac{1}{a_n}\right)$$

Consider a Taylor series

$$f(x) = \sum_{k=1}^{\infty} a_k x^k$$

Prove that if $0 \le x < 1$.

$$\sum_{k=1}^{\infty} a_k x^k \le \frac{1}{\sqrt{1-x^2}} \left(\sum_{k=1}^{\infty} a_k^2 \right)^{1/2}$$

Pf. $v_k = a_k$

$w_k = x^k$

$$\frac{1}{1-x^2}$$

CS: $$\left(\sum_{k=0}^{\infty} a_k x^k \right)^2 \le \left(\sum_{k=0}^{\infty} a_k^2 \right) \left(\sum_{k=0}^{\infty} x^{2k} \right)$$

So

$$\sum_{k=0}^{\infty} a_k x^k \le \frac{1}{\sqrt{1-x^2}} \left(\sum_{k=0}^{\infty} a_k^2 \right)^{1/2}$$

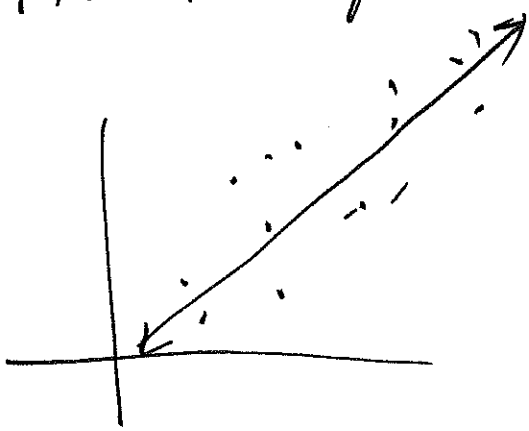
One More Inequality: Jensen's

↳ Introduce abstract algebra.

(Inner product spaces).

A theorem/formula we prove ~~theorem~~ about inner product spaces using only the axioms can be applied to any inner product. The same formula lets us:

→ Find closest point on a plane to a given pt

→ 

Find best fit line/parabola

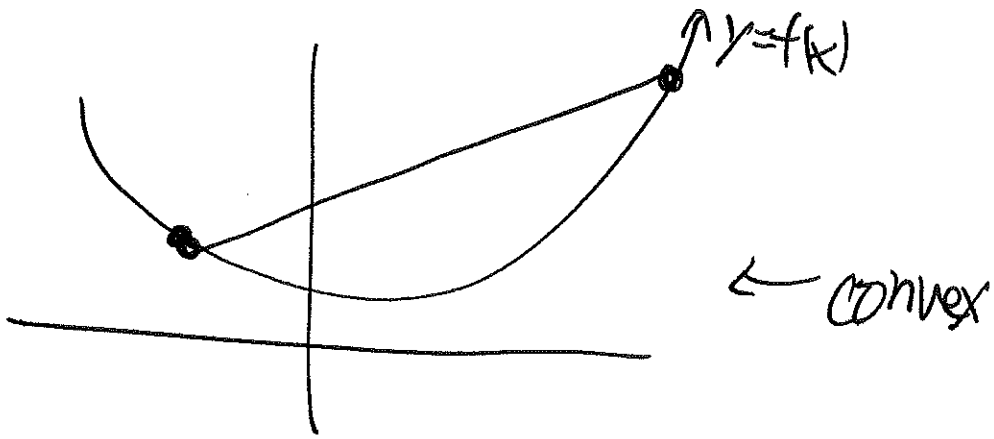
→ Best polynomial approx. to a non-polynomial fct.

→ Fourier series

$$\rightarrow \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Jensen's Inequality

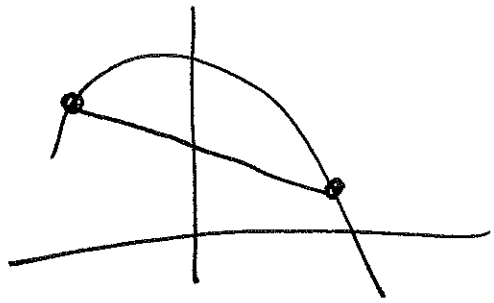
A function ~~a~~ is <u>convex</u> (on an interval.) if a secant ~~line~~ segment always lies above (or on) the graph.



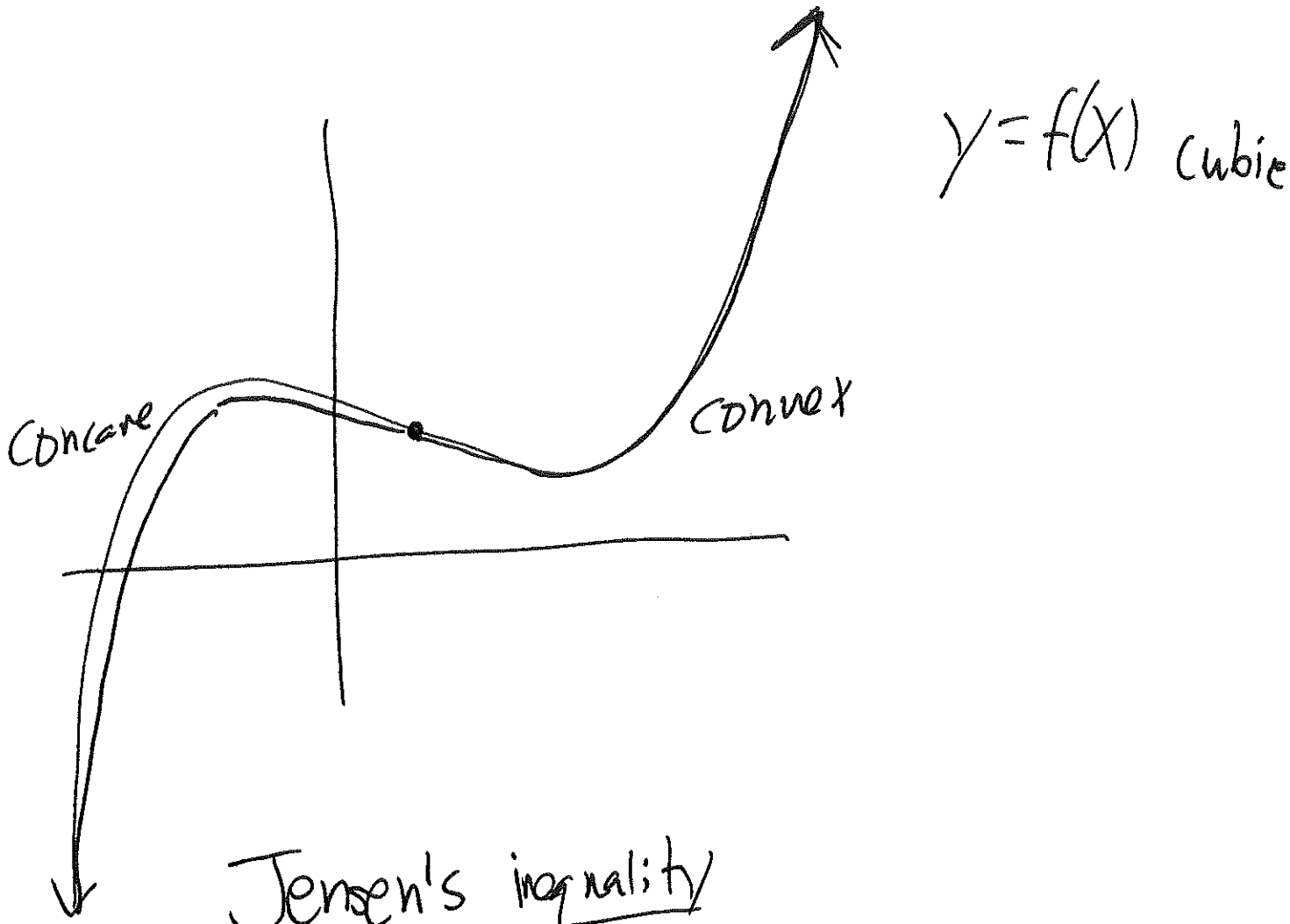
If $f'' \geq 0$, it's convex.

But f can be convex even if not differentiable! $|x|$

A <u>concave</u> fct has secant segments below or on the graph.



f convex $\iff$ $-f$ concave



Jensen's inequality

Version 1: Suppose f convex on interval (a,b).

Then for $x_1, \dots, x_n \in (a,b)$ we have

$$f\left(\frac{x_1 + \cdots + x_n}{n}\right) \leq \frac{f(x_1) + \cdots + f(x_n)}{n}.$$

If f is concave, reverse the inequality!

e.g. $f(x) = x^2$.

Supp $x_1 = 0.3$

$x_2 = 0.7$

$$f\left(\frac{x_1 + x_2}{2}\right) = f(0.5) = 0.25$$

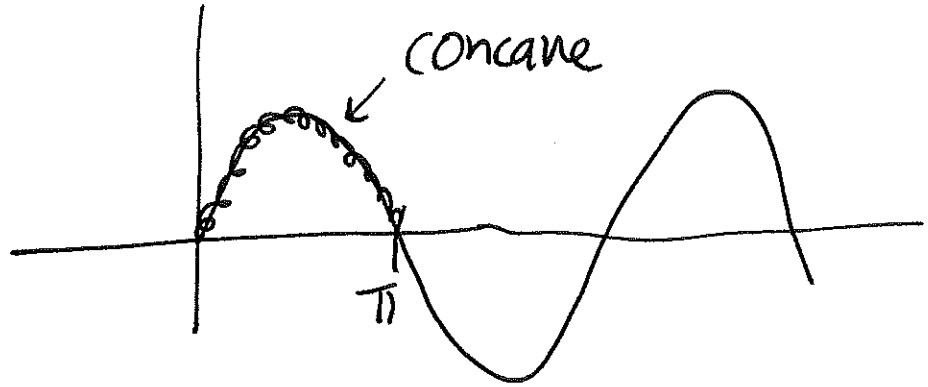
vs $$\frac{f(x_1) + f(x_2)}{2} = \frac{0.09 + 0.49}{2} = 0.29 \checkmark$$

Ex Suppose ABC is a triangle.

Prove

$$\sin(A) + \sin(B) + \sin(C) \leq \frac{3\sqrt{3}}{2}$$

$f(x) = \sin(x)$



Jensen's:

$$\sin\left(\frac{A+B+C}{3}\right) \geq \frac{\sin(A) + \sin(B) + \sin(C)}{3}$$

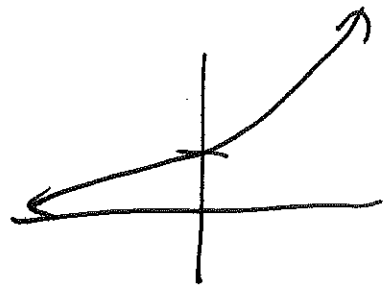
$$\frac{\sin(A) + \sin(B) + \sin(C)}{3} \leq \sin(60^\circ) = \frac{\sqrt{3}}{2}$$

$$\sin(A) + \sin(B) + \sin(C) \leq \frac{3\sqrt{3}}{2}.$$

Suppose $a_1, \dots, a_n$ are positive.

Let $x_i = \ln(a_i) = x_i$

Consider $f(x) = e^x$.



convex.

What does Jensen's ineq tell you?

$$f\left(\frac{x_1 + \cdots + x_n}{n}\right) \leq \frac{f(x_1) + \cdots + f(x_n)}{n}$$

$$e^{(\ln a_1 + \ln a_2 + \cdots + \ln a_n)/n} \leq \frac{e^{\ln a_1} + \cdots + e^{\ln a_n}}{n}$$

$$e^{\ln(a_1 a_2 \cdots a_n)/n} \leq \frac{a_1 + \cdots + a_n}{n}$$

$$(a_1 \cdots a_n)^{1/n} \leq \frac{a_1 + \cdots + a_n}{n}$$ [AM-GM inequality!

Example

Suppose $a, b, c > 0$ and $a+b+c = abc$.

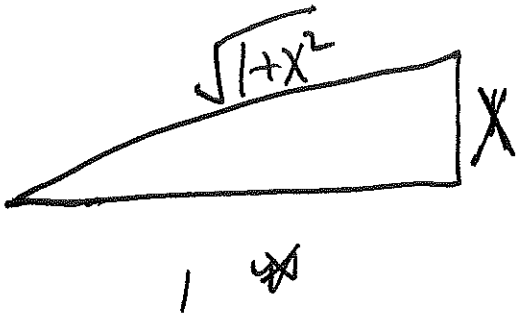
$$\frac{1}{\sqrt{1+a^2}} + \frac{1}{\sqrt{1+b^2}} + \frac{1}{\sqrt{1+c^2}} \leq \frac{3}{2}.$$

Can't simply use Jensen with $f(x) = \frac{1}{\sqrt{1+x^2}}$

because ~~Σ~~

~~Σ~~ left side $\approx \frac{f(a)+f(b)+f(c)}{3}$

right side: $\frac{f(a+b+c)}{3}$ but I don't know $a+b+c$.



Let $a = \tan A$, $b = \tan B$, $c = \tan C$) all between $0, \pi/2$.

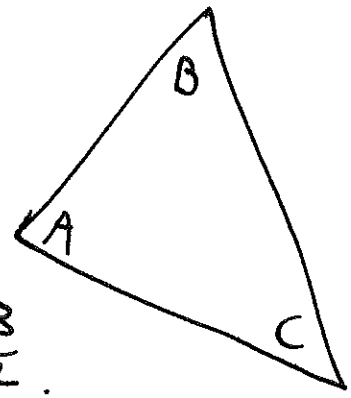
and apply Jensen's inequality to A, B, C instead.

$a+b+c = abc$ tells us what about A, B, C?

$$\tan(A+B+C) = \frac{\overbrace{\tan A + \tan B + \tan C - \tan A \tan B \tan C}^{a+b+c-abc}}{1 - \tan A \tan B - \tan B \tan C - \tan C \tan A} = 0$$

so $\tan(A+B+C) = 0$

and so $A+B+C = \pi$



we want $\cos(A) + \cos(B) + \cos(C) \leq \frac{3}{2}$.

$$\cos(A) + \cos(B) + \cos(C) \leq 3\cos\left(\frac{A+B+C}{3}\right) = 3\cos(60^\circ) = \frac{3}{2}.$$

Vector spaces

Suppose V is a set.

An <u>addition rule</u> on V means a rule assigning a sum $u+v \in V$ for any $u \in V$ and $v \in V$.

A <u>scalar multiplication rule</u> on V is a rule assigning a product $av \in V$ for any $v \in V$ and $a \in \mathbb{R}$.
(tells you how to do scalar × vector)

<u>Def</u> A <u>vector space</u> V is a set with an addition rule and a scalar mult rule that satisfy some axioms:

1) $u+v=v+u$ (addition is commutative)

2) $(u+v)+w=u+(v+w)$ and $(ab)v=a(bv)$

3) There's an identity $0\in V$ so $v+0=0+v=v$.

4) For any v, there's a w so $v+w=0$

5) $1v=v$

6) $a(u+v)=au+av$, $(a+b)v=av+bv$.

<u>Examples:</u>

- regular old vectors of length n (dimension) (for any n) $(\mathbb{R}^n)$
- $m\times n$ matrices are a vector space. $(M^{m\times n})$
- complex numbers $(\mathbb{C})$
- imaginary numbers (bi) incl $0\cdot i$. $(\mathbb{R}i)$
- continuous fcts $f:\mathbb{R}\to\mathbb{R}$ $(C^0(\mathbb{R}))$
- infinite sequences $(a_1, a_2, a_3, a_4, \ldots)$ $(\mathbb{R}^\infty)$

What about:

a) Integers

No: can't multiply by $\frac{1}{2}$

f) Functions with period π

Yes ✓ $f(x+\pi)=f(x)$ any x.

b) Positive real numbers

No: no additive identity 0 / can't mult by -1.

g) Periodic functions

$\sin(x)+\sin(\pi x)$

c) Functions f with $f(1)=1$

No: x^2+1 is one, x^4+1 is one but $x^4+x^2+\underline{\underline{2}}$ has $f(1)=2$.

d) Functions f with $f(1)=0$

Yes ✓

e) Polynomials of any degree

✓

What if we defined addition by $\oplus$

$$(f \oplus g)(x) = f(x) + g(x) - 1.$$

If $f(1)=1$ and $g(1)=1$ then $(f \oplus g)(1) = 1$.

Is functions with $f(1)=1$ a vector space if we use $\oplus$?

Is $a(u \oplus v) = au \oplus av$?

$$a(u+v-1) \stackrel{?}{=} au+av-1$$

$$au+av-a \stackrel{?}{=} au+av-1$$

A vector space is a collection of things V:

1) you can add them

2) you can mult. by (real) scalars

3) (+ ... axioms: associative, distributive, ..)

<u>Examples:</u>

$C^0(\mathbb{R})$ ← continuous functions, domain $\mathbb{R}$

$C^0([a,b])$ ← " domain $[a,b]$

$\mathbb{R}^n$ ← regular vectors of length n

$M^{m \times n}$ ← $m \times n$ matrices

$\mathcal{P}(\mathbb{R})$ ← polynomials whose coefficients are real

A subspace W of a vector space V is just a subset of V closed under addition & scalar mult.

if $w_1, w_2 \in W$ then $w_1 + w_2 \in W$

if $w \in W$ and $a \in \mathbb{R}$, then $aw \in W$.

<u>ex</u>

$\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}$.

subspaces:
- xy-plane $= \{(x, y, 0) : x, y \in \mathbb{R}\}$
- $W = \{(x, x, x) :$ all coords are equal$\}$
- $\{(x, y, z) : x + y + z = 0\}$ is a subspace.

non-subspaces: $\{(x, y, 1) : x, y \in \mathbb{R}\}$

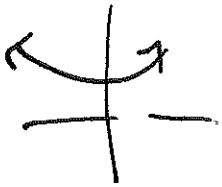
not a subspace: $(2, 3, 1) + (-2, 1, 1) = (0, 4, 2)$.

first ~~quadrant~~ octant: $\{(x, y, z) : x, y, z \geq 0\}$.

$(1, 1, 1) \in W$, but $(-1) \cdot (1, 1, 1)$ isn't.

$V = C^0(\mathbb{R})$.

subspaces?

- polynomials
- linear functions $mx+b$
- even functions 
- functions with period 2π.
- functions with $f(7)=0$

~~Vector~~

Other

Operations you can do to regular vectors in $\mathbb{R}^3$:
(besides addition, scalar mult).

1) dot product

2) cross product

Our definition of a vector space didn't require those operations.

An <u>inner product space</u> is a vector space that also requires something like dot product (satisfying some axioms):

An <u>inner product</u> on a vector space V is a rule that takes two elements of V as input, and outputs a number.

Write it as $\langle v, w \rangle$.

<u>Axioms for inner product:</u>

- $\langle v, v \rangle \geq 0$ for any v
- $\langle v, v \rangle = 0$ only happens if $v = 0$
- $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$
- $\langle \lambda u, v \rangle = \lambda \langle u, v \rangle$ if λ is a scalar
- $\langle u, v \rangle = \langle v, u \rangle$

<u>Example</u>: Dot product of vectors in $\mathbb{R}^n$ is an inner product!

Prove from inner product axioms that

$$\langle u, \lambda v\rangle = \lambda\langle u, v\rangle.$$

Pf. $\langle u, \lambda v\rangle \overset{\text{axiom 5}}{=} \langle \lambda v, u\rangle \overset{\text{axiom 4}}{=} \lambda\langle v, u\rangle \overset{\text{axiom 5}}{=} \lambda\langle u, v\rangle$

The other important inner product space:

for any a, b, $C^0([a, b])$ is an inner product space.

continuous fcts

$$\langle f, g\rangle = \int_a^b f(x)\, g(x)\, dx$$

(this will give us Fourier)

In $\mathbb{R}^n$, the length of a vector is defined to be: $\sqrt{\langle v, v\rangle}$.

e.g. length of $(1,2,3)$ is

$$\sqrt{\underbrace{1\cdot 1 + 2\cdot 2 + 3\cdot 3}_{(1,2,3)\cdot(1,2,3)}} = \sqrt{1^2+2^2+3^2}$$

Def: In any inner product space, the <u>norm</u> of v is $\|v\| = \sqrt{\langle v, v\rangle}$.

What's the norm of x^2 in $C^0([0,1])$?

$$\|x^2\| = \sqrt{\langle x^2, x^2\rangle} = \sqrt{\int_0^1 x^4\,dx} = \sqrt{\left(\frac{x^5}{5}\right)\Big|_0^1}$$

$$= \sqrt{\frac{1}{5}} = \frac{1}{\sqrt{5}}.$$

What's the norm of $2x^2$?

$\hookrightarrow \frac{2}{\sqrt{5}}$

<u>Problem:</u> Suppose $v \in V$ and c is a scalar.

Prove that $\|cv\| = \underset{\text{absolute val.}}{|c|} \cdot \|v\|$

Use only the axioms!

<u>Solutions:</u>

$$\|cv\| = \sqrt{\langle cv, cv\rangle} \overset{\text{axiom 4}}{=} \sqrt{c\langle v, cv\rangle} \overset{\text{proved that}}{=} \sqrt{c^2\langle v, v\rangle}$$

$$= \sqrt{c^2}\sqrt{\langle v, v\rangle} = |c| \cdot \|v\|.$$

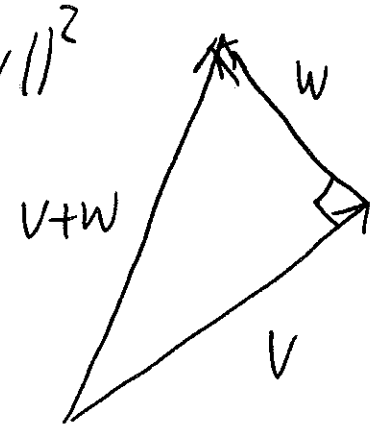
By analogy with regular vectors, we say v & w are <u>orthogonal</u> if $\langle v, w\rangle = 0$.

<u>Ex</u> In $C^0([-1,1])$, x and x^2 are orthogonal:

$$\langle x, x^2\rangle = \int_{-1}^{1} x \cdot x^3 \, dx = 0.$$

<u>Theorem</u> (Pythagorean)

If U is an inner product space with v, w orthogonal, then $\|v+w\|^2 = \|v\|^2 + \|w\|^2$



Pf.

axiom 3

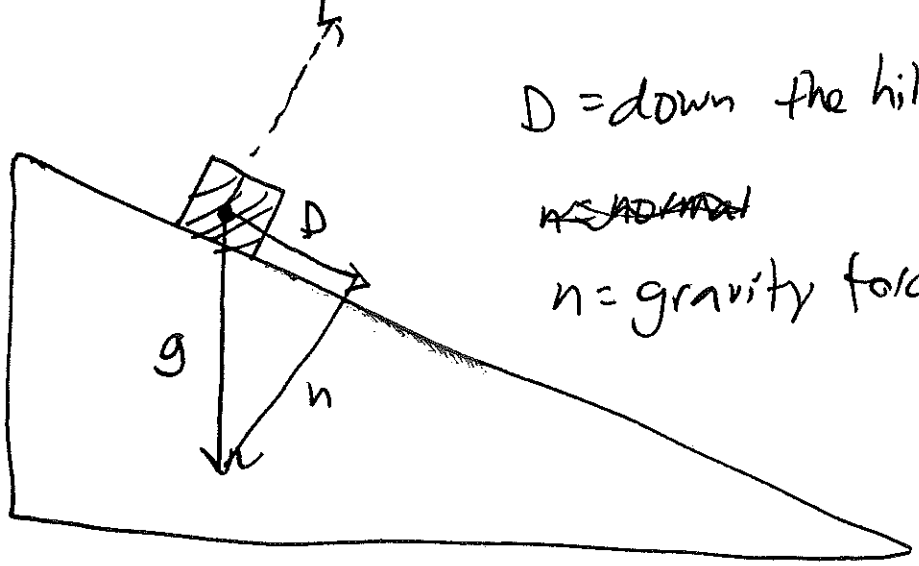
$$\|v+w\|^2 = \langle v+w, v+w\rangle = \langle v, v+w\rangle + \langle w, v+w\rangle$$

$$= \langle v+w, v\rangle + \langle v+w, w\rangle = \langle v,v\rangle + \langle w,v\rangle + \langle v,w\rangle + \langle w,w\rangle$$

$$= \langle v,v\rangle + \langle w,w\rangle + \underbrace{\langle v,w\rangle + \langle v,w\rangle}_{0:\ \text{assuming orthogonal}}$$

$$= \|v\|^2 + \|w\|^2$$

Mass on a ramp:



D = down the hill

~~n = normal~~

n = gravity force into ramp

<u>theorem</u>: Given u, v, you can decompose u as a multiple of v (something in direction of v), plus a vector orthogonal to v.

Recap:

Vector space: a set of things where it makes sense to add, multiply by numbers.
(ex: $\mathbb{R}^n$, functions)

subspace: a subset of a vector space closed under addition and scalar mult.
(ex: $\{(x,x,x)\} \subset \mathbb{R}^3$, functions with period π.

inner product: a rule for combining two vectors to get a number.

ex: In $\mathbb{R}^n$, $\langle v, w \rangle =$ dot product

In $C^0([a,b])$ continuous fcts $\langle f, g \rangle = \int_a^b fg \, dx$

Idea: this integral rule has all the same properties as dot product!

e.g. in $\mathbb{R}^n$ $\langle v, v \rangle \geq 0$

in $C^0([a,b])$ $\langle f, f \rangle = \int_a^b f^2 \, dx \geq 0$

Where we're going.

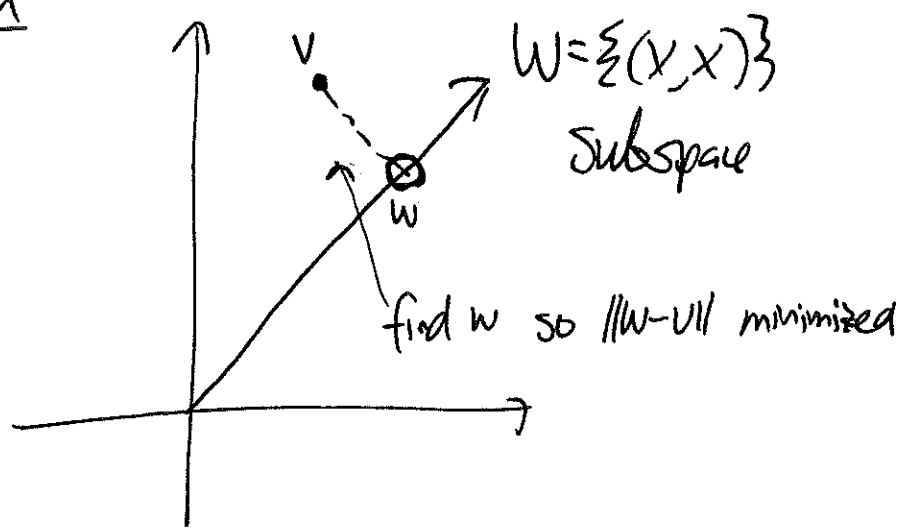
Given a ~~vector~~ inner product space V and a subspace $W \subset V$.

~~Theorem~~ Suppose we have a vector $v \in V$ not in W.

We'll find a formula for the point in W "closest" to v.

$V = \mathbb{R}^2$

ex



ex $V = C^0([-\pi, \pi])$ continuous functions

$W =$ polynomials of degree ≤ 5.

$v \in V$ could be $\cos(x)$. Formula will find the polynomial p of degree ≤ 5 "closest" to $\cos(x)$

"closest" means best approximation:

$$\int_{-\pi}^{\pi} (\cos(x) - p(x))^2 dx \quad \text{is minimized.}$$

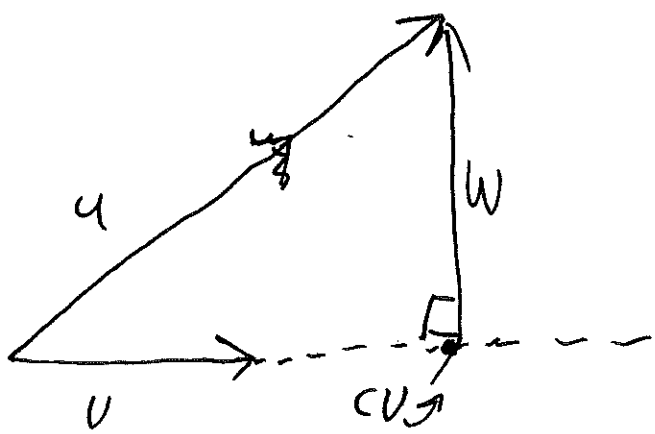
means norm of error

$\cos(x) - p$ is minimized: $\displaystyle\int_a^b (\cos(x) - p(x))^2 dx$

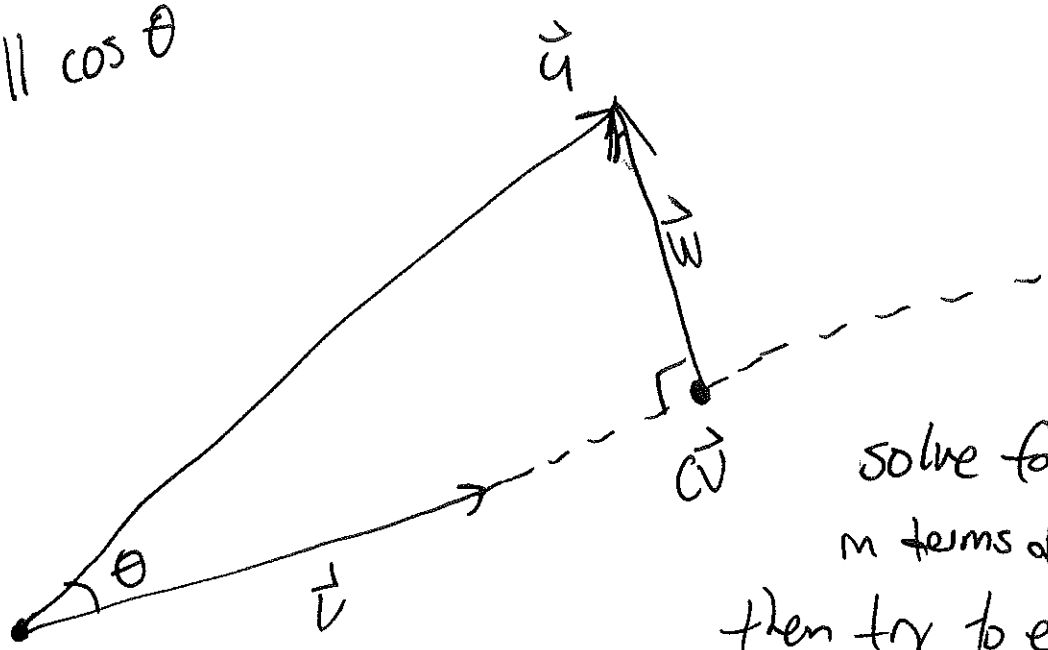
<u>Warm-up:</u> Given vectors u & v, how can we write u as $cv + w$ ← orthogonal to v

c is scalar, so cv parallel to v

[objects sliding down a ramp problem]



$v \cdot w = \|v\| \, \|w\| \cos\theta$



solve for $c, \vec{w}$ in terms of θ. then try to express it using only inner product!

$$\cos\theta = \frac{c\|v\|}{\|u\|}$$

$$\text{so} \quad c = \frac{\|u\|}{\|v\|}\cos\theta = \frac{\|u\|}{\|v\|}\,\frac{u \cdot v}{\|u\|\,\|v\|} = \frac{u \cdot v}{\|v\|^2} = \frac{u \cdot v}{v \cdot v}$$

$$\vec{w} = \vec{u} - c\vec{v}.$$

Thm Suppose u, v are vectors in an inner product space. Then we can always write

$$u = cv + w$$

with c a scalar, and w orthogonal to v ($\langle v, w\rangle = 0$)

Use formula

$$c = \frac{\langle u, v\rangle}{\langle v, v\rangle}, \quad w = u - cv.$$

Pf. We need to check that if we use that c value,

~~then $\langle w, w\rangle =$~~

then $\langle v, w\rangle = 0$.

$$\langle v, w\rangle = \langle v, u - cv\rangle = \cancel{\left\langle v, u - \frac{\langle u, v\rangle}{\langle v, v\rangle} v\right\rangle}$$

now use inner product axioms!

$$= \langle v, u\rangle - \langle v, cv\rangle$$

$$= \langle v, u\rangle - c\langle v, v\rangle = \langle v, u\rangle - \frac{\langle u, v\rangle}{\langle v, v\rangle}\langle v, v\rangle$$

$$= \langle v, u\rangle - \langle u, v\rangle = \langle v, u\rangle - \langle v, u\rangle = 0.$$

Take $V = C^0([0,1])$

Let $v = x^2$ and $u = x$. Write $u = cv + w$, where c is a scaler and w is orthogonal to v.

$$c = \frac{\langle u, v\rangle}{\langle v, v\rangle} = \frac{\int_0^1 x^3\,dx}{\int_0^1 x^4\,dx} = \frac{1/4}{1/5} = \frac{5}{4}$$

$$w = u - cv = x - \frac{5}{4}x^2$$

This w is orthogonal to $v = x^2$!

$$\int_0^1 \overset{v}{x^2}\overset{w}{\left(x - \tfrac{5}{4}x^2\right)}\,dx = 0$$

it works ✓

If $W \subset V$ is a subspace.

a <u>basis</u> for W is a collection of vectors $w_1, \dots, w_r$

such that: 1) Anything in W can be written as a combination.

$$a_1 w_1 + a_2 w_2 + \cdots a_r w_r$$

2) No redundancies: can't write

$w_i =$ (combination of the others).

<u>Ex</u> $V = \mathbb{R}^3$, $W = xy\text{-plane} = \{(x, y, 0)\}$.

Basis for W: $w_1 = (1, 0, 0)$

$w_2 = (0, 1, 0)$

eg. $(7, -3, 0) = 7(1, 0, 0) + (-3)(0, 1, 0)$.

$V = \mathbb{R}^3$, $W = \{(x, y, z) : x + y + z = 0\}$

BASIS: $w_1 = (1, 0, -1)$

$w_2 = (1, -1, 0)$

Check: can we get $(10, -7, -3)$

$$3w_1 + 7w_2$$
$$\shortparallel$$
$$3(1, 0, -1) + 7(1, -1, 0)$$
$$\shortparallel$$
$$(3, 0, -3) + (7, -7, 0)$$
$$\shortparallel$$
$$(10, -7, -3).$$

OR $w_1 = (0, 1, -1)$

$w_2 = (-1, 1, 0)$

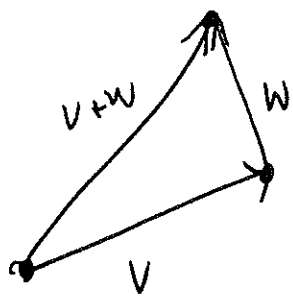
Can we get?

$(10, -7, -3) \leftarrow 3w_1 + (-10)w_2$

Good news: just like orthogonal decomposition formula, many geometric facts about vectors carry over to any inner product space:

1) Pythagorean: if $\langle v,w\rangle = 0$ then

$$\|v+w\|^2 = \|v\|^2 + \|w\|^2$$



2) Cauchy-Schwartz ineq:

For any v,w:

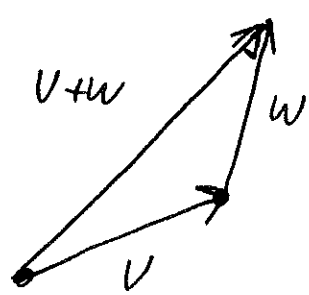
abs val

$$|\langle v,w\rangle| \leq \|v\|\,\|w\|$$

(proof: "boring": try it!)

3) Triangle ineq:

$$\|v\| + \|w\| \geq \|v+w\|$$



Today: The projection formula

vector space: a bunch of things where you can add them, multiply by scalars.

subspace: a subset of a vector space closed under addition, scalar mult.

inner product: a rule like dot product, but for a different vector space

<u>ex</u> $(f,g) = \int_a^b fg\,dx$

basis: A (probably finite) list of vectors that can be combined to make any other vector. (no "redundancy")

<u>Ex</u> $W = \{\text{polynomials of deg} \leq 2\}$ $\quad 1, x, x^2$

or $x^2+1,\ x+1,\ x^2+x$

(many possibilities for basis!)

W = all polynomials, no restriction of degree:

$$1, x, x^2, x^3, x^4, x^5, \ldots \quad *$$

W = 2x2 symmetric matrices $\begin{pmatrix} 1 & 7 \\ 7 & -3 \end{pmatrix}$

dim=3 $\rightarrow$ $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

dim=4 $\rightarrow$ 2x2 matrices: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

eg. $\begin{pmatrix} 2 & 3 \\ 4 & -5 \end{pmatrix} = 2\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 3\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + 4\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + (-5)\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

---

dimension of subspace = # of vectors in a basis

Problem V a vector space with an inner product

W a subspace

$v \in V$ a vector, maybe not in W.

minimize $\|v-w\|$

Key problem $\rightarrow$ How to find vector in W as close as possible to v? ignore this dot

---

Def A basis $v_1, \dots, v_n$ is <u>orthonormal</u>

if 1) $\langle v_i, v_j \rangle = 0$ if $i \neq j$ (basis vectors are orthogonal)
for any i, j

2) $\|v_i\| = 1$ i.e. $\langle v_i, v_i \rangle = 1$. (length 1)

Examples

$V = \mathbb{R}^3$

$W = (xy\text{-plane}) = \{(x, y, 0)\}$.

orthonormal basis for W? $(1,0,0), (0,1,0)$

not unique! another is $(-1,0,0), (0,1,0)$

another is $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right), \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0\right)$

$\sqrt{2}$ stuff is to make length 1.

non-orthonormal basis: $(2,0,0), (0,2,0)$

length not 1!

$V = \mathcal{P}(\mathbb{R})$ polynomials, any degree.

$W =$ polynomials of degree ≤ 1. $\langle f, g \rangle = \int_{-1}^{1} fg \, dx$

orthonormal basis for W?

A basis is $1, x$. Let's check it orthonormal

then adjust it if not.

length not 1!
not orthonormal

$$\langle 1, 1 \rangle = \int_{-1}^{1} 1 \cdot 1 \, dx = 2 \quad \text{so } \|1\| = \sqrt{2}$$

$$\langle 1, x \rangle = \int_{-1}^{1} 1 \cdot x \, dx = 0 \quad \checkmark$$

$$\langle x, x \rangle = \int_{-1}^{1} x^2 \, dx = \frac{2}{3} \quad \|x\| = \sqrt{\frac{2}{3}}$$

To make orthonormal: make lengths $= 1$!

$$\frac{1}{\sqrt{2}}, \sqrt{\frac{3}{2}}\, x \quad \leftarrow \text{orthonormal basis.}$$

$$\int \underset{u}{x} \underset{dv}{\sin x\, dx} = (-x\cos x) - \int (-\cos x)\, dx$$

$$= -x\cos x + \sin x$$

$$\cancel{= -x\cos x - \cos x}$$

$u = x \qquad v = -\cos x$

$du = dx \qquad dv = \sin x\, dx$

$$\int_{-1}^{1} \sqrt{\tfrac{3}{2}}\, x \sin x\, dx = \sqrt{\tfrac{3}{2}} \int_{-1}^{1} x \sin x\, dx$$

$$= \sqrt{\tfrac{3}{2}} \left(-x\cos x + \sin x\right)\Big|_{-1}^{1}$$

$$= \left[\sqrt{\tfrac{3}{2}}\left(-\cos 1 + \sin 1\right)\right] - \left[\sqrt{\tfrac{3}{2}}\left(\cos(-1) + \sin(-1)\right)\right]$$

$$= \sqrt{\tfrac{3}{2}} \cdot \left(-2\cos 1 + 2\sin 1\right)$$

$$= \sqrt{\tfrac{3}{2}} \cdot 2\left(\sin 1 - \cos 1\right) = \sqrt{6}\left(\sin 1 - \cos 1\right)$$

<u>Solution</u> Find orthonormal basis for W (how?)

$e_1, \dots, e_n$.

The vector in W closest to a given v is

$$\underbrace{\langle v, e_1 \rangle}_{\text{a number}} \underbrace{e_1}_{\text{a vector}} + \langle v, e_2 \rangle e_2 + \cdots + \langle v, e_n \rangle e_n$$

Ex. What vector in $\overbrace{\text{xy-plane}}^{W}$ is closest to

$\underbrace{(5, 7, -2)}_{v}$?

Sol. Basis: $\overset{e_1}{\overset{\shortparallel}{(1,0,0)}}, \overset{e_2}{\overset{\shortparallel}{(0,1,0)}}$

$$\langle v, e_1 \rangle e_1 + \langle v, e_2 \rangle e_2 = \big((5,7,-2)\cdot(1,0,0)\big)(1,0,0)$$

$$\big((5,7,-2)\cdot(0,1,0)\big)(0,1,0)$$

$$= 5(1,0,0) + 7(0,1,0) = (5,7,0)$$

$(5, 7, -2)$

Try a different Basis: $\overset{e_1}{\overset{\shortparallel}{\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right)}}$ $\overset{e_2}{\overset{\shortparallel}{\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0\right)}}$

$$(5, 7, -2) \cdot \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right) = \frac{12}{\sqrt{2}}$$

$$(5, 7, -2) \cdot \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0\right) = -\frac{2}{\sqrt{2}}.$$

Answer: $\frac{12}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right) - \frac{2}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0\right)$

$$= (6, 6, 0) - (1, -1, 0) = (5, 7, 0).$$

Find the linear function $y = mx + b$

closest to $y = \sin(x)$, using $\langle f, g \rangle = \int_{-1}^{1} fg\,dx$.

$V =$ all functions

$W =$ polynomials of degree ≤ 1

$v = \sin(x)$

Orthonormal basis for W: $\underset{e_1}{\frac{1}{\sqrt{2}}}, \underset{e_2}{\sqrt{\frac{3}{2}}\,x}$

$\langle v, e_1 \rangle e_1 + \langle v, e_2 \rangle e_2$

$$\left\langle \sin(x), \frac{1}{\sqrt{2}} \right\rangle = \int_{-1}^{1} \frac{1}{\sqrt{2}} \underbrace{\sin(x)}_{\text{odd}}\,dx = 0$$

$$\left\langle \sin(x), \sqrt{\frac{3}{2}}\,x \right\rangle = \int_{-1}^{1} \sqrt{\frac{3}{2}}\,x \cdot \sin x\,dx = \underbrace{\cdots}_{\text{parts}} = \sqrt{6}(\sin 1 - \cos 1)$$

Answer:

$$0 \cdot \frac{1}{\sqrt{2}} + \sqrt{6}(\sin 1 - \cos 1) \cdot \sqrt{\frac{3}{2}}\,x = 3(\sin 1 - \cos 1)\,x$$

But how to find an orthonormal basis?

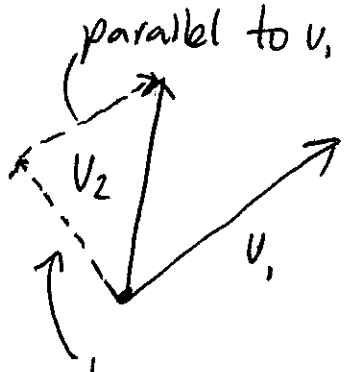
Problem

Find an orthonormal basis for

$$W = \{(x,y,z) : x+y+z=0\} \subset \mathbb{R}^3$$

Hint: start with a non-orthonormal basis and try to fix it.

$$\left.\begin{aligned} v_1 &= (1,-1,0) \\ v_2 &= (1,0,-1) \end{aligned}\right\} \text{ not orthonormal; how to fix it?}$$



take component of v_2 perpendicular to v_1, use that as second basis

Step 1: Make v_1 have length 1

$v_1 = (1, -1, 0)$.

$/\sqrt{2} \rightsquigarrow e_1 = \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0\right)$.

$v_2 = (1, 0, -1)$ not orthogonal to v_1 (or e_1)

We want to make it orthogonal without leaving plane!

$$v_2 = \underbrace{\underbrace{_____}_{\text{scalar}} e_1}_{\text{parallel to } e_1} + \underbrace{f_2}_{\text{perpendicular to } e_1}$$

from old formula $\dfrac{\langle v_2, e_2 \rangle}{\langle e_2, e_2 \rangle} = \dfrac{(1,0,-1)\cdot\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0\right)}{1} = \dfrac{1}{\sqrt{2}}$

so $f_2 = v_2 - ce_1 = (1,0,-1) - \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0\right)$ (perpendicular part)

$= \left(\frac{1}{2}, \frac{1}{2}, -1\right)$

But f_2 not length 1!

To get final answer e_2, normalize f_2:

$$e_2 = \frac{f_2}{\|f_2\|} = \frac{\left(\frac{1}{2}, \frac{1}{2}, -1\right)}{\left\|\left(\frac{1}{2}, \frac{1}{2}, -1\right)\right\|} = \sqrt{\frac{2}{3}}\left(\frac{1}{2}, \frac{1}{2}, -1\right)$$

$$= \left(\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, -\frac{2}{\sqrt{6}}\right)$$

Gram-Schmidt Orthonormalization.

Starts with any basis $v_1, \dots, v_n$

$\downarrow$

Ends with orthonormal basis $e_1, \dots, e_n$

(then use in projection formula!)

1. Fix length of v_1:

$$e_1 = v_1 / \|v_1\|$$

2. Make v_2 orthogonal to v_1

$$f_2 = v_2 - \langle v_2, e_1 \rangle e_1$$

3. Fix length!

$$e_2 = f_2 / \|f_2\|$$

4. Make v_3 perp to v_1, v_2

$$f_3 = v_3 - \langle v_3, e_1 \rangle e_1 - \langle v_3, e_2 \rangle e_2$$

5. Fix length

$$e_3 = f_3 / \|f_3\|.$$

...

More que

More projection formula

Find the point of the plane $x+2y+3z=0$] subspace W

closest to $v=(2,4,-3)$.

Steps.

1) Find a basis (maybe not orthonormal)

2) Make it orthonormal* (Gram-Schmidt process)
e_1, e_2

3) Find closest point: use projection

$$\hat{v} = \langle v, e_1 \rangle e_1 + \langle v, e_2 \rangle e_2$$

Gram-Schmidt

Given $v_1, v_2, \ldots, v_n$ a basis.

Set $e_1 = v_1 / \|v_1\| = v_1 / \sqrt{\langle v_1, v_1 \rangle}$ (make first vector length 1)

$$f_2 = v_2 - \underbrace{\langle v_2, e_1 \rangle e_1}_{\text{part of } v_2 \text{ parallel to } e_1}$$ (make 2nd perp. first)

$e_2 = f_2 / \|f_2\|$ (make 2nd length 1)

$$f_3 = v_3 - \langle v_3, e_1 \rangle e_1 - \langle v_3, e_2 \rangle e_2$$

$e_3 = f_3 / \|f_3\|$

...

Basis: $v_1 = (1, 1, -1)$

$v_2 = (-2, 1, 0)$.

$$e_1 = v_1 / \|v_1\| = \left(1/\sqrt{3},\ 1/\sqrt{3},\ -1/\sqrt{3}\right)$$

$$f_2 = v_2 - \langle v_2, e_1 \rangle e_1$$

$$= (-2, 1, 0) - \left\langle (-2, 1, 0), \left(1/\sqrt{3}, 1/\sqrt{3}, -1/\sqrt{3}\right)\right\rangle \left(1/\sqrt{3}, 1/\sqrt{3}, -1/\sqrt{3}\right)$$

$$= (-2, 1, 0) + 1/\sqrt{3}\left(1/\sqrt{3}, 1/\sqrt{3}, -1/\sqrt{3}\right)$$

$$= (-2, 1, 0) + \left(1/3, 1/3, -1/3\right) = \left(-5/3,\ 4/3,\ -1/3\right)$$

$$e_2 = f_2 / \|f_2\| \qquad \|f_2\| = \sqrt{\left(-5/3\right)^2 + \left(4/3\right)^2 + \left(-1/3\right)^2}$$

$$= \frac{\sqrt{42}}{3}$$

$$= \left(-5/\sqrt{42},\ 4/\sqrt{42},\ -1/\sqrt{42}\right)$$

$v = (2, 4, -3)$

<u>Projection</u>

$\hat{v} = \langle v, e_1 \rangle e_1 + \langle v, e_2 \rangle e_2 = \cdots$

$= \left(\frac{27}{14}, \frac{27}{7}, -\frac{45}{14} \right)$

$= \cancel{(3, 5, 3)}$

Function example

Approximate $\cos(x)$ by a quadratic function on $[-\pi, +\pi]$.

1) Find a basis for quadratic functions: $1, x, x^2$

2) Orthonormalize it

Gram-Schmidt, $\langle f, g \rangle = \int_{-\pi}^{\pi} fg \, dx$

3) $\langle \cos(x), e_1 \rangle e_1 + \langle \cos(x), e_2 \rangle e_2 + \langle \cos(x), e_3 \rangle e_3$

$v_1 = 1 \qquad v_2 = x \qquad v_3 = x^2$

$$e_2 = \frac{\frac{3}{2}\sqrt{\frac{2}{3}}\,x}{\pi^{3/2}}$$

$$= \sqrt{\frac{9/4 \cdot 2/3}{\pi^3}}\,x$$

$$= \sqrt{\frac{3}{2\pi^3}}\,x$$

$$e_1 = v_1 / \|v_1\| \qquad \|v_1\|^2 = \int_{-\pi}^{\pi} 1 \cdot 1\,dx = 2\pi$$

$$\|v_1\| = \sqrt{2\pi}$$

$$e_1 = \frac{1}{\sqrt{2\pi}}$$

$$f_2 = v_2 - \langle v_2, e_1 \rangle e_1 \qquad \langle v_2, e_1 \rangle = \int_{-\pi}^{\pi} x \cdot \frac{1}{\sqrt{2\pi}}\,dx = 0$$

$$e_2 = f_2 / \|f_2\| \qquad \|f_2\|^2 = \int_{-\pi}^{\pi} x^2\,dx = \frac{2\pi^3}{3}$$

so $e_2 = \sqrt{\frac{3}{2\pi^3}}\,x$.

computer says

$$e_3 = -\frac{5/4\,\sqrt{2/5}}{\pi^{5/2}}\left(\pi^2 - 3x^2\right) = \sqrt{\frac{5}{8\pi^5}}\left(3x^2 - \pi^2\right)$$

$$f_3 = v_3 - \langle v_3, e_1 \rangle e_1 - \langle v_3, e_2 \rangle e_2$$

$$\langle v_3, e_1 \rangle = \int_{-\pi}^{\pi} x^2 \frac{1}{\sqrt{2\pi}}\, dx = \frac{1}{\sqrt{2\pi}} \frac{2\pi^3}{3}$$

$$\langle v_3, e_1 \rangle e_1 = \frac{1}{\sqrt{2\pi}} \frac{2\pi^3}{3} \frac{1}{\sqrt{2\pi}} = \frac{\pi^2}{3}$$

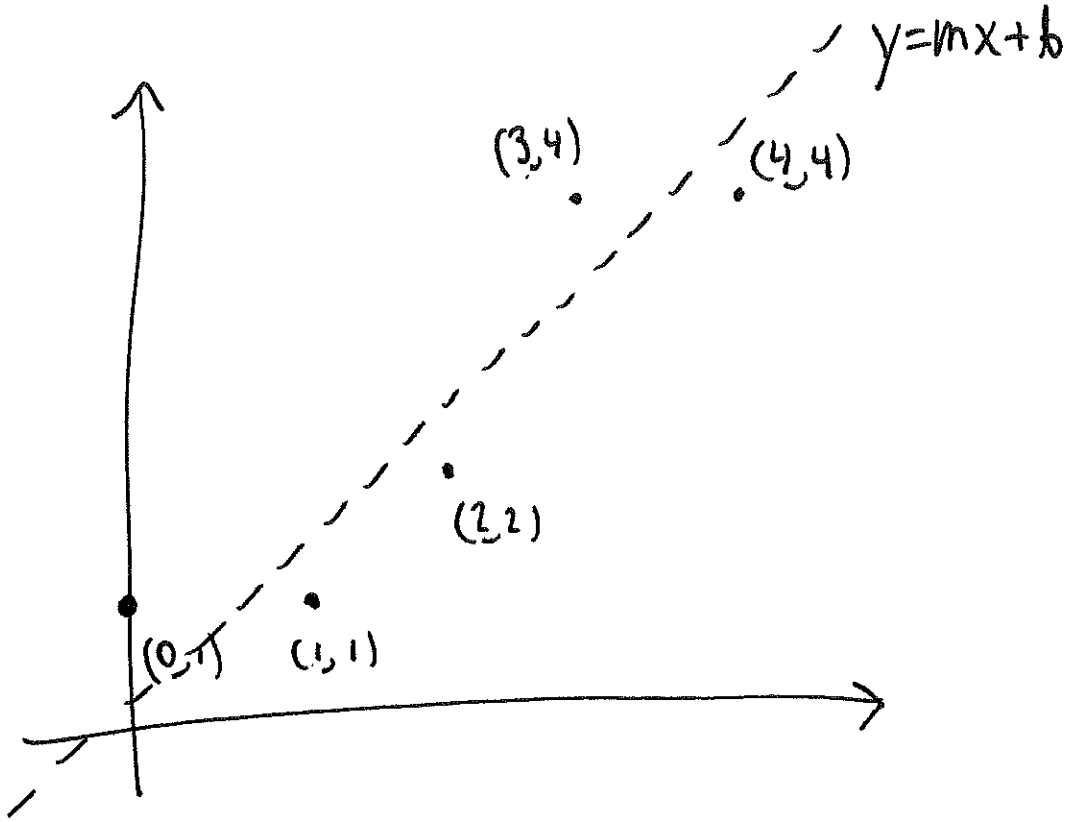
$$\langle v_3, e_2 \rangle = \int_{-\pi}^{\pi} x^2 (\sim x)\, dx = 0$$

$$f_3 = x^2 - \frac{\pi^2}{3}$$

$$\|f_3\|^2 = \int_{-\pi}^{\pi} \left(x^2 - \pi^2/3\right)^2 dx = \dots$$

$$e_3 = f_3 / \|f_3\|$$

Best-fit lines.



Let's solve for m & b to make line go through all points!

$$0m + b = 1$$
$$1m + b = 1$$
$$2m + b = 2$$
$$3m + b = 4$$
$$4m + b = 4$$

this has no solutions!

In matrix form:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 1 \\ 3 & 1 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} m \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 2 \\ 4 \\ 4 \end{pmatrix}$$

x-coords of our pts

all 1's

y-coords of point.

This is an "$Ax=y$" problem: A matrix, y vector, solve for x.

no solutions!

left

$$= \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} m + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} b$$

the set of y for which this equation has a solution is a plane in 5-D space $\mathbb{R}^5$: it's a subspace!

$Ax = y$ had no solutions.

Let's change y to $\hat{y}$, the closest vector for which there <u>is</u> a solution. That solution $\begin{pmatrix} m \\ b \end{pmatrix}$ gives a line.

Take projection of $\begin{pmatrix} 1 \\ 1 \\ 2 \\ 4 \\ 4 \end{pmatrix}$ onto W.

the set of y for which there <u>is</u> a solution.

Basis for W is $\underset{v_1}{\begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}}, \underset{v_2}{\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}}$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 1 \\ 3 & 1 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} m \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$$ have a sol?

for $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$, get $\begin{pmatrix} m \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

$\begin{pmatrix} m \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Want to project $\begin{pmatrix}1\\1\\2\\4\\4\end{pmatrix}$ onto W, which has basis

$$\begin{pmatrix}0\\1\\2\\3\\4\end{pmatrix}, \begin{pmatrix}1\\1\\1\\1\\1\end{pmatrix}$$

$$\text{Proj} = \begin{pmatrix}3/5\\3/2\\12/5\\33/10\\21/5\end{pmatrix}.$$

there is a solution here!

if you change y-coords to those, there is a solution.

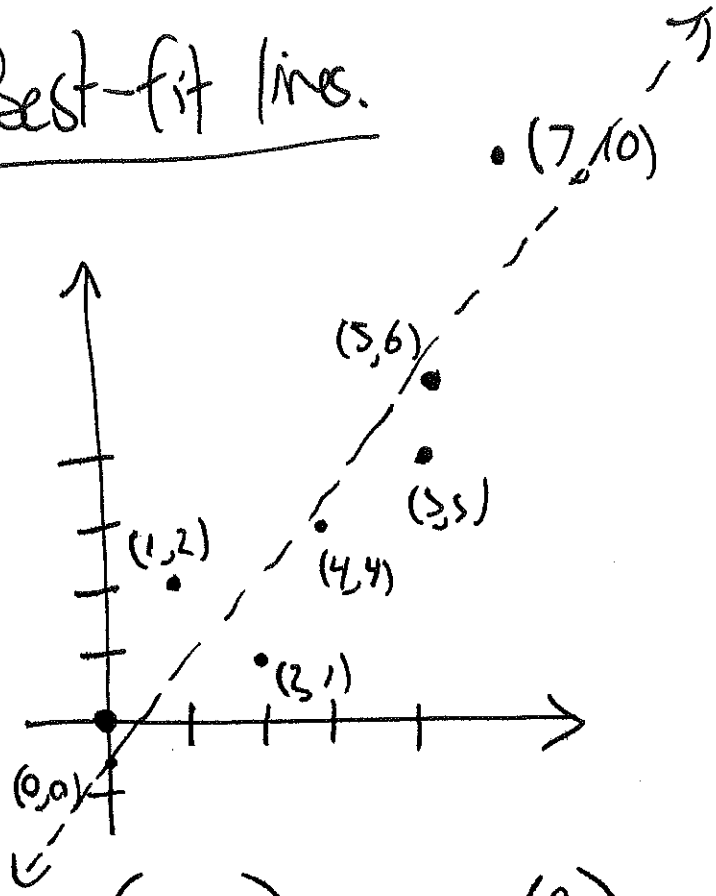
the distance from to $\begin{pmatrix}1\\1\\2\\4\\4\end{pmatrix}$ is

$$\sqrt{\left(\tfrac{3}{5}-1\right)^2+\left(\tfrac{3}{2}-1\right)^2+\left(\tfrac{12}{5}-2\right)^2+\left(\tfrac{33}{10}-4\right)^2+\left(\tfrac{21}{5}-4\right)^2}$$

Today: More of the same + Fourier

(experiment with G-S software).

Best-fit lines.



Strategy: $y = mx + b$

To satisfy all equations:

$0 = m0 + b$ $\quad$ $5 = m5 + b$

$2 = m1 + b$ $\quad$ $6 = m5 + b$

$1 = m2 + b$ $\quad$ $10 = m7 + b$

$4 = m4 + b$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 1 \\ 4 & 1 \\ 5 & 1 \\ 5 & 1 \\ 7 & 1 \end{pmatrix} \begin{pmatrix} m \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 4 \\ 5 \\ 6 \\ 10 \end{pmatrix}$$

"$Ax = y$"

try to find closest thing to this so there is a solution

Use Gram-Schmidt!

$$v_1 = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 4 \\ 5 \\ 5 \\ 7 \end{pmatrix} \qquad v_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \qquad \text{project} \begin{pmatrix} 0 \\ 2 \\ 1 \\ 4 \\ 5 \\ 6 \\ 10 \end{pmatrix}$$

computer says projection is $\begin{pmatrix} -5/11 \\ 223/264 \\ \vdots \\ 2281/264 \end{pmatrix}$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 1 \\ 4 & 1 \\ 5 & 1 \\ 5 & 1 \\ 7 & 1 \end{pmatrix} \begin{pmatrix} m \\ b \end{pmatrix} = \begin{pmatrix} -5/11 \\ 223/264 \\ \vdots \\ 2281/264 \end{pmatrix}$$

this has a solution!

how to find it?

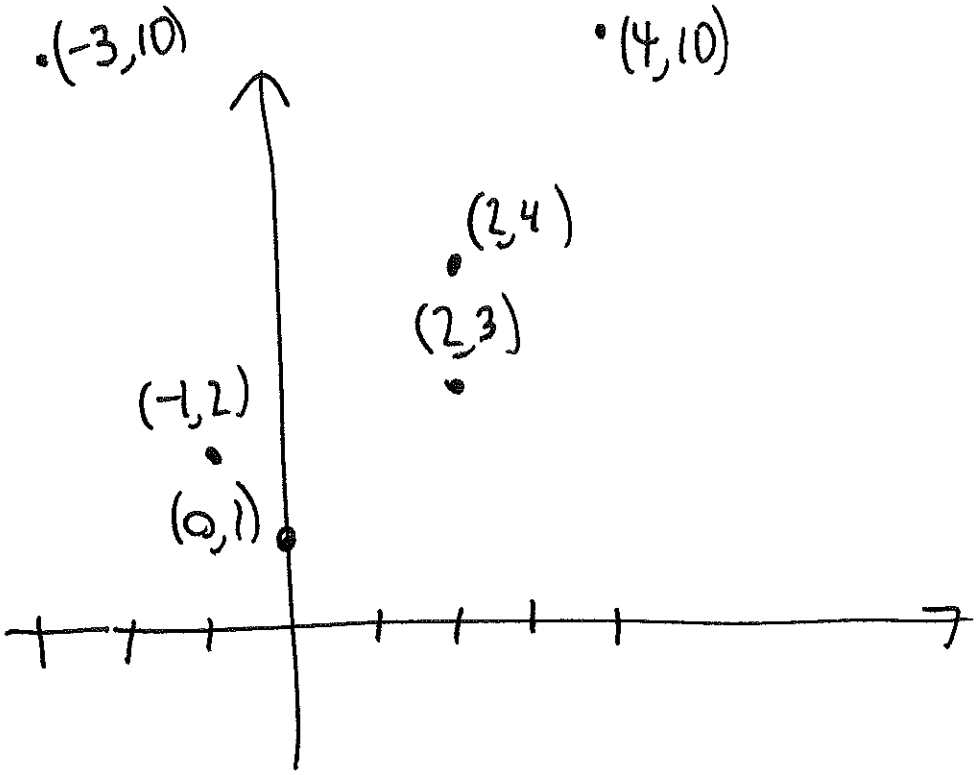
Eqn 1: $b = -5/11$

1.3

so

Eqn 2: $m + b = 223/264 \implies m = 223/264 + 5/11 = 343/264$

Find quadratic through:



$$y = ax^2 + bx + c$$

Dream equations:

$$10 = 9a - 3b + c$$

$$2 = 1a - 1b + c$$

$$1 = 0a + 0b + c$$

$$3 = 4a + 2b + c$$

$$4 = 4a + 2b + c$$

$$10 = 16a + 4b + c$$

$$\begin{pmatrix} 9 & -3 & 1 \\ 1 & -1 & 1 \\ 0 & 0 & 1 \\ 4 & 2 & 1 \\ 4 & 2 & 1 \\ 16 & 4 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 10 \\ 2 \\ 1 \\ 3 \\ 4 \\ 10 \end{pmatrix}$$

NO SOLUTIONS!

← replace with projection $\begin{pmatrix} 5663/587 \\ \vdots \\ 12229/1174 \end{pmatrix}$

use Gram-Schmidt on these (computer)

Fourier series

V = all periodic functions with period 2π

A basis* for V is

1
$\cos x$
$\sin x$
$\cos(2x)$
$\sin(2x)$
$\cos(3x)$
$\sin(3x)$
$\cos(4x)$
$\sin(4x)$
$\ldots$

Given a periodic function f, ~~how to~~ we can write it in terms of those?

Are those an orthonormal basis?

Use inner product

$$\langle f, g \rangle = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x)\, g(x)\, dx$$

Check a few:

$$\langle \cos(x), \cos(x) \rangle = \frac{1}{\pi}\int_{-\pi}^{\pi} \cos^2 x \, dx = \frac{1}{\pi}\int_{-\pi}^{\pi} \frac{1+\cos(2x)}{2} \, dx$$

$$= \frac{1}{\pi}\int_{-\pi}^{\pi} \frac{1}{2} \, dx + \frac{1}{\pi}\int_{-\pi}^{\pi} \cos(2x) \, dx = \frac{1}{\pi}\cdot\frac{1}{2}(2\pi) + \frac{1}{\pi}\left.\frac{\sin(2x)}{2}\right|_{-\pi}^{\pi}$$

✓

$$= 1 + 0 = 1$$

✓ $$\langle \cos(x), \sin(3x) \rangle = \frac{1}{\pi}\int_{-\pi}^{\pi} \cos x \sin 3x \, dx = 0$$

$$\langle 1, 1 \rangle = \frac{1}{\pi}\int_{-\pi}^{\pi} 1 \cdot 1 \, dx = \frac{1}{\pi}(2\pi) = 2.$$

So use $\frac{1}{\sqrt{2}}$ in your basis.

Everything else works!

$\frac{1}{\sqrt{2}}, \cos x, \sin x, \cos 2x, \sin 2x, \cos 3x, \sin 3x$

is <u>orthonormal</u>.

To write a random function f as a combination of those:

Warm-up: how to write (a,b) as combo of $(1,0)$ and $(0,1)$

$$\underbrace{\big((a,b)\cdot(1,0)\big)}_{1^{st}\text{ coef}}(1,0) + \underbrace{\big((a,b)\cdot(0,1)\big)}_{2^{nd}\text{ coef}}\cdot(0,1)$$

$$f = \left\langle f, \frac{1}{\sqrt{2}}\right\rangle \frac{1}{\sqrt{2}} + \langle f, \cos x\rangle \cos x + \langle f, \sin x\rangle \sin x$$

$$+ \langle f, \cos 2x\rangle \cos 2x, \langle f, \sin 2x\rangle \sin 2x + \cdots$$

Warm-up to Fourier series

Let's imagine we have an orthonormal basis $e_1, \dots, e_n$ for a vector space V.

Suppose we have a vector v and want to write

$$v = c_1 e_1 + c_2 e_2 + \cdots + c_n e_n. \qquad (c_i \text{ scalars})$$

How to find c_i? If orthonormal, it's easy!

$$\langle v, e_1 \rangle = \langle c_1 e_1 + \cdots + c_n e_n, e_1 \rangle$$

$$= c_1 \langle e_1, e_1 \rangle + c_2 \langle e_2, e_1 \rangle + \cdots c_n \langle e_n, e_1 \rangle.$$

$$= c_1 + 0 + 0 + \cdots + 0 = c_1$$

To get c_j, do $\langle v, e_j \rangle$!

Last time:

$\rightarrow V = \left\{ \begin{array}{l} \text{all periodic functions} \\ \text{period } 2\pi \end{array} \right\}$ $\quad \langle f, g \rangle = \frac{1}{\pi} \int_{-\pi}^{\pi} fg \, dx$

An orthonormal basis: $1/\sqrt{2}$, $\cos x$, $\sin x$, $\cos(2x)$, $\sin(2x)$

$\cos(3x)$, $\sin(3x)$, $\cos(4x)$, $\sin(4x)$, ...

Suppose f is periodic. How to write f as combo of sin & cos?

$$f = \frac{1}{\sqrt{2}} a_0 + \sum_{n=1}^{\infty} a_n \cos(nx) + \sum_{n=1}^{\infty} b_n \sin(nx).$$

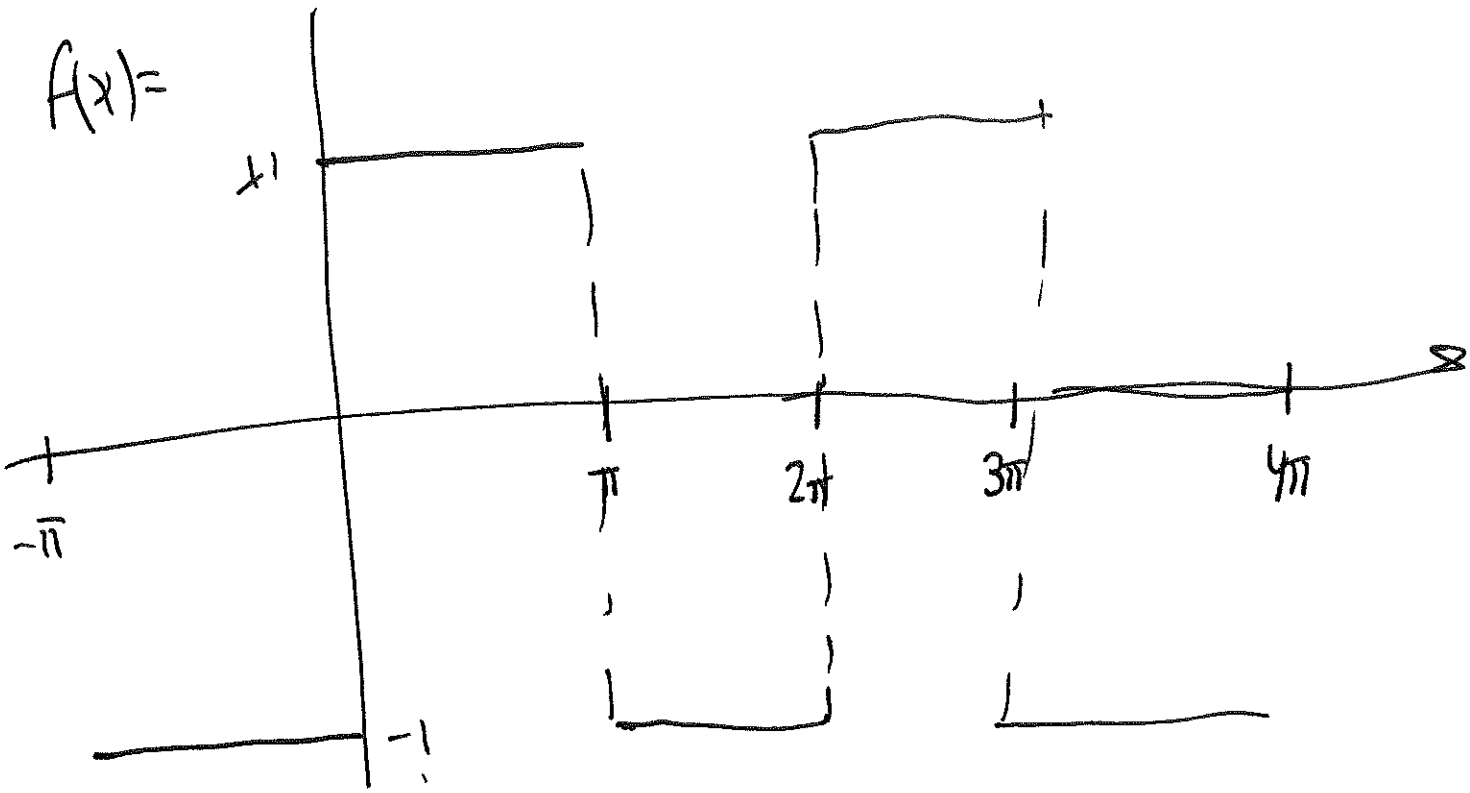
$\cancel{a_0 = \frac{1}{\pi}}$ $\quad a_0 = \langle f, \frac{1}{\sqrt{2}} \rangle = \frac{1}{\pi} \int_{-\pi}^{\pi} \frac{1}{\sqrt{2}} f \, dx$

$$a_n = \langle f, \cos(nx) \rangle = \frac{1}{\pi} \int_{-\pi}^{\pi} f \cos(nx) \, dx$$

$$b_n = \langle f, \sin(nx) \rangle = \frac{1}{\pi} \int_{-\pi}^{\pi} f \sin(nx) \, dx$$

Square wave

$f(x) =$



even × odd

$$a_0 = \frac{1}{\pi}\int_{-\pi}^{\pi} \frac{1}{\sqrt{2}} f \, dx = 0$$

$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f \sin(nx)\, dx$$

$$a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f \cos(nx)\, dx = 0$$

odd × even

$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} \overbrace{f \sin(nx)}^{\text{odd}\times\text{odd}=\text{even}}\,dx = \frac{2}{\pi}\int_{0}^{\pi} f \sin(nx)\,dx$$

$$= \frac{2}{\pi}\int_{0}^{\pi} \sin(nx)\,dx$$

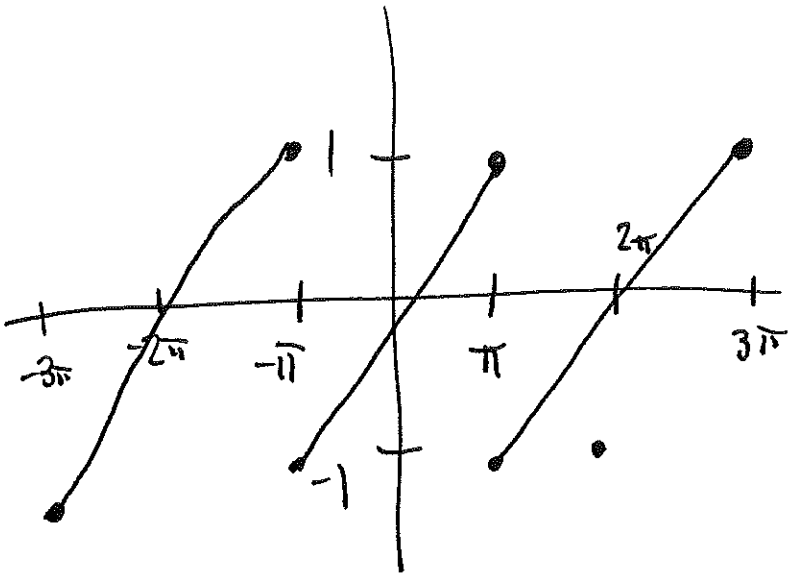
$$\cos(n\pi) = (-1)^n = \begin{cases} 1 & n \text{ even} \\ -1 & n \text{ odd} \end{cases}$$

$$= \frac{2}{\pi}\left(-\frac{1}{n}\cos(nx)\Big|_0^{\pi}\right)$$

$$= \begin{cases} 0 & n \text{ even} \\ \frac{4}{\pi n} & n \text{ odd} \end{cases}$$

$$f(x) = \frac{4}{\pi}\sin(x) + \frac{4}{3\pi}\sin(3x) + \frac{4}{5\pi}\sin(5x) + \frac{4}{7\pi}\sin(7x) + \dots$$

Sawtooth wave:



$$a_0 = \left\langle f, \frac{1}{\sqrt{2}} \right\rangle = \frac{1}{\pi} \int_{-\pi}^{\pi} \frac{1}{\sqrt{2}} f \, dx$$

$$a_n = \langle f, \cos(nx) \rangle = \frac{1}{\pi} \int_{-\pi}^{\pi} f \cos(nx) \, dx$$

$$b_n = \langle f, \sin(nx) \rangle = \frac{1}{\pi} \int_{-\pi}^{\pi} f \sin(nx) \, dx$$

$a_i = 0$ (odd!)

$$b_n = \frac{1}{\pi} \int_{-\pi}^{\pi} x \sin(nx) \, dx = \frac{2}{\pi} \int_{0}^{\pi} x \sin(nx) \, dx$$

$$\int x \sin(nx) \, dx = -\frac{x}{n} \cos(nx) + \int \frac{1}{n} \cos(nx) \, dx$$

$$= -\frac{x}{n} \cos(nx) + \frac{1}{n^2} \sin(nx)$$

$u = x \qquad v = -\frac{1}{n} \cos(nx)$

$du = dx \qquad dv = \sin(nx) \, dx$

$$= \frac{2}{\pi} \left(\left(-\frac{x}{n} \cos(nx) + \frac{1}{n^2} \sin(nx) \right) \Big|_0^{\pi} \right) = \left(\cancel{2} \right)$$

$$= \frac{2}{\pi}\left(\left(-\frac{\pi}{n}(-1)^n + \frac{0}{n}\cos(0x)\right)\right) = -\frac{2}{n}(-1)^n = \cancel{-\frac{2}{n}}$$

$$= \begin{cases} \frac{2}{n} & n \text{ odd} \\ -\frac{2}{n} & n \text{ even.} \end{cases}$$

$$f(x) = 2\sin(x) - \frac{2}{2}\sin(2x) + \frac{2}{3}\sin(3x) - \frac{2}{4}\sin(4x) + \frac{2}{5}\sin(5x)$$

<u>Pythagorean theorem.</u>

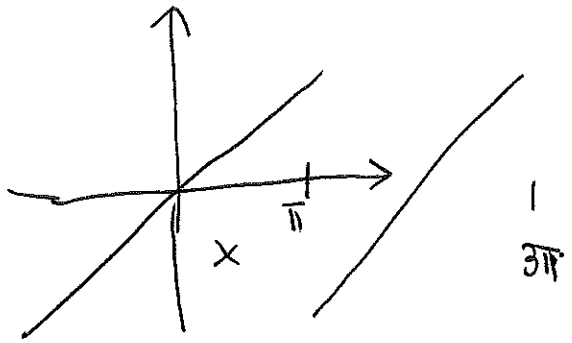
length of $(2,3,4)$? $\sqrt{2^2+3^2+4^2}$.

e_i orthonormal basis.

$$\|c_1e_1 + \cdots + c_ne_n\|^2 = \|c_1e_1\|^2 + \cdots + \|c_ne_n\|^2$$

$$= c_1^2\|e_1\|^2 + \cdots + c_n^2\|e_n\|^2$$

$$= c_1^2 + c_2^2 + c_3^2 + \cdots + c_n^2.$$



Before

$$f(x) = \frac{2}{1}\sin(x) - \frac{2}{2}\sin(2x) + \frac{2}{3}\sin(3x) - \frac{2}{4}\sin(4x) + \frac{2}{5}\sin(5x) - \cdots$$

$$= c_1 e_1 + c_2 e_2 + c_3 e_3 + c_4 e_4 + \cdots$$

$$\|f\|^2 = c_1^2 + c_2^2 + c_3^2 + c_4^2 + \cdots$$

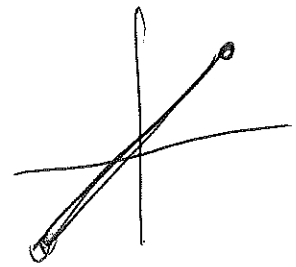
$$= \left(\frac{2}{1}\right)^2 + \left(-\frac{2}{2}\right)^2 + \left(\frac{2}{3}\right)^2 + \left(-\frac{2}{4}\right)^2 + \left(\frac{2}{5}\right)^2 + \cdots$$

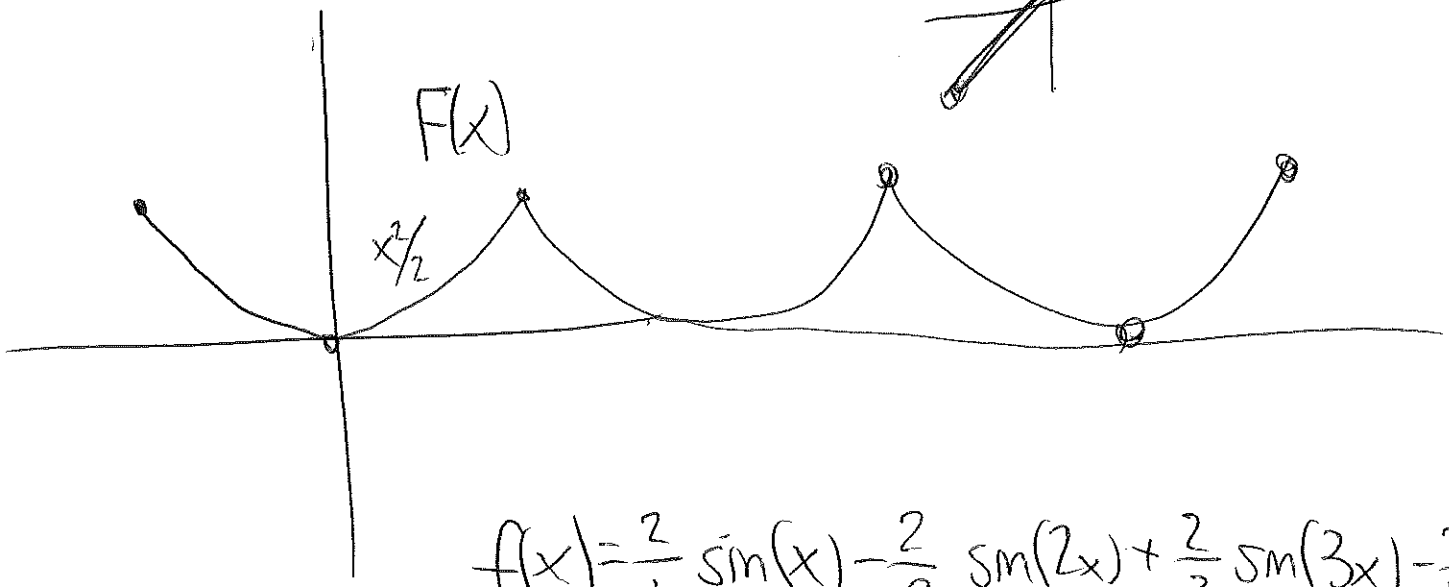
$$= 4\left(\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \cdots\right)$$

$$\|f\|^2 = \langle f, f\rangle = \frac{1}{\pi}\int_{-\pi}^{\pi} x^2\,dx = \frac{1}{\pi}\left(\frac{2\pi^3}{3}\right) = \frac{2\pi^2}{3}$$

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \cdots = \frac{2\pi^2}{3}\cdot\frac{1}{4} = \frac{\pi^2}{6}.$$

What other sums can we get?





$$f(x) = \frac{2}{1}\sin(x) - \frac{2}{2}\sin(2x) + \frac{2}{3}\sin(3x) - \frac{2}{4}\sin(4x)$$

$$C + F(x) = -\frac{2}{1}\cos(x) + \frac{2}{4}\cos(2x) - \frac{2}{9}\cos(3x) + \frac{2}{16}\cos(4x) + \cdots$$

Pythagorean thm:

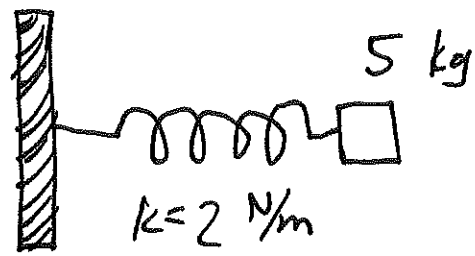
$$\left(-\frac{2}{1}\right)^2 + \left(\frac{2}{4}\right)^2 + \left(-\frac{2}{9}\right)^2 + \left(\frac{2}{16}\right)^2 + \left(-\frac{2}{25}\right)^2 \cdots$$

$$\shortparallel$$

$$4\sum_{n=1}^{\infty} \frac{1}{n^4} = \|f\|^2$$

$$\hookrightarrow \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}$$

Some differential equations



If we pull it out 3 m and release, where will it be in 10 seconds?

Hooke's law: $F = -kx$

$F = ma$

AP Physics: $\omega = \sqrt{\frac{k}{m}}$

Position at time t: $x(t)$

$$m\,x''(t) = -k\,x(t)$$ ← example differential equation.

how to find $x(t)$?

$$x''(t) = -\frac{k}{m}x(t)$$ ω

$$x(t) = \cos\left(\sqrt{\frac{k}{m}}\,t\right)$$ work.

$$\sin\left(\sqrt{\frac{k}{m}}\,t\right)$$

Any other solutions? $-\cos\left(\sqrt{\frac{k}{m}}\,t\right)$, $-\sin\left(\sqrt{\frac{k}{m}}\,t\right)$

- multiply by constants
- add any two solutions

} set of solutions is a vector space!

General solution is:

$$c_1 \cos\left(\sqrt{\frac{k}{m}}\,t\right) + c_2 \sin\left(\sqrt{\frac{k}{m}}\,t\right).$$

(every solution is like this for some c_1, c_2).

Another solution is e.g.

$$5 \cos\left(\sqrt{\frac{k}{m}}(t-2)\right)$$

$\cos(A-B) = \cos A \cos B + \sin A \sin B$

but that's

$$= \underbrace{5}_{\text{some constant}} \cos\left(\sqrt{\frac{k}{m}}\,t\right) \cos\left(2\sqrt{\frac{k}{m}}\right) + 5 \sin\left(\sqrt{\frac{k}{m}}\,t\right) \sin\left(2\sqrt{\frac{k}{m}}\right)$$

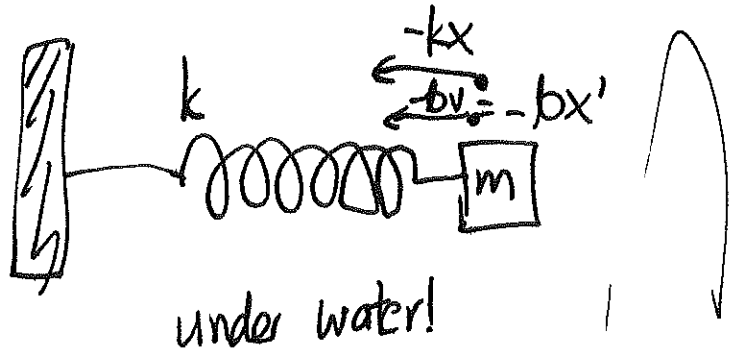
If you have specific initial conditions, like

$x(0)=5$

$x'(0)=2$

these determine a unique solution, because you can solve for c_1, c_2.

What if there's a drag force?



under water!
→ drag force
(proportional to velocity)

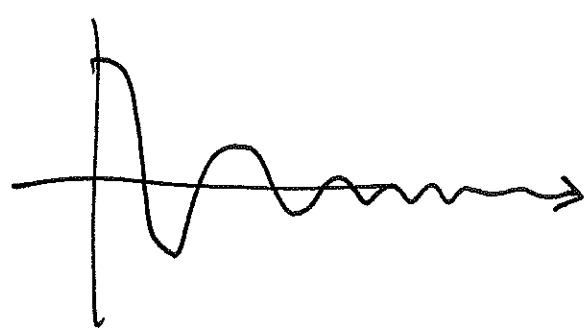
$$m x''(t) = -k\,x(t) - b\,x'(t)$$

$$m\,x''(t) + b\,x'(t) + k\,x(t) = 0$$

hard to guess answer!

It ends up being like:

$$e^{-t}\cos(3t)$$



If wall moves back & forth:

$$m x''(t) + b x'(t) + k x(t) = F(t)$$

external force.

how to solve?

Most differential equations can't be solved exactly!
(just like number equations)
But many common ones are solvable.

has $x'(t)$
but no higher derivatives.

Let's start with some <u>1st order</u> diff eqs.

Try it: $$t\,x'(t) + 2\,x(t) = 0$$

$$x'(t) = -\frac{2}{t}\,x(t)$$

<u>Method #1.</u>

$$\frac{x'(t)}{x(t)} = -\frac{2}{t}$$

Guess: $x(t) = Ct^a$ try it! see if we can find C, a that work. "ansatz" guess solution.

$$t\,x'(t) + 2\,x(t) = 0$$

$$t(aCt^{a-1}) + 2(Ct^a) = 0$$

unless $a=0$

$$aC(t^a) = -2Ct^a.$$

so $a=-2$ and solution is $x(t) = Ct^{-2}$.

Method #2

$$\frac{x'(t)}{x(t)} = -\frac{2}{t}$$

natural log

$$\frac{d}{dt}\left(\log\left(x(t)\right)\right) = -\frac{2}{t}$$

$$\log x(t) = -2\log(t) + C$$

$e^{\sim}$ $\rightarrow$ $x(t) = e^{-2\log(t) + C} = \tilde{C}\, t^{-2}$. ✓

Try it:

$$t^2 x(t) = 3x'(t)$$

$\downarrow$

$$\frac{d}{dt}\log x(t) = \frac{x'(t)}{x(t)} = \frac{t^2}{3}$$

$$\log x(t) = \frac{t^3}{9} + C$$

$$x(t) = e^{t^3/9} \cdot \tilde{C}$$ e^C.

Challenge:

$$t^2 x(t) = 3x'(t) + 2$$

other solutions?

$t^2 e^{-t}$? not quite.

Math How can we ever know there are no other solutions?

$$y' = 0$$

$y(t) = C$ works. are there any other solutions?

If not constant, $y(a) \neq y(b)$ for some a, b.

Mean value theorem: there's a c with $a < c < b$ so

$$y'(c) = \frac{y(b) - y(a)}{b-a} \neq 0.$$

this contradicts $y'(c) = 0$.

$$t\,x'(t) + 2x(t) = t^3$$

Multiply by "integrating factor", in this case t.

$$t^2 x'(t) + 2t\ x(t) = t^4$$

$$\frac{d}{dt}\left(t^2 x(t)\right) = t^4$$

product rule!

$$t^2\ x(t) = \frac{t^5}{5} + C$$

$$x(t) = \frac{t^3}{5} + \frac{C}{t^2}$$

$$t^2\, x(t) = 3\, x'(t) + 2$$

$$(t^2)x(t) + (-3)\, x'(t) = 2$$

want to multiply by $p(t)$ so left side is

chain rule...

what could $p(t)$ be?

$$(t^2\, p(t))\, x(t) + (-3\, p(t))\, x'(t) = 2\, p(t)$$

we need derivative of $-3\, p(t)$ to be $t^2\, p(t)$.

(so we can use product rule)

$$-3\, p'(t) = t^2\, p(t)$$

$$\frac{d}{dt} \log p(t) = \frac{p'(t)}{p(t)} = -\frac{t^2}{3}$$

$$\log(p(t)) = \frac{-t^3}{9} + 0$$

$$p(t) = e^{-t^3/9}.$$

$$\left(t^2 e^{-t^3/9}\right) x(t) + \underbrace{\left(-3e^{-t^3/9}\right)}_{f(t)} x'(t) = 2e^{-t^3/9}$$

$$= f'(t)\, x(t) + f(t)\, x'(t) = 2e^{-t^3/9}$$

$$\frac{d}{dt}\left(-3e^{-t^3/9}\, x(t)\right) = 2e^{-t^3/9}$$

$$-3e^{-t^3/9}\, x(t) = \int 2e^{-t^3/9}\, dt$$

$$\cdots$$

$$x(t) = \cdots$$

Today:

More differential equations.

Find $y(t)$:

<u>Review:</u> $y'(t) = t\,y(t)$

$$\frac{y'}{y} = t \rightsquigarrow \frac{d}{dt}(\log y) = t$$

$$\log y = t^2/2 + c$$

$$y = e^{t^2/2} \cdot \tilde{C}$$

$\tilde{C} = e^c$; new constant.

$$y(t) + \tan(t)\, y' = 1$$

"Integrating factor": multiply both sides by $\cos(t)$.

$$\cos t \cdot y + \sin t \cdot y' = \cos t$$

$$\frac{d}{dt}(\sin t \cdot y) = \cos t$$

$$\sin t \cdot y = \sin t + C$$

$$y = 1 + C \cdot \csc t.$$

Another example:

$$2y + ty' = 1$$

$$2ty + t^2 y' = t$$

$$\frac{d}{dt}(t^2 y) = t$$

$$t^2 y = \frac{t^2}{2} + c$$

$$y = \frac{1}{2} + \frac{c}{t^2}.$$

To solve

$$a(t)\,y + b(t)\,y' = c(t)$$

"First-order linear equation"

only $f(t)\cdot y$, $f(t)y'$: no $(y')^2$, $y\cdot y'$, $1/y$

only y', no y'', y''' etc.

general method

$$y + \frac{b(t)}{a(t)}\,y' = \frac{c(t)}{a(t)}.$$ ← need an integrating factor $p(t)$.

$$p(t)\,y + p(t)\frac{b(t)}{a(t)}\,y' = p(t)\,\frac{c(t)}{a(t)}$$

so

$$p(t) = \frac{d}{dt}\left(p(t)\,\frac{b(t)}{a(t)}\right) = p'(t)\,\frac{b(t)}{a(t)} + p(t)\left(\frac{d}{dt}\,\frac{b(t)}{a(t)}\right).$$

From here, solve for $\frac{p'(t)}{p(t)}$, integrate to get $\log p(t)$, done!

First order linear eqns → solvable.

But for higher order, it's hopeless!

can't always find a formula for solution.

Classic example: Airy equation $y'' = ty$.

Two-dimensional solution space

- One solution can be written as antiderivative of something easy
- Second solution can't be written in a simple way.

<u>Second-order</u> linear equations with <u>constant coefficients</u>

no $(y')^2$ etc

y, y', y''

<u>homogeneous</u>

$=0$ (every term must depend on y)

can't depend on t

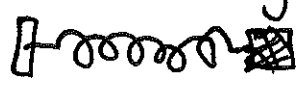
$$\boxed{ay'' + by' + cy = 0}$$

a, b, c are numbers.

Last time:

$my'' + by' + ky = 0$

mass on a spring with drag.



Example

$$y'' + 5y' + 6y = 0$$

What are all solutions?

Try: Guess $y(t) = e^{rt} + C$

$$r^2 e^{rt} + 5re^{rt} + 6e^{rt} + 6C = 0$$

0 for all t, so $C = 0$.

$$r^2 e^{rt} + 5re^{rt} + 6e^{rt} = 0$$

$$r^2 + 5r + 6 = 0$$

$$(r+2)(r+3) = 0 \quad r = -2 \text{ or } -3.$$

Solutions are e^{-2t}, e^{-3t}.

General solution to equation:

$$y(t) = C_1 e^{-2t} + C_2 e^{-3t}.$$

If we have initial conditions, you can solve for the constants.

$y(0)=2$
$y'(0)=3$ and $y''+5y'+6y=0$

solution is $C_1e^{-2t}+C_2e^{-3t}$ $\quad y'(t)=-2C_1e^{-2t}-3C_2e^{-3t}$

plug in 0 for t

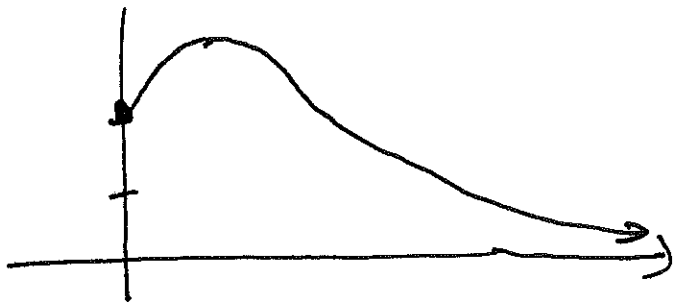
$y(0)=2$ tells us $C_1+C_2=2$

$y'(0)=3$ $\quad -2C_1-3C_2=3$

2 eqns, 2 vars

✓ $C_1=9$, $C_2=-7$

$$\boxed{y(t)=9e^{-2t}-7e^{-3t}}$$



$$4y'' - 8y' + 3y = 0 \qquad y(0) = 2$$

$$y'(0) = \tfrac{1}{2}$$

Try: $y(t) = e^{rt}$

what r value will work?

$$4r^2 e^{rt} - 8re^{rt} + 3e^{rt} = 0$$

$$4r^2 - 8r + 3$$

$$(2r-1)(2r-3) = 0$$

$$r = \tfrac{1}{2} \quad r = \tfrac{3}{2} \rightsquigarrow e^{t/2},\ e^{3t/2} \text{ solutions.}$$

General sol: $C_1 e^{t/2} + C_2 e^{3t/2}$

Initial conditions: $y(0) = 2$ says $C_1 + C_2 = 2$

$y'(0) = \tfrac{1}{2}$ says $\tfrac{1}{2}C_1 + \tfrac{3}{2}C_2 = \tfrac{1}{2}$

$$\rightsquigarrow \begin{array}{l} C_1 = 5/2 \\ C_2 = -1/2 \end{array}$$

To solve

$$ay'' + by' + cy = 0$$

Guess $y(t) = e^{rt}$

Plug in $\Rightarrow$ $ar^2 + br + c = 0$

solve for r $\Longrightarrow$ two possible values r_1, r_2.

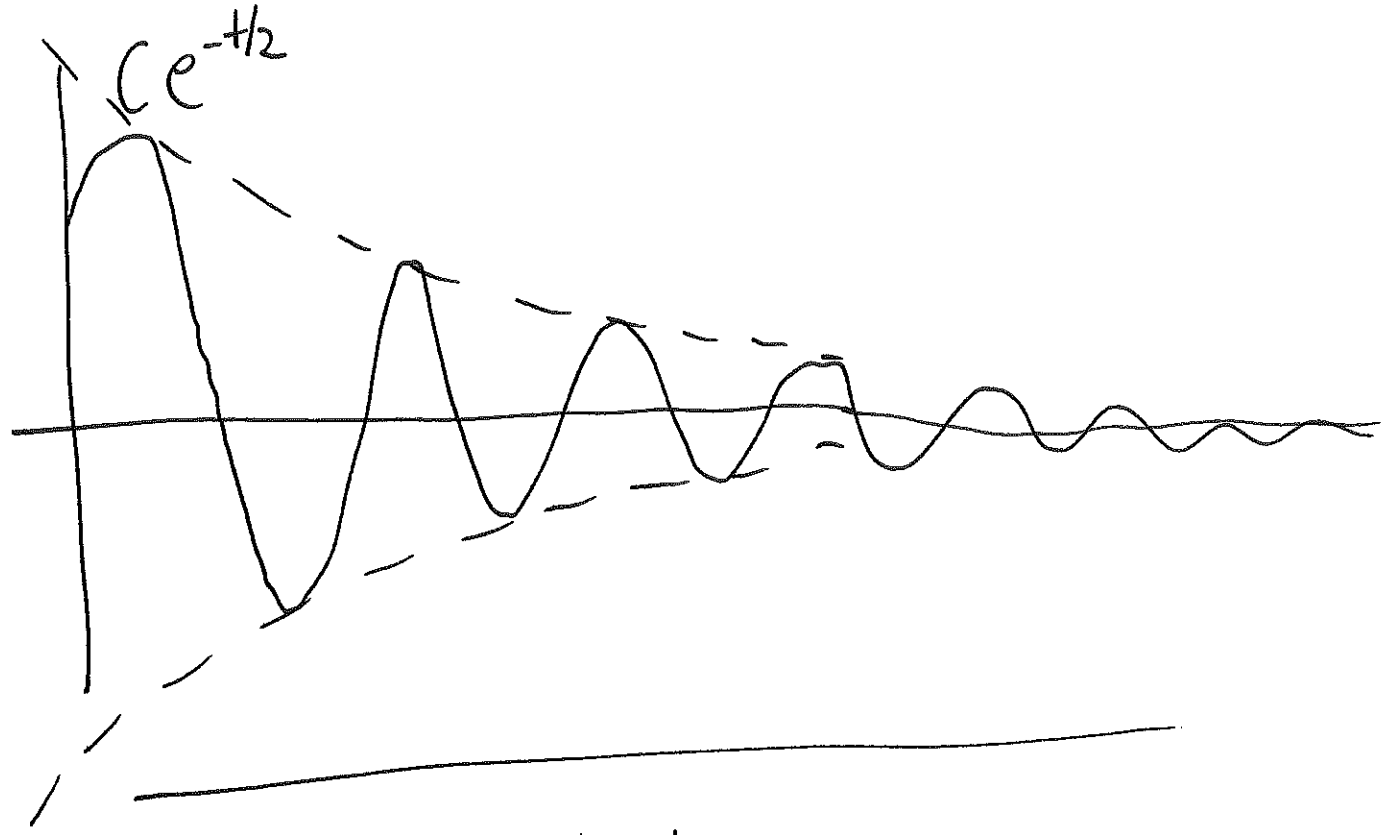
General solution: $C_1 e^{r_1 t} + C_2 e^{r_2 t}$

As long as: - r_1, r_2 distinct

- r_1, r_2 real.

What if they're not?

$\hookrightarrow$ $r_1 = r_2$ or $r_1 = \bar{r}_2$ complex conjugates.



Mass on spring:

$$my'' + by' + ky = 0$$

$$mr^2 + br + k = 0$$

$$r = \frac{-b \pm \sqrt{b^2 - 4mk}}{2m}$$ if complex roots:

~~a+bi~~ $a+ci$

real part of root is $a = -\frac{b}{2m}$

$e^{(a+ci)t}$

$\parallel$

$e^{at}\cos(ct)$

Imaginary part: $c = \frac{\sqrt{4mk-b^2}}{2m}$

Solution is: $e^{-b/2m\,t} \cdot \cos\left(\left(\frac{\sqrt{4mk-b^2}}{2m}\right)t\right)$

or sin

$$y'' + y' + 9.25y = 0$$ (this could be a mass on a spring: all coefs +)

Try

$y(t) = e^{rt}$

$$r^2 + r + 9.25 = 0$$

$$\left(r^2 + r + \tfrac{1}{4}\right) + 9 = 0$$

$$\left(r + \tfrac{1}{2}\right)^2 = -9$$

$$r + \tfrac{1}{2} = \pm 3i$$

$$r = -\tfrac{1}{2} \pm 3i$$

Solutions

$$e^{\left(-\frac{1}{2}+3i\right)t}, \quad e^{\left(-\frac{1}{2}-3i\right)t}.$$

$$\downarrow$$

$$e^{-t/2} e^{3it}$$

$$\shortparallel$$

$$e^{-t/2}(\cos 3t + i \sin 3t)$$

Real part

$$e^{-t/2} \cos 3t$$

Imaginary part

$$e^{-t/2} \sin 3t$$

both solutions.

General sol is

$$c_1 e^{-t/2} \cos 3t + c_2 e^{-t/2} \sin 3t$$

Repeated roots.

$$y'' - 4y' + 4y = 0.$$

Try e^{rt}:

$$r^2 - 4r + 4 = 0$$

$(r-2)(r-2)$. So e^{2t} is a solution.

What's the second solution?

Try $y = (a+bt)e^{rt}$

$$y' = be^{rt} + r(a+bt)e^{rt}$$

$$= (b+ar)e^{rt} + rbte^{rt}$$

$$y'' = r(b+ar)e^{rt} + rb(tre^{rt} + e^{rt})$$

$$= (2br + ar^2)e^{rt} + br^2te^{rt}$$

$$y'' - 4y' + 4y = 0$$

$$0 = e^{rt}(2br + ar^2 - 4b - 4ar + 4a) + te^{rt}(br^2 - 4br + 4b)$$

What a, b, r make this 0?

$$b(r^2 - 4r + 4) = 0.$$

$$\rightarrow (r-2)(r-2) = 0$$

so $r = 2$. to make te^{rt} term disappear.

Then e^{rt} term is 0 too. As long as $r=2$, a, b can be anything.

e^{2t} and te^{2t} are our basic solutions.

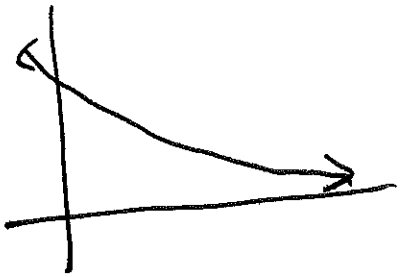
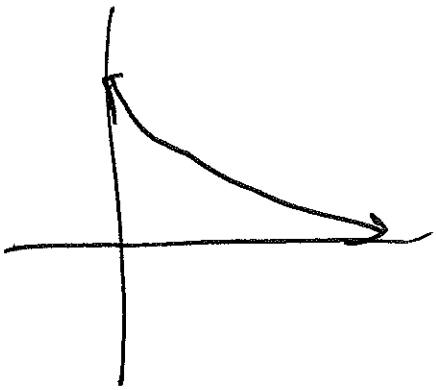
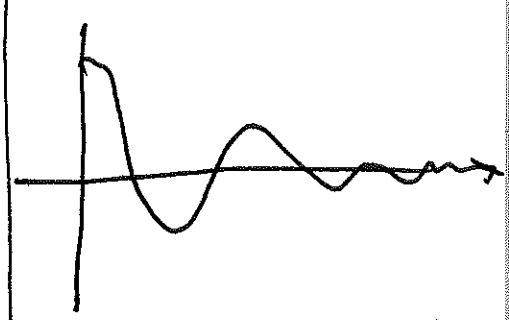
General solution is

$$C_1 e^{2t} + C_2 te^{2t}.$$

Mass on a spring.

$$my'' + by' + ky = 0.$$

Three options

Two distinct real	Double real root	Complex roots.
$b^2 > 4km$	$b^2 = 4km$	$b^2 < 4km$
$c_1 e^{r_1 t} + c_2 e^{r_2 t}$	$c_1 e^{rt} + c_2 t e^{rt}$	$c_1 e^{at}\cos(ct) + c_2 e^{at}\sin(ct)$
 "overdamped"	 "critically damped"	 "underdamped"

Today:

More diff eq.

But: I have to leave early, sorry!

Warm-up:

$$y'' + 6y' + 13y = 0$$

$$y'' + 2y' + y = 0$$

$$y'' - 4y = 0$$

Find general sol'n.

Hint: try $e^{rt} = y$, see what value of r makes it work.

$$r^2 e^{rt} + 6re^{rt} + 13e^{rt} = 0$$

$$r^2 + 6r + 13 = 0$$

$$\ldots$$

$$r^2 + 2r + 1 = 0$$

$$r^2 - 4 = 0$$

$$y'' - 4y = 0$$

$$r^2 - 4 = 0$$

$$r = \pm 2$$

Two real roots

$$\rightarrow c_1 e^{2t} + c_2 e^{-2t}$$

$$y'' + 2y' + y = 0$$

$$r^2 + 2r + 1 = 0$$

$$(r+1)^2 = 0$$

$$c_1 e^{-t} + c_2 t e^{-t}$$

(just remember) this formula

$$y'' + 6y' + 13y = 0$$

$$r^2 + 6r + 13 = 0$$

$$(r+3)^2 + 4 = 0$$

$$(r+3)^2 = -4$$

$$r + 3 = \pm 2i$$

$$r = -3 \pm 2i$$

use real & imag. parts of

$$e^{(-3+2i)t}$$

$$c_1 e^{-3t} \cos 2t + c_2 e^{-3t} \sin 2t.$$

$$y'' - 3y' - 4y = \underbrace{3e^{2t}}_{\text{not } 0!}$$

(this is a mass on a spring, subject to external force.)

$$r^2 - 3r - 4 = 0 \longrightarrow y'' - 3y' - 4y = 0$$

$$(r-4)(r+1) \qquad c_1 e^{4t} + c_2 e^{-t}$$

To find one solution:

guess $y = Ae^{2t}$

from problem

$$y'' - 3y' - 4y = 4Ae^{2t} - 6Ae^{2t} - 4Ae^{2t} = 3e^{2t}$$

$$-6Ae^{2t} = 3e^{2t}$$

$$A = -\frac{1}{2}e^{2t}$$

one solution with RHS

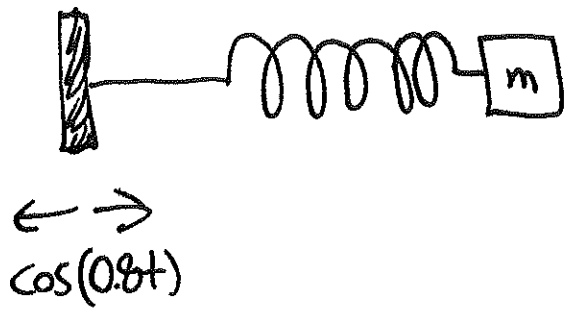
$$\boxed{y = -\frac{1}{2}e^{2t} + c_1 e^{4t} + c_2 e^{-t}}$$

general sol with RHS=0

Last time:

$$u''(t) + u(t) = 0.5\cos(0.8t) \qquad u(0) = 0$$
$$u'(0) = 0$$

Try: $\cos(\omega t)$



Step 1: Guess a "particular solution"
(one solution)

Want: $u''(t)$

$$u'' + u = 0.5\cos(\omega t)$$

Try: $u = A\cos(\omega t)$

$$-A\omega^2\cos(\omega t) + A\cos(\omega t) = 0.5\cos(\omega t)$$

$$(A - A\omega^2)\cos\omega t = 0.5\cos\omega t$$

$$A = \frac{0.5}{1-\omega^2} \Rightarrow u = \left(\frac{0.5}{1-\omega^2}\right)\cos(\omega t)$$

Find general solution

Solve "corresponding homogeneous" equation

right side = 0

$$u'' + u = 0$$

$$c_1 \cos t + c_2 \sin t$$

our general solution is.

$$u = \left(\frac{0.5}{1-\omega^2}\right)\cos(\omega t) + c_1 \cos t + c_2 \sin t.$$

Step 3 Find c_1, c_2 using initial conditions.

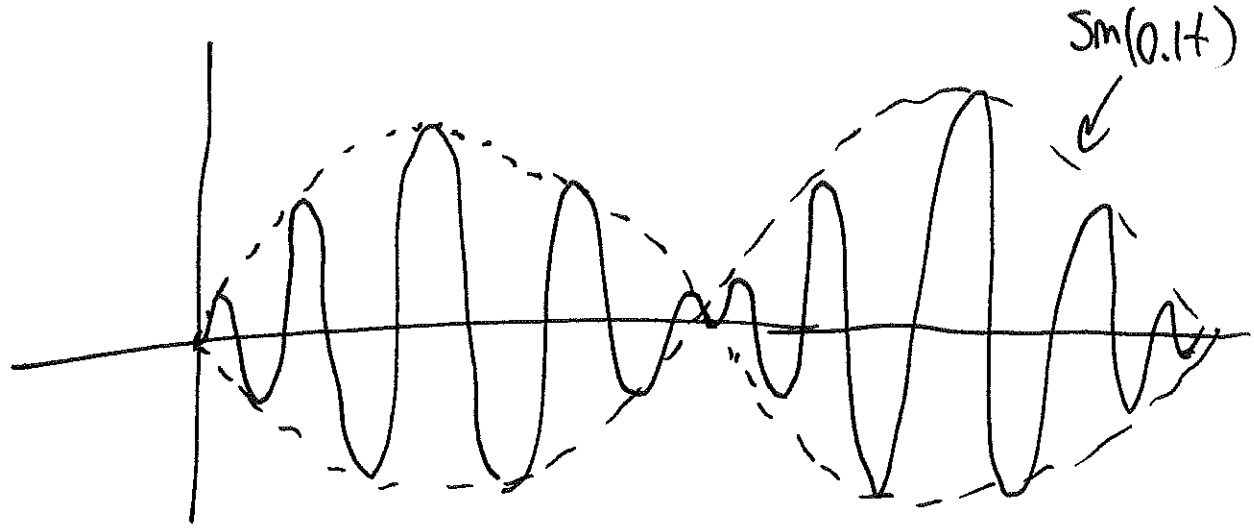
$u(0) = 0 \quad u'(0) = 0.$

$$u(0) = 0 \Rightarrow \frac{0.5}{1-\omega^2} + c_1 + 0 = 0$$

$$c_1 = -\frac{0.5}{1-\omega^2} \checkmark$$

$u'(0)=0. \Rightarrow c_2=0.$

$$u(t)= \frac{0.5}{1-\omega^2}\cos(\omega t) - \frac{0.5}{1-\omega^2}\cos t$$



e.g. $\omega=0.8$

$$\frac{0.5}{1-\omega^2}\left(\cos(\omega t)-\cos t\right) \qquad \boxed{\frac{25}{9}\sin(0.9t)\sin(0.1t)}$$

$$\cos A-\cos B = -2\sin\frac{A+B}{2}\sin\frac{A-B}{2}$$

"beat solution"

$$= \frac{0.5}{1-\omega^2}\cdot -2\sin\left(\frac{1+\omega}{2}t\right)\sin\left(\frac{\omega-1}{2}t\right)$$

$$= \frac{1}{1-\omega^2}\sin\left(\frac{1+\omega}{2}t\right)\sin\left(\frac{1-\omega}{2}t\right).$$

If $\omega = 1$. Then what?

$$u'' + u = 0.5 \cos(t).$$

The guess $u = A \cos t$ is no good, we get 0 no matter what A is.

Instead we guess:

$$\cancel{(A+Bt)\cos t}$$ (if that

$$u = (A+Bt)\cos t + (C+Dt)\sin t$$

$$u' = \left[(A+Bt)(-\sin t) + B\cos t\right] + \left[(C+Dt)\cos t + D\sin t\right]$$

$$= (D-A-Bt)\sin(t) + (B+C+Dt)\cos(t)$$

$$u'' = (D-A-Bt)\cos t + (-B)\sin t + (B+C+Dt)(-\sin t) + D\cos t$$

$$= (2D-A-Bt)\cos t + (-2B-C-Dt)\sin t$$

$u + u'' = 2D \cos t - 2B \sin t.$

want that to be $0.5\cos(t)$

$\hookrightarrow 2D = 0.5 \qquad D = 1/4$

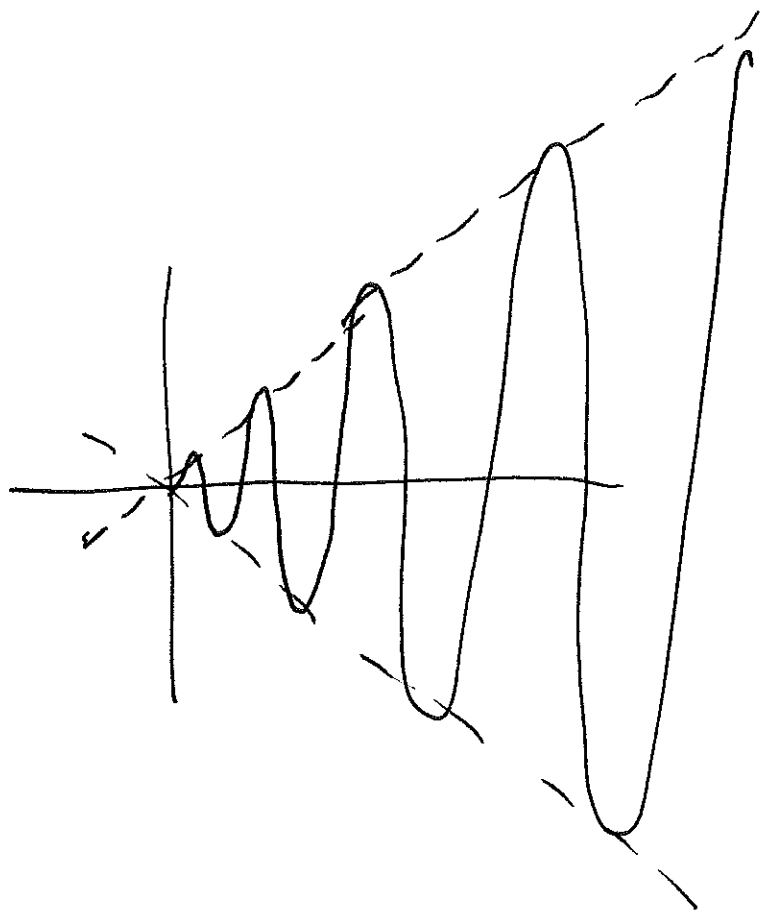
$B = 0 \qquad B = 0$

$u(0) = A \rightarrow A = 0$

$u'(0) = B + C \rightarrow C = 0.$

so

$u(t) = \frac{1}{4} t \sin t$



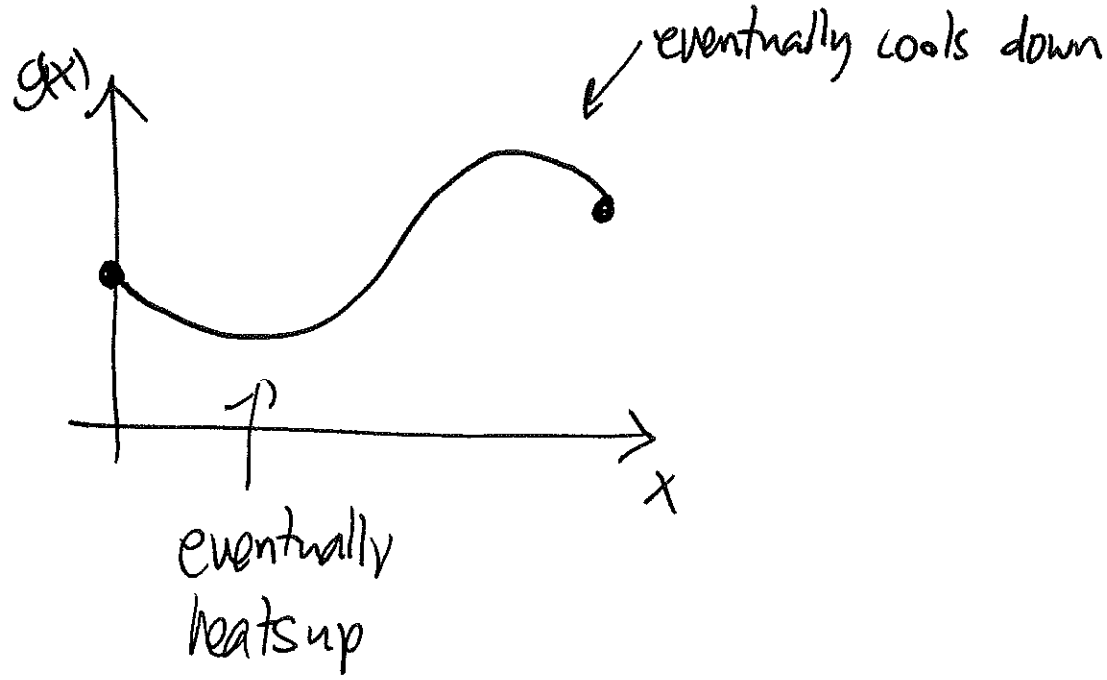
The heat equation

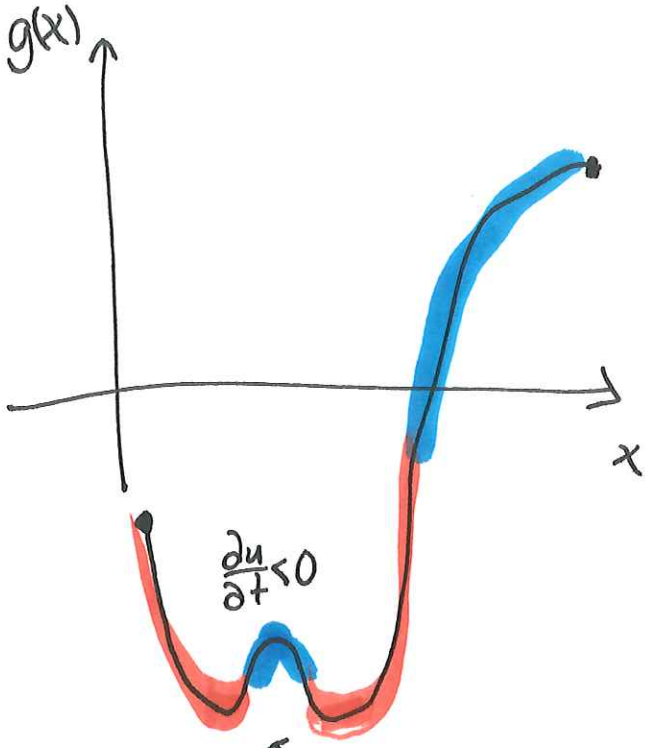
heat initially distributed as a function

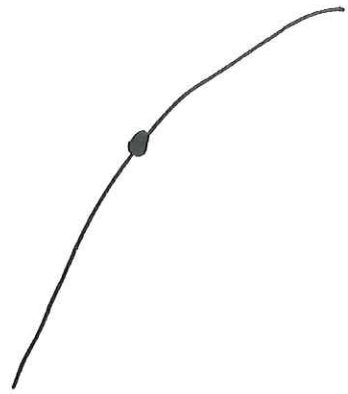
$g(x)$ = temperature at position x on the rod.

What happens when heat starts to flow?

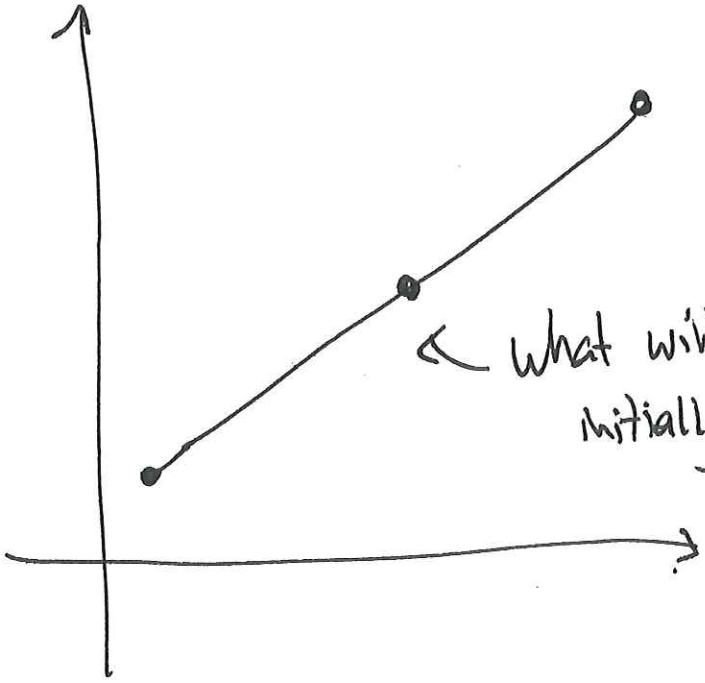
e.g.







this point will initially cool off, then eventually warm up.



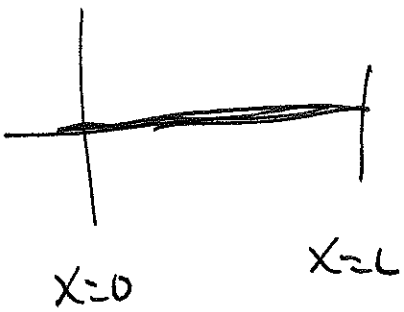
what will happen here initially

Let's hold ends at constant temperature 0.

Let $u(x,t) =$ temperature at position x at time t.

how do we find $u(x,t)$?

we know: $u(x,0) = g(x)$ ← initial condition



$$\left.\begin{aligned} u(0,t) &= 0 \\ u(L,t) &= 0 \end{aligned}\right\} \text{ends at constant temp.}$$

we need an equation for how $u(x,t)$ changes as time increases.

$$\frac{\partial u}{\partial t}(x,t) = \alpha^2 \frac{\partial^2 u}{\partial x^2}(x,t).$$

rate of increase at pt x at time t.

some constant

$u_t = \alpha^2 u_{xx}$ "Heat equation"

"thermal diffusivity"; depends on what rod is made of.

This is a "partial differential equation" has partial derivatives

	cm^2/s
Copper	1.14
aluminum	0.86
iron	0.12
brick	0.0038

$$u_t = \alpha^2 u_{xx}$$

Want to find $u(x,t)$ satisfying this eqn.

Let's try to find some solutions.

To simplify, let's look for "seperable" solutions.

<u>try</u> $u(x,t) = f(x)\, g(t)$

$$\left.\begin{aligned} u_t &= f g_t \\ u_{xx} &= f_{xx} g \end{aligned}\right] \quad \underline{\text{Heat eqn}} \quad f g_t = \alpha^2 f_{xx} g$$

$$\frac{f_{xx}}{f} = \frac{1}{\alpha^2}\frac{g_t}{g}$$

t only

x only

Must both be constant!

Call constant $-\lambda$. (assume $\lambda > 0$)

$$\cancel{f_{xx} = -\lambda f}$$

$$\cancel{g_t}$$

$$f_{xx} + \lambda f = 0 \quad \leftarrow \text{left} = -\lambda$$

$$g_t + \alpha^2 \lambda g = 0 \quad \leftarrow \text{right} = -\lambda$$

Solve separately.

$f(x)$ has

$$f'' = -\lambda f$$

$$f(x) = c_1 \cos(\sqrt{\lambda}\, x) + c_2 \sin(\sqrt{\lambda}\, x)$$

But! We need $f(0) = 0$ and $f(L) = 0$.

For most λ, this is impossible.

But! if $\lambda = \dfrac{n^2 \pi^2}{L^2}$ then

$$f(x) = \sin\left(\frac{n\pi x}{L}\right) \text{ works.}$$

For those λ values,

$$\lambda = \frac{n^2\pi^2}{L^2}$$

the equation

$g_t + \alpha^2 \lambda T = 0$ has solution

$$e^{-n^2\pi^2\alpha^2/(L^2)t}$$

So a solution to the heat eqn is:

$$u_n(x,t) = e^{-\frac{n^2\pi^2\alpha^2}{L^2}t} \sin\left(\frac{n\pi}{L}x\right).$$

for $n = 1, 2, 3, \ldots$

e.g. $L = \pi$, $\alpha^2 = 1$, $n = 1$

$$u(x,t) = e^{-t} \sin(x)$$

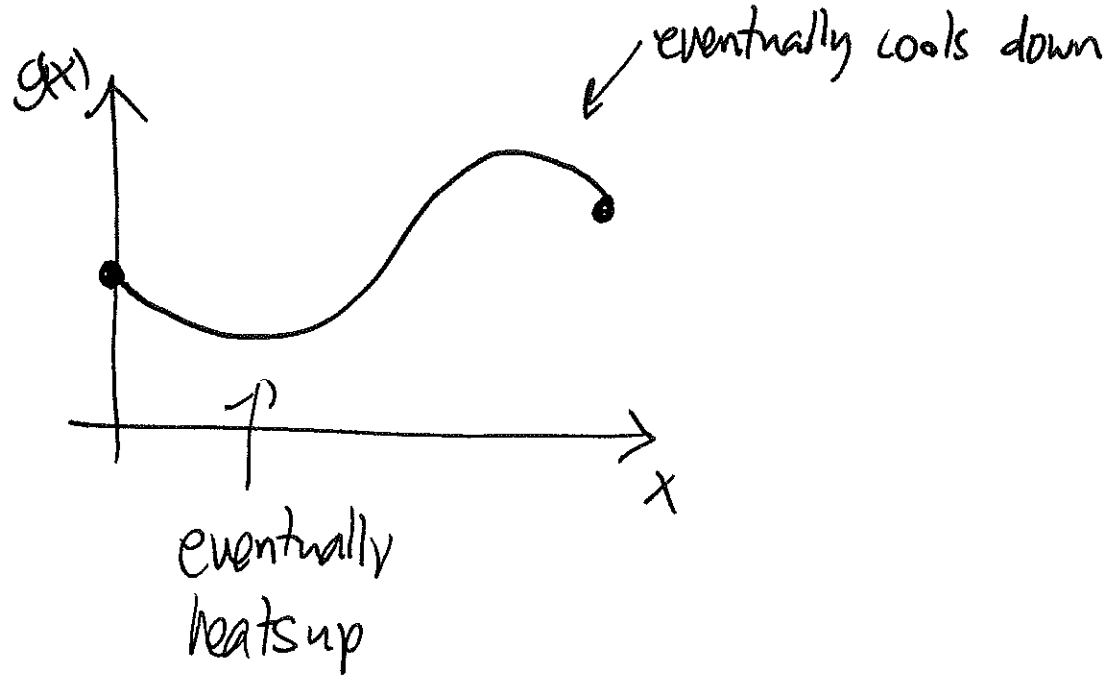
The heat equation

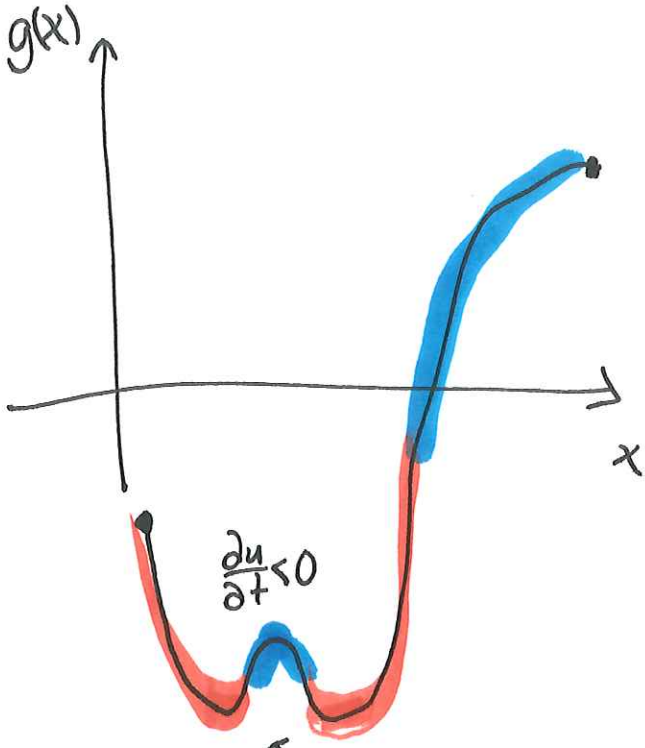
heat initially distributed as a function

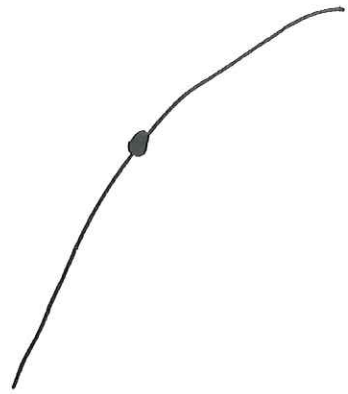
$g(x)$ = temperature at position x on the rod.

What happens when heat starts to flow?

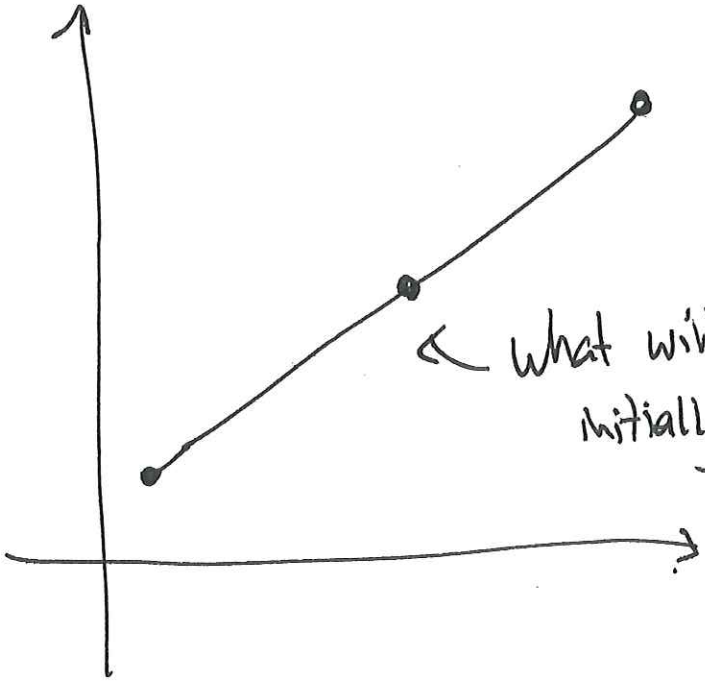
e.g.







this point will initially cool off, then eventually warm up.



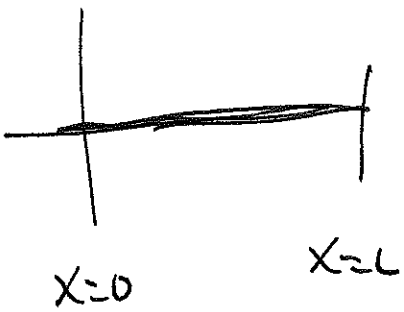
what will happen here initially

Let's hold ends at constant temperature 0.

Let $u(x,t) =$ temperature at position x at time t.

how do we find $u(x,t)$?

we know: $u(x,0) = g(x)$ ← initial condition



$$\left.\begin{aligned} u(0,t) &= 0 \\ u(L,t) &= 0 \end{aligned}\right\} \text{ends at constant temp.}$$

we need an equation for how $u(x,t)$ changes as time increases.

$$\frac{\partial u}{\partial t}(x,t) = \alpha^2 \frac{\partial^2 u}{\partial x^2}(x,t).$$

rate of increase at pt x at time t.

some constant

$u_t = \alpha^2 u_{xx}$ "Heat equation"

"thermal diffusivity"; depends on what rod is made of.

This is a "partial differential equation" has partial derivatives

	cm^2/s
Copper	1.14
aluminum	0.86
iron	0.12
brick	0.0038

$$u_t = \alpha^2 u_{xx}$$

Want to find $u(x,t)$ satisfying this eqn.

Let's try to find some solutions.

To simplify, let's look for "seperable" solutions.

<u>try</u> $u(x,t) = f(x)\, g(t)$

$$\left.\begin{aligned} u_t &= f g_t \\ u_{xx} &= f_{xx} g \end{aligned}\right] \quad \underline{\text{Heat eqn}} \quad f g_t = \alpha^2 f_{xx} g$$

$$\frac{f_{xx}}{f} = \frac{1}{\alpha^2}\frac{g_t}{g}$$

t only

x only

Must both be constant!

Call constant $-\lambda$. (assume $\lambda > 0$)

$$\cancel{f_{xx} = -\lambda f}$$

$$\cancel{g_t}$$

$$f_{xx} + \lambda f = 0 \quad \leftarrow \text{left} = -\lambda$$

$$g_t + \alpha^2 \lambda g = 0 \quad \leftarrow \text{right} = -\lambda$$

Solve separately.

$f(x)$ has

$$f'' = -\lambda f$$

$$f(x) = c_1 \cos(\sqrt{\lambda}\, x) + c_2 \sin(\sqrt{\lambda}\, x)$$

But! We need $f(0) = 0$ and $f(L) = 0$.

For most λ, this is impossible.

But! if $\lambda = \dfrac{n^2 \pi^2}{L^2}$ then

$$f(x) = \sin\left(\frac{n\pi x}{L}\right) \text{ works.}$$

For those λ values,

$$\lambda = \frac{n^2\pi^2}{L^2}$$

the equation

$g_t + \alpha^2 \lambda T = 0$ has solution

$$e^{-n^2\pi^2\alpha^2/(L^2)t}$$

So a solution to the heat eqn is:

$$u_n(x,t) = e^{-\frac{n^2\pi^2\alpha^2}{L^2}t} \sin\left(\frac{n\pi}{L}x\right).$$

for $n = 1, 2, 3, \ldots$

e.g. $L = \pi$, $\alpha^2 = 1$, $n = 1$

$$u(x,t) = e^{-t} \sin(x)$$

Today: More Heat Equation (+ demos)

Initial temperature $g(x)$ (as a function of x, $0 \le x \le L$)

Hold ends at $0°$, let ~~temp~~ heat flow.

$g(0) = g(L) = 0$.

Let $u(x,t)$ = temp at position x at time t

we want to figure out

$$\frac{\partial}{\partial t} u(x,t) = \alpha^2 \frac{\partial^2}{\partial x^2} u(x,t)$$

constant

We want to find a function $u(x,t)$ satisfying:

- $u(x,0) = g(x)$ (initial temp) known
- $u(0,t) = 0$
- $u(L,t) = 0$
- $u_t = \alpha^2 u_{xx}$

Last time: Here ~~so~~ are some solutions:

1) $u_1(x,t) = e^{-\frac{\pi^2\alpha^2}{L^2}t} \sin\left(\frac{\pi x}{L}\right)$

2) $u_2(x,t) = e^{-\frac{4\pi^2\alpha^2}{L^2}t} \sin\left(\frac{2\pi x}{L}\right)$

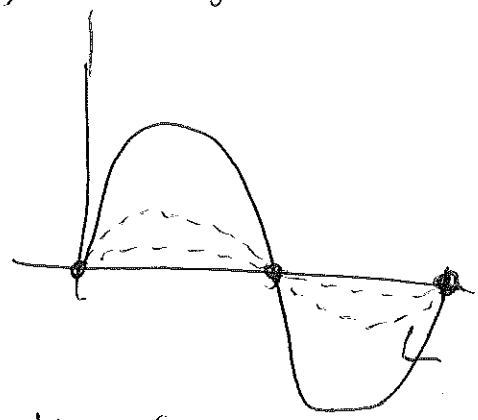
...

$$\boxed{n)\ u_n(x,t) = e^{-\frac{n^2\pi^2\alpha^2}{L^2}t} \sin\left(\frac{n\pi x}{L}\right)}$$

Check:

$$u_n(x,t) = e^{-\frac{n^2\pi^2\alpha^2}{L^2}t} \sin\left(\frac{n\pi x}{L}\right)$$

eg. $n=2$



- $u_n(x,0) = \sin\left(\frac{n\pi x}{L}\right)$

this describes evolution of temp when initial temp is $\sin\left(\frac{n\pi x}{L}\right)$

- $u_n(0,t) = u_n(L,t) = 0.$ ✓

If.

let $L=\pi$.

If our initial condition was

$$\sin(x) \xrightarrow{\text{sol is}} e^{-\alpha^2 t}\sin(x)$$

$$\sin(2x) \xrightarrow{\text{sol}} e^{-4\alpha^2 t}\sin(2x)$$

$$\sin(3x) \xrightarrow{\text{sol}} e^{-9\alpha^2 t}\sin(3x)$$

If initial condition is

$7\sin(x)-3\sin(2x)$, solution is:

$$u(x,t)=7e^{-\alpha^2 t}\sin(x)-3e^{-4\alpha^2 t}\sin(2x)$$

Given an initial condition $g(x)$,

Write Fourier series:

$$g(x) = \sum_{n=1}^{\infty} b_n \sin(nx).$$

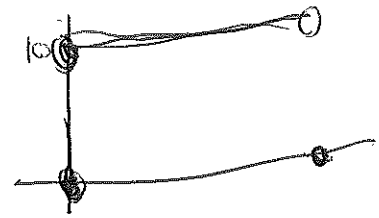
Then solution to heat eqn is

$$\cancel{u(x,t) = \sum_{n=1}^{\infty} b_n e^{-n^2 \pi^2 \alpha^2 t}}$$

$$\boxed{u(x,t) = \sum_{n=1}^{\infty} b_n e^{-n^2 \alpha^2 t} \sin(nx).}$$

Questions

$\boxed{\alpha^2 = 1}$ $\boxed{L = \pi}$



1) A rod is heated to temperature $10°$ C.

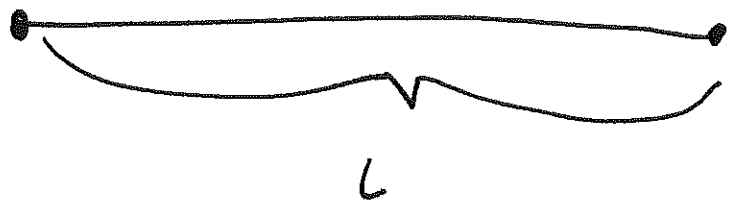
How long until $u(x,t) < 1°$ C for all x?

2) Can you come up with a initial temp function so it warms up in the middle, then cools off?

3) What happens if initial function $g(x)$ doesn't have $g(0) = 0$?

4) ~~How can~~

Pluck a string:



$u(x,t)$ = displacement of the string at horizontal position x and time t.

Physics: $\cancel{\rho \frac{\partial^2 u}{\partial t^2} = u_{xx}}$

T = tension

ρ = density of string

$$\frac{\partial^2 u}{\partial t^2}(x,t) = c^2 \frac{\partial^2 u}{\partial x^2}(x,t) \qquad c = \sqrt{\frac{T}{\rho}}$$

$$u_{tt} = c^2 u_{xx} \qquad u(0,t) = u(L,t) = 0$$

$$u_{tt} = c^2 u_{xx}$$

Assume $u(x,t) = f(x)\, g(t)$: try to find solutions of this form first.

$$f g_{tt} = c^2 f_{xx} g$$

f is function of only x,
g is function of only t!

$$\cancel{\frac{g_{tt}}{g}} \quad \frac{f_{xx}}{f} = \frac{1}{c^2} \frac{g_{tt}}{g}$$

function of only t!

function of only x!

both sides must equal a constant, $-\lambda$.

$$f(0) = f(L) = 0$$

$$\frac{f_{xx}}{f} = -\lambda$$

$$f'' + \lambda f = 0$$

$$f(x) = c_1 \cos(\sqrt{\lambda}\, x) + c_2 \sin(\sqrt{\lambda}\, x)$$

$f(0)=0$ says $\quad c_1 + 0 = c_1 = 0 \quad$ so $c_1 = 0$

so $f(x) = c_2 \sin(\sqrt{\lambda}\, x)$

$f(L)=0$ says $\quad c_2 \sin(\sqrt{\lambda}\, L) = 0$

this would tell us $c_2 = 0$ so $f(x)=0$ (boring!)

<u>unless</u> $\sin(\sqrt{\lambda}\, L) = 0$ which happens for special λ values.

$\sqrt{\lambda} L = n\pi$

$\lambda L^2 = n^2 \pi^2$

$\lambda = \dfrac{n^2 \pi^2}{L^2}$.

solution is

$$f(x) = c_2 \sin\left(\frac{n\pi}{L} x\right).$$

(for any integer $n \geq 1$)

Now we need to solve

$$\frac{1}{c^2}\frac{g_{tt}}{g} = -\lambda \quad \text{where} \quad \lambda = \frac{n^2\pi^2}{L^2}$$ (for other λ, the f eqn has no sols!)

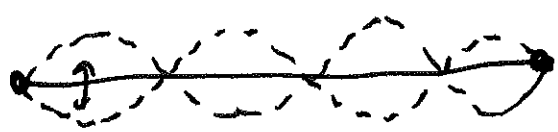
$$g(t) = \cos\left(\frac{n\pi c}{L}t\right)$$

Putting it together:

$$u_n(x,t) = \sin\left(\frac{n\pi}{L}x\right)\cos\left(\frac{n\pi c}{L}t\right).$$

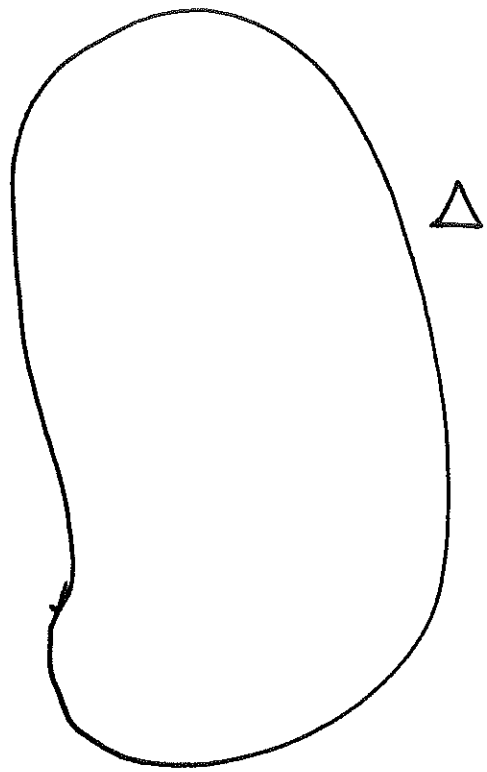
frequency $\frac{nc}{2L}$

$$c = \sqrt{\frac{\text{Tension}}{\text{density}}}$$



The sound of a string will be a combination of $u_n(x,t)$ all added together. What frequencies do we hear?

$$\underset{u_1}{\frac{c}{2L}}, \quad \underset{u_2}{\frac{2c}{2L}}, \quad \underset{u_3}{\frac{3c}{2L}}$$



drum in shape Δ.

what frequencies show up when we hit it?

(it depends on Δ)

You can set up a function $u(x, y, t)$

$$u_{tt} = c^2(u_{xx} + u_{yy}) = c^2 \Delta u$$

"Laplacian of u"

<u>Wave eqn for drum:</u>

$$u_{tt} = c^2 \Delta u$$

If f is function f where

$$\Delta f = \lambda f$$

multiple of f,

then λ is called "eigenvalue of Laplacian"

and it's a frequency of the drum!

The sound of the drum is determined

by the set of eigenvalues of laplacian (depends on Δ)
shape.

<u>Q</u> Can you hear shape of a drum?

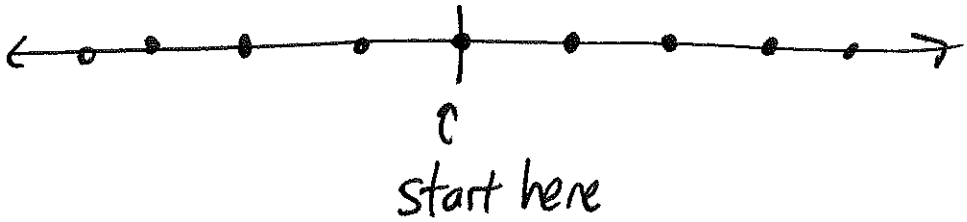
(Can two different shapes yield the same λ values?)

<u>A</u> Two drums <u>can</u> produce the same

frequencies!

Random walks

1D.



- move left or right with probability $1/2$.
- Q: what's the probability you get back to 0 eventually?
- warm-up: what's the probability you get back to 0 after exactly n steps?

  (what if $n=4$?)

What's the chance you're back after n steps?

If n is odd: 0. You need to have made same number of L and R.

If n is even:

Total number of length n strings with L&R:

$$2^n$$

Total number that get you back to 0: need the same number of L & R

$n=2m$. then

$$\underbrace{LLLL}_{n/2}\ \underbrace{RRRR}_{n/2} \qquad \frac{(2m)!}{m!\ m!} = \binom{2m}{m}$$

The chance we're back is $u_{2m} = \dfrac{\binom{2m}{m}}{2^{2m}}$

Now look at

$$S = \sum_{m=1}^{\infty} \frac{1}{2^{2m}} \binom{2m}{m}$$

this tells us: the expected number of times our random path comes back to 0.

If walk is guaranteed to return: $S = \infty$

sum diverges

if not: S is finite

sum converges.

$$S = \sum_{m=1}^{\infty} \frac{1}{2^{2m}} \binom{2m}{m} = \sum_{m=1}^{\infty} \frac{1}{2^{2m}} \frac{(2m)!}{m!\, m!}$$

Stirling's approximation:

$$n! \approx \sqrt{2\pi n}\, e^{-n} n^n$$

$$\sum_{m=1}^{\infty} \frac{1}{2^{2m}} \frac{(2m)!}{m!\,m!} = \cancel{\sum_{m=1}}$$

$$\frac{1}{2^{2m}} \frac{(2m)!}{m!\,m!} \approx \frac{1}{2^{2m}} \frac{\sqrt{4\pi m}\, e^{-2m} (2m)^{2m}}{\left(\sqrt{2\pi m}\, e^{-m} m^m\right)^2}$$

$$= \cancel{\frac{1}{2^{2m}}} \frac{\sqrt{4\pi m}}{\left(\sqrt{2\pi m}\right)^2} \cdot \frac{e^{-2m}}{\left(e^{-m}\right)^2} \cdot \frac{1}{2^{2m}} \frac{(2m)^{2m}}{\left(m^m\right)^2}$$

$$= \frac{1}{\sqrt{\pi m}} \cdot 1 \cdot 1$$

$$\sum_{m=1}^{\infty} \frac{1}{2^{2m}} \frac{(2m)!}{m!\,m!} \approx \sum_{m=1}^{\infty} \frac{1}{\sqrt{\pi m}}$$

diverges!

random walk comes back!

Last time:

Random walk:

Let $u_n =$ probability of coming back to 0 after n steps

~~= (last time) = 1/4~~ Last time: $u_{2n} = \left(\frac{1}{4}\right)^{2n}\binom{2n}{n}$.

* If $\sum u_n < \infty$ then the walk may not ever return
If $\sum u_n = \infty$ then guaranteed to return.

Last time: $\sum \left(\frac{1}{4}\right)^{2n}\binom{2n}{n}$ diverges (use Stirling's approx)

*

Suppose that some kind of random walk eventually comes back to 0 with probability u. (or disappears forever with prob $1-u$).

What's the probability that it returns to 0 exactly m times?

it's $u^m(1-u)$.

What's the expected number of returns (as a fct of u)

$$\sum_{m=0}^{\infty} \underbrace{m}_{\#\text{times}} \underbrace{\left(u^m(1-u)\right)}_{\text{prob of that number of times.}}$$

$$(1-u)\sum_{m=0}^{\infty} mu^m = u(1-u)\sum_{m=0}^{\infty} mu^{m-1}$$

$$= u(1-u)\frac{d}{du}\left(\sum_{m=0}^{\infty} u^m\right) \leftarrow \text{geometric}$$

$$= u(1-u)\frac{d}{du}\frac{1}{1-u}$$

$$= u(1-u)\frac{1}{(1-u)^2}$$

$$= \frac{u}{1-u}.$$

Expected number of returns is finite if $u<1$

Infinite if $u=1$.

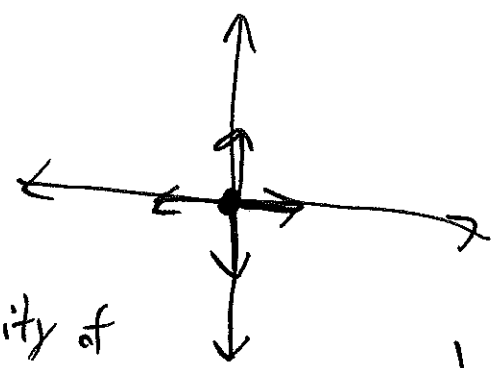
Three things to try:

a) What if we use a 1-D random walk,

but go left with probability p &
right with prob. $1-p$.

What is u_n? Does $\sum u_n$ converge?

b) What about 2D?



What is u_n? (Probability of coming back after exactly n steps.)

Does $\sum u_n$ converge?

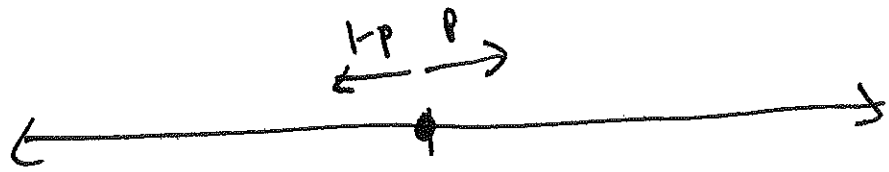
Hint: $\sum_{k=0}^{n} \binom{n}{k}^2 = ?$

It can be simplified!

c) Program it!

(draw some pictures of 2D walks. how far do you go before coming back?) try 3D and see if it comes.

More random walks



$p = 1/2$ comes back.

What about other p?

Chance of return after n steps is u_n:

$$u_{2n} = \binom{2n}{n} p^n (1-p)^n$$

total number of possible paths.

LRLLLRRLRR ← $2n$ symbols, with equal number left & right.

$$(1-p)\cdot p\,(1-p)\,(1-p)\,(1-p)\,p\;p = p^n(1-p)^n$$

$$\frac{(2n)!}{n!\,n!} = \binom{2n}{n}$$

Does

$$\sum_{n=1}^{\infty} \binom{2n}{n} p^n (1-p)^n \text{ converge?}$$

$$\sum_{n=1}^{\infty} \binom{2n}{n} p^n (1-p)^n$$

$\frac{(2n)!}{n!\,n!}$

$(2n)^{2n} = 2^{2n} \cdot n^{2n}$

$(n^n)^2 = n^{2n}$

Stirling: $n! = n^n e^{-n} \sqrt{2\pi n}$

$$\sum_{n=1}^{\infty} \frac{(2n)^{2n} \cdot e^{-2n} \sqrt{2\pi \cdot 2n}}{(n^n e^{-n} \sqrt{2\pi n})^2} p^n (1-p)^n$$

$$= \sum_{n=1}^{\infty} 2^{2n} \frac{1}{\sqrt{n}} p^n (1-p)^n \frac{1}{\sqrt{\pi}}$$

$$= \frac{1}{\sqrt{\pi}} \sum_{n=1}^{\infty} (4p(1-p))^n \frac{1}{\sqrt{n}}$$

Ratio test: For a sum $\sum_{n=1}^{\infty} a_n$,

if $\lim_{n\to\infty} \left| \frac{a_{n+1}}{a_n} \right| < 1$, converges.

(if > 1, diverges, if $= 1$, try another test)

If $a_n = (4p(1-p))^n \frac{1}{\sqrt{n}}$

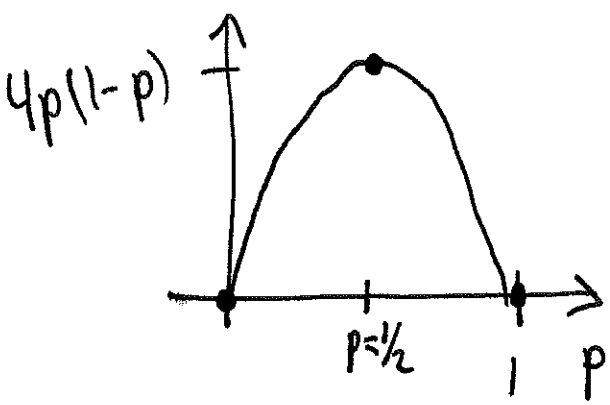
then

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \frac{(4p(1-p))^{n+1} \frac{1}{\sqrt{n+1}}}{(4p(1-p))^n \frac{1}{\sqrt{n}}} = \lim_{n\to\infty} 4p(1-p)\sqrt{\frac{n}{n+1}}$$

$$= 4p(1-p).$$

If $4p(1-p) < 1 \Rightarrow \sum u_{2n}$ converges $\Rightarrow$ lost forever

But which values of p is that? When is $4p(1-p) < 1$?

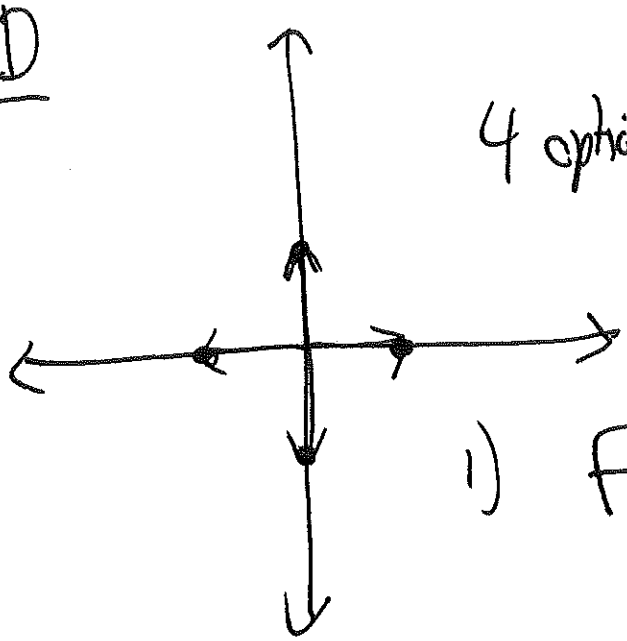


Conclusion about random walks:

$p = 1/2$ must come back

any other p values: maybe not!

2D



4 options, equal prob.

1) Find u_{2n} = chance of being back after $2n$ steps

[First: how many length $2n$ paths are there that end at $(0,0)$?

How many length $2n$ paths are ending at $(0,0)$ using exactly R rights? $(0 \le R \le n)$

→ also R lefts

→ $n-R$ ups

→ $n-R$ downs.

u_{2n}^{R}

not probability, number of paths, sorry!

$$u_{2n}^{R} = \frac{(2n)!}{R!\,R!\,(n-R)!\,(n-R)!}$$

So

$$\#\text{paths} = \sum_{R=0}^{n} u_{2n}^{R} = \sum_{R=0}^{n} \frac{(2n)!}{R!\,R!\,(n-R)!\,(n-R)!}$$

Probability of following a particular path: $\left(\frac{1}{4}\right)^{2n}$

probability

$$u_{2n} = \left(\frac{1}{4}\right)^{2n} \sum_{R=0}^{n} \frac{(2n)!}{R!\,R!\,(n-R)!\,(n-R)!} = \left(\frac{1}{4}\right)^{2n} \sum_{R=0}^{n} \frac{(2n)!\,n!\,n!}{R!\,R!\,(n-R)!\,(n-R)!\,n!\,n!}$$

$$= \left(\frac{1}{4}\right)^{2n} \sum_{R=0}^{n} \frac{(2n)!\,n!\,n!}{R!\,R!\,(n-R)!\,(n-R)!\,n!\,n!}$$

$$= \left(\frac{1}{4}\right)^{2n} \sum_{R=0}^{n} \binom{2n}{n}\binom{n}{R}\binom{n}{R} = \left(\frac{1}{4}\right)^{2n} \binom{2n}{n} \sum_{R=0}^{n} \binom{n}{R}^2$$

$$= \left(\frac{1}{4}\right)^{2n} \binom{2n}{n}^2$$

What is

$$\sum_{k=0}^{n} \binom{n}{k}^2$$

$$\begin{array}{lllllll}
 & & & 1 & & & \longrightarrow 1 \\
 & & 1 & & 1 & & \longrightarrow 2 \\
 & 1 & & 2 & & 1 & \longrightarrow 6 \\
1 & & 3 & & 3 & & 1 \longrightarrow 20 \\
1 & 4 & & 6 & & 4 & 1 \longrightarrow 70 \\
1 & 5 & 10 & & 10 & 5 & 1 \longrightarrow 252 \\
1 & 6 & 15 & 20 & 15 & 6 & 1
\end{array}$$

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

(prove by induction, or generating functions, ...)

Does

$$\sum u_{2n} = \sum \left(\frac{1}{4}\right)^{2n} \binom{2n}{n}^2 \text{ converge?}$$

Stirling's formula! $\lim_{n\to\infty} \frac{n!}{n^n e^{-n}\sqrt{2\pi n}} = 1$

$$\left(\frac{1}{4}\right)^{2n} \binom{2n}{n}^2 \approx \left(\frac{1}{4}\right)^{2n} \frac{\left((2n)^{2n} e^{-2n} \sqrt{2\pi 2n}\right)^2}{\left(n^n e^{-n} \sqrt{2\pi n}\right)^4}$$

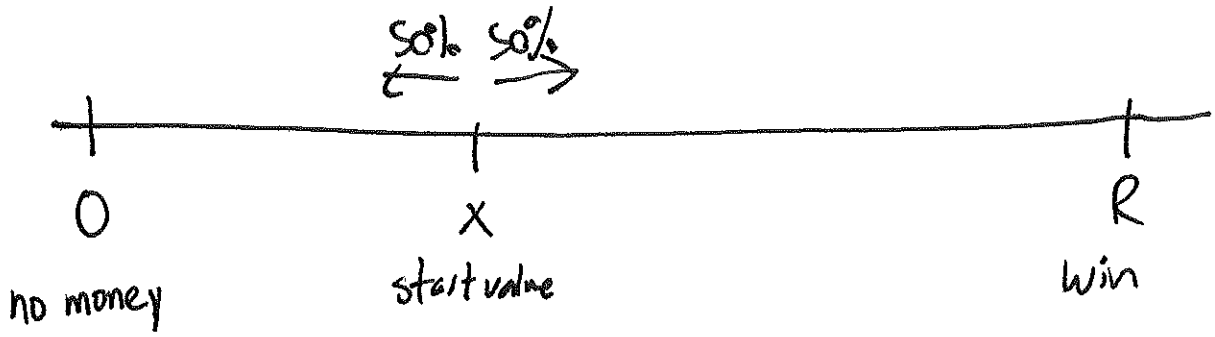
$$= \cancel{\left(\frac{1}{4}\right)^{2n}} = \frac{1}{\pi n}$$

$$\sum u_{2n} \approx \sum \frac{1}{\pi n} \text{ diverges!}$$

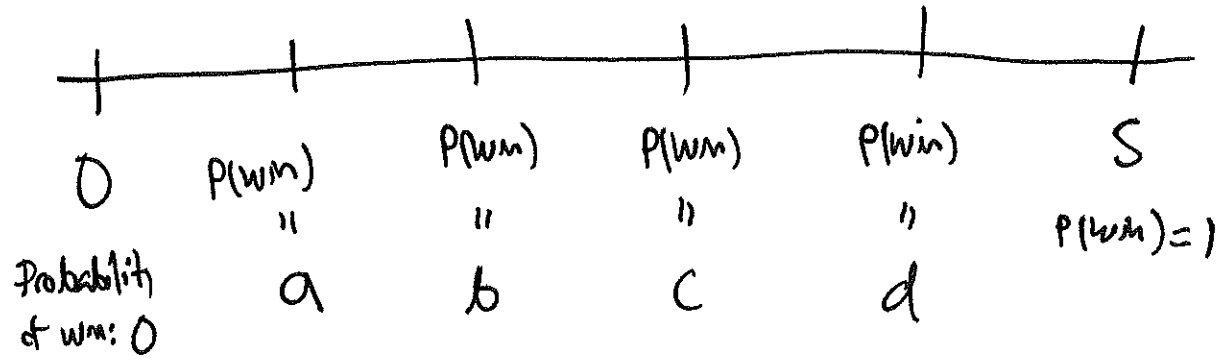
Random walk comes back infinitely many times!

(But it might take a long time!)

Gambler's ruin.



What's the chance the gambler gets to R before getting to 0?



Solve for a, b, c, d!

But we need equations!

$$a = \frac{1}{2}\cdot 0 + \frac{1}{2}\cdot b$$

$$b = \frac{1}{2}\cdot a + \frac{1}{2}\cdot c$$

$$c = \frac{1}{2}\cdot b + \frac{1}{2}\cdot d$$

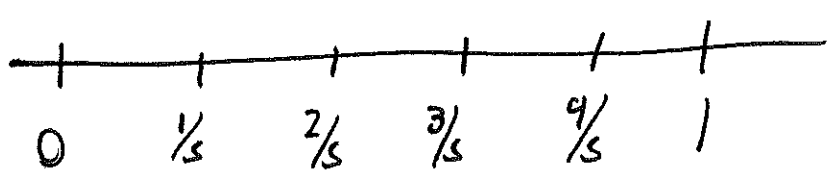
$$d = \frac{1}{2}\cdot c + \frac{1}{2}\cdot 1$$

4 eqns
4 vars

$$\left.\begin{aligned} 2a - b &= 0 \\ 2b - a - c &= 0 \\ 2c - b - d &= 0 \\ 2d - c - 1 &= 0 \end{aligned}\right\}$$

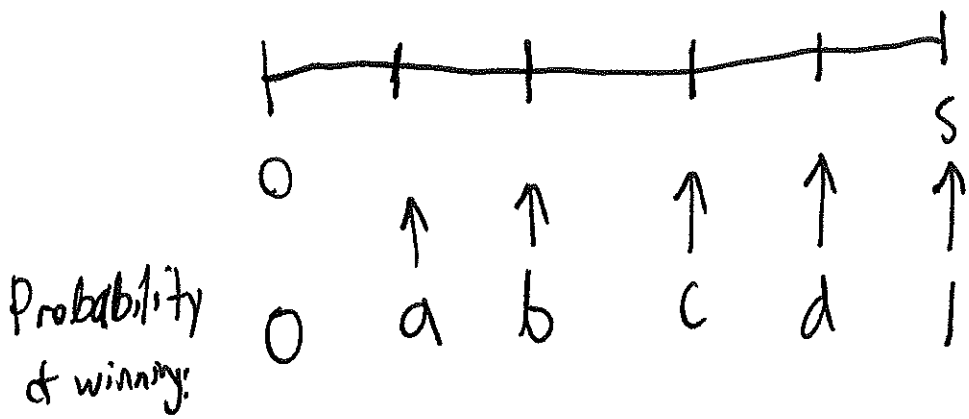
$$\left(\begin{array}{cccc|c} 2 & -1 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & 1 \end{array}\right)$$

$a = 1/5 \quad b = 2/5 \quad c = 3/5 \quad d = 4/5$



Today: Finish random walks, start calculus of variations

Try: Gambler's ruin with weights



Probability

losing $= p$

winning $= 1-p$

$$a = p\cdot 0 + (1-p)\,b$$

$$b = p\cdot a + (1-p)\,c$$

$$c = p\cdot b + (1-p)\,d$$

$$d = p\cdot c + (1-p)\cdot 1$$

Solve linear eqns

$$a = \frac{16}{211},\quad b = \frac{40}{211},\quad c = \frac{76}{211},\quad d = \frac{130}{211}$$

$p = 0.6$

3D random walk.

Compute

$u_{2n} = (\cdots)$ probability of coming back, by counting paths.

Answer is a mess, double $\sum\sum$, can't simplify it.

Q. Does $\sum u_{2n}$ converge?

Inequality tricks (Jensen's):

$u_{2n} \leq \frac{C}{n^{3/2}}$ so because $\sum \frac{1}{n^{3/2}}$ converges

$\Rightarrow \sum u_{2n}$ converges, and so random walk may never come back!

Polya's Random Walk Theorem

In dimension 1, 2, a fair random walk always returns to start.

In dim ≥ 3, it might not!

You can define a continuous-time version of random walk, a "Wiener process."

This is a good model for Brownian motion, maybe the stock market.

Reminder

Multivariable chain rule.

$$f(x,y) = x^3 y + y$$

$$x(s) = 1 + 2s$$

$$y(s) = 3 - 4s.$$

What's $\frac{df}{ds}$? If you change s by a little, how much does f change?

$$\boxed{\frac{df}{ds} = \frac{\partial f}{\partial x}\frac{dx}{ds} + \frac{\partial f}{\partial y}\frac{dy}{ds}}$$

Increase s by Δs, then x increases by $\frac{dx}{ds}\Delta s = \Delta x$

y increase by $\frac{dy}{ds}\Delta s = \Delta y$.

For f: x increases by Δx, which

makes f increase by $\frac{\partial f}{\partial x} \Delta x$

y increases by Δy, which makes

f increase by $\frac{\partial f}{\partial y} \Delta y$.

Total change in f is:

$$\frac{\partial f}{\partial x} \Delta x + \frac{\partial f}{\partial y} \Delta y = \frac{\partial f}{\partial x} \frac{dx}{ds} \Delta s + \frac{\partial f}{\partial y} \frac{dy}{ds} \Delta s$$

$$\boxed{\frac{df}{ds} = \frac{\partial f}{\partial x} \frac{dx}{ds} + \frac{\partial f}{\partial y} \frac{dy}{ds}.}$$

$$\frac{\partial f}{\partial x} = 3x^2 y$$

$$\frac{dx}{ds} = 2$$

$$\frac{\partial f}{\partial y} = x^3 + 1$$

$$\frac{dy}{ds} = -4$$

$$\frac{df}{ds} = \frac{\partial f}{\partial x}\frac{dx}{ds} + \frac{\partial f}{\partial y}\frac{dy}{ds}$$

$$= (3x^2 y)(2) + (x^3+1)(-4).$$

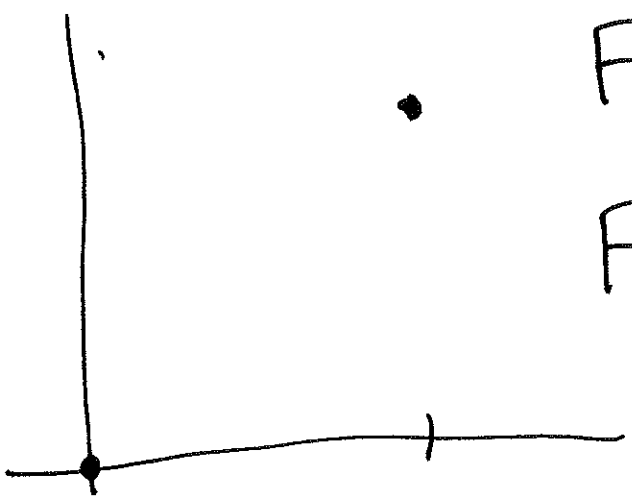
~~Next of variations~~

Next: Calculus of variations.

Let's say you're trying to find a function $y(x)$ that minimizes a

<u>functional</u> F.

takes a function as input, gives a number as output.



Find y that minimizes

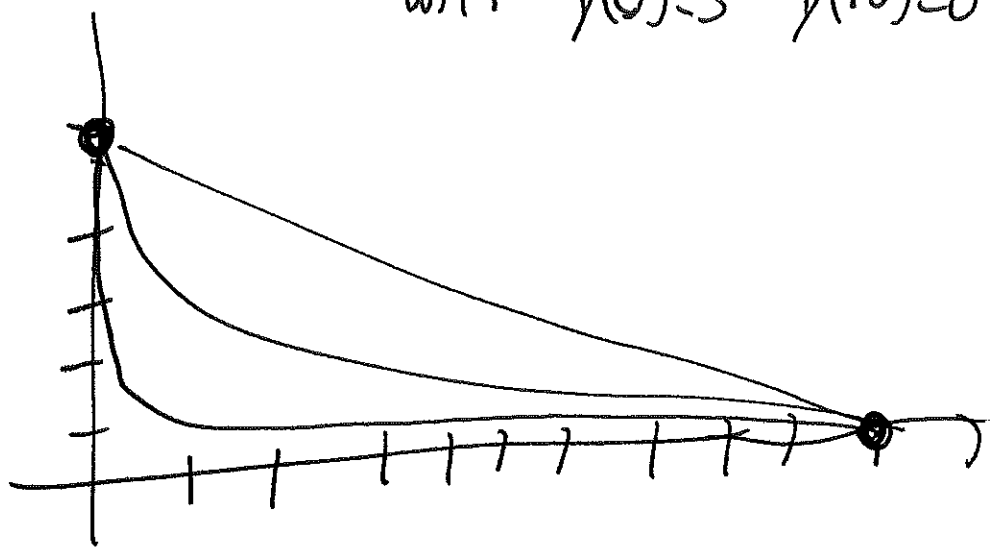
$$F(y) = \int_0^1 \sqrt{1+y'(x)^2}\, dx$$

with $y(0)=0$ and $y(1)=1$.

i.e. Find shortest path from $(0,0)$ to $(1,1)$.

or: let $F(y) = \left(\begin{array}{l}\text{the amount of time it takes a} \\ \text{ball to roll from } (0,5) \text{ to } (10,0) \\ \text{along the graph of } y\end{array}\right)$

with $y(0)=5 \quad y(10)=0$

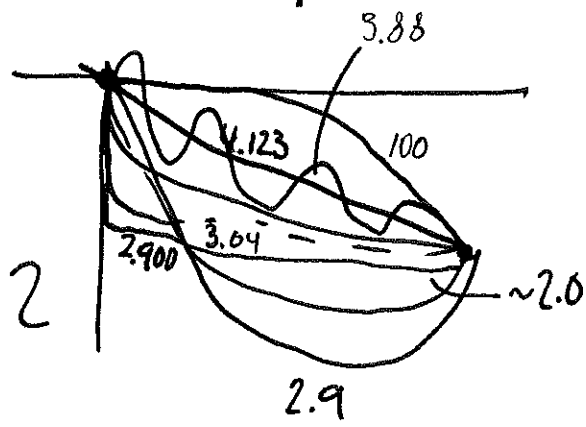


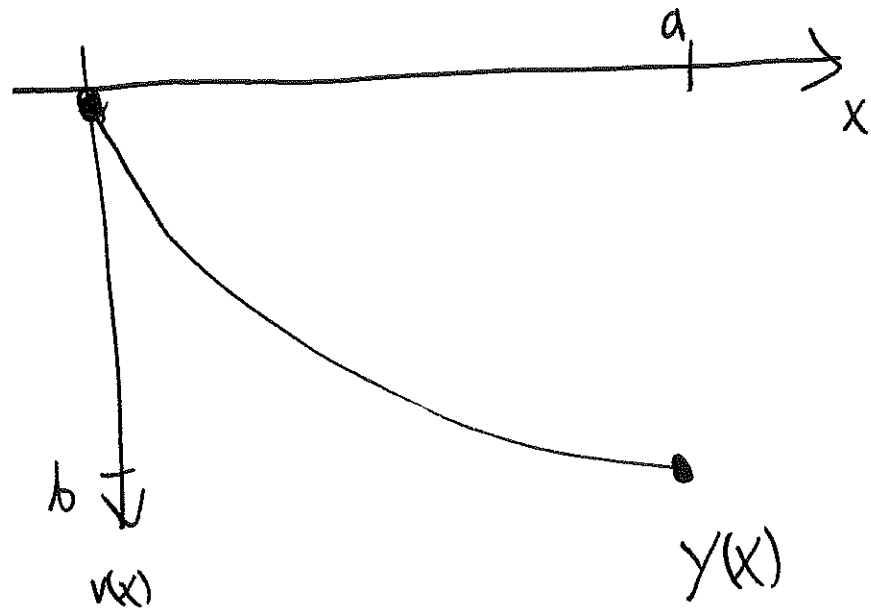
"brachistochrone problem"

$(0,0)$ to $(20,-5)$

$\dfrac{-5\log(x+1)}{\log(21)}$ | 2.9

y	$F(y)$ = time		
$-\sqrt{x}\,\frac{5}{\sqrt{20}}$ $\quad -x/4$	4.123	$\frac{(x-20)^2}{80} - 5$	3.32
$-\sqrt{x}\,\frac{\sqrt{20}}{4}$	3.04	$-\sqrt[4]{x}\,\frac{5}{\sqrt[4]{20}}$	
$-\frac{x^2}{80}$	100		
$-x^{3.5}/20^3$	10^{15}	$-\sqrt[1000]{x}\,\frac{5}{\sqrt[1000]{20}} \sim 2$	





How long to roll from (0,0) to (a,b) along this graph?

First: velocity as a function of y:

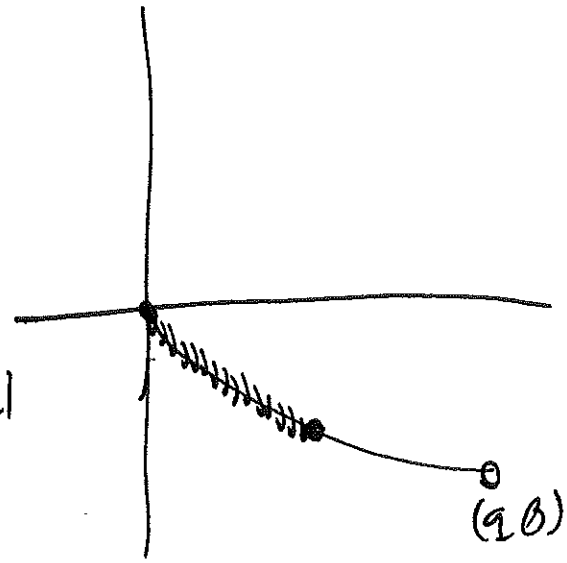
$$\underbrace{\frac{1}{2} m v(x)^2}_{\text{kinetic}} = \underbrace{mg\, y(x)}_{\Delta\text{ potential}}$$

$$v(x) = \sqrt{2g\, y(x)}$$

Let $s(x)$ be length of path from 0 to x.

arc length:

$$s(x) = \int_0^x \sqrt{1+y'(\tilde{x})^2}\, d\tilde{x}$$



$$\frac{ds}{dx} = \sqrt{1+y'(x)^2}$$ fundamental theorem

Total length:

$$L = \int_0^a \sqrt{1+y'(x)^2}\, dx$$

Now: want to take time as our variable:

$$v(t) = \frac{ds}{dt}$$

Total time:

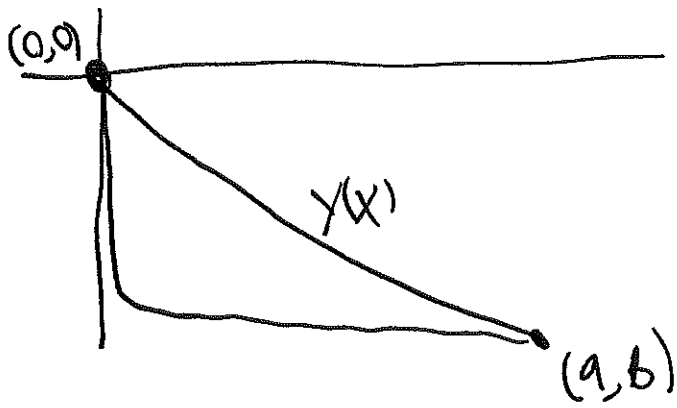
$$T = \int_0^T dt = \int_0^L \frac{1}{v(s)}\, ds = \int_0^a \frac{1}{\sqrt{2g\, y(x)}} \sqrt{1+y'(x)^2}\, dx$$

Final formula:

$$F(y) = \int_0^a \frac{\sqrt{1+y'(x)^2}}{\sqrt{2g\,y(x)}}\,dx$$

want to find y minimizing this

The brachistochrone



Last time: the amount of time it takes

is

$$F(y) = \int_0^a \frac{\sqrt{1+y'(x)^2}}{\sqrt{2g\,y(x)}}\,dx$$

want to find y satisfies $y(0)=0$, $y(a)=b$

which minizes F ("functional")

The idea:

To minimize $f(x,y,z)$:

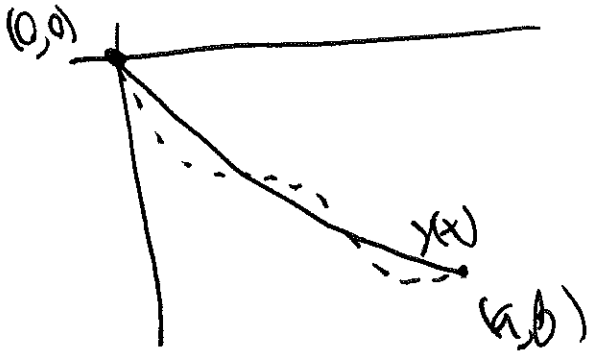
Find a point that make

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0.$$

"moving in x-direction doesn't make things better".

To minimize a functional $F(f)$ find f that can't be improved.

We want: no way to perturb f and make F get smaller.



one way to perturb:

add $\epsilon \cdot \sin\left(\frac{2\pi}{a}x\right)$

need $\frac{2\pi}{a}x$ to make sure our perturbed fct still goes through (a,b)

look at $y(x) + \epsilon \sin\left(\frac{2\pi}{a}x\right)$ is it better?

We could also try perturbing

$$y(x) + \epsilon \underbrace{x(x-a)}_{0 \text{ at } x=0 \text{ and } x=a}$$

In fact, [Calc break]

We found.
Perturbing a line usually makes it better.

We can perturb $y(x)$ not just by $\sin(\frac{2\pi}{a}x)$ or $x(x-a)$,

but by any function v with $v(0)=v(a)=0$

The <u>variation of functional</u> F in direction v is:

$$\delta F(y;v) = \lim_{\epsilon \to 0} \frac{1}{\epsilon}\left(F(y+\epsilon v) - F(y)\right) = \frac{d}{d\epsilon} F(y+\epsilon v)\Big|_{\epsilon=0}$$

If $\delta F(y;v)$ not 0, perturbing y by v improves it!

If a function $y(x)$ is minimizer of F,

then

$$\delta F(y;v) = 0 \text{ for } \underline{\text{all}} \ v \text{ with } v(a)=0 \text{ and } v(b)=0.$$

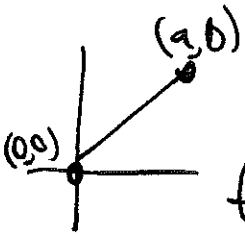
(But how to find y?)
(It's hard in general!)

<u>Euler-Lagrange equations.</u>

Suppose that the functional F looks like

$$F(y) = \int_0^a f(x, y, y')\, dx. \quad \text{(common in physics!)}$$

e.g. for brachistochrone: $F(y) = \int_0^a \underbrace{\frac{\sqrt{1+y'(x)^2}}{\sqrt{2gy(x)}}}_{f(x,y,y')} dx$



for shortest path $F(y) = \int_0^a \sqrt{1+y'(x)^2}\, dx$

Suppose

$$F(y) = \int_0^a f(x, y, y')\, dx$$

$$\delta F(y; v) = \frac{d}{d\epsilon}\Big(F(y + \epsilon v) \Big)\Big|_{\epsilon=0}$$

$$= \frac{d}{d\epsilon} \int_0^a f(x, y(x) + \epsilon v(x), y'(x) + \epsilon v'(x))\, dx \Big|_{\epsilon=0}$$

$$= \int_0^a \frac{d}{d\epsilon} f(x, y(x) + \epsilon v(x), y'(x) + \epsilon v'(x))\, dx \Big|_{\epsilon=0}$$

$$= \int_0^a \frac{\partial}{\partial y} f(x, y(x), y'(x))\, v(x)\, dx + \int_0^a \frac{\partial}{\partial y'} f(x, y(x), y'(x))\, v'(x)\, dx$$

$$= \int_0^a \frac{\partial}{\partial y} f(x, y(x), y'(x))\, v(x)\, dx - \int_0^a \frac{d}{dx}\frac{\partial}{\partial y'} f(x, y(x), y'(x))\, v(x)\, dx$$

$$= \int_0^a v(x) \left(\frac{\partial f}{\partial y} - \frac{d}{dx}\frac{\partial f}{\partial y'} \right) dx$$

If $y(x)$ is optimal, then this integral must be 0

for <u>any</u> v. $\frac{\partial f}{\partial y} - \frac{d}{dx}\frac{\partial f}{\partial y'}$ must be 0!

If y optimizes the functional

$$F(y) = \int_0^a f(x, y, y')\, dx$$

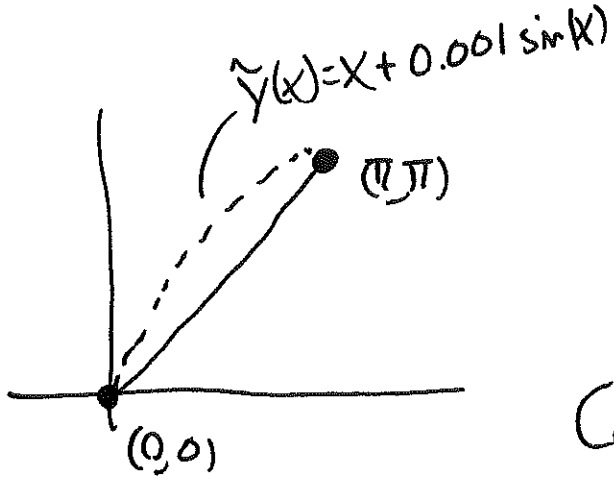
then

$$\frac{\partial}{\partial y} f(x, y, y') = \frac{d}{dx}\frac{\partial}{\partial y'} f(x, y, y').$$

ie. $$\boxed{\frac{\partial f}{\partial y} = \frac{d}{dx}\frac{\partial f}{\partial y'}.}$$

Euler-Lagrange eqn.

Shortest path.



Consider the initial path

$y(x) = x.$

Could perturbing this by $\sin(x)$ give a shorter path?

Compute

$$\delta F(y; \sin x) \quad \text{where} \quad f(x, y, y') = \sqrt{1 + y'(x)^2}$$

$$\frac{\partial f}{\partial y} = 0 \qquad \frac{\partial f}{\partial y'} = \frac{y'}{\sqrt{1 + (y')^2}}$$

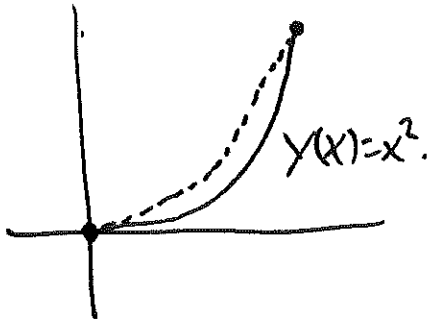
"$y' = z$)

$$\frac{d}{dz}\sqrt{1+z^2} = \frac{z}{2\sqrt{1+z^2}}$$

$$\frac{d}{dx} \frac{y'}{\sqrt{1+(y')^2}}$$

if $y(x) = x$, this is just $\frac{d}{dx} \frac{1}{\sqrt{2}} = 0.$

so $\delta F(y; \sin x) = \int_0^a \sin x \cdot 0 \, dx = 0$



can we make path shorter by adding $\epsilon \cdot \sin(\pi x)$.

is $\tilde{y}(x) = x^2 + \epsilon \sin(\pi x)$ a shorter or longer path?

we should get:

$$\delta F(y; \sin(\pi x)) < 0$$ length should get shorter.

$$f(x, y, y') = \sqrt{1 + y'(x)^2}$$

If $y = x^2$

$$\frac{\partial f}{\partial y} = 0 \qquad \frac{\partial f}{\partial y'} = \frac{y'}{\sqrt{1+(y')^2}}$$

$$= \frac{2x}{\sqrt{1+(2x)^2}} = \frac{2x}{\sqrt{1+4x^2}}$$

$$\frac{d}{dx}\frac{\partial f}{\partial y'} = -\frac{8x^2}{(1+4x^2)^{3/2}} + \frac{2}{(1+4x^2)^{1/2}}$$

$$\delta F(y; \sin(\pi x)) = \int_0^1 \left(-\frac{8x^2}{(1+4x^2)^{3/2}} + \frac{2}{(1+4x^2)^{1/2}}\right)(\sin \pi x)\, dx$$

Shortest path

$$f(x, y', y) = \sqrt{1+y'(x)^2}$$

We want to find y so

$$\frac{\partial f}{\partial y} - \frac{d}{dx}\frac{\partial f}{\partial y'} = 0.$$

$$\frac{\partial f}{\partial y} = 0 \qquad \frac{\partial f}{\partial y'} = \frac{y'}{\sqrt{1+(y')^2}}$$

so the shortest path is given by a function $y(x)$ satisfying

$$\frac{d}{dx}\frac{y'(x)}{\sqrt{1+y'(x)^2}} = 0$$

$$\frac{y'(x)}{\sqrt{1+y'(x)^2}} = C \qquad \frac{(y')^2}{1+(y')^2} = C^2$$

$$(y')^2 = C^2 + (y')^2 C^2$$

$$(1-C^2)(y')^2 = C^2$$

$$(y')^2 = \frac{C^2}{1-C^2}$$

$$y' = \sqrt{\frac{C^2}{1-C^2}} \longrightarrow y = dx + e \text{ is a line}$$

Brachistochrone

$$F(y) = \int_0^a \underbrace{\sqrt{\frac{1+(y')^2}{2gy}}}_{f}\, dx .$$

$$\boxed{\frac{\partial f}{\partial y} - \frac{d}{dx}\frac{\partial f}{\partial y'} = 0}$$

$$f(x, y, y') = \sqrt{\frac{1+(y')^2}{2gy}}$$

$$\frac{\partial f}{\partial y} = \frac{\partial}{\partial y}\sqrt{\frac{1+(y')^2}{2g}}\,\overbrace{\frac{1}{\sqrt{y}}}^{y^{-1/2}} = -\frac{1}{2}\sqrt{\frac{1+(y')^2}{2g}}\,\frac{1}{y^{3/2}}$$

$$\frac{\partial f}{\partial y'} = \frac{\partial}{\partial y}\,\frac{1}{\sqrt{2gy}}\sqrt{1+(y')^2} = \frac{1}{\sqrt{2gy}}\,\frac{y'}{\sqrt{1+(y')^2}} .$$

So

$$-\frac{1}{2}\sqrt{\frac{1+(y')^2}{y^3}} = \frac{d}{dx}\,\frac{y'}{\sqrt{y(1+(y')^2)}}$$

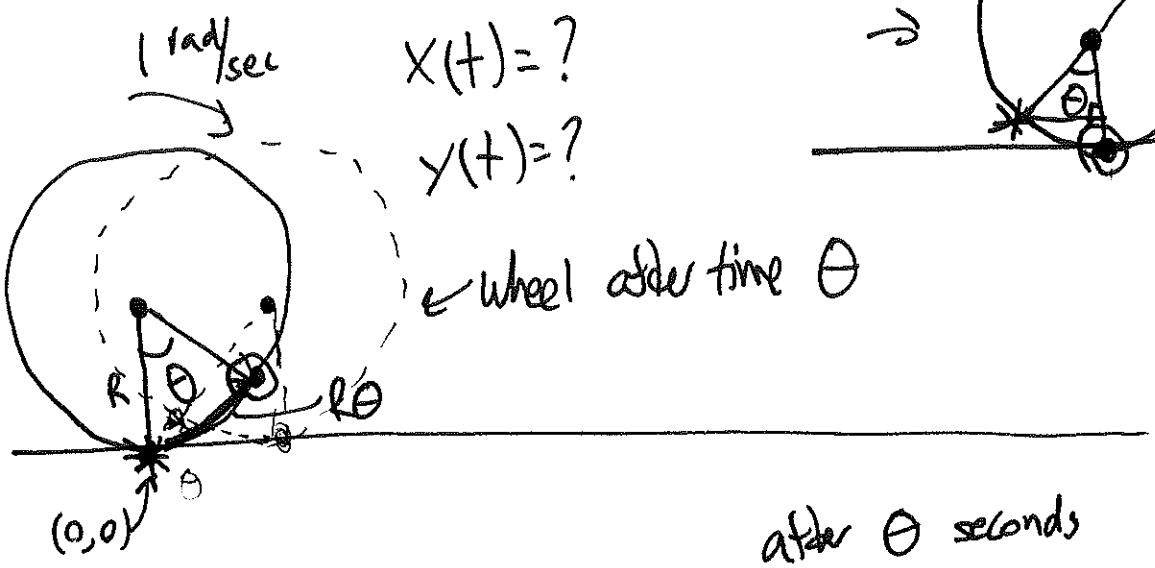
$y(x)$ solving this diff eq is solution to brachistochrone problem!

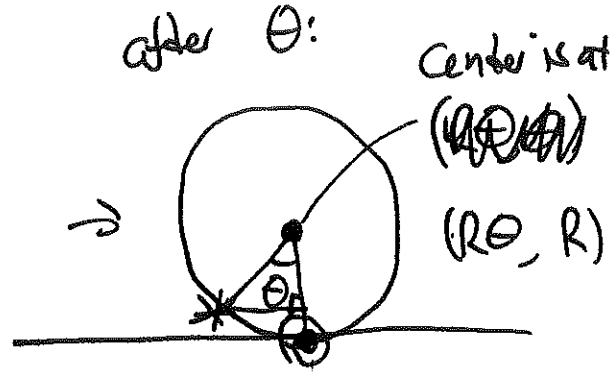
Answer

Easier to write parametrically

$$\begin{pmatrix} x(t) \\ y(t) \end{pmatrix} = C \begin{pmatrix} t - \frac{1}{2}\sin(2t) \\ \frac{1}{2} - \frac{1}{2}\cos(2t) \end{pmatrix}$$

Cycloid



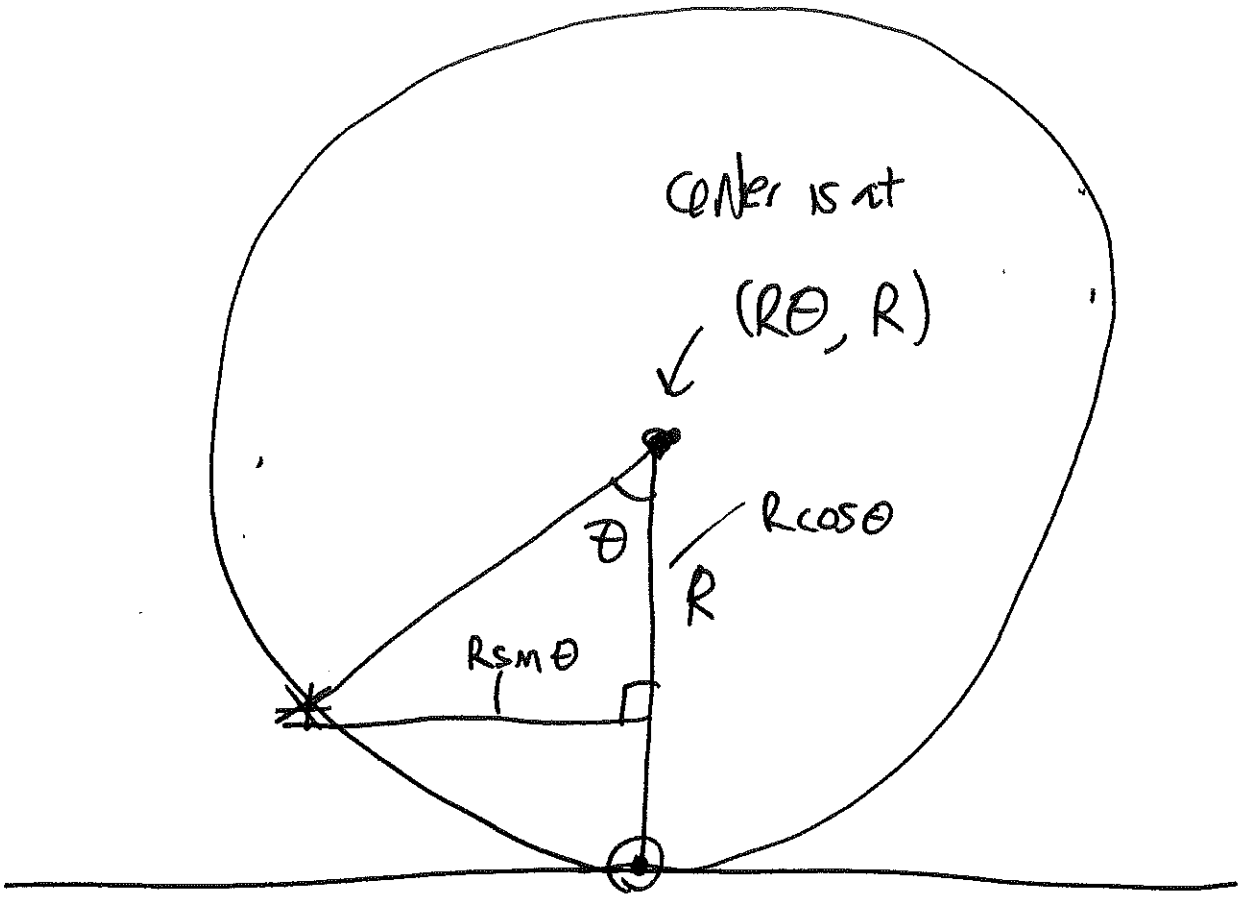


after θ seconds
"

after we roll an angle θ,

where is the middle of the wheel?

- moves forward by $R\theta$
- height is still R



$$x(\theta) = R\theta - R\sin\theta = R(\theta - \sin\theta)$$
$$y(\theta) = R - R\cos\theta = R(1 - \cos\theta)$$

"cycloid"

Last time:

We used Euler-Lagrange eqn to get a differential equation for brachistochrone problem!

It turns out an upside-down cycloid solves this eqn!

(movie from Wikipedia)

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} = 4 \qquad \left(\begin{matrix}\text{positive}\\ \text{integers}\end{matrix}\right)$$

$$a(c+a)(a+b) + b(b+c)(a+b) + c(b+c)(c+a)$$

$$= 4(b+c)(c+a)(a+b)$$

$$a^3 + b^3 + c^3 - 3(a^2b + ab^2 + a^2c + ac^2 + b^2c + bc^2) - 5abc = 0.$$

Degree 3 equation!

Remember completion of squares:

To solve $x^2 + bx + c = 0$

~~to~~ rewrite as $\left(x + \frac{b}{2}\right)^2 + \left(c - \frac{b^2}{4}\right) = 0.$

If we may a new variable $\tilde{x} = x + \frac{b}{2}$,

you get an equation with no "$\tilde{x}$" term:

$$\tilde{x}^2 + \left(c - \frac{b^2}{4}\right) = 0.$$

Substitute a la completion of squares:

$$x = \frac{-28(a+b+2c)}{6a+6b-c}$$

$$y = \frac{364(a-b)}{6a+6b-c}$$

our equation becomes

$$y^2 = x^3 + 109x^2 + 224x.$$

If you can find a solution (x,y) to that equation, you can get back (a,b,c):

$$a = \frac{56-x+y}{56-14x} \qquad b = \frac{56-x-y}{56-14x} \qquad c = \frac{-28-6x}{28-7x}.$$

This might give rational number, but in that case, clear denominators of a, b, c and get integer solution.

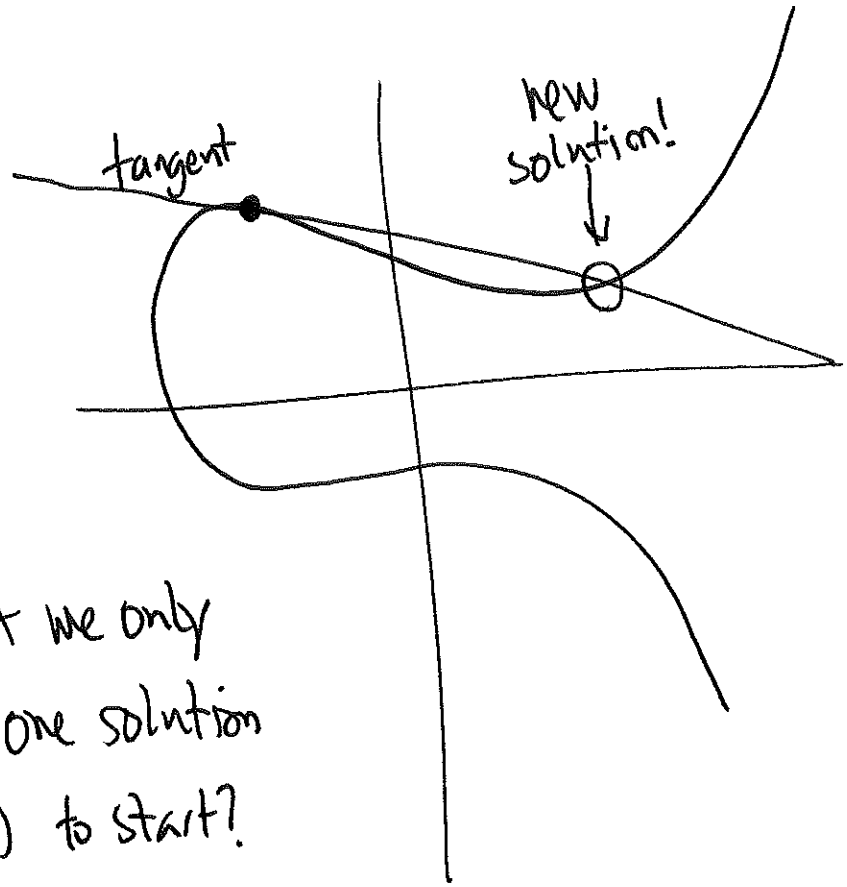
This is an <u>elliptic curve</u>.

$$y^2 = x^3 + ax^2 + bx + c$$

Sometimes you make one more substitution to put in <u>Weierstrass form</u>

$$y^2 = x^3 + bx + c.$$

What do elliptic curves look like?



$y^2 = x^3 - 7x + 10$

What if we only had one solution (x,y) to start?

In the fruit equation: $y^2 = x^3 + 109x^2 + 224x$

Let's start with solution we know

$x = -100 \quad y = 260,$

draw lines, solve for intersection,

find more solutions a, b, c of fruit,

hope they're positive.

$$y^2 = x^3 + 109x^2 + 224x$$

Brute force on computer:

$x = -100$
$y = 260$

solves first eqn

$a = 2/7$
$b = -1/14$
$c = 11/14.$

$\xrightarrow{\times 14}$

$a = 4$
$b = -1$
$c = 11.$

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} = 4$$

Does it work?

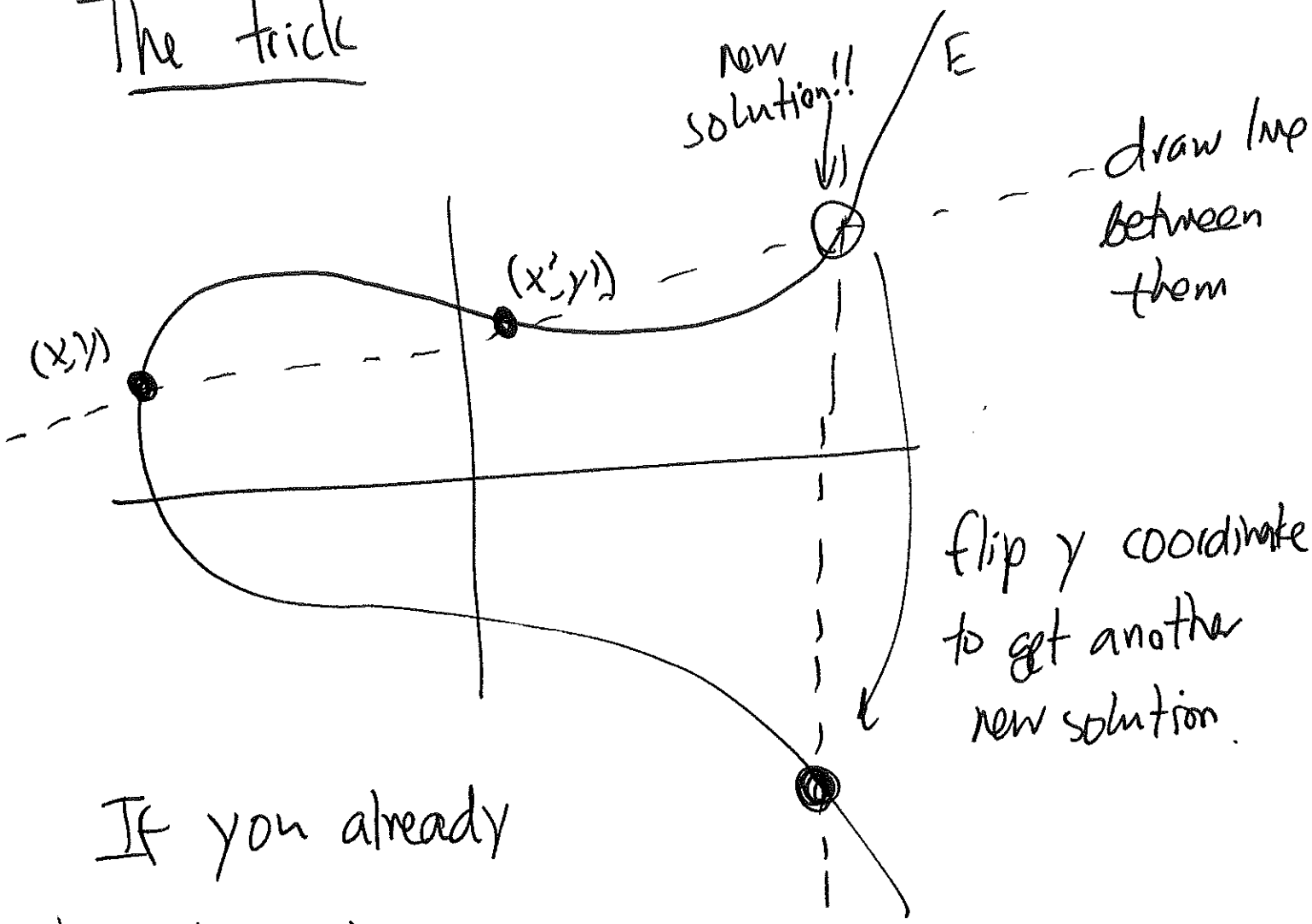
$$\frac{4}{10} + \frac{-1}{15} + \frac{11}{3}$$

$$= \frac{12}{30} + \frac{-2}{30} + \frac{110}{30} = \frac{120}{30} = \boxed{4}$$

To get solution where all positive, we need more solutions to

$$y^2 = x^3 + 109x^2 + 224x$$

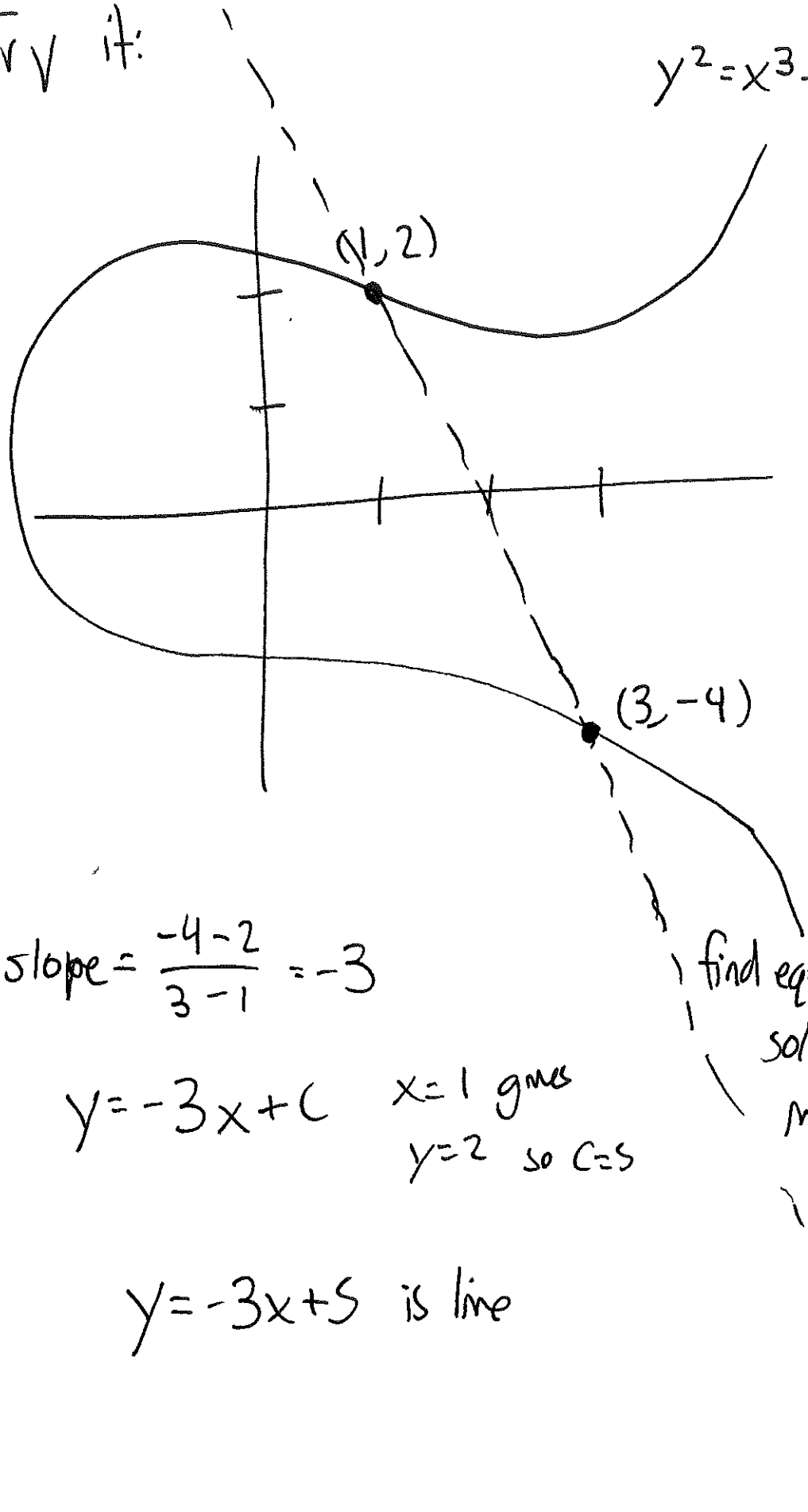
The trick



If you already have two solutions, you can use them to generate a new solution.

Try it:

$y^2 = x^3 - 7x + 10$



(1,2)
(3,-4) are solutions

find eqn of line, solve for third intersection point

$$\text{slope} = \frac{-4-2}{3-1} = -3$$

$y = -3x + C$ $\quad x = 1$ gives $y = 2$ so $C = 5$

$y = -3x + 5$ is line

$$(-3x+5)^2 = x^3 - 7x + 10$$

$$9x^2 - 30x + 25 = x^3 - 7x + 10$$

$$x^3 - 9x^2 + 23x - 15 = 0$$

$x = 1$
$x = 3$ are two solutions.

$$x^3 - 9x^2 + 23x - 15 = (x-1)(x-3)(x-\overset{??}{r})$$

$$= x^3 - (1+3+r)x^2 + (\text{don't care})$$

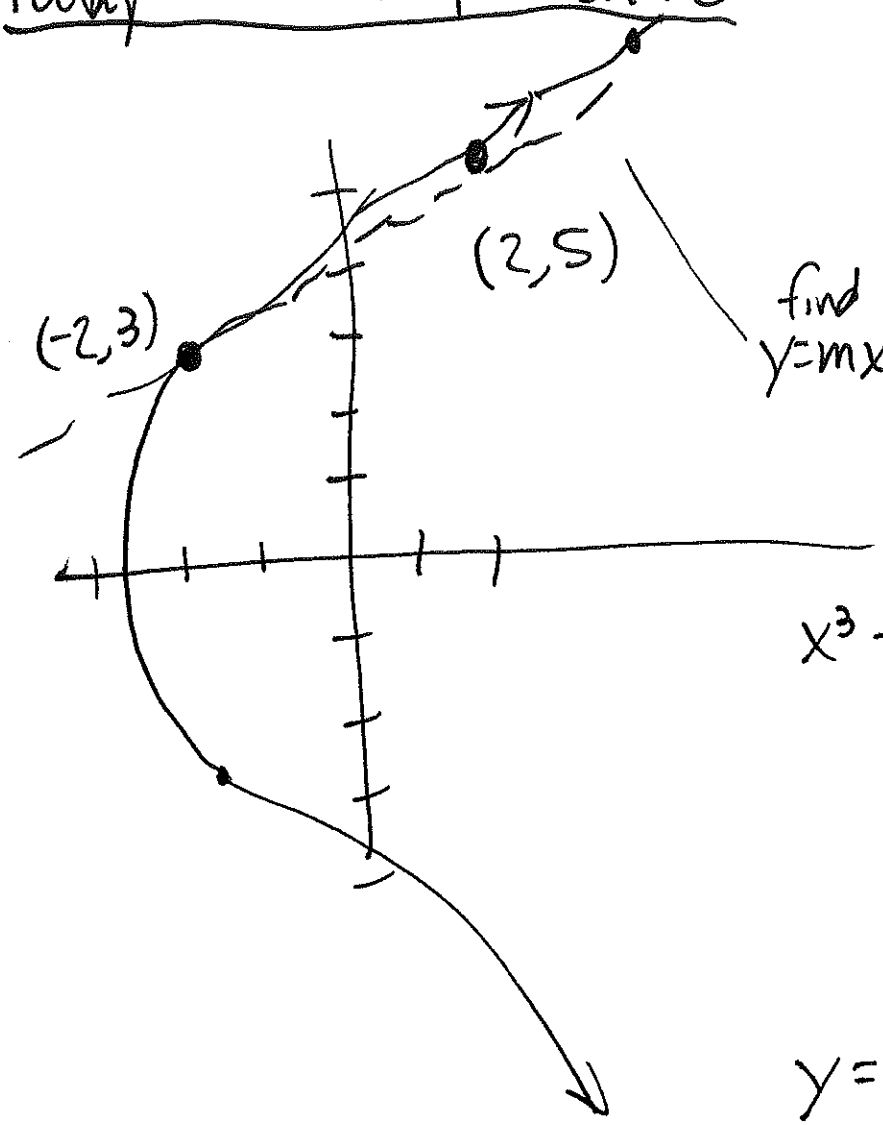
So $r = 5$ is the other root.

$y = -3x + 5$ so $y = -10$.

So $(5, 10)$ is a root

and so is $(5, -10)$

Today: More elliptic curves



$$y^2 = x^3 + 17$$

find $y = mx + b$

plug to here, solve for x

$$x^3 + ax^2 + bx + c$$

negative sum of roots

$$y = \tfrac{1}{2}x + 4$$

$$\left(\tfrac{1}{2}x + 4\right)^2 = x^3 + 17$$

$$\tfrac{1}{4}x^2 + 4x + 16 = x^3 + 17$$

$$x^3 - \tfrac{1}{4}x^2 - 4x + 1 = 0$$

$x = -2$, $x = 2$ already knew

$x = 1/4$

$$y = \frac{1}{2}x + 4 = \frac{1}{2}\left(\frac{1}{4}\right) + 4 = \frac{33}{8}$$

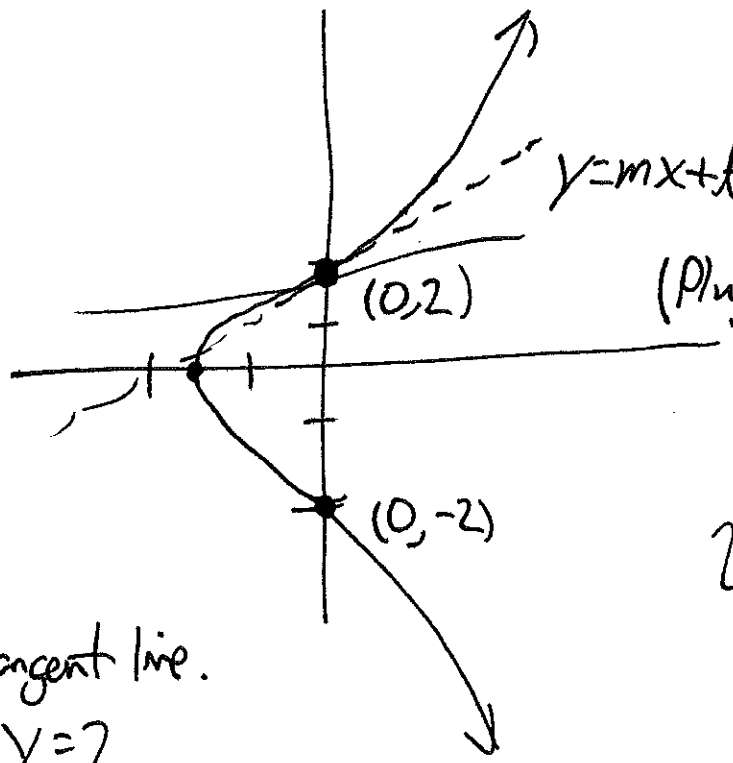
Third point: $\left(\frac{1}{4}, \frac{33}{8}\right)$

"Sum" of solutions:

$$(-2,3) + (2,5) = \left(\frac{1}{4}, -\frac{33}{8}\right)$$

Another: $y^2 = x^3 + 4$

$(0,2) + (0,2)$



$y = mx + b$ tangent line.

(Plug in to cubic eqn, find third point)

$$2y\frac{dy}{dx} = 3x^2$$

tangent line.

$y = 2$

$$\frac{dy}{dx} = \frac{3x^2}{2y} = 0.$$

plug in: $y^2 = x^3 + 4$

$$4 = x^3 + 4 \longrightarrow x^3 = 0$$

third point is <u>also</u> $(0,2)$.

$(0,2)+(0,2)=(0,-2)$.

what's $(0,2)+(0,-2)$?

line between points is: vertical.

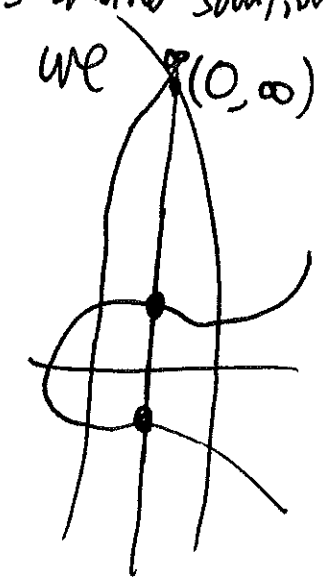
where does vertical line hit $y^2=x^3+4$?

only hits it at $(0,2)$ & $(0,-2)$!!

<u>Solution:</u> Add a point at infinity, denoted "∞".

pretend it's another solution

To make addition of points always work, we declare that $(x,y)+(x,-y)=\infty$.



We also declare

$(x,y)+\infty=(x,y)$

Def A <u>group</u> is a set G with a <u>binary operation</u> $\times$ satisfying

two elements of G as input, one element of G as output.

- associative:

$$(x \times y) \times z = x \times (y \times z)$$

- identity element:

there's some $e \in G$ where $x \times e = x$, $e \times x = x$

- inverse:

for any $x \in G$, there's a y in the group so $x \times y = e$.

Examples $G = \mathbb{R}^* = \{$all real numbers other than $0\}$

$\times$ is normal multiplication.

$e = 1$

(but $\mathbb{Z}^*$ wouldn't work; no inverses)

One more group:

G = the rational points on an elliptic curve E, plus ∞.

$\times$ = the addition operation we defined.

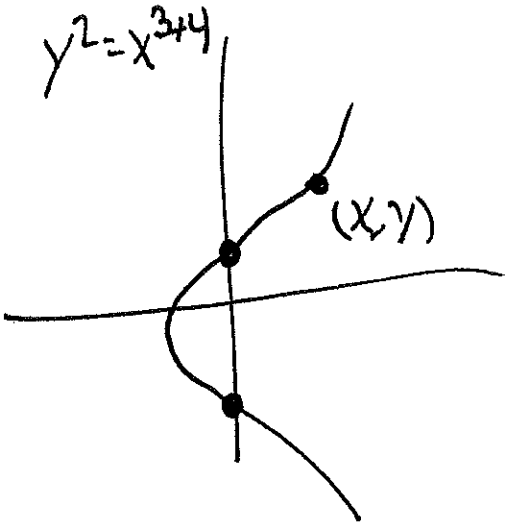
This is a group! (Trust me, it's associative.)

$$(P+Q)+R = P+(Q+R)$$

This is why we do the weird flip-the-y-coordinate trick.

What's identity?

∞



$$(x,y)+\infty = (x,y).$$

What's inverse of $(0,2)$?

$(0,-2)$

$$(0,2)+(0,-2) = \infty.$$

$G = \mathbb{Z}$ (or $\mathbb{R}$, or $\mathbb{C}$)

$\times$ is addition.

$e = 0$

G = integers from 0 to $n-1$.

~~add~~

Operation = addition mod n (add them and take remainder when divided by n)

$\boxed{\text{e.g if } n=10 \quad 6+7=3}$

$e = 0$

(inverse of 6 if $n=10$: 4)

G = 2×2 matrices with determinant not 0

$\times$ = multiplication.

$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

ABELIAN

"non-abelian group" since not commutative.

weird feature: $X \times Y \neq Y \times X$ in general

For cryptography, we look at mod-n solutions to elliptic curve eqns $y^2 = x^3 + ax + b$

(only has to work mod n)

How to solve $3x \equiv 2 \bmod 5$?

(x must be integer)

$x = 4$ works.

$x^2 \equiv 2 \bmod 7$

$x = 3$ or 4 (aka -3)

$x^2 \equiv 3 \bmod 7$

no solutions!

x	$x^2 \bmod 7$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Elliptic curves mod n: use the same trick for finding new solutions.

$$y^2 = x^3 - x - 1 \bmod 5$$

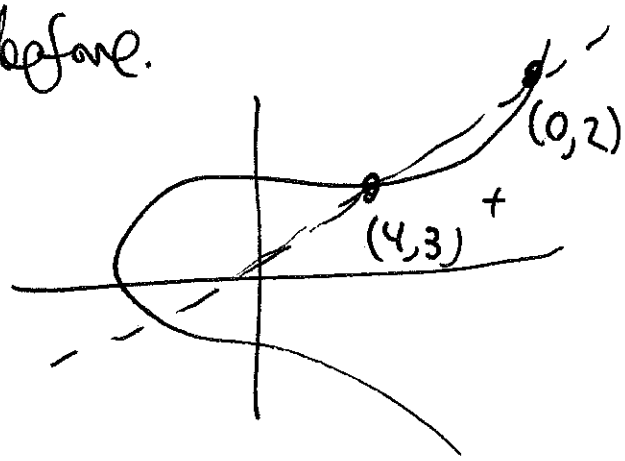
$(x_1, y_1) = (4,3)$
$(x_2, y_2) = (0,2)$ are solutions.

$$3^2 \stackrel{?}{=} 4^3 - 4 - 1 \bmod 5$$

$$9 \stackrel{?}{=} 64 - 4 - 1 \bmod 5$$

$$9 \equiv 59 \bmod 5 \checkmark$$

use these two to generate a new solution, as before.



$4 \cdot 4 \equiv 1 \bmod 5$

so "$\frac{1}{4}$" mod 5 is just 4.

line = $y = \frac{1}{4}x + 2$

$$y \overset{\text{mod } 5}{\equiv} 4x+2$$

$$(4x+2)^2 = x^3 - x - 1 \bmod 5$$

$$16x^2 + 16x + 4 = x^3 - x - 1 \bmod 5$$

$$x^3 - 16x^2 - 17x - 5 \equiv 0 \bmod 5$$

$$x^3 + 4x^2 + 3x \equiv 0 \bmod 5.$$

Know two roots: $x=0$, $x=4$

the other root is: $x=-8$ which mod 5 is $x=2$

then $y = 4x+2 = 10 = 0 \bmod 5$

$(2,0)$ is our third pt.

$y^2 = x^3 - x - 1 \bmod 5$?

How many solutions are there to

$$y^2 = x^3 + ax + b \mod p?$$

At most p^2, but in fact:

Hasse bound: number is

$$p+1-2\sqrt{p} < \downarrow < p+1+2\sqrt{p}$$

Elliptic curve cryptography

$$y^2 = x^3 + 2x + 2 \bmod 17$$ All solutions?

Hint

y	0	1	2	3	4	5	6	7	8	9	10
$y^2 \bmod 17$	0	1	4	9	16	8	2	15	13	13	15

y	11	12	13	14	15	16
$y^2 \bmod 17$	2	8	16	9	4	1

x	possible y's
0	6, 11
1	—
2	—
3	1, 16
4	—
5	1, 16
6	3, 14
7	6, 11
8	—
9	1, 16
10	6, 11

x	possible y's
11	—
12	—
13	7, 10
14	—
15	—
16	4, 13

18 total

What do we notice:

1) 18 solutions (≈ 17)

~~Each~~ For $y^2 \equiv x^3 + ax + b \mod p$

p^2 possible (x,y)

$\approx 1/p$ chance of a given pair working

$\rightarrow$ about p solutions.

Hasse Bound

The number of solutions N satisfies

$$p+1-2\sqrt{p} < N < p+1+2\sqrt{p}$$

Thm (Waterhouse 1969): All those possibilities are equally likely.

2) Possible y pairs always add to 17.

$y^2 = (-y)^2$, and $-y \bmod 17$ is $17-y$

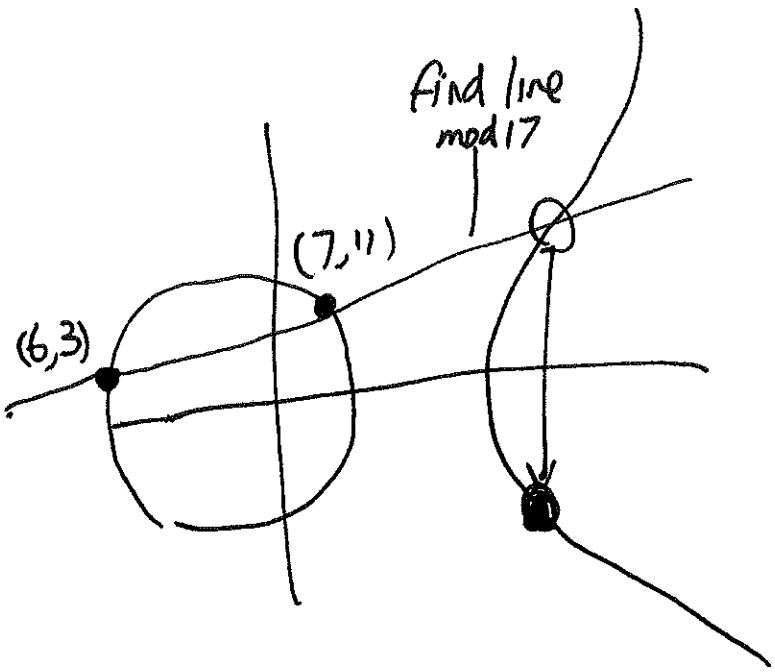
3) For about half x-values there are 2 y's
about half x-values, there are none.

$\rightarrow$ where there is a y that works for given x
depends on whether x^3+ax+b is a square mod p.
p. Half of numbers are squares, half aren't.
("Quadratic reciprocity" helps find which are which.)

(There could be some x's where only $y=0$ occurs)

You can still do elliptic curve addition mod p!

$(6,3)+(7,11)$



$(13,7)+(13,7)$

Line:

$y = 8x - 45 = 8x + 6$

$y = 6$ so third point is $(0,6)$

$(6,3)+(7,11) = (0,-6) = (0,11)$.

Plug in:

$y^2 = x^3 + 2x + 2 \mod 17$

$(8x+6)^2 = x^3 + 2x + 2$

$64x^2 + 96x + 36 = x^3 + 2x + 2$

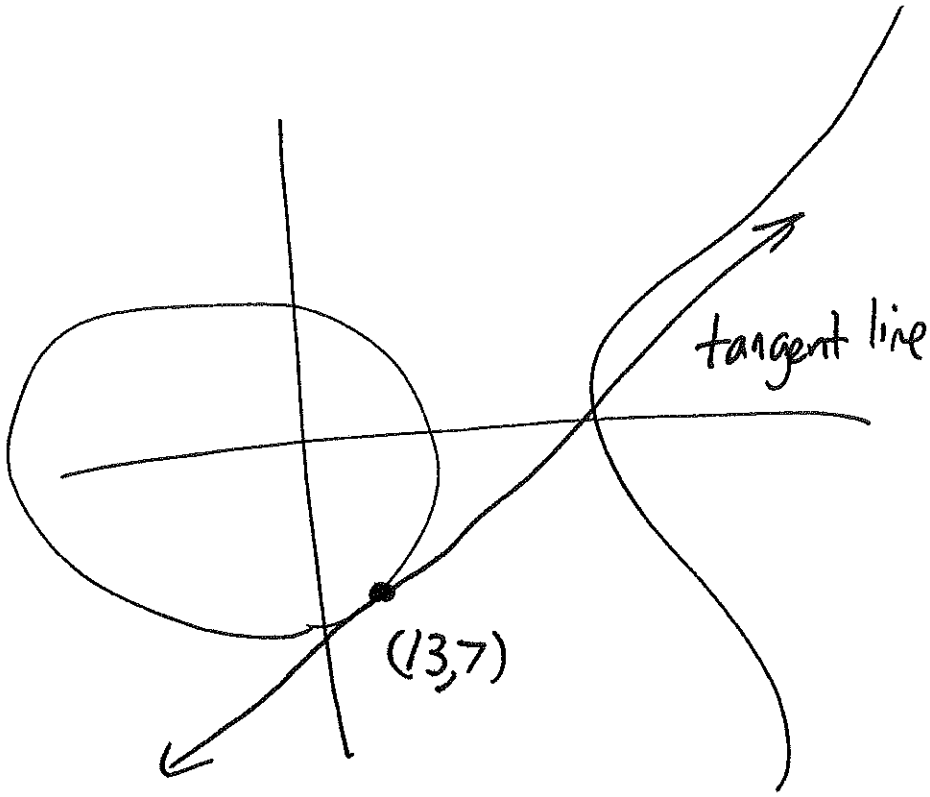
mod 17

$13x^2 + (??)x + (??) = x^3 + 2x + 2$

$0 \equiv x^3 - 13x^2 + (\text{junk})$

6, 7 are solutions

$\boxed{x = 0}$



$$y^2 = x^3 + 2x + 2$$

$$3 \cdot 13^2 + 2$$

$$= 3 \cdot (-1) + 2 = -1 = 16$$

$$2y \frac{dy}{dx} = 3x^2 + 2$$

at $(x,y) = (13,7)$

$$\frac{dy}{dx} = \frac{3x^2+2}{2y}$$

$$\frac{dy}{dx} = \frac{16}{14} = \frac{-1}{-3} = \frac{1}{3} = 6.$$

Tangent line:

or $\frac{16}{14} = 16 \cdot 11 = 6.$

$\cancel{y = 6x + 71}$ $y = 6x - 71$

$= 6x + 14 \mod 17$

$(6x+14)^2 = x^3+2x+2 \mod 17$

only care about x^2 term

$36x^2 + (\text{junk}) = x^3 + (\text{junk})$

$x^3 - 36x^2 + (\text{junk}) = 0$

13 is double root so

$13+13+r=36$

$\boxed{r=10}$

$x=10$

$y=6x+14=74=6.$

So $(13,7)+(13,7)=(10,-6)=(10,11)$

We did $(13,7)+(13,7)$.

How would you find $100\cdot(13,7)$?

$$\left[\ \big((13,7)+\cdots+(13,7)\big)\ \text{100 times}\right]$$

$(13,7)$

$\times 2 \downarrow$

$2\cdot(13,7)=(10,11)$

$\times 2 \downarrow$

$4\cdot(13,7)$

keep doubling

$8\cdot(13,7)$

$16\cdot(13,7)$

$32\cdot(13,7)$

$64\cdot(13,7)$

$128\cdot(13,7)$

$$100\cdot(13,7)=64\cdot(13,7)+32\cdot(13,7)+4\cdot(13,7)$$

NB: This works because $+$ is assortative. (E is a group)

$$5P \overset{\text{directly}}{=} (((P+P)+P)+P)+P$$

$$5P=\underbrace{\big((P+P)+(P+P)\big)}_{4P}+\underset{P}{P}$$

IVI

Calculating 100P

$100 \cdot (13,7)$ is easy (repeated doubling)

What if I told you

$n \cdot (13,7) = (0,11)$.

Can you tell me n? ← "Elliptic curve discrete log problem"

Only way is brute force!

<u>Elliptic curve cryptography</u>

First: Diffie-Hellman (Elliptic curve)

A & B want to agree on a secret shared key over public channel.

Here's what they do:

First: publicly agree on:

- prime p
- an elliptic curve $y^2 = x^3 + ax + b \bmod p$
- a point $G = (x,y)$ on elliptic curve

it's safe to always use same curve, G.

e.g. use government-issued one NIST P-192

Alice picks a number $d_A \in [1, n-1]$ (n = number of solutions, or use $p/2$ if you want.)

(keeps secret)

Bob picks a number $d_B \in [1, n-1]$

A computes ~~$d_A \cdot B$~~, $d_A \cdot G = Q_A$, sends to Bob

B computes $d_B \cdot G = Q_B$, sends to Alice

Now:

Bob does $d_B \cdot Q_A = d_B \cdot (d_A \cdot G)$ $\quad = K$

Alice does $d_A \cdot Q_B = d_A \cdot (d_B \cdot G)$) same thing! (group law is associative)

their shared secret key is the x-coordinate of K.

What does an eavesdropper know?

Q_A $\quad (p, E, a, b, G)$

Q_B $\quad$ elliptic curve data

But knowing Q_A isn't enough to find d_A

knows $Q_A = d_A \cdot G$ (discrete log problem)

Last time: Elliptic curve Diffie-Hellman

Agree On:

- Prime p
- An elliptic curve $y^2 = x^3 + ax + b$
- A point on the curve, $G = (x, y)$.

e.g. NIST P-192

Alice picks secret d_A and computes $Q_A = d_A \cdot G$ sends to Bob

Bob picks secret d_B and computes $Q_B = d_B \cdot G$ sends to Alice

repeated doubling

Now: Alice does $d_A \cdot Q_B$ $(= d_A(d_B G))$

Bob does $d_B \cdot Q_A$ $(= d_B(d_A G))$

Equal!

Use x-coordinate as key.

(lots of computation, but fast)

You've just agreed on a ~~[illegible]~~ ~60 digit key K.

This is a 180-digit binary string you both know. Now you can use this key to encrypt your messages.

Write your message in binary:

Bob's message 10111001101000010101 1

XOR with key 11001110011101110110

Send to Alice 0111011111011010110 1 ...

11001110011101110110 key again

XOR → 1011100110100001010 1

If message is longer than key, you'll run out.

Use "block cipher" (like AES)

Elliptic curve digital signatures. (ECDSA)

If Gerald wants to sign a digital message M, here's how it works:

1) Gerald generates a public key Q_G (private key d_G) and puts Q_G in a database on his website.

2) Given Message M, Gerald does some algorithm to generate a signature S. (using d_G)

3) Anyone who sees S, M and Q_G can verify that whoever generated S must know d_G.

Del

Details:

1) Gerald picks private d_G (a number)

2) computes $Q_G = d_G \cdot G$, and posts Q_G publicly.

3) To sign a message M:

   a) Gerald computes hash(M) which "digests" M into 256-bit string (in a nonreversible way)

   Call that h.

   n is number of pts on curve, ~p.

   b) Pick a random $k \in [1, n-1]$

   c) Compute $R = kG$ in ~~gro~~ elliptic curve.

   d) Let r be x-coordinate of R.

   e) Compute $s = k^{-1} \cdot (h + r d_G) \bmod n$

   random, hash, x-coordinate, private key

   f) Signature is (r, s)

Suppose somebody knows:

- M message
- (r,s) signature
- Q_G public.

They can check: whoever computed s must have known d_G:

1) Compute $s^{-1} \bmod n$ and then

$$R' = (hs^{-1}) \cdot G + (rs^{-1}) \cdot Q_G$$

simplifies to R.

2) If x-coordinate of R' is r, signature is valid!

For different k, you get different signatures, but they'll all pass verification.

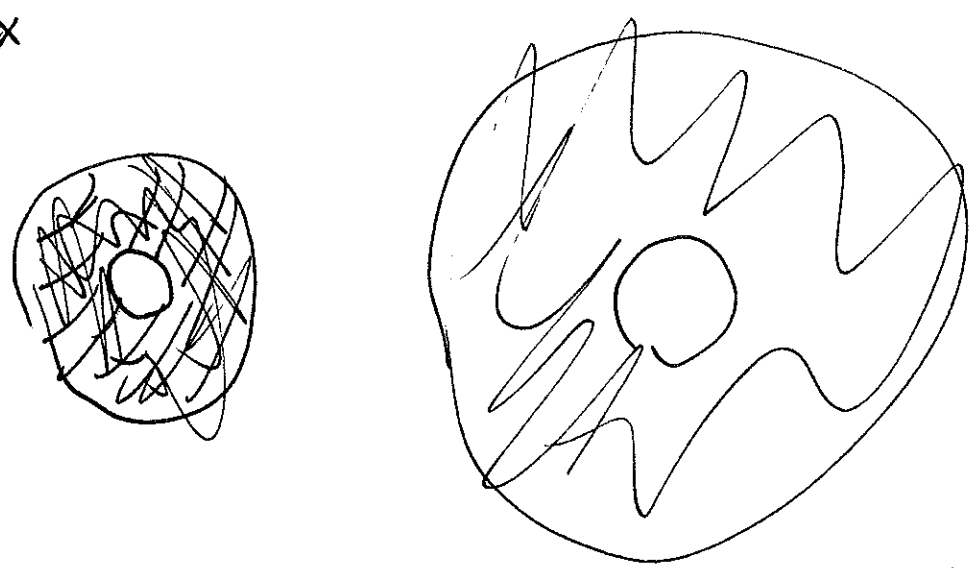
If you know (r,s) & (r',s'), two valid signatures generated using same k, you can solve for d_G and generate your own signatures!

Topology

- basic stuff (today)
- proving some other things using topology { Brouwer's fixed pt, fdtl theorem of algebra?
- applications to statistics

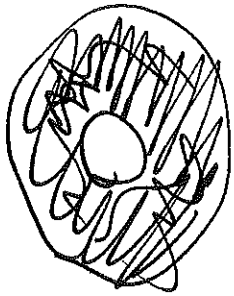
Two topological spaces are "homeomorphic" (the same) if one can be smoothly transformed into the other by stretching, bending, ...
(but no tearing or gluing)

ex

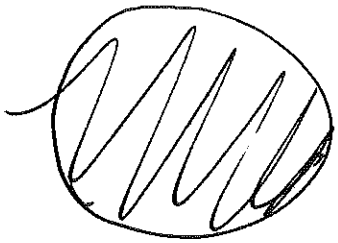


homeomorphic

two annuli of different sizes are homeomorphic



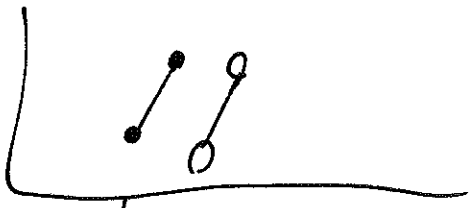
annulus

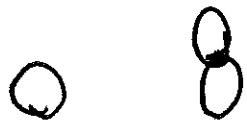


solid disk

not homeomorphic

More examples





circle figure 8 X

coffee cup

donut ✓

$\mathbb{R}$ real numbers

$(0,1)$ open interval

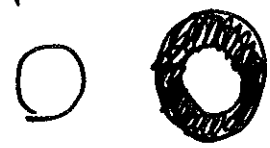
annulus biannulus X

Möbius strip

Cylinder

X

untwisted



X

$\mathbb{R}$ real numbers

vs

$\mathbb{R}^2$ X

~~Möbius strip~~ Cylinder

vs ~~twist~~

double-twisted Möbius strip

✓ ?

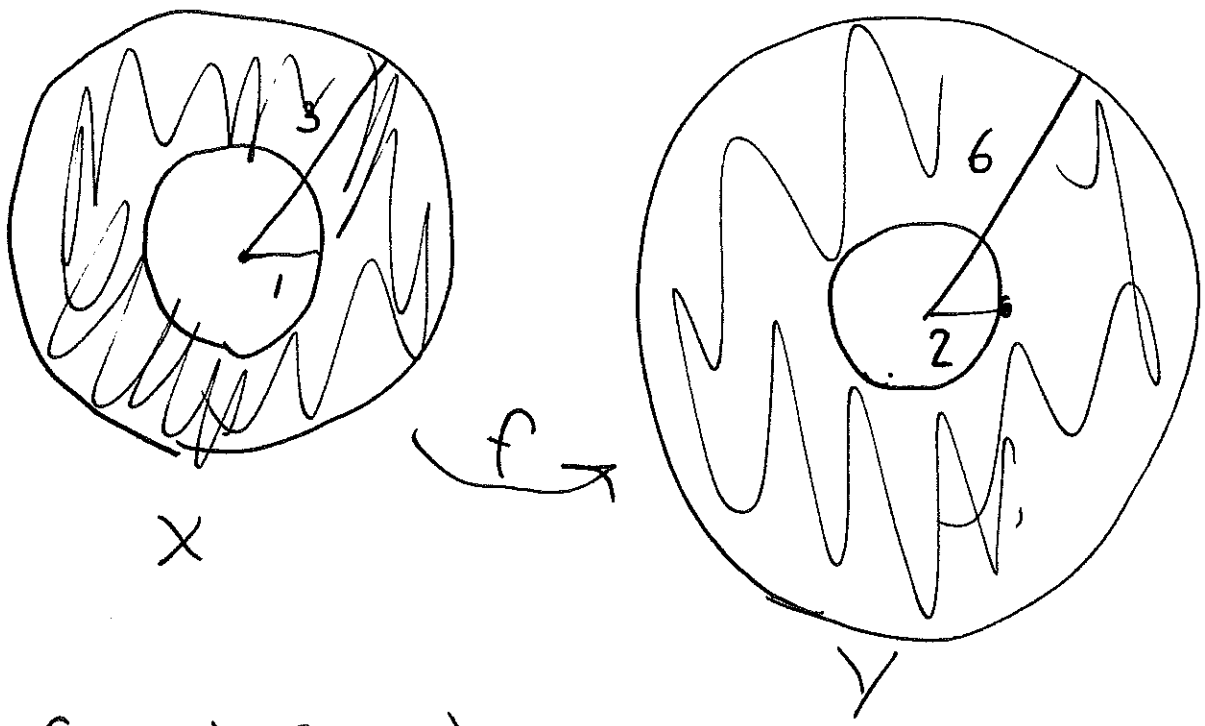
Officially:

Two spaces X and Y are <u>homeomorphic</u>
(sets, basically)

if there's an invertible function

$f: X \to Y$

that's continuous and has a continuous inverse.



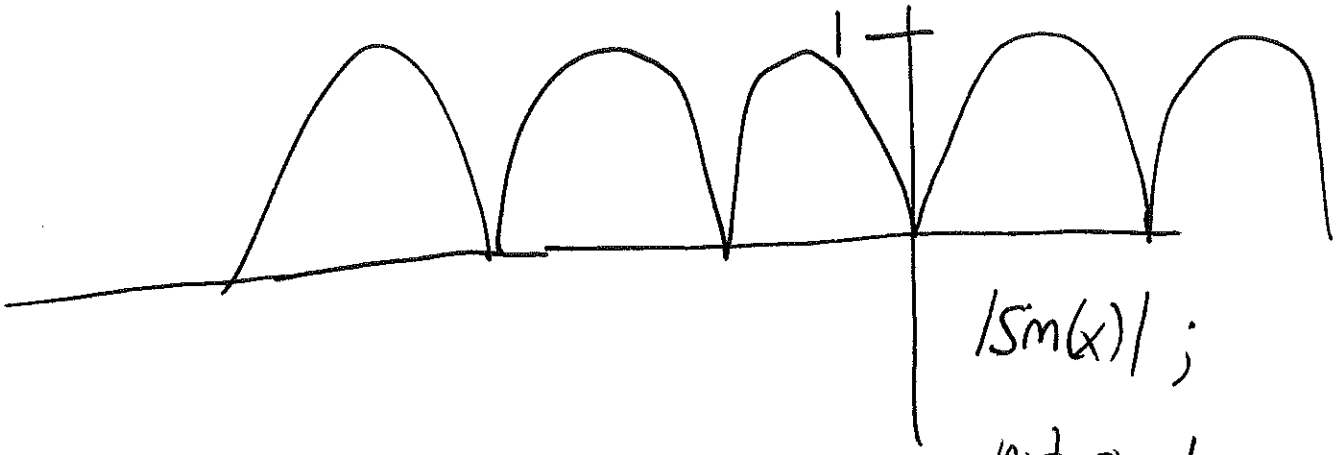
$f(r, \theta) = (2r, \theta)$
in polar

inverse function is $g(r, \theta) = (\frac{1}{2}, \theta)$

Ex $\mathbb{R}$ and $(0,1)$

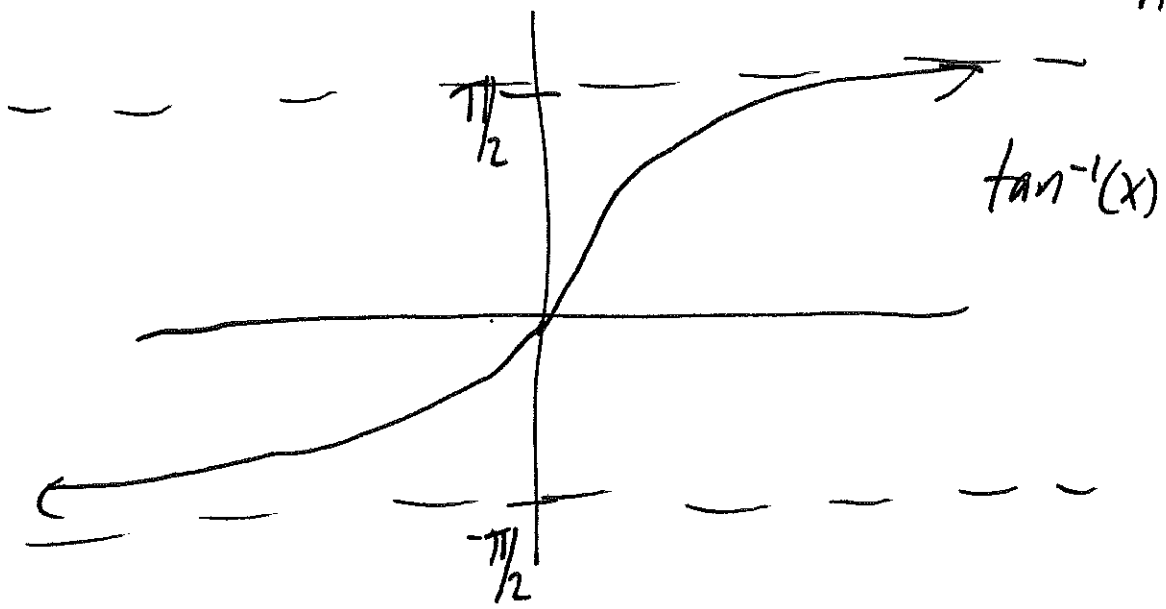
Are these homeomorphic?

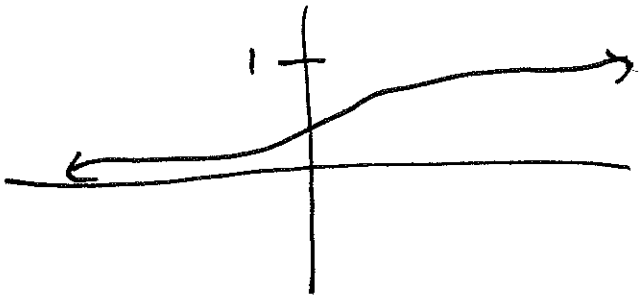
Can you find continuous $f:\mathbb{R}\to(0,1)$ with continuous inverse?



$|\sin(x)|$;

not one-to-one





$f(x) = \frac{1}{\pi}\tan^{-1}x + \frac{1}{2}$

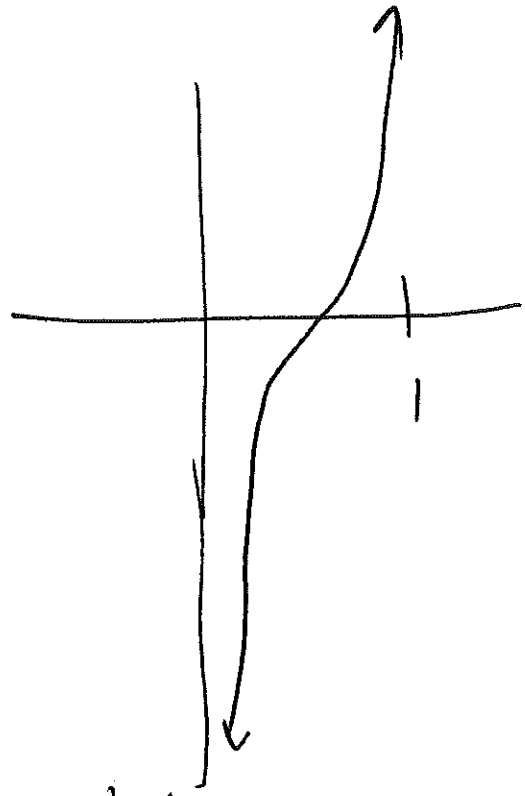
Inverse?

$$x = \frac{1}{\pi}\tan^{-1} y + \frac{1}{2}$$

$$\pi\left(x - \frac{1}{2}\right) = \tan^{-1} y$$

$$y = \tan\left(\pi\left(x - \frac{1}{2}\right)\right).$$

$$g(x) = \tan\left(\pi\left(x - \frac{1}{2}\right)\right)$$



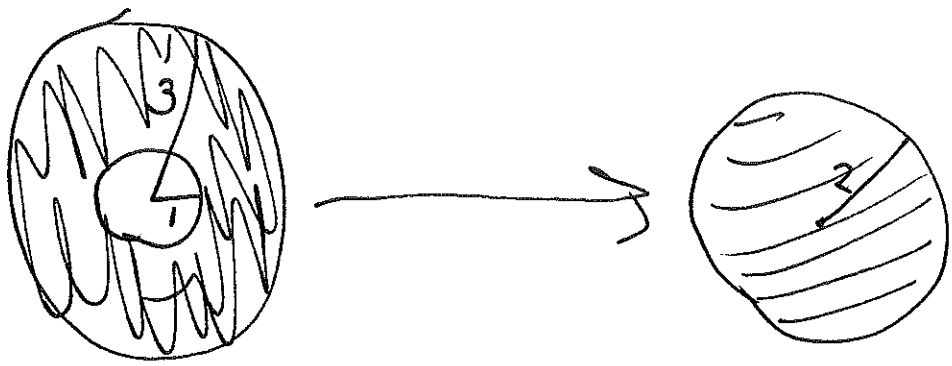
$\mathbb{R}$ and $(0,1)$ are homeomorphic!

A strategy to show spaces are homeomorphic (or not).

To show X and Y are <u>not</u> homeomorphic:
find a "characteristic" of spaces that's unaffected by homeomorphisms.

("topological invariants")

Not example



$$f(r,\theta) = (r-1, \theta)$$

Doesn't count!
This f is not invertible.

For g to be inverse of f means that

$$g(f(p)) = p \text{ for any } p$$

and $$f(g(p)) = p \text{ for any } p.$$

If
$g(r,\theta) = (r+1, \theta)$
then
$g(0, \pi/4) = (1, \pi/4)$
$g(0, \pi/2) = (1, \pi/2)$

same pt in polar!
g doesn't make sense when $r=0$.

Today: <u>More topology</u>

(But I have to leave extra early to give an exam.)
1:45

<u>Reminder:</u>

X and Y are homeomorphic if

there's a continuous $f: X \to Y$ with continuous

inverse $g: Y \to X$.

("Can stretch one into the other with no gluing/ripping").

How to know/prove two things <u>are</u> homeomorphic

Just find f & g.

How to prove two things are <u>not</u> homeomorphic:

Use a "topological invariant": a property/measure of X that's unaffected by homeomorphism.

- X is <u>simply connected</u> if every loop in X can be shrunk to point

annulus: not simply connected

disk: simply connected

$\Rightarrow$ ~~not simply connected~~ not homeomorphic.

- X is <u>connected</u> if it's just one "piece".

not connected

connected

- the <u>number of edges</u> is a topological invariant

(needs defined)

so cylinder and Möbius strip are not homeomorphic

2 edges 1 edge

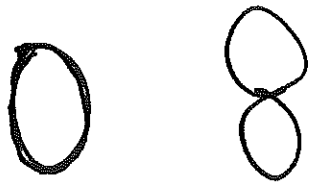
- <u>contractiblity</u> is a topological invariant

a set is ~~contractible~~ simply connected if any loop the set can be shrunk to a point.

contractible	not contractible
$\mathbb{R}$, $\mathbb{R}^2$ — anything convex	annulus
the sphere S^2	Möbius Strip

Examples

- number of holes
- 1-cuttable.

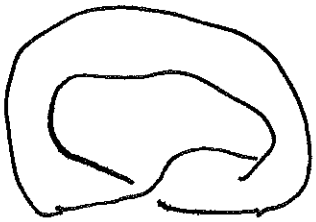


circle — not 1-cuttable

figure-8 — 1-cuttable

Say X is "1-cuttable" if you can remove a single point and make it not connected.

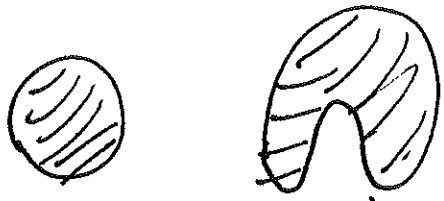
Möbius strip vs cylinder



- number of edges
- is edge connected

$\mathbb{R}$ vs $\mathbb{R}^2$	$\mathbb{R}^2$ vs $\mathbb{R}^3$	$(0,1)$ vs $[0,1]$
1-cuttable	remove pt not simply connected ↑ remove pt and still simply connected ↑	no edges — removing any pt makes disconnected; 2 edges — removing a pt can leave it connected

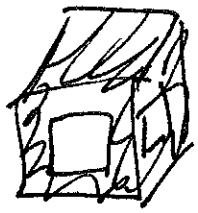
- <u>number of edges</u> is a topological invariant
  ("boundary")
- <u>convex</u> <u>not</u> a topological inv't



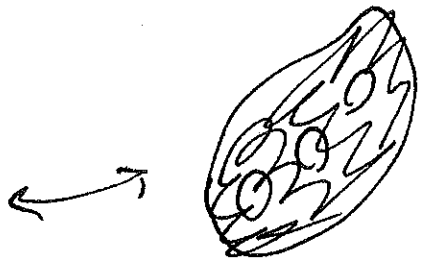
convex not

But they are homeomorphic.

- <u>number of holes</u> is topological inv't.
  (but had to define)



cube with holes in horizontal faces



3 holes
annulus.

~~Homotopy~~

Homotopy

Two functions $f: X \to Y$

$g: X \to Y$

are homotopic if you can smoothly turn one into the other.

This means you can find a time-dependent family of functions

$$F_t : X \to Y \quad (0 \le t \le 1)$$

where $F_0 = f$ and $F_1 = g$

You can also think of F as being a single function

ordered pair (x,t)

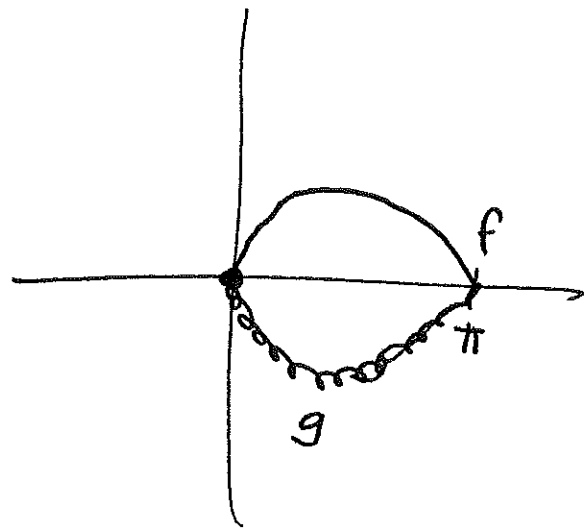
$$F : X \times [0,1] \to Y$$

Ex let $X = [0, \pi]$

$Y = \mathbb{R}^2$

$f(x) = (x, \sin x)$

$g(x) = (x, -\sin x)$



$F_t(x) = (x, (1-2t)\sin x)$

$F_0(x) = (x, \sin x)$

$F_1(x) = (x, -\sin x)$

you could think of this as

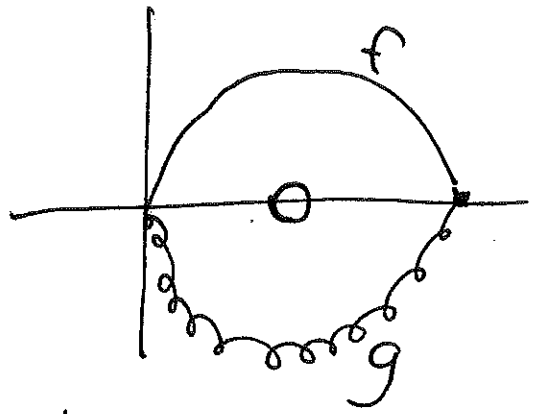
$F(x,t) = (x, (1-2t)\sin x)$

$X = [0, \pi]$

$Y = \mathbb{R}^2 \setminus \{(\frac{\pi}{2}, 0)\}$

$f(x) = (x, \sin x)$

$g(x) = (x, -\sin x)$



Can't use same F_t anymore!

Still homotopic (just move away from hole and do as before)

but finding eqn is hard.

<u>ex</u> $f: (-\pi/2, \pi/2) \to \mathbb{R}$

$f(x) = \tan(x)$

$g: (-\pi/2, \pi/2) \to \mathbb{R}$

$g(x) = x$

homotopic!

~~One more:~~

$$F_t : \left(-\tfrac{\pi}{2}, \tfrac{\pi}{2}\right) \to \mathbb{R}$$

$$F_0 = f$$

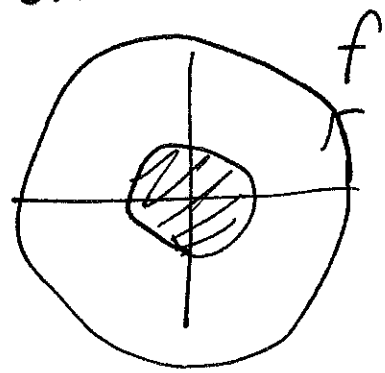
$$F_1 = g.$$

$$F_t(x) = (1-t)\tan(x) + tx$$

Can two things <u>not</u> be homotopic??

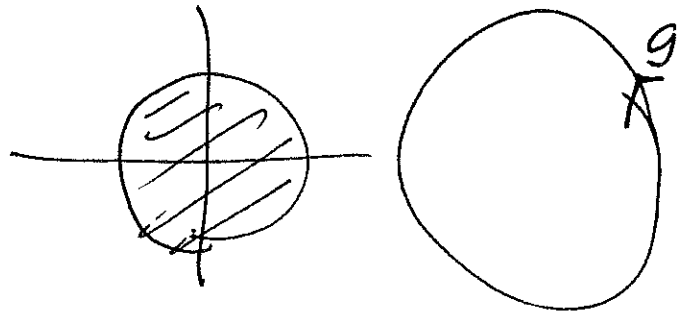
$$f : S^1 \to \mathbb{R}^2 \setminus D$$

circle plane minus unit disk



$$g : S^1 \to \mathbb{R}^2 \setminus D$$

circle



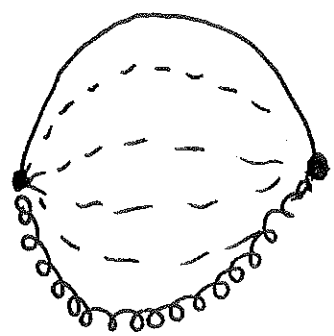
hard to prove!

Homotopy

Two functions $f: X \to Y$
$g: X \to Y$

are <u>homotopic</u> if there's a time-varying family $F_t: X \to Y$ so $F_0 = f$ $F_1 = g$.

<u>Ex</u>

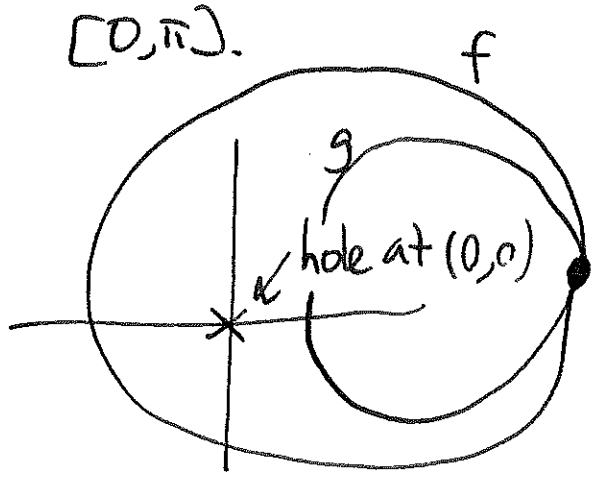


$g, f: [0, \pi] \to \mathbb{R}^2$

$f(x) = (x, \sin x)$

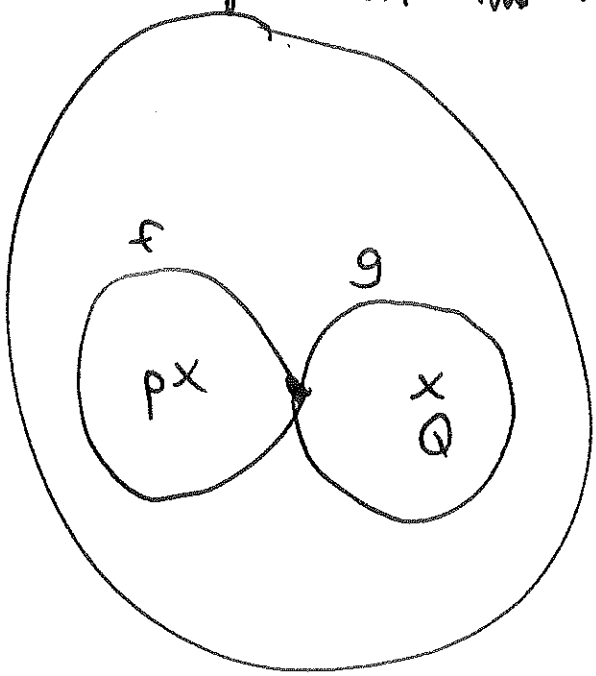
$g(x) = (x, -\sin x)$

<u>Not homotopic</u> use S^1 (circle) as domain instead of $[0, \pi]$.



$f, g: S^1 \to \mathbb{R}^2 \setminus \{(0,0)\}$
punctured plane

plane with two holes:

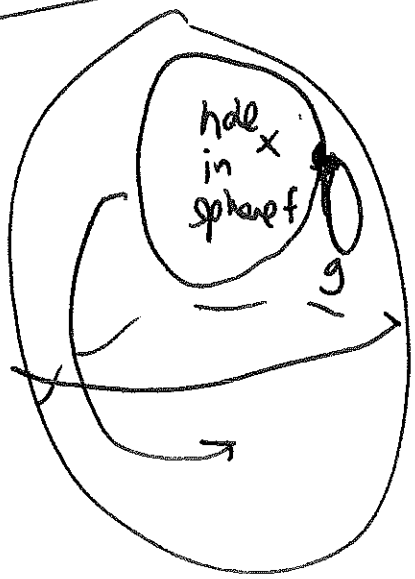


$f, g : S^1 \to \mathbb{R}^2 \setminus \{P, Q\}$

not homotopic

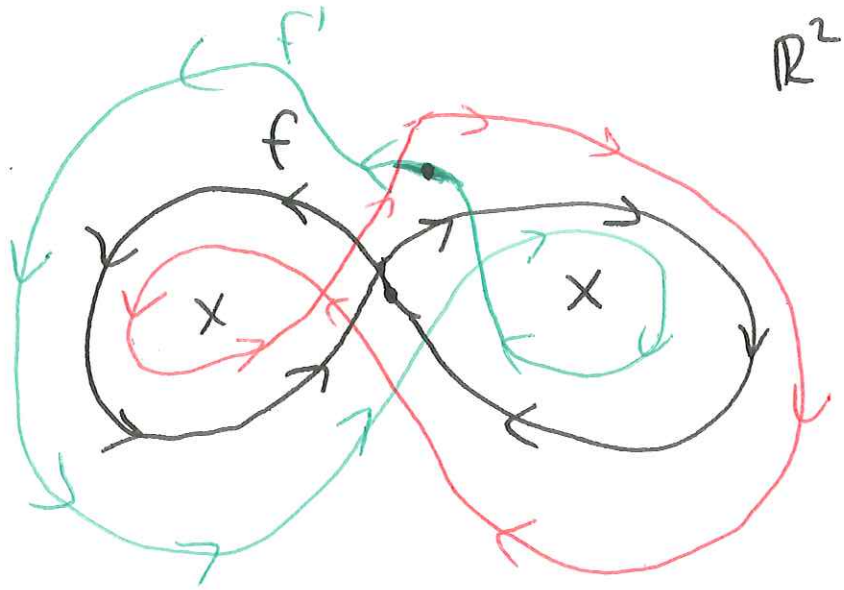
sphere with hole

$f, g : S^1 \to S^2 \setminus P$



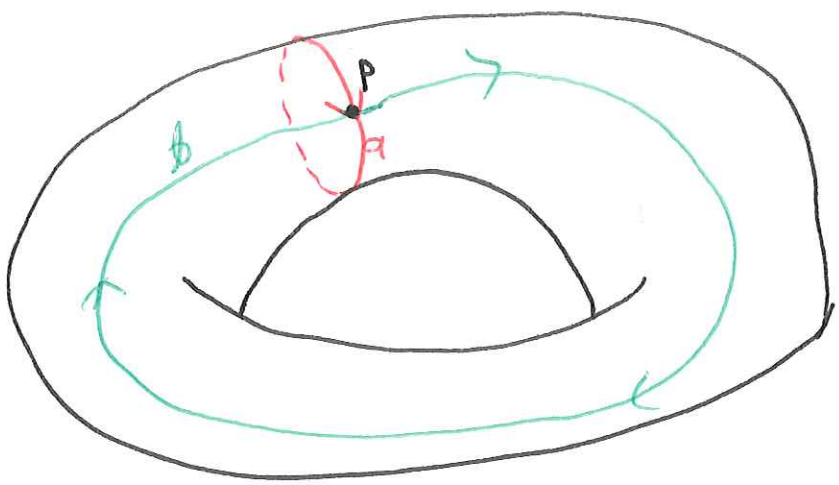
homotopic!

$\mathbb{R}^2 \setminus$ two holes



torus

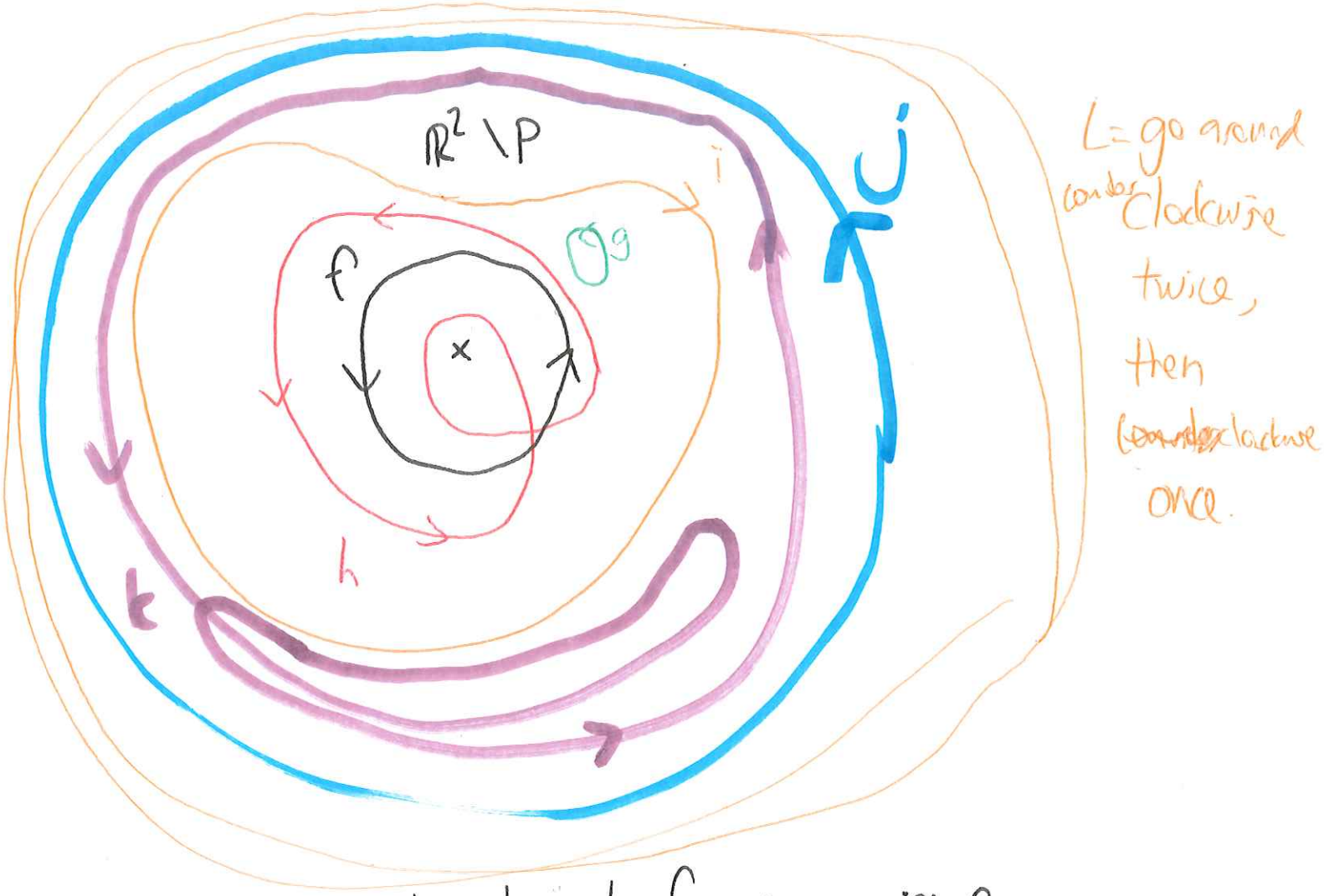
$a, b : S^1 \to T^2$



$f =$ start at p, follow a, then follow b.

$g =$ start at p, follow b, then follow a.

f, g homotopic! (see video)



j homotopic to f i.e. $j \simeq f$

$j \star f$

for a loop $S^1 \to \mathbb{R}^2 \setminus p$

the <u>degree</u> is the number of times it goes around the hole (negative if you go opposite direction)

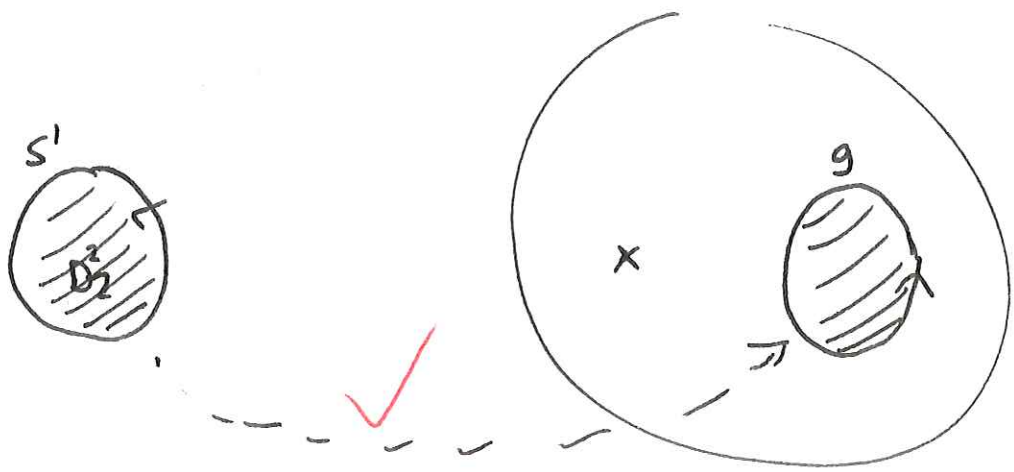
<u>Theorem:</u> Two loops are homotopic if and only if they have the same degree.

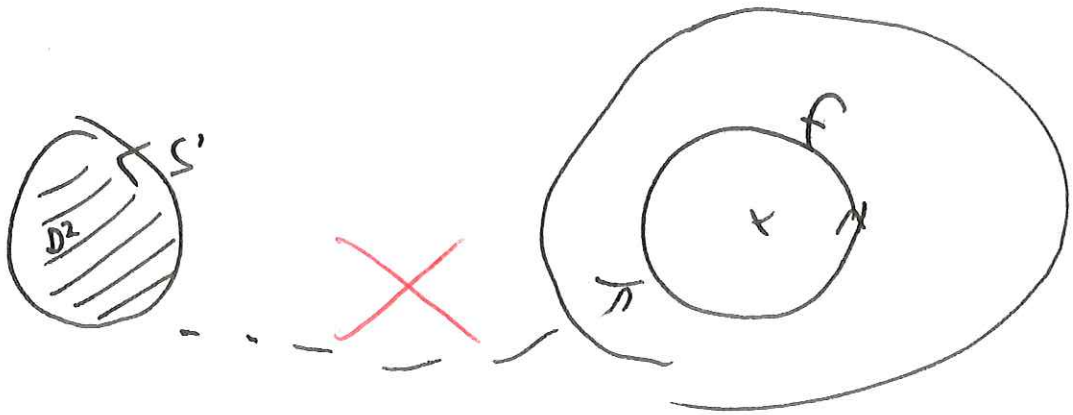
Let's say we have a loop

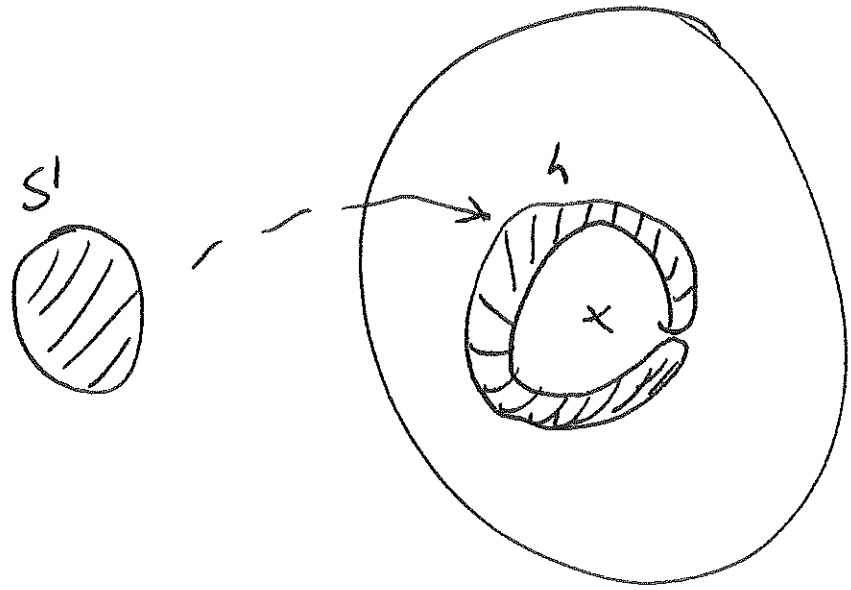
$$\underset{\text{unit circle}}{S^1} \longrightarrow \underset{\text{punctured plane}}{\mathbb{R}^2 \setminus P}$$

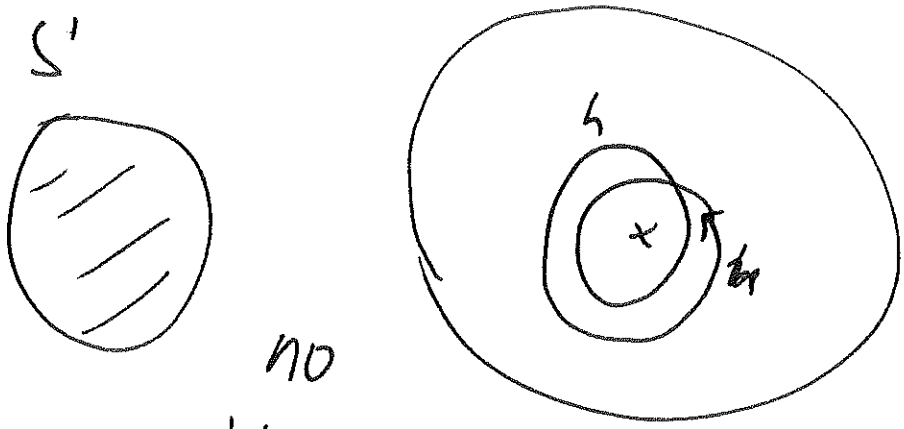
When can we "fill it in" at get a function

$$\underset{\text{unit disk}}{D^2} \longrightarrow \mathbb{R}^2 \setminus P ?$$









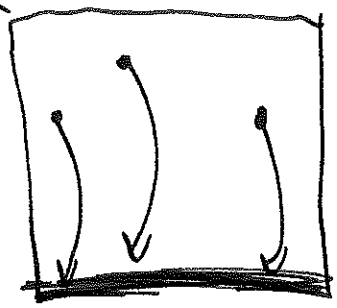
no way to extend

<u>Theorem</u> If $f : S^1 \to \mathbb{R}^2 \setminus p$ has degree 0, it can be extended to D^2. If degree not 0, it can't.

Def Suppose $A \subset X$ is a subset.

A <u>retraction</u> of X to A is a continuous function $f: X \to A$ with $f(a) = a$ for all $a \in A$. "smush X onto A"

X = unit square $\{(x,y) : 0 \le x \le 1,\ 0 \le y \le 1\}$

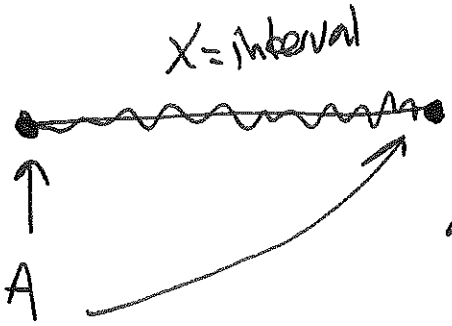


$f(x,y) = (x, 0)$

$A = \{(x,0) : 0 \le x \le 1\}$

How about X = annulus.

can we retract it to C_1?



a retraction would be a continuous function

$$f : [0,1] \to \{0,1\}$$

interval — two pt set

$f(a)=a$ means $f(0)=0$, $f(1)=1$

<u>NO</u>

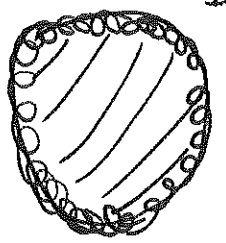
Intermediate value theorem!

Möbius strip onto edge?

<u>no retraction theorem!</u>

No retraction theorem

D^2 can't ~~contract~~ retract onto S^1.



S^1

Pf. Image you could retract it:

$$f : D^2 \to S^1$$

$f(a) = a$ for $a \in S^1$.

that mean you extended the function $f : S^1 \to S^1 \subset \mathbb{R}^2 \setminus P$

$f(\theta) = \theta$

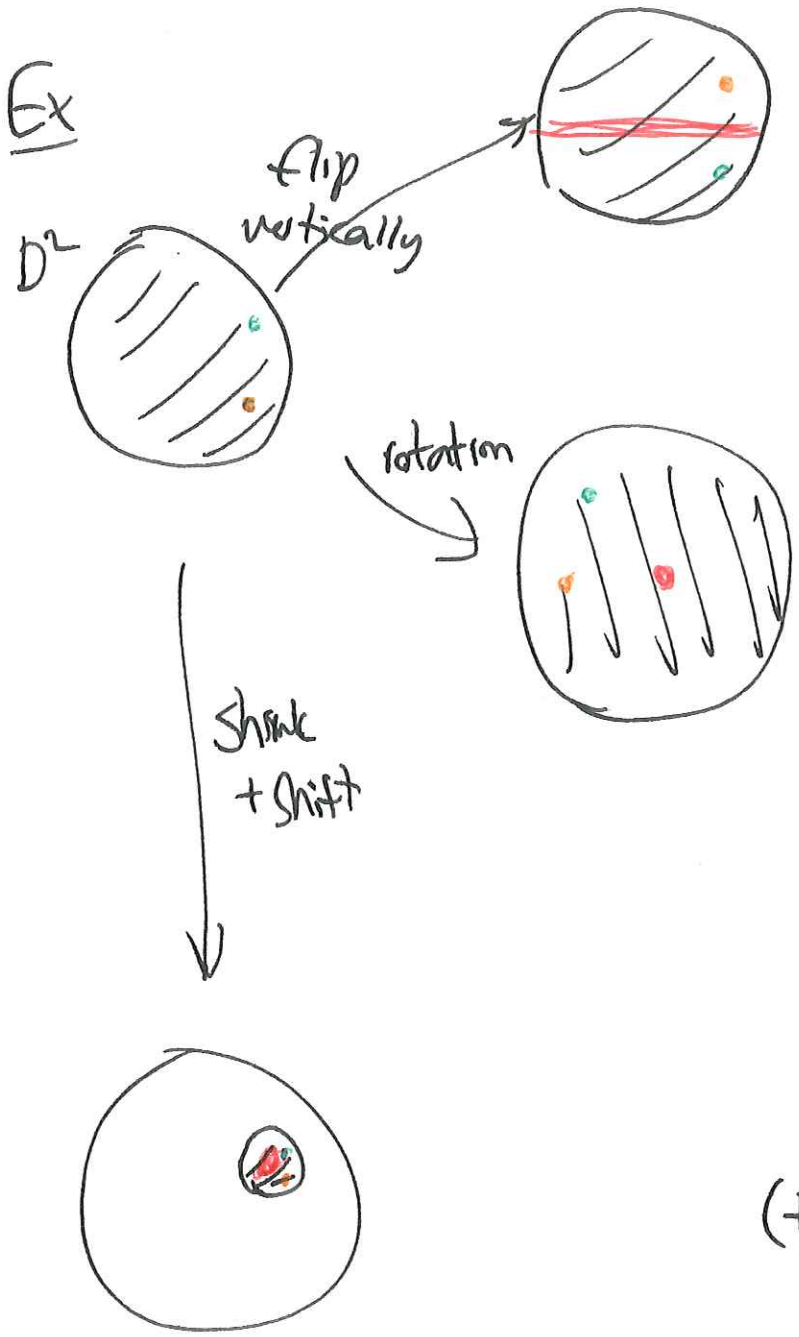
to have domain D^2.

Brouwer fixed point theorem

Any continuous function $f: D^2 \to D^2$ has a fixed pt.

$f(x) = x$

Ex

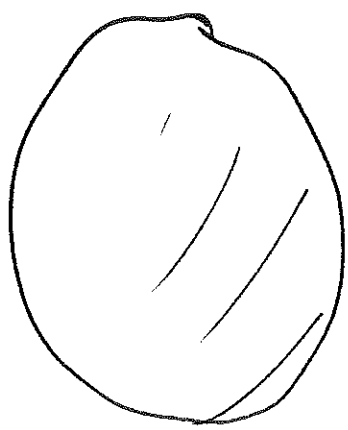


(+ the map thing)

Proof

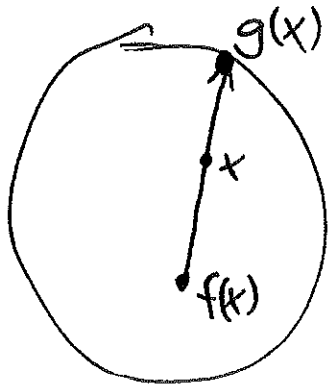
Suppose have continuous function

$f: D^2 \to D^2$ with no fixed points

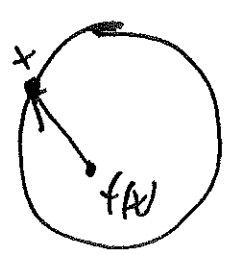


Define $g: D^2 \to S^1$ as follows:

- Given x,
- draw x, $f(x)$ (two different points)
- draw ray ~~f(x)~~ from $f(x)$ to x, see where hits edge. that's $g(x)$



If x is on edge S^1 already:



$g(x) = x$

This means we have:

$g: D^2 \to S^1$ which is continuous,

and $g(x) = x$ if $x \in S^1$.

This is a retract of D^2 onto S^1, impossible!

<u>Next time</u>(?)

1) Ham sandwich

2) Dirac's belt

3) Fundamental thm of algebra

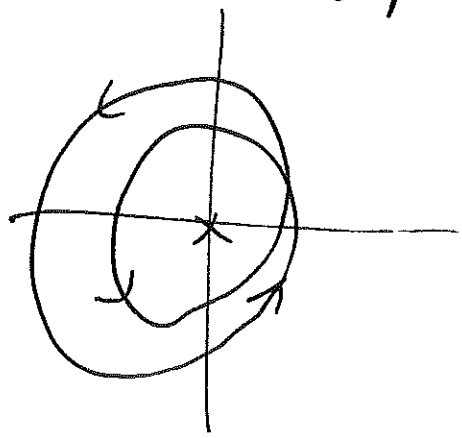
4) Topological analysis.

Homotopy & Degree

Reminder:

if you have a function $f : S^1 \to \mathbb{R}^2 \setminus p$

loop in the plane



the <u>degree</u> is $\deg(f)$ is number of times it goes around the hole.

Fact: Two loops f, g are homotopic if and only if they have the same degree.

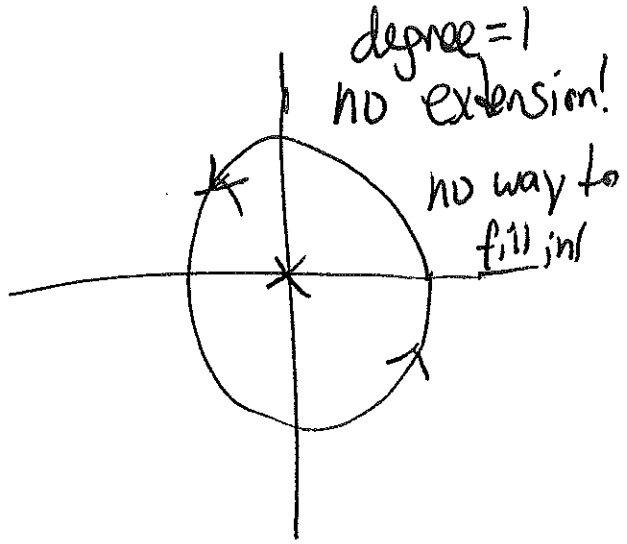
Fact #2:

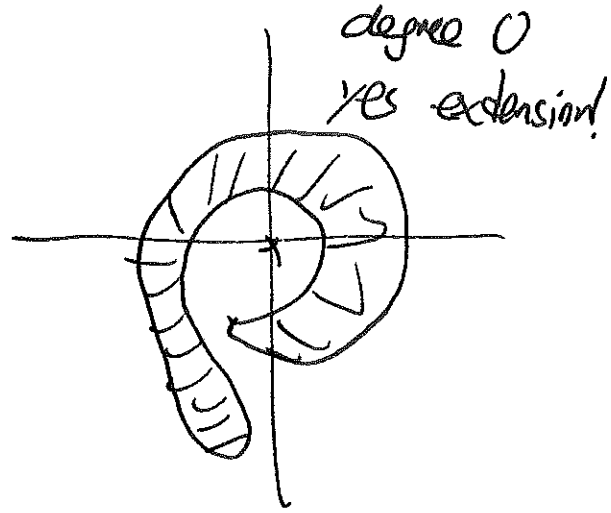
$$f : S^1 \to \mathbb{R}^2 \setminus P$$

can be extended to

$$\tilde{f} : D^2 \to \mathbb{R}^2 \setminus P$$

if and only if degree is 0.





The fundamental theorem of algebra

If $p(x)$ is a nonconstant polynomial with complex coefficients, then $p(x)$ has a (complex) root.

We had polynomial x^2+1, no roots.

So we invented a root: i.

This lets us solve <u>every</u> polynomial. That's crazy!

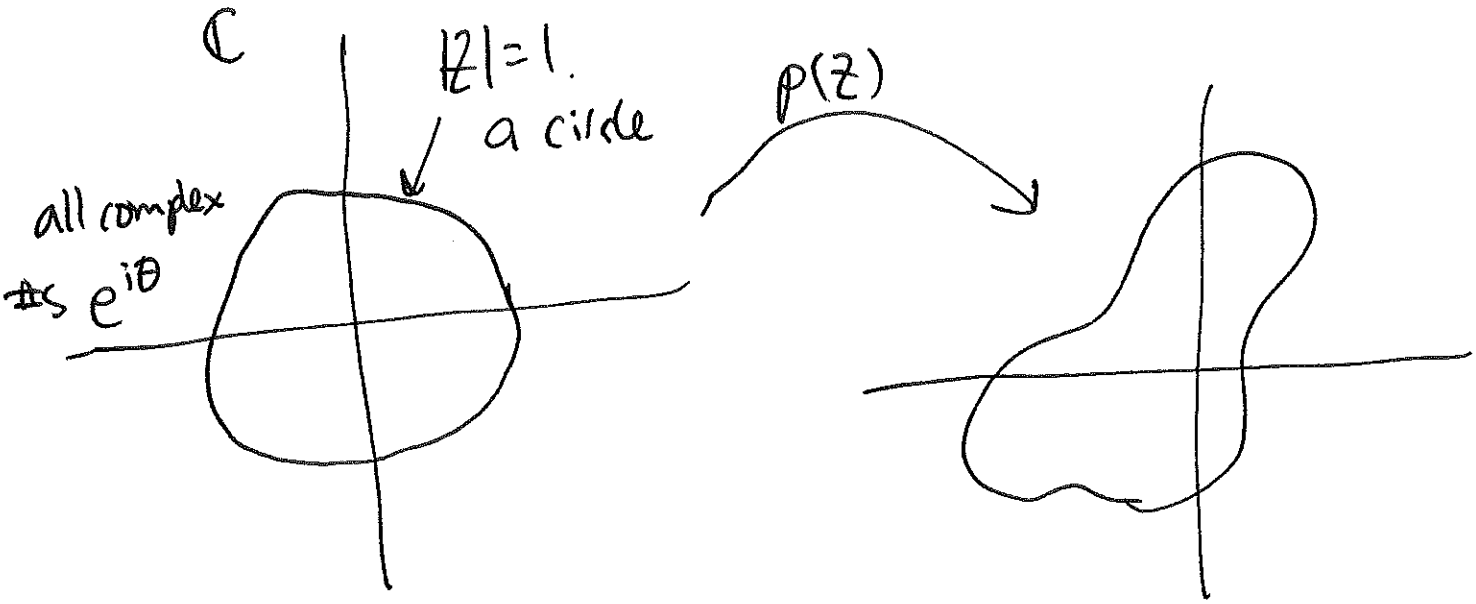
Just adding $\sqrt{2}$ to $\mathbb{Q}$ (for example) still creates many unsolvable things

Idea:

z = complex variable

Any time you have a polynomial $p(z)$

I can turn it into a loop:



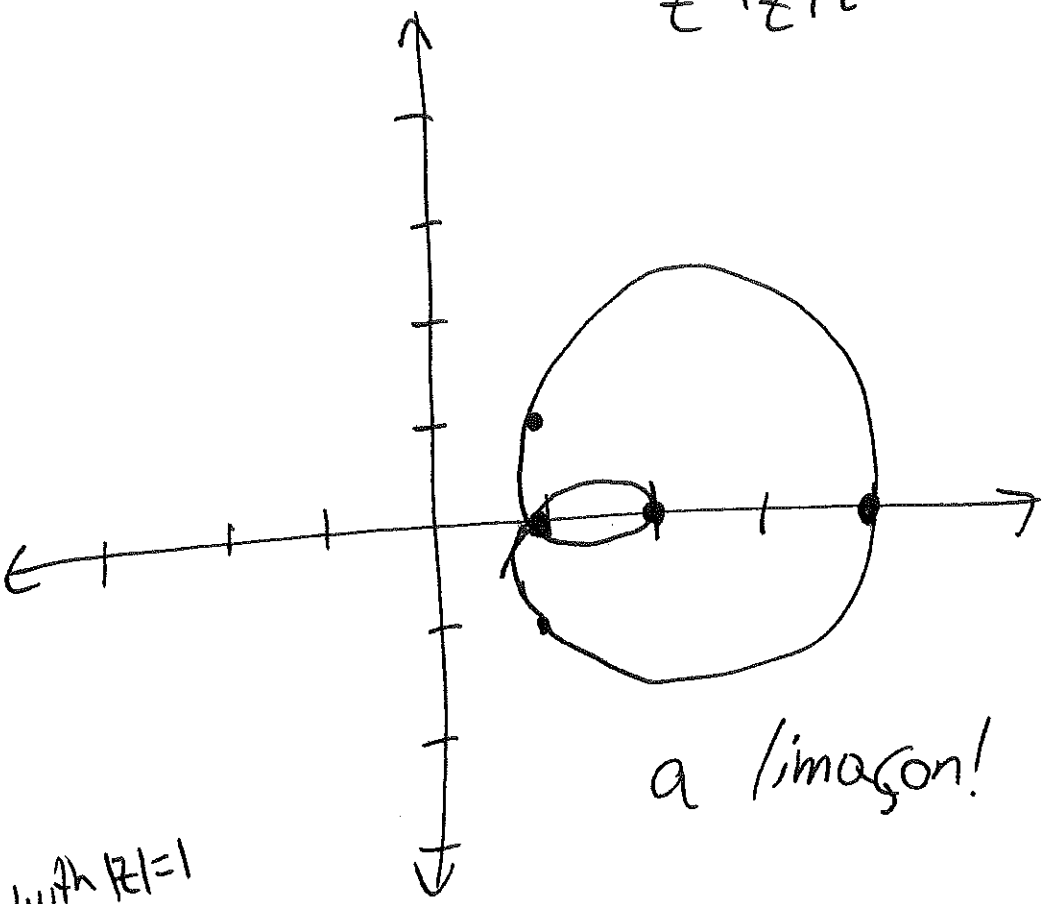
Q What's the loop corresponding

to

$$p(z) = z^2 + z + 2$$

?

z^2+z+2



a limaçon!

with $|z|=1$

z	$p(z)$
1	4
-1	2
i	$1+i$
$-i$	$1-i$
$e^{i\cdot 120^\circ}$	1

(tried lots on computer)

degree & path changes for different quadratics.

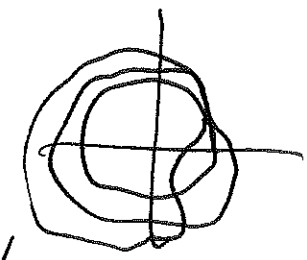
e.g shift limaçon left/right by adding constants.

What about z^3? $(e^{i\theta})^3 = e^{3i\theta}$

goes around 3 times. $\Rightarrow$ degree 3

What if we look at a polynomial like

$$z^3 + 0.1z^2 - 0.2z + 0.01$$



$\Rightarrow$ just adds a little wiggle to z^3 loop, but degree still 3.

Conclusion:

$$\text{for } z^n + \overbrace{(\quad)z^{n-1} + \cdots + \cdots}^{\text{all the coefficients very small}}$$

we get a loop of degree n,

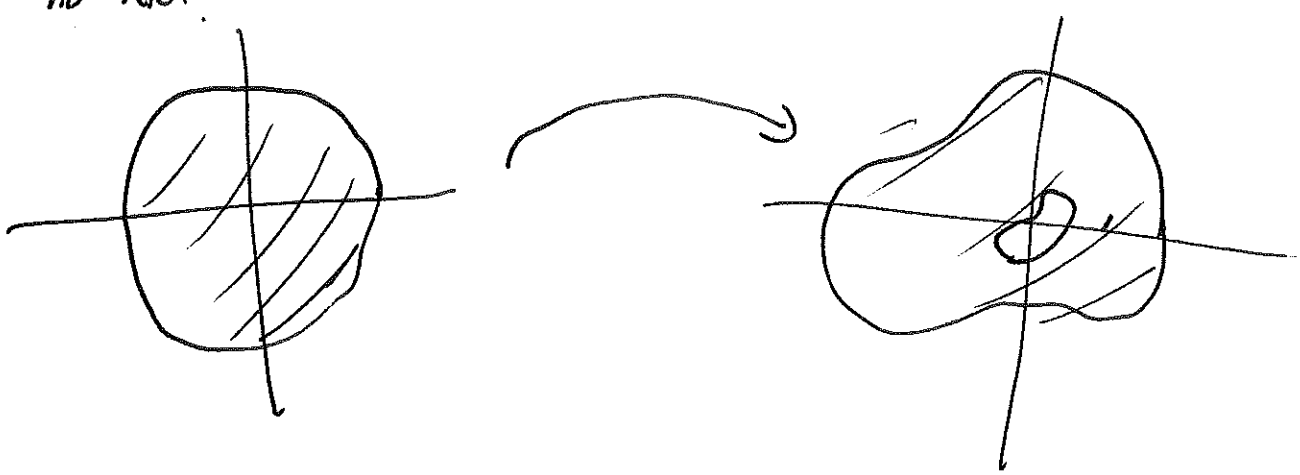
since it's just a wiggle of the z^n loop.

Here's the trick:

Suppose $p(z) = z^n +$ (terms with small coefficients)

has no root: there's no complex number z_0 with $p(z_0) = 0$.

Then we can extend the loop for $p(z)$ to a map from the disk, which misses $(0,0)$ since p had no root.



Impossible! Can't extend for degree n loop unless $n=0$.

$\rightarrow$ A polynomial $p(z) = z^n +$ (small stuff) must have a root!

But every polynomial can be turned into z^n+small stuff.

$$z^3+3z^2-7z+4=0$$

Let $y = z/1000$.

then

$$(1000y)^3+3(1000y)^2-7(1000y)+4=0$$

$\div 10^9$

$$y^3+\frac{3}{1000}y^2-\underbrace{\frac{7}{1000000}y+\frac{4}{1000000000}}_{\text{all small}}=0$$

that has a root y_0 by degree,

so our original does too:

$z_0 = 1000y_0$.

Borsuk-Ulam theorem (run-up to hom sandwich)

Suppose $f: S^2 \to \mathbb{R}^2$ is continuous.

the opposite point on sphere.

Then there's an x such that $f(x) = f(-x)$

Ex.

$$f\begin{pmatrix}\text{a point on} \\ \text{Earth}\end{pmatrix} = \begin{pmatrix}\text{temperature} & \text{humidity at} \\ \text{at } x, & x\end{pmatrix}$$

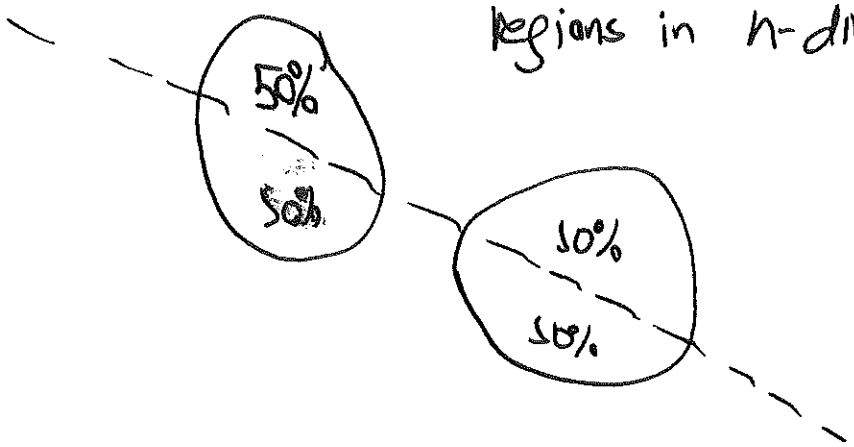
Let's just believe this for now.

(has to do with degree)

Assume B-U theorem

Ham sandwich theorem.

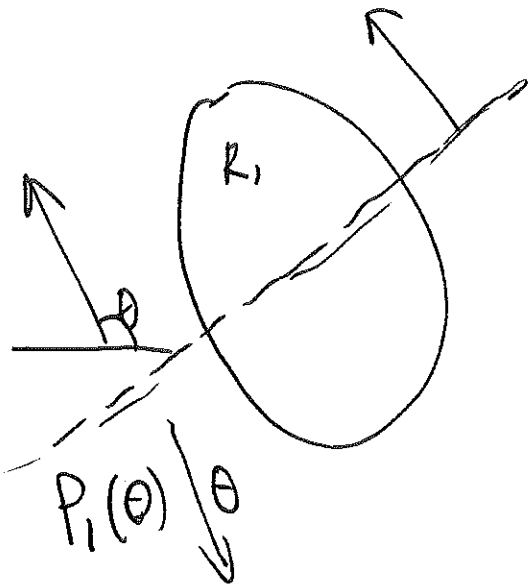
Say we have n regions in n-dimensional space.



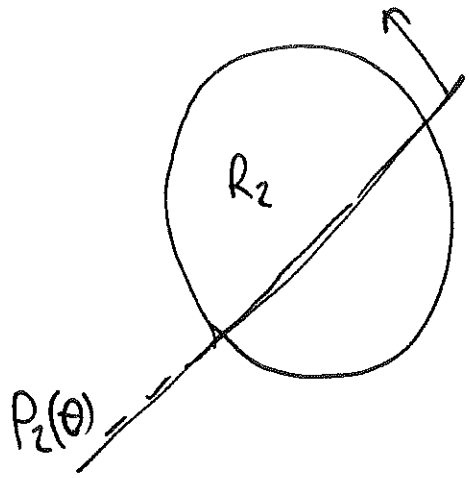
Can make a cut that splits every region in half.

2D proof.

2D proof



for any angle θ, you can find a ~~plane~~ cut $P_1(\theta)$ ~~cutting~~ with normal direction θ which cuts R_1 in half, and a ~~plane~~ cut $P_2(\theta)$ with normal θ which cuts R_2 in half.



$d(\theta)<0$ here.

goal: Show there's a θ where the two are the same.

Define a function $d(\theta)$ = distance between parallel planes $P_1(\theta)$ & $P_2(\theta)$

positive if $P_2(\theta)$ is in positive normal direction from $P_1(\theta)$

negative if $P_2(\theta)$ is in negative direction.

What if we use $-\theta$? $P_1(\theta)=P_1(-\theta)$

$P_2(\theta)=P_2(-\theta)$

$d(\theta)=-d(-\theta)$

$d: S^1 \to \mathbb{R}$

Sp:

2D Borsuk-Ulam theorem:

If $f: \overset{\text{circle}}{S^1} \to \mathbb{R}$, there's an x so $f(x)=f(-x)$

Applying to our d function from before:

There's a θ so $d(\theta)=d(-\theta)$

But we know: $d(\theta)=-d(-\theta)$.

This means $d(\theta)=0$! So $P_1(\theta)=P_2(\theta)$!

So cut at this angle θ: the two planes agree.

For 3D one let

For 3D,

given a point on sphere S^2, think of it as giving a normal direction $\hat{n}$.

find arcs $P_1(\hat{n})$, $P_2(\hat{n})$, $P_3(\hat{n})$ cutting regions in half. (want to find $\hat{n}$ that makes them the same.)

Define $d_{12}(\hat{n}) =$ signed distance $P_1(\hat{n})$ & $P_2(\hat{n})$

$d_{13}(\hat{n}) =$ distance $P_1(\hat{n})$ & $P_3(\hat{n})$.

$\longrightarrow$ Gives us

$$d : S^2 \to \mathbb{R}^2$$

$$d(\hat{n}) = (d_{12}(\hat{n}), d_{13}(\hat{n}))$$

$\cancel{d(\hat{n}) = -d(-\hat{n})}$

$d(-\hat{n}) = -d(\hat{n})$.

BU tells us there's an $\hat{n}$ so $d(\hat{n}) = d(-\hat{n})$ as before.

so $d(\hat{n}) = 0$, all three the same.

Today

- Finish topology
- Construct $\mathbb{R}$

The belt trick

$SO(3) = \{$ all 3×3 rotation matrices $\}$

what does it do to a vector? rotate it!

you can specify axis + angle

as a matrix

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

$T((0,0,1))$

$T((0,1,0))$

$T((1,0,0))$

rotation matrix?

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & -2 \end{pmatrix}$$

not rotation matrix! det is -2.

$SO(3)$ is a subset of all 3×3 matrices.

A twisted up belt with buckle + end in fixed orientations can be thought of as specifying a path in $SO(3)$

$$f : [0,1] \to SO(3)$$

ie it specifies a matrix M_t for any $t \in [0,1]$.

$$M_t = \left\{ \begin{array}{l} \text{what rotation happens to action} \\ \text{figure glued at position } t \text{ on the} \\ \text{belt} \end{array} \right\}$$

Moving the belt changes the path in a continuous way $\rightsquigarrow$ homotopy.

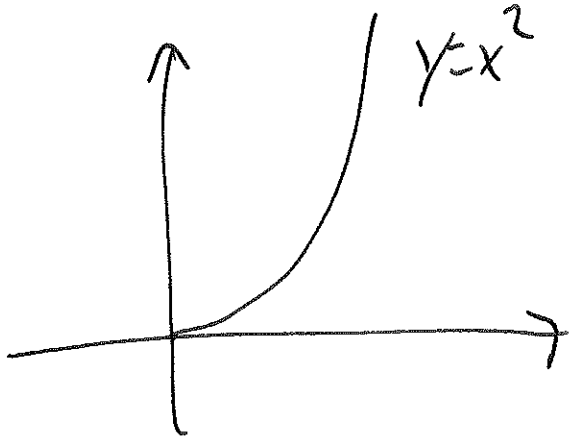
the path from 1x twisted belt $\longrightarrow$ can't be homotopied to constant path / not contractable

2x twisted belt $\rightsquigarrow$ can be homotopied to identity

<u>Fundemental group?</u>

Constructing $\mathbb{R}$

- How to prove intermediate value theorem?
- It works for $\mathbb{R}$ but not $\mathbb{Q}$, that's weird.



$f(0)=0$

$f(2)=4$

but there's no $0<a<2$ with $f(a)=2$...

(if you only know $\mathbb{Q}$)

- To prove it, you really need to know what a real number is.

But what's a real number?

- Everything that can be expressed as a (maybe infinite) decimal.
  - What's an infinite decimal?
  - 1.29999...

    1.30000...

We're going to start with natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$

How to define them?

<u>Peano's Postulates</u> There exists a set $\mathbb{N}$ with an element ($\in \mathbb{N}$) and a function $s: \mathbb{N} \to \mathbb{N}$ with three properties:

"successor"

a) There is no $n \in \mathbb{N}$ such that $s(n) = 1$.

b) The function s is injective (i.e. "one-to-one")

[if $s(a) = s(b)$ then $a = b$]

induction

c) Let $G \subseteq \mathbb{N}$ be a subset. Suppose $1 \in G$ and that ~~if~~ for all $g \in G$ ~~then~~ we have $s(g) \in G$. Then $G = \mathbb{N}$.

<u>Q's:</u>

- Are these even consistent?
- What's a "set" or a "function" anyway?

How to define addition of natural numbers?

$$\mathbb{N} = \{1, s(1), s(s(1)), s(s(s(1))), \ldots\}$$

$$s(1) + s(s(1)) = ?$$

<u>Theorem</u> (we'll skip).

Assuming Peano axioms there's a unique binary operation $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that

some element of $\mathbb{N}$ ie. $s(s(s(s(\cdots(1)))))$

a) $n + 1 = s(n)$

b) $n + s(m) = s(n+m)$

why not $n + (m+1) \overset{\text{by a)}}{=} (n+m) + 1$ associative, but we don't know that yet!

Now we prove basic facts about addition, ...

<u>Thm</u> ~~Suppose $(a+b)+c =$~~

$$(a+b)+c = a+(b+c) \quad \text{associativity}$$

<u>Pf.</u> Suppose $a, b \in \mathbb{N}$ are fixed.

Let $G = \{c \in \mathbb{N} : (a+b)+c = a+(b+c)\}$

(goal: show $G = \mathbb{N}$ using 3rd Peano Postulate)

First show $1 \in G$ i.e. $(a+b)+1 = a+(b+1)$

$$(a+b)+1 \overset{\text{def of } +}{=} s(a+b) \overset{(b)}{=} a+s(b) \overset{(a)}{=} a+(b+1)$$

Suppose $c \in G$. Let's prove $s(c) \in G$ (then done)

Need to show: $(a+b)+s(c) = a+(b+s(c))$

Pf

$$(a+b)+s(c) \overset{(b)}{=} s((a+b)+c) = s(a+(b+c))$$

since $c \in G$.

$$\overset{(b)}{=} a+(s(b+c)) \overset{(b)}{=} a+(b+s(c))$$

so $s(c) \in G$.

What about $a+b=b+a$?

<u>Next time:</u> - Define $\mathbb{Z}$, from $\mathbb{N}$

- Define $\mathbb{Q}$, from $\mathbb{Z}$

- Define $\mathbb{R}$, from $\mathbb{Q}$

Is $R \in R$?

<u>Sets:</u> - Russell's Paradox:

Let $R = \{$all sets X such that $X \notin X\}$

a set can contain other sets: $\{3, \{1,2\}\}$

- countability

- Banach-Tarski paradox.

Today:

- Finish defining real numbers straight from axioms.

- Countable vs uncountable

Last time: $\mathbb{N}$ defined using Peano Postulates.

d) There's a set $\mathbb{N}$ with an element 1 and a function $s: \mathbb{N} \to \mathbb{N}$ such that

a) No $n \in \mathbb{N}$ has $s(n) = 1$

b) s is injective

c) (induction, basically)

Then we defined $+$: there's unique binary operation $+$ such that:

a) $n + 1 = s(n)$

b) $n + s(m) = s(n+m)$

Then
(Prove all the basic rules using just these...)

- $a+b=b+a$
- $a+(b+c)=(a+b)+c$

...

We can also define "<":

Say $m<n$ if $m+a=n$ for some $a \in \mathbb{N}$.

(Prove all properties of $<$: $a<b$ and $b<c \Rightarrow a<c$)

Then define multiplication:

There's a unique binary operation $\times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

Satisfying

a) $n \times 1 = n$

b) $n \times s(m) = n \times m + n$

Then check distributive law, ...

Now:

Integers

One suggestion:

An integer is an ordered pair of natural numbers $[a,b]$ where $a =$ either 1 or 2 or 3

if $a = 1 \longrightarrow$ represents integer 0

$a = 2 \longrightarrow$ represents integer b

$a = 3 \longrightarrow$ represents integer $-b$

Now we need to define addition for integers:

$$[a,b] + [c,d] = \begin{cases} [2, b+d] \text{ if } a=c=2 \\ [3, b+d] \text{ if } a=c=3 \\ [a,b] \text{ if } c=1 \\ [2, b-d] \text{ if } a=2,\ c=3, \text{ and } b>d \\ \cdots \end{cases}$$

or combine

$[2,5]+[2,3]=[2,8]$

$[1,3]+[1,4]=[1,7]$

$[2,5]+[1,4]=[2,5]$

$[2,5]+[3,4]=[2,1]$

$[2,5]+[3,6]=[3,1]$

Then you need to check that addition satisfies all the axioms:

$$(x+y)+z = x+(y+z)$$

define multiplication too, check the axioms, ...
(lots of cases!)

There is a little slicker way: let $[a,b]$ (natural) to represent the integer $a-b$.

Downside: $[a,b]$ and $[c,d]$ represent same thing if $a+d=b+c$.

$$[1,4]=[2,5]=[3,6]=\cdots$$

Upside: No cases to define addition now:

$$[a,b]+[c,d]=[a+c,\ b+d]$$

Def

A rational number is an ordered pair $[a,b]$ of integers. (In our heads: $[a,b]$ represents a/b)

$[a,b]$ and $[c,d]$ represent same rational number if $ad-bc=0$.

$a/b \stackrel{?}{=} c/d$

$ad=bc$

Then define $+$, $\times$, $<$:

$[a,b]\times[c,d]=[ac,bd]$ $\quad$ $a/b \times c/d = ac/bd$

$[a,b]+[c,d]=[ad+bc,bd]$ $\quad$ $a/b + c/d = \frac{ad}{bd} + \frac{cb}{bd} = \frac{ad+bc}{bd}$

Then check associativity, distributive, commutative work for rational numbers using these rules!

At last: real numbers $\mathbb{R}$

A subset $A \subset \mathbb{Q}$ is called a <u>Dedekind cut</u>

if it has three properties:

a) $A \neq \phi$, $A \neq \mathbb{Q}$
notempty

b) If $x \in A$, and $y \in \mathbb{Q}$ has $y \geq x$, then $y \in A$ too.

c) If $x \in A$, there's some $y \in A$ so $y < x$ and $y \in A$ too.

<u>Examples</u>

positive rational numbers

$A_0 = \{x \in \mathbb{Q} : x > 0\}$ is a Dedekind cut

$A_{1/2} = \{x \in \mathbb{Q} : x > \frac{1}{2}\}$ is a Dedekind cut

$A_q = \{x \in \mathbb{Q} : x > q\}$ is a Dedekind cut

But

$$A = \{x \in \mathbb{Q} : \overset{x>0 \text{ and}}{x^2 > 2}\}$$ is a Dedekind cut

<u>Def</u> The real numbers $\mathbb{R}$ is the set of all of Dedekind cuts.

What's the Dedekind cut corresponding to $-\sqrt{2}$?

$$A_{-\sqrt{2}} = \{x \in \mathbb{Q} : x^2 < 2 \text{ or } x > 1\}$$

then define $\times$, $+$, $<$ for Dedekind cuts, etc.

Two sets A, B are ~~in object~~

the same size if you can find a one-to-one correspondence between elements of A and elements of B.

<u>Ex</u> $\overset{\text{natural}}{\mathbb{N}}$ and $\overset{\text{integers}}{\mathbb{Z}}$

$$\begin{array}{cccccccccccccc}
 & & & & & & & & & & & & & \mathbb{N} \\
 & 9 & 7 & 5 & 3 & 1 & 2 & 4 & 6 & 8 & & & & \\
 & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & & & \\
-5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & & \mathbb{Z}
\end{array}$$

Try it: which of these can you pair off with $\mathbb{N}$ (or with each other)

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $(0,1)$, $[0,1)$, $\mathbb{Z}^2$ (ordered pairs)

$\mathbb{R}^2$, polynomials with integer coefficients, sequences of integers, ..., $\{x \in \mathbb{Q} : 0 < x < 1\} = (0,1)_{\mathbb{Q}}$

I suggest: trying

$\mathbb{R}$ and $(0,1)$

$\mathbb{N}$ and $\mathbb{Z}^2$

$\mathbb{N}$ and $\mathbb{Q}$

$(0,1)$ and $[0,1)$

Sometimes not possible!

$(0,1)\times(0,1)$ vs $(0,1)$

ordered pairs (a,b) with both between 0 & 1.

e.g. $(0.7, 0.4)$

0.2317241527122304...

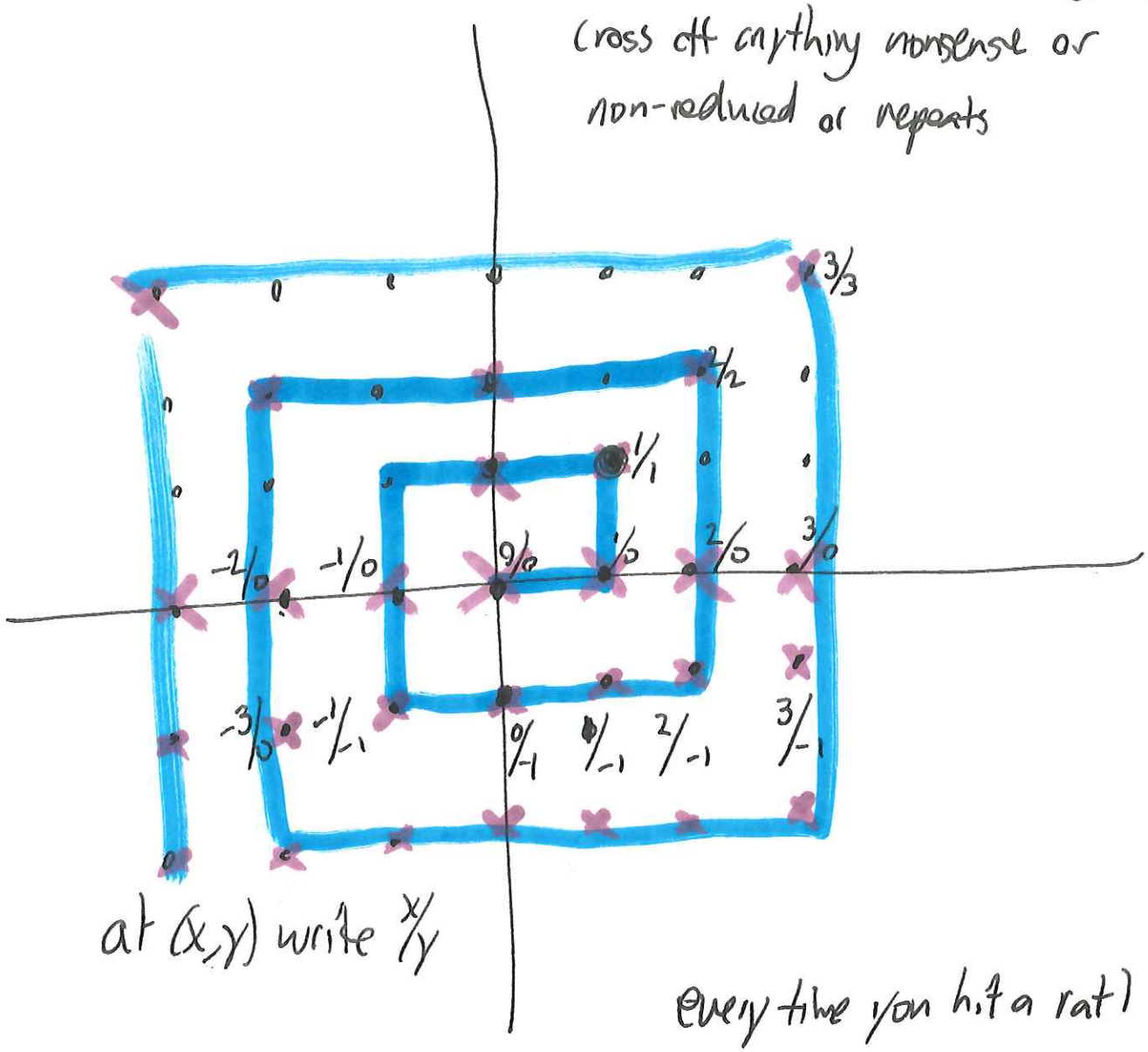
0.1126675689891 66...

$\updownarrow$ interlace the digits!

0.2131127626471 5...

$\mathbb{N}$ vs $\mathbb{Q}$

list all ratl numbers in a grid, cross off anything nonsense or non-reduced or repeats



at (x,y) write x/y

every time you hit a ratl that's not crossed out, add to list

$1/1,\ 0/1,\ -1/1,\ 2/1,\ 1/2$

→ Two sets are the "same size" if you can find a one-to-one correspondence between them.

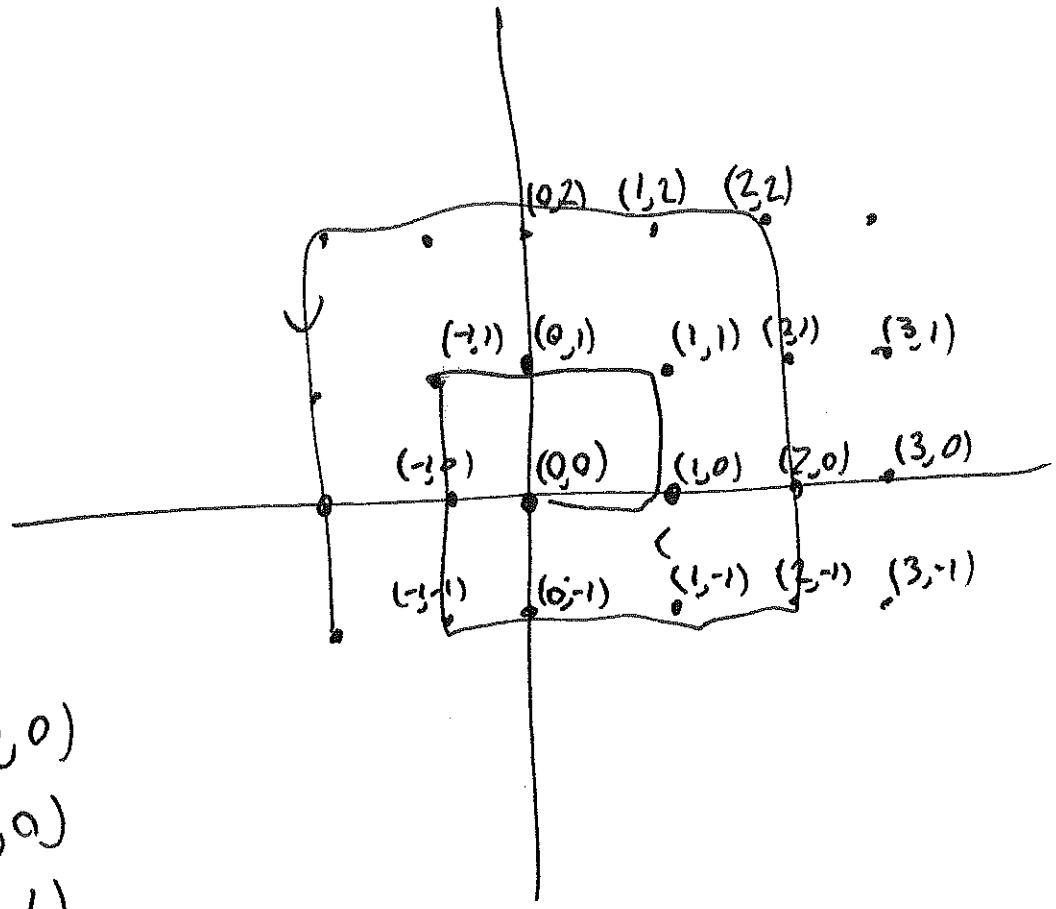
→ A set is called "countable" if it's the same size as $\mathbb{N}$.

$$\begin{array}{ccccccccc} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, \ldots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0, & 1, & -1, & 2, & -2, & 3, & -3, & 4, & -4, \ldots \end{array}$$

integers are countable!

What about $\mathbb{Z}^2$, ordered pairs of integers?

also countable!



(0,0)
(1,0)
(1,1)
(0,1)
(-1,1)
(-1,0)
⋮

Last time:

$\mathbb{Q}$ countable

rational numbers

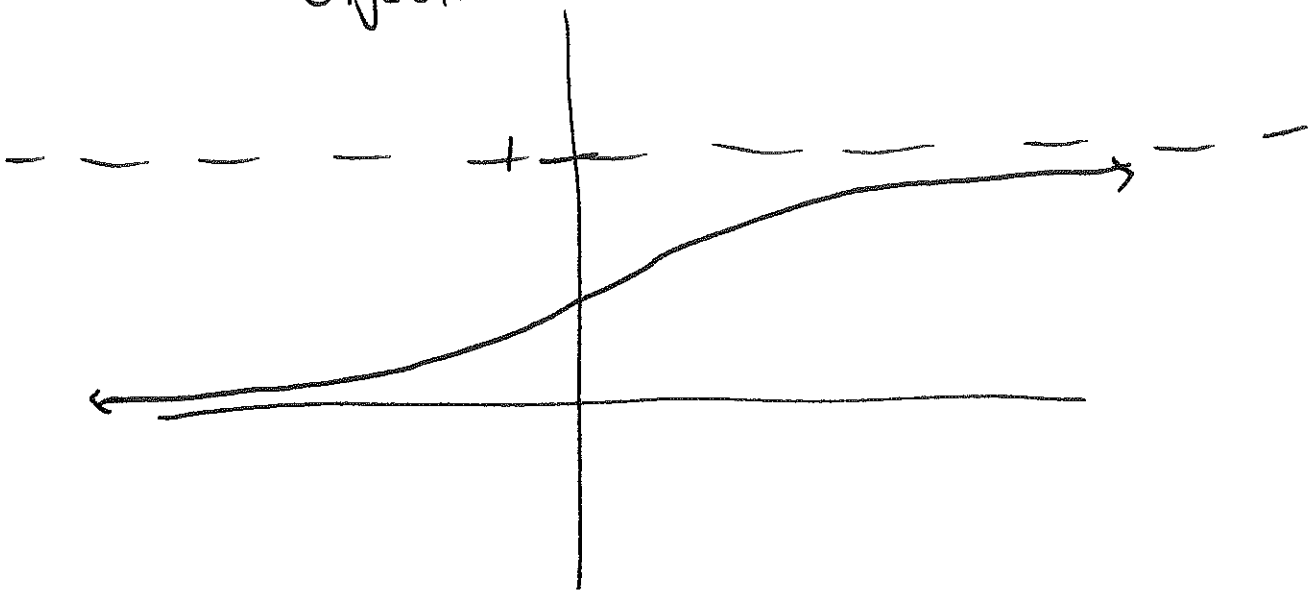
Digression on "jective" terminology.

Cantor-Schroder-Bernstein:

If you have two sets X and Y and you can find ~~one-to-one~~ injective maps $f: X \to Y$, $g: Y \to X$, then there exists a ~~onto~~ bijective $h: X \to Y$

$\mathbb{R}$ and $(0,1)$?

bijection:



$f(x) = \frac{1}{\pi}\tan^{-1} x + \frac{1}{2}$ (or something like that)

But are there infinite sets not of the same size? Are some infinities bigger than others?

Cantor-Schroder-Bernstein:

If there exist injective maps

$f: X \to Y$ and $g: Y \to X$

then there exists a bijection $h: X \to Y$.

$[0,1)$ and $[0,1) \times [0,1)$

$(0.3141592653\ldots, 0.1234567891011\ldots)$

$\updownarrow$ interweave

$(0.31124315\ldots)$

$\mathbb{R}$ and $\mathbb{N}$.

No bijection is possible!

"Cantor's diagonalization argument"

<u>Proof</u>: It's good enough to show no bijection between $(0,1)$ and $\mathbb{N}$. (since $(0,1)$ is in bijection with $\mathbb{R}$).

<u>I</u>magine you could make a list of <u>every</u> real number:

0.(2)137124661 3...

0.1(1)71234588 2...

0.31(7)8124561 23...

0.459(8)97891112...

0.3141(5)926535...

0.27182(8)1828459045...

⋮

We'll prove that the list must have missed some number.

Circle the nth digit of the nth number, and consider the real ~~α~~ number formed by adding one to each digit $(9 \to 0)$

$\alpha = 0.328969\ldots$

I claim that α is not in our list.

It can't be the nth number in the list,

since it has a different n^{th} digit from that number!

<u>Corollary:</u>

There exists a real number that is not rational.

<u>Pf.</u> $\mathbb{R}$ is uncountable, but $\mathbb{Q}$ is countable, so there must be elements of $\mathbb{R}$ that aren't in $\mathbb{Q}$.

"non-constructive proof"

Theorem

$\pi^{(\log_\pi 10)} = 10$

probably irrational but who knows

It's possible to have $\text{irrational}^{\text{irrational}} = \text{rational}$.

($\text{rational}^{\text{rational}} = \text{irrational}$ is easier: $2^{1/2} = \sqrt{2}$)

($e^{i\pi}$ works, but let's say real).

Consider $\overset{x}{\overset{\shortparallel}{\sqrt{2}^{\sqrt{2}}}} \approx 1.6325269\ldots$

Case I: x is irrational

~~done!~~

$$x^{\sqrt{2}} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$$

$\text{irrat}^{\text{irrat}} = \text{rat}$

Case II: x is rational

done! $\sqrt{2}^{\sqrt{2}} = x$ is

$\text{irrat}^{\text{irrat}} = \text{rat}$

So either $\sqrt{2}^{\sqrt{2}}$ or $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$ works, but which is it? Non-constructive.

The Banach-Tarski Paradox

It's possible to take a 3D ball D^3,

~~a~~ cut it into five disjoint parts:

$$D^3 = A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$$

Rotate and translate the parts and rearrange them into two identical copies of the ball:

$$A_1 \cup A_2 = D^3, \qquad A_3 \cup A_4 \cup A_5 = D^3.$$

Q What's an anagram for Banach-Tarski?

A Banach-Tarski Banach-Tarski.

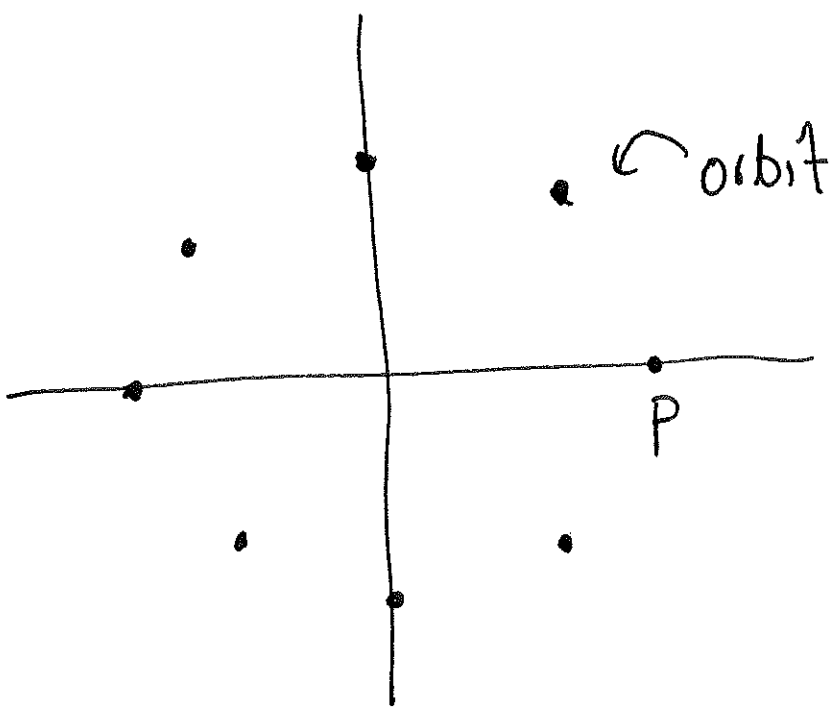
Let G be a set of transformations

e.g. $G = \{$ rotations by a multiple of $\pi/4$ radians $\}$
around origin

If P is a point, the "orbit of P under G"

is the set of all things you can get by applying

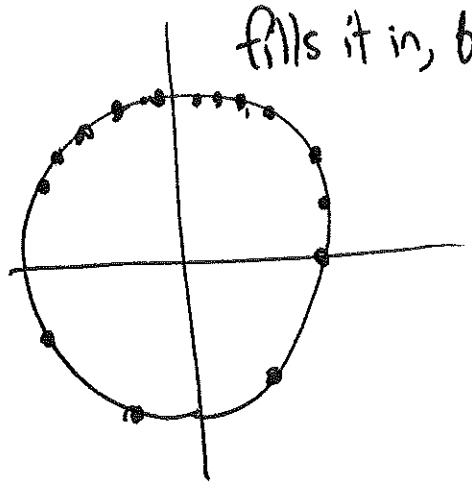
some member of G to P.



What if $G = \{$ rotations by a multiple of 1 radian $\approx 57.29° \}$

P never rotates back where it started!

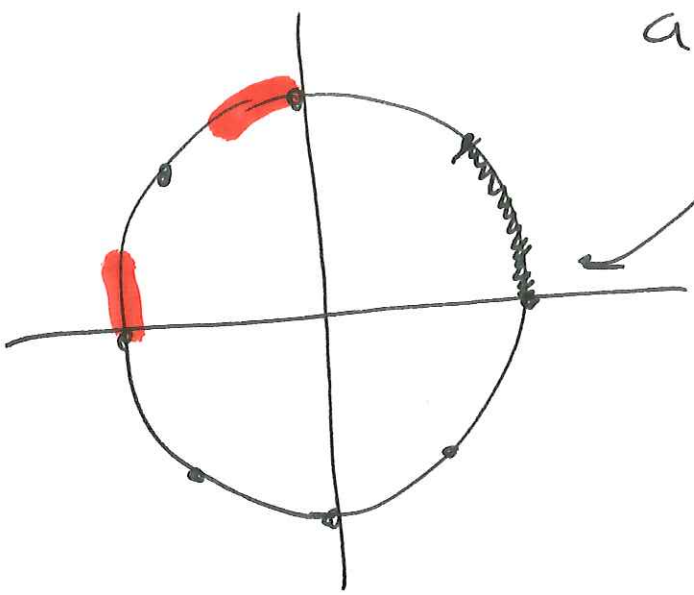
fills it in, but doesn't hit every point!



Terminology: if G is a set of rotations, a "set of orbit representatives for G" is a set of points M so that any x is obtained by apply some element of G to some element of M.

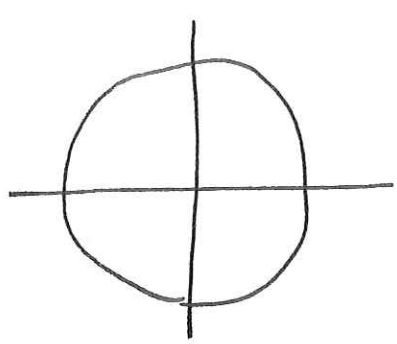
i.e. a set of points M so that any x is obtained by rotating ~~some~~ a unique element of M.
e.g. (subset of circle)

e.g. $G = \{\text{rotations by } \pi/4 = 45^\circ\}$



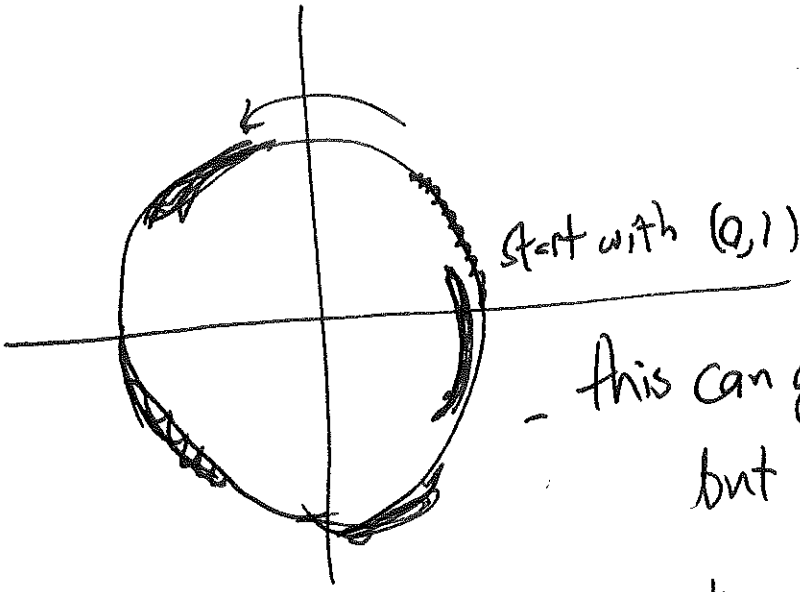
a set of orbit representatives is this arc.

What about orbit representatives for rotation by 1 radian $= \frac{180}{\pi}$ degrees.



does it exist?

A suggestion



- this can get to every point, but there are duplicates.

- any time it overlaps itself, remove extra points from part that overlapped it.

Banach-Tarski

It's possible to divide up the ball D^3:

$$D^3 = A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 \qquad \text{(disjoint)}$$

Rotate and translate the A_i and reassemble into two D^3's.

$$D^3 = A_1 \cup A_2 \cup A_3 \qquad D^3 = A_4 \cup A_5$$

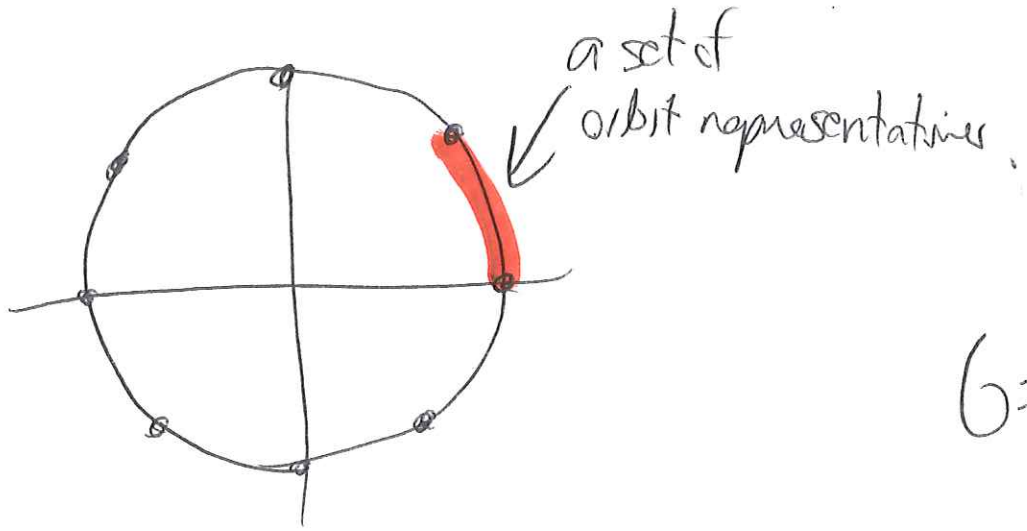
Last time: $G = \left\{ \begin{array}{l} \text{a set of transformations} \\ \text{e.g. all rotations by mult} \end{array} \right\}$
of $\pi/4$ or mults of 1 rad.

(rotations of circle)

Orbit representatives

A set of orbit representatives M for G is a collection of points such that <u>every point</u> can be obtained by applying some transformation in G to a (unique) point in M.

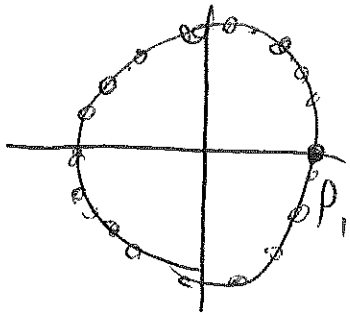
$G = \{\text{rotations by } \pi/4\}$



$G = \{\text{rotations by } 1 \text{ rad}\}$

Can we find a set of orbit reps?

<u>Algorithm:</u> Pick a point P_1 on circle, and delete its full orbit. $\approx \mathbb{R} \setminus \mathbb{Q}$



Pick a remaining point P_2, delete its full orbit. $\approx \mathbb{R} \setminus \mathbb{Q} \setminus \pi\mathbb{Q}$

Keep going until nothing left. ~~What's left is~~ The set $\{P_i\}$ is a set of orbit reps!

Another way to think about it:

G divides up the circle into an ~~infinite~~ infinite partition by orbits.

each O_α is orbit.

$$\underset{\text{circle}}{S^1} = \bigcup O_\alpha$$

Pick a point P_α in each O_α. That's a set of ORS!

combinations of rotation

To represent an transformation in G, you can use a "word" like:

$$A^{-1}B^{3}ABABA^{-2}B^{-3}A$$

first do A

then B^{-1} 3 times

then A^{-1} 2 times.

One rule: a word can't AA^{-1}, $A^{-1}A$, BB^{-1}, $B^{-1}B$.

Let $S(A) \subset G = \{$all words starting with $A\}$

$S(A^{-1})$, $S(B)$, $S(B^{-1})$ similar

$\in S(A^{-1})$

the empty thing

$$G = S(A) \cup S(A^{-1}) \cup S(B) \cup S(B^{-1}) \cup \{e\}$$

$$G = A\,S(A^{-1}) \cup S(A)$$

<u>and</u>

$$G = B\,S(B^{-1}) \cup S(B)$$

First: divide up the sphere S^2:

Let M be a set of orbit representatives for the rotations G on S^2. (Weird set!)
need choice.

$S(A)M =$ all points you can get by applying an $S(A)$ transformation to a point of M.

subset of sphere.

$\underline{S^2 = G\,M}$ ← for every $P \in S^2$, can find $m \in M$ and a rotation g so $g(m) = P$.

$$S^2 = S(A)M \cup S(A^{-1})M \cup S(B)M \cup S(B^{-1}M) \cup M.$$

sphere

five pieces!

What are all words ~~of the form~~ equivalent to:

$$A\,S(A^{-1})$$

$\uparrow$ A

$\uparrow$ followed by a word starting A^{-1}

e.g. BAB is $A(A^{-1}BAB)$. that counts:

$$BAB \in A\,S(A^{-1})$$

$A^{-1}B^2A$ is $A(A^{-2}B^2A)$

$ABBA$ is $A(\underbrace{A^{-1}A}_{\text{not a valid word!}}BBA)$

$A\,S(A^{-1})$ = all words, except those starting with 'A'!

$$S^2 = \overset{F_1}{S(A)M} \cup \overset{F_2}{S(A^{-1})M} \cup \overset{F_3}{S(B)M} \cup \overset{F_4}{S(B^{-1})M} \cup \overset{F_5}{M}$$

points obtained by rotating some point of M where last rotation used is an "A".

things in M

~~What is~~

What do we get if we rotate every element of F_2 by A?

rotated F_2

$$AF_2 = \underbrace{AS(A^{-1})}M$$

$$AF_2 \cup F_1 = \underbrace{AS(A^{-1})}M \cup \underbrace{S(A)}M$$

$$= (AS(A^{-1}) \cup S(A))M = GM = S^2$$

$$BF_4 \cup F_3 = S^2$$

F_5 is extra! (can be fixed)

Axiom of Choice (an candidate axiom of set theory)

Given any collection of sets U_α, ← indexed by reals, integers, who knows

it's possible to choose a p_α in each U_α.

Other axioms of set theory: you can always take union of two sets, etc.

You can use it or not. Choice is not implied by the other axioms of set theory.

(Theorem: assuming choice won't lead to a contradiction.)

You don't always need this axiom to make a choice.

Bertrand Russell: Imagine each U_α is a pair of shoes.

You can always take p_α = left shoe.

But if each U_α is a pair of socks.

You need choice!

Axiom of Choice

$\Updownarrow$

Well-Ordering Principle

$\Updownarrow$

Zorn's Lemma

"obviously true"

"obviously false"

"who knows"

$\Downarrow$

Banach-Tarski

~~First, divide up the sphere S^2:~~

~~Lem~~

To divide up D^3 instead, just use our decomposition of sphere and ~~connect~~ divide up radially. (We'll ignore center.)

<u>Proof for transcendental numbers existing:</u>

- The set of all polynomials with rational coefficients is countable (HW!)
- Each one has only finitely many roots.

$\Longrightarrow$ Algebraic numbers are countable.

$\mathbb{R}$ is uncountable, so non-algebraic numbers must exist!

Proof that π is irrational:

Suppose $f(x)$ is any function

Integrate

$$\int f(x) \sin x \, dx \quad \text{by parts twice.}$$

What do you get?

What is

$$\int_0^{\pi} f(x) \sin x \, dx$$

$u = f'(x)$

$$\int f(x) \sin x \, dx = -f(x) \cos x + \int f'(x) \cos x \, dx$$

$u = f(x)$ $\quad$ $v = -\cos x$

$du = f'(x)\,dx$ $\quad$ $dv = \sin x \, dx$

$= -f(x) \cos x$

Actually finding a transcendental number is hard:

π works.

It's easier to prove:

$$0.1\,1\,0\,0\,0\,1\,0\cdots0\,1$$

1st 2nd 3 4 5 6 24

every n! place put a 1:

$$L = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

"Liouville number" $\rightarrow$ easier to prove it's transcendental.

$$\int f(x) \sin x = -f(x)\cos x + f'(x)\sin x - \int f''(x)\sin x \, dx$$

We'll use this with $f(x)$ a clever polynomial.

Last time:

$$\int f(x)\sin(x)\,dx = -f(x)\cos(x) + f'(x)\sin(x) - \int f''(x)\sin(x)\,dx$$

Plug in $\int_0^\pi$ and we get:

$$\int_0^\pi f(x)\sin(x)\,dx = \left(-f(x)\cos x + f'(x)\sin x\right)\Big|_0^\pi - \int_0^\pi f''(x)\sin x\,dx$$

$$= \left((f(\pi)+0)-(-f(0)+0)\right) - \int_0^\pi f''(x)\sin x\,dx$$

$$= \left(f(0)+f(\pi)\right) - \int_0^\pi f''(x)\sin x\,dx.$$

But:

$$\int_0^\pi f''(x)\sin x\,dx = \left(f''(0)+f''(\pi)\right) - \int_0^\pi f''''(x)\sin x\,dx$$

So:

$$\int_0^\pi f(x)\sin x\,dx = \left(f(0)+f(\pi)\right) - \left(f''(0)+f''(\pi)\right) + \int_0^\pi \cancel{f(x)}\, f''''(x)\sin(x)\,dx$$

Again:

$$\int_0^{\pi} f(x)\sin(x)\,dx = \left(f(0)+f(\pi)\right) - \left(f''(0)+f''(\pi)\right) + \left(f^{(4)}(0)+f^{(4)}(\pi)\right)$$

$$- \int_0^{\pi} f^{(6)}(x)\sin(x)\,dx.$$

We could keep going forever.

But if $f(x)$ is a polynomial: eventually the integral is 0.

Suppose $f(x)$ is polynomial of degree $\underbrace{2n}_{\text{even}}$.

$$\int_0^{\pi} f(x)\sin x\,dx = F(0) + F(\pi)$$

where $F(x) = f(x) - f''(x) + f^{(4)}(x) - \cdots (-1)^n f^{(2n)}(x)$

Suppose $\pi = p/q$ is rational

Our plan: pick a clever $f(x)$ so

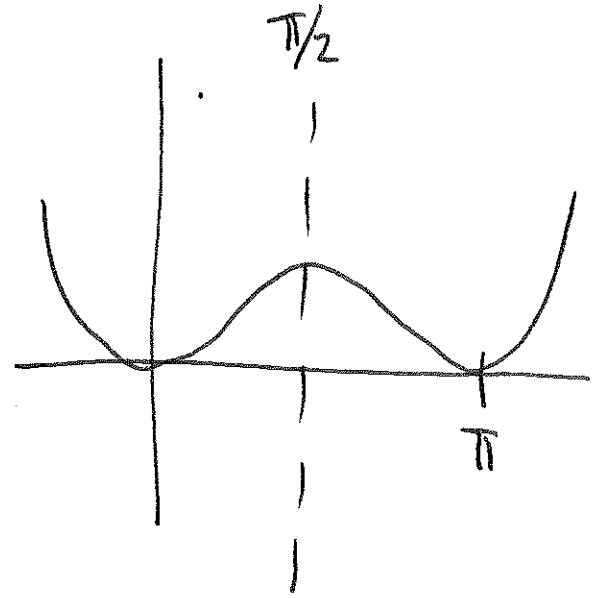
- $0 < \int_0^\pi f(x) \sin x \, dx < 1$

- All derivatives of f at $0, \pi$ are integers

then left side is not integer, but right is integer.

Let $$f_n(x) = q^n \frac{x^n(\pi - x)^n}{n!}$$

Plot:



Also: if $0 < x < \pi$, it's positive.

(this will work for $n \gg 0$)

$$f(x) = f(\pi - x)$$
$$f'(x) = -f(\pi - x)$$
$$f''(x) = f''(\pi - x)$$

I claim: all derivatives of $f(x)$ at 0 & π are integers.

$$\cancel{f_n(x) = \frac{q^n x^n (\pi - x)^n}{n!}}$$ why?

$\pi = p/q$

$$f_n(x) = q^n \frac{x^n(\pi - x)^n}{n!} \cancel{= x^n(\pi}$$

$$= \frac{x^n(p - qx)^n}{n!}$$

e.g. $n=4$, want to know x^7 term.

→ What's coefficient on x^j in there?

coefficient is 0 if $j < n$.

if $j \geq n$:

coefficient is $\frac{c_j}{n!}$ for some integer c_j.

you could with binomial thm if desired.

The jth derivative is

$$f_n^{(j)}(0) = \frac{j!}{n!} c_j$$

$\uparrow$

$j! \cdot$ (the x^j coefficient)

$\shortparallel$

$\frac{j!}{n!} c_j$ ← some integer, don't care

$\uparrow$

an integer if $j \geq n$

To know $f^{(3)}(0)$ for

~~$f(x)=$~~

$f(x) = 7 + 3x - 2x^2 + 5x^3 - 12x^4 + x^5$

$f'(x) = \cancel{3x-4}$

$= 3 - 2\cdot 2x + 3\cdot 5x^2 - 4\cdot 12x^3 + 4x^5$

$f''(x) = -2\cdot 2 + 2\cdot 3\cdot 5x - 3\cdot 4\cdot 12x^2 + 20x^4$

$f'''(x) = 1\cdot 2\cdot 3\cdot 5 - 2\cdot 3\cdot 4\cdot 12x + 80x^3$

$$\boxed{f'''(0) = 1\cdot 2\cdot 3\cdot 5}$$

so

$$\int_0^{\pi} f_n(x)\, \sin(x) = F_n(0) + F_n(\pi)$$

weird stuff about derivatives.

$= \text{integer}.$

(no matter what n is!)

$$f_n(x) = \frac{x^n (p-qx)^n}{n!}$$ ← when n is big this gets close to 0 function.

$$\int_0^{\pi} f_n(x) \sin(x)\, dx$$ ← small, since $f_n(x) \approx 0$ positive, $f_n(x)$ & $\sin(x)$ are positive

- positive
- less than 1
- integer

Impossible!

How good can rational approximations be?

Approximations for π: $\pi \approx 3/1$

$\approx 22/7 = 3.142857\ldots$

nobody even says. $\approx 355/113 =$ 6-digits right?

$\pi \approx 40/13 = 3.076.$

What would make an approximation "interesting"?

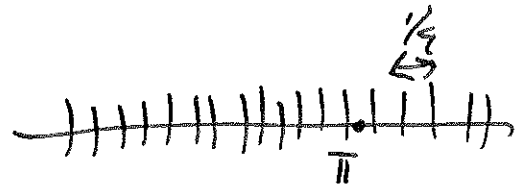
digits correct

vs

how big is q?

For any q, we can find a p so

$$\left|\pi - p/q\right| < 1/q$$



random #

$$\frac{3226}{1027} \approx \pi$$

$$\shortparallel$$

$$3.1411879$$

not very impressive

Theorem

Suppose α is any real number.

There are infinitely many p_n, q_n so that

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}$$

(p_n/q_n gets twice as many digits as # digits of q_n).

But: there are some irrational numbers where $1/q^3$ can't be achieved.

<u>Roth's theorem</u> If α is algebraic number, then

$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^r}$ has only finitely many sols if $r > 2$.

Start with $p_1/q_1 = 3/2$.

Define

$$p_{n+1} = p_n + 2q_n.$$

$$q_{n+1} = p_n + q_n.$$

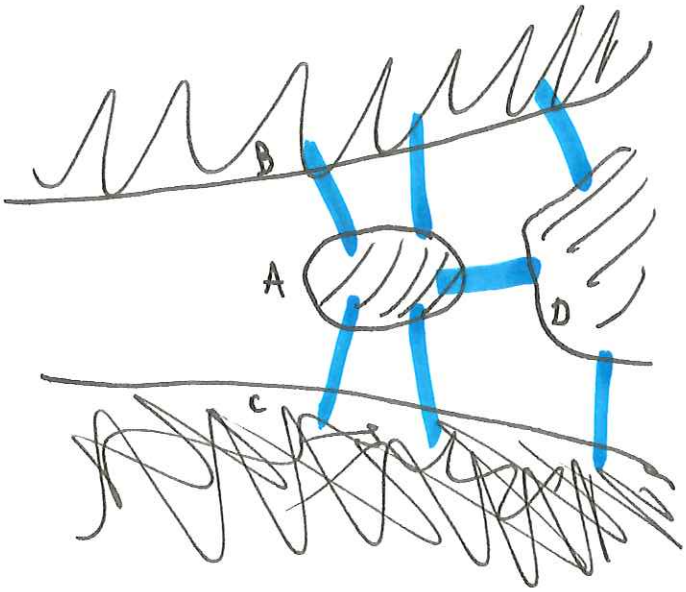
Challenge:

Prove $\lim_{n\to\infty} \frac{p_n}{q_n} = \sqrt{2}$

<u>and</u> $\left| \frac{p_n}{q_n} - \sqrt{2} \right| < \frac{1}{q_n^2}.$ <u>error:</u>

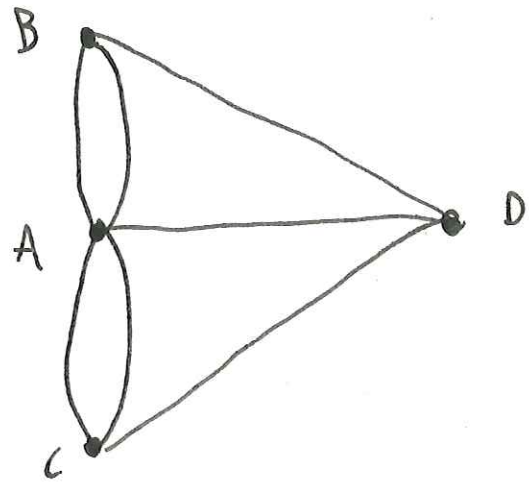
Graph theory

Kaliningrad
↓
Bridges of Königsberg



Can you find a path that hits every ~~island~~ bridges exactly once?

Euler:



if a vertex has an odd number of bridges, you have to either start there or end there.

but in Königsberg, all landmasses have an odd number!

No tour is possible.

Follow-up: if a city has all land masses with even number of bridges, is there always a tour?
(or maybe ≤2 odd)

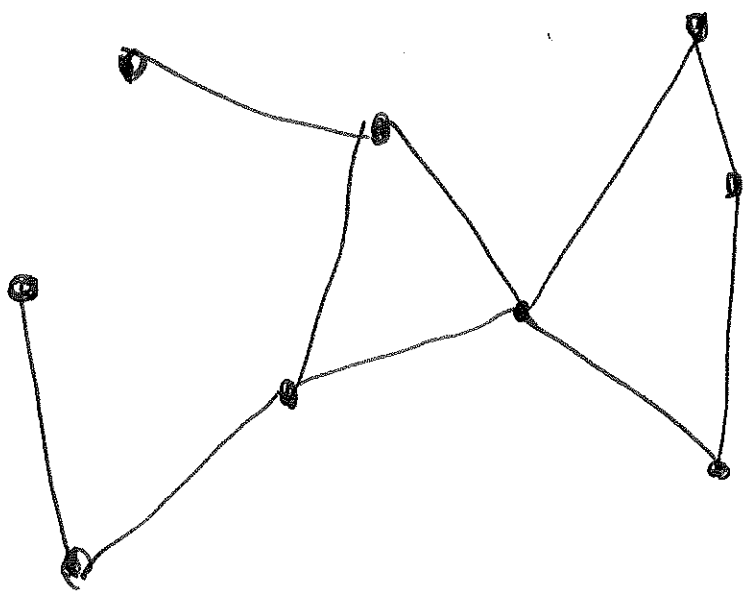
Harris "Combinatorics and Graph Theory."
(Google it.)

A <u>graph</u> is a set of vertices V and a set of edges E, each of which connects two vertices.

(In a graph: undirected, at most one edge between two vertices).

[Königsberg: not a graph, two bridges in some places.]

You can draw a picture:

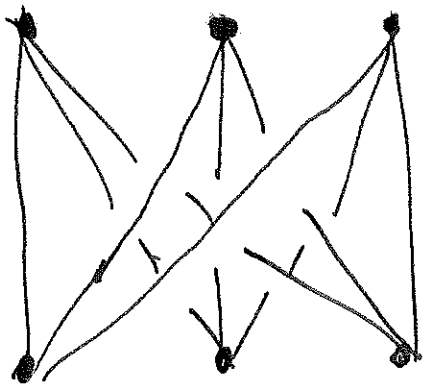


Variations on definition:

- In a "directed graph": edges have direction

- Multiple edges between a pair of vertices: "multigraph"
  (Königsberg)

- Edges between vertex & self
  "pseudograph"



3 houses

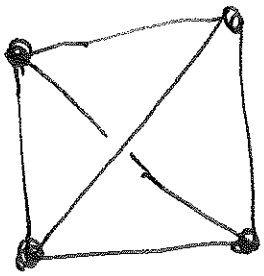
3 utilities electric
gas
water

Can you connect without crossing?

No

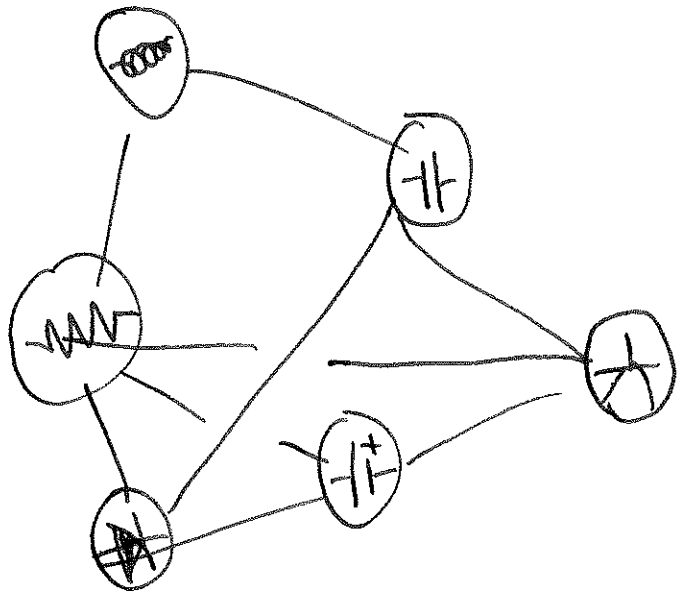
Can we fit that into the plane?

Q. Can edges intersect?

Yes:  counts.

A graph is "planar" if you can draw it in the plane. (that one is) Figuring out if a graph is planar is a useful question.

e.g. designing a circuit board?



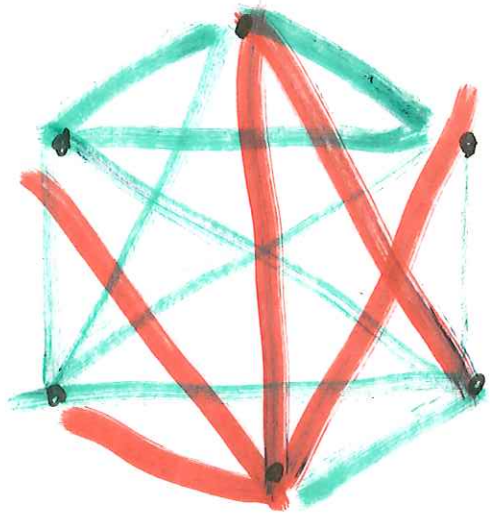
Imagine you have a party with six people.

Prove that either:

1) There's a group of 3 who all know each other.

2) There's a group of 3 none of whom know each other.

What happens with five people?

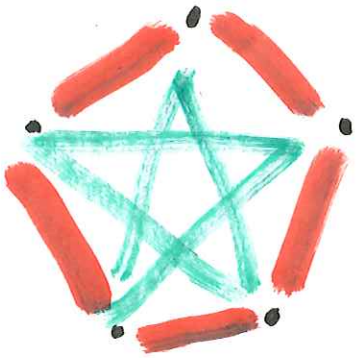


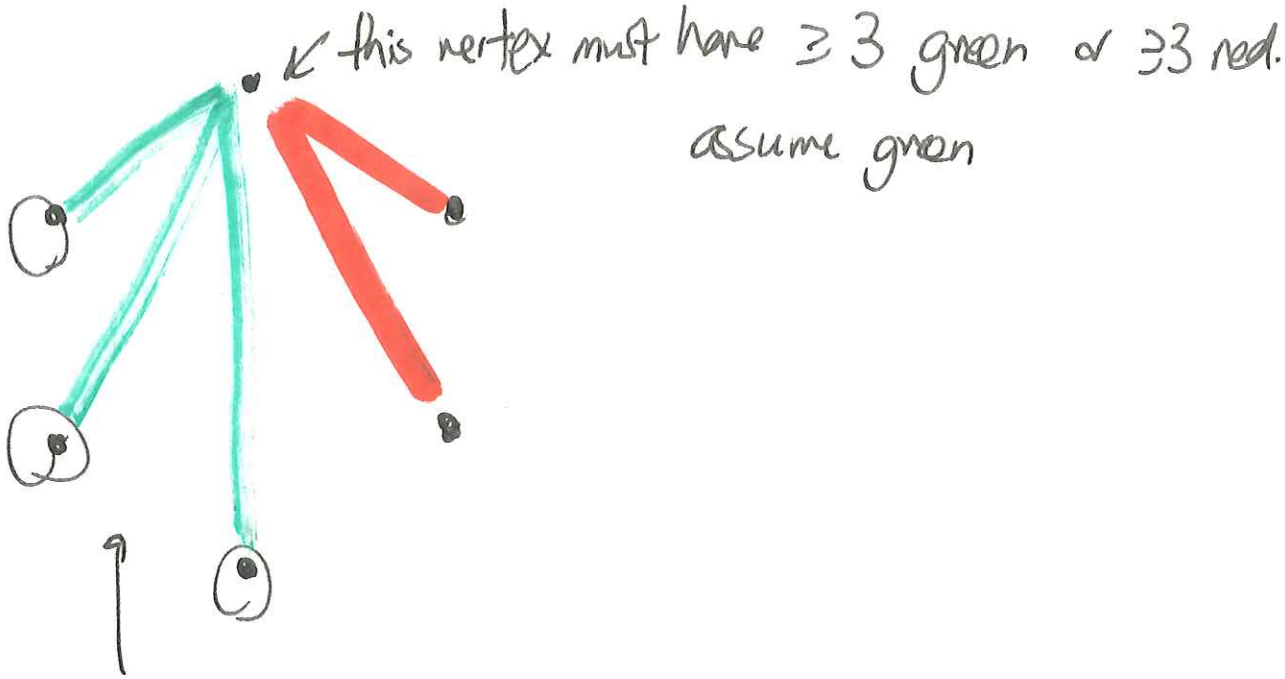
green = know each other

red = don't

must there be a red or green triangle?

With 5





if any of these two know each other, there's a green triangle with top.

if none of them know each other, they form a red triangle.

<u>Thm</u> (Ramsey's theorem)

For any r & s, there's a number $R(r,s)$ so that at any party with $\geq R(r,s)$ people, there's either a group of r who all know each other, or s none of whom know each other.

<u>ex</u> $R(3,3)=6$

Finding $R(r,s)$ is <u>really</u> hard.

$R(4,4) = 18$

$R(5,5) = ??$ $\qquad 43 \leq R(5,5) \leq 48$

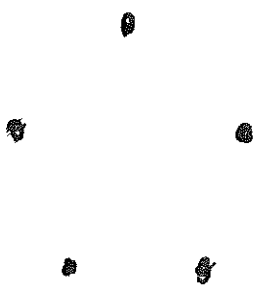
$R(6,6) =$ [weird Erdős story]

The <u>order</u> of a graph is the number of vertices.

If G has order n, how many edges could it have?

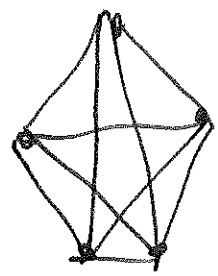
min

0



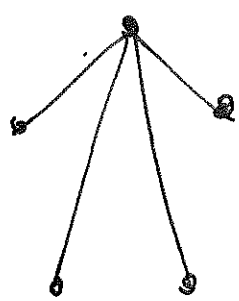
max

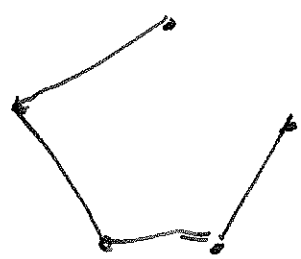
$\binom{n}{2}$



if graph is <u>connected</u>: (all one piece)

min is now $n-1$





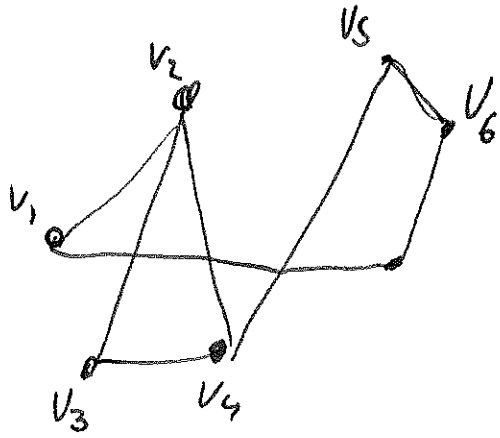
The <u>degree</u> of a vertex is the number of edges leaving it.

<u>Thm</u> The sum of degrees of <u>all</u> vertices is:

$$\sum_{v \in V} \deg(v) = 2 \cdot \#\text{edges}.$$

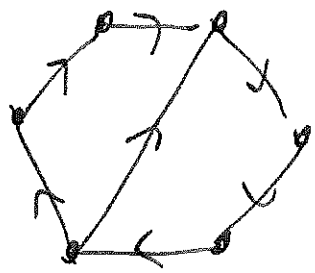
Consequently: you can't have just a single vertex of <u>odd degree</u>.

A <u>walk</u> on a graph is a sequence of vertices $v_1, \ldots, v_k$ where each v_i, v_{i+1} have an edge between



- If vertices of a walk are distinct, it's called a <u>path</u>.
- If edges of a walk are distinct, it's called a trail.

(Every path is trail, but not every trail is a path.)



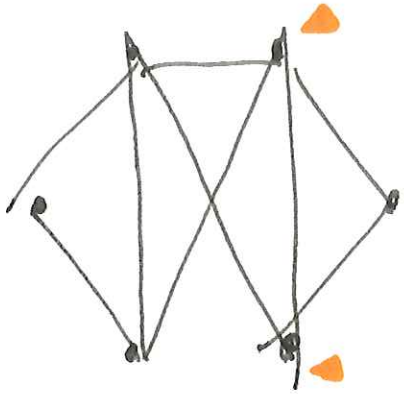
A circuit is a trail that begins and ends at same vertex.

A lot of questions like this: given a graph G, is there a trail that visits every edge?

A graph is <u>connected</u>: any two vertices can be joined by a path.

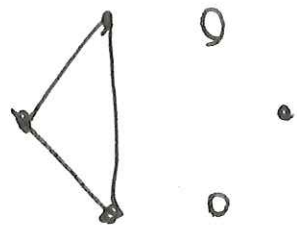
A <u>cut set</u> for G is a set of vertices that you can remove (and remove edges going to vertices) so graph becomes non-connected.

The <u>connectivity</u> of a graph is the size of smallest cut set.



how many vertices need removed for it to have more than one piece?

$\kappa(G)=2$.



<u>Problem:</u> Suppose G is a graph where <u>every</u> vertex has degree $\geq k$.

distinct vertices

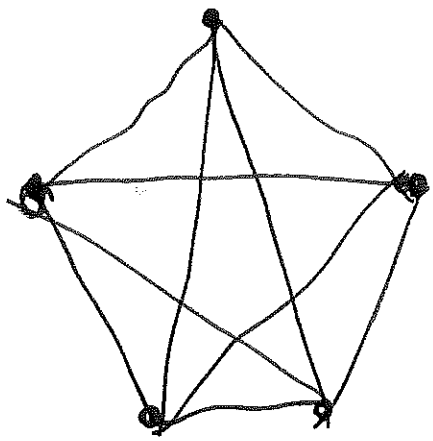
✓ a) Prove G has path of length $\geq k$ edges.

b) If $k \geq 2$, prove G has a cycle of length $\geq k+1$ edges

Graph vocab

1. Complete graph on n vertices

$n=5$



how many edges?

$\binom{n}{2}$

2. Regular graph: every vertex has the same degree.

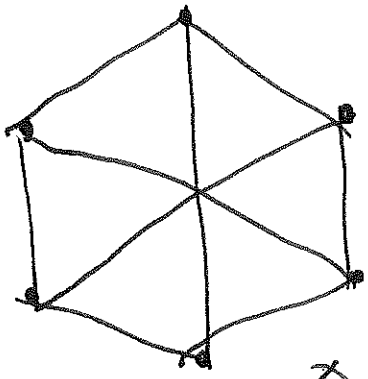
(complete graph is regular)

Puzzle: find 3-regular graphs with 6 vertices?

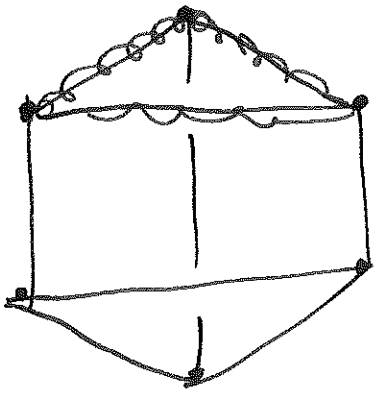
every vertex has 3 edges

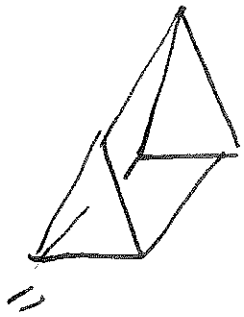
One? two? all?

7 vertices?



$K_{3,3}$



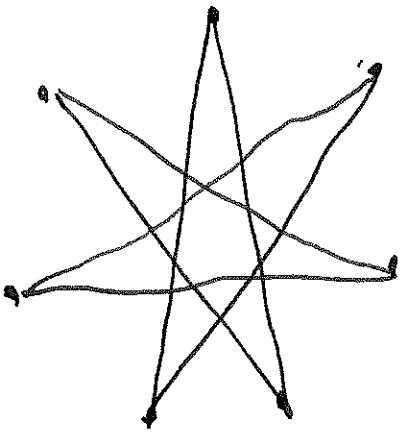


Why different?

contains loops of length 3!

doesn't.

7 vertices



it's not possible!

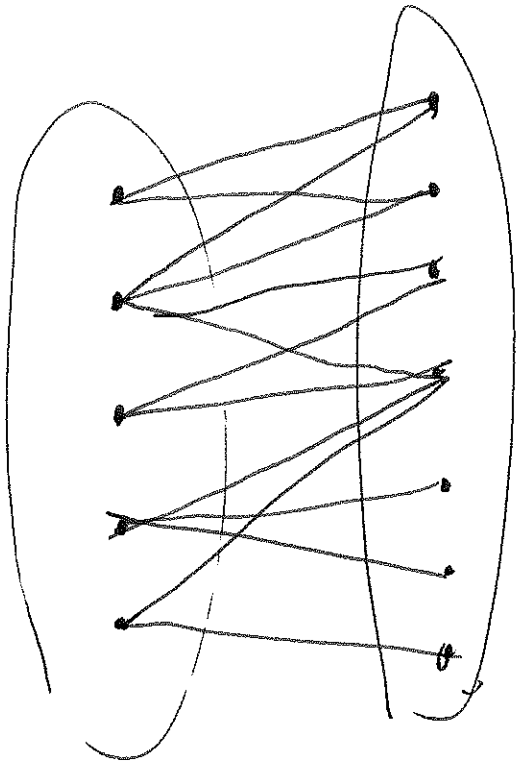
it would need 10.5 edges:

~~sum of edges~~

sum of degrees must be even, but 21 isn't!

Bipartite graph

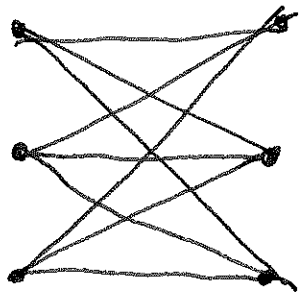
G is bipartite: you can split vertices into two sets (think: color some blue, some red) and every edge connected one vertex from each side.

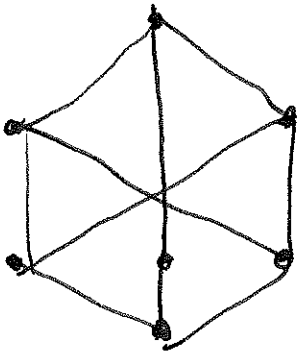


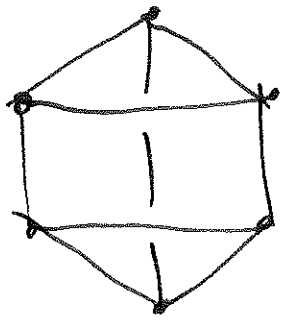
complete bipartite

$K_{m,n}$ = m blue, n red

make all possible cross-color connections







not bipartite

contains a triangle

bipartite $= K_{3,3}$

Thm In a bipartite graph, every cycle has even length.

If a graph has no cycles of odd length, it's automatically bipartite.

→ A graph is <u>Eulerian</u> if there's closed (loop.) trail that touches every edge once.

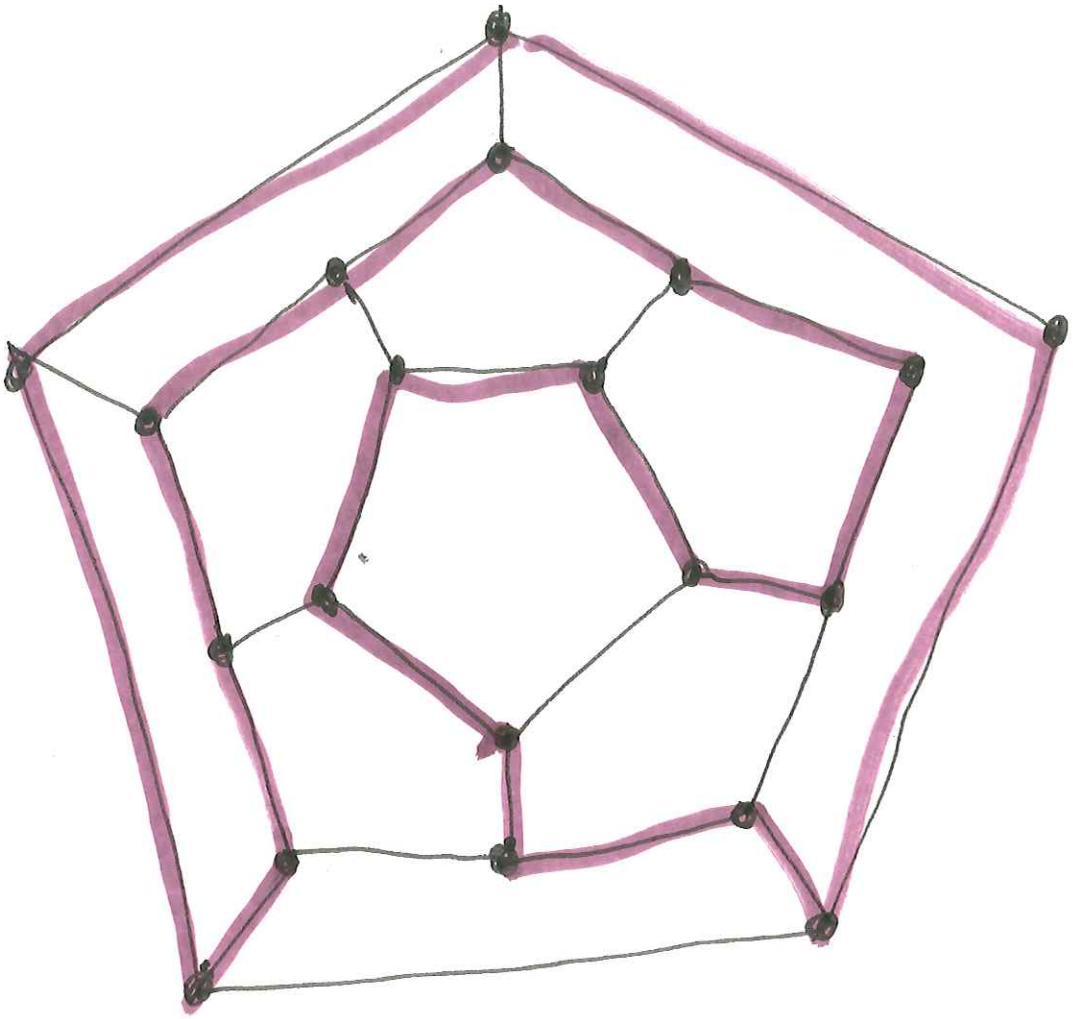
no repeat edges

(cf Königsberg)

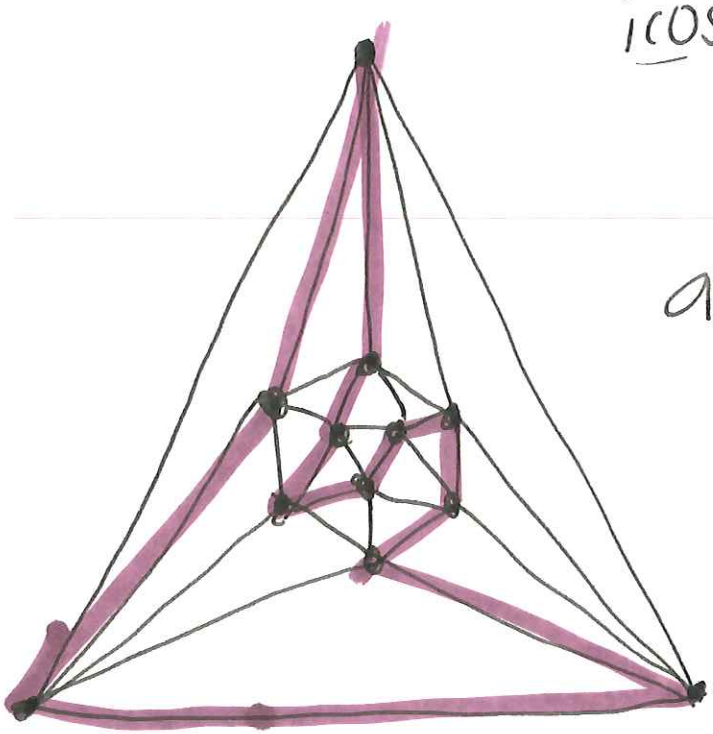
Thm G is Eulerian if and only if every vertex has even degree.

→ A graph is Hamiltonian if there's a closed trail that touches every <u>vertex</u> once.

How to tell?



icosahedral graph!

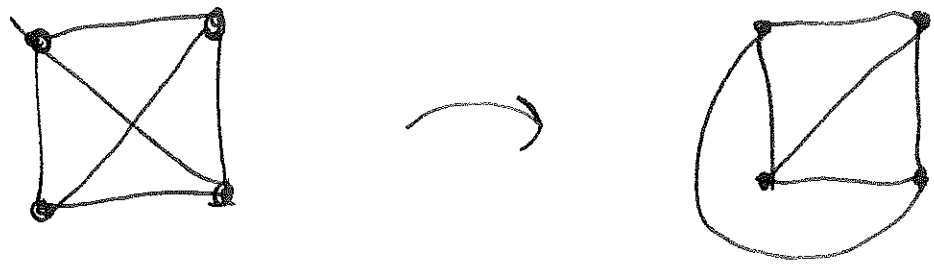


also Hamiltonian

no good algorithm.

Planar graphs:

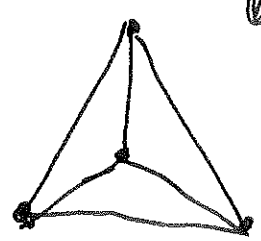
A graph is <u>planar</u> if it can be drawn where edges don't cross:



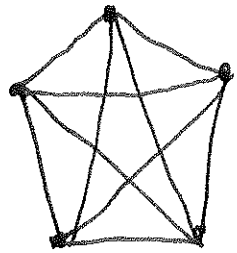
K_4 is planar

<u>Theorem.</u> "Planar" allows ~~bent~~ curved edges.

In fact any planar graph can be drawn with straight non-overlapping edges.

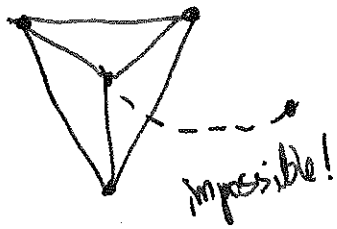


What about K_5?



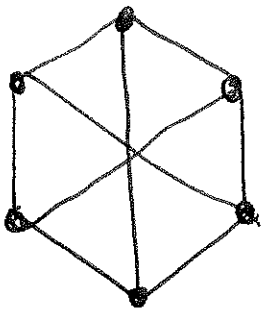
Not planar:

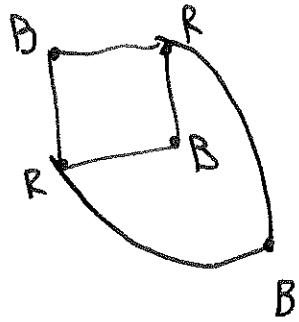
contains K_4, but need to add a point!



What about $K_{3,3}$?

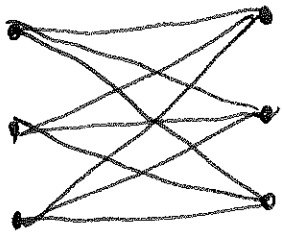
Not planar:





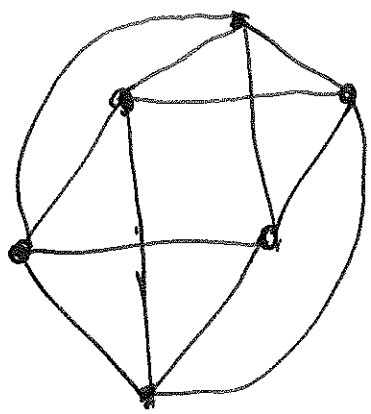
impossible!

I'm convinced.



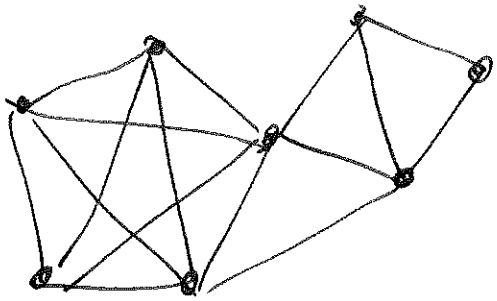
What about O?

is it planar?



vertices + edges of octahedron.

<u>Thm</u> "Kuratowski's theorem" G is planar if and only if it does not contain a copy of K_5 or $K_{3,3}$.

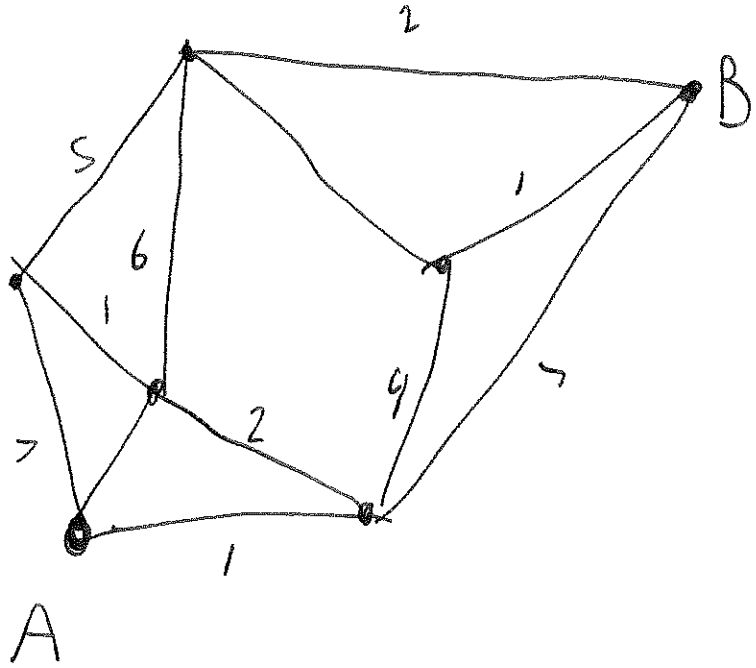


To check planar:

look at every subset of 5.
is it K_5?
" of 6. is it $K_{3,3}$?

Shortest path problem

Suppose G is a graph with a number on each edge ("travel time")



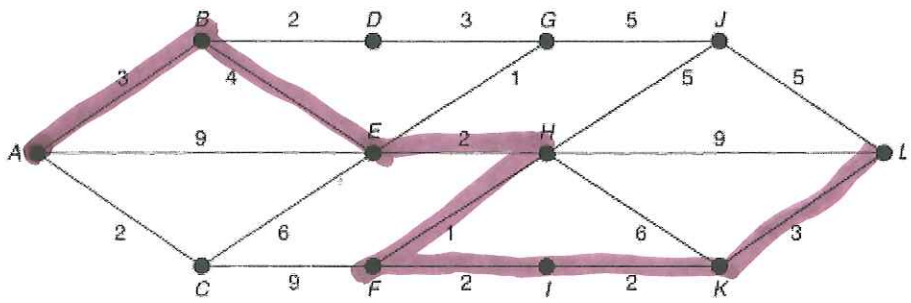
What's the fastest route between A & B?

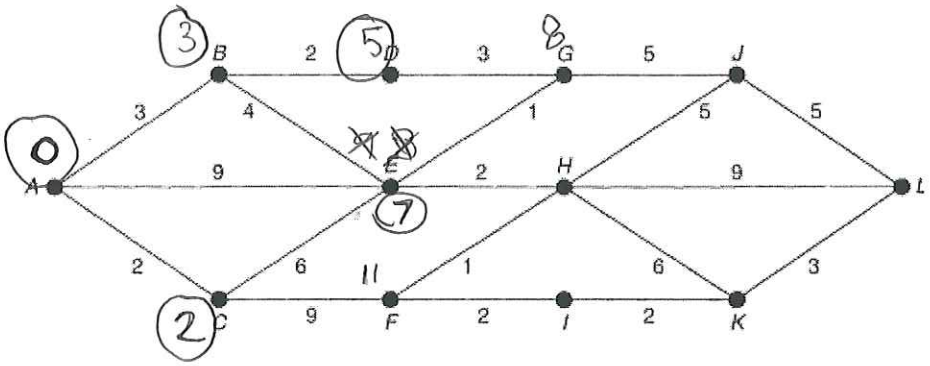
(path on graph minimizing the sum).

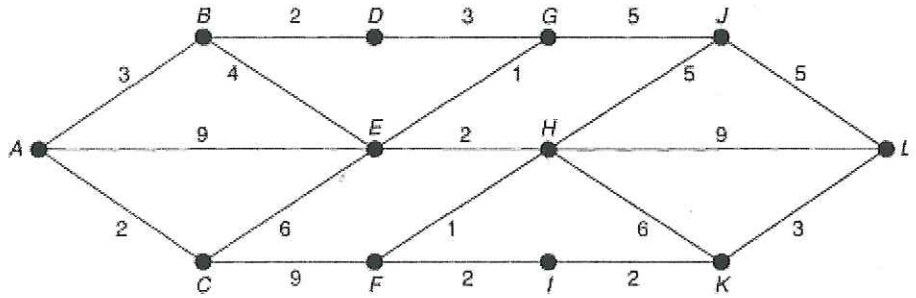
What to do?

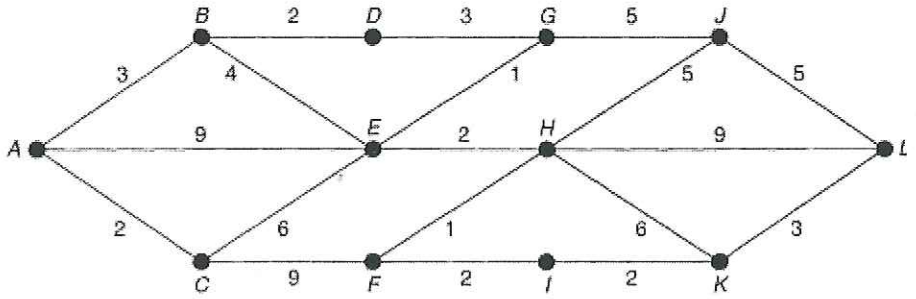
Dijkstra's algorithm.

17


A
B
C
D
E
F
G
H
I
J
K
L
3
2
9
4
2
3
1
6
9
2
5
1
6
2
5
9
5
3

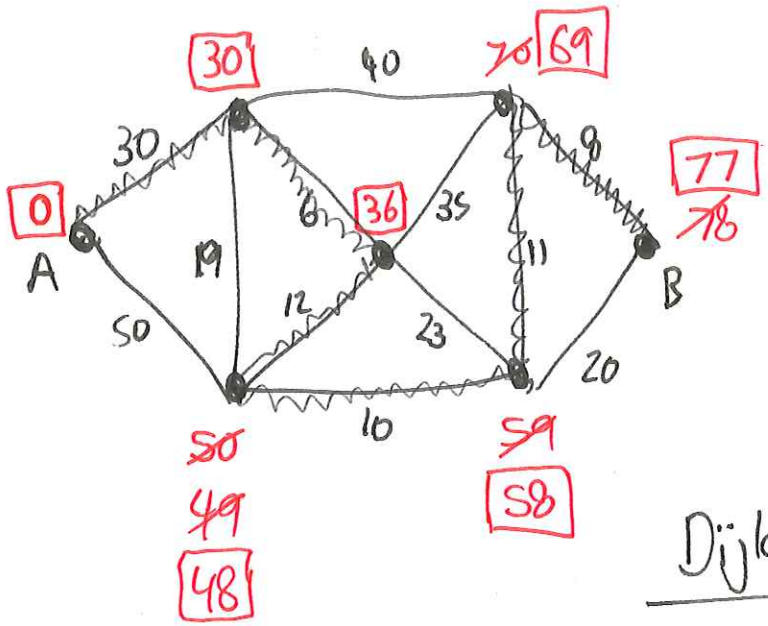

0
3
5
8
7
2
11
A
B
C
D
E
F
G
H
I
J
K
L
3
2
9
4
2
3
1
6
9
2
5
1
6
2
5
9
5
3


A
B
C
D
E
F
G
H
I
J
K
L
3
2
9
4
2
3
1
6
9
2
5
1
6
2
5
9
5
3


A
B
C
D
E
F
G
H
I
J
K
L
3
2
9
4
2
3
1
6
9
2
5
1
6
2
5
9
5
3

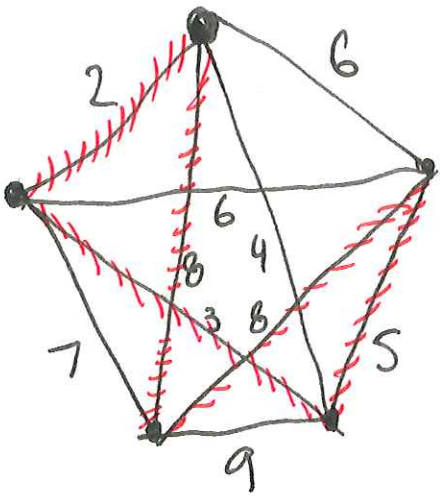
Shortest path

(all weights must be > 0!)



from A to B in 77 steps.

Dijkstra's algorithm.



Records

26

Travelling Salesman Problem:

→ find a loop visiting every vertex in shortest amount of time.

- astronomy
- DNA sequencing

One algorithm:

"Greedy algorithm"

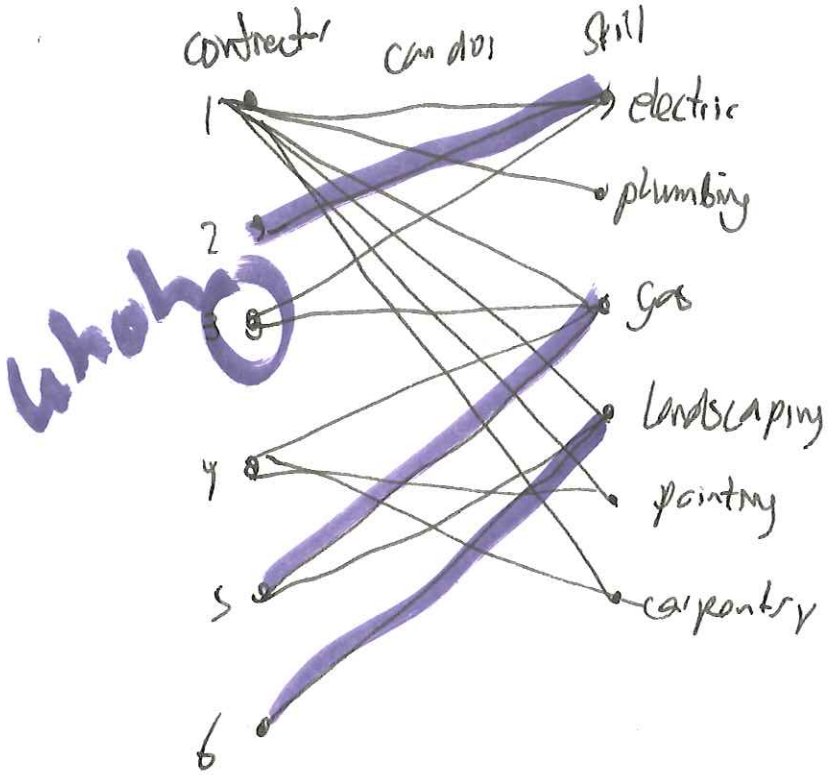
- At each step, add to your route the shortest remaining edge that wouldn't create a loop if you add it (other than completing whole loop) (or 3 at a vertex)

- "Nearest neighbor algorithm"

  Start at A. Always choose cheapest edge from current node that doesn't create a loop.

[did some examples on board]

The marriage problem



Theorem ("Hall's Marriage Theorem")

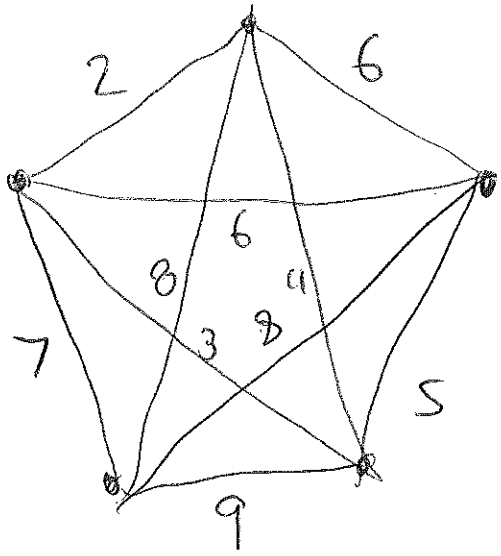
It is possible to assign ~~to~~ spouses / contractors as long as for every set of k contractors, they have at least k skills between them. (And vice versa)

→ Every person knows one skill

→ Every two people have at least two

→ ...

The minimum connector problem



Greedy algorithm:

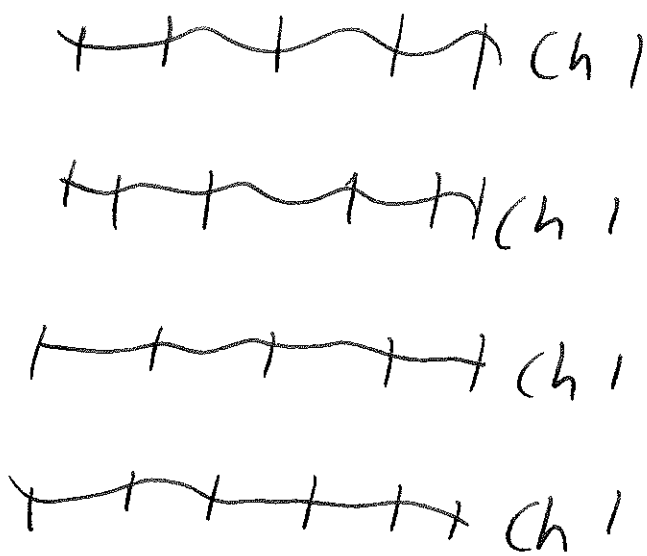
Keep adding shortest edge that won't create cycle.

It always gives best result!

DNA sequencing

Sanger method: 1977 (used in HGP)

randomly cut into pieces of 500-700 basepairs.



say you found these snippets

$S = \{ATC, CCA, CAG, TCC, AGT\}$

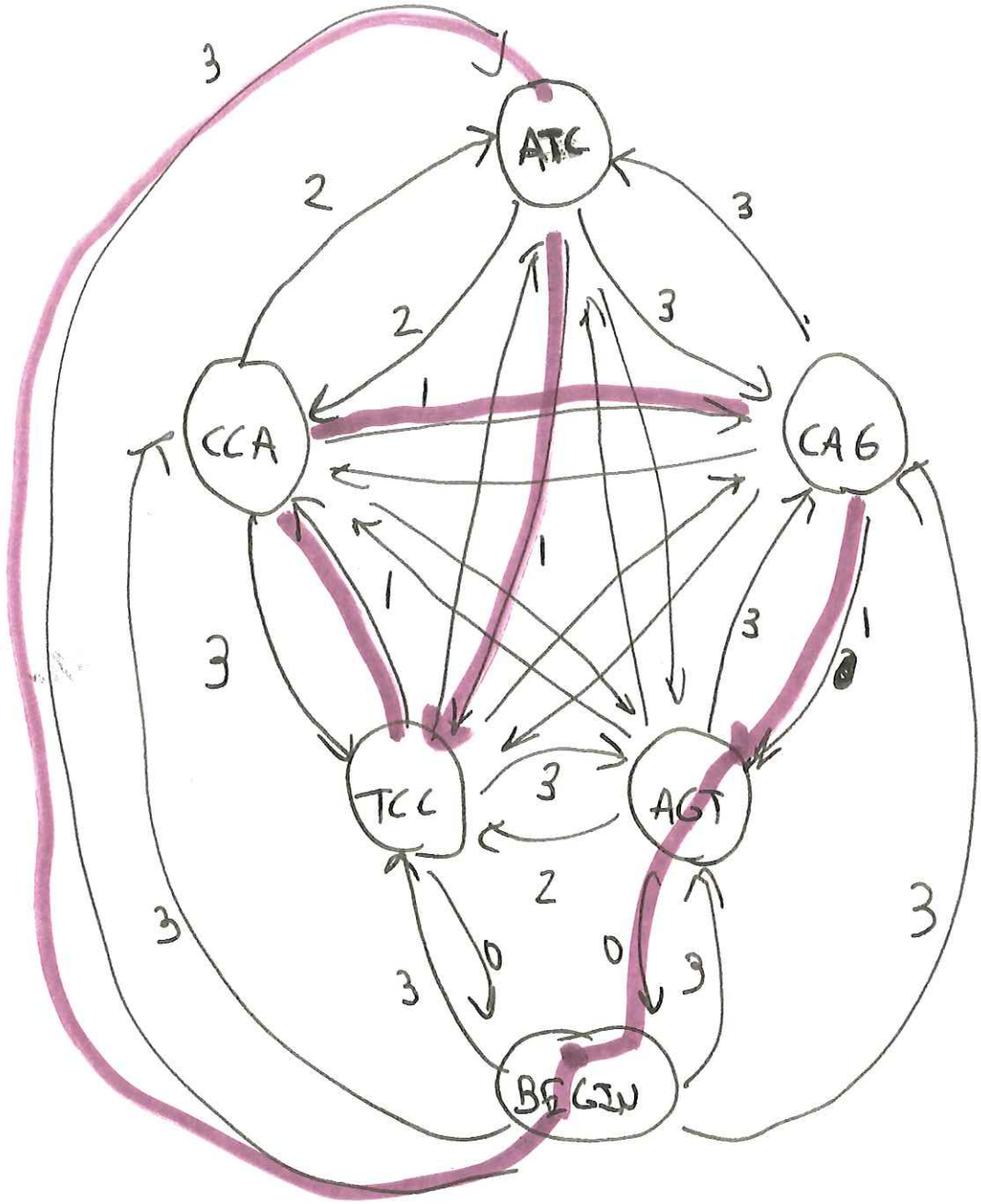
What's the shortest string? containing all of those?

ATCTCCAGAGT

ATCCAGT

Shortest SuperString Problem:

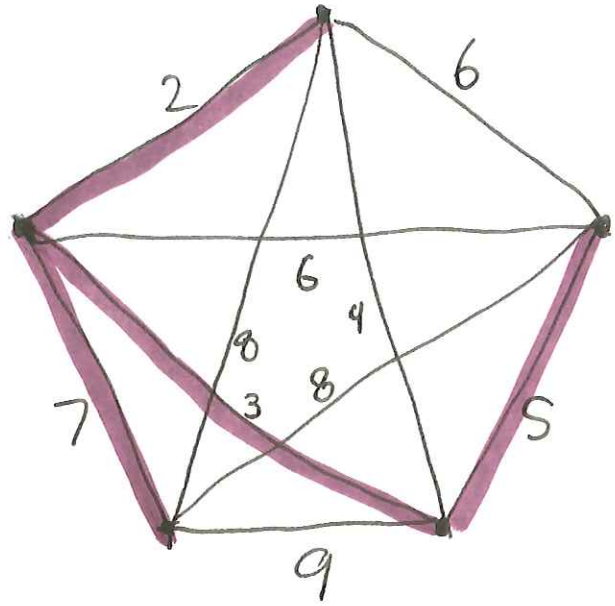
Given a set of strings, find the shortest string containing all of them.



Find Shortest path

Hamiltonian cycle

It's travelling salesman problem!



Minimum connector problem → find minimum "spanning tree" =

goes to every node

no cycle

Greedy algorithm always gives right answer.

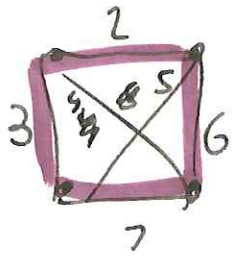
→ Keep picking shortest edge that doesn't give a cycle.

If you have a Hamiltonian cycle and you remove a vertex, what's left is a spanning tree.

So if you find the minimum spanning tree for a graph G with one node deleted, and you add two smallest weights connecting that node, you get a lower bound for TSP?

We have some algorithms to produce good guesses for TSP: given a graph, they find candidate best paths.

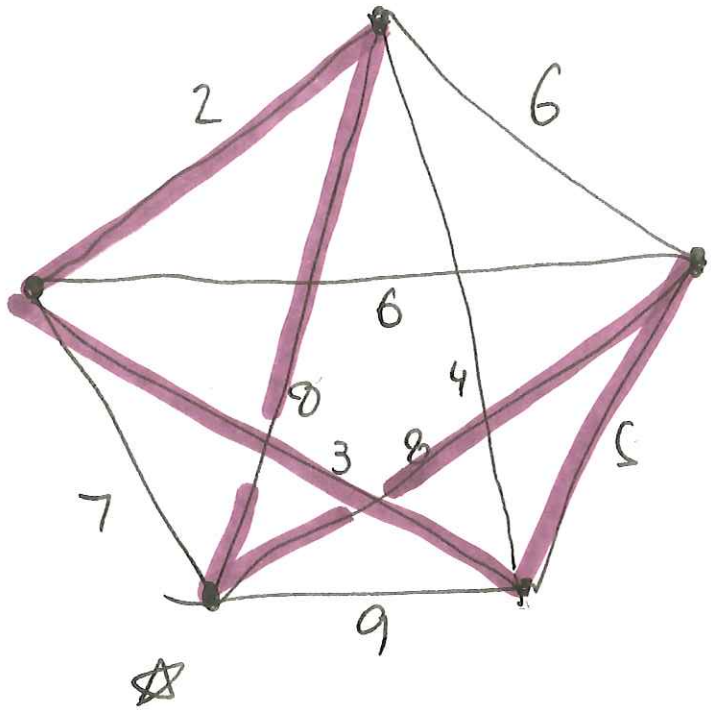
→ This gives an <u>upper</u> bound on the optimal cycle length.



Greedy algorithm: finds path of length $2+3+6+7=18$

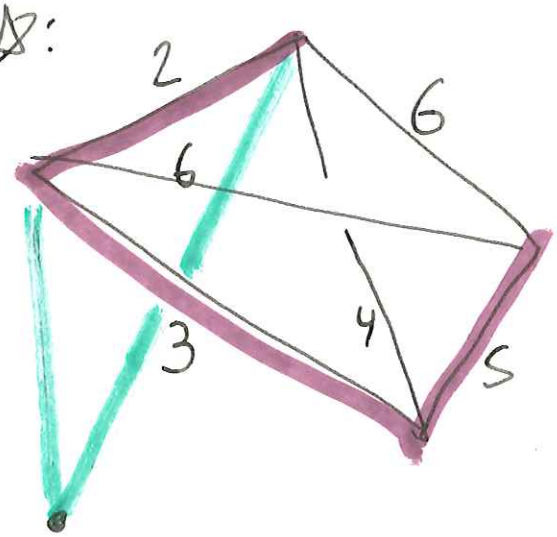
This tells me best path takes at <u>most</u> 18, but it be less.

→ How to find a <u>lower</u> bound?



Greedy: $2+3+5+8+8=26$

Delete ☆:

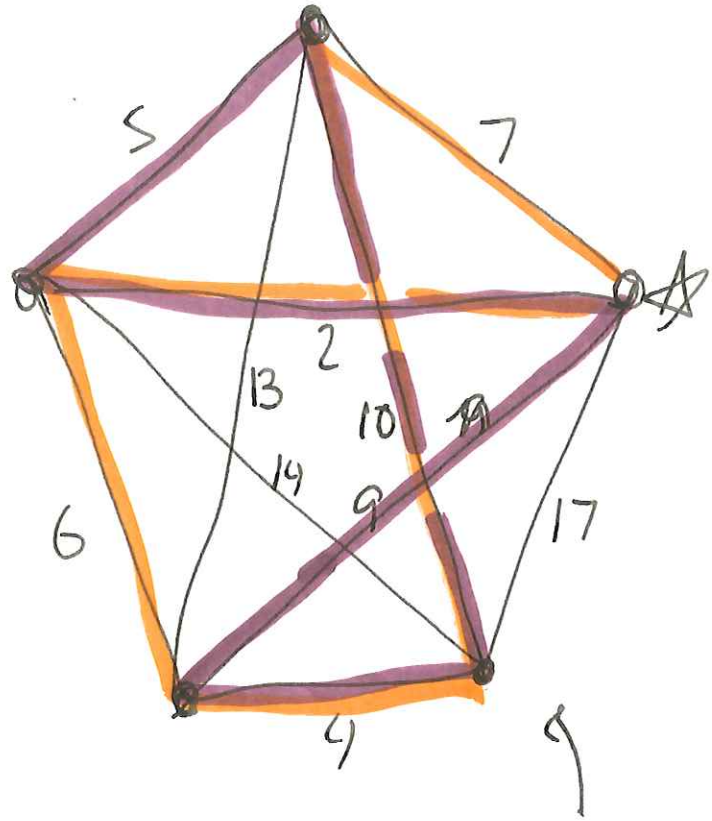


Spanning tree

shortest TSP $\geq$ minimum spanning tree for deleted graph

+ 2 shortest edges to deleted node.

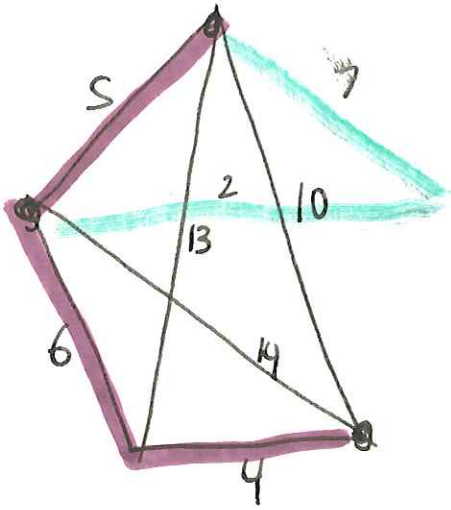
Try it:



$$\boxed{24 \le TSP \le \cancel{30}\ 29}$$

Lower bound:

Delete ☆



$MST = 5+6+4 = 15$

Greedy algorithm

$2+5+4+9+10 = 30$

$TSP \le 30$

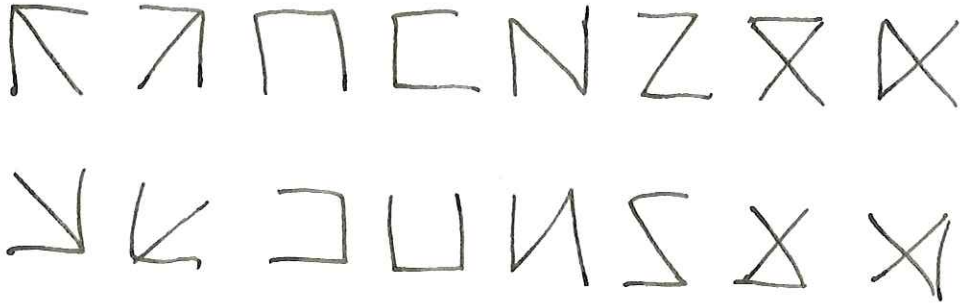
$= 29$ (proprietary algorithm)

shortest connections $+(2+7)$ so $TSP \ge 24$

counts seperately

How many <u>trees</u> connect the 4 nodes?

graph with no loops.



<u>16 of them</u>

5 nodes

Case I: Loop minus side

there are $\frac{5!}{2}$ of these $= 60$

order of sides

rotates

$\parallel$

5

$60 = 5 \times \binom{4}{3} \times 3$ = connect 1 to 3, then any of those three to last.

$n=4 \Rightarrow 16$

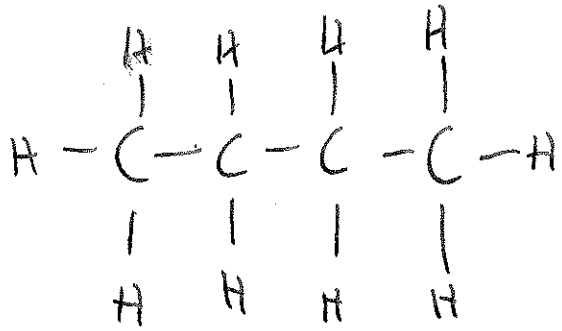
$n=5 \Rightarrow 125$ $\quad n=3 \Rightarrow 3.$

How many trees are there?

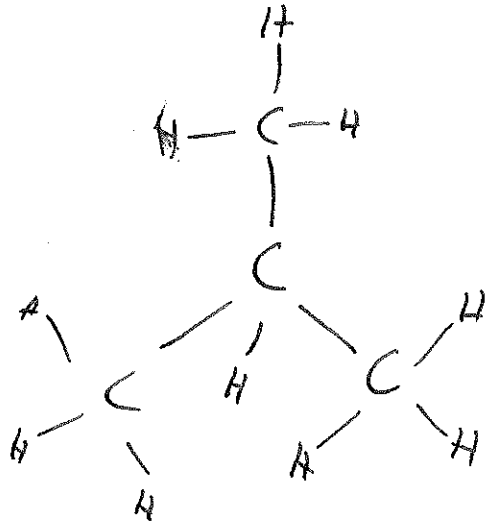
$$\boxed{n^{n-2}}$$

(Cayley; can you explain it?)

How many structural isomers of C_4H_{10}?

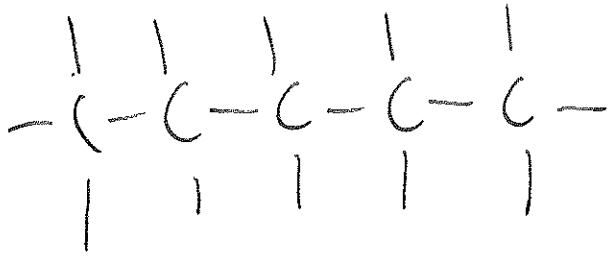


Butane



Isobutane
Methylpropane

C_5H_{12}



How many alkanes with n carbons?

<u>Complex analysis</u> (= calculus with complex numbers!)

→ Good news: usually easier than real analysis.

+ we'll practice multivariable calculus.

→ We'll be able to do some previously impossible ~~numbers~~ integrals.

Functions f whose domain and ~~range~~ codomain are complex numbers. $f: \mathbb{C} \to \mathbb{C}$.

<u>Ex</u> $f(z) = z^2$ ← z = complex variable (any other polynomial)

$f(z) = \frac{1}{1-z}$

$f(z) = iz$

$f(z) = e^z$

Reminder:

<u>FOIL</u>:

$(3+4i)^2 = (3+4i)(3+4i)$

$= 9 + 12i + 12i + 16i^2$

$= -7 + 24i$

$f(x+iy) = e^{x+iy} = e^x e^{iy}$

$= e^x(\cos y + i \sin y)$

$= (e^x \cos y) + i(e^x \sin y)$

You can plug in complex number to most familar functions!

what if z is complex?

$\sin(z)$

$\sin(i) = ??$

$$e^{i\theta} = \cos\theta + i\sin\theta$$

$$e^{-i\theta} = \cos(-\theta) + i\sin(-\theta)$$

$$= \cos\theta - i\sin(\theta)$$

$$e^{i\theta} + e^{-i\theta} = 2\cos\theta$$

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}.$$

$$\cos(2+3i) = \frac{e^{i(2+3i)} + e^{-i(2+3i)}}{2}$$

$$= \frac{e^{-3+2i} + e^{+3-2i}}{2} =$$

$$= \cancel{e^{-3}\left(\frac{e^{2i} + e^{-2i}}{2}\right)}$$

$$= \cancel{e^{-3}\left(\cos 2\right.}$$

$\cos(A+B)$ $\qquad$ $\cos A \cos B - \sin A \sin B$

$$\frac{e^{(A+B)i} + e^{-(A+B)i}}{2} \quad \text{vs} \quad \left(\frac{e^{Ai} + e^{-Ai}}{2}\right)\left(\frac{e^{Bi} + e^{-Bi}}{2}\right)$$

How to plot $\cos(z)$ where z is complex?

$$\cos(z) = \frac{e^{iz} + e^{-iz}}{2}$$

hard! but we could graph

$\cancel{|\cos(z)|}$

$|\cos(x+iy)|$ where x, y real

output is real.

$1/z$

z^2

$\sin(z)$

also plot: what does f do to a grid? [Cocalc]

$$\frac{e^{-3}(\cos 2 + i\sin 2) + e^{3}(\cos 2 - i\sin 2)}{2}$$

$$= \frac{(e^{-3}\cos 2 + e^{3}\cos 2) + (e^{-3}\sin 2 - e^{3}\sin 2)i}{2}$$

$$\cos^2\theta = \left(\frac{e^{i\theta} + e^{-i\theta}}{2}\right)\left(\frac{e^{i\theta} + e^{-i\theta}}{2}\right)$$

$$= \frac{e^{2i\theta} + 1 + 1 + e^{-2i\theta}}{4}$$

$$\boxed{\sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}}$$

$$= \frac{1}{2} + \frac{e^{2i\theta} + e^{-2i\theta}}{4} = \frac{1}{2} + \frac{1}{2}\cos(2\theta)$$

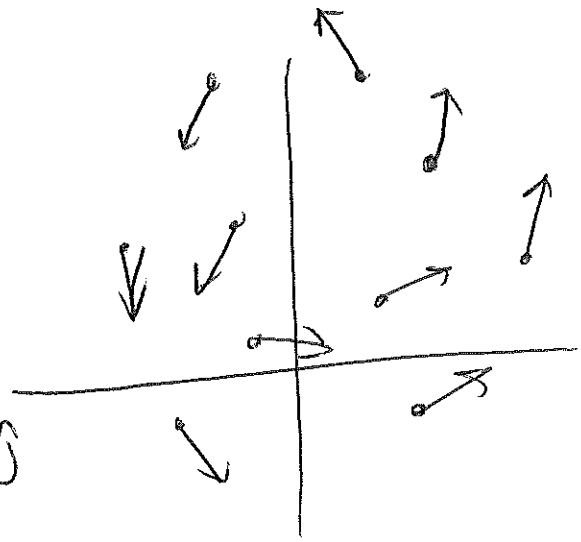
Observations

It's <u>conformal</u>: red and blue lines meet at angle even after we plot!

Recap: path integrals (for work)

$$\int \vec{F} \cdot d\vec{s}$$

$\vec{F}(x,y)$ vector field

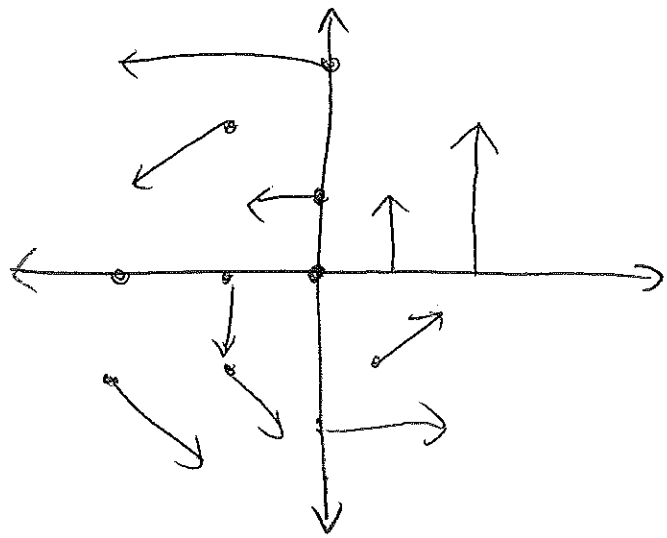


$$\vec{F}(x,y) = (3x+2y)\hat{\imath} + (x-y^2)\hat{\jmath}$$

e.g. $\vec{F}(1,1) = 5\hat{\imath} + 0\hat{\jmath}$

eg. imagine it's current in water.

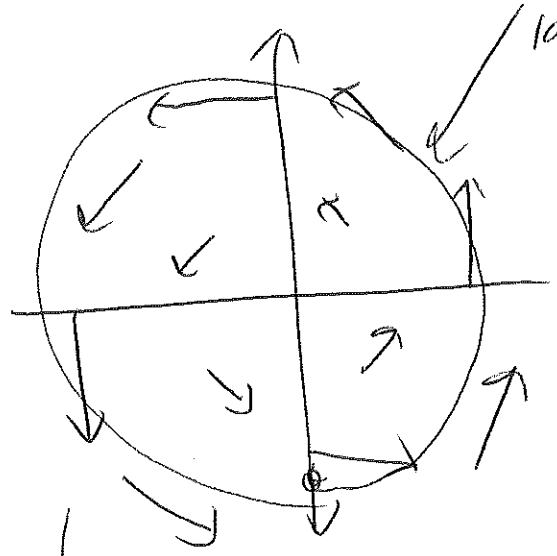
$$\vec{F}(x,y) = (-y)\hat{\imath} + x\hat{\jmath}$$



Imagine a path in the plane,

parametrized path

path = circle of radius 2



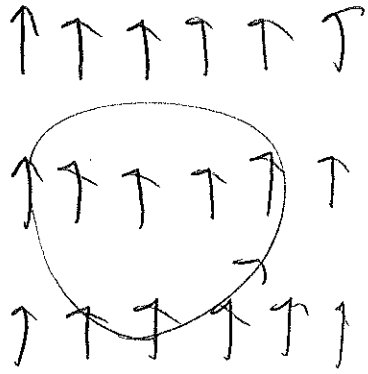
$\vec{r}(t) = (2\cos(t), 2\sin(t))$

$0 \le t \le 2\pi$

path integral

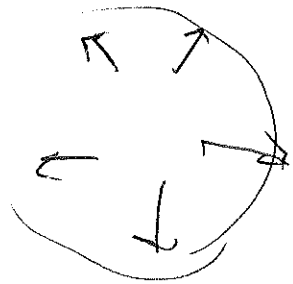
$$\int_C \vec{F} \cdot d\vec{r}$$

> 0 if same direction



probably > 0 $\int_C \vec{F} \cdot d\vec{r}$

$= 0$ $\int \vec{F} \cdot d\vec{r}$



To calculate it:

$$\vec{F}(x,y) = (-y)\hat{i} + x\hat{j}$$

$$\vec{r}(t) = \big(\underbrace{2\cos(t)}_{x(t)},\ \underbrace{2\sin(t)}_{y(t)}\big)$$

$$\int_C \vec{F}\cdot d\vec{r}$$

$$= \int_C \vec{F}\cdot\frac{d\vec{r}}{dt}\,dt$$

$$\frac{d\vec{r}}{dt} = \big(-2\sin(t),\ 2\cos(t)\big)$$

$$= \int_{t=0}^{2\pi} \underbrace{\langle -y, x\rangle}_{\vec{F}}\cdot\langle -2\sin t, 2\cos t\rangle\,dt$$

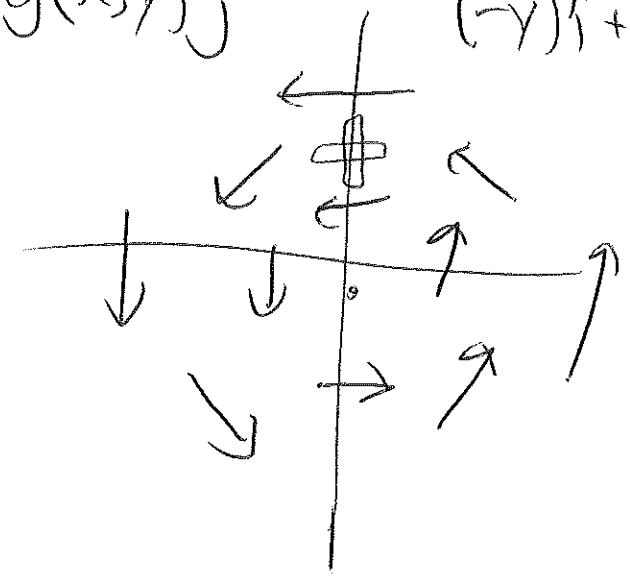
plug in x&y from $\vec{r}$

$$= \int_{t=0}^{2\pi} \langle -2\sin t, 2\cos t\rangle\cdot\langle -2\sin t, 2\cos t\rangle\,dt$$

$$= \int_{t=0}^{2\pi} 4\sin^2 t + 4\cos^2 t\,dt = \int_{t=0}^{2\pi} 4\,dt = \boxed{8\pi} > 0.$$

$$\vec{F}(x,y) = f(x,y)\hat{\imath} + g(x,y)\hat{\jmath}$$

$(-y)\hat{\imath} + x\hat{\jmath}$



$$(\text{curl } \vec{F})(x,y) = g_x - f_y$$

a function, in 2D case of x, y

$$\text{curl } \vec{F} = 1 - (-1) = 2$$

Today we started our review of multi-variable calculus. The plan is to work our way through a set of exams from an old version of this class:

`https://ocw.mit.edu/courses/18-02-multivariable-calculus-fall-2007/pages/exams/`

Today we finished Exam 1A and did the first three problems of 1B. We'll slow down once we hit the serious calculus.