PROPOSITIONAL LOGIC ①

$P \vee \neg P$ always true

P	Q	$P \Rightarrow Q$	$\neg P \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

vacuously true when hypothesis false

contrapositive: $\neg Q \Rightarrow \neg P$

converse: $Q \Rightarrow P$

$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x<y)$ True

$(\exists x \in \mathbb{Z})(\forall x \in \mathbb{Z})(x<y)$ False

DeMorgan's Laws

$\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$

$\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$

$(\exists x \in T)(\exists x, y \in S)$

$[B(x) \wedge B(y) \wedge F(x,y) \wedge E(x,t) \wedge E(y,t)]$

There is at least one day each week where two boba shops are ≤ 5 blocks apart w late employees

PROOFS ②

1. Direct
   (Assume P ∴ Q)
2. Contraposition
   (Assume $\neg Q$ ∴ $\neg P$)
   Pigeonhole Principle
3. Contradiction
   (Assume $\neg P \cdots \neg R \wedge R$ ∴ P)
   ∞ many prime, $\sqrt{2}$ irrational
4. Cases
5. Induction ③ for all ℕ graph proofs
   Strengthening IH
   Strong Induction
   write out all the base cases

if you see $\leq \rightarrow <$

odd : $2m+1$
even: $2m$
multiple: km

THEOREMS ②③

2.1[1] For any $a,b,c \in \mathbb{Z}$ $a|b$ and $a|c$ then $a|(b-c)$

2.2[1] If 9 | sum of digits of $n \Leftrightarrow 9|n$

2.4[2] $d|n$, if n odd then d odd

2.5[2] Pigeonhole Principle

2.6[3] Infinitely many prime #s

2.7[3] $\sqrt{2}$ is irrational $\rightarrow \frac{p}{q}$ $2 = \frac{p^2}{q^2}$ $p^2 = 2q^2$ if n^2 even, n even

2.8[4] Exists irrational x,y s.t. x^y is rational

3.3[5] Two color Theorem

3.4[5] Sum of first n odd num. is n^2 — strengthen

3.7[5] Every $n>1 \in \mathbb{N}$ can be written as prod. of primes — strong

SETS + COUNTABILITY ④⑤

$A \subseteq B$ A subset of B

complement

$A \cup \emptyset = A$ $A \cap B = B \cap A$ $A \cap \emptyset = \emptyset$

$A \setminus A = \emptyset$ $A \setminus \emptyset = A$ $\emptyset \setminus A = \emptyset$

finite — infinite

$\emptyset \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

countable — uncountable

if $f: A \to B$ one to one $|A| \leq |B|$

② show $|A| \leq |B|$ and $|B| \leq |A|$

cross product

power set
$|S| = k$
$|P(S)| = 2^k$

injection: no two x to one y
horizontal line test

surjective: hits every y

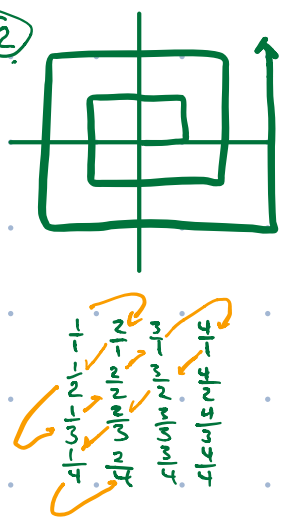
bijective
ℤ ① injective and surjective
ℚ ② injection both ways

① $f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ even} \\ \frac{-(n+1)}{2} & \text{if } n \text{ odd} \end{cases}$

injection: show $f(n_1) = f(n_2)$
will show $n_1 = n_2$
case 1: $\frac{n_1}{2} = \frac{n_2}{2}$
$n_1 = n_2$

surjective: find $n \in \mathbb{N}$ s.t. $f(n) = k$
case 1: let $n = 2k \in \mathbb{N}$
$f(n) = f(2k) = \frac{2k}{2} = k$ ✓

②



$|\mathbb{Q}| \leq |\mathbb{N}|$

Cantor's Diagonalization
- uncountable!
- no bijection btw ℕ

ex: [0,1] uncountable

$f(0) = 0.\textcircled{5}214$
$f(1) = 0.1\textcircled{4}16$
$f(2) = 0.94\textcircled{7}\cdots$ (+1)
⋮
$q = 0.658$

countable	uncountable
$\mathbb{N} \times \mathbb{N}$	real numbers
finite strings	infinite strings
finite bit strings	infinite bitstrings

COMPUTABILITY ⑤

TestHalt(P,x) = { "yes" if P halts; "no" if P loops on input x }

Turing(P) — used as subroutine
  if TestHalt(P,P) == "yes" → loop
  else halt

if proving: write program
if disproving: show reducable
  1) Assume foo(P,x)
  2) def testHalt(P,x) — written such that it does something if P(x) halts
       def helper(x)
     return foo(helper,x)
  3) Since TestHalt impossible and foo → testHalt, foo DNE

GRAPH THEORY ⑥

tour: no repeated edges, start/end same vertex
path: distinct vertices
cycle: only repeated vertex is start/end
deg v + deg v ≥ n-1 then G connected
if each vertex has deg > v/2 ↗

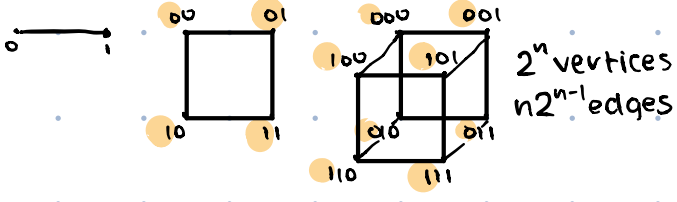
COMPLETE GRAPH
$\frac{n(n-1)}{2}$ edges

TREES two vertex colorable — draw out and try induction
f = 1
e = v-1

1. G is connected and contains no cycles
2. G is connected and has n-1 edges (n = |V|)
3. G is connected, and the removal of any edge disconnects G
4. G has no cycles, and the addition of any edge creates a cycle.

height h - vertices $\leq 2^{h+1}-1$
binary tree with n leaves has 2n-1 vertices
✕ build up error — k+1, reduce to k, then build back up to k+1

HYPERCUBE

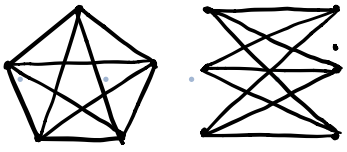


2^n vertices
$n2^{n-1}$ edges

Eulerian tour: even degree, connected
Eulerian walk: can have two odd

PLANAR GRAPHS can be arranged w/o crossing
If v + f = e + 2 (Euler's formula)
$e \leq 3v-6$
if e = 3v-6 every f incident to 3 e
nonplanar if contains K_5, $K_{3,3}$

DUALITY AND COLORING
4 colors enough
2 for trees



MODULAR ARITHMETIC ⑦ ⑧

create 1, -1 ?
factorials hit mod?
square up?
inverse ⇔ gcd(n,x) = 1

$7^{2020} \pmod{50} \equiv 49^{1010} \equiv (-1)^{1010} \equiv 1 \pmod{50}$
$218^3 \pmod 9 \equiv 2^3 \equiv 8 \pmod 9$ — square up
$3^{160} \pmod{23} \equiv (3^{22})^7 \cdot 3^6 \equiv (3^2)(3^4) \equiv 16 \pmod{23}$
$998^{156} \pmod{13} \equiv (998^{12})^{13} \equiv 1 \pmod{13}$

FERMAT'S — prime
$a^{p-1} \equiv 1 \pmod p$
$a^p \equiv a \pmod p$ — p does not divide a

EUCLID'S ALGORITHM
gcd(35,12)
$35 = 2(12)+11 \quad 35-2(12)=11$
$12 = 1(11)+1 \rightarrow 12-1(11)=1$
$12-(35-2(12))=1$
$3(12)-1(35)=1$
$12^{-1} \pmod{35} = 3$
$35^{-1} \pmod{12} = -1$

CRT MECHANICAL
$x \equiv 2 \pmod 3 \rightarrow 5\cdot 7\left((5\cdot 7)^{-1}(2 \bmod 3)\right)$
$x \equiv 3 \pmod 5 \rightarrow 3\cdot 7\left((3\cdot 7)^{-1}(3 \bmod 5)\right)$
$x \equiv 4 \pmod 7 \rightarrow 3\cdot 5\left((3\cdot 5)^{-1}(4 \bmod 7)\right)$
$x = 63+37+60 = 158 \equiv 53 \pmod{105}$

RSA

public key (N,e)
  N = pq — if N factored easily, you can break
  e = relatively prime to (p-1)(q-1)
    $c = x^e \bmod N$
private key (d)
  $d = e^{-1} \pmod{(p-1)(q-1)}$ — both coprime
    $x = c^d \bmod N$
  $ed \equiv 1 \pmod{(p-1)(q-1)}$

p=7 q=3 e=5
(21, 5)
$d = 5^{-1}(12) = 5$

x = 4
$c = 4^5 \pmod{21}$
$\equiv (4^3)(4^2) \equiv 16 \pmod{21}$
$x = 16^5 \pmod{21}$
$\equiv 4$ wow!

POLYNOMIALS ⑨

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

1. polynomial of deg $d \le d$ roots
2. $(d+1)$ pairs with distinct x_i forms a unique polynomial deg $\le d$

can express $p(x) = d(x)q(x) + r(x)$

LAGRANGE INTERPOLATION

(1,1) (2,2) (3,4) — degree pts-1

$$\Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)}$$

$$\Delta_2(x) = \frac{(x-1)(x-3)}{(2-1)(2-3)}$$

$$\Delta_3(x) = \frac{(x-1)(x-2)}{(3-1)(3-2)}$$

$$p(x) = 1\cdot\Delta_1(x) + 2\cdot\Delta_2(x) + 4\cdot\Delta_3(x)$$

ALTERNATE METHOD

$$a_2 + a_1 + a_0 = 1$$
$$4a_2 + 2a_1 + a_0 = 2$$
$$9a_2 + 3a_1 + a_0 = 4$$

INVERSE instead of DIVISION

$a_0 = 1 \quad a_1 = -1/2 \quad a_2 = 1/2$

$\Rightarrow p(x) = \frac{1}{2}x^2 - \frac{1}{2}x + 1$

FINITE FIELDS

elements – prime or prime power

GF(7) like working (mod 7)

COUNTING

Polynomials of degree $\le d$ over F_m

# of points	# of polynomials
$d+1$	1
d	m
$d-1$	m^2
⋮	⋮
$d-k$	m^{k+1}
⋮	⋮
0	m^{d+1}

d = degree

m = mod

SECRET SHARING

lagrang.

need k points to solve secret

create k-1 polynomial

ideally choose large GF(q)

(if GF(7) $0 \le s \le 6$ can guess)

ERROR CORRECTING

ERASURE ERRORS – lost

GF(q) $q \ge n+k = 6$ — message — lost

$\deg P(x) = n-1 = 3$

send $n+k = 6$

$n = 4 \quad k = 2$

any n can solve

A: (1,3) (2,1) (3,5) (4,0) | (5,6) (6,1)

$m_1 = 3 \quad m_2 = 1 \quad m_3 = 5 \quad m_4 = 0$

lagrange ↓

$P(x) = x^3 + 4x^2 + 5$

lagrange ↑

B: (1,3) (3,5) (4,0) (5,6) (2,1) (6,1)

GENERAL ERRORS – corrupted

GF(q) $q > n+2k$

send $n+2k = 5$

$n = 3 \quad k = 1$

$\deg E(x) = k = 1$

$\deg P(x) = n-1 = 2$

$\deg Q(x) = n+k-1 = 3$

$E(x) = (x-e_1)(x-e_2)\cdots(x-e_k)$

$P(i)E(i) = r_i E(i)$

BERLEKAMP WELCH

$Q(x) = P(x)E(x)$

$Q(x) = a_{n+k-1}x^{n+k-1} + \cdots + a_1 x + a_0$

$E(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$

A: "3" "0" "6" | (4,0) (5,3) (mod 7)

("3" = (1,3), "0" = (2,0), "6" = (3,6))

lagrange ↓

$P(x) = x^2 + x + 1$

(1,2) (2,0) (3,6) (4,0) (5,3)

berlekamp ↓

forms Q(x)

$a_3 + a_2 + a_1 + a_0 = 2(1-b_0)$ — $2-2b_0$

$a_3 + 4a_2 + 2a_1 + a_0 = 0$ — $4-6b_0$

$6a_3 + 2a_2 + 3a_1 + a_0 = 6(3-b_0)$

$a_3 + 2a_2 + 4a_1 + a_0 = 0$ — $1-3b_0$

$6a_3 + 4a_2 + 5a_1 + a_0 = 3(5-b_0)$

solve: $a_3 = 1 \quad a_2 = 0 \quad a_1 = 0, \quad a_0 = 6, \quad b_0 = 6 \equiv 1$

$$\frac{Q(x)}{E(x)} = \frac{x^3+6}{x-1} = x^2 + x + 1 \pmod 7$$

$P(1) = 3$

$a_3 + a_2 + a_1 + a_0 + 2b_0 = 2$
$a_3 + 4a_2 + 2a_1 + a_0 = 0$
$6a_3 + 2a_2 + 3a_1 + a_0 + 6b_0 = 4$
$a_3 + 2a_2 + 4a_1 + a_0 = 0$
$6a_3 + 4a_2 + 5a_1 + a_0 + 3b_0 = 1$

$a_0 = -2a_1 - 4a_2 - a_3$

$a_3 + a_2 + a_1 + a_0 + 2b_0 = 2$
$a_3 + a_2 + a_1 - 2a_1 - 4a_2 - a_3 + 2b_0 = 2$
$-3a_2 - a_1 + 2b_0 = 2$
$a_1 = -3a_2 + 2b_0 - 2$

$6a_3 + 2a_2 + 3a_1 - 2a_1 - 4a_2 - a_3 + 6b_0 = 4$
$5a_3 - 2a_2 + a_1 + 6b_0 = 4$

$a_3 + 2a_2 + 4a_1 - 2a_1 - 4a_2 - a_3 = 0$
$-2a_2 + 2a_1 = 0$

$6a_3 + 4a_2 + 5a_1 - 2a_1 - 4a_2 - a_3 + 3b_0 = 1$
$5a_3 + 3a_1 + 3b_0 = 1$

$5a_3 - 2a_2 - 3a_2 + 2b_0 - 2 + 6b_0 = 4$
$-2a_2 - 6a_2 + 4b_0 - 4 = 0$
$5a_3 - 9a_2 + 6b_0 - 6 + 3b_0 = 1$

$5a_3 - 9a_2 + 9b_0 = 7$
$5a_3 - 5a_2 + 8b_0 = 6$
$-8a_2 + 4b_0 = 4$
$-4a_2 + b_0 = 1$

$5a_3 + 0 + 8 = 6$
$5a_3 = 5$
$a_3 = 1$

$5a_3 + 5a_2 + 2b_0 = 0$
$5a_3 - 5a_2 + b_0 = 6$
$6a_2 + 4b_0 = 4$
$3a_2 + b_0 = 1$
$2b_0 = 2$

$2b_0 = 2$
$b_0 = 1 \neq 6$
$a_2 = 0$
$a_3 = 1$

$a_1 = 2 - 2 = 0$ ✓
$a_0 = -$