
O
G
D
O
O
O
O
D

Knights + Knaves

ZIGZAG

\# permutations ?

identical letters do not appear together

total # permutations

$\frac{6!}{2!\,2!} = 180$

repeated letters

$\frac{5!}{2!}$ ways to choose ZZ together

repeated GG

$$\boxed{\frac{6!}{2!\cdot 2!} - 2\cdot\frac{5!}{2!} + 4!}$$

RSA Encryption Problem

Bob's private key $p = 13$ $q = 11$

$e = 5$?

$n = pq$

$c = M^e \bmod n$ ← Alice

$M = c^d \bmod n$ ← Bob $\quad ed \equiv 1 \pmod{(p-1)(q-1)}$

$5d \equiv 1 \pmod{(13-1)(11-1)}$

$5d = 1 \pmod{120}$ Linear Congruence

Solve

$ax \equiv b \pmod m$ $\quad gcd(a,m) = 1$ ← solution only exists

thus $gcd(5,120) = 5 \neq 1$

Thus the choice of 5 for C is incorrect

Choice 2: $c = 7$

$gcd(7,120) = 1$ ✓

$7d \equiv 1 \bmod (120)$ $\quad d = ?$

$1 = s\cdot 7 + t\cdot 120$

$103\cdot 7 - 6\cdot 120$

$= 721 - 720 = 1$ ✓

$d = 103$

Truth Tables

p	q	p ∧ q	p ∨ q	p ⊕ q	p → q	p ↔ q
1	1	1	1	0	1	1
1	0	0	1	1	0	0
0	1	0	1	1	1	0
0	0	0	0	0	1	1

Domains

Natural : 0, 1, 2, 3 ....

Integers : ... -3, -2, -1, 0, 1, 2, 3

Rational : $-\infty, \infty$

Real : $-\infty, \infty$ including i

Predicat Logic

- order of quantifiers doesnt matter if they are the same type

$\forall x \forall y (x<y) \equiv \forall y \forall x (x<y)$

- Negations + De Morgans

$\neg \forall x P(x) \equiv \exists x \neg P(x)$

$\neg \exists x P(x) \equiv \forall x \neg P(x)$

$\forall x P(x) \equiv \neg \exists x \neg P(x)$

$\exists x P(x) \equiv \neg \forall x \neg P(x)$

can bring in or bring out ¬

proofs via game :

∀ chooses first trying to prove false

∃ chooses second trying to prove sentence true

if ∃ wins TRUE

Propositional Logic Rules

$p \to q \equiv \neg q \to \neg p$

$p \land q \equiv q \land p$

$p \lor q \equiv q \lor p$

$p \land (q \land r) \equiv (p \land q) \land r$

$\neg\neg p = p$

$p \land (p \lor q) \equiv p$

$p \lor (p \land q) \equiv p$

$\neg(p \land q) \equiv \neg p \lor \neg q$

$\neg(p \lor q) \equiv \neg p \land \neg q$

$A \leftrightarrow B \equiv (A \land B) \lor (\neg A \land \neg B)$

$\neg(p \leftrightarrow q) \equiv p \oplus q$

$p \leftrightarrow q \equiv (p \lor \neg q) \land (\neg p \lor q)$

Choosing Problems

wrong?

Table for Selection Problems

Repetitions Allowed	no	yes	order matters?
r-permutations	$\frac{n!}{(n-r)!}$	n^r	Yes
r-combinations	$\binom{n}{r}$	$\binom{r+n-1}{n-1}$	No

$\binom{n}{r} = \frac{n!}{r!(n-r)!}$

$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

Objects	Boxes: labeled	Boxes: unlabeled
labeled	$n!$ / $n_1!n_2!\cdots n_k!$	$\left\{ n \atop k \right\}$
unlabeled	$\binom{r+n-1}{n-1}$	$p(n)$

total options left

choices left each person

APPEASE

permutations

$\frac{7!}{2!2!2!}$ $\frac{5!}{2!}$ 2

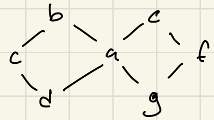
Ex: How many 10 digit #'s not starting with zero

permutations with 10 digits = 10!

permutations start with zero = 9!

answer $10! - 9! = 3265920$

- count subsets
- then count permutations of subsets



4 colors no same touching

a c,f b,c,d,g

$4 \cdot 3^2 \cdot 2^4$

$= 576$ choices

Fermats Little Thrm

Ex: $x \equiv 2703^{2019} \pmod 5$

$x = 3^{2019} \pmod 5$

Fermats applies

5 = prime and is not multiple of 3

$\boxed{a^{p-1} \equiv 1 \pmod p}$

$2019 = 4 \cdot 504 + 3$

$x \equiv 3^{4 \cdot 504} \cdot 3^3 \pmod 5$

$3^4 \equiv 1 \pmod 5$

$x \equiv 1 \cdot 27 \pmod 5$

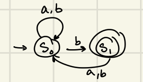
Thus $x \equiv 2$

2703 mod 13 = 12 = -1

DFA

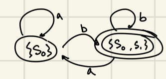
NFA → DFA

NFA



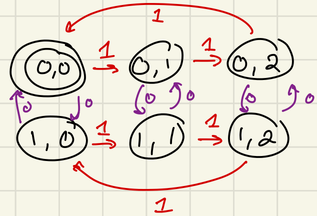
must end in b

DFA

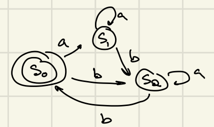


even # 0's

3 · # 1's



$(a,b)^*$ length ≤ 4



aabb
baab
abab
bbbb

$(a^* b a^* b)^*$

Proving Big-O

$0 < \lim_{x \to \infty} \frac{f(x)}{g(x)} < \infty$

least complexity

$2^x(x^2+x) = \Omega(2^x)$ ← proves this True

$\to \lim_{x\to\infty} \frac{|\cancel{2^x}(x^2+x)|}{|\cancel{2^x}|} = \lim_{x\to\infty} (x^2+x) = \infty$ → proves $O(2^x)$ false

$\to \lim_{x\to\infty} \frac{|2^x(x^2+x)|}{|3^x|} = \lim_{x\to\infty} \left(\frac{2}{3}\right)^x (x^2+x) = 0$ (<1)

proves $\Omega(3^x)$ false

proves $O(3^x)$ true

Injective: no two outputs the same (unique)

Surjective: every output is satisfied

Bijective: both

Countability

$\mathbb{R}$ not countable

Int countable

$\mathbb{N}$ countable

Rational #'s countable

S = {infinite set} → countable

power set (S) = uncountable

Strong Induction

$a_1 = 4$ $a_2 = 12$

prove $2^n | a_n$

Base case: $n=1$ $\frac{4}{2}$ ✓ $n=2$ $\frac{12}{4}$ ✓

strong induction because a_{n-1} and a_{n-2} must be proved

$a_n = 10a_{n-1} - 12a_{n-2}$

IH: $= 10s\,2^{n-1} - 12t\,2^{n-2}$

$2^n\left(\frac{10s}{2} - \frac{12t}{4}\right) = 2^n(5s-3t)$ proved

$\gcd(a,b) = \gcd(a, a-b)$

$\boxed{F_0 = 0 \quad F_1 = 1 \quad F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2}$

def of Fibonacchi sequence

Weak Induction

prove for all N, $5^n - 2^n$ is a multiple of 3

① (base case) $n=0$ $5^0 - 2^0 = 0$ $3 \cdot 0 = 0$ ✓

② (inductive step) $5^n + 2^n = 3k$ ← use for sub

$5^{n+1} - 2^{n+1} = 5 \cdot 5^n - 2 \cdot 2^n + 3 2^n - 3 2^n$

$5(5^n - 2^n) + 3 2^n$

IH $5(3k) + 3 2^n$

$3(5k + 2^n)$

Practice Problems

① write a scentence $\sqrt{2}$ is irrational

$$\forall n \forall m \left(\sqrt{2} \neq \frac{m}{n}\right)$$

$$\forall n \forall m (n\sqrt{2} \neq m)$$

$$\neg \exists n \exists m (n \neq 0 \wedge n \cdot n \cdot 2 = m \cdot m)$$

② $f: A \to B$ $\quad A_1 \subseteq A$, $A_2 \subseteq A$

$$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$$

$f(A_1) = \{ f(a) \in B \mid a \in A_1 \}$ imige of A_1

③ F_n $\quad \boxed{F_0 = 0 \quad F_1 = 1 \quad F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2}$

def of Fibonachi sequence

Prove F_{nm} is a multiple of F_n.

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55

$F_{10} = F_{2 \cdot 5}$ multiple of F_2, F_5

Proof by induction

Base Case: $m = 0$ $\quad F_{0 \cdot n} = F_0 = 0$ $\quad$ 0 is a multiple of all intigers

Inductive step: IH: $F_{m \cdot n} = l F_n$ $\quad l \in \mathbb{N}$

$$F_{(m+1)n} = F_{mn+n} = F_{mn} F_{n-1} + F_n F_{nm+1}$$

IH: $\rightarrow$

given $F_{n+k} = F_k F_{n+1} + F_{k-1} F_n$

$$l F_n F_{n-1} + F_n F_{mn+1}$$

$$= F_n (l F_{n-1} + F_{mn+1})$$

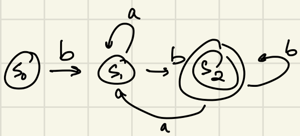
$$= \boxed{l' F_n}$$

$mn = n$
$n = k$

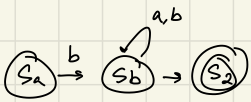
④ $\{a, b\}$ $b(a \cup b)^* b$

bb, bab, bbb, ...

Draw a DFA for Language:



deterministic



non deterministic

⑤ RSA Encryption Problem

Bob's private key $p = 13$ $q = 11$

$e = 5$?

$n = pq$

$c = M^e \bmod n$ ← Alice

$M = c^d \bmod n$ ↙ Bob

$ed \equiv 1 \pmod{(p-1)(q-1)}$

$5d \equiv 1 \pmod{(13-1)(11-1)}$

$5d = 1 \pmod{120}$ Linear Congruence

Solve

$ax \equiv b \pmod m$ $\boxed{\gcd(a, m) = 1}$ ↙ solution only exists

thus $\gcd(5, 120) = 5 \neq 1$

Thus the choice of 5 for C is incorrect

Choice 2: $c = 7$

$\gcd(7, 120) = 1$ ✓

$7d \equiv 1 \bmod (120)$ $d = ?$

$1 = s \cdot 7 + t \cdot 120$

$103 \cdot 7 - 6 \cdot 120$

$= 721 - 720 = 1$ ✓

$d = 103$

⑥ 1347 digit sum = 15

1030 digit sum = 4

how many 4 digit numbers have a digit sum = 9

0123
not a 4 digit number

1000 → 999

9 units into 4 boxes

1233 → 9

24 12 → 9

8010 → 9

first box must contain at least 1 digit

only realy 8 units into 4 boxes

$$\binom{8+4-1}{4-1} = \binom{11}{3} = \frac{11\cdot 10\cdot \cancel{9}}{\cancel{3}\cdot\cancel{2}\cdot 1} = 165$$

Table for Selection Problems

	Repititions Allowed: no	yes	order matters?
r-permutations	$\frac{n!}{(n-r)!}$	n^r	Yes
r-combinations	$\binom{n}{r}$	$\binom{r+n-1}{n-1}$	No

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

Practice Final Exams

① Allister + Bob

one is knight and one is knave

$t \to \neg b$

$b \to \neg t$

bob cannot be a knight

thus bob is a knave

② $A = \mathbb{N} - \{0,1\}$

$f : A \to A$

$f(15) = f(3 \cdot 5) = 3$

injective? surjective? bijective?

$f(2) = 2$ not injective
$f(4) = 2$

is surjective

③ $a_n = 10a_{n-1} - 12a_{n-2}$ for $n > 2$

$a_1 = 4$ $a_2 = 12$ Prove with strong induction $2^n \mid a_n$ for $n \geq 1$

base case: $n = 1$ $n = 2$

$2^1 = a_1 \Rightarrow \frac{4}{2} = 2$ $4 = 12$ $\frac{12}{4} = 3$

if $1 \leq m < n$ then $2^m \mid a_m$

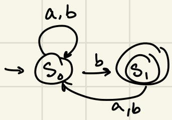
$a_n = 10a_{n-1} - 12a_{n-2}$

$\overset{IH}{=} 10s\,2^{n-1} - 12t\,2^{n-2}$

$2^n\left(\frac{10s}{2} - \frac{12t}{4}\right) = 2^n(5s - 3t)$

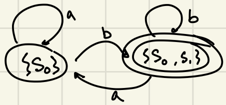
(4) NFA → DFA

NFA



must end in b

DFA



(5)

(6) $k \geq n$ both positive ints

distribute k indistinguishable apples into n distinguishable children where each child has at least 1 apple

$$\binom{k-n+n-1}{n-1} = \binom{k-1}{n-1}$$

in particular for $k=6 \quad n=4$

$$\binom{5}{3} = \frac{5!}{3!\cdot 2!} \quad \frac{5\cdot 4\cdot \cancel{3\cdot 2\cdot 1}}{\cancel{3\cdot 2\cdot 1}\cdot 2\cdot 1} = \boxed{10}$$

Practice Exam 2

① $a \to d \leftrightarrow \neg a$

$\neg d \to \neg a \leftrightarrow \neg a$

$\neg d \to$ True

manuscript not in Library

imposible to tell if Arch is truthfull

Good at knights + knaves

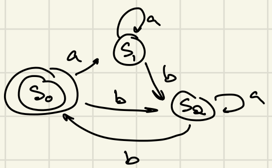
② injective function

$\mathbb{N}^2 \to \mathbb{Z}$ $|\mathbb{N} \times \mathbb{N}| < \mathbb{Z}$

$f_a(x,y) = 3^x - 2^y$ ✓ not injective

$f_b(x,y) = 3^x \cdot 2^y$

③ $(a,b)^*$ length ≤ 4



aabb
baab
abab
bbbb

$(a^* b a^* b)^*$

④ $2703^{2019^{12^{15}}}$

1300
×2
2600
2691

13 × 7
91

$12^{2019^{12^{15}}}$ ← posotive odd # power of thus odd

$12^{12} \equiv 1 \mod 13$

(5) How may 10 digit #'s not starting with zero

permutations with 10 digits = $10!$

permutations start with zero = $9!$

answer $10! - 9! = 3265920$

(6) ZIGZAG

permutations ?

identical letters do not apper together

total # permutations

$$\frac{6!}{2!\,2!} = 180$$

repeated letters

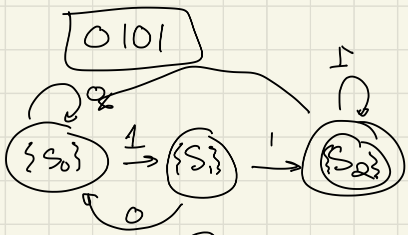
$\frac{5!}{2!}$ ways to choose ZZ together

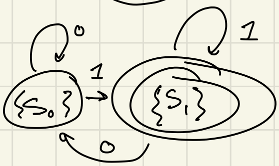
repeated GG

① All make the same claim must be on the same team

② The union of finite sets is not finite

③





④ $p = 5$ $q = 3$

odd prime #

$m = 3^{4/2}$ $m = 3^2 = 9$

⑤ 9 performances

3 different operas for each

Amneris Verdis Aida
Brunhilde Wagners walkure
Carmen Bizets Carmen

(5) $\frac{6!}{2!2!2!}$

(6) 3 dice 18 total options

2 must show same value

$\frac{r+n-1}{n-1} = \binom{4}{1}$ $\frac{4!}{3!}$

order doesnt matter 6 ways

order does matter 18 ways

3 rolls produce consecutive increasing values

2, 3, 4

order matters ...

$$\left.\begin{array}{ccc} 1 & 2 & 3 \\ \hline 2 & 3 & 4 \\ 3 & 4 & 5 \\ 4 & 5 & 6 \end{array}\right\} \quad 3!$$

(1)

$a \to b$

$b \to \neg c$

$c \to d \wedge e$

$d \to \neg a$

$e \to c \wedge \neg e$

e nave

b knight

a knight

d nave

c nave

(2) $\boxed{x^4,\ e^{(\log x)^2},\ x^{\sqrt{x}},\ e^x}$

2.5/3

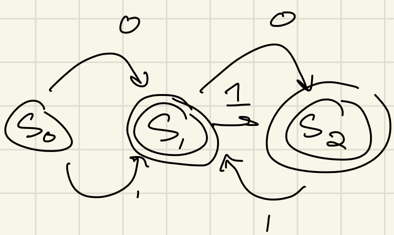
$e^{2\log x}$

$e^2 + e^{\log x}$

$\underline{e^2 + x}$ $\quad e^x \quad x^{x^{1/2}}$

(3) accepts all words {0,1} that do not contain 0,0,0

3.5/4



1930
193

193 x 10
1930
x11

2

(4) $2703^{2021^1} \bmod 193$

$1^{2021^1} \bmod 193$

$\boxed{1}$

(5) $\gcd(a,b) = \gcd(a \quad , a \div b)$

$\gcd(a, 1) = \underline{1}$

4/5

1, 2, ...

$n = 0$

(6)

①

$a \leftrightarrow t_1 \wedge (\neg a \wedge \neg b)$ a and
$b \leftrightarrow a$ b knaves
t_1 not tresure

$c \leftrightarrow t_2 \wedge (\neg c \wedge \neg d)$ both naves
$d \leftrightarrow c$ t_2 not treasure

$e \leftrightarrow t_3 \wedge \neg f$ e nave
$f \leftrightarrow t_3 \wedge e$ t_3 is treasure
f knight

② week induction

$n \in \mathbb{N}$ $(1+x)^n \geq 1 + nx$

$x > -1$

$\underline{(1+x)^n = 1 + nx}$ IH

<u>base case</u> $n=0$

$(1+x)^0 \geq 1 + 0x$ ✓
$1 \geq 1$

<u>induction</u>

$(1+x)^{n+1} \geq 1 + nx + x$

$(1+x)^n (1+x) \geq (1 + x) + nx$

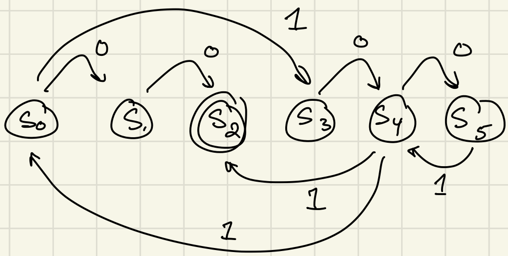
true
$\boxed{1+nx \geq 1 + \frac{nx}{(1+x)}}$

IH
$(1+nx)(1+x) \geq (1+x) + (nx) =$

(3) even # 0's

1's multiple of 3

minimal automaton 6 states



00

10011

(4) smallest > 2022

$$x \equiv 3 \pmod{4}$$
$$x \equiv 3 \pmod{27}$$
$$x \equiv 3 \pmod{25}$$