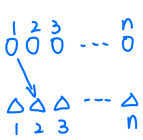
Cheatsheet

1. derangement 公式

$$D_n = n!\left(1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\cdots+(-1)^n\frac{1}{n!}\right)$$

$$\lim_{n\to\infty}\frac{D_n}{n!}=\frac{1}{e}$$



假如1选3 2(这步有(n-1)种选择)
然后假如2选了1，那么剩下的就是a_{n-2}
2不选1，那么相当于a_{n-1}

$a_n=(n-1)(a_{n-1}+a_{n-2})$

2. 存在 + imply 是个奇怪的组合 遇到个试试

$\exists x \exists y\ P(x)\to\neg P(y)$，又要找到 $P(x)=F$ 就行

3. countable 题

注意：(1) 2^N 量级的都算 uncountable
(2) 注意可能的对"无穷"的暗示
比如如果说某个数又能有偶数位
那就是暗示一定不是无穷位

4. Combination: 组合. 无序

permutation: 排列. 有序

k-combination: 从原来的set中无序地选k个 distinct element

- Roster method: 枚举set中的element
- singleton set: 只有一个元素的set
- proper subset: 真包含的subset
- cardinality: unique elements的数量
- power set: 所有子集的集合
- ordered n-tuple: 有序n元集合，或者看成 $\forall \in F^n$ 也行
- cartesian product: $A\{a,b\}\ B\{c,d\} \longrightarrow A*B\{(a,c),(a,d),(b,c),(b,d)\}$
- Relation: a relation from A to B ($A*B$的一个子集)
- disjoint: A and B is disjoint ($A\cap B=\emptyset$)
- difference: $A-B=\{1,3,5\}-\{1,2,3\}=\{5\}$
- (也叫complement) Universal compliment: 关于全集的补集
- conjunction: $\wedge$ disjunction: $\vee$
- $\oplus$: XOR, p,q一样为0，不一样为1
- converse: $q\to p$ inverse: $\neg p\to\neg q$
- biconditional: $p\leftrightarrow q$
- paradox 悖论 postulate = premise = 前提
- p if q: $q\to p$
- p only if q (p iff q): $p\to q$

PNF: 把所有quantifier扔到最前面

5. 中国剩余定理:

let $m_1, m_2, \cdots, m_n$ 两两互质且 $m_i>1$，a_i 为任意数

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ x\equiv a_2 \pmod{m_2} \\ \vdots \\ x\equiv a_n \pmod{m_n} \end{cases}$$

那 $x \bmod (m_1\cdots m_n)$ 有唯一确定值

Consider the 3 congruences from Sun-Tsu's problem:
$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.
Let $m = 3\cdot 5\cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$.
We see that

- 2 is an inverse of $M_1 \pmod 3$
- 1 is an inverse of $M_2 \pmod 5$
- 1 is an inverse of $M_3 \pmod 7$

Hence,
$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$
$= 2\cdot 35\cdot 2 + 3\cdot 21\cdot 1 + 2\cdot 15\cdot 1 = 233 \equiv 23 \pmod{105}$

Cryptograph

Secret Key Cryptography

(1) Caesar Cipher (Shift Cypher)

secret key: k
encryption 加密: $f(p)=(p+k) \bmod 26$
$p \to f(p)$
decryption 解密: $f^{-1}(p)=(p-k) \bmod 26$
$f^{-1}(f(p)) \mapsto p$

(2) Affine Ciphers

$ax+b\equiv y \pmod{26}$ has a unique solution

secret key: (a,b), s.t. $\gcd(a,26)=1$
$f(p)=(ap+b) \bmod 26$
$f^{-1}(p)$: solve $ap+b\equiv c \pmod{26}$

(3) Block Ciphers

粗浅地理解为把 mod 26 变成 mod 一个大数

$f(p)=ap+b \pmod{2^{80}}$
$f^{-1}(y)=a^{-1}(y-b) \pmod{2^{80}}$
- $\frac{1}{2}\cdot 2^{80}\cdot 2^{80}$ different keys

(4) Advanced Encryption Standard

repeated squaring technique

Compute $a^n \pmod m$ efficiently for large n

express $a^n \equiv a^{b_0\cdot 2^0}\cdot a^{b_1\cdot 2^1}\cdot\cdots \pmod m$
(first express $n=b_0\cdot 2^0+b_1\cdot 2^1+\cdots$)

代入 $\begin{cases} a^{2^1} \bmod m \\ a^{2^2} \bmod m = \left(a^{2^1} \bmod m\right)^2 \bmod m \\ \vdots \end{cases}$

discrete logarithm: solve $a^x\equiv r \pmod p$
for given a, r, p (very large)

Diffe-Hellman Key exchange

Alice $\xrightarrow{a^{k_1} \bmod p}$ Bob ($(a^{k_1})^{k_2} \bmod p$)
($(a^{k_2})^{k_1} \bmod p$) Alice $\xleftarrow{a^{k_2} \bmod p}$ Bob
shared key: $a^{k_1k_2} \bmod p$

Public Key Cryptography & RSA

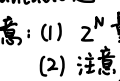
key { communicate physically / use DH protocol
→ { public key / private key

RSA Encryption ($n=p\cdot q$, which two large prime and hard to discover)
Alice $\xrightarrow{C}$ Bob
传递 $C=x^e \bmod n$ → 要加密的东西 → 从这里算出 x 很困难
(p,q) private key
(n,e) is public key → $\gcd(e,(p-1)(q-1))=1$ 一般 randomly picked

RSA Decryption
① Find d. $d=e^{-1} \pmod{(p-1)(q-1)}$
② Find $c^d \bmod n = X$

L08: Algorithm

selection sort: 每次把后面i个最大的放在第n-i个位置上



大O表示法:

Big-θ:
↑ infinitely many, 但有一组就行
$f(x)$ is $\theta(g(x)) \Leftrightarrow \exists c_1,c_2,k>0$ (witness), s.t. $c_1\cdot g(x)\le f(x)\le c_2\cdot g(x)$ $(x>k)$

$\log(n!)=\theta(n\log n)$ → 但 $n!\neq\theta(n^n)$ (用放缩来证) → $n!=O(n^n)$, $n!=\Omega((\frac{n}{2})^{\frac{n}{2}})$

$\sum\frac{1}{x}=\theta(\log n)$
$c_1^n >> n^{c_2}$

Big-Oh:
$f(x)$ is $O(g) \Leftrightarrow \exists c_2,k>0$ (witness), s.t. $f(x)\le c_2 g(x)$ $(x>k)$

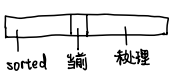
Big-Omega:
$f(x)$ is $\Omega(g) \Leftrightarrow \exists c_1,k>0$ (witness), s.t. $f(x)\ge c_1 g(x)$ $(x>k)$

$f(x)=\theta(g(x)) \Leftrightarrow f(x)=O(g(x))$ & $f(x)=\Omega(g(x))$

Comparison of algorithms:
计算 $\lim_{n\to\infty}\frac{T_1(n)}{T_2(n)}$ { $=0$ 比快 / $\to\infty$ 比快 / $=$ Constant / 振荡 (cannot tell)

↳ 假如 $T_1(n), T_2(n)$ 都可表示为 θ 记号
也可以研究 $\lim_{n\to\infty}\frac{g_1(n)}{g_2(n)}$
($T_1(n)=\theta(g_1(n))$ $T_2(n)=\theta(g_2(n))$)

Insertion sort



每次把key插入到 sorted sequence 中合适的位置

Worse-case Analysis (default analysis)

To show worse-case $=O(n^2)$:
{ show $O(n^2)$
* find a input which is $\Omega(n^2)$

Strong Induction

{ $P(1)\ \vee$
$(P(1)\wedge P(2)\wedge\cdots\wedge P(k))\to P(k+1)$

Fermat Little Theorem
$a^{p-1}\equiv 1 \pmod p$

Lemma: $a \bmod p, 2a \bmod p, \cdots, (p-1)a \bmod p$ 是 $\{1,2,\cdots,p-1\}$

* Structural induction:
假如一个set是recursively defined的
证明它有某性质P { base case 有P / 这个结构由base case construct construct 可保留P

E1, ..., En pairwise independent

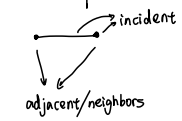
$\Leftrightarrow P(E_i\cap E_j)=P(E_i)\cdot P(E_j)$
for all $1\le i<j\le n$

E1, ..., En mutual independent

$\Leftrightarrow P(E_1\cap\cdots\cap E_n)=P(E_1)\cdots P(E_n)$
(且两两独立)

Mutual independent ⇒ Pairwise independent

L18: Graph



simple graph: graph without loops/multiple edges

edge { directed (u,v) / undirected $\{u,v\}$

degree { undirected: 跟该node incident的边
directed: { In-degree 指向该顶点的edge的数量 $\deg^-(v)$ / Out-degree 从该顶点出发的edge的数量 $\deg^+(v)$

$G_1=(V,E)$, undirected, m edges $\Rightarrow \sum_{v\in V}\deg(v)=2m$

$G_2=(V,E)$, directed, m edges $\Rightarrow m=\sum_{v\in V}\deg^-(v)=\sum_{v\in V}\deg^+(v)$

Special graphs

① complete graph K_n
点之间两两都有连线

② cycle C_n ($n\geq 3$)
△ □ ⬠ ---

Bipartite graph ∈ simple graph

↳ 能被完全分为两部分，边只能分别属于这两部分

complete Bipartite graph $K_{m,n}$
能被分size为m,n的两部分，使得两部分相互全连接
且每部分之间无连接

Subgraph

endpoint为edge是subset即可

Adjacent list

形容edge用

adjacency matrices { undirected symmetric & diagonal entry=0 (simple graph)
directed not necessarily symmetric

$a_{ij}=\begin{cases}1 & \text{if } \{v_i,v_j\} \text{ is an edge}\\ 0 & \text{otherwise}\end{cases}$

↳ non-simple graph: a_{ij}为i,j之间相连的边数

Incident matrices

$n\times m$ matrix, n=vertex数, m=edge数

$m_{ij}=\begin{cases}1 & (v_i \text{和} e_j \text{ incident})\\ 0 & (\text{otherwise})\end{cases}$

Graph Isomorphism

对两个simple graph $G_1=(V_1,E_1)$, $G_2=(V_2,E_2)$
isomorphic ⟺ 存在一个T(transformation), 使得
$T(v_1)=v_2$, $v_1\in V_1$, $v_2\in V_2$, 在
transform之后 E_1和E_2完全相同

determine if isomorphic (time complexity) { worse case: exponential / average case: linear

Path

$e_1,\cdots,e_n$ { directed: e_i connects x_{i-1} and x_i / undirected: $e_i=(x_{i-1},x_i)$

for simple graph: path: $x_0,x_1,\cdots,x_n$ ($x_i\in V$)
if $u=v$, path is a circuit/cycle (始=终)
simple path/circuit: 每条edge经过一次

Connectivity

2 vertices u,v are connected ⟺ there's a path from u to v

a/undirected graph is connected if 对$\forall$顶点对，都有通路

directed graph is { weakly connected if 忽略边向连通
strongly connected if 不忽略边向连通

connected component { connected subgraph
不能被包含于更大的connected subgraph里

strongly connected component { strongly connected subgraph
不能被包含于更大的strongly connected subgraph里

Euler circuit ⟺ 每个点的度数都是偶数 & 图是connected的
起点=终点，每条边经过一次

Euler path ⟺ 恰好两个点的degree是奇数，其他都是偶数 & 图connected
起点，不用=终点，每边经过一次
↓
证明：把两个奇点相连，则存在euler circuit ∨

Hamilton Paths & Circuits
contains every vertex once

Random Variables

↳ 一个把sample space中的element map到$\mathbb{R}$的函数
(这个function不是random的)

Bernoulli trials

结果binary且试验之间互相独立

Binomial distribution 二项分布

n次伯努利experiment的分布

$P(X=k)=C_n^k\cdot p^k\cdot(1-p)^{n-k}$
$E(X)=np$
$E(aX+b)=aE(X)+b$
$V(X)=np(1-p)$

Geometric distribution

X是伯努利试验第一次成功时的次数

$P(X=k)=(1-p)^k\cdot p$
$E(X)=\frac{1}{p}$
$V(X)=\frac{1-p}{p^2}$

Expected Value

$E(X)=\sum p(x)\cdot X$

Indicator random variable

$X_i\in\{0,1\}$，用来描述事件E_i是否发生

Independent random variables

$P(X=r_1 \,\&\, Y=r_2)=P(X=r_1)\cdot P(Y=r_2)$

$E(XY)=E(X)\cdot E(Y)$

Variance

$V(X)=E\left((X-E(X))^2\right)$
$=\sum p(x)\cdot(X-E(X))^2$
$=E(X^2)-E(X)^2$

$V(aX)=a^2V(X)$

Bienaymé's Formula

for independent random variables X, Y,

$V(X+Y)=V(X)+V(Y)$

if $X_1\sim X_n$ (pairwise independent)

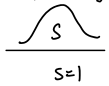
$\Rightarrow V(X_1+\cdots+X_n)=V(X_1)+\cdots+V(X_n)$

experiment: 比如扔骰子
sample space: 事件结果的集合
event: sample space的subset
↳ { Complement of Events: $\overline{E}$
Union of Events: $E_1\cup E_2$ $(P(E_1\cup E_2)=P(E_1)+P(E_2)-P(E_1\cap E_2))$
disjoint union: union中每个事件相互无重合 $(P(E_1\cup E_2)=P(E_1)+P(E_2))$

sampling without replacement: 无放回抽样
sampling with replacement: 放回抽样

↓

Probability distribution
pmf: probability mass distribution

pdf: probability density function


Uniform & non-uniform distribution
↳ sample space里的sample被选到的概率一样

Independence ⟺ $P(E\cap F)=P(E)\cdot P(F)$
check this { 用定义
两个event完全无关

L05: Modular Arithmetic

$a|b$ ⟺ a divides b ⟺ b/a is an integer
反面: $a\nmid b$
(a: factor/divisor of b
b: multiple of a

$(a \bmod mn) \bmod m = a \bmod m$
∵ $\begin{cases}a=gmn+s & (0\leq s<mn)\\ a=g'\cdot m+s' & (0\leq s'<m)\end{cases}$
⟺ $s \bmod m = s'$
⟺ $(a-gmn) \bmod m = s'$
⟺ $a \bmod m = s'$ ✓

☆ $\begin{cases}(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m\\ (a\cdot b) \bmod m = (a \bmod m \cdot b \bmod m) \bmod m\end{cases}$

Arithmetic modulo (在$\mathbb{Z}_m$上定义)

新记号: $\mathbb{Z}_m=\{0,1,\cdots,m-1\}$
对于$a,b\in\mathbb{Z}_m$
定义: $\begin{cases}a+_m b=(a+b) \bmod m\\ a\cdot_m b=(a\cdot b) \bmod m\end{cases}$
有交换，结合，分配律

Additive inverse & multiplicative inverse

① additive inverse (for a): $(-a \bmod m)$
有 $a+_m(-a \bmod m)=0$

② multiplicative inverse (for a): $a\cdot_m b=1$
for $\forall a\in\mathbb{Z}_m$, $m>1$, $\gcd(a,m)=1$
$\Rightarrow a$ 有 unique multiplicative inverse
if $\gcd(a,m)\neq 1$, a^{-1}不存在

☆找 a^{-1}: extended euclidean algorithm
用bézout theorem的办法找出
$1=c_1\cdot a+c_2\cdot m$
$\Rightarrow 1\equiv c_1\cdot a+c_2\cdot m \pmod m$
$\equiv c_1\cdot a \pmod m$
$\therefore c_1=a^{-1}$

Congruences (在$\mathbb{Z}$上定义)

a is congruent to b ⟺ $a \bmod m = b \bmod m$
⟺ $a\equiv b \pmod m$
↳ modulus
notation

☆ $a/c\neq b/d \pmod m$

L06: GCDs & Congruences

gcd: 最大公约数

Euclidean algorithm: 辗转相除法

Bézout's Theorem:
if $a,b\in\mathbb{Z}^+$, $\exists c_1,c_2\in\mathbb{Z}$, s.t. $\gcd(a,b)=c_1a+c_2b$
(gcd的$\forall$倍数都能找到c_1,c_2)

找c_1,c_2的办法:
例2: 找 $\gcd(252,198)$:

$252=198\times 1+54$	$\Rightarrow 54=252-198\times 1$
$198=3\cdot 54+36$	$36=198-3\cdot 54$
$54=1\cdot 36+18$	$=198-3\cdot(252-198\cdot 1)$
$36=2\times 18+0$	$=4\cdot 198-3\cdot 252$
$\Rightarrow \gcd(252,198)=18$	$=\cdots$
	$=4\cdot 252-5\cdot 198$

解同余方程

Linear congruence:

$ax\equiv b \pmod m$

① find a^{-1}
② $a^{-1}\cdot ax\equiv a^{-1}\cdot b \pmod m$
$\Rightarrow x\equiv a^{-1}\cdot b \pmod m$

if $\gcd(a,m)\neq 1$, 那么 $ax\equiv b \pmod m$ 可能有 { 0解 / or / 多解 } in $\mathbb{Z}_m$