Chapter 3 Algorithms

pseudocode example

procedure binary-search

Sorting algorithms studied in this book: binary(二分), insertion(插入), bubble(冒泡), selection(选择) merge(归并), quick(快排), tournament(锦标赛排序)

Greedy Algorithms

makes the "best" choice at each step.

Halting problems

§3.2 The growth of Functions

Definition: $O(g)$, at most order g

$$\{f: R \to R \mid \exists c,k: \forall x > k: f(x) \le cg(x)\}$$

f is $O(g)$

$\forall c>0, O(cf)=O(f+c)=O(f-c)=O(f)$

if $f_1 \in O(g_1) \wedge f_2 \in O(g_2) \to f_1 f_2 = O(g_1 g_2)$

$f_1 + f_2 \in O(g_1+g_2) = O(\max(g_1, g_2))$

Definition: Big-Omega $\Omega(g)$ at least order g

$f(x)$ is $\Omega(g(x))$ iff $g(x)$ is $O(f(x))$.

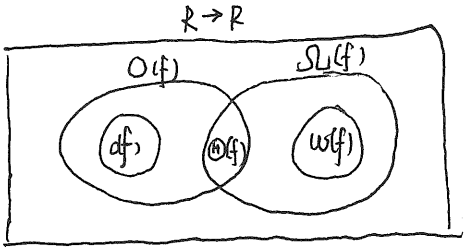
Definition: Big-Theta $\Theta(g)$, exactly order g

prove: $\left(\sum_{i=1}^{n} i\right) \in \Theta(n^2)$

solution $\left(\sum_{i=1}^{n} i\right) = \frac{n(n+1)}{2} = \frac{n}{2} \cdot \Theta(n)$

$= n \cdot \Theta(n)$

$= \Theta(n^2)$



$\Theta(1)$ constant

$\Theta(\log_c n)$ Logarithmic

$\Theta(n \log_c n)$ n log n complexity

$\Theta(n)$ linear

$\Theta(n^c)$ Polynomial

$\Theta(c^n), c>1$ Exponential

$\Theta(n!)$ Factorial

学术专业英语单词

Matrices 矩阵
Algorithms 算法
cryptography 密码学
paradigm 模型
pseudocode 伪码
iterate 迭代
restrict 控制
logarithmic 对数
polynomial 多项式
exponential 指数
factorial 阶乘
modular 模数
arithmetic 算法
congruence 全等
exponention 求幂
permutation 排列
combinations 组合
consecutive 连续的
parenthesize 加括号
homogeneous 齐次
recurrence 递推
coefficient 系数
reflexive 自反的
symmetric 对称的
composite 合成

Chapter 4

If n is a composite integer, then n has a prime divisor less than or equal $\sqrt{n}$

$a = dq + r$

d divisor 除数
a dividend 被除数
q quotient 商
r remainder 余数

remainder cannot be negative

$q \bmod 4 = 1$
$q \bmod 3 = 0$
$q \bmod 10 = 9$
$73 \bmod 4 = 3$

remainder must be positive

$a \equiv b \pmod m \iff a \bmod m = b \bmod m$

$46 \equiv 68 \pmod{11}$

$\because 11 \mid (68-46)$

if $a \equiv b \pmod m$ and $c \equiv d \pmod m$

then $a+c \equiv b+d \pmod m$ and $ac \equiv bd \pmod m$

$a = bq + r$

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

RSA

p and q should not be too close together

$(p-1)$ and $(q-1)$ should not have small prime factors