Notes of TAOCP V1

Sean Go

Feb, 2018

Chapter 1

Basic concepts

1.1 Algorithms

1.1.1 Algorithm

Algorithm E(Euclid's algorithm) for finding the greatest common divisor of two non-negative integers.

Algorithm 1: Algorithm E. Euclid's GCD algorithm

```
1  function EuclidGcd (m, n);
   Input  : Two non-negative integers m and n.
   Output: gcd(m, n)
2  if m < n then
3  |  m ↔ n
4  end
5  r ← m mod n;
6  repeat
7  |  m ← n;
8  |  n ← r;
9  |  r ← m mod n;
10 until r = 0;
11 return n
```

Proof. after line 5, we have $m = qn + r$, if $r = 0$ then m is a multipe of n. if $r \neq 0$, any number that divides both m and n, must divide $m - qn = r$, so $gcd(m, n) = gcd(n, r)$. □

Algorithm has five important features:

1. Finiteness
2. Definiteness
3. Input
4. Output
5. Effectiveness

1.1.2 Algorithmic Analysis

Algorithmic Analysis : Given an algorithm, we want to determinate its performance characteristics.
For Algorithm E, if n is known, what is the average times T_n for all positive m?
$T_n \sim ((12 \ln 2)\pi^2) \ln n$, when n is very large.
Analysis of Algorithm

1.1.3 Computational Method

A computational method is a quadruple $\{Q, I, \Omega, f\}$, in witch Q is a set containing subset I and Ω, and f is a function from Q into himself.

1.2 Mathematical preliminaries

1.2.1 Mathematical Induction

Mathematical Induction

1. give a proof that P(1) is true
2. if P(1), P(2), ..., P(n) is true, then P(n+1) is true, for all positive integer n.

partitions of n the number of different ways to write n as sum of positive integers, disregarding order. *Algorithm E(Extend Euclid's algorithm).* Give two positive integers m and n, we compute their greatest common divisor d, and two integers a and b such that $am + bn = d$.

List of Algorithms

List of source codes

Index