Discrete Mathematics Recitation Class

Tianyu Qiu

University of Michigan - Shanghai Jiaotong University

Joint Institute

Summer Term 2019

Contents

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $m_1, \ldots, m_n \in \mathbb{N} \setminus \{0\}$ *be pairwise relatively prime and let* $a_1, \ldots, a_n \in \mathbb{Z}$ *. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 (\mod m_1) \\ x &\equiv a_2 (\mod m_2) \\ &\vdots \\ x &\equiv a_n (\mod m_n) \end{aligned} \tag{1}$$

has a unique solution $(\mod m)$ *where* $m = m_1 \cdots m_n$.

Chinese Remainder Theorem

Proof.

We first prove the existence of a solution. For all $1 \leq k \leq n$, define

$$M_k = \frac{m}{m_k} = \prod_{i \neq k} m_i$$

Note that since $m_1, \ldots, m_n$ are pairwise relatively prime, it follows that for all $1 \leq k \leq n, \gcd(m_k, M_k) = 1$. Therefore for all $1 \leq k \leq n$ $[M_k]_{m_k} \in (\mathbb{Z}/m_k\mathbb{Z})^*$ and there exists $y_k \in \mathbb{Z}$ such that

$$[M_k y_k]_{m_k} = [M_k]_{m_k} \otimes_{m_k} [y_k]_{m_k} = [1]_{m_k} \text{ or } M_k y_k \equiv 1 \pmod{m_k}$$

Chinese Remainder Theorem

Proof(Continued).

Let

$$x = \sum_{k=1}^{n} a_k M_k y_k$$

since for all $1 \leq i, j \leq n$, if $i \neq j$, then $M_i \equiv 0 \pmod{m_j}$, it follows that x is a solution to (1).

We now turn to showing uniqueness. Let $x, x' \in \mathbb{Z}$ be such that for all $1 \leq k \leq n$,

$$x \equiv a_k \equiv x' \pmod{m_k}$$

We will show that x and x' must be congruent $\pmod{m}$. Now, for all $1 \leq k \leq n, m_k | (x - x')$. An elementary induction argument applied to one of the consequences of Bézout's Lemma that we proved shows that since for all $1 \leq i, j \leq n$ with $i \neq j, \gcd(m_i, m_j) = 1$

Chinese Remainder Theorem

Proof(Continued).

$$m = m_1 \cdots m_n | (x - x')$$

This shows that

$$x \equiv x' \pmod m$$

□

Useful Conclusion:
Given that b, c relatively prime, $a < b, a < c$

$$\begin{cases} x \equiv a \pmod b \\ x \equiv a \pmod c \end{cases} \Leftrightarrow x \equiv a \pmod{bc}$$

Wilson's Theorem

Theorem (Wilson's Theorem)

Let $p \in \mathbb{N}$ be prime. Then

$$(p-1)! \equiv -1 (mod\ p)$$

Theorem

There are infinitely many composite numbers in the form $n! + 1$

Classification of Algorithms

- By Function
  1. Sorting Algorithm:
     - Binary Sort
     - Insertion Sort
     - Selection Sort
     - Merge Sort
     - Quick Sort
  2. Searching Algorithm:
     - Linear Search
     - Binary Search
- By Form
  - Recursive Algorithm
  - Iterative Algorithm

Time Complexity

1. Classification
   - Time Complexity
   - Space Complexity (not covered in this course)
2. Cases
   - Best Case
   - Average Case
   - Worst Case

Attention:

- Only two cases with the same # of input n can be compared.
- It is usually hard to calculate $T(n)$ for the average case, but easier for the best or the worst case.

Landau Symbol

Definitions:

1. *big oh* (O): Let A be $\mathbb{R}$ or $\mathbb{N}$. Let $f : A \longrightarrow \mathbb{R}$ and $g : A \longrightarrow \mathbb{R}$. We say f is $O(g)$, pronounced "f is big-oh of g", if there exists $k, C \in \mathbb{N}$ such that for all $x \in A$ with $x > k, |f(x)| \leq C|g(x)|$. We call O the Landau symbol big-oh.
2. *big omega* (Ω): If g is $O(f)$, then f is $\Omega(g)$.
3. *big theta* (Θ): If f is $O(g)$ and f is $\Omega(g)$, then f is $\Theta(g)$.

Theorem

Let $f : \mathbb{N} \longrightarrow \mathbb{R}$ and $g : \mathbb{N} \longrightarrow \mathbb{R}$. If there exists $C \in \mathbb{R}$ with $C \geq 0$ such that

$$\lim_{n\to\infty} \frac{|f(n)|}{|g(n)|} = C$$

then f is $O(g)$.

Landau Symbol

Theorem

$\ln(n!)$ *is order* $n\ln(n)$

Theorem

Let $n \in \mathbb{N} \setminus \{0\}$. *If* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *is a polynomial of degree* n, *then* f *is order* x^n.

Theorem

Let $p, q \in \mathbb{R}$ *with* $0 < p < q$. *Then* n^q *is not* $O\left(n^p\right)$

Theorem

n *is not* $O(\ln(n))$

Recurrence Relations

Definition:
Let $f : \mathbb{N} \times \mathbb{C}^k \longrightarrow \mathbb{C}$ and let $a_0, \ldots, a_{k-1} \in \mathbb{C}$. A function $g : \mathbb{N} \longrightarrow \mathbb{C}$ that satisfies:

$$\begin{aligned} g(n) &= a_n & 0 \leqslant n < k \\ g(n) &= f(n, g(n-1), \cdots, g(n-k)) & n \geqslant k \end{aligned}$$

is said to satisfy recurrence relation defined by f with initial conditions $a_0, \cdots, a_{k-1}$. (P306)

Theorem

Let $f : \mathbb{N} \times \mathbb{C}^k \longrightarrow \mathbb{C}$ and let $a_0, \ldots, a_{k-1} \in \mathbb{C}$. Then there exists a unique $g : \mathbb{N} \longrightarrow \mathbb{C}$ that satisfies the recurrence relation define by f with initial conditions $a_0, \ldots, a_{k-1}$. (P308)

Linear Recurrence Relations

Definition:
linear recurrence relation (P316):

1. degree k
2. homogeneous & inhomogeneous

Theorem

Let (a_n) and (b_n) satisfy the homogeneous linear recurrence relation

$$x_n = c_1 x_{n-1} + \cdots + c_k x_{n-k} \tag{2}$$

Then for all $A, B \in \mathbb{C}$, the sequence $(Aa_n + Bb_n)$ also satisfies (2).

Characteristic Polynomial

Definition:
characteristic polynomial: If $\alpha \in \mathbb{C}$ and the sequence (a_n) defined by $a_n = \alpha^n$ satisfies the homogeneous linear recurrence relation

$$x_n = c_1 x_{n-1} + \cdots + c_k x_{n-k} \tag{3}$$

Then $\alpha^n = c_1\alpha^{n-1} + \cdots + c_k\alpha^{n-k}$. So, if $\alpha \neq 0$, then α is a root of the polynomial

$$\lambda^k - c_1\lambda^{k-1} - \cdots - c_k \tag{4}$$

(4) is the characteristic polynomial of the recurrence relation (3).

Characteristic Polynomial

Theorem

If $\alpha_1, \ldots, \alpha_k$ are roots of the characteristic polynomial of the linear recurrence relation (3) then for all $A_1, \ldots, A_k \in \mathbb{C}$, the sequence (a_n) defined by

$$a_n = A_1\alpha_1^n + \cdots + A_k\alpha_k^n$$

satisfies (3).

Vandermonde Matrix

Lemma

Let $\alpha_1, \dots, \alpha_k$ be distinct roots of the polynomial

$$\lambda^k - c_1\lambda^{k-1} - \dots - c_k$$

Then the $k \times k$ matrix

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_k^2 \\ \vdots & & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_k^{k-1} \end{pmatrix}$$

is invertible.

Homogenous Linear Recurrence Relations

Theorem

Let $a_0, \dots, a_{k-1} \in \mathbb{C}$. *Let* $\alpha_1, \dots, \alpha_k$ *be* k *distinct roots of the characteristic polymial of the recurrence relation*

$$x_n = c_1 x_{n-1} + \cdots + c_k x_{n-k} \tag{5}$$

Then there exists a sequence (a_n) *in the form*

$$a_n = q_1 \alpha_1^n + \cdots + q_k \alpha_k^n$$

that satisfies (5) with initial conditions $a_0, \dots, a_{k-1}$.

Homogenous Linear Recurrence Relations

Theorem

Let $a_0, \ldots, a_{k-1} \in \mathbb{C}$. Let $\alpha_1, \ldots, \alpha_t$ be roots of the characteristic polymial of the recurrence relation

$$x_n = c_1 x_{n-1} + \cdots + c_k x_{n-k} \tag{6}$$

with multiplicities $m_1, \ldots, m_t$, respectively. Then there exists a sequence (a_n) in the form

$$a_n = Q_1 \alpha_1^n + \cdots + Q_t \alpha_t^n$$

$$\text{with } Q_i = \sum_{j=0}^{m_i - 1} q_{i,j} n^j \text{ for } 1 \le i \le t$$

that satisfies (6) with initial conditions $a_0, \ldots, a_{k-1}$

Inhomogeneous Linear Recurrence Relations

Suppose that the sequences (a_n) and (b_n) both satisfy the recurrence relation

$$x_n = c_1 x_{n-1} + \cdots + c_k x_{n-k} + f'(n) \tag{7}$$

$$\text{So } a_n - b_n = c_1 (a_{n-1} - b_{n-1}) + \cdots + c_k (a_{n-k} - b_{n-k})$$

And $(a_n - b_n)$ satisfies the recurrence relation

$$x_n = c_1 x_{n-1} + \cdots + c_k x_{n-k} \tag{8}$$

Theorem

Let (a_n) satisfy the recurrence relation (12). If (b_n) satisfies the recurrence relation (12) then (b_n) is of the form

$$b_n = c_n + a_n$$

where (c_n) satisfies the recurrence relation (8).

Inhomogeneous Linear Recurrence Relations

This means that by finding a single sequence (a_n) satisfying

$$x_n = c_1 x_{n-1} + \cdots + c_k x_{n-k} + f'(n) \tag{9}$$

we can determine a sequence (b_n) satisfying (9) with any prescribed initial conditions.

Inhomogeneous Linear Recurrence Relations

Theorem

Let $c_1, \ldots, c_k \in \mathbb{R}$ and consider the inhomogenoeous recurrence relation

$$x_n = c_1 x_{n-1} + \cdots + c_k x_{n-k} + f'(n) \text{ with } f'(n) = \left(\sum_{i=0}^{t} b_i n^i \right) s^n \tag{10}$$

Then (10) has a particular solution in the form

$$n^m \left(\sum_{i=0}^{t} q_i n^i \right) s^n$$

JOINT INSTITUTE 交大密西根学院

Inhomogeneous Linear Recurrence Relations

Theorem (Continued)

where $m = 0$ if s is not a root of the characteristic polynomial of the homogeneous recurrence relation associated with (10), and if s is a root of the characteristic polynomial of the homogeneous recurrence relation associated with (10), then m is the multiplicity of that root.

Examples for Recurrence Relations

- Homogeneous Linear Recurrence Relation:
  1. Distinct Solutions for Characteristic Polynomial

$$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$$

  2. Solutions with Multiplicities for Characteristic Polynomial

$$a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$$

- Inhomogeneous Linear Recurrence Relation:
  1. $f(x)$ where x is not the solution for characteristic polynomial

$$a_n = 5a_{n-1} - 6a_{n-2} + 7^n$$

  2. $f(x)$ where x is the solution for characteristic polynomial

$$a_n = 6a_{n-1} - 9a_{n-2} + 3^n$$

Examples for Recurrence Relations

e.g.
Let (a_n) be the sequence such that $a_0 = 0, a_1 = 1,$

$$a_n = 5a_{n-1} - 6a_{n-2} + 2^n + 3^n$$

Determine a_n as function of n $(n \in \mathbb{N})$.