Unit 1.4 Mathematical Backgrounds

Algorithms

EE/NTHU

Mar. 17, 2020

Mathematical Backgrounds

Monotonicity

- A function $f(n)$ is monotonically increasing if $m \leq n$ implies $f(m) \leq f(n)$.
- A function $f(n)$ is monotonically decreasing if $m \leq n$ implies $f(m) \geq f(n)$.
- A function $f(n)$ is strictly increasing if $m < n$ implies $f(m) < f(n)$.
- A function $f(n)$ is strictly decreasing if $m < n$ implies $f(m) > f(n)$.

Floor and ceiling functions

- For any real number x, we denote the greatest integer less than or equal to x by $\lfloor x \rfloor$ and the least integer greater than or equal to x by $\lceil x \rceil$.
- For any real x

$$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1. \tag{1.4.1}$$

- For any integer n,

$$\lceil n/2 \rceil + \lfloor n/2 \rfloor = n. \tag{1.4.2}$$

- For any real number $x \geq 0$ and integers $m, n > 0$,

$$\lceil \lceil x/m \rceil / n \rceil = \lceil x/(mn) \rceil, \tag{1.4.3}$$

$$\lfloor \lfloor x/m \rfloor / n \rfloor = \lfloor x/(mn) \rfloor, \tag{1.4.4}$$

$$\lceil m/n \rceil \leq (m + (n-1))/n, \tag{1.4.5}$$

$$\lfloor m/n \rfloor \leq (m + (n-1))/n. \tag{1.4.6}$$

- The floor function $\lfloor x \rfloor$ is monotically increasing, so is the ceiling function $\lceil x \rceil$.

Mathematical Backgrounds, II

Modular arithmetic

- For any integer m and positive integer n, the value $m \bmod n$ is the remainder (or residue) of the quotient m/n:

$$m \bmod n = m - \lfloor m/n \rfloor n. \tag{1.4.7}$$

- If $(a \bmod n) = (b \bmod n)$, we write $a \equiv b \pmod n$ and say a is equivalent to b, modulo n.
- $a \equiv b \pmod n$ if a and b have the same remainder when divided by n.
- $a \equiv b \pmod n$ if and only if n is a divisor of $b - a$.
- We write $a \not\equiv b \pmod n$ if a is not equivalent to b, modulo n.

Mathematical Backgrounds, III

Polynomials

- Given a nonnegative integer n, a polynomial in x of degree n is a function $p(x)$ of the form

$$p(x) = \sum_{k=0}^{n} a_k x^k, \tag{1.4.8}$$

  where the constants $a_0, a_1, \cdots, a_n$ are the coefficients of the polynomial and $a_n \neq 0$.
- A polynomial is asymptotically positive if and only if $a_n > 0$.
- For an asymptotically positive polynomial $p(x)$ of degree n, we have $p(x) = \Theta(x^n)$.
- For any real constant $c >= 0$ then function x^c is monotonically increasing, and for any real constant $c <= 0$, the function x^c is monotonically decreasing.
- We say that a function $f(x)$ is polynomial bounded if $f(x) = \mathcal{O}(x^k)$ for some constant k.

Mathematical Backgrounds, IV

Exponentials

- For all real $a > 0$, m and n, we have the following identities:

$$a^0 = 1, \tag{1.4.9}$$

$$a^1 = a, \tag{1.4.10}$$

$$a^{-1} = 1/a, \tag{1.4.11}$$

$$(a^m)^n = a^{mn}, \tag{1.4.12}$$

$$(a^m)^n = (a^n)^m, \tag{1.4.13}$$

$$a^m \cdot a^n = a^{m+n}. \tag{1.4.14}$$

- For all n and $a \geq 1$, the function a^n is monotonically increasing in n. When convenient, we assume $0^0 = 1$.
- For all real constants a and b such that $a > 1$,

$$\lim_{n \to \infty} \frac{n^b}{a^n} = 0, \tag{1.4.15}$$

thus

$$n^b = o(a^n). \tag{1.4.16}$$

That is any exponential function with a base strictly greater than 1 grows faster than any polynomial function.

Mathematical Backgrounds, V

- Let e be the base of the natural logarithm function, $e = 2.71828\cdots$, we have for all real x

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \sum_{k=0}^{\infty} \frac{x^k}{k!}. \tag{1.4.17}$$

- For all real x, we have the inequality

$$e^x \geq 1 + x, \tag{1.4.18}$$

withe the equality holds only when $x = 0$.
- When $|x| \leq 1$, we have the approximation

$$1 + x \leq e^x \leq 1 + x + x^2. \tag{1.4.19}$$

- Considering $x \to 0$, we have

$$e^x = 1 + x + \Theta(x^2). \tag{1.4.20}$$

- For all real x, we have

$$\lim_{n \to \infty} (1 + \frac{x}{n})^n = e^x. \tag{1.4.21}$$

Mathematical Backgrounds, VI

Logarithms

- The following notations are adopted

$$\begin{aligned} \lg n &= \log_2 n && \text{(binary logarithm)}, \\ \ln n &= \log_e n && \text{(natural logarithm)}, \\ \lg^k n &= (\lg n)^k && \text{(exponentiation)}, \\ \lg \lg n &= \lg(\lg n) && \text{(composition)}. \end{aligned}$$

- We also adopt the convention that the logarithm functions only apply to the next term in the formula, so that $\lg n + k = (\lg n) + k$.
- If $b > 1$ is a constant, then for $n > 0$ the function $\log_b n$ is strictly increasing.
- For all $a > 0$, $b > 0$, $c > 0$ and n,

$$\begin{aligned} a &= b^{\log_b a}, \\ \log_c(ab) &= \log_c a + \log_c b, \\ \log_b a^n &= n \log_b a, \\ \log_b a &= \frac{\log_c a}{\log_c b}, \\ \log_b(1/a) &= -\log_b a, \\ \log_b a &= \frac{1}{\log_a b}, \\ a^{\log_b c} &= c^{\log_b a}, \end{aligned}$$

  where the base of each logarithm is not 1.

Mathematical Backgrounds, VII

- When $|x| < 1$,

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \cdots. \tag{1.4.22}$$

- For $x > -1$,

$$\frac{x}{1+x} \le \ln(1+x) \le x. \tag{1.4.23}$$

  where the equality holds only for $x = 0$.
- A function $f(n)$ is polylogarithmically bounded if $f(n) = \mathcal{O}(\lg^k n)$ for some constant k. Since

$$\lim_{n\to\infty} \frac{\lg^b n}{(2^a)^{\lg n}} = \lim_{n\to\infty} \frac{\lg^b n}{n^a} = 0, \tag{1.4.24}$$

  we have

$$\lg^b n = o(n^a) \tag{1.4.25}$$

  for any constant $a > 0$. Thus, any positive polynomial function grows faster than any polylogarithmic function.
- Change the base of a logarithm from one constant to another changes the value by a constant factor, so in conjunction with the $\mathcal{O}$-notation, the use of $\log$, or $\lg$ or $\log_2$ are equivalent.

Mathematical Backgrounds, VIII

Factorials

- The factorial function, $n!$, is define for integers $n \geq 0$ as

$$n! = \begin{cases} 1 & \text{if } n = 0, \\ n \cdot (n-1)! & \text{if } n > 0. \end{cases} \tag{1.4.26}$$

  Thus, $n! = 1 \cdot 2 \cdot 3 \cdots n$.
- A weak upper bound on the factorial function is $n! \leq n^n$.
- Stirling's approximation

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \left(1 + \Theta(\frac{1}{n})\right). \tag{1.4.27}$$

- Thus

$$\begin{aligned} n! &= o(n^n), \\ n! &= \omega(2^n), \\ \lg(n!) &= \Theta(n \lg n). \end{aligned}$$

- For $n \geq 1$

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\alpha_n}, \tag{1.4.28}$$

  where

$$\frac{1}{12n+1} < \alpha_n < \frac{1}{12n}.$$

Mathematical Backgrounds, IX

Function iteration

- The notation $f^{(i)}(x)$ is used to denote function $f(x)$ iteratively applied i times to an initial value of x.
- That is, let $f(x)$ be a function over the reals. Given a nonnegative integer i, define

$$f^{(i)}(x) = \begin{cases} n & \text{if } i = 0, \\ f(f^{(i-1)}(x)) & \text{if } i > 0. \end{cases} \tag{1.4.29}$$

- For example, if $f(x) = 2x$, then $f^{(i)}(x) = 2^i x$.
- Note the difference of $f^{(i)}(x)$ and $f^i(x)$, which is $f(x)$ raised to the ith power.

Iterative logarithm function

- The iterative logarithm function is defined as

$$\lg^* x = \min\{i \geq 0 | \lg^{(i)} x \leq 1\}. \tag{1.4.30}$$

- Example

$$\begin{aligned} \lg^* 2 &= 1, \\ \lg^* 4 &= 2, \\ \lg^* 16 &= 3, \\ \lg^* 65536 &= 4, \\ \lg^* 2^{65536} &= 5. \end{aligned}$$

  The iterative logarithm function is a very slow growing function.

Fibonacci numbers

- The Fibonacci numbers are defined as

$$\begin{aligned} F_0 &= 0, \\ F_1 &= 1, \\ F_i &= F_{i-1} + F_{i-2} \quad \text{for } i \geq 2. \end{aligned} \tag{1.4.31}$$

- The first few Fibonacci numbers are

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \cdots .$$

- The Fibonacci number is related to the golden ratio, ϕ, and its conjugate, $\widehat{\phi}$, as

$$F_i = \frac{\phi^i - \widehat{\phi}^i}{\sqrt{5}}. \tag{1.4.32}$$

  And,

$$\begin{aligned} \phi &= \frac{1+\sqrt{5}}{2} &= 1.61803\cdots , \\ \widehat{\phi} &= \frac{1-\sqrt{5}}{2} &= -0.61803\cdots . \end{aligned} \tag{1.4.33}$$

- It can be shown that

$$F_i = \left\lfloor \frac{\phi^i}{\sqrt{5}} \right\rfloor . \tag{1.4.34}$$

  Thus, the Fibonacci numbers grow exponentially.

TSING HUA UNIVERSITY