Math 788

Computational Number Theory

Web-page:

http://www.math.sc.edu/~filaseta/gradcourses/Math788M.html

Grading: **Homework (50%)**
1 Test (20% each)
Cumulative Final (30%)

The kinds of questions we are addressing in this course:

- **What is a good computational approach for ...?**
- **How fast can we ...?**
- **How do we justify this?**

Here, we may be referring to basic arithmetic operations, computing gcd's, primality testing, factoring integers, factoring polynomials, etc.

Big-Oh & Little-Oh Notation (as well as $\ll$, $\gg$, $\sim$, $\asymp$)

Definitions. Let $f(x)$ and $g(x)$ be functions with domain $[c, \infty)$ for some $c \in \mathbb{R}$ and range $\mathbb{R}$ and $\mathbb{R}^+$, respectively.

$f(x) = O(g(x))$ ("$f(x)$ is big-oh of $g(x)$")

$\iff \exists\, C > 0, x_0 > 0$ such that $|f(x)| \leq Cg(x), \forall\, x \geq x_0$

$f(x) \ll g(x)$ ("$f(x)$ is less than less than $g(x)$")

$\iff f(x) = O(g(x))$

$f(x) \gg g(x)$ ("$f(x)$ is greater than greater than $g(x)$")

$\iff g(x) = O(f(x))$

Definitions. Let $f(x)$ and $g(x)$ be functions with domain $[c, \infty)$ for some $c \in \mathbb{R}$ and range $\mathbb{R}$ and $\mathbb{R}^+$, respectively.

$f(x) = O(g(x))$ ("$f(x)$ is big-oh of $g(x)$")

$$\iff \exists\, C > 0, x_0 > 0 \text{ such that } |f(x)| \leq Cg(x), \forall\, x \geq x_0$$

$f(x) \ll g(x)$ ("$f(x)$ is less than less than $g(x)$")

$$\iff f(x) = O(g(x))$$

$f(x) \gg g(x)$ ("$f(x)$ is greater than greater than $g(x)$")

$$\iff g(x) = O(f(x))$$

$f(x) \asymp g(x)$ ("the asymptotic order of $f(x)$ is $g(x)$")

$$\iff g(x) \ll f(x) \ll g(x) \text{ (or write } f(x) \gg\ll g(x))$$

$f(x) = o(g(x))$ ("$f(x)$ is little-oh of $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 0$

$f(x) \sim g(x)$ ("$f(x)$ is aymptotic to $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$

Definitions. Let $f(x)$ and $g(x)$ be functions with domain $[c, \infty)$ for some $c \in \mathbb{R}$ and range $\mathbb{R}$ and $\mathbb{R}^+$, respectively.

$f(x) = O(g(x))$ ("$f(x)$ is big-oh of $g(x)$")

$$\iff \exists\, C > 0, x_0 > 0 \text{ such that } |f(x)| \leq Cg(x),\ \forall\, x \geq x_0$$

$f(x) \ll g(x)$ ("$f(x)$ is less than less than $g(x)$")

$$\iff f(x) = O(g(x))$$

$f(x) \gg g(x)$ ("$f(x)$ is greater than greater than $g(x)$")

$$\iff g(x) = O(f(x))$$

$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$

Note: Analogous definitions exist if the domain is $\mathbb{Z}^+$.

Examples

1. $\log(1 + (1/n)) = O(1/n)$

Definitions. Let $f(x)$ and $g(x)$ be functions with domain $[c, \infty)$ for some $c \in \mathbb{R}$ and range $\mathbb{R}$ and $\mathbb{R}^+$, respectively.

$f(x) = O(g(x))$ ("$f(x)$ is big-oh of $g(x)$")

$$\iff \exists\, C > 0, x_0 > 0 \text{ such that } |f(x)| \leq Cg(x), \forall\, x \geq x_0$$

$f(x) \ll g(x)$ ("$f(x)$ is less than less than $g(x)$")

$$\iff f(x) = O(g(x))$$

$f(x) \gg g(x)$ ("$f(x)$ is greater than greater than $g(x)$")

$$\iff g(x) = O(f(x))$$

$f(x) \asymp g(x)$ ("the asymptotic order of $f(x)$ is $g(x)$")

$$\iff g(x) \ll f(x) \ll g(x) \text{ (or write } f(x) \gg\ll g(x))$$

$f(x) = o(g(x))$ ("$f(x)$ is little-oh of $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 0$

$f(x) \sim g(x)$ ("$f(x)$ is aymptotic to $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$

Examples

1. $\log(1 + (1/n)) = O(1/n)$
2. **A positive integer n in base b contains $\asymp \log n$ digits.**

Definitions. Let $f(x)$ and $g(x)$ be functions with domain $[c, \infty)$ for some $c \in \mathbb{R}$ and range $\mathbb{R}$ and $\mathbb{R}^+$, respectively.

$f(x) = O(g(x))$ ("$f(x)$ is big-oh of $g(x)$")

$$\iff \exists\, C > 0, x_0 > 0 \text{ such that } |f(x)| \leq Cg(x), \forall\, x \geq x_0$$

$f(x) \ll g(x)$ ("$f(x)$ is less than less than $g(x)$")

$$\iff f(x) = O(g(x))$$

$f(x) \gg g(x)$ ("$f(x)$ is greater than greater than $g(x)$")

$$\iff g(x) = O(f(x))$$

$f(x) \asymp g(x)$ ("the asymptotic order of $f(x)$ is $g(x)$")

$$\iff g(x) \ll f(x) \ll g(x) \text{ (or write } f(x) \gg\ll g(x))$$

$f(x) = o(g(x))$ ("$f(x)$ is little-oh of $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 0$

$f(x) \sim g(x)$ ("$f(x)$ is aymptotic to $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$

Examples

1. $\log(1 + (1/n)) = O(1/n)$
2. **A positive integer n in base b contains $\asymp \log n$ digits.**
3. $1 + 2 + \cdots + n \sim \dfrac{n^2}{2}$

Definitions. Let $f(x)$ and $g(x)$ be functions with domain $[c, \infty)$ for some $c \in \mathbb{R}$ and range $\mathbb{R}$ and $\mathbb{R}^+$, respectively.

$f(x) = O(g(x))$ ("$f(x)$ is big-oh of $g(x)$")

$$\iff \exists\, C > 0, x_0 > 0 \text{ such that } |f(x)| \leq Cg(x), \forall\, x \geq x_0$$

$f(x) \ll g(x)$ ("$f(x)$ is less than less than $g(x)$")

$$\iff f(x) = O(g(x))$$

$f(x) \gg g(x)$ ("$f(x)$ is greater than greater than $g(x)$")

$$\iff g(x) = O(f(x))$$

$f(x) \asymp g(x)$ ("the asymptotic order of $f(x)$ is $g(x)$")

$$\iff g(x) \ll f(x) \ll g(x) \text{ (or write } f(x) \gg\ll g(x))$$

$f(x) = o(g(x))$ ("$f(x)$ is little-oh of $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 0$

$f(x) \sim g(x)$ ("$f(x)$ is aymptotic to $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$

Examples

1. $\log(1 + (1/n)) = O(1/n)$
2. A positive integer n in base b contains $\asymp \log n$ digits.
3. $1 + 2 + \cdots + n \sim \dfrac{n^2}{2}$
4. If f is a polynomial of degree k, then $f(n) = O(n^k)$.

Definitions. Let $f(x)$ and $g(x)$ be functions with domain $[c, \infty)$ for some $c \in \mathbb{R}$ and range $\mathbb{R}$ and $\mathbb{R}^+$, respectively.

$f(x) = O(g(x))$ ("$f(x)$ is big-oh of $g(x)$")

$$\iff \exists\, C > 0, x_0 > 0 \text{ such that } |f(x)| \leq Cg(x), \forall\, x \geq x_0$$

$f(x) \ll g(x)$ ("$f(x)$ is less than less than $g(x)$")

$$\iff f(x) = O(g(x))$$

$f(x) \gg g(x)$ ("$f(x)$ is greater than greater than $g(x)$")

$$\iff g(x) = O(f(x))$$

$f(x) \asymp g(x)$ ("the asymptotic order of $f(x)$ is $g(x)$")

$$\iff g(x) \ll f(x) \ll g(x) \text{ (or write } f(x) \gg\ll g(x))$$

$f(x) = o(g(x))$ ("$f(x)$ is little-oh of $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 0$

$f(x) \sim g(x)$ ("$f(x)$ is aymptotic to $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$

Examples

1. $\log(1 + (1/n)) = O(1/n)$
2. A positive integer n in base b contains $\asymp \log n$ digits.
3. $1 + 2 + \cdots + n \sim \dfrac{n^2}{2}$
4. If f is a polynomial of degree k, then $f(n) = O(n^k)$.
5. $(r+1)^\pi \sim r^\pi$

Definitions. Let $f(x)$ and $g(x)$ be functions with domain $[c, \infty)$ for some $c \in \mathbb{R}$ and range $\mathbb{R}$ and $\mathbb{R}^+$, respectively.

$f(x) = O(g(x))$ ("$f(x)$ is big-oh of $g(x)$")

$$\iff \exists\, C > 0, x_0 > 0 \text{ such that } |f(x)| \leq Cg(x), \forall\, x \geq x_0$$

$f(x) \ll g(x)$ ("$f(x)$ is less than less than $g(x)$")

$$\iff f(x) = O(g(x))$$

$f(x) \gg g(x)$ ("$f(x)$ is greater than greater than $g(x)$")

$$\iff g(x) = O(f(x))$$

$f(x) \asymp g(x)$ ("the asymptotic order of $f(x)$ is $g(x)$")

$$\iff g(x) \ll f(x) \ll g(x) \text{ (or write } f(x) \gg\ll g(x))$$

$f(x) = o(g(x))$ ("$f(x)$ is little-oh of $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 0$

$f(x) \sim g(x)$ ("$f(x)$ is aymptotic to $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$

Examples

1. $\log(1 + (1/n)) = O(1/n)$
2. A positive integer n in base b contains $\asymp \log n$ digits.
3. $1 + 2 + \cdots + n \sim \dfrac{n^2}{2}$
4. If f is a polynomial of degree k, then $f(n) = O(n^k)$.
5. $(r + 1)^\pi \sim r^\pi$
6. For every $k \in \mathbb{R}$ and $\varepsilon > 0$, we have $(\log x)^k = o(x^\varepsilon)$.

Definitions. Let $f(x)$ and $g(x)$ be functions with domain $[c, \infty)$ for some $c \in \mathbb{R}$ and range $\mathbb{R}$ and $\mathbb{R}^+$, respectively.

$f(x) = O(g(x))$ ("$f(x)$ is big-oh of $g(x)$")

$$\iff \exists\, C > 0, x_0 > 0 \text{ such that } |f(x)| \leq Cg(x), \forall\, x \geq x_0$$

$f(x) \ll g(x)$ ("$f(x)$ is less than less than $g(x)$")

$$\iff f(x) = O(g(x))$$

$f(x) \gg g(x)$ ("$f(x)$ is greater than greater than $g(x)$")

$$\iff g(x) = O(f(x))$$

$f(x) \asymp g(x)$ ("the asymptotic order of $f(x)$ is $g(x)$")

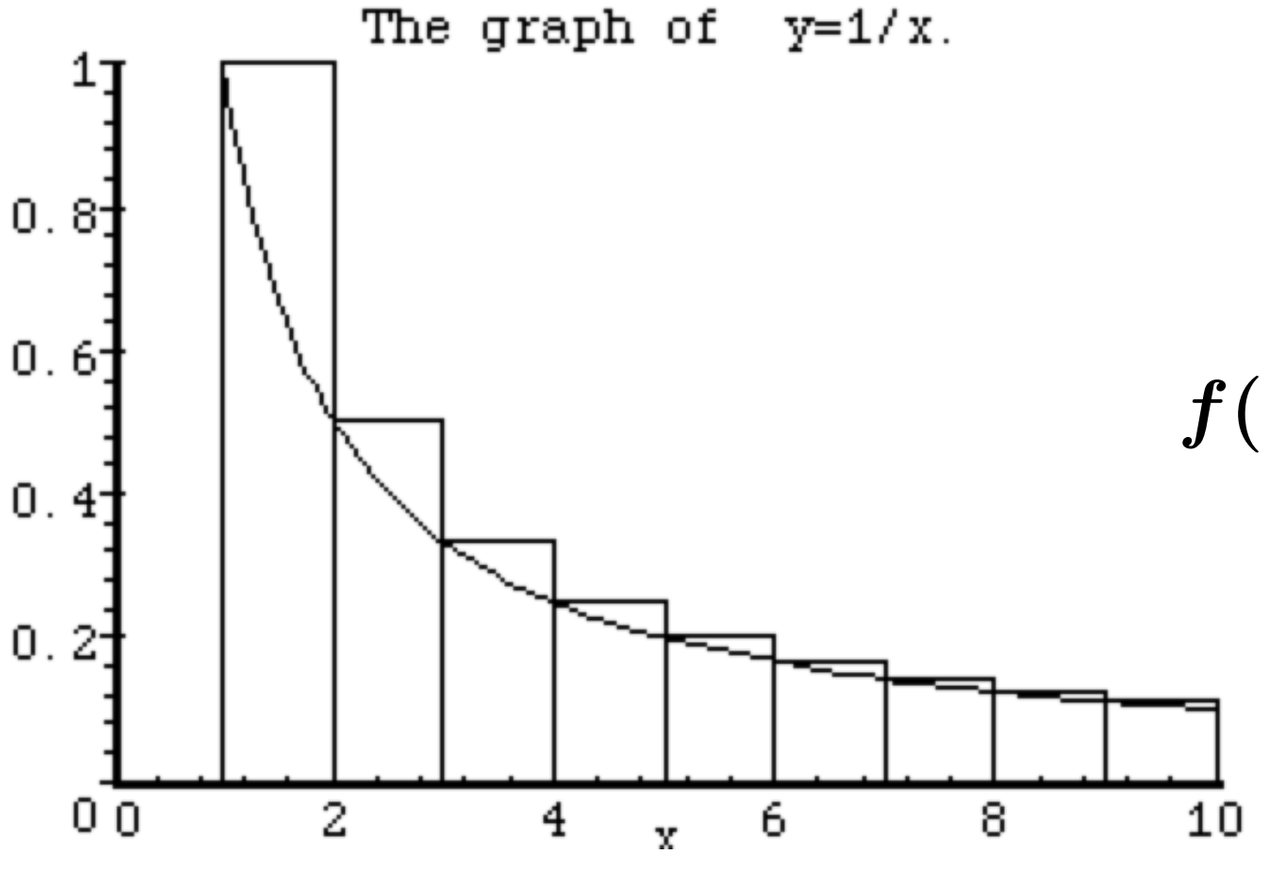
$$\iff g(x) \ll f(x) \ll g(x) \text{ (or write } f(x) \gg\ll g(x))$$

$f(x) = o(g(x))$ ("$f(x)$ is little-oh of $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 0$

$f(x) \sim g(x)$ ("$f(x)$ is aymptotic to $g(x)$") $\iff \lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$

Homework

(3) The value of $f(n) = \sum_{k=1}^{n} 1/k$ can be estimated by comparing it's value to an integral. For example, by comparing the sum of the areas of the rectangles indicated in the graph below with the area under the graph of $y = 1/x$, one obtains



$$f(9) \geq \int_1^{10} \frac{1}{x}\, dx = \log 10.$$

(c) Prove that $f(n) \sim \log n$.

Explicit Example: How quickly can we factor an $n \in \mathbb{Z}^+$?

We will want an "algorithm" that runs quickly (in a small number of steps) in comparison to the length of the input.

Explicit Example: How quickly can we factor an $n \in \mathbb{Z}^+$?

We will want an "algorithm" that runs quickly (in a small number of steps) in comparison to the length of the input. One considers the length of the input n to be $\lfloor \log_2 n \rfloor + 1$ (corresponding to the number of bits n has). An algorithm runs in polynomial time if the number of steps (or bit operations) it takes is bounded above by a polynomial in the length of the input. An algorithm to factor n in polynomial time would require that it take $O\left((\log n)^k\right)$ steps (and that it factor n).