Math/CSE 1019C: Discrete Mathematics for Computer Science
Fall 2012

Jessie Zhao
jessie@cse.yorku.ca

Course page:
http://www.cse.yorku.ca/course/1019

- Test 1 is ready to pick up!
  - For questions regarding Assignment 1 marking, please refer to Maria (mma@cse.yorku.ca).
  - For questions regarding Test 1 marking, please come to my office hours.
- Assignment 4 is released today!

Review: Countability

- A set is countable if
  - it is finite or
  - it has the same cardinality as the set of the positive integers Z^+ i.e. $|A| = |Z^+|$. The set is countably infinite
- We write $|A| = |Z+| = \aleph_0 =$ aleph null
- A set that is not countable is called uncountable
- Proving the set is countable infinite involves (usually) constructing an explicit bijection with Z^+

Review: Countability

- We have showed the following sets are countable by constructing a bijective function from each set to Z^+
  - The set of odd positive integers
    - f(n)=2n-1
  - The set of integers
    - f(n) = n/2 if n is even, and f(n)=(n-1)/2 if n is odd.

Review: Countability

- The union of two countable sets is countable.
  - Assume A and B are disjoint. (If not, then consider (A-B) and B, since $A \cup B = (A-B) \cup B$)
  - Both finite
    - $A \cup B$ is finite, and therefore countable
  - A is finite and B is countably infinite
    - $A=\{a_1,\ldots,a_{|A|}\}$, $g:N \to B$ is a bijection
    - New bijection $h_1: Z^+ \to A \cup B$
    - $h(n)=a_n$, if $n \le |A|$
      $=g(n-|A|)$, if $n>|A|$
  - Both countably infinite
    - $f: Z^+ \to A$, $g: Z^+ \to B$ are bijections
    - New bijection $h_2: Z^+ \to A \cup B$
    - $h_2(n) = f(n/2)$ if n is even
      $= g((n-1)/2)$ if n is odd.

The rationals are countable

- Step 1. Show that $Z^+ \times Z^+$ is countable.
- Step 2. Show injection between Q^+, $Z^+ \times Z^+$.
- Step 3. Construct a bijection from Q^+ to Q

(details done on the board)

The reals are not countable

- Wrong proof strategy:
- Suppose it is countable
- Write them down in increasing order
- Prove that there is a real number between any two successive reals.

- WHY is this incorrect?

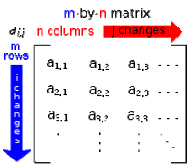
(Note that the above "proof" would show that the rationals are not countable!!)

The reals are not countable – 2

- Cantor diagonalization argument (1879)
- VERY powerful, important technique.
- Proof by contradiction.
- Sketch (details done on the board)
  - Assume countable
  - look at all numbers in the interval [0,1)
  - list them in ANY order
  - show that there is some number not listed

Matrix

- A matrix is a rectangular array of numbers.



Matrix Arithmetic

- A+B and A–B requires that A and B have the same number of columns and rows.

  Let A=[$a_{i,j}$], B=[$b_{i,j}$] be m–by–n matrices

  A+B=[$a_{i,j} + b_{i,j}$]

  A–B=[$a_{i,j} - b_{i,j}$]

Example: $A = \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$A+B = \begin{bmatrix} 2+1 & 4+0 \\ 3+0 & 1+1 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 3 & 2 \end{bmatrix} \quad A-B = \begin{bmatrix} 2-1 & 4-0 \\ 3-0 & 1-1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 3 & 0 \end{bmatrix}$$

- The product of A and B, denoted by AB.
- AB requires: The number of columns in A is the same as the number of rows in B.
- Let A be an m*k matrix and B be a k*n matrix. AB=[$c_{i,j}$] is a m*n matrix.

$$c_{i,j} = a_{i,1}b_{1,j} + a_{i,2}b_{2,j} + \ldots + a_{i,k}b_{k,j}$$

- Example $A = \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & -1 & 2 \\ 0 & 1 & 3 \end{bmatrix}$

- AB=?
- BA=?

Transpose

- Let A=[$a_{i,j}$] be an m*n matrix. The transpose of A, denoted by A', is an n*m matrix A'=[$a_{j,i}$]
- Example

$$B = \begin{bmatrix} 1 & -1 & 2 \\ 0 & 1 & 3 \end{bmatrix}$$

$$B' = \begin{bmatrix} 1 & 0 \\ -1 & 1 \\ 2 & 3 \end{bmatrix}$$

- More about Matrices: Linear Algebra

The Growth of Functions

- How fast does a function grow? How to measure it?
- We quantify the concept that g grows at least as fast as f.
- What really matters in comparing the complexity of algorithms?
  - We only care about the behaviour for large problems
  - Even bad algorithms can be used to solve small problems

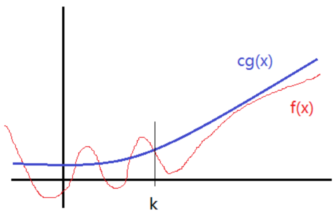
Big-O Notation

- Assume f:Z→R and g: Z→R.
- f(x) is O(g(x)) iff ∃ constants C and k such that

$$\forall x>k\ |f(x)| \leq C|g(x)|$$

  - Constants C and k are called witnesses
  - The choice of C may depend on the choice of k
  - When there is one pair of witnesses, there are infinitely many pairs of witnesses

Big-O Notation



Big-O Notation

- O(g) is a set called a complexity class
- O(g) contains all the functions which g dominates
- Notation: f is O(g) or f=O(g) means f∈O(g)

- Example: $f(x) = x^2+2x+1$ is $O(x^2)$.
- Proof:
  - Observe that whenever $x>1$, $1<x<x^2$ is true.
  - Then it follows that for $x>1$
  - $0 \leq x^2+2x+1 = |f(x)| \leq x^2+2x^2+x^2=4x^2 = 4|x^2|$
  - ∴k=1 and C=4
  - ∴$f(x) = O(x^2)$ or $f(x) \in O(x^2)$

- Example: $f(x) = 7x^2$ is $O(x^3)$.
- Proof:
  - Observe that whenever $x>1$, $x^2 <x^3$ is true.
  - Then it follows that for $x>1$
  - $0 \leq 7x^2 = |f(x)| \leq 7x^3 = 7|x^3|$
  - ∴k=1 and C=7
  - ∴$f(x) = O(x^3)$ or $f(x) \in O(x^3)$

- Is it true that x^3 is $O(7x^2)$?
  - Determine whether witnesses exist or not.
  - Assume we can find C and k such that
  - $x^3 \le C(7x^2)$ whenever $x>k$
  - i.e. $x \le 7C$ whenever $x>k$
  - No matter what C and k are, the inequality $x \le 7C$ cannot hold for all x with $x>k$.
  - So, x^3 is not $O(7x^2)$.

Growth of polynomial functions

- The leading term of a polynomial function determines its growth
- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$
  where $a_n, a_{n-1}, \ldots, a_1, a_0$ are real numbers.
- Then f(x) is **$O(x^n)$.**
- See the proof in textbook

Properties of Big-O

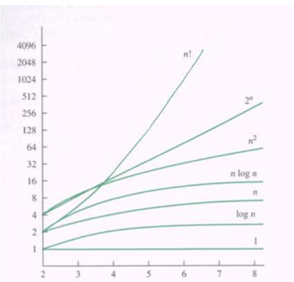
- f is O(g) iff $O(f) \subseteq O(g)$
- The set O(g) is closed under addition:
  - If $f_1(x)$ and $f_2(x)$ are both O(g(x)), then $(f_1 + f_2)(x)$ is O(g(x))
- The set O(g) is closed under multiplication by a scalar a ($a \in R$):
  - If f is O(g) then af is O(g)

Properties of Big-O

- If f is O(g) and g is O(h) then f=O(h)
  $O(f) \subseteq O(g) \subseteq O(h)$
- If f_1 is $O(g_1)$ and f_2 is $O(g_2)$ then
  - $f_1 f_2$ is $O(g_1 g_2)$
  - $f_1 + f_2$ is $O(\max\{g_1, g_2\})$

Important Complexity Classes

- $O(1) \subseteq O(\log n) \subseteq O(n) \subseteq O(n\log n) \subseteq O(n^2) \subseteq O(n^j) \subseteq O(c^n) \subseteq O(n!)$
- where j>2 and c>1



Some crucial facts

- Logarithmic << Polynomial
  - $\log 1000n << n^{0.001}$ for sufficiently large n
- Linear << Quadratic
  - $1000n << 0.0001n^2$ for sufficiently large n
- Polynomial << Exponential
  - $n^{1000} << 2^{0.001n}$ for sufficiently large n

- Example: Find the complexity class of the function $(nn!+3^{n+2}+3n^{100})(n^n+n2^n)$
- Solution:
  - This means to simplify the expression. Throw out stuff which you know doesn't grow as fast.
  - Use the property that if f is O(g) then f+g is O(g)
  - (i) For $nn!+3^{n+2}+3n^{100}$, eliminate 3^{n+2} and $3n^{100}$ since n! grows faster than both of them
  - (ii) Now simplify $n^n + n2^n$, which grows faster? Take the log (base 2) of both (since the log is an increasing function whatever conclusion we draw about the logs will also apply to the original functions)
  - Compare nlogn and logn+n, nlogn grows faster so we keep n^n.
  - The complexity class is $O(nn!\, n^n)$

Big-Omega

- Assume f:Z→R and g: Z→R.
- f(x) is Ω(g(x)) iff ∃ positive constants C and k such that

$$\forall x>k \ |f(x)| \geq C|g(x)|$$

- Big-O vs Big-Omega :
  - Big-O provides upper bound for functions
  - Big-Omega provides lower bound for functions

Big-Theta

- Assume f:Z→R and g: Z→R.
  f(x) is Θ(g(x)) iff f(x)=O(g(x)) and f(x)=Ω(g(x))

- Big-Theta Θ provides both upper and lower bounds for functions