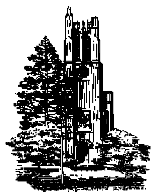
Wednesday June 1, 2016
Lecture 10

Functions



309

Notables

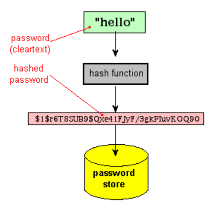
- Homework#6
  - Page 152, Problems 2, 6
  - Page 153, Problems 8, 20, and 22
  - Due Thursday June 2, 2016
- Tentative Schedule for the week

Week	M	T	W	R	Topic	Section
1						
		5-31			functions	2.3
			6-1		Sequences and summations	2.4
				6-2	Cardinality of sets	2.5

310

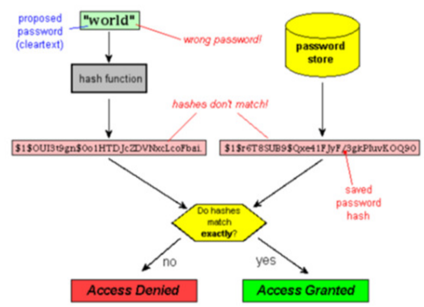
Hashing for Hiding Information

- Here, the hash function maps a string to another string with the property of being very difficult to reverse the result of the hash.
- Used in hiding user's password



311

How password is checked.



312

Hashing for file signature

- The hash function maps a large string (e.g., a file) to a fixed size string called *digest*
- Examples:
  - MD5 (Message-Digest algorithm 5), gives a 128-bit hash (digest)
  - SHA-1 (Secure Hash Algorithm) is a most commonly used from SHA series of cryptographic hash functions, designed by the National Security Agency
  - SHA-1 produces the 160-bit hash value. Original SHA (or SHA-0) also produce 160-bit hash value, but SHA-0 has been withdrawn by the NSA shortly after publication and was superseded by the revised version commonly referred to as SHA-1. The other functions of SHA series produce 224-, 256-, 384- and 512-bit hash values.

313

Hashing for file signature

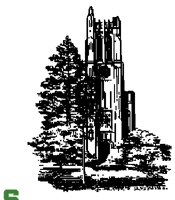
- The hash function maps a large string (e.g., a file) to a fixed size string called *digest*
- Examples:
  - MD5 (Message-Digest algorithm 5), gives a 128-bit hash (digest)
  - SHA-1 (Secure Hash Algorithm) is a most commonly used from SHA series of cryptographic hash functions, designed by the National Security Agency
  - SHA-1 produces the 160-bit hash value. Original SHA (or SHA-0) also produce 160-bit hash value, but SHA-0 has been withdrawn by the NSA shortly after publication and was superseded by the revised version commonly referred to as SHA-1. The other functions of SHA series produce 224-, 256-, 384- and 512-bit hash values.

314

MD5

- You can use this site:
  - http://www.miraclesalad.com/webtools/md5.php
- You can use Python
  - >>> from hashlib import md5
  - >>> m = md5()
  - >>> m.update(b“CSE 260”)
  - >>> h =m.hexdigest()
  - >>> h
  - 'c41f864302a3224f7a05d33f21f09e85'
  - >>> "{0:8b}".format(int(h,16))
  - '110001000001111110000110010000110000001010100011001000100100111101111010000001011101001100111111001000011111000010011110100 00101'

Sequences and Summations



Outline

- Sequences
- Special Integer Sequences
- Summations
- Cardinality: countable, uncountable infinite sets

Sequences

- Definition: A *sequence* is a function from a subset of N ={0, 1, 2, …}, the set of natural numbers, to a set S.
- Notation:
  - a_n, is called a *term* of the sequence and denotes the image of the integer n.
  - $\{a_n\}$ denotes the sequence.
    - Do not confuse the above notation with the set notation. This is a “misuse” of the set notation.

Example

Consider sequence $\{a_n\}$, where $a_n = \frac{1}{n}$.

Few terms are: $a_1 = 1,\ a_2 = \frac{1}{2},\ a_3 = \frac{1}{3},\ a_4 = \frac{1}{4}, \cdots$

Example

Consider the sequence $\{C_n\}$, where

$$C_n = \frac{(2n)!}{n! \times (n+1)!} \qquad n \ge 1$$

Find terms: $C_1, C_2, C_3, C_4, \ldots, C_{10}, \ldots$

Known as the Catalan numbers

Example

Consider the sequence $\{f_n\}$, where

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Find terms: $f_0, f_1, f_2, f_3, f_4, f_5, f_6, \ldots$

321

Geometric Progression

- A *geometric progression* is a sequence of the form:

  $a, ar, ar^2, \ldots, ar^n$

  where the *initial term*, a, and *common ratio*, r, are real numbers.

  - A geometric progression is a discrete analogous of the *exponential function* $f(x) = ar^x$.

322

Examples

- The sequence $\{b_n\}$, where $b_n = (-1)^n$ for $n = 1, 2, 3\ldots$ starts with: -1, 1, -1, 1, …
- The sequence $\{c_n\}$, where $c_n = 2^n$ for $n = 1, 2, 3\ldots$ starts with: 2, 4, 8, 16, …
- The sequence $\{d_n\}$, where $d_n = 6\cdot(1/3)^n$ for $n = 1, 2, 3\ldots$ starts with: 2, 2/3, 2/9, 2/27, …

323

Arithmetic Progression

- An arithmetic progression is a sequence of the form

  $a, a+d, a+2d, \ldots, a+nd$

  where the *initial term*, a, and the *common difference*, d, are real numbers.

  - A arithmetic progression is a discrete analogous of the *linear function* $f(x) = dx + a$.

324

Examples

- The sequence $\{s_n\}$, where $s_n = -1 + 4n$ for $n = 1,2,3\ldots$ starts with: 3, 7, 11, …
- The sequence $\{t_n\}$, where $t_n = 7 - 3n$ for $n = 1, 2, 3\ldots$ starts with: 4, 1, -2, …

325

Strings

- *Strings* are sequences of the form $a_1a_2\ldots a_n$
  - The *length* of the string is the number of its terms
  - The *empty string* is the string that has no terms

326

Special Integer Sequences

- How can we find the rule/formula for the sequence when we are given a few of its initial terms?

327

Special Integer Sequences

- To deduce a possible formula/rule for the terms of a sequence from initial terms, ask the following:
  - Are there runs of the same value?
  - Are terms obtained from previous terms by adding the same amount or an amount that depends on the position in the sequence?
  - Are terms obtained from previous terms by multiplying by a particular amount?
  - Are terms obtained by combining previous terms in a certain way?
  - Are there cycles among the terms?

328

Example

- Consider the sequence
  5, 11, 17, 23, 29, 35, 41, 47, 53, 59…
  Describe $\{a_n\}$
- $\{a_n\} = 5 + 6n \qquad n = 0, 1, 2, \ldots$

329

Examples

- Consider the sequence
  1, 7, 25, 79, 241, 727, 2185, 6559, 19681,
  Describe $\{a_n\}$
- Answer:
  - $A_n = 3^n - 2, \qquad n = 0, 1, 2, \ldots$

330

Examples

- Consider the sequence
  1, 2, 2, 3, 3, 3, 4, 4, 4, 4…

  Describe $\{a_n\}$

$$a_n = \left\lfloor \sqrt{2n} + \frac{1}{2} \right\rfloor, \qquad n = 1, 2, 3, \ldots$$

$$a_n = \left\lfloor \frac{1 + \sqrt{1 + 8n}}{2} \right\rfloor, \qquad n = 0, 1, 2, 3, \ldots.$$

331

Useful Sequences

nth Term	*First 10 Terms*
n^2	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, …
n^3	1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, …
n^4	1, 16, 81,256,625,1296,2401,4096,6561,10000,…
2^n	2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, …
$n!$	1,2,6,24,120,720,5040,40320,362880,3628800,…

332

Summation

- Consider the following expression:
  - $S = 3 + 5 + 7 + 9 + 11 + 13 + 15 + \ldots + 35$
  - $S = (2\times1 + 1) + (2\times2 + 1) + (2\times3 + 1) + \ldots + (2\times17 + 1)$
  - Terms of an arithmetic progression
- A more compact way of expressing S is to use the *summation notation*:

$$s = \sum_{i=1}^{17} (2i+1)$$

333

Summations

- Consider the sequence $\{a_n\}$.
  We define the following *summation*:

$$\sum_{j=m}^{n} a_j = a_m + a_{m+1} + a_{m+2} + \cdots + a_n$$

- Terminology:
  j is called the *index of summation*, always an integer
  m is the *lower limit*, always an integer
  n is the *upper limit*, always an integer.

334

Summations…

Note that the following are all the same:

$$\sum_{j=m}^{n} a_j = \sum_{i=m}^{n} a_i = \sum_{k=m}^{n} a_k = \sum_{m\le j\le n} a_j$$

335

Summations…

Do not be tempted to write, for example,

$$\sum_{k=2}^{n-1} k(k-1)(n-k)$$

instead of

$$\sum_{k=0}^{n} k(k-1)(n-k)$$

becasue the terms $k = 0$, 1 and n in this summation are zero.

Convention: If the summand is undefined, assume it is zero.

336

Summations…

Write out all the terms of the following summation:

$$\sum_{0\le k^2\le 5} a_{k^2} =$$

337

Summations…

Write out all the terms of the following summation:

$$\sum_{0\le k^2\le 5} a_{k^2} =$$

Solution 1:

$$\sum_{0\le k^2\le 5} a_{k^2} = a_0 + a_1 + a_2 + a_3 + a_4 + a_5$$

Solution 2:

$$\sum_{0\le k^2\le 5} a_{k^2} = a_4 + a_1 + a_0 + a_1 + a_4$$

with the assumption that $k \in \{-2, -1, 0, 1, 2\}$

338