Algorithms & Complexity 3/24/17- 3/29/17

0145-344-001

Note Taker: Jai Punjwani

ANNOUNCEMENTS

Topic: Random Numbers

PowerPoint: <http://home.adelphi.edu/~siegfried/cs344/344l8.pdf>

* Random numbers are very hard to get. Computers, for the most part, produce pseudorandom numbers, as there is some predictability or some factor in the algorithm that influences the output. Pseudorandom sequences of numbers eventually repeat themselves. True randomness is unpredictable, due entirely to chance.
* Random numbers are used for many useful things:  
    
  **Simulating Natural phenomena  
  Sample a data set  
  Decision Making – i.e. choose an arbitrary move in a game  
  Cryptographic Algorithms**

**Random Number Cycle**

* shows us that pseudorandom numbers have a finite set of integers; the sequence gets traversed in a particular order; the sequence will repeat if the period of the generator is exceeded

**Pseudorandom numbers aim to meet two conditions:**

1. Any two distinct numbers APPEAR to have the same probability
2. the numbers are INDEPENDENT

Condition 2 is never met – there is a dependence on what numbers previously occur, thus making the numbers pseudorandom.

**Von Neumann’s Method**

* A flawed method of squaring a number and clipping out the middle (i.e. 12342 = 01522757, which becomes 5227 after clipping out the middle). The issue is that about 50 numbers later, we see repetition and we know that the sequence is not random.

**Lehmer’s Method (aka Linear Congruential Method)**

* method to generate next random number using 3 constants.  
  xn+1 = (axn + c) mod m
* a is the multiplier; m is the modulus; c is the increment
* **the values we choose for *m* and *a* are critical.** if m is small, we will have a small cycle length and thus a lot of repetition. Additionally, c and m must be relatively prime, meaning that they don’t have any common factors aside from 1.
* the random number from the previous iteration is used as the seed for the next. To vary the algorithm more,