Random Number Generation

11-6-2002

Opening Discussion

- What did we talk about last class?
- Opening a file for writing creates that file in your directory. We’ll look at that today.
- stdin and stdout.
- What do we mean when we talk about random numbers on a computer? What does it mean for a number to be random?

File Code From Last Class

- Let’s now go to the code for files that we started last time. It was a simple line editor that we wanted to have the ability to read from a file or write to a file.
Random Numbers on Deterministic Machines

- You have already seen a use of the rand() function if you did the encrypt program. In reality that gives you a sequence of pseudo-random numbers.
- Computers are deterministic, given the same initial conditions and instructions you get identical behavior. As such, nothing is truly random on a computer. Instead we make a sequence where elements don’t seem closely related.

The Method

- The rand() function uses what is called a linear congruential uniform generator. This uses a simple formula to get a sequence of numbers that can have a long periodicity.
  \[ x_{n+1} = (a \times x_n + c) \mod m \]
- Sequence depends on \(a\), \(c\), \(m\), and \(x_0\). The last one is the “seed”.

The Details

- \(m\) is generally chosen to be a power of 2 to make the math faster because the modulo operator can be done by preserving the lower bits.
- The period for that sequence can be \(m\) iff, \(c\) is relatively prime to \(m\), \(a \mod p = 1\) for every prime factor \(p\) of \(m\), and \(a \mod 4 = 1\) if \(m\) is divisible by 4.
**Code**

- First let’s work through an example of this method on the board. Then we can write some code to implement a slightly larger random number generator and look at the rand and srand functions in stdlib.h.

**Minute Essay**

- Coding during class. One of the mid-semester questionnaires suggested that I come to class with completed code to show you. I don’t generally do this for 3 reasons. I write slower than I describe so it allows you to keep up. It allows you to see the construction process because you have to do that. When bugs occur you see how I look for them which you need to be able to do. What are your thoughts? Would you rather start with completed code or watch me write it?
- Quiz #5 next class.