Pseudorandom Number Generators in a Four-Bit Computer System

James C. Reber, Indiana University of Pennsylvania, Indiana, PA

Pseudorandom number generators can be introduced easily in the context of a four-bit computer system that allows students to explore and understand their properties. At the university we do this in a freshman-level mathematics course required of computer science majors that introduces logic, numeration, matrices, combinatorics, probability, and series. After considering arithmetic in bases 2, 8, 10, and 16 (including subtraction by complements), we introduce a simple four-bit computer system, show it behaves "just like" arithmetic modulo 16, and introduce pseudo-random number generators modulo 16.

First, we consider a four-bit computer system that uses binary representation for positive integers, and two's complements for negative integers. Here are the possible numbers with the corresponding decimal numbers they represent:

0000 : 0	0100 : 4	1000 : −8	1100 : −4
0001 : 1	0101 : 5	1001 : −7	1101 : −3
0010 : 2	0110 : 6	1010 : −6	1110 : −2
0011 : 3	0111 : 7	1011 : −5	1111 : −1

Next, we introduce equivalence classes of integers modulo 16 and arithmetic modulo 16. Students can convince themselves that addition modulo 16, with 0 to 15 as the representative elements for the equivalence classes, is "just like" addition in the four-bit computer system. We also discuss briefly the idea of isomorphism and its uses.

Then, we introduce some examples of pseudorandom number generators for the integers modulo 16. Start by letting L_0 be any number (called the "seed") between 0 and 15, and set

$$L_i = 5L_{i-1} + 3 \pmod{16}.$$

The seed $L_0 = 1$ generates:

$$8, 11, 10, 5, 12, 15, 14, 9, 0, 3, 2, 13, 4, 7, 6, 1, 8, \ldots,$$

which looks like a random ordering of the numbers (mod 16). Of course, it repeats once the seed is generated.

Students are then asked to explore several other examples. In each case, they choose a "seed" and determine L_i for $i = 1$ to 16. Would any of these be "suitable" pseudorandom generators mod 16?

(a) $L_i = 2L_{i-1} + 5 \pmod{16}$
(b) $L_i = 3L_{i-1} + 1 \pmod{16}$
(c) $L_i = 7L_{i-1} + 5 \pmod{16}$
(d) $L_i = 15L_{i-1} + 4 \pmod{16}$
(e) $L_i = 9L_{i-1} + 3 \pmod{16}$

In case (a), once 11 is generated, it is repeated indefinitely. The lengths of non-repeating sequences in cases (b), (c), and (d) are 8, 4, and 2, respectively. Case (e) is a "suitable" pseudorandom number generator.

Finally, students can explore the linear congruential pseudorandom number generator

$$L_i = aL_{i-1} + b \pmod{16}$$

for arbitrary a and b. A special case of Theorem 1 in S. J. Yakowitz's *Computational Probability and Simulation* [Addison-Wesley, 1977] shows that all 16 different numbers will be generated if and only if b is relatively prime to 16, and $a-1$ is a multiple of 4. With some guidance, students can discover this, as well as the fact that one number is repeated indefinitely in the sequence when $a-1$ is odd.

These student explorations can be used as the basis for discussing the "suitability" of pseudorandom number generators in real computers. In order for

$$L_i = aL_{i-1} + b \pmod{K}$$

to be "suitable," choose a and b so that K different numbers are generated. We would want the numbers in the sequence to be "uniformly distributed." For example, the number of the first n elements in the sequence less than or equal to n should approximate n/K. Moreover, the numbers in the sequence should be "independent." For example, the number of "runs up" should be comparable to a theoretical distribution. Students who explore pseudorandom number generators modulo 16 should be able to more easily understand the related ideas in later courses.

———o———

Conditional Expectations and the Correlation Function

Barthel W. Huff, Randolph-Macon College, Ashland, VA

If the random variables X and Y have joint density

$$f_{X,Y}(x, y) = x + y \quad \text{for } 0 \le x \le 1 \text{ and } 0 \le y \le 1,$$

then it is easily computed that

$$\rho(X, Y) = \frac{\operatorname{Cov}(X, Y)}{\sqrt{\operatorname{Var}(X) \cdot \operatorname{Var}(Y)}}$$

$$= \frac{E(XY) - E(X) \cdot E(Y)}{\sqrt{\operatorname{Var}(X) \cdot \operatorname{Var}(Y)}} = -\frac{1}{11}.$$

This appears as Example 22 on p. 156 of Mood, Graybill, and Boes' *Introduction to the Theory of Statistics*, 3rd edition, McGraw-Hill, 1974, where the authors conclude by asking if a negative correlation seems "right." In Example 24 on p. 158 of that volume, it is calculated that

$$E(Y|X = x) = \frac{3x + 2}{6x + 3} \quad \text{for } 0 \le x \le 1,$$

but there is no indication that this might be related to the earlier question. Since

$$\frac{d}{dx}E(Y|X = x) = \frac{d}{dx}\left(\frac{3x + 2}{6x + 3}\right) = \frac{-3}{(6x + 3)^2} < 0,$$

the conditional expectation is a decreasing function of x, and the observer might conclude that Y is expected to give smaller values as the value of X increases; that is, conclude that X and Y are tending in opposite directions and therefore should have a negative correlation.

In view of the above, we prove the following.