Teaching Labs on Pseudorandom Number Generation

Elizabeth Patitsas
University of Toronto
40 St George St.
Toronto ON M5S 2E4
patitsas@cs.toronto.edu

ABSTRACT

This presentation describes our approach to teaching pseudorandom number generation (PRNG) in CS labs. We use PRNG at two universities as an example of an application of sequential circuitry in our digital logic courses. Our goal is for our students to have meaningful assignments, and to relate digital logic not only to the larger CS curriculum, but to the students' lives. This also us a motivation to discuss "what is randomness?", security issues relating to seeding and encryption, and why and how we use randomness in computing.

Categories and Subject Descriptors

K.3.2 [**Computers and Information Science Education**]: Pedagogy, education research

General Terms

Design

Keywords

Digital logic, labs, computer science education

1. THE PRESENTATION

This "Tips, Techniques, and Courseware" session presents two lab activities aimed at teaching pseudorandom number generation (PRNG). Our goal in this presentation is to give CS educators a compelling example for students to practice with when learning sequential circuitry in a digital logic or hardware course. We believe this will be interesting to the ITiCSE community as it provides a new example for teaching sequential circuitry which can be related to "big picture" CS topics such as stochastic algorithms, cryptography, and computer security.

1.1 The Lab Activities

We will be presenting two lab activities on PRNG, a first-year lab from the University of British Columbia, and a second-year lab from the University of Toronto. The former is freely available under a Creative Commons License [1]. Both activities have students build PRNG circuits in courses which cover digital logic. In both cases, the activities provide a new example for teaching sequential circuitry. Learning how to design sequential circuits is analogous to learning to write recursive programs; the design approach is different from the combinational circuitry that we begin by teaching them.

In both labs, students implement linear shift feedback registers (LFSRs). These circuits have the advantage of being simple, yet the results are interesting to the students. For the students, the activity of building an LFSR is rated as being fun, interesting, and rewarding. They see it as a real-world problem that engages them. Previously, when teaching sequential circuitry, we opted to use "toy problems". This new activity has grounded this portion of the course by presenting a real world problem.

1.2 Benefits of teaching PRNG

We have found a number of benefits of teaching PRNG beyond how its grounds digital logic for the students:

1. Learning PRNG gives the students experience with the concept of seeding. Not only does this give them more familiarity with sequential circuitry, but it also teaches them the need to seed a PRNG properly. TAs in courses downstream of ours have reported that students who complete this lab activity now properly seed their C++ code when dealing with random algorithms.
2. The discussion of seeding bridges into a discussion of security. We also take this activity as an opportunity to teach students about cryptography, particularly one-time pads and stream ciphers.
3. It allows us to engage students in the discussion of "what is randomness?"
4. When students ask what random numbers are used for in CS, it allows a discussion of how randomness is used in the field. This also gives us an opportunity to bridge hardware-level topics with the CS theory students are learning concurrently.

2. ACKNOWLEDGMENTS

For feedback in lab development: Meghan Allen, Patrice Belleville, Steve Engels, Simon Hastings, Vanessa Kroeker, Kimberly Voll, Steve Wolfman, Bob Woodham, and the TAs of the two courses. For the author's supervision and funding: Steve Easterbrook.

[1] Available at `http://www.ugrad.cs.ubc.ca/~cs121/2011W2/Homepage/labs.html`

ITiCSE'12, July 3–5, 2012, Haifa, Israel.