RANDOM NUMBER GENERATOR

DEEP DIWANI(EE16B06) S.KHALID BASHA(EE16B35)

EE5811: FPGA LAB and EE3025: IDP

Department of Electrical Engineering

IIT HYDERABAD

April 26, 2019

Outline

1. First Section
   - Project Outline
   - Software Setup
   - Linear Feedback Shift Register
2. Second Section
   - Implementation of RAND in RTL
   - Hardware Implementation

Outline

1. First Section
   - Project Outline
   - Software Setup
   - Linear Feedback Shift Register

2. Second Section
   - Implementation of RAND in RTL
   - Hardware Implementation

Project Outline

- Our aim is to generate random numbers using Icoboard FPGA.
- We have used LFSR algorithm to generate random numbers.
- Input seed is given to mega aurdino which is connected to Icoboard whose output is being displayed on LCD.
- Random number being generated is displayed on the LCD.
- Statistical test has been performed to check the trueness of the random numbers generated.

- All the verilog and arduino codes, the presentation are accessible on the github interface which is a free open-source.

Outline

1. First Section
   - Project Outline
   - Software Setup
   - Linear Feedback Shift Register
2. Second Section
   - Implementation of RAND in RTL
   - Hardware Implementation

Software Setup

- **LINK for commands:** https://github.com/gadepall/EE5811/blob/master/icoboard_fpga/gvv_hemanth_icoboard.pdf
- Execute the following commands in your terminal for installing softwares:

- Wiring Pi
- Ico Prog
- Icestorm
- Arachne-pnr
- Yosys

- Creating **Makefile [1]**

Outline

1. First Section
    - Project Outline
    - Software Setup
    - Linear Feedback Shift Register

2. Second Section
    - Implementation of RAND in RTL
    - Hardware Implementation

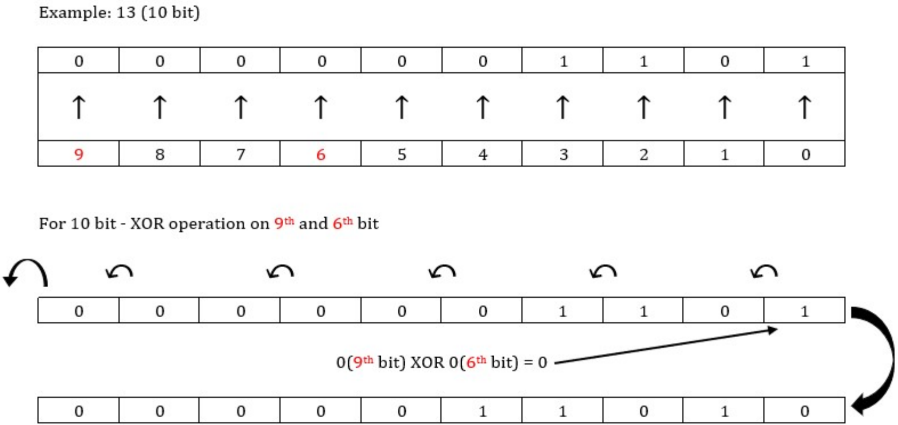
Linear Feedback Shift Register

- LFSR Random Number Generators are a class of Pseudo Number Generators.
- A Linear Feedback Shift Register is a shift register whose input bit is a linear function of previous state. The most commonly used linear function of single bits is exclusive-or (XOR)
- An N-bit LFSR will be able to generate $(2^N - 1)$ random numbers before it starts repeating.

Algorithm of LFSR

- Seed - Input
- For example: Seed = 13(10 bit)
- XOR operation on 9^{th} and 6^{th} bit
- Left Shift

Algorithm of LFSR



Example: 13 (10 bit)

0	0	0	0	0	0	1	1	0	1
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
9	8	7	6	5	4	3	2	1	0

For 10 bit - XOR operation on 9th and 6th bit

0	0	0	0	0	0	1	1	0	1

0(9th bit) XOR 0(6th bit) = 0

0	0	0	0	0	1	1	0	1	0

Figure: LFSR Algorithm

Outline

1. First Section
   - Project Outline
   - Software Setup
   - Linear Feedback Shift Register

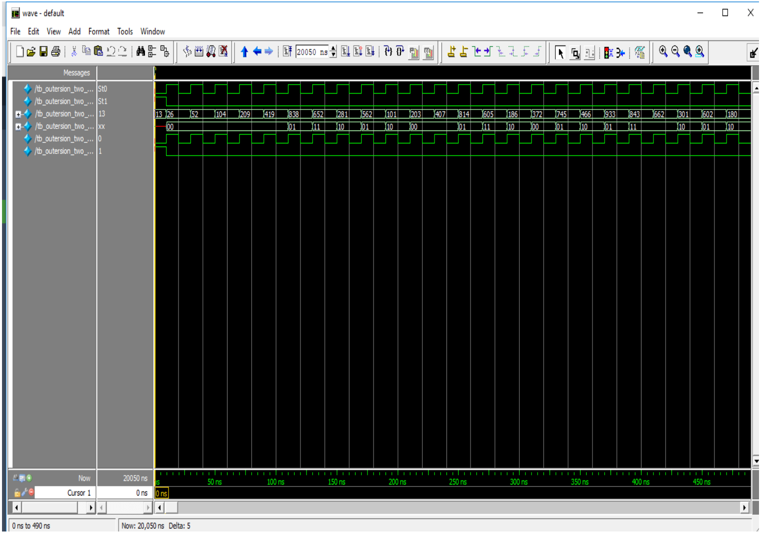
2. Second Section
   - Implementation of RAND in RTL
   - Hardware Implementation

Implementation of RAND in RTL

- Verilog code for generating sequence of Random numbers using LFSR algorithm:
  https://github.com/Md-Khalid-1129/FPGA_submissions

- Arduino code and Verrilog-pcf file are also available on github link.

Contd...



wave - default

File Edit View Add Format Tools Window

Messages	
/tb_outersion_two_...	St0
/tb_outersion_two_...	St1
/tb_outersion_two_...	13
/tb_outersion_two_...	xx
/tb_outersion_two_...	0
/tb_outersion_two_...	1
Now	20050 ns
Cursor 1	0 ns

0 ns to 490 ns

Now: 20,050 ns Delta: 5

Figure: RTL Simulation Results

Outline

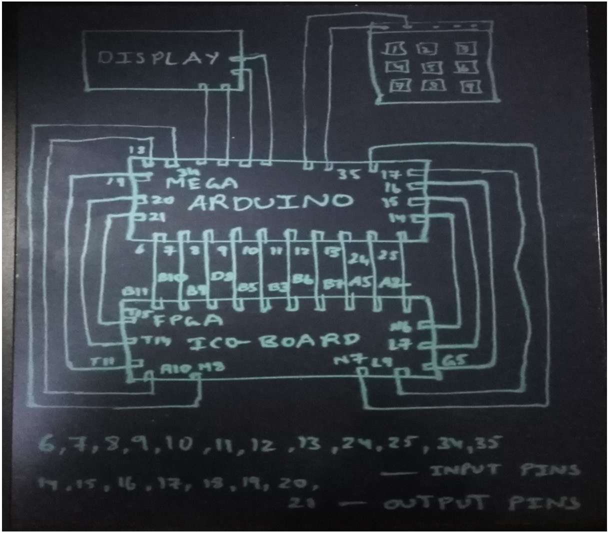
1. First Section
   - Project Outline
   - Software Setup
   - Linear Feedback Shift Register

2. Second Section
   - Implementation of RAND in RTL
   - Hardware Implementation

Components Required

- Mega-Arduino
- Raspberry Pi
- Ico-Board
- Keypad
- LCD
- Potentiometer

Connections



6,7,8,9,10,11,12,13,24,25,34,35
— INPUT PINS
14,15,16,17,18,19,20,
21 — OUTPUT PINS

Figure: Connections

Contd...

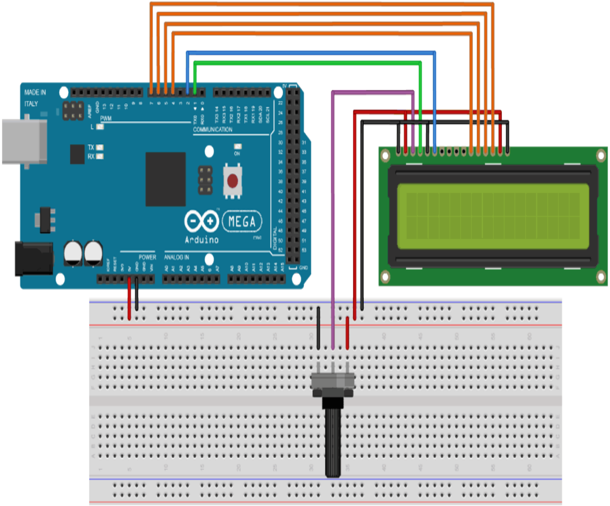


Figure: Connections of Mega-arduino and LCD

contd...

- Upload the code in the arduino
- Now, after all the connections are done open the terminal
- Run the verilog code by typing the following command

```
make v_fname=fileName
```

References I

- Github Link https://github.com/Md-Khalid-1129/FPGA_submissions
- https://vlsicoding.blogspot.com/2014/07/verilog-code-for-4-bit-linear-feedback-shift-register.html
- http://verilog-code.blogspot.com/2013/10/linear-feed-back-shift-registers-using.html