The Shortest Register with Non-linear Update for Generating a Given Finite or Periodic Sequence: [Experimental Results]

Shailendra Kumar Tripathi[1], Bhupendra Gupta[1], and K. K. Soundra Pandian[2]

1 email-shailendratripathi26@gmail.com, gupta.bhupendra@gmail.com

2 Soundra.pandian@cca.gov.in

1 **Department of Natural Science – Mathematics PDPM Indian Institute of Information and Technology, Jabalpur , India-482005,**

2 **Department of CCA – Ministry of Electronics and Information Technology, New Delhi, India 110003**

The experimental results are given to validate the analytical analysis of the expected circuit-size. For this, we have randomly generated periodic binary sequences for period up to 10^3, and 2^5 for the degree of parallelization p = 100, and 1 respectively. Then, we applied the proposed RNLU and algorithm [5] for this randomly generated binary periodic sequences.

For both the algorithms, the Register Transfer Level (RTL) codes for the feedback and feedforward functions are synthesized using Synopsys Design Compiler. The Semi-Conductor Library (SCL) i.e., tsl18fs120_scl_ss 180nm by specifying the cell invd0 to drive the circuit, is used for technology mapping. In this synopsis design compiler, the clock is specified with period 10ns for a frequency 100MHZ with rising and falling edges to occur at 0 and 5ns respectively. Then, the area is computed for the circuits of feedback and feedforward functions in μm^2. The area for p = 100 and 1 is shown in Fig. 1 and Fig. 2, respectively.

In Fig. 1, the degree of parallelization is 100 and the area is computed for an average of 20 randomly generated binary periodic sequences for period up to 10^3. In Fig. 1, for n = 3 (period $N = 3\times10^2$), and n = 7 (period $N = 7\times 10^2$), area is equal for proposed RNLU and algorithm [5] as same FSR (LFSR with same primitive polynomial) is used to generate the unique states, while for rest of the sequence lengths the area grows exponentially than proposed RNLU because the number of variables increases in the support set of functions. For period N = 9 x 10^2 and 10 x 10^2, the number of variables in the support set of updating functions do not

change in proposed algorithm that results small difference in area, and same as in algorithm [5] .

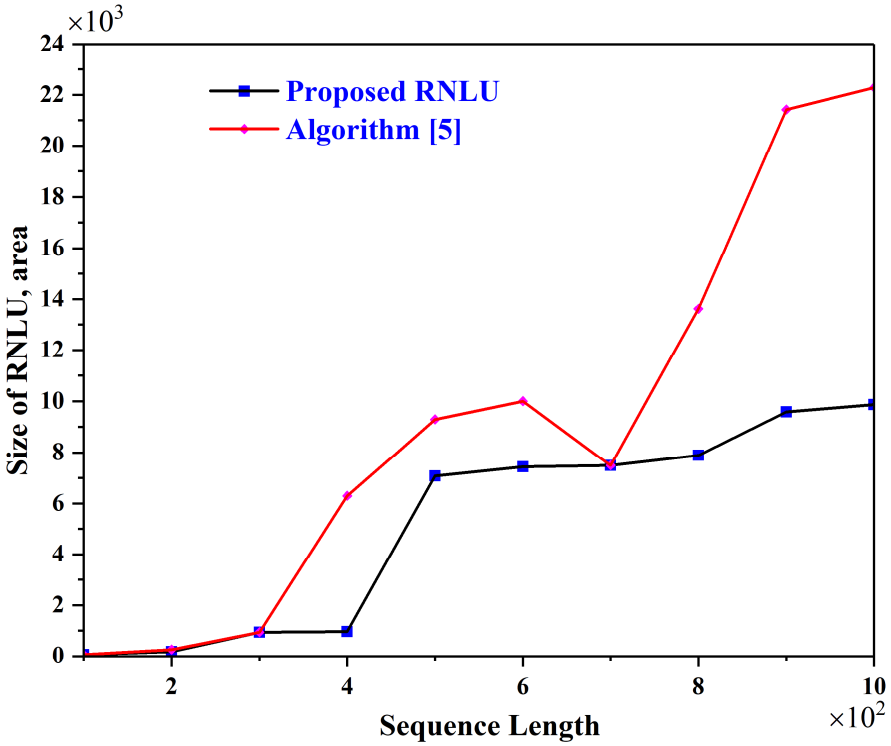

Fig. 1: Proposed RNLU and Algorithm [5] for p = 100

In Fig. 2, the area is computed for degree of parallelization p = 1 for period up to 2^5. The area is computed for 20 randomly generated binary periodic sequences for the period $N \geq 2^3$. As we can see that for period 2^3 the proposed algorithm requires 3-stage NLFSR and algorithm [5] requires 5-stage LFSR. Thus, there is no huge difference in the area. For the period 2^4 and 2^5, the proposed algorithm requires 4 and 5-stage NLFSRs, and the algorithm [5] requires 9 and 17-stage LFSRs. It is to be noted that area for algorithm [5] grows exponentially than proposed RNLU. As the sequence length increases, the rate of area for p = 1 is much larger than that for p = 100. Since, the proposed RNLU minimizes the number of variables in the support set of updating functions that minimized the overall expected circuit-size (as incorporated in section IV: Expected circuit-size analysis that proposed algorithm constructed for RNLU is asymptotically exponentially smaller than algorithm [5] for both p = 1 and 100).

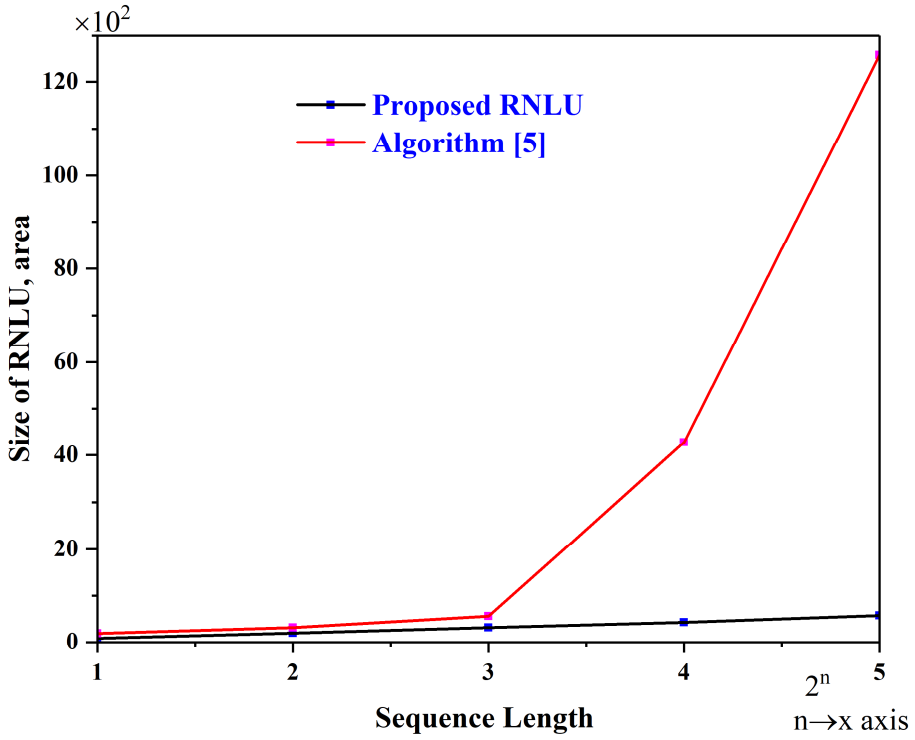

Fig. 2: Proposed RNLU and Algorithm [5] for p = 1.

[5] L. Nan, and E. Dubrova, "An algorithm for constructing a minimal register with non-linear update generating a given sequence," IEEE 44th International Symposium on Multiple-Valued Logic, May 19 2014, pp. 254-259.