Fuzzy Cellular Automata in the Generation Pseudorandom Numbers

CSI4900 Project Proposal

Youssef Makboul (8609614)

January 22, 2021

Objective

The main goal is to gather insight on achieving randomness with Fuzzy Cellular Automata(FCA).

We plan to investigate the role of parameters such as the type(ie. Moore, Von Neumann) as well as size of the neighborhood in the randomness(aperiodicity) of the FCA. Also, we can potentially evaluate whether the direction of gathering of the output to be used as a random number (eg. space$\rightarrow$ vs time$\downarrow$) can affect randomness.

Then, we attempt to gather insight on the generation of pseudorandom numbers using Fuzzy Cellular Automata.

This includes:

- **Implementation Feasibility**: details of implementation, potential drawbacks, robustness.
- **Algorithmic Complexity**: efficiency, optimizations, performance bottlenecks.
- **Quality of Randomness**: performance in Diehard tests, comparison with existing pseudo-number generators.

Rough Approach

1. Implement Boolean Cellular Automata for both Von Neumman and Moore neighborhoods.
2. Implement and Apply Fuzzification Algorithm [1].
3. Implement Radial Representation
4. Study and hunt for Class 3 [2] equivalent FCAs, if not found return to step 1 while changing neighborhood type/size

5. Extract outputs and perform randomness study.
    i. Define and Evaluate output to be used as Random Number (ie. the equivalent of the centre columns in the Rule 30 generator [3])
    ii. Extract statistically significant output (ie. number of iterations, number of generations per rule)
6. Evaluate Quality of Random Numbers using a testing suite such as Diehard Tests

Projected Timeline

Milestone	Target Completion Date
Information Gathering and Planning	January 18th ~ January 22nd
FCA and Radial Representation Development	February 15th ~ February 19th
Output Study and Experimentation	March 8th ~ March 12th
Randomness Quality Analysis	March 29th ~ April 2nd
Report Completion and Presentation Preparation	April 26th (Due Date)

References

1. H. Betel, P. Flocchini. On the relationship between fuzzy and Boolean cellular automata, Theoretical Computer Science, 412(8-10): 703-713, 2011. [Web Link]
2. P. Flocchini, V. Cezar. Radial View of Continuous Cellular Automata, Fundamenta Informaticae XXI 1001–1018: 703-713, 2001. [Web Link]
3. Lex Fridman (2018-03-02), MIT AGI: Computational Universe (Stephen Wolfram), retrieved 2021-01-15 [Web Link]