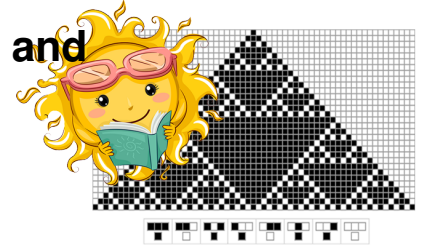


Reversibility in α -asynchronous Cellular Automata and Cryptography

Sourasish Das, Mainak Shaw, Aravind P
Mentor : Souvik Roy

August 24, 2022



Reversible computation has garnered a lot of attention over the years, though studied extensively in a great variety of synchronous computation models, it is virtually unexplored in an asynchronous framework. While discussing asynchronous frameworks, α -asynchronous cellular automata is a niche topic in the discussion of reversibility. α -Asynchronous cellular automata update their cells according to the value of α , since most of the updation process is based on probability, the experiments to be done to decide on the reversibility was done over a range of CA sizes. Further 88 rules were identified which depicted the characteristics of the 255 rules, and a sample of 10 probabilities were taken and experiments were conducted for all initial configurations for a given CA size and given value of α .

Definition 0.1. An elementary cellular automaton is a one-dimensional cellular automaton where there are two possible states (labeled 0 and 1) and the rule to determine the state of a cell in the next generation depends only on the current state of the cell and its two immediate neighbors.

Definition 0.2. A reversible cellular automaton is a cellular automaton in which every configuration has a unique predecessor.

Definition 0.3. An α -asynchronous cellular automaton is able to update individual cells independently, depending on the probability α

The set of 255 rules were reduced down to 88 characteristic rules, and a sample set of 10 probabilities were taken and for a range of CA sizes all initial configurations were checked for reversibility. While classifying rules each of the configurations were converted into their decimal representation and were plotted as a network of states and for the theoretical results a list of all the possible configurations for a given initial configuration and if the configuration list contains the initial configuration more than once then it can be declared as being reversible for that configuration, for a given α value and given CA size. **Probability Values :** 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9

Rules : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 18, 19, 22, 23, 24, 25, 26, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 40, 41, 42, 43, 44, 45, 46, 50, 51, 54, 56, 57, 58, 60, 72, 73, 74, 76, 77, 78, 90, 104, 105, 106, 108, 128, 129, 130, 131, 132, 133, 134, 136, 137, 138, 140, 142, 146, 150, 152, 154, 156, 160, 161, 162, 164, 168, 170, 172, 178, 184, 200, 204, 232

Sizes : 3, 4, 5, 6, 7, 8, 9, 10

For a given CA size, a given rule the classification is as follows:

Reversible:

- For all α values
- If all configurations are reversible then it is Reversible

Irreversible:

- For all α values
- If some configuration is irreversible then it is Irreversible

Partially Reversible:

- For some α values
- If all configurations are reversible then it is partially reversible

Now generalizing this classification over all values of α and CA sizes. The rules can be classified as:

Reversible:

- For all α values
- If all configurations are reversible then it is Reversible
- Example: 204

Irreversible:

- For all α values
- If all configurations are irreversible then it is irreversible
- Example: 0, 2, 4, 6, 8

Cell Size-Partially Reversible:

- For some α values
- If all configurations are reversible then it is Cell Size-Partially Reversible
- Example: 1, 3, 7, 9, 11

Cell Size-Reversible:

- For some CA sizes
- For all α values
- If all configurations are reversible then it is Cell Size-Reversible
- Example: 19, 27, 33

Table 1: Observations

Irreversible	0, 2, 4, 5, 6, 7, 8, 10, 12, 13, 14, 15, 18, 24, 26, 29, 32, 34, 36, 38, 40, 42, 44, 50, 72, 77, 78, 104, 106, 128, 130, 132, 133, 136, 138, 150, 152, 154, 160, 162, 168, 170, 178, 184, 232
Reversible	204
Cell Size-Reversible	19, 27, 33, 35, 37, 41, 43, 45, 51, 57, 105, 142
Cell Size-Partially-Reversible	1, 3, 7, 9, 11, 22, 23, 25, 28, 30, 46, 54, 58, 60, 73, 74, 76, 90, 10, 8, 129, 131, 134, 137, 140, 146, 156, 161, 164, 172, 200

All 88 rules that are representative of the 256 rules were classified and the only completely reversible rule is Rule Number 204. Other rules are dependent on the CA size and α values. The ratio of completely irreversible rules to reversible rules (partially, CA size reversible and completely reversible) are 1:1 as there are 43 rules that are reversible to an extent but the other 45 are completely irreversible. In conclusion except 1 rule (204) all other rules are either partially reversible / irreversible.