A Cellular Automaton for Factoring Integers

Bharathwaj Muthuswamy
Jonathan Ellithorpe

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2008-46
http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-46.html

May 3, 2008

A Cellular Automaton For Factoring Integers

Bharathwaj Muthuswamy, Jonathan D. Ellithorpe.

***Abstract*—In this report, we investigate the use of Cellular Automata for factoring integers, specifically the Fermat Numbers.**

***Index Terms*—Cellular Automata, Fermat Numbers, Factorization**

I. Introduction

Cellular Automata are models of computation proposed by John von Neumann [6]. Since then, Cellular Automata have been used in a variety of applications: modeling traffic [2], modeling chemical reactions [3] and cryptography [5]. In this report, we will investigate the use of a Cellular Automaton for factoring integers. Specifically, we will deal with a special class of numbers that have very interesting properties, the Fermat Numbers [4].

The organization of this report is: in the next section we will give a very brief introduction to Cellular Automata and Fermat Numbers. This is followed by Preliminary Results and then Future Work. The report concludes with an Acknowledgment and References section.

II. A Brief Introduction to Cellular Automata and Fermat Numbers

A. Cellular Automata

This discussion is based on Leon O. Chua's introduction to Cellular Automata from the perspective of nonlinear dynamics [1]. Fig. 1 shows that a Cellular Automata consists of L cells ($L = n + 1$ in Fig. 1) with periodic boundary conditions. The state of each cell is either a 0 or 1. Each cell i interacts with only its nearest neighbors $i-1$ and $i+1$. Table I shows how the state, x_i^n, of each cell at iteration n is updated based on the state of its nearest neighbors x_{i-1}^n and x_{i+1}^n. Here, $\beta_k \in \{0,1\}\ \forall k \in \{0,1,...,7\}$

TABLE I: Cellular Automaton Update Function

x_{i-1}^n	x_i^n	x_{i+1}^n	x_i^{n+1}
0	0	0	β_0
0	0	1	β_1
0	1	0	β_2
0	1	1	β_3
1	0	0	β_4
1	0	1	β_5
1	1	0	β_6
1	1	1	β_7

The cellular automaton rule that we are interested in is Rule 46. Table II shows the update function for Rule 46.

Bharathwaj Muthuswamy and Jonathan D. Ellithorpe are with the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, 94720 USA E-mail: {mbharat@cory.eecs.,jde@}berkeley.edu

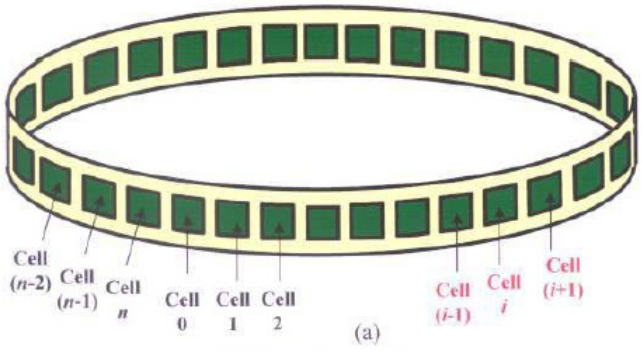

Fig. 1: Structure of a Cellular Automata

TABLE II: Rule 46 Update Function

x_{i-1}^n	x_i^n	x_{i+1}^n	x_i^{n+1}
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

B. Fermat Numbers

Fermat numbers are defined as numbers of the form $F_k = 2^{2^k} + 1$. These numbers find applications in signal processing [4] and cryptography [4]. Nevertheless, factoring Fermat numbers is a challenge and there exists no general algorithms for factoring these numbers [4].

III. Preliminary Work

Consider the evolution of a Cellular Automaton with $L = 6$ and initial condition 001001, shown in Fig. 2

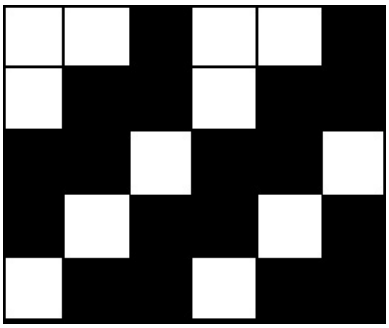

Fig. 2: Evolution of Rule 46 ($L = 6$) for a specific initial condition

TABLE III: Rule 46 Attractor List and Period(s) for a few bit lengths

L	Attractor(s)	Period(s)
7	$\{\{0\},\{3,6,12,24,48,96,65\}\}$, $\{27,54,108,89,51,102,77\}$	1,7
8	$\{\{0\},\{51,102,204,153\}$, $\{3,6,12,24,48,96,192,129\}$, $\{27,54,108,216,177,99,198,141\}\}$	1,4,8
12	$\{\{0\},\{1755,3510,2925\}$, $\{819,1638,3276,2457\}$, $\{195,390,780,1560,3120,2145\}$, $\{3,6,12,24,48,96,192,384,768,1536,3072,2049\}$, $\{27,54,108,216,432,864,1728,3456,2817,1539,3078,2061\}$, $\{51,102,204,408,816,1632,3264,2433,771,1542,3084,2073\}$, $\{99,198,396,792,1584,3168,2241,387,774,1548,3096,2097\}$, $\{219,438,876,1752,3504,2913,1731,3462,2829,1563,3126,2157\}$, $\{411,822,1644,3288,2481,867,1734,3468,2841,1587,3174,2253\}$, $\{435,870,1740,3480,2865,1635,3270,2445,795,1590,3180,2265\}$	1,3,4,6,12

Mathematica 5.1 was used to obtain all the results in this section. To obtain Fig. 2, we used the Mathematica command:

$$ArrayPlot[CellularAutomaton[46,\{0,0,1,0,0,1\},4]]$$

Fig. 2 is more informative if we view the evolution in the decimal number system:

$$\{\{9\},\{27,54,45,27\}\}$$

In our notation above, $\{27,54,45,27\}$ is called as the **attractor** and $\{9\}$ is the **basin of attraction**. The **period** of our attractor above is 3. Consider Table III. We list the bit length, the corresponding attractors and the periods for each attractor.

Based on our experimental work, here are three conjectures related to Rule 46:

Conjecture 1 *Given a Cellular Automaton of length L that is evolving under Rule 46, the attractor periods are:*

1) *1 and L if L is prime*
2) *1 and the factors of L (excluding 2) if L is composite*

Conjecture 2 *Given a Cellular Automaton of length L that is evolving under Rule 46, then **any** attractor **always** starts at x_{0A} such that $x_{0A} \equiv 0 \ (mod\ 3)$. In other words, x_{0A} is divisible by 3.*

Conjecture 3 *Given a Cellular Automaton of length L that is evolving under Rule 46, if L is **even**, then the attractor with period $\frac{L}{2}$ starts at the decimal number $(2^{\frac{L}{2}}+1)\cdot 3$.*

IV. Current Work

We are working on:

1) Trying to prove Conjectures 1 through 3 above. Approaches based on PDEs and Number theory are being considered.
2) Investigating the relationship between the properties of Rule 46 and Fermat Numbers.

Acknowledgment

Many thanks to Ian Tan and Carl Chun for advising me to write this report.

References

[1] L. O. Chua, S. Yoon, and R. Dogaru, "A nonlinear dynamics perspective of wolfram's new kind of science. part i: Threshold of complexity," *International Journal of Bifurcation and Chaos*, vol. 12, no. 12, pp. 2655 – 2766, 2002.

[2] J. Esser and M. Schreckenberg, "Microscopic simulation of urban traffic based on cellular automata," *International Journal of Modern Physics C*, vol. 8, no. 5, pp. 1025 – 1036, 1997.

[3] ——, "Microscopic simulation of urban traffic based on cellular automata," *International Journal of Modern Physics C*, vol. 8, no. 5, pp. 1025 – 1036, 1997.

[4] M. Krizek, F. Luca, and L. Somer, *17 Lectures on Fermat Numbers: From Number Theory to Geometry*. New York, USA: Springer-Verlag, 2002.

[5] M. Szaban, F. Seregynski, and P. Bouvry, "Evolving collective behavior of cellular automata for cryptography," *IEEE Melecon*, pp. 799 – 802, 2006.

[6] J. von Neumann, *The Theory of Self-reproducing Automata*. Illinois, USA: Univ. of Illinois Press, 1966.