

Autómatas Celulares Aditivos: la regla 150 vs. la regla 90

[Álvaro Álvarez Parrilla](#)¹ y [Aurora Espinoza Valdéz](#)²

¹Carrera de Matemáticas, Facultad de Ciencias,
Universidad Autónoma de Baja California
Ensenada, B.C.

E-mail: alvaro.uabc@gmail.com

²División de Matemáticas Aplicadas, IPICYT,
Tangamanga, San Luis Potosí, S.L.P.,

E-mail: aurora.espinoza@ipicyt.edu.mx

[Recibido: Marzo 25, 2008. Aceptado: Junio 30, 2008](#)

RESUMEN

En este trabajo se utiliza una metodología algebraica para estudiar la dinámica de los autómatas celulares unidimensionales con valores en el campo finito de dos elementos, con condiciones de frontera periódicas que, además, satisfacen una propiedad llamada **aditividad** (que es compartida solamente por las reglas 90 y 150).

Específicamente, se presentan resultados relativos a los ciclos límite para el caso de la regla 150, mismos que se comparan con los resultados ya reportados en la literatura sobre la regla 90.

Palabras Clave: Autómatas celulares aditivos, Regla 150.

ABSTRACT

In this paper an algebraic methodology is used to study the dynamics of unidimensional cellular automats with values within the finite field of two elements, with conditions of periodic limits that, besides, satisfy a property named **additivity** (shared only by rules 90 and 150).

Specifically, results related to limit cycles for rule 150 are presented and compared with results already reported in literature about rule 90.

Keywords: Additive cellular automats, Rule 150.

1. Introducción

Los autómatas celulares fueron introducidos a finales de los años 40 por J. von Neumann después de una sugerencia de S. Ulam. Esto fue con el objetivo de crear un modelo del comportamiento real de sistemas extensos y complejos.

Un autómata celular d -dimensional es un sistema discreto que consiste de una malla d -dimensional de celdas (el espacio subyacente es un subconjunto de Z^d). Cada celda es capaz de almacenar un elemento de un conjunto finito de estados S . La dinámica se da en términos de una función local f que especifica el estado siguiente de cada celda en función de los estados actuales en alguna vecindad local de la celda.

En otras palabras, un autómata celular unidimensional consiste en una sucesión o secuencia de sitios (una configuración o estado) donde cada sitio o celda contiene un valor numérico, y los valores de los sitios evolucionan en pasos de tiempo discretos según reglas determinísticas.

Los autómatas celulares son reversibles si su mapeo global es invertible, es decir, si cada configuración que por definición tiene exactamente un sucesor también tiene exactamente un predecesor.

En este trabajo se utiliza un formalismo apropiado para comenzar a estudiar la evolución de autómatas celulares unidimensionales sobre Z_2 y con condiciones de frontera periódicas.

2. Antecedentes matemáticos

En esta sección presentamos de manera breve los antecedentes que utilizaremos. Para mayores detalles consulte las referencias al final del documento, específicamente [1-3].

En el presente trabajo sólo se consideran autómatas celulares unidimensionales con valores en un anillo finito $Z_{\hat{k}}$ de \hat{k} elementos, con N sitios y con condiciones de frontera periódicas. Esto es, un autómata celular consiste de una secuencia de N sitios, donde cada uno lleva un valor entero de 0 a $\hat{k} - 1$. Es inmediato que un autómata celular finito con N sitios tiene \hat{k}^N posibles estados o configuraciones globales distintas.

La configuración global de un autómata celular en el tiempo t , se especifica por los valores de sus N sitios, y puede representarse por un polinomio característico,

$$A^{(t)}(x) = \sum_{i=0}^{N-1} a_i(t) x_i \quad [\text{Ec. 1}]$$

donde el valor del sitio i en el tiempo t está representado por el valor del coeficiente $a_i(t)$.

Los valores de los sitios evolucionan en pasos discretos de tiempo según reglas determinísticas. Por lo tanto, la evolución depende de los valores tanto de \hat{k} (el orden del anillo $Z_{\hat{k}}$) como del número r de vecinos que la regla tome en cuenta. El número de reglas distintas en función de \hat{k} y r está dado por \hat{k}^{2r+1} y por consiguiente tiende a aumentar rápidamente, incluso para \hat{k} y r pequeños. Un ejemplo es la regla dada por,

$$a_i(t) = a_{i-1}(t-1) + a_{i+1}(t-1) \quad [\text{Ec. 2}]$$

En este ejemplo se parte de que el valor de la celda i -ésima depende sólo de sus vecinos más cercanos ($r = 1$). Al considerar, como condición inicial, la configuración global que consiste de todos los sitios iguales a cero, con la excepción de un sitio que contiene un 1, se obtiene el extensamente estudiado Triángulo de Pascal (consulte [1, 3] para mayores detalles).

Cuadro 1. La regla 90: $01011010_2 = 90_{10}$

$r = 1, t - 1$	111	110	101	100	011	010	001	000
t	0	1	0	1	1	0	1	0

Así pues, en el caso en que $\hat{k} = 2$ y $r = 1$ existen $2^{2^{2r+1}} = 256$ reglas distintas, las cuales pueden clasificarse de la siguiente manera: Los valores de las ocho posibles combinaciones de los tres sitios anteriores forman un número binario que se cita como un entero decimal; es importante acomodar las ocho combinaciones como se presentan en el Cuadro 1. El ejemplo que en ella se muestra es para la regla dada por (2) con

aritmética módulo 2. Esto nos da el número binario 01011010_2 que en base decimal es 90_{10} . Es claro que este proceso etiqueta las 256 reglas de una manera unívoca. La regla 90 se ha estudiado ampliamente (por ejemplo en [1,2]), en particular se han estudiado sus posibles configuraciones y su evolución temporal mediante dipolinomios sobre un campo finito.

Consideremos ahora la regla dada por la suma módulo dos de los valores de sus tres vecinos más cercanos en el paso del tiempo anterior,

$$a_i(t+1) = a_{i-1}(t) + a_i(t) + a_{i+1}(t) \quad \text{mod } 2 \quad [\text{Ec. 3}]$$

De acuerdo con el método presentado arriba, los valores de las ocho posibles combinaciones de los tres sitios anteriores forman un número binario, cuya representación decimal corresponde a 150, esto se muestra en el Cuadro 2¹.

Cuadro 2. La regla 150: $10010110_2 = 150_{10}$

$r = 1, t - 1$	111	110	101	100	011	010	001	000
T	1	0	0	1	0	1	1	0

Esta regla, al igual que la regla 90, satisface una propiedad que resulta ser esencial para poder utilizar las técnicas algebraicas introducidas en [2]. Esta propiedad está basada en la siguiente

Definición 1. El *principio de superposición aditiva* dice que la configuración obtenida por la evolución para t pasos de tiempo a partir de una configuración inicial $A^{(0)}(x) + B^{(0)}(x)$ es idéntica a $A^{(0)}(x) + B^{(0)}(x)$ la cual es resultado de la evolución separada de $A^{(0)}(x)$ y $B^{(0)}(x)$.

En otras palabras si $T(x)$ representa la regla que rige al autómata celular, entonces la regla $T(x)$ es *aditiva* si satisface

$$T(x)(A^{(0)}(x) + B^{(0)}(x)) = T(x)A^{(0)}(x) + T(x)B^{(0)}(x) \quad [\text{Ec. 4}]$$

Este principio permite una descripción de la evolución de las configuraciones por medio de multiplicación de polinomios.

Se considerarán "polinomios" que contienen exponentes positivos y negativos. Por definición $H(x)$ es un *dipolinomio* si existe un entero m tal que $x^{(m)}H(x)$ es un polinomio ordinario de x . Los dipolinomios poseen propiedades de divisibilidad y de congruencia análoga a la de los polinomios ordinarios (véase [4] y Apéndice A.D de [3]).

La multiplicación de un polinomio característico $A(x)$ por $x^{\pm j}$, representa una configuración en que el valor de cada sitio se ha trasladado (movido) a un sitio j lugares a su derecha o izquierda, dependiendo si el signo es positivo o negativo, respectivamente.

De esta manera, la evolución que corresponde a la regla 150 mencionada anteriormente, se representa multiplicando al polinomio característico $A^{(0)}(x)$ por el dipolinomio

¹ Algunos trabajos previos relacionados con la Regla 150 son: (1) Espinoza Valdéz, A. (2002). Tesis de licenciatura en Matemáticas Aplicadas, UABC, *Autómatas Celulares: La regla 150*, noviembre. [En línea] Disponible en: <http://alvaro.uabc.googlepages.com/tesis_final.pdf>. (2) Álvarez Parrilla, A. y Espinoza Valdéz, A. "Autómatas Celulares: La regla 150", *Memorias de la XII Semana Regional de Investigación y Docencia en Matemáticas*, Universidad de Sonora, Hermosillo Sonora, México, pp. 1-9, marzo. [En línea] Disponible en: <<http://semana.mat.uson.mx/MemoriasXVII/portada.htm>>.

$$T(x) = x^{(-1)} + 1 + x \quad [\text{Ec. 5}]$$

y la correspondiente a la regla 90 mediante el dipolinomio

$$T(x) = x^{(-1)} + x \quad [\text{Ec. 6}]$$

Nótese que cualquier dipolinomio es congruente, módulo $x^{(N)} - 1$, a un polinomio de grado menor que N , por lo que la evolución de un autómata celular con N sitios y *con condiciones de frontera periódicas* se da mediante la multiplicación, módulo $(x^N - 1)$, del polinomio característico $A^{(t)}(x)$ por la regla $T(x)$.

Las propiedades globales de los autómatas celulares son entonces determinadas por las propiedades algebraicas de estos dipolinomios.

Así, la evolución del autómata celular sobre un anillo finito de 2 elementos con N sitios, y condiciones de frontera periódicas, toma una forma particularmente simple:

$$A^{(t+1)}(x) = T(x)A^{(t)}(x) \quad \text{mod } (x^{(N)} - 1), \quad [\text{Ec. 7}]$$

donde toda la aritmética en los coeficientes polinómicos se realiza en el módulo 2.

Un dipolinomio $A(x)$ divide a un dipolinomio $B(x)$ si existe un dipolinomio $C(x)$ tal que $B(x) = A(x)C(x)$. En particular el *máximo común divisor* de dos dipolinomios distintos de cero $A_1(x)$ y $A_2(x)$ se define como el polinomio ordinario que es el máximo común divisor MCD $(A_1^*(x), A_2^*(x))$, donde $A_i^*(x) = x^{m_i} A_i(x)$ son escogidos de tal manera que $A_i^*(x)$ son polinomios ordinarios con término no constante distinto de cero.

3. Resultados

A continuación se presentan los resultados obtenidos al realizar un estudio de la regla 150 de acuerdo al procedimiento algebraico con que se analizó la regla 90. [3] Cabe aclarar que algunas de las demostraciones son muy parecidas a las que aparecen en [3], sin embargo existen pequeñas diferencias que son intrínsecas a la regla 150, por lo cual optamos por reproducir la mayoría de ellas.

3.1. Configuraciones alcanzables: sucesores y predecesores

En esta sección mostramos condiciones que indican si una configuración específica es alcanzable o no. En particular, mostramos condiciones que nos indican cuáles configuraciones son predecesoras y sucesoras de otras.

Teorema 1. Una configuración $A(x)$ es alcanzable en una evolución de un autómata celular de tamaño N , descrito por $T(x)$, si y sólo si $A(x)$ es divisible por $\Lambda_1(x) = \text{MCD}(x^N - 1, T(x))$.

La prueba de este teorema se puede encontrar como en [3] (Lema 4.4 de dicha referencia).

Proposición 1. Considérese el caso de la regla 150, esto es $T(x) = x + 1 + x^{-1}$, entonces

$$\Lambda_1(x) = \text{MCD}(x^N - 1, T(x)) = \begin{cases} x^2 + x + 1 = T^*(x) & \text{si } N = 3l \\ 1 & \text{si } N \neq 3l \end{cases}$$

Prueba. Primero nótese que $T^*(x) = xT(x) = x^2 + x + 1$. Entonces por la definición de máximo común divisor para dipolinomios, se tiene que $\text{MCD}(x^N - 1, T(x)) = \text{MCD}(x^N - 1, T^*(x))$.

Sea $P(x)$ un polinomio tal que $P(x)|x^N - 1$ y $P(x)|x^2 + x + 1$ entonces existen $Q(x)$ y $H(x)$ tales que $P(x)Q(x) = x^N - 1$ y $P(x)H(x) = x^2 + x + 1$.

Para que $P(x)$ divida a $x^2 + x + 1$ es necesario que $P(x) = ax^2 + bx + c$, donde a , b y c son constantes y solamente pueden tomar los valores 0 o 1. Sustituyendo $P(x) = ax^2 + bx + c$, obtenemos que:

$$ax^2 + bx + cH(x) = x^2 + x + 1,$$

de donde se aprecia que $P(x) = x^2 + x + 1$ con $H(x) = 1$, o $P(x) = 1$ con $H(x) = x^2 + x + 1$.

Ahora consideremos la condición $P(x)Q(x) = x^N - 1$.

Para el caso $N = 3l$, notemos primero que

$$x^{(N)} - 1 = \sum_{i=0}^{N-1} x^i (x-1) = \sum_{i=0}^{N-1} x^{i+1} - \sum_{i=0}^{N-1} x^i$$

de modo que si

$$Q(x) = \sum_{i=0}^{\frac{N}{3}} x^{N-(3i+2)} - \sum_{i=1}^{N-1} x^{N-3i}$$

se aprecia que

$$Q(x)(x^2 + x + 1) = x^N - 1$$

Por lo que se concluye que $P(x) = x^2 + x + 1$.

En el caso de que $N \neq 3l$, nótese que

$$x^{(N)} - 1 = \prod_{\substack{d|N \\ d \neq N}} \Phi_d(x),$$

donde $\Phi_d(x)$ es el polinomio ciclotómico de orden d .

Enumerando los primeros polinomios ciclotómicos:

$$\begin{aligned}\Phi_1(x) &= x-1 \\ \Phi_2(x) &= x+1 \\ \Phi_3(x) &= x^2+x+1 \\ \Phi_4(x) &= x^2+1 \\ \Phi_5(x) &= x^4+x^3+x^2+x+1 \\ \Phi_6(x) &= x^2+x+1\end{aligned}$$

se tiene que $\Phi_d(x)$ es un polinomio mónico con coeficientes enteros para d/N , $d \neq N$. De modo que si $N \neq 3l$ ningún $\Phi_d(x) = x^2+x+1$, o sea $x^{N-1} \equiv (x^2+x+1)Q(x)$, por lo que $P(x)=1$.

Se concluye de la proposición anterior que si $N \neq 3l$ todas las 2^N configuraciones son alcanzables y si $N=3l$, $A(x)$ es alcanzable si y sólo si $x^2+x+1|A(x)$. Esto en contraste con lo que ocurre con la regla 90, donde se tiene que si N es par, $\frac{3}{4}$ de todas las configuraciones posibles no son alcanzables; y si N es impar exactamente la mitad de todas las configuraciones posibles son alcanzables.

Corolario 1. Para $N \neq 3l$ todas las 2^N configuraciones son alcanzables y si $N=3l$, $A(x)$ es alcanzable si y sólo si $x^2+x+1|A(x)$.

Teorema 2. Al contrario de los autómatas celulares de la regla 90, en la evolución de los definidos por la regla 150 si pueden generarse configuraciones que contienen un número impar de sitios con valor uno y no sólo pueden ocurrir como condiciones iniciales.

Prueba. Sea $A^0(x)=1$ la configuración inicial, que tiene como sucesor la configuración:

$$\begin{aligned}A^1(x) &= T(x)A^0(x) \\ &= (x+1+x^{-1})1 \\ &= 1+x+x^{N-1}, \quad \text{mod } (x^N-1).\end{aligned}$$

Para $N=1$, $A^1(x)=1 \pmod{2}$; para $N=2$, $A^1(x)=1 \pmod{2}$ y para $N>2$, $A^1(x)=1+x+x^{N-1} \pmod{2}$.

Como se puede observar, en la evolución del autómata celular sí se generan sitios impares con valor uno.

Lema 1. Dos configuraciones $A^0(x)=1$ y $B^0(x)=1$ evolucionan a una misma configuración $C(x) \equiv T(x)A^0(x) \equiv T(x)B^0(x)$ después de un paso de tiempo en la evolución del autómata celular si y sólo si $A^0(x) \equiv B^0(x) + Q(x)$, donde $T(x)Q(x)=0$.

Prueba. Sean $A^0(x)$ y $B^0(x)$ dos configuraciones cualesquiera, se dice que

$$T(x)A^0(x) \equiv T(x)B^0(x)$$

si y sólo si $A^0(x)=B^0(x)+Q(x)$, donde $T(x)Q(x)=0$.

Sea $A^0(x)=B^0(x)+Q(x)$, si multiplicamos por $T(x)$, entonces $T(x)A^0(x)\equiv T(x)B^0(x)+T(x)Q(x)$, y puesto que $T(x)Q(x)=0$, entonces $T(x)A^0(x)\equiv T(x)B^0(x)$.

Supóngase que $A^0(x)=B^0(x)+Q(x)$, con $T(x)Q(x)\neq 0$, entonces $T(x)A^0(x)\equiv T(x)B^0(x)+T(x)Q(x)$, $T(x)A^0(x)\equiv T(x)B^0(x)+T(x)Q(x) \pmod{(x^N-1)}$; para que evolucionen a la misma configuración $T(x)Q(x)=0$, lo cual implica una contradicción debido a que por construcción $T(x)Q(x)\neq 0$, por lo tanto la otra mitad del lema queda probada.

Este lema da la posibilidad de reconocer cuándo es que dos configuraciones tienen el mismo sucesor. Lo que da pie para obtener el siguiente

Teorema 3. Las configuraciones en el autómata celular que tienen por lo menos un predecesor, tienen un predecesor exactamente para $N\neq 3l$ y exactamente cuatro para $N=3l$.

Prueba. En este teorema se hace uso del lema anterior, se demuestra que $Q(x)$ evoluciona a la configuración nula después de un paso de tiempo.

Sea $Q(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, con $n=N-1$.

Se requiere un $Q(x)$ tal que $T(x)Q(x)=0$, de manera que sustituyendo se obtiene

$$(x+1+x^{-1})(a_0+a_1x+a_2x^2+\dots+a_nx^n)=0$$

entonces

$$(a_0+a_1x+a_2x^2+\dots+a_nx^{n+1})+a_0+a_1x+a_2x^2+\dots+a_nx^n+a_0x^{-1}+a_1+a_2x+\dots+a_nx^{n-1}=0 ,$$

Agrupando términos:

$$a_n+a_0+a_1x(a_0+a_1+a_2)+x^2(a_1+a_2+a_3)+\dots+x^{n-1}(a_{n-2}+a_{n-1}+a_n)+x^n(a_{n-1}+a_n+a_0)=0 \pmod{(x^N-1)} .$$

Para que se pueda cumplir la igualdad se tiene que cumplir que los coeficientes sean igual a cero, esto es:

$$\begin{aligned} a_n+a_0+a_1 &= 0 \\ a_0+a_1+a_2 &= 0 \\ a_1+a_2+a_3 &= 0 \\ &\vdots \\ a_{i-1}+a_i+a_{i+1} &= 0 \\ &\vdots \\ a_{n-2}+a_{n-1}+a_n &= 0 \\ a_{n-1}+a_n+a_0 &= 0 \end{aligned}$$

Por lo tanto, la relación general determina todos los coeficientes, en términos de a_0 y a_1 ; donde a_0 y a_1 pueden tomar el valor de 0 o 1. Al examinar las posibles combinaciones se obtienen las siguientes relaciones de recurrencia:

$$\begin{array}{ll} a_i = a_{i-2} + a_{i-1} & a_n = a_0 + a_1 \\ a_{n-1} = a_n + a_0 & a_{3i} = a_0 \\ a_{3i+1} = a_1 & a_{3i+2} = a_2 \end{array}$$

de donde se observan cuatro casos:

- 1) $a_0 = a_1 = 0$, entonces $a_i = 0$, para todo i .
- 2) $a_0 = a_1 = 1$, entonces $a_n = 0$, para $n = 2 + 3i$.
- 3) $a_0 = 1$, $a_1 = 1$, entonces $a_n = 1$, para $n = 2 + 3i$.
- 4) $a_1 = 1$, $a_0 = 0$, entonces $a_n = 1$, para $n = 2 + 3i$.

Nótese que los casos 2, 3 y 4 son válidos para $n = 2 + 3i$, pero inicialmente se consideró que $n = N - 1$, entonces el resultado es válido siempre y cuando $N = 3l$. De manera que se puede concluir que si $N \neq 3l$ sólo la configuración nula tiene esta propiedad y si $N = 3l$ son cuatro las posibles formas de $Q(x)$:

$$\begin{array}{l} 1) \quad \sum_{i=0}^{\frac{N}{3}} x^{3i+1} + \sum_{i=0}^{\frac{N}{3}} x^{3i} \\ 2) \quad \sum_{i=0}^{\frac{N}{3}} x^{3i+2} + \sum_{i=0}^{\frac{N}{3}} x^{3i+1} \\ 3) \quad \sum_{i=0}^{\frac{N}{3}} x^{3i+2} + \sum_{i=0}^{\frac{N}{3}} x^{3i} \\ 4) \quad 0. \end{array}$$

Al aplicarle la regla 150 a cualquiera de las configuraciones anteriores, se obtiene la configuración nula.

Analizando un poco este lema es posible darse cuenta de que la configuración nula tiene cuatro posibles predecesores para $N = 3l$, mientras que para $N \neq 3l$ sólo existe una.

Los puntos fijos para la regla 90, en este caso son predecesores para $N = 3l$.

Corolario 2. Para $N \neq 3l$, el único predecesor de la configuración nula es ella misma.

Obsérvese que conforme transcurra el tiempo siempre se entra en un ciclo con la configuración inicial dada.

Teorema 4. No se puede obtener la configuración nula después de un paso de tiempo, para cualquier configuración inicial con un solo sitio con valor 1 en cualquiera de sus sitios.

Prueba. Debido a la homogeneidad es suficiente probar que la configuración inicial $A^0(x)=1$ no es predecesor de la configuración nula para todo $N>0$.

Para $N=1$, se tiene que

$T(x)A^0(x)=x+1-x^{-1}=3 \pmod{(x^1-1)}$, pero recordando que se está trabajando sobre el campo Z_2 entonces $T(x)A^0(x)=1$.

Para $N=2$, se tiene que

$T(x)A^0(x)=x+1-x^{-1}=2x+1 \pmod{(x^2-1)}$, de manera que de nueva cuenta aplicando aritmética al módulo 2 se obtiene $T(x)A^0(x)=1$.

Para $N=3$, se tiene que

$$T(x)A^0(x)=x+1-x^{-1}=1+x+x^2 \pmod{(x^3-1)}.$$

Para $N>3$, se tiene que

$$T(x)A^0(x)=x+1-x^{-1}=1+x+x^{N-1} \pmod{(x^N-1)}.$$

3.2. Ciclos límite

En esta sección se muestran algunas condiciones bajo las cuales el autómata celular llega a ciclos límite en su evolución, así como una caracterización bastante completa de cuáles son estos posibles ciclos límite.

Una manera de visualizar la evolución de un autómata celular es considerando el diagrama de transición de estados (configuraciones). Éste es un grafo (o gráfica) donde cada nodo representa una de las 2^N configuraciones posibles y las aristas dirigidas

indican si es posible pasar de una configuración a otra en un paso de tiempo. Es conveniente notar que cada configuración tiene un solo sucesor, sin embargo, puede darse el caso en que algunas configuraciones tengan varios predecesores, lo que indica que en estos casos el autómata no es reversible. A los predecesores de una configuración que se encuentra en un ciclo límite, y que no sean parte del ciclo límite, les llamaremos *árbol arraigado* a dicha configuración o nodo.

Lema 2. Todos los árboles arraigados a los nodos en todos los ciclos del gráfico de transición de estados para el autómata celular definido por la regla 150 son idénticos.

Prueba. Este resultado se demuestra mostrando que el árbol arraigado a cualquier nodo de cualquier ciclo, es idéntico al árbol arraigado a la configuración nula.

Sea $A(x)$ una configuración que evoluciona exactamente a la configuración nula después de t pasos de tiempo, de manera que

$$T(x)^t A(x)=0 \pmod{(x^N-1)}.$$

Sea $R(x)$ una configuración en un ciclo y $R^{-t}(x)$ otra configuración en el mismo ciclo tal que

$$T(x)^t R^{-t}(x)=R(x) \pmod{(x^N-1)}.$$

Sea $\Psi_{R(x)}[A(x)]=A(x)+R^{-t}(x)$ entonces $\Psi_{R(x)}:A(x) \mapsto A(x)+R^{-t}(x)$. Después de t pasos de tiempo en la configuración $\Psi_{R(x)}$, obtenemos

$$T(x)^t \Psi_{R(x)}[A(x)] = T(x)^t A(x) + T(x)^t R^{-t}(x) = R(x) \pmod{(x^N - 1)},$$

y está claro que todas las configuraciones $\Psi_{R(x)}[A(x)]$ evolucionan después de t pasos de tiempo a $R(x)$.

Para mostrar que estas configuraciones quedan en un árbol arraigado a $R(x)$, uno debe mostrar que su evolución no alcanza ninguna otra configuración del ciclo para cualquier $b < t$.

Asumamos que es falsa esta suposición. Para que exista algún $m \neq 0$ tal que

$$T(x)^t \Psi_{R(x)}[A(x)] = T(x)^b A(x) + T(x)^b R^{-b}(x) = R^{-m}(x)$$

es necesario que $R^{-m}(x) = T(x)^b A(x) + R(x)^b R^{-b}(x) R^{-m}(x)$. Sea $t = m + b$ entonces $R^{-m}(x) = T(x)^b A(x) + R^{(b-t)}(x)$.

Subsecuentemente $T(x)^t A(x) = 0 \pmod{(x^N - 1)}$, esto implicaría que $R^{-m}(x) = R^{(b-t)}(x)$. Pero $R^{-m}(x) - R^{(b-t)}(x) = T(x)^t A(x)$, y por la construcción $T(x)^t A(x) \neq 0$ para cualquier $b < t$, obteniéndose una contradicción. De manera que en la evolución no se alcanza ninguna otra configuración del ciclo para cualquier $b < t$.

Sean $A(x)$ y $B(x)$ dos polinomios, $\Psi_{R(x)}[A(x)] = A(x) + R^{-t}(x)$ y $\Psi_{R(x)}[B(x)] = B(x) + R^{-t}(x)$, donde después de t pasos de tiempo, $\Psi_{R(x)}[A(x)] = \Psi_{R(x)}[B(x)]$ entonces $A(x) + R^{-t}(x) = B(x) + R^{-t}(x)$ de lo cual se obtiene que $A(x) = B(x)$, por tanto $\Psi_{R(x)}$ es uno a uno.

Finalmente si $T(x)A^0(x) = A^1(x)$, entonces $T(x)\Psi_{R(x)}[A^0(x)] = \Psi_{R(x)}[A^1(x)]$, lo cual se sigue inmediatamente de la definición de Ψ . Así Ψ es un isomorfismo, por lo que los árboles arraigados en todas las configuraciones son isomorfas al árbol arraigado que contiene la configuración nula.

Este resultado indica varias cosas entre las que destacan: en la evolución de un autómata celular bajo la regla 150 se tiene siempre una etapa de transición para luego llegar a un ciclo de configuraciones que se repiten. Además, el número de predecesores de una configuración que se encuentre en un ciclo, y que no sean elementos del ciclo, siempre es el mismo.

Un punto fijo es un ciclo de longitud uno. Entonces se obtiene el siguiente

Teorema 5. Para un autómata celular definido con la regla 150, para $N \neq 2l$ existen exactamente dos puntos fijos distintos y para $N = 2l$ exactamente cuatro puntos fijos distintos.

Prueba. Sea $A^0(x)$ un punto fijo, esto significa que $T(x)A^0(x) = A^0(x)$. Para demostrar cuáles son los únicos puntos fijos realizamos lo siguiente:

Sea $A^0(x) = a_0 + a_1(x) + a_2x^2 + \dots + a_nx^n$, con

$n = N - 1$, un punto fijo, entonces

$$T(x)A^0(x)=A^0(x) \cdot$$

Sustituyendo se obtiene:

$$(x+1+x^{-1})(a_0+a_1(x)+a_2x^2+\dots+a_nx^n)=a_0+a_1(x)+a_2x^2+\dots+a_nx^n$$

entonces

$$\begin{aligned} a_0x+a_1x^2+a_2x^3+\dots+a_nx^{n-1}+a_0+a_1x \\ a_2x^2+\dots+a_nx^n+a_0x^{-1}+a_1+a_2x+\dots+ \\ a_nx^{n-1}=a_0+a_1x+a_2x^2+\dots+a_nx^n, \end{aligned}$$

Agrupando términos, se obtiene:

$$\begin{aligned} a_nx+a_0+a_1x(a_0+a_1+a_2)+x^2(a_1+a_2+a_3)+ \\ \dots+x^{n-1}(a_{n-2}+a_{n-1}+a_n)+x^n(a_{n-1}+a_n+a_0)= \\ a_0x+a_1x+a_2x^2+\dots+a_nx^n \quad \text{mod } (x^N-1). \end{aligned}$$

Para que se pueda cumplir la igualdad se tiene, las relaciones entre los coeficientes, igualando término a término se ve que

$$\begin{aligned} a_0 &= a_2 \\ &\cdot \\ &\cdot \\ a_{i-1} &= a_{i+1} \\ &\cdot \\ &\cdot \\ a_{n-1} &= a_0 \\ a_n &= a_1. \end{aligned}$$

Recordando que estamos trabajando en \mathbb{Z}_2 , entonces los valores de los coeficientes sólo pueden ser 0 o 1. Por lo tanto, al realizar las posibles combinaciones se tienen cuatro casos:

1. 00000 ···, para todo i .
2. 11111 ···, para todo i .
3. 101010 ···, para $n=2i-1$.
4. 010101 ···, para para $n=2i-1$.

Nótese que los casos 3 y 4 se cumplen solamente para $n=2i-1$, recordando que inicialmente dijimos que $n=N-1$, obtenemos que en realidad son válidos para $N=2l$.

Si $N \neq 2l$, los dos únicos puntos fijos distintos son las configuraciones 00000 y 11111 ·, con demostración trivial. Para $N=2l$ los únicos puntos fijos distintos son las configuraciones 00000 ·, 11111 ·, 101010 ·, y 010101 ·.

Al aplicar la regla 150 a estas configuraciones inmediatamente puede observarse que se preserva la misma estructura del autómata celular conforme transcurre el tiempo.

Lema 3. Las longitudes de cada ciclo, de un autómata celular de tamaño N definido por la regla 150, divide la longitud Π_N del ciclo obtenido con una configuración inicial que contiene un solo sitio con valor uno.

Prueba. Sea Π_N como en el enunciado. Sea $A^0(x)=a_0+a_1(x)+a_2x^2+\dots+a_nx^n$ la configuración inicial, con $n=N-1$. Para obtener la longitud de ciclo de esta configuración en la evolución del autómata celular, podemos hacer una superposición de la configuración con un solo sitio con valor uno.

Se sabe que $0 \leq \Pi_B \leq \Pi_N$, donde Π_B es la configuración con un solo sitio con valor uno. Ahora bien supóngase que Π_B no divide a Π_N , entonces $\Pi_B > 1$. Si Π_B no divide a Π_N , entonces después de Π_N pasos de tiempo en la evolución del autómata celular se llega a la conclusión de que todas las configuraciones en el ciclo son iguales, teniendo así un ciclo de longitud uno, de lo que se concluye que $\Pi_B = 1$. Por lo tanto la suposición de que Π_B no divide a Π_N es incorrecta.

Cuando se generen las configuraciones de los *puntos fijos*, en la evolución del autómata celular, éstos son los únicos que tienen longitud igual a uno.

Teorema 6. Para un autómata celular definido con la regla 150, con $N=3 \cdot 2^j$, la longitud del ciclo obtenida a partir de la configuración $(1+x^{2^j})$ es 1.

Prueba. En este caso se evoluciona finalmente a un punto fijo que consiste en una configuración nula.

Primero nótese que: $(x+1+x^{-1})^{3 \cdot 2^j} (1+x^{2^j}) = [(x+1-x^{-1})^{2^j}]^3 (1+x^{2^j})$. Se sabe que $(x+1+x^{-1})^{2^j} = x^{2^j} + 1 + x^{2^j} \pmod 2$, ya que $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} \pmod p$, $n \geq 0$, donde a y $b \in \mathbb{Z}_p$, $p = \text{primo}$. Entonces $[x^{2^j} + 1 + x^{-2^j}]^3 (1+x^{2^j}) = 0 \pmod 2$.

Por lo tanto, para un autómata celular definido por la regla 150, de tamaño $N=3 \cdot 2^j$, y con configuración inicial $(1+x^{2^j})$, esta evoluciona después de N pasos de tiempo a la configuración nula.

Teorema 7. Dada una configuración inicial cualquiera para $N=2^j$, después de 2^{j-1} pasos de tiempo se vuelve a obtener la configuración inicial.

Prueba. Sea $A^0(x)=1$ la configuración inicial. Sustituyendo el valor de $A^0(x)$ y aplicando la regla 2^{j-1} veces, se obtiene lo siguiente: $T(x)^N \cdot A^0(x) = (x+1+x^{-1})^{2^{j-1}} (1)$. Entonces

$$\begin{aligned} (x^{2^{j-1}} + 1 + x^{-2^{j-1}})(1) &= (x^{2^{j-1}} + 1 + x^{-2^{j-1}}) \\ &= 1 + 2x^{2^{j-1}} \pmod{(x^{2^j} - 1)} \\ &= 1 \pmod 2. \end{aligned}$$

Por la propiedad de aditividad, cualquier configuración puede considerarse como una superposición de configuraciones inicial con un solo sitio diferente de cero, por lo tanto este resultado es válido para cualquier configuración inicial.

Por lo que, dada la configuración inicial, después de 2^{j-1} pasos de tiempo se está en un ciclo repetitivo conforme transcurra el tiempo.

También es importante notar que la longitud de cualquier ciclo divide a 2^{j-1} , por lo tanto $\prod_N |2^{j-1}|$.

Corolario 3. Nunca puede generarse la configuración nula en la evolución del autómata celular para $N=2^j$ y sólo puede ocurrir como condición inicial.

Se sabe que para $N=2^j$ uno de los predecesores es la configuración nula y que el único predecesor de la configuración nula es ella misma. Por lo tanto si el único predecesor de la configuración nula es ella misma, entonces en la evolución del autómata celular no se puede generar ésta y sólo puede ocurrir como configuración inicial. Sucede la mismo para la configuración 1111 . .

Un *ciclo puro* es aquel en el cual la \prod_N del ciclo de autómatas celulares es uno. Así, debido al lema 2, la configuración nula $A(x)$ entra a un ciclo puro si el árbol arraigado que la genera es nulo.

Corolario 4. Para un autómata celular que evoluciona en base a la regla 150, con $N=2^j$ todos los ciclos son ciclos puros.

4. Conclusiones

Se puede observar que existe una gran diferencia en cómo se alcanzan ciertas configuraciones en la evolución del autómata celular entre la regla 150 y la regla 90. Para el caso de la regla 150 si $N \neq 3l$ todas las 2^N configuraciones son alcanzables y si $N=3l$, la configuración $A(x)$ es alcanzable si y sólo si $x^2+x+1|A(x)$. Esto en contraste con lo que ocurre con la regla 90, donde se tiene que si N es par sólo $\frac{1}{4}$ de todas las

configuraciones posibles son alcanzables; y si N es impar exactamente la mitad de todas las configuraciones son alcanzables.[3] En la evolución de los autómatas celulares definidos en base a la regla 150 sí pueden generarse configuraciones que contengan un número impar de sitios con valor uno y no sólo pueden ocurrir como condiciones iniciales, como sucede para la regla 90 [3]. En la regla 150 puede reconocerse cuándo es que dos configuraciones tienen el mismo sucesor. Esto da pie para obtener los predecesores de la regla y así saber que existe exactamente un predecesor cuando $N \neq 3l$ y cuatro cuando $N=3l$. Mientras que para la regla 90 existen exactamente dos predecesores cuando N es impar y cuatro cuando N es par [3]. Cabe mencionar que el único predecesor cuando $N \neq 3l$ para la regla 150, es la configuración nula y que el predecesor de ésta, es ella misma. Al realizar este estudio puede observarse que los puntos fijos para la regla 90, en el caso de la regla 150, son predecesores para $N=3l$.

Una ventaja de estudiar autómatas celulares, es que tienen representaciones gráficas y algebraicas, lo que permite demostrar y entender mejor lo que sucede. En la evolución de un autómata celular bajo la regla 150 se tiene siempre una etapa de transientes para luego llegar a un ciclo de configuraciones que se repiten. Además, el número de

predecesores de una configuración que se encuentre en un ciclo, y que no sean elementos del ciclo, siempre es el mismo.

Para un autómata celular definido con la regla 150, para $N \neq 2^j$ existen exactamente dos puntos fijos distintos y para $N = 2^j$ exactamente cuatro puntos fijos distintos. Las longitudes de todos los ciclos de un autómata celular de tamaño N definido por la regla 150 divide a \prod_N , la longitud del ciclo obtenido con una configuración inicial que contiene un solo sitio con valor uno. Para un autómata celular definido con la regla 150, para $N = 3 \cdot 2^j$, la longitud del ciclo obtenida a partir de la configuración inicial $(1+x^{2^j})$ es 1, i.e., después de N pasos de tiempo evoluciona a la configuración nula. En el caso en que $N = 2^j$ dada la configuración inicial, después de 2^{j-1} pasos de tiempo se llega a un ciclo repetitivo, y es importante mencionar que la longitud de cualquier ciclo divide a 2^{j-1} , por lo tanto $\prod_N | 2^{j-1}$.

No se puede obtener la configuración nula después de un paso de tiempo, para cualquier configuración inicial con un solo sitio con valor 1 (y los demás con valor 0). Se sabe que para $N = 2^j$ uno de los predecesores es la configuración nula y que el único predecesor de la configuración nula es ella misma. Por lo tanto si el único predecesor de la configuración nula es ella misma, entonces en la evolución del autómata celular no se puede generar ésta y sólo puede ocurrir como configuración inicial. Sucede lo mismo para la configuración 1111.

En conclusión, se utilizó un formalismo apropiado para estudiar la evolución de autómatas celulares unidimensionales sobre Z_2 con condiciones de frontera periódicas. Los resultados muestran diferencias cualitativas a pesar de que tanto la regla 90 como la regla 150 son aditivas.

5. Referencias

- [1] Granville, A. (1992). Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's Triangle. *American Mathematical Monthly*, no. 99, pp. 318-331.
- [2] Wolfram, S. (1984). Geometry of binomial coefficients. *American Mathematica Monthly*, no. 91, pp. 566-571.
- [3] Martin, O.; Odlyzko, A. M. & Wolfram, S. (1984). Algebraic Properties of Cellular Automata. *Communications in Mathematical Physics*, no. 93, pp. 219-258, March.

6. Bibliografía

- Mac Williams, F. J. & Sloane, N. J. A. (1977). *The theory of error-correcting codes*. North-Holland, Amsterdam.
- Moore, E. F. (1962). Machine models of self-reproduction. In *Proceedings of Symposia in Applied Mathematics*. vol. 14, no. 17 reprinted in: Burks, A. W. (1966). *Essays on cellular automata*, University of Illinois Press.
- Packard, N. H. and Wolfram, S. (1985). Two-dimensional cellular automata. *Journal of Statistical Physics*, Piscataway, USA: Springer Netherlands, vol. 38, no. 5/6, pp. 901-946, March.
- Pines, D. (1988). Emerging syntheses in science. In *Proceedings of the Founding Workshops of the Santa Fe Institute*, Santa Fe, Nuevo México: Addison Wesley, 237 pp.
- Wolfram, S. (1986). Theory and Applications of Cellular Automata. *World Scientific*, Singapore: Advanced Series on Complex Systems.
- Wolfram, S. (1984). Universality and Complexity in Cellular Automata. *Physica D*, no. 10, pp. 1-35, January.