Sección de Matemáticas
Universidad de La Laguna

Pablo Heer

Autómatas Celulares. Análisis y experimentos en el caso unidimensional.

Cellular Automata. Analysis and experiments in the one-dimensional case.

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, septiembre de 2022

Dirigido por
Carlos González Alcón

Carlos González Alcón
Departamento de Matemáticas,
Estadística e Investigación Operativa
Universidad de La Laguna
38204 La Laguna, Tenerife

Agradecimientos

A mi tutor por los consejos y la inspiración. A mi amigo Pedro por la ayuda y paciencia. A Noelia por la revisión.

Pablo Heer
La Laguna, 6 de septiembre de 2022

Resumen · Abstract

Resumen

Los autómatas celulares son sistemas dinámicos discretos basados en reglas simples, capaces de generar patrones complicados. En este trabajo se introducen los autómatas celulares unidimensionales y se presenta una clasificación en cuatro clases de comportamiento según el aspecto de los patrones que generan. Además, se derivan resultados algebraicos para el conjunto particular de las reglas aditivas. Para ello, se utiliza un formalismo que identifica el espacio de configuraciones con el anillo de los dipolinomios, una generalización de los polinomios con coeficientes enteros. Se presenta un análisis empírico de la densidad de celdas negras en los patrones de evolución y de la aleatoriedad de la columna central del patrón generado por la regla particular 30. Los patrones generados y resultados numéricos se obtuvieron mediante la implementación de un autómata celular con el lenguaje de programación Julia.

Palabras clave: *Autómatas Celulares – Autómatas Aditivos – Regla 30*

Abstract

Cellular automata are discrete dynamical systems based on simple rules, that can generate complicated patterns. In this document, elementary cellular automata are introduced and a classification into four classes of behaviour is presented. Algebraic results on the special set of additive rules are derived. To do so, an algebraic formalism which identifies the space of configurations with the ring of dipolynomials, a generalized form of polynomials with whole coefficients, is used. Empirical results on the density of black cells in evolution patterns and on the randomness of the central column of the pattern generated by the particular rule 30 are also derived. The patterns generated as well as the numeric results were obtained through implementation of an cellular automata with the programming language Julia.

Keywords: *Cellular Automata – Additive Automata – Rule 30*

Índice general

Introducción

Los autómatas celulares son ejemplos, tal vez los más elementales, de sistemas basados en reglas simples, locales y aplicadas de manera reiterada. Hay interés científico creciente en la comprensión de cómo evolucionan este tipo de sistemas, tanto de carácter práctico en la modelización de procesos dinámicos como teórico en las ciencias de la computación.

En el campo de la investigación de los autómatas celulares destacan los trabajos de John H. Conway y Stephen Wolfram, enfocados a la generalización del concepto de computación y a la idea de universalidad computacional ya estudiada a mitad del siglo XX por Alan Turing, entre otros.

En la actualidad hay muchas preguntas abiertas acerca de la evolución de los autómatas celulares. Estos sistemas son de implementación fácil y con bajo coste computacional y mucho del trabajo hecho, por ejemplo por S. Wolfram, se reduce al estudio empírico. Varios intentos de probar resultados matemáticamente formales han demostrado las dificultades que existen a la hora de predecir el comportamiento de procesos con reglas simples. Algunos de los problemas considerados están estrechamente relacionados con cuestiones de la teoría de números.

Este trabajo quiere servir de introducción a los autómatas celulares y describir los diferentes tipos de comportamiento que se observan en estos. Se obtienen una serie de resultados de interés matemático para un conjunto particular de reglas y se concluye con un breve estudio empírico.

En el primer capítulo se introduce el concepto de autómata celular y se presentan los patrones generados por los mismos, que permiten caracterizarlos en cuatro clases de comportamiento. El hecho destacado que se observa es que estos sistemas, a pesar de ser basados en reglas simples, son capaces de generar complejidad sorprendente. En el segundo capítulo se presenta un formalismo algebraico para probar varios resultados relacionados con la evolución de las reglas de autómatas celulares aditivos, una clase particular de estos. Se concluye que la clasificación introducida en el primer capítulo presenta ciertas "debilidades" pues no detecta las implicaciones de la propiedad aditiva de estas reglas.

Por último, en el tercer capítulo se presenta un breve análisis empírico de un parámetro importante en la evolución de los autómatas celulares: la densidad de celdas negras. Además, se estudia la factibilidad de un autómata particular como generador de secuencias aleatorias.

1

Autómatas Celulares

Los *Autómatas Celulares* (AC) son sistemas dinámicos discretos constituidos por tres componentes: las celdas que presentan en cada instante un estado, una topología que describe, para cada celda, las celdas que influyen en su estado y una regla que determina el estado del autómata en el siguiente paso. Dependiendo de la dimensión del autómata en cuestión, se puede representar por medio de una cadena unidimensional, un plano bidimensional o, en general, un espacio de n dimensiones. La colección de valores que pueden tomar las celdas se denomina *conjunto de estados* o *alfabeto*. El conjunto formado por una celda y aquellas que influyen en su estado en el siguiente instante se llama *vecindario*. El tiempo en la evolución del autómata se mide en unidades discretas llamadas *iteraciones*. La regla local que determina el valor del autómata tras una iteración actúa de forma simúltanea (en paralelo) sobre todas las celdas y, en general, es la misma para todas.

Muchos procesos en la naturaleza son gobernados por leyes locales y homogéneas susceptibles a ser simulados por un autómata celular. Por ejemplo, la dinámica de fluidos puede ser modelada por partículas puntuales que se mueven a través de una cuadrícula. También son de utilidad en la investigación de fenómenos de gran escala, como la evolución de incendios forestales y pandemias. Muchas de las propiedades más estudiadas de los autómatas celulares son motivadas por la física, sin embargo también son investigados en ciencia de la computación y otras ramas de las matemáticas.

A pesar su construcción simple y la universalidad de sus características elementales, el concepto general de autómata celular no parece haber sido considerado hasta mediados del siglo XX. Alrededor del año 1900 emergen los métodos de aproximación en diferencias finitas para la resolución de ecuaciones diferenciales y en 1936 Alan Turing inventa su máquina universal, basada en la idea de operaciones arbitrarias sobre secuencias de elementos discretos. Inspirados en los avances de los computadores electrónicos, en los años cincuenta se desarrollan varios modelos, de forma independiente, que resultan ser equivalentes a los autómatas celulares.

La manera más documentada en la que fueron introducidos los autómatas celulares fue a través del trabajo de John von Neumann, con el propósito de desarrollar un modelo abstracto para la autorreproducción de sistemas biológicos. Los primeros modelos de von Neumman, posiblemente basados en ideas de ingeniería química, representaban máquinas tridimensionales capaces de construir copias de sí mismas, siguiendo procesos descritos por ecuaciones diferenciales. Reconociendo la analogía con el problema de distribución de circuitos electrónicos y siguiendo una proposición de Stanislaw Ulam (quien posiblemente ya había considerado el problema de forma independiente), von Neumann redujo su modelo a dos dimensiones. El autómata particular que consideró se basaba en un conjunto de reglas complicadas con 29 estados posibles para cada celda. Para dar una demostración rigurosa de la posibilidad de autorreproducción, von Neumann construyó una configuración formada por 200.000 celdas, capaz de construir una copia de ella misma. Aparentemente, von Neumann creía que tal nivel de complejidad era necesario para construir un modelo con la capacidad de autorreproducción, y que por tanto los mecanismos responsables del comportamiento complejo de sistemas biológicos deberían ser de una sofisticación similar.

A lo largo de los años sesenta se construyeron autómatas más sencillos con la capacidad de autorreproducción y comenzó un estudio más formal de las propiedades que eran relevantes para este propósito. Técnicas análogas a aquellas empleadas en el estudio de la máquina universal de Turing fueron usadas para demostrar varios resultados sobre las capacidades computacionales de los autómatas celulares. La mayoría del tiempo computacional invertido en investigación matemática fue dedicada a la simulación de sistemas más complejos, mayoritariamente al estudio de ecuaciones diferenciales. Sin embargo, Ulam usó ordenadores para simular varios autómatas bidimensionales para producir ejemplos de lo que denominaba *figuras geométricas recursivamente definidas.* Ulam notó que algunas reglas de crecimiento sencillas producían patrones complicados y consideró que podría ser un fenómeno relevante en biología.

Aunque la investigación científica relacionada con los autómatas celulares prácticamente había parado en los años setenta, un caso particular entra en el mundo de la computación recreativa. En 1968, John Conway comienza haciendo algunos experimentos con reglas sencillas para un autómata bidimensional e introduce un conjunto particular de reglas que denomina *The Game of Life.* Se invierten grandes esfuerzos para encontrar condiciones iniciales particulares que llevan a determinados comportamientos y patrones y se demuestra la universalidad computacional del conjunto particular de reglas, esto es, que es capaz de simular una máquina universal de Turing y, consecuentemente, ejecutar cualquier tarea computacional.

A principios de los años ochenta resurge el interés de la comunidad científica en los autómatas celulares. Con la publicación de varios artículos científicos, en-

tre ellos *Statistical Mechanics of Cellular Automata* ([3]) y *Algebraic Properties of Cellular Automata* ([2]), Stephen Wolfram revive la investigación alrededor de los autómatas celulares. Centrado en los autómatas celulares unidimensionales, Wolfram destaca la complejidad emergente en los patrones generados por reglas más sencillas que aquellas consideradas hasta el momento. Introduce la popular clasificación de los autómatas celulares en cuatro clases de comportamiento. Mathew Cook demuestra la universalidad de la regla 110, una regla unidimensional particular destacada en el trabajo de Wolfram, quien en su libro controvertido *A New Kind of Science* ([1]) publicado en 2002 remarca la necesidad de nuevas técnicas y formalismos científicos para estudiar fenómenos como la complejidad emergente en sistemas con reglas sencillas, ya que estos fenómenos "parecen escaparse de los sentidos de las matemáticas tradicionales", como él mismo afirma.

1.1. Autómatas celulares unidimensionales y la clasificación de Wolfram

Los autómatas celulares unidimensionales constituyen un conjunto particular ampliamente estudiado. Una parte de la investigación realizada sobre estos sistemas es de carácter empírico, como el intento de Wolfram de clasificar los autómatas sistemáticamente basándose en resultados observacionales. Por otro lado, se emplean métodos de teoría de la información y de sistemas dinámicos para el estudio de características fundamentales tales como la complejidad y la universalidad de las computaciones hechas por estos autómatas.

En un AC unidimensional, el espacio de celdas está formado por una cadena, denotada por L. En gran parte del estudio teórico se considera que L es un espacio infinito, con cada celda en correspondencia biunívoca con un número entero ($L \cong \mathbb{Z}$). Sin embargo, para la implementación de un autómata celular en un computador se debe considerar un espacio finito. La estructura particular de L depende entonces de la elección de las *condiciones de frontera*. En lo que sigue, se considerará generalmente la *condición de frontera periódica*, siendo L una cadena finita de N celdas unida por los extremos, de forma que $L \cong \mathbb{Z}_N$. En este caso el autómata celular se denomina *cilíndrico*, pues la evolución puede representarse por iteraciones consecutivas que ocurren sobre un cilindro (Véase la figura 1.1). Otras condiciones de frontera pueden ser implementadas, tales como la condición de frontera nula, en la que los valores de las celdas en los extremos son siempre cero, independientemente del autómata particular considerado.

El alfabeto o conjunto de estados S está formado por los símbolos que denotan los posibles estados de una celda. Usualmente el alfabeto se representa por un conjunto de enteros $S = \{0, 1, 2, ..., s-1\}$ para un autómata celular de s estados. La asignación de un elemento de S a cada celda de L se denomina *con-*

figuración. El conjuno de todas las posibles configuraciones se denomina *espacio de estados* y se denota por E de forma genérica. En el caso de un autómata celular cilíndrico el espacio de estados se denota por E_N. La regla que actualiza el estado de cada celda, de forma simultánea, se denomina *regla de evolución* y se representa por una aplicación definida sobre el espacio de configuraciones $X : E \to E$. Si $\mu \in E$ entonces μ_i es la entrada de la celda i-ésima en la configuración μ. La representación del estado μ en términos de los μ_i dada por $\mu = [\mu_0\mu_1...\mu_{N-1}]$ se llama *representación coordenada*. Configuraciones periódicas se representan subrayando la cadena de símbolos correspondiente al periodo. Las configuraciones periódicas de unos y ceros son $\underline{\mathbb{1}}$ y $\underline{\mathbb{0}}$ respectivamente.

En una iteración del autómata, la regla de evolución X reasigna valores a cada celda de la configuración actual, dependiendo de los valores de celdas vecinas. El *vecindario de k celdas* de una celda c consiste de un bloque consecutivo de k celdas en el que la celda c ocupa una posición determinada, llamada *celda cambiante*. Si k es impar y $c = \frac{k-1}{2}$ se trata de *vecindarios simétricos*. La acción de X queda determinada por la *aplicación local*

$$f_X : \mathbb{Z}_s^k \to \mathbb{Z}_s.$$

En este caso se dice que X es una regla de k celdas y $\mathbb{Z}_s^k$ es el conjunto de vecindarios de k celdas. Un vecindario $(i_{k-1}, ..., i_c, ..., i_0)$ de $\mathbb{Z}_s^k$ se escribe como $i_{k-1}, ..., i_c, ..., i_0$ donde c indica la celda cambiante. Esto es, el valor $f_X(i_{k-1}, ..., i_c, ..., i_0)$ se coloca en la celda c en la siguiente configuración de la regla. A menudo, la aplicación local f_X se denotará con el mismo símbolo, X, que la regla global que define. Luego $f_X(i_{k-1}, ..., i_c, ..., i_0)$ se escribe $X(i_{k-1}, ..., i_c, ..., i_0)$.

En lo que sigue, salvo en algunas generalizaciones y ejemplos, se consideran autómatas binarios con $S = \{0, 1\}$. El conjunto $\{i_{k-1}...i_1i_0 | i_j \in \{0, 1\}\}$, ordenado de orden numérico descendente, se llama *conjunto de vecindarios de k celdas*. Si X es una regla de evolución de k celdas, los resultados de aplicarle X a los vecindarios se denominan las *componentes* de X con respecto del conjunto de vecindarios de k celdas. Se denotan por:

$$x_d = X(i_{k-1}...i_1i_0) \tag{1.1}$$

con d la forma decimal del valor binario $i_{k-1}...i_1i_0$. La expresión

$$X = (x_{2^k-1}...x_1x_0)$$

se llama la *forma componente* de X.

Wolfram introdujo la práctica de enumerar las reglas siguiendo la expresión decimal de su forma componente [1]. Si $X = (x_{2^k-1}...x_1x_0)$ esta expresión viene dada por

$$N(X) = \sum_{d=0}^{2^k-1} x_d 2^d. \tag{1.2}$$

Ejemplo. Se consideran la reglas de evolución de vecindarios simétricos de 3 celdas, con alfabeto $S = \{0, 1\}$. El conjunto de vecindarios de k celdas es $\{111, 110, 101, 100, 011, 010, 001, 000\}$. Para la regla particular con forma componente $X = (x_7x_6x_5x_4x_3x_2x_1x_0) = (01101010)$, la aplicación local tiene el conjunto imagen

$$f_X(\{111, 110, 101, 100, 011, 010, 001, 000\}) = \{0, 1, 1, 0, 1, 0, 1, 0\}.$$

De acuerdo con la nomenclatura de Wolfram la regla X se identifica por la expresión decimal de su forma componente $N(X) = \sum_{d=0}^{d=2^3-1} x_d 2^d = 106$.

∘

Es usual representar la evolución de un autómata celular unidimensional como si tuviera lugar en una superficie cuadriculada. Las celdas de la cuadrícula se colorean en correspondencia con los valores del conjunto de estados. La configuración inicial se inserta en la primera fila de la cuadrícula e iteraciones sucesivas del autómata se corresponden con la coloración consecutiva de filas de la cuadrícula, en orden descendiente. Véase la figura 1.1. Es importante notar que los patrones obtenidos representan toda la evolución temporal del autómata y no únicamente la configuración actual. Para representar la evolución de un autómata bidimensional se necesita entonces una "cuadrícula" de tres dimensiones, y así sucesivamente para dimensiones superiores.

1.1.1. Autómatas Celulares Elementales

En general, para un AC unidimensional se tienen s^k vecindarios, con s el número de estados y k la longitud de los vecindarios. La aplicación local asigna un valor del conjunto de estados a cada vecindario. De ahí se sigue que hay un total de $s^{(s^k)}$ aplicaciones locales, cada una definiendo una única regla de evolución $X : E \to E$.

Los autómatas celulares unidimensionales con conjunto de estados $S = \{0, 1\}$ y vecindarios simétricos de 3 celdas se denominan *Autómatas Celulares Elementales* (ACE). El número de vecindarios de 3 celdas con estados binarios es $2^3 = 8$, consecuentemente hay un total de $2^8 = 256$ reglas de ACE distintas. De acuerdo con la nomenclatura de Wolfram, cada una de estas reglas se identifica con la expresión decimal de su forma componente. Esto permite ordenar las 256 reglas de ACE, siendo $X = (00000000)$ y $X = (11111111)$ las reglas 0 y 255 respectivamente. Existen equivalencias entre las reglas que se obtienen intercambiando los roles de 0 y 1 y/o de izquierda y derecha en la expresión de la aplicación local. Si se considera un vecindario simétrico de 3 celdas $v = v_iv_cv_d$

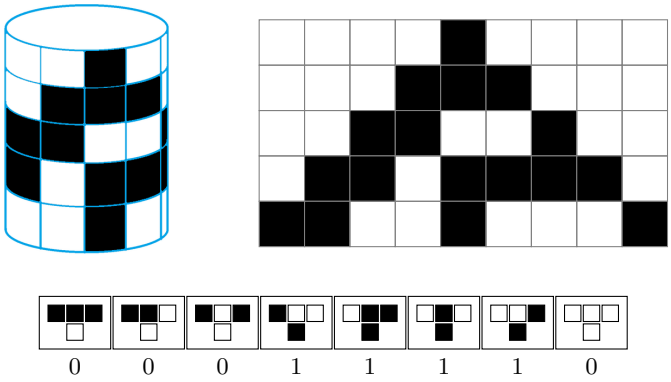

Figura 1.1: En el cilindro cuadriculado se representan 5 configuraciones consecutivas del autómata celular unidimensional, cilíndrico de longitud 9, definido por la regla de evolución $X = (00011110)$, $N(X) = 30$ en la nomenclatura de Wolfram. La fila superior corresponde a la configuración inicial $\mathbb{1}$. Debajo se representa la aplicación de vecindarios. Nótese que vecindarios de celdas adyacente no son disjuntos y comparten dos celdas. En la cuadrícula de la derecha se representa el mismo autómata. La vecina derecha de la celda en el extremo derecho es la celda del extremo izquierdo y viceversa.

se definen el *vecindario reflejado* por $\hat{v} = v_d v_c v_i$ y el *vecindario negativo* por $\bar{v} = 111 - v$. Esto da lugar a las siguientes definiciones:

Definición 1.1. *Sea X una regla de autómata celular elemental con aplicación local $f_X : \{v_7, ..., v_0\} \to \{0, 1\}$.*
*Se denomina **regla reflejada de** X a la regla de autómata celular elemental $\hat{X}$ cuya aplicación local viene dada por $f_{\hat{X}}(v) = f_X(\hat{v})$.*
*Se denomina **regla negativa de** X a la regla de autómata celular elemental $\bar{X}$ cuya aplicación local viene dada por $f_{\bar{X}}(v) = 1 - f_X(\bar{v})$.*
*Se denomina **regla complementaria de** X a la regla X^c definida por la negativa de la regla reflejada de X. La aplicación local es $f_{X^c}(v) = f_{\overline{\hat{X}}}(v) = 1 - f_X(\bar{\hat{v}})$.*

De las definiciones anteriores se sigue que, dada una regla de autómata celular elemental X expresada en la forma componente $X = (x_7x_6x_5x_4x_3x_2x_1x_0)$, las reglas reflejada, negativa y complementaria de X vienen dadas respectivamente por:

$$\begin{aligned} \hat{X} &= (x_7x_3x_5x_1x_6x_2x_4x_0), \\ \overline{X} &= 1 - (x_0x_1x_2x_3x_4x_5x_6x_7) \quad \text{y} \\ X^c &= 1 - (x_0x_4x_2x_6x_1x_5x_3x_7) \end{aligned}$$

Ejemplo. Se considera la regla 62 de autómata celular elemental. La forma componente de esta regla es $X = (00111110)$. Las reglas reflejada, negativa y complemento de la regla 62 vienen dadas por $\hat{X} = (01110110)$, $\bar{X} = (10000011)$ y $X^c =$

(10010001) correspondiendo a las reglas de ACE 118, 131 y 145 respectivamente. ○

Es una comprobación sencilla que, dada una regla X, el conjunto de reglas equivalentes $\{X, \hat{X}, \bar{X}, X^c\}$ es un conjunto cerrado en el sentido de que para cada regla del conjunto, las reglas reflejada, negativa y complemento están en el conjunto. Efectivamente se tiene que $\widehat{(\hat{X})} = X$, $\overline{(\bar{X})} = X$, $(X^c)^c = X$, etc. Este conjunto se denomina *conjunto de reglas equivalentes*. Véase la tabla de todas las reglas equivalentes A.1 en el apéndice del capítulo 1. Nótese que existen reglas tales que $\hat{X} = X$ y/o $\bar{X} = X$ y/o $X^c = X$. Las reglas equivalentes tienen la propiedad de que su "comportamiento" desde un punto de vista computacional es equivalente. El patrón generado por la regla reflejada a partir de una condición inicial simétrica puede verse como la reflexión a lo largo del eje vertical de simetría de la condición inicial. El patrón generado por la regla negativa corresponde al patrón generado por la regla original intercambiando los colores blanco y negro. Finalmente, la regla complemento corresponde a ambas inversiones. En la figura 1.2 se representan los cuatro patrones generados por las cuatro reglas equivalentes $\{62, 118, 131, 145\}$.

Nótese que la condición inicial considerada para las reglas 131 y 145 es la inversa de la condición inicial de una sola celda negra. Esto es debido a que las reglas negativas invierten el color tanto en el "input" como en el "output": una configuraición μ se transforma en la configurción ν tras un paso con una regla X si y solo si la configuración $\bar{\mu}$ se transforma en la configuración $\bar{\nu}$ tras un paso con la regla $\overline{X}$.

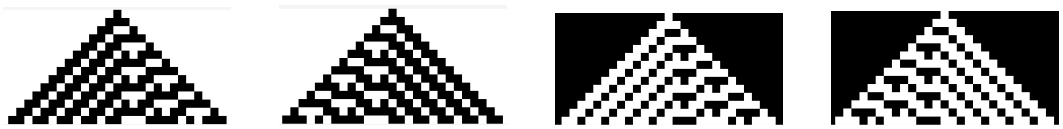

Figura 1.2: Patrones generados por las reglas 62, 118, 131 y 145 en orden de izquierda a derecha.

1.1.2. Patrones generados por AC Unidimensionales

La definición de algunas reglas de AC particulares en términos de la aplicación de vecindarios permite deducir ciertos aspectos del comportamiento a largo plazo de la regla. Por ejemplo: para las reglas triviales 0 y 255 es evidente que el patrón generado tendrá todas las celdas blancas tras una iteración con la regla 0, y todas negras con la regla 255. Para la regla 254, en su forma componente dada por $X = (11111110)$, es claro que, salvo partiendo de una condición inicial de celdas blancas, el patrón generado llegará a ser formado solo por celdas negras,

pues el único vecindario que genera celda blanca es $v_0 = 000$. Sin embargo, el número de reglas para las que se pueden deducir este tipo de predicciones es muy reducido. En general, dada una regla arbitraria, las cuestiones acerca de cómo evolucionará no pueden ser resueltas analizando su definición. Véase el *principio de irreductibilidad computacional* en el capítulo 12 de [1].

La implementación de los autómatas celulares en un ordenador surge de forma natural. Los códigos utilizados para la obtención de los patrones se encuentran en la ubicación web indicada en A.3. A continuación se muestran imágenes de los patrones generadas por varios autómatas celulares elementales.

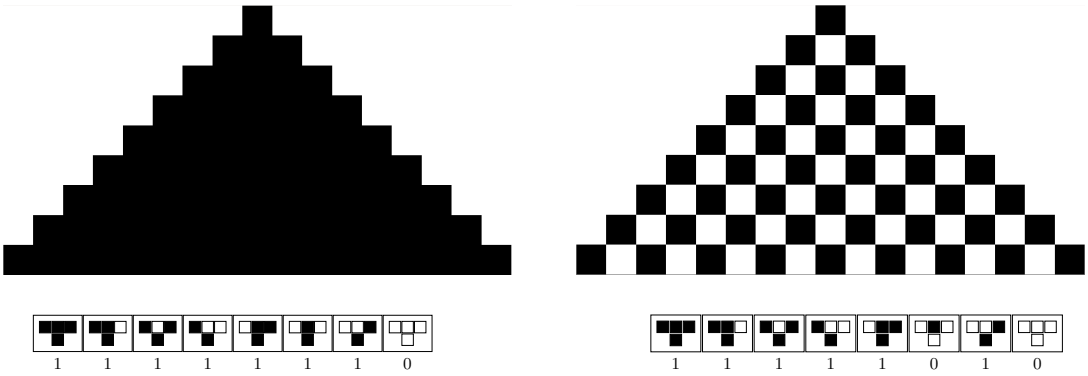

Figura 1.3: Regla 254 a la izquierda y regla 250 a la derecha. Ambas comenzando con una celda negra. Nótese que la aplicación de vecindarios solo difiere en un valor, sin embargo los patrones generados son cualitativamente diferentes.

La intuición podría llevar a creer que los patrones generados por sistemas con reglas tan sencillas como los autómatas celulares tendrán estructuras también simples. La figura 1.3, en la que muestran los patrones generados por las reglas 254 y 250, parece confirmar esta intuición. En ambas reglas la fracción de los de vecindarios que dan lugar a una celda negra tras una iteración es relativamente grande: $\frac{7}{8}$ y $\frac{6}{8}$ respectivamente. Quizá una distribución más equitativa entre vecindarios que dan lugar a celda negra y vecindarios que dan lugar a celda blanca tenga un efecto sobre el comportamiento de la regla. En la figura 1.4 se muestra la evolución de la regla 90. Nótese que el patrón generado es más complicado que en los casos anteriores, no obstante estos patrones también presentan estructura regular y simétrica.

Tras notar la estructura regular en los patrones anteriores se podría llegar a asumir que, al menos en los autómatas celulares con reglas tan sencillas como el caso de los elementales, siempre se obtendrán patrones regulares y simétricos a alguna escala. Sin embargo, esta conclusión sería equivocada.

El patrón generado por la regla 30 resulta notablemente más complejo que el generado por los ejemplos anteriores (véase la figura 1.5). Observando las primeras 25 iteraciones se descubre que la imagen no es simétrica, y que

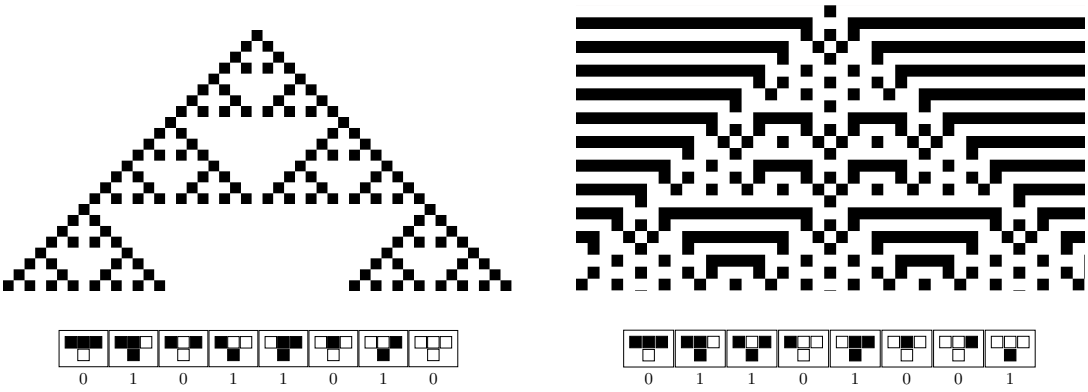

Figura 1.4: Regla 90 a la izquierda y regla 105 a la derecha. Ambas comenzando con una celda negra. En ambos casos la fracción de vecindarios que da lugar a una celda negra tras un paso es $\frac{1}{2}$. Para ambas reglas el patrón generado es notablemente más complicado que un patrón uniforme.

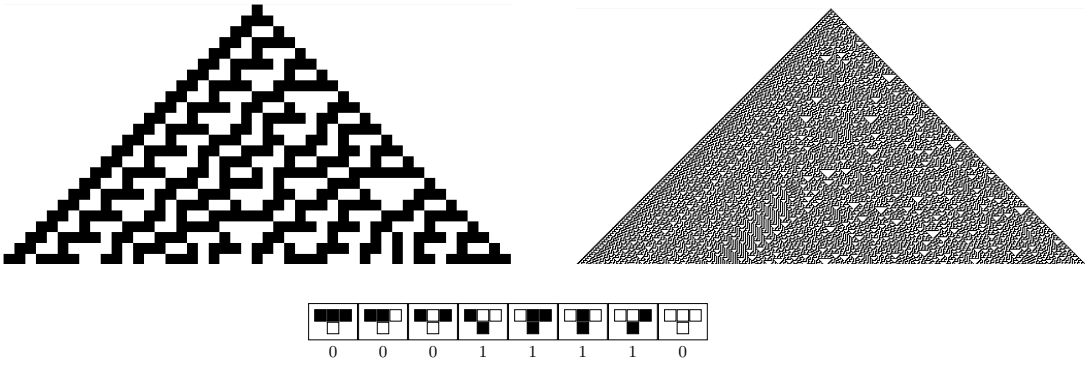

Figura 1.5: Patrón generado por la regla 30 partiendo de una celda negra. A la izquierda se muestra la evolución durante 25 pasos, a la derecha se muestran 250 pasos.

en el lado derecho presenta cierto comportamiento irregular mientras que en el lado izquierdo se detecta periodicidad en la estructura. Podría ser que la incapacidad de detectar estructura en el lado derecho se debe a que, tras 25 pasos, no "le ha dado tiempo" al autómata de generar un patrón regular. Sin embargo, analizando a simple vista el patrón generado por 250 iteraciones esto no parece ser el caso sino que, al contrario, parece que la irregularidad en la estructura es una propiedad inherente a la regla 30.

Es sorprendente que, a pesar de que las reglas subyacentes a estos sistemas son todas igual de sencillas en el sentido de que se necesita la misma cantidad de información para describirlas (asociar un valor a cada vecindario), presenten comportamientos globales tan diferentes. En principio, la regla 30 no es más que un caso particular de autómata celular elemental definido por un conjunto de transformaciones equivalentemente complejas que las de cualquier otra regla. No obstante, parece que las simetrías en las definiciones de la aplicación de

vecindarios de un autómata celular tiene un efecto sobre el aspecto del patrón generado. Nótese que en la regla 30, a diferencia de las anteriores, hay una "asimetría" en la definición de la aplicación local. El vecindario $v_6 = 110$ da lugar a celda blanca mientras que el reflejado $\hat{v}_6 = 011$ da lugar a celda negra. De las reglas vistas hasta el momento es la única que presenta este tipo de asimetría. ¿Serán estas asimetrías responsables de comportamientos como el de la regla 30? Para poder contestar este tipo de pregunta resulta necesario introducir primero una manera de clasificar los patrones de las reglas de AC unidimensional y concretar la idea de "comportamiento".

Las cuatro clases de Wolfram

En los anteriores ejemplos de patrones generados por autómatas celulares se ha considerado la configuración inicial que contiene una sola celda negra, siendo esta la condición inicial no trivial más sencilla. Aun partiendo de esta configuración con contenido de información bajo se ha visto que diferentes reglas generan patrones de distinta complejidad. ¿Qué ocurrirá si en lugar de la condición inicial sencilla anterior se comienza desde una configuración en la que celdas negras y blancas se distribuyen aleatoriamente? Quizá se esperaría que a partir de tal estado inicial desordenado los patrones generados seguirían pareciendo desordenados. En la figura 1.6 se tienen dos ejemplos de patrones que muestran que esto, al menos en general, no es el caso. ¿Será entonces que la evolución de un autómata celular induce orden en las configuraciones que alcanza? Observando la figura 1.7 se concluye que esto tampoco es siempre cierto.

Figura 1.6: Regla 250 a la izquierda y regla 108 a la derecha. Ambas comenzando de una configuración inicial aleatoria. Para ambas reglas el patrón generado muestra cierta organización. La regla 250 evoluciona hacia un patrón uniforme de todas las celdas negras. La regla 108 se ordena en estructuras locales estáticas o periódicas.

Se plantea ahora la cuestión de qué ocurrirá en la evolución de un autómata celular arbitrario. Si se observan las evoluciones de las 256 reglas diferentes de ACE resulta que, a pesar de que casi todas las reglas tienen alguna peculiaridad en el patrón que generan, el número de patrones fundamentalmente distintos es relativamente bajo. Wolfram introdujo la clasificación en cuatro clases de comportamiento, basadas en la observación "a simple vista" de los patrones generados por autómatas celulares y afirma que el estudio detallado de los autómatas

Figura 1.7: Regla 30 a la izquierda y regla 182 a la derecha. Ambas comenzando de una configuración inicial aleatoria. Para ambas reglas el patrón generado se mantiene desordenado indefinidamente y no se observa orden a escala global. Localmente se detecta cierto nivel de organización en la aparición de triángulos de celdas de un mismo color.

celulares revela que muchas de las propiedades estudiadas están estrechamente correlacionadas con esta clasificación. (Pág. 235 de [1]). Los cuatro tipos de reglas son los siguientes (véase la figura 1.8):

CLASE I: el comportamiento es muy simple y toda condición inicial lleva a un estado final uniforme.

CLASE II: hay diferentes estados finales pero todos consisten en un conjunto de estructuras simples que se repiten periódicamente.

CLASE III: los patrones generados son más complicados y parecen aleatorios a escala global a pesar de que siempre aparezcan estructuras como triángulos a alguna escala.

CLASE IV: las reglas presentan cierto nivel de organización y comportamiento aparentemente aleatorio. En los patrones generados por estas reglas aparecen estructuras sencillas a escalas pequeñas que interactúan y se desplazan a través del patrón de forma complicada.

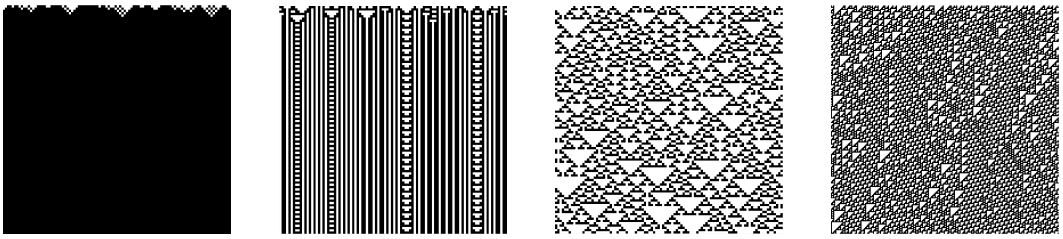

Figura 1.8: Representantes de las cuatro clases de Wolfram. Las reglas son 250, 94, 22 y 110 respectivamente representando las cuatro clases en orden creciente.

Una de las propiedades más sorprendente de las reglas de la clase IV es que son capaces de "imitar" cualquier otra regla si se imponen las condiciones iniciales adecuadas. Es más, como ya se ha mencionado anterioremente, se demuestra que la regla 110 resulta ser *Turing completa* y por lo tanto capaz de ejecutar cualquier proceso computacional. (Véase el capítulo 11 de [1]).

Es un hecho fundamental que la clasificación de Wolfram no se aplica solamente a los autómatas celulares elementales. Resulta que todos los AC uni-

dimensionales, independiente del número de estados posibles y del tamaño de vecindario, generan patrones que se pueden clasificar satisfactoriamente con estas mismas cuatro clases. Es notable que el aumento del número de configuraciones posibles no produce crecimiento en la complejidad de los sistemas en cuestión.

Se vuelve ahora a la cuestión planteada anteriormente: ¿será posible identificar aquellas reglas con comportamientos sencillos basado en la existencia de una expresión más sencilla para la aplicación de vecindarios? Nótese que tal expresión más sencilla de la aplicación f_X necesariamente restringe el conjunto de reglas. A continuación se describen estas posibles restricciones:

(1) Reglas que "no diferencian" entre vecina derecha y vecina izquierda.
La aplicación de vecindarios de estas reglas verifica $f_X(\hat{v}) = f_X(v)$. Para las reglas de ACE esto equivale a que $f_X(v_1) = f_X(v_4)$ y $f_X(v_3) = f_X(v_6)$. Dentro de estas, se diferencian los dos conjuntos de reglas con las siguientes restricciones :
   - (1.1) Reglas con aplicación de vecindarios verificando $f_X(v) = f_X(v_i v_c v_d) = f(v_i + v_c + v_d)$, esto es, que f_X se expresa en función de la suma de los valores de las tres celdas del vecindario. Equivalentemente son las reglas que verifican $f_X(v_1) = f_X(v_2) = f_X(v_4)$ y $f_X(v_3) = f_X(v_5) = f_X(v_6)$.
   - (1.2) Reglas con aplicación de vecindarios verificando $f_X(v) = f_X(v_i v_c v_d) = f(v_i + v_d)$. Por tanto, que f_X se expresa en función de la suma de los valores de las celdas izquierda y derecha del vecindario. En estas reglas la imagen a través de la aplicación de vecindarios no depende del valor de la celda cambiante, sino que solo depende de las celdas vecinas de la misma.

(2) Reglas en las que la aplicación de vecindarios f_X viene expresada en función de la celda cambiante y una única celda vecina. Se tienen las dos restricciones:
   - (2.1) $f_X(v) = f_X(v_c v_d)$ para todo vecindario v.
   - (2.2) $f_X(v) = f_X(v_i v_c)$ para todo vecindario v.

   Este conjunto particular de reglas de ACE equivalen a las reglas de autómata celular unidimensional con vecindarios de dos celdas.

En la columna *sim* de la tabla A.1 del apéndice se indican las reglas que verifican alguna o varias de las restricciones anteriores. Se observa que muchas de las reglas de clase III cumplen alguna restricción de simetría del tipo $f_X(\hat{v}) = f_X(v)$, luego la asimetría en la aplicación de vecindario no resulta fundamental para obtener el comportamiento de esta clase. Nótese, sin embargo, que ninguna de las reglas de la clase III cumple la condición de que la aplicación de vecindarios dependa solamente de la celda cambiante y una de las celdas vecinas. Esto es: los autómatas celulares unidimensionales, con conjunto de estados $\{0, 1\}$ y vecindarios de solo dos celdas, no son capaces de generar patrones aparentemente aleatorios. Por último se destaca que la regla 54 de clase IV presenta la simetría (1), luego nuevamente no es necesaria la asimetría en la aplicación de vecindarios para obtener comportamiento complejo.

2

Autómatas aditivos

En el capítulo anterior se introdujeron algunas de las diferencias de comportamiento que se detectan a simple vista, al comparar la evolución de varias reglas de autómata celular. A la vista de la clasificación de Wolfram, que distingue las reglas mayoritariamente por este criterio, podría concluirse que el interés de determinado autómata se reduce a estudiar un representante cualquiera de su clase. Se verá en lo que sigue que esto no es el caso.

Cuando se observan autómatas de la clase III, la característica más evidente es que, al menos localmente, generan patrones aparentemente aleatorios. Partiendo de condiciones iniciales aleatorias, muchos de los autómatas de esta clase generan patrones caóticos indistinguibles entre una regla y otra. Aunque en general la presencia de aleatoriedad en las condiciones iniciales no es una condición necesaria, por ejemplo con la regla 30 partiendo de una celda negra, muchas de las reglas de la clase III tienen comportamiento estructurado (de clase II) cuando parten de condiciones más sencillas. Véase la figura 2.1.

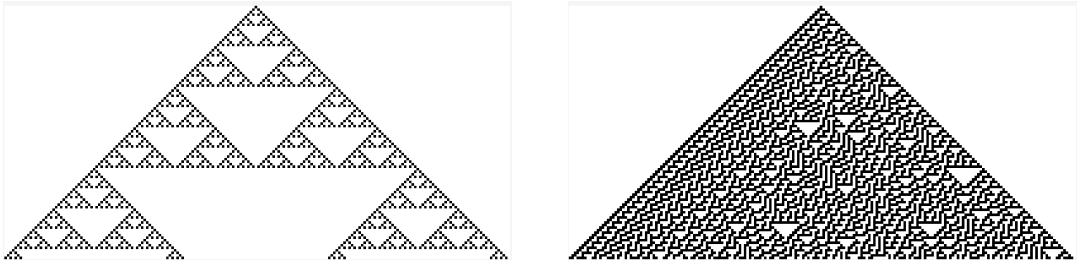

Figura 2.1: Regla 90 a la izquierda y regla 30 a la derecha. Ambas comenzando con una celda negra.

Anteriormente se ha visto que a partir de un comienzo aleatorio las reglas de clase III coinciden en su comportamiento aleatorio, al menos a simple vista. Ahora uno podría preguntarse por el umbral de aleatoriedad inicial para que esto ocurra. En la figura 2.2 se observa que la regla 22, partiendo de ciertas con-

diciones iniciales simples sigue desarrollando patrones estructurados parecidos a los que ocurren partiendo de una celda negra. Pero cambiando ligeramente el inicio, aun manteniéndolo sencillo, se obtiene la aleatoriedad característica de la clase III.

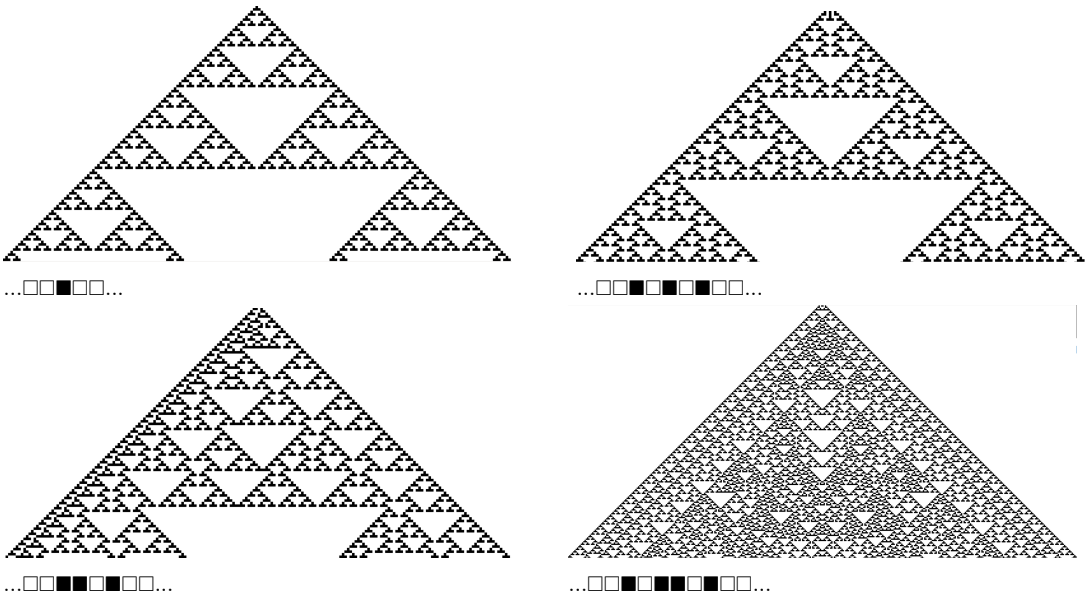

Figura 2.2: Regla 22 partiendo de diferentes condiciones iniciales simples.

Sin embargo, hay una serie de autómatas que desarrollan comportamiento aleatorio cuando parten de un inicio aleatorio, pero no se obtiene aleatoriedad significativa con condiciones iniciales sencillas.

Por ejemplo, en la regla 90, cuando la condición inicial involucra un número limitado de celdas negras, el patrón que produce siempre tiene una forma estructurada. Partiendo de una condición inicial simétrica, en las iteraciones en las que se genera un triángulo blanco en el centro, el patrón se divide en dos copias idénticas a ambos lados del triángulo central.

Este hecho se traduce en que la única forma de obtener configuraciones realmente aleatorias es partiendo de una condición inicial infinita con celdas negras distribuidas aleatoriamente, pues la regla 90 no genera aleatoriedad intrínsecamente. Más adelante se verá que la capacidad de algunas reglas de generar aleatoriedad a partir de condiciones simples es un fenómeno de mucho interés general.

Los comportamientos globales de las reglas 90 y 22 son distinguibles, incluso a simple vista. Partiendo de densidad baja de celdas negras, en la evolución de la regla 90 ocurren configuraciones con densidades notablemente más bajas que la media de generaciones anteriores y posteriores. La sensibilidad a las condiciones iniciales y la estructura distinguible son indicadores de que la regla 90 no es

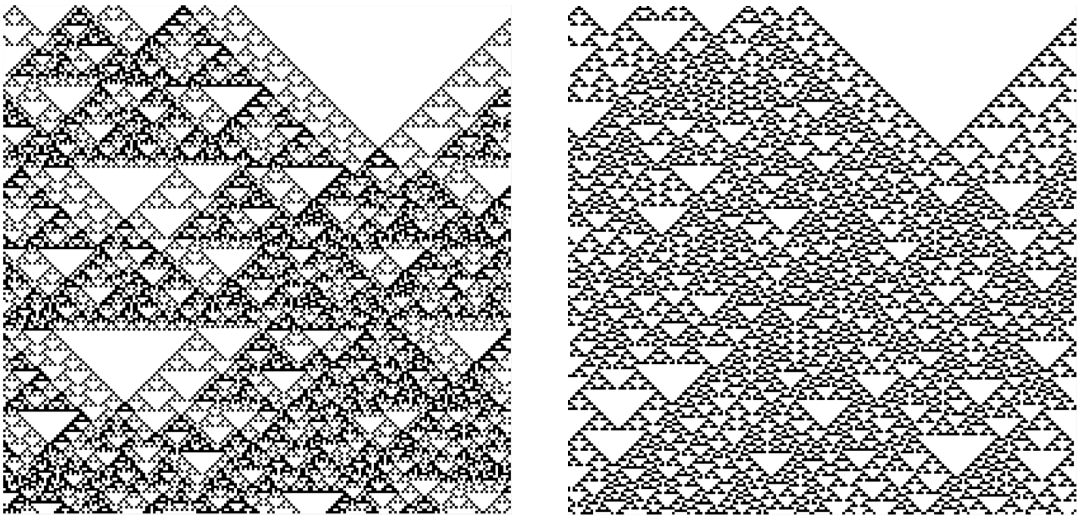

Figura 2.3: Regla 90 a la izquierda y regla 22 a la derecha. Ambas partiendo de la misma condición inicial con baja densidad de celdas negras.

igual de caótica que la 22. Este fenómeno no ocurre excepcionalmente para la regla 90, sino que es caracteístico de un conjunto particular: las reglas aditivas.

2.1. Análisis básico

Las reglas aditivas corresponden a un conjunto de autómatas celulares ampliamente estudiados. Se pueden definir en base a funciones locales sobre vecindarios más sencillas que el caso general de AC.

Martin, Odylzko, Wolfram y Jen obtuvieron numerosos resultados relacionados con puntos fijos, periodos de ciclos, alcanzabilidad de configuraciones, inyectividad y reversibilidad para el caso particular de reglas aditivas. En general, para la mayoría de autómatas no triviales, el estudio de estas propiedades resulta difícil.

2.1.1. Condiciones de Aditividad

La siguiente definición de autómata aditivo aparece en la mayor parte de la literatura. Algunos autores la intercambian con la definición de autómata lineal.

Definición 2.1 (Regla aditiva). *Una regla X es aditiva si*

$$X(\mu + \mu') = X(\mu) + X(\mu') \qquad \forall \mu, \mu' \in E \tag{2.1}$$

entendiéndose que aquí $+$ es la suma dígito a dígito módulo 2.

Ejemplo. Sea $X : E_5 \to E_5$ el operador correspondiente a la regla 150 (nomenclatura Wolfram). En su forma componente esta regla viene expresada por $X = (10010110)$.

Considerando las configuraciones $\mu, \mu' \in E_5$

$$\mu = [01010]$$
$$\mu' = [00100]$$

se tiene

$$X(\mu + \mu') = X([01110]) = [10101],$$

y por otra parte

$$X(\mu) + X(\mu') = [11011] + [01110] = [10101]$$

Nótese que todas las suma son dígito a dígito, y la aritmética es la modular en $\mathbb{Z}_2$. ∘

Si X es una regla de k celdas aditiva, en particular, la acción de X sobre la suma de vecindarios debe ser igual a la suma de las acciones de X sobre los vecindarios por separado. Esto es
$X(i_0...i_{k-1}) + X(j_0...j_{k-1}) = X(i_0...i_{k-1} + j_0...j_{k-1})$ para todos los vecindarios $(i_0...i_{k-1}), (j_0...j_{k-1})$. Equivalentemente, en forma de componentes respecto del conjunto de vecindarios

$$x_i + x_j + x_{i+j} = 0, \tag{2.2}$$

donde $i + j$ es la expresión decimal de la suma dígito a dígito de las formas binarias de i y j. Véase la definición de componentes de una regla en (1.1).

Para $k = 3$ la ecuación (2.2) se traduce en las condiciones no triviales

$$x_0 = x_1 + x_2 + x_3 = x_1 + x_4 + x_5 = x_1 + x_6 + x_7 = x_2 + x_4 + x_6$$
$$= x_2 + x_5 + x_7 = x_3 + x_4 + x_7 = x_3 + x_5 + x_6 = 0.$$

Tomando como ecuaciones independientes

$$x_0 = x_1 + x_2 + x_3 = x_1 + x_4 + x_5 = x_1 + x_6 + x_7 = x_2 + x_4 + x_6 = 0.$$

queda la forma general de reglas aditivas de 3 celdas

$$X = (0, x_1, x_2, x_1 + x_2, x_4, x_1 + x_4, x_2 + x_4, x_1 + x_2 + x_4). \tag{2.3}$$

Para las 2^3 posibles elecciones de $x_1, x_2, x_4 \in \{0, 1\}$ se obtienen todas las reglas aditivas de 3 celdas (tabla 2.1).

En lo que sigue, consideraremos generalmente el caso de reglas de 3 celdas con vecindarios simétricos sobre E_n. En este caso, la condición de aditividad puede expresarse como

$X = (x_0x_1...x_7)$	Wolfram	Suma de operadores
(00000000)	0	$\mathbf{0}$
(00001111)	240	σ^{-1}
(00110011)	204	$\mathbf{I}$
(01010101)	170	σ
(01100110)	102	$\mathbf{I} + \sigma$
(00111100)	60	$\sigma^{-1} + \mathbf{I}$
(01011010)	90	$\sigma^{-1} + \sigma$
(01101001)	150	$\sigma^{-1} + \mathbf{I} + \sigma$

Tabla 2.1: Reglas de 3 celdas aditivas

$$[X(\mu)]_i = \gamma\mu_{i-1} + \beta\mu_i + \alpha\mu_{i+1} \qquad \alpha, \beta, \gamma \in \mathbb{Z}_2. \tag{2.4}$$

El valor de la celda i-ésima de una configuración μ, tras una iteración con la regla X, corresponde a la combinación lineal con coeficientes en $\mathbb{Z}_2$ de los valores del vecindario de la celda. Equivalentemente se representa mediante la suma de operadores

$$X = \gamma\sigma^{-1} + \beta\mathbf{I} + \alpha\sigma, \tag{2.5}$$

siendo $\mathbf{I}$ el operador identidad sobre E_N.

Proposición 2.1 *Una regla de 3 celdas, de vecindarios simétricos y definida sobre E_n verifica la ecuación (2.2) si y solo si verifica la ecuación (2.5).*

Demostración. Se tiene por (2.3) que

$$X = x_4(00001111) + x_2(00110011) + x_1(01010101)$$

y por definición

$$\begin{aligned} \sigma^{-1} &= (00001111) \\ \sigma &= (01010101) \\ \mathbf{I} &= (00110011) \end{aligned}$$

Tomando $\gamma = x_4$, $\beta = x_2$, $\alpha = x_1$ se obtiene la equivalencia. □

2.1.2. Implicaciones de la Aditividad

Una consecuencia de la aditividad es que facilita el estudio de la longitud de ciclos y del conjunto de puntos fijos, esto es, de las configuraciones μ tales que $X(\mu) = \mu$.

Cualquier configuración inicial puede descomponerse en superposiciones de configuraciones iniciales que contienen una sola celda negra. La evolución de un autómata aditivo, partiendo de cualquier configuración, es igual a la superposición de las evoluciones por separado de estas configuraciones de una celda negra.

Se denota por $X^t(\mu)$ a la iteración sucesiva del operador X, t veces, partiendo de la configuración μ. De la definición de aditividad de una regla X dada en (2.2) se sigue que

$$X^t(\mu + \mu') = X^t(\mu) + X^t(\mu') \qquad \forall \mu, \mu' \in E. \tag{2.6}$$

Esta propiedad se denomina principio de superposición aditiva.

Ejemplo. En la figura 2.4 se tiene la evolución de la regla aditiva 60, partiendo de una sola celda negra y partiendo de una configuración inicial aleatoria con 54 celdas negras. Por la superposición aditiva se tiene

$$\begin{aligned} X^{128}(\mu) &= X^{128}(C_1 + C_2 + \cdots + C_{54}) = \\ &= X^{128}(C_1) + X^{128}(C_2) + \cdots + X^{128}(C_{54}) = \\ &= \underline{0} + \underline{0} + \cdots + \underline{0} = \underline{0} \end{aligned}$$

Aquí C_k denota la configuración con una celda negra correspondiente a la celda negra k-ésima en la configuración inicial μ.

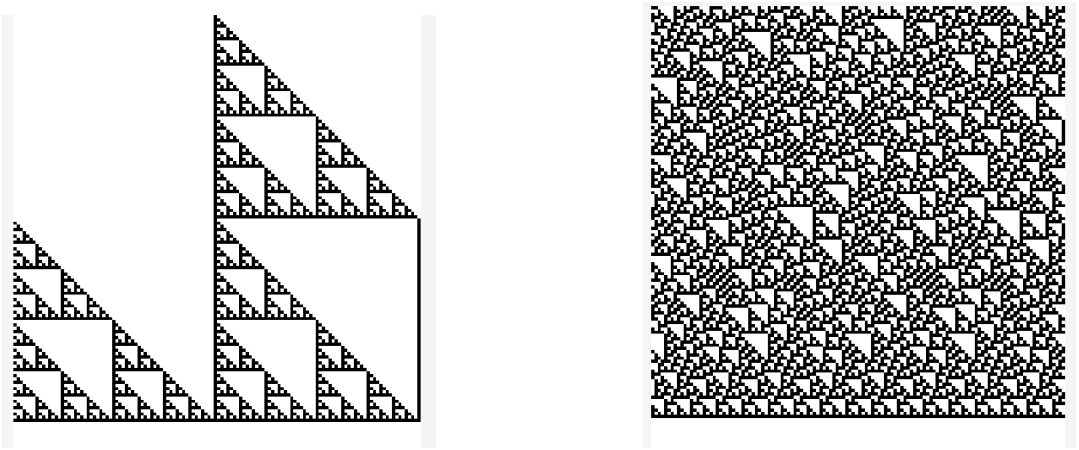

Figura 2.4: Regla 60: a la izquierda partiendo de una negra, a la derecha de configuración aleatoria. Ambas acaban en el punto fijo de la configuración nula.

Otra consecuencia de la superposición aditiva es la conservación de la longitud de ciclos para determinadas configuraciones iniciales. En la figura 2.5 se observa la evolución de la regla 150, partiendo de una celda negra y de una configuración aleatoria. En ambos casos se alcanza un ciclo de igual periodo.

Del principio de superposición aditiva se sigue que muchas cuestiones relativas a la evolución de las reglas aditivas se reducen al caso de una sola celda negra en la configuración inicial. Algunas de las preguntas que surgen de manera natural son las siguientes: ¿cuántas configuraciones son alcanzables? y ¿cuáles son?

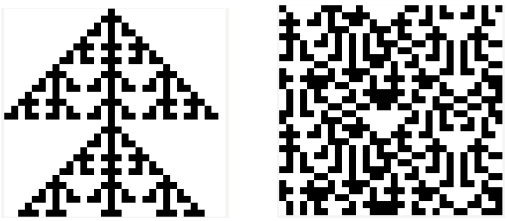

Figura 2.5: Regla 150: a la izquierda partiendo de una negra, a la derecha de configuración aleatoria.

¿De qué forma son los ciclos que ocurren en la evolución?, ¿qué configuraciones suponen puntos fijos?, etc.

En la siguiente sección se introducirán una serie de resultados relacionados con estas cuestiones para el caso particular de la regla 90. Por ejemplo se verá que no es excepcional que, partiendo de una configuración de 32 celdas, el ciclo generado tenga longitud la mitad de 32 (figura 2.5).

2.2. Propiedades algebraicas de las reglas aditivas. La regla 90.

En esta sección se introduce una notación alternativa para representar las configuraciones y la evolución de los autómatas celulares. Los formalismos y resultados que siguen se tomaron de [2]. Este artículo incluye un análisis extenso de las reglas aditivas, así como varios resultados de validez para el caso general.

Para el análisis particular de características de las reglas aditivas, conviene considerar las configuraciones en términos de polinomios llamados polinomios característicos. La evolución de un autómata se representa por multiplicaciones iteradas de estos polinomios característicos por polinomios fijos. Diversas propiedades algebraicas de los polinomios característicos son de utilidad al derivar resultados para las reglas aditivas.

En la primera subsección se introduce el formalismo correspondiente a la identificación de configuraciones con polinomios. Véase el apéndice para algunas aclaraciones sobre propiedades de divisibilidad y congruencia. En las siguientes subsecciones se obtienen resultados sobre longitud de ciclos, alcanzabilidad de estados y configuraciones de punto fijo, en particular para la regla 90.

2.2.1. Formalismo algebraico.

Se considera un autómata cilíndrico de N celdas, definido como un operador sobre el espacio de configuraciones E_N y con alfabeto $S = \{0, 1\}$. Una configuración $\mu(t) \in E_N$, queda determinada por los valores de las N celdas $a_0, a_1, ..., a_{N-1}$. Si $\mu(t) = [a_0^{(t)} a_1^{(t)} ... a_{N-1}^{(t)}]$ denota a la configuración del autómata

en el instante t de su evolución, esta puede ser representada por un polinomio característico

$$A^{(t)}(x) = \sum_{i=0}^{N-1} a_i^{(t)} x^i \tag{2.7}$$

siendo el valor de la celda i-ésima el coeficiente de x^i.

En lo que sigue será usual referirse a las configuraciones en términos de los polinomios característicos asociados y se escribirá $\mu \equiv A(x)$ para determinada configuración μ con polinomio característico asociado $A(x)$.

Multiplicar el polinomio característico por x coincide con la operación de desplazar los valores de la configuración una posición a la derecha, esto es, un paso con la regla desplazamiento a la derecha σ^{-1}. Análogamente, la multiplicación por x^{-1} corresponde con un paso con la regla desplazamiento a la izquierda σ.

Ejemplo. Considérese el autómata de longitud 7, con condiciones de frontera periódicas y con la regla desplazamiento a la derecha $X = \sigma^{-1}$. Sea la configuración $\mu = [1010110]$. El polinomio característico asociado es $A(x) = 1 + x^2 + x^4 + x^5$. Una iteración partiendo de la configuración μ resulta en $\sigma^{-1}(\mu) = [01010111]$.

$$\sigma^{-1}(\mu) \equiv xA(x) = x(1 + x^2 + x^4 + x^5) = x + x^3 + x^4 + x^6.$$

Figura 2.6: Un paso con la regla σ partiendo de $\mu = [1010110]$. Las posiciones de celdas negras coinciden con los coeficientes no nulos del polinomio característico.

○

Siguiendo esta representación, las configuraciones correspondientes a iteraciones sucesivas de las reglas de desplazamiento, y de las reglas aditivas en general, se representarán por "polinomios" que pueden contener potencias negativas y potencias mayores o iguales que N. Partiendo de la configuración del ejemplo anterior, un paso con la regla desplazamiento a la izquierda corresponde con

$$\sigma(\mu) \equiv x^{-1}(1 + x^2 + x^4 + x^5) = x^{-1} + x + x^3 + x^4.$$

Es conveniente considerar estos polinomios generalizados denominados dipolinomios. Se dirá que $H(x)$ es un dipolinomio si existe un entero m tal que $x^m H(x)$ es un polinomio.

Implementar las condiciones de frontera periódicas del autómata cilíndrico resulta en la reducción módulo N de los exponentes del dipolinomio asociado a una configuración.

Ejemplo. Considérese el autómata y la configuración inicial del ejemplo anterior. Tras dos iteraciones sucesivas se obtiene la configuración $\nu = (\sigma^{-1})^2(\mu) = [1010101]$. En términos de dipolinomios asociados la evolución se corresponde con

$$(\sigma^{-1})^2(\mu) \equiv x^2(A(x)) = x^2(1 + x^2 + x^4 + x^5) = x^2 + x^4 + x^6 + x^7$$

y el polinomio característico asociado a la configuración $(\sigma^{-1})^2(\mu)$ se obtiene reduciendo exponentes módulo 7:

$$(\sigma^{-1})^2(\mu) \equiv x^{2 \mod 7} + x^{4 \mod 7} + x^{6 \mod 7} + x^{7 \mod 7} = 1 + x^2 + x^4 + x^6.$$

Nótese que la configuración $(\sigma^{-1})^2(\mu)$ se identifica con el dipolinomio $x^2A(x)$ y con el polinomio característico obtenido tras reducir los exponentes módulo N. Ambas relaciones se denotan con el símbolo $\equiv$. Esta notación es consistente en el sentido de la congruencia de dipolinomios que se discutirá más adelante. ○

Para las reglas aditivas, la condición de aditividad dada en (2.4) se traduce en representar la evolución del autómata por la multiplicación por el dipolinomio fijo

$$\mathbb{T}(x) = \alpha x + \beta + \gamma x^{-1}. \tag{2.8}$$

Los coeficientes α, β y $\gamma \in \mathbb{Z}_2$ son los correspondientes a la regla aditiva en cuestión.

Como en el ejemplo anterior con las reglas de desplazamiento, siendo estas un caso particular de reglas aditivas, implementar la condición de frontera periódica resulta en la reducción módulo N de los exponentes del dipolinomio $A^{(t)}(x)$ obtenido tras un paso. Si $A^{(t-1)}(x) = \sum_{i=0}^{N-1} a_i x^i$ es el polinomio característico asociado a la configuración $(t-1)$-ésima, el dipolinomio asociado a la configuración obtenida tras un paso es

$$A^{(t)}(x) = \mathbb{T}(x)A^{(t-1)}(x) = (\alpha x + \beta + \gamma x^{-1}) \sum_{i=0}^{N-1} a_i x^i = \sum_{i=-1}^{N} b_i x^i$$

donde $b_i = (\gamma a_{i+1} + \beta a_i + \alpha a_{i-1})$ con $a_{-2} = a_{-1} = a_N = a_{N+1} = 0$. El polinomio característico asociado a la configuración t-ésima es entonces

$$\gamma a_0 x^{-1 \mod N} + \sum_{i=0}^{N-1} b_i x^i + \alpha a_{N-1} x^{N \mod N} = \sum_{i=0}^{N-1} c_i x^i$$

donde $c_i = b_i$ para $1 \leq i \leq N-2$, $c_0 = \alpha a_{N-1} + b_0$ y $c_{N-1} = \gamma a_0 + b_{N-1}$ lo que equivale a $c_i = \sum_{j \equiv i \mod N} b_j$ con $-1 \leq j \leq N$.

Si el polinomio característico asociado a una configuración inicial es $A^{(0)}(x)$, el dipolinomio asociado a la configuración k-ésima de la evolución de una regla aditiva viene dado por

$$A^{(k)}(x) = \mathbb{T}^k(x)A^{(0)}(x) = (\alpha x + \beta + \gamma x^{-1})^k A^{(0)}(x) = \sum_{i=-k}^{N+k} b_i x^i.$$

De la asociatividad de la suma en $\mathbb{Z}_N$ se sigue que la reducción de los exponentes módulo N del dipolinomio obtenido tras k pasos equivale a la reducción del dipolinomio obtenido en cada paso. En general se tiene que si $A(x)$ y $B(x)$ son dipolinomios y $A^*(x)$ y $B^*(x)$ los respectivos polinomios obtenidos tras la reducción módulo N de exponentes entonces

$$A^*(x)B^*(x) = (A(x)B(x))^*.$$

El polinomio característico asociado a la configuración k-ésima viene entonces dado por

$$A^{(k)}(x) = \sum_{i=0}^{N-1} c_i x^i \quad \text{con} \quad c_i = \sum_{j \equiv i \mod N} b_j.$$

En general, dada una configuración con dipolinomio asociado $\sum_j a_j x^j$, el polinomio característico asociado es

$$A(x) = \sum_{i=0}^{N-1} \left(\sum_{j \equiv i \mod N} a_j \right) x^i = \sum_{i=0}^{N-1} \left(\sum_j a_{i+jN} \right) x^i.$$

Una ventaja de la representación de configuraciones en términos de dipolinomios es que la condición de frontera periódica puede implementarse de forma escueta y natural. Resulta que la reducción módulo N de los exponentes de un determinado dipolinomio equivale a la reducción del mismo dipolinomio módulo $x^N - 1$. Si $D_{\mathbb{Z}_2}[x]$ denota el anillo de los dipolinomios con coeficientes en $\mathbb{Z}_2$, se considera la relación de congruencia módulo $x^N - 1$ que induce el conjunto cociente de clases de equivalencia $D_{\mathbb{Z}_2}[x]/(x^N - 1)$. Las propiedades de congruencia de los dipolinomios son análogas a las de los polinomios. Véase el apéndice del capítulo dos.

Se obtiene el polinomio característico como el único polinomio $A(x)$ de grado menor que N que verifica la congruencia de dipolinomios

$$\sum_j a_j x^j \equiv A(x) \mod (x^N - 1). \tag{2.9}$$

Se demuestra que todo dipolinomio es congruente módulo $(x^N - 1)$ a un único polinomio de grado menor que N (ver el apéndice A.2). Nótese que una

determinada configuración puede representarse por infinitos dipolinomios asociados. Configuraciones que estén en un ciclo aparecen repetidamente en la evolución de un autómata y, previo a la reducción módulo (x^N-1) , se representarán por dipolinomios diferentes. De la unicidad del polinomio que verifica (2.9) se deduce que dos dipolinomios corresponden a una misma configuración si y solo si son congruentes módulo (x^N-1).

Ejemplo. Considérese el autómata celular cilíndrico de longitud N definido por la regla 150. Partiendo de una configuración μ, el valor de la celda i-ésima tras un paso coincide con la suma módulo 2 de los valores de su vecindario. De acuerdo con (2.4) esto se denota por

$$[X(\mu)]_i = \mu_{i-1} + \mu_i + \mu_{i+1} \quad \text{mód } 2.$$

Si $A^{(0)}(x)$ es el polinomio característico asociado a la configuración μ, el dipolinomio $A^{(1)}(x)$ correspondiente a la configuración $X(\mu)$ es el resultado de multiplicar por el dipolinomio $\mathbb{T}(x) = x^{-1} + 1 + x$:

$$X(\mu) \equiv A^{(1)}(x) = \mathbb{T}(x)A^{(0)}(x) = (x^{-1} + 1 + x)A^{(0)}(x).$$

La periodicidad se traduce en que el polinomio característico asociado a $X(\mu)$ se obtiene reduciendo los exponentes de $A^{(1)}(x)$ módulo N.

Considérese la configuración $\mu = [110101]$ cuyo polinomio característico es $A^{(0)}(x) = 1 + x + x^3 + x^5$. Tras un paso se obtiene el dipolinomio

$$X(\mu) \equiv A^{(1)}(x) = (x^{-1} + 1 + x)(1 + x + x^3 + x^5) = x^{-1} + x + x^3 + x^5 + x^6.$$

El polinomio característico asociado a la configuración $X(\mu)$ es

$$X(\mu) \equiv x^{-1} \ {}^{\text{mód } 6} + x^1 \ {}^{\text{mód } 6} + x^3 \ {}^{\text{mód } 6} + x^5 \ {}^{\text{mód } 6} + x^6 \ {}^{\text{mód } 6} = x + x^3$$

y equivalentemente

$$X(\mu) \equiv x^{-1} + x + x^3 + x^5 + x^6 \quad \text{mód } (x^6 - 1) = x + x^3.$$

∘

2.2.2. La regla 90.

En esta sección se particulariza en el autómata celular correspondiente a la regla 90. Se consideran condiciones de frontera periódicas y longitud N. La función local que actualiza el valor de una celda en un determinado instante se define como la suma módulo 2 de los valores de las dos celdas vecinas en el instante anterior. Se consideran vecindarios de los dos vecinos más cercanos. El valor de la celda i-ésima tras un paso con la regla 90 viene dado por

$$[X(\mu)]_i = \mu_{i-1} + \mu_{i+1} \quad \text{mód } 2.$$

La evolución del autómata en términos de dipolinomios se representa por la multiplicación por el dipolinomio fijo

$$\mathbb{T}(x) = x^1 + x^{-1}. \tag{2.10}$$

Partiendo de la configuración inicial con una celda negra $\mathbb{1}$, al cabo de t iteraciones del autómata se obtiene la configuración de dipolinomio asociado

$$(\mathbb{T}(x))^t \mathbb{1} = (x^1 + x^{-1})^t \mathbb{1} = \sum_{i=0}^{t} \binom{t}{i} x^{2i-t}. \tag{2.11}$$

Ejemplo. Véase en la figura 2.7 la evolución de la regla 90, partiendo de una configuración con una celda negra y de longitud $N = 7$. La reducción módulo $x^N - 1$ corresponde a las condiciones de frontera periódicas. La configuración inicial de una celda negra se representa por el dipolinomio $A^{(0)}(x) = 0x^0 + 0x^1 + 0x^2 + 1x^3 + 0x^4 + 0x^5 + 0x^6$.

$\mathbf{x^0}$	$\mathbf{x^1}$	$\mathbf{x^2}$	$\mathbf{x^3}$	$\mathbf{x^4}$	$\mathbf{x^5}$	$\mathbf{x^6}$
0	0	0	1	0	0	0
0	0	1	0	1	0	0
0	1	0	0	0	1	0
1	0	1	0	1	0	1
1	0	0	0	0	0	1
1	1	0	0	0	1	1

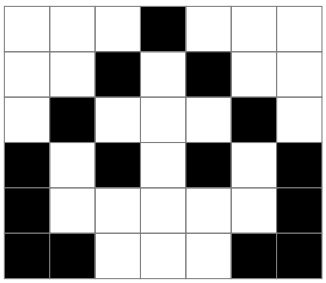

Figura 2.7: En la tabla de la izquierda se representan los coeficientes de los dipolinomios característicos de 6 configuraciones sucesivas de la regla 90 partiendo de una sola celda negra.

$$A^{(0)}(x) = x^3$$
$$A^{(1)}(x) = \mathbb{T}(x)A^{(0)}(x) = x^2 + x^4 \quad \text{mód } (x^7 - 1) = x^2 + x^4$$
$$A^{(2)}(x) = \mathbb{T}(x)A^{(1)}(x) = x^1 + x^5 \quad \text{mód } (x^7 - 1) = x^1 + x^5$$
$$A^{(3)}(x) = \mathbb{T}(x)A^{(2)}(x) = x^0 + x^2 + x^4 + x^6 \quad \text{mód } (x^7 - 1) = x^0 + x^2 + x^4 + x^6$$
$$A^{(4)}(x) = \mathbb{T}(x)A^{(3)}(x) = x^{-1} + x^7 \quad \text{mód } (x^7 - 1) = x^0 + x^6$$
$$A^{(5)}(x) = \mathbb{T}(x)A^{(4)}(x) = x^{-1} + x^1 + x^5 + x^7 \quad \text{mód } (x^7 - 1) = x^0 + x^1 + x^5 + x^6$$

○

Véase a continuación un primer resultado que muestra la utilidad de la representación en términos de polinomios característicos.

Proposición 2.2 *Sea $X : E_N \to E_N$ el autómata celular cilíndrico definido por la regla 90. Si $N = 2^j$, la configuración inicial de una celda negra evoluciona a la configuración nula tras exactamente 2^{j-1} iteraciones.*

Demostración. Sea la configuración inicial de una celda negra $\mathbb{1} = [100...0]$ con polinomio característico asociado

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

Una iteración con la regla 90 corresponde a la multiplicación del polinomio característico por el dipolinomio fijo $\mathbb{T}(x) = x^{-1} + x$.

Sea $X^{2^{j-1}}(\mathbb{1})$ la configuración del autómata tras 2^{j-1} iteraciones, entonces el dipolinomio característico asociado es

$$\begin{aligned} A^{(2^{j-1})}(x) = \mathbb{T}^{2^{j-1}}(x)A^{(0)}(x) = (x^{-1}+x)^{2^{j-1}}1 &= \sum_{i=0}^{2^{j-1}} \binom{2^{j-1}}{i} x^{2i-2^{j-1}} \\ &= \binom{2^{j-1}}{0} x^{-2^{j-1}} + \sum_{i=1}^{2^{j-1}-1} \binom{2^{j-1}}{i} x^{2i-2^{j-1}} + \binom{2^{j-1}}{2^{j-1}} x^{2^{j-1}} \\ &= x^{-2^{j-1}} + x^{2^{j-1}} = x^{-N/2} + x^{N/2} \equiv 0 \quad \text{mód } (x^N - 1), \end{aligned}$$

luego $X^{2^{j-1}}(\mathbb{1}) = \mathbb{0}$.

Supóngase que existe $0 < q < \frac{N}{2}$ tal que $X^q(\mathbb{1}) = \mathbb{0}$. Entonces

$$A^{(q)}(x) = (x^{-1} + x)^q 1 \equiv 0 \quad \text{mód } (x^N - 1),$$

y se sigue que existe un dipolinomio $P(x) = x^{p_1} + x^{p_2} + \cdots + x^{p_k}$ tal que

$$(x^{-1} + x)^q = (x^N - 1)P(x).$$

Si $Q(x) = \sum_{i=1}^{q-1} \binom{q}{i} x^{2i-q}$ la igualdad anterior queda

$$x^{-q} + x^q + Q(x) = x^{N+p_1} + x^{N+p_2} + \cdots + x^{N+p_k} - x^{p_1} - x^{p_2} - \cdots - x^{p_k}.$$

Luego existe p_i tal que $q = N + p_i$ o $q = p_i$, pero

$$q = N + p_i \implies p_i = q - N < \frac{-N}{2} < -q$$

$$q = p_i \implies N + p_i > q$$

concluyendo ambas posibilidades en un absurdo, pues q y $-q$ son el mayor y menor exponente del dipolinomio $(x^{-1}+x)^q$ respectivamente.

Se concluye que $\frac{N}{2}$ es el menor número de iteraciones que transforma la configuración de una celda negra en la configuración nula. La configuración nula es un punto fijo, luego $X^k(\mathbb{1}) = \mathbb{0}$ para todo $k \geq \frac{N}{2}$.

□

Corolario 2.1 *Sea $X : E_N \to E_N$ el autómata celular cilíndrico definido por la regla 90. Si $N = 2^j$, toda configuración inicial evoluciona a la configuración nula tras un máximo de 2^{j-1} iteraciones.*

Demostración. Sea μ una configuración inicial cualquiera, entonces, si $\mathbb{1}^i$ denota la configuración de una celda negra en la posición i-ésima, se tiene que

$$\mu = \sum_{i=0}^{N-1} \mu_i \mathbb{1}^i. \tag{2.12}$$

Por la proposición anterior se tiene que $X^k(\mathbb{1}^i) = \mathbb{0}$ para todo $k \geq \frac{N}{2}$. Del principio de superposición aditiva se sigue que

$$X^k(\mu) = \sum_{i=0}^{N-1} \mu_i X^k(\mathbb{1}^i) = \mathbb{0} \quad \forall k \geq \frac{N}{2}.$$

□

Ejemplo. En la figura 2.7 se muestra la evolución del autómata definido por la regla 90 y con longitud $N = 2^5$. Al cabo de 2^4 iteraciones se alcanza el punto fijo de la configuración nula.

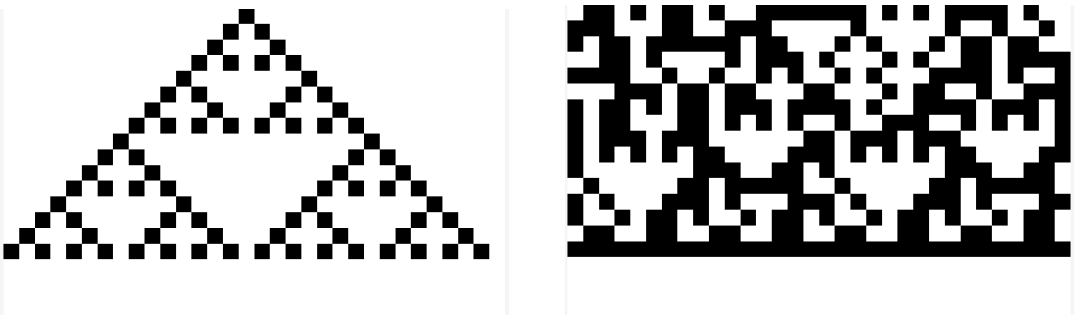

Figura 2.8: A la izquierda, la regla 90 partiendo de una configuración con una celda negra. A la derecha partiendo de una configuración inicial aleatoria. En ambos casos la longitud del autómata es 2^5.

○

En la evolución del autómata celular definido por la regla 90 existen configuraciones que evolucionan a una misma configuración tras un paso. Esto es, la regla 90 es irreversible. Equivalentemente la aplicación $X : E_N \to E_N$, que define el autómata celular cilíndrico con la regla 90, no es inyectiva.

La irreversibilidad de la regla 90 y el número finito de configuraciones posibles implica que no todas las configuraciones posibles aparecen en la evolución del autómata. A continuación se tienen varios resultados sobre el número configuraciones alcanzables, sucesores y predecesores de configuraciones.

Proposición 2.3 *Sea $X : E_N \to E_N$ el autómata celular cilíndrico definido por la regla 90. Toda configuración con un número impar de celdas negras solo puede aparecer como configuración inicial en la evolución de X.*

Demostración. Sea $\nu = X(\mu)$ la configuración obtenida tras un paso partiendo de una configuración μ cualquiera. Sea t tal que μ es la t-ésima configuración en la evolución partiendo de cierta configuración inicial. Entonces $A^{(t)}(x)$ es el polinomio característico asociado a μ y el dipolinomio correspondiente a la configuración ν viene dado por

$$A^{(t+1)}(x) = (x^{-1} + x)A^{(t)}(x).$$

Se tiene que $(x^{-1} + x) \equiv (1 + x^2) \mod (x^N - 1)$. De la propiedad 1 (Apéndice capítulo 2) se sigue que

$$(x^{-1} + x)A^{(t)}(x) \equiv (1 + x^2)A^{(t)}(x) \mod (x^N - 1),$$

luego

$$A^{(t+1)}(x) = B(x)(x^N - 1) + (1 + x^2)A^{(t)}(x),$$

para cierto dipolinomio $B(x)$. Entonces se tiene que $A^{(t+1)}(1) = 0$. Esto es que ν contiene un número par de términos y corresponde con una configuración con un número par de celdas negras. □

En la figura izquierda de 2.8 se tiene la evolución de la regla 90 partiendo de la configuración inicial de una celda negra. Se observa que el número de celdas negras es par en toda configuración, excepto la inicial. De la superposición aditiva se sigue que toda configuración que ocurre en la evolución de la regla 90, partiendo de cualquier configuración inicial $\mu = \sum_i \mu_i \mathbb{1}^i$, equivale a la superposición de las configuraciones alcanzadas en la evolución por separado, a partir de las configuraciones $\mathbb{1}^i$.

El siguiente es un resultado sobre el número de configuraciones que pueden ocurrir en la evolución del autómata definido por la regla 90. Las demostraciones de los resultados siguientes se tienen en el anexo externo indicado en A.3.

Proposición 2.4 *Sea $X : E_N \to E_N$ el autómata celular cilíndrico definido por la regla 90. El número de configuraciones que pueden ser alcanzadas en la evolución de X es $\frac{1}{2}2^N$ para N impar y $\frac{1}{4}2^N$ para N par.*

Lema 2.1 *Sea $X : E_N \to E_N$ el autómata celular cilíndrico definido por la regla 90. Sean dos configuraciones μ y ν con polinomios característicos asociados $A(x)$ y $B(x)$ respectivamente. $X(\mu) = X(\nu)$ si y solo si $A(x) = B(x) + Q(x)$ tal que $\mathbb{T}(x)Q(x) \equiv 0 \mod (x^N - 1)$.*

Proposición 2.5 *Sea $X : E_N \to E_N$ el autómata celular cilíndrico definido por la regla 90. Configuraciones que ocurren en la evolución del autómata tras al menos un paso tienen exactamente dos predecesoras para N impar y exactamente cuatro para N par.*

De la proposición 2.5 puede inferirse la ya mencionada irreversibilidad del autómata definido por la regla 90. Nótese que toda configuración tiene más de una configuración predecesora y evoluciones que parten desde estas son indistinguibles tras un paso. Así puede decirse que, en general, se produce una pérdida de la información inicial en la evolución de la regla 90. Véase en la figura 2.9 las evoluciones partiendo de las cuatro predecesoras de una configuración determinada.

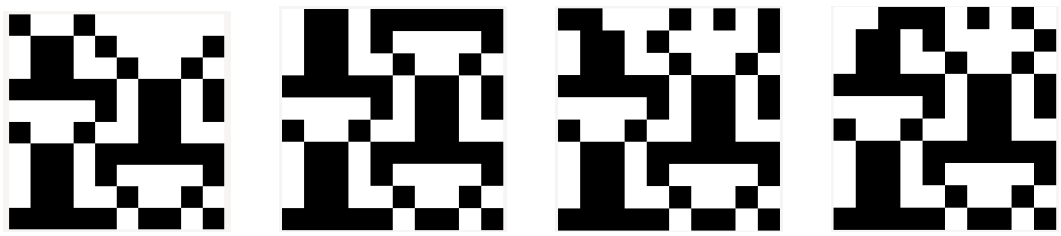

Figura 2.9: Regla 90 partiendo de las configuraciones $\mu = [1001000000]$, $\mu + [1111111111]$, $\mu + [0101010101]$ y $\mu + [1010101010]$ respectivamente.

2.2.3. Diagrama de transición de estados.

El *diagrama de transición de estados* (DTE) de un autómata celular es un grafo cuyos nodos representan las posibles configuraciones que ocurren en la evolución del autómata. Los arcos dirigidos que unen nodos representan la transición entre configuraciones correspondientes a un paso. Dado que toda configuración tiene una sola configuración sucesora, exactamente un arco sale de cada nodo. Esto es, el grado interior de cada nodo es uno. De acuerdo con lo mencionado en la sección anterior, en general el número de predecesores es diferente para configuraciones distinas. Por lo tanto, el grado interior de nodos distintos del DTE puede ser diferente. De las proposiciones 2.4 y 2.5 se sigue que para N impar, la mitad de todos los nodos tienen grado interior cero y la otra mitad tienen grado interior dos, mientras que para N par tres cuartos de los nodos tienen grado interior cero y el cuarto restante grado interior cuatro.

De la finitud del número de configuraciones posibles, se deduce que todo autómata celular cilíndrico, partiendo de cualquier configuración inicial, evoluciona hacia un ciclo tras un número finito de pasos. La secuencia de configuraciones que corresponde a la evolución desde una determinada configuración inicial hasta la primera configuración del ciclo se denomina *transición*.

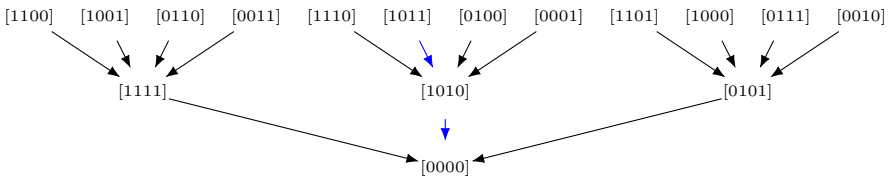

Figura 2.10: Diagrama de transición de estados del autómata celular cilíndrico definido por la regla 90, con $N = 4$. En azul la transición desde la configuración inicial [1011] hasta el punto fijo [0000].

Proposición 2.6 *Los árboles arraigados en todos los nodos de todos los ciclos del diagrama de transición de estados del autómata celular definido por la regla 90 son idénticos.*

Proposición 2.7 *Para N impar, hay un árbol de un solo arco arraigado en cada nodo de cada ciclo del diagrama de transición de estados del autómata celular cilíndrico definido por la regla 90.*

La *distancia* entre nodos de un árbol arraigado se define como el número de arcos que son visitados en la transición de un nodo al otro. La *altura* de un árbol arraigado es la máxima de las distancias entre los nodos terminales y la raíz. Se dice que un árbol es *equilibrado* si todos los nodos terminales están a la misma distancia de la raíz. Un árbol se dice *cuaternario* (resp. *binario*) si todos los nodos no terminales tienen grado interior cuatro (resp. dos).

Sea $D_2(N)$ la máxima potencia de dos que divide a N.

Proposición 2.8 *Para N par, hay un árbol equilibrado de altura $D_2(N)/2$ arraigado en cada nodo de cada ciclo del diagrama de transición de estados del autómata celular cilíndrico definido por la regla 90. Los árboles son cuaternarios, excepto que las raíces tienen grado interior tres.*

Corolario 2.2 *Para N impar, la mitad de las 2^N configuraciones posibles en la evolución del autómata celular cilíndrico definido por la regla 90 pueden ocurrir después de una o más iteraciones. Para N par, $\frac{1}{4^t}$ de las 2^N configuraciones posibles ocurren después de $t \leq D_2(N)/2$ iteraciones y el número de configuraciones que ocurren en ciclos es $2^{N-D_2(N)}$.*

Los resultados anteriores proporcionan información relevante acerca de la estructura del diagrama de transición de estados del autómata considerado en esta sección. Para una descripición completa del mismo, sin embargo, deben conocerse las multiplicidades y longitudes de todos los ciclos que ocurren en la evolución. Las tres proposiciones siguientes proporcionan cotas superiores para las longitudes de ciclos diferentes en dependencia de N. Véase [2] para la descripicón de un algoritmo que permite determinar las multiplicidades y longitudes de todos los ciclos que ocurren en la evolución del autómata en cuestión.

Proposición 2.9 *Las longitudes de todos los ciclos que ocurren en la evolución del autómata celular cilíndrico definido por la regla 90 dividen a la longitud Π_N del ciclo alcanzado a partir de la configuración inicial de una celda negra.*

Nótese que la longitud del ciclo alcanzado a partir de una configuración de una celda negra es la máxima, pues todo ciclo tiene longitud divisor de la misma. En el caso de que N sea primo las únicas longitudes de ciclos posibles son Π_N y 1.

El corolario que sigue se deduce inmediatamente de la proposición 2.2. Las demostraciones de las proposiciones 2.10 y 2.11 se dan en [2].

Corolario 2.3 *Para $N = 2^j$, el autómata celular cilíndrico definido por la regla 90 evoluciona a un ciclo de longitud uno.*

Proposición 2.10 *Para el autómata celular cilíndrico definido por la regla 90 con N par pero no de la forma 2^j, se tiene $\Pi_N = 2\Pi_{N/2}$.*

Proposición 2.11 *Para el autómata celular cilíndrico definido por la regla 90 con N impar se tiene $\Pi_N | (2^{\mathrm{sub}_2(N)} - 1)$ siendo $\mathrm{sub}_2(N)$ el mínimo entero tal que $2^{\mathrm{sub}_2(N)} = \pm 1 \mod N$.*

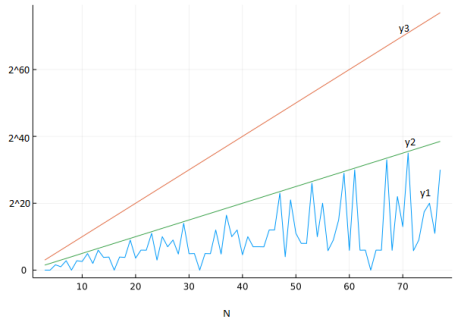

Figura 2.11: $y1 : \Pi_N$, $y2 : 2^{\frac{N-1}{2}} - 1$, $y3 : 2^N$. Los picos de la función Π_N coincidentes con $y2$ se dan para todo valor de N primo, excepto 17,31,41,43 y 73.

En la gráfica de la figura 2.11 se representan las longitudes de los ciclos máximos Π_N para el autómata celular considerado en esta sección. Se comprueba

que para casi todo N, $\Pi_N = 2^{\text{sub}_2(N)} - 1$. La única excepción para $N = 3, ..., 80$ se da en $N = 37$ con $\Pi_N = \frac{2^{\text{sub}_2(37)}-1}{3}$. Los valores máximos de Π_N están acotados por $2^{\frac{N-1}{2}}$. Se demuestra que la función $\text{sub}_2(N)$ está acotada superiormente por $\frac{N-1}{2}$ y si $\text{sub}_2(N) = \frac{N-1}{2}$ entonces N es primo.

Dada la información conjunta acerca de la estructura de los árboles arraigados en los ciclos y las longitudes y multiplicidades de los mismos, es posible determinar la topología del diagrama de transición de estados para determinado N. Véanse las figuras 2.12 y 2.13 siguientes.

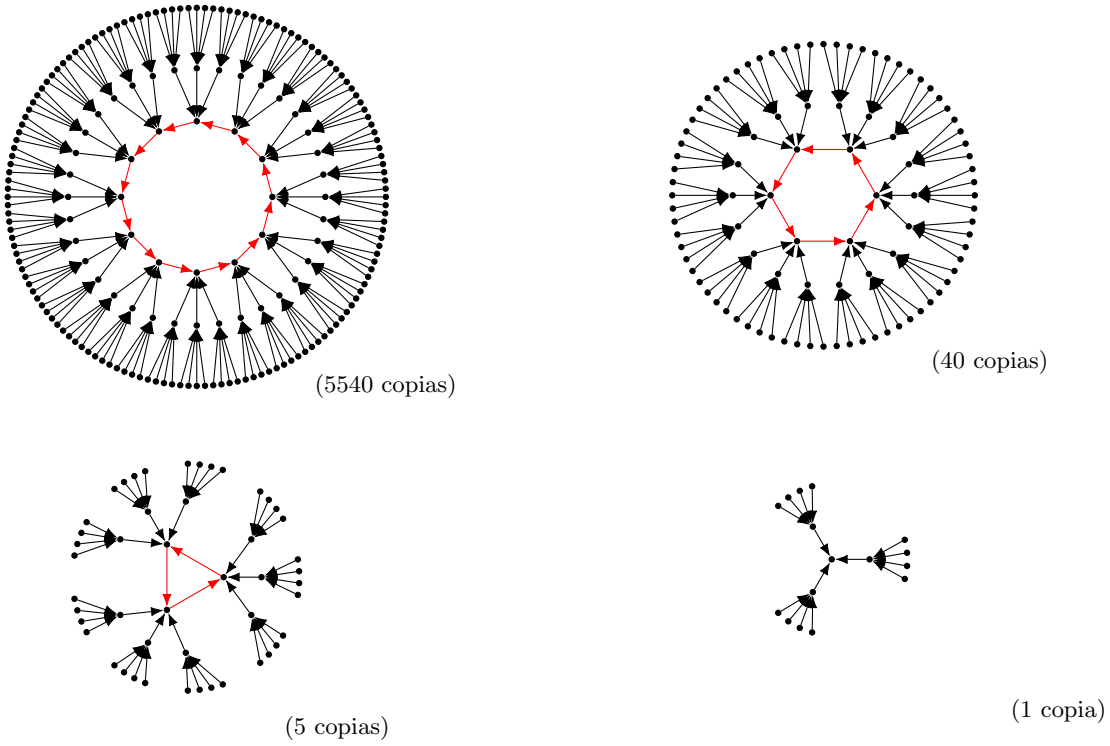

Figura 2.12: Diagrama de transición de estados del autómata cilíndrico definido por la regla 90 con longitud $N = 20$.

2.3. Conclusión y generalizaciones

Mediante el análisis algebraico de la regla 90 se han podido deducir propiedades no triviales relacionadas con la longitud de evolución de la regla y con particularidades de las configuraciones posibles. De la observación de un número considerable de evoluciones de la regla 90, se puede conjeturar la existencia de resultados como la proposición 2.2 y el corolario 2.1 correspondiente, y de las

Figura 2.13: Diagrama de transición de estados del autómata cilíndrico definido por la regla 90 con longitud $N = 31$.

proposiciones sobre longitudes de ciclos. Los resultados sobre el número de configuraciones posibles y particularidades de las mismas no parecen ser reconocibles por simple observación del patrón generado en la evolución. La aleatoriedad aparente, característica de la regla 90 y en general de las reglas de clase III, resulta ser algo "engañosa", pues le oculta a un observador poco cuidadoso que, por ejemplo, no hay configuraciones con número impar de celdas negras. Otra propiedad notable de la regla 90 como caso particular de las reglas aditivas, es la simetría del diagrama de transición de estados, que indica que la estructura de la evolución depende en mayor medida de la longitud N que de la configuración inicial particular.

Un análisis análogo al presentado puede realizarse con la regla 150. Véase [5]. Es posible la generalización de los procedimientos algebraicos para el caso de reglas aditivas con p colores para $|S| = p$ número primo. Véase la sección 4 de [2] donde se obtienen numerosos resultados para auómatas celulares aditivos en dimensión superior y con $|S| > 2$.

La aditividad de las reglas consideradas previamente permiten "adelantarse" a la evolución del autómata. El tiempo de computación necesario para conocer el estado de una determinada celda tras t iteraciones por medio de simulación directa de un autómata celular es de $O(t^2)$. En [8] se deriva un algoritmo que computa el valor de determinada celda en tiempo $O(\log t)$ para las reglas aditivas.

3

Propiedades estadísticas de los autómatas celulares. Secuencias pseudoaleatorias generadas por la regla 30.

La ocurrencia de patrones no triviales en la evolución de los autómtas celulares considerados es un fenómeno destacado que se puede apreciar en varias de las imágenes de los capítulos anteriores. Analizando a simple vista un número considerable de estos patrones, se solidifica la intuición de que, a pesar de ser gobernados por reglas simples, deterministas y que actúan a nivel local de vecindarios, muchos autómatas celulares elementales generan cierto comportamiento aleatorio, al menos aparentemente. La complejidad y en particular la "aleatoriedad" emergente que se observa, se han considerado propiedades fundamentales para la clasificación de las reglas (CLASES III y IV, de acuerdo con [1]).

Distintas reglas de clase III muestran diferencias notables de comportamiento. Por ejemplo las "granulosidades"de los patrones se distinguen a simple vista, siendo posible reconocer con bastante certeza algunas reglas particulares a partir de su patrón. Por otro lado, muchas reglas se diferencian en su manejo de la información acumulada en su condición inicial. Ocurre que, por ejemplo, la regla 30 genera comportamiento aparentemente aleatorio a partir de la condición inicial de una sola celda negra. Otras reglas tienen la capacidad de generar "aleatoriedad" únicamente a partir de condiciones iniciales desordenadas. Hay reglas que amplifican el desorden inicial, y otras, tales como las aditivas presentadas en el capítulo anterior que, a pesar de desarrollar comportamiento caótico a partir de condiciones iniciales aleatorias, permiten la predicción de algunos aspectos por medio de su análisis algebraico. La parte final del capítulo se dedica al estudio de la secuencia generada por la columna central de la regla 30, que fue utilizada como generador pseudoaleatorio de números naturales grandes [4].

3.1. Propiedades locales

Una configuración se puede considerar aleatoria cuando los estados de celdas diferentes no están estadísticamente correlacionados. De la comparación cualitativa del patrón generado por un autómata celular, con una malla de celdas a las que se asignan valores aleatoriamente, se deduce que la evolución de todo

autómata celular a partir de una configuración inicial aleatoria lleva a cierta medida de "autoorganización". En la figura 3.1 se compara una parte del patrón generado por la regla 30 con una malla en la que se han coloreado celdas aleatoriamente con una probabilidad de un medio, generando un patrón denominado *ruido blanco*.

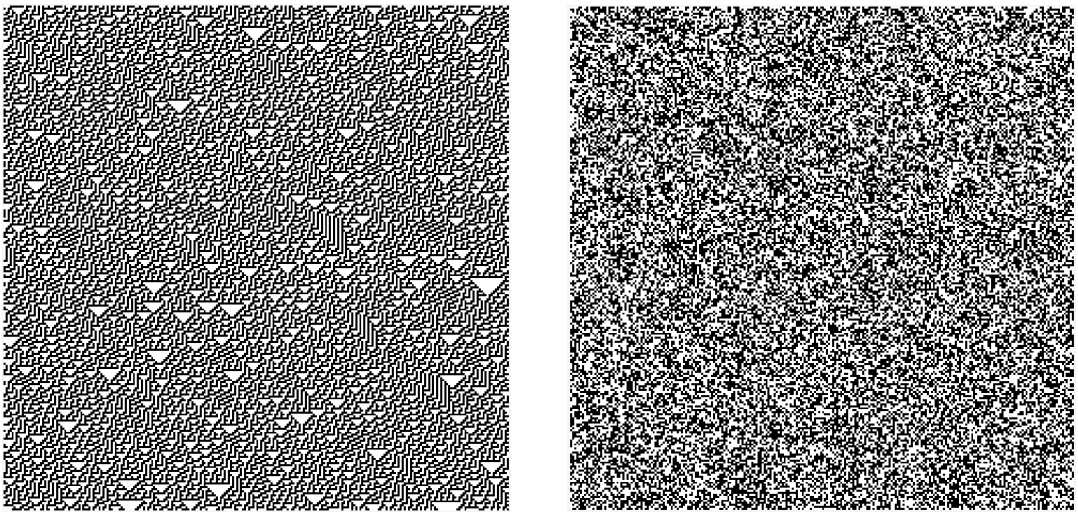

Figura 3.1: Regla 30 a la izquierda y *ruido blanco* a la derecha. En ambos patrones la fracción de celdas negras es aproximadamente un medio. La correlación inducida por la evolución de la regla 30 genera estructura que la distingue de un patrón totalmente uniforme.

Uno de los parámetros cuantitativos más elementales que caracteriza una configuración de autómata celular es la fracción de celdas negras denotada por ρ. Será usual referirse a esta cantidad como densidad de celdas negras o solamente densidad. Para una configuración aleatoria (de longitud infinita) la densidad viene dada por la probabilidad independiente p de cada celda de ser negra. Nótese que se requieren de configuraciones de longitud infinita para garantizar la igualdad entre los parámetros p y ρ. Alternativamente podría considerarse que ρ denota la densidad o fracción media de celdas negras de infinitas configuraciones. En lo que sigue se considerarán configuraciones de longitud infinita.

Considérese la densidad ρ_1 obtenida tras un paso con determinado autómata celular, partiendo de una configuración inicial aleatoria con densidad $\rho_0 = 1/2$. Tal configuración inicial contiene todos los vecindarios con igual probabilidad y consecuentemente la densidad en la configuración obtenida tras un paso viene dada por la fracción de vecindarios correspondiente a la regla que generen celda negra. Esta fracción viene dada por

$$\rho_1 = n_1(X)/8$$

donde $n_1(X)$ denota al número de unos en la expresión binaria de la regla X. De acuerdo con la enumeración de reglas introducida anteriormente, $n_1(X)$ coincide con el número vecindarios que generan celda negra en la regla X.

Para configuraciones iniciales con probabilidad de celdas negras $p \neq \frac{1}{2}$, vecindarios con diferente número de celdas negras dejan de ser equiprobables. La probabilidad de un vecindario v (de 3 celdas) con $n_1(v)$ celdas negras viene dada por $P(v) = p^{n_1(v)}(1-p)^{n_0(v)}$, con $n_0(v) = 3 - n_1(v)$. Partiendo de una configuración inicial aleatoria de densidad ρ_0, después de un paso con determinado autómata celular X se obtiene una configuración con densidad

$$\rho_1 = \sum_{i \in I} P(v_i) \quad \text{donde} \quad P(v_i) = \rho_0^{n_1(v_i)}(1-_0)^{n_0(v_i)} \tag{3.1}$$

y con I el conjunto de índices de los vecindarios que generan celda negra en la regla X. Si X_i denota el i-ésimo dígito en la expresión binaria de X, $I = \{i \in \{1, ..., 8\}/X_i = 1\}$.

Ejemplo. Sea el autómata celular definido por la regla 19. La representación binaria viene dada por $X = (00010011)$. En una configuración inicial aleatoria de densidad $\rho_0 = \frac{1}{4}$, se tienen los vecindarios que generan celda negra $v_0 = 000$, $v_1 = 001$ y $v_4 = 100$ con probabilidades $P(v_0) = (\frac{1}{4})^0(\frac{3}{4})^3$, $P(v_1) = (\frac{1}{4})^1(\frac{3}{4})^2$ y $P(v_4) = (\frac{1}{4})^1(\frac{3}{4})^2$ respectivamente. La densidad obtenida tras un paso viene dada por

$$\rho_1 = \sum_{i \in I} P(v_i) = \left(\frac{3}{4}\right)^3 + \frac{2}{4}\left(\frac{3}{4}\right)^2 \approx 0.7031.$$

∘

Las expresiones para las probabilidades de los vecindarios dadas en (3.1) dependen de que en una configuración inicial aleatoria los valores de celdas consecutivas sean independientes. Tras una iteración del autómata, los valores de dos celdas consecutivas de la configuración obtenida dependen de vecindarios en la configuración inicial anterior que se intersectan en dos celdas. En consecuencia, estos valores no pueden considerarse independientes y no es posible aplicar la expresión (3.1) para obtener la densidad correspondiente a la siguiente configuración. En su lugar, para conocer la distribución de los vecindarios en la configuración obtenida tras una iteración podría procederse teniendo en cuenta las probabilidades de vecindarios de cinco celdas en la configuración inicial, pues estos determinan los vecindarios de tres celdas en la configuración tras un paso. (Véase la figura 3.2). Ahora este procedimiento podría extenderse para conocer la densidad de celdas negras tras la iteración t-ésima, obteniendo las probabilidades de vecindarios de longitud $2t + 1$ en la configuración inicial. Pero esto resulta ser un desperdicio teniendo en cuenta que, en general, determinar los vecindarios de $2t + 1$ celdas que generen una celda negra en la iteración t-ésima

es una tarea de igual o mayor coste computacional que el asociado a la evolución del autómata.

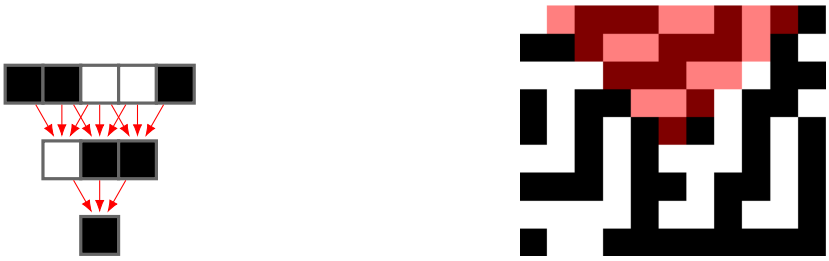

Figura 3.2: A la izquierda se representa la dependencia de una celda de la configuración obtenida tras dos iteraciones con la regla 30, partiendo de una configuración inicial aleatoria. La probabilidad de que una celda cualquiera sea negra tras dos iteraciones viene dada por la suma de probabilidades de vecindarios de 5 celdas en la configuración inicial, que generen celda negra tras dos pasos. A la derecha se representa la región (cono de luz pasado) del patrón generado por la regla 30, de la que depende el valor de la celda del centro. Valores de celdas cuyos conos de luz pasados tienen intersección no vacía están correlacionados.

A continuación se considera el comportamiento de la densidad de celdas negras correspondiente a configuraciones en el límite cuando $t \to \infty$. Como se ha indicado anteriormente, en general, la correlación inducida por la evolución del autómata impide expresar la densidad de celdas negras para $t > 1$ simplemente en función de la fracción de vecindarios que generen celda negra. Para algunas reglas particulares (0, 32, 128,...) el patrón generado a partir de una configuración inicial desordenada sugiere que $\rho_\infty = 0$. Para la regla 0 esto es trivialmente cierto mientras que para las regla 32 y 128 pueden ocurrir transiciones de longitud infinita para configuraciones iniciales particulares (véase la figura 3.3). Análogamente se obtiene $\rho_\infty = 1$ para las reglas 255, 254 y 251 entre otras. La regla 204 es la identidad y en consecuencia $\rho_\infty = \rho_0$. La regla 4 se caracteriza por una densidad final proporcional al número de secuencias de la forma [0,1,0] en la configuración inicial. Así para una configuración inicial aleatoria de densidad ρ_0 se tiene $\rho_\infty = \rho_0(1-\rho_0)^2$.

Figura 3.3: Regla 32 a la izquierda y regla 128 a la derecha. Ambas comenzando con $\rho_0 = 2/3$. Las probabilidades de que ocurran transiciones de longitud mayor o igual que τ son $P(T > \tau) = (2/3)^{\tau+1}(1-2/3)^\tau$ y $P(T > \tau) = (2/3)^{2\tau+1}$ respectivamente.

Con el objetivo de obtener estimaciones para las densidades asociadas a configuraciones sucesivas en la evolución, se asume que los estados de todas las celdas en cada paso son totalmente aleatorios. Esto es que, en toda configuración de densidad ρ, cada celda tiene probabilidad independiente $p = \rho$ de ser negra. Tras un paso, la densidad se obtiene de acuerdo a la ecuación 3.1 y las densidades de configuraciones consecutivas se aproximan iterando la expresión $\rho_{t+1} = \sum_{i \in I} \rho_t^{n_1(v_i)} (1 - \rho_t)^{n_0(v_i)}, \quad t = 0, 1, \ldots$. Siguiendo este procedimiento, en el límite $t \to \infty$ se alcanza la densidad estable correspondiente al punto fijo de esta función. Desviaciones de la densidad estable aproximada con respecto a la densidad real indican el nivel de correlación inducido por la evolución del autómata.

Ejemplo. Se considera el autómata celular (cilíndrico) definido por la regla 22. A partir de una configuración aleatoria de densidad ρ_0 se obtiene una configuración de densidad $\rho_1 = \sum_{i \in I} P(v_i) = 3\rho_0(1 - \rho_0)^2$. La densidad estable de esta función corresponde al punto fijo $\rho = 3\rho(1 - \rho)^2$, que resulta ser aproximadamente $\rho = 0,42$. En la gráfica 3.4 se representan las densidades observadas en las 1100 primeras iteraciones de la regla 22. El autómata parte de una configuración inicial aleatoria de longitud $2 \cdot 10^5$ y $\rho_0 = 1/8$. La densidad media sobre 10^5 iteraciones es aproximadamente 0,3509. Se concluye que hay diferencia significativa entre la densidad aproximada y la densidad real. La elección de la densidad inicial $\rho_0 = 1/8$ es arbitraria. Partiendo de diferentes densidades iniciales se comprueba que la densidad final se estabiliza en torno al mismo valor. ○

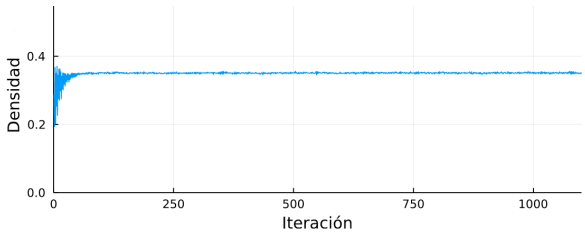

Figura 3.4: Densidades de las primeras 1100 iteraciones con la regla 22. Los valores convergen a la densidad media al cabo de aproximadamente 50 iteraciones. La desviación media de las densidades es aproximadamente 0,0019 para 10^5 iteraciones.

En la aproximación anterior no se tiene en cuenta la correlación entre valores de celdas vecinas inducida por la evolución del autómata, pues se consideran que en cada paso, las celdas toman valores de forma independiente. Se pueden incluir sistemáticamente estas correlaciones considerando las densidades obtenidas tras más de una iteración. Para dos iteraciones, la función de densidad viene determinada por las probabilidades de vecindarios de cinco celdas que generen

celda negra tras dos iteraciones. En el ejemplo anterior con la regla 22 esta función viene dada por $\rho_2 = \rho_0(1-\rho_0)^2(2+3\rho_0^2)$. El punto fijo de esta función es $p \approx 0.3501$. Obsérvese que esta aproximación es considerablemente mejor que la anterior. Véase la gráfica 3.5 en la que se representan aproximaciones considerando vecindarios de más celdas, incluyendo sucesivamente mayor parte de la correlación inducida por la evolución de la regla 22. La sucesión de los puntos fijos de las funciones aproximantes parece converger lentamente a la densidad media observada.

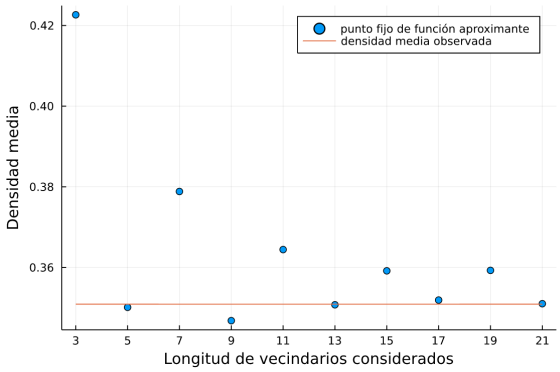

Figura 3.5: Las funciones aproximantes consideradas se obtienen de la generalización de la expresión 3.1 para las densidades tras t pasos: $\rho_t = \sum_{i\in I} P(v_i)$ donde I es el conjunto de índices de vecindarios de $2t+1$ celdas que generan celda negra tras t iteraciones. Nótese que para la regla 22, la función aproximante $\rho_2 = \rho_0(1-\rho_0)^2(2+3\rho_0^2)$ compuesta por las probabilidades de 5-vecindarios es una aproximación considerablemente mejor que ρ_1.

En la segunda columna de la tabla 3.1 siguiente se tienen las densidades medias sobre 10^5 iteraciones de los autómatas celulares cilíndricos de longitud $N = 2(\times)10^4$ definidos por las reglas de clases III y IV. Nuevamente, en la tabla se muestran los resultados para el menor representante de cada clase. Nótese que para la regla negativa y complemento de determinada regla las densidades vendrán dadas por $1-\rho$. En la tercera columna se tiene la desviación típica de las densidades sobre el total de iteraciones. En las restantes columnas se obtuvieron los puntos fijos de las funciones aproximantes considerando vecindarios hasta longitud 21.

La consideración de vecindarios cada vez mayores implica crecimiento exponencial del coste computacional, pues deben considerarse las probabilidades asociadas a 2^{2t+1} vecindarios para determinar la densidad tras t pasos.

Regla	$\overline{\rho}$	Sd	3	5	7	9	11	13	15	17	19	21
18	0.2513	0.0081	0.2929	0.2929	0.2788	0.2782	0.2774	0.2734	0.2727	0.2682	0.2702	0.2695
22	0.3505	0.0149	0.4226	0.3501	0.3788	0.3468	0.3644	0.3507	0.3592	0.3519	0.3593	0.351
30	0.4995	0.0111	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
45	0.4996	0.0112	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
54	0.4779	0.0318	0.5	0.4214	0.3874	0.437	0.4164	0.4314	0.4548	0.4513	0.4385	0.458
60	0.4995	0.0111	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
90	0.4997	0.0111	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
105	0.4994	0.0112	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
106	0.4991	0.0109	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
110	0.5704	0.0036	0.618	0.5285	0.5156	0.5306	0.5163	0.537	0.5429	0.5413	0.5346	0.5458
122	0.5006	0.016	0.618	0.618	0.5649	0.5605	0.5496	0.5315	0.5315	0.5318	0.5283	0.5247
126	0.501	0.016	0.6884	0.4392	0.4715	0.5421	0.4487	0.5169	0.5326	0.5231	0.4542	0.5165
146	0.2512	0.008	0.3333	0.2776	0.2759	0.2752	0.2759	0.273	0.2732	0.2661	0.269	0.2694
150	0.4995	0.0111	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5

Tabla 3.1: Densidades medias observadas y puntos fijos de las funciones aproximantes ρ_t para la densidad tras t pasos, considerando vecindarios de longitud $2t+1$. Obsérvese que para las reglas con $\overline{\rho} \approx 0.5$, excepto la regla 122, el punto fijo de todas las funciones aproximantes es 0.5. Para las reglas con $\overline{\rho} \neq 0.5$ se tiene que los puntos fijos de las funciones aproximantes convergen lentamente a la densidad observada.

3.2. Secuencias pseudoaleatorias generadas por la regla 30

La generación de secuencias aleatorias tiene aplicaciones en diversas áreas de las matemáticas: simulación de procesos estocásticos, el método de Monte Carlo, etc.

En este capítulo se estudian propiedades estadísticas de las secuencias generadas por iteraciones consecutivas con el autómata celular definido por la regla 30. En particular se aplican varios test de aleatoriedad a la secuencia generada por la celda central, correspondiendo con la columna central en el patrón de evolución, para comprobar la factibilidad de esta regla como un generador de números pseudoaleatorios.

Establecer una definición universal de aleatoriedad resulta ser una tarea delicada. En general se considera que una secuencia es aleatoria si no permite detectar patrones, hacer predicciones ni encontrar una descripción más sencilla que la misma secuencia. Una definición más estricta de aleatoriedad implica la inexistencia de tal tipo de descripción, en lugar de la dificultad de encontrarla. Para secuencias generadas por algoritmos inherentemente deterministas como un autómata celular, ciertamente existe una descripción sencilla, aunque quizá sea arbitrariamente difícil de encontrar. Luego estas secuencias no verifican este último criterio estricto de aleatoriedad y se consideran *secuencias pseudoaleatorias*.

3.2.1. Implementación

A la hora de implementar un autómata celular en cualquier máquina, por ejemplo un ordenador digital, se dispone de una cantidad finita de memoria. En consecuencia la longitud del autómata implementado ha de ser finita. Como se ha descrito con anterioridad (ver página 3), hay diferentes formas de limitar la longitud de las configuraciones manteniendo un comportamiento coherente en los bordes.

Para un autómata finito, las secuencias pseudoaleatorias que se obtienen considerando los valores consecutivos de una celda se repiten después de un número finito de pasos. Se recuerda que cualquier autómata de longitud finita da lugar a un conjunto finito de configuraciones posibles y ha de entrar en un ciclo tras una transición finita. Se tiene entonces una cota superior para la longitud de secuencias que pueden ser consideradas aleatorias, pues alcanzada la longitud del ciclo la secuencia se repite.

En la práctica, sin embargo, resulta posible obtener secuencias pseudoaleatorias largas si la longitud del autómata es suficientemente grande. No se han encontrado resultados explícitos para las longitudes de ciclos alcanzados en la evolución de la regla 30, no obstante el enfoque empírico sugiere que las longitudes de ciclos crecen aproximadamente de forma exponencial con la longitud del autómata. Para los autómatas cilíndricos definidos por la regla 30 con $N \leq 59$ se obtiene $\Pi_N \approx 2^{0.61N}$. El número de configuraciones que evolucionan al ciclo de longitud máxima parece crecer con N, siendo 96 % para $N = 17$. Sin embargo, tanto la longitud máxima de ciclo como el número de configuraciones que evolucionan al ciclo maximal presentan irregularidades debidas a propiedades de simetría en determinadas configuraciones. Algunas de estas irreguaridades se derivan de propiedades numerico teóricas de los valores de N.[4].

El tipo de condición de frontera implementado tiene un efecto notable en las longitudes maximales de ciclos. Del estudio hecho en [6] se concluye que las condiciones de frontera constantes siempre producen decrecimiento en la complejidad del comportamiento. De nuevo, el análisis empírico dado en [4] sugiere que la condición de frontera periódica, esto es cuándo el autómata celular es cilíndrico, da lugar a ciclos de mayor longitud, y parece por tanto la adecuada para la implementación práctica.

3.2.2. Pruebas estadísticas

Para comprobar la validez de la regla 30 como generador de secuencias aleatorias se deben aplicar una serie de procedimientos estadísticos a las secuencias generadas. En general, la elección de estos procedimientos depende del contexto en el que se obtienen las secuencias y del nivel de confianza exigido en la aleatoriedad de las mismas. En principio, no hay un conjunto definido de pruebas estadísticas tras cuya aplicación se puede estar “totalmente convencido”

de la aleatoriedad de una secuencia. Este hecho no es particular a la hipótesis de aleatoriedad de una secuencia, sino que ocurre en general en cualquier test de hipótesis. Si una secuencia se comporta adecuadamente con respecto a un conjunto finito $T_1, T_2, ..., T_n$ de pruebas de aleatoriedad, en general, no se puede asegurar que no fallará en otra prueba T_{n+1}. En esta sección se describen 5 pruebas estadísticas tomadas de [7], que en la práctica se han demostrado fiables para secuencias usadas en computación.

Se consideran las secuencias de bloques disjuntos de n bits consecutivos en la columna central del autómata celular definido por la regla 30. Cada bloque de n bits se corresponde con un número entre 0 y $2^n - 1$, así la secuencia equivale a una secuencia de números naturales. Dependiendo de la prueba se toma $n = 4$ o $n = 8$, dando lugar a secuencias de números entre 0 y 15 y entre 0 y 255 respectivamente.

1. **Prueba de equidistribución.**
   Se espera que los valores de la secuencia se distribuyan uniformemente entre 0 y $2^n - 1$. Se considera el experimento de escoger un elemento aleatorio de la secuencia y la variable aleatoria X:"Valor del elemento escogido". Entonces se tiene $X \sim U(0, ..., 2^n - 1)$ con probabilidad para un determinado valor x: $P(X = x) = \frac{1}{2^n}$ con $x = 0, 1, ..., 2^n - 1$.
2. **Prueba de brechas.**
   En esta prueba se examinan las longitudes de "brechas" entre las ocurrencias de valores dentro de un rango determinado. Se consideran dos valores l y u tales que $0 < l < u < 2^n - 1$ y se cuentan las longitudes de subsecuencias $s_i, s_{i+1}, ..., s_{i+r}$ tales que s_{i+r} sea el primer elemento de la secuencia verificando que $l \leq s_{i+r} \leq u$. Esto es, una *brecha* de longitud r. Se considera el experimento de escoger una brecha aleatoria y la variable aleatoria R:"Longitud de la brecha". Se tiene que $R \sim Geo(\frac{u-l+1}{2^n})$ con probabilidad para determinada longitud r: $P(R = r) = p(1 - p)^r$ con $p = \frac{u-l+1}{2^n}$ con $r = 0, 1, ...$
3. **Prueba de elementos distintos.**
   Se consideran las subsecuencias S_k consecutivas y disjuntas de longitud $k < 2^n$ y se cuenta el número de elementos distintos que hay en S_k. Si D es la variable aleatoria que mide el número de elementos distinos en una subsecuencia escogida al azar se tienen las probabilidades:
   $P(D = d) = \binom{2^n}{d} \frac{\binom{k}{d} d! d^{k-d}}{(2^n)^k}$ con $d = 0, 1, ..., k$.
4. **Prueba de rachas monótonas.**
   En esta prueba se consideran las longitudes de subsecuencias de valores crecientes (no estrictamente). Nótese que las longitudes de dos de estas rachas monótonas no son independientes, pues tras una racha larga hay mayor probabilidad de que siga una racha corta, y viceversa. Para evitar esta dependencia se "salta" el elemente inmediatamente consecutivo a cada racha,

dando lugar a subsecuencias estadísticamente independientes. Si L es la variable aleatoria de la longitud de una racha monótona creciente se tienen las probabilidades: $P(L = l) = \frac{1}{l!} - \frac{1}{(l+1)!}$ para $l = 1, 2, \ldots$.

5. **Prueba de máximos.**
   Se consideran los valores máximos de las subsecuencias de longitud k. Si M es la variable aleatoria que mide el valor del máximo de una subsecuencia de longitud t escogida al azar se tienen las probabilidades:
   $P(M = m) = (\frac{m+1}{2^n})^k - (\frac{m}{2^n})^k$ con $m = 0, 1, \ldots, 2^n - 1$.

El procedimiento clásico para la realización de pruebas estadísticas del tipo anterior es por medio de un *test de bondad de ajuste*. La idea general consiste en asumir que cierto parámetro de la muestra estudiada, en este caso de la secuencia pseudoaleatoria generada por el autómata, sigue una determinada distribución estadística conocida. Por ejemplo, en la prueba de equidistrución se asume que los valores están uniformemente distribuidos. Ahora se calcula un parámetro denomidado *estadístico de la prueba*, generalmente expresado en términos de la diferencia entre los valores observados (los de la muestra) y los valores esperados (los correspondientes valores teóricos de la distribución asumida). El estadístico de la prueba mide "cuánto se aleja" la muestra de la distribución esperada y la teoría de los test de bondad de ajuste permite asociar una probabilidad a que la muestra tenga un estadístico dentro de un rango determinado. Para el estudio de variables aleatorias discretas, como es el caso en todas las pruebas aquí planteadas, es usual la *prueba de Chi-Cuadrado* (χ^2), o, en el caso de tener muchas categorías de observaciones como en la prueba 5, el test *Kolmogorov-Smirnov*. Véase [7] para una descripción de estos procedimientos en el contexto de pruebas estadísticas para secuencias aleatorias.

Alternativamente, cuando se dispone de los recursos computacionales necesarios, puede compararse el rendimiento de la secuencia candidata a ser aleatoria en las pruebas estadísticas con el rendimiento de secuencias obtenidas con un generador pseudoaleatorio de cuya bondad ya se esté convencido. Esto tiene la limitación de que, como mucho, se puede garantizar que la secuencia estudiada es tan aleatoria como una obtenida con el generador pseudoaleatorio usado. Sin embargo este procedimiento tiene una gran ventaja: no es necesario conocer la distribución teórica del parámetro estudiado en la prueba estadística, pues puede obtenerse una distribución "pseudoteórica" por medio de la simulación de un gran número de secuencias con el generador pseudoaleatorio. Una segunda ventaja de este método es que permite evitar el problema de la adecuación de la muestra estudiada a un determinado test de bondad de ajuste. Resulta que, por ejemplo, en general no es evidente cuántas observaciones deben obtenerse para poder hacer una prueba de Chi-Cuadrado "apropiada" [7].

Para el estudio presente de la secuencia generada por el autómata celular definido por la regla 30 se ha optado por esta última alternativa. Las secuencias pseudoaleatorias se han obtenido vía la función `rand()` de *Julia 1.6*. El código

utilizado para la realización de todas las pruebas se encuentra en el anexo. El experimento realizado consiste en los siguientes pasos, donde la distribución es la correspondiente a la prueba estadística en cuestión:

1. Se obtiene la secuencia correspondiente a la columna central del autómata.
2. Se estima la distribución esperada simulando 10^4 secuencias pseudoaleatorias.
3. Se calcula la suma de los cuadrados de las diferencias entre los valores observados en la secuencia generada por el autómata y los valores esperados correspondientes a la distribución estimada. Este estadístico indica cuánto se aleja la secuencia generada por el autómata de la media esperada para la prueba estadística en cuestión.
4. Se calcula el estadístico anterior para un número grande de secuencias pseudoaleatorias.
5. Se obtiene la fracción de secuencias pseudoaleatorias simuladas que se alejan más de la distribución esperada que la secuencia generada por el autómata.

La hipótesis de que la secuencia generada por el autómata es aleatoria implica que la fracción obtenida en el último paso del experimento debe seguir una disrtribución uniforme entre 0 y 1. Este hecho se sigue de que, si las secuencias generadas por el autómata efectivamente son aleatorias, los estadísticos de estas secuencias deberán seguir la misma distribución que los correspondientes a las secuencias pseudoaleatorias simuladas.

En las tablas siguientes se muestran los resultados del experimento para las cinco pruebas estadísticas descritas en esta sección. En la tabla 3.2 se tienen las fracciones de secuencias pseudoaleatorias con estadístico mayor que el de la secuencia particular generada por el autómata a partir de una celda negra. Salvo para $N = 17$ las fracciones parecen estar distribuidas uniformemente, apoyando la hipótesis de que la secuencia generada a partir de una celda negra es aleatoria. En la tabla 3.3 se muestran los resultados de un total de 10^3 experimentos donde las secuencias generadas por el autómata se obtienen a partir de condiciones iniciales aleatorias de densidad $\rho = 1/2$. Para cada una de las 10^3 secuencias generadas por el autómata a partir de una condición inicial aleatoria diferente, se realiza el experimento descrito anteriormente. Se espera que la media de los resultados de los experimentos sea 0.5. Nuevamente, salvo para N tal que $L > \Pi_N$, los resultados apoyan la hipótesis de que el autómata celular cilíndrico definido por la regla 30 es factible como un generador de secuencias pseudoaleatorias.

Prueba	N=17	N=23	N=25	N=29	N=35	N=37	N=44	N=47	N=49	N=53
1 (L=64K)	**0**	0.9239	0.8138	0.2258	0.3264	0.6489	0.7002	0.4412	0.4869	0.1347
2 (L=64K)	0.1663	0.0145	0.6505	0.7423	0.4871	0.1268	0.0367	0.7162	0.0436	0.3899
3 (L=16K)	0.4687	0.7144	0.2567	0.7318	0.2400	0.0737	0.6076	0.0101	0.8178	0.3941
4 (L=64K)	0.4504	0.3391	0.5669	0.9828	0.4466	0.1562	0.4572	0.6301	0.1306	0.7952
5 (L=64K)	**0**	0.7728	0.6123	0.1266	0.6501	0.7205	0.9350	0.6423	0.0201	0.6132

Tabla 3.2: Fracción de secuencias pseudoaleatorias con resultados más extremos que para la secuencia generada por el autómata celular cilíndrico definido por la regla 30 (la columna central), de longitud N y partiendo de una sola celda negra. El número de secuencias pseudoaleatorias generadas para obtener la fracción es 10^4. Nótese que en las pruebas 1 y 5 con $N = 17$ la secuencia generada por el autómata difiere más de la distribución media que todas las secuencias simuladas. Esto se debe a que $\Pi_{17} = 10845 < 64000$ y el autómata ha entrado en un ciclo. Se observa que las pruebas 2, 3 y 4 no detectan este fenómeno. En general, no se detecta desviación de la distribución uniforme esperada para las fracciones.

Prueba	N=17	N=23	N=25	N=29	N=35	N=37	N=44	N=47	N=49	N=53
$\Pi_N \approx$	10^4	$3.8 \cdot 10^4$	$5.8 \cdot 10^5$	$1.5 \cdot 10^6$	$1.8 \cdot 10^7$	$4.9 \cdot 10^7$	$1.9 \cdot 10^8$	$8.1 \cdot 10^8$	$9.9 \cdot 10^9$	$4 \cdot 10^{10}$
1 (L=64K)	$\sim$ **0**	0.8626	0.5064	0.4609	0.4806	0.5060	0.5068	0.5109	0.5121	0.5097
2 (L=64K)	0.2634	0.3685	0.4789	0.4602	0.4894	0.4854	0.4950	0.5103	0.5100	0.4812
3 (L=16K)	0.4769	0.4415	0.5031	0.5145	0.5123	0.5073	0.5182	0.5030	0.4975	0.4923
4 (L=64K)	0.3233	0.4783	0.4921	0.5234	0.4933	0.4968	0.4985	0.4982	0.5066	0.4999
5 (L=64K)	$\sim$ **0**	0.7310	0.5132	0.5292	0.5014	0.4869	0.5132	0.4797	0.4869	0.5025

Tabla 3.3: Fracción media de secuencias pseudoaleatorias con resultados más extremos que para una secuencia generada por el autómata celular cilíndrico definido por la regla 30, de longitud N y partiendo de una condición inicial aleatoria de densidad $\rho = 1/2$. La fracción media se obtiene para un total de 10^3 experimentos. En cada uno de los experimentos se generan 10^4 secuencias pseudolaeatorias para obtener la fracción. La fracción media esperada es de 0.5. Desviaciones se detectan para $N = 17$ y $N = 23$.

Conclusiones

El estudio de la evolución de los autómatas celulares, en particular de los patrones generados por estos, muestra un hecho sorprendente: es posible que sistemas basados en reglas sencillas desarrollen comportamientos diversos y complejos.

Como se destacó en el capítulo introductorio, a excepción de algunas características particulares, la predicción del comportamiento de un autómata celular no trivial es una tarea difícil. Sin embargo, en el caso de las reglas aditivias es posible derivar resultados algebraicos sobre el conjunto de configuraciones y la estructura del diagrama de transición de estas. Las reglas de autómata celular que no verifiquen el principio de superposición aditiva no permiten, en general, un análisis algebraico análogo al que se ha desarrollado en el segundo capítulo.

La fácil implementación de los autómatas celulares en un ordenador permiten un extenso análisis empírico. Por un lado, para las reglas que generen patrones complejos, la densidad de celdas negras resulta converger siempre, independientemente de la condición inicial. Es posible aproximar el límite de convergencia por medio de funciones recursivas. Por el otro lado, los resultados de cinco pruebas de aleatoriedad clásicas indican que la columna central del patrón generado por la regla 30 puede considerarse aleatoria.

Hay un número interminable de preguntas abiertas sobre los autómatas celulares. Muchas de ellas relacionadas con problemas abiertos en teoría de la computación y teoría de números. Algunas de ellas, en particular las 3 siguientes, fueron propuestas por S. Wolfram y se refieren a la regla 30 en un autómata sin frontera (infinito): ¿Es posible demostrar que la columna central es no-periódica? ¿Ocurren las celdas blancas y negras con la misma frecuencia? y ¿Es posible computar el valor de la celda n-ésima en un tiempo computacional menor que $O(n)$? También son interesantes muchas cuestiones de carácter empírico: ¿Cómo se distribuyen los triángulos en los patrones de clase III? ¿Aparece orden a todas las escalas?

Se acaba esta memoria con una breve anéctoda, que contó Stephen Wolfram en una entrevista con Alexander Fridman, sobre la época en la que él mismo trabajaba junto al famoso físico Richard Feynman en la empresa Thinking Machines, en los años ochenta. Stephen Wolfram había descubierto el comportamiento extraño de la regla 30 por mera casualidad al ejecutar una serie de simulaciones con reglas escogidas al azar. Primero pensaba que debía tratarse de una anomalía y decidió imprimir el patrón generado en un formato grande, de varios metros cuadrados, y estirarlo por el suelo de la empresa. Cuando estaba inspeccionando el patrón se le acerca Richard Feynman y le pregunta "¡¿Cómo sabías que la regla iba a producir todo esto?!" a lo que Wolfram responde que no lo sabía de antemano, sino que lo descubrió por accidente. Tranquilizado por esta respuesta Feynman responde que estaría aliviado al saber que él (Wolfram) tampoco tuviera intuición sobre el fenómeno que estaban observando.

A

Apéndice

A.1. Tabla de reglas equivalentes

X	$\bar{X}$	$\hat{X}$	X^c	sim
CLASE I				
0	255	0	255	b,c,d
8	239	64	253	
32	251	32	251	a
40	235	96	249	
128	254	128	254	b
136	238	192	252	d
160	250	160	250	c
168	234	224	248	
CLASE II				
1	127	1	127	b
2	191	16	247	
3	63	17	119	d
4	223	4	223	a
5	95	5	95	c
6	159	20	215	
7	31	21	87	
9	111	65	125	
10	175	80	245	
11	47	81	117	
12	207	68	221	d
13	79	69	93	
14	143	84	213	

X	$\bar{X}$	$\hat{X}$	X^c	sim
15	15	85	85	d
19	55	19	55	a
23	23	23	23	b
24	231	66	189	
25	103	67	61	
26	167	82	181	
27	39	83	53	
28	199	70	157	
29	71	71	29	
33	123	33	123	a
34	187	48	243	d
35	59	49	115	
36	219	36	219	a
37	91	37	91	a
38	155	52	211	
41	107	97	121	
42	171	112	241	
43	43	113	113	
44	203	100	217	
46	139	116	209	
50	179	50	179	a
51	51	51	51	a,d
56	227	98	185	

X	$\bar{X}$	$\hat{X}$	X^c	sim
57	99	99	57	
58	163	114	177	
62	131	118	145	
72	237	72	237	a
73	109	73	109	a
74	173	88	229	
76	205	76	205	a
77	77	77	77	a
78	141	92	197	
94	133	94	133	a
104	233	104	233	b
108	201	108	201	a
130	190	144	246	
132	222	132	222	a
134	158	148	214	
138	174	208	244	
140	206	196	220	
142	142	212	212	
152	230	194	188	
154	166	210	180	
156	198	198	156	
162	186	176	242	
164	218	164	218	a

X	$\bar{X}$	$\hat{X}$	X^c	sim
170	170	240	240	d
172	202	228	216	
178	178	178	178	a
184	226	226	184	
200	236	200	236	a
204	204	204	204	a,d
232	232	232	232	b
CLASE III				
18	183	18	183	a
22	151	22	151	b
30	135	86	149	
45	75	101	89	
60	195	102	153	
90	165	90	165	c
105	105	105	105	b
122	161	122	161	a
126	129	126	129	b
146	182	146	182	a
150	150	150	150	b
CLASE IV				
54	147	54	147	a
106	169	120	225	
110	137	124	193	

Tabla A.1: Las 88 reglas inequivalentes ordenadas por clases de Wolfram. En la primera columna de cada clase de equivalencia se tiene la regla representante (menor valor en la nomenclatura de Wolfram). En la columna *sim* se indican las restricciones que cumplen las reglas, siendo los identificadores (véase la página 12): a si cumple la restricción (1), b si cumple la restricción (1.1) c si verifica la restricción (1.2) y d si cumple restricciones (2.1) o bien (2.2). Es evidente que si una regla cumple b o c también cumple a. En este caso solo se indicara la simetría más restrictiva.

A.2. Anillo de los dipolinomios

Se denota por $D_{\mathbb{Z}_2}[x]$ al anillo conmutativo de los dipolinomios con coeficientes en el cuerpo $\mathbb{Z}_2$. Un dipolinomio $A(x)$ se dice que divide a otro dipolinomio $B(x)$ si existe un dipolinomio $C(x)$ tal que $B(x) = A(x)C(x)$. Esto se denota por $A(x) \mid B(x)$. Se define la congruencia como sigue: $A(x) \equiv B(x)$ mód $(C(x))$ para dipolinomios $A(x)$,$B(x)$ y $C(x)$ si $C(x) \mid A(x) - B(x)$..

La relación de congruencia de dipolinomios, al igual que ocurre con polinomios, es una relación de equivalencia. Considerando $C(x) = x^N - 1$ se obtiene el conjunto de clases de equivalencia, o conjunto cociente, $D_{\mathbb{Z}_2}[x]/(x^N - 1)$, donde $(x^N - 1)$ denota al ideal generado por el dipolinomio $x^N - 1$.

En general, para todo anillo conmutativo A tal que $I \subset A$ es un ideal de A, si $[a] = \{b \in A / a - b \in I\}$ es la clase de equivalencia de determinado elemento a, el conjunto de clases de equivalencia $A/I = \{[a]/a \in A\}$ es también un anillo conmutativo. Las operaciones en A/I son las inducidas por las operaciones en A. Se denomina proyección canónica al homomorfismo $\pi : A \to A/I$ definido por $\pi(a) = [a] \quad \forall\, a \in A$.

Se tiene entonces que el conjunto cociente $D_{\mathbb{Z}_2}[x]/(x^N - 1)$ es un anillo conmutativo con las operaciones

$$[p(x)] + [q(x)] = [p(x) + q(x)] \tag{1}$$

y

$$[p(x)][q(x)] = [p(x)q(x)]. \tag{2}$$

Nótese que, en lo presente, las clases de equivalencia inducidas por la relación de congruencia módulo $x^N - 1$ se denotan por $p(x) \mod (x^N - 1)$ para todo $p(x) \in D_{\mathbb{Z}_2}[x]$. Esto es $[p(x)] = p(x) \mod (x^N - 1)$.

Proposición A.1 *Todo dipolinomio $D(x) = \sum_j a_j x^j$ es congruente módulo $(x^N - 1)$ con un único polinomio de grado menor que N. Además este polinomio viene dado por*

$$\sum_{i=0}^{N-1} \left(\sum_j a_{i+jN} \right) x^i.$$

Demostración. De 1 se sigue que

$$D(x) = \sum_j a_j x^j \mod (x^N - 1) = \sum_j (a_j x^j \mod (x^N - 1)).$$

Se comprueba que para todo j se tiene $x^j \equiv x^i \mod (x^N - 1)$ donde $j \equiv i$ mód (N) con $0 \le i \le N - 1$ y entonces

$$\sum_j (a_j x^j \mod (x^N - 1)) = \sum_{i=0}^{N-1} \left(\sum_{j \equiv i \mod (N)} a_j \right) x^i = \sum_{i=0}^{N-1} \left(\sum_j a_{i+jN} \right) x^i.$$

Propiedad 1 *Para dipolinomios $A(x)$, $B(x)$, $C(x)$, $D(x)$ y $M(x)$, si*

$$A(x) \equiv B(x) \mod M(x) \quad y \quad C(x) \equiv D(x) \mod M(x)$$

entonces

$$A(x)C(x) \equiv B(x)D(x) \mod M(x)$$

Demostración.

$$A(x) = T(x)M(x) + B(x) \quad y \quad C(x) = S(x)M(x) + D(x)$$

y entonces

$$A(x)C(x) = [T(x)S(x)M(x) + T(x)D(x) + B(x)S(x)]M(x) + B(x)D(x)$$

y por tanto

$$A(x)C(x) \equiv B(x)D(x) \mod M(x).$$

Propiedad 2 *Para dipolinomios $A(x)$, $B(x)$, $C(x)$, $D(x)$ y $M(x)$ si*

$$C(x) \mid A(x) \quad y \quad C(x) \mid M(x) \quad y \quad A(x) \equiv D(x) \mod M(x)$$

entonces

$$C(x) \mid D(x).$$

Demostración. Se tiene que $A(x) = Q(x)C(x)$, $M(x) = S(x)C(x)$ y $A(x) = T(x)M(x) + D(x)$ para ciertos dipolinomios $Q(x)$, $S(x)$ y $T(x)$. Entonces

$$A(x) = T(x)S(x)C(x) + D(x) = Q(x)C(x),$$

por lo que $D(x) = (Q(x) - T(x)S(x))C(x)$, y por tanto $C(x) \mid D(x)$.

A.3. Anexo externo

En el siguiente enlace se encuentra el anexo externo a esta memoria: https://drive.google.com/drive/folders/1ryohkENHy7_0u2jORPaU_YZFxLql4lV_?usp=sharing

El documento contiene los códigos de *Julia* que se han utilizado para la creación de los patrones de evolución de AC, imágenes de los patrones para las 256 reglas de AC elemental y las demostraciones correspondientes a las proposiciones y lemas del capítulo dos.

Bibliografía

[1] WOLFRAM, Stephen. *A New Kind of Science.* Champaign, IL: Wolfram Media, 2002.

[2] OLIVIER, M., ODLYZKO, A. M. y WOLFRAM, S. Algebraic Properties of Cellular Automata. En WOLFRAM, Stephen. *Cellular automata and collected papers*. Westview Press, Perseus Books Group, 1994.

[3] WOLFRAM, Stephen. Statistical Mechanics of Cellular Automata. En WOLFRAM, Stephen. *Cellular automata and collected papers*. Westview Press, Perseus Books Group, 1994.

[4] WOLFRAM, Stephen. Random Sequence Generation by Cellular Automata. En WOLFRAM, Stephen. *Cellular automata and collected papers*. Westview Press, Perseus Books Group, 1994.

[5] ALVAREZ-PARRILLA, A. y ESPINOSA VALDEZ, A. Autómatas Celulares Aditivos: la regla 150 vs. la regla 90. *Revista del Centro de Investigación*. Universidad La Salle. 2008. Disponible en: https://www.researchgate.net/publication/242480367_Automatas_Celulares_Aditivos_la_regla_150_vs_la_regla_90.

[6] LUVALLE, Brian J. The Effects of Boundary Conditions on Cellular Automata. *Complex Systems*. Volumen **28** (2019). 97-124. Disponible en: https://content.wolfram.com/uploads/sites/13/2019/04/28-1-5.pdf.

[7] KNUTH, Donald E. *The Art of Computer Programing. Volume 2. Seminumerical Algorithms*. 3ª ed. Massachusets: Addison-Wesley, 1998.

[8] ROBISON, Arch D. Fast Computation of Additive Cellular Automata. *Complex Systems*. Volumen **1** (1987). 211-216. Disponible en: https://wpmedia.wolfram.com/uploads/sites/13/2018/02/01-1-15.pdf.

Cellular Automata. Analysis and experiments in the one-dimensional case.

Pablo Heer
Facultad de Ciencias • Sección de Matemáticas
Universidad de La Laguna
alu0101106793@ull.edu.es

Abstract

BEHAVIOUR of a particular class of one-dimensional cellular automata is presented. Using algebraic methods, results on number and type of configurations are derived for the set of additve automata. Density distribution of black cells in cellular automata evolution and pseudorandom sequences generated by cellular automata with rule number 30 are studied empirically.

1. Cellular Automata

Cellular Automata are discrete dynamical systems capable of generating complicated patterns while based on very simple underlying rules. The following figure shows a particular rule for an Elementary Cellular Automaton.

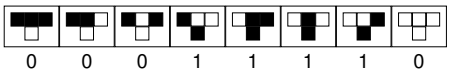

Figure 1: *Particular rule for a cellular automaton with* 3*-cell neighbourhoods and two possible states: black and white. The rule indicates the color of the cell in the middle of each neighbourhood in the next step of the automaton evolution.*

Different rules show various kinds of behaviour. It is possible to classify the behaviour of a particular automaton according to four different classes shown in the next figure:

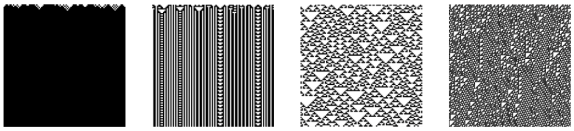

Figure 2: *Four classes of cellular automaton behaviour.*

The idea of cellular automata first came up in the 50s. John von Neumann and Stanislav Ulam considered these systems to understand the mechanisms behind self-reproducing structures in biology.
Many features of biological systems and complex systems in general turn out to be part of cellular automaton behaviour. The next figure shows the striking similarity between the pattern on a seashell and the pattern generated by a particular cellular automaton.

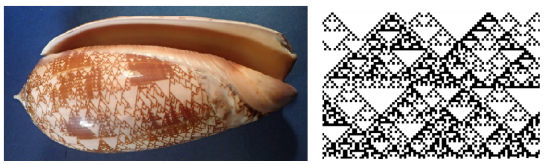

Figure 3: *Oliva Porphyria shell (fotograph by Donna Pomeroy). The pigmentation pattern compares to the evolution pattern of the elementary cellular automaton rule 22.*

2. Additive Automata

Additve cellular automata verify the *additive superposition principle*:

$$X(\mu + \mu') = X(\mu) + X(\mu')$$

for X a particular additive rule and μ, μ' two given configurations of the state space. For this particular set of rules algebraic results can be derived based on the identification of configurations of the state space with dipolynomials. For cylindrical elementary automata a unique correspondance between configurations and polynomials with coefficients in $\mathbb{Z}_2$ exists:

$$\mu = [...01101...] \leftrightarrow \cdots x^i + x^{i+1} + x^{i+3} \cdots$$

The transition between configurations of the state space can be represented with an oriented graph called the *state transition diagram*. For additive automata, general results on the structure of this graph can be derived.

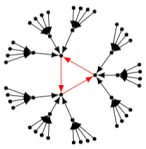

Figure 4: *State Transition Diagram for the rule 90 cylindrical cellular automaton.*

3. Randomness in rule 30.

The particular cellular automaton rule 30 can be used as an effective random sequence generator.

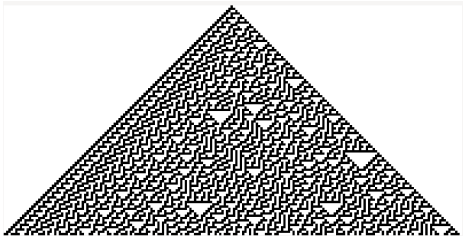

Figure 5: *Rule 30 starting from a single black cell.The sequence of black and white cells in the center column turns out to be effectively random.*

References

[1] WOLFRAM, Stephen. *A New Kind of Science.* Champaign, IL: Wolfram Media, 2002.

[2] WOLFRAM, Stephen. *Cellular automata and collected papers.* Westview Press, Perseus Books Group, 1994.

[3] KNUTH, Donald E. *The Art of Computer Programing. Volume 2. Seminumerical Algorithms.* 3ª ed. Massachusets: Addison-Wesley, 1998.