



# VNiVERSiDAD D SALAMANCA

FACULTAD DE CIENCIAS  
GRADO EN MATEMÁTICAS

TRABAJO DE FIN DE GRADO:

---

## AUTÓMATAS CELULARES REVERSIBLES: DEFINICIÓN, PROPIEDADES Y APLICACIONES

---

Autor: Samir Llamazares Elías

Tutores: Ángel Martín del Rey y Guillermo Hernández González

Salamanca, Julio de 2020



# VNiVERSiDAD D SALAMANCA

FACULTAD DE CIENCIAS  
GRADO EN MATEMÁTICAS

TRABAJO DE FIN DE GRADO:

---

## AUTÓMATAS CELULARES REVERSIBLES: DEFINICIÓN, PROPIEDADES Y APLICACIONES

---

Autor: Samir Llamazares Elías

Tutores: Ángel Martín del Rey y Guillermo Hernández González

Salamanca, Julio de 2020

*esamin*

# Contenidos

<b>1</b>	<b>Introducción</b>	<b>1</b>
<b>2</b>	<b>Preliminares</b>	<b>2</b>
2.1	Primeras Definiciones . . . . .	2
2.2	Vecindades . . . . .	4
2.3	Configuraciones finitas y periódicas . . . . .	5
2.4	Autómatas Celulares Elementales . . . . .	8
2.5	Topología del Espacio de Configuraciones . . . . .	9
<b>3</b>	<b>Reversibilidad y Equilibrio</b>	<b>13</b>
3.1	Reversibilidad . . . . .	13
3.2	Epiyectividad y Equilibrio . . . . .	15
<b>4</b>	<b>El Teorema del Jardín de Edén</b>	<b>20</b>
<b>5</b>	<b>AC unidimensionales</b>	<b>26</b>
5.1	Resultados teóricos . . . . .	26
5.2	Grafos de de Bruijn . . . . .	28
<b>6</b>	<b>Autómatas Celulares Particionados</b>	<b>37</b>
<b>7</b>	<b>Aplicaciones</b>	<b>43</b>
<b>8</b>	<b>Conclusiones</b>	<b>46</b>

# 1 Introducción

## Introducción

Este trabajo busca estudiar de forma rigurosa los autómatas celulares (ACs), céntrándose de manera especial en la propiedad de la reversibilidad. El concepto de AC fue creado por John von Neumann cuando su estudio de la autorreplicación le llevo a construir un AC capaz de copiarse a si mismo. Posteriormente, en el año 1980, los ACs ganaron en popularidad con la creación por John Conway de un AC llamado el Juego de la Vida. El AC de John Conway era universalmente computacional, es decir, podía emular cualquier cosa computable. Además destacaba por su autoorganización, o lo que es lo mismo, el surgimiento de un orden global a partir del desorden inicial. En los años 80 Stephen Wolfram continuó el estudio de los ACs analizando una plétora de aspectos de los ACs[1]. En la actualidad los ACs tienen varias aplicaciones y son el centro de cada vez más investigaciones. Los ACs se usan en la criptografía para cifrar información, como sistemas computacionales para resolver problemas algorítmicos, en el estudio de la complejidad, en la formación de patrones y para modelar una gran cantidad de sistemas en la biología, física, química y sociología. Para más información acerca de la historia de los ACs véase [2].

Un AC es un sistema dinámico en el que evolucionan los estados de un "universo" a lo largo del tiempo. El universo, que habitualmente llamaremos configuración, consiste en un conjunto células, cada una de ellas en un estado de un alfabeto. Es posible estudiar ACs en el que las células son elementos de un grupo cualquiera y el alfabeto es infinito. Este planteamiento es desarrollado en [4]. Sin embargo, en este trabajo consideraremos solo el caso más tradicional en el que las células son elementos de  $\mathbb{Z}^d$  y el alfabeto es finito. De esta forma podemos visualizar el universo como una red de dimensión  $d$  formada por celdas o células que están en un estado de nuestro alfabeto. El AC es la regla que dicta como evoluciona el universo o configuración. Esta regla puede ser tanto determinista como probabilista[3]. En este trabajo consideraremos solo los ACs deterministas y cada vez que esté escrito AC se sobreentenderá que éste es de carácter determinista. El universo evoluciona de forma discreta en el tiempo al aplicar iterativamente el AC. La particularidad de los ACs es que esta regla determina el nuevo estado de cada celda en base a los estados en los que están las células en una vecindad finita de la celda. La actualización del estado de cada célula se realiza de forma simultánea y de forma independiente a las actualizaciones que se producen en las otras células. Además, tanto la regla de actualización como la vecindad es uniforme en el espacio y el tiempo. De esta forma el comportamiento global del AC surge a partir de interacciones locales entre células del universo, por lo cual los ACs son sistemas descentralizados. Buena parte del interés de los ACs reside en como a partir de reglas locales sencillas surgen una gran variedad de patrones permitiendo que se usen los ACs en diversos campos científicos.

En este trabajo nos centraremos en los ACs reversibles. Estos ACs se caracterizan por que toda configuración tiene un único predecesor. Por tanto, dado un universo cualquiera podemos determinar el estado del universo en cualquier momento anterior. Crucialmente, estos ACs resultan de gran utilidad para modelar sistemas dinámicos reversibles en el tiempo, en particular, sistemas que evolucionan según las leyes de la mecánica clásica.

En el primer capítulo daremos la definición matemática de AC, estudiaremos la topología del espacio de configuraciones y demostraremos el teorema de Curtis-Hedlund-Lyndon que caracteriza a los ACs. En el segundo capítulo veremos la definición de AC reversible y estudiaremos varias propiedades de la inyectividad y epiyectividad de los ACs con la finalidad de simplificar la condición de reversibilidad. En el tercer capítulo veremos el teorema más conocido acerca de los ACs, el teorema del Jardín de Edén. La nomenclatura bíblica es debida a que el teorema trata los ACs con algún universo sin predecesor y que por tanto solo puede aparecer en el instante inicial. Dedicaremos el cuarto capítulo a un estudio más detallado de los ACs unidimensionales. Primero veremos que es posible simplificar la reversibilidad de los ACs a su inyectividad sobre las configuraciones periódicas y después usaremos los grafos de de Bruijn para estudiar estos ACs. En el quinto y último capítulo trataremos los ACs particionados, los cuales resultan un método sencillo de construir ACs reversibles y demostraremos que los ACs reversibles de dimensión uno son Turing completos.

## 2 Preliminares

### 2.1 Primeras Definiciones

Un autómata celular (AC) es un modelo de un sistema dinámico discreto en el espacio y el tiempo. Este modelo consiste de una red de células idénticas que contienen un único estado. El AC avanza en pasos discretos según una regla uniforme que determina el nuevo estado de cada célula en base a los estados de cada una de las células de su entorno. La idea es simular un sistema dinámico complejo, como puede ser la difusión de un fluido, a partir de reglas locales sencillas.

**Definición 2.1.** *Formalmente un autómata celular  $A$  es un cuarteto  $A = (d, S, V, f)$  donde:*

1.  $d \in \mathbb{Z}^+$  es la dimensión de la red de células  $\mathbb{Z}^d$
2.  $S$  es el conjunto finito de estados que pueden tomar las células
3.  $V = (v_1, v_2, \dots, v_m)$  es la vecindad finita (de tamaño  $m$ ) donde  $v_i \in \mathbb{Z}^d$  para  $1 \leq i \leq m$  y  $v_i \neq v_j$  para  $1 \leq i < j \leq m$ .
4.  $f$  es la función de transición local  $f : S^m \rightarrow S$

**Definición 2.2.** *Una configuración  $c$  del AC  $A$  es una función que asigna a cada célula un estado.*

$$c : \mathbb{Z}^d \rightarrow S$$

Se puede pensar  $c$  como una foto de los estados de cada célula en un instante de tiempo determinado. El AC cambia el estado de cada célula  $z$  según la regla local  $f$ , en base a los estados de las células de su vecindario  $V(z)$ . De esta forma  $A$  induce la función global de transición  $G$  con la que a menudo se identificará el AC  $A$ .

$$G : S^{\mathbb{Z}^d} \longrightarrow S^{\mathbb{Z}^d}$$

$G$  le asigna a cada configuración  $c$  la nueva configuración  $G(c)$  que se define como sigue

$$G(c)(z) = f(c(z + v_1), c(z + v_2), \dots, c(z + v_m))$$

Esta nueva configuración  $G(c)$  es la que da los nuevos estados de las células tras el paso discreto en el tiempo que se ha producido. Si dos AC tienen la misma función global de transición  $G$  diremos que son equivalentes.

**Ejemplo 2.3.** *El AC más famoso es el juego de la vida de Conway. Consideremos una configuración que en este caso es una red infinita, ortogonal y de dimensión dos en la que cada una de las células se encuentra en uno de los dos estados posibles, viva o muerta. El juego de la vida rige como avanza la configuración en el tiempo. En la Figura 1 vemos un ejemplo de la evolución de una configuración bajo la acción de este AC.*

1. **Nacimiento:** si en el instante  $t$  una célula está muerta y tiene exactamente tres células adyacentes vivas entonces pasa a estar viva en el instante  $t + 1$ .
2. **Supervivencia:** si en el instante  $t$  una célula está viva y tiene dos o tres células adyacentes vivas entonces sigue con vida en el instante  $t + 1$ .
3. **Muerte por despoblación:** una célula (viva o muerta) con como máximo una célula adyacente viva en el instante  $t$  pasa a estar (o sigue estando) muerta en el instante  $t + 1$ .
4. **Muerte por sobrepoblación:** una célula (viva o muerta) con más de tres células adyacentes vivas en el instante  $t$  pasa a estar (o sigue estando) muerta en el instante  $t + 1$ .

Matemáticamente tenemos que el juego de la vida es el AC

$$A = (d, S, V, f)$$

donde la dimensión del juego de la vida es  $d = 2$ , el conjunto de estados es  $S = \{0, 1\}$ ,  $0$  representa que la célula muerta y  $1$  que está viva, la vecindad es el cuadrado de radio 1 centrado en el origen  $V = \{-1, 0, 1\}^2$  y la función local  $f : S^9 \rightarrow S$  se define como

$$f(s_1, s_2, \dots, s_9) = \begin{cases} 1 & \text{si } \begin{cases} \sum_{i=1}^9 s_i = 3 \\ \text{ó} \\ \sum_{i=1}^9 s_i = 4 \text{ y } s_5 = 0 \end{cases} \\ 0 & \text{en otro caso} \end{cases}$$

Si representamos los ceros como cuadros en blanco y los unos como cuadros negros podemos obtener una representación gráfica de la evolución en el tiempo de una configuración inicial.

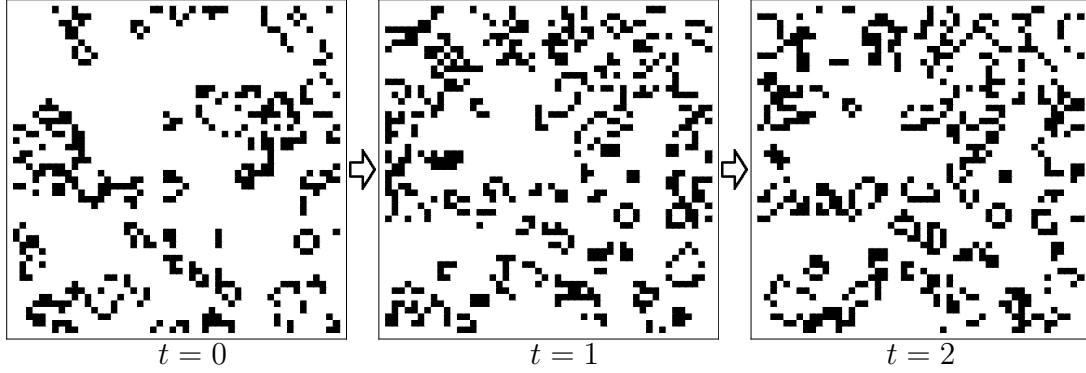


Figura 1: La evolución de una cuadrícula  $50 \times 50$  al aplicarle sucesivamente  $f$

## 2.2 Vecindades

Dado un AC  $A = (d, S, V, f)$  con vecindad  $V = (v_1, v_2, \dots, v_m)$  se dice que la vecindad de una célula  $z \in \mathbb{Z}^d$  es

$$V(z) = (z + v_1, z + v_2, \dots, z + v_m)$$

y sus células vecinas son

$$V(\{z\}) = \{z + v_i \mid 1 \leq i \leq m\}.$$

Más en general las células vecinas de un conjunto  $C \subseteq \mathbb{Z}^d$  son

$$V(C) = \{z + v_i \mid z \in C \text{ y } 1 \leq i \leq m\}.$$

Denotaremos los estados de la vecindad  $V(z)$  de una célula  $s$  por

$$c(V(z)) = (c(z + v_1), c(z + v_2), \dots, c(z + v_m)).$$

De esta forma tenemos que

$$G(c)(z) = f(c(V(z))).$$

Dado que los AC son sobre todo usados para simular modelos físicos y biológicos la vecindad de una célula normalmente constará de un conjunto de células cercanas. Las vecindades más frecuentes son la de Moore y la de von Neumann. Vemos algunos ejemplos de estas vecindades en las Figuras 2 y 3.

La vecindad de von Neumann  $V_r^d$  de radio  $r \in \mathbb{N}$  y dimensión  $d$  se define como

$$V_r^d = \{z = (z_1, z_2, \dots, z_d) \in \mathbb{Z}^d \mid \|z\|_1 = \sum_{i=1}^d |z_i| \leq r\}.$$

La vecindad de Moore  $M_r^d$  de radio  $r$  y dimensión  $d$  es

$$M_r^d = \{z = (z_1, z_2, \dots, z_d) \in \mathbb{Z}^d \mid \|z\|_\infty = \max\{|z_i| \mid 1 \leq i \leq m\} \leq r\}$$

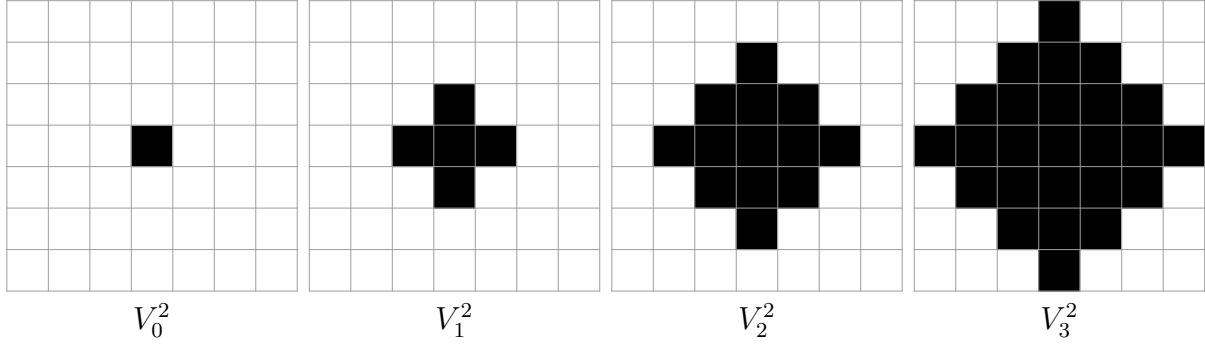


Figura 2: Las vecindades de von Neumann de dimensión  $d = 2$  y radios  $0 \leq r \leq 3$ .

con lo que,  $M_r^d(z)$  es el hipercubo de dimensión  $d$  y aristas de longitud  $2r + 1$  centrado en la célula  $z$ . Por tanto  $M_r^d(z)$  contiene  $(2r + 1)^d$  células.

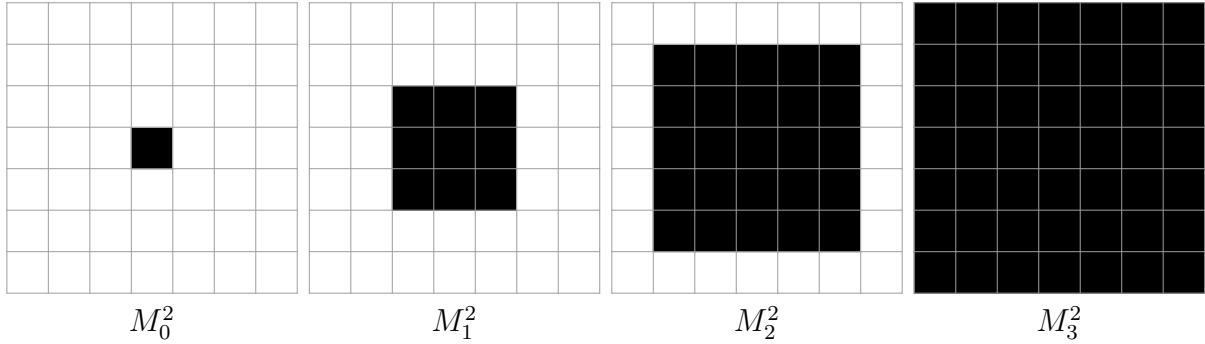


Figura 3: Las vecindades de Moore de dimensión  $d = 2$  y radios  $0 \leq r \leq 3$ .

Un AC  $A = (d, S, V, f)$  es equivalente al autómata celular  $A' = (S, d, V', f')$  donde  $V(\{0\}) \subseteq V'(\{0\})$  y  $f'$  solo depende de las primeras  $m$  coordenadas, reordenando si hace falta. De esta forma si los elementos de  $V$  están contenidos en la vecindad de Moore de dimensión  $d$  y radio  $r$ , es decir,

$$V(\{0\}) \subseteq M_r^d$$

decimos que  $A$  está determinado por un AC de radio  $r$  o simplemente que es un AC de radio  $r$  refiriéndonos a que es equivalente al AC  $A' = (S, d, \bar{B}_r^\infty(0), f')$ .

### 2.3 Configuraciones finitas y periódicas

Dada una configuración  $c \in S^{\mathbb{Z}^d}$  y un estado  $s \in S$  se define el  $s$ -soporte de  $c$  como

$$\text{sop}_s(c) = \{z \in \mathbb{Z}^d \mid c(z) \neq s\}.$$

Es decir, las células que no están en el estado  $s$ . Se dice que  $c$  tiene  $s$ -soporte finito o simplemente que  $c$  es  $s$ -finito si

$$|\text{sop}_s(c)| < \infty.$$

El conjunto de las configuraciones de  $S^{\mathbb{Z}^d}$  que son  $s$ -finitas se denota



$$F_s(d, S) = \{c \in S^{\mathbb{Z}^d} \mid |\text{sop}_s(c)| < \infty\}$$

o simplemente  $F_s$  si  $d$  y  $S$  se sobreentienden. Un estado  $q \in S$  se dice que es quiescente si

$$f(q, q, \dots, q) = q.$$

Una vez fijado un estado quiescente  $q$  se deja de mencionar el estado en los conjuntos definidos anteriormente pues se sobreentiende el estado. De esta forma hablaríamos simplemente del soporte de  $c$

$$\text{sop}(c) = \{z \in \mathbb{Z}^d \mid c(z) \neq q\}$$

y de configuraciones finitas

$$F = \{c \in S^{\mathbb{Z}^d} \mid |\text{sop}(c)| < \infty\}.$$

Es claro que  $G|_F$  manda configuraciones finitas a configuraciones finitas. Esto es por que si  $c$  es configuración finita existe un conjunto finito  $B \subset \mathbb{Z}^d$  tal que dada cualquier célula  $z$  fuera de  $B$  su vecindad  $V(z)$  consistirá en células en el estado  $q$ . Luego tenemos que

$$\forall z \in \mathbb{Z}^d \setminus B \quad G(z) = f(c(V(z))) = f(q, q, \dots, q) = q.$$

Denotamos  $G_F$  por

$$\begin{aligned} G_F : F &\rightarrow F \\ c &\mapsto G(c) \end{aligned}$$

Pasemos ahora a las configuraciones periódicas.

Dado  $r \in \mathbb{Z}^d$  denotamos la traslación por  $r$  por  $\tau_r$  donde

$$\tau_r : S^{\mathbb{Z}^d} \longrightarrow S^{\mathbb{Z}^d}$$

y

$$\forall z \in \mathbb{Z}^d \quad \tau_r(c)(z) = c(r + z).$$

Dado  $k \in \mathbb{Z}$  denotaremos por  $\sigma_k^i$  la traslación por  $k$  en la coordenada  $i$ , es decir

$$\sigma_k^i(c)(z) = c(z_1, z_2, \dots, z_{i-1}, z_i + k, z_{i+1}, \dots, z_d) \quad \forall z = (z_1, z_2, \dots, z_d) \in \mathbb{Z}^d$$

Claramente tenemos que

$$\tau_{r_1} \circ \tau_{r_2} = \tau_{r_1+r_2} \quad \forall r_1, r_2 \in \mathbb{Z}^d$$

Dado  $r \in \mathbb{Z}^d$  una configuración  $c$  se dice que es  $r$ -periódica si  $\tau_r(c) = c$ .

Una configuración  $c \in S^{\mathbb{Z}^d}$  se dice que es totalmente periódica si existen  $z_1, z_2, \dots, z_d \in \mathbb{Z}^d$  linealmente independientes tales que  $c$  es  $z_i$ -periódica,  $1 \leq i \leq d$ . Para un ejemplo de configuración totalmente periódica vease la Figura 4.

El conjunto de configuraciones de  $S^{\mathbb{Z}^d}$  totalmente periódicas se denota  $P(d, S)$  o simplemente  $P$  si la dimensión  $d$  y los estados  $S$  se sobreentienden.

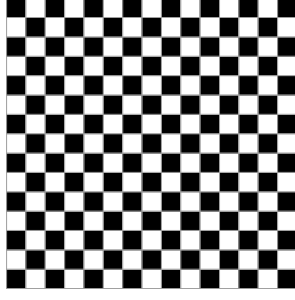


Figura 4: La configuración que asemeja un tablero de ajedrez infinito es totalmente periódica de períodos  $(0,1)$  y  $(1,0)$ .

Como ocurría en el caso de las configuraciones finitas  $G|_P$  manda configuraciones totalmente periódicas a configuraciones totalmente periódicas. Denotaremos por  $G_P$  la restricción de  $G$  a  $P$ .

$$G_P : P \rightarrow P$$

$$c \mapsto G(c)$$

Esto es una consecuencia de la siguiente proposición.

**Proposición 2.4.** Sean  $G$  un AC y  $r \in \mathbb{Z}^d$  cualesquiera la traslación  $\tau_r$  conmuta con  $G$ , es decir,  $\tau_r \circ G = G \circ \tau_r$ .

*Demostración.* Sean  $z \in \mathbb{Z}^d$  y  $c \in S^{\mathbb{Z}^d}$  cualesquiera queremos ver que

$$\tau_r(G(c))(z) = G(\tau_r(c))(z).$$

En efecto, tenemos que

$$\begin{aligned} \tau_r(G(c))(z) &= G(c)(r+z) = f(c(r+z+v_1), \dots, c(r+z+v_m)) \\ &= f(\tau_r(c)(z+v_1), \dots, \tau_r(c)(z+v_m)) = G(\tau_r(c))(z). \end{aligned}$$

□

Esto lo que quiere decir es que da igual trasladar antes o después de aplicar el AC. Por tanto si una configuración es  $r$ -periódica la configuración transformada por un AC también lo será.

Esta proposición nos da otra forma de pensar los AC. Gracias al hecho de que los AC conmutan con traslaciones tenemos que

$$G(c)(z) = \tau_z(G(c))(0) = G(\tau_z(c))(0) = f(\tau_z(c)(v_1), \dots, \tau_z(c)(v_m)).$$

Luego en realidad  $G(c)(z)$  solo depende de los valores que toma la configuración trasladada  $\tau_z(c)$  sobre el conjunto  $\{v_1, v_2, \dots, v_m\}$ . En base a esta discusión podemos definir un AC como una aplicación  $G : S^{\mathbb{Z}^d} \rightarrow S^{\mathbb{Z}^d}$  tal que existe un conjunto finito  $V$  llamado vecindad y una aplicación  $f : S^V \rightarrow S$  llamada función de transición local verificando que

$$G(c)(z) = f(\tau_z(c|_V))$$

para todo  $c \in S^{\mathbb{Z}^d}$  y para todo  $z \in \mathbb{Z}^d$ . Por tanto puesto que las funciones de transición locales de los ACs solo dependen de sus valores sobre  $S^{V\{0\}}$  podemos representar gráficamente un AC dibujando los posibles estados en los que se pueden encontrar el entorno de una célula e indicando el nuevo estado que adquiere la célula. Esto es lo que hacemos en la Figura 5 y la Figura 6.

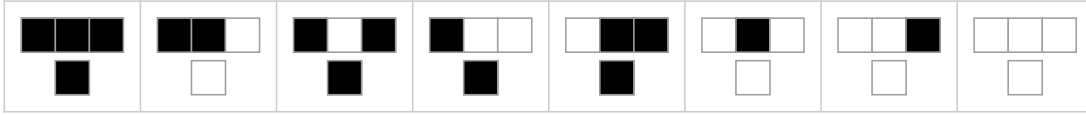


Figura 5: Representación gráfica del AC 184. El cuadrado bajo cada raya indica el nuevo estado de la celda central.

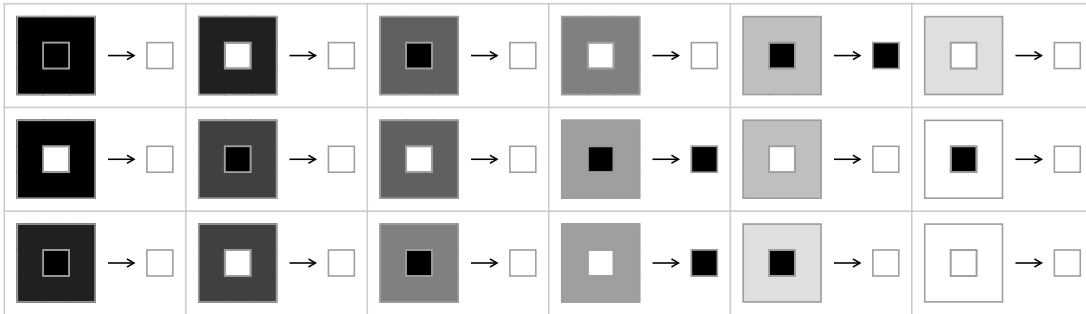


Figura 6: La regla del Juego de la Vida. La célula central es negra si está viva y blanca si está muerta. Las otras ocho células de su vecindad se representan en base a cuantas están vivas. La tonalidad más oscura indica que todas las células están vivas y la menos oscura indica que todas las células están muertas.

## 2.4 Autómatas Celulares Elementales

Un tipo de ACs son los llamados ACs elementales. Fueron estudiados y clasificados por Stephen Wolfram en el año 1983 [5]. Un AC elemental  $A$  es un AC de dimensión  $d = 1$  de radio 1 y con estados  $S = \{0, 1\}$ . Están determinado por sus funciones locales luego podemos identificar un AC elemental de función local  $f$  con los 8 dígitos

$$f(1, 1, 1)f(1, 1, 0)f(1, 0, 1)f(1, 0, 0)f(0, 1, 1)f(0, 1, 0)f(0, 0, 1)f(0, 0, 0).$$

Si convertimos esto a binario obtenemos un entero en el intervalo  $[0, 255]$  mediante la fórmula

$$f(1, 1, 1) \cdot 2^8 + f(1, 1, 0) \cdot 2^7 + \dots + f(0, 0, 1) \cdot 2^1 + f(0, 0, 0) \cdot 2^0.$$

Ahora identificando los  $|S^{V\{0\}}| = 2^{2^3} = 256$  posibles AC elementales con este número tenemos el número de Wolfram del AC  $A$ .

Los AC elementales se pueden representar gráficamente empezando en una fila con una configuración inicial  $c_1$  que consta de una sola célula en el estado 1 y el resto en el estado 0. La segunda fila será la representación de  $G(c_1)$  y así sucesivamente, bajando de fila a volver a aplicar el AC. Realizamos este proceso con el AC 184 en la Figura 7.

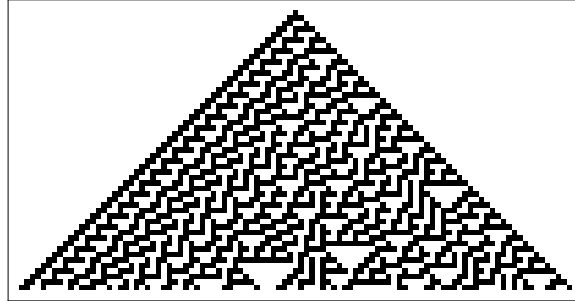


Figura 7: La representación gráfica del AC elemental número 184.

## 2.5 Topología del Espacio de Configuraciones

Definiremos una métrica sobre  $S^{\mathbb{Z}^d}$  como sigue

$$d(c_1, c_2) = \begin{cases} 0 & \text{si } c_1 = c_2 \\ 2^{-\min\{\|z\|_\infty : c_1(z) \neq c_2(z)\}} & \text{si } c_1 \neq c_2 \end{cases}$$

Comprobemos que  $d$  es una métrica:

Es evidente que  $d$  es una función no-negativa, simétrica y que cumple el axioma de co-incidencia. Además veamos que cumple la desigualdad triangular. Sean  $c_1, c_2, c_3 \in S^{\mathbb{Z}^d}$  cualesquiera y denotemos  $z_1, z_2$  y  $z_3$  los elementos mínimos de  $\mathbb{Z}^d$  con la norma infinito tales que  $c_1 \neq c_2, c_2 \neq c_3$  y  $c_3 \neq c_1$  respectivamente. Supongamos por reducción al absurdo que

$$d(c_1, c_2) + d(c_2, c_3) < d(c_1, c_3)$$

entonces por la definición de  $z_1, z_2$  y  $z_3$

$$\begin{aligned} 2^{-\|z_1\|_\infty} + 2^{-\|z_2\|_\infty} < 2^{-\|z_3\|_\infty} &\Rightarrow \|z_3\|_\infty < \min\{\|z_2\|_\infty, \|z_1\|_\infty\} \\ &\Rightarrow c_1(z_3) = c_2(z_3), c_2(z_3) = c_3(z_3) \\ &\Rightarrow c_1(z_3) = c_3(z_3) \end{aligned}$$

Lo cual es una contradicción pues  $c_1(z_3) \neq c_3(z_3)$  por la definición de  $z_3$  con lo que concluimos.

Como acabamos de ver tenemos un espacio métrico  $M = (S^{\mathbb{Z}^d}, d)$  luego la métrica  $d$  induce una topología  $\tau$  cuya base de abiertos consiste en las bolas abiertas de  $M$ . Explícitamente una bola abierta de radio  $\varepsilon = 2^{-r} > 0$  centrada en la configuración  $c$  es

$$B_\varepsilon(c) = \{e \in S^{\mathbb{Z}^d} \mid c(z) = e(z), \|z\|_\infty \leq r\}.$$

Ahora que hemos definido una topología sobre el espacio de configuraciones veremos que una sucesión de configuraciones converge a una configuración  $c$  equivale a que en cualquier célula los valores que toma la sucesión en esa célula coinciden con el valor que toma  $c$  a partir de algún término de la sucesión.

**Proposición 2.5.** *Una sucesión de configuraciones  $(c_n)_{n \in \mathbb{N}}$  converge a la configuración  $c$  si y solo si para todo  $z \in \mathbb{Z}^d$  existe  $N_z \in \mathbb{N}$  tal que para todo  $n \geq N_z$  se cumple que  $c_n(z) = c(z)$ .*

*Demostración.* Si  $(c_n)_{n \in \mathbb{N}}$  converge a  $c$  entonces para todo  $\varepsilon = 2^{-r} > 0$  existe  $N_\varepsilon$  tal que para todo  $n \geq N_\varepsilon$ ,  $c_n \in B_\varepsilon(c)$ . Por tanto dado  $z \in \mathbb{Z}^d$  cualquiera de norma infinito  $k = \|z\|_\infty$  basta considerar  $N_\varepsilon$  para  $\varepsilon = 2^{-k}$  y tenemos que a partir del elemento  $c_{N_\varepsilon}$  todos los elementos de la sucesión  $(c_n)_{n \in \mathbb{N}}$  coinciden en los elementos de  $\mathbb{Z}^d$  de norma infinito menor o igual que  $k$ . Luego en particular coinciden en  $z$ .

Recíprocamente, sea  $\varepsilon = 2^{-r} > 0$  cualquiera queremos encontrar  $N_\varepsilon$  tal que  $c_n \in B_\varepsilon(c)$  para todo  $n \geq N_\varepsilon$ . Es decir, que a partir del elemento número  $N_\varepsilon$  los elementos de la sucesión coincidan en los elementos de  $\mathbb{Z}^d$  cuya norma infinito es menor o igual que  $r$ . Denotemos  $B = \{z \in \mathbb{Z}^d \mid \|z\|_\infty \leq r\}$ . Sabemos por hipótesis que para todo  $z \in B$  existe  $N_z$  tal que  $c_n(z) = c(z)$  para todo  $n \geq N_z$ . Consideremos el número natural  $N_\varepsilon = \max\{N_z \mid z \in B\}$  que existe por ser  $B$  finito. Por definición de  $N_\varepsilon$  tenemos que  $c(z) = c_n(z)$  para todo  $n \geq N_\varepsilon$  y para todo  $z \in B$  luego  $N_\varepsilon$  es el buscado y concluimos.  $\square$

Esta caracterización de la convergencia resulta muy útil y la utilizaremos para demostrar tanto la continuidad de las funciones de AC como la compacidad del espacio de configuraciones

**Proposición 2.6.** *Sea  $(c_n)_{n \in \mathbb{N}}$  una sucesión de  $S^{\mathbb{Z}^d}$  y  $G$  un AC. Si la sucesión  $(c_n)_{n \in \mathbb{N}}$  converge a la configuración  $c$  entonces la sucesión  $(G(c_n))_{n \in \mathbb{N}}$  converge a la configuración  $G(c)$ .*

*Demostración.* Sea  $V = (v_1, v_2, \dots, v_m)$  una vecindad de  $G$  y  $z \in \mathbb{Z}^d$  cualquiera. Sabemos por hipótesis que  $\lim_{n \rightarrow \infty} c_n = c$  luego dado cualquier  $x \in V(\{z\}) = \{z + v_i \mid 1 \leq i \leq m\}$  existe  $N_x > 0$  tal que  $c_n(z) = c(z)$  para todo  $n \geq N_x$ . Consideremos ahora

$$N = \max\{N_x \mid x \in V(\{z\})\}.$$

Este  $N$  nos da la continuidad de  $G$  en  $z$  puesto que si  $n \geq N$  entonces

$$\begin{aligned} G(c_n)(z) &= f(c_n(V(z))) = f(c_n(z + v_1), c_n(z + v_2), \dots, c_n(z + v_m)) \\ &= f(c(z + v_1), c(z + v_2), \dots, c(z + v_m)) = G(c)(z) \end{aligned}$$

con lo que concluimos al ser  $z \in \mathbb{Z}^d$  cualquiera.  $\square$

Veamos ahora que el espacio métrico  $M = (S^{\mathbb{Z}^d}, d)$  es secuencialmente compacto y por tanto compacto. Para ello lo que haremos es dada una sucesión de configuraciones construiremos una subsucesión cuyos elementos coincidan en cada vez más células. Esto último nos dará la convergencia.

**Proposición 2.7.** *Toda sucesión de configuraciones tiene una subsucesión convergente.*

*Demostración.* Sea  $(c_n)_{n \in \mathbb{N}}$  una sucesión de  $S^{\mathbb{Z}^d}$ ,  $n_0 \in \mathbb{N}$  y  $h : \mathbb{N} \simeq \mathbb{Z}^d$  una enumeración de  $\mathbb{Z}^d$  creamos la subsucesión  $(c_{n_k})_{k \in \mathbb{N}}$  donde

$$n_k = \min\{m_k \in \mathbb{N} \text{ verificando las propiedades } (1_k), (2_k) \text{ y } (3_k)\} \quad \text{para } k \geq 1$$

- (1<sub>k</sub>)  $m_k > n_{k-1}$
- (2<sub>k</sub>)  $c_{m_k}(h(i)) = c_{n_{k-1}}(h(i))$  para  $1 \leq i \leq k-1$
- (3<sub>k</sub>) Existe  $A_k \cong \mathbb{N}$  tal que  $c_a(h(i)) = c_{m_k}(h(i))$  para todo  $a \in A_k$  y  $1 \leq i \leq k$

Veamos que existen  $m_k$  verificando estas condiciones. En primer lugar estudiemos el caso  $k = 1$ .

Dado que  $S$  es finito mientras que  $\mathbb{N}$  es infinito existe un número infinito de configuraciones de la sucesión  $(c_n)_{n \in \mathbb{N}}$  que toman el mismo valor  $s$  en el punto  $h(1)$ . Luego existe  $m_1 > n_0$ , es decir, cumpliendo (1<sub>1</sub>) tal que  $c_{m_1}(h(1)) = s$ . Por tanto existe también  $A_1$  verificando (3<sub>1</sub>) mientras que la condiciones (2<sub>1</sub>) se cumple por ser vacía.

Ahora veamos que una vez verificado el caso  $k = 1$  podemos construir los siguientes índices recurrentemente. En efecto, si existen  $n_1, n_2, \dots, n_k$  con  $k \geq 1$  verificando las condiciones que hemos impuesto también existirán un número infinito de  $m_{k+1}$  que verifiquen (2<sub>k+1</sub>) gracias a la condición (3<sub>k</sub>). Además por el argumento de antes al ser  $S$  finito existirán infinitos  $m_{k+1}$  que verifiquen (3<sub>k+1</sub>) y (2<sub>k+1</sub>) luego de entre estos también habrá infinitos que satisfacen (1<sub>k+1</sub>). Por tanto la subsucesión construida existe. Además esta subsucesión converge pues dado  $z = h(i)$  cualquiera gracias a la condición (2<sub>k</sub>) se cumple que

$$c_{n_i}(h(i)) = c_{n_j}(h(i)) \quad \forall j \geq i$$

Por tanto como un espacio métrico es compacto si y solo si es secuencialmente compacto el espacio métrico  $M = (S^{\mathbb{Z}^d}, d)$  es compacto.  $\square$

Otra propiedad que nos será útil más adelante es que las sucesiones totalmente periódicas y las finitas son densas en  $M = (S^{\mathbb{Z}^d}, d)$ . Con esta propiedad en muchos casos podremos generalizar información conocida de estos dos tipos de configuraciones a todo el espacio de configuraciones.

**Proposición 2.8.** *Sea  $c \in S^{\mathbb{Z}^d}$  y  $s \in S$  existen dos sucesiones  $(p_n)_{n \in \mathbb{N}} \subseteq P(d, S)$  y  $(c_n)_{n \in \mathbb{N}} \subseteq F_s(d, S)$  tales que*

$$\lim_{n \rightarrow \infty} p_n = \lim_{n \rightarrow \infty} c_n = c$$

*Demostración.* Para construir una sucesión de configuraciones totalmente periódicas  $(p_n)_{n \in \mathbb{N}}$  convergentes a  $c$  basta con definir  $p_i$  como una configuración que coincide con  $c$  sobre el hipercubo de tamaño  $(2i+1)^d$  centrado en el origen  $C_i^d = \{-i, -i+1, \dots, i\}^d$  y cuyo período es mayor o igual que  $2i+1$  en todas las coordenadas. Claramente una sucesión de este tipo converge a  $c$  pues dado  $z \in \mathbb{Z}^d$   $p_n(z) = c(z)$  para todo  $n \geq \|z\|_\infty$

De forma analoga dada una enumeración  $n : \mathbb{N} \longleftrightarrow \mathbb{Z}^d$  para  $i \geq k$  definimos  $c_i$  como la configuración que coincide con  $c$  en  $\{n(1), \dots, n(k)\}$  y que vale  $s \in S$  fuera de  $\{n(1), \dots, n(k)\}$ , es decir

$$c_i(z) = \begin{cases} c(z) & \text{si } z \in \{f(1), \dots, f(k)\} \\ s & \text{si } z \notin \{n(1), \dots, n(k)\} \end{cases}$$

De nuevo es sencillo ver que la sucesión definida  $(c_n)_{n \in \mathbb{N}}$  converge a  $c$  pues dado  $z \in \mathbb{Z}^d$  sea  $N \in \mathbb{N}$  tal que  $z = n(N)$  para todo  $i \geq N$  se cumple que  $c_i(z) = c(z)$ . Además la sucesión esta formada únicamente por configuraciones finitas por definición luego concluimos.  $\square$

Para acabar esta sección veremos es teorema de Curtis–Hedlund–Lyndon que nos será de utilidad para decidir si un AC es reversible. Pero primero veamos el siguiente lema.

**Lema 2.9.** *Si  $(X, d)$  es un espacio métrico compacto,  $(Y, \rho)$  es un espacio métrico y  $f : X \rightarrow Y$  es una función continua entonces  $f$  es uniformemente continua.*

*Demostración.* Para evitar confusiones denotaremos las bolas en  $X$  con  $B$  y las bolas en  $Y$  con  $B'$ . Puesto que  $f$  es continua para todo  $x \in X$  existe  $\delta_x > 0$  tal que

$$f(B_{\delta_x}(x)) \subseteq B'_{\frac{\varepsilon}{2}}(f(x))$$

Además  $\{B_{\frac{\delta_x}{2}}(x)\}_{x \in X}$  es un recubrimiento de  $X$  por abiertos luego existe un subrecubrimiento finito  $\{B_{\frac{\delta_{x_i}}{2}}(x_i)\}_{i=1}^n$ . Definimos  $\delta = \min\{\frac{\delta_{x_i}}{2} \mid 1 \leq i \leq n\}$  comprobemos que  $\delta$  así definido cumple que

$$f(B_{\delta}(x)) \subseteq B'_{\varepsilon}(f(x)) \quad \forall x \in X.$$

Por ser  $\{B_{\frac{\delta_{x_i}}{2}}(x_i)\}_{i=1}^n$  un recubrimiento de  $X$  existe  $x_i$  tal que  $x \in B_{\frac{\delta_{x_i}}{2}}(x_i)$  además por la definición de  $\delta$  tenemos que si  $y \in B_{\delta}(x)$  entonces  $y \in B_{\delta_{x_i}}(x_i)$  pues

$$d(x_i, y) \leq d(x_i, x) + d(x, y) < \frac{\delta_{x_i}}{2} + \frac{\delta_{x_i}}{2} = \delta_{x_i}$$

Luego si  $d(x, y) < \delta$  entonces

$$\rho(f(x), f(y)) \leq \rho(f(x), f(x_i)) + \rho(f(x_i), f(y)) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

como queríamos ver  $\square$

Ahora estamos listos para ver el teorema de Curtis–Hedlund–Lyndon [6].

**Teorema 2.10.** *Sea  $G : S^{\mathbb{Z}^d} \rightarrow S^{\mathbb{Z}^d}$  una función las siguientes condiciones son equivalentes:*

1.  $G$  es la función de transición global de un AC.
2.  $G$  es continua y conmuta con traslaciones.

*Demostración.* Ya hemos visto que (1)  $\Rightarrow$  (2). Veamos ahora (2)  $\Rightarrow$  (1).

Por el lema anterior al ser  $G$  continua y  $M = (S^{\mathbb{Z}^d}, d)$  un espacio métrico compacto  $G$  es uniformemente continua. Por tanto existe  $r > 0$  tal que para todo  $c \in S^{\mathbb{Z}^d}$

$$G(B_{2-r}(c)) \subseteq B_1(G(c)).$$

Por tanto dados  $c_1, c_2 \in S^{\mathbb{Z}^d}$  si  $c_1(z) = c_2(z)$  para todo  $z \in \mathbb{Z}^d$  tal que  $\|z\|_{\infty} \leq r$  entonces  $G(c_1)(0) = G(c_2)(0)$ . Esto lo que quiere decir es que  $G(c)(0)$  solo depende de la restricción de  $c$  a la bola cerrada  $B = \{z \in \mathbb{Z}^d \mid \|z\|_{\infty} \leq r\}$ . Por tanto existe una función

$$f : S^B \rightarrow S$$

tal que

$$G(c)(0) = f(c|_B)$$

para todo  $c \in S^{\mathbb{Z}^d}$ . Ahora, como por hipótesis  $G$  conmuta con permutaciones tenemos que

$$G(c)(z) = \tau_z(G(c))(0) = G(\tau_z(c))(0) = f(\tau_z(c|_B)).$$

Esto lo que significa es que en efecto  $G$  es la función global de un AC de vecindad  $B$  y función de transición local  $f$ .  $\square$

## 3 Reversibilidad y Equilibrio

### 3.1 Reversibilidad

En esta sección estudiaremos como afectan la inyectividad y epiyectividad de  $G$  a la inyectividad y epiyectividad sus restricciones  $G_F$  y  $G_P$  y viceversa.

**Definición 3.1.** *Un AC  $A = (d, S, V, f)$  con función de transición global  $G$  es inyectivo o epiyectivo si lo es  $G$ .*

**Definición 3.2.** *Se dice que un AC  $A = (d, S, V, f)$  es reversible si su función de transición global  $G$  es biyectiva y  $G^{-1}$  es la función de transición global de un AC.*

Equivalentemente por el teorema de Curtis–Hedlund–Lyndon  $A$  es reversible si  $G$  es una función biyectiva y su función inversa  $G^{-1}$  es continua y conmuta con traslaciones.

Es evidente que si  $G$  es inyectivo  $G_F$  y  $G_P$  también por ser sus restricciones. Sin embargo el recíproco no es cierto. Veamos un contraejemplo de la inyectividad. El AC de disyunción exclusiva  $A = (d = 1, S = \{0, 1\}, v = (0, 1), f)$  donde

$$f(a, b) = \begin{cases} 0 & \text{si } (a, b) = (0, 0) \\ 1 & \text{si } (a, b) = (1, 0) \\ 1 & \text{si } (a, b) = (0, 1) \\ 0 & \text{si } (a, b) = (1, 1) \end{cases}$$

Tenemos que  $G$  no es inyectiva pues por ejemplo si consideramos la configuración  $c_0 \equiv 0$  tenemos que

$$G^{-1}(c) = \{c_0, c_1 \equiv 1\}.$$

Sin embargo  $G_F$  sí es inyectiva pues si fijamos el estado quiescente  $q = 0$  tenemos que  $G$  es inyectiva sobre las configuraciones 0-finitas  $F$ .

Veamos que efectivamente si existen dos configuraciones finitas  $c_1$  y  $c_2$  tales que  $G(c_1) = G(c_2)$  se debe de cumplir que  $c_1 = c_2$ . Por ser  $c_1$  y  $c_2$  distintas existe  $z \in \mathbb{Z}$  tal que  $c_1(z) \neq c_2(z)$ . Supongamos sin pérdida de generalidad que  $c_1(z) = 0$  y  $c_2(z) = 1$ . Usando que  $G(c_1)(z) = G(c_2)(z)$  deducimos que existen dos posibles valores para la pareja  $(c_1(z + 1), c_2(z + 1))$ .

$$\begin{cases} G(c_1)(z) = 0 \Rightarrow (c_1(z + 1), c_2(z + 1)) = (0, 1) \\ G(c_1)(z) = 1 \Rightarrow (c_1(z + 1), c_2(z + 1)) = (1, 0) \end{cases}$$



En todo caso una de las configuraciones tomará el valor 1 en la siguiente célula  $z + 1$  mientras que la otra tomara el estado 0. Podemos seguir usando el mismo razonamiento mientras nos movemos a la derecha de la célula  $z$ . Obtenemos que si la configuración  $c_1$  toma el valor 0  $k$  veces sobre el conjunto  $\{z, z + 1, \dots, z + n\}$  entonces la configuración  $c_2$  toma el valor 1  $n - k + 1$  veces. Por lo tanto al menos una de las configuraciones toma el valor 1 un número infinito de veces lo cual es una contradicción con que es finita.

En cambio la epiyectividad de las restricciones si asegura la epiyectividad del AC

**Proposición 3.3.** *Sea  $G$  un AC tal que  $G_P$  o  $G_F$  es epiyectiva entonces  $G$  también es epiyectiva.*

*Demostración.* Veremos solo el caso en el que  $G_P$  es epiyectiva. El caso en el que  $G_F$  es epiyectiva se demuestra del mismo modo. Dada una configuración  $c'$  veamos que tiene antiimagen. Gracias a la Proposición 2.8 existe una sucesión  $(c'_n)_{n \in \mathbb{N}} \subseteq P$  tal que

$$\lim_{n \rightarrow \infty} c'_n = c'.$$

Por hipótesis  $G_P$  es epiyectiva luego existe una sucesión  $(c_n)_{n \in \mathbb{N}}$  tal que

$$G(c_n) = c'_n \quad \forall n \in \mathbb{N}$$

Por la compacidad de  $S^{\mathbb{Z}^d}$  existe una subsucesión convergente  $(c_{\sigma(n)})_{n \in \mathbb{N}}$  con límite  $c$

$$\lim_{n \rightarrow \infty} c_{\sigma(n)} = c.$$

Ahora usando la continuidad de  $G$  tenemos que

$$\lim_{n \rightarrow \infty} G(c_{\sigma(n)}) = G(\lim_{n \rightarrow \infty} c_{\sigma(n)}) = G(c).$$

Además

$$\lim_{n \rightarrow \infty} G(c_{\sigma(n)}) = \lim_{n \rightarrow \infty} c'_{\sigma(n)} = \lim_{n \rightarrow \infty} c'_n = c'$$

con lo que concluimos que  $G(c) = c'$  como queríamos.  $\square$

**Proposición 3.4.** *Si  $G_P$  es inyectiva entonces  $G_P$  es biyectiva.*

*Demostración.* Dado  $c$  una configuración totalmente periódica veamos que si  $G_P$  es inyectiva entonces  $c$  tiene antiimagen. Por ser  $c$  totalmente periódica existen  $d$  enteros  $\{k_1, k_2, \dots, k_d\}$  tales que

$$\sigma_{k_i}^i(c) = c \quad 1 \leq i \leq d.$$

Denotemos

$$C = \{c \in S \mid \sigma_{k_i}^i(c) = c \quad 1 \leq i \leq d\}.$$

Por la definición de  $C$  una configuración  $c$  perteneciente a  $C$  esta determinado por su imagen sobre el hiperréctangulo de dimensión  $d$  y lados de longitud  $k_i$ . Las configuraciones de  $C$  pueden tomar cualquier valor  $s \in S$  sobre las células del hiperréctangulo. Por tanto

$$|C| = |S^{k_1 \dots k_d}|$$

con lo que  $C$  es finito. Vimos que  $G$  conmuta con permutaciones luego  $G(C) \subseteq C$  pero por hipótesis  $G_P$  es inyectiva luego  $|C| = |G(C)|$  con lo que concluimos que, al ser  $C$  finito,  $G(C) = C$ .  $\square$

**Corolario 3.5.** *Si  $G_P$  es inyectiva entonces  $G$  es epiyectiva.*

*Demostración.* Si  $G_P$  es inyectiva entonces por la Proposición 3.4  $G_P$  es epiyectiva. Ahora usando la Proposición 3.3 concluimos que  $G$  es epiyectiva.  $\square$

**Corolario 3.6.** *Un AC  $G$  es biyectivo si y solo si es inyectivo.*

*Demostración.* Si  $G$  es inyectiva entonces  $G_P$  también lo es. Consecuentemente además de ser inyectiva  $G$  es epiyectiva por el Corolario 3.5.  $\square$

Intentemos ahora simplificar las condiciones que se imponen sobre un AC para que sea reversible. Pero antes veamos el siguiente lema.

**Lema 3.7.** *Si  $f : X \rightarrow Y$  es una función continua y biyectiva definida en un espacio compacto  $X$  y valorada en un espacio métrico  $Y$  entonces  $f^{-1}$  también es continua.*

*Demostración.* Queremos ver que cualquier cerrado  $C \subseteq X$  tiene imagen cerrada. Veamos primero que  $C$  es compacto. Sea  $\{U_i\}_{i \in I}$  un recubrimiento abierto de  $C$  entonces  $C^c \cup \{U_i\}_{i \in I}$  forma un recubrimiento abierto del compacto  $X$  luego existe un subrecubrimiento abierto finito  $\{U_j\}_{j \in J}$ . Este subrecubrimiento está formado únicamente por la unión abiertos de  $\{U_i\}_{i \in I}$  y posiblemente  $C^c$  luego  $\{U_j\}_{j \in J} \setminus C^c$  es un subrecubrimiento finito de  $\{U_i\}_{i \in I}$ .

Visto esto como  $f$  es continua entonces  $f(C)$  es compacto en el espacio métrico  $Y$  luego en particular es cerrado como queríamos.  $\square$

**Proposición 3.8.**  *$G$  es reversible si y solo si es inyectiva.*

*Demostración.* Hemos visto en el Corolario 3.6 que  $G$  es inyectiva si y solo si es biyectiva. Consecuentemente si  $G$  es inyectiva existe su función inversa  $G^{-1}$ . Falta ver que  $G^{-1}$  es la función de transición local de algún AC. Lo haremos usando el Teorema de Curtis–Hedlund–Lyndon. Por la Proposición 2.7 el espacio de configuraciones es compacto con lo que podemos aplicar el Lema 3.7 a  $G$  para obtener que  $G^{-1}$  es una función continua. Además  $G^{-1}$  conmuta con traslaciones pues sea  $\tau_r$  una traslación cualquiera entonces

$$G^{-1} \circ \tau_r = G^{-1} \circ \tau_r \circ G \circ G^{-1} = G^{-1} \circ G \circ \tau_r \circ G^{-1} = \tau_r \circ G^{-1}.$$

Por tanto  $G^{-1}$  es continua y conmuta con traslaciones luego por el teorema de Curtis–Hedlund–Lyndon es la función de transición global de una AC.  $\square$

## 3.2 Epiyectividad y Equilibrio

Para empezar daremos varias definiciones que nos serán de utilidad.

– Dado un AC  $G$  se dice que una configuración  $c$  es una configuración Jardín de Edén si no tiene antiimagen. Es decir, si

$$G^{-1}(c) = \emptyset$$

Por definición tenemos que la existencia de configuraciones Jardín de Edén equivale a la no epiyectividad del AC.

– Dado un subconjunto de  $D \subseteq \mathbb{Z}^d$  definimos un patrón  $p$  sobre  $D$  como una aplicación

$$p : D \rightarrow S.$$

– Un patrón  $p \in S^D$  decimos que es finito si su dominio  $D$  es finito.

– Decimos que dos patrones  $p_1 \in S^{D_1}$  y  $p_2 \in S^{D_2}$  son disjuntos si sus respectivos dominios son disjuntos,  $D_1 \cap D_2 = \emptyset$ .

– Se dice que  $p_2$  es un subpatrón de  $p_1$  si  $D_2 \subseteq D_1$  y  $p_1|_{D_2} = p_2$ .

– Se dice que  $p_1$  contiene una copia de  $p_2$  si existe una traslación  $\tau_r$  tal que el patrón trasladado  $\tau_r(p_2) = (\tau_r(D), g \circ \tau_r)$  es un subpatrón de  $p_1$ .

Los patrones se pueden pensar como mini-configuraciones aunque si el dominio de un patrón es la totalidad de  $\mathbb{Z}^d$  entonces el patrón también es una configuración.

Podemos estudiar el cambio que produce un AC sobre un patrón de forma similar a como vimos como transforman los AC a las configuraciones. De forma análoga al caso de las configuraciones tenemos que dado un AC  $G$  de vecindad  $V$ , un patrón  $p \in S^D$  y un subconjunto  $D' \subseteq \mathbb{Z}^d$  cuya vecindad  $V(D')$  está contenida en  $D$  el AC  $G$  induce un nuevo patrón  $p' \in S^{D'}$  definido de la siguiente forma:

$$p'(z) = p(V(z)) \quad \forall z \in D'.$$

Esta transformación se denotará

$$G^{D \rightarrow D'} : S^D \rightarrow S^{D'}$$

$$p \mapsto p'$$

Tenemos que  $G^{\mathbb{Z}^d \rightarrow \mathbb{Z}^d} = G$ . El concepto análogo al de configuración Jardín de Edén para el caso de los patrones es un patrón huérfano.

**Definición 3.9.** *Un patrón finito  $p' \in S^{D'}$  es huérfano si no tiene antiimagen, es decir, si no existe ningún patrón  $p = (D, g)$  tal que  $G^{D \rightarrow D'}(p) = p'$ .*

En realidad basta con que no exista antiimagen entre los patrones de dominio  $V(D')$  pues  $G^{D \rightarrow D'}(p)$  está determinado por  $p|_{V(D')}$  por la definición de  $G^{D \rightarrow D'}$ . Además se cumple que la existencia de huérfanos es equivalente a la no epiyectividad del AC como veremos en la siguiente proposición.

**Proposición 3.10.** *Un AC  $G$  tiene una configuración Jardín de Edén si y solo si también tiene algún patrón huérfano.*

*Demostración.* Si  $p \in S^D$  es huérfano entonces todas las configuraciones que coinciden con  $p$  sobre  $D$  y tienen cualquier valor en  $D^c$  son configuraciones Jardín de Edén. Es decir, una configuración que contiene un patrón huérfano es una configuración Jardín de Edén.

Recíprocamente si  $G$  no es epiyectivo entonces  $G(S^{\mathbb{Z}^d}) \subsetneq S^{\mathbb{Z}^d}$ . Además sabemos que  $G$  es una aplicación continua sobre el espacio de configuraciones que es compacto con la métrica  $d$  definida anteriormente. Luego  $G(S^{\mathbb{Z}^d})$  también es compacto en un espacio métrico y por tanto cerrado. Por tanto el conjunto de las configuraciones Jardín de Edén  $G(S^{\mathbb{Z}^d})^c \neq \emptyset$  es abierto y contiene alguna bola abierta  $B_{2-r}(c')$ . Consecuentemente  $B_{2-r}(c') = \{e \in S^{\mathbb{Z}^d} \mid c'(z) = e(z) \forall z \in \mathbb{Z}^d \mid \|z\|_\infty \leq r\}$  esta formado únicamente por configuraciones Jardín de Edén. Ahora si consideramos el patrón  $p' = c'|'_D$  donde  $D' = \{z \in \mathbb{Z}^d \mid \|z\|_\infty \leq r\}$  es la bola de radio  $r$  con la norma infinito tenemos que  $p'$  es huérfano. Esto es porque si existiese  $p \in S^D$  tal que  $G^{D \rightarrow D'}(p) = p'$  entonces una configuración que coincidiese con  $p$  sobre  $D$  tendría imagen en  $B_{2-r}(c')$  que está formado únicamente por configuraciones Jardín de Edén. Por tanto llegamos a contradicción al suponer que  $p'$  no es huérfano con lo que concluimos.  $\square$

La parte central de esta subsección es la relación que existe entre la epiyectividad de un AC y el equilibrio del AC.

**Definición 3.11.** *Un AC es equilibrado si se cumple que todos los patrones (con dominio) del mismo tamaño tienen el mismo número de antiimágenes.*

**Lema 3.12.** *Para todo  $s, d, n, r \in \mathbb{Z}^+$  existe  $k_0 \in \mathbb{Z}^+$  tal que  $\forall k > k_0$*

$$(s^{n^d} - 1)^{k^d} < s^{(kn-2r)^d}$$

*Demostración.* Esta desigualdad es equivalente a las siguientes:

$$k^d \cdot \log_s(s^{n^d} - 1) < (kn - 2r)^d$$

$$\log_s(s^{n^d} - 1) < \left(n - \frac{2r}{k}\right)^d$$

Además tenemos que  $\log_s(s^{n^d} - 1) < n^d$  y por otra parte  $\lim_{k \rightarrow \infty} \left(n - \frac{2r}{k}\right)^d = n^d$  luego concluimos.  $\square$

Si  $s$  es el número de estados  $|S|$  y consideramos un AC  $G$  radio  $r$  tenemos que  $s^{(kn)^d}$  es el número de patrones posibles con dominio un hipercubo  $D$  de dimensión  $d$  y lado  $kn$  mientras que  $(kn - 2r)^d$  es el número máximo de sus imágenes por  $G^{D \rightarrow D'}$  donde  $D'$  es el hipercubo de dimensión  $d$  y lado  $kn - 2r$ . Luego intuitivamente lo que nos dice este lema es que si hay algunos patrones con la misma imagen entonces  $G$  no es epiyectiva. Usaremos este lema para demostrar la siguiente proposición.

**Proposición 3.13.** *Sea  $G$  un AC de radio  $r$ ,  $s = |S|$  el número de estados,  $p' \in S^{D'}$  un patrón finito y  $D \subseteq \mathbb{Z}^d$  un conjunto finito cumpliendo que  $V(D') \subseteq D$ . Entonces si  $G$  es epiyectivo se cumple que el número de antiimágenes del patrón  $p$  con dominio  $D$  son*

$$|\{p \in S^D \mid G^{D \rightarrow D'}(p) = p'\}| = s^{|D| - |D'|}.$$

*En particular el AC  $G$  es equilibrado.*

*Demostración.* Primero veamos que la proposición se cumple para el caso en el que  $D$  y  $D'$  son hipercubos. Sean  $D$  y  $D'$  hipercubos de dimensión  $d$  y aristas de longitud  $n$  y  $n - 2r$  respectivamente. Supongamos por reducción al absurdo que existe algún patrón  $p_0 \in S^{D'}$  tal que

$$|(G^{D \rightarrow D'})^{-1}(p_0)| \neq s^{|D|-|D'|}.$$

Entonces necesariamente existe algún patrón  $p'_0 \in S^{D'}$  tal que

$$a = |(G^{D \rightarrow D'})^{-1}(p'_0)| < s^{|D|-|D'|}.$$

Si esto no fuese cierto entonces todos los patrones de dominio  $D'$  tendrían al menos  $s^{|D|-|D'|}$  antiimágenes con dominio  $D$  y al menos uno de ellos tendría más antiimágenes. Pero entonces

$$|(G^{D \rightarrow D'})^{-1}(S^{D'})| > \sum_{p \in S^{D'}} s^{|D|-|D'|} = |S^D|$$

lo cual es imposible. Ahora sea  $k \in \mathbb{Z}^+$  cualquiera. Sea  $H$  un hipercubo de dimensión  $d$  y lado  $kn$  y sea  $H'$  el hipercubo de lado  $kn - 2r$  centrado dentro de  $H$  definimos

$$P = \{H_i, 1 \leq i \leq k^d\}$$

como la partición de  $H$  en  $k^d$  hipercubos de lado  $n$ . legimos otros  $k^d$  hipercubos  $H'_i$  tales que

$$H'_i \subset H' \cap H_i \quad 1 \leq i \leq k^d.$$

Podemos ver una representación gráfica de estas particiones en la Figura 8.

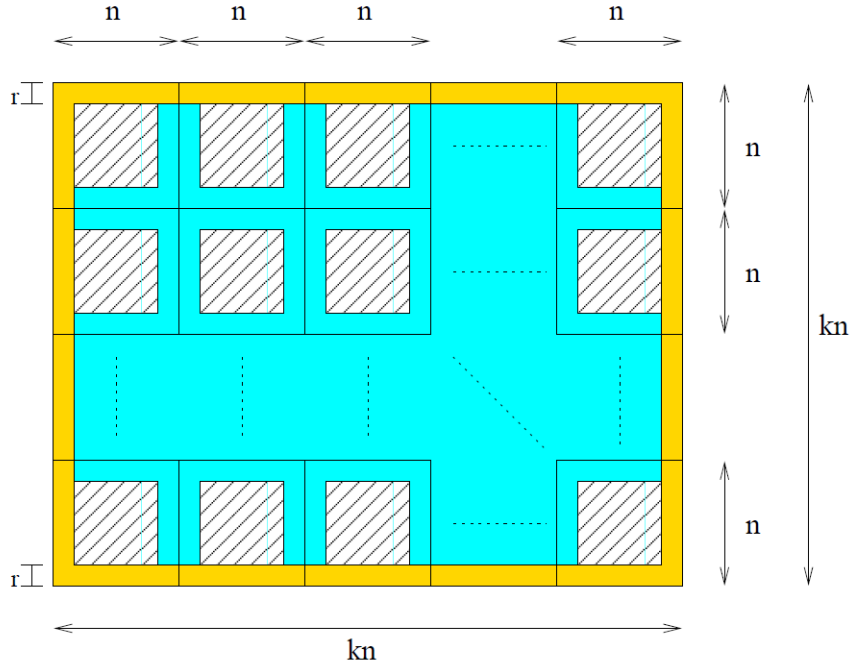


Figura 8: Los hipercubos  $H$ ,  $H'$ ,  $H_i$  y  $H'_i$  en dimensión 2. Imagen extraída de [7].

Consideremos  $C'$  el conjunto de los patrones con dominio  $H'$  que contienen una copia trasladada de  $p'$  en cada uno de los  $k^d$  hipercubos  $H'_i$ . Los patrones que están en  $C'$  están determinados en los  $k^d$  hipercubos  $H'_i$  por  $p'_0$  y pueden tomar cualquier valor en el resto de las  $|H'| - k^d|D'| = |H'| - k^d(n - 2r)^d$  células. Por lo tanto

$$|C'| = s^{|H'| - k^d(n - 2r)^d}.$$

Por otro lado consideremos

$$C = \{p \in S^H \mid G^{H \rightarrow H'}(p) \in C'\}.$$

el conjunto de patrones sobre  $H$  cuya imagen por  $G$  coincide con la de  $p'_0$  sobre los hipercubos  $H'_i$ . Por la definición de  $a$

$$|C| = a^{k^d}.$$

Hemos construido estos conjuntos porque ahora queremos ver que  $|C| < |C'|$  y así llegar a contradicción con que el AC  $G$  es epiyectivo pues  $C = (G^{D \rightarrow D'})^{-1}(C')$ .

Por la elección de  $p'_0$ , el hecho de que  $a$  y  $s^{|D| - |D'|}$  son enteros positivos y que  $0 < s^{-|D'|} \leq 1$  tenemos que las siguientes desigualdades son ciertas:

$$\begin{aligned} a &< s^{|D| - |D'|} \\ a &\leq s^{|D| - |D'|} - s^{-|D'|} \\ a^{k^d} &\leq (s^{|D| - |D'|} - s^{-|D'|})^{k^d} \\ a^{k^d} &\leq s^{-k^d|D'|} (s^{|D|} - 1)^{k^d}. \end{aligned}$$

Sabemos por el Lema3.12 que para algún  $k$  suficientemente grande

$$(s^{n^d} - 1)^{k^d} < s^{(kn - 2r)^d}$$

y como

$$|D| = n^d \quad |H'| = (kn - 2r)^d$$

tenemos que para  $k$  suficientemente grande

$$(s^{|D|} - 1)^{k^d} < s^{|H'|}.$$

Luego sustituyendo en la desigualdad  $a^{k^d} \leq s^{-k^d|D'|} (s^{|D|} - 1)^{k^d}$  tenemos que

$$a^{k^d} < s^{|H'| - k^d|D'|}$$

o lo que es lo mismo

$$|C| < |C'|$$

como queríamos ver.

Falta ver que la proposición sigue siendo cierta en el caso general en el que  $D$  y  $D'$  son conjuntos finitos tales que  $V(D') \subseteq D$ . Podemos escoger  $n$  tal que  $D$  esté contenido en un hipercubo  $H$  de dimensión  $d$  y lado  $n$  y  $D'$  esté contenido en un hipercubo  $H'$  de dimensión  $d$  y lado  $n - 2r$ . Sea  $p' \in S^{D'}$  un patrón cualquiera con dominio  $D'$  llamemos

$$a = |(G^{D \rightarrow D'})^{-1}(p')|.$$

Queremos ver que  $a = s^{|D|-|D'|}$ . Definamos

$$P' = \{p \in S^{H'} : p|_{D'} = p'\}$$

como el conjunto de patrones sobre  $H'$  que contienen al patrón  $p'$ . Están determinados en  $D'$  y pueden tomar cualquier estado en el resto de las  $|H'| - |D'|$  células. Por tanto

$$|P'| = s^{|H'|-|D'|}.$$

Por la parte de la proposición que demostramos para hipercubos como los que tenemos ahora se cumple que

$$|(G^{H \rightarrow H'})^{-1}(P')| = |P'| \cdot s^{|H|-|H'|} = s^{|H'|-|D'|} \cdot s^{|H|-|H'|} = s^{|H|-|D'|}.$$

Por otro los patrones de dominio  $H$  cuya imagen por  $G$  está en  $H'$  son justamente los patrones que contienen una antiimagen de  $p'$  en  $D'$  luego por la definición de  $a$

$$|(G^{H \rightarrow H'})^{-1}(P')| = a \cdot s^{|H|-|D'|}.$$

Por tanto obtenemos la igualdad

$$s^{|H|-|D'|} = a \cdot s^{|H|-|D'|}.$$

Despejando obtenemos  $a = s^{|D|-|D'|}$  con lo que concluimos al ser  $p'$  un patrón cualquiera sobre  $D'$ .  $\square$

## 4 El Teorema del Jardín de Edén

El teorema del Jardín de Edén fue desarrollado por Moore[8] y Myhill[9] en los años 60. Estos autores demostraron que la epiyectividad de un AC es equivalente a una propiedad denominada pre-inyectividad. Como su nombre sugiere la pre-inyectividad es una condición necesaria pero no suficiente para la inyectividad.

**Definición 4.1.** *Dos patrones finitos  $p_1, p_2 \in S^D$  son gemelos respecto a un AC  $G$  si para todo par de configuraciones  $c_1$  y  $c_2$  tales que*

1.  $c_1|_D = p_1$
2.  $c_2|_D = p_2$
3.  $c_1|_{D^c} = c_2|_{D^c}$

*se cumple que  $G(c_1) = G(c_2)$ .*

Esto lo que quiere decir es que dos patrones con el mismo dominio finito son gemelos si en una configuración que contiene uno de los patrones se puede sustituir el patrón por su gemelo sin cambiar cual es la imagen de la configuración por el AC. Además fijado un dominio finito  $D \subseteq \mathbb{Z}^d$  el hecho de ser gemelos es una relación de equivalencia sobre los patrones con dominio  $D$ . De esta forma decimos que  $p_1$  y  $p_2$  están relacionados  $p_1 \sim p_2$  si  $p_1$  y  $p_2$  son gemelos.

**Definición 4.2.** Un AC  $G$  es pre-inyectivo si existen dos configuraciones  $c_1, c_2 \in S^{\mathbb{Z}^d}$  tales que

$$|\{z \in \mathbb{Z}^d \mid c_1(z) \neq c_2(z)\}| < \infty \quad y \quad G(c_1) = G(c_2).$$

Es decir,  $G$  es pre-inyectivo si existen dos configuraciones casi iguales con distinta imagen.

**Proposición 4.3.** Dado un AC  $G$  las siguientes condiciones son equivalentes

1.  $G_F$  no es inyectiva
2.  $G$  tiene patrones gemelos
3.  $G$  no es pre-inyectivo

Veamos  $1 \iff 2 \iff 3$

*Demostración.* ( $1 \iff 2$ )

Si los patrones  $p_1 \in S^D$  y  $p_2 \in S^D$  son gemelos respecto a  $G$  y  $q$  es un estado quiescente entonces las configuraciones finitas  $c_1$  y  $c_2$  tienen la misma imagen por  $G$  donde

$$c_1(z) = \begin{cases} p_1(z) & \text{if } z \in D \\ q & \text{if } z \in D^c \end{cases} \quad c_2(z) = \begin{cases} p_2(z) & \text{if } z \in D \\ q & \text{if } z \in D^c \end{cases}$$

Recíprocamente si  $G_F$  no es inyectiva entonces existen dos configuraciones finitas  $c_1$  y  $c_2$  tales que  $G(c_1) = G(c_2)$ . Llamemos  $A = \{z \in \mathbb{Z}^d \mid c_1(z) \neq c_2(z)\}$  el conjunto finito donde  $c_1$  y  $c_2$  son distintos y sea  $r \in \mathbb{Z}$  tal que  $G$  es un AC de radio  $r$ . Fijemos  $x \in \mathbb{Z}^d$  cualquiera y elijamos  $n \in \mathbb{Z}^+$  tal que el hipercubo  $\bar{B}_{n-2r}^\infty(x)$  de dimensión  $d$  y lado  $n - 2r$  centrado en la célula  $x$  contiene a  $A$ . Consideremos ahora los patrones

$$p_1 = c_1|_{\bar{B}_n^\infty(x)} \quad p_2 = c_2|_{\bar{B}_n^\infty(x)}$$

y veamos que son gemelos. Sea  $c$  una configuración cualquiera que contiene el patrón  $p_1$  y denotemos  $c'$  el patrón que se obtiene al cambiar el patrón  $p_1$  por el patrón  $p_2$ . Queremos ver que  $G(c)(z) = G(c')(z)$  para todo  $z \in \mathbb{Z}^d$ .

En efecto sea  $z \in \mathbb{Z}^d$  tal que  $V(\{z\}) \subseteq A^c$ , es decir, tal que la vecindad de  $z$  no contiene células en las que se diferencian  $c_1$  y  $c_2$  entonces

$$c(V(z)) = c'(V(z))$$

luego  $G(c)(z) = G(c')(z)$ . Ahora sea  $z \in \mathbb{Z}^d$  tal que  $V(z) \cap A \neq \emptyset$ . Por la definición de  $r$  la célula  $z$  se encuentra como mucho a una distancia  $r$  (con la norma infinito) de  $A$  luego se encuentra en  $\bar{B}_n^\infty(x)$  y por tanto

$$G(c)(z) = G(c_1)(z) = G(c_2)(z) = G(c')(z)$$

como queríamos ver.

( $2 \iff 3$ )

Si  $p_1 \in S^D \sim p_2 \in S^D$  entonces por definición de patrones gemelos cualquier par de configuraciones  $c_1, c_2$  tales que

$$c_1|_{D^c} = c_2|_{D^c} \quad c_2|_D = p_2 \quad c_1|_D = p_1$$



niegan la pre-inyectividad. Recíprocamente si  $G$  no es pre-inyectiva existen  $c_1, c_2$  configuraciones distintas, casi iguales y con la misma imagen por  $G$ . Definamos

$$dif(c_1, c_2) = \{z \in \mathbb{Z}^d \mid c_1(z) \neq c_2(z)\}$$

Definamos

$$D = dif(c_1, c_2) + V(\{0\}) - V(\{0\})$$

y veamos que los patrones  $p_1 = c_1|_D$  y  $p_2 = c_2|_D$  son gemelos. Consideremos una configuración  $c$  que contiene el patrón  $p_1$  y llamemos  $c'$  la configuración obtenida al intercambiar el patrón  $p_1$  por  $p_2$ . Deseamos verificar que  $G(c)(z) = G(c')(z)$  para todo  $z \in \mathbb{Z}^d$

En efecto sea  $z \in (dif(c_1, c_2) - V(\{0\}))^c$  entonces

$$V(\{z\}) \subseteq (dif(c_1, c_2) - V(\{0\}))^c + V(\{0\}) \subseteq dif(c_1, c_2)^c$$

con lo que el vecindario de  $z$  no tiene células en las que difieren  $c_1$  y  $c_2$  y consecuentemente

$$G(c)(z) = f(c(V(z))) = f(c'(V(z))) = G(c')(z).$$

Ahora si  $z \in dif(c_1, c_2) - V(\{0\})$  entonces

$$V(z) \in dif(c_1, c_2) - V(\{0\}) + V(\{0\}) = D$$

luego

$$G(c)(z) = G(c|_D)(z) = G(c_1)(z) = G(c_2)(z) = G(c'|_D)G(c')(z)$$

con lo que concluimos.  $\square$

**Proposición 4.4.** *Un AC  $G$  es epiyectivo si solo si su restricción a configuraciones finitas  $G_F$  es inyectiva.*

*Demostración.* Supongamos primero que  $G_F$  no es inyectiva. Por la proposición anterior sabemos que existen dos patrones  $p_1, p_2$  gemelos que tienen como dominio común un hipercubo  $D$  de dimensión  $d$  y lado  $n$  para algún  $n > 2r$ , donde un AC de radio  $r$  determina a  $G$ . Sea  $H$  un hipercubo de lado  $kn$ , para lo que veremos a continuación da igual donde está el hipercubo pues los ACs son invariantes por traslaciones. Podemos particionar  $H$  en  $k^d$  hipercubos de radio  $r$ . Denotaremos a esta partición

$$P = \{H_i, 1 \leq i \leq k^d\}.$$

Además definimos  $H'$  como el hipercubo cocéntrico con  $H$  de lado  $kn - 2r$ . Si  $G$  fuese epiyectivo entonces  $G^{H \rightarrow H'}$  también lo sería con lo que tendríamos que

$$|Im(G^{H \rightarrow H'})| = |S^{H'}| = s^{(kn-2r)^d}.$$

Veamos que no es el caso. Para ello definimos la familia de relaciones de equivalencia sobre cada uno de los hipercubos de la partición  $P$ :

$$R = \{\sim_i, 1 \leq i \leq k^d\}$$

donde  $p = (H_i, g) \sim_i p' = (H_i, g)$  si son gemelos. Es decir, dos patrones están relacionados por la relación  $\sim_i$  si son patrones gemelos con dominio común el hipercubo  $H_i$  de la partición  $P$ . Por último definamos la relación de equivalencia  $\sim$  sobre el hipercubo  $H$  donde dos patrones con dominio común  $H$  están relacionados si son gemelos. A partir de estas definiciones podemos observar lo siguiente:

1. Dos gemelos tienen la misma imagen luego  $p \sim p' \Rightarrow G^{H \rightarrow H'}(p) = G^{H \rightarrow H'}(p')$ . Por tanto

$$|Im(G^{H \rightarrow H'})| \leq |S^H \setminus \sim|.$$

2. Si las restricciones de dos patrones con dominio común  $H$  están relacionados en todos los hipercubos de la partición  $P$  entonces esos patrones también están relacionados sobre  $H$ . Es decir si  $p, p' \in S^H$  entonces

$$p|_{H_i} \sim p'|_{H_i}, 1 \leq i \leq k^d \Rightarrow p \sim p'.$$

3. Si  $\tau_i$  es la traslación tal que aplicada al dominio común  $D$  de los gemelos  $p_1, p_2$  resulta el hipercubo  $H_i$  de la partición  $P$

$$\tau_i(D) = H_i$$

entonces puesto que los  $AC$  conmutan con traslaciones

$$p_1 \circ \tau_i \sim_i p_2 \circ \tau_i.$$

Por lo tanto cada hipercubo de  $P$  tiene al menos dos elementos que están relacionados. Consecuentemente

$$|S^{H_i} \setminus \sim_i| \leq s^{n^d} - 1$$

donde  $s = |S|$ .

Ahora usemos estas observaciones para demostrar la primera implicación

$$\begin{aligned} |Im(G^{H \rightarrow H'})| &\stackrel{1.}{\leq} |S^H \setminus \sim| = |(S^{H_1} \times S^{H_2} \times \dots \times S^{H_{k^d}}) \setminus \sim| \\ &\stackrel{(*)}{\leq} \prod_{i=1}^{n^d} |S^{H_i} \setminus \sim_i| \stackrel{3.}{\leq} \prod_{i=1}^{n^d} (s^{n^d} - 1) = (s^{n^d} - 1)^{k^d} \end{aligned}$$

donde hemos usado en  $(*)$  que por 2. la función

$$\begin{aligned} f : S^{H_1} \setminus \sim_1 \times S^{H_2} \setminus \sim_2 \times \dots \times S^{H_{k^d}} \setminus \sim_{k^d} &\longrightarrow S^H \setminus \sim \\ ([p^1]_1, [p^2]_2, \dots, [p^{k^d}]_{k^d}) &\mapsto [p^1, p^2, \dots, p^{k^d}] \end{aligned}$$

está bien definida y es epiyectiva donde  $[p^i]_i$  denota la clase de equivalencia del patrón  $p^i$  por la clase de equivalencia  $\sim_i$  y el patrón  $(p^1, p^2, \dots, p^{k^d}) \in S^H$  denota el patrón que restringido al hipercubo  $H_i$  es igual al patrón  $p_i \in S^{H_i}$ . Además sabemos que para  $k$  suficientemente grande

$$(s^{n^d} - 1)^{k^d} < s^{(kn-2r)^d}$$

luego concluimos que

$$|Im(G^{H \rightarrow H'})| < s^{(kn-2r)^d}$$

para  $k$  suficientemente grande. Es decir,  $G$  tiene un huérfano de dominio  $H'$  con lo que  $G$  no es epiyectivo por la Proposición 3.10 como queríamos ver.

Recíprocamente si  $G$  no es epiyectiva entonces existe un patrón huérfano de la forma

$p \in S^D$ . Podemos suponer que  $D$  es un hipercubo de lado  $n \geq 2r$  pues si no basta considerar un patrón de dominio un hipercubo de lado mayor o igual que  $2r$  y que contiene a  $p$  por lo que también sería un patrón huérfano. Sea  $H$  un hipercubo de lado  $kn$  lo podemos particionar igual que antes en

$$P = \{H_i, 1 \leq i \leq k^d\}.$$

Definimos  $H'$  como el hipercubo cocéntrico con  $H$  de lado  $kn - 2r$ . Sea

$$K = \{c \in S^{\mathbb{Z}^d} \mid \text{sop}(c) \subseteq H'\}$$

el conjunto de configuraciones finitas con soporte en  $H'$ . Veamos que  $|G(K)| < |K|$ . En efecto por la elección de  $r$  tenemos que

$$\forall c \in K \text{ sop}(c) \in H.$$

Además  $G(c)$  no puede contener una copia del patrón  $p \in S^D$  en ninguno de los  $n^d$  hipercubos en los que esta particionado  $H$  pues  $p$  es huérfano. Luego como  $G(c)$  está determinado por sus valores en  $H$  hay

$$(s^{n^d} - 1)^{k^d}$$

posibles configuraciones  $G(c)$ . Pero

$$|K| = (kn - 2r)^d$$

luego por el lema anterior existe  $k > 0$  tal que

$$|G(K)| < |K|.$$

□

**Ejemplo 4.5.** *El AC  $G$  del Juego de la Vida no es inyectivo. Por ejemplo la configuración  $c_1 \equiv 0$  y la configuración  $c_2$  en la que todas las células están muertas (en el estado 0) salvo la célula 1 tienen la misma imagen*

$$G(c_1) = c_1 = G(c_2).$$

Luego como  $G$  es de radio 1 los patrones

$$p_1 = c_1|_{\bar{B}_2^\infty(z)} \quad p_2 = c_2|_{\bar{B}_2^\infty(z)}$$

centrados en la célula  $z$  son gemelos. En la Figura 9 vemos un ejemplo de patrones gemelos de tamaño  $3 \times 3$ , en la Figura 10 representamos un cuadrado  $15 \times 15$  que puede contener nueve patrones de tamaño  $3 \times 3$  y en la Figura 11 vemos un ejemplo de patrones gemelos de tamaño  $15 \times 15$ .

0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0

0	0	0	0	0
0	0	0	0	0
0	0	1	0	0
0	0	0	0	0
0	0	0	0	0

Figura 9: patrones  $p_1$  y  $p_2$  donde la célula roja es la célula  $z$ .

Sea  $k \in \mathbb{Z}$  consideremos el cuadrado  $H$  de lado  $5k$  particionado en  $k^2$  cuadrados  $\{H_i, 1 \leq i \leq k^2\}$  de lado 5

$H_1$	$H_2$	$H_3$
$H_4$	$H_5$	$H_6$
$H_7$	$H_8$	$H_9$

Figura 10:  $H$  para  $k = 3$ .

Para  $1 \leq i \leq k^2$  en  $S^{H_i}$  definimos la relación de equivalencia  $\sim_i$  tal que dos patrones  $p_i, p'_i \in S^{H_i}$  están relacionados si y solo si son gemelos. Ahora si dos patrones  $p, p' \in S^H$  sobre el cuadrado grande  $H$  cumplen que sus restricciones a los cuadrados pequeños están relacionados tenemos que  $p$  y  $p'$  están relacionados y en particular tienen la misma imagen por  $G$ .

$p_1$	$p_2$	$p_2$	$p_2$	$p_2$	$p_2$
$p_1$	$p_2$	$p_2$	$p_2$	$p_2$	$p_2$
$p_1$	$p_1$	0 0 0 0 0 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0	$p_2$	$p_1$	0 0 0 0 0 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0

Figura 11: dos patrones sobre  $H$  cuyas restricciones son gemelas.

Básicamente cualquier vez que un patrón  $p \in S^H$  contiene el patrón  $p_1$  o  $p_2$  en alguno de los cuadrados pequeños en los que se divide podemos cambiar este patrón por su gemelo sin cambiar su imagen por  $G$ . Por tanto podemos descontar de las imágenes de  $G$  las que provienen de un patrón en  $S^H$  con  $p_2$  en uno de los cuadrados pequeños. De esta forma conseguimos que

$$|Im(G^{H \rightarrow H'})| \leq (2^{5^2} - 1)^{k^2}$$

y se cumple que si  $k = 4651631920$  entonces

$$(2^{5^2} - 1)^{k^2} < 2^{(5k-2)^2} = |H'|$$

con lo que  $G$  no es epiyectivo aunque a priori es imposible encontrar el huérfano.

## 5 AC unidimensionales

### 5.1 Resultados teóricos

Trataremos ahora los AC unidimensionales. Veremos que se puede simplificar incluso más la reversibilidad en una dimensión.

**Definición 5.1.** *Dos configuraciones  $c_1, c_2$  son positivamente (respectivamente negativamente) asintóticas si existe  $z_0 \in \mathbb{Z}$  tal que*

$$c_1(z) = c_2(z) \quad \forall z \geq z_0 \text{ (respectivamente } z \leq z_0 \text{)}.$$

**Definición 5.2.** *Dos configuraciones  $c_1, c_2$  están positivamente (respectivamente negativamente)  $r$ -separadas con  $r \in \mathbb{Z}$  si existe  $z_0 \in \mathbb{Z}$  tal que*

$$\exists k \in \{z, z+1, \dots, z+r\} \mid c_1(k) \neq c_2(k) \quad \forall z \geq z_0 \text{ (respectivamente } z \leq z_0 \text{)}.$$

**Proposición 5.3.** *Sea  $G$  un AC unidimensional determinado por un AC de radio  $r$ . Si  $G$  es epiyectivo y  $c_1 \neq c_2$  son dos configuraciones tales que  $G(c_1) = G(c_2)$  entonces se cumple exactamente una de las siguientes condiciones:*

1.  $c_1$  y  $c_2$  están positiva y negativamente  $2r$ -separadas.
2.  $c_1$  y  $c_2$  son positivamente asintóticas y están negativamente  $2r$ -separadas.
3.  $c_1$  y  $c_2$  son negativamente asintóticas y están positivamente  $2r$ -separadas.

*Demostración.* Se puede cumplir como mucho una de las siguientes condiciones pues dos configuraciones no pueden ser a la vez positivamente (respectivamente negativamente) asintóticas y estar positivamente (respectivamente negativamente)  $k$ -separadas con  $k \in \mathbb{Z}^+$ . El teorema del Jardín de Edén nos dice que puesto que  $G$  es epiyectiva no pueden existir dos configuraciones casi iguales con la misma imagen luego en particular es imposible que dos configuraciones positiva y negativamente asintóticas tengan la misma imagen. Concluiríamos al ver que  $c_1$  y  $c_2$  tienen que estar positivamente  $2r$ -separadas o ser positivamente asintóticas y que además tienen que estar negativamente  $2r$ -separadas o ser negativamente asintóticas pues entonces se tendría que dar una de las condiciones del enunciado. En efecto si por reducción al absurdo  $c_1$  y  $c_2$  no están positivamente  $2r$ -separadas ni son positivamente asintóticas entonces existen:

1. Un intervalo  $I_1 = \{z_1, z_1 + 1, \dots, z_1 + 2r\}$  de longitud  $2r$  tal que  $c_1|_{I_1} = c_2|_{I_1}$ .
2. Un entero  $k > z_1 + 2r$  a la derecha de  $I_1$  tal que  $c_1(k) \neq c_2(k)$ .
3. Otro intervalo  $I_2 = \{z_2, z_2 + 1, \dots, z_2 + 2r\}$  de longitud  $2r$  a la derecha del entero  $k$  tal que  $c_1|_{I_2} = c_2|_{I_2}$ .

Pero entonces si definimos  $D$  como el conjunto  $D = \{z_1 + 2r, z_1 + 2r + 1, \dots, z_2\}$  y definimos la configuración  $c'_1$  como la obtenida al sustituir en  $c_1$  el patrón  $p_1 = c_1|_D$  por el patrón  $p_2 = c_2|_D$  tenemos que  $c_1$  y  $c'_1$  son casi iguales y

$$G(c_1) = G(c'_1).$$

Pues si  $V(\{z\}) \cap D = \emptyset$  entonces

$$G(c_1)(z) = f(c(V(z))) = f(c'(V(z))) = G(c'_1)(z)$$

Mientras que si  $V(\{z\}) \cap D \neq \emptyset$  puesto que el autómata celular es de radio  $r$  entonces

$$V(\{z\}) \subseteq D \cup I_1 \cup I_2.$$

y por lo tanto

$$G(c')(z) = f(c'(V(z))) = f(c_2(V(z))) = G(c_2)(z) = G(c_1)(z)$$

con lo que hemos llegado a contradicción con el teorema del Jardín de Edén. El razonamiento para ver que  $c_1$  y  $c_2$  deben de ser negativamente asintóticas o estar  $2r$ -separadas es completamente simétrico luego concluimos.  $\square$

**Proposición 5.4.** *Si  $G$  es un AC unidimensional entonces  $G$  es reversible si y solo si  $G_P$  es inyectiva.*

*Demostración.* Si  $G$  es reversible, es decir, inyectiva entonces su restricción a las configuraciones periódicas también. Recíprocamente si  $G_P$  es inyectiva entonces por el Corolario 3.5  $G$  es epiyectiva. Por tanto si existen dos configuraciones  $c_1$  y  $c_2$  tales que

$$c_1 \neq c_2 \quad G(c_1) = G(c_2)$$

por la Proposición 5.3  $c_1$  y  $c_2$  deben de estar positiva o negativamente  $2r$ -separadas donde  $G$  está determinado por un AC de radio  $r$ . Veamos el caso en el cual las configuraciones están positivamente  $2r$ -separadas pues al igual que antes el caso negativo es simétrico. Definimos  $I = \{0, 1, \dots, 2r\}$  un intervalo de longitud  $2r + 1$  y definimos  $C_1$  como el conjunto de patrones contenidos en la configuración  $c_1$  de dominio  $2r + 1$  enteros consecutivos

$$C_1 = \{c_1|_{\tau_k(I)} \mid k \in \mathbb{Z}\}.$$

Solo hay  $s^{2r+1}$  posibles combinaciones de estados que se pueden dar sobre un dominio de  $2r + 1$  células. Sin embargo,  $C_1$  es un conjunto infinito con lo que existe al menos un patrón  $p_1 \in C_1$  que se repite infinitas veces. Es decir, que está contenido infinitas veces en la configuración  $c_1$ . Por tanto existe una sucesión creciente de enteros  $(k_n)_{n \in \mathbb{N}}$  tal que los patrones  $c_1|_{\tau_{k_n}(I)}$  son copias trasladadas  $\forall n \in \mathbb{N}$ . Ahora definamos  $C_2$  como el conjunto de patrones contenidos en  $c_2$  de dominios  $\tau_{k_n}(I)$ .

$$C_2 = \{c_2|_{\tau_{k_n}(I)} \mid n \in \mathbb{N}\}.$$

Una vez más  $C_2$  es un conjunto infinito luego hay algún patrón que se repite infinitas veces. Es decir, existe una subsucesión creciente  $(\sigma(k_n))_{n \in \mathbb{N}}$  de  $(k_n)_{n \in \mathbb{N}}$  tal que los patrones  $c_2|_{\tau_{\sigma(k_n)}(I)}$  son copias trasladadas  $\forall n \in \mathbb{N}$ . Además por ser  $(\sigma(k_n))_{n \in \mathbb{N}}$  una subsucesión de

$(k_n)_{n \in \mathbb{N}}$  se cumple que existen  $\sigma(k_{n_1})$  y  $\sigma(k_{n_2})$ , que denotaremos  $k_1$  y  $k_2$  para aligerar la notación, arbitrariamente grandes tales que

$$k_2 \geq k_1 + 2r + 1 \quad c_1|_{\tau_{k_1}(I)} \sim c_1|_{\tau_{k_2}(I)} \quad c_2|_{\tau_{k_1}(I)} \sim c_2|_{\tau_{k_2}(I)}.$$

Donde  $p_1 \sim p_2$  denota que  $p_1$  y  $p_2$  son copias trasladadas. Además puesto que  $c_1$  y  $c_2$  están  $2r$  separadas podemos escoger  $k_1$  y  $k_2$  como antes de forma que

$$c_1|_{\tau_{k_1}(I)} \approx c_2|_{\tau_{k_1}(I)}.$$

Definamos ahora las configuraciones de periódicas  $c'_1$  y  $c'_2$  como las que coinciden con  $c_1$  y  $c_2$  respectivamente en  $D = \{k_1, k_1 + 1, \dots, k_1 + 2r, \dots, k_2 - 1\}$  y cuyo período es  $k_2 - k_1$ . Dado  $z \in \mathbb{Z}$  existen  $n \in \mathbb{Z}$  y  $a \in \mathbb{Z}$  tales que

$$z = n(k_2 - k_1) + a$$

luego por construcción de  $c'_1$  y  $c'_2$

$$c'_1(V(z)) = c_1(V(a)) \quad c'_2(V(z)) = c_2(V(a))$$

por lo que  $G(c'_1)(z) = G(c'_2)(z)$  para todo  $z \in \mathbb{Z}$ . Por la elección de  $k_1$  y  $k_2$  las configuraciones  $c'_1$  y  $c'_2$  difieren en algún elemento del intervalo  $D$ . Pero entonces  $G_P$  no es inyectiva con lo que hemos llegado a una contradicción con la hipótesis al suponer que  $G$  no es reversible.  $\square$

## 5.2 Grafos de de Bruijn

Sigamos con el estudio de ACs unidimensionales. Esta vez lo haremos con los grafos de de Bruijn.

**Definición 5.5.** *Un grafo dirigido es un par ordenado  $H = (N, E)$  donde*

1.  $N$  es un conjunto cualquiera cuyos elementos llamaremos nodos o vértices.
2.  $E$  es un subconjunto de  $N^2$  cuyos elementos llamaremos aristas.

**Definición 5.6.** *Un grafo dirigido etiquetado  $H = (N, E, e)$  es un grafo  $(N, E)$  junto con una función*

$$e : E \rightarrow X.$$

*En tal caso  $e$  asigna a cada arista  $a \in E$  el elemento  $e(a) \in X$  que llamaremos la etiqueta de  $a$ .*

Vemos un ejemplo de este tipo de grafo en la Figura 12.

**Definición 5.7.** *Dado un grafo dirigido  $H$  definimos la función cola  $\alpha$  como*

$$\begin{aligned} \alpha : E &\rightarrow N \\ (n_1, n_2) &\mapsto n_1 \end{aligned}$$

*y la función cabeza  $\beta$  como*

$$\begin{aligned} \beta : E &\rightarrow N \\ (n_1, n_2) &\mapsto n_2 \end{aligned}$$

*Decimos que la arista  $a$  tiene cola  $\alpha(a)$  y cabeza  $\beta(a)$ . Además decimos que la arista  $a$  conecta su cola con su cabeza y que la cola y la cabeza son nodos adyacentes.*

Los grafos dirigidos etiquetados se pueden representar gráficamente dibujando los nodos como puntos o círculos entorno al nodo y dibujando las aristas como flechas que van de su cola a su cabeza. Las etiquetas se escriben sobre las flechas o aristas a las que corresponden.

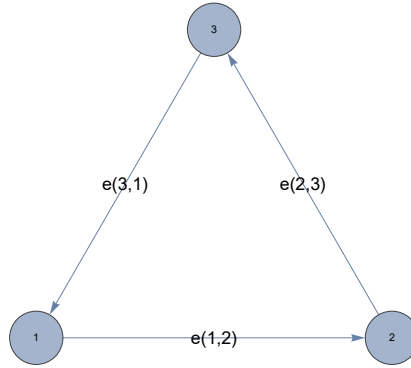


Figura 12: El grafo dirigido de nodos  $N = \{1, 2, 3\}$  aristas  $E = \{(1, 2), (2, 3), (3, 1)\}$  y etiqueta  $e$

**Definición 5.8.** Un trayecto o camino  $t$  de longitud  $k$  del grafo dirigido  $H = (N, E)$  es una función

$$t : \{1, 2, \dots, k\} \rightarrow E$$

tal que

$$\alpha(t(i + 1)) = \beta(t(i)), 1 \leq i < k.$$

Es decir, es un conjunto ordenado  $\{t(1), \dots, t(k)\}$  de  $k$  aristas tal que la cabeza de cada arista conecta con la cola de la siguiente arista. Análogamente definimos un trayecto infinito  $t$  como una función

$$t : \mathbb{Z} \rightarrow E$$

tal que

$$\forall i \in \mathbb{Z} \quad \alpha(t(i + 1)) = \beta(t(i)).$$

Si el grafo  $H$  está etiquetado por la función  $e$  entonces decimos que un trayecto  $t$  de  $H$  está etiquetado por  $e_t$  o que  $e_t$  es la etiqueta de  $t$  donde

$$e_t = e \circ t.$$

Además decimos que el trayecto  $t$  conecta los nodos  $\alpha(t(i))$  y  $\beta(t(i))$  donde  $i$  pertenece al dominio  $Dom(t)$  de  $t$ . Por último definimos los nodos  $N(t)$  y las aristas  $E(t)$  del trayecto  $t$  como los conjuntos

$$N(t) = \{\alpha(t(i)), \beta(t(i)) \mid i \in Dom(t)\},$$

$$E(t) = \{t(i) \mid i \in Dom(t)\}.$$

Los trayectos se pueden representar de la misma forma que los grafos considerando ahora el conjunto de nodos como  $N(t)$  y de aristas como  $E(t)$ . Dos subtipos de trayectos son los ciclos y los bucles



**Definición 5.9.** Un ciclo de longitud  $k$  es un trayecto  $t$  de longitud  $k$  tal que el primer y el último vértice son iguales, es decir,

$$\alpha(t(1)) = \beta(t_k).$$

Un ciclo infinito es un trayecto infinito  $t$  cuyos vértices se repiten periódicamente, es decir, existe  $i \in \mathbb{N}$  tal que

$$\forall j \in \mathbb{Z} \quad \alpha(t(j+i)) = \alpha(t(j)).$$

Un bucle  $t$  es un trayecto cuyos nodos son todos iguales, es decir, tal que

$$|N(t)| = 1$$

Veamos ahora un tipo de grafo particular que usaremos para representar los ACs de dimensión uno.

**Definición 5.10.** El grafo de de Bruijn  $B$  de dimensión  $m$  sobre el conjunto finito de estados  $S$  es el grafo dirigido  $B = (N, E)$  donde

1.  $N = S^m$
2.  $E = \{((s_1, s_2, \dots, s_m), (s_2, s_3, \dots, s_m, s_{m+1})) \in S^m \times S^m\}$

En la Figura 13 mostramos un ejemplo de grafo de de Bruijn. En los grafos de de Bruijn las aristas pueden tener cualquier nodo de cola pero la cabeza debe conseguirse eliminando la primera coordenada de la cola, desplazando el resto un espacio hacia la izquierda y añadiendo un estado cualquiera al final. Por este motivo podemos por simplicidad identificar la arista

$$a = ((s_1, s_2, \dots, s_m), (s_2, s_3, \dots, s_m, s_{m+1})) \in (S^m)^2$$

con

$$(s_1, s_2, s_3, \dots, s_m, s_{m+1}) \in S^{m+1}.$$

Esta es la notación que utilizaremos a partir de ahora. De esta forma los trayectos del grafo de de Bruijn son los que conectan nodos que se solapan. De esto deducimos que los grafos de de Bruijn están fuertemente conectados, es decir dado dos nodos cualesquiera del grafo existe un trayecto que los conecta.

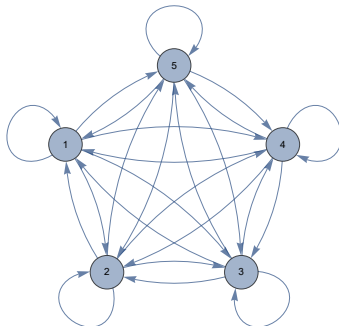


Figura 13: Grafo de de Bruijn de dimensión  $m = 1$  sobre  $S = \{1, 5\}$

Dada una configuración unidimensional  $c \in S^{\mathbb{Z}}$  existe un trayecto infinito que denotaremos  $t_c$  tal que

$$\forall i \in \mathbb{Z} \quad t_c(i) = (c(i), c(i+1), \dots, c(i+m)).$$

Análogamente dado un trayecto infinito  $t \in (S^{m+1})^{\mathbb{Z}}$  existe una configuración unidimensional  $c_t \in S^{\mathbb{Z}}$  tal que

$$\forall i \in \mathbb{Z} \quad c_t(i) = \pi_1(t(i)).$$

Donde  $\pi_1$  es la proyección en la primera en la primera coordenada de  $S^{m+1}$ . Claramente estas asignaciones son cada una la inversa de la otra pues

$$\begin{aligned} \forall i \in \mathbb{Z} \quad t_{c_t}(i) &= (c_t(i), c_t(i+1), \dots, c_t(i+m)) = (\pi_1(t(i)), \pi_1(t(i+1)), \dots, \pi_1(t(i+m))) \\ &= (\pi_1(t(i)), \pi_2(t(i)), \dots, \pi_{m+1}(t(i))) = t(i) \end{aligned}$$

donde se ha usado que

$$\forall i \in \mathbb{Z} \quad \pi_1(t(i+k)) = \pi_{1+k}(t(i)), 1 \leq k \leq m$$

por ser  $t$  un trayecto infinito en un grafo de de Bruijn. Por otro lado tenemos que

$$\forall i \in \mathbb{Z} \quad c_{t_c}(i) = \pi_1(t_c(i)) = \pi_1(c(i), c(i+1), \dots, c(i+m)) = c(i)$$

como queríamos ver.

Ahora que hemos visto estas definiciones podemos ver como se relacionan los grafos de de Bruijn con los AC.

**Definición 5.11.** *Dado un AC  $A = (d, S, V, f)$  de radio  $r$  definimos la representación de de Bruijn  $B(A)$  de  $A$  como el grafo de de Bruijn de dimensión  $m = 2r$  sobre  $S$  etiquetado por la función de transición local  $f$ .*

Para estudiar los ACs a partir de sus representaciones de de Bruijn será fundamental la siguiente relación entre la etiqueta de un trayecto en la representación de de Bruijn y la imagen por el AC de la configuración inducida por el trayecto.

**Proposición 5.12.** *Dado un trayecto infinito  $t$  etiquetado por  $f_t$  tenemos que*

$$G(c_t) = f_t \circ \sigma_{-r}$$

y dada una configuración  $c \in S^{\mathbb{Z}}$

$$G(c) = f_{t_c} \circ \sigma_{-r}.$$

Es decir, la imagen por  $G$  de la configuración inducida por el trayecto es la etiqueta traslada por menos el radio del AC. La relación entre la imagen por el AC de una configuración y la etiqueta del trayecto inducido es la misma.

*Demostración.* Sea  $i \in \mathbb{Z}$  cualquiera y  $t$  un trayecto infinito entonces

$$\begin{aligned} G(c_t)(i) &= f(c_t(i-r), c_t(i-r+1), \dots, c_t(i+r)) \\ &= f(t(i-r)) = f_t(i-r) = f_t \circ \sigma_{-r}(i) \end{aligned}$$

Con lo que la primera parte de la proposición es cierta. Por otro lado dada una configuración  $c \in S^{\mathbb{Z}}$  si  $i \in \mathbb{Z}$  es cualquiera entonces.

$$\begin{aligned} G(c)(i) &= f(c(i-r), c(i-r+1), \dots, c(i+r)) \\ &= f(t_c(i-r)) = f(t_c \circ \sigma_{-r}(i)) = f_{t_c} \circ \sigma_{-r}(i) \end{aligned}$$

con lo que concluimos. □

Una vez vista esta relación fundamental traduzcamos algunos otros conceptos de los ACs a las representaciones de de Bruijn

**Proposición 5.13.** *Si  $A = (d, S, V, f)$  es un AC de radio  $r$  y  $B(A)$  es su representación de de Bruijn entonces las siguientes afirmaciones son ciertas:*

1.  *$A$  es inyectivo si y solo si todas los trayectos infinitos distintos de  $B(A)$  tienen etiquetas distintas.*
2.  *$A$  es epiyectivo si y solo si dada cualquier configuración  $c$  existe un trayecto infinito  $t$  tal que  $t$  está etiquetado por  $c$ .*
3. *Dado  $s \in S$  y dada una configuración  $c$  que es  $s$ -finita el trayecto inducido por  $c$  consiste en un bucle infinito en el vértice  $(s, s, \dots, s)$  seguido de un ciclo finito que acaba en el mismo vértice  $(s, s, \dots, s)$ .*
4. *Una configuración periódica de período  $k$  induce un ciclo infinito de período  $k$ .*

*Demostración.* 1. Por reducción al absurdo si  $A$  es inyectivo y existen dos trayectos distintos  $t_1 \neq t_2$  tales que

$$f_{t_1} = f_{t_2}$$

entonces

$$c_{t_1} \neq c_{t_2}$$

y

$$G(c_{t_1}) = f_{t_1} \circ \sigma_{-r} = f_{t_2} \circ \sigma_{-r} = G(c_{t_2})$$

lo cual es una contradicción puesto que  $A$  es inyectivo. Recíprocamente supongamos por reducción al absurdo que  $A$  no es inyectivo. Entonces existen dos configuraciones distintas  $c_1 \neq c_2$  tales que

$$G(c_1) = G(c_2).$$

Pero entonces

$$f_{t_{c_1}} \circ \sigma_{-r} = f_{t_{c_2}} \circ \sigma_{-r} \iff f_{t_{c_1}} = f_{t_{c_2}}$$

con lo que los trayectos  $t_{c_1}$  y  $t_{c_2}$  tendrían la misma etiqueta lo cual es una contradicción pues al ser  $c_1 \neq c_2$  entonces también  $t_{c_1} \neq t_{c_2}$ .

2. Supongamos primero que  $A$  es epiyectivo y sea  $c' \in S^{\mathbb{Z}}$  una configuración cualquiera. Por la epiyectividad de  $A$  existe  $c \in S^{\mathbb{Z}}$  tal que

$$G(c) = c'.$$

Pero entonces por la proposición 5.12

$$f_{t_{c \circ \sigma_r}} = G(c_{t_{c \circ \sigma_r}}) \circ \sigma_{-r} = G(c_t) = G(c) = c'$$

con lo que  $c'$  es la etiqueta del trayecto  $t_{c \circ \sigma_r}$ . Recíprocamente supongamos que toda configuración es la etiqueta de algún trayecto infinito. Sea  $c'$  una configuración cualquiera y sea  $t$  el trayecto tal que

$$f_t = c'.$$

Entonces

$$G(c_t) = f_t \circ \sigma_{-r} = c' \circ \sigma_{-r}$$

luego dado que las traslaciones conmutan con los AC

$$G(c_t \circ \sigma_r) = c'.$$

3. Se sigue la Definición 5.9.

4. Se sigue de la Definición 5.9.

□

Ahora definiremos el grafo doble que nos servirá para estudiar la inyectividad y la epiyectividad de los ACs unidimensionales.

**Definición 5.14.** *Dado un grafo etiquetado  $H = (N, E, e)$  definimos su grafo doble  $H_2$  como el grafo etiquetado*

$$H_2 = (N \times N, E_2, e_2)$$

donde

$$E_2 = \{(a_1, a_2) \in E^2 \mid e(a_1) = e(a_2)\}$$

y

$$e_2((a_1, a_2)) = e(a_1) = e(a_2).$$

Es decir, las aristas del grafo doble son los pares ordenados de aristas del grafo original que tienen misma etiqueta. En particular si consideramos el grafo doble de la representación de de Bruijn de un AC la arista  $(a_1, a_2)$  pertenece al grafo doble si y solo si

$$f(a_1) = f(a_2).$$

Consideremos ahora los trayectos de los grafos dobles. Claramente existe una biyección entre un trayecto en el grafo doble  $H_2$  y dos trayectos con la misma etiqueta en el grafo original  $H$ . Los trayectos  $t_1$  y  $t_2$  de  $H$  a los que se corresponde el trayecto  $t$  de  $H_2$  son los que cumplen que

$$(t_1(i), t_2(i)) = t(i)$$

donde  $1 \leq i \leq \text{long}(t)$  si  $t$  es un trayecto finito o  $i \in \mathbb{Z}$  si  $t$  es un trayecto infinito. De esta forma dado un trayecto  $t$  del grafo doble escribiremos

$$t = (t_1, t_2).$$

**Definición 5.15.** El conjunto diagonal  $\Delta$  del grafo doble  $H_2 = (N \times N, E_2, e_2)$  de  $H = (N, E)$  es

$$\Delta = \{(n, n) \in N^2\}.$$

Por la definición de  $\Delta$  es claro que los trayectos de  $H' = (N^2, E^2, e_2)$  con todos sus nodos dentro de  $\Delta$  son trayectos del grafo doble  $H_2$ . Además tenemos la siguiente proposición

**Proposición 5.16.** El conjunto diagonal  $\Delta$  del grafo doble  $B(A)_2$  de la representación de de Bruijn  $B(A)$  de un AC  $A$  está fuertemente conectado.

*Demostración.* Existe un isomorfismo de grafos entre el subgrafo

$$B(A)_2[\Delta] = (\Delta, E_2[\Delta], f_2)$$

inducido por  $\Delta$  y la representación de de Bruijn

$$B(A) = (S^{2r}, S^{2r+1}, f)$$

donde  $E_2[\Delta]$  son las aristas del grafo doble que tienen cabeza y cola en  $\Delta$ . Es decir, existe una biyección  $g$  entre  $\Delta$  y  $S^{2r}$  tal que dos nodos  $n_1, n_2$  de  $\Delta$  son adyacentes si y solo si  $g(n_1)$  y  $g(n_2)$  son nodos adyacentes de  $S^{2r}$ . Este isomorfismo es

$$g : \Delta \rightarrow S^{2r}$$

$$(n, n) \mapsto n$$

Por tanto dos nodos  $n_1$  y  $n_2$  de  $\Delta$  están conectados por el trayecto  $g^{-1} \circ t$  donde  $t$  es un trayecto de  $B(A)$  que une los nodos  $f(n_1)$  y  $f(n_2)$ . El trayecto  $t$  existe por ser los grafos de de Bruijn fuertemente conectados.

□

**Proposición 5.17.** Si  $B$  es la representación de de Bruijn del AC  $G$  entonces  $G$  es reversible si y solo si todos los trayectos infinitos del grafo doble  $B_2$  tienen sus nodos contenidos en el conjunto diagonal  $\Delta$ .

*Demostración.* Sea  $G$  un AC inyectivo y supongamos por reducción al absurdo que existe un trayecto  $t = (t_1, t_2)$  de  $B_2$  con algún nodo fuera de  $\Delta$ . Puesto que algún nodo de  $t$  está fuera de  $\Delta$  se cumple que  $t_1 \neq t_2$  luego las configuraciones  $c_{t_1}$  y  $c_{t_2}$  inducidas por  $t_1$  y  $t_2$  respectivamente son distintas. Por ser  $t = (t_1, t_2)$  un trayecto del grafo doble  $t_1$  y  $t_2$  tienen la misma etiqueta, es decir

$$f_{t_1} = f_{t_2}.$$

Ahora usando la Proposición 5.12

$$\forall i \in \mathbb{Z} \quad G(c_{t_1})(i) = f_{t_1} \circ \sigma_{-r}(i) = f_{t_2} \circ \sigma_{-r}(i) = G(c_{t_2})(i)$$

con lo que llegamos a una contradicción con que  $G$  es inyectivo.

Recíprocamente supongamos que que todos los trayectos infinitos del grafo doble  $B_2$

tienen sus nodos en el conjunto diagonal  $\Delta$ . Por reducción al absurdo si  $G$  no es inyectivo existen dos configuraciones distintas  $c_1$  y  $c_2$  tales que

$$G(c_1) \neq G(c_2).$$

Los trayectos inducidos  $t_{c_1}$  y  $t_{c_2}$  tienen la misma etiqueta pues por la proposición 5.12

$$f_{t_{c_1}} = G(c_1) \circ \sigma_r = G(c_2) \circ \sigma_r = f_{t_{c_2}}$$

consecuentemente el trayecto  $t = (t_{c_1}, t_{c_2})$  es un trayecto del grafo doble  $B_2$ . Además

$$c_1 \neq c_2 \Rightarrow t_{c_1} \neq t_{c_2}$$

luego el trayecto  $t$  no tiene a todos sus nodos contenidos en  $\Delta$  con lo que hemos llegado a un contradicción al suponer que  $G$  no es inyectivo.  $\square$

Podemos reducir incluso más las condiciones que pedimos al grafo doble  $B_2$  para que  $G$  sea reversible. Vimos en la proposición 5.4 que si  $G$  es un AC unidimensional entonces  $G$  es reversible si y solo si  $G_P$  es inyectiva. Veamos como se refleja esto en el grafo doble.

**Proposición 5.18.** *Dado un AC unidimensional  $G$  las siguientes afirmaciones son ciertas*

1.  $G$  es reversible si y solo si todos los ciclos de su grafo doble tienen sus nodos en  $\Delta$ .
2.  $G$  no es epiyectiva si y solo si su grafo doble tiene un ciclo con al menos un nodo en  $\Delta$  y al menos un nodo fuera de  $\Delta$ .

1. Por la Proposición 5.17 si  $G$  es reversible todos los ciclos infinitos del grafo doble tienen sus nodos en  $\Delta$ . Consecuentemente los ciclos finitos también deben tener sus nodos en  $\Delta$  pues si existiese un ciclo  $t$  de longitud  $k$  con algún nodo fuera de  $\Delta$  entonces el ciclo infinito

$$\begin{aligned} t' : \mathbb{Z} &\rightarrow E_2 \\ a + ki &\mapsto t(a) \end{aligned}$$

que se consigue repitiendo periódicamente los nodos de  $t$  tendría infinitos nodos fuera de  $\Delta$  lo cual sería una contradicción con la proposición anterior.

Recíprocamente si  $G$  no es reversible entonces por la proposición 5.4  $G_P$  no es inyectiva con lo que existen configuraciones periódicas  $c_1, c_2$  distintas y con la misma imagen por el AC  $G$ . Luego siguiendo el mismo procedimiento que en la Proposición 5.17 el trayecto  $(t_{c_1}, t_{c_2})$  inducido está en el grafo doble y tiene nodos fuera de  $\Delta$ . Luego por la proposición 5.13 es un ciclo infinito del grafo doble.

2. Por el teorema del Jardín de Edén si  $G$  no es epiyectiva entonces existen dos configuraciones finitas  $c_1, c_2 \in S^{\mathbb{Z}}$  distintas y con la misma imagen por  $G$ . Como vimos en la demostración de la proposición 5.17 al tener las dos configuraciones la misma imagen por  $G$  el trayecto inducido  $(t_{c_1}, t_{c_2})$  está en el grafo doble de  $G$  y por la proposición 5.13 este trayecto es un ciclo con un bucle infinito en  $\Delta$  y algún nodo fuera de  $\Delta$ .

Recíprocamente si existe un ciclo  $t = (t_1, t_2)$  con nodos dentro y fuera de  $\Delta$  podemos

construir un ciclo  $t' = (t'_1, t'_2)$  cuyas configuraciones inducidas  $c_{t'_1}, c_{t'_2}$  son finitas y tienen la misma imagen por  $G$ . Sea  $k \in \mathbb{N}$  el período del ciclo  $t$  y sea  $i \in \mathbb{Z}$  tal que  $t(i) = (n, n) \in \Delta$  construimos el nuevo ciclo  $t'$  donde

$$t'(j) = \begin{cases} t(i) & \text{si } j \leq i \\ t(j) & \text{si } i < j \leq i + k - 1 \\ t(i) & \text{si } i + k \leq j. \end{cases}$$

El nuevo trayecto  $t'$  consiste en un bucle infinito en un nodo de  $\Delta$ , es igual que  $t$  en un ciclo de longitud  $k$  y luego vuelve a ser un bucle infinito en el mismo nodo de  $\Delta$ . Es claro que  $t'$  es un trayecto del grafo doble por serlo  $t$  luego las configuraciones que induce tienen la misma imagen por  $G$ . Por su definición las configuraciones que induce son finitas y distintas con lo que obtenemos dos configuraciones finitas y con la misma imagen por  $G$ . Por el teorema del Jardín de Edén concluimos.

Esta proposición es muy útil pues nos permite estudiar la reversibilidad de un AC unidimensional basándonos solo si los ciclos salen de  $\Delta$ . Si representamos el grafo doble y asignamos un único nodo al conjunto de nodos  $\Delta$  nos basta con ver si hay algún ciclo que pasa por este nodo. Además usando la simetría del grafo doble podemos solo representar la mitad de los nodos pues si  $t : i \mapsto (n_i^1, n_i^2)$  es un trayecto en este grafo entonces  $t' : i \mapsto (n_i^2, n_i^1)$  también lo será. Ponemos esto en práctica en la Figura 14, en la Figura 15 exponemos un ciclo de la Figura 14 que no pasa por  $\Delta$ .

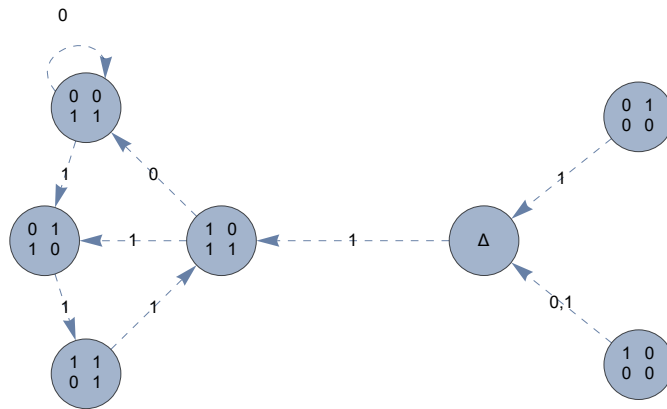


Figura 14: Grafo doble simplificado del AC elemental 110.

Podemos ver que hay varios ciclos fuera de  $\Delta$  por ejemplo el ciclo de longitud 3

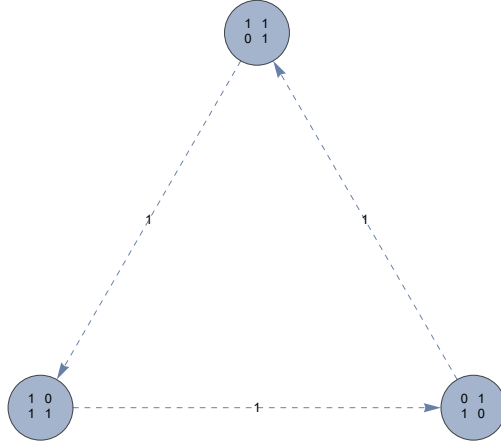


Figura 15: Ciclo de longitud 3 en el grafo doble del AC 110

Con lo que concluimos que el AC 110 no es reversible. Sin embargo es epiyectivo pues no existe ningún ciclo con nodos dentro y fuera de  $\Delta$ .

En consecuencia del proceso que hemos detallado la reversibilidad es decidible para los ACs de dimensión uno. Sin embargo tal y como demuestra Jarko Kari en [7] la reversibilidad no es decidible para ACs de dimensión mayor.

## 6 Autómatas Celulares Particionados

En esta sección estudiaremos un subtipos de ACs. Los llamados ACs particionados que denotaremos ACPs.

**Definición 6.1.** *Un ACP  $A_p$  con  $m$  vecinos es un AC de la forma*

$$A_p = (d, S, V, f)$$

donde

1.  $d$  es un entero mayor que 1.
2. El conjunto finito de estados  $S = S_1 \times S_2 \times \dots \times S_m$  es el producto de otros  $m$  conjuntos finitos.
3. La vecindad  $V = (v_1, v_2, \dots, v_m)$  es de tamaño  $m$ .
4. La función local  $f = g \circ \pi$  es la composición de una función

$$f : S \rightarrow S$$

y la función

$$\pi = (\pi_1, \pi_2, \dots, \pi_m) : S^m \rightarrow S$$

$$((s_1^1, s_2^1, \dots, s_m^1), (s_1^2, s_2^2, \dots, s_m^2), \dots, (s_1^m, s_2^m, \dots, s_m^m)) \mapsto (s_1^1, s_2^2, \dots, s_m^m).$$



Donde  $\pi_i$  es la proyección en la coordenada  $i$  de  $S$ :

$$\begin{aligned} \pi &= (\pi_1, \pi_2, \dots, \pi_m) : S^m \rightarrow S \\ (s_i^j)_{i,j=1}^m &\mapsto (s_i^i)_{i=1}^m \end{aligned}$$

Es conveniente pensar las configuraciones de un ACP con  $m$  vecinos como configuraciones que están particionadas en bloques (células) que a su vez están divididos en  $m$  partes. Vemos un ejemplo de esto en la Figura 16. En la Figura 17 vemos como combinan los estados de los bloques para crear un nuevo bloque central.

**Ejemplo 6.2.** *El ACP que usaremos más adelante es de dimensión 1 y con 3 vecinos, es decir, del tipo*

$$A = (1, S_1 \times S_2 \times S_3, (1, 0, -1), f)$$

*Podemos visualizar las configuraciones por bloques de tres celdas. Por definición de  $A$  el vecindario de una célula o bloque consta de ella misma y sus bloques adyacentes.*



Figura 16: Un patrón de longitud tres representado por bloques de tres celdas. El patrón es la vecindad del bloque central

*Por definición de  $A$  los nuevos estados del bloque central tras un paso en el tiempo están determinados por los estados de las celdas a la izquierda y a la derecha del bloque central.*

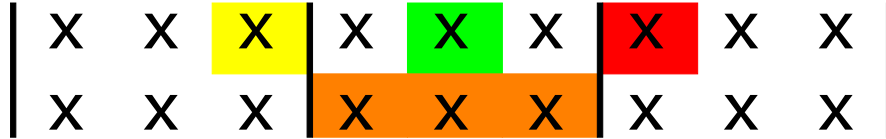


Figura 17: Representación de los nuevos estados del bloque central al aplicar  $A$

En la siguiente proposición veremos como debemos definir un PCA para ser reversible.

**Proposición 6.3.** *Sea  $A = (d, S, V, f)$  es un ACP con  $m$  vecinos de función de transición global  $G$  y función de transición local  $f = g \circ \pi$ .  $A$  es reversible si y solo  $g$  es biyectiva.*

*Demostración.* Supongamos por reducción al absurdo que  $G$  es inyectiva pero  $g$  no lo es. Puesto que  $g$  no es inyectiva existen dos estados distinto  $q, s \in S$  tales que

$$g(q) = g(s).$$

Sean  $c_1, c_2 \in S^{\mathbb{Z}^d}$  dos configuraciones tales que

$$\pi(c_1(V(0))) = q \quad \pi(c_2(V(0))) = s$$

y

$$\pi(c_1(V(i))) = \pi(c_2(V(i))), i \in (\mathbb{Z}^d \setminus \{0\}).$$

Estas configuraciones existen por ser  $\pi$  epiyectiva y además son distintas pues  $q \neq s$ . Dado que  $g(q) = g(s)$  y usando las propiedades que impusimos a las configuraciones  $c_1$  y  $c_2$  tenemos que

$$G(c_1)(i) = g(\pi(c_1(V(i)))) = g(\pi(c_2(V(i)))) = G(c_2)(i) \quad \forall i \in \mathbb{Z}^d.$$

Pero  $c_1 \neq c_2$  luego  $G$  no es inyectiva. Con esto hemos llegado a una contradicción al suponer que  $G$  era inyectiva pero  $g$  no lo era.

Ahora supongamos por reducción al absurdo que  $g$  es inyectiva pero que  $G$  no lo es. Puesto que  $G$  no es inyectiva existen dos configuraciones distintas  $c_1, c_2 \in S^{\mathbb{Z}^d}$  tales que

$$G(c_1) = G(c_2).$$

Sea  $V = (v_1, v_2, \dots, v_m)$  la vecindad de  $A$  y sea  $i \in \mathbb{Z}^d$  tal que

$$c_1(i) \neq c_2(i)$$

si

$$c_1(i) = (s_1, s_2, \dots, s_m) \quad \text{y} \quad c_2(i) = (q_1, q_2, \dots, q_m)$$

escojamos  $1 \leq j \leq m$  tal que

$$s_j \neq q_j$$

y  $l \in \mathbb{Z}^d$  tal que

$$v_j + l = i.$$

Por las elecciones de  $i, j$  y la definición de  $l$  tenemos que

$$\pi_j(c_1(v_j + l)) = \pi_j(c_1(i)) \neq \pi_j(c_2(i)) = \pi_j(c_2(v_j + l))$$

luego

$$\begin{aligned} \pi(c_1(V(l))) &= \pi(c_1(v_1 + l), c_1(v_2 + l), \dots, c_1(v_j + l), \dots, c_1(v_l + m)) \\ &= (\pi_1(c_1(v_1 + l)), \pi_2(c_1(v_1 + l)), \dots, \pi_j(c_1(v_j + l)), \dots, \pi_m(c_1(v_m + l))) \\ &\neq (\pi_1(c_2(v_1 + l)), \pi_2(c_2(v_1 + l)), \dots, \pi_j(c_2(v_j + l)), \dots, \pi_m(c_2(v_m + l))) \\ &= \pi(c_2(V(l))). \end{aligned}$$

Sin embargo, por la elección de  $c_1$  y  $c_2$

$$G(c_1)(l) = g(\pi(c_1(V(l)))) = g(\pi(c_2(V(l)))) = G(c_2)(l)$$

luego  $g$  no es inyectiva lo cual es una contradicción y concluimos.  $\square$

Ahora que hemos visto bajo que condición un ACP es reversible veremos algunas definiciones acerca de las máquinas de Turing de con la finalidad de mostrar que los AC reversibles son Turing completos.

**Definición 6.4.** *Una maquina de Turing  $T$  de una cinta es una 6-tupla*

$$T = (Q, S, q_0, F, s_0, \delta)$$

donde

1.  $Q$  es un conjunto finito de estados.
2.  $S$  es un conjunto finito de símbolos.
3.  $q_0 \in Q$  es el estado inicial.
4.  $F \subseteq Q$  es un conjunto de estados finales.
5.  $s_0$  es el símbolo en blanco.
6.  $\delta \subseteq A_1 \cup A_2$  es la tabla de transición de  $T$  donde

$$A_1 = (Q \setminus F) \times S \times Q \times S$$

$$A_2 = (Q \setminus F) \times \{\cdot\} \times Q \times \{-, 0, +\}.$$

Un cuarteto en  $\delta$  de la forma

$$[q_1, s_1, q_2, s_2] \in A_1$$

lo interpretamos de la siguiente forma. Si la máquina de Turing  $T$  se encuentra en el estado  $q_1$  y lee el símbolo  $s_1$  entonces pasa a estar en el estado  $q_2$  y reemplaza el símbolo  $s_1$  por el símbolo  $s_2$ . Si un cuarteto de  $\delta$  es de la forma

$$[q_1, \cdot, q_2, a] \in A_2$$

entonces la interpretación es que si  $T$  se encuentra en el estado  $q_1$  pasa a estar en el estado  $q_2$ , el símbolo que lee se mantiene constante y la cabeza de  $T$  se mueve hacia la izquierda, no se mueve, o se mueve a la derecha según sea a igual a  $-$ ,  $0$  ó  $+$ .

**Definición 6.5.** Una máquina de Turing de una cinta  $T = (Q, S, q_0, F, s_0, \delta)$  se dice que es determinista si dados dos cuartetos distintos  $[q_1, s_1, q_2, s_2], [q'_1, s'_1, q'_2, s'_2] \in \delta$

$$q_1 \neq q'_1 \text{ o } s_1 \neq s'_1.$$

Es decir, la tabla de transición  $\delta$  prescribe una única acción en cada situación. En este caso podemos identificar  $\delta$  con una función.

**Definición 6.6.** Una máquina de Turing de una cinta  $T = (Q, S, q_0, F, s_0, \delta)$  se dice que es reversible si dados dos cuartetos distintos  $[q_1, s_1, q_2, s_2], [q'_1, s'_1, q'_2, s'_2] \in \delta$  se verifica:

$$q_2 = q'_2 \Rightarrow (s_2 \neq s'_2) \text{ y } (s_1 \neq \cdot \neq s_2)$$

**Definición 6.7.** Un sistema se dice que es Turing completo si puede simular cualquier máquina de Turing.

Según la tesis de Church-Turing [10] un sistema es Turing completo si puede computar cualquier algoritmo. K. Morita A. Shirasaki e Y. Gono[11] demostraron que las máquinas de Turing de una cinta y con dos estados son Turing completos. De esta forma si conseguimos simular una máquina de Turing de este tipo por un AC reversible habremos demostrado que los ACs reversibles son Turing completos. Veremos de forma incluso más contundente que lo son los ACs reversibles unidimensionales.

**Proposición 6.8.** *Dada una máquina de Turing de una cinta  $T = (Q, S, q_0, F, \delta)$  determinista y reversible existe un ACP*

$$A_P = (1, I \times C \times D, (1, 0, -1), f_P)$$

*reversible, unidimensional y con 3 vecinos que simula a  $A$ .*

*Demostración.* Definimos los elementos del conjunto de estados  $I \times C \times D$  del ACP como sigue

$$I = D = Q \cup \{\#\}$$

$$C = Q \cup \{\#\} \times S$$

Para definir la función local  $f_P := g_P \circ \pi$  basta definir  $g_P : I \times C \times D \rightarrow I \times C \times D$ . Además por la proposición 6.3 para que  $A_P$  sea reversible basta con que  $g_P$  sea inyectiva. Definiremos a  $g_P$  sobre el subconjunto de su dominio requerido para simular a  $A$  y hecho esto basta extenderla de forma que preserve la inyectividad.

1. Si  $[q_1, s_1, q_2, s_2] \in A_1$  entonces

$$g_P([\#, (q_1, s_1), \#]) = [\#, (q_2, s_2), \#]$$

2. Si  $[q_1, \cdot, q_2, -] \in A_2$  entonces

$$2.1 \quad g_P([\#, (q_1, s_1), \#]) = [q_2, (\#, s_1), \#] \quad \forall s_2 \in S$$

$$2.2 \quad g_P([\#, (\#, s_2), q_1]) = [\#, (q_2, s_2), \#] \quad \forall s_2 \in S$$

3. Si  $[q_1, \cdot, q_2, 0] \in A_2$  entonces

$$g_P([\#, (q_1, s_1), \#]) = [\#, (q_2, s_1), \#] \quad \forall s \in S$$

4. Si  $[q_1, \cdot, q_2, +] \in A_2$  entonces

$$4.1 \quad g_P([\#, (q_1, s_1), \#]) = [\#, (\#, s_1), q_2] \quad \forall s_1 \in S$$

$$4.2 \quad g_P([q_2, (\#, s_2), \#]) = [\#, (q_2, s_2), \#] \quad \forall s_2 \in S$$

5. Si  $s \in S$  y  $1_f \in F$  entonces

$$5.1 \quad g_P([\#, (\#, s), \#]) = [\#, (\#, s), \#]$$

$$5.2 \quad g_P([\#, (q_f, s), \#]) = [\#, (\#, s), q_f]$$

$$5.3 \quad g_P([q_f, (\#, s), \#]) = [\#, (q_f, s), \#]$$

Si

$$\dots, s_0, s_1, s_2, \dots, s_{n-1}, q_0, s_n, s_{n+1}, \dots, s_m, s_0, \dots$$

es la entrada de  $T$  entonces la configuración inicial de  $A_P$  es

$$\dots, [\#, (\#, s_0), \#], [\#, (\#, s_1), \#], \dots, [\#, (\#, s_{n-1}), \#], [\#, (q_0, s_n), \#], \dots, [\#, (\#, s_m), \#], [\#, (\#, s_0), \#], \dots$$

Veamos como simula  $A_P$  a  $T$ . Visualizar las configuraciones en bloques con tres columnas y dos filas hará mas simple la demostración. La configuración inicial la representamos como

$$t = 0 \left| \begin{array}{ccc|ccc|ccc|ccc|ccc} \# & \# & \# & \# & q_0 & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\ & & & s_{n-1} & s_n & & & & s_{n+1} & & & s_{n+2} & & & s_{n+3} & & & s_{n+4} & \end{array} \right|$$

Figura 18: Parte de la configuración inicial

Al aplicar  $A_P$  todas las células (los bloques) permanecerán iguales por la regla 5.1 salvo posiblemente el que tiene el estado  $q_0$ . En esta célula cambiarán el estado y el símbolo que aparecen en el centro, quedándose en la zona central hasta que en el instante  $t'$  el bloque pase a ser de la forma

$$[\#, (q', s'), \#]$$

y

$$[\#, (q', s'), \#] \in ((Q \times \{\cdot\} \times Q \times +) \cup (Q \times \{\cdot\} \times Q \times -)) \cap \delta.$$

Veremos el caso

$$[\#, (q', s'), \#] \in (Q \times \{\cdot\} \times Q \times +) \cap \delta$$

pues el otro es análogo. En este caso la célula se transforma en

$$[\#, (\#, s'), q']$$

por la regla 4.1 y ahora la representación de la configuración es

$$t = t' \left| \begin{array}{ccc|ccc|ccc|ccc|ccc} \# & \# & \# & \# & q' & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\ & & & s_{n-1} & s' & & & & s_{n+1} & & & s_{n+2} & & & s_{n+3} & & & s_{n+4} & \end{array} \right|$$

Figura 19: Parte de la configuración en el instante  $t'$

Ahora en el instante  $t' + 1$  gracias a la regla 5.1 la célula en la que está  $q'$  pasa a ser

$$[\#, (\#, s'), \#]$$

mientras que debido a la regla 4.2 la célula a su derecha se convierte en

$$[\#(q', s_{n+1}), \#]$$

$$t = t' + 1 \left| \begin{array}{ccc|ccc|ccc|ccc|ccc} \# & \# & \# & \# & q' & \# & \# & \# & \# & \# & \# & \# & \# & \# & \# \\ & & & s_{n-1} & s' & & & & s_{n+1} & & & s_{n+2} & & & s_{n+3} & & & s_{n+4} & \end{array} \right|$$

Figura 20: Parte de la configuración en el instante  $t'+1$

Con lo que  $A_P$  simula que  $T$  se mueva a la derecha (o a la izquierda) como queríamos. Nos queda por ver que pasa cuando el estado cambia a un estado  $q_f \in F$ . Podemos suponer que cuando aparece un estado final la cabeza de la maquina de Turing  $T$  no se mueve pues al parar  $T$  este movimiento es irrelevante. De esta forma si el bloque en el que estamos es de la forma

$$[\#, (q, s), \#]$$

y

$$[q, s_m, q_f, s'_m] \in A_1$$

entonces

$$\left| \begin{array}{ccc|ccc|ccc|ccc|ccc|ccc} \# & \# & \# & \# & \# & \# & \# & q & \# & \# & \# & \# & \# & \# & \# & \# & \# \\ & s_{m-2} & & & s_{m-1} & & & s_m & & & s_{m+1} & & & s_{m+2} & & & s_{m+3} \end{array} \right|$$

se convierte en

$$\left| \begin{array}{ccc|ccc|ccc|ccc|ccc|ccc} \# & \# & \# & \# & \# & \# & \# & q_f & \# & \# & \# & \# & \# & \# & \# & \# & \# \\ & s_{m-2} & & & s_{m-1} & & & s'_m & & & s_{m+1} & & & s_{m+2} & & & s_{m+3} \end{array} \right|$$

por las reglas 1. y 5.1. Ahora por las reglas 5.2 y 5.3 el estado final se desplaza hacia la derecha dejando igual los estados de la cinta. El estado  $q_f$  señala que  $T$  ha parado. Puesto que queremos que  $A_P$  sea reversible no podemos dejar que el  $A_P$  pare con lo que hemos construido  $A_P$  de esta forma. Se cumple que  $A_P$  es reversible pues las imágenes que hemos puesto son todas distintas. Con esto concluimos.  $\square$

## 7 Aplicaciones

Una vez desarrollada toda esta teoría acerca de los ACs reversibles el paso más natural sería analizar algunas de sus posibles aplicaciones. Empecemos por el ámbito de la criptología. Una de las ramas principales de la criptología es estudiar como encriptar información de tal forma que se pueda recuperar a partir de una clave y que resulte casi imposible hacerlo sin ella. Los ACs resultan interesantes para esta tarea pues, además de su gran variedad, a partir de reglas sencillas se puede obtener una evolución de gran complejidad. Más aún, es preciso usar ACs reversibles para poder decodificar la información. Así por ejemplo, en zcrypto los autores proponen un algoritmo que funciona de la siguiente forma. En primer lugar se permutan los píxeles de forma caótica mediante una aplicación logística. Posteriormente para dificultar la obtención de la imagen por individuos sin la clave se aplica de forma sucesiva un AC reversible a los bits de los píxeles permutados. En este caso la clave serían los parametros de la aplicación logística, algo que permita identificar el AC y el número de veces que se aplica este AC. La Figura 21 es un ejemplo de este tipo de cifrado.



Figura 21: Imagen original y encriptada. Imágenes extraídas de [12].

En la física los ACs son usados para representar sistemas dinámicos. Uno de los campos de la física susceptible a la modelización de ACs es la estadística mecánica. La estadística mecánica analiza como propiedades físicas macroscópicas dependen de parámetros microscópicos. Claramente esto es análogo a como surgen comportamientos de carácter global en ACs a partir de interacciones locales. Los ACs estocásticos, en los que la regla local es probabilista, suelen ser los más apropiados para esta rama por su enfoque probabilista. Sin embargo, los deterministas también pueden ser de utilidad. Es el caso del modelo de Ising, que es usado para estudiar el ferromagnetismo. Este modelo consiste de una red de células con spin (momento angular) hacia arriba o hacia abajo. El spin de cada célula varia según el spin de sus células adyacentes. En [13] los autores proponen un modelo de Ising que consiste de un AC reversible. En él, cada célula cambia de spin siempre que se conserve la energía. Para hacer esto la red se particiona en células pares (las casillas blancas de un tablero de ajedrez) e impares (las casillas negras de un tablero de ajedrez). Primero se actualizan las células pares y luego las impares de la siguiente forma: el spin de una célula cambia si la mitad de sus células adyacentes tienen spin hacia arriba y permanece igual en otro caso. Este planteamiento también es estudiado en [14] donde los autores realizan una simulación recogida en la Figura 22. Como indican los autores, a partir de una configuración inicial con un spin dominante (da igual en que sentido) se obtiene una configuración estacionaria más equilibrada. En esta última configuración zonas con el spin en un sentido están rodeadas por zonas con spin en el sentido contrario.

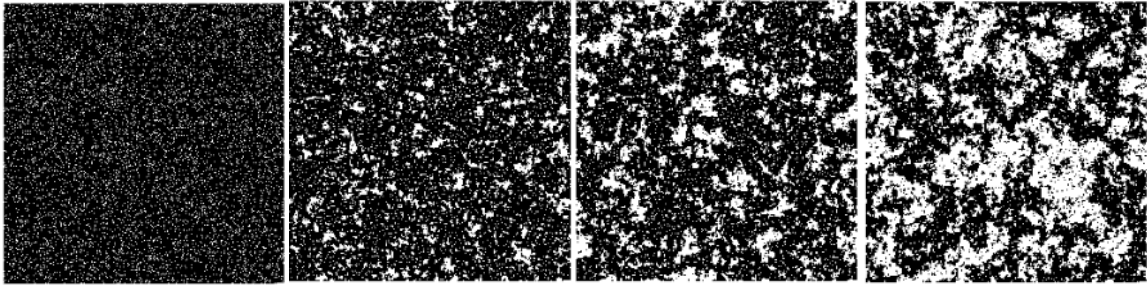


Figura 22: Evolución del modelo de Ising. Imágenes extraídas de [14]

Otro sistema que puede ser modelado por ACs son los fluidos. En particular el movimiento de sus partículas. Un AC reversible para modelar este sistema es el AC llamado HPP[15]. En él, cada célula representa una parte del fluido que puede contener hasta un máximo de cuatro partículas moviéndose en sentidos distintos. El estado de cada célula representa las partículas que están en esa región del fluido y en que sentido se mueven. La regla local se define de forma que se conserven tanto el número de partículas como la cantidad de movimiento. Esta regla establece que una partícula continúa moviéndose en el mismo sentido hasta que experimente un choque frontal con otra partícula o llegue al final de la red en el caso de aplicar el AC a un patrón finito. En caso de un choque frontal la partícula se desvía perpendicularmente. Si la partícula llega a la frontera de la red rebota en sentido contrario. La regla local es resumida en la Figura 23 y la Figura 24 es la simulación del modelo con una barrera.

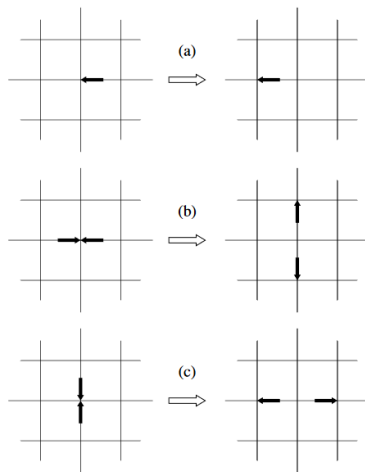


Figura 23: Comportamiento de las partículas en el modelo HPP. Imagen extraída de [14]



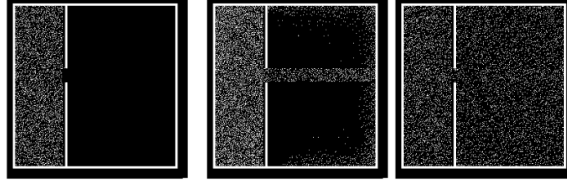


Figura 24: Simulación del modelo HPP. Imagen extraída de [14]

Sin embargo, este sistema posee varios defectos que han ocasionado la creación del modelo FHP. Este nuevo modelo es también un AC pero pasa a serlo sobre una red hexagonal en la que los choques frontales producen cambios de sentido aleatorios. Recientemente los ACs han sido empleados incluso en la computación cuántica. Los ACs cuánticos[16] (ACCs) son ACs que actúan sobre redes de células que están en sistemas cuánticos. Es decir, los estados son *cudits*, o lo que es lo mismo, sistemas cuánticos que pueden estar en cualquier superposición de  $d$  estados cuánticos (distribuciones para todas las posibles mediciones sobre el sistema). Además, debido a que se suele tomar como axioma que la evolución de un estado cuántico es dado por un operador unitario y por tanto reversible, son de especial interés aquí los ACCs reversibles.

## 8 Conclusiones

En este trabajo se han abordado varios aspectos cruciales de los ACs reversibles que resumiremos a continuación. El primer capítulo del trabajo está dedicado sobre todo a nociones introductorias de los ACs. Además vemos uno de los resultados más fundamentales de la teoría de ACs. El teorema de Curtis–Hedlund–Lyndon, que identifica los ACs con las funciones sobre el espacio de configuraciones que son continuas e invariantes por traslaciones.

En el segundo capítulo obtenemos el primer fruto de nuestro estudio de los ACs reversibles. Demostramos que un AC es reversible si y solo si es inyectivo. Además vemos que todos los ACs epiyectivos son equilibrados, y que por tanto los reversibles lo son también.

En el tercer capítulo demostramos el Teorema del Jardín de Edén. Este teorema establece la equivalencia entre la epiyectividad y la pre-inyectividad de un AC. Puesto que, como su nombre indica, la pre-inyectividad es una propiedad necesaria para la inyectividad, este teorema nos ofrece una nueva herramienta para ver si un AC es reversible.

El cuarto capítulo, el más extenso de todos, se centra en los ACs unidimensionales. Resulta que en el caso unidimensional podemos reducir la reversibilidad de un AC a su inyectividad sobre configuraciones periódicas. En el mismo capítulo explicamos como se pueden representar los ACs por un tipo particular de grafos, los grafos de de Bruijn. Al usar el resultado anterior junto con algunas propiedades de los grafos de de Bruijn estudiamos la reversibilidad de un AC usando su grafo doble. Demostramos que el AC es reversible si y solo si los ciclos de su grafo doble están contenidos en el conjunto diagonal. Consecuentemente la reversibilidad es decidible en el caso unidimensional pues existen

algoritmos que determinan si los ciclos están contenidos en el grafo doble.

El quinto capítulo es el dedicado a los ACs particionados (ACPs) que son los ACs en los que la función local es la composición de una permutación con otra función  $g$ . Los ACPs nos ofrecen una forma de construir ACs reversibles, pues demostramos que un ACP es reversible si y solo si  $g$  lo es. Finalmente usamos los ACPs para demostrar que los ACs reversibles son Turing completos, lo cual nos da una indicación de su flexibilidad y trascendencia.

En el sexto capítulo explicamos brevemente algunas de las muchas aplicaciones de los ACs reversibles. La codificación, elaboración de modelos del ferromagnetismo y fluidos y la computación cuántica.

En conclusión los ACs son de gran utilidad debido a su versatilidad y simplicidad, y por ello son usados en diversos ámbitos en la ciencia. En particular su simplicidad les da una ventaja importante frente a otros sistemas computacionales pues permite que sean implementados más fácilmente. El objeto de este trabajo, los ACs reversibles, son particularmente adecuados como sistemas de computación reversibles y para modelar procesos reversibles. Debido a ello su estudio es tanto interesante como fructífero.

## Referencias

- [1] Wolfram, S.: Cellular Automata and Complexity: Collected Papers, Addison-Wesley Reading, MA (1984).
- [2] Wolfram, S.: A New Kind of Science, Wolfram Media, Inc. 2002
- [3] P.-Y. Louis, F. R. Nardi (eds.): Probabilistic Cellular Automata: Theory, Applications and Future Perspectives, Springer, New York (2018).
- [4] Ceccherini-Silberstein, T.: Cellular Automata and Groups, Springer, New York (2010).
- [5] Wolfram, S.: Statistical Mechanics of Cellular Automata, Rev. Mod. Phys. 55, 601-644 (1983).
- [6] Hedlund, Gustav A.: Endomorphisms and Automorphisms of the Shift Dynamical Systems, Mathematical System Theory, 3, 320–375 (1969).
- [7] Kari, J.: Cellular Automata, University of Turku, <http://users.utu.fi/jkari/ca2016/> (2016).
- [8] Moore, E. F.: Machine models of self-reproduction, Proc. Symp. Applied Mathematics, Proceedings of Symposia in Applied Mathematics, 14, 17–33 (1962).
- [9] Myhill, J.: The converse of Moore’s Garden-of-Eden theorem, Proceedings of the American Mathematical Society, 14, 685–686 (1963).
- [10] Copeland, B. J.: The Church–Turing Thesis, Stanford encyclopedia of philosophy, E.Zalta (ed.), <https://plato.stanford.edu/archives/sum2020/entries/church-turing/> (2020).
- [11] Morita, K., Harao, M.: Computational Universality of One-Dimensional Reversible (Injective) Cellular Automata. Trans IEICE E72:758-762 (1989).
- [12] Wang, X.Y., Luan, D.P.: A Novel Image Encryption Algorithm Using Chaos and Reversible Cellular Automata, Commun. Nonlinear Sci. Numer. Simul. 18, 3075–3085 (2013).
- [13] Toffoli, T., Margolus, N.: Cellular Automata Machines: a New Environment for Modeling, MIT press, Cambridge (1987).
- [14] Chopard, B., Luthi P., Masselot, A.: Cellular Automata and Lattice Boltzmann Techniques: An Approach to Model and Simulate Complex Systems, University of Geneva (1998).
- [15] Wolf-Gladrow, D.A.: Lattice-Gas Cellular Automata and Lattice Boltzmann Models - An Introduction, Springer, Berlin (2005).
- [16] Arrighi, P.: Quantum Cellular Automata, Université de Grenoble (2009).