Aspectos de la dinámica topológica de los k-autómatas celulares aditivos

José Soto

Universidad Centroccidental Lisandro Alvarado

Decanato de Ciencias y Tecnología

Departamento de Matemáticas

Junio, 2011

Dedicatoria

Dedico este trabajo A:

- Mi amado Dios,

- La memoria de mi padre Rafael,

- Mi madre Mireya,

- Mis hermanos Oliver, Rafael, Milennys y Deibi.

Gracias por su apoyo.

Agradecimientos

A Dios todopoderoso por darme la vida, sabiduría y fortaleza en todo momento.

A mi madre y hermanos por su apoyo incondicional.

A mi tutor, Dr. Neptalí Romero, por brindarme conocimiento para el éxito de mi trabajo de grado.

A mis compañeros Elvis Aponte, Andy El Achouche, Edgar Guédez y Minoru Akiyama por su constante colaboración.

A mis amigas Karmela Lozada, Mónica Garcia y Celismar Roa por su lealtad en todo momento.

A la UCLA por impartirme conocimiento para mi formación profesional.

Al FONACIT (Fondo Nacional de Ciencia y Tecnología) por su valioso financiamiento en la categoría de Beca para la realización de mis estudios de postgrado.

Resumen

En este Trabajo de Grado tratamos algunos aspectos pertinentes a la dinámica topológica de los k-autómatas celulares aditivos sobre el anillo $\mathbb{Z}_N$.

Se extendieron al contexto de los k-autómatas celulares aditivos sobre el anillo $\mathbb{Z}_N$ en la topología de Cantor las propiedades dinámicas tales como la regularidad y equicontinuidad. Además se demuestra siguiendo el mismo método empleado por Kari (ver [16]) una caracterización de los k-autómatas celulares aditivos inyectivos y sobreyectivos sobre el anillo $\mathbb{Z}_N$.

La monografía está constituida de cuatro capítulos y la correspondiente bibliografía. A continuación damos una breve descripción de cada uno de tales capítulos.

En el primer capítulo se hace una presentación de los conceptos básicos referentes a los Sistemas Dinámicos.

En el segundo capítulo se expone acerca de la regularidad de los k-autómatas celulares lineales sobreyectivos sobre $\mathbb{Z}_N$, relacionandolos con autómatas celulares y usando algunas propidades básicas de los autómatas celulares lineales sobreyectivos.

En el tercer capítulo se introducen los conceptos polinomios y series de Laurent que se utilizan para dar una caracterización de las propiedades de inyectividad y sobreyectividad de los k-autómatas celulares lineales sobre $\mathbb{Z}_N$.

En el cuarto capítulo estudiamos los k-autómatas celulares lineales equicontinuos sobre $\mathbb{Z}_N$, donde se usan caracterizaciones expuestas por Romero en [30], para caracterizar tales k-autómatas celulares en términos de los coeficientes de las k reglas locales que los generan.

Índice general

Introducción

En la actualidad, el estudio de *sistemas dinámicos discretos en retículos* (SDDR) ha ganado considerable atención debido al notable número de modelos matemáticos y computacionales que hacen uso de ellos para describir la evolución y comportamiento asintótico de los estados de diferentes sistemas; incluso en aquellos provenientes de discretizaciones de ecuaciones diferenciales ordinarias y parciales, que en particular son empleados para describir estructuras espacio-temporales en dinámica de fluidos, física del estado sólido y sistemas de reacciones químicas, entre otros.

Para definir un SDDR se requiere de un retículo $\mathcal{R}$ (espacio topológico discreto) cuyos elementos son llamados *células*, en cada $\omega \in \mathcal{R}$ se considera un espacio topológico X_ω (en muchos casos es el mismo en cada célula) denominado *espacio de estados de la célula* ω; el *espacio de configuraciones* de cualquier SDDR con retículo $\mathcal{R}$ y espacios X_ω ($\omega \in \mathcal{R}$) es el conjunto $\mathcal{M} = \prod_{\omega \in \mathcal{R}} X_\omega$ dotado con la topología producto. De esta forma, un SDDR sobre $\mathcal{M}$ es una aplicación $F : \mathcal{M} \to \mathcal{M}$, conocida como *transformación de transición global* que preserva la estructura producto; esto es, para cada $\omega \in \mathcal{R}$ existe un función $F_\omega : \mathcal{M} \to X_\omega$ tal que para todo $x = (x(\omega))_{\omega \in \mathcal{R}}$ se tiene $F(x) = (F_\omega(x))_{\omega \in \mathcal{R}}$. La dinámica del sistema $(\mathcal{M}, F)$ es dada por la ecuación en diferencia

$$x_{n+1} = F(x_n),\ n \geq 0, \tag{1}$$

lo cual equivale a

$$x_{n+1}(\omega) = F_\omega(x_n), \ \text{ para cada } \ n \geq 0 \ \text{ y } \ \omega \in \mathcal{R}.$$

Es claro que para cada configuración inicial del sistema, $x_0 = (x_0(\omega))_{\omega\in\mathcal{R}}$, la evolución temporal de ésta es expresada por la ecuación (1). De hecho, la solución de (1) con condición inicial $x_0 \in \mathcal{M}$ es la sucesión $(F^n(x_0))_{n\geq 0}$, que se conoce como la *órbita de* x_0.

En este trabajo sólo serán considerados los SDDR que tienen como retículo a los enteros; es decir, $\mathcal{R} = \mathbb{Z}$; en cada $\omega \in \mathbb{Z}$ el espacio de estados X_ω es un conjunto finito $\mathcal{A}$, conocido como el *alfabeto del sistema*. En el espacio de configuraciones $\mathcal{A}^{\mathbb{Z}}$, existe un grupo de permutaciones que tiene un papel especial en los sistemas dinámicos discretos que acá tratamos; tal grupo es generado por la transformación *shift* $\sigma : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$, definida como

$$\sigma(x)(\omega) = x(\omega+1), \text{ para todo } x \in \mathcal{A}^{\mathbb{Z}} \text{ y } \omega \in \mathbb{Z}. \qquad (2)$$

Dado que $\mathcal{A}$ es finito, al considerarlo dotado de la topología discreta, el espacio de configuraciones $\mathcal{A}^{\mathbb{Z}}$ adquiere la estructura de un espacio de Cantor el cual es compacto, perfecto y totalmente disconexo. Tal topología admite variadas métricas compatibles; entre las más empleadas se encuentra justamente la métrica de Cantor, la cual es definida, para cada $x = (x(n))_{n\in\mathbb{Z}}$ y $y = (y(n))_{n\in\mathbb{Z}}$ en $\mathcal{A}^{\mathbb{Z}}$, como:

$$d(x,y) = \begin{cases} 0, & \text{si } x(n) = y(n) \text{ para todo } n \in \mathbb{Z} \\ 2^{-k}, & \text{si } x \neq y \text{ y } k = \min\{|n| : x(n) \neq y(n)\}. \end{cases}$$

A lo largo del trabajo será considerada exclusivamente la topología de Cantor sobre $\mathcal{A}^{\mathbb{Z}}$.

En lo que sigue, una transformación $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ *preserva la potencia* r*-ésima del shift* si satisface $F \circ \sigma^r = \sigma^r \circ F$, donde $\mathcal{A}$ es el albabeto del sistema.

Como una subclase de las transformaciones que preservan potencias del shift tenemos a los denominados *autómatas celulares*, aquellos cuando $r = 1$.

Recordamos que un autómata celular (unidimensional) sobre un albabeto $\mathcal{A}$ es toda transformación $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ cuya evolución de estados es gobernada por una *regla local*; más precisamente, dado un conjunto finito $\mathbb{V}$ de $\mathbb{Z}$, se conoce como regla local en la vecindad $\mathbb{V}$ a cualquier función $f : \mathcal{A}^{\mathbb{V}} \to \mathcal{A}$, donde $\mathcal{A}^{\mathbb{V}}$ denota el conjunto de todas las funciones de $\mathbb{V}$ en $\mathcal{A}$; así, el autómata celular $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ dado por la regla local f es definido, para cada $x \in \mathcal{A}^{\mathbb{Z}}$ y todo $n \in \mathbb{Z}$, como

$$F(x)(n) = f\left(x\mid_{n+\mathbb{V}}\right), \tag{3}$$

donde $x\mid_{n+\mathbb{V}}: \mathbb{V} \to \mathcal{A}$ es dada por $x\mid_{n+\mathbb{V}}(k) = x(n+k) = \sigma^n(x)(k)$, para todo $k \in \mathbb{V}$. Claramente tal transformación F es continua y además conmuta con el shift σ. Un conocido y notable resultado, debido a Curtis, Hedlund y Lyndon (ver [17]), establece que toda transformación continua $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ que conmute con σ, es un autómata celular.

Como una extensión de los autómatas celulares tenemos los denominados k-autómatas celulares; esto es, dados un alfabeto $\mathcal{A}$, conjuntos finitos $\mathbb{V}_0, \cdots, \mathbb{V}_{k-1} \subset \mathbb{Z}$ y reglas locales $f_j : \mathcal{A}^{\mathbb{V}_j} \to \mathcal{A}$, $0 \leq j < k$, el *k-autómata celular* por ellas generado es la transformación $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ definida, para cada $x \in \mathcal{A}^{\mathbb{Z}}$ y $n \in \mathbb{Z}$, por

$$F(x)(n) = f_{n_k}\left(x\mid_{n+\mathbb{V}_{n_k}}\right), \tag{4}$$

donde n_k es el entero n tomado módulo k.

Observe que la evolución de los estados en cada célula del retículo depende de la clase de equivalencia módulo k a la cual pertenece y de los estados en un número finito de células vecinas, las cuales son determinadas por las vecindades $\mathbb{V}_j$; más aún, estas vecindades pueden considerarse todas iguales, ello se obtiene introduciendo variables mudas, ver [30]. Por otra parte; es bien conocido (ver [31]) que toda transformación continua que conmute con la potencia k-ésima del shift es un k-autómata celular, este resultado constituye obviamente una extensión de la caracterización de los autómatas celulares arriba comentada. Existen otras extensiones de la caracterización de Curtis-Hedlund-Lyndon; remitimos a [1], [2], [31] donde se presentan algunas de tales extensiones.

Los autómatas celulares, y en general los k-autómatas celulares, vienen siendo empleados en un considerable número de modelos para estudiar fenómenos dinámicos de problemas pertinentes a la Física, Biología, Química y Ciencias de la Computación. Ver [13], [14], [20] y [33]. Cabe destacar que como elemento motivacional y de aplicabilidad adicional, los k-autómatas celulares lineales, a ser definidos más adelante, vienen siendo considerados como modelos para la codificación discreta en subbandas, ver [19].

La dinámica de los k-autómatas celulares es la descripción (topológica o probabilística) del comportamiento asintótico de las órbitas, ofrece una rica variedad de fenómenos de compleja evolución temporal. De hecho la descripción exacta de la evolución temporal de una determinada configuración no siempre es simple, puede resultar muy difícil e incluso hasta imposible. Un conjunto importante de propiedades de la dinámica topológica de los k-autómatas celulares, pueden encontrarse en [30], especialmente propiedades relacionadas con la sobreyectividad, transitividad, equicontinuidad, permutatividad y sensibilidad a las condiciones iniciales.

Los k-autómatas celulares aditivos sobre el anillo $\mathbb{Z}_N$ son aquellos generados por reglas locales aditivas. Sin perder generalidad suponemos que los subconjuntos finitos $\mathbb{V}_0, \ldots, \mathbb{V}_{k-1}$ son todos iguales al intervalo cerrado de números enteros $[\ell, \ell + r]$, $(\ell, r \in \mathbb{Z}, r \geq 0)$.

Ahora bien, para cada $0 \leq j < k$ consideramos constantes $\lambda_0^j, \ldots, \lambda_r^j$ en $\mathbb{Z}_N$ y una función $f_j : \mathbb{Z}_N^{r+1} \to \mathbb{Z}_N$ (*regla local aditiva*) definida para cada

$(a_0, \cdots, a_r) \in \mathbb{Z}_N^{r+1}$ por

$$f_j(a_0, \ldots, a_r) = \sum_{i=0}^{r} \lambda_i^j a_i \pmod{\mathrm{N}}; \tag{5}$$

las constantes λ_i^j $(0 \leq i \leq r, 0 \leq j < k)$ son conocidas como coeficientes de las reglas locales, de esta forma, el k-autómata celular aditivo generado por $[\ell, \ell + r]$ y las reglas locales f_j $(0 \leq j < k)$ es la transformación $F : \mathbb{Z}_N^{\mathbb{Z}} \to \mathbb{Z}_N^{\mathbb{Z}}$ definida, para cada $x \in \mathbb{Z}_N^{\mathbb{Z}}$ y cada $n \in \mathbb{Z}$, por

$$F(x)(n) = \sum_{i=0}^{r} \lambda_i^{n_k} x(n + \ell + i) \pmod{\mathrm{N}}; \tag{6}$$

como antes, n_k es el entero n tomado módulo k.

Dado que el conjunto $\mathbb{Z}_N^{\mathbb{Z}}$ es un $\mathbb{Z}_N$-módulo con las operaciones usuales de adición y multiplicación por escalares en $\mathbb{Z}_N$, el k-autómata celular aditivo F arriba definido es lineal; esto es, para cada $\alpha \in \mathbb{Z}_N$ y todo $x, y \in \mathbb{Z}_N^{\mathbb{Z}}$, siempre se satisface

$$F(\alpha x + y) = \alpha F(x) + F(y).$$

En el caso de los autómatas celulares lineales, es decir cuando $k = 1$, son conocidas varias propiedades importantes de la dinámica topológica de tales sistemas; incluso varias caracterizaciones de algunas de estas propiedades, son expresadas en términos de los coeficientes que definen al autómata celular aditivo en consideración. A manera de ejemplo remitimos a: [8], [9], [11], [15], [18], [23], [24] y [26], donde podrá encontrarse información al respecto.

En [19] son descritas propiedades relativas a la sobreyectividad e inyectividad empleando técnicas de series formales de potencias y polinomios de Laurent. Una caracterización de la sobreyectividad de estos sistemas dinámicos es también obtenida en [1], ver también [3], mediante el uso de la denominada forma normal de Smith. En el caso de k-autómatas celulares aditivos $(k \geq 2)$ son conocidos pocos resultados.

1

Preliminares

Este capítulo contiene fundamentalmente conceptos básicos acerca de Sistemas Dinámicos Discretos, necesarios para el desarrollo de está monografía.

Definición 1.1. Un Sistema Dinámico Discreto, o simplemente un Sistema Dinámico, es cualquier par (X, F), donde X es un espacio métrico compacto y $F : X \longrightarrow X$ es una transformación continua.

Definición 1.2. Un homomorfismo entre Sistemas Dinámicos (X, F) y (Y, G) es cualquier aplicación continua $\varphi : X \longrightarrow Y$ tal que $\varphi \circ F = G \circ \varphi$.

Si la aplicación φ es homeomorfismo, se le denomina *conjugación* y los sistemas dinámicos son topológicamente conjugados.

Definición 1.3. Dados un Sistema Dinámico (X, F) y un punto $x \in X$:

1. x se dice periódico, si existe un entero $n \geq 1$ tal que $F^n(x) = x$; al menor entero con tal propiedad se le denomina período de x. Al conjunto de puntos periódicos lo denotamos por $Per(F)$.

2. x es eventualmente periódico, si existe un entero $m \geq 0$ tal que $F^m(x)$ es periódico; es decir, existe un entero $n \geq 1$ tal que $F^{n+m}(x) = F^m(x)$. En el caso que $m \geq 1$, x se dice preperiódico.

Observemos que la órbita de un punto x es finita si, y sólo si, x es eventualmente periódico. Además, si F es un homeomorfismo y x es eventualmente periódico, entonces x es periódico.

Definición 1.4. Si (X, d) es un espacio métrico, $x \in X$ y $\delta > 0$. La bola centrada en x y radio δ es el conjunto $B_\delta(x) = \{y \in X : d(x, y) < \delta\}$.

Definición 1.5. Un punto $x \in X$ se dice equicontinuo, o Lyapunov estable, si para cada $\epsilon > 0$ existe $\delta > 0$ tal que, para todo $y \in B_\delta(x)$ y cada entero $n \geq 1$ se tiene $d(F^n(x), F^n(y)) < \epsilon$. Al conjunto de puntos de equicontinuidad de F se le denota por $Eq(F)$. Cuando $Eq(F) = X$, se dice que F es equicontinuo.

Nótese que la noción de equicontinuidad de un punto está asociada con la idea de que las órbitas de puntos arbitrariamente próximos de x no se separan de la órbita de x.

Definición 1.6. El Sistema Dinámico (X, F), se dice sensitivo a las condiciones iniciales, o simplemente sensitivo, si existe $\epsilon > 0$ tal que para todo $\delta > 0$ y $x \in X$, existen $y \in B_\delta(x)$ y un entero $n \geq 1$ de forma que $d(F^n(x), F^n(y)) \geqslant \epsilon$. A la constante ϵ se le conoce con el nombre de constante de sensitividad.

Intuitivamente una transformación es sensible a las condiciones iniciales, o simplemente sensible, si existen puntos arbitrariamente cerca de $x \in X$ que eventualmente se separan de x bajo la iteración de F al menos ϵ.

Definición 1.7. Un Sistema Dinámico se dice positivamente expansivo si existe una constante $\epsilon > 0$, denominada constante de expansividad, tal que para todo $x, y \in X$, con $x \neq y$, existe un entero $n \geq 0$ tal que $d(F^n(x), F^n(y)) \geqslant \epsilon$.

Observemos que si X es perfecto (ningún punto es aislado), entonces todo Sistema Dinámico (X, F) positivamente expansivo es sensitivo.

Definición 1.8. Se dice que un Sistema Dinámico (X, F) es topológicamente transitivo si para cada par de abiertos no vacíos U, V de X, existe un entero $n \geq 1$ tal que $F^n(U) \cap V \neq \emptyset$.

La noción de transitividad además de ofrecer intuitivamente alguna idea de inestabilidad, también indica que el conjunto de órbitas del sistema no se puede descomponer; esto es, X no se puede expresar como la unión de dos abiertos no vacíos, disjuntos e invariantes. Es simple verificar que los sistemas transitivos son sobreyectivos. Véase [21].

Definición 1.9. Un Sistema Dinámico (X, F) se dice caótico según Devaney si son satisfechas las propiedades de transitividad, densidad de los puntos periódicos de F y sensitividad a las condiciones iniciales.

Debe ser mencionado que cuando X tiene infinitos puntos, si son satisfechas las propiedades de transitividad y densidad de los puntos periódicos, entonces se cumple la propiedad de sensitividad a las condiciones iniciales, véase [6].

Cabe destacar teoremas clásicos de álgebra y topología, que se aplican en algunos capítulos de está monografía.

Teorema 1.1. *(N. McCoy [27]). Sea R un anillo conmutativo con unidad y A una matriz cuadrada cuyas entradas son elementos de R, entonces*

1. *A es invertible si, y sólo si, $\det A$ es invertible.*

2. *A es un divisor de cero si, y sólo si, $\det A$ es un divisor de cero.*

Teorema 1.2. *(J. Munkres [28]). Dada $f : X \to Y$ una función continua y biyectiva. Si X es compacto y Y es Hausdorff, entonces f es un homeomorfismo.*

En lo que sigue, serán considerados k-autómatas celulares de radio r; esto es, generado por k reglas locales definidas sobre el mismo vecindario $[-r, r]$.

Ahora enunciaremos y demostraremos algunos teoremas de la teoría de los k-autómatas celulares, que serán indispensables en el desarrollo de esta monografía.

Teorema 1.3. *Si F es un k-autómata celular, entonces $F \circ \sigma^k = \sigma^k \circ F$.*

Demostración: Supongamos que F es de radio r y es generado por k reglas locales, denotemos cada regla local por φ_j, donde $0 \leq j < k$.

Sean $x \in \mathcal{A}^{\mathbb{Z}}$ y $m \in \mathbb{Z}$; así, por definición de σ^k y F se cumple

$$\sigma^k(F(x))(m) = F(x)(m+k) \text{ y } F(x)(m+k) = \varphi_{(m+k)_k}(x_{[m+k-r,m+k+r]}). \quad (1.1)$$

Por otro lado,

$$\begin{aligned} F(\sigma^k(x))(m) &= \varphi_{m_k}(\sigma^k(x)_{[m-r,m+r]}) \\ &= \varphi_{m_k}(x_{[m+k-r,m+k+r]}) \\ &= \varphi_{(m+k)_k}(x_{[m+k-r,m+k+r]}). \end{aligned} \quad (1.2)$$

Ahora, por (1.1) y (1.2) tenemos que $F \circ \sigma^k = \sigma^k \circ F$. □

Teorema 1.4. *Si* $(\mathcal{A}^{\mathbb{Z}}, F)$ *es un* k*-autómata celular lineal biyectivo, entonces su inversa es un* k*-autómata celular lineal.*

Demostración: Supongamos $(\mathcal{A}^{\mathbb{Z}}, F)$ lineal y biyectivo, entonces existe una transformación g tal que $g \circ F = F \circ g = I$, donde I es la identidad de $\mathcal{A}^{\mathbb{Z}}$. Más aún, puesto que F es lineal, es notorio que su inversa g también lo es.

Por otra parte, como F es un k-autómata celular, por el teorema 1.3 se sigue que $F \circ \sigma^k = \sigma^k \circ F$ y en consecuencia

$$g \circ \sigma^k = \sigma^k \circ g. \quad (1.3)$$

Ahora bien, como F es biyectiva, continua y $\mathcal{A}^{\mathbb{Z}}$ es compacto y Hausdorff, entonces por el teorema 1.2, F es un homeomorfismo y en particular g es continua.

Luego, por (1.3) y al ser g continua y lineal se tiene que g es un k-autómata celular lineal. □

2 Regularidad

La propiedad de regularidad en Sistemas Dinámicos Discretos (X, T), significa que el conjunto de puntos periódicos de la transformación $T : X \to X$ es denso en el espacio topológico X. Esta propiedad es uno de los componentes de la noción de caos introducida por Devaney, ver [12]. En el contexto de los autómatas celulares existe una importante conjetura la cual indica que todo autómata celular sobreyectivo es regular.

Esta conjetura es famosa en la teoría de autómatas celulares. Además, todavia no ha sido probada. Sin embargo, existen algunos resultados parciales de está conjetura, por ejemplo los autómatas celulares lineales sobreyectivos son regulares (ver [8]) más generalmente los D-autómatas celulares lineales sobreyectivos son regulares, ver [9], en este mismo artículo se demuestra que la clase de autómatas celulares permutativos en la primera y última variable, son regulares. Otra importante clase de autómatas celulares regulares son los llamados autómatas celulares cerrados, ver [7].

Aunque esta conjetura es un problema abierto, en este capítulo abordaremos una demostración de dicha conjetura en el ámbito de los k-autómatas celulares lineales cuyo alfabeto es el anillo $\mathbb{Z}_N$. Para tal fin usaremos principalmente propiedades de autómatas celulares sobreyectivos.

2.1. Sobreyectividad y Regularidad

Se inicia esta sección enunciando dos resultados clásicos de la teoría de autómatas celulares.

Teorema 2.1. *(Hedlund [17]). Si* $(\mathcal{A}^{\mathbb{Z}}, F)$ *es un autómata celular, entonces* F *es sobreyectivo si y sólo si para cada* $y \in \mathcal{A}^{\mathbb{Z}}$*,* $card(F^{-1}(y)) < +\infty$*.*

Teorema 2.2. *(M. Boyle, B. Kitchens [7]). Si* $(\mathcal{A}^{\mathbb{Z}}, F)$ *es un autómata celular cerrado, entonces el conjunto de puntos periódicos por* F *y* σ *es denso.*

Definición 2.1. Dados $a, b, c, d \in \mathbb{Z}$ con $a < b$, denotaremos por:

1. (a, b) al intervalo abierto de números enteros entre a y b.

2. $[a, b]$ al intervalo cerrado de números enteros entre a y b.

3. $(-\infty, c)$ al intervalo abierto de números de enteros entre $-\infty$ y c.

4. $(d, +\infty)$ al intervalo abierto de números enteros entre d y $+\infty$.

5. Si $x \in \mathbb{Z}_N^{\mathbb{Z}}$ y α un intervalo de números enteros como en 1, 2, 3 o 4, se entiende por x_α; la restricción de x a α.

Definición 2.2. Dado un alfabeto $\mathcal{A}$, se dice que:

1. $x, y \in \mathcal{A}^{\mathbb{Z}}$ son asintóticos a izquierda (resp. a derecha) si, y sólo si, existe $n \in \mathbb{Z}$ tal que

$$x_{(-\infty,n)} = y_{(-\infty,n)} \text{ (resp. } x_{(n,+\infty)} = y_{(n,+\infty)}).$$

2. Un autómata celular $(\mathcal{A}^{\mathbb{Z}}, F)$ es cerrado a izquierda (resp. a derecha) si, y sólo si, para cada $x, y \in \mathcal{A}^{\mathbb{Z}}$ con $x \neq y$ asintóticos a derecha (resp. a izquierda), se tiene $F(x) \neq F(y)$.

3. Un autómata celular $(\mathcal{A}^{\mathbb{Z}}, F)$ es cerrado si, y sólo si, es cerrado a derecha ó cerrado a izquierda.

Ejemplo 2.1. El shift es inyectivo, por tanto es cerrado a izquierda y a derecha.

Ejemplo 2.2. Consideremos el alfabeto $\mathcal{A} = \mathbb{Z}_2$ y $(\mathcal{A}^{\mathbb{Z}}, F)$ el autómata celular lineal dado por $F(x)(n) = x(n-1) + x(n+1) \pmod 2$, para cada $x \in \mathcal{A}^{\mathbb{Z}}$ y $n \in \mathbb{Z}$. Afirmamos que F es cerrado a izquierda y a derecha. En efecto, sean $x, y \in \mathcal{A}^{\mathbb{Z}}$ con $x \neq y$ asintóticos a derecha, por definición de asintoticidad a derecha podemos suponer que existe $n \in \mathbb{Z}$ tal que

$$x(n) \neq y(n) \text{ y } x_{(n,+\infty)} = y_{(n,+\infty)}.$$

Luego, de la definición de F es $F(x)(n+1) \neq F(y)(n+1)$ y por lo tanto F es cerrado a izquierda. De forma análoga se demuestra que F es cerrado a derecha.

Definición 2.3. Dados $x, y \in \mathcal{A}^{\mathbb{Z}}$ y un entero $s \geq 1$ se dice que:

1. x, y están s-separados si, y sólo si, para cada $n \in \mathbb{Z}$ se tiene que

$$x_{[n,n+s-1]} \neq y_{[n,n+s-1]}.$$

2. x, y están s-separados a izquierda (resp. a derecha) si existe $m \in \mathbb{Z}$ tal que $x_{[n,n+s-1]} \neq y_{[n,n+s-1]}$ para cada $n \leq m$ (resp. $n \geq m$).

Ejemplo 2.3. Sean $x, y \in \mathbb{Z}_2^{\mathbb{Z}}$, dados por:

$$x(i) = \begin{cases} 1, & \text{si } i \text{ es par} \\ 0, & \text{si } i \text{ es impar} \end{cases} \text{ y } y(i) = \begin{cases} 0, & \text{si } i \text{ es par} \\ 1, & \text{si } i \text{ es impar} \end{cases}.$$

Note que x, y están s-separados para cada entero $s \geq 1$, ya que por definición y y x difieren en cada entero.

El siguiente resultado, aunque no se encontró una publicación que lo contenga, ha sido demostrado por M. Akiyama en una sesión del seminario de Sistemas Dinámicos de la UCLA. Se incluye su demostración, ya que el hecho que nos presenta es relevante para la prueba del teorema principal de este capítulo.

Teorema 2.3. *Todo k-autómata celular en $\mathbb{Z}$ es topológicamente conjugado a un autómata celular en $\mathbb{Z}$.*

Demostración: Supongamos que $F : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ es un k-autómata celular de radio r; es decir, tenemos k reglas locales $\varphi_0, \ldots, \varphi_{k-1} : \mathcal{A}^{[-r,r]} \longrightarrow \mathcal{A}$ tales que para cada $x \in \mathcal{A}^{\mathbb{Z}}$ y $n \in \mathbb{Z}$,

$$F(x)(n) = \varphi_{n_k}(x(n-r, \ldots, n+r)),$$

donde n_k es el entero n tomando módulo k.

Sea $\mathcal{B} = \mathcal{A}^k$ y consideremos las funciones $h : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{B}^{\mathbb{Z}}$ y $\hat{h} : \mathcal{B}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ definidas, para cada $x \in \mathcal{A}^{\mathbb{Z}}$, $\hat{x} \in \mathcal{B}^{\mathbb{Z}}$ y $m \in \mathbb{Z}$, por:

$$h(x)(m) = x_{[mk,mk+k-1]} \text{ y } \hat{h}(\hat{x})(m) = \hat{x}_j(n),$$

donde $m = nk + j$, $0 \leq j \leq k-1$ y $\hat{x}(n) = \hat{x}_0(n) \cdots \hat{x}_j(n) \cdots \hat{x}_{k-1}(n)$.

Afirmamos que h y $\hat{h}$ son funciones continuas y una es la inversa de la otra.

En efecto, sean $\hat{x} \in \mathcal{B}^{\mathbb{Z}}$, $x \in \mathcal{A}^{\mathbb{Z}}$ y $m \in \mathbb{Z}$; nótese que por definición de $\hat{h}$ y h tenemos

$$\hat{h}(\hat{x})(mk+j) = \hat{x}_j(m), \text{ para cada } 0 \leq j < k \text{ y } h(\hat{h}(\hat{x}))(m) = \hat{h}(\hat{x})_{[mk,mk+k-1]},$$

pero $\hat{h}(\hat{x})_{[mk,mk+k-1]} = \hat{x}_0(m)\hat{x}_1(m) \cdots \hat{x}_{k-1}(m)$, luego

$$(h \circ \hat{h})(\hat{x}) = \hat{x}. \tag{2.1}$$

Por otro lado, sabemos que dado $m \in \mathbb{Z}$, existen $0 \leq j < k$ y $n \in \mathbb{Z}$ tales que $m = nk + j$. Además, puesto que $x(nk + j) = (h(x))_j(n)$, entonces

$$(\hat{h} \circ h)(x)(m) = \hat{h}(h(x))(m) = (h(x))_j(n) = x(nk + j) = x(m);$$

esto es,

$$(\hat{h} \circ h)(x) = x. \tag{2.2}$$

Así (2.1) y (2.2) implican que h es biyectiva. Observemos que es simple verificar la continuidad de h a partir de su definición.

Ahora bien, ya que $\mathcal{A}^{\mathbb{Z}}$ y $\mathcal{B}^{\mathbb{Z}}$ son espacios compactos y Hausdorff; h es una función continua, entonces por el teorema 1.2, h es un homeomorfismo. Además, el homeomorfismo h y la transformación F definen la transformación $G : \mathcal{B}^{\mathbb{Z}} \longrightarrow \mathcal{B}^{\mathbb{Z}}$ dada por $G = h \circ F \circ \hat{h}$, claramente G es conjugación de F. Más aún, G es una transformación continua que conmuta con el shift de $\mathcal{B}^{\mathbb{Z}}$. Verifiquemos tal afirmación, G es continua ya que es composición de funciones continuas.

Por otro lado, denotemos el shift de $\mathcal{B}^{\mathbb{Z}}$ por σ_0 y el shift de $\mathcal{A}^{\mathbb{Z}}$ por σ, y demostremos que la siguiente relación entre σ_0 y σ,

$$\sigma_0 \circ h = h \circ \sigma^k, \tag{2.3}$$

implica la conmutatividad de G con σ_0.

Sean $x \in \mathcal{A}^{\mathbb{Z}}$ y $m \in \mathbb{Z}$, recordando la definición de σ_0 y h tenemos

$$\sigma_0(h(x))(m) = h(x)(m + 1) \text{ y } h(\sigma^k(x))(m) = \sigma^k(x)_{[km,km+k-1]}, \tag{2.4}$$

pero

$$\begin{aligned} h(x)(m + 1) &= x_{[(m+1)k,(m+1)k+k-1]} \\ &= x_{[mk+k,mk+k-1+k]} \\ &= \sigma^k(x)_{[mk,mk+k-1]}. \end{aligned} \tag{2.5}$$

Luego, por (2.4) y (2.5) se sigue (2.3) y como consecuencia inmediata se tiene

$$h^{-1} \circ \sigma_0 = \sigma^k \circ h^{-1}. \tag{2.6}$$

Note por otra parte que (2.3) y (2.6) implican que

$$\sigma_0 \circ G = (h \circ \sigma^k) \circ (F \circ h^{-1}) \text{ y } G \circ \sigma_0 = (h \circ F) \circ (\sigma^k \circ h^{-1})$$

y puesto que F es un k-autómata celular, por el teorema 1.3, F conmuta con la k-ésima potencia de σ; por lo tanto G conmuta con σ_0.

Es bien conocido que toda transformación continua que conmute con el shift es un autómata celular, ver teorema 3.4 en [17], así esta completa la demostración. □

Observación 2.1. El homeomorfismo h del teorema 2.3 es lineal en $\mathbb{Z}_N^{\mathbb{Z}}$, pues, si $x, y \in \mathbb{Z}_N^{\mathbb{Z}}$, $m \in \mathbb{Z}$, y $\alpha \in \mathbb{Z}_N$, entonces

$$\begin{aligned} h(\alpha x + y)(m) &= (\alpha x + y)_{[mk, mk+k-1]} \\ &= \alpha x_{[mk, mk+k-1]} + y_{[mk, mk+k-1]} \\ &= \alpha h(x)(m) + h(y)(m), \end{aligned}$$

por lo tanto, $h(\alpha x + y) = \alpha h(x) + h(y)$.

Por otra parte, puesto que h es un homeomorfismo lineal y como $(\mathbb{Z}_N^k)^{\mathbb{Z}}$ es un $\mathbb{Z}_N^k$-módulo con las operaciones usuales de adición y multiplicación por escalar en $\mathbb{Z}_N^k$; esto es, dados $a_0 \cdots a_{k-1}$, $b_0 \cdots b_{k-1}$ en $\mathbb{Z}_N^k$ y $\alpha \in \mathbb{Z}_N$, se define la adición en $\mathbb{Z}_N^k$ por $a_0 \cdots a_{k-1} + b_0 \cdots b_{k-1} = (a_0 + b_0)_0 \cdots (a_{k-1} + b_{k-1})_{k-1}$ y la multiplicación por escalar, $\alpha(a_0 \cdots a_{k-1}) = \alpha a_0 \cdots \alpha a_{k-1}$, entonces el homeomorfismo $\hat{h}$ es lineal en $(\mathbb{Z}_N^k)^{\mathbb{Z}}$.

Corolario 2.1. *Si* $(\mathbb{Z}_N^{\mathbb{Z}}, F)$ *es un* k*-autómata celular lineal, entonces* $((\mathbb{Z}_N^k)^{\mathbb{Z}}, G)$ *es un autómata celular lineal, donde* G *y* $\mathbb{Z}_N^k$ *son como en el teorema 2.3.*

Demostración: Supongamos F lineal. Ya que F es un k-autómata celular, el teorema 2.3 indica que F es conjugado topológicamente al autómata celular G definido sobre $(\mathbb{Z}_N^k)^{\mathbb{Z}}$ como $G = h \circ F \circ \hat{h}$, donde h y $\hat{h}$ están definidas como en el teorema 2.3. Por lo tanto, de la observación 2.1 y la linealidad de F, deducimos que G es lineal. □

Vamos ahora a enunciar y demostrar algunos resultados de Hedlund, debido a su importancia para el desarrollo del presente capítulo. Destacamos que tales resultados fueron expuestos por Jesus Silva en [32].

Teorema 2.4. *(Hedlund [17]). Sean $(\mathcal{A}^{\mathbb{Z}}, F)$ un autómata celular sobreyectivo y $x \in Per(\sigma)$, entonces para cada $y \in F^{-1}(x)$, $y \in Per(\sigma)$.*

Demostración: Supongamos que existe un punto y no perteneciente al $Per(\sigma)$ tal que $y \in F^{-1}(x)$, sea $p \geq 1$ tal que $\sigma^{jp}(x) = x$, para cada $j \in \mathbb{Z}$. Es claro que si $i, l \in \mathbb{Z}$ con $i \neq l$, entonces $\sigma^{ip}(y) \neq \sigma^{lp}(y)$ de lo contrario $y \in Per(\sigma)$.

Ahora bien, para cada $j \in \mathbb{Z}$ se cumple $F(\sigma^{jp}(y)) = \sigma^{jp}(F(y)) = \sigma^{jp}(x)$ y $\sigma^{jp}(x) = x$; luego $\sigma^{jp}(y) \in F^{-1}(x)$, para cada $j \in \mathbb{Z}$ y $\sigma^{ip}(y) \neq \sigma^{lp}(y)$ con $i \neq l$. De esta forma, $card(F^{-1}(x)) = \infty$, lo cual contradice la sobreyectividad de F, ver teorema 2.1. □

Definición 2.4. Sea $n \in \mathbb{Z}$, $n \geq 1$. Un n-bloque sobre $\mathcal{A}$ es un conjunto ordenado $a_1 a_2 \cdots a_n$, donde $a_i \in \mathcal{A}$ $(i = 1, \cdots, n)$. Se denota por $\mathcal{A}^n$ al conjunto de todos los n-bloques sobre $\mathcal{A}$.

Sea $\psi : \mathcal{A}^n \to \mathcal{A}$ una función de $\mathcal{A}^n$ sobre $\mathcal{A}$. El conjunto de tales funciones para un entero n, con $n \geq 1$ dado, será denotado por $L(\mathcal{A}, n)$.

Sean $\psi \in L(\mathcal{A}, n+1)$ y $s \in \mathbb{Z}$, $s \geq 0$; se define $\psi^s : \mathcal{A}^{s+n+1} \to \mathcal{A}^{s+1}$ como sigue, para cada $b_0 b_1 \cdots b_{s+n} \in \mathcal{A}^{s+n+1}$ consideremos $a_i = \psi(b_i b_{i+1} \cdots b_{i+n})$, donde $i = 0, 1, \cdots, s$, entonces $\psi^s(b_0 b_1 \cdots b_{s+n}) = a_0 a_1 \cdots a_s$.

Es común denominar a la función ψ^s como regla local de n variables.

Nota 2.1. Sea $\mathcal{A}$ un alfabeto, de aquí en adelante trabajaremos con autómatas celulares generados por una regla local ψ, definida sobre el vecindario V de la forma $[q, q+p]$ con $p, q \in \mathbb{Z}$, $p \geq 1$. Es también importante mencionar que para cualquier par $A \in \mathcal{A}^m$; $B \in \mathcal{A}^n$, AB denotará el $(m+n)$-bloque sobre $\mathcal{A}$ obtenido concatenando A y B; es decir, $AB \in \mathcal{A}^{m+n}$.

Teorema 2.5. *(Hedlund [17]). Sean p, q enteros con $p \geq 1$; $\psi \in L(\mathcal{A}, p+1)$, $V = [q, q+p]$ y $(\mathcal{A}^{\mathbb{Z}}, F)$ el autómata celular generado por ψ y V, entonces $(\mathcal{A}^{\mathbb{Z}}, F)$ no es sobreyectivo si se cumple al menos una de las siguientes condiciones:*

1. *Existen $W \in \mathcal{A}^p$, $n \geq 1$ y $P, Q \in \mathcal{A}^n$ con $P \neq Q$ tales que: $\psi^{p+n-1}(WPW) = \psi^{p+n-1}(WQW)$.*
2. *Existen $W_1, W_2 \in \mathcal{A}^p$, $n \geq 1$ y $P, Q \in \mathcal{A}^n$ con $P \neq Q$ tales que: $\psi^{p+n-1}(W_1PW_2) = \psi^{p+n-1}(W_1QW_2)$.*

Demostración: Supongamos que la condición 1 es cierta. Sean $S_0 = WP$ y $S_j = WQ$ si $j \neq 0$, definamos $x \in \mathcal{A}^{\mathbb{Z}}$ como sigue,

$$x = \cdots S_{-1}\dot{S}_0 S_1 \cdots = \cdots WQ\dot{W}PWQ \cdots$$

y sea $H = \psi^{p+n-1}(WPW) = \psi^{p+n-1}(WQW)$. Note que si $y = \sigma^{-q}(x)$, entonces para cada intervalo de la forma $I_j = [j(n+p), (j+1)(n+p)-1]$ con $j \in \mathbb{Z}$, se tiene que

$$\begin{aligned} F(y)_{[j(n+p),(j+1)(n+p)-1]} &= \psi^{p+n-1}(y_{[j(p+n)+q,(j+1)(n+p)+q+p-1]}) \\ &= \psi^{p+n-1}(x_{[j(p+n)),(j+1)(p+n)+p-1]}) \\ &= \psi^{p+n-1}(S_jW) \\ &= H. \end{aligned}$$

Luego $F(y) = \cdots H\dot{H}H \cdots$, note que y no es periódico pues $P \neq Q$, en virtud del teorema 2.4 deducimos que F no es sobreyectivo.

Supongamos ahora que la condición 2 es cierta y sean $H_1 = \psi^{p-1}(W_2W_1)$ y $H_2 = \psi^{p+n-1}(W_1PW_2) = \psi^{p+n-1}(W_1QW_2)$, de esta manera

$$\psi^{2p+n-1}(W_1PW_2W_1) = H_2H_1 = \psi^{2p+n-1}(W_1QW_2W_1).$$

Así, la condición 1 es cierta y por lo tanto F no es sobreyectivo. $\square$

Teorema 2.6. *(Hedlund [17]). Sean p, q enteros con $p \geq 1$; $\psi \in L(\mathcal{A}, p+1)$, $V = [q, q+p] \subset \mathbb{Z}$ y $(\mathcal{A}^{\mathbb{Z}}, F)$ un autómata celular generado por ψ y V. Si $(\mathcal{A}^{\mathbb{Z}}, F)$ es sobreyectivo y existen $y, x \in \mathcal{A}^{\mathbb{Z}}$ con $y \neq x$ tales que $F(y) = F(x)$, entonces y, x están p-separados a derecha ó a izquierda; (posiblemente ambos).*

Demostración: Supongamos que x, y no están p-separados ni a derecha ni a izquierda. Sean $i \in \mathbb{Z}$ tal que $y(i) \neq x(i)$ y $M = max\{| i |, p+1\}$.

Como y, x no están p-separados a derecha, existe un entero $m > M$ tal que $y_{[m,m+p-1]} = x_{[m,m+p-1]}$; así, $H_1 = y_{[m,m+p-1]}$. De igual forma, como y, x no están p-separados a izquierda, existe $n < -M-p$ tal que $y_{[n,n+p-1]} = x_{[n,n+p-1]}$; sean $H_2 = y_{[n,n+p-1]}$, $H_3 = y_{[n+p,m-1]}$ y $H_4 = x_{[n+p,m-1]}$. Claramente, como $n + p < i \leq m - 1$ se tiene que $H_3 \neq H_4$, además

$$y_{[n,m+p-1]} = H_2H_3H_1 \text{ y } x_{[n,m+p-1]} = H_2H_4H_1.$$

Dado que $F(y) = F(x)$, en particular $F(y)_{[n-q,m-q-1]} = F(x)_{[n-q,m-q-1]}$, luego $\psi^{m-n-1}(y_{[n,m+p-1]}) = \psi^{m-n-1}(x_{[n,m+p-1]})$. En virtud del teorema 2.5 F no es sobreyectivo. $\square$

Nota 2.2. Si consideramos $\mathcal{A}$ un anillo finito y ψ una regla local lineal en $\mathcal{A}^V$ donde $V = [q, q+p]$ con $p, q \in \mathbb{Z}$; $p \geq 1$, entonces el autómata celular generado por ψ y $[q, q+p]$ es lineal.

Teorema 2.7. *Sean p, q enteros con $p \geq 1$; $\psi \in L(\mathcal{A}, p+1)$, $\mathcal{A}$ un anillo finito, ψ lineal y $(\mathcal{A}^{\mathbb{Z}}, F)$ el autómata celular generado por ψ y la vecindad $V = [p, p+q] \subset \mathbb{Z}$. Si $(\mathcal{A}^{\mathbb{Z}}, F)$ es sobreyectivo, entonces existe $s > 0$ tal que para cada $y \in \mathcal{A}^{\mathbb{Z}}$, $card(F^{-1}(y)) = s$.*

Demostración: Supongamos F lineal y sobreyectivo, entonces por el teorema 2.1, para cada $y \in \mathcal{A}^{\mathbb{Z}}$; $card(F^{-1}(y)) < +\infty$.

Ahora bien, sea $y \in \mathcal{A}^{\mathbb{Z}}$ fijo pero arbitrario, definamos una función ϕ de $F^{-1}(0)$ a $F^{-1}(y)$ como $\phi(z) = z + w$, donde $w \in F^{-1}(y)$ es fijo. Verifiquemos que ϕ esta bién definida, para esto considere $z \in F^{-1}(0)$ y aplíquese F a $\phi(z)$; así, $F(z+w) = F(z) + F(w) = y$.

Es importante mencionar que ϕ arriba definida es biyectiva, de hecho si $z_1, z_2 \in F^{-1}(0)$ son tales que $\phi(z_1) = \phi(z_2)$, entonces $z_1 + w = z_2 + w$, y esto implica claramente $z_1 = z_2$, por consiguiente, ϕ es inyectiva.

Verifiquemos ahora la sobreyectividad de ϕ; esto es,
dado $u \in F^{-1}(y)$ deseamos hallar $x \in F^{-1}(0)$ tal que $\phi(x) = u$.

Observemos que si $x = u - w$, entonces

$$F(x) = F(u-w) = F(u) - F(w) = 0 \text{ y } x \text{ es tal que } \phi(x) = u.$$

Así, ϕ es sobreyectiva.

Sabemos de la teoría de conjuntos que si existe una función biyectiva definida entre dos conjuntos finitos estos tienen el mismo número de elementos, por lo tanto para cada $y \in \mathcal{A}^{\mathbb{Z}}$, $card(F^{-1}(y)) = car(F^{-1}(0))$. $\square$

Teorema 2.8. *Sean p, q enteros con $p \geq 1$; $\psi \in L(\mathcal{A}, p+1)$, $\mathcal{A}$ un anillo finito, ψ lineal y $(\mathcal{A}^{\mathbb{Z}}, F)$ el autómata celular generado por ψ y la vecindad $V = [p, p+q] \subset \mathbb{Z}$. Si $(\mathcal{A}^{\mathbb{Z}}, F)$ es sobreyectivo, entonces existe $b > 0$ tal que para cada $w \in \mathcal{A}^{\mathbb{Z}}, card(F^{-1}(w)) = b$ y si $b \geq 2$, entonces para cada $1 \leq i < j \leq b$, $w_i, w_j \in F^{-1}(w)$ están p-separados.*

Demostración: Supongamos F lineal y sobreyectivo, entonces por el teorema 2.7, existe $b > 0$ tal que para cada $w \in \mathcal{A}^{\mathbb{Z}}, card(F^{-1}(w)) = b$. Supongamos ahora $b \geq 2$ y que para algún $z \in \mathcal{A}^{\mathbb{Z}}$ existen $x, y \in F^{-1}(z)$ con $x \neq y$ tales que x, y no están p-separados; así, existe $n \in \mathbb{Z}$ tal que

$$x_{[n,n+p-1]} = y_{[n,n+p-1]}. \tag{2.7}$$

Destacamos que por el teorema 2.6, las configuraciones x, y están p-separados a derecha ó a izquierda. Consideremos primero el caso en que las configuraciones x, y están p-separados a derecha; luego, por definición de separabilidad a derecha, existe $m > n + p - 1$ tal que para cada $j \geq m$

$$x_{[j,j+p-1]} \neq y_{[j,j+p-1]}. \tag{2.8}$$

Ahora bien, como F es lineal y $F(x) = F(y)$, entonces $F(x - y) = 0$. Además, $0 \in Per(\sigma)$ y $x - y \in F^{-1}(0)$; así, por el teorema 2.4 se tiene que $x - y \in Per(\sigma)$ y por lo tanto, existe $a \geq 1$ tal que

$$\sigma^a(x - y) = x - y. \tag{2.9}$$

Nótese que (2.9) implica que, para cada $i \geq 1$

$$\sigma^{ia}(x - y) = x - y. \tag{2.10}$$

Por otro lado, si $n \in \mathbb{Z}$ como en (2.7) y seleccionamos $s \geq 1$ tal que $n + sa > m$, entonces combinando (2.7), (2.10) y considerando $\sigma^{sa}(x - y)$, $(x - y)$ restrictas al intervalo entero $[n, n + p - 1]$ tenemos

$$(x - y)_{[n+sa,n+sa+p-1]} = (x - y)_{[n,n+p-1]} = 0. \tag{2.11}$$

Pero claramente (2.11) contradice (2.8) para $sa + n > m$. Esto último demuestra que x, y están p-separados si x, y están p-separados a derecha, el caso x, y p-separados a izquierda se demuestra de forma análoga. $\square$

Corolario 2.2. *Sean p, q enteros con $p \geq 1$; $\psi \in L(\mathcal{A}, p+1)$, $\mathcal{A}$ un anillo finito, ψ lineal y $(\mathcal{A}^{\mathbb{Z}}, F)$ el autómata celular generado por ψ y la vecindad $V = [p, p+q] \subset \mathbb{Z}$. Si $(\mathcal{A}^{\mathbb{Z}}, F)$ es sobreyectivo, entonces $(\mathcal{A}^{\mathbb{Z}}, F)$ es cerrado a derecha y a izquierda.*

Demostración: Supongamos $(\mathcal{A}^{\mathbb{Z}}, F)$ lineal, sobreyectivo y que no es cerrado a derecha, entonces exiten $x, y \in \mathcal{A}^{\mathbb{Z}}$ con $x \neq y$ asintóticos a izquierda tales que $F(x) = F(y)$, pero esto contradice el teorema 2.8.

De forma análoga se demuestra que F es cerrado a izquierda. $\square$

Teorema 2.9. *(teorema principal)*
Si $(\mathbb{Z}_N^{\mathbb{Z}}, F)$ es un k-autómata celular lineal sobreyectivo, entonces $(\mathbb{Z}_N^{\mathbb{Z}}, F)$ es regular.

Demostración: Supongamos F lineal y sobreyectivo, entonces por el corolario 2.1 se identifica $(\mathbb{Z}_N^{\mathbb{Z}}, F)$ con el autómata celular lineal sobreyectivo $((\mathbb{Z}_N^k)^{\mathbb{Z}}, G)$; así, por el corolario 2.2 se sigue que $((\mathbb{Z}_N^k)^{\mathbb{Z}}, G)$ es cerrado. Ahora bien, por el teorema 2.2, $((\mathbb{Z}_N^k)^{\mathbb{Z}}, G)$ es regular.

Por lo tanto, debido a que $((\mathbb{Z}_N^k)^{\mathbb{Z}}, G)$ y $(\mathbb{Z}_N^{\mathbb{Z}}, F)$ son topológicamente conjugados, obtenemos que F es regular. $\square$

3 Inyectividad y Sobreyectividad de los k-autómatas celulares lineales

En el presente capítulo se caracterizan las propiedades de inyectividad y sobreyectividad en el contexto de los k-autómatas celulares lineales usando las mismas técnicas empleadas por Kari, en [19]. Destacamos que se hará uso de las denominadas series y polinomios de Laurent introducidas por Masanobu Itô, Nobuyasu Ôsato y Masakazu Nasu para lograr dichas caracterizaciones, ver [18].

3.1. Polinomios y Series de Laurent

Se inicia está sección considerando el anillo $\mathbb{Z}_N$; $N \geq 2$, y un autómata celular lineal $(\mathbb{Z}_N^{\mathbb{Z}}, H)$ generado por la regla local aditiva $\varphi : \mathbb{Z}_N^{[-r,r]} \longrightarrow \mathbb{Z}_N$, dada por $\varphi(x_{-r}, \cdots, x_r) = \sum_{j=-r}^{r} b_j x_j$ módulo N, donde $b_j \in \mathbb{Z}_N$ para cada $j = -r, \ldots, r$. Cabe destacar que la regla local φ define un polinomio sobre $\mathbb{Z}_N$ dado por

$$P(X) = \sum_{j=-r}^{r} b_j X^{-j} \tag{3.1}$$

y una configuración $C = (c(j))_{j\in\mathbb{Z}}$, define una serie sobre $\mathbb{Z}_N$ dada por

$$S_C(X) = \sum_{j=-\infty}^{+\infty} c(j) X^j. \tag{3.2}$$

Además, cualquier serie, define una configuración C de la siguiente manera, para cada entero j, $c(j)$ es el coeficiente de la potencia X^j de dicha serie.

Es importante mencionar que al polinomio $P(X)$ definido en (3.1), se le conoce como polinomio de Laurent y a la serie $S_C(X)$ definida en (3.2) como serie de Laurent. Es bien conocido de la teoría de autómatas celulares lineales que la serie de Laurent asocida a la configuración $H(C)$ es

$$P(X)S_C(X) = \sum_{m=-\infty}^{+\infty} (\sum_{j=-r}^{r} b_j c(m+j))X^m. \tag{3.3}$$

Verifiquemos la relación (3.3), puesto que $P(X)$ está definido sobre un vecindario simétrico lo podemos reescribir como sigue, $P(X) = \sum_{j=-r}^{r} b_{-j}X^j$; además, $P(X)$ se extiende a una serie suponiendo cero los coefientes cuyos subíndices no pertenescan al intervalo de números enteros $[-r, r]$. De esta forma, podemos aplicar el criterio de Cauchy para series de Laurent, y obtener que

$$P(X)S_C(X) = \sum_{m=-\infty}^{+\infty} (\sum_{j=-r}^{r} b_{-j} c(m-j))X^m.$$

Nuevamente, por la simétria de $[-r, r]$ tenemos

$$P(X)S_C(X) = \sum_{m=-\infty}^{+\infty} (\sum_{j=-r}^{r} b_j c(m+j))X^m.$$

Así, (3.3) nos permite describir la dinámica del autómata celular lineal H; como sigue, sabemos que para cada entero positivo n, $H^n(C) = H(H^{n-1})(C)$, por lo tanto (3.3) indica que la serie de Laurent asociada a $H^n(C)$ es la serie $P(X)(P^{n-1}(X)(C))$.

Por otra parte, cualquier polinomio de Laurent $Q(X)$ sobre $\mathbb{Z}_N$ define un autómata celular lineal cuyo polinomio de Laurent es precisamente $Q(X)$.

Verifiquemos la última afirmación, sea $Q(X)$ un polinomio de Laurent; es decir, $Q(X) = \sum_{i \in M} \alpha_i X^{-i}$ donde $M \subset \mathbb{Z}$, finito. Ahora si consideremos el conjunto $L = \{-i : i \in M\}$ claramente finito, entonces la regla local $\sum_{j \in L} \alpha_j x_j$ define un autómata celular lineal cuyo polinomio de Laurent es $Q(X)$.

Vamos ahora a enunciar los resultados referentes a la inyectividad y sobreyectividad de los autómatas celulares lineales, pues serán de utilidad en este capítulo después que caracterizeremos la inyectividad y sobreyectividad de los k-autómatas celulares lineales.

Teorema 3.1. *(M. Itô, N. Ôsato and M. Nasu [18]). El autómata celular lineal representado por el polinomio $P(X) = \sum_{i=1}^{n} a_i X^{v_i}$ sobre $\mathbb{Z}_N$ es:*

1. *Sobreyectivo si, y sólo si, $mcd(N, a_1, \ldots, a_n) = 1$.*

2. *Inyectivo si, y sólo si, para cada $p \in P$ existe un único elemento a_j del conjunto $\{a_1, \ldots, a_n\}$ tal que p no divide a_j.*

Donde *mcd* representa el máximo común divisor de $N, a_1, \ldots, a_n$ y P es el conjunto de factores primos de N.

Nuestro próximo objetivo es modelar la dinámica de los k-autómatas celulares lineales en términos de polinomios y series de Laurent.

Iniciemos considerando $(\mathbb{Z}_N^{\mathbb{Z}}, F)$ un k-autómata celular de radio r, generado por reglas locales de la forma $\varphi_i(x_{-r}, \ldots, x_r) = \sum_{j=-r}^{r} \alpha_j^i x_j$ módulo N, donde $\alpha_j^i \in \mathbb{Z}_N$ para cada $i \in \{0, \ldots, k-1\}$ y cada $j \in \{-r, \ldots, r\}$.

Evidentemente, cada regla local φ_i está asociada a un polinomio de Laurent,

$$P_i(X) = \sum_{j=-r}^{r} \alpha_j^i X^{-j}. \tag{3.4}$$

Se define para cada entero $m \in [0, k-1]$ el siguiente conjunto

$$I_m = \{q : -r \leq q \leq r \text{ y } q = m \quad (\text{ mod k })\}. \tag{3.5}$$

Nótese que cada polinomio $P_i(X)$ como en (3.4) lo podemos reescribir en términos de los conjuntos I_m definidos en (3.5), de la siguiente manera

$$P_i(X) = \sum_{j=0}^{k-1}(\sum_{s\in I_j} \alpha_s^i X^{-s}); \tag{3.6}$$

así, para cada $p = 0, \dots, k-1$ denotemos por $Q_p^i(X)$ la siguiente suma

$$Q_p^i(X) = \sum_{s \in I_p} \alpha_s^i X^{-s}. \tag{3.7}$$

Destacamos que los polinomios mencionados en (3.7) nos permite definir una matriz de orden $k \times k$, como sigue

$$P_{ij}(X) = \begin{cases} Q_0^i(X) & \text{si} \quad i = j \\ Q_{j-i}^i(X) & \text{si} \quad i \neq j, \end{cases} \tag{3.8}$$

denotemos tal matriz por $A(X)$.

Observación 3.1. Es claro que para cada $i \in [0, k-1]$ fijo, los subíndices $0-i, 1-i, \cdots, (k-1)-i$ de los polinomios de la fila i de la matriz $A(X)$ no se repiten. Además, cuando $j-i$ es negativo ($i > j$) considere su equivalente módulo k. Luego, $\sum_{j=0}^{k-1} Q_{j-i}^i(X) = P_i(X)$.

Consideremos ahora una configuración $C = (c(j))_{j \in \mathbb{Z}}$, recuerde que tal configuración está asociada a la serie de Laurent $S_C(X)$ como en (3.2), es fácil ver que la serie $S_C(X)$ es igual a

$$S_C(X) = \sum_{i=0}^{k-1} (\sum_{j \in [i]} c(j) X^j), \tag{3.9}$$

donde $[i]$ es la clase de i módulo k. Luego, para cada $i = 0, \dots, k-1$ denotemos por $C_i(X)$ la siguiente serie

$$C_i(X) = \sum_{j \in [i]} c(j) X^j. \tag{3.10}$$

Observe que las series definidas en (3.10) definen una matriz columna de orden $k \times 1$, dada por $C_{i1}(X) = C_i(X)$, para cada $i = 0, \dots, k-1$, denotemos esta matriz por $C(X)$.

Afirmamos que el producto de la matriz $A(X)$ con la matriz $C(X)$ es la matriz $F(C)(X)$ asociada a la configuración $F(C)$.

En efecto, la entrada $i1$ de la matriz $A(X)C(X)$ es $\sum_{n=0}^{k-1} P_{in}(X)C_{n1}(X)$. Ahora bien, para calcular la serie anterior es conveniente calcular la serie de cada sumando; esto es, calcular $Q^i_{n-i}(X)C_n(X)$, para cada $n = 0, \ldots, k-1$. Para tal fin definamos $Y \in \mathbb{Z}_N^{\mathbb{Z}}$ como sigue,

$$y(j) = \begin{cases} c(j) & \text{si} \quad j \text{ está en } [n] \\ 0 & \text{si} \quad j \text{ no está en } [n]. \end{cases}$$

Así, su serie de Laurent es $S_Y(X) = \sum_{j=-\infty}^{+\infty} y(j)X^j$.

Por otro lado, al polinomio $Q^i_{n-i}(X)$ lo podemos extender a un polinomio definido sobre el intervalo entero $[-r, r]$ como sigue $P(X) = Q^i_{n-i}(X) + M(X)$, donde $M(X) = \sum_{s\in[-r,r]-I_{n-i}} 0X^{-s}$. De esta manera, aplicando (3.3) al producto $P(X)S_Y(X)$ se tiene

$$\sum_{m=-\infty}^{+\infty} \Big(\sum_{s\in I_{n-i}} \alpha^i_s + \sum_{s\in[-r,r]-I_{n-i}} 0 \Big) y(m+s)X^m. \tag{3.11}$$

Note que, $m + s \in [n]$ si, y sólo si, $m \in [n - s]$; pero $s \in I_{n-i}$, por lo tanto $m \in [n-s]$ si, y sólo si, $m \in [i]$. De este modo, para cada m en el complemento de $[i]$ tenemos que $y(m + s) = 0$; así, la serie (3.11) es

$$\sum_{m\in[i]} \sum_{s\in I_{n-i}} \alpha^i_s c(m+s)X^m. \tag{3.12}$$

Luego, por la observación 3.1 y como el producto de la fila i de la matriz $A(X)$ con la única columna de la matriz $C(X)$ da origen a k sumas como en (3.12), entonces

$$\sum_{n=0}^{k-1} P_{in}(X)C_{n1}(X) = \sum_{m\in[i]} \Big(\sum_{s=-r}^{r} \alpha^i_s c(m+s) \Big) X^m \, .$$

Por lo tanto, aplicando el procedimiento anterior a cada fila i de $A(X)$, deducimos que $A(X)C(X) = F(C)(X)$.

La importancia de está última relación es que nos permite definir de manera recursiva la matriz $F^n(C)(X)$; como sigue, la matriz $F^n(C)(X)$ asociada a la configuración $F^n(C)$ es $A(X)(A^{n-1}(X)C(X))$.

Para finalizar está sección estudiaremos la relación que hay entre una matriz cualquiera de orden $k \times k$ cuyas entradas son polinomios de Laurent y los k-autómatas celulares lineales. Comencemos denotando por $B(X)$ la matriz mencionada anteriormente y $P_{ij}(X)$ sus entradas, se define para cada i el siguiente polinomio, $Q_i(X) = \sum_{j=0}^{k-1} P_{ij}(X)$, tal como en el caso de autómatas celulares lineales $Q_i(X)$ define un autómata celular lineal tal que su polinomio de Laurent es el mismo $Q_i(X)$; así, tenemos k-reglas locales que definen un k-autómata celular lineal, y por construcción su matriz asociada es $B(X)$.

3.2. Inyectividad y Sobreyectividad

En esta sección caracterizaremos los k-autómatas celulares lineales inyectivos y sobreyectivos en térmimos de polinomios y series de Laurent.

Vamos ahora a enunciar un resultado clásico de la teoria de autómatas celurares, que se aplica en el presente capítulo.

Teorema 3.2. *(Hedlund [17]). Si F es un autómata celular no sobreyectivo de radio r, entonces existen $A \in \mathcal{A}^{2r}, m \geqslant 1$ y $P, Q \in \mathcal{A}^m$ con $P \neq Q$ tales que $\psi^{2r+m-1}(APA) = \psi^{2r+m-1}(AQA)$.*

Recuerde que para cada entero $s \geq 1$, ψ^s es definida como en el capítulo 2.

Definición 3.1. Sea $\mathcal{A}$ un anillo finito, se dice que $S \subset \mathcal{A}^{\mathbb{Z}}$ es el conjunto de configuraciones finitas de $\mathcal{A}^{\mathbb{Z}}$, si se cumple que $x \in S$ si, y sólo si, existen

$n, m \in \mathbb{Z}$ con $n \leqslant m$ tales que $x(i) = 0$ para cada i en el complemento de $[n, m]$.

Teorema 3.3. *Sea r un entero con $r \geqslant 0$, $\varphi \in L(\mathcal{A}, 2r+1)$, $V = [-r, r] \subset \mathbb{Z}$ y F el autómata celular lineal generado por φ y V, entonces F es sobreyectivo si, y sólo si, F es inyectivo sobre S.*

Demostración: Supongamos F sobreyectivo y no inyectivo sobre S; esto es, F sobreyectivo y existen $x, y \in S$ con $x \neq y$ tales que $F(x) = F(y)$. Luego, Por el teorema 2.6, x, y están $2r$-separados a derecha o a izquierda; pero como $x, y \in S$, son asintóticos a derecha y izquierda, que claramente contradice la separabilidad de y y x.

Recíprocamente, si F es inyectivo sobre S y no es sobreyectivo, entonces por teorema 3.2 existen $A \in \mathcal{A}^{2r}, m \geqslant 1$ y $P, Q \in \mathcal{A}^m$ con $P \neq Q$ tales que $\psi^{2r+m-1}(APA) = \psi^{2r+m-1}(AQA)$.

Ahora si $z = \cdots AP\dot{A}PAP \cdots$ y $w = \cdots AP\dot{A}QAP \cdots$, entonces

$$z - w \neq 0, z - w \in S \quad \text{y} \quad F(w - z) = 0;$$

pero esto último contradice la inyectividad de F en S. □

Teorema 3.4. *Sea F un k-autómata celular lineal, entonces F es sobreyectivo si y sólo si F es inyectivo sobre S.*

Demostración: Puesto que F es un k-autómata celular lineal, por el corolario 2.1 F es conjugado topológicamente al autómata celular lineal G definido sobre $(\mathbb{Z}_N^k)^{\mathbb{Z}}$ como $G = h \circ F \circ \hat{h}$ donde h y $\hat{h}$ son como en el teorema 2.3.

Supongamos ahora que F es sobreyetivo, luego G también lo es; así, por el teorema 3.3, G es inyectivo sobre el conjunto de configuraciones finitas de $(\mathbb{Z}_N^k)^{\mathbb{Z}}$, se denotará este conjunto por H. Deseamos demostrar que F es inyectivo sobre S, para tal fin demostraremos primero lo siguiente

$$h(S) \subset H. \tag{3.13}$$

En efecto, sea $x \in S$ por definición 3.1, existen $n, m \in \mathbb{Z}$ con , $n \leqslant m$ tales que $x(i) = 0$ para cada i en el complemento de $[n, m]$; note que para cada $p > m$, $h(x)(p) = x_{[pk,pk+k-1]} = 0$. Por otro lado, si seleccionamos q tal que $qk + k - 1 < n$, entonces para cada $p < q$ tenemos $h(x)(p) = x_{[pk,pk+k-1]} = 0$, por lo tanto la relación (3.13) queda demostrada.

Afirmación: Si G es inyectivo sobre H, entonces F es inyectivo sobre S.

Probemos esto último, sean $x_1, x_2 \in S$ tales que $x_1 \neq x_2$, recordando que h una función inyectiva, ocurre que $h(x_1) \neq h(x_2)$, ahora combinando los siguientes resultados, G inyectivo sobre H y la relación 3.13 se sigue

$$G(h(x_1)) \neq G(h(x_2)) \tag{3.14}$$

y puesto que $\hat{h}$ es inyectivo deducimos que

$$\hat{h}(G(h(x_1))) \neq \hat{h}(G(h(x_2))),$$

por lo tanto F es inyectivo sobre S.

Recíprocamente, si F es inyectivo sobre S, por la definición de $\hat{h}$ tenemos

$$\hat{h}(H) \subset S. \tag{3.15}$$

Luego, por la relación (3.15) y puesto que $G = h \circ F \circ \hat{h}$, empleamos un razonamiento análogo a la afirmación anterior para verificar que, si $x_1, x_2 \in H$ son tales que $x_1 \neq x_2$, entonces $G(x_1) \neq G(x_2)$. Así, G es inyectivo sobre H y por el teorema 3.3 se tiene que G es sobreyectivo, de este modo F es sobreyectivo. $\square$

Teorema 3.5. *Sea* $(\mathbb{Z}_N^{\mathbb{Z}}, F)$ *un k-autómata celular lineal, entonces*

1. F es inyectivo si, y sólo si, $A(X)$ es invertible.

2. F es sobreyectivo si, y sólo si, para cada matriz de orden $k \times k$, $B(X) \neq 0$ se tiene que $A(X)B(X) \neq 0$.

Donde $A(X)$ es la matriz asociada a F como lo indicado en (3.8).

Demostración: Comencemos demostrando 1.

Supongamos $A(X)$ invertible. Ahora bien, si $C_1, C_2 \in \mathbb{Z}_N^{\mathbb{Z}}$ son tales que $F(C_1) = F(C_2)$, entonces $A(X)C_1(X) = A(X)C_2(X)$, ya que $A(X)$ es invertible se sigue $C_1(X) = C_2(X)$ y por lo tanto $C_1 = C_2$.

Recíprocamente, si F es inyectivo, particularmente F es inyectivo sobre S; así, por el teorema 3.4 tenemos que F es sobreyectivo. Luego, F es lineal y biyectiva, entonces por el teorema 1.4, existe un k-autómata celular lineal g tal que $g \circ F = F \circ g = I$, donde I es la identidad de $\mathcal{A}^{\mathbb{Z}}$.

Por lo tanto, existe una matriz $B(X)$ asociada a g tal que $A(X)B(X) = I_k$, donde I_k es la matriz identidad de orden k.

Demostremos ahora 2.

Supongamos F sobreyectivo y que existe una matriz $B(X) \neq 0$ de orden $k \times k$ tal que $A(X)B(X) = 0$. Puesto que F es sobreyectivo, el teorema 3.4 implica que F es inyectivo sobre S.

Por otra parte, ya que $B(X) \neq 0$ y $A(X)B(X) = 0$ asociamos a $B(X)$ un k-autómata celular lineal $(\mathbb{Z}_N^{\mathbb{Z}}, T)$, $T \neq 0$ tal que $F \circ T = 0$. Nótese que por ser T lineal, $T(S) \subset S$. Además, como $T \neq 0$, sabemos que existe una regla local φ_j tal que alguno de sus coeficientes es no nulo módulo N, denótese tal coeficiente por α_i^j. Observemos que al definir la configuración $C \in \mathbb{Z}_N^{\mathbb{Z}}$ como sigue

$$c(n) = \begin{cases} 1 & \text{si} \quad n = i + j \\ 0 & \text{si} \quad n \neq i + j \end{cases},$$

tenemos que $C \in S$ y $T(C)(j) = \sum_{u=-r}^{r} \alpha_u^j C(u+j) = \alpha_i^j \neq 0$, pero esto contradice la inyectividad de F en S.

Recíprocamente, consideremos ahora $B(X) \neq 0$ de orden $k \times k$, tal que $A(X)B(X) \neq 0$. Nótese que para demostrar la sobreyectidad de F con está última suposición, es suficiente mostrar que F es inyectivo sobre S.

Sea $C \in S$ una configuración no nula, claramente por definición 3.1 la serie de Laurent $C(X)$ asociada a C es un polinomio de Laurent no nulo; así, cada serie de Laurent $C_i(X)$ con $i = 0, \ldots, k-1$ es un polinomio de Laurent, denotemos cada polinomio por $Q_i(X)$.

Cabe destacar que estos últimos polinomios nos permite definir una matriz $B(X)$ de orden $k \times k$ con entradas $P_{ij}(X)$ dadas por

$$P_{ij}(X) = \begin{cases} Q_i(X) & \text{si} \quad i \in \{0, \ldots, k-1\} \text{ y } j = 0 \\ 0 & \text{si} \quad j > 0 \end{cases}.$$

Ahora bien, denótese por $H_{ij}(X)$ las entradas de la matriz $A(X)$, entonces las entradas de la matriz $A(X)B(X)$ estan dadas por

$$M_{ij}(X) = \begin{cases} \sum_{s=0}^{k-1} H_{is}(X)P_{sj}(X) & \text{si} \quad i \in \{0, \ldots, k-1\} \text{ y } j = 0 \\ 0 & \text{si} \quad j > 0 \end{cases}, \tag{3.16}$$

pero $A(X)B(X) \neq 0$; luego, si $j = 0$, existe $i \in \{0, \ldots, k-1\}$ tal que $M_{ij}(X) \neq 0$.

Por otro lado, al realizar el producto $A(X)C(X)$, obtenemos una matriz columna cuyas entradas son $N_{i0}(X) = M_{i0}(X)$, para cada $i = 0, \ldots, k-1$. Luego, por (3.16) tenemos que $A(X)C(X) \neq 0$; así, $F(C) \neq 0$ y por lo tanto F es inyectivo sobre S. $\square$

Observación 3.2. Es conocido de la teoría de autómatas celulares lineales, ver [18], que si H es un autómata celular lineal y $P(X)$ es el polinomio de Laurent como el indicado en (3.1), entonces $P(X)$ es invertible si, y sólo si, $P(X)$ es inyectivo y $P(X)$ no es divisor de cero si, y sólo si, $P(X)$ es sobreyectivo.

Teorema 3.6. *(Kari [19]). Sea F un k-autómata celular lineal, entonces*

1. *F es inyectivo si, y sólo si, $detA(X)$ es inyectivo.*

2. *F es sobreyectivo si, y sólo si, $detA(X)$ es sobreyectivo.*

Donde $A(X)$ es la matriz asociada a F como lo indica (3.8) y $detA(X)$ representa un autómata celular lineal.

Demostración: Comencemos demostrando 1.

Note que por el teorema 3.5, F es inyectivo si, y sólo si, $A(X)$ es invertible, ahora por el teorema 1.1 tenemos que, $A(X)$ es invertible si, y sólo si, $detA(X)$ es invertible.

Luego, por la observación 3.2, $detA(X)$ es invertible si, y sólo si, $detA(X)$ es inyectivo. Por lo tanto, F es inyectivo si, y sólo si, $detA(X)$ es inyectivo.

Demostremos ahora 2.

Observe que F es sobreyectivo si, y sólo si, $A(X)$ no es un divisor de cero, ver teorema 3.5. Así, por el teorema 1.1, $A(X)$ no es divisor de cero si, y sólo si, $detA(X)$ no es divisor de cero.

Por otro lado, por la observación 3.2, $detA(X)$ no es divisor de cero si, y sólo si, $detA(X)$ es sobreyectivo.

Por lo tanto, F es sobreyectivo si, y sólo si, $detA(X)$ es sobreyectivo.

$\square$

Observación 3.3. Destacamos que los teoremas 3.1 y 3.6 nos propocionan un criterio para estudiar la inyectividad y sobreyectividad de los k-autómatas celulares lineales en terminos de los coeficientes de las reglas locales que los generan; más precisamente, dado un k-autómata celular lineal y $A(X)$ su matriz asociada como lo indica (3.8). Estudiar la inyectividad y sobreyectividad de tal k-autómata celular se reduce a estudiar la inyectividad y sobreyectividad del autómata celular lineal $detA(X)$ usando las caracterizaciones vistas en el teorema 3.1.

4 Caracterización de la equicontinuidad de los k-autómatas celulares lineales

En este capítulo se estudia la propiedad dinámica de equicontinuidad, en el contexto de k-autómatas celulares lineales sobre $\mathbb{Z}_N$.

Comencemos recordando que los autómatas celulares equicontinuos se conocen como transformaciones eventualmente periódicas; es decir, si $(\mathcal{A}^{\mathbb{Z}}, F)$ es un autómata celular, entonces F es equicontinuo si y sólo si, existen $m, n \in \mathbb{Z}$; $m > 0$ y $n \geq 0$ tales que $F^{m+n}(x) = F^n(x)$ para cada $x \in \mathcal{A}^{\mathbb{Z}}$, ver [22].

En el caso de los autómatas celulares lineales equicontinuos sobre $\mathbb{Z}_N$, es bien conocido que G. Manzini y L. Margara caracterizaron la equicontinuidad de tales autómatas celulares lineales en términos de los coeficientes de las reglas locales aditivas que los generan; esto es, si $(\mathbb{Z}^{\mathbb{Z}}, F)$ es un autómata celular generado por la regla local aditiva, $\varphi(x_1, \ldots, x_s) = \sum_{i=1}^{s} b_i x_i$ con $b_i \in \mathbb{Z}_N$, entonces F es equicontinuo si y sólo si, cada factor primo de N divide el máximo cómun divisor de los siguientes coeficientes de φ, $b_2, \ldots, b_s$. Ver [25].

Acá se presenta una caracterización de los k-autómatas celulares lineales equicontinuos sobre el anillo $\mathbb{Z}_N$, en términos de los coeficientes de las k reglas locales que los generan.

4.1. Equicontinuidad

Iniciemos esta sección recordando primeramente que un k-autómata celular equicontinuo $(\mathcal{A}^{\mathbb{Z}}, F)$ es una transformación eventualmente periódica, este último resultado lo garantiza nuestro próximo teorema.

Teorema 4.1. *(N. Romero [30]). Si* $(\mathcal{A}^{\mathbb{Z}}, F)$ *es un* k*-autómata celular, entonces* F *es equicontinuo si y sólo si, existen* $m, n \in \mathbb{Z}$*;* $m > 0$ *y* $n \geq 0$ *tales que* $F^{m+n}(x) = F^n(x)$ *para cada* $x \in \mathcal{A}^{\mathbb{Z}}$*.*

Sea $(\mathcal{A}^{\mathbb{Z}}, F)$ un k-autómata celular lineal de radio r; es decir, generado por reglas locales de la forma $\varphi_i(x_{-r}, \ldots, x_r) = \sum_{j=-r}^{r} \alpha_j^i x_j$ módulo N, donde $\alpha_j^i \in \mathbb{Z}_N$ para cada $i \in \{0, \ldots, k-1\}$ y cada $j \in \{-r, \ldots, r\}$.

Ahora bien, para cada $\hat{n} \geq 1$ y $p \in \mathbb{Z}$ tal que $\mid p \mid \leqslant \hat{n}r$, denotemos por $I_{\hat{n}}(p)$ al conjunto

$$I_{\hat{n}}(p) = \{(i_1, \ldots, i_{\hat{n}}) : \sum_{j=1}^{\hat{n}} i_j = p\},$$

donde $i_j \in \{-r, \ldots, r\}$ para cada j entre 1 y $\hat{n}$.

Afirmamos que, para todo $x \in \mathbb{Z}_N^{\mathbb{Z}}$, $l \in \mathbb{Z}$ y $\hat{n} \geq 1$, se cumple

$$F^{\hat{n}}(x)(l) = \sum_{p=-\hat{n}r}^{\hat{n}r} \Big(\sum_{(i_1, \cdots, i_{\hat{n}}) \in I_{\hat{n}}(p)} \alpha_{i_1}^{l_k} \alpha_{i_2}^{(l+i_1)_k} \cdots \alpha_{i_{\hat{n}}}^{(l+\sum_{j=1}^{\hat{n}-1} i_j)_k} \Big) x(l+p). \tag{4.1}$$

En efecto, para $\hat{n} = 1$; $F(x)(l) = \sum_{i=-r}^{r} \alpha_i^{l_k} x(m+i)$.

Para estudiar el caso $\hat{n} = 2$, recordemos que $F^2(x)(l) = F(F(x))(l)$; es decir,

$$\begin{aligned} F^2(x)(l) &= \textstyle\sum_{i=-r}^{r} \alpha_i^{l_k} F(x)(l+i) \\ &= \textstyle\sum_{i=-r}^{r} \sum_{j=-r}^{r} \alpha_i^{l_k} \alpha_j^{(l+i)_k} x(l+i+j). \end{aligned} \tag{4.2}$$

Por otra parte, sabemos que F^2 es un k-autómata celular lineal de radio $2r$; así, para cada p tal que $\mid p \mid \leq 2r$, reagrupando las sumas en (4.2) tal que los subíndices i, j sumen p, tenemos la siguiente suma $(\sum_{i+j=p} \alpha_i^{l_k} \alpha_i^{(l+i)_k}) x(l+p)$. Luego,

$$F^2(x)(l) = \sum_{p=-2r}^{2r} \Big(\sum_{i+j=p} \alpha_i^{l_k} \alpha_i^{(l+i)_k} \Big) x(l+p).$$

Supongamos ahora que (4.1) es cierto para el entero positivo $\hat{n}-1$; esto es,

$$F^{\hat{n}-1}(x)(l) = \sum_{p=-(\hat{n}-1)r}^{p=(\hat{n}-1)r} \Big(\sum_{(i_1,\cdots,i_{\hat{n}-1})\in I_{\hat{n}-1}(p)} \alpha_{i_1}^{l_k} \alpha_{i_2}^{(l+i_1)_k} \cdots \alpha_{i_{\hat{n}-1}}^{(l+\sum_{j=1}^{\hat{n}-2} i_j)_k} \Big) x(l+p) \quad (4.3)$$

Deseamos demostrar que (4.1) es cierto para el entero positivo $\hat{n}$, recordando que $F^{\hat{n}}(x)(l) = F(F^{\hat{n}-1})(x)(l)$ tenemos

$$F^{\hat{n}}(x)(l) = \sum_{i=-r}^{r} \alpha_i^{l_k} F^{\hat{n}-1}(x)(l+i)$$

Luego, por hipótesis inductiva (4.3), $F^{\hat{n}}(x)(l)$ es

$$\sum_{i=-r}^{r} \alpha_i^{l_k} \sum_{p=-(\hat{n}-1)r}^{p=(\hat{n}-1)r} \Big(\sum_{(i_1,\cdots,i_{\hat{n}-1})\in I_{\hat{n}-1}(p)} \alpha_{i_1}^{(l+i)_k} \alpha_{i_2}^{(l+i_1+i)_k} \cdots \alpha_{i_{\hat{n}-1}}^{(l+\sum_{j=1}^{\hat{n}-2} i_j+i)_k} \Big) x(l+p) \quad (4.4)$$

Es notorio que $F^{\hat{n}}$ es un k-autómata celular lineal de radio $\hat{n}r$; así, para cada $\hat{p}$ con $\mid \hat{p} \mid \leq \hat{n}r$, si reagrupamos las sumas en (4.4) tal que los indices p, i sumen $\hat{p}$, entonces

$$\Big(\sum_{(i_1,\cdots,i_{\hat{n}-1},i)\in I_{\hat{n}(\hat{p})}} \alpha_i^{l_k} \alpha_{i_1}^{(l+i)_k} \alpha_{i_2}^{(l+i_1+i)_k} \cdots \alpha_{i_{\hat{n}-1}}^{(l+\sum_{j=1}^{\hat{n}-2} i_j+i)_k} \Big) x(l+p+i),$$

del cual se deduce

$$F^{\hat{n}}(x)(l) = \sum_{p=-\hat{n}r}^{\hat{n}r} \Big(\sum_{(i_1,\cdots,i_{\hat{n}-1},i)\in I_{\hat{n}(\hat{p})}} \alpha_i^{l_k} \alpha_{i_1}^{(l+i)_k} \alpha_{i_2}^{(l+i_1+i)_k} \cdots \alpha_{i_{\hat{n}-1}}^{(l+\sum_{j=1}^{\hat{n}-2} i_j+i)_k} \Big) x(l+\hat{p}),$$

por lo tanto la relación 4.1 es cierta para cada $n \geq 1$.

En lo que sigue, para cada $\hat{n} \geq 1$, $l \in \mathbb{Z}$ y $p \in \mathbb{Z}$ tal que $\mid p \mid \leqslant \hat{n}r$, denotemos por $\omega(\hat{n}, l, p)$ la siguiente suma módulo N,

$$\omega(\hat{n}, l, p) = \sum_{(i_1,\ldots,i_{\hat{n}})\in I_{\hat{n}}(p)} \alpha_{i_1}^{l_k} \alpha_{i_2}^{(l+i_1)_k} \cdots \alpha_{i_{\hat{n}}}^{(l+\sum_{j=1}^{\hat{n}-1} i_j)_k}. \quad (4.5)$$

Note que, para $x \in \mathbb{Z}_N^{\mathbb{Z}}$, $l \in \mathbb{Z}$ y $\hat{n} \geq 1$, podemos reescribir $F^{\hat{n}}(x)(l)$ en terminos de (4.5) como sigue

$$F^{\hat{n}}(x)(l) = \sum_{p=-\hat{n}r}^{\hat{n}r} \omega(\hat{n}, l, p)x(l+p). \tag{4.6}$$

En nuestro próximo teorema caracterizamos la propiedad dinámica de equicontinuidad en el contexto de los k-autómatas celulares lineales sobre el anillo $\mathbb{Z}_N$.

Teorema 4.2. *Sea $(F, \mathbb{Z}_N^{\mathbb{Z}})$ un k-autómata celular lineal de radio r, entonces F es equicontinuo si, y sólo si, existen $a, b \in \mathbb{Z}$, con $a > b \geq 0$ tales que para cada $s = 0, \cdots, k-1$, y cada $p \in \mathbb{Z}$ con $\mid p \mid \leq ar$ se cumplen las condiciones:*

1. *N divide $\omega(a, s, p)$ cuando $\mid p \mid > br$.*

2. *$\omega(a, s, p) = \omega(b, s, p)$ cuando $\mid p \mid \leqslant br$.*

Demostración: Supongamos F equicontinuo, entonces por el teorema 4.1, existen $m, n \in \mathbb{Z}$; $m > 0$ y $n \geq 0$ tales que $F^{m+n}(x) = F^n(x)$ para cada $x \in \mathcal{A}^{\mathbb{Z}}$. Si consideramos $a = m + n$ y $b = n$, por la caracterización de equicontinuidad tenemos particularmente

$$F^a(x)_{[0,k-1]} = F^b(x)_{[0,k-1]}. \tag{4.7}$$

Sean $s \in \{0, \cdots, k-1\}$ y $\hat{p} \in \mathbb{Z}$ con $\mid \hat{p} \mid \leq ar$. Obsérvese que definiendo la configuración $x \in \mathcal{A}^{\mathbb{Z}}$ por

$$x(i) = \begin{cases} 1 & si \quad i = \hat{p} + s \\ 0 & si \quad i \neq \hat{p} + s, \end{cases} \tag{4.8}$$

tenemos que, para cada $p \neq \hat{p}$

$$\omega(a, s, p)x(s+p) = \omega(b, s, p)x(s+p) = 0. \tag{4.9}$$

Por otra parte, (4.8) y (4.9) implican que

$$\begin{aligned} F^a(x)(s) &= \textstyle\sum_{p=-ar}^{ar} \omega(a,s,p)x(s+p) \\ &= \omega(a,s,\hat{p})x(s+\hat{p}) \\ &= \omega(a,s,\hat{p})1 \\ &= \omega(a,s,\hat{p}). \end{aligned} \tag{4.10}$$

Ahora bien, cuando $\mid \hat{p} \mid > br$ para cada $\mid p \mid \leq br$ se cumple, $p \neq \hat{p}$. Luego, por (4.9) tenemos

$$F^b(x)(s) \;=\; \textstyle\sum_{p=-br}^{br} \omega(b,s,p)x(s+p) \;=\; 0\ . \tag{4.11}$$

Por lo tanto (4.7), (4.10) y (4.11) implican que $\omega(a,s,\hat{p}) = 0$ módulo N.

Consideremos ahora $\mid \hat{p} \mid \leq br$ y calculemos $F^b(x)(s)$. Sabemos que (4.9) y (4.8) implican que

$$\begin{aligned} F^b(x)(s) &= \textstyle\sum_{p=-br}^{br} \omega(b,s,p)x(s+p) \\ &= \omega(b,s,\hat{p})x(s+\hat{p}) \\ &= \omega(b,s,\hat{p})1 \\ &= \omega(b,s,\hat{p}). \end{aligned} \tag{4.12}$$

Luego, por (4.7), (4.10) y (4.12) tenemos $\omega(a,s,\hat{p}) = \omega(b,s,\hat{p})$, de esta forma las condiciones 1 y 2 quedan demostradas.

Supongamos ahora que, existen $a, b \in \mathbb{Z}$, con $a > b \geq 0$ tales que para cada $s = 0, \cdots, k-1$, y cada $p \in \mathbb{Z}$ con $\mid p \mid \leq ar$ se cumplen:

1. N divide $\omega(a,s,p)$ cuando $\mid p \mid > br$.

2. $\omega(a,s,p) = \omega(b,s,p)$ cuando $\mid p \mid \leqslant br$.

Sea $x \in \mathcal{A}^{\mathbb{Z}}$ una configuración cualquiera; para cada $w \in \mathbb{Z}$ sucede que

$$F^a(x)(w) = \sum_{p=-ar}^{ar} \omega(a,w,p)x(w+p).$$

Es claro que para cada $w \in \mathbb{Z}$, existe $s \in [0, k-1]$ tal que $w = s$ módulo k; así, $\omega(a, w, p) = \omega(a, s, p)$ y por lo tanto,

$$F^a(x)(w) = \sum_{p=-ar}^{ar} \omega(a, s, p)x(w + p). \tag{4.13}$$

Por otra parte, la condición 1 implica que para cada p tal que $\mid p \mid > br$, $\omega(a, s, p) = 0$, módulo N. Luego, la suma en (4.13) es

$$F^a(x)(w) = \sum_{p=-br}^{br} \omega(a, s, p)x(w + p), \tag{4.14}$$

pero de la condición 2 , para cada p tal que $\mid p \mid \leqslant br$ tenemos que $\omega(a, s, p) = \omega(b, s, p)$. Por lo tanto,

$$F^a(x)(w) = \sum_{p=-br}^{br} \omega(b, s, p)x(w + p) = F^b(x)(w). \tag{4.15}$$

Ahora como $a > b$ y $b \geq 0$, existe $l > 0$ tal que $a = b + l$ y puesto que (4.15) se cumple para cada $x \in \mathcal{A}^{\mathbb{Z}}$ y $m \in \mathbb{Z}$, deducimos que F es equicontinuo. $\square$

Bibliografía

[1] ARCAYA, I. *Sobre transformaciones que preservan potencias del shift.* Tesis de Grado de Maestría. UCV. (2008).

[2] ARCAYA, I. AND N. ROMERO. *On a Hedlund's Theorem and place-dependent cellular automata.* Publicado en Divulgaciones Matemáticas 15, 81-92 (2007).

[3] ARCAYA, I. AND N. ROMERO. *Surjective Linear Multiband Cellular Automata and Smith's Normal Form.* Editado en Publicaciones de Ciencias y Tecnología. UCLA (2010).

[4] BLANCHARD, F., CERVELLE J. AND FORMENTI, E. *Some results about the chaotic behavior of cellular automata.* Theoretical Computer Science, **349** (2005) 318–336.

[5] BLANCHARD, F., FORMENTI E. AND KŮRKA, *P. Cellular Automata in the Cantor, Besicovitch and Weyl topological spaces.* Complex Systems, **11(2)** (1999) 107–123.

[6] BANKS, J., BROOKS, J., CAIRNS, G., DAVIS, G. AND STACEY, P. *On Devaney's Definition of Chaos.* AMER. MATH. MONTH. **99** (1992) 332-334.

[7] BOYLE, M., KITCHENS, B. *Periodic points for onto cellular automata*, INDAGATIONES MATHEMATICAE-NEW SERIES **10**, (1999) 483-493.

[8] Cattaneo, G., Formenti, E., Manzini, G. and Margara, L. *Ergodicity, transitivity, and regularity for linear cellular automata over $\mathbb{Z}_m$.* Theoret. Comput. Sci. **233**, (2000) 147–164.

[9] Cattaneo, G., Dennunzio A. and Margara, L. *Solution of some conjectures about topological properties of linear cellular automata.* Theoret. Comput. Sci. **325**, (2004) 249–271.

[10] Codenotti, B. and Margara, L. *Transitive cellular automata are sensitive.* Amer. Math. Monthly **103**, (1996) 58–62.

[11] D'amico, M., Manzini, G. and Margara, L. *On computing the entropy for cellular automata.* Theoret. Comput. Sci. **290**, (2003) 1629–1646.

[12] Devaney, R. *An Introduction to Chaotic Dynamical Systems.* Addison-Wesley, New York. (1989).

[13] Epstein, I. R. *Spiral Waves in Chemistry and Biology. Science* **252**, (1991).

[14] Ermentrout, G. B. and Keshet, L. E. *Cellular Automata Approaches to Biological Modeling.* Journal Theoretical Biology **160**, (1993) 97–133.

[15] Favati, P. Lotti, G. and Margara, L. *Additive one-dimensional Cellular Automata are chaotic according to Devaney's definition of Chaos.* Theoret. Comput. Sci. **174**, (1997) 157–170.

[16] Formenti, E. *On the sensitivity of additive cellular automata in Besicovitch topologies.* Theoretical Computer Science, **301** (2003) 341–354.

[17] HEDLUND, .G. *Endomorphisms of the shift dynamical systems.* MATH. SYS. TH. **3**, (1969) 320–375.

[18] ITÔ, M. ÔSATO, N. AND NASU, M. *Linear Cellular Automata over* $\mathbb{Z}_m$. JOURNAL OF COMPUTER AND SYSTEM SCIENCES **27**, (1983) 125–140.

[19] KARI, J. *Linear Cellular Automata with Multiple State Variable.* LECTURE NOTES IN COMPUTER SCIENCE **1770**. PROCEEDINGS OF THE 17TH ANNUAL SYMPOSIUM ON THEORETICAL ASPECTS OF COMPUTER SCIENCE. (2000) 110 – 121.

[20] KOHRING, G. A. *An efficient Hydrodynamic Cellular Automata for Simulating Fluids with Large Viscosity.* JOURNAL OF STATISTICAL PHYSICS **66**, (1992) 1177–1184.

[21] KOLYADA S. AND SNOHA L. *Some aspects of topological transitivity.* A SURVEY. PREPRINT. WWW.MATH.SLU.CZ/KONFERENCE/ECIT/PDF/003-035.PDF.

[22] KŮRKA, P. *Topological dynamics of cellular automata. Codes, Systems and Graphical Model (Brian Marcus and Joachim Rosental, eds.)* THE IMA VOLUMEN IN MATHEMATICS AND APPLICATIONS; VOL. **123**. SPRINGER-VERLAG (2000) 417-433. SOCIÉTÉ MATHÉMATIQUE DE FRANCE (2003).

[23] MANZINI, G. AND MARGARA, L. *Invertible Linear Cellular Automata over* $\mathbb{Z}_m$*: Algorithmic and Dynamical Aspects.* JOURNAL OF COMPUTERS AND SYSTEMS SCIENCES **56**, (1998) 60–67.

[24] Manzini, G. and Margara, L. *Attractors in Linear Cellular Automata.* Journal of Computers and Systems Sciences **58**, (1999) 597–610.

[25] Manzini, G. and Margara, L. *A complete and efficiently computable topological classification of D-dimensional linear cellular automata over* $\mathbb{Z}_m$. Theoretical Computer Science **221**, (1999) 157–177.

[26] Mass, A., Martínez, S., Pivato, M. and Yassawi, R. *Attractiveness of the Haar measure for linear cellular automata on Markov subgroups.* IMS Lecture Notes-Monograph Series. Dynamics & Stochastics. **48**, (2006) 100–108.

[27] McCoy, N. H. *Rings and ideals*, Carus Monograph Series, no. 8, Open Court, LaSalle, Ill., 1948. MR 10, 96.

[28] Munkres, J. R. , *Topology a first course*, Prentice-Hall, Inc. Englewood Cliffs, New Jersey, (1975).

[29] Romero, N. *Comentarios sobre la definición de Autómatas Celulares.* Boletín de la AMV **X(1)**, (2003) 59–77.

[30] Romero, N. *Dinámica Topológica y Autómatas Celulares.* Monografias del Postgrado de Matemáticas de la Facultad de Ciencias, UCV. (2006).

[31] Romero, N., Rovella, A, and Villamajó, F. *Remark on cellular automata and shift preserving maps.* Applied Mathematics Letters. 19, 576-580 (2006).

[32] Silva, J. *Formalismo matemático de los autómatas celulares según G. A. Hedlund.* Trabajo Especial de Grado. Universidad Centroccidental Lisandro Alvarado (2008).

[33] Wolfram, S. *Computation Theory of Cellular Automata.* Commun. Math. Phys. **96**, (1984) 15–57.