Descripción y Aplicaciones de los Autómatas Celulares

David Alejandro Reyes Gómez
Lic. en Matemáticas Aplicadas y Computación
FES Acatlán, U. N. A. M.

Verano de Investigación 2011
Departamento de Aplicación de Microcomputadoras
Universidad Autónoma de Puebla

email: dargmandeurantia@hotmail.com

25 de Agosto del 2011

Resumen

Se presenta en este articulo una breve explicación de los autómatas celulares, sus características y elementos que lo componen, así como su aplicación en diversas áreas de estudio, destacando su uso como un sistema dinámico con una enorme adaptabilidad. Se dará el marco teórico general y la problemática del área, así como un ejemplo que ilustre su función. Se pretende estimular al lector, con o sin conocimientos previos del tema, a interesarse y difundir el tema, y esperando exista un progreso futuro en esta área de investigación

Índice

1. Introducción

Para los matemáticos es fundamental el utilizar y desarrollar herramientas, que expliquen los fenómenos que nos rodean. Esto se logra, generalmente, a través de modelos matemáticos que den respuesta a dichos fenómenos. Así, se puede señalar el gran avance adquirido en el estudio del caos([1]) y de los sistemas dinámicos ([2]), en este ultimo destaca el de los autómatas celulares.

Por otro lado, la computación puede verse como la transformación de la información, donde al inicio de este proceso siempre hay condiciones iniciales. Sin embargo, hay procesos de cómputo donde nuevas entradas de información pueden darse durante el proceso mismo. Esta información nueva a veces determina el resultado del proceso, lo que implica un enfoque distinto para estudiar la computación, donde el sistema sea capaz de cambiar de comportamiento ante cualquier perturbación, incorporando información nueva durante el proceso.

Para auxiliar a ambos enfoques, es de mucha ayuda el estudio y simulación de sistemas dinámicos, evitando las desventajas existentes en la matemática clásica para expresar la complejidad de estos sistemas. Es por eso que se recurre a un método de modelización conocido como autómatas celulares.

Ciertos autómatas celulares son universales, es decir son capaces de representar cualquier algoritmo. Estos son maquinas abstractas capaces de construir nuevos autómatas que a su vez pueden generar otros. En otras palabras, son capaces de procesar cualquier cosa computable. Ahora ¿hay cosas incomputables?. Esta es una pregunta difícil, y es por eso que los autómatas universales son las maquinas abstractas - concepto general de computadoramas potentes que se conocen.

2. Autómatas Celulares

Los autómatas celulares(AC) surgen en la década de 1940 con John Von Neumann, que intentaba modelar una maquina que fuera capaz de autoreplicarse, llegando así a un modelo matemático de dicha maquina con reglas complicadas sobre una red rectangular. Inicialmente fueron interpretados como conjunto de células que crecían, se reproducían y morían a medida que pasaba el tiempo. A esta similitud con el crecimiento de las células se le debe

su nombre.

Un autómata celular es un modelo matemático para un sistema dinámico, compuesto por un conjunto de celdas o células que adquieren distintos estados o valores. Estos estados son alterados de un instante a otro en unidades de tiempo discreto, es decir, que se puede cuantificar con valores enteros a intervalos regulares. De esta manera este conjunto de células logran una evolución según una determinada expresión matemática, que es sensible a los estados de las células vecinas, la cual se le conoce como *regla de transición local.*

El aspecto que mas caracteriza a los AC es su capacidad de lograr una serie de propiedades que surgen de la propia dinámica local a través del paso del tiempo y no desde un inicio, aplicándose a todo el sistema en general. Por lo tanto no es fácil analizar las propiedades globales de un AC desde su comienzo, complejo por naturaleza, a no ser por vía de la simulación, partiendo de un estado o configuración inicial de células y cambiando en cada instante los estados de todas ellas de forma síncrona.

2.1. Elementos de un Autómata Celular

La definición de un AC requiere mencionar sus elementos básicos:

- **Arreglo Regular.** Ya sea un plano de 2 dimensiones o un espacio n-dimensional, este es el espacio de evoluciones, y cada división homogénea de arreglo es llamada célula.
- **Conjunto de Estados.** Es finito y cada elemento o célula del arreglo toma un valor de este conjunto de estados. También se denomina *alfabeto.* Puede ser expresado en valores o colores.
- **Configuración Inicial.** Consiste en asignar un estado a cada una de las células del espacio de evolución inicial del sistema
- **Vecindades.** Define el conjunto contiguo de células y posición relativa respecto a cada una de ellas. A cada vecindad diferente corresponde un elemento del conjunto de estados
- **Función Local.** Es la regla de evolución que determina el comportamiento del AC. Se conforma de una célula central y sus vecindades. Define como debe cambiar de estado cada célula dependiendo de los estados anteriores de sus vecindades. Puede ser una expresión algebraica

o un grupo de ecuaciones. Para un estudio mas completo véase [3].

Adicionalmente para poder entender mejor su representación visual, se requiere mencionar los tipos de limites o fronteras, del plano en el cual se desarrolla, en los cuales se clasifica:

(a). *Frontera Abierta.* Se considera que todas las células fuera del espacio del autómata toman un valor fijo.

(b). *Frontera Reflectora.* Las células fuera del espacio del autómata toman los valores que están dentro, como si se tratara de un espejo.

(c). *Frontera Periódica o Circular.* las células que están en la frontera interaccionan con sus vecinos inmediatos y con las células que están en el extremo opuesto del arreglo, como si dobláramos el plano a manera de cilindro.

(d). *Sin Frontera.* La representación de autómata no tiene limites, es infinito. Esto solo es practico cuando se cuenta con un software que simule la evolución del autómata.

Es importante destacar la complejidad que se logra con un AC. De acuerdo a la dimensión en la que se genere (linea, plano,espacio,etc.) tendrá un numero potencial de vecinos. Por ejemplo, digamos que la vecindad sera de 1, estos es solo las células inmediatas o mas cercanas serán tomadas en cuenta. Para el caso de una sola dimensión cada célula tendrá solo 2 vecinos. Para un AC en dos dimensiones contara con 4 (arriba, abajo, izquierda, derecha) u 8 vecinas si tomamos en cuenta también las diagonales. Y en el caso de un AC en 3D llegara a tener hasta 26 vecinos cada célula.

Como el siguiente estado de cada célula se computa en base al estado anterior y de sus vecinas (es decir que el estado 2 surge del estado 1 y el 3 del 2,etc.), se tiene un sistema que es dinámico y con un comportamiento muy difícil de predecir.

Algunos ejemplos de AC:

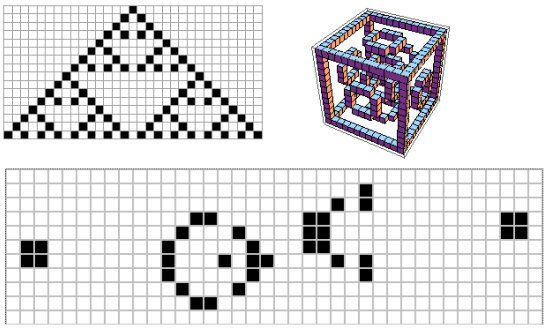

Figura 1: Regla 90 de Wolfram (arriba izq.), AC en 3 dimensiones (arriba derecha) y *Game of life* de John Conway (abajo).

3. Aplicaciones de los Autómatas Celulares

Los autómatas celulares han sido utilizados con éxito en distintas disciplinas. Por ejemplo, en Física es una de las técnicas mas interesantes para simular fenómenos concretos en dinámica de fluidos. En el estudio de los sistemas complejos en Biología, los AC representan desde mediados de los 80 una seria alternativa a la modelización con ecuaciones diferenciales. En 1986 Wolfram publica la obra *Teoria y Aplicación de los Autómatas Celulares*, promoviendo el interés por esta técnica de modelización y simulación. En ese mismo año Langton propone la utilización de los AC como técnica principal para el estudio de la vida artificial. Uno de los factores que mas a contribuido a su uso es la sencillez con que se pueden realizar simulaciones. A finales de los años 90 el uso de los AC abarcan numerosas disciplinas, siendo de gran utilidad en el estudio de sistemas biológicos: reproducción, auto-organización, evolución, etc. En Química se utiliza para el estudio cinético de las reacciones y en la simulación del crecimiento de los cristales. Una de las aplicaciones mas interesantes hoy en día, es en las Ciencias de la Computación, donde los AC han permitido a los investigadores construir modelos con los que estudiar fácilmente el procesamiento de información en paralelo así como el diseño de computadoras cuya arquitectura sea basada en principios y materiales biológicos.

Hay evidencia de su uso en: simulación de evacuación de barcos y salas de cines, estudio de mercados y efectos de la publicidad, diversión y arte,

desarrollo de órganos, distribución de poblaciones, germinación vegetal, ciclos climaticos e incluso hay teorías que cohesionan la mecánica newtoniana con la relativista y la cuántica haciendo uso de los AC. Dicen algunos autores de que hay posibilidad de nuestro universo sea parecido a un gigantesco autómata celular, siendo los objetos y nosotros mismos fluctuaciones de información binaria codificándose a cada instante, forjando futuros exactos, ya contados desde hace tiempo.

Ahora se mostraran algunos ejemplos de como funciona un AC en diversas áreas.

3.1. Arquitectura

La conexión que se hace con la arquitectura, es la capacidad de los AC de generar patrones o modelos y, de una forma organizada, estos modelos nos pueden sugerir formas arquitectónicas. Sabemos que un AC difiere de los modelos deterministas en que los resultados obtenidos son la base para el siguiente grupo de resultados. El método de sustitución recursivo continua hasta que llegamos a una configuración final. Muchos métodos digitales en arquitectura han tenido un acercamiento del tipo paramétrico ([4] y [5]), donde un grupo inicial de parámetros se usan para llegar a un solo resultado. Si se desea un resultado distinto, los parámetros necesitan ser modificados y el método se repite. La diferencia esta entonces, en que los resultados de los métodos paramétricos pueden ser fácilmente anticipados, mientras que en los métodos recursivos de un autómata usualmente no tarea sencilla. Esto ofrece una interesante y rica plataforma donde desarrollar modelos arquitectónico.

Siendo el espacio de 3 dimensiones el que mas interesa al tema, digamos que el AC consiste en una red infinita de células. Cada célula tiene un estado especifico, ocupado o vacío, representado por una marca o símbolo para ubicar su posición. El proceso inicia con un estado inicial de células ocupadas y siguiendo un grupo de reglas para el siguiente paso o generación. Las reglas determinan que célula vivirá, morirá o nacerá en la siguiente generación y ocupan la vecindad de cada una de ellas para determinar su futuro.

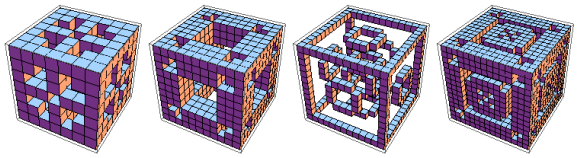

Figura 2: Algunos ejemplos de AC en 3 dimensiones.

El llevar un AC desde su forma matemática pura hacia una forma arquitectónica significa una serie obstáculos que harían imposible su construcción en la realidad. Primero tenemos que establecer un limite a su evolución a nivel del piso, creciendo únicamente hacia arriba y a los lados, y no por debajo.

Una revisión inicial mostrara los siguientes problemas: algunas células no estarán conectadas horizontalmente con otras y algunas no tendrán soporte vertical. También las células no muestran una escala arquitectónica ni sugieren algún espacio interior como se muestra en la figura 3.

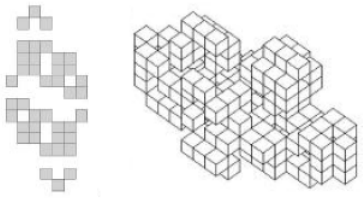

Figura 3

El centro de cada célula sera la base de nuestro desarrollo. En la configuración de la figura anterior, las células están únicamente una junto a la otra, cubriendo la mayor área de suelo posible. ¿Que pasaría si traslapamos ligeramente una célula con otra?. Acercando los centros de cada célula uno con otro, las diagonales de cada una se conectan, la naturaleza de los bordes de las células iniciales cambia,crea espacios interiores horizontales entre ellas y una serie de aberturas interesantes comienzan a surgir.

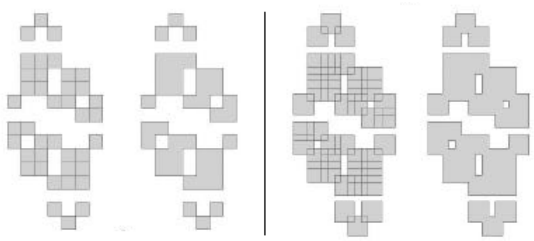

Figura 4: Configuración inicial (izquierda) y con traslape de células (derecha), las cuales cubren una mayor área interior.

Adicionalmente, no solo se puede usar la unidad cuadrada como base para nuestra construcción, sino que hay una variedad de formas a implementar que modificarían la orientación y darían a la construcción de mayores áreas abiertas.

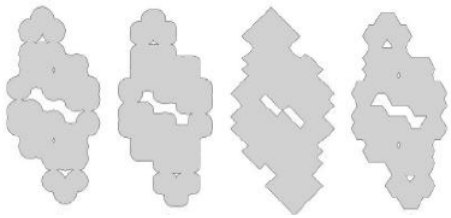

Figura 5: Posibles formas para la base: circular, elipse, rombo y hexágono.

Como mencionamos anteriormente, la configuración inicial carecía de soporte vertical. Esto podría resolverse colocando soportes, ya sea en las esquinas de cada célula o al centro de ellas en la configuración final. Como se muestra abajo, la combinación de estos elementos forma espacios modulares independientes, a los cuales se les puede dividir en varios pisos a la vez, cada uno con formas interiores distintas según su vecindad y las células emergentes.

Figura 6: Formas arquitectónicas básicas que surgen de un AC.

Podemos agregar un par de condiciones extras para darle un aspecto mas interesante a cada construcción. La primera que podemos utilizar es fijar un máximo y un mínimo al tamaño de la célula, y asignarlo a cada una de manera aleatoria . Otro seria establecer que cada célula aumente su tamaño, únicamente si sobrevive de una generación a otra. Este ultimo enfoque considera el proceso de crecimiento real de un AC y lo interpreta directamente.

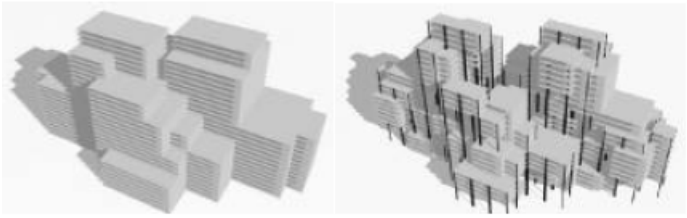

Figura 7: Otras construcciones usando diferentes condiciones.

Aun así hay varios métodos que se están desarrollando, dando posibilidades a futuras investigaciones. La variedad de estos solo están limitados por el uso de las matemáticas para generar nuevos conceptos, en la habilidad de las herramientas para conformarlos, y últimamente por nuestra imaginación. Mas ejemplos en [6] y [7].

Lo mas importante de todo esto es el proceso; usar los datos generados por un AC, encontrar un patrón que nos sirva y saber interpretar y modificar los resultados para su uso en la arquitectura. El objetivo no son esos resultados en si, mas bien lo que se puede aprender e inferir en el proceso de generarlos.

3.2. Bioinformática

La forma y la naturaleza son el conocimiento que heredamos de la arquitectura estructural del cosmos.
– Pier Luigi Nervi

La bioinformática consiste en analizar, comprender y predecir procesos biológicos con la ayuda de herramientas computacionales. Puede ser vista como la disciplina que une dos ciencias: Biología y Computación. Se ha visto impulsada por varios factores:

- El interés creciente en la investigación genómica, donde los conjuntos de información son difíciles de entender sin el uso de herramientas analíticas.
- El avance reciente en las herramientas matemáticas (como la teoría del Caos) que ayudan a comprender mecanismos complejos y no lineales en la Biología.
- Un incremento en los últimos años en la capacidad computacional, que permite hacer cálculos y simulaciones que no eran previamente posibles.

La Bioinformática se divide generalmente en 4 áreas de estudio: Genómica Computacional, Bioinformatica Estructural, Biología de Sistemas y Algoritmos y bases de Datos.

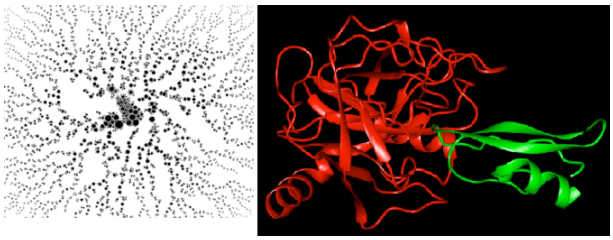

Figura 8: Interacciones entre proteínas, tema común de estudio de la Bioinformática.

La complejidad de los sistemas biológicos no suele, por lo general, conducir a modelos cuya estructura se parezca a una ecuación diferencial ordinaria. Por el contrario, lo habitual es que los sistemas biológicos se comporten de una manera que refleje la auto-organización de sus componentes, manifestando cambios en el tiempo y espacio alejados de la uniformidad. Estos sistemas, por lo tanto, requieren modelos cuya estructura sea expresada por ecuaciones diferenciales en derivadas parciales (EDP). Aunque debemos mencionar que un modelo realista basado en EDP permite reproducir en cantidad y detalle el comportamiento de un sistema, su modelización y simulación presenta algunas dificultades. En primer lugar, los investigadores encuentran inconvenientes al realizar estos modelos, ya sea porque la estructura del sistema no resulta evidente o el fenómeno al cual se refiere se encuentra en proceso de investigación. En segundo lugar, suponiendo que se logran obtener las EDP del sistema, los problemas surgen cuando al momento de obtener soluciones, ya sean analíticas o por métodos numéricos, donde se requiere de

computadoras con gran cantidad de memoria y velocidad de procesamiento. Finalmente resulta difícil hacer que la interpretación del modelo simulado sea aproximado a lo que podemos deducir directamente de la observación de los fenómenos naturales. Por otro lado no es fácil representar gráficamente estos modelos basados en EDP, ya que algunas estructuras biológicas, son resultado de la unión de sub-unidades, como las células o moléculas, haciendo difícil su entendimiento por esta vía y a veces complicándolo aun mas.

Un sistema biológico esta, generalmente, compuesto por varias partes interconectadas o entrelazadas cuyos vínculos contienen información adicional y oculta al observador. Como resultado de las interacciones entre elementos, surgen propiedades nuevas o emergentes que no pueden explicarse a partir de las propiedades de los elementos aislados. La mayoría de los procesos que son objeto de estudio de las ciencias biológicas son emergentes, ya sea porque el proceso esta en fase de estabilización o este reaccionando ante cambios externos que puedan modificar su estructura. Por lo anterior se dice que existe en la naturaleza la *auto-organización.*

Alan Turing trabajo desde 1952 hasta que falleció en la *Biología Matemática* (disciplina que estudia los procesos biológicos utilizando técnicas matemáticas), destacando sus escritos sobre la morfogénesis y la filotaxis, ejemplos clásicos de patrones resultantes en un proceso auto-organizativo en la naturaleza.

Dependiendo de la naturaleza compleja del sistema y de la posibilidad de identificar estados locales y reglas generales de evolución, se podrían simular los fenómenos naturales por medio de un AC, y por lo menos se requiere conocer su comportamiento global. Ejemplos de esto pueden ser: propagación de virus, epidemias y bacterias, comportamiento de glóbulos en el cuerpo, contaminación, evolución galáctica, ecosistemas, genética, etc.

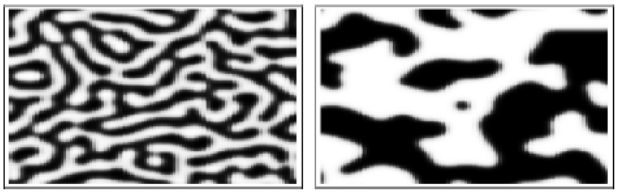

Figura 9: Patrones de Turing,que pueden modelar las manchas en la piel de animales vertebrados como las jirafas, vacas y jaguares.

3.2.1. El Cerebro y los Autómatas Celulares

Como es que el cerebro funciona es una de las preguntas fundamentales de la biología, y ha sido objeto de simulación desde la aparición de las primeras computadoras. Con un peso de apenas 1.5 Kg. es el organo responsable de funciones elementales como caminar o respirar, hasta otras menos sencillas como pensar, aprender o hablar. A pesar de los avances en la investigación de células y moléculas que lo componen, unas cuestiones básicas quedan sin resolver. Una seria por ejemplo como es que se determina la conexión neuronal a nivel genético desde el desarrollo del ser vivo diferenciando el cerebro humano de otras especies, logrando así la capacidad intelectual. Es necesario responder esta y muchas otras preguntas, con un marco teórico y una experimentación adecuados.

La modelización y simulación de las funciones cerebrales se encuentran íntimamente relacionadas con el origen, desarrollo y aplicación del concepto de autómata. La posibilidad de construir una maquina que emulara al cerebro fue lo que dio nacimiento a una de las áreas de investigación de la ciencia mas prometedoras: la inteligencia artificial. Un buen punto de inicio es el AC construido por Von Neumann, capaz de auto-reproducirse, demostrando que con un grupo pequeño de reglas se pueden lograr estructuras muy complejas. Esto muestra un poco la idea de como un órgano como el cerebro puede desarrollarse a partir de poca información genética. También con las observaciones que se han hecho sobre la corteza cerebral, se nota que esta compuesta de una red de neuronas que interactúan a través de impulsos eléctricos, similar al comportamiento de un AC, que resulta de un arreglo simple de elementos. Se han modelado ya redes neuronales artificiales basadas en el concepto de autómata, aunque al principio sin la posibilidad de aprendizaje, una función característica del cerebro humano y animal. En 1952 Ross Ashby publicó el libro titulado *Design for a Brain*, dando la posibilidad años mas tarde de diseñar modelos de redes neuronales con capacidad de aprendizaje. Una de los primeros modelos con esta propiedad fue el *perceptrón*, propuesto en 1962 por Frank Rosenblatt, consiguiendo que la red neuronal aprendiera por medio de la modificación adaptativa de las conexiones entre neuronas. Las redes neuronales artificiales exhiben muchas de las funciones del cerebro siendo capaces de aprender, memorizar conjuntos de patrones, clasificarlos, inferir a que clase pertenece un nuevo objeto a partir de la experiencia acumulada por la red neuronal durante el reconocimiento de otros previos, establecer asociaciones entre objetos, reconocer símbolos, letras, números y mas. El reconocimiento de patrones es su principal aplicación.

La fascinación por los resultados obtenidos ha conducido a que psicólogos y biólogos entre otros especialistas, hayan intentado entender el cerebro humano y animal a partir de los modelos computacionales que representan las redes neuronales artificiales. Quedan todavía por resolver las cuestiones de numero de elementos, escala, modelo, etc. del AC para una correcta aplicación a esta cuestión.

3.3. Autómatas Celulares en el Control de Incendios Forestales

Un incendio forestal es la propagación libre y no programada del fuego sobre la vegetación en los bosques, selvas, zonas áridas y semiáridas. El combustible es el factor principal que determina la magnitud del mismo.

Es importante controlarlos por que se pierden cantidades considerables de suelo, como consecuencia de la devastación y la erosión posterior de viento y lluvias, destruyendo también el hábitat de la fauna silvestre. Se eliminan también las plantas que generan oxigeno, incrementando el efecto invernadero por la emisión excesiva de carbono y otros elementos nocivos al ambiente. Igualmente, se destruyen grandes volúmenes de madera afectando esto directamente sobre la economía.

Los hay de tres tipos según la naturaleza de los combustibles presentes: incendios superficiales, de copa o aéreos y subterráneos. Las causas son variadas, siendo el 99 % de origen humano y solo el 1 % de fenómenos naturales derivados de eventos meteorológicos, como descargas eléctricas o erupciones volcánicas (información obtenida del Centro Nacional para la Prevención de Desastres, `http://www.cenapred.unam.mx/es/`). De acuerdo a su origen pueden ser: accidentales, intencionales, naturales o por negligencia.

La simulación de incendios forestales son de gran utilidad para la planificación y mantenimiento de grandes áreas boscosas, ya sean naturales o artificiales, puesto que permiten conocer de antemano dónde deben de existir zonas para la contención de incendios y contribuye a la toma de decisiones en caso de un evento perjudicial.

En caso de presentarse un incendio es muy importante tener el sistema listo para ingresar la información necesaria: foco del mismo y las condiciones geográficas y meteorológicas al momento del suceso. Se deben obtener resultados fiables y en el menor tiempo posible, para combatir y minimizar el área afectada por el fuego.

En general las áreas forestales ocupan grandes extensiones de terreno y la cantidad de flora y fauna en ellas es elevada, siendo tal vez demasiado grande como para realizar una simulación. Por lo tanto conviene establecer la manera en que esto se realizara.

Primero se define un Autómata Celular bidimensional con reglas especificas de propagación del fuego según la velocidad y dirección del viento, determinando esto también las vecindades de cada célula en la simulación. Es deseable que se incluya la densidad del bosque o conjunto de arboles como un parámetro mas en la concepción del modelo. Es posible incluir características propias de cada árbol, planta o elemento del bosque, proporcionando atributos particulares a cada célula o sub-conjunto de células del autómata celular. Esta posibilidad de crecimiento y precisión compleja del modelo son una ventaja adicional en el empleo del mismo.

3.3.1. Definición y desarrollo del modelo de simulación

El modelo de simulación consiste en un bosque representado por una matriz de N $*$ N posiciones. El estado inicial estará representado en dicha matriz, donde cada célula puede estar vacía u ocupada por un elemento del bosque. Ademas, se debe conocer la posición especifica del fuego en cada instante, así como las condiciones del viento (velocidad, dirección).

La vecindad de cada una de las células variará según la dirección e intensidad o velocidad del viento. Para verlo de manera mas simple, restringimos la velocidad a 3 valores posibles(0,1 y 2) y las direcciones a ocho(Norte, Noreste, Este, Sudeste, Sur, Suroeste, Oeste y Noroeste).

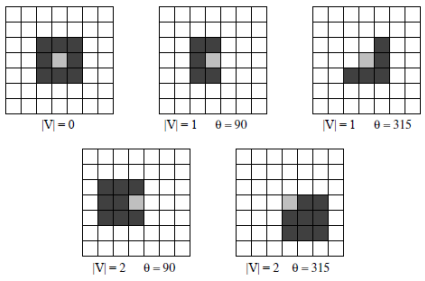

Figura 10: AC que representa las posibles vecindades(negro) de una célula(gris) según las condiciones del viento. |V| es la intensidad del viento y θ la dirección en la que se mueve representada en ángulos.

Para hacer de esto un proceso mas rápido, conviene usar computadoras con procesamiento en paralelo, esto consiste en hacer la ejecución del modelo de forma simultanea desde el mismo programa, pero en diferentes procesadores, así se dividen las instrucciones para reducir el tiempo de ejecución. Aunque esta tecnología requiere de una gran sincronización y comunicación entre los procesadores.

En la Universidad Boliviana de San Pablo ya se han logrado resultados usando este método. Se ha aplicado el modelo a conjuntos de arboles de hasta un millón de elementos con distribuciones aleatorias. Se tomo también la densidad del bosque como un parámetro mas en la concepción del modelo. El origen del fuego se sitúa al azar dentro del conjunto de arboles y se alcanza el estado final cuando ya no existen focos de incendio, ya sea que se han quemado la totalidad de los arboles o cuando el último árbol en combustión queda aislado de los demás, sin permitir que el fuego se propague.

Las pruebas realizadas siguiendo este modelo, muestran que cuando la velocidad del viento es nula, se tienen mayores posibilidades de un incendio devastador, no llegando a sobrevivir ni el 10 % de la población de arboles existentes. Esto es independiente del tamaño del bosque, de su distribución inicial e incluso del foco de origen del incendio.

Sin embargo cuando el viento sopla con velocidad y dirección cambiantes, aunque esos cambios no sean frecuentes ni bruscos, bosques que están densamente habitados pueden incluso salvar un alto porcentaje de su población inicial sin intervención externa, pero dependiendo en este caso del foco de origen del fuego.

Otra conclusión a la que se llego, que coincide con la intuición, es que si el incendio destruye una cantidad reducida de arboles, termina en un lapso reducido y, por el contrario, si alcanza grandes proporciones, demora un tiempo correspondientemente mayor.

Estas observaciones y conclusiones, junto con lo que parece indicar la experiencia, sugieren la validez del modelo y una fácil integración de factores complejos en las ecuaciones y reglas de producción que lo definen. Por ejemplo se pueden incluir distintas especies para poblar el bosque incrementado el numero de estados para cada célula y las reglas de transición entre ellas. Arboles con maderas resistentes al fuego, pueden simularse a través de células para las cuales la transición entre el estado inicial y el de calcinado, dure mas de un intervalo de tiempo en la simulación. De esta manera, el árbol permanece vivo mas tiempo, pero su capacidad de pasar fuego a los

vecinos también perdura un lapso mayor. Por el contrario, arboles con maderas muy combustibles o resinosas se pueden representar con células que evolucionan rápidamente entre estado inicial y de combustión; en este caso perecerá velozmente, en tanto que su poder de contagiar fuego es menor.

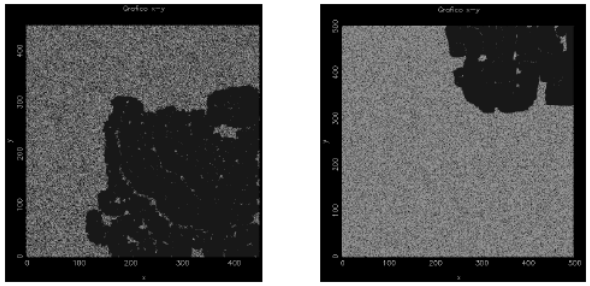

Figura 11: Gráfico del programa usado para la simulación que muestra los resultados después del incendio. El incendio puede ser devastador (izquierda) o quedar contenido incluso para densidades altas (derecha) .

Así la eficacia de los AC para modelar fenómenos naturales, queda una vez demostrada a través de un aplicación que no solo importa a los estudiosos del tema, sino que se combina con otras áreas (ecología, biología, agricultura) para contribuir a un problema actual del medio ambiente.

3.4. Criptografía

El desarrollo de la teoría, comúnmente surge por la necesidad de aplicar el conocimiento.En esta sección veremos una aplicación, la criptografía, que tiene mucho que ver con los sistemas complejos, y que representa claramente la relación entre teoría y aplicación.

3.4.1. ¿Que es la Criptografía?

En la actualidad, es casi una necesidad primaria estar en comunicación con otras personas. Ya sea por motivos laborales, personales o académicos, y no importando que se haga a través de un medio de transporte convencional o de manera electrónica, en la mayoría de los casos es necesario que esta información se transmita de manera fiable y segura. Es por eso que la criptología (del griego *cripto*-oculto- y *logos*-tratado, ciencia) tiene un gran auge, dividiéndose en dos ramas: *criptografía*, cuya tarea es cifrar la información a enviar, y *criptoanalisis* que se encarga de analizar técnicas y métodos para obtener la información cifrada.

El proceso para cifrar un mensaje consiste en transformarlo mediante un algoritmo de modo que sólo el destinatario pueda descifrarlo y recuperar el mensaje original. En dicho algoritmo se generan claves, un mensaje cifrado llamado criptograma y el proceso en conjunto se denomina criptosistema. El ideal de criptógrafo es lograr que el mensaje carezca de significado para cualquiera que no posea la clave de desencriptación, y aun así no restarle contenido que pueda ser extraído por alguien que si posea la clave. El proceso debe ser rápido en encriptación y desencriptación, usar una clave corta, de tamaño manejable y que no altere el tamaño de la información que lleva consigo. Si la clave es única y solo es conocida por emisor y el receptor, se le llama *clave simétrica*; en otro caso, si la clave para cifrar es de dominio publico, mientras que la que sirve para descifrar se mantiene en secreto, el criptosistema se denomina de clave asimétrica.

Para descifrar un mensaje, existen 2 tipos de ataques:

- **Ataques pasivos**
  - *Ataque al texto cifrado.* En este caso sólo se conoce un trozo del criptograma correspondiente al mensaje original.

- *Ataque al texto claro conocido.* en este ataque se utiliza un trozo del mensaje y su correspondiente criptograma.

- **Ataques activos**

  - *Ataque al texto claro elegido.* Aquí el atacante elige un texto del mensaje original y consigue el criptograma correspondiente. No hace falta conocer la clave, solo tener acceso temporal al criptosistema.

  - *Ataque al texto cifrado elegido.* En este, el atacante elige parte del mensaje cifrado o criptograma y obtiene el mensaje original. Igualmente no hace falta conocer la clave.

Actualmente, un buen criptosistema debe resistir ataques que permitan elegir tanto mensaje original como el cifrado, por cualquier método que el atacante o criptoanalista prefiera.

3.4.2. Criptosistemas basados en Autómatas Celulares.

Ahora se mostrara como producir un modelo ideal de cifrado. El estado futuro de un sistema dinámico depende de su estado inicial. Después de algún tiempo transcurrido esta configuración inicial es olvidada, es decir, no quedan rastros o pistas aparentes para volverla a generar. Pero, dado que es determinístico, se llegara al mismo resultado partiendo de la misma configuración inicial. Así que, la llave maestra del criptosistema puede ser la configuración inicial de un sistema dinámico conocido. El usuario, al compartir esta *llave* con otro, puede mandar mensajes secretos usando este sistema dinámico con su *secreta* configuración inicial. Cualquier otra persona que no conozca esta configuración inicial, no sera capaz de recuperar el mensaje aunque conozca como opera el sistema dinámico.

Una versión de esta idea ([12]) emplea el AC regla 30 de Wolfram (AC de 2 estados -0 y 1- y una vecindad, donde todas las posibles combinaciones de grupos de tres celdas ordenadas de menor a mayor en binario, tienen asignada una sola evolución con uno de los símbolos de los estados, representando una cifra también en binario, en este caso 30 (ver tabla 1). Se generan con esto secuencias simbólicas con un alto grado de aleatoriedad([13]). La llave secreta sigue siendo el arreglo inicial del sistema. El que envía el mensaje produce un texto cifrado gracias a la suma de bits de su mensaje original con la secuencia generada por el AC. El que recibe produce una secuencia aleatoria a partir

del mismo arreglo inicial, y vuelve a sumar el mensaje encriptado con esta secuencia recuperando el mensaje original.

Cuadro 1: Tabla que muestra la evolución del conjunto de células para la regla 30 (2 estados y una vecindad de cada lado). La suma del valor en binario de los conjuntos que evolucionan a uno es igual a 30

Célula central y vecindades	Estado al que evoluciona	Representación binaria del conjunto
0 0 0	0	1
0 0 1	1	2
0 1 0	1	4
0 1 1	1	8
1 0 0	1	16
1 0 1	0	32
1 1 0	0	64
1 1 1	0	128

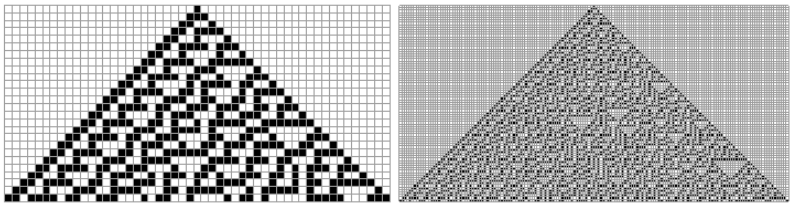

Figura 12: Diagrama de evolución del AC regla 30 en 25 y 100 generaciones. No se observa simetría, ni patrones repetidos, señal de su aleatoriedad.

Figura 13: Diagrama de evolución de la regla 30 modificada que indica la capacidad de retorno a la configuración original.

El considerar AC reversibles en las iteraciones, abre el camino para diseñar mas sistemas de encriptación. Esta propiedad de *reversibilidad* en los AC's, consiste en que cada configuración tiene un ancestro u origen único, permitiendo regresar al origen, así haya transcurrido un gran lapso de tiempo. Así no hace falta combinar el mensaje cada vez que se quiera encriptar o desencriptar, si no simplemente aplicar la regla de evolución y después su inverso. Al iterar hacia delante y hacia atrás, la llave es un sistema dinámico por si mismo. Si un AC tiene un inverso, ese mismo inverso también es un AC.

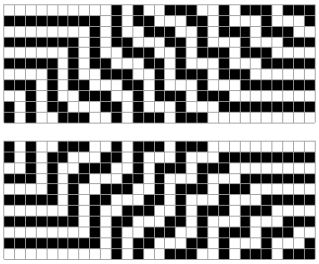

Figura 14: Diagrama de evolución de la regla 85 en 10 generaciones (arriba). Nótese que al hacer el diagrama de su inverso, la regla 15 (abajo), con la configuración final de la anterior y en el mismo numero de generaciones, llegamos a la configuración inicial de la regla 85 nuevamente.

Para ilustrar mejor todo esto veamos un ejemplo:

Supongamos que tenemos el AC definido por la regla 30, para el que se utiliza la siguiente configuración inicial:

(0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0)

La regla también se puede expresar de manera algebraica:

$$a_i^{(t+1)} = (a_{i-1}^{(t)} + a_i^{(t)} + a_{i+1}^{(t)} \cdot a_{i+1}^{(t)}) mod 2$$

$$= a_{i-1}^{(t)} XOR (a_i^{(t)} OR a_{i+1}^{(t)})$$

Donde a representa una célula, i es la posición(al sumarle o restarle nos movemos a las vecinas) y t es el instante en el tiempo.

Después de 100 iteraciones obtenemos una gran salida de ceros y unos;

1,0,1,1,1,0,0,1,1,0,0,0,1,0,1,1,0,0,1,0,0,1,1,1,1,0,1,1,1,1,0,1,0,1,1,1,1,0,1,
0,1,0,0,1,0,0,0,1,0,1,1,1,0,0,0,0,0,1,0,0,1,1,0,1,1,1,1,1,1,0,0,1,0,0,1,0,0,1,0,0,1,
0,1,1,1,1,0,1,0,1,1,1,0,0,1,0,1,0,1,0,0.

Ahora se encriptara un mensaje que contiene la palabra *SECRETO*. Basta con concatenar el valor en binario de cada una de las letras del mensaje, según el código ASCII, y luego sumar, bit a bit, la secuencia obtenida (M) con una porción de la secuencia de bits o clave (K), de igual tamaño, generada por el autómata.

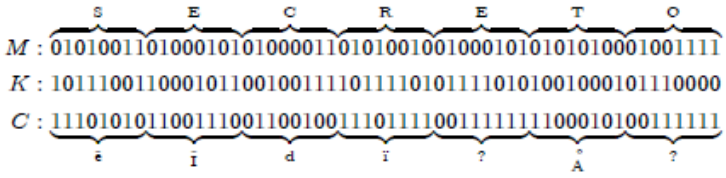

Figura 15: Suma de bits del mensaje original con la clave generada por el AC y su resultado en símbolos según el código ASCII.

De este modo el criptograma que se envía es el siguiente:

$$\hat{e}\ \hat{I}\ d\ \ddot{i}\ ?\ \mathring{A}\ ?$$

El destinatario recupera el mensaje original sin mas que concatenar el valor en binario de cada una de las letras o símbolos del criptograma recibido y sumarlo, bit a bit, con la clave, haciendo lo contrario a la evolución, es decir una involución.

La seguridad de este criptosistema está basada en la impredicibilidad de la clave generada, es decir, en la dificultad de poder obtener la secuencia pseudoaleatoria originada por el AC. De ahí la importancia de que los AC elegidos como generadores de claves pseudoaleatorias tengan buenas propiedades aleatorias.

En un estudio realizado sobre la seguridad del criptosistema definido anteriormente ([14]), se simularon varios ataques al criptosistema, observando que la intrusión tiene éxito si el tamaño de la clave esta entre 300 y 500 bits. Por los resultados obtenidos, se recomienda que el tamaño de la clave sea superior a 1000 bits.

También existe la posibilidad de utilizar las secuencias de bits generadas por un AC para generar claves numéricas únicas, claves parciales e incluso con propiedades particulares, como por ejemplo el que sean solo números primos.

Para completar esta sección, se puede decir que algunas herramientas del criptoanálisis pueden encontrar nuevos usos en la teoría de sistemas complejos, con un correcto entrenamiento en el área y una conveniente motivación se puede diseñar un sistema bien adaptado, que sea casi invulnerable a cualquier tipo de ataque.

4. Conclusiones

Es notable la gran capacidad que tienen los AC para simular fenómenos naturales, ayudando a una interpretación mas completa de los resultados de una investigación o incluso favoreciendo la prevención de situaciones no deseadas. También contribuye en las actividades humanas, al lograr que muchas operaciones matemáticas y de cómputo sean mas rápidas y permitan un manejo de datos superior a otros modelos abstractos.

Es favorable observar la difusión que se le ha dado a los AC en varias disciplinas, haciendo de esta herramienta parte en sus metodologías y aplicaciones, fomentando así el énfasis en su investigación por parte de escuelas, universidades, institutos, etc.

También invita a reflexionar en lo que se puede lograr profundizando en su entendimiento. Tal vez abra las puertas a nuevos paradigmas científicos que permitan, como los propios autómatas, pequeños avances, pero a pasos de gigante.

Nota: si se desean ver aplicaciones interesantes de los AC visitar el sitio: `http://cafaq.com/apps/index.php`

- -

Se agradece a la Universidad Autónoma de Puebla, especialmente al Dr. Harold V. Mcintosh, por su enseñanza en el Verano de Investigación y por incrustar el interés en la investigación de temas que son base para un gran desarrollo en el área científica.

También se agradece al Dr. Genaro Juárez Martínez, que siguiendo sus pasos, me permitió iniciar este proyecto, inspirando nuevos intereses durante su desarrollo.

5. Referencias

[1] Lorenz, E. N. *La esencia del caos.* Debate, Pensamiento. Barcelona, España. 1995.

[2] Schmitz, R. *Use of chaotic dynamical systems in cryptography.* J. Franklin Inst 228. 2001.

[3] M. Sipper. *The evolution of parallel cellular machine: The cellular programming approach.* Springer-Verlag. Berlin, Alemania. 1997.

[4] Krawczyc, Robert. *Programs as Pencils: Investigating Form Generation.* Association for Computer-Aided Design in Architecture. ACADIA Conference. 1997.

[5] Krawczyc, Robert. *Evolution of Mathematically Based Form Development.* Mathematical Connections in Art, Music and Science, Bridges Conference. 2000.

[6] Skavara, Marilena. *Adaptive Facade.* `http://www.interactivearchitecture.org/marilena-skavara-adaptive-facade.html`. 2010.

[7] Moya, Andrés. *Autómatas Celulares Aplicados a la Arquitectura.* `http://www.bitacoravirtual.cl/2010/03/29/automatas-celulares-aplicados-a-la-arquitectura-2/`. 2011.

[8] Lahoz-Beltrá, Rafael. *Bioinformática: simulación, vida artificial e inteligencia artificial.* Diaz de Santos. Madrid, España. 2004.

[9] Segura, Antinoo. *La Bioinformática: una ciencia de riesgo.* Revista Omnis Cellula. Cataluña, España. 2007.

[10] Victor, Jonathan David. *What can Automaton Theory tell us about the brain.* Elsevier Science Publishers. Amsterdam, Holanda. 1990.

[11] Gutowitz Howard. *Cellular Automata and the Sciences of Complexity.* `http://tuvalu.santafe.edu/~hag/complex2/complex2.html`. 1995.

[12] Wolfram, Stephen. *Cryptography with Cellular Automata.* Springer-Verlag. Heidelberg, Alemania. 1986

[13] Wolfram, Stephen. *Random Sequence Generation by Cellular Automata.* Advances in Applied Mathematics Vol. 7 No. 123. Florida, USA. 1984.

[14] Meier W. and Staffelbach O. *Analysis of pseudo random sequences generated by cellular automata.* Advances in Cryptology-Proceedings of EUROCRYPT. Berlin, Alemania. 1991.

[15] Peredo, Marco J. y Ramallo, Ramiro. *Aplicación de Autómatas Celulares a Simulación Básica de Incendios Forestales.* Acta Nova Vol. 2 No. 3. Cochabamba, Bolivia. 2003.

[16] Palma-Orozco, Rosaura. *La Matemática en la Bioinformática y los Autómatas Celulares.* `http://www.cudi.mx/aplicaciones/dias_cudi/08_08_21/Rosaura.pdf`. 2008.

[17] Krawczyc, Robert. *Architectural Interpretation of Cellular Automata.* Generative Art 2002. Chicago, U.S.A. 2002.

[18] Hernández Encinas, L. et al. *Aplicaciones de los autómatas celulares a la generación de bits.* Bol. Soc. Esp. Mat. Apl. No. 21, 65-87. Salamanca, España. 2002.