Resumen del paper "The Markov Chain Monte Carlo Revolution" de Perci Diaconis

Carlos M. Martinez

Junio de 2022

Abstract

Los autores presentan dos aplicaciones, una con relación al criptoanálisis y otra con vinculaciones a la mecánica estadística, que son tratables mediante "random walks" en espacios de estado.

Presentan un algoritmo conocido como "Algoritmo de Metrópolis" que es aplicable con ciertas precauciones a ambos tipos de problema.

Claves: Random walks, Algoritmo de Metrópolis

1 Consignas de la entrega

- Resumen de máximo 2 carillas en letra 10 o 12 pt.
- Explicar:
  - Que problemas se estudian o se resuelven
  - Que métodos se proponen
  - Discutir si se aplican técnicas similares a las del curso o más avanzadas
  - Que resultados numéricos se muestran
  - Otros puntos interesantes, que conclusiones se proponen y si se pudieran identificar debilidades del estudio

2 ¿Qué problemas se estudian o resuelven?

El autor se centra principalmente en dos problemas. Primero analiza el problema de decodificar un texto que ha sido cifrado mediante una técnica conocida como "cifrado de sustitución" y luego continua con un problema conocido como el "problema de los discos rígidos" (Hard Disc Problem)

2.1 Criptoanálisis

El autor presenta el problema de decodificar un texto cifrado mediante un cifrado de sustitución. Un cifrado de sustitución consiste en intercambiar cada carácter de nuestro alfabeto usual (incluyendo potencialmente símbolos de puntuación y espacios en blanco) sobre si mismo o sobre otro alfabeto. En el caso que se presenta en el paper el alfabeto destino se compone de símbolos gráficos con un cierto parecido con los jeroglíficos.

Un cifrado de sustitución puede verse entonces como una función invertible entre dos conjuntos:

$$f : \{S\} -> \{D\}$$

Donde S es el alfabeto de origen y D el alfabeto de destino.

El problema entonces de decodificar o descifrar un texto cifrado consiste en lograr identificar la función f y naturalmente su inversa.

Es conocido el hecho de las Cadenas de Markov son útiles para este tipo de análisis. Las probabilidades de transición de un elemento del alfabeto a otro pueden modelarse satisfactoriamente utilizando esta aproximación.

El autor describe un algoritmo para muestrear el espacio de todas las funciones f posibles buscando maximizar una *función de plausibilidad* que lo que mide es que tan bien se adapta cada muestra de f a la matriz que describe la cadena de Markov del texto.

Esta "plausibilidad" es un valor numérico asociado a cada función de cifrado f posible. El algoritmo propuesto muestrea vía Montecarlo el espacio de funciones de cifrado posibles buscando maximizar este valor. Como técnica avanzada el algoritmo introduce un paso aleatorio adicional mediante el cual en ciertos casos el algoritmo prefiere un paso "peor" (de plausibilidad menor).

El objetivo de este paso es evitar que el recorrido se confunda con máximos locales.

2.2 El "Hard Disc Problem"

El segundo problema que se presenta, "El problema de los discos duros" consiste en encontrar las posibles configuraciones para ubicar n discos sólidos de radio ϵ, que no pueden superponerse, en un cuadrado de lado 1.

Se propone un algoritmo similar, donde el espacio a recorrer es el *espacio de configuraciones o espacio de estados* de la caja. Las configuraciones están dadas por las ubicaciones de todos los centros de los discos que han podido ser ubicados.

El algoritmo propuesto lo que hace es sortear nuevos centros en el espacio de estados, desplazarlos aleatoriamente y chequear si la configuración resultante es una configuración válida.

3 El algoritmo de Metrópolis

Los autores describen el *Algoritmo de Metrópolis* como ejemplo de un algoritmo que permite recorrer una cadena de Markov buscando maximizar algún tipo de objetivo.

4 Conclusiones y otros puntos interesantes

Los problemas descritos en este paper son diferentes a los vistos en el curso. Claramente están relacionados, pero tienen características propias.

Los autores comentan que las técnicas Montecarlo aplicadas a recorridos en cadneas de Markov tienen múltiples aplicaciones, incluyendo Física y Química, Biología y propiamente Matemáticas.