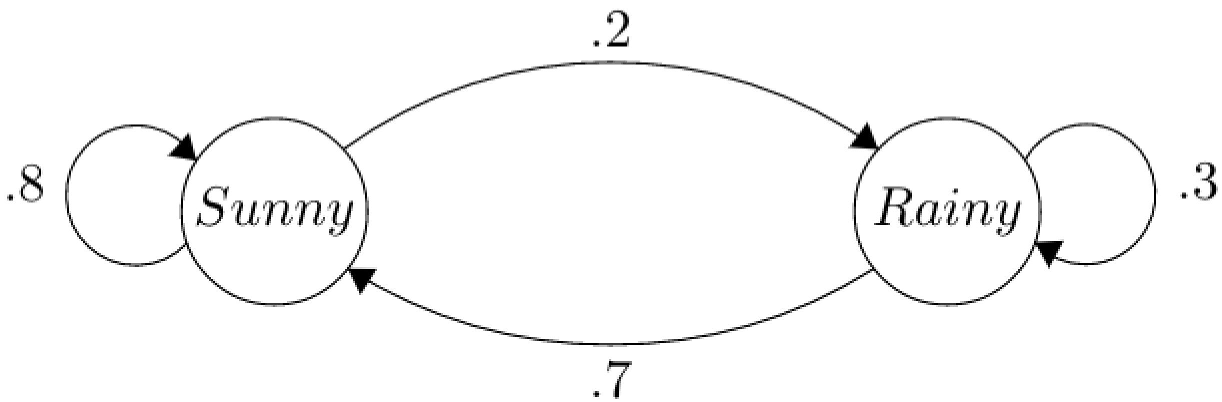
Markov Chain Monte Carlo

Algoritmo de Metrópolis-Hastings para Desencriptado

Alejandro Barón García

Qué es una cadena de Markov

- Proceso estocástico en el que la probabilidad del siguiente evento solo depende del inmediatamente anterior



Conceptos clave

- Matriz de transición: contiene las probabilidades de ir del estado I al j
- Distribución estacionaria: frecuencia/probabilidad de visitar un estado a largo plazo
- Periodicidad: nº mínimo de pasos necesarios para retornar a un estado

Algoritmo de Metropolis-Hastings

- 1953-Metropolis | 1970-Hastings
- Distribución desconocida π (discreta) a simular
- Matriz J muestreable finita irreducible con los mismos estados que π
- Algoritmo:

 1.-Elegir un estado j a partir del estado actual I con la matriz J

 2.-Decidir si pasar al estado j o permanecer en el estado I según la función de aceptación a(i,j)

Función de aceptación

- A partir de los estados a muestrear, sus probabilidades π, y la matriz J conocida, se define la función de aceptación como:

$$a(i,j)=\pi_j*J_{ji} /\pi_i*J_{ij}$$

- Si a(i,j)>1 ,aceptar estado j
- Si a(i,j)<=1, aceptar estado j con probabilidad a(i,j)

Cadena de Markov generada

- La Cadena de Markov generada por este algoritmo es una matriz con distribución estacionaria π.

- La frecuencia de visitas a los estados recorridos por el camino aleatorio generado por el algoritmo convergerá a π

Desencriptado Algoritmo M-H

- Aplicado a cifrados por sustitución

- Tendremos que recorrer las funciones de desencriptado e ir probando hasta dar con el mensaje correcto

- La idea es asignar a cada función una “probabilidad” según sea más factible que sea la función de desencriptado o no

Cómo asignar la probabilidad

- Definimos un score para cada función de desencriptado f. Tenemos una matriz M con estadísticas de ocurrencias obtenidas procesando Textos

- El score será el producto de el número de ocurrencias de los pares de caracteres dentro del texto al desencriptar f (se recorren todos los pares de caracteres al desencriptar. A más veces ocurran los pares, mayor será el score)

Cómo asignar la probabilidad

- Entonces la probabilidad de una función f_j será

$$\pi_j = score(f_j) / \Sigma_g\, score(f_g) \quad \text{(score total de las f)}$$

- Este score total puede no ser computable (27! términos)
- Distribuciones desconocidas

Recordemos $a(i,j)=\pi_j * J_{ji} / \pi_i * J_{ij}$

- Si J es simétrica (permutando dos letras de f), a(i,j) se reduce al cociente de π_j/π_i (ratio de ocurrencias de j frente a I) y los score totales no son necesarios $a(i,j)=score(f_j)/score(f_i)$

Algoritmo:

1. Seleccionar una función inicial f i (con i=0 en el primer paso)

2. Permutar 2 letras al azar de f i para obtener f_j

3. Calcular a(i,j) y decidir si aceptar f_j

4. Volver al paso 1, iterando tantas veces como sean necesarias hasta llegar a la solución

Reflexión propia: Problemas del Algoritmo

- Mensaje de Entrada
- Lenguaje Castellano
- Fallo del Algoritmo

Coste criptografía

- Suponiendo tamaño del mensaje L

Algorithm 1 Desencriptado MCMC

Require: Mensaje encriptado en minúsuculas, solo letras y sin puntuacion

O(1) $f_i \leftarrow funcion\_identidad$

O(L) $score_i \leftarrow score(funcion\_identidad)$

for $i < n\_iteraciones; i++$ **do**

O(cte) $f_j = permutar2(f_i)$

$score_j = score(f_j)$ ← Desencriptado O(L) + CálculoScore O(L) =O(2L)

O(1) $a(i,j) = score_j / score_i$

O(1) **if** $runif(0,1) < a(i,j)$ **then**

$f_i = f_j$

$score_i = score_j$

end if

end for

O(2L*n)

Convergencia M-H: Prueba de Convergencia a π

P_{ij} tomará los valores:

$$a(i,j)*J_{ij} \text{ si } \pi_j J_{ji} <= \pi_j J_{ij}$$

$$J_{ij} \text{ si } \pi_j J_{ji} > \pi_j J_{ij}$$

Se dice que un proceso de Markov cumple las ecuaciones de equilibrio si para todo x, ydel conjunto de estados se tiene que (si se cumplen, π es la distribución estacionaria)

$$\pi_x P_{xy} = \pi_y P_{yx}$$

Para el caso de π j J ji ≤ π i J ij

$$\pi_i P_{ij} = \pi_i J_{ij} a(i, j) = \pi_i J_{ij} \pi_j J_{ji} / \pi_i J_{ij} = \pi_j J_{ji} = \pi_j \underline{P_{ji}}$$

Convergencia del error

- Problema muy complicado.

- Perci Diaconis propone

$$\|P_x^n - \pi\| = \frac{1}{2}\sum_y |P^n(x,y) - \pi_y| = \max_{A\subseteq X} |P^n(x,A) - \pi_A|$$

- Dobrow:

$$\varepsilon < |\lambda_{2º\text{Más grande}}|^n * cte$$