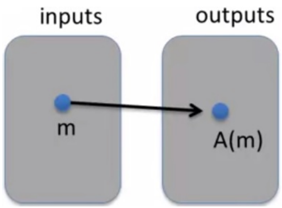
Repaso de Probabilidad Discreta

Alan Reyes-Figueroa

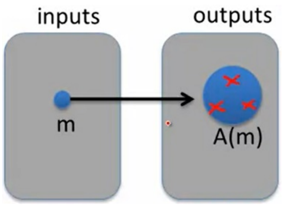
Criptografía y Cifrado de Información (Aula 04) 22.julio.2021

Algoritmos deterministas vs. algoritmos aleatorios

Un **algoritmo determinista** es una función $\mathbf{x} \mapsto \mathbf{y} = A(\mathbf{x})$. Dada una entrada **x**, siempre devuelve el mismo valor al repetirlo.



Un **algoritmo aleatorio** es una función $\mathbf{x}\mathbf{y} = A(\mathbf{x}, \mathbf{r})$, donde $\mathbf{r} = R(\mathbf{z})$ es una variable aleatoria. Siempre devuelve distintos valores cada vez que se repite.



UNIVERSIDAD DEL VALLE DE GUATEMALA

Algoritmos Aleatorios

Ejemplo: Algoritmo que encripta un mensaje $E(m, \mathbf{k})$, donde **k** se define como una clave aleatoria.

Por ejemplo **k** se elige con distribución uniforme dentro de un conjunto de cadenas de bits $\Omega = \{0, 1\}^n$.

Independencia

La idea de **independencia** es determinar si hay o no relación entre dos eventos A y B.
En otras palabras, si al conocer A, cambia nuestro conocimiento sobre B (o al conocer B cambia nuestro conocimiento sobre A).

Definición

*Dos eventos A y B son **independientes** si, y sólo si,*

$$\mathbb{P}(A \cap B) = \mathbb{P}(A)\,\mathbb{P}(B).$$

Ejemplo

Lanzamiento de dos dados D_1 y D_2. Consideremos los eventos $A = \{D_1 + D_2 \text{ es par}\}$, $B = \{D_1 < 5\}$, $C = \{D_1 \leq 3, D_2 \leq 3\}$. Sabemos que $\mathbb{P}(A) = \frac{1}{2}$, $\mathbb{P}(A \cap B) = \frac{1}{2}$, $\mathbb{P}(A \cap C) = \frac{5}{9}$.

$D_1 \setminus D_2$	1	2	3	4	5	6
1	X		X		X	
2		X		X		X
3	X		X		X	
4		X		X		X
5						
6						

$D_1 \setminus D_2$	1	2	3	4	5	6
1	X		X			
2		X				
3	X		X			
4						
5						
6						

Luego, A y B son independientes; mientras que A y C no lo son.

Definición

Dos variables aleatorias discretas X y Y definidas sobre el mismo espacio Ω son ***independientes*** *si*

$$\mathbb{P}(X = a, Y = b) = \mathbb{P}(X = a)\,\mathbb{P}(Y = b), \quad \forall\, a, b \in \mathbb{R}.$$

En general, las v.a. discretas $X_1, \ldots, X_n$ son ***mutuamente independientes*** *si*

$$\mathbb{P}(X_1 = x_1, \ldots, X_n = x_n) = \prod_{i=1}^{n} \mathbb{P}(X_i = x_i), \quad \forall x_1, x_2, \ldots, x_n \in \mathbb{R}.$$

Independencia

Ejemplo: $\Omega = \{0,1\}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$ y p la distribución uniforme.

Definimos las variables aleatorias $X = \mathbf{lsb}_1(\mathbf{x})$, $Y = \mathbf{msb}_1(\mathbf{x})$.

- Para $X = 0, Y = 0$: $\mathbb{P}(X = 0, Y = 0) = \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2} = \mathbb{P}(X = 0)\,\mathbb{P}(Y = 0)$.
- Para $X = 0, Y = 1$: $\mathbb{P}(X = 0, Y = 1) = \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2} = \mathbb{P}(X = 0)\,\mathbb{P}(Y = 1)$.
- Para $X = 1, Y = 0$: $\mathbb{P}(X = 1, Y = 0) = \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2} = \mathbb{P}(X = 1)\,\mathbb{P}(Y = 0)$.
- Para $X = 1, Y = 1$: $\mathbb{P}(X = 1, Y = 1) = \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2} = \mathbb{P}(X = 1)\,\mathbb{P}(Y = 1)$.

Esto comprueba que X y Y son independientes.

Propiedad del XOR

Teorema (Propiedad de la función XOR)

Si X es una variable aleatoria en $\{0,1\}^n$, y Y es otra v.a. independiente de X, con $Y \sim U(\{0,1\}^n)$, entonces $Z = X \oplus Y \sim U(\{0,1\}^n)$.

Comentario: Si a una cadena de bits X le hacemos XOR con una cadena de bits aleatoria Y (donde la probabilidad de que los bits en Y sean 0 ó 1 es la misma: $\mathbb{P}(Y_i = 0) = \mathbb{P}(Y_i = 1) = \frac{1}{2}$), entonces la cadena de bits

$$Z = X \oplus Y = XOR(X, Y),$$

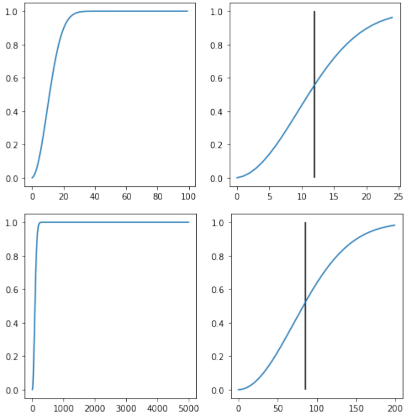
también cumple que $\mathbb{P}(Z_i = 0) = \mathbb{P}(Z_i = 1) = \frac{1}{2}$.

Así, la función XOR esconde las probabilidades de ocurrencia de caracteres en la cadena de bits original X.

Teorema (Paradoja del cumpleaños)

Sean $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k \in \Omega$ *variables aleatorias independientes con distribución uniforme en* Ω, $|\Omega| = n$.

Entonces, para $k \approx 1.2\sqrt{n}$, *se tiene con probabilidad* $\mathbb{P} \geq \frac{1}{2}$, *existen* $1 \leq i, j \leq k$, $i \neq j$, *tales que* $\mathbf{x}_i = \mathbf{x}_j$.



UVG UNIVERSIDAD DEL VALLE DE GUATEMALA