PROPEDÉUTICO DE MATEMÁTICAS

Generación 13

[2019]

Luis J. Dominguez Perez

GOBIERNO DE MÉXICO

Sesión 1

Contenido, sección 1

Los seis fundamentales

Hay seis conceptos elementales que necesitan enfatizarse en las matemáticas de la criptografía. Sea S un conjunto de elementos, y $+$, $\times$, $\odot$ operadores binarios en S:

- Cerradura: S está cerrado sobre $\odot$ si para todo $a, b \in S$, $a \odot b \in S$
- Asociatividad: S es asociativo sobre $\odot$ si para todo $a, b, c \in S$:

$$a \odot (b \odot c) = (a \odot b) \odot c.$$

los elementos en $\mathbb{R}$ son asociativos sobre $+$, y $\times$.

. . . los seis fundamentales

- Conmutabilidad: S es conmutativa sobre $\odot$ si para todo $a, b, c \in S$:

$$a \odot b = b \odot a$$

los elementos en $\mathbb{R}$ son conmutativos sobre $+$, y $\times$.

- Distributiva: S es distributivo sobre $+$ si para todo $a, b, c \in S$:

$$a \times (b + c) = (a \times b) + (a \times c)$$

los elementos en $\mathbb{R}$ son distributivos sobre la suma

. . . los seis fundamentales

- Identidad: El elemento $I \in S$ es una identidad sobre $+$ si para todo $a \in S$:

$$a + I = I + a = a$$

  los elementos en $\mathbb{R}$ tienen el 0 como elemento identidad para la suma, y el 1 para la multiplicación

- Inverso: Sean $0, 1 \in S$ las identidades aditivas y multiplicativas, respectivamente, de S. Un elemento $a \in S$ es el inverso aditivo de $b \in S$ si $a + b = b + a = 0$. Es el inverso multiplicativo si $a \times b = b \times a = 1$. Por ejemplo, 2 es el inverso aditivo de -2 (y viceversa), mientras que 0.5 es su inverso multiplicativo.

Bases matemáticas generales

- Tipos de números
- Teorema, lema, colorario, proposición
- Teoría de conjuntos, matrices, y vectores

Bases matemáticas generales

- Tipos de números
- Teorema, lema, colorario, proposición
- Teoría de conjuntos, matrices, y vectores

El objetivo de esta unidad es recordar los conceptos generales de matemáticas aplicadas. . .

otros temas a cubrir

. . .se incluyen además los siguientes temas:

- Teoría de probabilidad
- Teoría de la información
- Teoría de la complejidad
- Teoría de números
- Álgebra abstracta
- Campos finitos

otros temas a cubrir

. . .se incluyen además los siguientes temas:

- Teoría de probabilidad
- Teoría de la información
- Teoría de la complejidad
- Teoría de números
- Álgebra abstracta
- Campos finitos

De hecho, Teoría de números y Campos finitos tienen su propia sección en este curso.

Contenido de la sección 2

Clases de números

- Naturales
- Enteros
- Reales
- Imaginarios

- Racionales
- Irracionales

Notación

- $\mathbb{Z}$ denota el conjunto de números *enteros*:
  $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- $\mathbb{Q}$ denota el conjunto de número *racionales*:
  $\{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$
- $\mathbb{R}$ denota el conjunto de los números *reales*
- $[a, b]$ denota a todos los enteros x que satisfacen:
  $a \leq x \leq b$
- $\lfloor x \rfloor$ denota el entero más grade que es menor o igual a x:
  $\lfloor 5.2 \rfloor = 5, \lfloor -5.2 \rfloor = 6$
- $\lceil x \rceil$ denota el entero más pequeño que es mayor o igual a x: $\lceil 5.2 \rceil = 6, \lceil -5.2 \rceil = 5$

Notación

- Una *función* o *mapeo* $f : A \to B$ es una regla que asigna a cada elemento a en A un solo elemento b en B. Si $a \in A$ se mapea a $b \in B$, entonces a b se le conoce como la *imagen* de a, y a la a se le conoce como la *preimagen* de b, y se escribe como: $f(a) = b$. El conjunto A se le conoce como el *dominio* de f, y al conjunto B se le conoce como *codominio* de f.

Notación

- Una functión $f : A \to B$ es $1 - -1$ (*uno-a-uno*) or *inyectiva* si cada elemento en B es la imagen de al menos un elemento en A. Por lo que $f(a_1) = f(a_2)$ implica que $a_1 = a_2$.
- Una función $f : A \to B$ es *sobreyectiva* si cada $b \in B$ es la imagen de al menos un elemento $a \in A$.
- Una función $f : A \to B$ es *biyectiva* si es inyectiva y sobreyectiva. Si f es una biyección entre los conjuntos finitos A y B, entonces $|A| = |B|$. Si f es una biyección entre el conjunto A y sí mismo, entonces f es una *permutación* de A.

Notación

- Si A es un conjunto finito, entonces $|A|$ denota el número de elementos en A, o *cardinalidad* de A
- π es la constante matemática: $\pi \approx 3.14159$
- e es la base de los logaritmos naturales: $e \approx 2.71828$

Contenido de la sección 3

Teorema

Definición

Un teorema es una fórmula bien formada que puede ser demostrada dentro de un sistema formal.

CIMAT

Definición

Un teorema es una fórmula bien formada que puede ser demostrada dentro de un sistema formal.

Para que una afirmación de este tipo pueda ser considerada un teorema, esta debe ser interesante o útil desde un punto de vista matemático.

Ejemplo: el teorema de Pitágoras

Práctica

- Verifique el teorema de Pitágoras. (en Sage)

Lema

Definición

Es una afirmación probada, y que está ligada a un teorema, normalmente como consecuencia.

Lema

Definición

Es una afirmación probada, y que está ligada a un teorema, normalmente como consecuencia.

Teorema de Euclides: Si p es un número primo, y divide al producto de dos enteros positivos, entonces p divide al menos a uno de estos.

Lema

Definición

Es una afirmación probada, y que está ligada a un teorema, normalmente como consecuencia.

Teorema de Euclides: Si p es un número primo, y divide al producto de dos enteros positivos, entonces p divide al menos a uno de estos.

Lema: Si n es un entero positivo, y divide al producto de dos enteros positivos, y si además, es coprimo de uno de ellos, entonces, divide al otro.

Práctica

- Verifique el teorema de Euclides, y su lema. (en Sage)

Corolario

Definición

Designar la evidencia de un teorema o de una definición ya demostrados, sin necesidad de invertir esfuerzo adicional en su demostración

Esto es, es una afirmación tan evidente, que no necesita comprobación

Corolario

Definición

Designar la evidencia de un teorema o de una definición ya demostrados, sin necesidad de invertir esfuerzo adicional en su demostración

Esto es, es una afirmación tan evidente, que no necesita comprobación

Ejemplo:

- La suma de los ángulos interiores de un triángulo es igual a 180°

Corolario

Definición

Designar la evidencia de un teorema o de una definición ya demostrados, sin necesidad de invertir esfuerzo adicional en su demostración

Esto es, es una afirmación tan evidente, que no necesita comprobación

Ejemplo:

- La suma de los ángulos interiores de un triángulo es igual a 180°
- En un triángulo rectángulo la suma de los dos ángulos contiguos a la hipotenusa es igual a 90°.

CIMAT

Proposición

Una sentencia portadora de valores de verdad

Ejemplo: Está lloviendo (válida sólo si está lloviendo)

Conjetura

Afirmación que se supone cierta, pero que no ha sido probada ni refutada hasta la fecha

Ejemplo: $P \neq NP$

CIMAT

Postulado

Un postulado es una proposición no evidente por sí misma, ni demostrada, pero que se acepta ya que no existe otro principio al que pueda ser referida.

Ejemplo: Los postulados de Euclides, que dieron nacimiento a la geometría euclidiana. Cuando algunos de sus postulados fueron cuestionados, nació la geometría no-euclidiana, la hiperbólica, etc.

Contenido de la sección 4

CIMAT

Definición

Es una colección bien definida de objetos

- Estos objetos se llaman *elementos*, y se dice que son *miembros* del conjunto.
- Se escribe:
  - $a \in A$, si a es un elemento de A
  - $b \notin A$, si b no es un elemento de A
- Para enumerar los elementos de un conjunto, se escribe:
  - $A = \{1, 2, 3, 4, 5\}$
  - $A = \{x | x \text{ es un entero, y } 1 \leq x \leq 5\}$
- La *cardinalidad* o *tamaño* de un conjunto se denota por $|A|$

CIMAT

Definición

Si C, D son conjuntos del universo $\mathcal{U}$, se dice que C es un *subconjunto* de $\mathcal{D}$ (escrito así: $C \subseteq D$, o $C \supset C$), si cada elemento de C es un elemento de D.

Si D contiene al menos un elemento que no está en C, entonces C es un *subconjunto propio* de D: $C \subset D$, o $D \supset C$.

Reglas de pertenencia

Para cualquier conjunto C, D, en el universo $\mathcal{U}$:

- $C \subseteq D \Leftrightarrow \forall x[x \in C \Rightarrow x \in D]$
- $C \subset D \Rightarrow C \subseteq D$

cuando C, D son finitos:

- $C \subseteq D \Rightarrow |C| \leq |D|$
- $C \subset D \Rightarrow |C| < |D|$

Igualdad y transitividad entre conjuntos

CIMAT

Definición

Para un universo dado $\mathcal{U}$, los conjuntos C y D (contenidos en $\mathcal{U}$) son *iguales* (denotado como $C = D$), cuando $C \subseteq D$, y $D \subseteq C$.

Teorema

Sean $A, B, C \subseteq \mathcal{U}$:

- $(A \subseteq B \land B \subseteq C) \Rightarrow A \subseteq C$
- $(A \subset B \land B \subseteq C) \Rightarrow A \subset C$
- $(A \subseteq B \land B \subset C) \Rightarrow A \subset C$
- $(A \subset B \land B \subset C) \Rightarrow A \subset C$

Conjuntos vacíos y potencia

Definición

El conjunto *vacío* o *nulo* es el (único) conjunto que no contiene elementos. Se denota: $\emptyset$ o $\{\}$.

Teorema

Para cualquier universo $\mathcal{U}$, sea $A \subseteq \mathcal{U}$. Entonces $\emptyset \subseteq A$, y si $A \neq \emptyset$, entonces $\emptyset \subset A$.

Definición

Si A es un conjunto del universo $\mathcal{U}$, el *conjunto potencia*, que se denota $\mathcal{P}(A)$ es el conjunto de todos los subconjuntos de A.

Teorema

Para cualquier conjunto finito A con $|A| = n \geq 0$, $|\mathcal{P}(A)| = 2^n$

Operaciones de conjuntos

Definiciones (entre los conjuntos A y B):

- Unión: $A \cup B = \{x | x \in A \vee x \in B\}$
- Intersección: $A \cap B = \{x | x \in A \wedge x \in B\}$
- Diferencia simétrica: $A \triangle B = \{x | x \in A \cup B \wedge x \notin A \cap B\}$

Un resultado importante es que: $A \cap B \subseteq A \subseteq A \cup B$

CIMAT

Definición

Sean $S, T \subseteq \mathcal{U}$, los conjuntos S y T son *disjuntos* o *mutuamente disjuntos* si $S \cap T = \emptyset$

Teorema

Si $S, T \subseteq \mathcal{U}$, entonces S y T son disjuntos sí, y sólo sí $S \cup T = S \triangle T$

CIMAT

Definiciones

- Para un conjunto $A \subset \mathcal{U}$, el *complemento* de A, que se denota con $\mathcal{U} - A$, o $\bar{A}$, está dado por $\{x | x \in \mathcal{U} \wedge x \notin A\}$
- Para $A, B \subseteq \mathcal{U}$, el *complemento (relativo)* de A en B, que se denota con $B - A$ está dado por $\{x | x \in B \wedge x \notin A\}$

Teorema

$A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B \Leftrightarrow \bar{B} \subseteq \bar{A}$

Propiedades de la teoría de conjuntos

CIMAT

$$\bar{\bar{A}} = A$$

Ley del doble complemento

$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$
$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

Leyes de De Morgan

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

Propiedades conmutativas

$$A \cup (B \cup C) = (A \cup B) \cup C$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$

Propiedades asociativas

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Propiedades distributivas

más propiedades de la teoría de conjuntos

CIMAT

$$A \cup A = A$$
$$A \cap A = A$$

Propiedades idempotentes

$$A \cup \emptyset = A$$
$$A \cap \mathcal{U} = A$$

Propiedades del neutro

$$A \cup \bar{A} = \mathcal{U}$$
$$A \cap \bar{A} = \emptyset$$

Propiedades del investo

$$A \cup \mathcal{U} = \mathcal{U}$$
$$A \cap \emptyset = \emptyset$$

Propiedades de dominación

$$A \cup (A \cap B) = A$$
$$A \cap (A \cup B) = A$$

Propiedades de absorción

CIMAT

Definición

Sea s una proposición (general) que trata de la igualdad de dos expresiones de conjuntos. cada una de estas expresiones puede contener una o más ocurrencias de conjuntos (como A, $\bar{A}$, B, etc.), una o más ocurrencias de $\emptyset$ y $\mathcal{U}$, y solamente los símbolos de las operaciones de conjuntos $\cup$ y $\cap$. El *dual* de s, denotado s^d, se obtiene de s al reemplazar:

- cada ocurrencia de $\emptyset$ y $\mathcal{U}$ (en s) por $\mathcal{U}$y $\emptyset$, respectivamente
- cada ocurrencia de $\cup$ e $\cap$ (en s) por $\cap$ y $\cup$ respectivamente.

Principio de dualidad

Teorema

El principio de dualidad. Sea s un teorema relativo a la igualdad de dos expresiones con conjuntos (como en la definición anterior). Entonces s^d, el dual de s, es también un teorema.

Contenido de la sección 5

CIMAT

Definición

Un *espacio de probabilidad* finito es el par $(\Omega, \Pr)$, en donde Ω es un conjunto finito (llamado el *espacio de muestra*, y cuyos elementos son llamados *eventos elementales*), y

$$\Pr : \Omega \to \mathbb{R}$$

es una *distribución de probabilidad*, o una función que satisface las siguientes condiciones:

- $0 \leq \Pr(\omega) \leq 1$ para todo $\omega \in \Omega$
- $\sum_{\omega \in \Omega} \Pr(\omega) = 1$

En otras palabras

- Un *experimento* es un procedimiento que produce un conjunto dado de resultados. Los posibles resultados individuales se llaman *eventos simples*. El conjunto de todos los posibles resultados es el *espacio de muestra*.

- La *distribución de probabilidad* P en Ω es una secuencia de números $p_1, p_2, \ldots, p_n$ no-negativos que suman 1. El número p_i se interpreta como la *probabilidad* de ω_i de ser el resultado de un experimento.

Podemos extender estos conceptos a los subconjuntos...

Definición

Un evento E es un subconjunto del espacio de muestra Ω, $E \subseteq \Omega$. La *probabilidad* de que el evento E ocurra, $\Pr(E)$, es la suma de las probabilidades p_i de todos los eventos simples ω_i que pertenecen a E: $\Pr(E) = \sum_{\omega \in E} \Pr(\omega)$.

Definición

Si E es un evento, el *evento complementario* es el conjunto de los eventos simples que no pertenecen a E, denotado como $\bar{E}$, $\bar{E} = \Omega - E$.

Sean $E \subseteq \Omega$ un evento:

- $0 \leq \Pr(E) \leq 1$. Adicionalmente, $\Pr(\Omega) = 1$, y $\Pr(\emptyset) = 0$
- $\Pr(\bar{E}) = 1 - \Pr(E)$
- Si los resultados en Ω tienen igual probabilidad de suceder, entonces $\Pr(E) = \frac{|E|}{|\Omega|}$.

Ejemplo

El tirar un dado se puede interpretar como un experimento de un espacio de muestra $\Omega = \{1, 2, \ldots, 6\}$ y, asumiendo de que el dado es justo, cada resultado tiene la misma probabilidad de resultar, entonces $\Pr(n) = \frac{1}{6}$ para cada $n \in \Omega$

CIMAT

Definición

Dados dos eventos $E_1, E_2 \in \Omega$, se llaman *mutuamente exclusivos* si $P(E_1 \cap E_2) = 0$. Esto es, si la ocurrencia de uno de los eventos excluye la posibilidad de que el otro ocurra.

Definición

Dados dos eventos $E_1, E_2 \in \Omega$, la *unión de eventos* $E_1 \cup E_2$ está dada por

$$\Pr(E_1 \cup E_2) = \Pr(E_1) + \Pr(E_2) - \Pr(E_1 \cap E_2)$$

Unión e intersección, ejemplo

CIMAT

Ejemplo de los dados

Si Ω consiste en todos los posibles resultados de tirar un dado, definamos un evento E_1 descrito como la probabilidad de tirar un número par, y un evento E_2 consistente de lanzar un múltiplo de 3.

- $\Pr(E_1) \cap \Pr(E_2)$ es tirar un 6 (par y múltiplo de 3), así que su posibilidad es de $\frac{1}{6}$
- $\Pr(E_1) = \frac{1}{2}$
- $\Pr(E_2) = \frac{1}{3}$

Así, tenemos que

$$\Pr(E_1) \cup \Pr(E_2) = \Pr(E_1) + \Pr(E_2) - \Pr(E_1 \cap E_2) = \frac{1}{2} + \frac{1}{3} - \frac{1}{6} = \frac{2}{3}.$$

CIMAT

Observación

Sean E_1 y E_2 dos eventos

- Si $E_1 \subseteq E_2$, entonces $\Pr(E_1) \leq \Pr(E_2)$
- $\Pr(E_1 \cup E_2) + \Pr(E_1 \cap E_2) = \Pr(E_1) + \Pr(E_2)$.
- Si E_1, y E_2 son *mutuamente exclusivos*, $\Pr(E_1 \cup E_2) = \Pr(E_1) + \Pr(E_2)$

Definición

Dos eventos $E_1, E_2 \in \Omega$ son independientes si

$$\Pr(E_1 \cap E_1) = \Pr(E_1) \cdot \Pr(E_2)$$

Ejemplo: ¿cuál es la probabilidad de tirar un 3, y un 5?

CIMAT

Definición

Sean E_1 y E_2 dos eventos con $\Pr(E_1) > 0$. La *probabilidad condicional de E_2 dado E_1*, denotada como $\Pr(E_2|E_1)$, es:

$$\Pr(E_2|E_1) = \frac{\Pr(E_2 \cap E1)}{\Pr(E_1)} \tag{1}$$

Observación

Si E_1 y E_2 so independientes, entonces $\Pr(E_2|E_1) = \Pr(E_2)$, y $\Pr(E_1|E_2) = \Pr(E_1)$. Esto es, que la ocurrencia de un evento no influye en la probabilidad de ocurrir de el otro.

Probabilidad condicional, ejemplo

Regresando al ejemplo de los dados:

- Tirar un número par, $\Pr(E_1) = \frac{1}{2}$
- Tirar un múltiplo de 3, $\Pr(E_2) = \frac{1}{3}$

Tenemos que:

- $\Pr(E_2|E_1) = \frac{\Pr(E_2 \cap E1)}{\Pr(E_1)} = \frac{\frac{1}{6}}{\frac{1}{2}} = \frac{1}{3}$
- $\Pr(E_1|E_2) = \frac{\Pr(E_1 \cap E2)}{\Pr(E_2)} = \frac{\frac{1}{6}}{\frac{1}{3}} = \frac{1}{2}$

Teorema de Bayes

Si E_1 y E_2 son eventos con $\Pr(E_2) > 0$, entonces:

$$\Pr(E_1|E_2) = \frac{\Pr(E1) \cdot \Pr(E_2|E_1)}{\Pr(E_2)} \tag{2}$$

El teorema de Bayes busca obtener la probabilidad de que un evento E_1 suceda, dado un evento E_2 que depende de este ...

- Por ejemplo, ¿cuál es la probabilidad de que el América gane la ida de visitante, si es casi seguro que gane la vuelta en su casa?

Dados los eventos E_1, y E_2,

$$\Pr(E_1) = \Pr(E_1|E_2) \cdot \Pr(E_2) + \Pr(E_1|E_2') \cdot \Pr(E_2') \tag{3}$$

$$\begin{aligned}
&\Pr(E_1|E_2) \cdot \Pr(E_2) + \Pr(E_1|E_2') \cdot \Pr(E_2') \\
&\quad = \Pr(E_1 \cap E_2) + \Pr(E_1 \cap E_2') \\
&\quad = \Pr((E_1 \cap E_2) \cup (E_1 \cap E_2')) \\
&\quad = \Pr(E_1)
\end{aligned}$$

$$\Pr(E_1|E_2) = \frac{\Pr(E_2|E_1) \cdot \Pr(E_1)}{\Pr(E_2|E_1) \cdot \Pr(E_1) + \Pr(E_2|E_1') \cdot \Pr(E_2|E_1') \cdot \Pr(E_1')} \quad (4)$$

Se invierten los valores en la Ecuación 3...

$$\Pr(E_1|E_2) = \frac{\Pr(E_2|E_1) \cdot \Pr(E_1)}{\Pr(E_2|E_1) \cdot \Pr(E_1) + \Pr(E_2|E_1') \cdot \Pr(E_1')} \quad (5)$$

y se sustituye la Ecuación 5 en el denominador de la Ecuación 2, y se obteniene la Ecuación 4.

CIMAT

Ejemplo

Se tienen dos tómbolas con monedas de oro y de plata. En la primera se tienen 10 monedas de oro y 5 de plata, en la segunda se tienen 2 de oro y 8 de plata. Si se escoge una tómbola al azar, y se saca una moneda al azar, ¿cuál es la probabilidad de que sea de oro?

Sea

$$E_1 = \{\text{una moneda de oro}\}$$

la probabilidad de E_1 depende de la tómbola seleccionada, y luego de la moneda que se saque, entonces tenemos que

$$E_2 = \{\text{tómbola 1}\}(E_2' = \{\text{tómbola 2}\})$$

...

Así que la fórmula de probabilidad queda así

$$\Pr(E_1) = \Pr(E_1|E_2) \cdot \Pr(E_2) + \Pr(E_1|E_2') \cdot \Pr(E_2')$$

calculando las probabilidades condicionales

$$\Pr(E_1|E_2) = \frac{10}{15} = \frac{2}{3}, \quad \Pr(E_1|E_2') = \frac{2}{10} = \frac{1}{5}, \quad \Pr(E_2) = \Pr(E_2') = \frac{1}{2}$$

queda así

$$\Pr(E_1) = \Pr(E_1|E_2)\cdot\Pr(E_2)+\Pr(E_1|E_2')\cdot\Pr(E_2') = \frac{2}{3}\cdot\frac{1}{2}+\frac{1}{5}\cdot\frac{1}{2} = \frac{13}{30} \approx 0.433.$$

Definition

Una *variable aleatoria* es una función

$$X : \Omega \to \mathbb{R}$$

cuyo dominio es el espacio de muestra Ω, y toma valores en los números reales.

- Dado que el espacio de muestra es finito, una variable aleatoria también tiene valores finitos.
- Se utilizan para definir eventos:

$$\{\omega \in \Omega : X(\omega) \leq x\}, \{\omega \in \Omega : X(\omega) = x\}, \{\omega \in \Omega : X(\omega) > x\}$$

CIMAT

Definición

Sea $X : \Omega \to \mathbb{R}$ una variable aleatoria. La *función de densidad de probabilidad de X*, denotada como $f(x)$, se define como

$$f_X(x) = \Pr(X = x)$$

en otras palabras, $f_X(x)$ es la probabilidad de que X tome el valor x.

En algunos casos, se utiliza (en lugar de) la *función de distribución de X*, la cual es la función:

$$F_X(x) = \Pr(X \leq x)$$

Funciones de densidad estándar

Existen algunas funciones de densidad estándar que se utilizan en el cálculo de la probabilidad discreta.

- Distribución uniforme
- Distribución binomial
- Distribución hipergeométrica
- Distribución de densidad conjunta de X y Y

CIMAT

Definición

Sea S un conjunto conteniendo N elementos,
$S = \{0, 1, \ldots, N-1\}$. Sea X una variable aleatoria que satisface:

$$f_X(j) = \Pr(X = j) = \begin{cases} \frac{1}{N} & \text{if } j \in S \\ 0 & \text{if } j \notin S \end{cases}$$

Se dice que la variable X está *uniformemente distribuida*, o que tiene *densidad uniforme*

CIMAT

Definición

Sea n y k enteros no negativos. El *coeficiente binomial* $\binom{n}{k}$ es el número de diferentes maneras de escoger k objetos diferentes de un conjunto de n objetos diferentes, en donde el orden no es importante

Propiedades de los coeficientes binomiales

Sean n y k enteros no negativos:

- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
- $\binom{n}{k} = \binom{n}{n-k}$
- $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$

CIMAT

Teorema binomial

Para todos los números reales a, b, y enteros no negativos n:
$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Definición

Un *intento de Bernoulli* es un experimento con exactamente dos resultados posibles, llamados *éxito* y *fracaso*. Entonces la probabilidad de que k tenga éxito en una secuencia de n intentos independientes es:

$$f_X(k) = \Pr(X = k) = \binom{n}{k} p^k (1-p)^{n-k}, \text{ para cada } 0 \leq k \leq n$$

A esto se le conoce como *función de densidad binomial*

Distribución hipergeométrica

Suponga que una tómbola contiene 100 bolas, de las cuales 21 son blancas, y el resto negras. Si tomamos 10 bolas al azar (y sin reemplazos), ¿cuál es la probabilidad de que exáctamente 3 sean blancas?

El número total de maneras de seleccionar 10 bolas de entre las 100 es de $\binom{100}{10}$. Similarmente, hay $\binom{21}{3}$ maneras de seleccionar 3 bolas blancas de las 21 que son, y hay $\binom{79}{7}$ maneras de seleccionar 7 bolas negras de las 79 que hay...

Por lo que tenemos $\binom{21}{3}\binom{79}{7}$ maneras de seleccionar 3 bolas blancas (y 7 bolas negras) para este ejercicio. Así que la probabilidad de tomar 3 bolas blancas en 10 intentos es:

$$\Pr\left(\begin{array}{c}\text{exactamente 3 bolas blancas}\\ \text{n 10 intentos}\end{array}\right) = \frac{\binom{21}{3}\binom{79}{7}}{\binom{100}{10}} = \frac{20271005}{91015876} \approx 0.223$$

CIMAT

Definición

Una tómbola contiene N bolas, de las cuales m son blancas, y $N - m$ son negras. De esta colección, n bolas son seleccionadas aleatoriamente sin reemplazo. Sea X el número de bolas blancas seleccionadas. Entonces X es una variable aleatoria que toma los siguientes valores enteros:

$$0 \leq X(\omega) \leq \min(m, n).$$

Por lo que la función de densidad de la variable X es:

$$f_X(j) = \Pr(X = j) = \frac{\binom{m}{j}\binom{N-m}{n-j}}{\binom{N}{m}}$$

Esta es llamada la *función de densidad hipergeométrica*.

CIMAT

Definición

Sean X Y dos variables aleatorias. La *función de densidad con junta de X y Y*, denotada por $f_{X,Y}(x, y)$, es la probabilidad de que X tome el valor de x, y que Y tome el valor de y. Así que

$$f_{X,Y}(x, y) = \Pr(X = x \text{ y } Y = y)$$

(para el evento $\{w \in \Omega : X(\omega) = x\}$, y $Y(\omega) = y\}$)

...

Similarmente,

Definición

La *función de densidad condicional*, denotada por $f_{X|Y}(x|y)$, es la probabilidad de que X tome el valor x, si la Y toma el valor de y:

$$f_{X|Y}(x, y) = f_X(x) f_Y(y) \forall x, y.$$

Esto es equivalente a los eventos $\{X = x\}$ y $\{Y = y\}$ si son independientes en el sentido de que $\Pr(X \cap Y) = \Pr(X) \cdot \Pr(Y)$.

Ejemplo

Se tiene una tómbola con cuatro monedas de oro, y tres de plata. Se toma una moneda al azar, se examina, y se regresa; se toma una segunda moneda al azar, se examina, y se regresa. Sea X el número de monedas de oro sacadas, y Y el número de monedas de plata sacadas.

Para encontrar la función de densidad conjunta $f_{X,Y}(x, y)$, se necesita calcular el evento $\{X = x, Y = y\}$. Sea

$$F = \begin{cases} 1 & \text{si primero es de oro} \\ 0 & \text{si primero es de plata} \end{cases} \qquad S = \begin{cases} 1 & \text{si después es de oro} \\ 0 & \text{si después es de plata} \end{cases}$$

...

Note que $X = F + S$, y $Y = 2 - X = 2 - F - S$. Los eventos F y S son independientes y $\Pr(F = 1) = \Pr(S = 1) = \frac{4}{7}$. Se calcula la función $f_{X,Y}(1, 2)$ como sigue:

$$\begin{aligned} f_{X,Y}(1,1) &= \Pr(X = 1, Y = 1) \\ &= \Pr(F = 1, S = 0) + \Pr(F = 0, S = 1) \\ &= \Pr(F = 1) \cdot \Pr(S = 0) + \Pr(F = 0) \cdot \Pr(S = 1) \\ &= \frac{4}{7} \cdot \frac{3}{7} + \frac{3}{7} \cdot \frac{4}{7} = \frac{24}{49} \approx 0.4898. \end{aligned}$$

En otras palabras, la probabilidad de sacar una moneda de oro y una de plata es de 0.4898.

¿Cómo afectarían a los cálculos el hecho de que no se reemplace la primera moneda?

Ahora, la probabilidad de sacar plata en la segunda depende de qué se sacó en la primera:

$$\begin{aligned} f_{X,Y}(1,1) &= \Pr(X=1, Y=1) \\ &= \Pr(F=1, S=0) + \Pr(F=0, S=1) \\ &= \Pr(S=0|F=1)\cdot\Pr(F=1) + \Pr(S=1|F=0)\cdot\Pr(F=0) \\ &= \frac{3}{6}\cdot\frac{4}{7} + \frac{4}{6}\cdot\frac{3}{7} = \frac{4}{7} \approx 0.5714. \end{aligned}$$

En otras palabras, la probabilidad de sacar una moneda de oro y una de plata es un poco mayor si las monedas no son devueltas a las tómbolas.

Fórmula de Bayes con variables

Sean X, y Y dos variables aleatorias, y asumiendo que $f_Y(y) > 0$:

$$f_{X|Y}(x, y) = \frac{f_X(x) f_{Y|X}(y|x)}{f_Y(y)}.$$

Si X y Y son independientes $\Leftrightarrow f_{X|Y}(x|y) = f_X(x) \quad \forall x, y$

Definición

Una familia de dos o o más variables aleatorias $\{X_1, X_2, \ldots, X_n\}$ es *independiente* si los eventos

$$\{X_1 = x_1, X_2 = x_2, \ldots X_n = x_n\}$$

son independientes para cada valor de $x_1, x_2, \ldots, x_n$.

Valor esperado

El *valor esperado* de una variable aleatoria X es el promedio de sus valores posibles respecto a la probabilidad de su ocurrencia. Esto nos da una idea de su comportamiento.

Definición

Sea X una variable aleatoria que toma los valores $x_1, x_2, \ldots, x_n$. El *valor esperado* (o *media*) de X es la cantidad:

$$E(X) = \sum_{i=1}^{n} x_i \cdot f_X(x_i) = \sum_{i=1}^{n} x_i \cdot \Pr(X = x_i).$$

Ejemplo

Sea X una variable aleatoria cuyo valor es la suma de los números que resulten de tirar dos dados. Los posibles valores de X caen en el rango de $2 \ldots 12$,

$$E(X) = \sum_{i=2}^{12} i \cdot \Pr(X = i).$$

Hay 36 maneras de que caigan dos dados. La probabilidad de que $X = i$ es de $\frac{1}{36}$ veces la manera de obtener i, quedando:

$$\begin{aligned} E(X) &= 2 \cdot \frac{1}{36} + 3 \cdot \frac{2}{36} + 4 \cdot \frac{3}{36} + 5 \cdot \frac{4}{36} + 6 \cdot \frac{5}{36} + 7 \cdot \frac{6}{36} \\ &\quad + 8 \cdot \frac{5}{36} + 9 \cdot \frac{4}{36} + 10 \cdot \frac{3}{36} + 11 \cdot \frac{2}{36} + 12 \cdot \frac{1}{36} \\ &= 7. \end{aligned}$$

CIMAT

Definición

El número esperado de éxitos en una secuencia de n intentos independientes de Bernoulli, con probabilidad p de éxitos en cada intento es np. La varianza de el número de éxitos es $np(1-p)$.

Ley de números largos

Sea X una variable aleatoria denotando la fracción de éxitos en n intentos independientes de Bernoulli, con probabilidad p de éxito en cada intento. Para cada $\epsilon > 0$:

$$P(|X - p| > \epsilon) \to 0, \text{ as } n \to \infty$$

En otras palabras, mientras n crezca, la proporción de éxitos se debería de acercar a p (la probabilidad de éxito en cada intento)

Contenido de la sección 6

Sea S el espacio de muestra con una distribución de probabilidad P.

Definición

Una *variable aleatoria* X es una función del espacio de muestra S a el conjunto de los números reales; para cada evento simple $s_i \in S$, X asigna un número real $X(s_i)$.

Dado que S se considera finito, X sólo puede tomar un número finito de valores.

Definición

Sea X una variable aleatoria en S. El *valor esperado* o *media* de X es $E(X) = \sum_{s_i \in S} X(s_i)P(s_i)$

CIMAT

Observación

Sea X una variable aleatoria en S. Entonces
$E(X) = \sum_{x \in \mathbb{R}} x \cdot P(X = x)$

Observación

Si $X_1, X_2, \ldots, X_m$ son variables aleatorias en S, y $a_1, a_2, \ldots, a_m$ son números reales, entonces $E(\sum_{i=1}^{m} a_i X_i) = \sum_{i=1}^{m} a_i E(X_i)$

CIMAT

Definición

La *varianza* de una variable aleatoria X de una media μ es un número no negativo definido por>

$$\text{Var}(X) = E((X - \mu)^2)$$

La *desviación estándar* de X es la raíz cuadrada no negativa de $\text{Var}(X)$.

Si una variable aleatoria tiene poca varianza, entonces grades variaciones de la media podrían no ser observadas...

CIMAT

Inequalidad de Chebyshev

Sea X una variable aleatoria con media $\mu = E(X)$ y una varianza $\sigma^2 = \text{Var}(X)$, entonces para todo $t > 0$:

$$P(|X - \mu| \geq t) \leq \frac{\sigma^2}{t^2}.$$

Entropía

- Sea X una variable aleatoria a partir de un conjunto finito de valores $x_1, x_2, \ldots, x_n$ con probabilidad $P(X = x_i) = p_i$, donde $0 \leq p_i \leq 1$ para cada i, $1 \leq i \leq n$, y donde $\sum_{i=1}^{n} p_i = 1$. Sean Y y Z variables aleatorias con valores dentro de conjuntos finitos.
- La entropía de X es la medida matemática de la cantidad de información proveída por una observación de X. En otras palabras, es la incertidumbre acerca de los resultados a obtener antes de la observación de X. La entropía es útil para aproximar el número promedio de bits requeridos para codificar los elementos de X.

CIMAT

Definición

La *entropía*, o *incertidumbre* de X está definida como: $H(X) = -\sum_{i=1}^{n} p_i \lg p_i = \sum_{i=1}^{n} p_i \lg\left(\frac{1}{p_i}\right)$ en donde, por convención, $p_i \cdot \lg p_i = p_i \cdot \lg\left(\frac{1}{p_i}\right) = 0$, si $p_i = 0$.

Propiedades de la entropía

Sea X una variable aleatorio que produce n valores:

- $0 \leq H(X) \leq \lg n$
- $H(X) = 0$ sí y sólo sí $p_i = 1$ para i, con $p_j = 0$ para todo $j \neq i$ (no hay duda del siguiente valor)
- $H(X) = \lg n$ sí y sólo si $p_i = 1/n$ para todo i con $1 \leq i \leq n$ (todos los valores son igualmente posibles)

CIMAT

Definición

La *entropía conjunta* de X y Y está definida como:

$$H(X,Y) = -\sum_{x,y} P(X=x, Y=y)\lg(P(X=x, Y=y))$$

en donde los índices x y y de la suma pasan por todos los valores de X y Y respectivamente.

Observación

Si X y Y son variables alreatorias, entonces $H(X,Y) \leq H(X) + H(Y)$ y viceversa, sí y sólo sí X y Y son independientes.

CIMAT

Definición

Si X, Y son variables aleatorias, la *entropía condicional de X dado Y = y* es:

$$H(X|Y=y) = -\sum_{x} P(X=x|Y=y)\lg(P(X=x|Y=y))$$

en donde el índice x de la suma toma todos los valores de X.

La *entropía condicional de X dado Y* también conocida como la *equivocación de Y acerca de X* es:

$$H(X|Y) = \sum_{y} P(Y=y)H(X|Y=y)$$

en donde el índice y de la suma toma todos los valores de Y.

CIMAT

Propiedades de la entropía condicional

Sean X y Y variables aleatorias:

- $H(X|Y)$ mide la cantidad de incertidumbre restante de X después de que Y ha sido observado
- $H(X|Y) \geq 0$, y $H(X|X) = 0$
- $H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
- $H(X|Y) \leq H(X)$, con equalidad sí y sólo sí X y Y son independientes

CIMAT

Definición

La *información mutua* o *transinformación* de las variables aleatorias X y Y se denota como: $I(X;Y) = H(X) - H(X|Y)$.
Similarlmente, la transinformación de X y la pareja Y y Z se define como: $I(X;Y,Z) = H(X) - H(X|Y,Z)$.

Propiedades de la transinformación mutua

- La cantidad $I(X;Y)$ se puede interpretar como la cantidad de información que Y revela sobre X. Similarmente, $I(X;Y,Z)$ sería la cantidad de información que Y y Z conjuntamente revelan sobre X
- $I(X;Y) \geq 0$
- $I(X;Y) = 0$ sí y sólo si X y Y son independientes (esto es, que Y no revela nada sobre X)
- $I(X;Y) = I(Y;X)$

CIMAT

Definición

La *transinformación condicional* del par X, Y dado Z se define como:

$$I_Z(X;Y) = H(X|Z) - H(X|Y,Z)$$

propiedades de la transinformación condicional

- La cantidad $I_Z(X;Y)$ puede ser interpreatada como la cantidad de información que Y provee acerca de X, una vez que Z ya ha sido observada.
- $I(X;Y,Z) = I(X;Y) + I_Y(X;Z)$
- $I_Z(X;Y) = I_Z(Y;Z)$

Contenido de la sección 7

El principal objetivo de la teoría de la complejidad es proveer de mecanismos para clasificar los problemas computacionales de acuerdo a los recursos necesarios para resolverlos.

Definición

Un *algoritmo* es un procedimiento computacional bien definido que toma una variable de entrada y se detiene con una salida

"Bien definido" es un concepto muy ambigüo. Cuando un algoritmo se desea formalizar, se utilizan máquinas de Turín, máquinas de acceso aleatorio, o circuitería booleana.

Definición

El *tamaño* de la entrada es el número total de nits necesarios para representar la entrada en notación binaria, ya codificada.

Definición

El *tiempo de ejecución* de un algoritmo para una entrada en particular es el número de operaciones primiticas, o “pasos” ejecutados.

Definición

El *tiempo de ejecución en el peor escenario* de un algoritmo es el límite superior del tiempo de ejecución para cualquier valor de entrada, expresado como una función de tamaño de entrada

Definición

El *tiempo de ejecución en el caso promedio* de un algoritmo es el tiempo de ejecución promedio de todas las entradas de un tamaño de entrada fijo, expresado como una función del tamaño de entrada

En algunas ocasiones es difícil estimar el tiempo de ejecución exacto de un algoritmo, por lo que en ocasiones uno hace aproximaciones, y uno termina derivando el tiempo de ejecución *asintótico*; esto es, variando el tiempo de ejecución de acuerdo al tamaño de los datos de entrada.

Notación de orden

- *El límite superior asintótico* $f(n) = \mathcal{O}(g(n))$, si hay una constante positiva c, y un entero positivo n_0 tal que $0 \leq f(n) \leq cg(n)$ para todo $n \geq n_0$
- *El límite inferior asintótico* $f(n) = \Omega(g(n))$, si existe una constante positiva c, y un entero positivo n_0 tal que $0 \leq cg(n) \leq f(n)$ para todo $n \geq n_0$
- *El límite justo asintótico* $f(n) = \Theta(g(n))$, si existen constantes positivas c_1, y $c - 2$, y un entero positivo n_0 tal que $c_1 g(n) \leq f(n) \leq c_2 g(n)$ para todo $n \geq n_0$
- *o-notation* $f(n) = o(g(n))$, si para cualquier constante positiva $c > 0$ existe una constante $n_0 > 0$ tal que $0 \leq f(n), cg(n)$ para todo $n \geq n_0$

CIMAT

Definición

Un *algoritmo de tiempo polinomial* es un algoritmo cuyo tiempo de ejecución en el peor escenario es de la forma $\mathcal{O}(n^k)$, donde n es el tamaño de la entrada, y k es una constante. Cualquier algoritmo cuyo tiempo de ejecución no pueda delimitarse, se considera *algoritmo de tiempo exponencial*

Los algoritmos de tiempo polinomial se definen como *buenos*, o *eficientes*, mientras que los exponenciales como *ineficientes*.

CIMAT

Definición

Un *algoritmo de tiempo sub-exponencial* es un algoritmo cuyo tiempo de ejecución en el peor escenario es de la forma $e^{\mathcal{O}(n)}$, donde n es el tamaño de la entrada

Un algoritmo de tiempo sub-exponencial es asintóticamente más lento que un algoritmo de tiempo polinomial, pero más rápido que un algoritmo de tiempo exponencial.

Definición

La clase de complejidad **P** es el conjunto de problemas decisionales que se pueden resolver en tiempo polinomial

Definición

La clase de complejidad **NP** es el conjunto de problemas decisionales para los cuales un SÍ como respuesta puede verificarse en tiempo polinomial siempre y cuando exista cierta información adicional (llamada *certificado*)

Definición

La clase de complejidad **co-NP** es el conjunto de problemas decisionales para los cuales un NO como respuesta puede verificarse en tiempo polinomial co el certificado apropiado

CIMAT

Observación

$P \subseteq NP$, y $P \subseteq$ co-NP

Preguntas:

- $P \stackrel{?}{=} NP$
- $NP \stackrel{?}{=}$ co-NP
- $P \stackrel{?}{=} NP \cap$ co-NP

Sean L_1, y L_2 tres problemas decisionales...

Definición

Se dice que L_1 reduce polinomialmente a L_2, denotado como $L_1 \leq_{\mathbf{P}} L_2$, si existe un algoritmo que resuelva L_1 utilizando como subrutina, un algoritmo que resuelve L_2, el cual sea de tiempo polynomial tanto para L_1 como para L_2

Definición

Si $L_1 \leq_{\mathbf{P}} L_2$, y $L_2 \leq_{\mathbf{P}} L_1$, entonces L_1 y L_2 son *computacionalmente equivalentes*.

Sean L_1, L_2, y L_3 tres problemas decisionales...

Observaciones

- (transitividad): Si $L_1 \leq_{\mathbf{P}} L_2$, u $L_2 \leq_{\mathbf{P}} L_3$, entonces $L_1 \leq_{\mathbf{P}} L_3$
- Si $L_1 \leq_{\mathbf{P}} L_2$, y $L_2 \in \mathbf{P}$, entonces $L_1 \in \mathbf{P}$.

Definición

Se dice que un problema decisional L es **NP**-*completo* si:

- $L \in$**NP**, y
- $L_1 \leq_{\mathbf{P}} L$ para cada $L_1 \in$**NP**

La clase que agrupa a todos los problemas **NP**-completos se denota como **NPC**. Dicha clase agrupa a los problemas más difíciles, ya que son cuando menos tanto como otros problemas **NP**

CIMAT

Observaciones

- Si L_1 es **NP**-completo, y $L_1 \in \mathbf{P}$, entonces $\mathbf{P} = \mathbf{NP}$
- Si $L_1 \in \mathbf{NP}$, L_2 is **NP**-completo, y $L_2 \leq L_1$, entonces L_1 también es **NP**-completo
- Si L_1 es **NP**-completo, y $L_1 \in \mathbf{co\text{-}NP}$, entonces $\mathbf{NP} = \mathbf{co\text{-}NP}$

Definición

Un problema es **NP**-duro si existe algún problema **NP**-completo que lo reduzca a tiempo polinomial.

Tiempos de complejidad

CIMAT

Descripción	Notación	Ejemplo
Tiempo constante	$\mathcal{O}(1)$	Determinar si un entero es par
T. Logarítmico	$\mathcal{O}(\log n)$	Búsqueda binaria
T. Linear	$\mathcal{O}(n)$	Buscar un elemento en una lista
T. linearitmico	$\mathcal{O}(n\log n)$	Método quicksort
T. quadrático	$\mathcal{O}(n^2)$	Método de la burbuja
T. cúbico	$\mathcal{O}(n^3)$	Multiplicación de 2 matrices $n \times n$
T. polinomial	$2^{\mathcal{O}(\log n)}$	Pruebas de primalidad
T. exponencial	$2^{\mathcal{O}(n)}$	Problema del vendedor viajero
T. factorial	$2^{\mathcal{O}(n!)}$	... por fuerza bruta

- Fin de la unidad 1