Clase 1: preliminares matemáticos I

Fernando Virdia, versión: 0.0.1, junio 2024

1 Preliminares

1.1 Números y conjuntos

Usamos $\mathbb{Z}_{>0}$ para representar el conjunto de Números enteros positivos $\{1, 2, 3, \dots\}$. Dado $n \in \mathbb{Z}_{>0}$, denotamos con $[n]$ el conjunto $\{1, 2, \dots, n\}$.
Usamos $\emptyset$ para representar el conjunto vacío, $\emptyset = \{\ \}$. Usamos $|S|$ para representar la cardinalidad de S.
Dado un valor lógico V definimos $[\![V]\!] \coloneqq 1$ si V es verdadero, y $[\![V]\!] \coloneqq 0$ si V es falso.
Dados dos bits $b, c \in \{0, 1\}$, escribimos $b \oplus c = b$ `XOR` $c = [\![b \neq c]\!] = \begin{cases} 0 & \text{si } b = c, \\ 1 & \text{si } b \neq c. \end{cases}$
Usamos $\{0,1\}^\ell$ para representar el conjunto de cadenas de ℓ bits. Si $\ell = *$, las cadenas pueden ser arbitrariamente largas. Dada una cadena de bits c, denotamos $|c|$ el numero de bits en c.
Si $b = b_1 b_2 \dots b_n$ y $c = c_1 c_2 \dots c_n$ son dos cadenas de n bits, escribimos $b \oplus c$ para representar la cadena $d = d_1 d_2 \dots d_n$ donde $d_i = b_i \oplus c_i$.

Lemma 1 (Desigualdad triangular) *Dados $x, y \in \mathbb{R}$, $|x + y| \leq |x| + |y|$.*

1.2 Probabilidad

Dado un conjunto finito S, usamos $U(S)$ para representar la distribución de probabilidad uniforme sobre S. Una variable aleatoria X distribuida según $U(S)$, $X \sim U(S)$, es tal que

$$\Pr[X = x] = \frac{1}{|S|} \quad \forall x \in S.$$

Dado un segundo conjunto S', y una función $f \colon S \to S'$, podemos definir una secunda variable aleatoria $Y = f(X)$. La distribución de Y no es necesariamente la misma de X. A veces escribimos

$$\Pr_{X \sim U(S)}[Y = y]$$

para indicar $\Pr[Y = y] = \Pr[f(X) = y]$ cuando $X \sim U(S)$.
Dadas dos variable aleatorias A y B, la *probabilidad condicional* de $A = a$ dado $B = b$ puede definirse de varias maneras. En este curso consideramos $\Pr[A = a \mid B = b]$ como la probabilidad que $A = a$ asumido que ya se sabe que $B = b$ (por ejemplo, A podría ser el resultado de un experimento, donde B determina parte de la aleatoriedad del mismo). Se mantiene que si $\Pr[B = b] > 0$,

$$\Pr[A = a \mid B = b] = \frac{\Pr[A = a \wedge B = b]}{\Pr[B = b]}.$$

Dados eventos $A = a$ y $B = b$:

- $\Pr[A \neq a] = 1 - \Pr[A = a]$,
- $\Pr[A = a \mid B = b] = 1 - \Pr[A \neq a \mid B = b]$.[1]

Teorema 1 (Teorema de la probabilidad total, informal) *Dada una variable aleatoria B con valores en un conjunto finito S, podemos descomponer el evento $A = a$ como*

$$\begin{aligned} \Pr[A = a] &= \sum_{b \in S} \Pr[A = a \wedge B = b] \\ &= \sum_{b \in S} \Pr[A = a \mid B = b] \cdot \Pr[B = b]. \end{aligned}$$

Lemma 2 (Union bound, cota de la unión) *Dados eventos $A_1, \dots, A_n$,*

$$\Pr[A_1 \vee A_2] \leq \Pr[A_1] + \Pr[A_2], \text{ e iterando, } \Pr\left[\bigvee_{i=1}^{n} A_i\right] \leq \sum_{i=1}^{n} \Pr[A_i].$$

[1] Demostración: $1 = \frac{\Pr[B=b \wedge A=a] + \Pr[B=b \wedge A \neq a]}{\Pr[B=b]} = \Pr[A = a \mid B = b] + \Pr[A \neq a \mid B = b]$.

1.3 Aleatoriedad

Postulado 1 *Dado un conjunto finito R, podemos tomar muestras r_i de la distribución uniforme sobre R, $r_i \sim U(R)$.*

Comentario 1 *Generalmente consideramos $R = \{0,1\}^n$ con $n \in \mathbb{Z}_n$.*

Comentario 2 *Generalmente, llamamos una tal muestra $r_i \sim U(R)$,* monedas *("coins"). A veces escribimos $r_i \xleftarrow{\$} R$.*

Definición 1 (Algoritmo aleatorio) *Sea $\mathcal{A}$ un algoritmo con conjunto de inputs I y conjunto de outputs O. Decimos que $\mathcal{A}$ es aleatorio si dado $x \in I$, $\mathcal{A}(x)$ es una variable aleatoria con valor $\mathcal{A}(x) \in O$.*

En criptografía, definimos la variante "de-randomizada" $\overline{\mathcal{A}}$ de $\mathcal{A}$ como la función $\overline{\mathcal{A}}\colon I \times R \to O$ tal que

$$\forall y \in O, \quad \Pr[A(x) = y] = \Pr_{r \sim U(R)}[\overline{\mathcal{A}}(x, r) = y].$$

Generalmente abusamos notación y escribimos $\mathcal{A}(x; r)$ en lugar de $\overline{\mathcal{A}}(x, r)$.

En criptografía trabajamos con "adversarios" que interceptan comunicaciones e intentan vulnerarlas de varias maneras. Estos adversarios son modelados como algoritmos aleatorios, que corren en tiempo $\leq t$. En criptografía a menudo argumentamos que dos variables aleatorias tienen una distribución muy "parecida". A través del siguiente teorema, eso nos permite de prever los logros de un adversario.

Teorema 2 (Informal, "data processing inequality") *Dadas dos variables aleatorias X, Y con distribución "parecidas", y dada una función o algoritmo aleatorio $\mathcal{A}$, las variables aleatorias $\mathcal{A}(X)$, $\mathcal{A}(Y)$ "se parecen" al menos cuanto X e Y.*

Definición 2 (función aleatoria) *Sea $\mathcal{D}$ un conjunto, y $\mathcal{R}$ un conjunto finito. Decimos que $f\colon \mathcal{D} \to \mathcal{R}$ es una función aleatoria, si cada salida $f(x)$ fue muestreada aleatoriamente en $\mathcal{R}$.*

Generalmente, f puede ser realizada a través de la siguiente maquina de estados.

```
f(x)
1 : if L = ⊥ :
2 :     L ← [ ]   // una tabla hash
3 : if x ∉ L :
4 :     L[x] ≔ y ←$ R
5 : return L[x]
```

Si $\mathcal{D}$ es un conjunto finito, esta definición coincide con la de una función muestreada uniformemente del conjunto (finito) $\{f \mid f\colon \mathcal{D} \to \mathcal{R}\}$ de funciones de $\mathcal{D}$ a $\mathcal{R}$.

Comentario 3 (Algoritmos "eficientes") *Durante este curso vamos a ver varios algoritmos usados para cifrar y autenticar datos. Aunque no los tratamos de manera asintótica, vamos a requerir implícitamente que estos algoritmos sean eficientes. Cifrado y autenticado generalmente tardan tiempo proporcional a $|input|$. Para un input de pocos bits, estas operaciones suelen tardar pocos milisegundos o menos (en Linux, corran* `openssl speed` *para ver un ejemplo).*