信息安全技术

离散概率基础

U: finite set (e.g. $U = \{0,1\}^n$)

Def: **Probability distribution** P over U is a function $P: U \longrightarrow [0,1]$

such that $\sum_{x \in U} P(x) = 1$

Examples:

1. **<u>Uniform distribution</u>**: for all $x \in U$: $P(x) = 1/|U|$
2. Point distribution at x_0: $P(x_0) = 1$, $\forall x \neq x_0$: $P(x) = 0$

Distribution vector: (P(000), P(001), P(010), … , P(111))

Events

- For a set $A \subseteq U$: $\Pr[A] = \sum_{x \in A} P(x) \in [0,1]$

- The set A is called an **event**

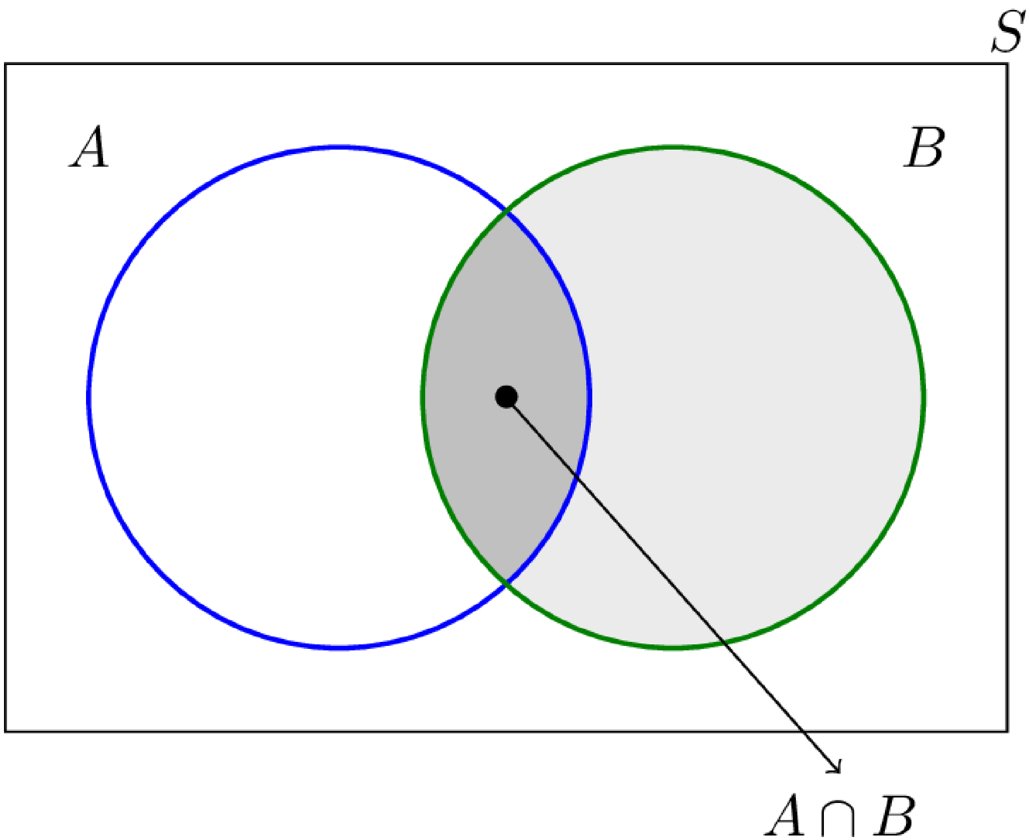
note: $\Pr[U]=1$

Example: $U = \{0,1\}^8$

- $A = \{$ all x in U such that $\mathrm{lsb}_2(x)=11$ $\} \subseteq U$

for the uniform distribution on $\{0,1\}^8$: $\Pr[A] = 1/4$

Conditional Probability



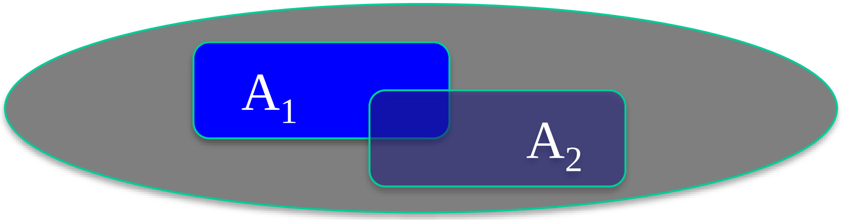
$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

The union bound

- For events A_1 and A_2

$$\Pr[\, A_1 \cup A_2 \,] \le \Pr[A_1] + \Pr[A_2]$$

$A_1 \cap A_2 = \phi \Rightarrow \Pr[A_1 \cup A_2] = \Pr[A_1] + \Pr[A_2]$



Example:

$A_1 = \{$ all x in $\{0,1\}^n$ s.t $lsb_2(x)=11$ $\}$;

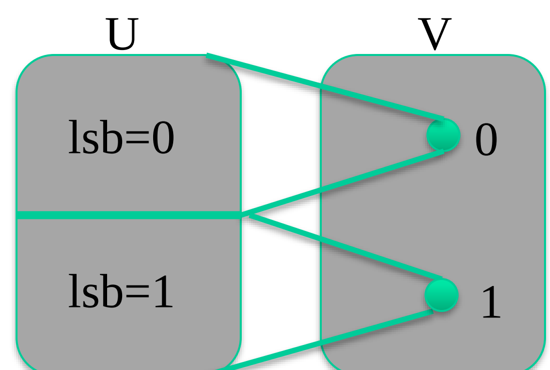
$A_2 = \{$ all x in $\{0,1\}^n$ s.t. $msb_2(x)=11$ $\}$

$\Pr[\, lsb_2(x)=11$ or $msb_2(x)=11 \,] = \Pr[A_1 \cup A_2] \le \frac{1}{4}+\frac{1}{4} = \frac{1}{2}$

Random Variables

Def: a random variable **X** is a function $\mathbf{X}: U \longrightarrow V$

Example: $\mathbf{X}: \{0,1\}^n \longrightarrow \{0,1\}$; $\mathbf{X}(y) = \text{lsb}(y) \in \{0,1\}$



For the uniform distribution on U:

$$\Pr[\,X=0\,] = 1/2\,, \quad \Pr[\,X=1\,] = 1/2$$

More generally:

rand. var. **X** induces a distribution on V: $\Pr[\,X=v\,] := \Pr[\,X^{-1}(v)\,]$

The uniform random variable

Let U be some set, e.g. $U = \{0,1\}^n$

We write $r \xleftarrow{R} U$ to denote a **uniform random variable** over U

$$\text{for all } a \in U: \quad \Pr[\, r = a \,] = 1/|U|$$

(formally, r is the identity function: $r(x)=x$ for all $x \in U$)

Let r be a uniform random variable on $\{0,1\}^2$

Define the random variable $X = r_1 + r_2$

Then $\Pr[X=2] = 1/4$

Hint: $\Pr[X=2] = \Pr[\ r=11\ ]$

Randomized algorithms

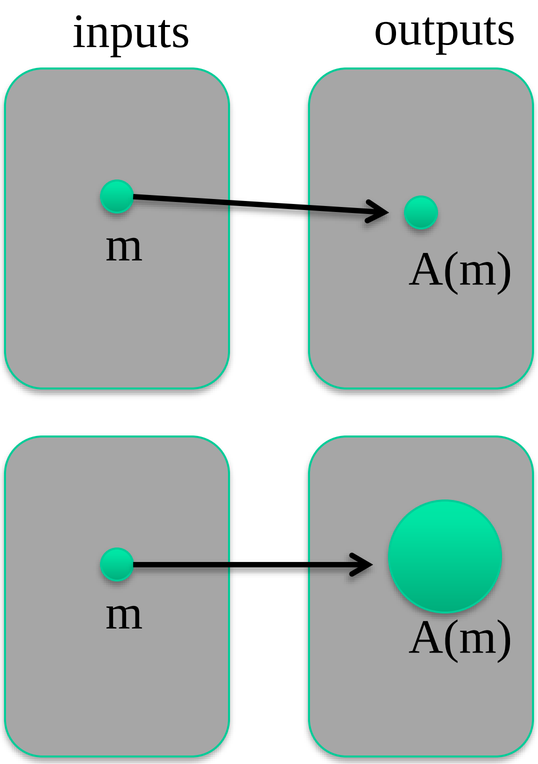
- Deterministic algorithm: $y \leftarrow A(m)$

- Randomized algorithm

  $y \leftarrow A(\, m \,;\, r \,)$ where $r \xleftarrow{R} \{0,1\}^n$

  output is a random variable

  $$y \xleftarrow{R} A(\, m \,)$$



Example: $A(m\,;\,k) = E(k, m),\ y \xleftarrow{R} A(\, m \,)$