See also: http://en.wikibooks.org/High_School_Mathematics_Extensions/Discrete_Probability

Introduction

Discrete Probability (crash course)

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. Uniform distribution: 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: $\big(P(000), P(001), P(010), \ldots, P(111) \big)$

Events

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

note: $\Pr[U]=1$

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

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

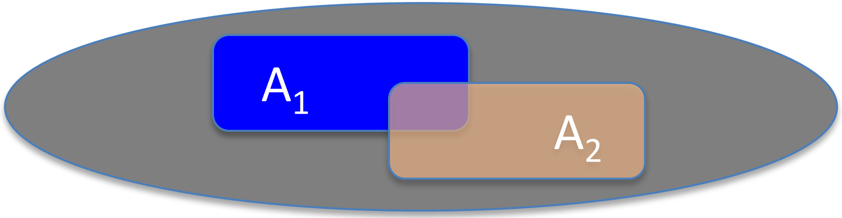
- $A = \{$ all x in U such that $\text{lsb}_2(x)=11$ $\} \subseteq U$

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

The union bound

- For events A_1 and A_2

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



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. $msb_2(x)=11$ $\}$

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

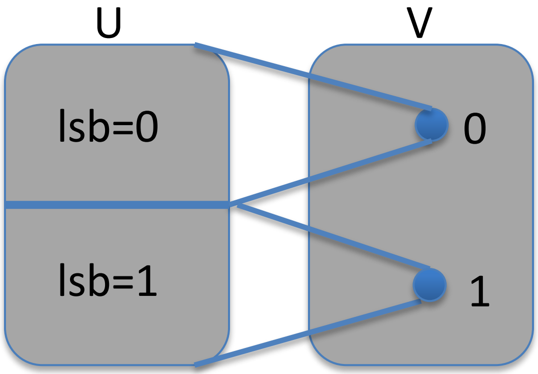
Random Variables

Def: a random variable X is a function $X:U \longrightarrow V$

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

For the uniform distribution on U:

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



More generally:

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

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

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

(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 $\Pr[X=2] =$

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

Randomized algorithms

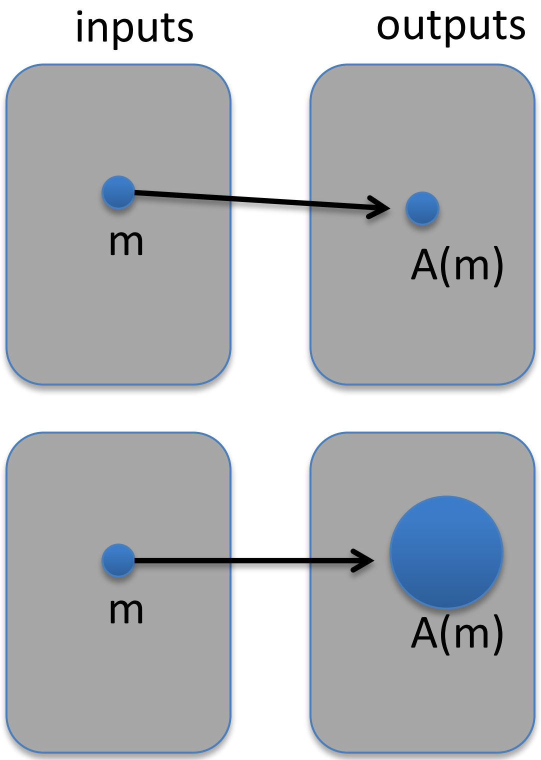
- Deterministic algorithm: $y \longleftarrow A(m)$

- Randomized algorithm

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

  output is a random variable

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



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

End of Segment