h



Introduction



Discrete Probability

(crash course, cont.)

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

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

such that Σ P(x) = 1

x∈U

Examples:

1. Uniform distribution: for all x∈U: P(x) = 1/|U|

2. Point distribution at x0: P(x0) = 1, ∀x≠x0: P(x) = 0

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

Events

• For a set A ⊆ U: Pr[A] = Σ P(x) ∈ [0,1]

x∈A

note: Pr[U]=1

• The set A is called an **event**

**Example:** U = {0,1}8

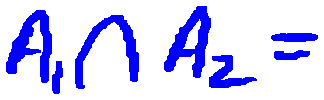
• A = { all x in U such that lsb2(x)=11 } ⊆ U

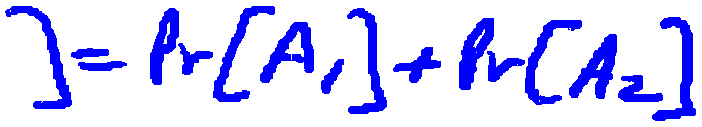
for the uniform distribution on {0,1}8 : Pr[A] = 1/4

The union bound

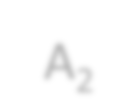
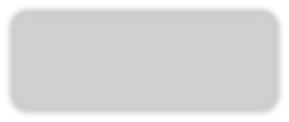
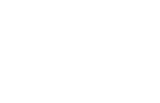
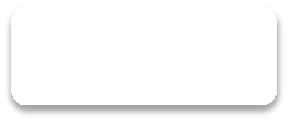
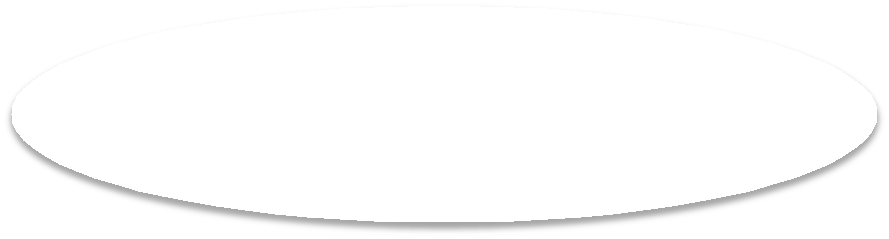
• For events A1 and A2

Pr[ A1 ∪ A2 ] ≤ Pr[A1] + Pr[A2]





A1



A2

**Example:**

A1 = { all x in {0,1}n s.t lsb2(x)=11 } ; A2 = { all x in {0,1}n s.t. msb2(x)=11 }

Pr[ lsb2(x)=11 or msb2(x)=11 ] = Pr[A1∪A2] ≤ ¼+¼ = ½

Random Variables

Def: a random variable X is a function X:U⟶V

Example: X: {0,1}n ⟶ {0,1} ; X(y) = lsb(y) ∈{0,1}

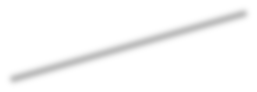
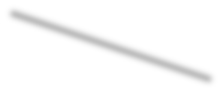
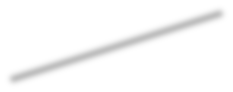
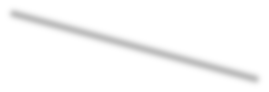
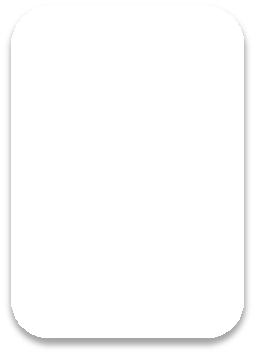
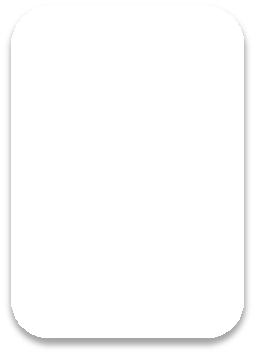
For the uniform distribution on U:

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

More generally:

U V

lsb=0 0



lsb=1 1

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 ⟵R

U to denote a  **uniform random variable** over U

for all a∈U: Pr[ r = a ] = 1/|U|

( formally, r is the identity function: r(x)=x for all x∈U )

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

Define the random variable X = r1 + r2

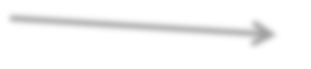
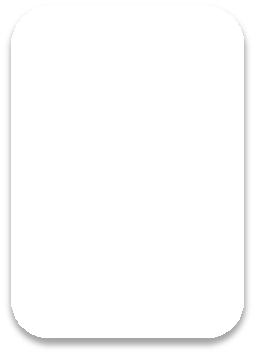
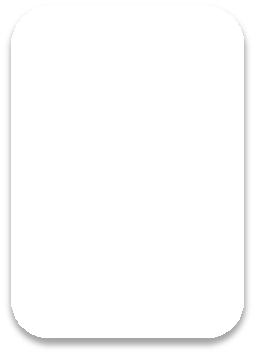
Then Pr[X=2] = ¼

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

Randomized algorithms

inputs outputs

m

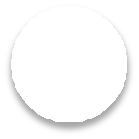
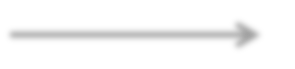
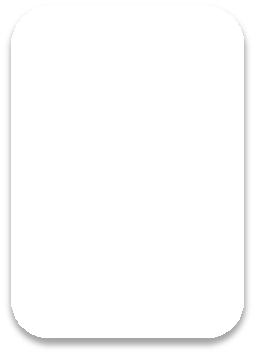
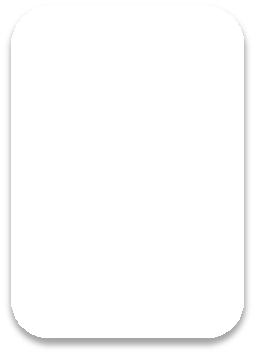


• Deterministic algorithm: y ⟵ A(m)

• Randomized algorithm

y ⟵ A( m ; r ) where r ⟵R

{0,1}n



A(m)

output is a random variable

y ⟵R

A( m )

m A(m)

Example: A(m ; k) = E(k, m) , y ⟵R

A( m )