Randomness in Computer Science

-
-
-
-
-
-
-
-

Randomized Algorithms at a High Level

How can randomness be used in computation?

Given some algorithm that solves a problem:

1.
2.

A randomized algorithm is an algorithm that

Deterministic vs Randomized

Deterministic

```
def A(x):
    y = 1
    if(y == 0):
        while(x > 0):
            x = x - 1
    return x+y
```

Randomized

```
def A(x):
    y = Bernoulli(0.5)
    if(y == 0):
        while(x > 0):
            x = x - 1
    return x+y
```

For any fixed input x (e.g. $x = 3$):

A **deterministic algorithm** A computes $f : \Sigma^* \to \Sigma^*$ in time $T(n)$ if

-
-

What is the corresponding definition for randomized algorithm?

$\forall x \in \Sigma^*$

		Correctness	Run-time
Deterministic			
Randomized	Type 0		
	Type 1		
	Type 2		
	Type 3		

Battleship Example
Input: An array B with $n/4$ 1's and $3n/4$ 0's.
Output: An index that contains a 1.

```
for i = 1 to n:
    if B[i] = 1:
        return i
```

```
repeat 500 times:
    i = RandInt(n)
    if B[i] = 1:
        return i
return "Failed"
```

```
repeat:
    i = RandInt(n)
    if B[i] = 1:
        return i
```

for all inputs

	Correctness	Run-time
Deterministic		
Monte Carlo		
Las Vegas		

Formal Definitions

Deterministic Algorithm

Let $f : \Sigma^* \to \Sigma^*$ be a computational problem. We say that a deterministic algorithm A computes f in time $T(n)$ if:

Picture:

Monte Carlo Algorithm
Let $f : \Sigma^* \to \Sigma^*$ be a computational problem. We say that a randomized algorithm A is a $T(n)$-time Monte Carlo algorithm for f with ϵ error probability if:

Picture:

Las Vegas Algorithm
Let $f : \Sigma^* \to \Sigma^*$ be a computational problem. We say that a randomized algorithm A is a $T(n)$-time Las Vegas algorithm for f if:

Picture:

Other Examples

Integer Factoring

isPrime

```
def isPrime(N):
    if (N < 2):  return False
    maxFactor = round(N**0.5)
    for factor in range(2, maxFactor+1):
        if (N % factor == 0):  return False
    return True
```

Generating a (random) n-bit prime