



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Algorithms (PhD Course)

Mohammad Farshi

Department of Computer Science,
Yazd University

1394-2



Randomized Algorithms



Prerequisites

What is Randomized Algorithms about?

Prerequisites:



Randomized
Algorithms

What you need to know:

- **Basic Algorithms and Algorithm Analysis:** $\mathcal{O}$, Θ notations, sorting, searching.
- **Basic Data Structures:** Priority Queue (Heap), Binary Search Tree, ... and their analysis.
- **Basic Probability theory:** Expected value, ...

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?



Prerequisites:



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

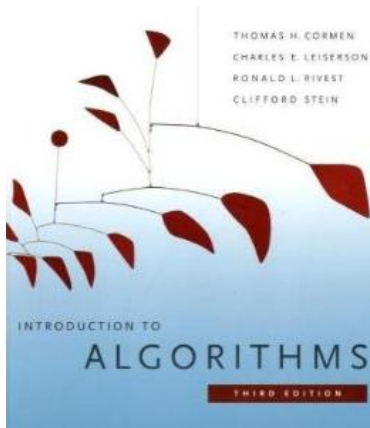
Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?





دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Introduction



What is Randomized Algorithms about?



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Algorithms

Applying randomness to:

- designing algorithms that are very fast in most cases, but slow in very rare cases (in comparison to deterministic algorithms).
- designing algorithms that are very fast, but in most cases the output of the algorithm is true, but in some rare cases the output is false.
- prove deterministic results (existence of something)
- get rid of the adversary, or make the algorithm independent to the shape of input.



What is Randomized Algorithms about?



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Algorithms

Applying randomness to:

- designing algorithms that are very fast in most cases, but slow in very rare cases (in comparison to deterministic algorithms).
- designing algorithms that are very fast, but in most cases the output of the algorithm is true, but in some rare cases the output is false.
- prove deterministic results (existence of something)
- get rid of the adversary, or make the algorithm independent to the shape of input.



What is Randomized Algorithms about?



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Algorithms

Applying randomness to:

- designing algorithms that are very fast in most cases, but slow in very rare cases (in comparison to deterministic algorithms).
- designing algorithms that are very fast, but in most cases the output of the algorithm is true, but in some rare cases the output is false.
- prove deterministic results (existence of something)
- get rid of the adversary, or make the algorithm independent of the shape of input.



What is Randomized Algorithms about?



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Algorithms

Applying randomness to:

- designing algorithms that are very fast in most cases, but slow in very rare cases (in comparison to deterministic algorithms).
- designing algorithms that are very fast, but in most cases the output of the algorithm is true, but in some rare cases the output is false.
- prove deterministic results (existence of something)
- get rid of the adversary, or make the algorithm independent to the shape of input.



What is Randomized Algorithms about?



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Applications

- designing practical algorithms (very simple to implement, very fast in practice),
- make complicated problems very easy,
- an step forward to a deterministic algorithm for a problem,
- proving the existence of something (if the probability of an event is non-zero, it can happens),
- and so on.



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

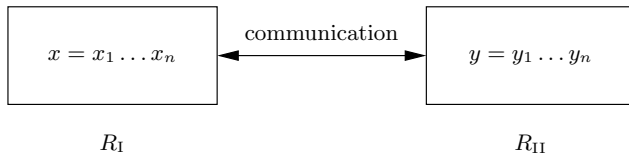
Prerequisites

Introduction

What is Randomized
Algorithms about?

An Example:

- We have two computers R_I and R_{II} that are very far apart.
- At the beginning both have a database with the same content (say, $n = 10^{16}$ bits).
- The contents of these databases dynamically developed simultaneously in both databases.
- After some time, we want to check whether R_I and R_{II} contain the same data.
- **Goal:** Design a communication protocol between R_I and R_{II} to check this.



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

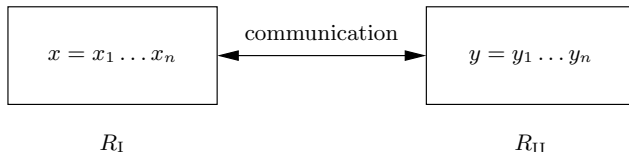
Prerequisites

Introduction

What is Randomized
Algorithms about?

An Example:

- We have two computers R_I and R_{II} that are very far apart.
- At the beginning both have a database with the same content (say, $n = 10^{16}$ bits).
- The contents of these databases dynamically developed simultaneously in both databases.
- After some time, we want to check whether R_I and R_{II} contain the same data.
- **Goal:** Design a communication protocol between R_I and R_{II} to check this.



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

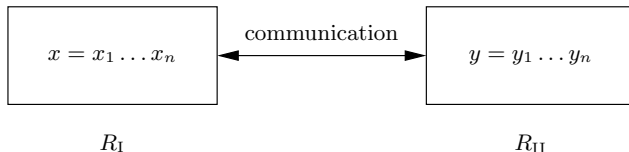
Prerequisites

Introduction

What is Randomized
Algorithms about?

An Example:

- We have two computers R_I and R_{II} that are very far apart.
- At the beginning both have a database with the same content (say, $n = 10^{16}$ bits).
- The contents of these databases dynamically developed simultaneously in both databases.
- After some time, we want to check whether R_I and R_{II} contain the same data.
- **Goal:** Design a communication protocol between R_I and R_{II} to check this.



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

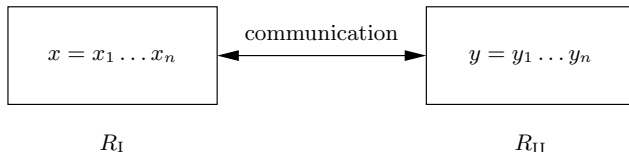
Prerequisites

Introduction

What is Randomized
Algorithms about?

An Example:

- We have two computers R_I and R_{II} that are very far apart.
- At the beginning both have a database with the same content (say, $n = 10^{16}$ bits).
- The contents of these databases dynamically developed simultaneously in both databases.
- After some time, we want to check whether R_I and R_{II} contain the same data.
- **Goal:** Design a communication protocol between R_I and R_{II} to check this.



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

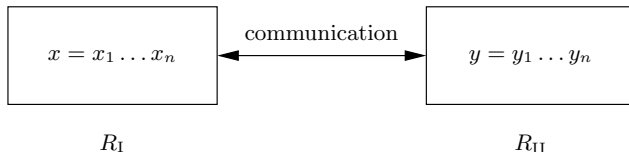
Prerequisites

Introduction

What is Randomized
Algorithms about?

An Example:

- We have two computers R_I and R_{II} that are very far apart.
- At the beginning both have a database with the same content (say, $n = 10^{16}$ bits).
- The contents of these databases dynamically developed simultaneously in both databases.
- After some time, we want to check whether R_I and R_{II} contain the same data.
- **Goal:** Design a communication protocol between R_I and R_{II} to check this.



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

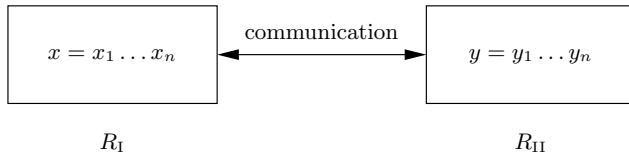
Prerequisites

Introduction

What is Randomized
Algorithms about?

The solution:

- The complexity of the communication protocol = the number of bits exchange between computers.
- There exist no deterministic protocol that solves this task by communicating $< n$ bits.
- Sending $n = 10^{16}$ bits safely is a practically nontrivial task, so one would probably not do it in this way.
- Randomness can help here!



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

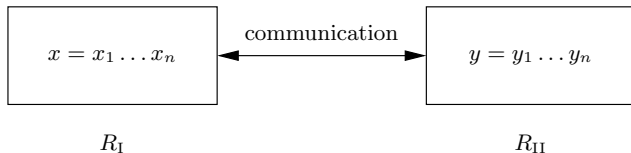
Prerequisites

Introduction

What is Randomized
Algorithms about?

The solution:

- The complexity of the communication protocol = the number of bits exchange between computers.
- There exist no deterministic protocol that solves this task by communicating $< n$ bits.
- Sending $n = 10^{16}$ bits safely is a practically nontrivial task, so one would probably not do it in this way.
- Randomness can help here!



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

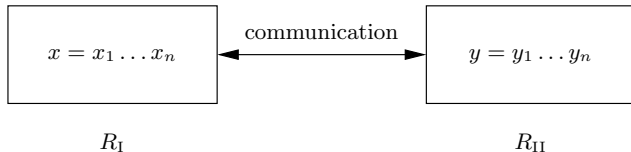
Prerequisites

Introduction

What is Randomized
Algorithms about?

The solution:

- The complexity of the communication protocol = the number of bits exchange between computers.
- There exist no deterministic protocol that solves this task by communicating $< n$ bits.
- Sending $n = 10^{16}$ bits safely is a practically nontrivial task, so one would probably not do it in this way.
- Randomness can help here!



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

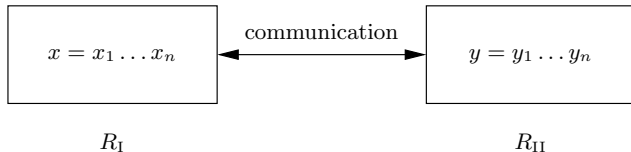
Prerequisites

Introduction

What is Randomized
Algorithms about?

The solution:

- The complexity of the communication protocol = the number of bits exchange between computers.
- There exist no deterministic protocol that solves this task by communicating $< n$ bits.
- Sending $n = 10^{16}$ bits safely is a practically nontrivial task, so one would probably not do it in this way.
- Randomness can help here!



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Protocol for Equality

- Initial situation: R_I has a sequence x of n bits, $x = x_1 \cdots x_n$, and R_{II} has a sequence y of n bits $y = y_1 \cdots y_n$.
- Phase 1: R_I chooses uniformly a prime p from the interval $[2, n^2]$ at random.
- Phase 2: R_I computes the integer $s = \text{Number}(x) \bmod p$ and sends the binary representations of s and p to R_{II} . Observe that $s \leq p < n^2$ and so each of these integers can be represented by $\lceil \log_2 n^2 \rceil$ bits.
- Phase 3: After reading s and p , R_{II} computes the number $q = \text{Number}(y) \bmod p$.
If $q \neq s$, then R_{II} outputs $x \neq y$.
If $q = s$, then R_{II} outputs $x = y$.

Example: Randomized Protocol for Equality



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Protocol for Equality

- Complexity of the protocol: Since $s \leq p < n^2$, the length of the message is $\leq 2\lceil \log_2 n^2 \rceil \leq 4 \log_2 n$. For $n = 10^{16}$, it is 256.
- Reliability (error probability) of the protocol:



Example: Randomized Protocol for Equality

Randomized Protocol for Equality

- Complexity of the protocol: Since $s \leq p < n^2$, the length of the message is $\leq 2\lceil \log_2 n^2 \rceil \leq 4 \log_2 n$. For $n = 10^{16}$, it is 256.
- Reliability (error probability) of the protocol:



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?



Example: Randomized Protocol for Equality



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Protocol for Equality

- Complexity of the protocol: Since $s \leq p < n^2$, the length of the message is $\leq 2\lceil \log_2 n^2 \rceil \leq 4 \log_2 n$. For $n = 10^{16}$, it is 256.
- Reliability (error probability) of the protocol:
The answer of the protocol is not always correct:
For instance, if $x = 01111$ and $y = 10110$, i.e.,
 $Number(x) = 15$ and $Number(y) = 22$, then the
choice of the prime 7 from the set
 $\{2, 3, 5, 7, 11, 13, 17, 19, 23\}$ yields the wrong answer,
because $15 \bmod 7 = 1 = 22 \bmod 7$.



Example: Randomized Protocol for Equality



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Protocol for Equality

- Complexity of the protocol: Since $s \leq p < n^2$, the length of the message is $\leq 2\lceil \log_2 n^2 \rceil \leq 4 \log_2 n$. For $n = 10^{16}$, it is 256.
- Reliability (error probability) of the protocol:

$$PRIM(n^2) = \{p \text{ is a prime} | p \leq n^2\}$$



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

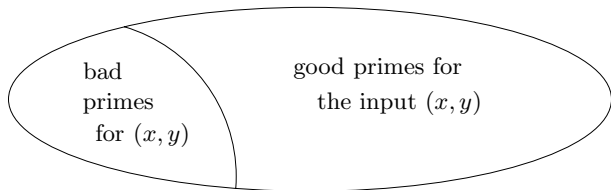
Introduction

What is Randomized
Algorithms about?

Randomized Protocol for Equality

- Complexity of the protocol: Since $s \leq p < n^2$, the length of the message is $\leq 2\lceil \log_2 n^2 \rceil \leq 4 \log_2 n$. For $n = 10^{16}$, it is 256.
- Reliability (error probability) of the protocol:

$$PRIM(n^2) = \{p \text{ is a prime} \mid p \leq n^2\}$$



all primes $\leq n^2$



Example: Randomized Protocol for Equality



دانشگاه یزد
Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

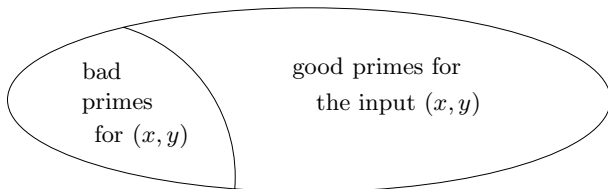
What is Randomized
Algorithms about?

Randomized Protocol for Equality

- Complexity of the protocol: Since $s \leq p < n^2$, the length of the message is $\leq 2\lceil \log_2 n^2 \rceil \leq 4 \log_2 n$. For $n = 10^{16}$, it is 256.
- Reliability (error probability) of the protocol:

$$PRIM(n^2) = \{p \text{ is a prime} \mid p \leq n^2\}$$

$$\text{Error probability for } (x, y) = \frac{\# \text{ bad primes for } (x, y)}{PRIM(n^2)}.$$



all primes $\leq n^2$



Example: Randomized Protocol for Equality



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Protocol for Equality

- Complexity of the protocol: Since $s \leq p < n^2$, the length of the message is $\leq 2\lceil \log_2 n^2 \rceil \leq 4 \log_2 n$. For $n = 10^{16}$, it is 256.
- Reliability (error probability) of the protocol:

$$PRIM(n^2) = \{p \text{ is a prime} | p \leq n^2\}$$

$$\text{Error probability for } (x, y) = \frac{\# \text{ bad primes for } (x, y)}{Prim(n^2)}.$$

$$\text{For } m > 67, Prim(m) > \frac{m}{\log m}.$$



Example: Randomized Protocol for Equality



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Protocol for Equality

- Complexity of the protocol: Since $s \leq p < n^2$, the length of the message is $\leq 2\lceil \log_2 n^2 \rceil \leq 4 \log_2 n$. For $n = 10^{16}$, it is 256.
- Reliability (error probability) of the protocol:

$$PRIM(n^2) = \{p \text{ is a prime} | p \leq n^2\}$$

Error probability for $(x, y) = \frac{\# \text{ bad primes for } (x, y)}{Prim(n^2)}$.

For $m > 67$, $Prim(m) > \frac{m}{\log m}$.

If we show that $\# \text{ bad primes} \leq n - 1$, then the error probability

$$\leq \frac{n - 1}{Prim(n^2)} \leq \frac{n - 1}{n^2 / \log n^2} \leq \frac{\log n^2}{n}.$$

For $n = 10^{16}$, this probability is 0.36892×10^{-14}

Example: Randomized Protocol for Equality

Randomized Protocol for Equality: # bad primes



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

bad primes

- p is a bad prime if $x \neq y$ but

$$\text{Number}(x) \bmod p = \text{Number}(y) \bmod p.$$

i.e. p divides $w = |\text{Number}(x) - \text{Number}(y)|$.

- Let $w = p_1^{i_1} \times p_2^{i_2} \times \cdots \times p_k^{i_k}$ is prime factorization of w ($p_i < p_{i+1}$).
- p_i s are all bad primes.
- **claim:** $k \leq n - 1$. Assume $k \geq n$.

$$\begin{aligned} w &= p_1^{i_1} \times p_2^{i_2} \times \cdots \times p_k^{i_k} \\ &\geq p_1 \times p_2 \times \cdots \times p_k \\ &> 1 \times 2 \times \cdots \times n = n! > 2^n (\text{Contradiction!}) \end{aligned}$$

Example: Randomized Protocol for Equality



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?

Randomized Protocol for Equality

- Reliability (error probability) of the protocol: not satisfying?

- Run the protocol 10 times, the error probability $\leq$

$$\leq \left(\frac{n-1}{\text{Prim}(n^2)} \right)^{10} \leq \left(\frac{n-1}{n^2 / \log n^2} \right)^{10} \leq \frac{2^{10} \log n^{10}}{n^{10}}.$$

For $n = 10^{16}$, this probability is 0.4717×10^{-141}



Example: Randomized Protocol for Equality



دانشگاه یزد

Yazd Univ.

Randomized
Algorithms

Randomized Protocol for Equality

- Reliability (error probability) of the protocol: not satisfying?
- Run the protocol 10 times, the error probability $\leq$

$$\leq \left(\frac{n-1}{\text{Prim}(n^2)} \right)^{10} \leq \left(\frac{n-1}{n^2/\log n^2} \right)^{10} \leq \frac{2^{10} \log n^{10}}{n^{10}}.$$

For $n = 10^{16}$, this probability is 0.4717×10^{-141}

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized
Algorithms about?





دانشگاه یزد

Yazd Univ.

Randomized Algorithms

Course Outline

Textbook

Prerequisites

Introduction

What is Randomized Algorithms about?

