# Discrete Mathematics and Its Applications 2 (CS147)

***Lecture 8: Quick-sort, probability space***

**Fanghui Liu**

Department of Computer Science, University of Warwick, UK

# Why introduce randomness/probability in this course?

Randomness is everywhere!

- randomized algorithms: correct with high probability
- data sampling
- noise

# Why introduce randomness/probability in this course?

Randomness is everywhere!

- randomized algorithms: correct with high probability
- data sampling
- noise

**Problem (Open question in complexity theory)**

*One of the biggest* **open questions** *in complexity theory is*

*whether randomness really helps?*

# Why introduce randomness/probability in this course?

Randomness is everywhere!

- randomized algorithms: correct with high probability
- data sampling
- noise

### Problem (Open question in complexity theory)

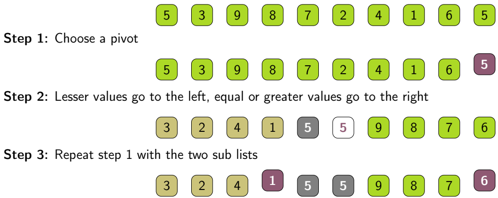
*One of the biggest* **open questions** *in complexity theory is*

*whether randomness really helps?*

- randomized algorithms
- de-randomized techniques

# Quick-sort

- consists of 3 steps:
  - Select a **pivot** from the array
  - partitioning the other elements into two sub-arrays, according to whether they are less than or greater than the pivot.
  - recursively do this: a divide-and-conquer algorithm



# Illustration

5 3 9 8 7 2 4 1 6 5

**Step 1:** Choose a pivot

5 3 9 8 7 2 4 1 6 5

**Step 2:** Lesser values go to the left, equal or greater values go to the right

3 2 4 1 5 5 9 8 7 6

**Step 3:** Repeat step 1 with the two sub lists

3 2 4 1 5 5 9 8 7 6

**Step 4:** Repeat step 2 with the sub lists:

1 3 2 4 5 5 6 9 8 7

**Step 5:** and again and again!

1 3 2 4 5 5 6 9 8 7

1 3 2 4 5 5 6 7 9 8

1 3 2 4 5 5 6 7 9 8

1 2 3 4 5 5 6 7 8 9

1 2 3 4 5 5 6 7 8 9

1 2 3 4 5 5 6 7 8 9

1 2 3 4 5 5 6 7 8 9

# Deterministic Quick-sort algorithm

**Algorithm 1:** Deterministic Quick-sort

**Input:** An array $A[1, 2, \ldots, n]$
**Output:** An sorted array $A[1, 2, \ldots, n]$

pivot $\leftarrow A[n]$ % we can choose any position we want.;
$S_{\text{smaller}} \leftarrow [], S_{\text{larger}} \leftarrow []$;
**for** $i = 1, \ldots, n$ **do**
  **if** $A[i] \leq$ *pivot* **then**
    $S_{\text{smaller.append}}(A[i])$;
  **end**
  **else** $S_{\text{larger.append}}(A[i])$;
**end**
**return** [Quick-sort($S_{\text{smaller}}$, pivot, $S_{\text{larger}}$) ];

# Deterministic Quick-sort algorithm

**Algorithm 1:** Deterministic Quick-sort

**Input:** An array $A[1, 2, \ldots, n]$
**Output:** An sorted array $A[1, 2, \ldots, n]$

pivot $\leftarrow A[n]$ % we can choose any position we want.;
$S_{\text{smaller}} \leftarrow []$, $S_{\text{larger}} \leftarrow []$;
**for** $i = 1, \ldots, n$ **do**
    **if** $A[i] \leq$ *pivot* **then**
        $S_{\text{smaller.append}}(A[i])$;
    **end**
    **else** $S_{\text{larger.append}}(A[i])$;
**end**
**return** [Quick-sort($S_{\text{smaller}}$, pivot, $S_{\text{larger}}$) ];

$$T(n) = T(a) + T(n-a) + \Theta(n)$$

# Running time analysis

**Statement (Worst case $\Theta(n^2)$)**

*If the array is* $\{n, n-1, n-2, \cdots, 2, 1\}$, *a sorted array, then there will be a total of* $\frac{n(n-1)}{2} = \Theta(n^2)$ *comparisons.*

# Running time analysis

**Statement (Worst case $\Theta(n^2)$)**

*If the array is* $\{n, n-1, n-2, \cdots, 2, 1\}$*, a sorted array, then there will be a total of* $\frac{n(n-1)}{2} = \Theta(n^2)$ *comparisons.*

How to improve it?

# Running time analysis

## Statement (Worst case $\Theta(n^2)$)

*If the array is* $\{n, n-1, n-2, \cdots, 2, 1\}$, *a sorted array, then there will be a total of* $\frac{n(n-1)}{2} = \Theta(n^2)$ *comparisons.*

How to improve it?

- How to choose pivot is important!
- Randomly choose it.

## Statement

*Worst-case expected-time bound is* $\Theta(n \log n)$.

We will prove later in this module.

# Recall some knowledge about set theory...

- A set $A$ is **finite** if it has finite elements, e.g., $A = \{a_1, a_2, \cdots, a_n\}$; otherwise it is infinite.

# Recall some knowledge about set theory...

- A set $A$ is **finite** if it has finite elements, e.g., $A = \{a_1, a_2, \cdots, a_n\}$; otherwise it is infinite.
- A set $A$ is **countable** if it has a *bijection* to a subset of $\mathbb{N}$, i.e., it can be “listed"; otherwise it is uncountable.

## Recall some knowledge about set theory...

- A set $A$ is **finite** if it has finite elements, e.g., $A = \{a_1, a_2, \cdots, a_n\}$; otherwise it is infinite.
- A set $A$ is **countable** if it has a *bijection* to a subset of $\mathbb{N}$, i.e., it can be “listed"; otherwise it is uncountable.
- A finite set is always countable. If a set is countably infinite, then it is in the form of $A = \{a_1, a_2, \cdots, a_n, \cdots\}$. Real numbers $\mathbb{R}$ or any interval $[a, b] \in \mathbb{R}$ is uncountable.

# Recall some knowledge about set theory...

- A set $A$ is **finite** if it has finite elements, e.g., $A = \{a_1, a_2, \cdots, a_n\}$; otherwise it is infinite.
- A set $A$ is **countable** if it has a *bijection* to a subset of $\mathbb{N}$, i.e., it can be "listed"; otherwise it is uncountable.
- A finite set is always countable. If a set is countably infinite, then it is in the form of $A = \{a_1, a_2, \cdots, a_n, \cdots\}$. Real numbers $\mathbb{R}$ or any interval $[a, b] \in \mathbb{R}$ is uncountable.
- The **power set** of $A$ is the collection of all of its subsets, i.e., $2^A = \{B : B \subset A\}$.

# Randomness and sample space

- Uncertainty phenomenon: there are some phenomenon that might occur or not.
- Random trial: study the uncertainty phenomenon by some observations and experiments.
- In probability theory, we assume *random trials* can be repeated under the same setting.

## Randomness and sample space

- Uncertainty phenomenon: there are some phenomenon that might occur or not.
- Random trial: study the uncertainty phenomenon by some observations and experiments.
- In probability theory, we assume *random trials* can be repeated under the same setting.

### Definition (Sample space)

One possible outcome of a random trial is a *sample point*, denoted as $\omega$. The set of all possible outcome is called the sample space, denoted as $\Omega$.

**Remark:** the outcome of *random trials* can be different, unpredictable

# Randomness and sample space

- Uncertainty phenomenon: there are some phenomenon that might occur or not.
- Random trial: study the uncertainty phenomenon by some observations and experiments.
- In probability theory, we assume *random trials* can be repeated under the same setting.

## Definition (Sample space)

One possible outcome of a random trial is a *sample point*, denoted as $\omega$. The set of all possible outcome is called the sample space, denoted as $\Omega$.

**Remark:** the outcome of *random trials* can be different, unpredictable

## Example

- toss a coin twice: (head, head), (head, tail), (tail,head), (tail,tail)
- $\Omega = \{HH, HT, TH, TT\}$

# Events

## Definition

We define *event* as a set of outcomes, denoted as $A \subseteq \Omega$. We call an *event* occurs if and only if some sample point(s) included in $A$ occur.

Given a set $A$, we can confirm whether $\omega \in A$ or $\omega \notin A$ for any $\omega \in \Omega$.

# Events

## Definition

We define *event* as a set of outcomes, denoted as $A \subseteq \Omega$. We call an *event* occurs if and only if some sample point(s) included in $A$ occur.

Given a set $A$, we can confirm whether $\omega \in A$ or $\omega \notin A$ for any $\omega \in \Omega$.

## Example

- the results are the same at each time: (head, head),(tail,tail)
- the tail occurs at most once: (head, head), (head, tail), (tail,head)

# Events

## Definition

We define *event* as a set of outcomes, denoted as $A \subseteq \Omega$. We call an *event* occurs if and only if some sample point(s) included in $A$ occur.

Given a set $A$, we can confirm whether $\omega \in A$ or $\omega \notin A$ for any $\omega \in \Omega$.

## Example

- the results are the same at each time: (head, head),(tail,tail)
- the tail occurs at most once: (head, head), (head, tail), (tail,head)

## Example (Experiment with countably infinite outcomes)

Consider an experiment: keep tossing a coin until the head appears.

- countably infinite outcomes: H, TH, TTH, TTTH, $\cdots$
- we're interested in:
  $A_k =$ "H appears exactly in the $k$-th toss"

# Property of events

## Property (using Venn diagram)

*An event is a set!*

- *complement:* $A^c = \{\omega : \omega \notin A\}$
- *union:* $A \cup B = \{\omega : \omega \in A, \text{ or } \omega \in B\}$
- *intersection:* $A \cap B = \{\omega : \omega \in A, \text{ and } \omega \in B\}$
- *difference:* $A - B = \{\omega : \omega \in A, \text{ and } \omega \notin B\}$
- *symmetric difference:* $A \Delta B = (A - B) \cup (B - A)$
- *Event $A$ and $B$ are called disjoint if $A \cap B = \emptyset$.*

**Remark:** Not arbitrary event can be assigned to a probability.

# *$\sigma$ field

When studying random trials, given an event $A$, we know the following **information**

# *$\sigma$ field

When studying random trials, given an event $A$, we know the following **information**

- $A$ occurs $\Rightarrow A^c$ doesn't occur
- if $A_1, A_2, \cdots$ , occur, then $\cup_{i=1}^{\infty} A_i$ occurs.

## *$\sigma$ field

When studying random trials, given an event $A$, we know the following **information**

- $A$ occurs $\Rightarrow$ $A^c$ doesn't occur
- if $A_1, A_2, \cdots$ , occur, then $\cup_{i=1}^{\infty} A_i$ occurs.

### Definition ($\sigma$-field)

$\mathcal{F}$ is a set of events, i.e., a (nonempty) collection of the subsets of $\Omega$. $\mathcal{F}$ is called $\sigma$-field if

- $A \in \mathcal{F}$, then $A^c \in \mathcal{F}$
- $A_i \in \mathcal{F}$, $i = 1, 2, \ldots$, then $\cup_{i=1}^{\infty} A_i \in \mathcal{F}$
- $\emptyset \in \mathcal{F}$

# *$\sigma$ field

When studying random trials, given an event $A$, we know the following **information**

- $A$ occurs $\Rightarrow$ $A^c$ doesn't occur
- if $A_1, A_2, \cdots$ , occur, then $\cup_{i=1}^{\infty} A_i$ occurs.

## Definition ($\sigma$-field)

$\mathcal{F}$ is a set of events, i.e., a (nonempty) collection of the subsets of $\Omega$. $\mathcal{F}$ is called $\sigma$-field if

- $A \in \mathcal{F}$, then $A^c \in \mathcal{F}$
- $A_i \in \mathcal{F}$, $i = 1, 2, \ldots$, then $\cup_{i=1}^{\infty} A_i \in \mathcal{F}$
- $\emptyset \in \mathcal{F}$

**Remark:** $\circ$ $\mathcal{F} = \{\emptyset, \Omega\}$, $\mathcal{F} = \{\emptyset, A, A^c, \Omega\}$, $\mathcal{F} = 2^{\Omega}$ are all $\sigma$-fields.

# *$\sigma$ field

When studying random trials, given an event $A$, we know the following **information**

- $A$ occurs $\Rightarrow$ $A^c$ doesn't occur
- if $A_1, A_2, \cdots$, occur, then $\cup_{i=1}^{\infty} A_i$ occurs.

## Definition ($\sigma$-field)

$\mathcal{F}$ is a set of events, i.e., a (nonempty) collection of the subsets of $\Omega$. $\mathcal{F}$ is called $\sigma$-field if

- $A \in \mathcal{F}$, then $A^c \in \mathcal{F}$
- $A_i \in \mathcal{F}$, $i = 1, 2, \ldots$, then $\cup_{i=1}^{\infty} A_i \in \mathcal{F}$
- $\emptyset \in \mathcal{F}$

**Remark:** ○ $\mathcal{F} = \{\emptyset, \Omega\}$, $\mathcal{F} = \{\emptyset, A, A^c, \Omega\}$, $\mathcal{F} = 2^{\Omega}$ are all $\sigma$-fields.
○ If $A, B \in \mathcal{F}$, then $A \cap B, A - B, A \Delta B \in \mathcal{F}$

# *$\sigma$ field

When studying random trials, given an event $A$, we know the following **information**

- $A$ occurs $\Rightarrow$ $A^c$ doesn't occur
- if $A_1, A_2, \cdots$ , occur, then $\cup_{i=1}^{\infty} A_i$ occurs.

## Definition ($\sigma$-field)

$\mathcal{F}$ is a set of events, i.e., a (nonempty) collection of the subsets of $\Omega$. $\mathcal{F}$ is called $\sigma$-field if

- $A \in \mathcal{F}$, then $A^c \in \mathcal{F}$
- $A_i \in \mathcal{F}$, $i = 1, 2, \ldots$, then $\cup_{i=1}^{\infty} A_i \in \mathcal{F}$
- $\emptyset \in \mathcal{F}$

**Remark:** ∘ $\mathcal{F} = \{\emptyset, \Omega\}$, $\mathcal{F} = \{\emptyset, A, A^c, \Omega\}$, $\mathcal{F} = 2^{\Omega}$ are all $\sigma$-fields.
∘ If $A, B \in \mathcal{F}$, then $A \cap B, A - B, A \Delta B \in \mathcal{F}$
**Proof:** Using De Morgan's laws: $A \cap B = (A^c \cup B^c)^c$.
∘ If $\mathcal{F}_1, \mathcal{F}_{\in}$ are $\sigma$-fields, then $\mathcal{F}_1 \cap \mathcal{F}_2$ is also a $\sigma$-field.

# *$\sigma$ field

When studying random trials, given an event $A$, we know the following **information**

- $A$ occurs $\Rightarrow A^c$ doesn't occur
- if $A_1, A_2, \cdots$ , occur, then $\cup_{i=1}^{\infty} A_i$ occurs.

## Definition ($\sigma$-field)

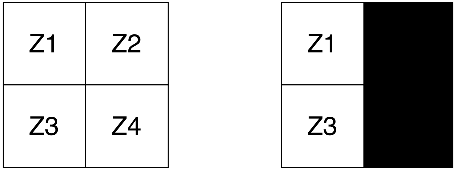
$\mathcal{F}$ is a set of events, i.e., a (nonempty) collection of the subsets of $\Omega$. $\mathcal{F}$ is called $\sigma$-field if

- $A \in \mathcal{F}$, then $A^c \in \mathcal{F}$
- $A_i \in \mathcal{F}$, $i = 1, 2, \ldots$, then $\cup_{i=1}^{\infty} A_i \in \mathcal{F}$
- $\emptyset \in \mathcal{F}$

**Remark:** ◦ $\mathcal{F} = \{\emptyset, \Omega\}$, $\mathcal{F} = \{\emptyset, A, A^c, \Omega\}$, $\mathcal{F} = 2^{\Omega}$ are all $\sigma$-fields.
◦ If $A, B \in \mathcal{F}$, then $A \cap B, A - B, A \Delta B \in \mathcal{F}$
**Proof:** Using De Morgan's laws: $A \cap B = (A^c \cup B^c)^c$.
◦ If $\mathcal{F}_1, \mathcal{F}_{\in}$ are $\sigma$-fields, then $\mathcal{F}_1 \cap \mathcal{F}_2$ is also a $\sigma$-field.
◦ $(\Omega, \mathcal{F})$ is called a measurable space

# *Example: Intuition on a set of “measurable" events

○ a small ball in a box equally split into four regions (from the front): Z1, Z2, Z3, Z4
○ shake the box and the ball rolls randomly
○ which region does the ball stay?

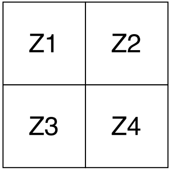


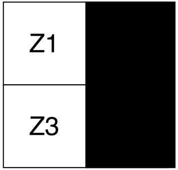

- case 1: a transparent box (left)
- case 2: half covered by opaque cloth

# *Example: Intuition on a set of “measurable" events

◦ a small ball in a box equally split into four regions (from the front): Z1, Z2, Z3, Z4
◦ shake the box and the ball rolls randomly
◦ which region does the ball stay?

sample space $\Omega = \{Z1, Z2, Z3, Z4\}$

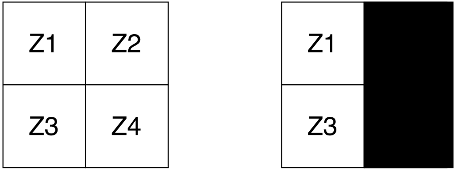



- case 1: a transparent box (left)
- case 2: half covered by opaque cloth

# *Example: Intuition on a set of “measurable" events

○ a small ball in a box equally split into four regions (from the front): Z1, Z2, Z3, Z4
○ shake the box and the ball rolls randomly
○ which region does the ball stay?



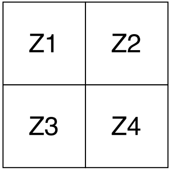

- case 1: a transparent box (left)
- case 2: half covered by opaque cloth

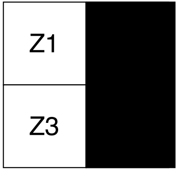
sample space $\Omega = \{Z1, Z2, Z3, Z4\}$

- case 1: $\mathcal{F}_1$ : a collection of all subsets of $\Omega$

# *Example: Intuition on a set of “measurable" events

○ a small ball in a box equally split into four regions (from the front): Z1, Z2, Z3, Z4
○ shake the box and the ball rolls randomly
○ which region does the ball stay?




- case 1: a transparent box (left)
- case 2: half covered by opaque cloth

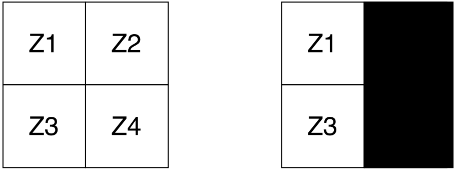
sample space $\Omega = \{Z1, Z2, Z3, Z4\}$

- case 1: $\mathcal{F}_1$ : a collection of all subsets of $\Omega$
- case 2: $\mathcal{F}_2$ is

$$\mathcal{F}_2 = \{\Omega, \emptyset, \{Z1\}, \{Z2, Z3, Z4\}, \{Z3\}, \{Z1, Z2, Z4\}, \{Z1, Z3\}, \{Z2, Z4\}\}$$

# *Example: Intuition on a set of “measurable" events

◦ a small ball in a box equally split into four regions (from the front): Z1, Z2, Z3, Z4
◦ shake the box and the ball rolls randomly
◦ which region does the ball stay?




- case 1: a transparent box (left)
- case 2: half covered by opaque cloth

sample space $\Omega = \{Z1, Z2, Z3, Z4\}$

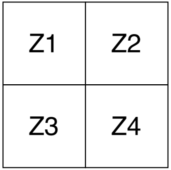
- case 1: $\mathcal{F}_1$ : a collection of all subsets of $\Omega$
- case 2: $\mathcal{F}_2$ is

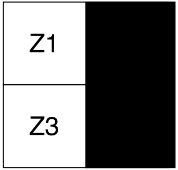
$$\mathcal{F}_2 = \{\Omega, \emptyset, \{Z1\}, \{Z2, Z3, Z4\}, \{Z3\}, \{Z1, Z2, Z4\}, \{Z1, Z3\}, \{Z2, Z4\}\}$$

**Remark:** For some random trials, we know the ball can stay in the covered area, but we don't know it stays at Z2 or Z4. That means, we don't know the event $\{Z2\}$ occurs or not.

# *Example: Intuition on a set of “measurable" events

◦ a small ball in a box equally split into four regions (from the front): Z1, Z2, Z3, Z4
◦ shake the box and the ball rolls randomly
◦ which region does the ball stay?




- case 1: a transparent box (left)
- case 2: half covered by opaque cloth

sample space $\Omega = \{Z1, Z2, Z3, Z4\}$

- case 1: $\mathcal{F}_1$ : a collection of all subsets of $\Omega$
- case 2: $\mathcal{F}_2$ is

$$\mathcal{F}_2 = \{\Omega, \emptyset, \{Z1\}, \{Z2, Z3, Z4\}, \{Z3\}, \{Z1, Z2, Z4\}, \{Z1, Z3\}, \{Z2, Z4\}\}$$

**Remark:** For some random trials, we know the ball can stay in the covered area, but we don't know it stays at Z2 or Z4. That means, we don't know the event $\{Z2\}$ occurs or not.

the event $\{Z2\}$ is $\mathcal{F}_1$-*measurable* but not $\mathcal{F}_2$-*measurable*!

# Probability

- a metric/measure/function $f$ of "event $A$ occurs": frequency interpretation of probability

# Probability

- a metric/measure/function $f$ of "event $A$ occurs": frequency interpretation of probability
  - Suppose we perform the experiment for $n$ times and denote $N(A)$ as the number of times event $A$ occurs, then we have $f \approx \frac{N(A)}{n}$.

# Probability

∘ a metric/measure/function $f$ of "event $A$ occurs": frequency interpretation of probability

- Suppose we perform the experiment for $n$ times and denote $N(A)$ as the number of times event $A$ occurs, then we have $f \approx \frac{N(A)}{n}$.

## Definition (Probability)

Probability $\Pr : \mathcal{F} \to [0, 1]$ is a function that assigns a value to events

- nonnegativity: $\Pr(A) \geq 0$
- normalization: $\Pr(\Omega) = 1$
- countable additivity: if $A_i \in \mathcal{F}$ is a countable sequence of disjoint sets, then $\Pr(\cup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \Pr(A_i)$

# Probability

- a metric/measure/function $f$ of "event $A$ occurs": frequency interpretation of probability
  - Suppose we perform the experiment for $n$ times and denote $N(A)$ as the number of times event $A$ occurs, then we have $f \approx \frac{N(A)}{n}$.

## Definition (Probability)

Probability $\Pr : \mathcal{F} \to [0, 1]$ is a function that assigns a value to events

- nonnegativity: $\Pr(A) \geq 0$
- normalization: $\Pr(\Omega) = 1$
- countable additivity: if $A_i \in \mathcal{F}$ is a countable sequence of disjoint sets, then $\Pr(\cup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \Pr(A_i)$

- $(\Omega, \mathcal{F})$ is a measurable space
- $(\Omega, \mathcal{F}, \Pr)$ is a probability space

## Properties of probability

- $\forall A \in \mathcal{F}$, we have $\Pr(A^c) = 1 - \Pr(A)$.
- If $A, B \in \mathcal{F}$ and $A \subseteq B$, then $\Pr(B) = \Pr(A) + \Pr(B - A) \geq \Pr(A)$.
- If $A, B \in \mathcal{F}$, then $\Pr(A \cup B) = \Pr(A) + \Pr(B) - \Pr(A \cap B)$.