Quiz 3

Based on randomized methods.

Duration: 60 minutes | Total Marks: 30

Problem 1. Total: 18

A **binary operation** "$\odot$" on a finite set X is an arbitrary mapping $X \times X \to X$. For every two elements $x, y \in X$, the element $x \odot y \in X$ is specified by a table with rows and columns indexed by X, where the entry in row x and column y stores $x \odot y$. A set X together with a binary operation is called a **groupoid**.

The operation "$\odot$" is **associative** if $(x \odot y) \odot z = x \odot (y \odot z)$ for all $x, y, z \in X$. A groupoid with an associative operation is called a **semigroup**. We call a triple $(x, y, z) \in X^3$ **associative** if $(x \odot y) \odot z = x \odot (y \odot z)$, and **nonassociative** otherwise.

Here we investigate an algorithmic question: given a binary operation "$\odot$" on a finite set X with n elements, specified by its $n \times n$ table, is "$\odot$" associative?

(1.a) (1 point) Consider the following binary operation on $X = \{1, 2, 3\}$:

$\odot$	**1**	**2**	**3**
1	1	2	3
2	2	1	3
3	3	3	1

Is the triple $(3, 3, 2)$ associative?

A. Yes B. No

(1.b) (1 point) For the operation in Part A, how many of the 27 triples in X^3 are nonassociative?

A. 0 B. 2 C. 6 D. 9

(1.c) (1 point) An obvious algorithm for checking associativity is to test every triple $(x, y, z) \in X^3$. For each triple, we need two lookups to compute $(x \odot y) \odot z$ and two lookups to compute $x \odot (y \odot z)$. What is the running time of this brute-force approach on an n-element set?

A. $O(n)$ B. $O(n^2)$ C. $O(n^3)$ D. $O(n^2 \log n)$

(1.d) (2 points) A natural randomized approach is to repeatedly pick a random triple $(x, y, z) \in X^3$ uniformly at random and test it. If a nonassociative triple is found, we declare the operation nonassociative; otherwise, after some number of samples, we declare it associative.

It turns out that one can construct an operation on an n-element set that has exactly **one** nonassociative triple (for any $n \geqslant 3$). For such an operation, even if we test n^2 independently and uniformly random triples, the probability of detecting nonassociativity is only:

A. at least $\frac{1}{2}$ B. roughly $\frac{1}{n^2}$ C. roughly $\frac{1}{n}$ D. roughly $1 - \frac{1}{n}$

(1.e) (2 points) We now develop a much better algorithm. The idea is to "lift" the operation from individual elements to *vectors*, creating many more chances to detect nonassociativity.

Fix a field $\mathbb{K}$ (for concreteness, you may think of $\mathbb{K} = \mathbb{F}_7$, the field with 7 elements). Consider the vector space $\mathbb{K}^X$, whose vectors are n-tuples of elements of $\mathbb{K}$ indexed by elements of X. For every $x \in X$, let $\mathbf{e}(x) \in \mathbb{K}^X$ be the standard basis vector that has 1 in position x and 0 elsewhere.

We define a binary operation "$\square$" on $\mathbb{K}^X$ as a **linear extension** of "$\odot$." For two vectors $\mathbf{u} = \sum_{x \in X} \alpha_x \mathbf{e}(x)$ and $\mathbf{v} = \sum_{y \in X} \beta_y \mathbf{e}(y)$, we define:

$$\mathbf{u} \,\square\, \mathbf{v} = \sum_{x,y \in X} \alpha_x \beta_y \,\mathbf{e}(x \odot y).$$

Now consider $X = \{1, 2\}$ with the operation $1 \odot 1 = 1, 1 \odot 2 = 2, 2 \odot 1 = 2, 2 \odot 2 = 1$, and working over the rationals. For $\mathbf{u} = 2\,\mathbf{e}(1) + 3\,\mathbf{e}(2)$ and $\mathbf{v} = 4\,\mathbf{e}(1) + 1\,\mathbf{e}(2)$, what is $\mathbf{u} \,\square\, \mathbf{v}$?

A. $8\,\mathbf{e}(1) + 14\,\mathbf{e}(2)$ B. $11\,\mathbf{e}(1) + 14\,\mathbf{e}(2)$ C. $14\,\mathbf{e}(1) + 11\,\mathbf{e}(2)$ D. $11\,\mathbf{e}(1) + 11\,\mathbf{e}(2)$

(1.f) (1 point) Suppose "$\odot$" is associative. Is "$\square$" necessarily associative as well?

A. Yes B. No

(1.g) (1 point) Now suppose (a, b, c) is a **nonassociative** triple for "$\odot$", meaning $(a \odot b) \odot c \neq a \odot (b \odot c)$. Is $(\mathbf{e}(a), \mathbf{e}(b), \mathbf{e}(c))$ a nonassociative triple for "$\square$"?

A. Yes B. No C. Not enough information

(1.h) (2 points) We are now ready to describe the algorithm for associativity testing. Fix a 6-element subset $S \subset \mathbb{K}$.

1. For every $x \in X$, choose $\alpha_x, \beta_x, \gamma_x \in S$ uniformly at random, all choices independent.
2. Set $\mathbf{u} := \sum_{x \in X} \alpha_x \,\mathbf{e}(x)$, $\mathbf{v} := \sum_{y \in X} \beta_y \,\mathbf{e}(y)$, $\mathbf{w} := \sum_{z \in X} \gamma_z \,\mathbf{e}(z)$.
3. Compute the vectors $(\mathbf{u} \,\square\, \mathbf{v}) \,\square\, \mathbf{w}$ and $\mathbf{u} \,\square\, (\mathbf{v} \,\square\, \mathbf{w})$. If they are equal, answer YES; otherwise, answer NO.

Given two arbitrary vectors $\mathbf{u}, \mathbf{v} \in \mathbb{K}^X$, the product $\mathbf{u} \,\square\, \mathbf{v}$ can be computed using $O(n^2)$ lookups in the table and $O(n^2)$ operations in $\mathbb{K}$. What is the overall running time of the algorithm?

A. $O(n)$ B. $O(n^2)$ C. $O(n^3)$ D. $O(n^2 \log n)$

(1.i) (2 points) We now analyze the error probability. Fix a nonassociative triple (a, b, c) for "$\odot$", and let $r := (a \odot b) \odot c$. Note that $a \odot (b \odot c) \neq r$.

Consider the r-th component of the vectors $(\mathbf{u} \,\square\, \mathbf{v}) \,\square\, \mathbf{w}$ and $\mathbf{u} \,\square\, (\mathbf{v} \,\square\, \mathbf{w})$. Define:

$$f(\alpha_a, \beta_b, \gamma_c) := \big((\mathbf{u} \,\square\, \mathbf{v}) \,\square\, \mathbf{w}\big)_r, \qquad g(\alpha_a, \beta_b, \gamma_c) := \big(\mathbf{u} \,\square\, (\mathbf{v} \,\square\, \mathbf{w})\big)_r,$$

where we view all other α_x $(x \neq a)$, β_y $(y \neq b)$, γ_z $(z \neq c)$ as fixed constants.

Using the definition of "$\square$", we can expand:

$$f(\alpha_a, \beta_b, \gamma_c) = \sum_{\substack{x,y,z \in X \\ (x \odot y) \odot z = r}} \alpha_x \beta_y \gamma_z.$$

The monomial $\alpha_a \beta_b \gamma_c$ appears in f because $(a \odot b) \odot c = r$. Does the monomial $\alpha_a \beta_b \gamma_c$ appear in g?

A. Yes, with coefficient 1 B. No C. Yes, with coefficient -1

(1.j) (1 point) What is the total degree of the polynomial $f(\alpha_a, \beta_b, \gamma_c) - g(\alpha_a, \beta_b, \gamma_c)$ in the three variables $\alpha_a, \beta_b, \gamma_c$?

A. At most 1 B. At most 2 C. At most 3 D. Exactly 3

(1.k) (2 points) From Parts I and J, we know that $f - g$ is a **nonzero** polynomial of total degree **at most** 3 in the variables $\alpha_a, \beta_b, \gamma_c$.

Recall the **Schwartz–Zippel Lemma**: if $p(x_1, \ldots, x_k)$ is a nonzero polynomial of total degree d over a field $\mathbb{K}$, and each x_i is chosen independently and uniformly from a finite set $S \subseteq \mathbb{K}$, then

$$\Pr[p(x_1, \ldots, x_k) = 0] \leqslant \frac{d}{|S|}.$$

In our algorithm, $\alpha_a, \beta_b, \gamma_c$ are chosen independently and uniformly from S with $|S| = 6$. What is the probability that the algorithm *fails to detect* that (a, b, c) is nonassociative — i.e., that $f(\alpha_a, \beta_b, \gamma_c) = g(\alpha_a, \beta_b, \gamma_c)$?

A. 0 B. at most $\frac{1}{6}$ C. at most $\frac{1}{3}$ D. at most $\frac{1}{2}$ E. at most $\frac{2}{3}$

(1.l) (2 points) Which of the following correctly describes the guarantees of this algorithm?

A. If "$\odot$" is associative, the algorithm always answers YES. If "$\odot$" is not associative, the algorithm always answers NO.

B. If "$\odot$" is associative, the algorithm always answers YES. If "$\odot$" is not associative, the algorithm answers NO with probability at least $\frac{1}{2}$.

C. If "$\odot$" is associative, the algorithm answers YES with probability at least $\frac{1}{2}$. If "$\odot$" is not associative, the algorithm always answers NO.

D. If "$\odot$" is associative, the algorithm answers YES with probability at least $\frac{1}{2}$. If "$\odot$" is not associative, the algorithm answers NO with probability at least $\frac{1}{2}$.

Problem 2. Total: 12

Let n and N be positive integers, and let $\mathcal{F}$ be an arbitrary nonempty family of subsets of the universe $\{1, \ldots, n\}$. Suppose each element $x \in \{1, \ldots, n\}$ in the universe receives an integer weight $w(x)$, each of which is chosen independently and uniformly at random from $\{1, \ldots, N\}$. The weight of a set S in $\mathcal{F}$ is defined as

$$w(S) = \sum_{x \in S} w(x)$$

We want to explore the probability of the following "good" event: *there is a unique set in $\mathcal{F}$ that has the minimum weight among all sets of $\mathcal{F}$.*

(2.a) (1 point) Suppose $n = 3$, $N = 100$ and the family $\mathcal{F}$ consists of the following sets:

$$\mathcal{F} = \{\{1, 2\}, \{2, 3\}, \{3\}\}.$$

Suppose the randomly assigned weights are:

$$w(1) = 30, \quad w(2) = 20, \quad w(3) = 50.$$

Is there a unique set in $\mathcal{F}$ that has the minimum weight among all sets of $\mathcal{F}$?

A. Yes B. No

(2.b) (1 point) Suppose $n = 2$, $N = 100$ and the randomly assigned weights are:

$$w(1) = 25, \quad w(2) = 50.$$

Consider all non-empty families $\mathcal{F}$ over non-empty subsets of $\{1, 2\}$. There are seven such families. How many of them have a unique minimum-weight subset?

A. None B. One C. Three D. All

(2.c) (1 point) Suppose $n = 2$, $N = 100$ and the randomly assigned weights are:

$$w(1) = 25, \quad w(2) = 25.$$

Consider all non-empty families $\mathcal{F}$ over non-empty subsets of $\{1, 2\}$. There are seven such families. How many of them *do not* have a unique minimum-weight subset?

A. None B. One C. Three D. All

(2.d) (1 point) Suppose $n = 2$, $N = 5$ and $\mathcal{F} = \{\{1\}, \{2\}\}$. What is the probability of the good event?

A. 0 B. $\frac{1}{5}$ C. $\frac{4}{5}$ D. 1

(2.e) (1 point) Suppose $n = 3$, $N = 100$ and $\mathcal{F} = \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$. What is the probability of the good event?

A. 0 B. $\frac{1}{3}$ C. $\frac{2}{3}$ D. 1

(2.f) (1 point) Suppose $n = 3$, $N = 5$ and $\mathcal{F} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$. Note that there are 125 possible weight functions overall. How many of these lead to a good event?

A. 25 B. 60 C. 90 D. 120

(2.g) (1 point) Suppose $n = 3$, $N = 5$ and $\mathcal{F} = \{\{1\}, \{3\}, \{2, 3\}, \{1, 2\}\}$. Note that there are 125 possible weight functions overall. How many of these lead to a good event?

A. 25 B. 50 C. 90 D. 100

(2.h) (1 point) We introduce some notation:

- Let $\mathcal{P}_i \subseteq \mathcal{F}$ denote all those sets in $\mathcal{F}$ that contain i, and
- let $\mathcal{Q}_i \subseteq \mathcal{F}$ denote all those sets in $\mathcal{F}$ that *do not* contain i.

Notice that $\mathcal{Q}_i = \mathcal{F} \setminus \mathcal{P}_i$. For example, if $\mathcal{F} = \{\{1\}, \{1, 2\}, \{2, 3\}\}$, then:

- $\mathcal{P}_1 = \{\{1\}, \{1, 2\}\}$ and $\mathcal{Q}_1 = \{\{2, 3\}\}$, and
- $\mathcal{P}_2 = \{\{1, 2\}, \{2, 3\}\}$ and $\mathcal{Q}_2 = \{\{1\}\}$, and
- $\mathcal{P}_3 = \{\{2, 3\}\}$ and $\mathcal{Q}_3 = \{\{1\}, \{1, 2\}\}$.

Let $\mathcal{E}_i$ be the event:

$$\min\{w(S) : S \in \mathcal{P}_i\} = \min\{w(S) : S \in \mathcal{Q}_i\}.$$

We can conclude that the good event occurs if:

A. None of the events $\mathcal{E}_i$ occur

B. At least one of the events $\mathcal{E}_i$ occur

C. Exactly one of the events $\mathcal{E}_i$ occur

D. All of the events $\mathcal{E}_i$ occur

(2.i) (1 point) Further, if the good event occurs, then:

A. None of the events $\mathcal{E}_i$ occur

B. At least one of the events $\mathcal{E}_i$ occur

C. Exactly one of the events $\mathcal{E}_i$ occur

D. All of the events $\mathcal{E}_i$ occur

(2.j) (1 point) Fix some $1 \leqslant i \leqslant n$. The probability that $\mathcal{E}_i$ occurs is:

A. at most $\frac{1}{n}$ B. at least $\frac{1}{n}$ C. at most $\frac{1}{2^n}$ D. at least $\frac{1}{2^n}$ E. at most $\frac{1}{N}$ F. at least $\frac{1}{N}$

(2.k) (1 point) Consider the problem of finding perfect matchings in a simple, undirected graph. Recall that the Tutte matrix of a graph G, denoted Z_G, is given by:

$$Z_G[i,j] = \begin{cases} z_{ij} & \text{if } (i,j) \text{ is an edge and } i < j \\ -z_{ji} & \text{if } (i,j) \text{ is an edge and } j > i \\ 0 & \text{if } (i,j) \text{ is not an edge} \end{cases}$$

Suppose each edge is assigned a random weight in $\{1, \ldots, 2m\}$, and $\mathcal{F}$ is the set of perfect matchings.

Further, let us replace each indeterminate z_{ij} in the Tutte matrix of the graph with $2^{w_{ij}}$ where w_{ij} is the randomly assigned weight of the edge (i,j) from above.

If G has no perfect matching, what is the determinant of Z with the variables substituted for these weights?

A. 0 B. 1 C. m D. $m!$

(2.l) (1 point) We continue the notation from the previous question. Suppose the randomly assigned weights lead to the good event, that is, there is a unique perfect matching in G with minimum weight, and say this minimum weight is r. What can you say about the determinant of Z in this case?

A. r

B. 2^r

C. $2^r \cdot k$, where k is an odd number

D. $2^r \cdot k$, where k is an even number