CSL202: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Discrete Probability

Definition (Expectation)

The *expected value*, also called the *expectation* or *mean*, of the random variable X on the sample space S is equal to

$$\mathbf{E}[X] = \sum_{s \in S} p(s) \cdot X(s).$$

The *deviation* of X at $s \in S$ is $X(s) - \mathbf{E}[X]$, the difference between the value of X and the mean of X.

Definition (Expectation)

The *expected value*, also called the *expectation* or *mean*, of the random variable X on the sample space S is equal to

$$\mathbf{E}[X] = \sum_{s \in S} p(s) \cdot X(s).$$

The *deviation* of X at $s \in S$ is $X(s) - \mathbf{E}[X]$, the difference between the value of X and the mean of X.

- A fair coin is flipped three times. Let S be the sample space of the eight possible outcomes, and let X be the random variable that assigns to an outcome the number of heads in this outcome. What is the expected value of X?

Definition (Expectation)

The *expected value*, also called the *expectation* or *mean*, of the random variable X on the sample space S is equal to

$$\mathbf{E}[X] = \sum_{s \in S} p(s) \cdot X(s).$$

The *deviation* of X at $s \in S$ is $X(s) - \mathbf{E}[X]$, the difference between the value of X and the mean of X.

Theorem

If X is a random variable and $\mathbf{Pr}[X = r]$ is the probability that $X = r$, so that $\mathbf{Pr}[X = r] = \sum_{s \in S, X(s) = r} p(s)$, then

$$\mathbf{E}[X] = \sum_{r \in X(S)} \mathbf{Pr}[X = r] \cdot r.$$

Theorem

If X is a random variable and $\mathbf{Pr}[X = r]$ is the probability that $X = r$, so that $\mathbf{Pr}[X = r] = \sum_{s \in S, X(s) = r} p(s)$, then

$$\mathbf{E}[X] = \sum_{r \in X(S)} \mathbf{Pr}[X = r] \cdot r.$$

- What is the expected value of the sum of the numbers that appear when a pair of fair dice is rolled?

Theorem

The expected number of successes when n mutually independent Bernoulli trials are performed, where p is the probability of success on each trial, is np.

Theorem (Linearity of expectation)

If X_i, $i = 1, 2, ..., n$ with n a positive integer, are random variables on S, and if a and b are real numbers, then
(i) $\mathbf{E}[X_1 + X_2 + ... + X_n] = \mathbf{E}[X_1] + \mathbf{E}[X_2] + ... + \mathbf{E}[X_n]$,
(ii) $\mathbf{E}[aX + b] = a \cdot \mathbf{E}[X] + b$.

Theorem (Linearity of expectation)

If X_i, $i = 1, 2, ..., n$ with n a positive integer, are random variables on S, and if a and b are real numbers, then
(i) $\mathbf{E}[X_1 + X_2 + ... + X_n] = \mathbf{E}[X_1] + \mathbf{E}[X_2] + ... + \mathbf{E}[X_n]$,
(ii) $\mathbf{E}[aX + b] = a \cdot \mathbf{E}[X] + b$.

- What is the expected value of the sum of the numbers that appear when a pair of fair dice is rolled?
- What is the expected value of the number of successes when n independent Bernoulli trials are performed, where p is the probability of success on each trial?

- Average-case complexity: Let the sample space I consist of all possible inputs to the algorithm. Let X be a random variable denoting the running time of the algorithm. Then the average-case complexity of the algorithm is $\mathbf{E}[X] = \sum_{i \in I} p(i) \cdot X(i)$.
- What is the average-case complexity of insertion sort if we just count the number of comparisons?

Definition (Geometric distribution)

A random variable X has a *geometric distribution with parameter* p if $\mathbf{Pr}[X = k] = (1-p)^{k-1}p$ for $k = 1, 2, 3, \ldots$, where p is a real number with $0 \leq p \leq 1$.

- Example: Suppose that the probability that a coin comes up tails is p. This coin is flipped repeatedly until it comes up tails. What is the expected number of flips until this coin comes up tails?

Theorem

If the random variable X has the geometric distribution with parameter p, then $\mathbf{E}[X] = 1/p$.

Definition (Independent random variables)

The random variables X and Y on a sample space S are independent if

$$\mathbf{Pr}[X = r_1 \text{ and } Y = r_2] = \mathbf{Pr}[X = r_1] \cdot \mathbf{Pr}[Y = r_2],$$

or in other words, if the probability that $X = r_1$ and $Y = r_2$ equals the product of the probabilities that $X = r_1$ and $Y = r_2$, for all real numbers r_1 and r_2.

- Example: Let X_1 and X_2 be the random variable denoting the number that appears on two dice when rolled. Are X_1 and X_2 independent?

Definition (Independent random variables)

The random variables X and Y on a sample space S are independent if

$$\mathbf{Pr}[X = r_1 \text{ and } Y = r_2] = \mathbf{Pr}[X = r_1] \cdot \mathbf{Pr}[Y = r_2],$$

or in other words, if the probability that $X = r_1$ and $Y = r_2$ equals the product of the probabilities that $X = r_1$ and $Y = r_2$, for all real numbers r_1 and r_2.

Theorem

If X and Y are independent random variables on a sample space S, then $\mathbf{E}(XY) = \mathbf{E}(X) \cdot \mathbf{E}(Y)$.

Theorem

If X and Y are independent random variables on a sample space S, then $\mathbf{E}(XY) = \mathbf{E}(X) \cdot \mathbf{E}(Y)$.

- Does the above theorem hold for non-independent random variables?

Definition (Variance)

Let X be a random variable on a sample space S. The *variance* of X, denoted by $\mathbf{Var}[X]$, is

$$\mathbf{Var}[X] = \sum_{s \in S} (X(s) - \mathbf{E}[X])^2 \cdot p(s).$$

That is, $\mathbf{Var}[X]$ is the weighted average of the square of the deviation of X. The *standard deviation* of X, denoted by $\sigma[X]$ is defined to be $\sqrt{\mathbf{Var}[X]}$.

Theorem

If X is a random variable on a sample space S, then $\mathbf{Var}[X] = \mathbf{E}[X^2] - (\mathbf{E}[X])^2$.

Definition (Variance)

Let X be a random variable on a sample space S. The *variance* of X, denoted by $\textbf{Var}[X]$, is $\textbf{Var}[X] = \sum_{s \in S}(X(s) - \textbf{E}[X])^2 \cdot p(s)$.
That is, $\textbf{Var}[X]$ is the weighted average of the square of the deviation of X. The *standard deviation* of X, denoted by $\sigma[X]$ is defined to be $\sqrt{\textbf{Var}[X]}$.

Theorem

If X is a random variable on a sample space S, then $\textbf{Var}[X] = \textbf{E}[X^2] - (\textbf{E}[X])^2$.

Theorem

If X is a random variable on a sample space S and $\textbf{E}[X] = \mu$, then $\textbf{Var}[X] = \textbf{E}[(X - \mu)^2]$.

Theorem

If X is a random variable on a sample space S, then $\mathbf{Var}[X] = \mathbf{E}[X^2] - (\mathbf{E}[X])^2$.

Theorem

If X is a random variable on a sample space S and $\mathbf{E}[X] = \mu$, *then* $\mathbf{Var}[X] = \mathbf{E}[(X - \mu)^2]$.

- What is the variance of the random variable X, where X is the number that comes up when a fair die is rolled?

Theorem (Bienayme's Formula)

If X and Y are two independent random variables on a sample space S, then $\mathbf{Var}[X+Y] = \mathbf{Var}[X] + \mathbf{Var}[Y]$. Furthermore, if $X_i, i = 1, 2, ..., n$, with n a positive integer, are pairwise independent random variables on S , then $\mathbf{Var}[X_1 + X_2 + ... + X_n] = \mathbf{Var}[X_1] + \mathbf{Var}[X_2] + ... + \mathbf{Var}[X_n]$.

- What is the variance of the number of successes when n independent Bernoulli trials are performed, where, on each trial, p is the probability of success and q is the probability of failure?

Theorem (Markov's inequality)

Let X be a non-negative random variable on a sample space and a be a positive real number. Then

$$\mathbf{Pr}[X \geq a] \leq \mathbf{E}[X]/a.$$

Theorem (Markov's inequality)

Let X be a non-negative random variable on a sample space and a be a positive real number. Then

$$\mathbf{Pr}[X \geq a] \leq \mathbf{E}[X]/a.$$

Theorem (Chebychev's inequality)

Let X be a random variable on a sample space and a be a positive real number. Then

$$\mathbf{Pr}[|X - \mathbf{E}[X]| \geq a] \leq \mathbf{Var}[X]/a^2.$$

Birthday Problem

You sample r items with replacement from a collection of n distinct items. What is the probability that two items are the same?

- Let X_{ij} be an indicator random variable that is 1 if the i^{th} and the j^{th} sample are the same and 0 otherwise.
- Lemma 1: $\mathbf{E}[X_{ij}] = 1/n$.

Birthday Problem

You sample r items with replacement from a collection of n distinct items. What is the probability that two items are the same?

- Let X_{ij} be an indicator random variable that is 1 if the i^{th} and the j^{th} sample are the same and 0 otherwise.
- Lemma 1: $\mathbf{E}[X_{ij}] = 1/n$.
- Let $X = \sum_{i<j} X_{ij}$. Note that X denotes the number of distinct pairs of samples that are the same.
- Lemma 2: $\mathbf{E}[X] = \frac{r(r-1)}{2n}$.

Birthday Problem

You sample r items with replacement from a collection of n distinct items. What is the probability that two items are the same?

- Let X_{ij} be an indicator random variable that is 1 if the i^{th} and the j^{th} sample are the same and 0 otherwise.
- Lemma 1: $\mathbf{E}[X_{ij}] = 1/n$.
- Let $X = \sum_{i<j} X_{ij}$. Note that X denotes the number of distinct pairs of samples that are the same.
- Lemma 2: $\mathbf{E}[X] = \frac{r(r-1)}{2n}$.
- If $r \approx c \cdot \sqrt{2n}$, then $\mathbf{E}[X] = 10$.
- Lemma 3: $\mathbf{Var}[X_{ij}] = \frac{n-1}{n^2}$.

Birthday Problem

You sample r items with replacement from a collection of n distinct items. What is the probability that two items are the same?

- Let X_{ij} be an indicator random variable that is 1 if the i^{th} and the j^{th} sample are the same and 0 otherwise.
- Lemma 1: $\mathbf{E}[X_{ij}] = 1/n$.
- Let $X = \sum_{i<j} X_{ij}$. Note that X denotes the number of distinct pairs of samples that are the same.
- Lemma 2: $\mathbf{E}[X] = \frac{r(r-1)}{2n}$.
- If $r \approx c \cdot \sqrt{2n}$, then $\mathbf{E}[X] = 10$.
- Lemma 3: $\mathbf{Var}[X_{ij}] = \frac{n-1}{n^2}$.
- Lemma 4: $\mathbf{Var}[X] = \sum_{i<j} \mathbf{Var}[X_{ij}] = \frac{r(r-1)(n-1)}{2n^2}$.

Birthday Problem

You sample r items with replacement from a collection of n distinct items. What is the probability that two items are the same?

- Let X_{ij} be an indicator random variable that is 1 if the i^{th} and the j^{th} sample are the same and 0 otherwise.
- Lemma 1: $\mathbf{E}[X_{ij}] = 1/n$.
- Let $X = \sum_{i<j} X_{ij}$. Note that X denotes the number of distinct pairs of samples that are the same.
- Lemma 2: $\mathbf{E}[X] = \frac{r(r-1)}{2n}$.
- If $r \approx c \cdot \sqrt{2n}$, then $\mathbf{E}[X] = 10$.
- Lemma 3: $\mathbf{Var}[X_{ij}] = \frac{n-1}{n^2}$.
- Lemma 4: $\mathbf{Var}[X] = \sum_{i<j} \mathbf{Var}[X_{ij}] = \frac{r(r-1)(n-1)}{2n^2}$.
- So, $\mathbf{Var}[X] = 10 \cdot (1 - 1/n)$ when $r \approx c \cdot \sqrt{2n}$.
- Lemma 5: $\mathbf{Pr}[X < 1] < 1/4$.

Theorem (Chernoff-bound)

Let $X_1, ..., X_n$ be independent, 0/1 random variables, and let $p_i = \mathbf{E}[X_i]$ for all $i = 1, 2, ..., n$. Let $X = X_1 + X_2 + ... + X_n$ and let $\mu = \mathbf{E}[X]$. Let $\delta > 0$ be any real number. Then

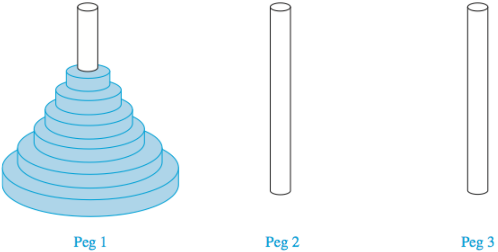
$$\begin{aligned} \mathbf{Pr}[X > (1+\delta)\cdot\mu] &\leq e^{-f(\delta)\cdot\mu}, \text{ and} \\ \mathbf{Pr}[X < (1-\delta)\cdot\mu] &\leq e^{-g(\delta)\cdot\mu} \end{aligned}$$

where $f(\delta) = (1+\delta)\cdot\ln(1+\delta) - \delta$ and $g(\delta) = (1-\delta)\cdot\ln(1-\delta) + \delta$.

- For all $\delta > 0, g(\delta) \geq \delta^2/2$ and $f(\delta) \geq \frac{\delta^2}{2+\delta}$.

Advanced Counting Techniques

- Tower of Hanoi: Let H_n denote the number of moves needed to solve the Tower of Hanoi problem with n disks. Set up a recurrence relation for the sequence $\{H_n\}$.



- Find a recurrence relation and give initial conditions for the number of bit strings of length n that do not have two consecutive 0s. How many such bit strings are there of length five?

- Dynamic Programming: This is an algorithmic technique where a problem is recursively broken down into simpler overlapping subproblems, and the solution is computed using the solutions of the subproblems.
- Problem: Given a sequence of integers, find the length of the *longest increasing subsequence* of the given sequence.
  - Example: The longest increasing subsequence of the sequence $(7, 2, 8, 10, 3, 6, 9, 7)$ is $(2, 3, 6, 7)$ and its length is 4.

End