CMSC 250: Discrete Structures
Summer 2017

Lecture 16 - Outline
June 27, 2017

Strong Induction.

If we are trying to prove a claim:

$$\forall n \in \mathbb{Z}, n \geq BC, P(n)$$

we can equivalently prove:

$$P(BC) \wedge (\forall k \in \mathbb{Z}, k \geq BC, (P(BC) \wedge P(BC+1) \wedge P(BC+2) \wedge \cdots \wedge P(k)) \implies P(k+1))$$

Note that the only difference between "normal" induction and "strong" induction is what we assume in the Induction Hypothesis. In normal induction, we assume that $P(k)$ is true, and go on to show that $P(k+1)$ is true. In strong induction, we assume that $P(j)$ is true, for any j between the base case and k, and go on to show that $P(k+1)$ is true.

The rest of the induction step proceeds in a similar fashion.

Problem: Suppose we have the following sequence:

$$a_1 = 1 \quad a_2 = 3 \quad a_i = a_{i-2} + 2a_{i-1}, \quad i \in \mathbb{Z}, i \geq 3$$

Use strong induction to prove that for any $n \in \mathbb{Z}^+$, a_n is odd.

Solution: Define $P(k)$ to be the claim that a_k is odd.

Base Cases: When $n = 1$, $a_1 = 1$, which is odd.

When $n = 2$, $a_2 = 3$, which is also odd.

We need 2 base cases, the Induction Step does not prove that claim for $P(2)$.

Induction Hypothesis: Assume $P(j)$ is true, for $1 \leq j \leq k$, for some $k \in \mathbb{Z}^+$.

Induction Step: We want to show that $a_{k+1} = 2\ell + 1$, for some $\ell \in \mathbb{Z}$.

$$a_{k+1} = a_{k-1} + 2a_k$$

By the Induction Hypothesis, a_{k-1} and a_k are both odd. Let $a_{k-1} = 2x + 1$ and $a_k = 2y + 1$, for some integers x and y.

$$a_{k+1} = (2x + 1) + 2(2y + 1)$$
$$a_{k+1} = 2x + 1 + 4y + 2 = 2(x + 2y + 1) + 1$$

Thus, a_{k+1} is odd.

Problem: Prove that, for any positive integer n, if $x_1, x_2, \ldots, x_n$ are n distinct real numbers, then no matter how the parenthesis are inserted into their product, the number of multiplications used to compute the product is $n - 1$.

Solution: Let $P(n)$ be the predicate that "If $x_1, x_2, \ldots, x_n$ are n distinct real numbers, then no matter how the parentheses are inserted into their product, the number of multiplications used to compute the product is $n - 1$".

Base Case: $P(1)$ is true, since x_1 is computed using 0 multiplications.

Induction Hypothesis: Assume that $P(j)$ is true for all j such that $1 \leq j \leq k$, for some $k \in \mathbb{Z}^+$.

Induction Step: We want to prove $P(k+1)$. Consider the product of $k+1$ distinct factors, $x_1, x_2, \ldots, x_{k+1}$. When parentheses are inserted in order to compute the product of factors, some multiplication must be the final one. Consider the two terms, of this final multiplication. Each one is a product of at most k factors. Suppose the first and the second term in the final multiplication contain f_k and s_k factors. Clearly, $1 \leq f_k, s_k \leq k$.

Thus, by induction hypothesis, the number of multiplications to obtain the first term of the final multiplication is $f_k - 1$ and the number of multiplications to obtain the second term of the final multiplication is $s_k - 1$. It follows that the number of multiplications to compute the product of $x_1, x_2, \ldots, x_k, x_{k+1}$ is

$$(f_k - 1) + (s_k - 1) + 1 = f_k + s_k - 1 = k + 1 - 1 = k$$

Introduction to Probability

Probability theory has many applications in engineering, medicine, etc. It has also found many useful applications in computer science, such as cryptography, networking, game theory etc. Many algorithms are randomized and we need probability theory to analyze them. In this course, our goal is to understand how to describe uncertainty using probabilistic arguments. To do this we first have to define a probabilistic model.

A probabilistic model is a mathematical description of a random process or an experiment. In a random process exactly one outcome from a set of outcomes is sure to occur but no outcome can be predicted with certainty. For example, tossing a coin is an experiment. Below are definitions of entities associated with the probabilistic model.

- The **outcome/sample space** of a random process or experiment is the set of all possible outcomes. The outcome/sample space is often denoted by Ω. Since we are going to study discrete probability Ω

will be finite or countably infinite (such as integers and not real numbers).

- The **probability function/distribution** is a function $\Pr : \Omega \to [0, 1]$ that assigns each outcome $\omega \in \Omega$ a probability value that is a real number from 0 to 1.

  The probability function must satisfy the following requirements:

  - $0 \leq \Pr[\omega] \leq 1$
  - $\sum_{\omega \in \Omega} \Pr[\omega] = 1$

- The **probability space** is the combination of an outcome space and a probability distribution.

In an experiment we are usually interested in the probability that an event occurs. An **event** is a set containing of the outcomes of interest. For example, when tossing a coin we may be interested in knowing the probability that the result is heads. Below we define formally what an event is and what does it mean to calculate the probability of an event.

- A subset of the sample space is called an *event*.
- For any event, $A \subseteq \Omega$, the probability of A is defined as

$$\Pr[A] = \sum_{\omega \in A} \Pr[\omega]$$

For any event A, we also have a concept of a complementary event, denoted $\overline{A}$ or A^c. The complement event contains all of the outcomes that do not belong to the event A. Formally, we can say that $\overline{A} := \Omega \setminus A$.

Note that the probability of any complement event has the following relationship with the event:

$$\Pr[\overline{A}] = 1 - \Pr[A]$$

This follows immediately from the following equality:

$$\Pr[A] + \Pr[\overline{A}] = 1$$

We know that the above equality is true, since any outcome must either be in A or $\overline{A}$, and the sum of the probabilities over all outcomes must equal 1.

Let us see an example probabilistic game so we can make the above definitions/concepts concrete.

Example:

Let us consider the probabilistic game that is the roll of a fair six-sided dice.

Note that $\Omega = \{1, 2, 3, 4, 5, 6\}$, and the probability function $\Pr = \{(1, \frac{1}{6}), (2, \frac{1}{6}), (3, \frac{1}{6}), (4, \frac{1}{6}), (5, \frac{1}{6}), (6, \frac{1}{6})\}$.

We can check that the sum of the probabilities of all outcomes is 1.

$$\sum_{\omega \in \Omega} [\omega] = \Pr[1] + \Pr[2] + \cdots + \Pr[6] = 6 \times \frac{1}{6} = 1$$

By inspection, we can see that the probability of any outcome is between 0 and 1, as required.

Let us consider A, where A is the event that we roll an even number. Note that $A = \{2, 4, 6\}$. We can also compute $\Pr[A]$:

$$\Pr[A] = \sum_{\omega \in A} \Pr[\omega] = \Pr[2] + \Pr[4] + \Pr[6] = 3 \times \frac{1}{6} = \frac{1}{2}$$

Let us consider $\overline{A}$. In English, we would say that the complement event is where we roll an odd number. Clearly, $\overline{A} = \{1, 3, 5\}$.

We can compute $\overline{A}$ in two ways. First, using the definition of the probability of any event:

$$\Pr[\overline{A}] = \sum_{\omega \in \overline{A}} \Pr[\omega] = \Pr[1] + \Pr[3] + \Pr[5] = 3 \times \frac{1}{6} = \frac{1}{2}$$

Second, using the relationship between the probability of an event and its complement:

$$\Pr[\overline{A}] = 1 - \Pr[A] = 1 - \frac{1}{2} = \frac{1}{2}$$

Uniform Probability Space

One of the most important and common probability spaces that we encounter is called the **uniform probability space**. A probability space or probability function is called **uniform** if each outcome in the space is assigned an equal probability.

Suppose we have an outcome space Ω and a uniform probability function Pr. For any $\omega \in \Omega$, what is $\Pr[\omega]$?

We can solve this from our definitions above. We know that:

$$\sum_{\omega \in \Omega} \Pr[\omega] = 1$$

Let $\forall \omega \in \Omega, \Pr[\omega] = x$, for some $x \in [0, 1]$. So we have:

$$\begin{aligned} \sum_{\omega \in \Omega} \Pr[\omega] &= 1 \\ \sum_{\omega \in \Omega} x &= 1 \\ |\Omega| \cdot x &= 1 \\ x &= \frac{1}{|\Omega|} \end{aligned}$$

Hence, we have that $\forall \omega \in \Omega, \Pr[\omega] = \dfrac{1}{|\Omega|}$.

Suppose we have an event A in a uniform probability space. What is $\Pr[A]$? Again, we can work this out from

the definitions above.

$$\Pr[A] = \sum_{\omega \in A} \Pr[\omega] = \sum_{\omega \in A} \frac{1}{|\Omega|} = \frac{|A|}{|\Omega|}$$

Hence, we have that the probability for any event A in a uniform probability space is:

$$\Pr[A] = \frac{|A|}{|\Omega|}$$

Problem:

Consider a probabilistic game that is 5 fair coin flips.

(a) What is the probability that we get exactly 3 heads?

(b) What is the probability that we get at least 1 head?

Solution: Let us consider some possible outcomes for this game. One possible outcome would be $HHTHH$, which would be getting heads on flip 1, 2, 4, 5, and getting tails on flip 3. Another possible outcome would be $TTHHH$, which would be getting heads on flip 3, 4, 5, and getting tails on flip 1, 2.

Note that each of these outcomes should occur with the same probability, since we are flipping fair coins. Hence, we have a uniform probability space.

(a) Let A be the event where we get exactly 3 heads. We seek $\Pr[A]$.

Note that $|\Omega| = 2^5$, since there are 5 flips and each flip can either be Heads or Tails.

Note that $|A| = \binom{5}{3}$, since we can construct an outcome in A by selecting 3 flips to be Heads, and let the others be Tails.

Since we have a uniform probability space, we have that:

$$\Pr[A] = \frac{|A|}{|\Omega|} = \frac{\binom{5}{3}}{2^5}$$

(b) Let B be the event where we get at least 1 head. We seek $\Pr[B]$. This seems hard to determine, so let us try to work out $\Pr[\overline{B}]$ instead. In English, $\overline{B}$ is the event where we do not get any heads.

Again, $|\Omega| = 2^5$. This should not change, as we are studying the same probabilistic game.

Note that $|\overline{B}| = 1$, since there is only one outcome where we do not get any heads (the outcome $TTTTT$).

Since we have a uniform probability space, we have that:

$$\Pr[\overline{B}] = \frac{|\overline{B}|}{|\Omega|} = \frac{1}{2^5}$$

So we have that:

$$\Pr[B] = 1 - \Pr[\overline{B}] = 1 - \frac{1}{2^5}$$

Catalog of LaTeX Commands

$\overline{A}$ - `\overline{A}` | $\Pr[A]$ - `\Pr[A]`