CSE 5852: Lecture 2

Jonathan Huang

September 8, 2016

Today we'll cover some background in probability theory. This will be a brief review, students should consult a probability text (such as [Gut12]) or consider taking a class in the math department.

1 Probability Theory

We will refer to a set of outcomes by Ω. In this class, we will consider finite outcome spaces. Example a six sided dice could come up as a number from $1, 2, 3, 4, 5$ or 6. Thus, $\Omega = \{1, 2, 3, 4, 5, 6\}$.

An event $E \in \Omega$ is a subset of Ω. For example, the dice coming up even can be described as $E = \{2, 4, 6\}$. Since events are subsets of a larger space they can be operated on using set operations. For example, define the event E' as the dice coming up divisible by 3 that is $E' = \{3, 6\}$. Then $E \cap E' = \{6\}$ defines the event where the roll was even and divisible by 3.

Definition 1. *$\mathcal{E}$, a set of events is a partition if $\forall E_1, E_2 \in \mathcal{E}, E_1 \cap E_2 = \emptyset$, and $\forall e \in \Omega$, then there exists $E \in \mathcal{E}$ such that $e \in E$. The second condition can alternatively be written as $\cup_{E_i \in \mathcal{E}} E_i = \Omega$.*

Example of partitions (considering the outcome space as the draw of a single card from a standard deck of cards):

- E_1 = all hearts, E_2 = all clubs, E_3 = all spades, E_4 = all diamonds
  $\mathcal{E} = \{E_1, E_2, E_3, E_4\}$
- E_1 = all cards, $\mathcal{E} = \{E_1\}$
- $\mathcal{E}$ contains 52 sets each containing a single unique card.

Some examples that are not a partition:

- E_1 = all hearts, E_2 = all aces, E_3 = all clubs and spades, E_4 = all diamonds
  $\mathcal{E} = \{E_1, E_2, E_3, E_4\}$ is not a partition because $E_2 \cap E_3 \neq \emptyset$

Definition 2. *A set of events $\mathcal{F} \subset 2^\Omega$ is called a σ-algebra if the following are true:*

1. *$\emptyset \in \mathcal{F}$.*
2. *For all $E \in \mathcal{F}$, $E^c \in \mathcal{F}$. (E^c represents of complement of E).*

3. *For any* $E_1, E_2 \in \mathcal{F}$, $E_1 \cup E_2 \in \mathcal{F}$.

Some basic facts about σ-algebra:

1. $\Omega \in \mathcal{F}$.
2. For all $E_1, E_2 \in \mathcal{F}, E_1 \cap E_2 \in \mathcal{F}$

Some basic examples of $\mathcal{F}$ based on our above dice example:

1. $\mathcal{F} = \{\emptyset, \{1,2,3,4,5,6\}\}$.
2. $\mathcal{F} = 2^{\Omega}$. (This is the power set -set of all possible subsets)
   - Contains $\emptyset$
   - Complement of any subset E is also a subset E^c.
   - If E_1 and E_2 are in $\mathcal{F}$ then $E_1 \cup E_2 \in \mathcal{F}$
3. $\mathcal{F} = \{\emptyset, \{1,2,3,4,5,6\}, \{1,2,3\}, \{4,5,6\}\}$.

Definition 3. *Let* $(\Omega, \mathcal{F})$ *where* $\mathcal{F}$ *is a* σ*-algebra. Then, a function* $\Pr : 2^{\Omega} \to [0,1]$ *is said to be a probability measure if the following hold:*

1. $\Pr[\emptyset] = 0$.
2. $\Pr[\Omega] = 1$.
3. *For all* $E_1, E_2 \in \mathcal{F}$, *such that* $E_1 \cap E_2 = \emptyset$, $\Pr[E_1 \cup E_2] = \Pr[E_1] + \Pr[E_2]$.

We can define a probability measure for the die tossing example, setting each set of size 1 to occur with probability 1/6. Then the probability of $\Pr[\{2,4,6\}] = 1/2$. We can also define a probability measure for drawing a card where the probability of any unique card is 1/52. **Note:** If we define our probability measure on every individual event, it is immediately defined for every subset of events. Think about why this is true.

Definition 4. *The* conditional probability *of* E_1 *conditioned on* E_2, *denoted* $\Pr[E_1|E_2]$ *is defined as* $\frac{\Pr[E_1 \cap E_2]}{\Pr[E_2]}$ *when* $\Pr[E_2] \neq 0$.[1]

Note that conditioning on E_2 this can increase, decrease, or not change the probability of the event E_1. An important concept throughout this course will be the notion of independence, this means that one event does not effect the probability of the other event.

Definition 5. *The events* E_1, E_2 *are said to be independent if* $\Pr[E_1 \cap E_2] = \Pr[E_1]\Pr[E_2]$. *(When* $\Pr[E_2] \neq 0$*).*[2]

[1] Conditioning on an event with probability 0 does not make sense as it will never happen.

[2] If $\Pr[E_1] \neq 0$ and $\Pr[E_2] \neq 0$, an alternative formulation of this definition is that $\Pr[E_1|E_2] = \Pr[E_1]$.

1.1 Some basic manipulations

Proposition 1. $\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B]$.

Theorem 1 (Bayes' theorem)**.** $\Pr[A|B] = \frac{\Pr[B|A]\Pr[A]}{\Pr[B]}$.

Proof. By rearranging terms we see that

$$\Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]} = \frac{\Pr[A]\Pr[B]}{\Pr[B]} = \Pr[A]$$

Similarly, $\Pr[B|A] = \Pr[B]$.[3] □

2 Defining perfect secrecy

As a quick preview of the next class, we know have enough machinery to define perfect secrecy. What we want is that the plaintext is independent of the ciphertext. We'll cover this more next time.

References

[Gut12] Allan Gut. *Probability: a graduate course*, volume 75. Springer Science & Business Media, 2012.

[3] Assuming that $\Pr[A] \neq 0$ and $\Pr[B] \neq 0$.