CS 591-06, Lecture 8

Jared Saia
University of New Mexico

Class Outline

A reasonable probability is the only certainty. - E.W. Howe

- Intro to probability theory
- Some basic Probability definitions and facts
- Linearity of Expectation
- Union Bounds

Intro to Probability Theory

Defns:

- An *Event Space* is a set of "events" which is closed under complement and union.
- A *Probability Function* P is a mapping from an event space, Γ, to the real numbers such that:
  - For all $\gamma \in \Gamma$, $0 \leq P(\gamma) \leq 1$
  - $P(\Omega) = 1$, where Ω is the set containing all atomic events and their complements.
  - For mutually disjoint events, $\gamma_1, \gamma_2, \ldots, \gamma_l$,

$$P(\bigcup_{i=1}^{l} \gamma_i) = \sum_{i=1}^{l} P(\gamma_i)$$

Example

Consider event space when we flip a coin. Let γ_1 be the event that the coin turns up heads.

Then $\Gamma = \{\{\}, \gamma_1, \bar{\gamma_1}, \{\gamma_1 \cup \bar{\gamma_1}\}\}$

and:

- Every element in Γ has probability of occurence between 1 and 0.
- $P(\Omega) = P(\{\gamma_1 \cup \bar{\gamma_1}\}) = 1$
- Probabilities of events that are disjoint (can't occur together) add.
  E.g. $P(\gamma_1 \cup \bar{\gamma_1}) = P(\gamma_1) + P(\bar{\gamma_1})$

Basic Facts

- **Complement Fact:** For any event γ, $P(\bar{\gamma}) = 1 - P(\gamma)$
- **Independence Fact** A set of events $\{\gamma_i | i \in I\}$, is said to be *independent* if for any subset S of I, $P(\bigcap_{i \in S} \gamma_i) = \prod_{i \in S} P(\gamma_i)$

In Class Exercise

Imagine we flip two independent coins. Let γ_1 be the event that the first coin is heads, γ_2 be the event that the second coin is heads.

Let $P(\gamma_1) = 1/2$ and $P(\gamma_2) = 1/2$.

- Question 1: What is the probability that both coins turn up heads? (Hint: Use the fact that γ_1 and γ_2 are independent).
- Question 2: What is the probability that at least one coin turns up heads? (Hint: Use the complement fact and independence of the events $\bar{\gamma_1}$ and $\bar{\gamma_2}$).

Useful Algebraic Tricks

Some useful algebraic facts to know:

- $(1 - x) \leq e^{-x}$
- $e^x * e^y = e^{x+y}$

Sailors and Cabins

There are n sailors and n cabins and sailor i is assigned to cabin i.

After a night of drunken revelry, the sailors return to ship and each of them chooses uniformly at random one of n cabins to sleep in.

- Question: What is (an upper bound on) the probability that *no* sailor sleeps in his own cabin?

Sailors and Cabins

- Let γ_i be the event that sailor i sleeps in his own cabin.
- Note that for all i, $P(\gamma_i) = 1/n$
- Note that all of the events γ_i are independent.
- We want $P(\bigcap_{i=1}^{n} \bar{\gamma}_i)$

Sailors and Cabins

$$
\begin{aligned}
P(\bigcap_{i=1}^{n} \bar{\gamma}_i) &= \prod_{i=1}^{n} P(\bar{\gamma}_i) && (1)\\
&= \prod_{i=1}^{n} (1 - P(\gamma_i)) && (2)\\
&= \prod_{i=1}^{n} (1 - 1/n) && (3)\\
&\leq \prod_{i=1}^{n} e^{-1/n} && (4)\\
&\leq e^{-1} && (5)
\end{aligned}
$$

The first step holds by Independence, and the second step holds by Complement.

Random Variables

- A *Random Variable* is a variable which randomly takes on some value in the real numbers.

Example Random Variables:

- Let X be 1 with probability 1/2 and 0 with probability 1/2
- Let Y take on a value in the range $\{1, \ldots, n\}$ uniformly at random.
- Let $Z = X + Y$.
- Let $W = X * Y$.

Expectation

The *Expectation* of a random variable X (written $E(X)$), which takes on values in some range R, is defined as follows:

- $E(X) = \sum_{r \in R}(r * P(X = r))$

Linearity of Expectation

Linearity of Expecation Fact: If there are random variable $X, X_1, \ldots, X_n$, such that $X = \sum_{i=1}^{n} X_i$, then

- $E(X) = \sum_{i=1}^{n} E(X_i)$

Example:

Let the variable X_i be 1 if the i-th flip of a coin is heads and 0 otherwise and say that $E(X_i) = 1/2$. Let $X = \sum_{i=1}^{n} X_i$. Then:

$E(X) = n/2$

More Drunken Sailors

There are n sailors and n cabins and sailor i is assigned to cabin i.

After a night of drunken revelry, the sailors return to ship and each of them chooses uniformly at random one of n cabins to sleep in.

- What is the expected number of sailors that actually sleep in their own cabin?

Sailors and Cabins

- Let r_i be an random variable which has value one of sailor i sleeps in his own cabin and 0 otherwise.
- $E(r_i) = (1/n)$
- Let $R = \sum_{i=1}^{n} r_i$
- Then we know by Linearity of Expectation:

$$
\begin{aligned}
E(R) &= E(\sum_{i=1}^{n} r_i) && (6)\\
&= \sum_{i=1}^{n} E(r_i) && (7)\\
&= \sum_{i=1}^{n} 1/n && (8)\\
&= 1 && (9)
\end{aligned}
$$

Union Bound

Union Bound Fact: Let Γ be any event space, P be any probability function and $\gamma_1, \gamma_2, \ldots \gamma_n$ be any events in Γ. Then:

$$P(\bigcup_{i=1}^{n} \gamma_i) \leq \sum_{i=1}^{n} P(\gamma_i)$$

Example:

Let γ_1 be the event that coin 1 is heads, γ_2 be the event that coin 2 is heads. Then:

$$P(\gamma_1 \bigcup \gamma_2) \leq P(\gamma_1) + P(\gamma_2)$$

Drunk Sailors, the next day

There are n sailors and n mugs (of coffee). The i-th mug belongs to sailor i.

The next morning, each sailor wakes up and randomly takes *exactly* one mug.

- **Question: What is an upper bound on the probability that one of the first three sailors gets the first mug?**

Drunk Sailors, the next day

- For $i = \{1, 2, 3\}$, let γ_i be the event that the i-th sailor gets the first mug.
- We want $P(\gamma_1 \cup \gamma_2 \cup \gamma_3)$
- By the Union Bound, $P(\gamma_1 \cup \gamma_2 \cup \gamma_3) \leq P(\gamma_1) + P(\gamma_2) + P(\gamma_3)$
- So $P(\gamma_1 \cup \gamma_2 \cup \gamma_3) \leq 3/n$

Another Union Bound Example

Imagine an Attack-Resistant Peer-to-peer network over n peers.

- Assume that for any fixed set of $n/2$ peers, the probability that deletion of that set foils the network is p_f.
- There are n choose $n/2$ sets of size $n/2$
- Hence the probability that no set exists such that its deletion will foil the network is no more than $p_f * (n$ choose $n/2)$.