This handout recaps the concept of independent events.

1 Recap of 2/4 and 2/6

The conditional probability of event $A$ given $B$ as

$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$

implying that

$$P(A \cap B) = P(A|B)P(B).$$

We say $A$ and $B$ are independent iff

$$P(A|B) = P(A).$$

If $A$ and $B$ are independent,

$$P(A \cap B) = P(A|B)P(B) = P(A)P(B),$$

and again, if $A$ and $B$ are independent,

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{P(B)P(A)}{P(A)} = P(B).$$

Note that if $P(A \cap B) = P(A)P(B)$, $A$ and $B$ are independent since

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(A)P(B)}{P(B)} = P(A),$$

and similarly, if $P(B|A) = P(B)$, $A$ and $B$ are independent.

As we discussed in class, except for trivial cases, independent events are not disjoint. Independence from the point of view of set theory is a special way sets can intersect.

The trivial case where events are disjoint and independent is when one of the sets is an empty set.

**HW 1** Empty sets and sample spaces. Let $\Omega$ be the sample space. Note that $\subset$ means a strict subset, namely $\{1, 2\} \subset \{1, 2, 3\}$, but $\{1, 2\} \not\subset \{1, 2\}$. On the other hand, $\subseteq$ also includes equality, so $\{1, 2\} \subseteq \{1, 2, 3\}$ and $\{1, 2\} \subseteq \{1, 2\}$.

1. Show that for all nonempty sets $A \subseteq \Omega$, $A$ and $\emptyset$ (the empty set) are independent.

2. Show that for all sets $A \subset \Omega$, $A$ and $\Omega$ are independent.

3. If a nonempty $A \subset \Omega$, is $A$ independent of itself ($A$)?

4. What should $A$ satisfy so that $A$ is independent of $A$?
2 Examples

1. Binary symmetric channels (BSC) Let the input of the channel be $X$ while the output of the channel is $Y$. A BSC is defined by the conditional probabilities

$$P(Y = 1|X = 0) = P(Y = 0|X = 1) = \epsilon.$$  

Note that we automatically get $P(Y = 0|X = 0) = 1 - P(Y = 1|X = 0) = 1 - \epsilon$ and $P(Y = 1|X = 1) = 1 - P(Y = 0|X = 1) = 1 - \epsilon$. Recall that given a particular event, conditional probabilities add up to 1 just like regular probabilities.

Suppose the input data satisfies $P(X = 1) = p$. Namely, 1 is sent into the channel with probability $p$.

As we computed in class

$$P(X = 0, Y = 0) = P(X = 0)P(Y = 0|X = 0) = (1 - p)(1 - \epsilon)$$
$$P(X = 0, Y = 1) = P(X = 0)P(Y = 1|X = 0) = (1 - p)\epsilon$$
$$P(X = 1, Y = 0) = P(X = 1)P(Y = 0|X = 1) = p\epsilon$$
$$P(X = 1, Y = 1) = P(X = 1)P(Y = 1|X = 1) = p(1 - \epsilon).$$

Therefore

$$P(Y = 0) = P(Y = 0, X = 0) + P(Y = 0, X = 1) = (1 - p)(1 - \epsilon) + p\epsilon$$
$$P(Y = 1) = P(Y = 1, X = 0) + P(Y = 1, X = 1) = (1 - p)\epsilon + p(1 - \epsilon) = 1 - P(Y = 0).$$

HW 2 When trying to communicate over the BSC described above, suppose the receiver (at the output) sees a 0. Either a 0 or a 1 could have been transmitted, the receiver has to figure out what is the probability of the input given the output. What is $P(X = 0|Y = 0)$ and $P(X = 1|Y = 0)$? What is $P(X = 1|Y = 1)$ and $P(X = 0|Y = 1)$?

In particular, if $\epsilon = \frac{1}{2}$, $P(Y = 1|X = 1) = 1 - \epsilon = \frac{1}{2}$, while $P(Y = 1|X = 0) = \epsilon = \frac{1}{2}$. Furthermore,

$$P(Y = 1) = P(Y = 0, X = 0) + P(Y = 0, X = 1) = (1 - p)\epsilon + p(1 - \epsilon) = \frac{1}{2}.$$  

This implies that $X$ and $Y$ are independent of each other when $\epsilon$ is $\frac{1}{2}$. It is impossible in this case to obtain any information about $X$ by looking at $Y$—and in general the following statement is true: if $X$ and $Y$ are independent, you cannot obtain any information about $X$ by looking at $Y$ (or vice versa).

2. Pairwise independence Consider a binary sequence $X_1, X_2, X_3$. Our sample space will be the set of all values $(X_1, X_2, X_3)$ can take, and the probabilities we assigned them were

<table>
<thead>
<tr>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
<th>$P(X_1, X_2, X_3)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$\frac{1}{4}$</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$\frac{1}{4}$</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>$\frac{1}{4}$</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$\frac{1}{4}$</td>
</tr>
</tbody>
</table>

It is easy to see that

$$P(X_1 = 1) = \frac{1}{2},$$
$$P(X_2 = 1) = \frac{1}{2},$$
$$P(X_3 = 1) = \frac{1}{2}.$$
while

\[ P(X_2 = 1 | X_1 = 1) = \frac{1}{2}, \]
\[ P(X_2 = 1 | X_1 = 0) = \frac{1}{2}, \]
\[ P(X_3 = 1 | X_1 = 1) = \frac{1}{2}, \]
\[ P(X_3 = 1 | X_1 = 0) = \frac{1}{2}, \]
\[ P(X_3 = 1 | X_2 = 1) = \frac{1}{2}, \]
\[ P(X_3 = 1 | X_2 = 0) = \frac{1}{2}, \]

namely \( X_1 \) and \( X_2 \) are independent, \( X_2 \) and \( X_3 \) are independent, as well as the pair \( X_3 \) and \( X_1 \). However, given \( X_1 \) and \( X_2 \), we know what \( X_3 \) is. We say \( X_1, X_2, X_3 \) are pairwise independent, but not fully independent.

**HW 3**

1. We say binary \( X_1, X_2, X_3 \) are fully independent (from now on, we will just use independent to mean fully independent) if in addition to pairwise independence, \( P(X_i = 1 | X_j, X_k) = P(X_i = 1) \) for all \( i \neq j \neq k \neq i \) and \( i,j,k \in \{1,2,3\} \). Note that the above notation means that you need to check whether all the following are equal: \( P(X_i = 1 | X_j = 0, X_k = 0), P(X_i = 1 | X_j = 0, X_k = 1), P(X_i = 1 | X_j = 1, X_k = 0), \) and \( P(X_i = 1 | X_j = 1, X_k = 1) \). What do you think the conditions should be for \( X_1, X_2, X_3, X_4 \) to be independent?

2. This is a counting problem. Consider \( n \) bits, \( X_1, X_2, \ldots, X_n \). \( X_i \) are binary. Let \( J \subseteq \{1, \ldots, n\} \), and let the size of \( J \) be \(|J|\). If \( J = \{j_1, \ldots, j_{|J|}\} \), denote by \( X_J \) the sequence \( X_{j_1}, X_{j_2}, \ldots, X_{j_{|J|}} \).

We say that \( X_1, \ldots, X_n \) are independent if for all \( J \subset \{1, \ldots, n\} \) (meaning \( J \) is any subset, but not the set \( \{1, \ldots, n\} \) itself, and for all \( i \notin J \), \( P(X_i = 1 | X_J) = P(X_i = 1) \) (see note on notations in the previous subproblem). If you verify for independence this way, how many conditions must you compute before you know \( X_1, \ldots, X_n \) are independent?

Quite hard, but a significant bonus set of problems: (a) Are we doing too many tests (each test is checking one equality)? Why? (b) How would you reduce the number of tests? (c) What does it tell you about how much freedom you have to assign probabilities if you know \( X_1, \ldots, X_n \) are independent? The completely correct answer pushes you up by half a grade (unless you already have a A+). If, in addition, I am convinced you have a good insight (as opposed to reading up many sources—though it will be hard for this one), another half a grade.

3. Consider a variation of the example we did in class. The sample space is the set of all possible sequences of three bits. The probabilities we assign are as follows

<table>
<thead>
<tr>
<th>( X_1 ) ( X_2 ) ( X_3 )</th>
<th>( P(X_1, X_2, X_3) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0</td>
<td>1/9</td>
</tr>
<tr>
<td>0 0 1</td>
<td>1/18</td>
</tr>
<tr>
<td>0 1 0</td>
<td>2/9</td>
</tr>
<tr>
<td>0 1 1</td>
<td>1/9</td>
</tr>
<tr>
<td>1 0 0</td>
<td>1/9</td>
</tr>
<tr>
<td>1 0 1</td>
<td>1/18</td>
</tr>
<tr>
<td>1 1 0</td>
<td>2/9</td>
</tr>
<tr>
<td>1 1 1</td>
<td>1/9</td>
</tr>
</tbody>
</table>
Are $X_1, X_2, X_3$ pairwise independent? Independent? Be careful with computations, feel free to use MATLAB or MATHEMATICA or any computational assistance.