

Assignment 2: (Un)Fairness and Probability

Machine Learning

Fall 2019

🔗 Learning Objectives

- The concept of independence and conditional independence
- The basic components of a Bayesian Networks (BN)
- The rules of d-separation to compute conditional independence relationships in a BN
- The Compas recidivism risk algorithm controversy

Note: This assignment is a bit longer than average. We are trying to shift things so that weekend assignments are a bit longer and the assignments during the week are a bit shorter. If you decide to ask for an extension, we suggest that you prioritize looking at the COMPAS Model section, so that you are prepared for our class discussion.

A quick thanks to two former students, Micah Reid (currently a CA) and Miranda Lao for their contributions to this and the following assignment. As part of their final project, they explored metrics of fairness and disparity and proposed assignment extensions (pieces of which appear in this and the following assignment).

1 COMPAS Model: Race, Criminal Justice, and Machine Learning

⚠️ Notice

We are going to think about race and criminal justice in the United States. Before we dive into this, we want to acknowledge:

- This is a complex and intricate issue that involves policy, society, technology, individual beliefs/values, and history. This topic directly (but not equally) impacts the lives of many people.
- We all have our own lenses through which we view the world.
- In this class, we will scratch the surface of the way the US justice system works. Your instructors are not criminal justice experts, but they do care about this topic. We are also continuing to learn more.
- This topic will likely be uncomfortable to grapple with regardless of your background and identity. It may resonate differently with each of us. We (Sam/Carrie) are available in person and via email, if you would like to discuss how we can best support you in class. We are planning to have some group discussion in class. One method of support could be pairing you with a partner of your choosing for this discussion. Another could be including your ideas about how class discussion can be informative and challenging without creating unnecessary pain. Please reach out to us if you have any concerns or want to discuss this more.

A few basics about the US criminal justice system.

A police officer can place a person under arrest. However, an arrest does not necessarily mean that person committed a crime (both in fact and in a legal sense). Legally, someone is considered innocent until proven guilty in court. However, arrested people are often held in jail for months before trial (this is called pretrial detention). To get out of jail before

trial, the arrested person can post bail. Bail is a considerable amount of money (“money bond”) that is given to the court to ensure the person shows up to trial. As you might guess, bail represents a way people with money are treated differently by the system than people without money. (Optional: For more on bail, listen to [Episode 62](#) of the podcast [Ear Hustle](#)).

Legally, a person is considered guilty if they are convicted in court. Practically, innocent people are sometimes convicted. People with a lot of money can hire many lawyers who will work many days, weeks, or years, fighting the case. People without funds for a lawyer will be assigned a public defender. Public defenders are often overwhelmed, and might have just a minute to look over the details of a case, right before trial.

If you are interested in this topic and want to hear stories from incarcerated people, we recommend listening to the podcast [Ear Hustle](#). (This is optional)

Exercise 1 🧠 (20 minutes)

- (a) (Read the Report of [The Sentencing Project to the United Nations Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance](#).

This article is intended to provide some background information on criminal justice and race in the US.

1.1 Confusion Matrices

Before we dig into the articles on the COMPAS algorithm, we want to introduce refresh on the confusion matrix and some related terms. These will be essential to making sense of the debate below and for learning about different metrics of fairness. The binary confusion matrix is a 2x2 chart where the y axis is whether the model output predicts a positive or negative response, and the x axis is whether or not the actual or measured output is positive or negative. This gives us four quadrants: true positives, false positives, true negatives, and false negatives.

	Actual Positive	Actual Negative
Predicted Positive	True Positive (TP)	False Positive (FP)
Predicted Negative	False Negative (FN)	True Negative (TN)

It is worth stating that the confusion matrix only works for classification, so if the model outputs are continuous, a cutoff threshold may be necessary. These confusion matrix metrics can be more informative than more general accuracy metrics like log loss, because they can pinpoint the strong and weak points of a model. The four quadrants can also be used to calculate a number of metrics that can show how the model performs with regards to different concerns.

These definitions are relatively straightforward. We call the total number of actual positives the **condition positive (P)**, where $P = TP + FN$. The total number of actual negatives is the **condition negative (N)**, where $N = FP + TN$.

A variety of combinations of these 4 quadrants (TP, FP, FN, and TN) are found in the building blocks widely used fairness metrics in machine learning. These building blocks include:

- **True Positive Rate (TPR):** $TPR = \frac{TP}{P}$

- **True Negative Rate (TNR):** $TNR = \frac{TN}{N}$
- **False Positive Rate (FPR):** $FPR = \frac{FP}{P}$
- **False Negative Rate (FNR):** $FNR = \frac{FN}{P}$
- **Positive Predictive Value (PPV):** $PPV = \frac{TP}{TP+FP}$
- **Negative Predictive Value (NPV):** $NPV = \frac{TN}{TN+FN}$
- **False Discovery Rate (FDR):** $FDR = \frac{FP}{TP+FP}$
- **False Omission Rate (FOR):** $FOR = \frac{FN}{TN+FN}$

It may be helpful to check out this [write-up from Google of the loan example](#). The visualizations are good.

Exercise 2 🧠 (30 minutes)

Consider the following confusion matrix:

	Actual Positive	Actual Negative
Predicted Positive	100	20
Predicted Negative	5	40

- Compute the metrics listed above for this confusion matrix.
- If you've completed part a, you may have noticed that each metric above other than CSI has an inverse (for example the True Positive Rate is equal to 1 - False Negative Rate). Find the inverse for each of the metrics listed above.
- Consider the following scenarios: imagine you are creating a model to determine whether someone should be brought in for an additional cancer screening based upon initial test results. Which metric would you care most about minimizing? What if instead you were creating a model to determine whether a defendant should be prosecuted for a low level offense?

Exercise 3 🧠 (90 minutes)

In this module, we'll be spending time talking about the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) algorithm, produced by the company Northpointe, Inc. COMPAS was intended to assess the risk of recidivism. This is a well-known algorithm in machine learning communities.

Below we will provide you a list of readings on this topic. As you read, please prepare to reflect on the following themes:

- Social justice in a non-ideal world.

- The roles of machine learning engineers and the roles of other professional roles in the application of machine learning in our society.
- The major things that you would want to consider in this type of undertaking.
- Framing things mathematically versus from a social justice standpoint.
- The level of technical debate in model choices that is brought up in this discussion (especially in the technical responses).

(a) First, read the [ProPublica article](#).

(b) Next, you'll read the technical details of the ProPublica analysis.

We would like to be clear about when the COMPAS metric is applied. It is applied after someone is arrested, and the prediction COMPAS gives is if that person will be arrested again. A person who was arrested twice could be legally and actually innocent. It is important to be clear in our language that these are arrested people, and not convicted criminals. The term recidivism, which is generally defined as a criminal who commits a second crime, is used in the readings. ProPublica actually redefines recidivism as “a criminal offense that resulted in a jail booking and took place after the crime for which the person was COMPAS scored.” Here, ProPublica conflates an arrest for a crime with a conviction for that crime. Note that a jail booking is pre-trial, and different than prison, which is post-trial and conviction. This language is also used by the Northpointe rebuttal. Carrie would argue that since these are not people who have been yet convicted of crimes, they are not necessarily recidivists, and the language in the readings should be corrected.

Please read [How We Analyzed the COMPAS Recidivism Algorithm](#).

(c) Please read the [Northpointe rebuttal](#). This is a long reading. It has a lot of jargon, and some acronyms are not defined. We strongly suggest limiting yourself to 60 minutes for this reading (perhaps read the conclusion early on). You may consider working with a classmate on this reading, so you can both discuss what you think the author is saying. We're including this whole reading here because we would like you to engage with the real-world material.

Exercise 4 (40 minutes)

- (a) Please summarize what you see as the key parts of the ProPublica and Northpointe cases. You can use words, diagrams, concept maps, or another method that works for you.
- (b) Reflect on what you've just read. We think the themes brought up above will provide good fodder for your response, but please feel free to take it in any direction. Aim for around two paragraphs in your response.

2 Motivation and Context for Probability

In the last assignment we learned the basic definition of a probability and acquired some very powerful rules for working with probabilities. In the rest of this assignment you'll be taking these ideas and extending them in the following significant ways.

- You'll learn a graphical way to represent the relationships between probabilities that will make it much easier to work

with large probabilistic models.

- You'll be taking the ideas of probability using them to derive a whole new way of approaching the classification problem in machine learning.

3 Product Rule and Marginalization for Random Variables

↔ Recall: Product Rule and Marginalization for Events

Last assignment we learned about two very powerful techniques for computing the probability of events.

- We learned the product rule (or conjunction rule), which states that for any two events \mathcal{A} and \mathcal{B} ,

$$\begin{aligned} p(\mathcal{A}, \mathcal{B}) &= p(\mathcal{A})p(\mathcal{B}|\mathcal{A}) \\ &= p(\mathcal{B})p(\mathcal{A}|\mathcal{B}) . \end{aligned} \tag{1}$$

- We learned the rule of marginalization, which states that for any two events \mathcal{A} and \mathcal{B} ,

$$p(\mathcal{A}) = p(\mathcal{A}, \mathcal{B}) + p(\mathcal{A}, \neg\mathcal{B}) . \tag{2}$$

It turns out that these rules can be modified slightly to apply to random variables as well (instead of just events).

3.1 Product Rule for Random Variables

Suppose we have two random variables X and Y . If we want to know the probability of random variable X taking on value x (it is common to use a lower case letter to refer to a particular value of a random variable) and random variable Y simultaneously taking on value y , we can decompose the joint probability (the probability of both of these things occurring simultaneously) using the product rule.

$$\begin{aligned} p(X = x, Y = y) &= p(X = x)p(Y = y|X = x) && \text{or equivalently,} \\ &= p(Y = y)p(X = x|Y = y) \end{aligned} \tag{3}$$

Notice that this looks pretty much identical to Equation 1 except that instead of referencing whether an event happens, we are now referencing a random variable taking on a particular value.

⚠ Notice

It's very common to use the shorthand $p(x, y)$ to refer to $p(X = x, Y = y)$. The motivation for this shorthand is that it is obvious from the context that $p(x, y)$ really means the probability of random variable X taking on value x and random variable Y taking on value y . In this assignment we're going to avoid using this shorthand, but we will start using the shorthand in future assignments (we'll warn you when we start using it). Also, you may see this notation used in external resources, so it helps to know about it.

3.2 Marginalization for Random Variables

Again, suppose we have two random variables X and Y . We are interested in computing $p(X = x)$, but suppose it is difficult to compute this probability directly. Just as we did for events in the last assignment, we can compute $p(X = x)$ by marginalizing out the random variable Y . For simplicity, let's assume that Y can only take on integer values from 1 to k . We can write the marginal distribution $p(X = x)$ in the following way.

$$p(X = x) = \sum_{y=1}^k p(X = x, Y = y) \quad (4)$$

You should notice that this equation is similar to Equation 2 except that instead of summing over the probability for the two possible outcomes with respect to the event \mathcal{B} (i.e., \mathcal{B} either happens or it does not), we are now summing over the k possible values that Y could take. Random variables don't necessarily have to take on values from 1 to k . In general, if the random variable Y can take on any value from some discrete set of values \mathcal{Y} (we are using the calligraphic font because we are referring to a set), then the marginal distribution of X can be written as:

$$p(X = x) = \sum_{y \in \mathcal{Y}} p(X = x, Y = y) . \quad (5)$$

Notice that Equation 4 is a special case of Equation 5 where $\mathcal{Y} = \{1, 2, \dots, k\}$.

Exercise 5 (15 minutes)

This exercise is from the [Wikipedia article on marginal distribution](#).

Notice

Strictly speaking a random variable only takes on real numbers as its value (i.e., a random variable cannot take on the value of “blue”). That said, it's common to see folks bend this rule a bit by allowing the random variable to take on values that are not real numbers (e.g., you will see that in the Wikipedia article linked above). Allowing for random variables to have non-numeric values doesn't really change the math except it makes it meaningless to compute quantities such as the mean. Since in many cases allowing random variables to take on non-numeric values will make things clearer, we will allow this in our materials.

Suppose you want to compute the probability that a pedestrian will be hit by a car, while crossing the road at a pedestrian crossing, without paying attention to the traffic light (a bit morbid, we know). Let H be a discrete random variable taking on the value “hit” if the pedestrian is struck and “not hit” if the pedestrian makes it safely across. Let L (for traffic light) be a discrete random variable taking on the value “red” when the light is red, “yellow” when the light is yellow, and “green” when the light is green. The model that governs the prior probability of the light (L) is as follows.

$$\begin{aligned} p(L = \text{red}) &= 0.2 \\ p(L = \text{yellow}) &= 0.1 \\ p(L = \text{green}) &= 0.7 \end{aligned} \quad (6)$$

The model that governs the conditional probability of H given L is as follows.

$$\begin{aligned}
 p(H = \text{hit} | L = \text{red}) &= 0.01 \\
 p(H = \text{not hit} | L = \text{red}) &= 0.99 \quad \text{Note: the probability of "not hit" = 1 - probability of hit} \\
 p(H = \text{hit} | L = \text{yellow}) &= 0.1 \\
 p(H = \text{not hit} | L = \text{yellow}) &= 0.9 \\
 p(H = \text{hit} | L = \text{green}) &= 0.8 \\
 p(H = \text{not hit} | L = \text{green}) &= 0.2
 \end{aligned}$$

What is $p(H = \text{hit})$?

4 Some Twists on Bayes' Rule

By now hopefully you are starting to feel comfortable with the vanilla form of Bayes' rule. There are a few quite useful variants that we'd like to point out. There are no exercises for you to do here, just add these to your bag of tricks (you'll be leveraging them later in this assignment, so you'll have a chance to solidify them then).

$$p(\mathcal{A} | \mathcal{B}) = \frac{p(\mathcal{B} | \mathcal{A})p(\mathcal{A})}{p(\mathcal{B})} \quad \text{as a reminder, here is vanilla Bayes' rule} \quad (7)$$

$$p(\mathcal{A}, \mathcal{B} | \mathcal{C}) = \frac{p(\mathcal{C} | \mathcal{A}, \mathcal{B})p(\mathcal{A}, \mathcal{B})}{p(\mathcal{C})} \quad \text{you can bring over multiple events} \quad (8)$$

$$p(\mathcal{A} | \mathcal{B}, \mathcal{C}) = \frac{p(\mathcal{B} | \mathcal{A}, \mathcal{C})p(\mathcal{A} | \mathcal{C})}{p(\mathcal{B} | \mathcal{C})} \quad \text{you can leave an event to the right of the conditioning bar} \quad (9)$$

5 Independence and Conditional Independence

Two of the most important concepts in probability theory are independence and the closely related concept of conditional independence. These ideas are important because they let you analyze probabilistic quantities in isolation. For instance, if you know that two events that you are interested in predicting are independent of each other, then you can make a model of each event in isolation. Modeling events independently can make your life much easier since you don't have to consider how the two events interact. Next, we'll make this high-level idea precise.

5.1 Independence

The product rule of probability can be simplified when two events, \mathcal{A} and \mathcal{B} are independent. As an example, suppose \mathcal{A} represents the event that the first flip of a coin comes up heads and event \mathcal{B} is the event that the second flip of the same coin comes up heads. Since whether or not \mathcal{A} occurs tells us nothing about whether \mathcal{B} would occur, we say that \mathcal{A} and \mathcal{B} are independent events (we use the notation $\mathcal{A} \perp\!\!\!\perp \mathcal{B}$ to indicate that \mathcal{A} is independent of \mathcal{B}). An event \mathcal{A} is independent of another event \mathcal{B} if and only if the following condition holds.

$$p(\mathcal{A}, \mathcal{B}) = p(\mathcal{A})p(\mathcal{B}) \quad (10)$$

A direct consequence of Equation 10 is that if $\mathcal{A} \perp\!\!\!\perp \mathcal{B}$, then

$$\begin{aligned} p(\mathcal{A}|\mathcal{B}) &= p(\mathcal{A}) & \text{and} \\ p(\mathcal{B}|\mathcal{A}) &= p(\mathcal{B}) . \end{aligned}$$

A very similar equation to Equation 10 can be defined for random variables. Two random variables X and Y are independent if and only if the following condition holds for any values x and y .

$$p(X = x, Y = y) = P(X = x)p(Y = y) \quad (11)$$

Similar to the rule for events, $p(X = x|Y = y) = P(X = x)$ if $X \perp\!\!\!\perp Y$.

Exercise 6 (10 minutes)

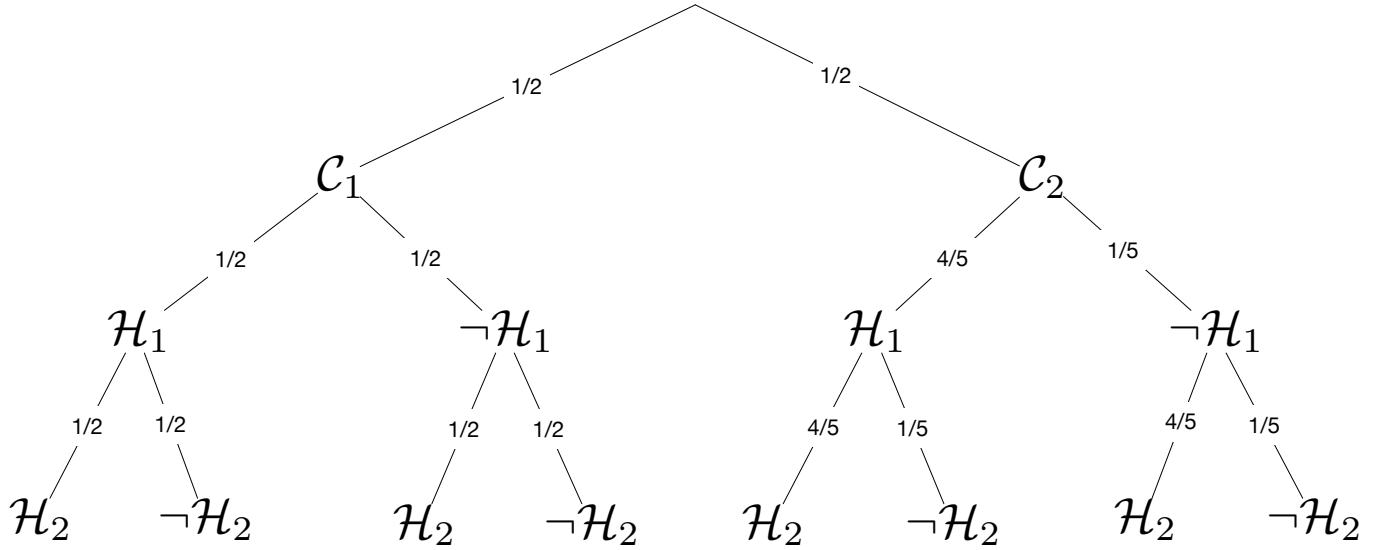
- (a) Provide at least 3 examples of events or random variables that are independent of each other.
- (b) Provide at least 3 examples of events or random variables that are not independent of each other.

5.2 Conditional Independence

Sometimes two events (or two random variables) that are not independent might become independent when conditioned on another event.

Exercise 7 (20 minutes)

As a motivating example for the concept of conditional independence, consider a variant of the coin problem we saw last assignment. A bag contains two coins. Suppose we choose one of the two coins with equal probability. Let \mathcal{C}_1 represent the event that we choose coin 1 and \mathcal{C}_2 represent the event that we choose coin 2. Coin 1 is fair $p(\mathcal{H}|\mathcal{C}_1) = \frac{1}{2}$. Coin 2 is not fair ($p(\mathcal{H}|\mathcal{C}_2) = \frac{4}{5}$). We then flip the coin twice (we don't pick a new coin for the second flip). Let \mathcal{H}_1 represent the event that the first flip comes up heads and \mathcal{H}_2 represent the event that the second flip comes up heads. Are \mathcal{H}_1 and \mathcal{H}_2 independent (i.e., is $\mathcal{H}_1 \perp\!\!\!\perp \mathcal{H}_2$)? To help you get started, here is a tree diagram illustrating the problem.



Given the tree diagram above, is $H_1 \perp\!\!\!\perp H_2$?

It turns out that even though H_1 and H_2 are not independent, they are what's called *conditionally independent* given C_1 (or C_2). Formally, events \mathcal{A} and \mathcal{B} are considered conditionally independent given \mathcal{C} (written $\mathcal{A} \perp\!\!\!\perp \mathcal{B} \mid \mathcal{C}$) if and only if

$$p(\mathcal{A}, \mathcal{B} \mid \mathcal{C}) = p(\mathcal{A} \mid \mathcal{C})p(\mathcal{B} \mid \mathcal{C})$$

Exercise 8 (20 minutes)

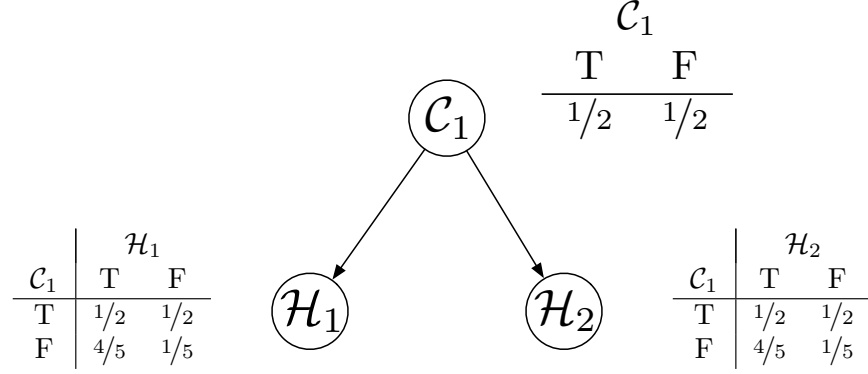
- Show that $H_1 \perp\!\!\!\perp H_2 \mid C_1$. Remember to use the tree above! Notation comment: Interpret this as: $(H_1 \perp\!\!\!\perp H_2) \mid C_1$
- Show that $H_1 \perp\!\!\!\perp H_2 \mid C_2$

The definition of the conditional independence of events extends to random variables. Random variables X and Y are conditionally independent given random variable Z (i.e., $X \perp\!\!\!\perp Y \mid Z$) if and only if the following holds for all x, y, z .

$$p(X = x, Y = y \mid Z = z) = p(X = x \mid Z = z)p(Y = y \mid Z = z) \quad (12)$$

6 Bayesian Networks

The calculations in the previous section were a bit tedious. It would be great if there was some way to reason about the conditional independence properties of two random variables conditioned on some other random variable. Luckily... drum roll... there is! A Bayesian network (sometimes called a Bayesian belief network or a probabilistic directed acyclic graphical model) represents the conditional independence relationships between random variables through a graphical, causal structure. We'll use BN as shorthand for "Bayesian network." Take for instance, the BN that represents the coin problem that we did in the last section.



The graphical structure (edges and nodes in the graph) tell us everything we need to infer the conditional independence properties in the graph (Note that we haven't told you *how* you can extract the conditional independence properties from the graph; that's coming later in the assignment). The tables by each node provide the probability of the event conditioned on whether or not the node's parents (a "parent" of a node, A , is a node B where there is an edge pointing from A to B) happened (T stands for *True* or that the event happens and F stands for *False* or that the event doesn't happen).

The BN provides us with a way of computing any relevant probability (e.g., marginal, conditional, joint) for the nodes in the network. The condition that must hold for any BN is that if we write the joint distribution of all of the random variables (or events, the relationship is the same for either) in the network, it must factorize in the following way (we'll use X_1, X_2, \dots, X_n to represent random variables in the network and we'll define the function $Pa(X_i)$ to return all of the random variables that are parents of X_i).

$$p(X_1, X_2, \dots, X_n) = p(X_1|Pa(X_1)) \times p(X_2|Pa(X_2)) \times \dots \times p(X_n|Pa(X_n)) \quad (13)$$

Back to our coin BN, this means that we can write the joint distribution like so.

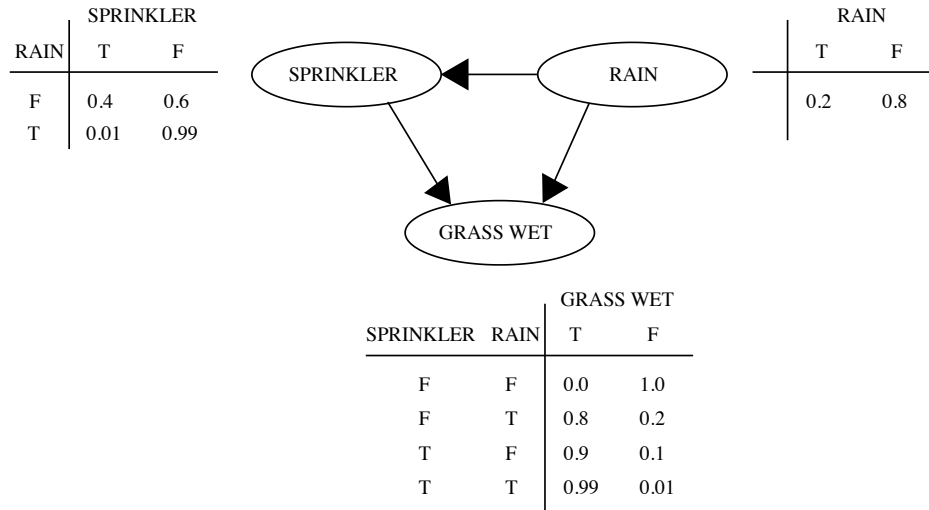
$$p(\mathcal{C}_1, \mathcal{H}_1, \mathcal{H}_2) = p(\mathcal{C}_1)p(\mathcal{H}_1|\mathcal{C}_1)p(\mathcal{H}_2|\mathcal{C}_1) \quad (14)$$

✓ Understanding Check

Make sure you understand how we arrived at Equation 14. Refer back to Equation 13 and hopefully you will see the connection.

Exercise 9 (20 minutes)

Consider the BN below (source: https://en.wikipedia.org/wiki/Bayesian_network#Example).



Compute the following probabilities. For brevity we'll use the first letter of each node to indicate that the corresponding event happens (e.g., we'll use \mathcal{R} to refer to the event "rain").

- (a) $p(\mathcal{R}, \mathcal{G}, \neg \mathcal{S})$
- (b) $p(\mathcal{R})$
- (c) $p(\neg \mathcal{G}, \neg \mathcal{S})$ (hint: marginalize over \mathcal{R})

6.1 D-separation

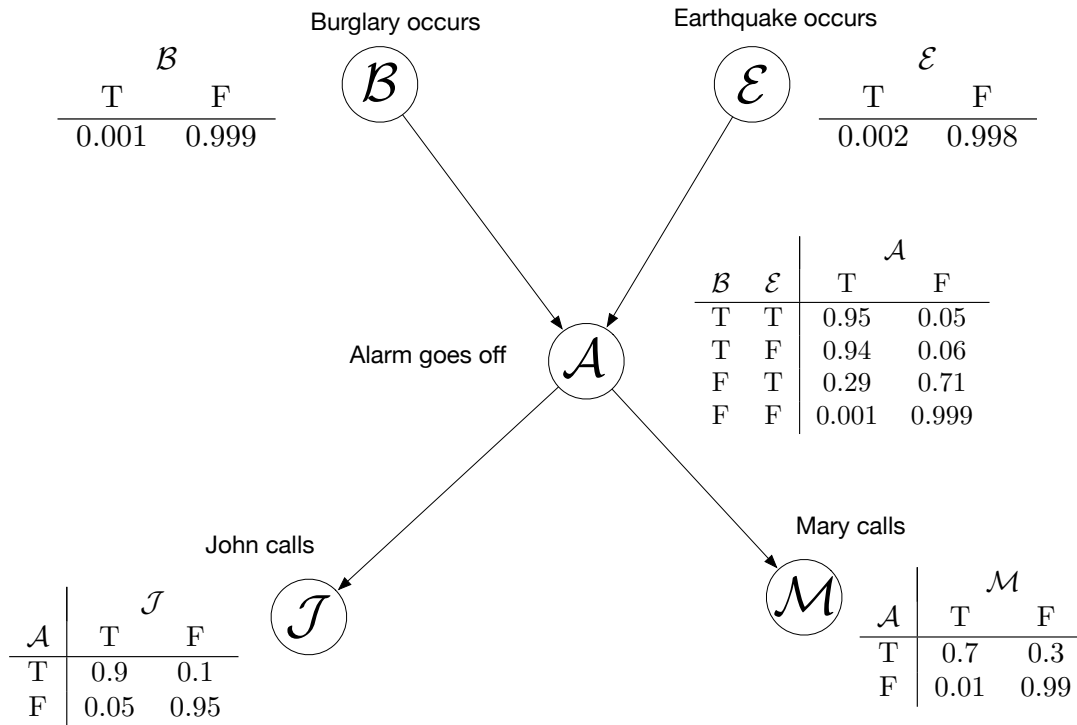
While the graphical structure of the BN is useful for decomposing the joint distribution of the random variables in the graph, it can also be used to reason about the conditional independence relationships in the graph. For instance, it's possible that simply by looking at the graph structure in the BN for the coin problem, we can determine $\mathcal{H}_1 \perp\!\!\!\perp \mathcal{H}_2 \mid \mathcal{C}_1$. In order to figure out conditional independence relationships from a BN, we need to learn about the concept of d-separation.

External Resource(s) (30 minutes)

- Read [d-Separation without Tears](#).
- These videos are pretty good, but the reading seems clearer to us [part 1](#), [part 2](#).

Exercise 10 (15 minutes)

Consider the following BN that describes how two people John and Mary respond to an alarm in their apartment building. In this case the alarm is triggered either by an earthquake, a burglary, or might go off on accident.



For each of the following potential conditional independence relationships, state whether they are true or false (justify your answer). You should use the rules of d-separation to determine your answers. Hint: the specific probability values given in the BN are not relevant for answering this question. The connections between the nodes are all you need to determine conditional independence (we will use the probability tables in the next exercise).

- (a) $\mathcal{B} \perp\!\!\!\perp \mathcal{E}$
- (b) $\mathcal{B} \perp\!\!\!\perp \mathcal{M} \mid \mathcal{A}$
- (c) $\mathcal{B} \perp\!\!\!\perp \mathcal{E} \mid \mathcal{J}$
- (d) $\mathcal{J} \perp\!\!\!\perp \mathcal{M}$
- (e) $\mathcal{J} \perp\!\!\!\perp \mathcal{M} \mid \mathcal{A}$

Exercise 11 (60 minutes)

Consider the following BN from the previous problem that describes how two people John and Mary respond to an alarm in their apartment building. Compute the following probabilities (for some problems you will be able to simplify your calculations by testing for the independence (or conditional independence) using d-separation).

- (a) $p(\mathcal{B}, \mathcal{E})$
- (b) $p(\mathcal{J}, \mathcal{M} \mid \mathcal{A})$

- (c) $p(\mathcal{B}|\mathcal{A})$ (hint: don't forget about Bayes' rule) (hint 2: don't forget about marginalization)
- (d) $p(\mathcal{B}|\mathcal{A}, \mathcal{E})$ (this is known as the phenomenon of *explaining away*). Hint: when you apply Bayes' rule, you can leave some of the events on the right hand side of the conditioning bar (look back at the earlier section "Some Twists on Bayes' Rule". If you need a hint to get you started, try applying the following version of Bayes' rule.

$$p(\mathcal{B}|\mathcal{A}, \mathcal{E}) = \frac{p(\mathcal{A}|\mathcal{B}, \mathcal{E})p(\mathcal{B}|\mathcal{E})}{p(\mathcal{A}|\mathcal{E})}$$