

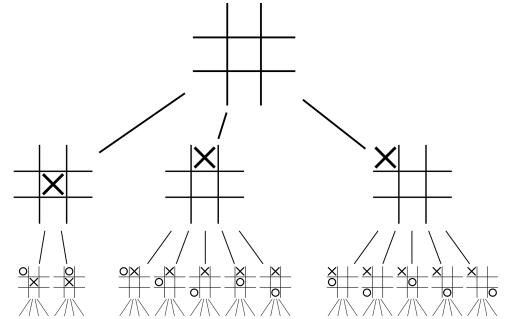
Introduction to Machine Learning

Julie LaChance

Slides adapted from Wells Santo (AI4ALL)
and Agata Foryciarz (Princeton)

Recap

- **Artificial Intelligence:** A field of computer science that attempts to have computers make decisions intelligently



Learning from Examples

- Let's think about human intelligence



Learning from Examples

- Let's think about human intelligence
- Think about how a human learns to identify a cheetah



Learning from Examples

- Let's think about human intelligence
- Think about how a human learns to identify a cheetah
- If someone tries to describe to us how a cheetah looks, we *might* have an idea of a cheetah



Learning from Examples

- Let's think about human intelligence
- Think about how a human learns to identify a cheetah
- If someone tries to describe to us how a cheetah looks, we *might* have an idea of a cheetah
- But if we see an actual example of a cheetah, we know pretty well what a cheetah looks like



Learning from Examples

- Let's think about human intelligence
- Think about how a human learns to identify a cheetah
- If someone tries to describe to us how a cheetah looks, we *might* have an idea of a cheetah
- But if we see an actual example of a cheetah, we know pretty well what a cheetah looks like
- Humans learn and gain intelligence by seeing examples



Machine Learning

- Could we use this understanding of how humans learn to be intelligent and apply that to computers?



Machine Learning

- Could we use this understanding of how humans learn to be intelligent and apply that to computers?
- **Machine Learning** (ML) is an approach to teach computers how to make decisions and predictions, by giving them the ability to learn from data



Why use Machine Learning?

- Computers can be programmed to follow instructions



John Q. Sample
123 Any Street,
US. 12345

Why use Machine Learning?

- Computers can be programmed to follow instructions
- But what if the task is too complicated to describe with specific instructions?



John Q. Sample
123 Any Street,
US. 12345

Why use Machine Learning?

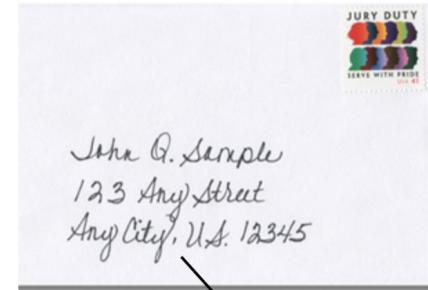
- Computers can be programmed to follow instructions
- But what if the task is too complicated to describe with specific instructions?
- Example: Writing a program to look at handwritten text and figure out what it says



John Q. Sample
123 Any Street,
US. 12345

Why use Machine Learning?

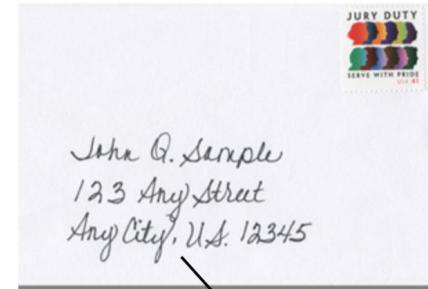
- Computers can be programmed to follow instructions
- But what if the task is too complicated to describe with specific instructions?
- Example: Writing a program to look at handwritten text and figure out what it says
- There are too many different handwriting styles for us to create instructions to capture *all* variations



John Q. Sample
123 Any Street,
US. 12345

Why use Machine Learning?

- Computers can be programmed to follow instructions
- But what if the task is too complicated to describe with specific instructions?
- Example: Writing a program to look at handwritten text and figure out what it says
- There are too many different handwriting styles for us to create instructions to capture *all* variations
- Machine learning allows us to solve this task by learning from examples



John Q. Sample
123 Any Street,
US. 12345

Machine Translation



The screenshot shows a machine translation application with a blue border. At the top, there are language selection dropdowns for "English" and "Chinese (Simplified)", along with icons for microphone, speaker, and a double-headed arrow. Below the dropdowns, the English sentence "AI is for everybody!" is displayed in a large font. To its right, the Chinese translation "AI是给大家的!" is shown above its pinyin transcription "AI shì gěi dàjiā de!". There is also a small icon of a document with a checkmark.

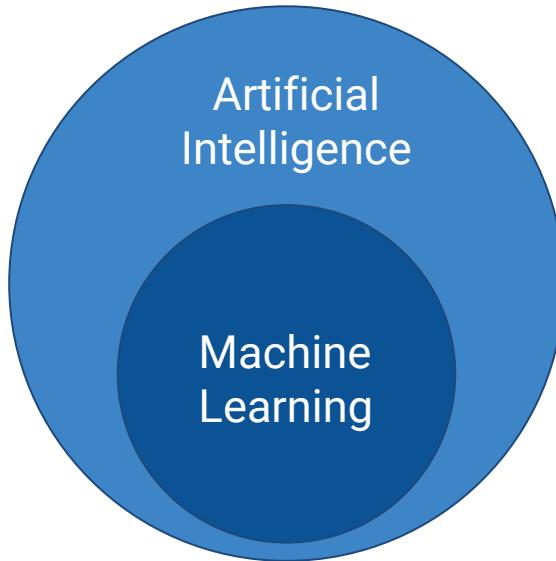
Benefits of using ML for translation:

1. Can translate a language that you have no idea how to speak
2. Can reduce the time spent programming
3. Can easily reuse the same approaches to learn new languages



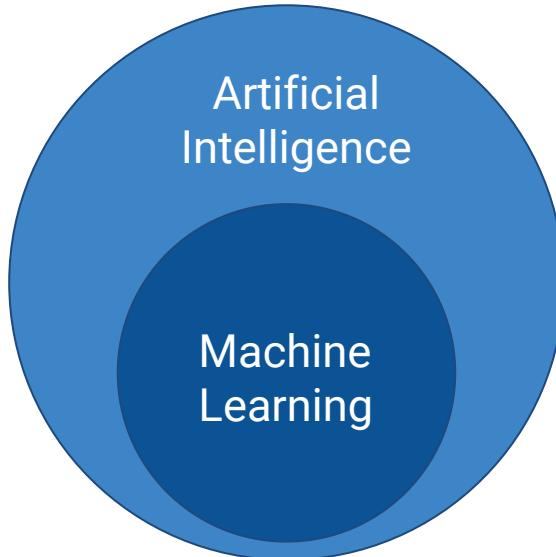
How is ML different from AI?

- Machine learning is a type of artificial intelligence



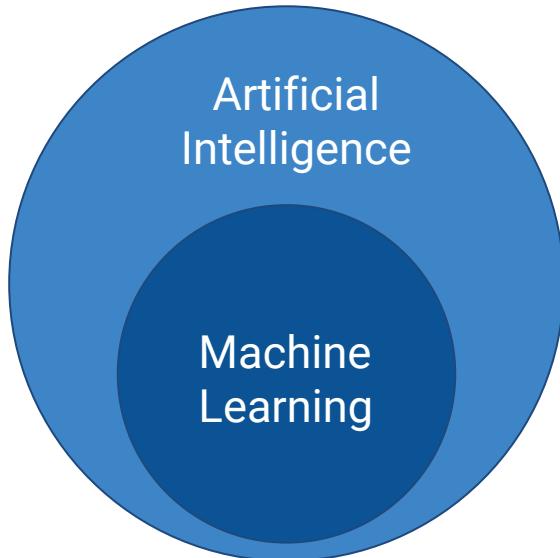
How is ML different from AI?

- Machine learning is a type of artificial intelligence
- Machine learning makes decisions based on data it has seen



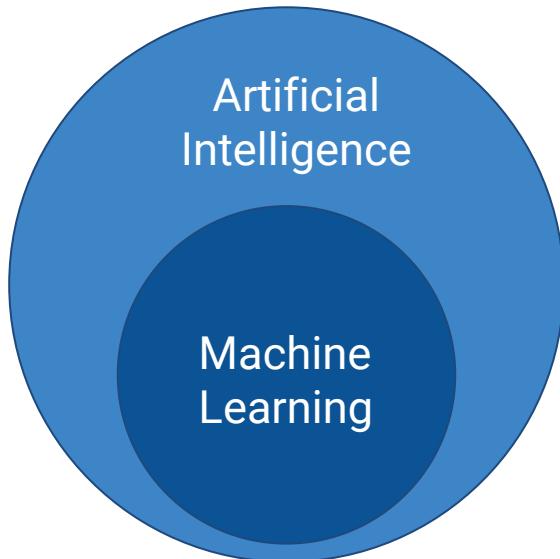
How is ML different from AI?

- Machine learning is a type of artificial intelligence
- Machine learning makes decisions based on data it has seen
- Not all AI algorithms need to do this



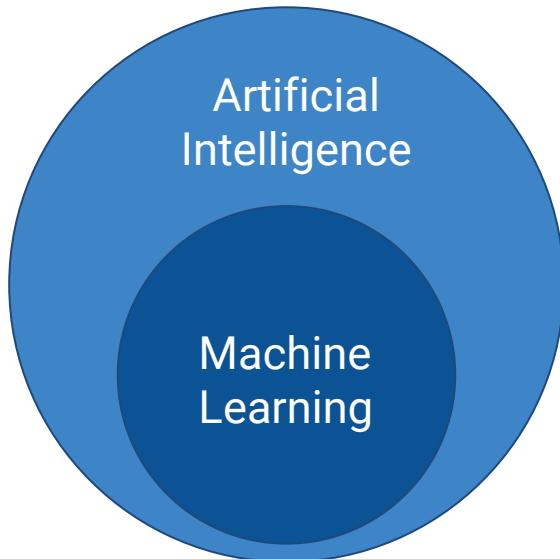
How is ML different from AI?

- Machine learning is a type of artificial intelligence
- Machine learning makes decisions based on data it has seen
- Not all AI algorithms need to do this
- Many of the latest AI systems all make use of ML



How is ML different from AI?

- Machine learning is a type of artificial intelligence
- Machine learning makes decisions based on data it has seen
- Not all AI algorithms need to do this
- Many of the latest AI systems all make use of ML
- For this reason, many people use the terms AI and ML interchangeably





Baron Schwartz

@xaprb

Follow



When you're fundraising, it's AI
When you're hiring, it's ML
When you're implementing, it's linear regression
When you're debugging, it's printf()

6:52 AM - 15 Nov 2017

5,598 Retweets 12,720 Likes



91



5.6K



13K





Baron Schwartz

@xaprb

Follow



When you're fundraising, it's AI
When you're hiring, it's ML

When you're implementing, it's linear
regression

When you're debugging, it's printf()

6:52 AM - 15 Nov 2017

5,598 Retweets 12,720 Likes



91



5.6K



13K





Baron Schwartz

@xaprb

Follow



When you're fundraising, it's AI
When you're hiring, it's ML
When you're implementing, it's linear regression

When you're debugging, it's printf()

Yesterday

6:52 AM - 15 Nov 2017

5,598 Retweets 12,720 Likes



91



5.6K



13K





Baron Schwartz

@xaprb

Follow



When you're fundraising, it's AI
When you're hiring, it's ML

When you're implementing, it's linear
regression

When you're debugging, it's printf()

Friday
Lecture

6:52 AM - 15 Nov 2017

5,598 Retweets 12,720 Likes



91



5.6K



13K



Machine Learning in the News



Machine learning predicts World Cup winner

MIT Technology Review - Jun 12, 2018

But in recent years, researchers have developed **machine-learning** techniques that have the potential to outperform conventional statistical ...

FIFA World Cup: Machine learning predicts two possible winners

Digit - Jun 13, 2018

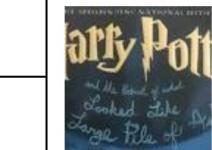
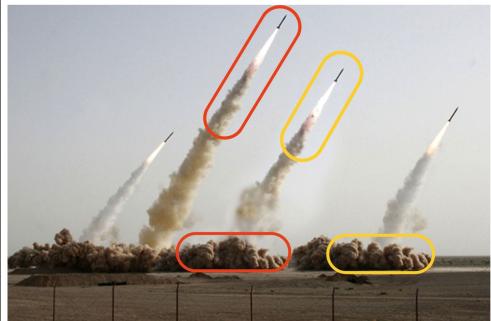
[View all](#)

Adobe is using machine learning to make it easier to spot Photoshopped images

New research uses AI to automate traditional digital forensics

By James Vincent | @jvincent | Jun 22, 2018, 11:00am EDT

f t SHARE



This Harry Potter AI-generated fanfiction is remarkably good

The Verge - Dec 12, 2017

Botnik Studios created the three-page chapter, titled "Harry Potter and ... which the company refers to as "collaborating with machines," mixes ...

"He began to eat Hermione's family": bot tries to write Harry Potter book ...

Blog - The Guardian (blog) - Dec 13, 2017

[View all](#)



New machine learning approach could accelerate bioengineering

Science Daily - Jun 1, 2018

Machine learning, however, uses data to train a computer algorithm to make predictions. The algorithm learns a system's behavior by analyzing ...

Scientists Use **Machine Learning** to Speed Up Biofuel Production

R & D Magazine - Jun 1, 2018

[View all](#)

Activity



Machine learning in the world around you

Machine learning

Machine learning is already shaping the world around us in surprising and exciting ways. Click on the library for an introduction to machine learning or explore the other buildings to find out how machine learning features in our daily lives.

<https://royalsociety.org/topics-policy/projects/machine-learning/machine-learning-in-the-world-around-you-infographic/>





Types of Machine Learning

Supervised Learning

- The first type of machine learning we will learn about is called **supervised learning**

Supervised Learning

- The first type of machine learning we will learn about is called **supervised learning**
- Say we have an image of an animal and want to identify what type of animal is in that image



Supervised Learning

- The first type of machine learning we will learn about is called **supervised learning**
- Say we have an image of an animal and want to identify what type of animal is in that image
- Or say we have a collection of emails and want to identify which emails are spam and which are not



Supervised Learning

- The first type of machine learning we will learn about is called **supervised learning**
- Say we have an image of an animal and want to identify what type of animal is in that image
- Or say we have a collection of emails and want to identify which emails are spam and which are not
- Or say we have weather history for a decade and want to predict tomorrow's weather



Supervised Learning

- The first type of machine learning we will learn about is called **supervised learning**
- Say we have an image of an animal and want to identify what type of animal is in that image
- Or say we have a collection of emails and want to identify which emails are spam and which are not
- Or say we have weather history for a decade and want to predict tomorrow's weather
- How are they all related?



Supervised Learning

- **Supervised Learning:** a type of machine learning where we take data as an input and output a **label**

Supervised Learning

- **Supervised Learning:** a type of machine learning where we take data as an input and output a **label**
- For example, we can take an email as input and assign it the label *spam* or *not spam*

Supervised Learning

- **Supervised Learning:** a type of machine learning where we take data as an input and output a **label**
- For example, we can take an email as input and assign it the label *spam* or *not spam*
- Or, we can take an image as input and assign it with the label *cheetah*, *dog*, *wolf*, etc.

Supervised Learning

- **Supervised Learning:** a type of machine learning where we take data as an input and output a **label**
- For example, we can take an email as input and assign it the label *spam* or *not spam*
- Or, we can take an image as input and assign it with the label *cheetah*, *dog*, *wolf*, etc.
- A specific instance of our data (one particular email or image) is called an **example**

Supervised Learning

- With supervised learning, we learn from examples that are already labelled

7 → 7 5 → 5

8 → 8 3 → 3

2 → 2 4 → ?

Supervised Learning

- With supervised learning, we learn from examples that are already labelled
- For instance, say we want to figure out from an image of a handwritten number what digit it is

7 → 7 5 → 5

8 → 8 3 → 3

2 → 2 4 → ?

Supervised Learning

- With supervised learning, we learn from examples that are already labelled
- For instance, say we want to figure out from an image of a handwritten number what digit it is
- We look at many labelled examples and then try to predict the label of a new, unseen example

7 → 7 5 → 5

8 → 8 3 → 3

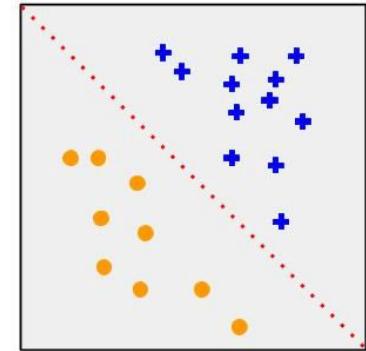
2 → 2 4 → ?

Supervised Learning

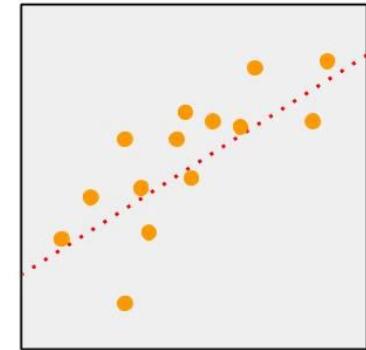
- Within supervised learning, there are two primary types of tasks that we try to accomplish

Supervised Learning

- Within supervised learning, there are two primary types of tasks that we try to accomplish
- **Classification:** When the output (label) is a specific *class*
 - Determining if mail is spam or not spam
 - Determining if a picture has a cat or not



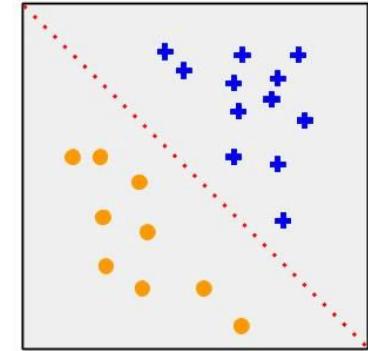
Classification



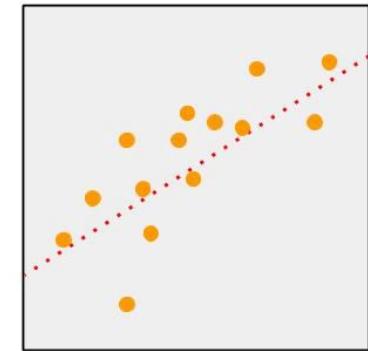
Regression

Supervised Learning

- Within supervised learning, there are two primary types of tasks that we try to accomplish
- **Classification:** When the output (label) is a specific *class*
 - Determining if mail is spam or not spam
 - Determining if a picture has a cat or not
- **Regression:** When the output (label) is a *real number*
 - Determining tomorrow's temperature
 - Determining the cost of coffee in 2020



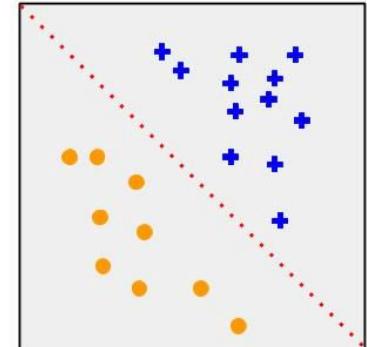
Classification



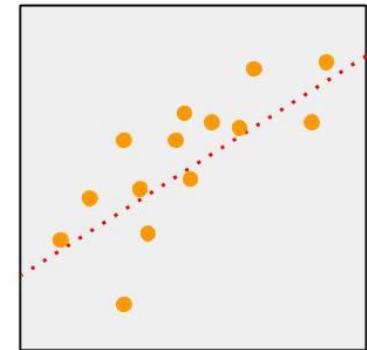
Regression

Supervised Learning

- With classification, there are a specific, finite number of labels that we want to predict



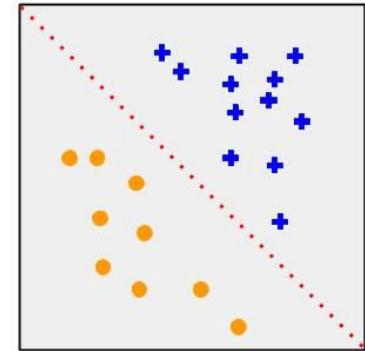
Classification



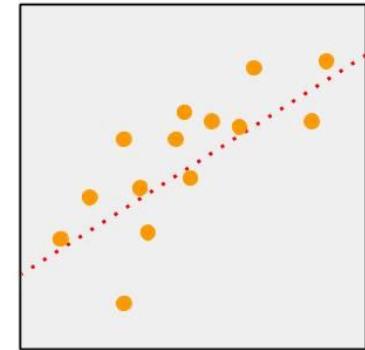
Regression

Supervised Learning

- With classification, there are a specific, finite number of labels that we want to predict
- We say that this output is **discrete**



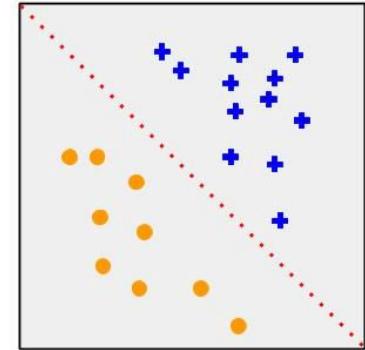
Classification



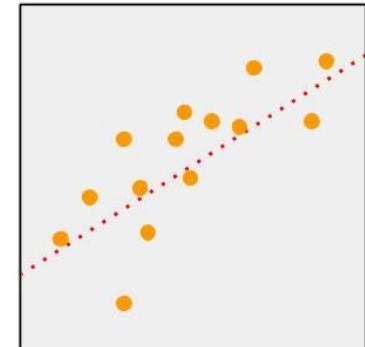
Regression

Supervised Learning

- With classification, there are a specific, finite number of labels that we want to predict
- We say that this output is **discrete**
- With regression, the labels that we want to predict can be any real number on the number line



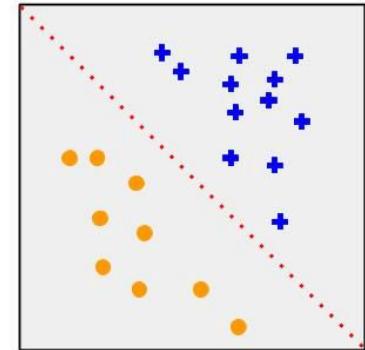
Classification



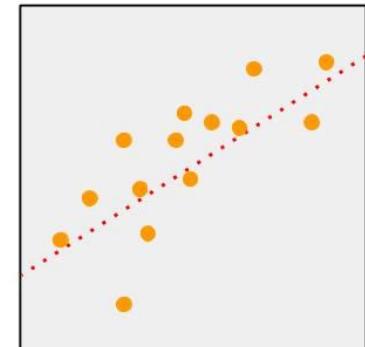
Regression

Supervised Learning

- With classification, there are a specific, finite number of labels that we want to predict
- We say that this output is **discrete**
- With regression, the labels that we want to predict can be any real number on the number line
- We say that this output is **continuous**



Classification



Regression

Building Models

- In supervised learning, we want to build a **model** of the world, one that understands how to correctly assign a label to an example

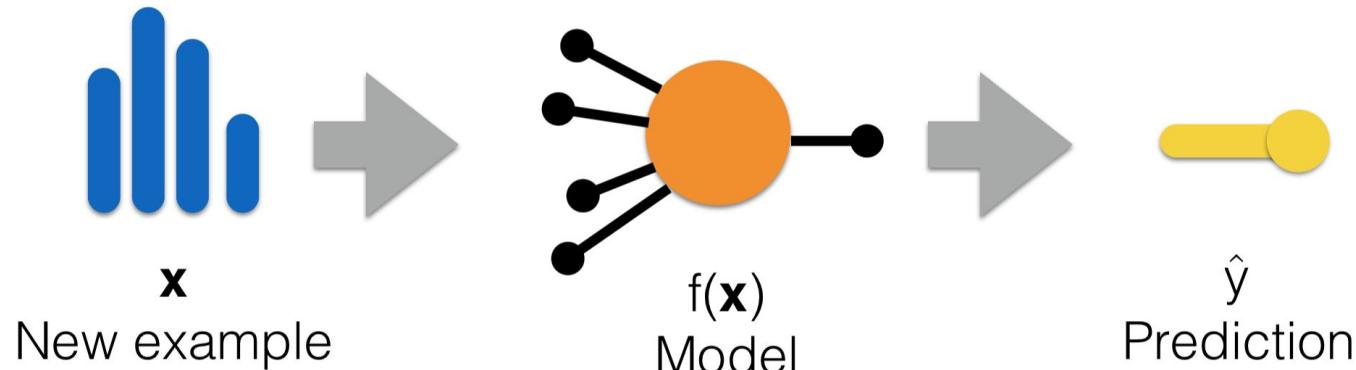
Building Models

- In supervised learning, we want to build a **model** of the world, one that understands how to correctly assign a label to an example
- You can think of a machine learning model as a mathematical function that maps examples to predicted labels

Building Models



- In supervised learning, we want to build a **model** of the world, one that understands how to correctly assign a label to an example
- You can think of a machine learning model as a mathematical function that maps examples to predicted labels



Unsupervised Learning

- The next type of machine learning we will learn about is **unsupervised learning**



Discussion - Classification and Regression

Which method would you use for each of the following tasks:

- Predicting tomorrow's weather based on past weather reports
- Predicting a dog's breed based on their fur color
- Filtering spam emails

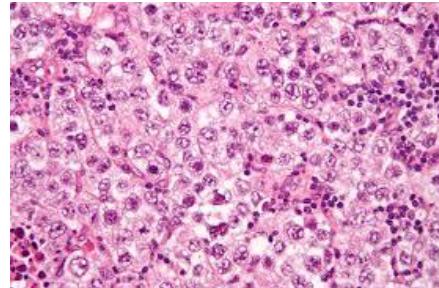
Unsupervised Learning

- The next type of machine learning we will learn about is **unsupervised learning**
- Say we have a collection of music and we want to group them into categories based on shared properties



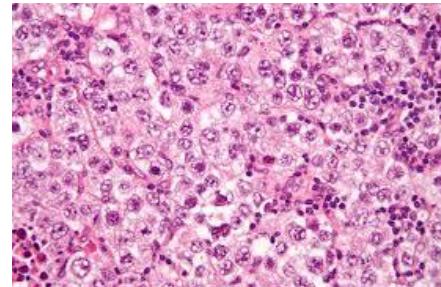
Unsupervised Learning

- The next type of machine learning we will learn about is **unsupervised learning**
- Say we have a collection of music and we want to group them into categories based on shared properties
- Or say we have images of skin cells and want to find cells that look similar to each other



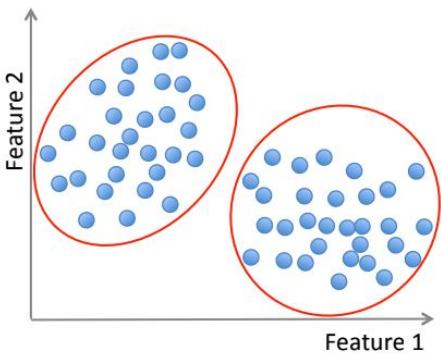
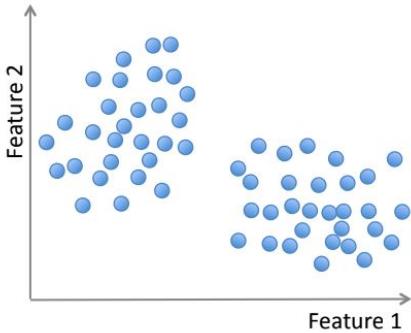
Unsupervised Learning

- The next type of machine learning we will learn about is **unsupervised learning**
- Say we have a collection of music and we want to group them into categories based on shared properties
- Or say we have images of skin cells and want to find cells that look similar to each other
- Unsupervised learning helps us with finding patterns and similarities within our data in order to discover new groupings for them



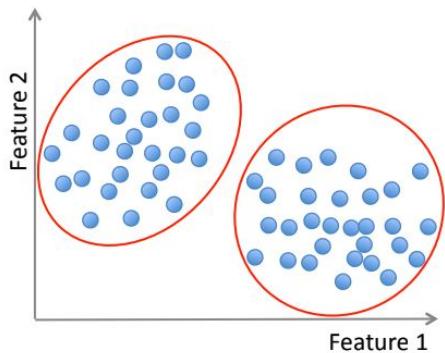
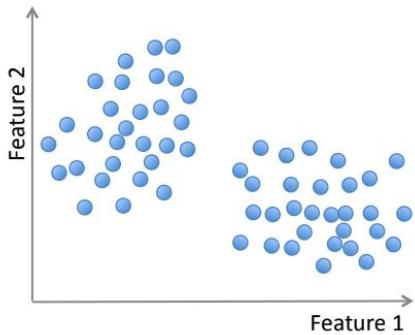
Unsupervised Learning

- **Unsupervised Learning:** a type of machine learning where we take *unlabelled* data as input and output inferences about that data



Unsupervised Learning

- **Unsupervised Learning:** a type of machine learning where we take *unlabelled* data as input and output inferences about that data
- These inferences could be:
 - Different ways to group that data
 - Anomalies that exist in the data
 - Finding new patterns in the data



Supervised vs Unsupervised

- The main difference between supervised and unsupervised learning is whether we have labelled data or not

Supervised vs Unsupervised

- The main difference between supervised and unsupervised learning is whether we have labelled data or not
- When we have labelled data (supervised learning), there is an expectation of what the “right” answer is

Supervised vs Unsupervised

- The main difference between supervised and unsupervised learning is whether we have labelled data or not
- When we have labelled data (supervised learning), there is an expectation of what the “right” answer is
- When we do not have labelled data (unsupervised learning), we want to discover potentially new patterns in the data

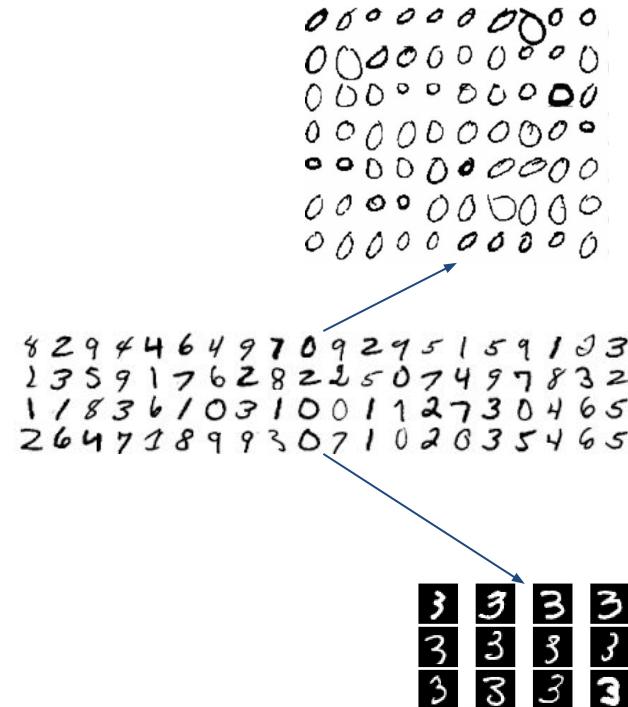
Supervised vs Unsupervised

Which method is supervised, and which is unsupervised? Why?

7 → 7 5 → 5

8 → 8 3 → 3

2 → 2 4 → ?



Supervised vs Unsupervised



7 → 7 5 → 5

8 → 8 3 → 3

$$2 \rightarrow 2 \quad 4 \rightarrow ?$$

Supervised Learning

Unsupervised Learning

Reinforcement Learning

- A completely different way of thinking about Machine Learning, based on human psychology



Reinforcement Learning

- A completely different way of thinking about Machine Learning, based on human psychology
- Based on how we learn about good decisions from *rewards* and bad decisions from *penalties*



Reinforcement Learning

- A completely different way of thinking about Machine Learning, based on human psychology
- Based on how we learn about good decisions from *rewards* and bad decisions from *penalties*
- For example, if I touch a hot stove and it burns my hand, I might learn never to touch a hot stove again



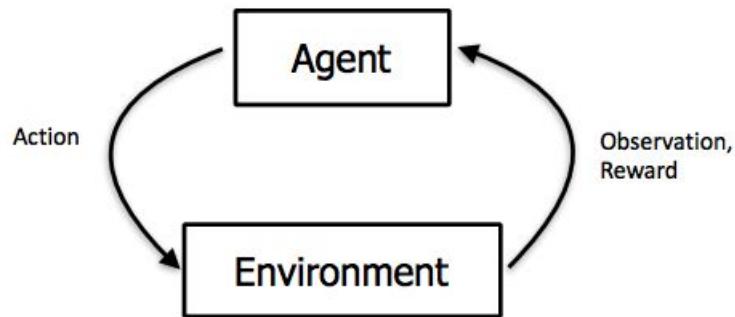
Reinforcement Learning

- A completely different way of thinking about Machine Learning, based on human psychology
- Based on how we learn about good decisions from *rewards* and bad decisions from *penalties*
- For example, if I touch a hot stove and it burns my hand, I might learn never to touch a hot stove again
- Or if I press a button and get a piece of candy, I might learn to want to press that button again



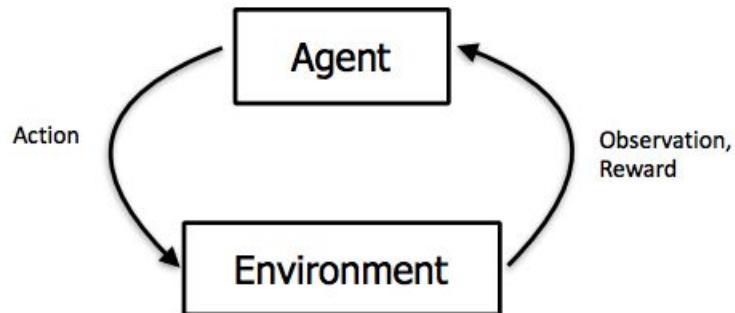
Reinforcement Learning

- Frames the question of intelligence as getting the most reward in a particular environment
- Learn from trial-and-error by taking different actions and seeing which actions give you the most reward



Reinforcement Learning

- Particularly useful for tasks where we need to learn how to make sequential decisions
- Like playing a video game or manueving a robot



Discussion: Supervised, Unsupervised and Reinforcement Learning

Which method would you use for each of the following:

- Predicting the best next move of a self-driving car based on visual information about the environment
- Finding the most attractive advertisement to show to a user on Google based on a search query
- Predicting a student's GPA based on their past grades
- Finding the best move in a game of chess based on the current board arrangement



Data

Describing data to computers

- Data in the real world is extremely complex

Describing data to computers

- Data in the real world is extremely complex
- We can't communicate with computers the same way we communicate to humans

Describing data to computers

- Data in the real world is extremely complex
- We can't communicate with computers the same way we communicate to humans
- For example, we can't just show a computer an image on its own

Describing data to computers

- Data in the real world is extremely complex
- We can't communicate with computers the same way we communicate to humans
- For example, we can't just show a computer an image on its own
- We have to pick and choose what about that image we want to tell our computers

Describing data to computers

- Data in the real world is extremely complex
- We can't communicate with computers the same way we communicate to humans
- For example, we can't just show a computer an image on its own
- We have to pick and choose what about that image we want to tell our computers
- The simplified properties that we use to describe our data to computers are called **features**

Features

- A **feature** is a property of an example we can use to describe it



Features

- A **feature** is a property of an example we can use to describe it
- Used to quantify attributes of an example in a way that a computer can understand

Features



- A **feature** is a property of an example we can use to describe it
- Used to quantify attributes of an example in a way that a computer can understand
- Picking *what* features to use is a really important task in machine learning (**feature selection**)

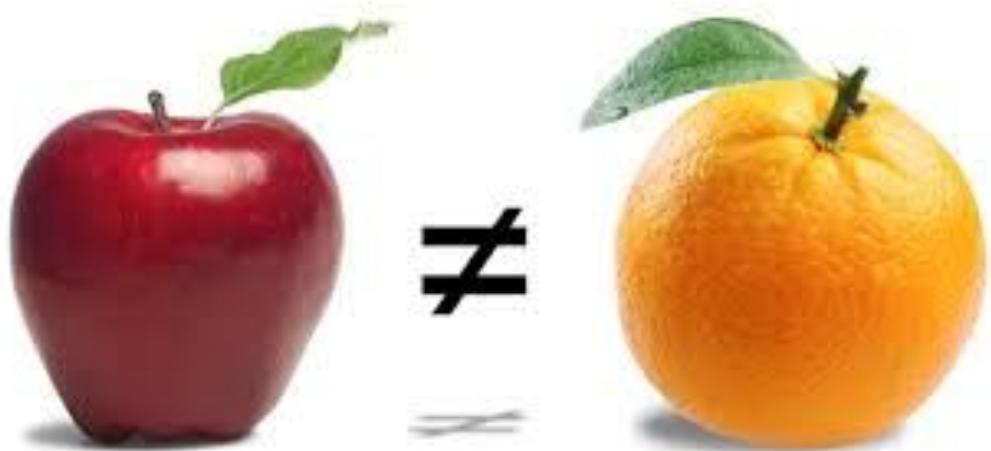


Features

- A **feature** is a property of an example we can use to describe it
- Used to quantify attributes of an example in a way that a computer can understand
- Picking *what* features to use is a really important task in machine learning (**feature selection**)
- Features can be:
 - Binary (yes / no)
 - Real-valued (any real number)
 - Discrete (small number of specific values)

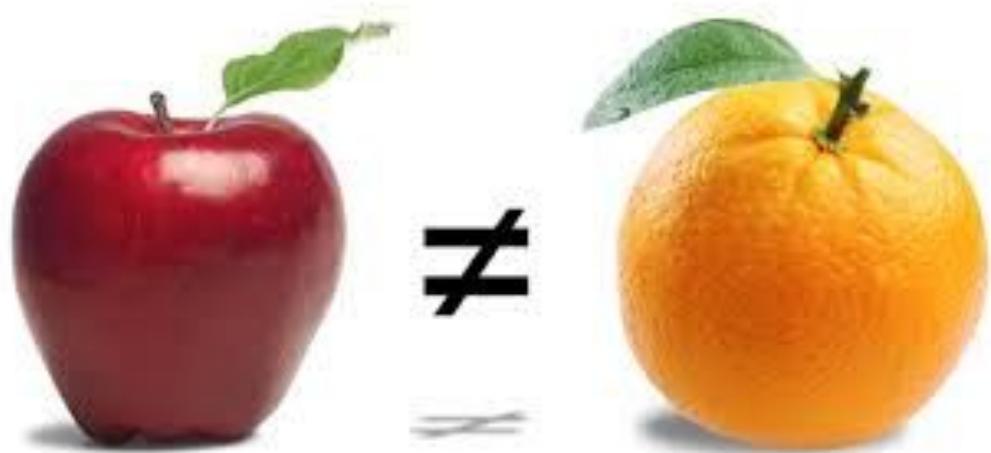
Example: Apple vs Orange

- Say we wanted to teach a computer how to tell the difference between apples and oranges
- What features might be useful for it to know?



Example: Apple vs Orange

- Say we wanted to teach a computer how to tell the difference between apples and oranges
- What features might be useful for it to know?
- Size?
- Shape?
- Color?
- Has seeds?



Examples and Datasets

- An **example**, x , is a particular instance of data (could be a picture, an email, a sentence, a song) which is represented by a set of features

$x = (x_1, x_2, x_3, \dots)$ like $x = (1.5, \text{green}, \text{yes})$

Examples and Datasets

- An **example**, x , is a particular instance of data (could be a picture, an email, a sentence, a song) which is represented by a set of features

$x = (x_1, x_2, x_3, \dots)$ like $x = (1.5, \text{green}, \text{yes})$

- A **labelled example** has both a feature and a label: (x, y)

$((1.5, \text{green}, \text{yes}), \text{apple})$

Examples and Datasets

- An **example**, \mathbf{x} , is a particular instance of data (could be a picture, an email, a sentence, a song) which is represented by a set of features

$\mathbf{x} = (x_1, x_2, x_3, \dots)$ like $\mathbf{x} = (1.5, \text{green}, \text{yes})$

- A **labelled example** has both a feature and a label: (\mathbf{x}, y)

$((1.5, \text{green}, \text{yes}), \text{apple})$

- A **dataset** is a collection of labelled or unlabelled examples

$D = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots\}$

like $D = \{((1.5, \text{green}, \text{yes}), \text{apple}), ((1.5, \text{orange}, \text{yes}), \text{orange})\}$

Fitting to your data

- One of the main goals of machine learning is to understand our data well



Fitting to your data

- One of the main goals of machine learning is to understand our data well
- In machine learning terms, if we understand our data well, we say it has a **good fit**

Fitting to your data

- One of the main goals of machine learning is to understand our data well
- In machine learning terms, if we understand our data well, we say it has a **good fit**
- But we also want to do well on future data that we have not yet seen!

Fitting to your data

- **Memorization:** Ability to do well on data we have already seen
- **Generalization:** Ability to do well on data we have not seen

Fitting to your data

- **Memorization:** Ability to do well on data we have already seen
- **Generalization:** Ability to do well on data we have not seen
- We look at existing data to try to learn patterns that help us generalize -- we do not want to just memorize

Fitting to your data



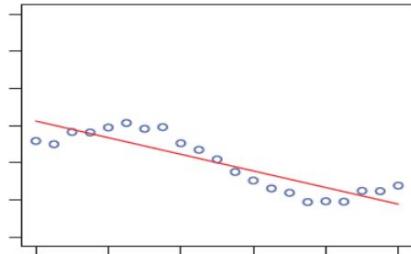
- **Memorization:** Ability to do well on data we have already seen
- **Generalization:** Ability to do well on data we have not seen
- We look at existing data to try to learn patterns that help us generalize -- we do not want to just memorize
- It's like preparing for a math test:
 - Memorizing would be memorizing the answers to the specific questions asked on a practice test
 - Generalizing would be understanding the rules used in the practice test and applying them to the actual test



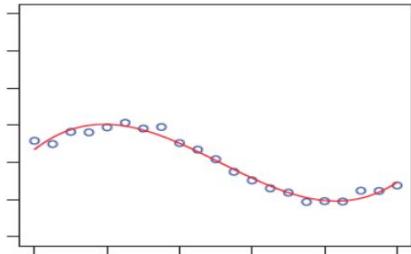
Fitting to your data

- When we don't even fit well to the data we've seen, this is called **underfitting**
- When we fit too well to the data we've seen, but do not generalize well, this is called **overfitting**

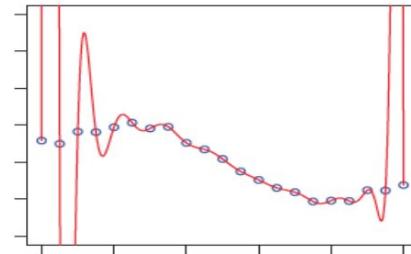
Underfit



Good Fit



Overfit





Discussion

Think about a few scenarios where overfitting could be dangerous.

What types of applications should be most concerned about overfitting?

Using data to improve our system

- How do we learn to generalize well?



Using data to improve our system

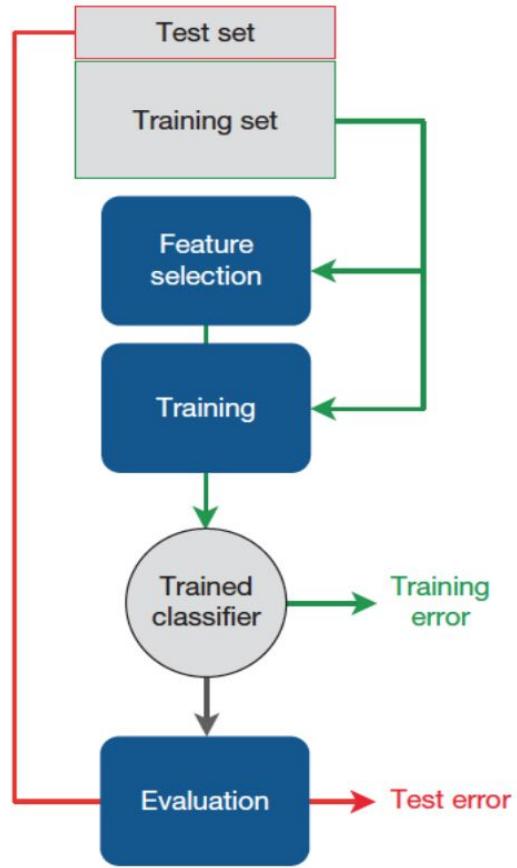
- How do we learn to generalize well?
- We have to evaluate our algorithms on data it hasn't seen before!

Using data to improve our system

- How do we learn to generalize well?
- We have to evaluate our algorithms on data it hasn't seen before!
- To do this, we typically split the data we have into two sets:
 - **Training Set:** data used to train a model
 - **Test Set:** data used to test a model

Using data to improve our system

- How do we learn to generalize well?
- We have to evaluate our algorithms on data it hasn't seen before!
- To do this, we typically split the data we have into two sets:
 - **Training Set:** data used to train a model
 - **Test Set:** data used to test a model
- We then measure performance in two ways:
 - **Training Error:** how well the model performs on data we have seen
 - **Test Error:** how well the model performs on unseen data



Where do we get the data?

- There are a few different ways we can collect data for our dataset

Where do we get the data?

- There are a few different ways we can collect data for our dataset
- Typically, for labelled data, we need to get it from subject area experts

Where do we get the data?



- There are a few different ways we can collect data for our dataset
- Typically, for labelled data, we need to get it from subject area experts
- For example, if we want medical images of lung cancer with the correct labels, we need doctors to collect and then manually label these images



Where do we get the data?

- There are a few different ways we can collect data for our dataset
- Typically, for labelled data, we need to get it from subject area experts
- For example, if we want medical images of lung cancer with the correct labels, we need doctors to collect and then manually label these images
- For examples that require less expertise to label, we can collect them from the internet or create them ourselves

Where do we get the data?

- There are a few different ways we can collect data for our dataset
- Typically, for labelled data, we need to get it from subject area experts
- For example, if we want medical images of lung cancer with the correct labels, we need doctors to collect and then manually label these images
- For examples that require less expertise to label, we can collect them from the internet or create them ourselves
- Free sources of data that we can use are often called **open source datasets**

The Importance of Datasets

The world's most valuable resource is no longer oil, but data

The data economy demands a new approach to antitrust rules



How Much Money Facebook Gets From Selling Your Data

Mark Zuckerberg is making bank on your information.

Jun 19, 2018



The Importance of Datasets

- Datasets are really, really important for machine learning to do well



The Importance of Datasets

- Datasets are really, really important for machine learning to do well
- This is why companies often create good datasets: to sell and profit from them!

The Importance of Datasets

- Datasets are really, really important for machine learning to do well
- This is why companies often create good datasets: to sell and profit from them!
- A good dataset can help your machine learning algorithm, but a bad dataset can hurt

The Importance of Datasets

- Datasets are really, really important for machine learning to do well
- This is why companies often create good datasets: to sell and profit from them!
- A good dataset can help your machine learning algorithm, but **a bad dataset can hurt**
- Not all open-source datasets are good: some may not be labelled accurately or contain missing or biased information



Discussion

Often, datasets generated by users are

Data Protection and Privacy

- The collection and selling of data has brought up legal questions of privacy and anonymity

PRIVACY & SECURITY

Do Not Sell My Personal Information: California Eyes Data Privacy Measure

May 28, 2018 · 9:26 AM ET

Heard on All Things Considered



LAURA SYDELL



Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence

GDPR And The Trusted Framework For Data Privacy

Data Protection and Privacy

- The collection and selling of data has brought up legal questions of privacy and anonymity
- Because data can sometimes contain personal or sensitive information, we should follow good practices to protect privacy: this is called **data stewardship**

PRIVACY & SECURITY

Do Not Sell My Personal Information: California Eyes Data Privacy Measure

May 28, 2018 · 9:26 AM ET

Heard on All Things Considered



LAURA SYDELL



Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence

GDPR And The Trusted Framework For Data Privacy

Data Protection and Privacy

- The collection and selling of data has brought up legal questions of privacy and anonymity
- Because data can sometimes contain personal or sensitive information, we should follow good practices to protect privacy: this is called **data stewardship**
- Laws like the EU's **GDPR** have been passed to help protect consumer data

PRIVACY & SECURITY

Do Not Sell My Personal Information: California Eyes Data Privacy Measure

May 28, 2018 · 9:26 AM ET

Heard on All Things Considered



LAURA SYDELL



Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence

GDPR And The Trusted Framework For Data Privacy



Discussion

What are possible ways you can imagine gathering data while protecting users' privacy?

What sources of data might be more sensitive require more care in using?



Evaluation

How can we tell how good our system is?

- We mentioned earlier that we want to fit our data well -- how do we measure this?



How can we tell how good our system is?

- We mentioned earlier that we want to fit our data well -- how do we measure this?
- One way is to look at the **accuracy** of a model



How can we tell how good our system is?

- We mentioned earlier that we want to fit our data well -- how do we measure this?
- One way is to look at the **accuracy** of a model
- Say we have 100 images of street lights that we want to classify as being green, yellow, or red
- If our model correctly classifies 95 of these 100 images, then we say our model has a 95% accuracy



Other Metrics for Evaluation

- However, accuracy doesn't tell us the whole picture
- There are different types of mistakes that we can make

Other Metrics for Evaluation

- However, accuracy doesn't tell us the whole picture
- There are different types of mistakes that we can make
- Take the example of detecting whether there is a fire in your home or not

Other Metrics for Evaluation



- However, accuracy doesn't tell us the whole picture
- There are different types of mistakes that we can make
- Take the example of detecting whether there is a fire in your home or not
- **False Positive (FP)**: When you think there is a fire, but there isn't
- **False Negative (FN)**: When you think there is not a fire, but there is



Other Metrics for Evaluation



- However, accuracy doesn't tell us the whole picture
- There are different types of mistakes that we can make
- Take the example of detecting whether there is a fire in your home or not
- **False Positive (FP)**: When you think there is a fire, but there isn't
- **False Negative (FN)**: When you think there is not a fire, but there is
- Are these errors equally bad?



Other Metrics for Evaluation



	Actual: Yes	Actual: No
Predicted: Yes	True Positive (TP)	False Positive (FP)
Predicted: No	False Negative (FN)	True Negative (TN)

This table, when filled in with actual numbers,
is called a **confusion matrix**



Other Metrics for Evaluation

- **Precision:** Probability that a positive prediction is actually correct, $TP / (TP + FP)$
- **Recall** (or Sensitivity): Probability that an actually positive outcome is predicted correctly, $TP / (TP + FN)$
- **Specificity:** Probability that an actually negative outcome is predicted correctly, $TN / (TN + FP)$
- **F1 Score:** Combines precision and recall (how well do we predict a positive outcome -and- how good are our positive predictions)
$$(2 * \text{precision} * \text{recall}) / (\text{precision} + \text{recall})$$

Concepts Learned

- Machine Learning
- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning
- Models
- Features
- Examples and datasets
- Overfitting vs underfitting
- Accuracy
- True Positive / False Positive
- Precision / Recall