Machine Learning Notes

[Week 1 Introduction 3](#_Toc471333922)

[Supervised Learning 3](#_Toc471333923)

[Unsupervised Learning 4](#_Toc471333924)

[Model Representation 5](#_Toc471333925)

[Cost Function 6](#_Toc471333926)

[Cost Function - Intuition I 6](#_Toc471333927)

[Cost Function - Intuition II 8](#_Toc471333928)

[Gradient Descent 10](#_Toc471333929)

[Gradient Descent Intuition 11](#_Toc471333930)

[Gradient Descent For Linear Regression 13](#_Toc471333931)

[Installing Octave on Windows 15](#_Toc471333932)

[Week 2 Linear Regression with Multiple Features 15](#_Toc471333933)

[Gradient Descent for Multiple Variables 16](#_Toc471333934)

[Gradient Descent in Practice I - Feature Scaling 17](#_Toc471333935)

[Gradient Descent in Practice II - Learning Rate 18](#_Toc471333936)

[Features and Polynomial Regression 19](#_Toc471333937)

[Polynomial Regression 19](#_Toc471333938)

[Normal Equation 20](#_Toc471333939)

[Normal Equation Noninvertibility 21](#_Toc471333940)

[Week 3 Logistic Regresion 21](#_Toc471333941)

[Classification 21](#_Toc471333942)

[Hypothesis Representation 21](#_Toc471333943)

[Decision Boundary 22](#_Toc471333944)

[Cost Function 23](#_Toc471333945)

[Simplified Cost Function and Gradient Descent 25](#_Toc471333946)

[Gradient Descent 25](#_Toc471333947)

[Advanced Optimization 26](#_Toc471333948)

[Multiclass Classification: One-vs-all 27](#_Toc471333949)

[The Problem of Overfitting 28](#_Toc471333950)

[Cost Function 29](#_Toc471333951)

[Regularized Linear Regression 30](#_Toc471333952)

[Gradient Descent 30](#_Toc471333953)

[Normal Equation 31](#_Toc471333954)

[Regularized Logistic Regression 32](#_Toc471333955)

[Cost Function 32](#_Toc471333956)

[Week 4 Neuron Network 33](#_Toc471333957)

[Model Representation I 33](#_Toc471333958)

[Model Representation II 35](#_Toc471333959)

[Examples and Intuitions I 36](#_Toc471333960)

[Examples and Intuitions II 38](#_Toc471333961)

[Multiclass Classification 39](#_Toc471333962)

[Week 5 Neural Networks: Learning 41](#_Toc471333963)

[Cost Function 41](#_Toc471333964)

[Backpropagation Algorithm 42](#_Toc471333965)

[Backpropagation Intuition 44](#_Toc471333966)

[Implementation Note: Unrolling Parameters 45](#_Toc471333967)

[Gradient Checking 46](#_Toc471333968)

[Random Initialization 47](#_Toc471333969)

[Week 6 Advice for Applying Machine Learning 48](#_Toc471333970)

[Evaluating a Hypothesis 48](#_Toc471333971)

[The test set error 48](#_Toc471333972)

[Model Selection and Train/Validation/Test Sets 49](#_Toc471333973)

[Diagnosing Bias vs. Variance 50](#_Toc471333974)

[Regularization and Bias/Variance 51](#_Toc471333975)

[Learning Curves 52](#_Toc471333976)

[Deciding What to Do Next Revisited 53](#_Toc471333977)

[Diagnosing Neural Networks 54](#_Toc471333978)

[Model Selection 54](#_Toc471333979)

[Machine Learning System Design 56](#_Toc471333980)

[Prioritizing What to Work On 56](#_Toc471333981)

[Error Analysis 56](#_Toc471333982)

[Error Metrics for Skewed Classes 56](#_Toc471333983)

[Trading Off Precision and Recall 57](#_Toc471333984)

[Data for Machine Learning 58](#_Toc471333985)

[Quiz instructions 59](#_Toc471333986)

[Week 7 Optimization Objective 59](#_Toc471333987)

On Demand videos cannot be downloaded. However, you may find the videos from a previous version of the course <https://www.coursera.org/learn/machine-learning>

Sample problems: <http://cs229.stanford.edu/materials.html>

You may find the notes from a previous version of the course: <https://www.coursera.org/learn/machine-learning>

Wiki page: <https://share.coursera.org/wiki/index.php/ML:Main>

# Week 1 Introduction

Two definitions of Machine Learning are offered. Arthur Samuel described it as: "the field of study that gives computers the ability to learn without being explicitly programmed." This is an older, informal definition.

Tom Mitchell provides a more modern definition: "A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E."

Example: playing checkers.

E = the experience of playing many games of checkers

T = the task of playing checkers.

P = the probability that the program will win the next game.

In general, any machine learning problem can be assigned to one of two broad classifications:

Supervised learning and Unsupervised learning.

Supervised Learning

Right answers given,

Regression Problem: predict continuous valued output

Classification Problem: discrete valued output (0 or 1)

In supervised learning, we are given a data set and already know what our correct output should look like, having the idea that there is a relationship between the input and the output.

Supervised learning problems are categorized into "regression" and "classification" problems. In a regression problem, we are trying to predict results within a continuous output, meaning that we are trying to map input variables to some continuous function. In a classification problem, we are instead trying to predict results in a discrete output. In other words, we are trying to map input variables into discrete categories.

**Example 1:**

Given data about the size of houses on the real estate market, try to predict their price. Price as a function of size is a continuous output, so this is a regression problem.

We could turn this example into a classification problem by instead making our output about whether the house "sells for more or less than the asking price." Here we are classifying the houses based on price into two discrete categories.

**Example 2**:

(a) Regression - Given a picture of a person, we have to predict their age on the basis of the given picture

(b) Classification - Given a patient with a tumor, we have to predict whether the tumor is malignant or benign.

## Unsupervised Learning

Don’t know the right answer, just differentiate into different clusters.

Cocktail party algorithm

Unsupervised learning allows us to approach problems with little or no idea what our results should look like. We can derive structure from data where we don't necessarily know the effect of the variables.

We can derive this structure by clustering the data based on relationships among the variables in the data.

With unsupervised learning there is no feedback based on the prediction results.

**Example:**

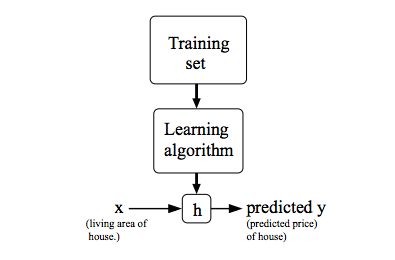
Clustering: Take a collection of 1,000,000 different genes, and find a way to automatically group these genes into groups that are somehow similar or related by different variables, such as lifespan, location, roles, and so on.

Non-clustering: The "Cocktail Party Algorithm", allows you to find structure in a chaotic environment. (i.e. identifying individual voices and music from a mesh of sounds at a [cocktail party](https://en.wikipedia.org/wiki/Cocktail_party_effect)).

## Model Representation

To establish notation for future use, we’ll use *x*(*i*) to denote the “input” variables (living area in this example), also called input features, and *y*(*i*) to denote the “output” or target variable that we are trying to predict (price). A pair (*x*(*i*),*y*(*i*)) is called a training example, and the dataset that we’ll be using to learn—a list of m training examples (*x*(*i*),*y*(*i*));*i*=1,...,*m*—is called a training set. Note that the superscript “(i)” in the notation is simply an index into the training set, and has nothing to do with exponentiation. We will also use X to denote the space of input values, and Y to denote the space of output values. In this example, X = Y = ℝ.

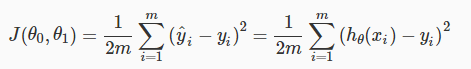
To describe the supervised learning problem slightly more formally, our goal is, given a training set, to learn a function h : X → Y so that h(x) is a “good” predictor for the corresponding value of y. For historical reasons, this function h is called a hypothesis. Seen pictorially, the process is therefore like this:



When the target variable that we’re trying to predict is continuous, such as in our housing example, we call the learning problem a regression problem. When y can take on only a small number of discrete values (such as if, given the living area, we wanted to predict if a dwelling is a house or an apartment, say), we call it a classification problem.

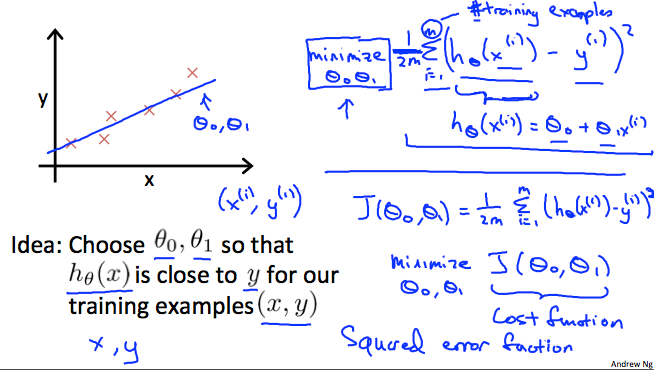
## Cost Function

We can measure the accuracy of our hypothesis function by using a **cost function**. This takes an average difference (actually a fancier version of an average) of all the results of the hypothesis with inputs from x's and the actual output y's.



To break it apart, it is 12 *x*¯ where *x*¯ is the mean of the squares of *hθ*(*xi*)−*yi* , or the difference between the predicted value and the actual value.

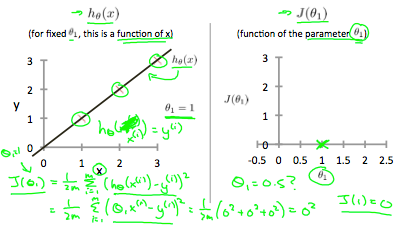
This function is otherwise called the "Squared error function", or "Mean squared error". The mean is halved (12)as a convenience for the computation of the gradient descent, as the derivative term of the square function will cancel out the 12 term. The following image summarizes what the cost function does:



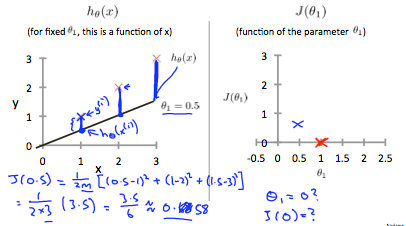
## Cost Function - Intuition I

If we try to think of it in visual terms, our training data set is scattered on the x-y plane. We are trying to make a straight line (defined by *hθ*(*x*)) which passes through these scattered data points.

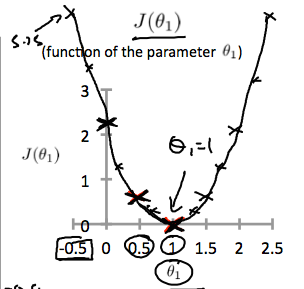
Our objective is to get the best possible line. The best possible line will be such so that the average squared vertical distances of the scattered points from the line will be the least. Ideally, the line should pass through all the points of our training data set. In such a case, the value of *J*(*θ*0,*θ*1) will be 0. The following example shows the ideal situation where we have a cost function of 0.



When *θ*1=1, we get a slope of 1 which goes through every single data point in our model. Conversely, when *θ*1=0.5, we see the vertical distance from our fit to the data points increase.



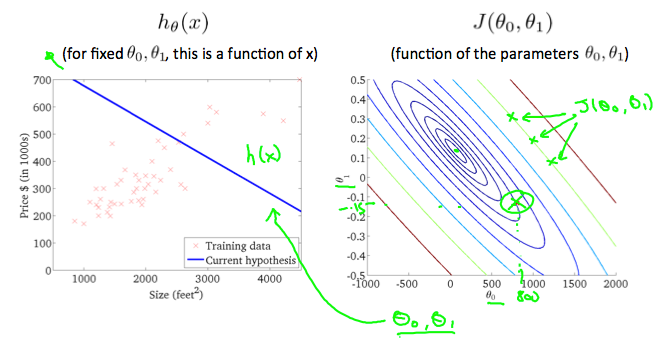
This increases our cost function to 0.58. Plotting several other points yields to the following graph:



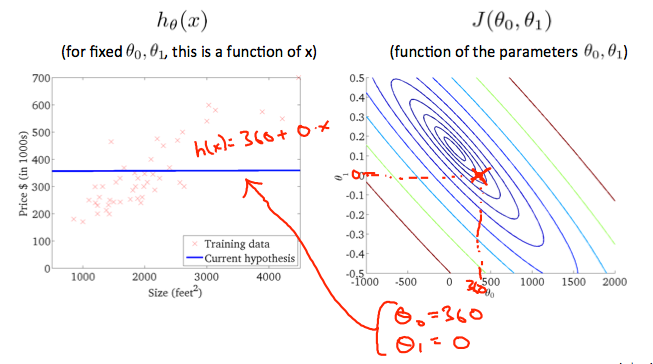
Thus as a goal, we should try to minimize the cost function. In this case, *θ*1=1 is our global minimum.

## Cost Function - Intuition II

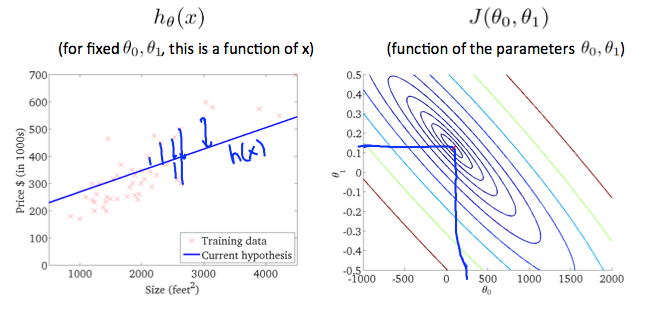
A contour plot is a graph that contains many contour lines. A contour line of a two variable function has a constant value at all points of the same line. An example of such a graph is the one to the right below.



Taking any color and going along the 'circle', one would expect to get the same value of the cost function. For example, the three green points found on the green line above have the same value for *J*(*θ*0,*θ*1) and as a result, they are found along the same line. The circled x displays the value of the cost function for the graph on the left when *θ*0 = 800 and *θ*1= -0.15. Taking another h(x) and plotting its contour plot, one gets the following graphs:



When *θ*0 = 360 and *θ*1 = 0, the value of *J*(*θ*0,*θ*1) in the contour plot gets closer to the center thus reducing the cost function error. Now giving our hypothesis function a slightly positive slope results in a better fit of the data.



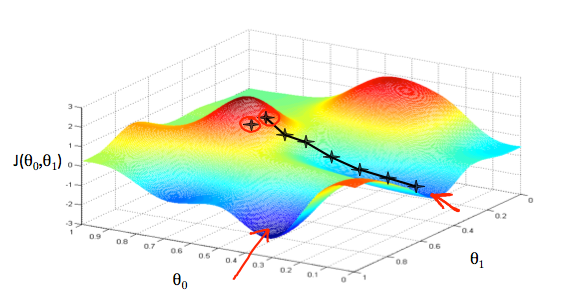
The graph above minimizes the cost function as much as possible and consequently, the result of *θ*1 and *θ*0 tend to be around 0.12 and 250 respectively. Plotting those values on our graph to the right seems to put our point in the center of the inner most 'circle'.

## Gradient Descent

So we have our hypothesis function and we have a way of measuring how well it fits into the data. Now we need to estimate the parameters in the hypothesis function. That's where gradient descent comes in.

Imagine that we graph our hypothesis function based on its fields *θ*0 and *θ*1 (actually we are graphing the cost function as a function of the parameter estimates). We are not graphing x and y itself, but the parameter range of our hypothesis function and the cost resulting from selecting a particular set of parameters.

We put *θ*0 on the x axis and *θ*1 on the y axis, with the cost function on the vertical z axis. The points on our graph will be the result of the cost function using our hypothesis with those specific theta parameters. The graph below depicts such a setup.



We will know that we have succeeded when our cost function is at the very bottom of the pits in our graph, i.e. when its value is the minimum. The red arrows show the minimum points in the graph.

The way we do this is by taking the derivative (the tangential line to a function) of our cost function. The slope of the tangent is the derivative at that point and it will give us a direction to move towards. We make steps down the cost function in the direction with the steepest descent. The size of each step is determined by the parameter α, which is called the learning rate.

For example, the distance between each 'star' in the graph above represents a step determined by our parameter α. A smaller α would result in a smaller step and a larger α results in a larger step. The direction in which the step is taken is determined by the partial derivative of *J*(*θ*0,*θ*1). Depending on where one starts on the graph, one could end up at different points. The image above shows us two different starting points that end up in two different places.

The gradient descent algorithm is:

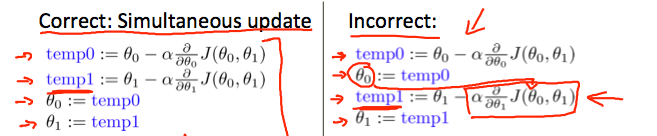
repeat until convergence:



where

j=0,1 represents the feature index number.

At each iteration j, one should simultaneously update the parameters *θ*1,*θ*2,...,*θn*. Updating a specific parameter prior to calculating another one on the *j*(*th*) iteration would yield to a wrong implementation.



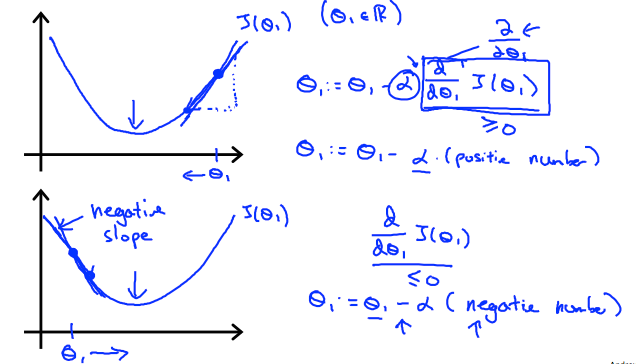
## Gradient Descent Intuition

In this video we explored the scenario where we used one parameter *θ*1 and plotted its cost function to implement a gradient descent. Our formula for a single parameter was :

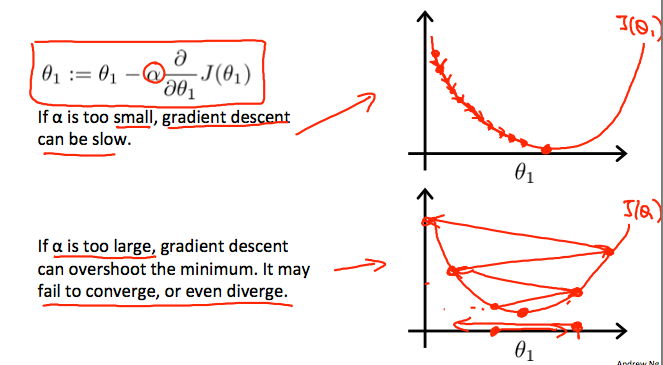
Repeat until convergence:

|  |
| --- |
|  |

Regardless of the slope's sign for *ddθ*1*J*(*θ*1), *θ*1 eventually converges to its minimum value. The following graph shows that when the slope is negative, the value of *θ*1 increases and when it is positive, the value of *θ*1 decreases.



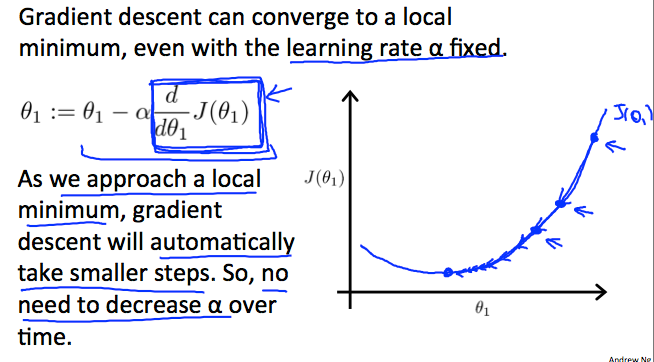
On a side note, we should adjust our parameter *α* to ensure that the gradient descent algorithm converges in a reasonable time. Failure to converge or too much time to obtain the minimum value imply that our step size is wrong.



How does gradient descent converge with a fixed step size***α***?

The intuition behind the convergence is that *ddθ*1*J*(*θ*1) approaches 0 as we approach the bottom of our convex function. At the minimum, the derivative will always be 0 and thus we get:

|  |
| --- |
| *θ*1:=*θ*1−*α*∗0 |



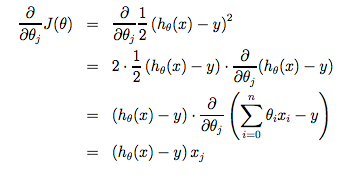
## Gradient Descent For Linear Regression

|  |
| --- |
|  |

When specifically applied to the case of linear regression, a new form of the gradient descent equation can be derived. We can substitute our actual cost function and our actual hypothesis function and modify the equation to :

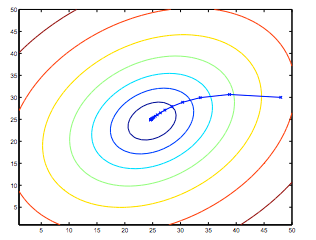
where m is the size of the training set, *θ*0 a constant that will be changing simultaneously with *θ*1 and *xi*,*yi* are values of the given training set (data).

Note that we have separated out the two cases for *θj* into separate equations for *θ*0 and *θ*1; and that for *θ*1 we are multiplying *xi* at the end due to the derivative. The following is a derivation of *J*(*θ*) for a single example :



The point of all this is that if we start with a guess for our hypothesis and then repeatedly apply these gradient descent equations, our hypothesis will become more and more accurate.

So, this is simply gradient descent on the original cost function J. This method looks at every example in the entire training set on every step, and is called **batch gradient descent**. Note that, while gradient descent can be susceptible to local minima in general, the optimization problem we have posed here for linear regression has only one global, and no other local, optima; thus gradient descent always converges (assuming the learning rate α is not too large) to the global minimum. Indeed, J is a convex quadratic function. Here is an example of gradient descent as it is run to minimize a quadratic function.



The ellipses shown above are the contours of a quadratic function. Also shown is the trajectory taken by gradient descent, which was initialized at (48,30). The x’s in the figure (joined by straight lines) mark the successive values of θ that gradient descent went through as it converged to its minimum.

## Installing Octave on Windows

**Use this link to install Octave for windows:** <http://wiki.octave.org/Octave_for_Microsoft_Windows>

**Octave on Windows can be used to submit programming assignments** in this course but will likely need a patch provided in the discussion forum. Refer to [https://www.coursera.org/learn/machine-learning/discussions/vgCyrQoMEeWv5yIAC00Eog?](https://www.coursera.org/learn/machine-learning/discussions/vgCyrQoMEeWv5yIAC00Eog?page=2) for more information about the patch for your version.

# Week 2 Linear Regression with Multiple Features

Linear regression with multiple variables is also known as "multivariate linear regression".

We now introduce notation for equations where we can have any number of input variables.

|  |
| --- |
|  |

The multivariable form of the hypothesis function accommodating these multiple features is as follows:

*hθ*(*x*)=*θ*0+*θ*1*x*1+*θ*2*x*2+*θ*3*x*3+⋯+*θnxn*

In order to develop intuition about this function, we can think about *θ*0 as the basic price of a house, *θ*1 as the price per square meter, *θ*2 as the price per floor, etc. *x*1 will be the number of square meters in the house, *x*2 the number of floors, etc.

Using the definition of matrix multiplication, our multivariable hypothesis function can be concisely represented as:

|  |
| --- |
|  |

This is a vectorization of our hypothesis function for one training example; see the lessons on vectorization to learn more.

Remark: Note that for convenience reasons in this course we assume *x*(*i*)0=1 for (*i*∈1,…,*m*). This allows us to do matrix operations with theta and x. Hence making the two vectors 'theta' and *x*(*i*) match each other element-wise (that is, have the same number of elements: n+1).]

The training examples are stored in X row-wise. The following example shows us the reason behind setting *x*(*i*)0=1 :

|  |
| --- |
|  |

As a result, you can calculate the hypothesis as a column vector of size (m x 1) with:

*hθ*(*X*)=*Xθ*

## Gradient Descent for Multiple Variables

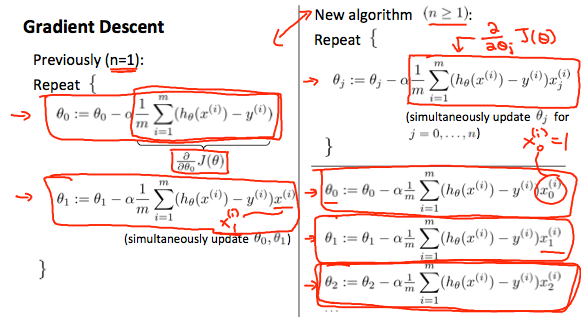
The gradient descent equation itself is generally the same form; we just have to repeat it for our 'n' features:

|  |
| --- |
|  |

In other words:

|  |
| --- |
|  |

The following image compares gradient descent with one variable to gradient descent with multiple variables:



## Gradient Descent in Practice I - Feature Scaling

We can speed up gradient descent by having each of our input values in roughly the same range. This is because θ will descend quickly on small ranges and slowly on large ranges, and so will oscillate inefficiently down to the optimum when the variables are very uneven.

The way to prevent this is to modify the ranges of our input variables so that they are all roughly the same. Ideally:

−1 ≤ *x*(*i*) ≤ 1

or

−0.5 ≤ *x*(*i*) ≤ 0.5

These aren't exact requirements; we are only trying to speed things up. The goal is to get all input variables into roughly one of these ranges, give or take a few.

Two techniques to help with this are **feature scaling** and **mean normalization**. Feature scaling involves dividing the input values by the range (i.e. the maximum value minus the minimum value) of the input variable, resulting in a new range of just 1. Mean normalization involves subtracting the average value for an input variable from the values for that input variable resulting in a new average value for the input variable of just zero. To implement both of these techniques, adjust your input values as shown in this formula:

Where *μi* is the **average** of all the values for feature (i) and *si* is the range of values (max - min), or *si* is the standard deviation.

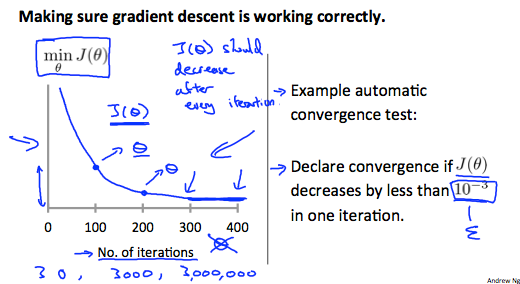
Note that dividing by the range, or dividing by the standard deviation, give different results. The quizzes in this course use range - the programming exercises use standard deviation.

For example, if *xi* represents housing prices with a range of 100 to 2000 and a mean value of 1000, then,  .

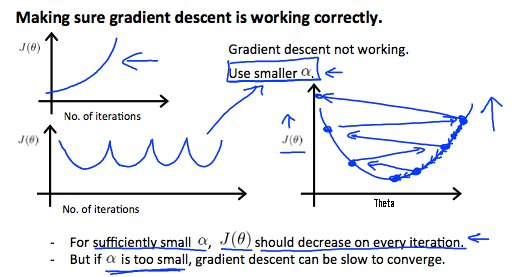
## Gradient Descent in Practice II - Learning Rate

**Debugging gradient descent.** Make a plot with number of iterations on the x-axis. Now plot the cost function, J(θ) over the number of iterations of gradient descent. If J(θ) ever increases, then you probably need to decrease α.

**Automatic convergence test.** Declare convergence if J(θ) decreases by less than E in one iteration, where E is some small value such as 10−3. However in practice it's difficult to choose this threshold value.



It has been proven that if learning rate α is sufficiently small, then J(θ) will decrease on every iteration.



To summarize:

If *α* is too small: slow convergence.

If *α* is too large: ￼may not decrease on every iteration and thus may not converge.

## Features and Polynomial Regression

We can improve our features and the form of our hypothesis function in a couple different ways.

We can **combine** multiple features into one. For example, we can combine *x*1 and *x*2 into a new feature *x*3 by taking *x*1⋅*x*2.

## ****Polynomial Regression****

Our hypothesis function need not be linear (a straight line) if that does not fit the data well.

We can **change the behavior or curve** of our hypothesis function by making it a quadratic, cubic or square root function (or any other form).

For example, if our hypothesis function is *hθ*(*x*)=*θ*0+*θ*1*x*1 then we can create additional features based on *x*1, to get the quadratic function *hθ*(*x*)=*θ*0+*θ*1*x*1+*θ*2*x1*2 or the cubic function *hθ*(*x*)=*θ*0+*θ*1*x*1+*θ*2*x1*2+*θ*3*x1*3

In the cubic version, we have created new features *x*2 and *x*3 where *x*2=*x1*2 and *x*3=*x1*3.

To make it a square root function, we could do: 

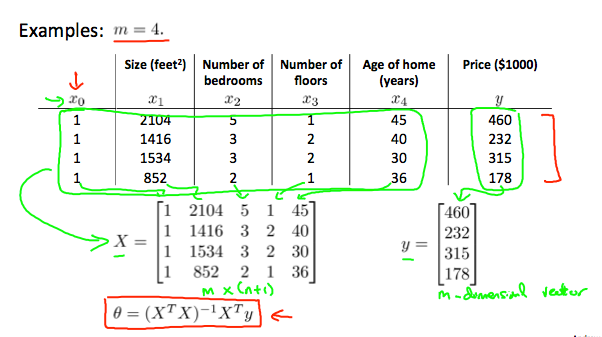
One important thing to keep in mind is, if you choose your features this way then feature scaling becomes very important.

eg. if *x*1 has range 1 - 1000 then range of *x1*2 becomes 1 - 1000000 and that of *x1*3 becomes 1 - 1000000000

## Normal Equation

Gradient descent gives one way of minimizing J. Let’s discuss a second way of doing so, this time performing the minimization explicitly and without resorting to an iterative algorithm. In the "Normal Equation" method, we will minimize J by explicitly taking its derivatives with respect to the θj ’s, and setting them to zero. This allows us to find the optimum theta without iteration. The normal equation formula is given below:

*θ*=(*XTX*)−1*XTy*



There is **no need** to do feature scaling with the normal equation.

The following is a comparison of gradient descent and the normal equation:

|  |  |
| --- | --- |
| **Gradient Descent** | **Normal Equation** |
| Need to choose alpha | No need to choose alpha |
| Needs many iterations | No need to iterate |
| O (*kn*2) | O (*n*3), need to calculate inverse of *XTX* |
| Works well when n is large | Slow if n is very large |

With the normal equation, computing the inversion has complexity O(*n*3). So if we have a very large number of features, the normal equation will be slow. In practice, when n exceeds 10,000 it might be a good time to go from a normal solution to an iterative process.

## Normal Equation Noninvertibility

When implementing the normal equation in octave we want to use the 'pinv' function rather than 'inv.' The 'pinv' function will give you a value of *θ* even if *XTX* is not invertible.

If *XTX* is **noninvertible,** the common causes might be having :

* Redundant features, where two features are very closely related (i.e. they are linearly dependent)
* Too many features (e.g. m ≤ n). In this case, delete some features or use "regularization" (to be explained in a later lesson).

Solutions to the above problems include deleting a feature that is linearly dependent with another or deleting one or more features when there are too many features.

# Week 3 Logistic Regresion

## Classification

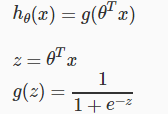
To attempt classification, one method is to use linear regression and map all predictions greater than 0.5 as a 1 and all less than 0.5 as a 0. However, this method doesn't work well because classification is not actually a linear function.

The classification problem is just like the regression problem, except that the values y we now want to predict take on only a small number of discrete values. For now, we will focus on the **binary classification** **problem** in which y can take on only two values, 0 and 1. (Most of what we say here will also generalize to the multiple-class case.) For instance, if we are trying to build a spam classifier for email, then *x*(*i*) may be some features of a piece of email, and y may be 1 if it is a piece of spam mail, and 0 otherwise. Hence, y∈{0,1}. 0 is also called the negative class, and 1 the positive class, and they are sometimes also denoted by the symbols “-” and “+.” Given *x*(*i*), the corresponding *y*(*i*) is also called the label for the training example.

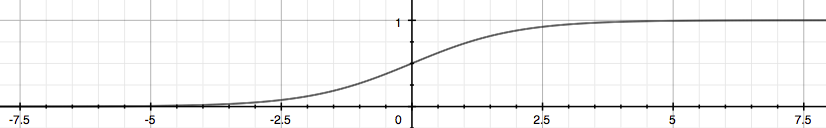
## Hypothesis Representation

We could approach the classification problem ignoring the fact that y is discrete-valued, and use our old linear regression algorithm to try to predict y given x. However, it is easy to construct examples where this method performs very poorly. Intuitively, it also doesn’t make sense for *hθ*(*x*) to take values larger than 1 or smaller than 0 when we know that y ∈ {0, 1}. To fix this, let’s change the form for our hypotheses *hθ*(*x*) to satisfy 0≤*hθ*(*x*)≤1. This is accomplished by plugging *θTx* into the Logistic Function.

Our new form uses the "Sigmoid Function," also called the "Logistic Function":



The following image shows us what the sigmoid function looks like:



The function g(z), shown here, maps any real number to the (0, 1) interval, making it useful for transforming an arbitrary-valued function into a function better suited for classification.

*hθ*(*x*) will give us the **probability** that our output is 1. For example, *hθ*(*x*)=0.7 gives us a probability of 70% that our output is 1. Our probability that our prediction is 0 is just the complement of our probability that it is 1 (e.g. if probability that it is 1 is 70%, then the probability that it is 0 is 30%).



## Decision Boundary

In order to get our discrete 0 or 1 classification, we can translate the output of the hypothesis function as follows:

|  |
| --- |
| *hθ*(*x*)≥0.5→*y*=1  *hθ*(*x*)<0.5→*y*=0 |

The way our logistic function g behaves is that when its input is greater than or equal to zero, its output is greater than or equal to 0.5:

|  |
| --- |
| *g*(*z*)≥0.5 *when z*≥0 |

Remember.

|  |
| --- |
| *z*=0,*e*0=1⇒*g*(*z*)=1/2  *z*→∞,*e*−∞→0⇒*g*(*z*)=1  *z*→−∞,*e*∞→∞⇒*g*(*z*)=0 |

So if our input to g is *θTX*, then that means:

|  |
| --- |
| *hθ*(*x*)=*g*(*θTx*)≥0.5 *whenθTx*≥0 |

From these statements we can now say:

|  |
| --- |
| *θTx*≥0 ⇒ *y*=1  *θTx*<0 ⇒ *y*=0 |

The **decision boundary** is the line that separates the area where y = 0 and where y = 1. It is created by our hypothesis function.

**Example**:

|  |
| --- |
|  |

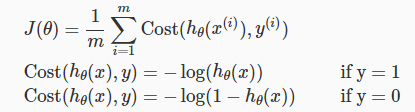
In this case, our decision boundary is a straight vertical line placed on the graph where *x*1=5, and everything to the left of that denotes y = 1, while everything to the right denotes y = 0.

Again, the input to the sigmoid function g(z) (e.g. *θTX*) doesn't need to be linear, and could be a function that describes a circle (e.g. *z*=*θ*0+*θ*1*x1*2+*θ*2*x*22) or any shape to fit our data.

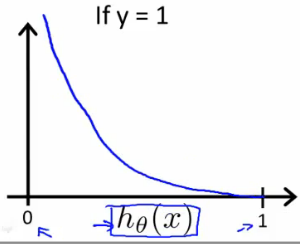
## Cost Function

We cannot use the same cost function that we use for linear regression because the Logistic Function will cause the output to be wavy, causing many local optima. In other words, it will not be a convex function.

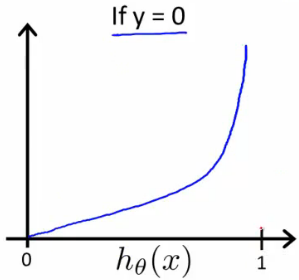
Instead, our cost function for logistic regression looks like:

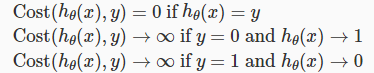


When y = 1, we get the following plot for *J*(*θ*) vs *hθ*(*x*):



Similarly, when y = 0, we get the following plot for *J*(*θ*) vs *hθ*(*x*):





If our correct answer 'y' is 0, then the cost function will be 0 if our hypothesis function also outputs 0. If our hypothesis approaches 1, then the cost function will approach infinity.

If our correct answer 'y' is 1, then the cost function will be 0 if our hypothesis function outputs 1. If our hypothesis approaches 0, then the cost function will approach infinity.

Note that writing the cost function in this way guarantees that J(θ) is convex for logistic regression.

## Simplified Cost Function and Gradient Descent

We can compress our cost function's two conditional cases into one case:

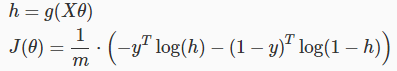


Notice that when y is equal to 1, then the second term (1−*y*)log(1−*hθ*(*x*)) will be zero and will not affect the result. If y is equal to 0, then the first term −*y*log(*hθ*(*x*)) will be zero and will not affect the result.

We can fully write out our entire cost function as follows:

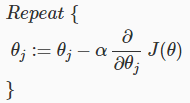


A vectorized implementation is:

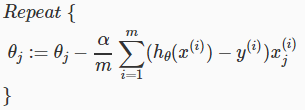


## ****Gradient Descent****

Remember that the general form of gradient descent is:



We can work out the derivative part using calculus to get:



Notice that this algorithm is identical to the one we used in linear regression. We still have to simultaneously update all values in theta.

A vectorized implementation is:



## Advanced Optimization

"Conjugate gradient", "BFGS", and "L-BFGS" are more sophisticated, faster ways to optimize θ that can be used instead of gradient descent. We suggest that you should not write these more sophisticated algorithms yourself (unless you are an expert in numerical computing) but use the libraries instead, as they're already tested and highly optimized. Octave provides them.

We first need to provide a function that evaluates the following two functions for a given input value θ:



We can write a single function that returns both of these:

function [jVal, gradient] = costFunction(theta)

jVal = [...code to compute J(theta)...];

gradient = [...code to compute derivative of J(theta)...];

end

Then we can use octave's "fminunc()" optimization algorithm along with the "optimset()" function that creates an object containing the options we want to send to "fminunc()". (Note: the value for MaxIter should be an integer, not a character string - errata in the video at 7:30)

options = optimset('GradObj', 'on', 'MaxIter', 100);

initialTheta = zeros(2,1);

[optTheta, functionVal, exitFlag] = fminunc(@costFunction, initialTheta,

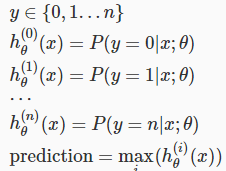
     options);

We give to the function "fminunc()" our cost function, our initial vector of theta values, and the "options" object that we created beforehand.

## Multiclass Classification: One-vs-all

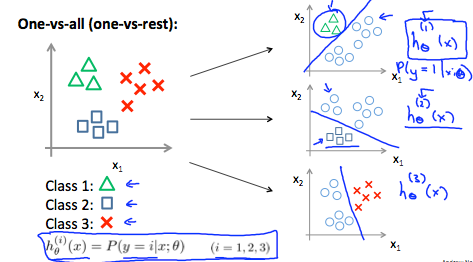
Now we will approach the classification of data when we have more than two categories. Instead of y = {0,1} we will expand our definition so that y = {0,1...n}.

Since y = {0,1...n}, we divide our problem into n+1 (+1 because the index starts at 0) binary classification problems; in each one, we predict the probability that 'y' is a member of one of our classes.



We are basically choosing one class and then lumping all the others into a single second class. We do this repeatedly, applying binary logistic regression to each case, and then use the hypothesis that returned the highest value as our prediction.

The following image shows how one could classify 3 classes:



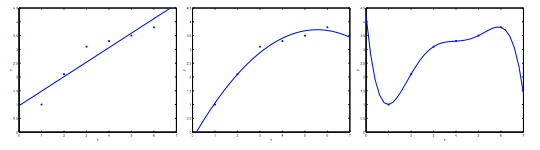
**To summarize:**

Train a logistic regression classifier *hθ*(*x*) for each class to predict the probability that y = i.

To make a prediction on a new x, pick the class that maximizes *hθ*(*x*)

## The Problem of Overfitting

Consider the problem of predicting y from x ∈ R. The left most figure below shows the result of fitting a y = *θ*0+*θ*1*x* to a dataset. We see that the data doesn’t really lie on straight line, and so the fit is not very good.



Instead, if we had added an extra feature *x*2 , and fit *y*=*θ*0+*θ*1*x*+*θ*2*x*2 , then we obtain a slightly better fit to the data (See middle figure). Naively, it might seem that the more features we add, the better. However, there is also a danger in adding too many features: The rightmost figure is the result of fitting a 5*th* order polynomial . We see that even though the fitted curve passes through the data perfectly, we would not expect this to be a very good predictor of, say, housing prices (y) for different living areas (x). Without formally defining what these terms mean, we’ll say the figure on the left shows an instance of **underfitting**—in which the data clearly shows structure not captured by the model—and the figure on the right is an example of **overfitting**.

Underfitting, or high bias, is when the form of our hypothesis function h maps poorly to the trend of the data. It is usually caused by a function that is too simple or uses too few features. At the other extreme, overfitting, or high variance, is caused by a hypothesis function that fits the available data but does not generalize well to predict new data. It is usually caused by a complicated function that creates a lot of unnecessary curves and angles unrelated to the data.

This terminology is applied to both linear and logistic regression. There are two main options to address the issue of overfitting:

1) Reduce the number of features:

* Manually select which features to keep.
* Use a model selection algorithm (studied later in the course).

2) Regularization

* Keep all the features, but reduce the magnitude of parameters *θj*.
* Regularization works well when we have a lot of slightly useful features.

## Cost Function

If we have overfitting from our hypothesis function, we can reduce the weight that some of the terms in our function carry by increasing their cost.

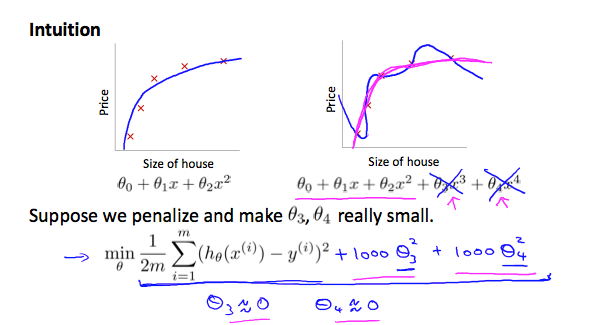
Say we wanted to make the following function more quadratic:



We'll want to eliminate the influence of *θ*3*x*3 and *θ4x*4. Without actually getting rid of these features or changing the form of our hypothesis, we can instead modify our **cost function**:



We've added two extra terms at the end to inflate the cost of *θ*3 and *θ*4. Now, in order for the cost function to get close to zero, we will have to reduce the values of *θ*3 and *θ*4 to near zero. This will in turn greatly reduce the values of *θ*3*x*3and *θ4x*4in our hypothesis function. As a result, we see that the new hypothesis (depicted by the pink curve) looks like a quadratic function but fits the data better due to the extra small terms *θ*3*x*3and *θ4x*4.



We could also regularize all of our theta parameters in a single summation as:



The λ, or lambda, is the **regularization parameter**. It determines how much the costs of our theta parameters are inflated.

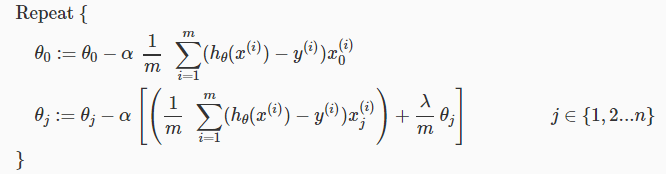
Using the above cost function with the extra summation, we can smooth the output of our hypothesis function to reduce overfitting. If lambda is chosen to be too large, it may smooth out the function too much and cause underfitting. Hence, what would happen if *λ*=0 or is too small ?

## Regularized Linear Regression

We can apply regularization to both linear regression and logistic regression. We will approach linear regression first.

## Gradient Descent

We will modify our gradient descent function to separate out *θ*0 from the rest of the parameters because we do not want to penalize *θ*0.



The term  performs our regularization. With some manipulation our update rule can also be represented as:

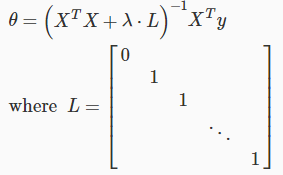


The first term in the above equation,  will always be less than 1. Intuitively you can see it as reducing the value of *θj* by some amount on every update. Notice that the second term is now exactly the same as it was before.

## ****Normal Equation****

Now let's approach regularization using the alternate method of the non-iterative normal equation.

To add in regularization, the equation is the same as our original, except that we add another term inside the parentheses:

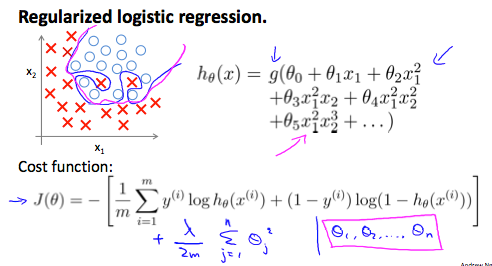


L is a matrix with 0 at the top left and 1's down the diagonal, with 0's everywhere else. It should have dimension (n+1)×(n+1). Intuitively, this is the identity matrix (though we are not including *x*0), multiplied with a single real number λ.

Recall that if m ≤ n, then *XTX* is non-invertible. However, when we add the term λ⋅L, then *XTX* + λ⋅L becomes invertible.

## Regularized Logistic Regression

We can regularize logistic regression in a similar way that we regularize linear regression. As a result, we can avoid overfitting. The following image shows how the regularized function, displayed by the pink line, is less likely to overfit than the non-regularized function represented by the blue line:



## Cost Function

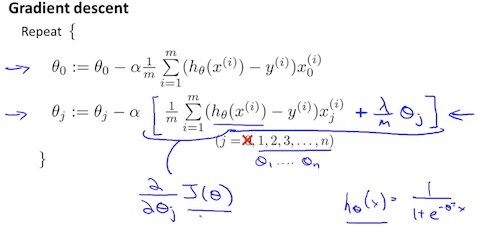
Recall that our cost function for logistic regression was:



We can regularize this equation by adding a term to the end:



The second sum,  **means to explicitly exclude** the bias term, *θ*0. I.e. the θ vector is indexed from 0 to n (holding n+1 values, *θ*0 through *θn*), and this sum explicitly skips *θ*0, by running from 1 to n, skipping 0. Thus, when computing the equation, we should continuously update the two following equations:

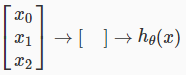


# Week 4 Neuron Network

## Model Representation I

Let's examine how we will represent a hypothesis function using neural networks. At a very simple level, neurons are basically computational units that take inputs (**dendrites**) as electrical inputs (called "spikes") that are channeled to outputs (**axons**). In our model, our dendrites are like the input features *x*1⋯*xn*, and the output is the result of our hypothesis function. In this model our *x*0 input node is sometimes called the "bias unit." It is always equal to 1. In neural networks, we use the same logistic function as in classification, , yet we sometimes call it a sigmoid (logistic) **activation** function. In this situation, our "theta" parameters are sometimes called "weights".

Visually, a simplistic representation looks like:



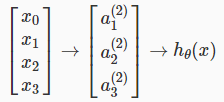
Our input nodes (layer 1), also known as the "input layer", go into another node (layer 2), which finally outputs the hypothesis function, known as the "output layer".

We can have intermediate layers of nodes between the input and output layers called the "hidden layers."

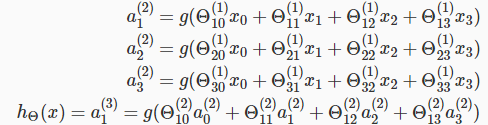
In this example, we label these intermediate or "hidden" layer nodes *a02*⋯*a*n2 and call them "activation units."



If we had one hidden layer, it would look like:



The values for each of the "activation" nodes is obtained as follows:



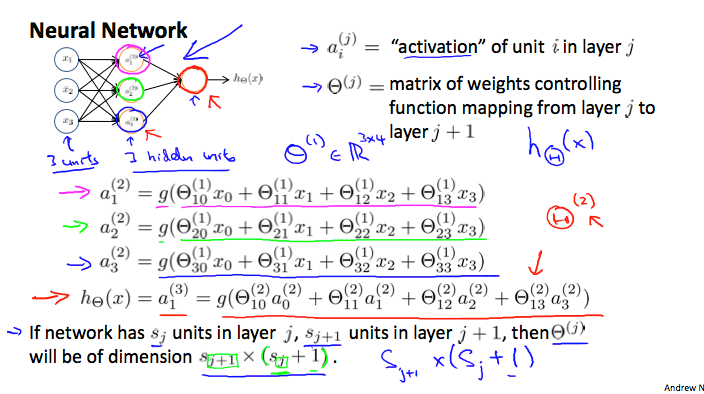
This is saying that we compute our activation nodes by using a 3×4 matrix of parameters. We apply each row of the parameters to our inputs to obtain the value for one activation node. Our hypothesis output is the logistic function applied to the sum of the values of our activation nodes, which have been multiplied by yet another parameter matrix Θ(2) containing the weights for our second layer of nodes.

Each layer gets its own matrix of weights, Θ(*j*).

The dimensions of these matrices of weights is determined as follows:

If network has *sj* units in layer *j* and *sj*+1 units in layer *j*+1, then Θ(*j*) will be of dimension *sj*+1×(*sj*+1).

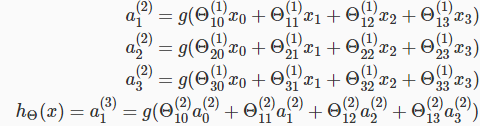
The +1 comes from the addition in Θ(*j*) of the "bias nodes," *x*0 and Θ0(*j*). In other words the output nodes will not include the bias nodes while the inputs will. The following image summarizes our model representation:



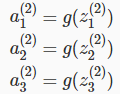
Example: layer 1 has 2 input nodes and layer 2 has 4 activation nodes. Dimension of Θ(1) is going to be 4×3 where *sj*=2 and *sj*+1=4, so *sj*+1×(*sj*+1)=4×3.

## Model Representation II

To re-iterate, the following is an example of a neural network:



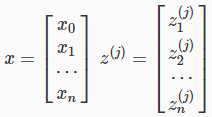
In this section we'll do a vectorized implementation of the above functions. We're going to define a new variable *zk*(*j*) that encompasses the parameters inside our g function. In our previous example if we replaced by the variable z for all the parameters we would get:



In other words, for layer j=2 and node k, the variable z will be:



The vector representation of x and *zj* is:



Setting *x*=*a*(1), we can rewrite the equation as:



We are multiplying our matrix Θ(*j*−1) with dimensions *sj*×(*n*+1) (where *sj* is the number of our activation nodes) by our vector *a*(*j*−1) with height (n+1). This gives us our vector *z*(*j*) with height *sj*. Now we can get a vector of our activation nodes for layer j as follows:



Where our function g can be applied element-wise to our vector *z*(*j*).

We can then add a bias unit (equal to 1) to layer j after we have computed *a*(*j*). This will be element *a0*(*j*) and will be equal to 1. To compute our final hypothesis, let's first compute another z vector:

*z*(*j*+1)=Θ(*j*)*a*(*j*)

We get this final z vector by multiplying the next theta matrix after Θ(*j*−1) with the values of all the activation nodes we just got. This last theta matrix Θ(*j*) will have only **one row**which is multiplied by one column *a*(*j*) so that our result is a single number. We then get our final result with:

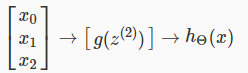
*h*Θ(*x*)=*a*(*j*+1)=*g*(*z*(*j*+1))

Notice that in this **last step**, between layer j and layer j+1, we are doing **exactly the same thing** as we did in logistic regression. Adding all these intermediate layers in neural networks allows us to more elegantly produce interesting and more complex non-linear hypotheses.

## Examples and Intuitions I

A simple example of applying neural networks is by predicting *x*1 AND *x*2, which is the logical 'and' operator and is only true if both *x*1 and *x*2 are 1.

The graph of our functions will look like:

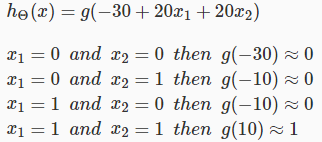


Remember that *x*0 is our bias variable and is always 1.

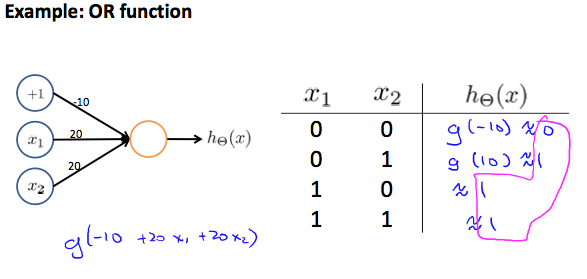
Let's set our first theta matrix as:



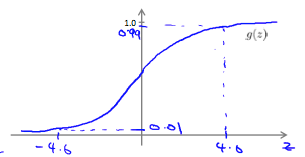
This will cause the output of our hypothesis to only be positive if both *x*1 and *x*2 are 1. In other words:



So we have constructed one of the fundamental operations in computers by using a small neural network rather than using an actual AND gate. Neural networks can also be used to simulate all the other logical gates. The following is an example of the logical operator 'OR', meaning either *x*1 is true or *x*2 is true, or both:

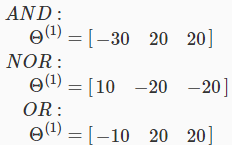


Where g(z) is the following:

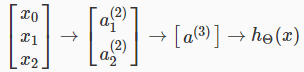


## Examples and Intuitions II

The Θ(1) matrices for AND, NOR, and OR are:



We can combine these to get the XNOR logical operator (which gives 1 if *x*1 and *x*2 are both 0 or both 1).



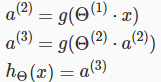
For the transition between the first and second layer, we'll use a Θ(1) matrix that combines the values for AND and NOR:



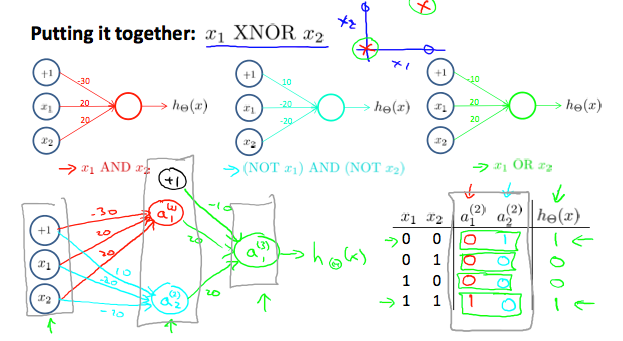
For the transition between the second and third layer, we'll use a Θ(2) matrix that uses the value for OR:



Let's write out the values for all our nodes:

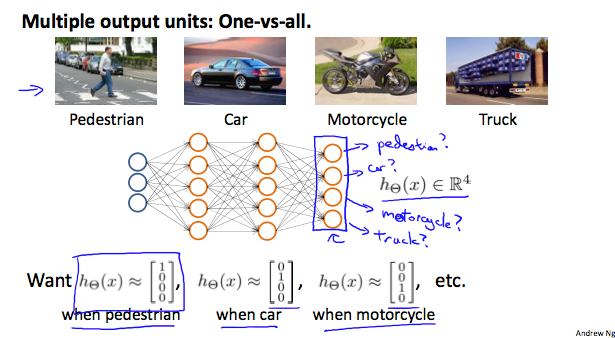


And there we have the XNOR operator using two hidden layers! The following summarizes the above algorithm:

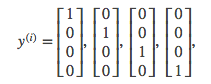


## Multiclass Classification

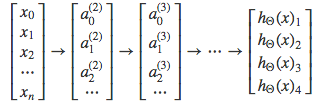
To classify data into multiple classes, we let our hypothesis function return a vector of values. Say we wanted to classify our data into one of four categories. We will use the following example to see how this classification is done. This algorithm takes as input an image and classifies it accordingly:



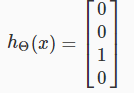
We can define our set of resulting classes as y:



Each *y*(*i*) represents a different image corresponding to either a car, pedestrian, truck, or motorcycle. The inner layers, each provide us with some new information which leads to our final hypothesis function. The setup looks like:



Our resulting hypothesis for one set of inputs may look like:



In which case our resulting class is the third one down, or *h*Θ(*x*)3, which represents the motorcycle.

# Week 5 Neural Networks: Learning

## Cost Function

Let's first define a few variables that we will need to use:

* L = total number of layers in the network
* *sl* = number of units (not counting bias unit) in layer l
* K = number of output units/classes

Recall that in neural networks, we may have many output nodes. We denote *h*Θ(*x*)*k* as being a hypothesis that results in the *kth* output. Our cost function for neural networks is going to be a generalization of the one we used for logistic regression. Recall that the cost function for regularized logistic regression was:



For neural networks, it is going to be slightly more complicated:



We have added a few nested summations to account for our multiple output nodes. In the first part of the equation, before the square brackets, we have an additional nested summation that loops through the number of output nodes.

In the regularization part, after the square brackets, we must account for multiple theta matrices. The number of columns in our current theta matrix is equal to the number of nodes in our current layer (including the bias unit). The number of rows in our current theta matrix is equal to the number of nodes in the next layer (excluding the bias unit). As before with logistic regression, we square every term.

Note:

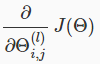
* the double sum simply adds up the logistic regression costs calculated for each cell in the output layer
* the triple sum simply adds up the squares of all the individual Θs in the entire network.
* the i in the triple sum does **not** refer to training example i

## Backpropagation Algorithm

"Backpropagation" is neural-network terminology for minimizing our cost function, just like what we were doing with gradient descent in logistic and linear regression. Our goal is to compute:

minΘ*J*(Θ)

That is, we want to minimize our cost function J using an optimal set of parameters in theta. In this section we'll look at the equations we use to compute the partial derivative of J(Θ):



In back propagation we're going to compute for every node:

*δj*(*l*) = "error" of node j in layer l

Recall that *aj(l)* is activation node j in layer l. For the **last layer**, we can compute the vector of delta values with:

*δ*(*L*)=*y*−*a*(*L*)

Where L is our total number of layers and *a*(*L*) is the vector of outputs of the activation units for the last layer. So our "error values" for the last layer are simply the differences of our actual results in the last layer and the correct outputs in y. To get the delta values of the layers before the last layer, we can use an equation that steps us back from right to left:

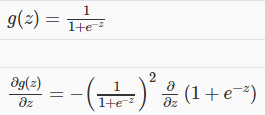


The delta values of layer l are calculated by multiplying the delta values in the next layer with the theta matrix of layer l. We then element-wise multiply that with a function called g', or g-prime, which is the derivative of the activation function g evaluated with the input values given by *z*(*l*).

The g-prime derivative terms can also be written out as:



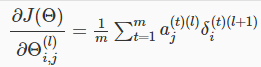
This can be shown and proved in calculus :



The derivation and proofs are complicated and involved, but you can still implement the above equations to do back propagation without knowing the details. If you are familiar with calculus you can try to finish the derivation, else do not worry about it. The full back propagation equation for the inner nodes is then:



We can compute our partial derivative terms by multiplying our activation values and our error values for each training example t:

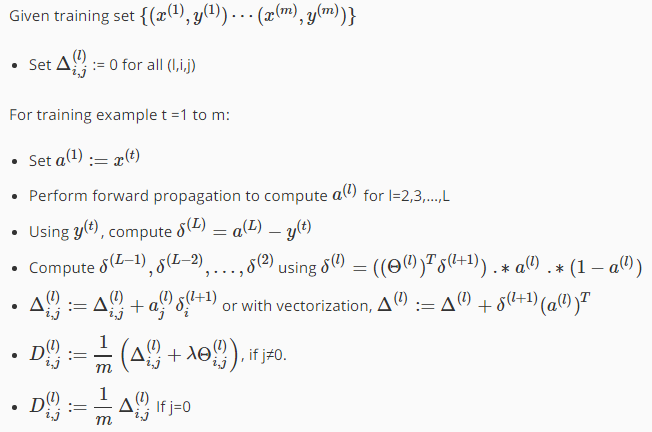


This however ignores regularization, which we'll deal with later.

Note: *δl*+1 and *al*+1 are vectors with *sl*+1 elements. Similarly,  *a*(*l*) is a vector with *sl* elements. Multiplying them produces a matrix that is *sl*+1 by *sl* which is the same dimension as Θ(*l*). That is, the process produces a gradient term for every element in Θ(*l*).

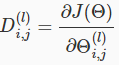
We can now take all these equations and put them together into a backpropagation algorithm:

**Back propagation Algorithm**



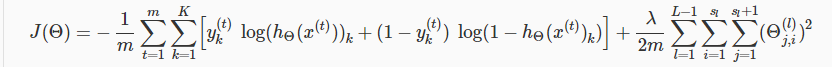
The capital-delta matrix is used as an "accumulator" to add up our values as we go along and eventually compute our partial derivative.

The actual proof is quite involved, but, the *Di*,*j(l)* terms are the partial derivatives and the results we are looking for:



## Backpropagation Intuition

Recall that the cost function for a neural network is:



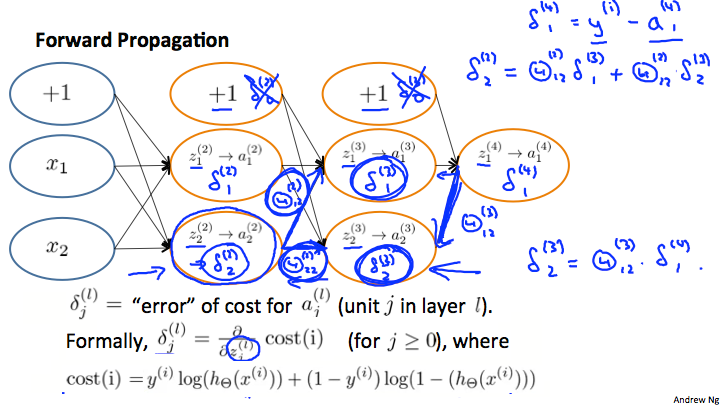
If we consider simple non-multiclass classification (k = 1) and disregard regularization, the cost is computed with:



Intuitively, *δj*(*l*) is the "error" for *aj*(*l*) (unit j in layer l). More formally, the delta values are actually the derivative of the cost function:



Recall that our derivative is the slope of a line tangent to the cost function, so the steeper the slope the more incorrect we are. Let us consider the following neural network below and see how we could calculate some *δj*(*l*):



In the image above, to calculate *δ2(2)*, we multiply the weights Θ12(2) and Θ22(2) by their respective *δ* values found to the right of each edge. So we get *δ2(2)*= Θ12(2)\**δ1(3)*+Θ22(2)\**δ2(3)*. To calculate every single possible *δj(l)*, we could start from the right of our diagram. We can think of our edges as our Θ*ij*. Going from right to left, to calculate the value of *δj(l)*, you can just take the over all sum of each weight times the *δ* it is coming from. Hence, another example would be *δ2*(3)=Θ12(3)\**δ1*(4).

## Implementation Note: Unrolling Parameters

With neural networks, we are working with sets of matrices:

|  |
| --- |
| Θ(1),Θ(2),Θ(3),…*D*(1),*D*(2),*D*(3),… |

In order to use optimizing functions such as "fminunc()", we will want to "unroll" all the elements and put them into one long vector:

thetaVector = [ Theta1(:); Theta2(:); Theta3(:); ]

deltaVector = [ D1(:); D2(:); D3(:) ]

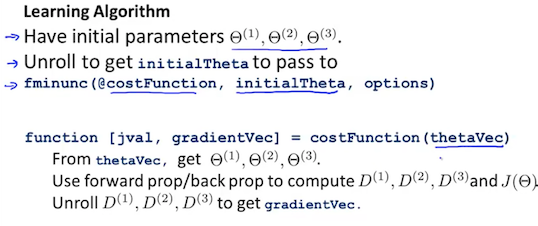
If the dimensions of Theta1 is 10x11, Theta2 is 10x11 and Theta3 is 1x11, then we can get back our original matrices from the "unrolled" versions as follows:

Theta1 = reshape(thetaVector(1:110),10,11)

Theta2 = reshape(thetaVector(111:220),10,11)

Theta3 = reshape(thetaVector(221:231),1,11)

To summarize:



## Gradient Checking

Gradient checking will assure that our backpropagation works as intended. We can approximate the derivative of our cost function with:



With multiple theta matrices, we can approximate the derivative **with respect to** Θ*j* as follows:



A small value for *ϵ* (epsilon) such as *ϵ*=10−4, guarantees that the math works out properly. If the value for *ϵ* is too small, we can end up with numerical problems.

Hence, we are only adding or subtracting epsilon to the Θ*j* matrix. In octave we can do it as follows:

epsilon = 1e-4;

for i = 1:n,

thetaPlus = theta;

thetaPlus(i) += epsilon;

thetaMinus = theta;

thetaMinus(i) -= epsilon;

gradApprox(i) = (J(thetaPlus) - J(thetaMinus))/(2\*epsilon)

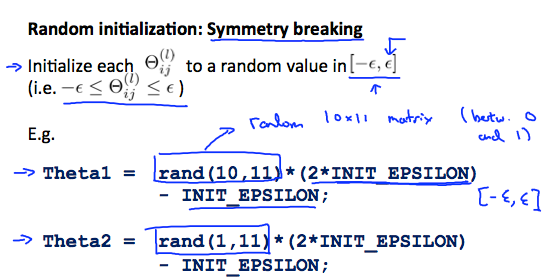
end;

We previously saw how to calculate the deltaVector. So once we compute our gradApprox vector, we can check that gradApprox ≈ deltaVector.

Once you have verified **once** that your backpropagation algorithm is correct, you don't need to compute gradApprox again. The code to compute gradApprox can be very slow.

## Random Initialization

Initializing all theta weights to zero does not work with neural networks. When we backpropagate, all nodes will update to the same value repeatedly. Instead we can randomly initialize our weights for our Θ matrices using the following method:



Hence, we initialize each Θij(l) to a random value between[−*ϵ*,*ϵ*]. Using the above formula guarantees that we get the desired bound. The same procedure applies to all the Θ's. Below is some working code you could use to experiment.

If the dimensions of Theta1 is 10x11, Theta2 is 10x11 and Theta3 is 1x11.

Theta1 = rand(10,11) \* (2 \* INIT\_EPSILON) - INIT\_EPSILON;

Theta2 = rand(10,11) \* (2 \* INIT\_EPSILON) - INIT\_EPSILON;

Theta3 = rand(1,11) \* (2 \* INIT\_EPSILON) - INIT\_EPSILON;

rand(x,y) is just a function in octave that will initialize a matrix of random real numbers between 0 and 1.

(Note: the epsilon used above is unrelated to the epsilon from Gradient Checking)

# Week 6 Advice for Applying Machine Learning

## Evaluating a Hypothesis

Once we have done some trouble shooting for errors in our predictions by:

* Getting more training examples
* Trying smaller sets of features
* Trying additional features
* Trying polynomial features
* Increasing or decreasing λ

We can move on to evaluate our new hypothesis.

A hypothesis may have a low error for the training examples but still be inaccurate (because of overfitting). Thus, to evaluate a hypothesis, given a dataset of training examples, we can split up the data into two sets: a **training set** and a **test set**. Typically, the training set consists of 70 % of your data and the test set is the remaining 30 %.

The new procedure using these two sets is then:

1. Learn Θ and minimize *Jtrain*(Θ) using the training set
2. Compute the test set error *Jtest*(Θ)

## The test set error

1. For linear regression: 
2. For classification ~ Misclassification error (aka 0/1 misclassification error):



This gives us a binary 0 or 1 error result based on a misclassification. The average test error for the test set is:



This gives us the proportion of the test data that was misclassified.

## Model Selection and Train/Validation/Test Sets

* Just because a learning algorithm fits a training set well, that does not mean it is a good hypothesis.
* The error of your hypothesis as measured on the data set with which you trained the parameters will be lower than any other data set.

In order to choose the model of your hypothesis, you can test each degree of polynomial and look at the error result.

**Without the Validation Set (note: this is a bad method - do not use it)**

1. Optimize the parameters in Θ using the training set for each polynomial degree.
2. Find the polynomial degree d with the least error using the test set.
3. Estimate the generalization error also using the test set with *Jtest*(Θ(*d*)), (d = theta from polynomial with lower error);

In this case, we have trained one variable, d, or the degree of the polynomial, using the test set. This will cause our error value to be greater for any other set of data.

**Use of the CV set**

To solve this, we can introduce a third set, the **Cross Validation Set**, to serve as an intermediate set that we can train d with. Then our test set will give us an accurate, non-optimistic error.

One example way to break down our dataset into the three sets is:

* Training set: 60%
* Cross validation set: 20%
* Test set: 20%

We can now calculate three separate error values for the three different sets.

**With the Validation Set (note: this method presumes we do not also use the CV set for regularization)**

1. Optimize the parameters in Θ using the training set for each polynomial degree.
2. Find the polynomial degree d with the least error using the cross validation set.
3. Estimate the generalization error using the test set with *Jtest*(Θ(*d*)), (d = theta from polynomial with lower error);

This way, the degree of the polynomial d has not been trained using the test set.

(Mentor note: be aware that using the CV set to select 'd' means that we cannot also use it for the validation curve process of setting the lambda value).

## Diagnosing Bias vs. Variance

In this section we examine the relationship between the degree of the polynomial d and the underfitting or overfitting of our hypothesis.

* We need to distinguish whether **bias** or **variance** is the problem contributing to bad predictions.
* High bias is underfitting and high variance is overfitting. We need to find a golden mean between these two.

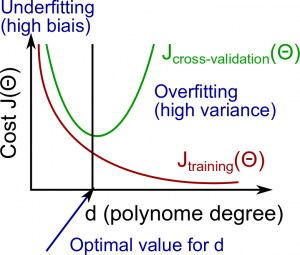
The training error will tend to **decrease** as we increase the degree d of the polynomial.

At the same time, the cross validation error will tend to **decrease** as we increase d up to a point, and then it will **increase** as d is increased, forming a convex curve.

**High bias (underfitting)**: both *Jtrain*(Θ) and *JCV*(Θ) will be high. Also, *JCV*(Θ)≈*Jtrain*(Θ).

**High variance (overfitting)**: *Jtrain*(Θ) will be low and *JCV*(Θ) will be much greater than*Jtrain*(Θ).

The is represented in the figure below:



## Regularization and Bias/Variance

Instead of looking at the degree d contributing to bias/variance, now we will look at the regularization parameter λ.

* Large λ: High bias (underfitting)
* Intermediate λ: just right
* Small λ: High variance (overfitting)

A large lambda heavily penalizes all the Θ parameters, which greatly simplifies the line of our resulting function, so causes underfitting.

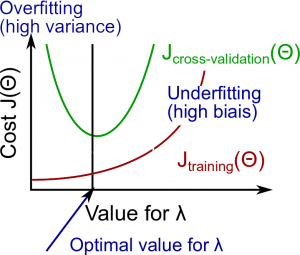
The relationship of λ to the training set and the variance set is as follows:

**Low λ**: *Jtrain*(Θ) is low and *JCV*(Θ) is high (high variance/overfitting).

**Intermediate λ**: *Jtrain*(Θ) and *JCV*(Θ) are somewhat low and *Jtrain*(Θ)≈*JCV*(Θ).

**Large λ**: both *Jtrain*(Θ) and *JCV*(Θ) will be high (underfitting /high bias)

The figure below illustrates the relationship between lambda and the hypothesis:



In order to choose the model and the regularization λ, we need:

1. Create a list of lambda (i.e. λ∈{0,0.01,0.02,0.04,0.08,0.16,0.32,0.64,1.28,2.56,5.12,10.24});
2. Select a lambda to compute;
3. Create a model set like degree of the polynomial or others;
4. Select a model to learn Θ;
5. Learn the parameter Θ for the model selected, using *Jtrain*(Θ) **with** λ selected (this will learn Θ for the next step);
6. Compute the train error using the learned Θ (computed with λ ) on the *Jtrain*(Θ) **without** regularization or λ = 0;
7. Compute the cross validation error using the learned Θ (computed with λ) on the *JCV*(Θ) **without** regularization or λ = 0;
8. Do this for the entire model set and lambdas, then select the best combo that produces the lowest error on the cross validation set;
9. Now if you need visualize to help you understand your decision, you can plot to the figure like above with: (λ x Cost *Jtrain*(Θ) and (λ x Cost *JCV*(Θ));
10. Now using the best combo Θ and λ, apply it on *Jtest*(Θ) to see if it has a good generalization of the problem.
11. To help decide the best polynomial degree and λ to use, we can diagnose with the learning curves, that is the next subject.

## Learning Curves

Training 3 examples will easily have 0 errors because we can always find a quadratic curve that exactly touches 3 points.

* As the training set gets larger, the error for a quadratic function increases.
* The error value will plateau out after a certain m, or training set size.

**With high bias**

**Low training set size**: causes *Jtrain*(Θ) to be low and *JCV*(Θ) to be high.

**Large training set size**: causes both *Jtrain*(Θ) and *JCV*(Θ) to be high with *Jtrain*(Θ)≈*JCV*(Θ).

If a learning algorithm is suffering from **high bias**, getting more training data **will not (by itself) help much**.

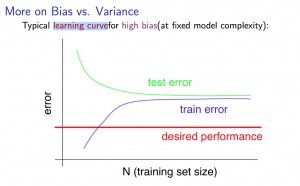
For high variance, we have the following relationships in terms of the training set size:

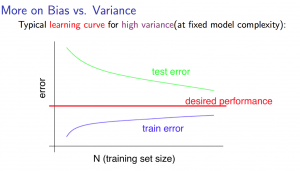
**With high variance**

**Low training set size**: *Jtrain*(Θ) will be low and *JCV*(Θ) will be high.

**Large training set size**: *Jtrain*(Θ) increases with training set size and *JCV*(Θ) continues to decrease without leveling off. Also, *Jtrain*(Θ)<*JCV*(Θ) but the difference between them remains significant.

If a learning algorithm is suffering from **high variance**, getting more training data is **likely to help.**





## Deciding What to Do Next Revisited

Our decision process can be broken down as follows:

* Getting more training examples

Fixes high variance

* Trying smaller sets of features

Fixes high variance

* Adding features

Fixes high bias

* Adding polynomial features

Fixes high bias

* Decreasing λ

Fixes high bias

* Increasing λ

Fixes high variance

## Diagnosing Neural Networks

* A neural network with fewer parameters is **prone to underfitting**. It is also **computationally cheaper**.
* A large neural network with more parameters is **prone to overfitting**. It is also **computationally expensive**. In this case you can use regularization (increase λ) to address the overfitting.

Using a single hidden layer is a good starting default. You can train your neural network on a number of hidden layers using your cross validation set.

## Model Selection

Choosing M the order of polynomials.

How can we tell which parameters Θ to leave in the model (known as "model selection")?

There are several ways to solve this problem:

* Get more data (very difficult).
* Choose the model which best fits the data without overfitting (very difficult).
* Reduce the opportunity for overfitting through regularization.

**Bias: approximation error (Difference between expected value and optimal value)**

* High Bias = UnderFitting (BU)
* *Jtrain*(Θ) and *JCV*(Θ) both will be high and *Jtrain*(Θ) ≈ *JCV*(Θ)

**Variance: estimation error due to finite data**

* High Variance = OverFitting (VO)
* *Jtrain*(Θ) is low and *JCV*(Θ) ≫*Jtrain*(Θ)

**Intuition for the bias-variance trade-off:**

* Complex model => sensitive to data => much affected by changes in X => high variance, low bias.
* Simple model => more rigid => does not change as much with changes in X => low variance, high bias.

One of the most important goals in learning: finding a model that is just right in the bias-variance trade-off.

**Regularization Effects:**

* Small values of λ allow model to become finely tuned to noise leading to large variance => overfitting.
* Large values of λ pull weight parameters to zero leading to large bias => underfitting.

**Model Complexity Effects:**

* Lower-order polynomials (low model complexity) have high bias and low variance. In this case, the model fits poorly consistently.
* Higher-order polynomials (high model complexity) fit the training data extremely well and the test data extremely poorly. These have low bias on the training data, but very high variance.
* In reality, we would want to choose a model somewhere in between, that can generalize well but also fits the data reasonably well.

**A typical rule of thumb when running diagnostics is:**

* More training examples fixes high variance but not high bias.
* Fewer features fixes high variance but not high bias.
* Additional features fixes high bias but not high variance.
* The addition of polynomial and interaction features fixes high bias but not high variance.
* When using gradient descent, decreasing lambda can fix high bias and increasing lambda can fix high variance (lambda is the regularization parameter).
* When using neural networks, small neural networks are more prone to under-fitting and big neural networks are prone to over-fitting. Cross-validation of network size is a way to choose alternatives.

## Machine Learning System Design

### Prioritizing What to Work On

Different ways we can approach a machine learning problem:

* Collect lots of data (for example "honeypot" project but doesn't always work)
* Develop sophisticated features (for example: using email header data in spam emails)
* Develop algorithms to process your input in different ways (recognizing misspellings in spam).

It is difficult to tell which of the options will be helpful.

### Error Analysis

The recommended approach to solving machine learning problems is:

* Start with a simple algorithm, implement it quickly, and test it early.
* Plot learning curves to decide if more data, more features, etc. will help
* Error analysis: manually examine the errors on examples in the cross validation set and try to spot a trend.

It's important to get error results as a single, numerical value. Otherwise it is difficult to assess your algorithm's performance.

You may need to process your input before it is useful. For example, if your input is a set of words, you may want to treat the same word with different forms (fail/failing/failed) as one word, so must use "stemming software" to recognize them all as one.

### Error Metrics for Skewed Classes

It is sometimes difficult to tell whether a reduction in error is actually an improvement of the algorithm.

* For example: In predicting a cancer diagnoses where 0.5% of the examples have cancer, we find our learning algorithm has a 1% error. However, if we were to simply classify every single example as a 0, then our error would reduce to 0.5% even though we did not improve the algorithm.

This usually happens with **skewed classes**; that is, when our class is very rare in the entire data set.

Or to say it another way, when we have lot more examples from one class than from the other class.

For this we can use **Precision/Recall**.

* Predicted: 1, Actual: 1 --- True positive
* Predicted: 0, Actual: 0 --- True negative
* Predicted: 0, Actual, 1 --- False negative
* Predicted: 1, Actual: 0 --- False positive

**Precision**: of all patients we predicted where y=1, what fraction actually has cancer?

|  |
| --- |
| True PositivesTotal number of predicted positives=True PositivesTrue Positives+False positives |

**Recall**: Of all the patients that actually have cancer, what fraction did we correctly detect as having cancer?

|  |
| --- |
| True PositivesTotal number of actual positives=True PositivesTrue Positives+False negatives |

These two metrics give us a better sense of how our classifier is doing. We want both precision and recall to be high.

In the example at the beginning of the section, if we classify all patients as 0, then our **recall** will be 00+*f*=0, so despite having a lower error percentage, we can quickly see it has worse recall.

Note 1: if an algorithm predicts only negatives like it does in one of exercises, the precision is not defined, it is impossible to divide by 0. F1 score will not be defined too.

Note 2: a manual calculation of precision and other functions is a error prone process. it is very easy though to create an Excel file for this. Put into it a table 2\*2 for all necessary input values, label them like "TruePositives", "FalsePositives", and on other cells of Excel add formulas like =SUM(TruePositive, FalsePositive, TrueNegative, FalseNegative), label this one AllExamples. Then on another cell label Accuracy and a formula: =SUM(TruePositive,TrueNegative)/AllExamples. The same with others. After 10 minutes you will have a spreadsheet for all examples and questions. [Snap shot <https://share.coursera.org/wiki/index.php/File:Spreadsheetquiz6.GIF> ]

### Trading Off Precision and Recall

We might want a **confident** prediction of two classes using logistic regression. One way is to increase our threshold:

* Predict 1 if: *hθ*(*x*)≥0.7
* Predict 0 if: *hθ*(*x*)<0.7

This way, we only predict cancer if the patient has a 70% chance.

Doing this, we will have **higher precision** but **lower recall** (refer to the definitions in the previous section).

In the opposite example, we can lower our threshold:

* Predict 1 if: *hθ*(*x*)≥0.3
* Predict 0 if: *hθ*(*x*)<0.3

That way, we get a very **safe** prediction. This will cause **higher recall** but **lower precision**.

The greater the threshold, the greater the precision and the lower the recall.

The lower the threshold, the greater the recall and the lower the precision.

In order to turn these two metrics into one single number, we can take the **F value**.

One way is to take the **average**:

*P*+*R*2

This does not work well. If we predict all y=0 then that will bring the average up despite having 0 recall. If we predict all examples as y=1, then the very high recall will bring up the average despite having 0 precision.

A better way is to compute the **F Score** (or F1 score):

F Score=2*PRP*+*R*

In order for the F Score to be large, both precision and recall must be large.

We want to train precision and recall on the **cross validation set** so as not to bias our test set.

### Data for Machine Learning

How much data should we train on?

In certain cases, an "inferior algorithm," if given enough data, can outperform a superior algorithm with less data.

We must choose our features to have **enough** information. A useful test is: Given input x, would a human expert be able to confidently predict y?

**Rationale for large data**: if we have a **low bias** algorithm (many features or hidden units making a very complex function), then the larger the training set we use, the less we will have overfitting (and the more accurate the algorithm will be on the test set).

### Quiz instructions

When the quiz instructions tell you to enter a value to "two decimal digits", what it really means is "two significant digits". So, just for example, the value 0.0123 should be entered as "0.012", not "0.01".

References:

* <https://class.coursera.org/ml/lecture/index>
* <http://www.cedar.buffalo.edu/~srihari/CSE555/Chap9.Part2.pdf>
* <http://blog.stephenpurpura.com/post/13052575854/managing-bias-variance-tradeoff-in-machine-learning>
* <http://www.cedar.buffalo.edu/~srihari/CSE574/Chap3/Bias-Variance.pdf>

# Week 7 Optimization Objective

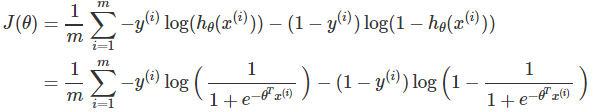
The **Support Vector Machine** (SVM) is yet another type of supervised machine learning algorithm. It is sometimes cleaner and more powerful.

Recall that in logistic regression, we use the following rules:

if y=1, then *hθ*(*x*)≈1 and Θ*Tx*≫0

if y=0, then *hθ*(*x*)≈0 and Θ*Tx* ≫0

Recall the cost function for (unregularized) logistic regression:



SVM library <http://www.csie.ntu.edu.tw/~cjlin/libsvm/>

# Week 8 **Clustering**

## Unsupervised Learning: Introduction

Unsupervised learning is contrasted from supervised learning because it uses an **unlabeled** training set rather than a labeled one.

In other words, we don't have the vector y of expected results, we only have a dataset of features where we can find structure.

Clustering is good for:

* Market segmentation
* Social network analysis
* Organizing computer clusters
* Astronomical data analysis

# 知乎讲座

Level 1： 掌握基础技能和思想

* 1. 数据产品经理（不同于用户产品经理），产品架构师（数据使用逻辑和功能的设计与优化）
     + 基础工具 Excel， SQL，Hive or Pig
     + 典型问题：机制设计(price modeling)，冷启动，标签体系
     + 思维模式：依赖数据做决策，建立产品闭环
     + 职能分工：功能产品（类似用户产品），策略产品
  2. 系统工程师
     + 编辑语言：C/C++、Go、Java （选一到两种熟练使用）
     + 开源工具：No-SQL、Nginx、 Spark、Kafka
     + 主要问题：大数据存储与计算、高并发服务
  3. 算法工程师
     + 编程数据：C/C++、Java、Python（后两个最重要）
     + 知识准备：ML/DL、最优化（推荐书：最优化Convex optimization, numerical optimization，建模：PRML，deep learning）、分布式计算
     + 主要问题：报表/BI（OLAP框架，订制报表）、用户画像、预测模型

Level 2：参与一个业务闭环过程

* 业务闭环（OPEN）
  + 建立明确的优化目标（Objective）- 第一步要定义好，最重要。要明确写成一个数学表达式
  + 打通数据记录和分析流程（Process）- 建流程， 搭框架，（系统工程师和算法工程师）
  + 建立A/B测试优化的框架（Experiment）- 尽早建立实验框架，使之自动进化
  + 将目标按转化网络分解（Net）- 具体落实到某个环节上去优化， 做分解
* 通过闭环的优化过程，抚摸和感知数据

Level 3：主持一项数据产品

误区一：数据科学关键在于模型

两个重要定理：

1. No Free Lunch NFL 定理：没有任何算法在所有数据情形下有天然优势，哪怕跟随机猜测比。所有模型从期望啥严格一致，如果把所有数据都用上。但对某些数据集，会有好的模型。所以必须有领域知识来指导模型的选择。
2. The Ugly Ducking 定理：丑小鸭与白天鹅之间的区别和两只白天鹅之间的区别一样大。这里区别怎么定义？如果在没有定义清楚的情况下，区别是一样大的。

误区二：我需要成为全栈工程师

* 全栈工程师
  + 只需同时具备前端和后台能力，并能利用多种技能独立完成产品的人 – 中国特色。什么是产品？
  + 杂则必然不精
* 不同的技术岗位，需要不同的素养
  + 系统工程师：良好的代码习惯、严谨的测试流程 – 代码质量要高，由测试驱动
  + 算法工程师： 很多算法逻辑是不容易测试的 – 不crash，总有结果，靠测试不能解决问题

误区三：我不是技术出身所以不懂产品

* 什么是技术
  + 实现产品逻辑的代码、模型和架构
  + 例如：深度学习、爬虫、Nginx服务器
* 什么是产品
  + 定义问题、解决问题的逻辑
  + 例如：用户标签系统、冷启动策略、语义检索
* 所有岗位都必须深入理解产品

误区四：不断切换从事的业务领域

* 业务领域先验知识的积累，是成功进行数据建模的基础
* 业务领域的商业逻辑需要花时间搞清楚，这对于产品决策至关重要
* 同一个领域的不断努力可以形成个人口碑