

Chapter 8

Optimization for Training Models

Deep learning algorithms involve optimization in many contexts. Performing inference in models such as PCA involves solving an optimization problem. We often use analytical optimization to write proofs. Of all of the many optimization problems involved in deep learning, the most difficult is neural network training. It is quite common to invest a lot of time on hundreds of machines in order to solve even a single neural network training problem. Because this problem is so important, a specialized set of optimization techniques have been developed. This chapter presents these optimization techniques for neural networks.

If you are unfamiliar with the basic principles of gradient descent, we suggest reviewing [chapter 4](#). That chapter includes a brief review of the basic principles of gradient descent.

the second derivatives of the cost function. Finally, we combine several optimization strategies that are formed by combining lower-level algorithms into higher-level procedures.

8.1 How Learning Differs from Pure Optimization

Optimization algorithms used for training of deep models differ from pure optimization algorithms in several ways. Machine learning optimization is different from pure optimization in several ways. In most machine learning scenarios, we care about some performance metric P , that is defined with respect to the test set and may also be different from the cost function J . We therefore optimize J only indirectly. We reduce a different cost function J with the hope that doing so will improve P . This is in contrast to pure optimization where minimizing J is a goal in and of itself. Optimization algorithms for deep models also typically include some specialization on the type of machine learning objective functions.

Typically, the cost function can be written as an average over the data, such as

$$J(\boldsymbol{\theta}) = \mathbb{E}_{(\mathbf{x}, y) \sim \hat{p}_{\text{data}}} L(f(\mathbf{x}; \boldsymbol{\theta}), y),$$

where L is the per-example loss function, $f(\mathbf{x}; \boldsymbol{\theta})$ is the predicted output for the input \mathbf{x} , \hat{p}_{data} is the empirical distribution. In the supervised case, y is the target output. Throughout this chapter, we develop the supervised case, where the arguments to L are $f(\mathbf{x}; \boldsymbol{\theta})$ and y . To extend this development, for example, to include $\boldsymbol{\theta}$ or to exclude y as arguments, in order to develop various forms of unsupervised learning.

Equation 8.1 defines an objective function with respect to

solvable by an optimization algorithm. However, when we can only have a training set of samples, we have a machine learning problem.

The simplest way to convert a machine learning problem to an optimization problem is to minimize the expected loss on test data. This means replacing the true distribution $p(\mathbf{x}, y)$ with the empirical distribution defined by the training set. We now minimize the **empirical risk**

$$\mathbb{E}_{\mathbf{x}, y \sim \hat{p}_{\text{data}}(\mathbf{x}, y)} [L(f(\mathbf{x}; \boldsymbol{\theta}), y)] = \frac{1}{m} \sum_{i=1}^m L(f(\mathbf{x}^{(i)}; \boldsymbol{\theta}), y^{(i)})$$

where m is the number of training examples.

The training process based on minimizing this average loss is called **empirical risk minimization**. In this setting, machine learning is similar to straightforward optimization. Rather than optimizing the true risk, we optimize the empirical risk, and hope that the risk decreases well. A variety of theoretical results establish conditions under which the risk can be expected to decrease by various amounts.

However, empirical risk minimization is prone to overfitting. High capacity can simply memorize the training set. In this case, risk minimization is not really feasible. The most effective algorithms are based on gradient descent, but many useful loss functions, such as 0-1 loss, have no useful derivatives (the derivative is either 0 or 1 everywhere). These two problems mean that, in the context of machine learning, we rarely use empirical risk minimization. Instead, we must use a surrogate approach, in which the quantity that we actually optimize is a surrogate for the quantity that we truly want to optimize.

In some cases, a surrogate loss function actually results more. For example, the test set 0-1 loss often continues to decrease over time after the training set 0-1 loss has reached zero, while the log-likelihood surrogate continues to decrease. This is because even when the expected 0-1 loss is zero, one can improve the robustness of the classifier by further pulling the weights apart from each other, obtaining a more confident and reliable classifier. The log-likelihood surrogate uses more information from the training data than would have been possible by simply minimizing the average 0-1 loss on the training set.

A very important difference between optimization in general and as we use it for training algorithms is that training algorithms often halt at a local minimum. Instead, a machine learning algorithm often uses a surrogate loss function but halts when a convergence criterion (section 7.8) is satisfied. Typically the early stop criterion is based on the true underlying loss function, such as 0-1 loss measurement, but the algorithm is designed to cause the algorithm to halt whenever overfitting is detected. Training often halts while the surrogate loss function still decreases, which is very different from the pure optimization setting, where the algorithm is considered to have converged when the gradient is zero.

8.1.3 Batch and Minibatch Algorithms

One aspect of machine learning algorithms that separates them from standard optimization algorithms is that the objective function is usually estimated over the training examples. Optimization algorithms for machine learning often compute each update to the parameters based on an expected gradient of the function estimated using only a subset of the terms of the function.

For example, maximum likelihood estimation problem

most commonly used property is the gradient:

$$\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}) = \mathbb{E}_{\mathbf{x}, y \sim \hat{p}_{\text{data}}} \nabla_{\boldsymbol{\theta}} \log p_{\text{model}}(\mathbf{x}, y;$$

Computing this expectation exactly is very expensive, requiring evaluating the model on every example in the entire dataset. We can estimate these expectations by randomly sampling a small number of examples from the dataset, then taking the average over only those examples.

Recall that the standard error of the mean (equation 5.1) for n samples is given by σ / \sqrt{n} , where σ is the true standard deviation of the samples. The denominator of \sqrt{n} shows that there are diminishing returns to using more examples to estimate the gradient. Comparing two estimates of the gradient, one based on 100 examples and another based on 10,000 examples. The latter requires 100 times more computation but only reduces the standard error of the mean only by a factor of 10. Stochastic algorithms converge much faster (in terms of total computation or number of updates) if they are allowed to rapidly compute noisy estimates of the gradient rather than slowly computing the exact gradient.

Another consideration motivating statistical estimation is that with a small number of samples is redundancy in the training set. If a small number of samples in the training set could be identical copies of each other, a naive estimate of the gradient could compute the correct gradient by using a single sample, using m times less computation than the naive approach. While it is unlikely to truly encounter this worst-case situation, in practice, many numbers of examples that all make very similar contributions to the gradient.

Optimization algorithms that use the entire training set to compute the gradient are called **deterministic** gradient methods, because they process all of the data simultaneously in a large batch. This terminology can be

than one but less than all of the training examples. These are called **minibatch** or **minibatch stochastic** methods and it is also common to call them **stochastic** methods.

The canonical example of a stochastic method is stochastic gradient descent, presented in detail in section 8.3.1.

Minibatch sizes are generally driven by the following factors:

- Larger batches provide a more accurate estimate of the gradient, which leads to less than linear returns.
- Multicore architectures are usually underutilized by extremely small batch sizes. This motivates using some absolute minimum batch size. If the batch size is too small, there is no reduction in the time to process a minibatch.
- If all examples in the batch are to be processed in parallel (e.g., on a GPU), then the amount of memory scales with the batch size. On many hardware setups this is the limiting factor in batch size.
- Some kinds of hardware achieve better runtime with smaller batch sizes. Especially when using GPUs, it is common for power of 2 batch sizes to achieve better runtime. Typical power of 2 batch sizes range from 16 to 1024, and sometimes being attempted for large models.
- Small batches can offer a regularizing effect (Wilson et al., 2016), perhaps due to the noise they add to the learning process. In some cases, the error is often best for a batch size of 1. Training with a small batch size might require a small learning rate to maintain stable training due to the variance in the estimate of the gradient. The total runtime is often higher due to the need to make more steps, both because of the small learning rate and the need to make more steps.

\mathbf{H} or its inverse amplifies pre-existing errors, in this case, Very small changes in the estimate of \mathbf{g} can thus cause large $\mathbf{H}^{-1}\mathbf{g}$, even if \mathbf{H} were estimated perfectly. Of course, \mathbf{H} approximately, so the update $\mathbf{H}^{-1}\mathbf{g}$ will contain even more predict from applying a poorly conditioned operation to the

It is also crucial that the minibatches be selected random unbiased estimate of the expected gradient from a set of samples be independent. We also wish for two subsequent gradients independent from each other, so two subsequent minibatches also be independent from each other. Many datasets are mixed in a way where successive examples are highly correlated. I have a dataset of medical data with a long list of blood samples. The list might be arranged so that first we have five blood samples from the first patient, then we have three blood samples from the second patient, then the blood samples from the third patient. If we were to draw examples in order from this list, then each of our minibatches would be extremely biased, because it would represent primarily one patient in many patients in the dataset. In cases such as these where correlation holds some significance, it is necessary to shuffle the examples in the minibatches. For very large datasets, for example datasets that live on examples in a data center, it can be impractical to sample examples at random every time we want to construct a minibatch. For these datasets it is usually sufficient to shuffle the order of the dataset once in a shuffled fashion. This will impose a fixed set of possible minibatches that all models trained thereafter will use, and the models will be forced to reuse this ordering every time it passes through the data. However, this deviation from true random selection does not affect the

the model's ability to learn the underlying pattern in the data.

descent shuffle the dataset once and then pass through it a second time. On the first pass, each minibatch is used to compute an unbiased estimate of the generalization error. On the second pass, the estimate becomes unbiased by re-sampling values that have already been used, as if they were new fair samples from the data generating distribution.

The fact that stochastic gradient descent minimizes the generalization error is easiest to see in the online learning case, where examples are drawn from a **stream** of data. In other words, instead of receiving a fixed dataset, the learner is similar to a living being who sees a new example with every example (\mathbf{x}, y) coming from the data generating distribution. In this scenario, examples are never repeated; every example is drawn from p_{data} .

The equivalence is easiest to derive when both \mathbf{x} and y are continuous. In this case, the generalization error (equation 8.2) can be written

$$J^*(\boldsymbol{\theta}) = \sum_{\mathbf{x}} \sum_y p_{\text{data}}(\mathbf{x}, y) L(f(\mathbf{x}; \boldsymbol{\theta}), y)$$

with the exact gradient

$$\mathbf{g} = \nabla_{\boldsymbol{\theta}} J^*(\boldsymbol{\theta}) = \sum_{\mathbf{x}} \sum_y p_{\text{data}}(\mathbf{x}, y) \nabla_{\boldsymbol{\theta}} L(f(\mathbf{x}; \boldsymbol{\theta}), y)$$

We have already seen the same fact demonstrated for the case of discrete data in equation 8.5 and equation 8.6; we observe now that this holds for continuous data besides the likelihood. A similar result can be derived when the loss is not the squared error, under mild assumptions regarding p_{data} and L .

Hence, we can obtain an unbiased estimator of the

of course, the additional epochs usually provide enough training error to offset the harm they cause by increasing the error and test error.

With some datasets growing rapidly in size, faster training is becoming more common for machine learning applications. For example, one might only have to make an incomplete pass over the training set. When using an extremely large training set, overfitting, underfitting and computational efficiency become the primary concerns. See also [Bottou and Bousquet \(2008\)](#) for a discussion of the bottlenecks on generalization error, as the number of training examples grows.

8.2 Challenges in Neural Network Optimization

Optimization in general is an extremely difficult task. In machine learning, the difficulty of general optimization is compounded by the fact that the objective function and constraints to ensure that the optimization is convex. When training neural networks, we must confront this difficulty. Even convex optimization is not without its complications. In this section, we summarize several of the most prominent challenges in optimization for training deep models.

8.2.1 Ill-Conditioning

Some challenges arise even when optimizing convex functions. One prominent problem is ill-conditioning of the Hessian matrix \mathbf{H} . This is a common problem in most numerical optimization, convex or otherwise.

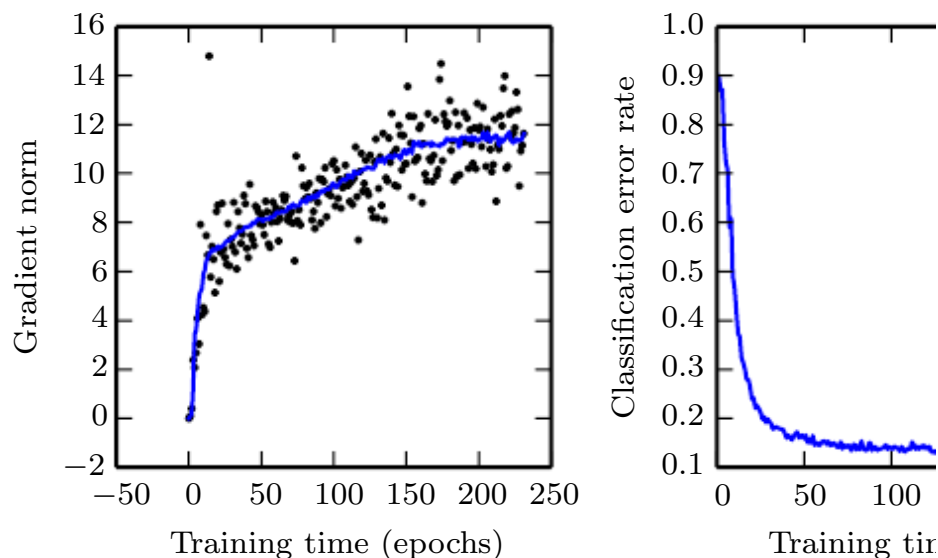


Figure 8.1: Gradient descent often does not arrive at a critical point, the gradient norm increases throughout training of a convolutional neural network for object detection. *(Left)* A scatterplot showing how the gradient norm evaluations are distributed over time. To improve legibility, only one evaluation is plotted per epoch. The running average of all gradient norm evaluations is plotted as a blue curve. The gradient norm clearly increases over time, rather than staying constant as expected if the training process converged to a critical point. *(Right)* In this example, gradient descent, the training process is reasonably successful. The validation error decreases to a low level.

the $\mathbf{g}^\top \mathbf{H} \mathbf{g}$ term. In many cases, the gradient norm does not decrease throughout learning, but the $\mathbf{g}^\top \mathbf{H} \mathbf{g}$ term grows by more than a factor of 10. The result is that learning becomes very slow despite the large gradient because the learning rate must be shrunk to compensate for the curvature. Figure 8.1 shows an example of the gradient norm during the successful training of a neural network.

guaranteed to be a global minimum. Some convex functions have a flat region at the bottom rather than a single global minimum point, but a flat region is an acceptable solution. When optimizing, we don't know that we have reached a good solution if we find a critical point.

With non-convex functions, such as neural nets, it is not guaranteed to find a local minimum. Indeed, nearly any deep model is essential an extremely large number of local minima. However, as we will see, this is not necessarily a major problem.

Neural networks and any models with multiple equivalent local minima all have multiple local minima because of the non-convex problem. A model is said to be identifiable if a sufficiently large number of local minima rule out all but one setting of the model's parameters. Models are often not identifiable because we can obtain equivalent local minima by permuting latent variables with each other. For example, we could take a model and modify layer 1 by swapping the incoming weight vector for unit i with the weight vector for unit j , then doing the same for the outgoing weights. If a model has m layers with n units each, then there are $n!^m$ ways to permute the units. This kind of non-identifiability is known as **weight space symmetry**.

In addition to weight space symmetry, many kinds of models have other additional causes of non-identifiability. For example, in a maxout network, we can scale all of the incoming weights by α if we also scale all of its outgoing weights by $\frac{1}{\alpha}$. This model's loss function does not include terms such as weight decay that depend on the weights rather than the models' outputs—every local minimum in a maxout network lies on an $(m \times n)$ -dimensional hyperplane of local minima.

These model identifiability issues mean that there can be many different settings of the model's parameters that all result in the same loss function.

for networks of practical interest and whether optimization them. For many years, most practitioners believed that common problem plaguing neural network optimization. appear to be the case. The problem remains an active area c now suspect that, for sufficiently large neural networks, mo low cost function value, and that it is not important to find rather than to find a point in parameter space that has low (Saxe *et al.*, 2013; Dauphin *et al.*, 2014; Goodfellow *et al* *et al.*, 2014).

Many practitioners attribute nearly all difficulty with ne tion to local minima. We encourage practitioners to car problems. A test that can rule out local minima as the j norm of the gradient over time. If the norm of the gradi insignificant size, the problem is neither local minima nor ar point. This kind of negative test can rule out local minima spaces, it can be very difficult to positively establish that problem. Many structures other than local minima also ha

8.2.3 Plateaus, Saddle Points and Other Flat

For many high-dimensional non-convex functions, local r are in fact rare compared to another kind of point with z point. Some points around a saddle point have greater cost while others have a lower cost. At a saddle point, the He positive and negative eigenvalues. Points lying along eigen positive eigenvalues have greater cost than the saddle poi along negative eigenvalues have lower value. We can thin

be heads. See [Dauphin et al. \(2014\)](#) for a review of the related literature.

An amazing property of many random functions is that the Hessian become more likely to be positive as we reach regions of low cost. In our coin tossing analogy, this means we are more likely to get heads n times if we are at a critical point with low cost. Local minima are much more likely to have low cost than high cost. High cost are far more likely to be saddle points. Critical points with high cost are more likely to be local maxima.

This happens for many classes of random functions. Do neural networks have global minima? [Baldi and Hornik \(1989\)](#) showed theoretically that shallow (feedforward networks trained to copy their input to their output) with no nonlinearities have global minima and local minima with higher cost than the global minimum. The proof that these results extend to deeper networks without nonlinearities is that the output of such networks is a linear function of their input. We study such networks as a model of nonlinear neural networks because they are a non-convex function of their parameters. Such networks are composed of multiple matrices composed together. [Saxe et al. \(2013\)](#) provide a proof to the complete learning dynamics in such networks and show that these models captures many of the qualitative features observed in deep models with nonlinear activation functions. [Dauphin et al. \(2014\)](#) experimentally that real neural networks also have loss functions with many high-cost saddle points. [Choromanska et al. \(2014\)](#) provide theoretical arguments, showing that another class of high-cost saddle points in functions related to neural networks does so as well.

What are the implications of the proliferation of saddle points for optimization algorithms? For first-order optimization algorithms that use only

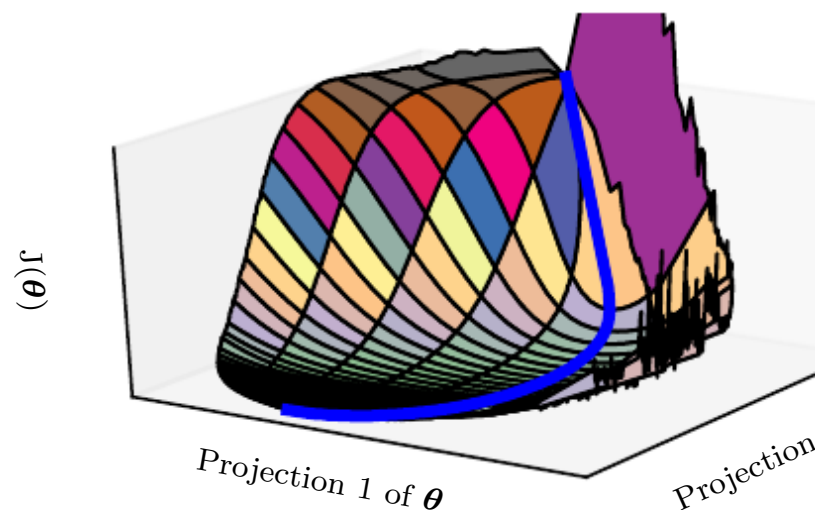


Figure 8.2: A visualization of the cost function of a neural network with permission from [Goodfellow *et al.* \(2015\)](#). These visualizations for feedforward neural networks, convolutional networks, and recurrent neural networks used for real object recognition and natural language processing tasks usually do not show many conspicuous obstacles. When using stochastic gradient descent for training very large models, the neural net cost function surfaces were generally believed to have a smoother structure than is revealed by these projections. The primary cost projection is a saddle point of high cost near where the parameters

Gradient descent is designed to move “downhill” and is not designed to seek a critical point. Newton’s method, however, is designed to seek a point where the gradient is zero. Without appropriate modifications, it can converge to a saddle point. The proliferation of saddle points in high-dimensional spaces presumably explains why second-order methods have not been widely adopted for neural network training. [Dauphin et al. \(2014\)](#) proposed a **saddle-free Newton method** for second-order optimization that improves significantly over the traditional version. Second-order methods are difficult to scale to large neural networks, but this saddle-free method holds promise if it could be scaled.

There are other kinds of points with zero gradient besides saddle points. There are also maxima, which are much like saddle points from the perspective of optimization—many algorithms are not designed to find them. An unmodified Newton’s method is designed to find minima. Maxima of many classes of functions become exponentially rare in high dimensional space, just as saddle points do.

There may also be wide, flat regions of constant value. In these regions, the gradient and also the Hessian are all zero. Such degenerate regions are a problem for all numerical optimization algorithms. In a convex problem, a flat region must consist entirely of global minima, but in a non-convex problem, such a region could correspond to a high value of the loss function.

8.2.4 Cliffs and Exploding Gradients

Neural networks with many layers often have extremely steep gradients, as illustrated in figure 8.3. These result from the many layers of large weights together. On the face of an extremely steep gradient, a gradient update step can move the parameters extremely far in a single step, leading to instability.

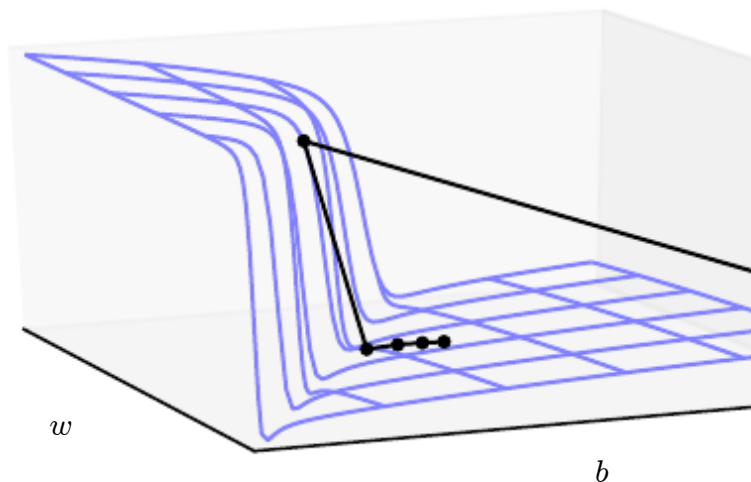


Figure 8.3: The objective function for highly nonlinear deep recurrent neural networks often contains sharp nonlinearities in part from the multiplication of several parameters. These nonlinearities can lead to high derivatives in some places. When the parameters get close to the cliff, a gradient descent update can catapult the parameters very far, potentially undoing optimization work that had been done. Figure adapted with permission from [Goodfellow et al. \(2013\)](#).

The cliff can be dangerous whether we approach it from the left or the right, but fortunately its most serious consequences can be avoided using the **clipping** heuristic described in section 10.11.1. The basic idea is that the gradient does not specify the optimal step size, but only the direction of the step within an infinitesimal region. When the traditional gradient descent proposes to make a very large step, the gradient clipping heuristic reduces the step size to be small enough that it is less likely to overshoot the cliff where the gradient indicates the direction of approximately

by repeatedly applying the same operation at each time step in a sequence. Repeated application of the same parameters is often a source of pronounced difficulties.

For example, suppose that a computational graph contains a sequence of repeatedly multiplying by a matrix \mathbf{W} . After t steps, this is equivalent to multiplying by \mathbf{W}^t . Suppose that \mathbf{W} has an eigendecomposition $\mathbf{W} = \mathbf{V} \text{diag}(\boldsymbol{\lambda}) \mathbf{V}^{-1}$. In this simple case, it is straightforward to see that

$$\mathbf{W}^t = (\mathbf{V} \text{diag}(\boldsymbol{\lambda}) \mathbf{V}^{-1})^t = \mathbf{V} \text{diag}(\boldsymbol{\lambda})^t \mathbf{V}^{-1}$$

Any eigenvalues λ_i that are not near an absolute value of 1 will either grow or shrink. If they are greater than 1 in magnitude, they will grow, and if they are less than 1, they will shrink. This **vanishing and exploding gradient problem** refers to the fact that gradients that flow through such a graph are also scaled according to $\text{diag}(\boldsymbol{\lambda})^t$. This makes it difficult to know which direction the parameters should be updated in to decrease the cost function, while exploding gradients can make learning unstable. These are the structures described earlier that motivate gradient clipping to mitigate the exploding gradient phenomenon.

The repeated multiplication by \mathbf{W} at each time step is similar to the **power method** algorithm used to find the dominant eigenvalue of a matrix \mathbf{W} and the corresponding eigenvector. From this, it is not surprising that $\mathbf{x}^\top \mathbf{W}^t$ will eventually discard all components orthogonal to the principal eigenvector of \mathbf{W} .

Recurrent networks use the same matrix \mathbf{W} at each time step, while feedforward networks do not, so even very deep feedforward networks can suffer from the vanishing and exploding gradient problem (Sussillo, 2014).

We defer a further discussion of the challenges of training recurrent networks to Chapter 9.

... .. 107

with the more advanced models in part III. For example, [Goodfellow et al. \(2015\)](#) gives a technique for approximating the gradient of the log-likelihood of a Boltzmann machine.

Various neural network optimization algorithms are designed to address imperfections in the gradient estimate. One can also avoid the problem by using a surrogate loss function that is easier to approximate than the true loss.

8.2.7 Poor Correspondence between Local and Global Minima

Many of the problems we have discussed so far correspond to the loss function at a single point—it can be difficult to make progress if the loss is poorly conditioned at the current point θ , or if θ lies on a plateau, or if the current point is hiding the opportunity to make progress downhill from a better point.

It is possible to overcome all of these problems at a single point, but the algorithm may perform poorly if the direction that results in the most improvement is not toward distant regions of much lower cost.

[Goodfellow et al. \(2015\)](#) argue that much of the runtime of training is spent on the length of the trajectory needed to arrive at the solution. In many cases, the learning trajectory spends most of its time tracing out a path on a mountain-shaped structure.

Much of research into the difficulties of optimization in deep learning training arrives at a global minimum, a local minimum, or a saddle point. In practice neural networks do not arrive at a critical point and instead continue to improve. It shows that neural networks often do not arrive at a region of low loss. In fact, such critical points do not even necessarily exist. For example, the cross-entropy loss $-\log p(y \mid \mathbf{x}; \theta)$ can lack a global minimum point and instead approach some value as the model becomes more confident.

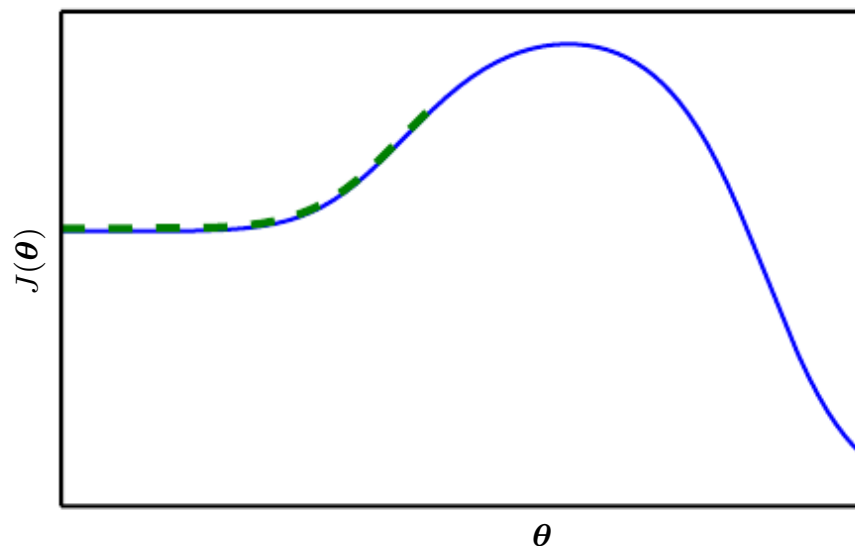


Figure 8.4: Optimization based on local downhill moves can fail not point toward the global solution. Here we provide an example even if there are no saddle points and no local minima. This contains only asymptotes toward low values, not minima. The trajectory in this case is being initialized on the wrong side of the “mountain” and must traverse it. In higher dimensional space, learning algorithms can encounter such mountains but the trajectory associated with doing so may require excessive training time, as illustrated in figure 8.2.

of the process.

Many existing research directions are aimed at finding problems that have difficult global structure, rather than those that use non-local moves.

Gradient descent and essentially all learning algorithms for training neural networks are based on making small, local

high computational cost. Sometimes local information proves the function has a wide flat region, or if we manage to land on a point (usually this latter scenario only happens to methods for critical points, such as Newton's method). In these cases, we cannot define a path to a solution at all. In other cases, local minima can lead us along a path that moves downhill but away from the minimum (figure 8.4), or along an unnecessarily long trajectory to the solution. Currently, we do not understand which of these problems are making neural network optimization difficult, and this is an

Regardless of which of these problems are most significant, they can be avoided if there exists a region of space connected reasonably well by a path that local descent can follow, and if we are able to start within that well-behaved region. This last view suggests that finding good initial points for traditional optimization algorithms is

8.2.8 Theoretical Limits of Optimization

Several theoretical results show that there are limits on the performance of any optimization algorithm we might design for neural networks (Brent, 1992; Judd, 1989; Wolpert and MacReady, 1997). Typically, these results have little bearing on the use of neural networks in practice.

Some theoretical results apply only to the case where the network output is discrete values. However, most neural networks output smoothly increasing values that make optimization via local methods difficult. Theoretical results show that there exist problem classes for which it can be difficult to tell whether a particular problem falls into the easy or hard category. Results show that finding a solution for a network of a given

8.3 Basic Algorithms

We have previously introduced the gradient descent (section 5.9) which follows the gradient of an entire training set downhill. This can be improved considerably by using stochastic gradient descent to follow the gradient by taking the average gradient over a set of selected minibatches downhill, as discussed in section 5.9 and 8.3.1.

8.3.1 Stochastic Gradient Descent

Stochastic gradient descent (SGD) and its variants are popular optimization algorithms for machine learning in general and in particular. As discussed in section 8.1.3, it is possible to estimate the gradient by taking the average gradient over a set of examples drawn i.i.d from the data generating distribution.

Algorithm 8.1 shows how to follow this estimate of the gradient.

Algorithm 8.1 Stochastic gradient descent (SGD) update

Require: Learning rate ϵ_k .

Require: Initial parameter θ

while stopping criterion not met **do**

 Sample a minibatch of m examples from the training set and their corresponding targets $\mathbf{y}^{(i)}$.

 Compute gradient estimate: $\hat{\mathbf{g}} \leftarrow +\frac{1}{m} \nabla_{\theta} \sum_i L(f(\mathbf{x}^{(i)}); \mathbf{y}^{(i)})$

 Apply update: $\theta \leftarrow \theta - \epsilon \hat{\mathbf{g}}$

end while

A crucial parameter for the SGD algorithm is the learning rate ϵ .

$$\sum_{k=1}^{\infty} \epsilon_k^2 < \infty.$$

In practice, it is common to decay the learning rate linearly:

$$\epsilon_k = (1 - \alpha) \epsilon_0 + \alpha \epsilon_\tau$$

with $\alpha = \frac{k}{\tau}$. After iteration τ , it is common to leave ϵ constant.

The learning rate may be chosen by trial and error, or to choose it by monitoring learning curves that plot the cost function of time. This is more of an art than a science, and the subject should be regarded with some skepticism. When choosing the parameters to choose are ϵ_0 , ϵ_τ , and τ . Usually τ may be the number of iterations required to make a few hundred passes through the training data. ϵ_τ should be set to roughly 1% the value of ϵ_0 . The main question is how to choose ϵ_0 . If it is too large, the learning curve will show violent oscillations, and the cost function often increases significantly. Gentle oscillations are usually a sign of training with a stochastic cost function such as the cost function with dropout. If the learning rate is too low, learning progress will be slow. If the initial learning rate is too low, learning may become stuck. Typically, the optimal initial learning rate, in terms of total final cost value, is higher than the learning rate that yields the lowest cost after the first 100 iterations or so. Therefore, it is usually better to start with several iterations and use a learning rate that is higher than the current learning rate at this time, but not so high that it causes severe oscillations.

The most important property of SGD and related minibatch-based optimization is that computation time per update does not depend on the size of the training set. This allows for training on large datasets with a single machine.

and Bousquet (2008) argue that it therefore may not be an optimization algorithm that converges faster than $O(\frac{1}{k})$ tasks—faster convergence presumably corresponds to overfitting. Asymptotic analysis obscures many advantages that stochastic gradient descent has after a small number of steps. With large datasets, the rapid initial progress while evaluating the gradient for one batch often outweighs its slow asymptotic convergence. Most of the algorithms in the remainder of this chapter achieve benefits that matter in the constant factors obscured by the $O(\frac{1}{k})$ asymptotic analysis. We trade off the benefits of both batch and stochastic gradient descent by increasing the minibatch size during the course of learning.

For more information on SGD, see Bottou (1998).

8.3.2 Momentum

While stochastic gradient descent remains a very popular method for training deep learning with it can sometimes be slow. The method of momentum is designed to accelerate learning, especially in the face of high variance or inconsistent gradients, or noisy gradients. The momentum algorithm maintains an exponentially decaying moving average of past gradients and uses it to update the parameters in their direction. The effect of momentum is illustrated in Figure 8.3.

Formally, the momentum algorithm introduces a variable called *velocity*—it is the direction and speed at which the parameters move in parameter space. The velocity is set to an exponentially decaying moving average of negative gradients. The name **momentum** derives from physics, where the negative gradient is a force moving a particle through parameter space according to Newton’s laws of motion. Momentum in physics is the product of mass and velocity, and it is conserved in a closed system. In the momentum algorithm, the velocity is updated as follows:

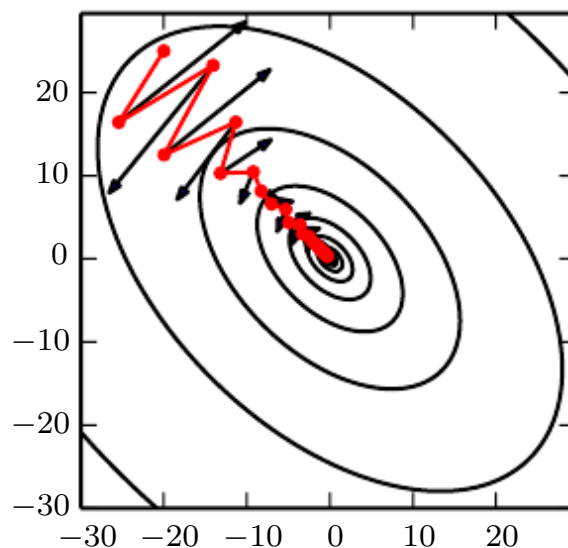


Figure 8.5: Momentum aims primarily to solve two problems: \bullet the ill-conditioned Hessian matrix and variance in the stochastic gradient. Here, we illustrate how momentum overcomes the first of these two problems. The contour lines represent the level sets of the function with a poorly conditioned Hessian matrix. The red line indicates the path followed by the momentum learning function. At each step along the way, we draw an arrow indicating the direction of descent would take at that point. We can see that a poorly conditioned Hessian looks like a long, narrow valley or canyon with steep sides. Momentum helps in navigating this valley by smoothing out the oscillations.

Previously, the size of the step was simply the norm of \mathbf{g} scaled by the learning rate. Now, the size of the step depends on how aligned a *sequence* of gradients are. The step size is largest when all gradients point in exactly the same direction. If the momentum algorithm observes gradient \mathbf{g} , then it will accelerate in the direction of \mathbf{g} until it reaches a terminal velocity where the size of each step is

$$\frac{\epsilon \|\mathbf{g}\|}{1 - \alpha}.$$

It is thus helpful to think of the momentum hyperparameter α . For example, $\alpha = .9$ corresponds to multiplying the maximum step size of the gradient descent algorithm.

Common values of α used in practice include .5, .9, and .99. In some cases, α may also be adapted over time. Typically it begins at a low value and is later raised. It is less important to adapt α over time than

Algorithm 8.2 Stochastic gradient descent (SGD) with momentum

Require: Learning rate ϵ , momentum parameter α .

Require: Initial parameter $\boldsymbol{\theta}$, initial velocity \mathbf{v} .

while stopping criterion not met **do**

 Sample a minibatch of m examples from the training set and their corresponding targets $\mathbf{y}^{(i)}$.

 Compute gradient estimate: $\mathbf{g} \leftarrow \frac{1}{m} \nabla_{\boldsymbol{\theta}} \sum_i L(f(\mathbf{x}^{(i)}; \boldsymbol{\theta}); \mathbf{y}^{(i)})$

 Compute velocity update: $\mathbf{v} \leftarrow \alpha \mathbf{v} - \epsilon \mathbf{g}$

 Apply update: $\boldsymbol{\theta} \leftarrow \boldsymbol{\theta} + \mathbf{v}$

end while

We can view the momentum algorithm as simulating

$$\mathbf{f}(t) = \frac{\partial}{\partial t} \mathbf{v}(t).$$

The momentum algorithm then consists of solving the differential equation numerically. A simple numerical method for solving differential equations is Euler's method, which simply consists of simulating the differential equation by taking small, finite steps in the direction of the derivative.

This explains the basic form of the momentum update, but what about the forces? One force is proportional to the negative gradient of the cost function, $-\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta})$. This force pushes the particle downhill along the direction of the negative gradient. The gradient descent algorithm would simply take a single step in this direction, but the Newtonian scenario used by the momentum algorithm uses this force to alter the velocity of the particle. We can think of this as being like a hockey puck sliding down an icy surface. When it reaches a steep part of the surface, it gathers speed and continues sliding until it begins to go uphill again.

One other force is necessary. If the only force is the gradient, then the particle might never come to rest. Imagine a hockey puck sliding down one side of a valley and straight up the other side, oscillating forever. To resolve this, we add a second force, proportional to $-\mathbf{v}(t)$. In physics terminology, this is called viscous drag, as if the particle must push through a resistive medium like syrup. This causes the particle to gradually lose energy over time and converge to a local minimum.

Why do we use $-\mathbf{v}(t)$ and viscous drag in particular? The reason we use $-\mathbf{v}(t)$ is mathematical convenience—an integer power of the velocity is easy to work with. However, other physical systems have other forces proportional to other integer powers of the velocity. For example, a par-

that the gradient can continue to cause motion until a minimum is reached. If the gradient is not strong enough to prevent motion if the gradient does not j

8.3.3 Nesterov Momentum

Sutskever *et al.* (2013) introduced a variant of the momentum method inspired by Nesterov's accelerated gradient method (Nesterov 1983). The update rules in this case are given by:

$$\begin{aligned} \mathbf{v} &\leftarrow \alpha \mathbf{v} - \epsilon \nabla_{\boldsymbol{\theta}} \left[\frac{1}{m} \sum_{i=1}^m L(\mathbf{f}(\mathbf{x}^{(i)}; \boldsymbol{\theta} + \alpha \mathbf{v}), y^{(i)}) \right] \\ \boldsymbol{\theta} &\leftarrow \boldsymbol{\theta} + \mathbf{v}, \end{aligned}$$

where the parameters α and ϵ play a similar role as in the standard gradient descent method. The difference between Nesterov momentum and standard momentum is that the gradient is evaluated at $\boldsymbol{\theta} + \alpha \mathbf{v}$ instead of $\boldsymbol{\theta}$. This is equivalent to evaluating the gradient after the current velocity is applied. Thus one can interpret Nesterov momentum as attempting to add a *correction factor* to the standard momentum method. The complete Nesterov momentum algorithm is presented in Algorithm 8.3.

In the convex batch gradient case, Nesterov momentum improves the convergence of the excess error from $O(1/k)$ (after k steps) to $O(1/k^2)$ by Nesterov (1983). Unfortunately, in the stochastic gradient case, Nesterov momentum does not improve the rate of convergence.

Algorithm 8.3 Stochastic gradient descent (SGD) with Nesterov Momentum

Require: Learning rate ϵ , momentum parameter α .

Require: Initial parameter $\boldsymbol{\theta}$, initial velocity \mathbf{v} .

8.4 Parameter Initialization Strategies

Some optimization algorithms are not iterative by nature solution point. Other optimization algorithms are iterative applied to the right class of optimization problems, converge in an acceptable amount of time regardless of initialization. algorithms usually do not have either of these luxuries. Training learning models are usually iterative in nature and thus require some initial point from which to begin the iterations. Finding a good initial point for a model is a sufficiently difficult task that most algorithms make the choice of initialization. The initial point can determine whether the model converges at all, with some initial points being so unstable that the model encounters numerical difficulties and fails altogether. When the model does converge, the initial point can determine how quickly learning converges to a point with high or low cost. Also, the initial point can have wildly varying generalization error, and the initial point can determine the final generalization as well.

Modern initialization strategies are simple and heuristic. Choosing a good initialization strategy is a difficult task because neural networks are not yet well understood. Most initialization strategies are based on nice properties when the network is initialized. However, we have a poor understanding of which of these properties are preserved and which are lost after learning begins to proceed. A further difficulty is that a property that may be beneficial from the viewpoint of optimization but is detrimental from the viewpoint of generalization. Our understanding of how to choose a good initialization point for generalization is especially primitive, offering little to no guidance for choosing the initial point.

motivates random initialization of the parameters. We could choose for a large set of basis functions that are all mutually different, but this often incurs a noticeable computational cost. For as many outputs as inputs, we could use Gram-Schmidt on an initial weight matrix, and be guaranteed that each unit computes a different function from each other unit. Random initialization over a high-dimensional space is computationally cheaper than to assign any units to compute the same function as each other.

Typically, we set the biases for each unit to heuristically small values. We initialize only the weights randomly. Extra parameters, for encoding the conditional variance of a prediction, are usually not used, chosen constants much like the biases are.

We almost always initialize all the weights in the network randomly from a Gaussian or uniform distribution. The choice of Gaussian or uniform distribution does not seem to matter very much, but has been exhaustively studied. The scale of the initial distribution, however, has a large effect on both the outcome of the optimization procedure and the ability of the network to generalize.

Larger initial weights will yield a stronger symmetry breaking, helping to avoid redundant units. They also help to avoid losing signals during back-propagation through the linear component of each layer. Small initial weights result in larger outputs of matrix multiplication. If the initial weights are too large may, however, result in exploding values during forward and back-propagation. In recurrent networks, large weights can lead to vanishing or exploding gradients (such extreme sensitivity to small perturbations of the initial conditions). In the deterministic forward propagation procedure appears to be a problem to some extent, the exploding gradient problem can be mitigated.

due to triggering some early stopping criterion based on a prior that the final parameters should be close to the initial values. From section 7.8 that gradient descent with early stopping can be seen as a form of weight decay for some models. In the general case, gradient descent is not the same as weight decay, but does provide a loose analogy to the effect of initialization. We can think of initializing the parameters as being similar to imposing a Gaussian prior $p(\boldsymbol{\theta})$ with mean $\boldsymbol{\theta}_0$. From this point of view, it makes sense to choose $\boldsymbol{\theta}_0$ to be near 0. This prior expresses the belief that units do not interact with each other than that they interact only if the likelihood term of the objective function indicates a preference for them to interact. On the other hand, if we have good prior values, then our prior specifies which units should interact and how they should interact.

Some heuristics are available for choosing the initial scale. One common heuristic is to initialize the weights of a fully connected layer with m inputs and n outputs by sampling each weight from $U(-\frac{1}{\sqrt{m}}, \frac{1}{\sqrt{m}})$, which Glorot and Foutier (2010) suggest using the **normalized initialization**

$$W_{i,j} \sim U\left(-\sqrt{\frac{6}{m+n}}, \sqrt{\frac{6}{m+n}}\right).$$

This latter heuristic is designed to compromise between the desire for all layers to have the same activation variance and the desire for all layers to have the same gradient variance. The formula is based on the assumption that the network consists only of a chain of layers with no nonlinearities. Real neural networks obviously violate this assumption, but many strategies designed for the linear model perform reasonably well on their nonlinear counterparts.

1,000 layers, without needing to use orthogonal initialization. One of the advantages of this approach is that in feedforward networks, activations expand or shrink on each step of forward or back-propagation, following a similar behavior. This is because feedforward networks use a different weight matrix at each layer. If this random walk is tuned to preserve norm, feedforward networks can mostly avoid the vanishing and exploding gradient problem. This arises when the same weight matrix is used at each step, decreasing the norm of the signal.

Unfortunately, these optimal criteria for initial weight matrices are not always optimal for performance. This may be for three different reasons. First, it may be using the wrong criteria—it may not actually be beneficial to preserve the norm of a signal throughout the entire network. Second, the optimal initialization may not persist after learning has begun. Third, the optimal criteria might succeed at improving the speed of optimization but might also increase generalization error. In practice, we usually need to tune the initial weights as a hyperparameter whose optimal value lies somewhere between the theoretical predictions.

One drawback to scaling rules that set all of the initial weights to the same standard deviation, such as $\frac{1}{\sqrt{m}}$, is that every individual weight is extremely small when the layers become large. **Martens** proposed an alternative initialization scheme called **sparse initialization**, where each unit is initialized to have exactly k non-zero weights. The idea is to make the variance of input to the unit independent from the number of inputs. The magnitude of individual weight elements shrink with m . Sparse initialization to achieve more diversity among the units at initialization imposes a very strong prior on the weights that are chosen. It restricts the values. Because it takes a long time for gradient descent to discover the optimal values, this initialization scheme can cause problems for units that are not initialized properly.

increasing its weights, it is possible to eventually obtain a non-zero initial activations throughout. If learning is still too slow it is useful to look at the range or standard deviation of the gradients of the activations. This procedure can in principle be automated but is computationally costly than hyperparameter optimization. The error because it is based on feedback from the behavior of a single batch of data, rather than on feedback from a trained model set. While long used heuristically, this protocol has recently been formalized and studied by [Mishkin and Matas \(2015\)](#).

So far we have focused on the initialization of the weights. The initialization of other parameters is typically easier.

The approach for setting the biases must be coordinated with the settings for the weights. Setting the biases to zero is common in many initialization schemes. There are a few situations where we want non-zero values:

- If a bias is for an output unit, then it is often beneficial to obtain the right marginal statistics of the output. To do this, if the initial weights are small enough that the output of the unit is only by the bias. This justifies setting the bias to the value that the activation function applied to the marginal statistics of the output. For example, if the output is a distribution over classes and the marginal probability is a highly skewed distribution with the marginal probability concentrated on element c_i of some vector \mathbf{c} , then we can set the bias to the value that satisfies the equation $\text{softmax}(\mathbf{b}) = \mathbf{c}$. This applies not only to models we will encounter in Part III, such as autoencoders and generative machines. These models have layers whose output should match a target distribution.

can view h as a gate that determines whether $uh \approx$ situations, we want to set the bias for h so that $h \approx$ initialization. Otherwise u does not have a chance to. [Jozefowicz *et al.* \(2015\)](#) advocate setting the bias to 1 in the LSTM model, described in section [10.10](#).

Another common type of parameter is a variance or precision. For example, we can perform linear regression with a conditionally Gaussian using the model

$$p(y \mid \mathbf{x}) = \mathcal{N}(y \mid \mathbf{w}^T \mathbf{x} + b, 1/\beta)$$

where β is a precision parameter. We can usually initialize variance parameters to 1 safely. Another approach is to assume the initial bias is close enough to zero that the biases may be set while ignoring the variance. We then set the biases to produce the correct marginal mean and set the variance parameters to the marginal variance of the output.

Besides these simple constant or random methods of initialization, it is possible to initialize model parameters using machine learning. One strategy discussed in part [III](#) of this book is to initialize a subset of the parameters learned by an unsupervised model trained on the data. One can also perform supervised training on a related task and use the parameters learned. Supervised training on an unrelated task can sometimes yield better results. It offers faster convergence than a random initialization. Some initialization strategies may yield faster convergence and better generalization. They encode information about the distribution in the initial parameters. Others apparently perform well primarily because they set the right scale or set different units to compute different functions.

rate for each parameter, and automatically adapt these learning rates during the course of learning.

The **delta-bar-delta** algorithm (Jacobs, 1988) is an early method for adapting individual learning rates for model parameters. This approach is based on a simple idea: if the partial derivative of the loss with respect to a given model parameter, remains the same sign, then the learning rate should increase. If the partial derivative with respect to that parameter changes sign, then the learning rate should decrease. Of course, this kind of adaptation is only applied to full batch optimization.

More recently, a number of incremental (or mini-batch) algorithms have been introduced that adapt the learning rates of model parameters. We will briefly review a few of these algorithms.

8.5.1 AdaGrad

The **AdaGrad** algorithm, shown in algorithm 8.4, individually adapts the learning rates of all model parameters by scaling them inversely proportional to the square root of the sum of all of their historical squared values (Duchi et al., 2012). Parameters with the largest partial derivative of the loss function experience a rapid decrease in their learning rate, while parameters with small partial derivatives have a relatively small decrease in their learning rate. This results in rapid progress in the more gently sloped directions of parameter space.

In the context of convex optimization, the AdaGrad algorithm has several desirable theoretical properties. However, empirically it has been found to perform poorly when training deep neural network models—the accumulation of small gradients at the beginning of training can result in a premature and exponentially decreasing effective learning rate. AdaGrad performs well for some but

Algorithm 8.4 The AdaGrad algorithm

Require: Global learning rate ϵ **Require:** Initial parameter θ **Require:** Small constant δ , perhaps 10^{-7} , for numerical sInitialize gradient accumulation variable $\mathbf{r} = \mathbf{0}$ **while** stopping criterion not met **do**Sample a minibatch of m examples from the training set
corresponding targets $\mathbf{y}^{(i)}$.Compute gradient: $\mathbf{g} \leftarrow \frac{1}{m} \nabla_{\theta} \sum_i L(f(\mathbf{x}^{(i)}; \theta), \mathbf{y}^{(i)})$ Accumulate squared gradient: $\mathbf{r} \leftarrow \mathbf{r} + \mathbf{g} \odot \mathbf{g}$ Compute update: $\Delta\theta \leftarrow -\frac{\epsilon}{\delta + \sqrt{\mathbf{r}}} \odot \mathbf{g}$. (Division an
element-wise)Apply update: $\theta \leftarrow \theta + \Delta\theta$ **end while**

have made the learning rate too small before arriving at success. RMSProp uses an exponentially decaying average to discount the extreme past so that it can converge rapidly after finding a good direction. It was an instance of the AdaGrad algorithm initialized with

RMSProp is shown in its standard form in algorithm 8.5. Nesterov momentum in algorithm 8.6. Compared to Adam, the moving average introduces a new hyperparameter, ρ , that controls the decay of the moving average.

Empirically, RMSProp has been shown to be an effective optimization algorithm for deep neural networks. It is currently one of the optimization methods being employed routinely by deep learning practitioners.

Algorithm 8.5 The RMSProp algorithm

Require: Global learning rate ϵ , decay rate ρ .**Require:** Initial parameter θ **Require:** Small constant δ , usually 10^{-6} , used to stabilize numbers.Initialize accumulation variables $\mathbf{r} = 0$ **while** stopping criterion not met **do** Sample a minibatch of m examples from the training set and their corresponding targets $\mathbf{y}^{(i)}$. Compute gradient: $\mathbf{g} \leftarrow \frac{1}{m} \nabla_{\theta} \sum_i L(f(\mathbf{x}^{(i)}; \theta), \mathbf{y}^{(i)})$ Accumulate squared gradient: $\mathbf{r} \leftarrow \rho \mathbf{r} + (1 - \rho) \mathbf{g} \odot \mathbf{g}$ Compute parameter update: $\Delta \theta = -\frac{\epsilon}{\sqrt{\delta + \mathbf{r}}} \odot \mathbf{g}$. $(\frac{1}{\sqrt{\delta + \mathbf{r}}})$ Apply update: $\theta \leftarrow \theta + \Delta \theta$ **end while**

bias corrections to the estimates of both the first-order moment (the first-order term) and the (uncentered) second-order moments to account for the bias at the origin (see algorithm 8.7). RMSProp also incorporates a (uncentered) second-order moment, however it lacks the bias correction. Unlike in Adam, the RMSProp second-order moment estimate is initialized early in training. Adam is generally regarded as being fairly robust to choices of hyperparameters, though the learning rate sometimes needs to be set to the suggested default.

8.5.4 Choosing the Right Optimization Algorithm

In this section, we discussed a series of related algorithms that

Algorithm 8.6 RMSProp algorithm with Nesterov momentum

Require: Global learning rate ϵ , decay rate ρ , momentum

Require: Initial parameter $\boldsymbol{\theta}$, initial velocity \mathbf{v} .

Initialize accumulation variable $\mathbf{r} = \mathbf{0}$

while stopping criterion not met **do**

 Sample a minibatch of m examples from the training set
 corresponding targets $\mathbf{y}^{(i)}$.

 Compute interim update: $\tilde{\boldsymbol{\theta}} \leftarrow \boldsymbol{\theta} + \alpha \mathbf{v}$

 Compute gradient: $\mathbf{g} \leftarrow \frac{1}{m} \nabla_{\tilde{\boldsymbol{\theta}}} \sum_i L(f(\mathbf{x}^{(i)}; \tilde{\boldsymbol{\theta}}), \mathbf{y}^{(i)})$

 Accumulate gradient: $\mathbf{r} \leftarrow \rho \mathbf{r} + (1 - \rho) \mathbf{g} \odot \mathbf{g}$

 Compute velocity update: $\mathbf{v} \leftarrow \alpha \mathbf{v} - \frac{\epsilon}{\sqrt{\mathbf{r}}} \odot \mathbf{g}$. $(\frac{1}{\sqrt{\mathbf{r}}}$ a

 Apply update: $\boldsymbol{\theta} \leftarrow \boldsymbol{\theta} + \mathbf{v}$

end while

largely on the user’s familiarity with the algorithm (for e tuning).

8.6 Approximate Second-Order Methods

In this section we discuss the application of second-order methods to the training of deep networks. See [LeCun *et al.* \(1998a\)](#) for an earlier treatment. For simplicity of exposition, the only objective function we consider is the risk:

$$J(\boldsymbol{\theta}) = \mathbb{E}_{\mathbf{x}, y \sim \hat{p}_{\text{data}}(\mathbf{x}, y)} [L(f(\mathbf{x}; \boldsymbol{\theta}), y)] = \frac{1}{m} \sum_{i=1}^m L(f(\mathbf{x}^{(i)}; \boldsymbol{\theta}), y^{(i)})$$

Algorithm 8.7 The Adam algorithm

Require: Step size ϵ (Suggested default: 0.001)
Require: Exponential decay rates for moment estimate
(Suggested defaults: 0.9 and 0.999 respectively)
Require: Small constant δ used for numerical stabilization
(10^{-8})
Require: Initial parameters θ
Initialize 1st and 2nd moment variables $\mathbf{s} = \mathbf{0}$, $\mathbf{r} = \mathbf{0}$
Initialize time step $t = 0$
while stopping criterion not met **do**
 Sample a minibatch of m examples from the training set
 corresponding targets $\mathbf{y}^{(i)}$.
 Compute gradient: $\mathbf{g} \leftarrow \frac{1}{m} \nabla_{\theta} \sum_i L(f(\mathbf{x}^{(i)}; \theta), \mathbf{y}^{(i)})$
 $t \leftarrow t + 1$
 Update biased first moment estimate: $\mathbf{s} \leftarrow \rho_1 \mathbf{s} + (1 - \rho_1) \mathbf{g}$
 Update biased second moment estimate: $\mathbf{r} \leftarrow \rho_2 \mathbf{r} + (1 - \rho_2) \mathbf{g} \mathbf{g}^T$
 Correct bias in first moment: $\hat{\mathbf{s}} \leftarrow \frac{\mathbf{s}}{1 - \rho_1^t}$
 Correct bias in second moment: $\hat{\mathbf{r}} \leftarrow \frac{\mathbf{r}}{1 - \rho_2^t}$
 Compute update: $\Delta \theta = -\epsilon \frac{\hat{\mathbf{s}}}{\sqrt{\hat{\mathbf{r}} + \delta}}$ (operations applied
 elementwise)
 Apply update: $\theta \leftarrow \theta + \Delta \theta$
end while

Newton's method is an optimization scheme based on using
Taylor series expansion to approximate $J(\theta)$ near some point θ
of higher order:

Algorithm 8.8 Newton's method with ob
 $\frac{1}{m} \sum_{i=1}^m L(f(\mathbf{x}^{(i)}; \boldsymbol{\theta}), \mathbf{y}^{(i)})$.

Require: Initial parameter $\boldsymbol{\theta}_0$

Require: Training set of m examples

while stopping criterion not met **do**

 Compute gradient: $\mathbf{g} \leftarrow \frac{1}{m} \nabla_{\boldsymbol{\theta}} \sum_i L(f(\mathbf{x}^{(i)}; \boldsymbol{\theta}), \mathbf{y}^{(i)})$

 Compute Hessian: $\mathbf{H} \leftarrow \frac{1}{m} \nabla_{\boldsymbol{\theta}}^2 \sum_i L(f(\mathbf{x}^{(i)}; \boldsymbol{\theta}), \mathbf{y}^{(i)})$

 Compute Hessian inverse: \mathbf{H}^{-1}

 Compute update: $\Delta \boldsymbol{\theta} = -\mathbf{H}^{-1} \mathbf{g}$

 Apply update: $\boldsymbol{\theta} = \boldsymbol{\theta} + \Delta \boldsymbol{\theta}$

end while

For surfaces that are not quadratic, as long as the Hessian is positive definite, Newton's method can be applied iteratively. This is an iterative procedure. First, update or compute the inverse Hessian (using the quadratic approximation). Second, update the parameters using equation 8.27.

In section 8.2.3, we discussed how Newton's method is problematic if the Hessian is not positive definite. In deep learning, the surface of the loss function is typically non-convex with many features, such as saddle points, which are problematic for Newton's method. If the eigenvalues of the Hessian are all positive, for example, near a saddle point, then Newton's method can cause updates to move in the wrong direction. This situation can be avoided by regularizing the Hessian. Common regularization strategies include adding a constant, α , along the diagonal of the Hessian. The regularized update is

$$\boldsymbol{\theta}^* = \boldsymbol{\theta}_0 - [\mathbf{H}(f(\boldsymbol{\theta}_0)) + \alpha \mathbf{I}]^{-1} \nabla_{\boldsymbol{\theta}} f(\boldsymbol{\theta}_0)$$

such as saddle points, the application of Newton’s method for networks is limited by the significant computational burden. The number of elements in the Hessian is squared in the number of parameters (and for even very small neural networks the k can be in the millions), Newton’s method would require to invert a $k \times k$ matrix—with computational complexity of $O(k^3)$. Also, since the Hessian changes with every update, the inverse Hessian has to be recomputed at every *iteration*. As a consequence, only networks with a very small number of parameters can be practically trained via Newton’s method. In the remainder of this chapter we will discuss alternatives that attempt to gain some of the efficiency of Newton’s method while side-stepping the computational hurdles.

8.6.2 Conjugate Gradients

Conjugate gradients is a method to efficiently avoid the calculation of the Hessian by iteratively descending **conjugate directions**. This approach follows from a careful study of the weakness of steepest descent (see section 4.3 for details), where line searches are performed in the direction associated with the gradient. Figure 8.6 illustrates that steepest descent, when applied in a quadratic bowl, progresses in a back-and-forth, zig-zag pattern. This happens because each step, when given by the gradient, is guaranteed to be orthogonal to the previous search direction.

Let the previous search direction be \mathbf{d}_{t-1} . At the minimum the search terminates, the directional derivative is zero in direction \mathbf{d}_{t-1} , $\mathbf{d}_{t-1}^T \nabla_{\theta} J(\theta) = 0$. Since the gradient at this point defines the conjugate direction $\mathbf{d}_t = \nabla_{\theta} J(\theta)$ will have no contribution in the direction \mathbf{d}_{t-1} .

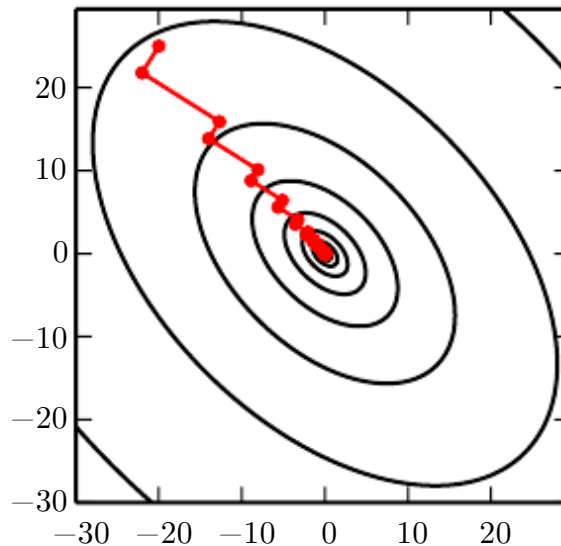


Figure 8.6: The method of steepest descent applied to a quadratic function. The method of steepest descent involves jumping to the point of local minimum defined by the gradient at the initial point on each step. This results in a zig-zag path, as seen with using a fixed learning rate in figure 4.6, but even without momentum, the algorithm still makes back-and-forth progress toward the optimum. If the minimum of the objective is along a given direction, the gradient is orthogonal to that direction.

the form:

$$\mathbf{d}_t = -\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}) + \beta_t \mathbf{d}_{t-1}$$

where β_t is a coefficient whose magnitude controls how much we should add back to the current search direction.

Two directions, \mathbf{d}_t and \mathbf{d}_{t-1} , are defined as conjugate if \mathbf{H} is the Hessian matrix.

The straightforward way to impose conjugacy would involve

2. Polak-Ribière:

$$\beta_t = \frac{(\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}_t) - \nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}_{t-1}))^\top \nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}_{t-1})}{\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}_{t-1})^\top \nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}_{t-1})}$$

For a quadratic surface, the conjugate directions ensure that the previous direction does not increase in magnitude. We find the minimum along the previous directions. As a consequence, in the parameter space, the conjugate gradient method requires at most n steps to achieve the minimum. The conjugate gradient algorithm is

Algorithm 8.9 The conjugate gradient method

Require: Initial parameters $\boldsymbol{\theta}_0$

Require: Training set of m examples

Initialize $\boldsymbol{\rho}_0 = \mathbf{0}$

Initialize $g_0 = 0$

Initialize $t = 1$

while stopping criterion not met **do**

Initialize the gradient $\mathbf{g}_t = \mathbf{0}$

Compute gradient: $\mathbf{g}_t \leftarrow \frac{1}{m} \nabla_{\boldsymbol{\theta}} \sum_i L(f(\mathbf{x}^{(i)}; \boldsymbol{\theta}), \mathbf{y}^{(i)})$

Compute $\beta_t = \frac{(\mathbf{g}_t - \mathbf{g}_{t-1})^\top \mathbf{g}_t}{\mathbf{g}_{t-1}^\top \mathbf{g}_{t-1}}$ (Polak-Ribière)

(Nonlinear conjugate gradient: optionally reset β_t to zero if it is not a multiple of some constant k , such as $k = 5$)

Compute search direction: $\boldsymbol{\rho}_t = -\mathbf{g}_t + \beta_t \boldsymbol{\rho}_{t-1}$

Perform line search to find: $\epsilon^* = \operatorname{argmin}_{\epsilon} \frac{1}{m} \sum_{i=1}^m L(f(\mathbf{x}^{(i)}; \boldsymbol{\theta}_t - \epsilon \boldsymbol{\rho}_t), \mathbf{y}^{(i)})$

(On a truly quadratic cost function, analytically solve for ϵ^* by explicitly searching for it)

Update parameters: $\boldsymbol{\theta}_t \leftarrow \boldsymbol{\theta}_{t-1} - \epsilon^* \boldsymbol{\rho}_{t-1}$

Increment $t \leftarrow t + 1$

end while

are no longer assured to remain at the minimum of the directions. As a result, the **nonlinear conjugate gradient** occasional resets where the method of conjugate gradients search along the unaltered gradient.

Practitioners report reasonable results in applications of the conjugate gradients algorithm to training neural networks, though it is common to initialize the optimization with a few iterations of stochastic gradient descent commencing nonlinear conjugate gradients. Also, while the conjugate gradients algorithm has traditionally been cast as a batch method, mini-batch versions have been used successfully for the training of neural networks (Bottou, 2011). Adaptations of conjugate gradients specifically for training neural networks have been proposed earlier, such as the scaled conjugate gradient algorithm (Morfitt, 1993).

8.6.3 BFGS

The **Broyden–Fletcher–Goldfarb–Shanno (BFGS)** algorithm brings some of the advantages of Newton’s method without the computational burden. In that respect, BFGS is similar to the conjugate gradient method. However, BFGS takes a more direct approach to the approximation of the Hessian update. Recall that Newton’s update is given by

$$\boldsymbol{\theta}^* = \boldsymbol{\theta}_0 - \mathbf{H}^{-1} \nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}_0),$$

where \mathbf{H} is the Hessian of J with respect to $\boldsymbol{\theta}$ evaluated at $\boldsymbol{\theta}_0$. The computational difficulty in applying Newton’s update is the computation of the inverse Hessian \mathbf{H}^{-1} . The approach adopted by quasi-Newton methods (the BFGS algorithm is the most prominent) is to approximate the Hessian by a rank-1 update to the previous approximation.

unlike conjugate gradients, the success of the approach is on the line search finding a point very close to the true minimum. Thus, relative to conjugate gradients, BFGS has the advantage of less time refining each line search. On the other hand, the algorithm must store the inverse Hessian matrix, \mathbf{M} , that requires $O(n^2)$ memory, which is impractical for most modern deep learning models that typically have millions of parameters.

Limited Memory BFGS (or L-BFGS) The memory requirement of the BFGS algorithm can be significantly decreased by avoiding storing the full Hessian approximation \mathbf{M} . The L-BFGS algorithm computes the search direction using the same method as the BFGS algorithm, but beginning with the assumption that $\mathbf{M}^{(t-1)}$ is the identity matrix, rather than storing the full Hessian approximation from step to the next. If used with exact line searches, the search directions are mutually conjugate. However, unlike the method of conjugate gradients, the procedure remains well behaved when the minimum of the function is not known only approximately. The L-BFGS strategy with no storage can be generalized to include more information about the Hessian by storing the vectors used to update \mathbf{M} at each time step, which costs $O(mn)$ memory, where m is the number of stored vectors.

8.7 Optimization Strategies and Meta-

Many optimization techniques are not exactly algorithmic templates that can be specialized to yield algorithms, or so much as they are incorporated into many different algorithms.

example, suppose we have a deep neural network that has l layers and does not use an activation function at each hidden layer. Here, w_i provides the weight used by layer i . The output of the network is \hat{y} . The output \hat{y} is a linear function of the input x , but a nonlinear function of the weights w_i . Suppose our cost function has put a gradient on \hat{y} to decrease \hat{y} slightly. The back-propagation algorithm can then compute the gradient $\mathbf{g} = \nabla_{\mathbf{w}} \hat{y}$. Consider what happens when we make an update to \mathbf{w} using a first-order Taylor series approximation of \hat{y} predicts that the new value of \hat{y} will be $\hat{y} + \epsilon \mathbf{g}^\top \mathbf{g}$. If we wanted to decrease \hat{y} by .1, this first-order approximation suggests we could set the learning rate ϵ to $\frac{-.1}{\mathbf{g}^\top \mathbf{g}}$. However, this update will include second-order and third-order effects, on which the first-order approximation is not accurate. The new value of \hat{y} is given by

$$x(w_1 - \epsilon g_1)(w_2 - \epsilon g_2) \dots (w_l - \epsilon g_l).$$

An example of one second-order term arising from this update is $-\epsilon^2 \mathbf{g}^\top \mathbf{H} \mathbf{g}$, where \mathbf{H} is the Hessian matrix. This term might be negligible if $\prod_{i=3}^l w_i$ is small, or might be significant if the weights on layers 3 through l are greater than 1. To choose an appropriate learning rate, because the effect of a change in one parameter depends so strongly on all of the other parameters, many optimization algorithms address this issue by computing an approximation of the second-order interactions into account, but we can see that even higher-order interactions can be significant. Even second-order approximations are expensive and usually require numerous approximations to the Hessian. Thus, an n -th order optimization algorithm for $n > 2$ thus seems like a bad idea. What should we do instead?

Batch normalization provides an elegant way of reparameterizing the weights and biases of each layer to reduce the variance of the

and dividing by σ_j . The rest of the network then operates the same way that the original network operated on \mathbf{H} .

At training time,

$$\boldsymbol{\mu} = \frac{1}{m} \sum_i \mathbf{H}_{i,:}$$

and

$$\boldsymbol{\sigma} = \sqrt{\delta + \frac{1}{m} \sum_i (\mathbf{H} - \boldsymbol{\mu})_i^2},$$

where δ is a small positive value such as 10^{-8} imposed to avoid the undefined gradient of \sqrt{z} at $z = 0$. Crucially, *we do not use these operations* for computing the mean and the standard deviation, but only for applying them to normalize \mathbf{H} . This means that the gradient of the normalization operation acts simply to increase the standard deviation of h_i ; the normalization operations remove the effect of such a change on its component in the gradient. This was a major insight in the proposed normalization approach. Previous approaches had involved modifying the cost function to encourage units to have normalized statistics, which involved intervening to renormalize unit statistics after each update. The former approach usually resulted in imperfect normalization, while the latter usually resulted in significant wasted time as the learning algorithm proposed changing the mean and variance and the normalization operation undid this change. Batch normalization reparametrizes the network so that units always be standardized by definition, deftly sidestepping the need for such interventions.

At test time, $\boldsymbol{\mu}$ and $\boldsymbol{\sigma}$ may be replaced by running averages of the training data. This allows the model to be evaluated without needing to use definitions of $\boldsymbol{\mu}$ and $\boldsymbol{\sigma}$ that depend on the training data.

of one of the lower weights can flip the relationship between situations are very rare. Without normalization, nearly every unit has an extreme effect on the statistics of h_{l-1} . Batch normalization makes this model significantly easier to learn. In this example, this of course came at the cost of making the lower layers useless. Without the lower layers no longer have any harmful effect, but they also have any beneficial effect. This is because we have normalized only the first-order statistics, which is all that a linear network can influence. In a network with nonlinear activation functions, the lower layers perform nonlinear transformations of the data, so they remain useful. Batch normalization standardizes only the mean and variance of each unit in order to stabilize the learning process, but allows the relationships between units and the nonlinear activation function to change.

Because the final layer of the network is able to learn a mapping from the input to the output, we may actually wish to remove all linear relationships between the input and the output layer. Indeed, this is the approach taken by [Desjardins et al.](#) (2015), which was the inspiration for batch normalization. Unfortunately, learning these interactions is much more expensive than standardizing the mean and standard deviation of each individual unit, and so far batch normalization remains a practical approach.

Normalizing the mean and standard deviation of a unit can increase the expressive power of the neural network containing that unit. In order to increase the expressive power of the network, it is common to replace the nonlinear activations \mathbf{H} with $\gamma\mathbf{H}' + \beta$ rather than simply the normal \tanh or ReLU . γ and β are learned parameters that allow the new variance and standard deviation. At first glance, this may seem unnecessary if we set the mean to $\mathbf{0}$, and then introduce a parameter that allows

the latter. More specifically, $\mathbf{XW} + \mathbf{b}$ should be replaced by \mathbf{XW} . The bias term should be omitted because it becomes the β parameter applied by the batch normalization repair. The input to a layer is usually the output of a nonlinear activation function, such as the rectified linear function in a previous layer. The statistics of the input are more non-Gaussian and less amenable to standardization than the output.

In convolutional networks, described in chapter 9, it is important to use the same normalizing μ and σ at every spatial location within a feature map so that the statistics of the feature map remain the same regardless of its location.

8.7.2 Coordinate Descent

In some cases, it may be possible to solve an optimization problem by breaking it into separate pieces. If we minimize $f(\mathbf{x})$ with respect to variable x_i , then minimize it with respect to another variable x_j , and repeatedly cycling through all variables, we are guaranteed to reach a local minimum. This practice is known as **coordinate descent**. Minimizing one coordinate at a time. More generally, **block coordinate descent** is minimizing with respect to a subset of the variables simultaneously. “coordinate descent” is often used to refer to block coordinate descent, but the strictly individual coordinate descent.

Coordinate descent makes the most sense when the difficult optimization problem can be clearly separated into groups of variables with isolated roles, or when optimization with respect to one variable is significantly more efficient than optimization with respect to a group. For example, consider the cost function

us an optimization strategy that allows us to use efficient algorithms, by alternating between optimizing \mathbf{W} with \mathbf{H} fixed and \mathbf{H} with \mathbf{W} fixed.

Coordinate descent is not a very good strategy when the first term strongly influences the optimal value of another variable, as in $(x_1 - x_2)^2 + \alpha (x_1^2 + x_2^2)$ where α is a positive constant. The optimal solution is for the two variables to have similar value, while the second term wants them to be near zero. The solution is to set both to zero. Newton's method solves the problem in a single step because it is a positive definite Hessian. However, for small α , coordinate descent will make very slow progress. The first term does not allow a single variable to be changed significantly from the current value of the other variable.

8.7.3 Polyak Averaging

Polyak averaging (Polyak and Juditsky, 1992) consists of averaging all points in the trajectory through parameter space visited by the algorithm. If t iterations of gradient descent visit points $\theta_1, \dots, \theta_t$, the output of the Polyak averaging algorithm is $\hat{\theta}^{(t)} = \frac{1}{t} \sum_i \theta_i$. For convex classes, such as gradient descent applied to convex problems, Polyak averaging has strong convergence guarantees. When applied to neural networks, it is more heuristic, but it performs well in practice. The standard gradient descent optimization algorithm may leap back and forth across the valley without ever visiting a point near the bottom of the valley. With Polyak averaging, the locations on either side should be close to the bottom of the valley.

In non-convex problems, the path taken by the optimization algorithm is very complicated and visits many different regions. Including

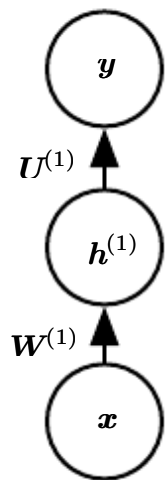
8.7.4 Supervised Pretraining

Sometimes, directly training a model to solve a specific task if the model is complex and hard to optimize or if the task is sometimes more effective to train a simpler model to solve the model more complex. It can also be more effective to train a simpler task, then move on to confront the final task. This involves training simple models on simple tasks before confronting training the desired model to perform the desired task are **pretraining**.

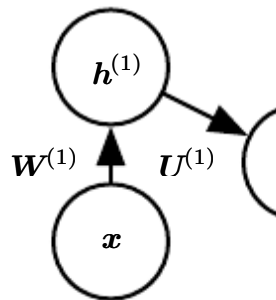
Greedy algorithms break a problem into many components and find the optimal version of each component in isolation. Unfortunately, individually optimal components is not guaranteed to yield a global solution. However, greedy algorithms can be computationally efficient algorithms that solve for the best joint solution, and the quality is often acceptable if not optimal. Greedy algorithms may be used in a **fine-tuning** stage in which a joint optimization algorithm is used to find a solution to the full problem. Initializing the joint optimization with a greedy solution can greatly speed it up and improve the quality of the final solution.

Pretraining, and especially greedy pretraining, are common in deep learning. In this section, we describe specifically those algorithms that break supervised learning problems into other simpler problems. This approach is known as **greedy supervised**

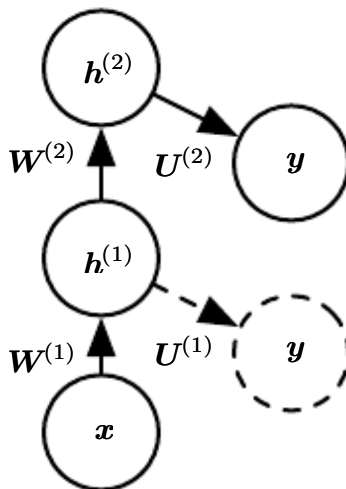
In the original (Bengio *et al.*, 2007) version of greedy supervised pretraining, each stage consists of a supervised learning training task involving training the layers in the final neural network. An example of greedy



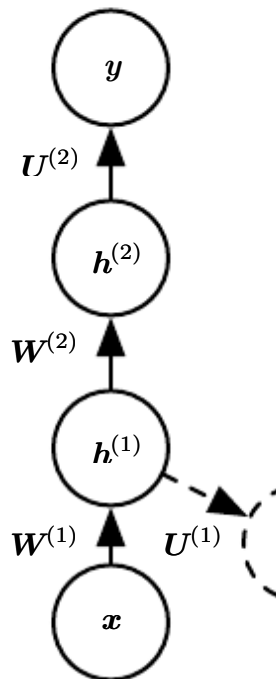
(a)



(b)



(c)



(d)

intermediate levels of a deep hierarchy. In general, pretraining helps in terms of optimization and in terms of generalization.

An approach related to supervised pretraining extends to a form of transfer learning: Yosinski *et al.* (2014) pretrain a deep convolutional network with k layers of weights on a set of tasks (a subset of the 1000 ImageNet categories) and then initialize a same-size network with the first k layers of the first network and the layers of the second network (with the upper layers initialized to zero). The two networks are then jointly trained to perform a different set of tasks (another subset of the 1000 ImageNet object categories), with fewer training examples and more tasks. Other approaches to transfer learning with neural networks are discussed in section 15.2.

Another related line of work is the **FitNets** (Romero *et al.*, 2014). This approach begins by training a network that has low enough width (number of units per layer) to be easy to train. This network becomes a **teacher** for a second network, designated the **student**. The student network is much deeper and thinner (eleven to nineteen layers) and is difficult to train with SGD under normal circumstances. The student network is made easier by training the student network to match the output for the original task, but also to predict the values of the hidden layers of the teacher network. This extra task provides a set of targets for the hidden layers of the student network. The number of hidden layers should be used and can simplify the optimization. The parameters are introduced to regress the middle layer of the teacher network from the middle layer of the deeper student network. However, since the final classification target, the objective is to predict the output of the teacher network. The lower layers of the student network are trained on two objectives: to help the outputs of the student network agree with the teacher network as well as to predict the intermediate layer of the teacher network.

8.7.5 Designing Models to Aid Optimization

To improve optimization, the best strategy is not always to improve the algorithm. Instead, many improvements in the optimization come from designing the models to be easier to optimize.

In principle, we could use activation functions that induce jagged non-monotonic patterns. However, this would make optimization difficult. In practice, *it is more important to choose a model that is easy to optimize than to use a powerful optimization algorithm*. Most of the advances in neural network learning over the past 30 years have been in changing the model family rather than changing the optimization algorithm. Gradient descent with momentum, which was used to train neural networks in the 1980s, remains in use in the modern state of the art neural network.

Specifically, modern neural networks reflect a *design choice* to use linear transformations between layers and activation functions that are everywhere and have significant slope in large portions of the domain. Particular, model innovations like the LSTM, rectified linear units, and batch normalization have all moved toward using more linear functions than previous models based on sigmoidal units. These models have nice properties that make optimization easier. The gradient flows through many layers, and the Jacobian of the linear transformation has reasonable singular values. If the current output of a linear function consistently increases in a single direction, and the current output is very far from correct, it is clear simply from context which direction its output should move to reduce the loss function. In other words, modern neural nets have been designed so that their *local gradient* corresponds reasonably well to moving toward a distant solution.

Other model design strategies can help to make optimization

should do, via a shorter path. These hints provide an error

8.7.6 Continuation Methods and Curriculum [1]

As argued in section 8.2.7, many of the challenges in optimizing the global structure of the cost function and cannot be resolved by local estimates of local update directions. The predominant strategy for this problem is to attempt to initialize the parameters in a region close to the solution by a short path through parameter space to discover.

Continuation methods are a family of strategies that make optimization easier by choosing initial points to ensure that local optimization spends its time in well-behaved regions of space. The idea behind continuation is to construct a series of objective functions over the same parameter space. To minimize a cost function $J(\theta)$, we will construct new cost functions $J^{(i)}$. These cost functions are designed to be increasingly difficult to minimize, with $J^{(1)}$ being the easiest and $J^{(n)}$, the most difficult, being $J(\theta)$, motivating the entire process. When we say that $J^{(i)}$ is well behaved, it means that it is well behaved over more of θ space. A random point is likely to land in the region where local descent can minimize $J^{(i)}$ successfully because this region is larger. The series of cost functions is constructed so that a solution to one is a good initial point of the next. We solve an easy problem then refine the solution to solve the next problem until we arrive at a solution to the true underlying problem.

Traditional continuation methods (predating the use of continuation for neural network training) are usually based on smoothing the cost function. See Wu (1997) for an example of such a method and a re-

become approximately convex when blurred. In many cases, enough information about the location of a global minimum can be obtained by solving progressively less blurred versions. This approach can break down in three different ways. First, it may be a series of cost functions where the first is convex and the next is not, arriving at the global minimum, but then many incremental cost functions that the cost of the entire process is NP-hard optimization problems remain NP-hard, even when continuation methods are applicable. The other two ways that continuation methods may fail are to the method not being applicable. First, the function may not become convex no matter how much it is blurred. Consider for example the function $f(x) = \sin(x)$. Second, the function may become convex as a result of blurring, but the minimum of this blurred function may track to a local rather than a global minimum of the original cost function.

Though continuation methods were mostly originally designed to solve the problem of local minima, local minima are no longer believed to be a problem for neural network optimization. Fortunately, continuation methods still help. The easier objective functions introduced by the continuation method can eliminate flat regions, decrease variance in gradient estimates, smooth the Hessian matrix, or do anything else that will either make the problem easier to compute or improve the correspondence between the current solution and progress toward a global solution.

[Bengio *et al.* \(2009\)](#) observed that an approach called **curriculum learning** or **shaping** can be interpreted as a continuation method. It is based on the idea of planning a learning process to begin by learning simple concepts and progress to learning more complex concepts that depend on the simple concepts. This basic strategy was previously known to accelerate learning.

more prototypical examples and then help the learner refine with the less obvious cases. Curriculum-based strategies teaching humans than strategies based on uniform sampling also increase the effectiveness of other teaching strategies (2013).

Another important contribution to research on curriculum context of training recurrent neural networks to capture long Zaremba and Sutskever (2014) found that much better results *stochastic curriculum*, in which a random mix of easy and difficult presented to the learner, but where the average proportion of examples (here, those with longer-term dependencies) is greater than a deterministic curriculum, no improvement over the baseline (from the full training set) was observed.

We have now described the basic family of neural network architectures, how to regularize and optimize them. In the chapters ahead, we turn to the neural network family, that allow neural networks to scale to process input data that has special structure. The optimization techniques in this chapter are often directly applicable to these special cases with little or no modification.