

# Deep Learning

Muchang Bahng

Summer 2023, Spring 2025

## Contents

<b>1 Multi-Layered Perceptrons</b>	<b>6</b>
1.1 Feedforward Fully-Connected Networks . . . . .	6
1.2 Function Space and Universal Approximation . . . . .	8
1.3 Tensors . . . . .	10
1.3.1 Strides . . . . .	12
1.3.2 Automatic Differentiation . . . . .	12
1.4 Forward and Back Propagation . . . . .	13
1.5 Overparamterization is Good? . . . . .	17
1.6 Engineering Heuristics . . . . .	19
1.6.1 Weight Initialization . . . . .	19
1.6.2 Activation Functions . . . . .	21
1.7 Datasets and Dataloaders . . . . .	23
1.8 Exercises . . . . .	24
<b>2 Training and Control</b>	<b>28</b>
2.1 Early Stopping . . . . .	28
2.2 L1 and L2 Regularization . . . . .	28
2.3 Dropout . . . . .	28
2.4 Data Augmentation . . . . .	29
2.5 Normalization Layers . . . . .	29
2.6 Residual Connections . . . . .	32
2.7 Network Pruning . . . . .	32
2.8 Curriculum Learning . . . . .	33
2.9 Summary . . . . .	33
<b>3 Convolutional Neural Networks</b>	<b>35</b>
3.1 Convolutional and Pooling Layers . . . . .	35
3.2 Backpropagation . . . . .	40
3.3 Visualizing Activation Maps . . . . .	40
3.4 CAM and Grad-CAM . . . . .	40
3.5 Exercises . . . . .	40
<b>4 Recurrent Neural Networks</b>	<b>42</b>
4.1 Unidirectional RNNs . . . . .	43
4.1.1 Loss Functions . . . . .	44
4.1.2 Backpropagation Through Time . . . . .	44
4.1.3 Stacked Unidirectional RNNs . . . . .	45
4.2 Bidirectional RNNs . . . . .	46
4.2.1 PyTorch Implementation . . . . .	46
4.3 Long Short Term Memory (LSTMs) . . . . .	47

4.3.1 Multilayer LSTMs . . . . .	50
4.4 Gated Recurrent Units . . . . .	51
<b>5 Encoder-Decoder Models</b>	<b>52</b>
5.1 Autoencoders . . . . .	52
5.2 Sequence to Sequence . . . . .	55
5.3 More Flexible Models . . . . .	57
<b>6 Energy Models</b>	<b>58</b>
6.1 Boltzmann Machines . . . . .	58
6.2 Restricted Boltzmann Machines . . . . .	60
6.2.1 Contrastive Divergence . . . . .	61
6.2.2 Inference with Bernoulli-Bernoulli RBMs . . . . .	64
6.2.3 Inference with Gaussian-Bernoulli RBMs . . . . .	66
6.3 Deep Belief Network . . . . .	66
6.4 Hopfield Networks . . . . .	66
<b>7 Variational Autoencoders</b>	<b>67</b>
7.1 Reparameterization Trick . . . . .	73
7.2 Importance Weighted Autoencoders . . . . .	77
7.3 Conditional VAEs . . . . .	77
<b>8 Generative Adversarial Networks</b>	<b>78</b>
8.1 Conditional GAN . . . . .	82
8.2 CycleGAN . . . . .	82
8.3 Deep Convolution GAN (DCGAN) . . . . .	82
<b>9 Normalizing Flows</b>	<b>83</b>
9.1 Finite Normalizing Flows . . . . .	84
9.2 Coupling-Layer Flows . . . . .	87
9.2.1 RealNVP . . . . .	88
9.2.2 NICE . . . . .	88
9.3 GLOW . . . . .	89
9.4 Augoregressive Flows . . . . .	89
9.5 Infinitesimal Flows . . . . .	89
<b>10 Score Based Models</b>	<b>90</b>
<b>11 Attention Models</b>	<b>91</b>
11.1 Seq2Seq with Attention . . . . .	91
11.2 Self-Attention Layer . . . . .	94
11.2.1 Tokenization and Positional Embeddings . . . . .	96
11.2.2 Stacked Attention Layers and Multi-Head Attention . . . . .	96
11.3 Transformers . . . . .	98
11.3.1 Masking . . . . .	99
11.4 Practical Implementation . . . . .	99
11.4.1 Key, Value, Query Matrices and In Projections . . . . .	99
11.4.2 Masking . . . . .	100
11.4.3 Computing Attention . . . . .	100
11.4.4 Forward Pass of MultiheadAttention . . . . .	101
11.4.5 Transformer . . . . .	102
11.5 Vision Transformers . . . . .	103
<b>12 Diffusion Models</b>	<b>105</b>

<b>13 Semi Supervised Learning</b>	<b>106</b>
13.1 Pseudo Label Learning . . . . .	106
13.2 Consistency Regularization . . . . .	106
13.3 Distribution Alignment . . . . .	106
13.4 Weak Supervision . . . . .	106
13.5 Student Teacher Models . . . . .	106
<b>References</b>	<b>107</b>

Why do we even *need* deep neural networks in the first place? Well with classical machine learning, the models that we worked with were “simple” enough<sup>1</sup> to interpret. For example, linear regression had a simple parametric form, and decision trees, though nonlinear and nonparametric, were very interpretable both in training and prediction. However, it may be that the very notion of interpretability is limiting the power of our models. Maybe the world is so complex that it may not be even possible to model it with these interpretable functions. Therefore, we should try to create a model with a simple enough parametrization, but something that is expressive enough to cover an extremely large space of functions. This may sound contradictory, but it is possible.

Unlike my machine learning notes, which focuses mostly on the theoretical soundness of classical (e.g. pre-deep and interpretable) models, the theory of deep neural networks have not been developed as well yet. Furthermore, the recency of developments, especially in the post-2010s, results in a pretty nonlinear<sup>2</sup> timeline that is difficult to categorize effectively. Before I give my motivation, the direct prerequisites for deep learning are basic knowledge of my notes in probability theory, machine learning, and real analysis.

Therefore, after much thought, I think organizing my notes in chronological order would be best. It turned out that in the early days of deep learning, most researchers like Andrew Ng stated that he focused on supervised models,<sup>3</sup> and it wasn’t until the 2010s that the development of unsupervised models burgeoned.

1. We start by introducing *multilayered perceptrons* (MLPs), which build upon generalized linear models (GLMs) that we have went over in machine learning. This is pretty much the “foundational” model that we will build on. We then talk about practical methodologies regarding training and control.
2. Then we introduce the other two architectures. The *convolutional neural network* (CNN) gives us a scalable way to perform sparse matrix multiplication efficiently, by taking advantage of locality. Then in *recurrent neural networks* (RNNs), we are not limited to a single  $n$ -dimensional vector input and are able to process a time series of inputs.
3. With these building blocks, we are able take and two neural networks together to create an encoder-decoder model. The two main applications of this was dimensionality reduction with *autoencoders*, followed by *seq2seq* for machine translation between sequences of words.
4. The practical success of autoencoders led to the development of not just density estimation models, but *generative* ones that seek to sample from the learned distribution. These generative models were “deep” extensions of the classical linear factor models resulting in *restricted Boltzmann machines* (RBMs) and *variational autoencoders* (VAEs), which attempted to explicitly model an approximation of the true data generating distribution. More specifically, RBMs were *energy models* that borrowed ideas from physics to learn a distribution of the form  $p_X(x) = \frac{1}{Z} e^{-f_\theta(x)}$ . To sample from this, researchers already had access to the established Markov Chain Monte Carlo (MCMC) algorithms designed for this exact problem. As for VAEs, these were trained and sampled through *variational inference* methods.
5. In 2014, a completely new architecture composed of 2 neural networks competing each other gave rise to *generative adversarial networks* (GANs) which blew RBMs and VAEs away. A similar architecture followed with *generative stochastic networks* (GSNs).
6. In 2016, *normalizing flow models*, which attempted to model a smooth function that transformed simple latent variables to the true data generating distribution, were invented by Google DeepMind and surpassed GANs.
7. In 2017, *attention* took the world by storm, which had drastically improved machine translation in seq2seq, and the resulting *self-attention* plus the *transformer* architectures led to the success of OpenAI’s ChatGPT.

Again, I emphasize that the math in these notes are not very advanced. However, implementing these simple models and training algorithms from scratch is a challenge in itself. I will go through implementing everything

---

<sup>1</sup>I am using simple in a very loose sense, since this doesn’t really mean that the model space is finite-dimensional or have any correlation with complexity.

<sup>2</sup>No pun intended.

<sup>3</sup>He states this in his podcast with Lex Fridman.

from scratch as if we were building a mini-version of PyTorch as we learn new topics. My implementations can be found [here](#).

## 1 Multi-Layered Perceptrons

We build upon what we already know: generalized linear models. In simple regression, we transform the inputs into the relevant features  $\mathbf{x}_n \mapsto \phi(\mathbf{x}_n) = \phi_n$  and then, when we construct a generalized linear model, we assume that the conditional distribution  $Y | X = x$  is in the canonical exponential family, with some natural parameter  $\eta(x)$  and expected mean  $\mu(x) = \mathbb{E}[Y | X = x]$ . Then, to choose the link function  $g$  that related  $g(\mu(x)) = x^T \beta$ , we can set it to be the canonical link  $g$  that maps  $\mu$  to  $\eta$ . That is, we have  $g(\mu(x)) = x^T \beta = \eta(x)$  such that the natural parameter is linearly dependent on the input. The inverse  $g^{-1}$  of the link function is called the **activation function**, which connects the expected mean to a linear function of  $x$ .

$$h_\beta(x) = g^{-1}(x^T \beta) = \mu(x) = \mathbb{E}[Y | X = x] \quad (1)$$

Now, note that for a classification problem, the decision boundary defined in the  $\phi$  feature space is linear, but it may not be linear in the input space  $\mathcal{X}$ . We would like to extend this model by making the basis functions  $\phi_n$  depend on the parameters  $\mathbf{w}$  and then allow these parameters to be adjusted during training.

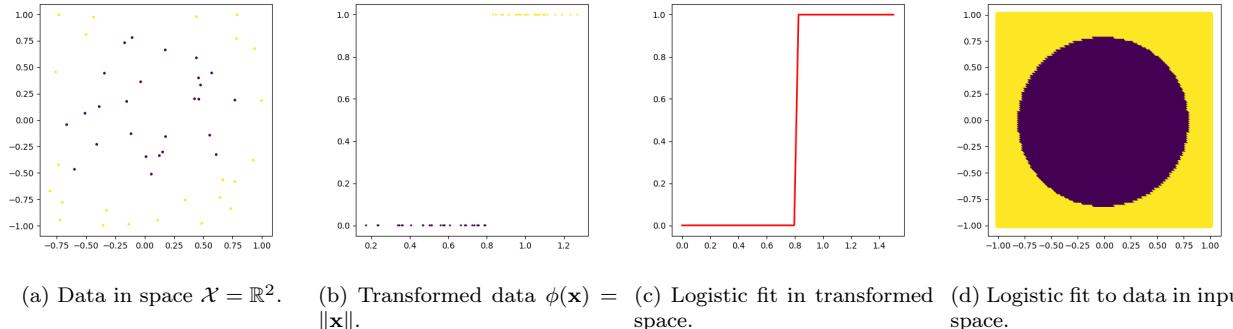


Figure 1: Consider the set of points in  $\mathbb{R}^2$  with the corresponding class. We transform the features to  $\phi(x_1, x_2) = x_1^2 + x_2^2$ , which gives us a new space to work with. Fitting logistic regression onto this gives a linear decision boundary in the space  $\phi$ , but the boundary is circular in  $\mathcal{X} = \mathbb{R}^2$ .

### 1.1 Feedforward Fully-Connected Networks

So how should we construct parametric nonlinear basis functions? One way is to have a similar architecture as GLMs by having a linear map followed by an activation function  $f(x) = \sigma(w^T x + b)$ . The simplest such function with the activation function as the step function

$$f(z) = \begin{cases} 1 & \text{if } z \geq 0 \\ 0 & \text{if } z < 0 \end{cases} \quad (2)$$

is the perceptron algorithm. It divides  $\mathbb{R}^d$  using a hyperplane  $\omega^T \mathbf{x} + b = 0$  and linearly classifies all points on one side to value 1 and the other side to value 0. This is similar to a neuron, which takes in a value and outputs a "signal" if the function evaluated gets past a threshold. However, for reasons regarding training these networks, we would like to use smooth activation functions for this, so we would use different activations. Hence we have a neuron.

#### Definition 1.1 (Neuron)

A **neuron** is a function of form

$$y = \sigma(\mathbf{w}^T \mathbf{x} + b) \quad (3)$$

where  $\sigma : \mathbb{R} \rightarrow \mathbb{R}$  is any nonlinear function, called an **activation functions**.

Ultimately, a neural net is really just a generalized linear model with some trained feature extractors, which is why in practice, if researchers want to predict a smaller dataset, they take a pretrained model on a related

larger dataset and simply tune the final layer, since the second last layer most likely encodes all the relevant features. This is called *transfer learning*. But historically, it was called a *multilayer perceptron* and the name stuck.

### Definition 1.2 (Feedforward, Fully-Connected Multilayer Perceptron)

A  $L$ -layer **multilayer perceptron (MLP)**  $f_\theta : \mathbb{R}^D \rightarrow \mathbb{R}^M$ , with parameters  $\theta$ , is a function of form

$$h_\theta(\mathbf{x}) := \sigma^{[L]} \circ W^{[L]} \circ \sigma^{[L-1]} \circ W^{[L-1]} \circ \dots \circ \sigma^{[1]} \circ W^{[1]}(\mathbf{x}) \quad (4)$$

where  $\sigma^{[l]} : \mathbb{R}^{N^{[l]}} \rightarrow \mathbb{R}^{N^{[l]}}$  is an activation function and  $W^{[l]} : \mathbb{R}^{N^{[l-1]}} \rightarrow \mathbb{R}^{N^{[l]}}$  is an affine map. We will use the following notation.

1. The inputs will be labeled  $\mathbf{x} = a^{[0]}$  which is in  $\mathbb{R}^{N^{[0]}} = \mathbb{R}^D$ .
2. We map  $a^{[l]} \in \mathbb{R}^{N^{[l]}} \mapsto W^{[l+1]}a^{[l]} + b^{[l+1]} = z^{[l+1]} \in \mathbb{R}^{N^{[l+1]}}$ , where  $z$  denotes a vector after an affine transformation.
3. We map  $z^{[l+1]} \in \mathbb{R}^{N^{[l+1]}} \mapsto \sigma(z^{[l+1]}) = a^{[l+1]} \in \mathbb{R}^{N^{[l+1]}}$ , where  $a$  denotes a vector after an activation function.
4. We keep doing this until we reach the second last layer with vector  $a^{[L-1]}$ . Note that in the last layer we do *not* apply an activation function.

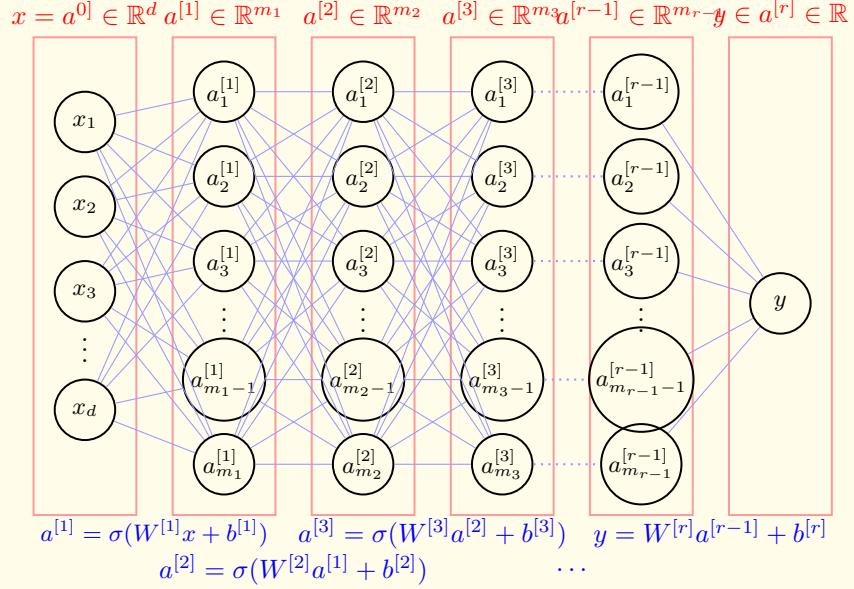


Figure 2: If there does not exist any edge from a potential input  $x$  to an output  $y$ , then this means that  $x$  is not relevant in calculating  $y$ , i.e. the weight is 0. However, we usually work with **fully-connected neural networks**, which means that every input is relevant to calculating every output, since we usually cannot make assumptions about which variables are relevant or not.

Note that each layer corresponds to how close a neuron is to the output. But really any neuron can be a function of any other neuron. For example, we can connect a neuron from layer 4 back to a neuron of layer 1. For now, we will consider networks that are restricted to a **feed-forward** architecture, in other words having no closed directed cycles.

### Code 1.1 (Parameters and Neural Nets in PyTorch)

At this point, you have learned the theory of MLPs. To actually implement them in PyTorch, look at this module here, which will tell you on how to construct linear maps and activations functions, and more importantly see how you can look at the weights, modify them, and see how they are initialized. You can then learn how to explore the weights and biases of a neural network.

## 1.2 Function Space and Universal Approximation

Great, so we have defined our architecture, but how do we know that this class of functions is expressive? Neural networks have been mathematically studied back in the 1980s, and the reason that they are so powerful is that we can theoretically prove the limits on what they can learn. For very specific classes of functions, the results are easier, but for more general ones, it becomes much harder. We prove one of the theorems below.

Let us think about how one would construct approximations for such functions. Like in measure theory, we can think of every measurable function as a linear combination of a set of bump functions, and so we can get a neural network to do the same.

### Example 1.1 (Bump Functions in $\mathbb{R}$ )

Assuming the sigmoid activation function is used, the bump function

$$f(x) = \begin{cases} 1 & \text{if } a < x < b \\ 0 & \text{if else} \end{cases} \quad (5)$$

can be approximated by taking a linear combination of a sigmoid function stepping up and one stepping down. That is,

$$f(x) \approx \frac{1}{2}\sigma(k(x - a)) - \frac{1}{2}\sigma(k(x - b)) \quad (6)$$

where  $k$  is a scaling constant that determines how steep the steps are for each function. Therefore, as  $k \rightarrow \infty$ , the function begins to look more like a step function.

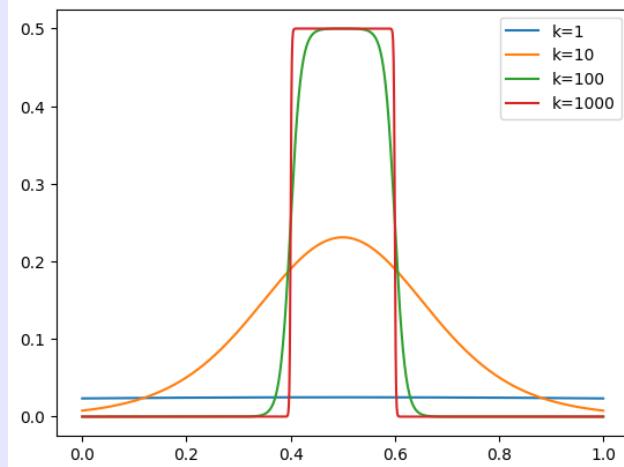


Figure 3: Bump function approximated with  $a = 0.4, b = 0.6$ , with differing values of  $k$ .

**Example 1.2 (Bump Functions in  $\mathbb{R}^2$ )**

To do this for a 2-D step function, of the form

$$f(x_1, x_2) = \begin{cases} 1 & \text{if } a < x_1 < b \\ 0 & \text{if else} \end{cases} \quad (7)$$

this is a simple extension of the first one. We just don't need to make our linear combination dependent on  $x_2$  and we're done.

$$f(x) \approx \frac{1}{2}\sigma(k(x_1 - a)) - \frac{1}{2}\sigma(k(x_1 - b)) \quad (8)$$

**Example 1.3 (Tower Functions in  $\mathbb{R}^2$ )**

Now to construct a tower function of the form

$$f(x_1, x_2) = \begin{cases} 1 & \text{if } a_1 < x_1 < b_1, a_2 < x_2 < b_2 \\ 0 & \text{if else} \end{cases} \quad (9)$$

we need slightly more creativity. Now we can approximate it by doing

$$f(x) \approx \sigma\left(k_2[\sigma(k_1(x_1 - a_1)) - \sigma(k_1(x_1 - b_1)) + \sigma(k_1(x_2 - a_2)) - \sigma(k_1(x_2 - b_2))] - b_2\right) \quad (10)$$

At this point, we can see how this would extend to  $\mathbb{R}^n$ , and by isolating parts of the network we can have it approximate tower functions that are completely separate from each other, at any height, and then finally take a linear combination of them to approximate the original function of interest.

**Theorem 1.1 (CS671 Fall 2023 PS5)**

Suppose you have a 2D,  $L$ -lipschitz function  $f(x_1, x_2)$  defined on a unit square ( $x_1, x_2 \in [0, 1]$ ). You want to approximate this with an arbitrary neural net  $\tilde{f}$  such that

$$\sup_{x \in [0,1]^2} |f(x) - \tilde{f}(x)| \leq \epsilon \quad (11)$$

If we divide the square into a checkerboard of  $K \times K$  nonoverlapping squares, approximate the restriction of  $f$  to each subsquare with a tower function, what is the least  $K$  we would need to ensure that the error is less than  $\epsilon$ ?

Early in the development of the theory of neural nets, An Mei Chen, (currently VP of engineering in Qualcomm) showed that for certain neural networks, there are multiple parameters  $\theta$  that map to the same function  $f$ . [CLHN93]

**Theorem 1.2 (Parameter Symmetry)**

Consider a 2-layer feedforward network of form

$$f = W^{[2]} \circ \sigma \circ W^{[1]} \quad (12)$$

where  $\sigma = \tanh$ . Let  $z$  be the hidden vector. We can see that by changing the signs of the  $i$ th row of  $W^{[1]}$ ,  $z_i$ 's sign will be flipped. From the properties that  $\tanh$  is an odd function (i.e.  $\tanh(-x) = -\tanh(x)$ ), therefore the activation will be also sign-flipped, but this effect can be negated by flipping the  $i$ th column of the  $W^{[2]}$ . Therefore, given that  $z \in R^N$ , i.e there are  $N$  hidden units, we can

choose any set of row-column pairs of the weight matrices to invert, leading to a total of  $2^N$  different weightings that produce the same function  $f$ .

Similarly, imagine that we permute the columns of  $W^{[2]}$  and rows of  $W^{[1]}$  in the same way. Then this will also lead to an invariance in  $f$ , and so this leads to  $N!2^N$  different weight vectors that lead to the same function!

### 1.3 Tensors

In numerical computing packages like `numpy` in Python and `eigen` in C++, we often work with scalars, vectors, and matrices. From linear algebra, the generalization of these objects is a tensor, which is an element of a tensor product space.<sup>4</sup> The full mathematical abstraction is rarely needed in practice, and so developers call tensors by their realization as *multidimensional arrays*.

#### Definition 1.3 (Tensor)

A **tensor** is an element of a tensor product space  $\bigotimes_i V_i$ . It is represented as a **multidimensional array** of shape  $(\dim(V_1), \dots, \dim(V_n))$ .

If we were trying to build a **Tensor** class from scratch, what attributes should it have? Well obviously we need the actual data in the tensor, which we will call `storage`, plus some metadata about the `shape` (in math, known as the tensor *rank*). Usually, these packages optimize as much as possible for efficiency, and so these are implemented as C-style arrays, which then requires knowledge of the type of each element of the Tensor, called the `dtype`. Great, with these three attributes, we can do almost every type of arithmetic manipulation. Let's first introduce the most basic math tensor operations, which includes the normal operations supported in an algebra, plus some other ones. We will denote the shapes as well.

1. *Tensor Addition.*
2. *Tensor Additive Inverse.*
3. *Scalar Multiplication.*
4. *Matrix Multiplication.*
5. *Elementwise Multiplication.*
6. *Elementwise Multiplicative Inverse.*
7. *Transpose.*

We would probably like some constructors that allows you to directly initialize tensors filled with 0s (`zeros`), 1s (`ones`), a multiplicative identity (`eye`<sup>5</sup>) Some random initializers would be good, such as sampling from uniforms (`uniform`), gaussians (`gaussian`, `randn`).

Finally, we would like some very fundamental operations, such as typecasting, comparison, and indexing as well.

<sup>4</sup>For a refresher, look at my linear algebra notes.

<sup>5</sup>homophone for  $I$ , used to denote the identity matrix.

---

**Algorithm 1** Tensor Class Implementation

---

```

1: class Tensor:
2: Attributes:
3:   storage: array
4:   shape: tuple
5:   dtype: type
6: Constructors:
7: def __init__(data, shape, dtype):
8:   Initialize tensor with given data, shape, and dtype
9: Static Constructors:
10: @staticmethod
11: def zeros(shape, dtype):
12:   return tensor filled with zeros
13: @staticmethod
14: def ones(shape, dtype):
15:   return tensor filled with ones
16: @staticmethod
17: def eye(n, dtype):
18:   return  $n \times n$  identity matrix
19: @staticmethod
20: def uniform(shape, low, high, dtype):
21:   return tensor with uniform random values
22: @staticmethod
23: def gaussian(shape, mean, std, dtype):
24:   return tensor with gaussian random values
25: Arithmetic Operations:
26: def __add__(self, other):
27:   return element-wise addition
28: def __neg__(self):
29:   return additive inverse
30: def __mul__(self, other):
31:   return scalar or element-wise multiplication
32: def matmul(self, other):
33:   return matrix multiplication
34: def __truediv__(self, other):
35:   return element-wise division
36: def transpose(self):
37:   return transposed tensor
38: Utility Operations:
39: def __repr__(self):
40:   return string representation
41: def __str__(self):
42:   return human-readable string
43: def __getitem__(self, index):
44:   return indexed value(s)
45: def __eq__(self, other):
46:   return element-wise equality comparison

```

▷Underlying data storage  
▷Dimensions of tensor  
▷Data type of elements

---

Note that there are other operations, such as concatenation, splitting, and stacking that would be a good idea to implement.

### 1.3.1 Strides

A specific property of PyTorch is that they use strides as another source of metadata in storing tensors, which greatly speeds up operations. Consider that we want to transpose the first two dimensions of a tensor. Then, we would have to create a new tensor and fill it in with all the elements, which may be too computationally expensive for such a small operation.

#### Definition 1.4 (Stride)

Given a tensor  $T$  of size  $(N_1, \dots, N_M)$ , it is stored as a contiguous array of  $\prod_m T_m$  elements, and we can index it as

$$T[n_1, n_2, \dots, n_M], \quad 1 \leq n_i \leq N_i \quad (13)$$

To counteract this, the **stride** is a array  $S$  of  $M$  elements,

$$S = (S_1, \dots, S_M) \quad (14)$$

where indexing with some  $I = (n_1, \dots, n_M)$  is equivalent to computing  $S \cdot I$  and taking that index in the array in memory. It defines a mapping.

If we do some calculation, the default stride of such a vector is defined

$$S_m = \prod_{m < j} N_j, \quad S_M = 1 \quad (15)$$

#### Example 1.4 (Transposing)

If we want to transpose the tensor above, then we change the stride from

$$S = \left( \prod_{1 < j} N_j, \prod_{2 < j} N_j, \dots, 1 \right) \quad (16)$$

to

$$S = \left( \prod_{2 < j} N_j, \prod_{1 < j} N_j, \dots, 1 \right) \quad (17)$$

### 1.3.2 Automatic Differentiation

#### Lemma 1.1 (Derivative of $+/ -$ )

Given two tensors  $X, Y$  and  $Z_+ = X + Y, Z_- = X - Y$ , we have

$$\frac{\partial Z_+}{\partial X} = +1 \quad \frac{\partial Z_+}{\partial Y} = +1 \quad (18)$$

$$\frac{\partial Z_-}{\partial X} = +1 \quad \frac{\partial Z_-}{\partial Y} = -1 \quad (19)$$

where  $\pm 1$  are tensors of 1 or  $-1$ s of the same shape as  $X, Y$ .

#### Lemma 1.2 (Derivative of Element-wise Multiplication)

Given two tensors  $X, Y$  and  $Z = X \odot Y$ , we have

$$\frac{\partial Z}{\partial X} = Y \quad \frac{\partial Z}{\partial Y} = X \quad (20)$$

**Lemma 1.3 (Derivative of Matrix Multiplication)**

Given  $X \in (N, M)$  and  $Y \in (M, P)$ , with  $Z = XY \in (N, P)$ , the derivative of matrix multiplication is

$$\frac{\partial Z}{\partial X} \in (N, P, N, M) \quad \left( \frac{\partial Z}{\partial X} \right)_{i,j,k,l} := \frac{\partial Z_{i,j}}{\partial X_{k,l}} \quad (21)$$

$$\frac{\partial Z}{\partial Y} \in (N, P, M, P) \quad \left( \frac{\partial Z}{\partial Y} \right)_{i,j,k,l} := \frac{\partial Z_{i,j}}{\partial Y_{k,l}} \quad (22)$$

## 1.4 Forward and Back Propagation

Back in the supervised learning notes, we have gone through the derivation for linear, logistic, and softmax regression. It turns out that despite them having very different architectures, with identity, sigmoid, and softmax activation function, our choice of loss to be the mean squared loss, the binary cross-entropy, and the cross-entropy loss, had given very cute formulas in computing the gradient of the loss. Unfortunately, the formulas do not get cute when we differentiate neural networks, but they do come in a very structured way. To gain intuition, I would recommend to go over the exercises at the end of the chapter labeled ECE 689 Fall 2021 Midterm. If you just use chain rule to do the calculations, you can see that they require us to compute all the intermediate  $z^{(i)}$ 's and the  $a^{(i)}$ 's, a process called *forward propagation*, before we compute the gradients.

**Definition 1.5 (Forward Propagation)**

Given an MLP  $f$  and an input  $x$ , the process of sequentially evaluating

$$x = a^{[0]} \mapsto z^{[1]} \mapsto a^{[1]} \mapsto \dots \mapsto z^{[L]} \mapsto a^{[L]} = f(x) \quad (23)$$

is called **forward propagation**.

When we want to compute the derivative of  $f$ . we can see that the intermediate partial derivatives in the chain rule are repeatedly used. That is, if we have layer  $0 \leq l \leq L$ , then to compute the derivative with respect to the  $l$ th layer we use the chain rule

$$\frac{\partial f}{\partial z^{[l]}} = \frac{\partial f}{\partial z^{[l+1]}} \cdot \frac{z^{[l+1]}}{z^{[l]}} \quad (24)$$

which requires us to know the derivative at the  $(l + 1)$ th layer, along with the current values of  $z^{[l]}, z^{[l+1]}$  to evaluate the derivatives at the current point. Therefore, we must complete forward propagation first and then compute *backwards* from the result to the input to compute the gradients.

**Definition 1.6 (Backward Propagation)**

Given an MLP  $f$  with input  $x$  that has been forward propagated, the process of sequentially evaluating

$$\frac{\partial f}{\partial a^{[L]}} \mapsto \frac{\partial f}{\partial z^{[L]}} \mapsto \dots \mapsto \frac{\partial f}{\partial z^{[1]}}, \quad (25)$$

is called **backward propagation**, or **backprop**.

Backpropagation is not hard, but it is cumbersome notation-wise. What we really want to do is just compute a very long vector with all of its partials  $\partial E / \partial \theta$ .

**Algorithm 1.1 (Backpropagation)**

To compute  $\frac{\partial E_n}{\partial w_{ji}^{[l]}}$ , it would be natural to split it up into a portion where  $E_n$  is affected by the term before activation  $\mathbf{z}^{[l]}$  and how that is affected by  $w_{ji}^{[l]}$ . The same goes for the bias terms.

$$\frac{\partial E_n}{\partial w_{ji}^{[l]}} = \underbrace{\frac{\partial E_n}{\partial \mathbf{z}^{[l]}}}_{1 \times N^{[l]}} \cdot \underbrace{\frac{\partial \mathbf{z}^{[l]}}{\partial w_{ji}^{[l]}}}_{N^{[l]} \times 1} \quad \text{and} \quad \frac{\partial E_n}{\partial b_i^{[l]}} = \underbrace{\frac{\partial E_n}{\partial \mathbf{z}^{[l]}}}_{1 \times N^{[l]}} \cdot \underbrace{\frac{\partial \mathbf{z}^{[l]}}{\partial b_i^{[l]}}}_{N^{[l]} \times 1} \quad (26)$$

It helps to visualize that we are focusing on

$$\mathbf{h}_\theta(\mathbf{x}) = g\left(\dots \sigma\left(\underbrace{\mathbf{W}^{[l]} \mathbf{a}^{[l-1]} + \mathbf{b}^{[l]}}_{\mathbf{z}^{[l]}}\right) \dots\right) \quad (27)$$

We can expand  $\mathbf{z}^{[l]}$  to get

$$\mathbf{z}^{[l]} = \begin{pmatrix} w_{11}^{[l]} & \dots & w_{1N^{[l-1]}}^{[l]} \\ \vdots & \ddots & \vdots \\ w_{N^{[l]}1}^{[l]} & \dots & w_{N^{[l]}N^{[l-1]}}^{[l]} \end{pmatrix} \begin{pmatrix} a_1^{[l-1]} \\ \vdots \\ a_{N^{[l-1]}}^{[l-1]} \end{pmatrix} + \begin{pmatrix} b_1^{[l]} \\ \vdots \\ b_{N^{[l]}}^{[l]} \end{pmatrix} \quad (28)$$

$w_{ji}^{[l]}$  will only show up in the  $j$ th term of  $\mathbf{z}^{[l]}$ , and so the rest of the terms in  $\frac{\partial \mathbf{z}^{[l]}}{\partial w_{ji}^{[l]}}$  will vanish. The same logic applies to  $\frac{\partial \mathbf{z}^{[l]}}{\partial b_i^{[l]}}$ , and so we really just have to compute

$$\frac{\partial E_n}{\partial w_{ji}^{[l]}} = \underbrace{\frac{\partial E_n}{\partial z_j^{[l]}}}_{1 \times 1} \cdot \underbrace{\frac{\partial z_j^{[l]}}{\partial w_{ji}^{[l]}}}_{1 \times 1} = \delta_j^{[l]} \cdot \frac{\partial z_j^{[l]}}{\partial w_{ji}^{[l]}} \quad \text{and} \quad \frac{\partial E_n}{\partial b_i^{[l]}} = \underbrace{\frac{\partial E_n}{\partial z_j^{[l]}}}_{1 \times 1} \cdot \underbrace{\frac{\partial z_j^{[l]}}{\partial b_i^{[l]}}}_{1 \times 1} = \delta_j^{[l]} \cdot \frac{\partial z_j^{[l]}}{\partial b_i^{[l]}} \quad (29)$$

where the  $\delta_j^{[l]}$  is called the  $j$ th **error term** of layer  $l$ . If we look at the evaluated  $j$ th row,

$$z_j^{[l]} = w_{j1}^{[l]} a_1^{[l-1]} + \dots + w_{jN^{[l-1]}}^{[l]} a_{N^{[l-1]}}^{[l-1]} + b_j^{[l]} \quad (30)$$

We can clearly see that  $\frac{\partial z_j^{[l]}}{\partial w_{ji}^{[l]}} = a_i^{[l-1]}$  and  $\frac{\partial z_j^{[l]}}{\partial b_i^{[l]}} = 1$ , which means that our derivatives are now reduced to

$$\frac{\partial E_n}{\partial w_{ji}^{[l]}} = \delta_j^{[l]} a_i^{[l-1]}, \quad \frac{\partial E_n}{\partial b_i^{[l]}} = \delta_j^{[l]} \quad (31)$$

What this means is that we must know the intermediate values  $\mathbf{a}^{[l-1]}$  beforehand, which is possible since we would compute them using forward propagation and store them in memory. Now note that the partial derivatives at this point have been calculated without any consideration of a particular error function or activation function. To calculate  $\delta^{[L]}$ , we can simply use the chain rule to get

$$\delta_j^{[L]} = \frac{\partial E_n}{\partial z_j^{[L]}} = \frac{\partial E_n}{\partial \mathbf{a}^{[L]}} \cdot \frac{\partial \mathbf{a}^{[L]}}{\partial z_j^{[L]}} = \sum_k \frac{\partial E_n}{\partial a_k^{[L]}} \cdot \frac{\partial a_k^{[L]}}{\partial z_j^{[L]}} \quad (32)$$

which can be rewritten in the matrix notation

$$\delta^{[L]} = \left( \frac{\partial \mathbf{g}}{\partial \mathbf{z}^{[L]}} \right)^T \left( \frac{\partial E_n}{\partial \mathbf{a}^{[L]}} \right) = \underbrace{\begin{bmatrix} \frac{\partial g_1}{\partial z_1^{[L]}} & \dots & \frac{\partial g_{N^{[L]}}}{\partial z_1^{[L]}} \\ \vdots & \ddots & \vdots \\ \frac{\partial g_1}{\partial z_{N^{[L]}}^{[L]}} & \dots & \frac{\partial g_{N^{[L]}}}{\partial z_{N^{[L]}}^{[L]}} \end{bmatrix}}_{N^{[L]} \times N^{[L]}} \begin{bmatrix} \frac{\partial E_n}{\partial a_1^{[L]}} \\ \vdots \\ \frac{\partial E_n}{\partial a_{N^{[L]}}^{[L]}} \end{bmatrix} \quad (33)$$

Note that as soon as we make a model assumption on the form of the conditional distribution  $Y | X = x$  (e.g. it is Gaussian), with it being in the exponential family, we immediately get two things: the loss function  $E_n$  (e.g. sum of squares loss), and the canonical link function  $\mathbf{g}$

1. If we assume that  $Y | X = x$  is Gaussian in a regression (of scalar output) setting, then our canonical link would be  $g(x) = x$ , which gives the sum of squares loss function. Note that since the output is a real-valued scalar,  $\mathbf{a}^{[L]}$  will be a scalar (i.e. the final layer is one node,  $N^{[L]} = 1$ ).

$$E_n = \frac{1}{2}(y^{(n)} - a^{[L]})^2 \quad (34)$$

To calculate  $\delta^{[L]}$ , we can simply use the chain rule to get

$$\delta^{[L]} = \frac{\partial E_n}{\partial z^{[L]}} = \frac{\partial E_n}{\partial a^{[L]}} \cdot \frac{\partial a^{[L]}}{\partial z^{[L]}} = a^{[L]} - y^{(n)} \quad (35)$$

2. For classification (of  $M$  classes), we would use the softmax activation function (with its derivative next to it for convenience)

$$\mathbf{g}(\mathbf{z}) = \mathbf{g}\left(\begin{bmatrix} z_1 \\ \vdots \\ z_M \end{bmatrix}\right) = \begin{bmatrix} e^{z_1} / \sum_k e^{z_k} \\ \vdots \\ e^{z_M} / \sum_k e^{z_k} \end{bmatrix}, \quad \frac{\partial g_k}{\partial z_j} = \begin{cases} g_j(1 - g_j) & \text{if } k = j \\ -g_j g_k & \text{if } k \neq j \end{cases} \quad (36)$$

which gives the cross entropy error

$$E_n = -\mathbf{y}^{(n)} \cdot \ln(\mathbf{h}_\theta(\mathbf{x}^{(n)})) = -\sum_i y_i^{(n)} \ln(a_i^{[L]}) \quad (37)$$

where the  $\mathbf{y}$  has been one-hot encoded into a standard unit vector in  $\mathbb{R}^M$ . To calculate  $\delta^{[L]}$ , we can again use the chain rule again

$$\delta_j^{[L]} = \sum_k \frac{\partial E_n}{\partial a_k^{[L]}} \cdot \frac{\partial a_k^{[L]}}{\partial z_j^{[L]}} \quad (38)$$

$$= -\sum_k \frac{y_k^{(n)}}{a_k^{[L]}} \cdot \frac{\partial a_k^{[L]}}{\partial z_j^{[L]}} \quad (39)$$

$$= \left( -\sum_{k \neq j} \frac{y_k^{(n)}}{a_k^{[L]}} \cdot \frac{\partial a_k^{[L]}}{\partial z_j^{[L]}} \right) - \frac{y_j^{(n)}}{a_j^{[L]}} \cdot \frac{\partial a_j^{[L]}}{\partial z_j^{[L]}} \quad (40)$$

$$= \left( -\sum_{k \neq j} \frac{y_k^{(n)}}{a_k^{[L]}} \cdot -a_k^{[L]} a_j^{[L]} \right) - \frac{y_j^{(n)}}{a_j^{[L]}} \cdot a_j^{[L]} (1 - a_j^{[L]}) \quad (41)$$

$$= a_j^{[L]} \underbrace{\sum_k y_k^{(n)} - y_j^{(n)}}_1 = a_j^{[L]} - y_j^{(n)} \quad (42)$$

giving us

$$\delta^{[L]} = \mathbf{a}_j^{[L]} - \mathbf{y}^{[L]} \quad (43)$$

Now that we have found the error for the last layer, we can continue for the hidden layers. We can again expand by chain rule that

$$\delta_j^{[l]} = \frac{\partial E_n}{\partial z_j^{[l]}} = \frac{\partial E_n}{\partial \mathbf{z}^{[l+1]}} \cdot \frac{\partial \mathbf{z}^{[l+1]}}{\partial z_j^{[l]}} = \sum_{k=1}^{N^{[l+1]}} \frac{\partial E_n}{\partial z_k^{[l+1]}} \cdot \frac{\partial z_k^{[l+1]}}{\partial z_j^{[l]}} = \sum_{k=1}^{N^{[l+1]}} \delta_k^{[l+1]} \cdot \frac{\partial z_k^{[l+1]}}{\partial z_j^{[l]}} \quad (44)$$

By going backwards from the last layer, we should already have the values of  $\delta_k^{[l+1]}$ , and to compute the second partial, we recall the way  $a$  was calculated

$$z_k^{[l+1]} = b_k^{[l+1]} + \sum_{j=1}^{N^{[l]}} w_{kj}^{[l+1]} \sigma(z_j^{[l]}) \implies \frac{\partial z_k^{[l+1]}}{\partial z_j^{[l]}} = w_{kj}^{[l+1]} \cdot \sigma'(z_j^{[l]}) \quad (45)$$

Now this is where the "back" in backpropagation comes from. Plugging this into the equation yields a final equation for the error term in hidden layers, called the **backpropagation formula**:

$$\delta_j^{[l]} = \sigma'(z_j^{[l]}) \sum_{k=1}^{N^{[l+1]}} \delta_k^{[l+1]} \cdot w_{kj}^{[l+1]} \quad (46)$$

which gives the matrix form

$$\boldsymbol{\delta}^{[l]} = \boldsymbol{\sigma}'(\mathbf{z}^{[l]}) \odot (\mathbf{W}^{[l+1]})^T \boldsymbol{\delta}^{[l+1]} = \begin{bmatrix} \sigma'(z_1^{[l]}) \\ \vdots \\ \sigma'(z_{N^{[l]}}^{[l]}) \end{bmatrix} \odot \begin{bmatrix} w_{11}^{[l+1]} & \dots & w_{N^{[l+1]}1}^{[l+1]} \\ \vdots & \ddots & \vdots \\ w_{1N^{[l]}}^{[l+1]} & \dots & w_{N^{[l+1]}N^{[l]}}^{[l+1]} \end{bmatrix} \begin{bmatrix} \delta_1^{[l+1]} \\ \vdots \\ \delta_{N^{[l+1]}}^{[l+1]} \end{bmatrix} \quad (47)$$

and putting it all together, the partial derivative of the error function  $E_n$  with respect to the weight in the hidden layers for  $1 \leq l < L$  is

$$\frac{\partial E_n}{\partial w_{ji}^{[l]}} = a_i^{[l-1]} \sigma'(z_j^{[l]}) \sum_{k=1}^{N^{[l+1]}} \delta_k^{[l+1]} \cdot w_{kj}^{[l+1]} \quad (48)$$

A little fact is that the time complexity of both forward prop and back prop should be the same, so if you ever notice that the time to compute these two functions scales differently, you're probably making some repeated calculations somewhere.

### Algorithm 1.2 (Epoch of Training)

Before training, we initialize all the parameters to be

$$\boldsymbol{\theta} = (\mathbf{W}^{[1]}, \mathbf{b}^{[1]}, \mathbf{W}^{[2]}, \dots, \mathbf{W}^{[L]}, \mathbf{b}^{[L]}) \quad (49)$$

Then, we repeat the following for one epoch of training.

1. *Choose Batch*: We choose an arbitrary data point  $(\mathbf{x}^{(n)}, \mathbf{y}^{(n)})$ , a minibatch, or the entire batch to compute the gradients on.
2. *Forward Propagation*: Apply input vector  $\mathbf{x}^{(n)}$  and use forward propagation to compute the values of all the hidden and activation units

$$\mathbf{a}^{[0]} = \mathbf{x}^{(n)}, \mathbf{z}^{[1]}, \mathbf{a}^{[1]}, \dots, \mathbf{z}^{[L]}, \mathbf{a}^{[L]} = h_{\boldsymbol{\theta}}(\mathbf{x}^{(n)}) \quad (50)$$

3. *Back Propagation*:

- (a) Evaluate the  $\boldsymbol{\delta}^{[l]}$ 's starting from the back with the formula

$$\boldsymbol{\delta}^{[L]} = \left( \frac{\partial \mathbf{g}}{\partial \mathbf{z}^{[L]}} \right)^T \left( \frac{\partial E_n}{\partial \mathbf{a}^{[L]}} \right) \quad (51)$$

$$\boldsymbol{\delta}^{[l]} = \boldsymbol{\sigma}'(\mathbf{z}^{[l]}) \odot (\mathbf{W}^{[l+1]})^T \boldsymbol{\delta}^{[l+1]} \quad l = 1, \dots, L-1 \quad (52)$$

where  $\frac{\partial \mathbf{g}}{\partial \mathbf{z}^{[L]}}$  can be found by taking the derivative of the known link function, and the rest of the terms are found by forward propagation (these are all functions which have been fixed in value by inputting  $\mathbf{x}^{(n)}$ ).

(b) Calculate the derivatives of the error as

$$\frac{\partial E_n}{\partial \mathbf{W}^{[l]}} = \boldsymbol{\delta}^{[l]} (\mathbf{a}^{[l-1]})^T, \quad \frac{\partial E_n}{\partial \mathbf{b}^{[l]}} = \boldsymbol{\delta}^{[l]} \quad (53)$$

4. *Gradient Descent*: Subtract the derivatives with step size  $\alpha$ . That is, for  $l = 1, \dots, L$ ,

$$\mathbf{W}^{[l]} = \mathbf{W}^{[l]} - \alpha \frac{\partial E_n}{\partial \mathbf{W}^{[l]}}, \quad \mathbf{b}^{[l]} = \mathbf{b}^{[l]} - \alpha \frac{\partial E_n}{\partial \mathbf{b}^{[l]}} \quad (54)$$

The specific optimizer can differ, e.g. Adam, SGD, BFGS, etc., but the specific algorithm won't be covered here. It is common to use Adam, since it usually works better. If we can afford to iterate over the entire batch, L-BFGS may also be useful.

### Code 1.2 (Neural Net from Scratch)

Now it's time to implement what most newcomers fear most: a neural net from scratch using only numpy. Doing this will get you to understand the inner workings of a neural net, and you can find the relevant code here.

### Code 1.3 (Pytorch Implementation of Forward and Backward Propagation)

Once you have finished implementing from scratch, you can now use the PyTorch API to access the same model weights. The code here shows how to look at the forward propagation and backpropagation steps in PyTorch in intermediate layers and shows the backend behind storing gradients.

## 1.5 Overparameterization is Good?

Given that the input dimension is  $D$ , say that all the hidden layers are of dimension  $D$  and we have  $L$  layers. Then, we are storing a matrix (plus bias vector) at each layer, resulting in a scaling of  $O(D^2L)$ . This quadratic scaling leads to overparameterized models, which should raise a red flag. This naturally leads to overfitting, but a strange phenomenon occurs.<sup>6</sup>

1. In the beginning, the training loss goes down along with the validation loss.
2. Soon the validation loss starts to go up while the training loss goes down, leading to overfitting.
3. The overfitting is worst when the training loss is 0.
4. At this point, the training loss remains at 0, but generalization starts to improve, and mysteriously the validation loss starts going down.

There are many theories of why the last step ever happens. To interpret this, let's revisit what overfitting means. It means that small perturbations of the inputs will result in large variances in the outputs. If we generalize well,  $x + \epsilon$  should also result in  $f(x) + O(\epsilon)$ . Therefore, this means that the more parameters it has, the better this stability is and therefore the more robust the model. How should we measure this sense of stability? In analysis, a metric to assess the robustness of a deep neural net  $f_\theta : \mathbb{R}^n \rightarrow \mathbb{R}^m$  is its Lipschitz constant, which effectively bounds how much  $f$  can change given some change in  $x$ .

### Definition 1.7 (Lipschitz Continuity)

A function  $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$  is called **Lipschitz continuous** if there exists a constant  $L$  such that for all  $x, y \in \mathbb{R}^n$

$$\|f(x) - f(y)\|_2 \leq L\|x - y\|_2 \quad (55)$$

<sup>6</sup>I found this from Lex Fridman's podcast with Ilya Sutskever.

and the smallest  $L$  for which the inequality is true is called the **Lipschitz constant**, denoted  $\text{Lip}(f)$ .

### Theorem 1.3 (Lipschitz Upper Bound with Operator Norm of Total Derivative)

If  $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$  is Lipschitz continuous, then

$$\text{Lip}(f) = \sup_{x \in \mathbb{R}^n} \|D_x f\|_{\text{op}} \quad (56)$$

where  $\|\cdot\|_{\text{op}}$  is the operator norm of a matrix. In particular, if  $f$  is scalar-valued, then its Lipschitz constant is the maximum norm of its gradient on its domain

$$\text{Lip}(f) = \sup_{x \in \mathbb{R}^n} \|\nabla f(x)\|_2 \quad (57)$$

The above theorem makes sense, since indeed the stability of the function should be equal to the stability of its "maximum" linear approximation  $D_x f$ .

### Theorem 1.4 (Lipschitz Upper Bound for MLPs)

It has already been shown that for a  $K$ -layer MLP

$$h_\theta(\mathbf{x}) := \mathbf{T}_K \circ \rho_{K-1} \circ \mathbf{T}_{K-1} \circ \cdots \circ \rho_1 \circ \mathbf{T}_1(\mathbf{x}) \quad (58)$$

the Lipschitz constant for an affine map  $\mathbf{T}_k(\mathbf{x}) = M_k \mathbf{x} + b_k$  is simply the operator norm (largest singular value) of  $M_k$ , while that of an activation function is always bounded by some well-known constant, usually 1. So, the Lipschitz constant of the entire composition  $h$  is simply the product of all operator norms of  $M_k$ .

What about  $K$ -computable functions in general? That is, given a function  $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$  with

$$v_0(\mathbf{x}) = \mathbf{x} \quad (59)$$

$$v_1(\mathbf{x}) = g_1(v_0(\mathbf{x})) \quad (60)$$

$$v_2(\mathbf{x}) = g_2(v_0(\mathbf{x}), v_1(\mathbf{x})) \quad (61)$$

$$\dots = \dots \quad (62)$$

$$v_k(\mathbf{x}) = g_k(v_0(\mathbf{x}), v_1(\mathbf{x}), \dots, v_{k-1}(\mathbf{x})) \quad (63)$$

$$\dots = \dots \quad (64)$$

$$v_K(\mathbf{x}) = g_K(v_0(\mathbf{x}), v_1(\mathbf{x}), \dots, v_{K-2}(\mathbf{x}), v_{K-1}(\mathbf{x})) \quad (65)$$

where  $v_k : \mathbb{R}^n \rightarrow \mathbb{R}^{n_k}$ , with  $n_0 = n$  and  $n_K = m$ , and

$$g_k : \prod_{i=0}^{k-1} \mathbb{R}^{n_i} \rightarrow \mathbb{R}^{n_k} \quad (66)$$

To differentiate  $v_k$  w.r.t.  $\mathbf{x}$ , we can use the chain rule, resulting in the total derivative

$$\underbrace{\frac{\partial v_k}{\partial \mathbf{x}}}_{n_k \times n} = \sum_{i=1}^{k-1} \underbrace{\frac{\partial g_k}{\partial v_i}}_{n_k \times n_i} \underbrace{\frac{\partial v_i}{\partial \mathbf{x}}}_{n_i \times n} \quad (67)$$

Therefore, it is this Lipschitz property that might entail how stable an MLP is. We have seen from the universal approximation theorems that for a data set of any size, we can always fit a one-layer perceptron

that perfectly fits through all of them, given that the layer is large enough. In these cases, we are interested in fitting the data *smoothly*, and theoretical research in bounding the Lipschitz constant is popular.

In practice this behavior is reflected in *most* cases, but they may be very sensitive in some cases, which we call *adversarial examples*. Adversarial examples take advantage of this weakness by adding carefully chosen perturbations that drastically change the output of the network. Adversarial machine learning attempts to study these weaknesses and hopefully use them to create more robust models. It is natural to expect that the precise configuration of the minimal necessary perturbations is a random artifact of the normal variability that arises in different runs of backpropagation learning. Yet, it has been found that adversarial examples are relatively robust, and are shared by neural networks with varied number of layers, activations or trained on different subsets of the training data. This suggest that the deep neural networks that are learned by backpropagation have *intrinsic* blind spots, whose structure is connected to the data distribution in a non-obvious way.

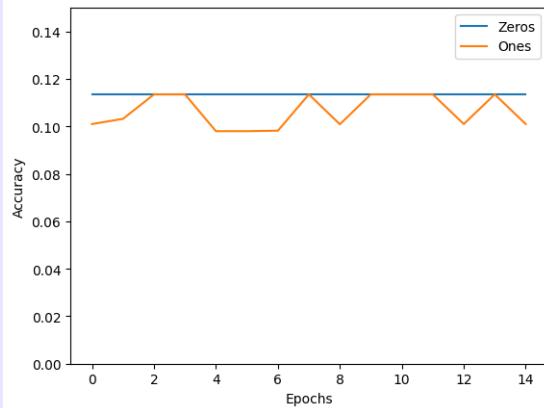
## 1.6 Engineering Heuristics

### 1.6.1 Weight Initialization

The way that we initialize our weights can have a huge impact on our training performance. Imagine that you are creating the first neural network and you want to decide how to initialize it. You may consider many different cases.

#### Example 1.5 (Constant Initialization)

You may first think of initializing everything to 0 or 1, which is the simplest. Let's run this, but we can already see by epoch 15 that we have some problems.



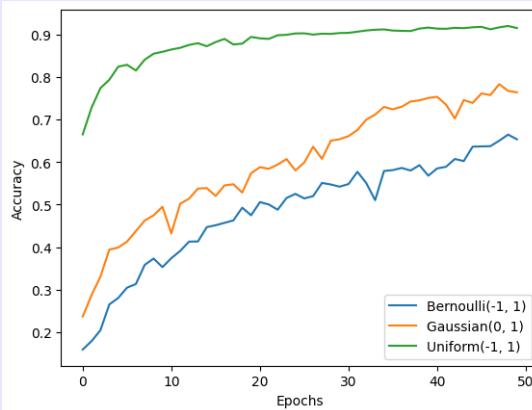
Clearly, this is not good, and theoretically this makes sense since it means all our activations are going to be the same, and thus all our gradients will be the same, meaning that updates will be the same for every weight, which is not good mixing. We can see this below:

#### Example 1.6 (Random Initialization with High Variance)

Okay, this didn't work, so perhaps you think it would be a good idea have more randomness to the initialization so that all the weights aren't exactly one number. You could think of initializing everything with three distinct schemes:

1. Randomly initialize everything to be  $-1$  or  $1$  with equal probability.
2. Randomly initialize everything to be a Gaussian random variable with standard deviation  $1$ .
3. Randomly initialize everything to be a uniform random variable between  $-1$  and  $1$ .

Running the experiments give the following.

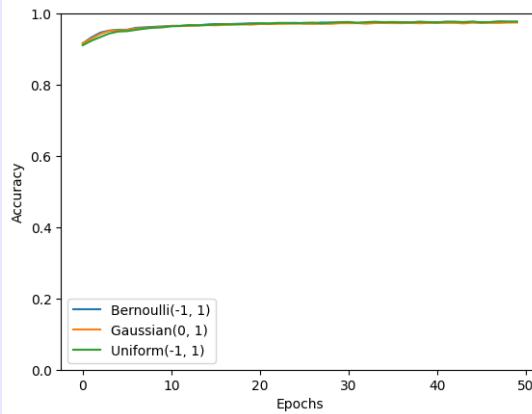


However, this is also not good since it means that the activations will be very large, and thus the gradients will be very large, and so the updates will be very large. This is not good since it means that the weights will be jumping around a lot, and we won't be able to converge. Furthermore, depending on what activations we choose, e.g. tanh or sigmoid, very large activations may saturate the gradients and kill the learning.

### Example 1.7 (Random Initialization with Low Variance)

This improves the next problem but now you want to fix the situation of the gradients being too big. Therefore, you should initialize the parameters to be smaller values, but not so small that they are zeros and we have the same problem as before. We use improved schemes:

1. Randomly initialize everything to be  $-0.1$  or  $0.1$  with equal probability.
2. Randomly initialize everything to be a Gaussian random variable with standard deviation  $0.1$ .
3. Randomly initialize everything to be a uniform random variable between  $-0.1$  and  $0.1$ .



Through out experiments, we have learned that a good rule of thumb for initializing weights is to make them small and uniformly random without being too small. While it is harder to get better than this for MNIST, a slightly better approach is Xavier initialization, which builds upon our same ideas.

### Definition 1.8 (Xavier Initialization)

The **Xavier initialization** simply initializes each weight as a uniform distribution, with its range dependent on the size of the input.

$$w_{ij}^{[l]} \sim U\left(-\frac{1}{\sqrt{N^{[l-1]}}}, \frac{1}{\sqrt{N^{[l-1]}}}\right) \quad (68)$$

where  $N^{[l-1]}$  is the number of neurons in the previous layer. This is a good rule of thumb for the weights, but the biases can be initialized to 0 (though they are also initialized uniformly by default).

#### Code 1.4 (Experimenting with Weight Initializations)

The code used for generating the figures can be found [here](#).

### 1.6.2 Activation Functions

The choice of the activation function can have a significant impact on your training, and we will describe a few examples below. The first thing to note is that we must ensure that there is a nonzero gradient almost everywhere. If, for example, we had a piecewise constant activation function, the gradient is 0 almost everywhere, and it would kill the gradient of the entire network. In the early days of deep learning, researchers used the probability-inspired sigmoid and tanh functions as the main source of nonlinearity. Let's go over them below.

#### Definition 1.9 (Sigmoid)

Sigmoid activations are historically popular since they have a nice interpretation as a saturating “fire rate” of a neuron. However, there are 3 problems:

1. The saturated neurons “kill” the gradients, since if the input at any one point in the layers is too positive or negative, the gradient will vanish, making very small updates. This is known as the **vanishing gradient problem**. Therefore, the more layers a neural network has, the more likely we are to see this vanishing gradient problem.
2. Sigmoid functions are not zero centered (i.e. its graph doesn’t cross the point  $(0, 0)$ ). Consider what happens when the input  $x$  to a neuron is always positive. Then, the sigmoid  $f$  will have a gradient of

$$f\left(\sum_i w_i x_i + b\right) \Rightarrow \frac{\partial f}{\partial w_i} = f'\left(\sum_i w_i x_i + b\right) x_i \quad (69)$$

which means that the gradients  $\nabla_w f$  will always have all positive elements or all negative elements, meaning that we will be restricted to moving in certain nonoptimal directions when updating our parameters.

#### Definition 1.10 (Hyperbolic Tangent)

The hyperbolic tangent is zero centered, which is nice, but it still squashes numbers to range  $[-1, 1]$  and therefore kills the gradients when saturated.

It turns out that these two activations were ineffective in deep learning due to saturation. A less probability inspired activation was the ReLU, which showed better generalization and speed of convergence.

#### Definition 1.11 (Rectified Linear Unit)

The ReLU function has the following properties:

1. It does not saturate in the positive region.
2. It is very computationally efficient (and the fact that it is nondifferentiable at one point doesn’t really affect computations).
3. It converges much faster than sigmoid/tanh in practice.
4. However, note that if the input is less than 0, then the gradient of the ReLU is 0. Therefore, if we input a vector that happens to have all negative values, then the gradient would vanish and we wouldn’t make any updates. These ReLU “dead zones” can be a problem since it will never

activate and never update, which can happen if we have bad initialization. A more common case is when your learning rate is too high, and the weights will jump off the data manifold.

Unfortunately, the ReLU had some weaknesses, mainly being the *dying ReLU*, which is when the ReLU is stuck in the negative region and never activates. This is a problem since the gradient is 0 in the negative region, and so the weights will never update. Therefore, some researchers have proposed some modifications to the ReLU.

#### Definition 1.12 (Leaky ReLU)

The leaky ReLU

$$\sigma(x) = \max\{0.01x, x\} \quad (70)$$

does not saturate (i.e. gradient will not die), is computationally efficient, and converges much faster than sigmoid/tanh in practice. We can also parameterize it with  $\alpha$  and have the neural net optimize  $\alpha$  along with the weights.

$$\sigma(x) = \max\{\alpha x, x\} \quad (71)$$

#### Definition 1.13 (ELU)

The exponential linear unit has all the benefits of ReLU, with closer to mean outputs. It has a negative saturation regime compared with leaky ReLU, but it adds some robustness to noise.

$$\sigma(x) = \begin{cases} x & \text{if } x > 0 \\ \alpha(\exp x - 1) & \text{if } x \leq 0 \end{cases} \quad (72)$$

#### Definition 1.14 (SELU)

The scaled exponential linear unit is a self-normalizing activation function, which means that it preserves the mean and variance of the input. This is useful for deep networks, since the mean and variance of the input will be preserved through the layers. Its formula is

$$\sigma(x) = \lambda \begin{cases} x & \text{if } x > 0 \\ \alpha(\exp x - 1) & \text{if } x \leq 0 \end{cases} \quad (73)$$

where  $\lambda$  and  $\alpha$  are constants.

Later on, some further modifications were made, such as the **Swish** and the **Mish** [Mis20] activation functions. These functions have a distinctive negative concavity, unlike ReLU, which accounts for preservation of small negative weights.

#### Definition 1.15 (Swish)

The Swish activation function is defined as

$$\sigma(x) = x \cdot \sigma(\beta x) \quad (74)$$

where  $\beta$  is a parameter that can be learned.

**Definition 1.16 (Mish)**

The Mish activation function is defined as

$$\sigma(x) = x \cdot \tanh(\ln(1 + \exp(x))) \quad (75)$$

**Code 1.5 (Generating Graphs)**

Code used to generate these graphs are here.

## 1.7 Datasets and Dataloaders

For here, we will go over some of the main datasets that are used in deep learning.

**Definition 1.17 (MNIST and Fashion MNIST)**

The MNIST dataset consists of 60k training images and 10k test images of handwritten digits. The Fashion MNIST dataset consists of 60k training images and 10k test images of clothing items. These are considered quite easy with the basic benchmarks:

1. Linear classifiers can reach past 90% accuracy.
2. A 2 layer MLP can reach up to 97% accuracy.
3. A CNN can reach up to 99% accuracy.

**Definition 1.18 (CIFAR10 and CIFAR 100)**

The CIFAR10 dataset consists of 60k 32x32 color images in 10 classes, with 6k images per class. The CIFAR100 dataset consists of 60k 32x32 color images in 100 classes, with 600 images per class. These are considered quite hard with the basic benchmarks:

1. Linear classifiers can reach past 40% accuracy.
2. A 2 layer MLP can reach up to 60% accuracy.
3. A CNN can reach up to 80% accuracy.

**Definition 1.19 (ImageNet)**

The ImageNet dataset, created at Stanford by Fei-Fei Li [DDS<sup>+</sup>09], consists of 1.2 million training images and 50k validation images in 1000 classes. This is considered very hard with the basic benchmarks.

Creating your own custom dataset with spreadsheets or images is easy.<sup>7</sup> Loading it to a dataloader that shuffles and outputs minibatches of data is trivial. However, when doing so, you should pay attention to a couple things.

1. Batch size: The dataloader stores the dataset (which can be several hundred GBs) in the drive, and extracts batches into memory for processing. You should set your batch sizes so that they can fit into the GPU memory, which is often smaller than the CPU memory.

<sup>7</sup>[https://pytorch.org/tutorials/beginner/data\\_loading\\_tutorial.html](https://pytorch.org/tutorials/beginner/data_loading_tutorial.html)

## 1.8 Exercises

### Exercise 1.1 (Tarokh, ECE685 2021 Midterm 1.1)

Let  $x \in \mathbb{R}$  denote a random variable with the following *cumulative distribution function*

$$F(x) = \exp\left(-\exp\left(-\frac{x-\mu}{\beta}\right)\right) \quad (76)$$

where  $\mu$  and  $\beta > 0$  denote the location and scale parameters, respectively. Let  $\mathcal{D} = \{x_1, \dots, x_n\}$  be a set of  $n$  iid observations of  $x$ .

1. Write an equation for a cost function  $L(\mu, \beta \mid \mathcal{D})$  whose minimization gives the maximum likelihood estimates for  $\mu$  and  $\beta$ .
2. Compute the derivatives of  $L(\mu, \beta \mid \mathcal{D})$  with respect to  $\mu$  and  $\beta$  and write a system of equations whose solution gives the MLEs of  $\mu$  and  $\beta$ .

### Solution 1.1

We can derive the PDF of the observation as

$$f(x; \mu, \beta) = \frac{dF(x)}{dx} = \frac{1}{\beta} \exp\left\{-\left(\frac{x-\mu}{\beta} + \exp\left(-\frac{x-\mu}{\beta}\right)\right)\right\} \quad (77)$$

and the likelihood is then

$$L(\mu, \beta \mid \mathcal{D}) = \prod_{i=1}^N \frac{1}{\beta} \exp\left\{-\left(\frac{x^{(i)}-\mu}{\beta} + \exp\left(-\frac{x^{(i)}-\mu}{\beta}\right)\right)\right\} \quad (78)$$

Rather than maximizing this likelihood, we minimize the negative log of it, defined as

$$\ell(\mu, \beta \mid \mathcal{D}) = -\ln L(\mu, \beta \mid \mathcal{D}) = N \ln \beta + \frac{\sum_i x^{(i)} - N\mu}{\beta} + \sum_{i=1}^N \exp\left(-\frac{x^{(i)}-\mu}{\beta}\right) \quad (79)$$

The derivatives of  $\ell$  can be computed simply by using the derivative rules.

$$\frac{\partial \ell}{\partial \mu} = -\frac{N}{\beta} + \frac{1}{\beta} \sum_{i=1}^N \exp\left(-\frac{x^{(i)}-\mu}{\beta}\right) \quad (80)$$

$$\frac{\partial \ell}{\partial \beta} = \frac{N}{\beta} - \frac{\sum_i x^{(i)} - N\mu}{\beta^2} + \frac{1}{\beta^2} \sum_{i=1}^N (x^{(i)} - \mu) \exp\left(-\frac{x^{(i)}-\mu}{\beta}\right) \quad (81)$$

and so the MLE estimates that minimizes  $\ell$  can be found by setting the equations above equal to 0.

### Exercise 1.2 (ECE 685 Fall 2021 Midterm 1.2)

The figure depicts a simple neural network with one hidden layer. The inputs to the network are denoted by  $x_1, x_2, x_3$ , and the output is denoted by  $y$ . The activation functions of the neurons in the hidden layer are given by  $h_1(z) = \sigma(z)$ ,  $h_2(z) = \tanh(z)$ , and the output unit activation function is  $g(z) = z$ , where  $\sigma(z) = \frac{1}{1+\exp(-z)}$  and  $\tanh(z) = \frac{\exp(z)-\exp(-z)}{\exp(z)+\exp(-z)}$  are the logistic sigmoid and hyperbolic tangent, respectively. The biases  $b_1, b_2$  are added to the inputs of the neurons in the hidden layer before passing them through the activation functions. let

$$\mathbf{w} = (b_1, b_2, w_{11}^{(1)}, w_{12}^{(1)}, w_{21}^{(1)}, w_{31}^{(1)}, w_{32}^{(1)}, w_1^{(2)}, w_2^{(2)}) \quad (82)$$

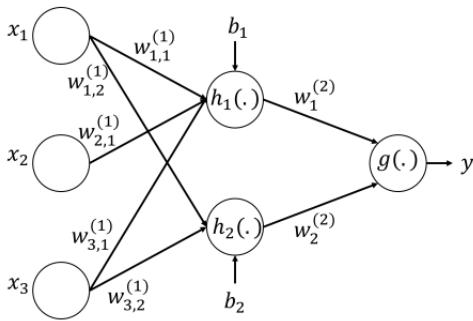
denote the vector of network parameters.

1. Write the input output relation  $y = f(x_1, x_2, x_3; \mathbf{w})$  in explicit form.
2. Let  $\mathcal{D} = \{(x_{1,n}, x_{2,n}, x_{3,n})\}$  denote a training dataset of  $N$  points where  $y_n \in \mathbb{R}$  are labels of the corresponding data points. We want to estimate the network parameters  $\mathbf{w}$  using  $\mathcal{D}$  by minimizing the mean squared error loss

$$L(\mathbf{w}) = \frac{1}{2} \sum_{n=1}^N (f(x_{1,n}, x_{2,n}, x_{3,n}; \mathbf{w}) - y_n)^2 \quad (83)$$

Compute the gradient of  $L(\mathbf{w})$  with respect to the network parameters  $\mathbf{w}$ .

3. Write pseudo code for one iteration for minimizing  $L(\mathbf{w})$  with respect to the network parameters  $\mathbf{w}$  using SGD with learning rate  $\eta > 0$ .



## Solution 1.2

We can write the computation graph as

$$z_1^{(1)} = w_{11}^{(1)} x_1 + w_{21}^{(1)} x_2 + w_{31}^{(1)} x_3 + b_1 \quad (84)$$

$$z_2^{(1)} = w_{12}^{(1)} x_1 + w_{32}^{(1)} x_3 + b_2 \quad (85)$$

$$a_1^{(1)} = \sigma(z_1^{(1)}) \quad (86)$$

$$a_2^{(1)} = \tanh(z_2^{(1)}) \quad (87)$$

$$z^{(2)} = w_1^{(2)} a_1^{(1)} + w_2^{(2)} a_2^{(1)} \quad (88)$$

$$y = a^{(2)} = g(z^{(2)}) \quad (89)$$

and composing these gives

$$y = w_1^{(2)} \sigma(w_{11}^{(1)} x_1 + w_{21}^{(1)} x_2 + w_{31}^{(1)} x_3 + b_1) + w_2^{(2)} \tanh(w_{12}^{(1)} x_1 + w_{32}^{(1)} x_3 + b_2) \quad (90)$$

The gradient of the network can be written as

$$\nabla_{\mathbf{w}} L(\mathbf{w}) = \frac{1}{2} \sum_{n=1}^N \nabla_{\mathbf{w}} (f(x_{1,n}, x_{2,n}, x_{3,n}; \mathbf{w}) - y_n)^2 \quad (91)$$

$$= \sum_{n=1}^N (f(x_{1,n}, x_{2,n}, x_{3,n}; \mathbf{w}) - y_n) \nabla_{\mathbf{w}} f(x_{1,n}, x_{2,n}, x_{3,n}) \quad (92)$$

where

$$\nabla_{\mathbf{w}} f(x_{1,n}, x_{2,n}, x_{3,n}) = \left. \frac{\partial f}{\partial \mathbf{w}} \right|_{\mathbf{x}=\mathbf{x}^{(n)}} \quad (93)$$

Now we can take derivatives using chain rule, working backwards, and using the derivative identities

$\sigma'(z) = \sigma(z)(1 - \sigma(z))$  and  $\tanh'(z) = 1 - \tanh^2(z)$ .

$$\frac{\partial f}{\partial w_1^{(2)}} = \frac{\partial f}{\partial z^{(2)}} \frac{\partial z^{(2)}}{\partial w_1^{(2)}} = a_1^{(1)} \quad (94)$$

$$\frac{\partial f}{\partial w_2^{(2)}} = \frac{\partial f}{\partial z^{(2)}} \frac{\partial z^{(2)}}{\partial w_2^{(2)}} = a_2^{(1)} \quad (95)$$

$$\frac{\partial f}{\partial w_{11}^{(1)}} = \frac{\partial f}{\partial z^{(2)}} \frac{\partial z^{(2)}}{\partial a_1^{(1)}} \frac{\partial a_1^{(1)}}{\partial z_1^{(1)}} \frac{\partial z_1^{(1)}}{\partial w_{11}^{(1)}} = w_1^{(2)} a_1^{(1)} (1 - a_1^{(1)}) x_1 \quad (96)$$

$$\frac{\partial f}{\partial w_{21}^{(1)}} = \frac{\partial f}{\partial z^{(2)}} \frac{\partial z^{(2)}}{\partial a_1^{(1)}} \frac{\partial a_1^{(1)}}{\partial z_1^{(1)}} \frac{\partial z_1^{(1)}}{\partial w_{21}^{(1)}} = w_1^{(2)} a_1^{(1)} (1 - a_1^{(1)}) x_2 \quad (97)$$

$$\frac{\partial f}{\partial w_{31}^{(1)}} = \frac{\partial f}{\partial z^{(2)}} \frac{\partial z^{(2)}}{\partial a_1^{(1)}} \frac{\partial a_1^{(1)}}{\partial z_1^{(1)}} \frac{\partial z_1^{(1)}}{\partial w_{31}^{(1)}} = w_1^{(2)} a_1^{(1)} (1 - a_1^{(1)}) x_3 \quad (98)$$

$$\frac{\partial f}{\partial b_1} = \frac{\partial f}{\partial z^{(2)}} \frac{\partial z^{(2)}}{\partial a_1^{(1)}} \frac{\partial a_1^{(1)}}{\partial z_1^{(1)}} \frac{\partial z_1^{(1)}}{\partial b_1} = w_1^{(2)} a_1^{(1)} (1 - a_1^{(1)}) \quad (99)$$

$$\frac{\partial f}{\partial w_{12}^{(1)}} = \frac{\partial f}{\partial z^{(2)}} \frac{\partial z^{(2)}}{\partial a_2^{(1)}} \frac{\partial a_2^{(1)}}{\partial z_2^{(1)}} \frac{\partial z_2^{(1)}}{\partial w_{12}^{(1)}} = w_2^{(2)} (1 - (a_2^{(1)})^2) x_1 \quad (100)$$

$$\frac{\partial f}{\partial w_{13}^{(1)}} = \frac{\partial f}{\partial z^{(2)}} \frac{\partial z^{(2)}}{\partial a_2^{(1)}} \frac{\partial a_2^{(1)}}{\partial z_2^{(1)}} \frac{\partial z_2^{(1)}}{\partial w_{13}^{(1)}} = w_2^{(2)} (1 - (a_2^{(1)})^2) x_3 \quad (101)$$

$$\frac{\partial f}{\partial b_2} = \frac{\partial f}{\partial z^{(2)}} \frac{\partial z^{(2)}}{\partial a_2^{(1)}} \frac{\partial a_2^{(1)}}{\partial z_2^{(1)}} \frac{\partial z_2^{(1)}}{\partial b_2} = w_2^{(2)} (1 - (a_2^{(1)})^2) \quad (102)$$

To compute one step of SGD, we must first choose a minibatch  $\mathcal{M} \subset \mathcal{D}$  and then compute

$$\nabla_{\mathbf{w}; \mathcal{M}} L(\mathbf{w}) = \sum_{(\mathbf{x}, y) \in \mathcal{M}} (f(\mathbf{x}; \mathbf{w}) - y) \nabla_{\mathbf{w}} f(\mathbf{x}) \quad (103)$$

where we compute the gradient simply over the minibatch. Then, we update the parameters according to

$$\mathbf{w} = \mathbf{w} - \eta \nabla_{\mathbf{w}; \mathcal{M}} L(\mathbf{w}) \quad (104)$$

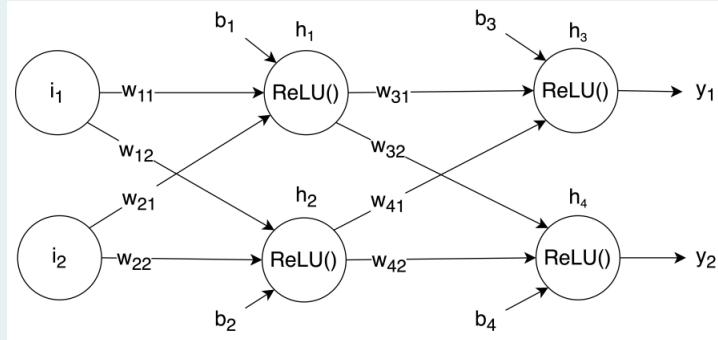
### Exercise 1.3 (ECE 685 Fall 2021 Midterm 1.3)

Given the following neural network with 2 inputs  $(x_1, x_2)$ , fully-connected layers and ReLU activations. The weights and biases of hidden units are denoted  $w$  and  $b$ , with  $h$  as activation units. For example,

$$h_1 = \text{ReLU}(x_1 w_{11} + x_2 w_{21} + b_1) \quad (105)$$

The outputs are denoted as  $(y_1, y_2)$  and the ground truth targets are denoted as  $(t_1, t_2)$ .

$$y_1 = \text{ReLU}(h_1 w_{31} + h_2 w_{41} + b_3) \quad (106)$$



The values of the variables are given as follows:

$i_1$	$i_2$	$w_{11}$	$w_{12}$	$w_{21}$	$w_{22}$	$w_{31}$	$w_{32}$	$w_{41}$	$w_{42}$	$b_1$	$b_2$	$b_3$	$b_4$	$t_1$	$t_2$
1	2	1	0.5	-0.5	1	0.5	-2	-1	0.5	-0.5	-0.5	1	1	2	4

1. Compute the output  $(y_1, y_2)$  of the input  $(x_1, x_2)$  using the network parameters as specified above.
2. Compute the mean squared error of the computed output and the target labels.
3. Using the calculated MSE, update the weight  $w_{31}$  using GD with  $\eta = 0.01$ .
4. Do the same with weight  $w_{42}$ .
5. Do the same with weight  $w_{22}$ .

## 2 Training and Control

### 2.1 Early Stopping

Since neural networks are overparameterized, it makes sense that given enough training time, they will overfit to the training set. Therefore, you must stop training when the validation loss starts to decrease. This simple method is known as **early stopping**.

### 2.2 L1 and L2 Regularization

Another way to regularize is by simply adding in a L1 or L2 regularization term.

Sometimes, it may not always be the best idea to regularize a neural net equally through all weights. For example, weights which may be deeper down the forward pass may focus on more high level features and therefore should be regularized differently than those that are close to the input. Other types of regularization, such as Fiedler regularization [TD20] focuses on preserving the graph structure of the weights.

### 2.3 Dropout

Overfitting is always a problem. With unlimited computation, the best way to regularize a fixed-sized model is to average the predictions of all possible settings of the parameters, weighting each setting by its posterior probability given the training the data. However, this is computationally expensive and cannot be done for moderately complex models.

The dropout method introduced by [SHK<sup>+</sup>14], addresses this issue. We literally drop out some features (not the weights!) before feeding them to the next layer by setting some activation functions to 0. Given a neural net of  $N$  total nodes, we can think of the set of its  $2^N$  thinned subnetworks. For each training minibatch, a new thinned network is sampled and trained.

At each layer, recall that forward prop is basically

$$\begin{aligned}\mathbf{z}^{[l+1]} &= \mathbf{W}^{[l+1]} \mathbf{a}^{[l]} + \mathbf{b}^{[l+1]} \\ \mathbf{a}^{[l+1]} &= \sigma(\mathbf{z}^{[l+1]})\end{aligned}$$

Now what we do with dropout is

$$\begin{aligned}r_j^{[l]} &\sim \text{Bernoulli}(p) \\ \tilde{\mathbf{a}}^{[l]} &= \mathbf{r}^{[l]} \odot \mathbf{a}^{[l]} \\ \mathbf{z}^{[l+1]} &= \mathbf{W}^{[l+1]} \tilde{\mathbf{a}}^{[l]} + \mathbf{b}^{[l+1]} \\ \mathbf{a}^{[l+1]} &= \sigma(\mathbf{z}^{[l+1]})\end{aligned}$$

Basically we sample a vector of 0s and 1s from a multivariate Bernoulli distribution. We element-wise multiply it with  $\mathbf{a}^{[l]}$  to create the thinned output  $\tilde{\mathbf{a}}^{[l]}$ . In test time, we do not want the stochasticity of having to set some activation functions to 0. That is, consider the neuron  $\mathbf{a}^{[l]}$  and the random variable  $\tilde{\mathbf{a}}^{[l]}$ . The expected value of  $\mathbf{z}^{[l+1]}$  is

$$\mathbb{E}[\mathbf{z}^{[l+1]}] = \mathbb{E}[\mathbf{W}^{[l+1]} \tilde{\mathbf{a}}^{[l]} + \mathbf{b}^{[l+1]}] = \mathbb{E}[\mathbf{W}^{[l+1]} \tilde{\mathbf{a}}^{[l]}] = p \mathbb{E}[\mathbf{W}^{[l+1]} \mathbf{a}^{[l]}]$$

and to make sure that the output at test time is the same as the expected output at training time, we want to multiply the weights by  $p$ :  $W_{\text{test}}^{[l]} = p W_{\text{train}}^{[l]}$ . Another way is to use **inverted dropout**, where we can divide by  $p$  in the training stage and keep the testing method the same.

#### Code 2.1 ()

The code here shows how to implement dropout in PyTorch, which uses dropout layers.

## 2.4 Data Augmentation

It is well known that having more training data helps with overfitting, and so we may be able to perform basic transformations to our current data to artificially generate more training data. For example, if we have images, then we can flip, crop, translate, rotate, stretch, shear, and lens-distort these images with the same label.

## 2.5 Normalization Layers

Just like how we have to normalize our data before we input into a linear model, it may help to normalize the outputs of one layer of a neural net before we input it into the next layer. This is an engineer's method to help with the training process. There are two ways that we can generally normalize data. First is to normalize each sample, known as **layer normalization**, and the other way is to normalize the samples over the batch.

### Definition 2.1 (Layer Norm)

Given some batched output data  $X \in \mathbb{R}^{b \times d}$ , where  $b$  represents the batch size and  $d = d_1 \times \dots \times d_k$  the dimension of each sample, we can normalize each  $x_i = X_{i,:}$  in the batch with **layer normalization** by

$$x_i \mapsto \frac{x_i - \mathbb{E}[x_i]}{\sqrt{\text{Var}[x_i] + \varepsilon}} \odot \gamma + \beta \quad (107)$$

where  $\gamma, \beta$  are learnable parameters that are the same shape as  $x_i$ . If  $X$  is of dimension  $b \times d$ , we must use `nn.LayerNorm(d)` since these are the sizes of the learnable parameters.

### Example 2.1 (Layer Norm)

The following example shows that each row (sample in batch) is normalized independently from one another.

```

1  ln = nn.LayerNorm(5)
2  x = torch.Tensor(range(10)).reshape(2, 5)
3  print(x)
4  tensor([[0., 1., 2., 3., 4.],
5          [5., 6., 7., 8., 9.]])
6
7  print(ln(x))
8  tensor([[-1.4142, -0.7071,  0.0000,  0.7071,  1.4142],
9          [-1.4142, -0.7071,  0.0000,  0.7071,  1.4142]],
10         grad_fn=<NativeLayerNormBackward0>)

```

This also works for higher dimensions.

```

1  ln = nn.LayerNorm((5, 2))
2  x = torch.Tensor(range(20)).reshape(2, 5, 2)
3  print(x)
4  tensor([[[ 0.,  1.],
5          [ 2.,  3.],
6          [ 4.,  5.],
7          [ 6.,  7.],
8          [ 8.,  9.]],

9          [[10., 11.],
11          [12., 13.],
12          [14., 15.]]])

```

```

13     [16., 17.],
14     [18., 19.]])
15 print(ln(x))
16 tensor([[-1.5667, -1.2185],
17         [-0.8704, -0.5222],
18         [-0.1741,  0.1741],
19         [ 0.5222,  0.8704],
20         [ 1.2185,  1.5667]], grad_fn=<NativeLayerNormBackward0>
21
22     [[-1.5667, -1.2185],
23      [-0.8704, -0.5222],
24      [-0.1741,  0.1741],
25      [ 0.5222,  0.8704],
26      [ 1.2185,  1.5667]]], grad_fn=<NativeLayerNormBackward0>

```

The tunable parameters  $\gamma, \beta$  are indeed the same size. They are initialized to 1s and 0s.

```

1 >>> for k, v in ln.state_dict().items():
2 ...     print(k, v)
3 ...
4 weight tensor([[1., 1.],
5                 [1., 1.],
6                 [1., 1.],
7                 [1., 1.],
8                 [1., 1.]])
9 bias tensor([0., 0.],
10            [0., 0.],
11            [0., 0.],
12            [0., 0.]))
13

```

### Definition 2.2 (Batch Norm)

**Batch normalization** targets each feature over all batches rather than each sample (like columns vs rows). Therefore, given some batched output data  $X \in \mathbb{R}^{b \times d}$ , where  $b$  represents the batch size and  $d = d_1 \times \dots \times d_k$  the dimension of each output, we can normalize each feature  $x_i = X_{:, i \in d}$  by

$$x_i \mapsto \frac{x_i - \mathbb{E}[x_i]}{\sqrt{\text{Var}[x_i] + \varepsilon}} \odot \gamma + \beta \quad (108)$$

where  $\gamma, \beta \in \mathbb{R}^b$  are learnable parameters that are the same size as the batch. There are two types of batch norms implemented in pytorch.

1. If  $X$  has hyperdimension 2 with  $b \times d$ , we use `BatchNorm1d(d)` since we are normalizing over the batch for each feature and we have  $d$  features to normalize.
2. If  $X$  has hyperdimension 3 with  $b \times d_1 \times d_2$ , we use `BatchNorm1d(d_1)`.
3. If  $X$  has hyperdimension 4 with  $b \times d_1 \times d_2 \times d_3$ , we use `BatchNorm2d(d_1)`.

### Example 2.2 (Batch Norm 1D)

We can see that each feature is normalized independently from one another. For 2D,

```

1 >>> bn = nn.BatchNorm1d(5)
2 >>> x = torch.Tensor(range(10)).reshape(2, 5)

```

```

3  >>> print(x)
4  tensor([[0., 1., 2., 3., 4.],
5          [5., 6., 7., 8., 9.]])
6  >>> print(bn(x))
7  tensor([[-1.0000, -1.0000, -1.0000, -1.0000, -1.0000],
8          [ 1.0000,  1.0000,  1.0000,  1.0000,  1.0000]],
9          grad_fn=<NativeBatchNormBackward0>)

```

For 3D inputs,

```

1  >>> bn = nn.BatchNorm1d(5)
2  >>> x = torch.Tensor(range(30)).reshape(2, 5, 3)
3  >>> print(x)
4  tensor([[[ 0.,  1.,  2.],
5          [ 3.,  4.,  5.],
6          [ 6.,  7.,  8.],
7          [ 9., 10., 11.],
8          [12., 13., 14.]],

9          [[15., 16., 17.],
10         [18., 19., 20.],
11         [21., 22., 23.],
12         [24., 25., 26.],
13         [27., 28., 29.]])
15 >>> print(bn(x))
16 tensor([[[[-1.1267, -0.9941, -0.8616],
17           [-1.1267, -0.9941, -0.8616],
18           [-1.1267, -0.9941, -0.8616],
19           [-1.1267, -0.9941, -0.8616],
20           [-1.1267, -0.9941, -0.8616]],

21           [[ 0.8616,  0.9941,  1.1267],
22           [ 0.8616,  0.9941,  1.1267],
23           [ 0.8616,  0.9941,  1.1267],
24           [ 0.8616,  0.9941,  1.1267],
25           [ 0.8616,  0.9941,  1.1267]]], grad_fn=<NativeBatchNo
27 rmBackward0>)

```

### Example 2.3 (Batch Norm 2D)

Here is an example of batch norm 2d. There really isn't a difference between these two methods except the dimension that they take in. That is all.

```

1  >>> bn = nn.BatchNorm2d(5)
2  >>> x = torch.Tensor(range(60)).reshape(2, 5, 3, 2)
3  >>> print(x)
4  tensor([[[[ 0.,  1.],
5             [ 2.,  3.],
6             [ 4.,  5.]],

7             ...,
8             [58., 59.]]]])
9  >>> print(bn(x))
10 tensor([[[[-1.1592, -1.0929],
11           [-1.0267, -0.9605],
12           ...

```

```

13      [ 1.0929,  1.1592]]], grad_fn=<NativeBatchNormBack
14      ward0>

```

## 2.6 Residual Connections

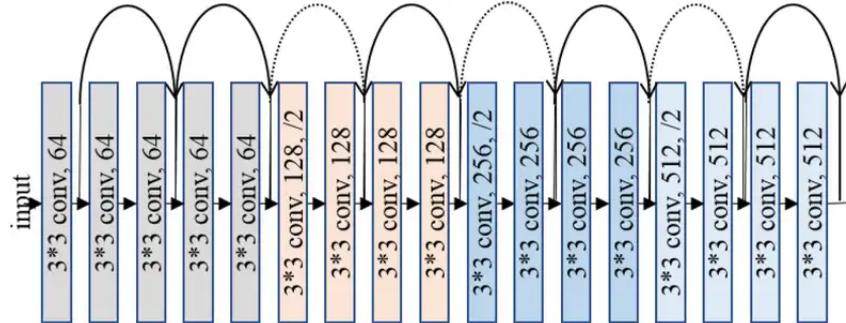


Figure 4: Resnet architecture.

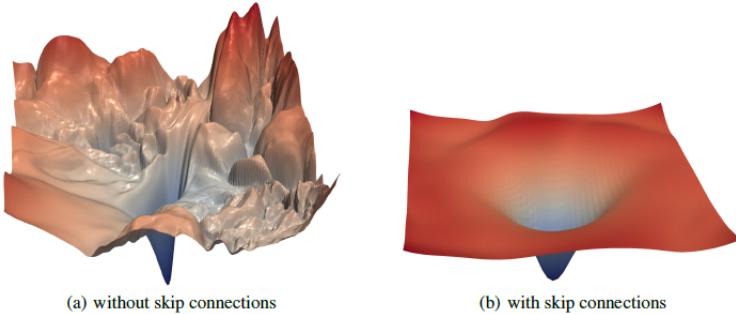


Figure 5: Low-dimensional visual of loss with vs without residual connections.

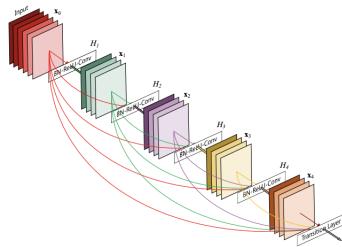
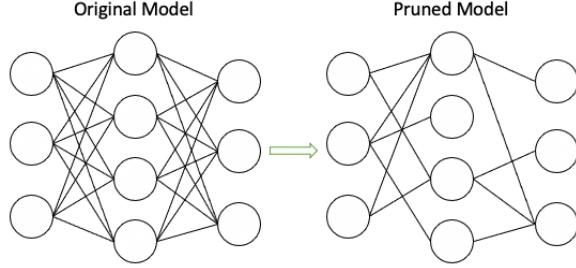


Figure 6: Densenet architecture.

## 2.7 Network Pruning

It can be computationally and memory intensive to train and utilize neural networks. This is where network pruning comes in, which attempts to identify a subnetwork that performs as well as the original. Given a neural net  $f(\mathbf{x}, \boldsymbol{\theta})$  where  $\boldsymbol{\theta} \in \mathbb{R}^M$ , a pruned neural network can be thought of as a subnetwork  $f(\mathbf{x}, \mathbf{m} \odot \boldsymbol{\theta})$ , where  $\mathbf{m}$  is a **mask**, i.e. a vector in  $\{0, 1\}^M$  that, when multiplied component-wise to  $\boldsymbol{\theta}$ , essentially “deletes” a portion of the parameters.



This idea has been around for a long time, and the general method of pruning is as such:

1. We initialize the neural network  $f(\mathbf{x}, \theta_0)$  and train it until we have  $f(\mathbf{x}, \theta)$ .
2. We now prune the network. The most basic pruning scheme is to keep the top  $k\%$  largest weights, since smaller weights do not contribute much to the forward prop, and thus can be ignored.

These pruned networks have been shown to reach accuracies as high as the original network, with equal training progress. Now, if we were to take only this pruned network and train it from the beginning, it will perform as well as the original network, *only under* the condition that we start from the same initialization  $\mathbf{m} \odot \theta$ . If we take this subnetwork and initialize it differently at  $\theta'_0$ , then this subnetwork would not train well. Therefore, the performance of the pruned network is dependent on the initialization!

If we had initialized the full network differently, trained it, and then pruned again, we may have a different subnetwork that will only train well on its own given this new initialization. Therefore, a good initialization is extremely important for training subnetworks. This fact doesn't help much since we can't just take some arbitrary subnetwork and train it since we don't know the good initialization. We must always train the full network, then find the subnetwork, and then find its initialization.

This is essentially the **lottery ticket hypothesis** [FC19], which states that a randomly-initialized, dense neural network contains a subnetwork that is initialized such that, when trained in isolation, it can match the test accuracy of the original network after training for at most the same number of iterations.

This paper hints at why neural networks work at all. It first states that only a very small subnetwork is responsible for the vast majority of its performance, but it must be initialized at the right position. But by overparameterizing these neural nets so much (by a certain margin), they have so many different combinations of subnetworks such that whatever initialization you throw at it, it is guaranteed that some subnetwork within it will train well with this initialization. This subnetwork is called the *winning ticket*.

## 2.8 Curriculum Learning

## 2.9 Summary

Here is a few steps you can take as a guide to training a neural network.<sup>8</sup>

1. Preprocess the data.
2. Choose your neural net architecture (number of layers/neurons, etc.)
3. Do a forward pass with the initial parameters, which should be small, and check that the loss is reasonable (e.g.  $\log(1/10) \approx 2.3$  for softmax classification of 10 classes).
4. Now crank up the regularization term, and your loss should have gone up.
5. Now try to train on only a very small portion of your data without regularization using SGD, which you should be able to overfit and get the accuracy to 100%.
6. Now you can train your whole dataset. Start off with a small regularization (e.g. 1e-6) and find a learning rate that makes the loss go down.

<sup>8</sup>From Stanford CS 229 NLP.

- (a) Run for a few epochs to see if the cost goes down too slowly (step size is too small) or the cost explodes (step size too big). A general tip is that if the cost is ever bigger than 3 times the original cost, then this is an indication that the cost has exploded.
  - (b) We can run a grid search (in log space) over the learning rate and the regularization hyperparameters over say 10 epochs each, and compare which one makes the most progress.
7. Monitor and visualize the loss curve.

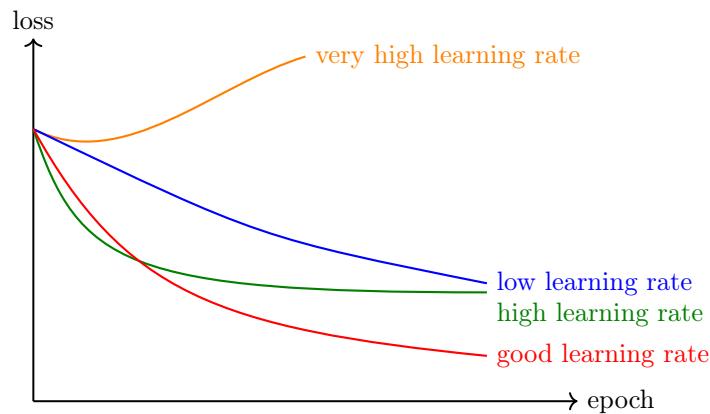


Figure 7: If you see loss curves that are flat for a while and then start decreasing, then bad initialization is a prime suspect.

8. We also want to track the ratio of weight updates and weight magnitudes. That is, we can take the norm of the weights  $\theta$  and the gradient updates  $\nabla\theta$ , and a rule of thumb is that the ratio should be about

$$\frac{\|\nabla\theta\|}{\|\theta\|} \approx 0.001 \text{ or } 0.01$$

### 3 Convolutional Neural Networks

Convolutional networks work with images, so let's introduce a nice way to represent them as vectors.

#### Definition 3.1 (Image)

An image is a vector in some tensor product space. More specifically, avoiding the technicality that each pixel element is bounded and discrete,

1. A grayscale image of resolution of  $H \times W$  is a vector in  $\mathbb{R}^H \otimes \mathbb{R}^W$ .
2. An image with  $C$  channels of the same resolution is an element of  $\mathbb{R}^C \otimes \mathbb{R}^H \otimes \mathbb{R}^W$ .
3. A video with  $C$  channels and of the same resolution is an element of  $\mathbb{R}^T \otimes \mathbb{R}^C \otimes \mathbb{R}^H \otimes \mathbb{R}^W$ , where  $T$  is the time dimension which is usually represented in some discrete frames.

Since tensor product spaces are also vector space, there is nothing new we have to introduce. Everything we talked about so far applies to images when treated as vectors. In fact, so far we have been interpreting images of size  $(C, H, W)$  through the isomorphism

$$\phi : \mathbb{R}^C \otimes \mathbb{R}^H \otimes \mathbb{R}^W \rightarrow \mathbb{R}^{C \times H \times W} \quad (109)$$

that essentially “unravels” the image.

#### 3.1 Convolutional and Pooling Layers

So far, we have seen the power of multilayer perceptrons and their predictive ability on moderately sized vectors. In fact, if we process the MNIST with a simple MLP of 2 layers and 512 nodes each, we can easily get 95% accuracy within 10 epochs. However, these MNIST pictures are extremely low resolution, at  $1 \times 28 \times 28$ , and for even moderately sized images we can see that there is a huge blowup of parameters needed.<sup>9</sup> Clearly, this is not efficient, and so the only way to move on is to create a sparser representation of the network. This is where convolutional kernels come in (note that this is completely different than the kernels mentioned in supervised learning, with support vector machines and RKHS), introduced in [LBBH98]. The general idea is to take a small dot product.

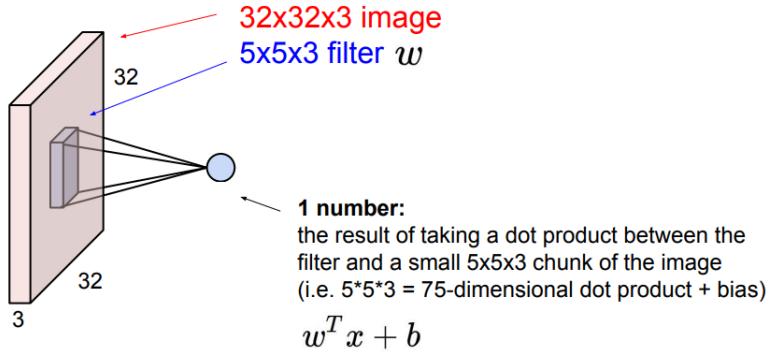


Figure 8

<sup>9</sup>For example, an RGB image that is  $3 \times 1024 \times 1024$  would have 3m parameters, and then defining a dense linear map to even 1000 dimensions would take 3 billion parameters. Given that 32-bit floating point is 4 bytes, this already takes up 12GB of memory just to load the network.

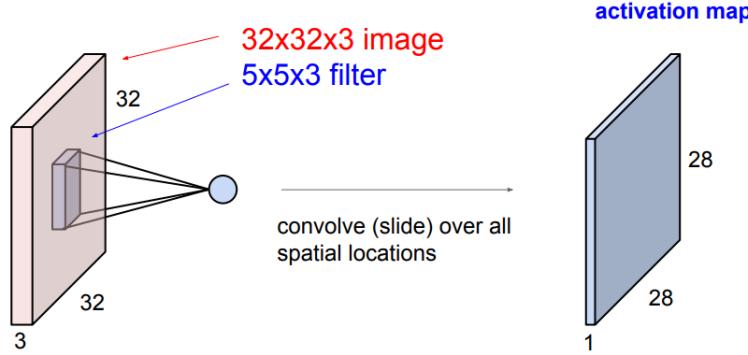


Figure 9

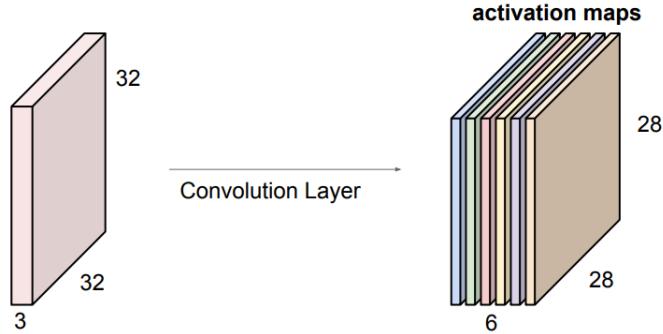


Figure 10

### Definition 3.2 (Convolutional Kernel)

A **convolution operator** on a vector space  $V$  representing an image space is simply a special type of linear map that is parameterized by a much smaller set of numbers, stored within a **kernel** or **filter**. In all honesty, it is much easier to go through examples to see how they work, so in this definition I will focus more on describing the hyperparameters. Given an image of shape  $(C, H, W)$ , the convolution is essentially a sliding window that computes a dot product between the kernel and the window that the kernel covers over the image.

1. The sliding window size is  $(W_{ker}, H_{ker})$ , which is conventionally square but does not need to be.
2. This sliding window must compute over all channels, so in fact it is of shape  $(C_{in}, W_{ker}, H_{ker})$ . This would generate one output channel image.
3. Multiple kernels can be used concurrently to generate different channel images. Therefore, if we want to have a collection of  $C_{out}$  outputs that are extracted from each kernel, our total kernel would be a collection of  $C_{out}$  kernels of shape  $(C_{in}, W_{ker}, H_{ker}, C_{out})$ . Therefore, the total equation is

$$(X * K)_{f,i,j} := \sum_c \sum_{p,q} X_{c,i+p,j+q} \cdot K_{c,p,q,f} + b_{f,i,j} \quad (110)$$

where  $c$  is the channel index,  $p, q$  are the location indices,  $f$  is the output channel index, and  $b$  is some bias term.

4. The stride parameter  $s$  can also be set to determine the stride of the kernel  $K$ .
5. Another thing to note is that the output image of a kernel would be slightly smaller than the input image, since the kernel cannot go over the edge. However, there are padding schemes to preserve the original dimensions.

From the equation above, we can see that a convolutional layer, assuming that it has full padding, is a linear map

$$\mathcal{K} : \mathbb{R}^{C_{in}} \otimes \mathbb{R}^H \otimes \mathbb{R}^W \rightarrow \mathbb{R}^{C_{out}} \otimes \mathbb{R}^H \otimes \mathbb{R}^W \quad (111)$$

The vector space of linear maps mapping between these two spaces has  $C_{in}H^2W^2C_{out}$  dimensions, which is extremely large, but parameterizing  $\mathcal{K}$  with this matrix reduces the set of relevant convolutional maps to a subspace that is  $(1+C_{in}H_{ker}W_{ker})C_{out}$  dimensional (with the +1 due to a bias term, making this an affine map). This is essentially what a convolution is: sparse matrix multiplication, and there is nothing else that makes it different from a classical feedforward neural network. It's just computationally efficient matrix multiplication for high-dimensional vectors.

In addition to computational efficiency and weight sharing, convolutional operators capitalize on the principle of **locality**, i.e. that pixels are directly related to adjacent pixels. For example, a pixel representing a portion of a dog's ear would not be related to the background, but the color and positioning should be related to the dog's face, which may be within a certain neighborhood around. This has been shown to be similar to the human visual system and is thus well motivated.

Though this next topic has more to do with classical image processing than computer vision, there are a surprising number of features that these convolutional filters can extract from an image. By treating them as a discretized form of a partial derivative (as the vertical and horizontal edge detection) or as the Hessian operator (sharpening), we can extract many features from them.

### Example 3.1 (Blurs, Edge Detection)

Given the original image below, we show various convolutional filters applied on the image. Note that the kernel matrix may have the property that all of its entries sum to 1, meaning that on average, the expected value of the brightness of each pixel will be 0, and the values will be left unchanged on average. However, this is not a requirement.

$$\begin{aligned} \text{Original} &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} & \text{Mean} &= \frac{1}{25} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} & \text{Gaussian} &= \frac{1}{273} \begin{bmatrix} 1 & 4 & 7 & 4 & 1 \\ 4 & 16 & 26 & 16 & 4 \\ 7 & 26 & 41 & 26 & 7 \\ 4 & 16 & 26 & 16 & 4 \\ 1 & 4 & 7 & 4 & 1 \end{bmatrix} \\ \text{Sharpen} &= \begin{bmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{bmatrix} & \text{Horizontal} &= \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} & \text{Vertical} &= \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix} \end{aligned}$$

These filters visually output the following images. Note that these filters are each acting on the image by acting individually on each channel and then combining the 3 outputs to create the new RGB image.

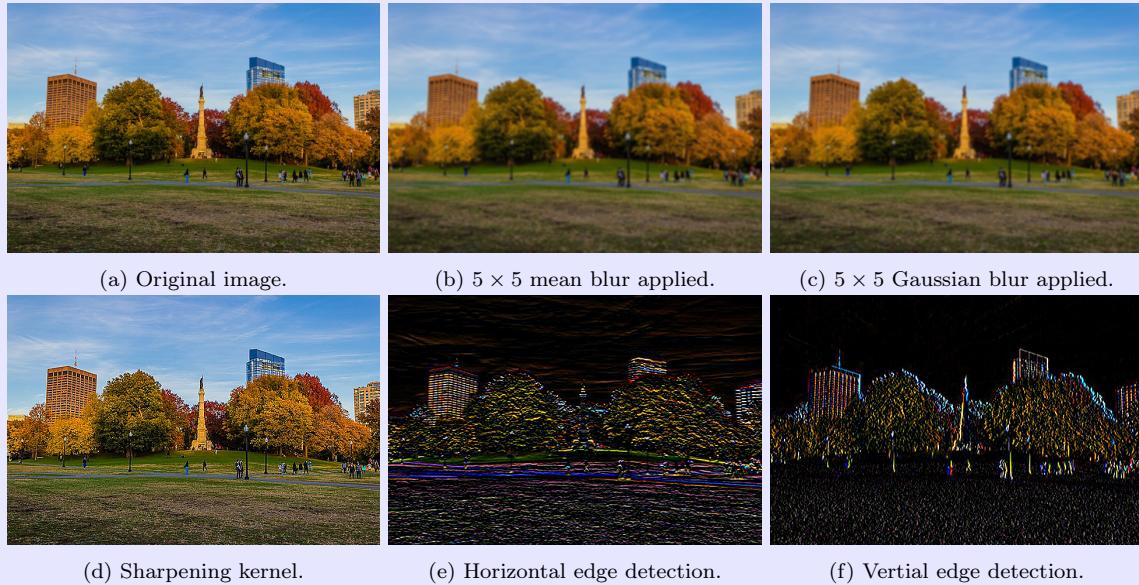


Figure 11: Different convolutional kernels acting on the same image. Several useful features like edges can be detected with these simple linear maps.

We have seen in the example above that we can interpret each output channel of a convolution as a feature. That is, our original input image with  $C_{in} = 3$  channels may go through a convolution that has  $C_{out} = 10$  output channels, producing 10 grayscale images. Each of these images may represent a feature that is extracted from the image through a custom kernel. When we stack convolutional layers together (with nonlinearities in between, of course), we can produce more complicated transformations that extract more abstract features. For example, while the first layer or two may extract certain edges within a dog, perhaps the fourth or fifth convolutional layer will be able to detect the presence of ears. This is a hand-wavy example, but if you actually visualize the outputs of these layers during forward prop, it is possible to see this in action.

What we eventually hope for is that we can extract higher level features that can be encoded in moderate-dimensional vectors. Unfortunately, the rate at which regular convolutional filters (especially when there is padding and a stride of 1) does not shrink the resolution of the input images at a fast enough rate. For example, having a  $3 \times 3 \times 3 \times 3$  kernel with no padding on a  $(3, 100, 100)$  image will decrease the dimensions to only  $(3, 98, 98)$  only. Therefore, we do some very simple operations to reduce the resolution faster.

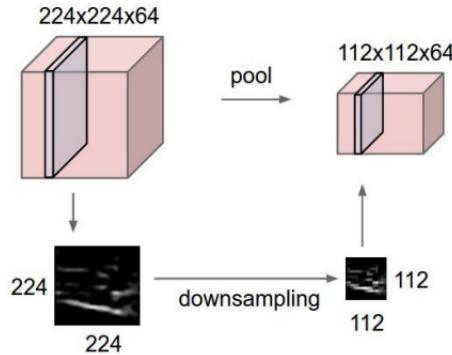


Figure 12

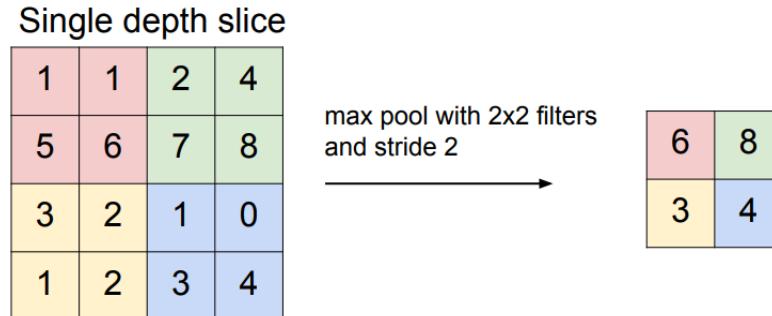


Figure 13

### Definition 3.3 (Pooling Layers)

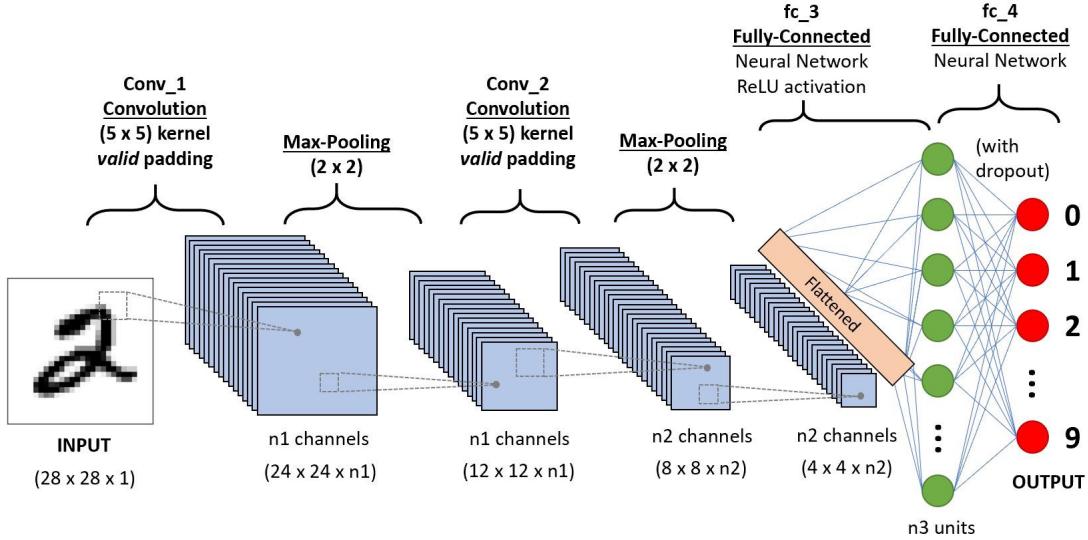
A pooling layer takes in an input image of dimension  $(C, H, W)$  and essentially does **downsampling** on it, involving some method of pooling local groups of pixels together into one value. There are several ways to do this:

1. **Max Pooling** refers to dividing each channel of the image into a “checkerboard” of  $P \times P$  (where  $P$  is a hyperparameter and does not necessarily have to be a square) matrices and simply choosing the maximum pixel value from it.
2. **Average Pooling** is the same as max pooling but we just take the average.

Clearly, these are not expensive operations and are an effective way to downsample. Therefore, the same  $(3, 100, 100)$  image, after one convolutional layer followed by a pooling layer, will result in a  $(3, 49, 49)$  image.

Ultimately, after a series of convolutions and pooling, we would want to reduce this image to a form of  $(C, H, W)$ , where both  $H$  and  $W$  are small and  $C$  is large. This is because for each value of  $C$ , say  $C = 1$ , the cross section  $\{(1, W, H)\}$  would encode the value of the feature identified by  $C$ . In fact, it could be the fact that both  $H$  and  $W$  are 1, and  $C = 10$ . Then, we would essentially be looking at an array of 10 numbers, which could encode the presence of some abstract features. For example, the first value  $C = 1$  would encode the presence of an eye, which in the end has a value of 0.9 (high probability), the second  $C = 2$  could encode the presence of an ear, and so on.

Perhaps the sparsity of these maps may not allow the convolutional layers alone to extract all the features we need, so it is common to unwrap the features and then add a few fully connected layers at the end, which is much more computationally feasible now that the convolutions and pooling layers have reduced the dimensionality whilst extracting useful features with the concept of locality. This turns out to have comparable performance to regular MLPs with a fraction of the computational cost, and can easily reach 98% validation accuracy on the MNIST dataset.



### 3.2 Backpropagation

The fully connected layers are all taken care of, but now it's the convolutional layers and the pooling layers. The convolutional layers are also linear maps, so they can be treated the same way. However, the pooling layers may be nonlinear.

1. Average pooling is linear, so no worries here.
2. Max pooling is not linear, but it is the next best thing: piecewise linear.

### 3.3 Visualizing Activation Maps

#### 3.4 CAM and Grad-CAM

#### 3.5 Exercises

##### Example 3.2 (Tarokh, Duke ECE685)

Consider an RGB image  $X = [X_0, X_1, X_2]$  with three channels, and given as follows

$$X_0 = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 2 & 0 & 1 \\ 2 & 1 & 0 & 1 \end{bmatrix}, \quad X_1 = \begin{bmatrix} 2 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad X_2 = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad (112)$$

The image is passed through the convolutional filter with the weights  $W = [W_0, W_1, W_2] \in \mathbb{R}^{3 \times 3 \times 3}$  and step size 1, and given as follows

$$W_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad W_1 = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 0 & -1 \\ 0 & -1 & 1 \end{bmatrix}, \quad W_2 = \begin{bmatrix} 0 & 0 & -2 \\ 0 & 1 & 2 \\ -2 & 2 & 0 \end{bmatrix} \quad (113)$$

The output of the convolutional filter is given as

$$Y = \text{ReLU} \left( \sum_{i=0}^2 (X'_i * W_i) + 2 \cdot 1_{4 \times 4} \right) \quad (114)$$

where  $Y$  is the output image,  $X'$  is the input image after applying 0 padding around the edges, and  $*$  is the discrete convolution operator. Compute the output  $Y$ , and then apply max pooling on nonoverlapping  $2 \times 2$  submatrices, and then apply average pooling on non-overlapping  $2 \times 2$  submatrices.

### Solution 3.1

We can compute

$$X_0 * W_0 = \begin{bmatrix} -4 & -4 & -1 & 0 \\ -2 & 2 & -4 & -2 \\ -1 & -4 & -1 & 0 \\ -4 & -2 & 2 & -2 \end{bmatrix}$$

$$X_1 * W_1 = \begin{bmatrix} -2 & 6 & 3 & -1 \\ 4 & 6 & -1 & 4 \\ 1 & -3 & 5 & 7 \\ -1 & 0 & 5 & 2 \end{bmatrix}$$

$$X_2 * W_2 = \begin{bmatrix} 4 & 1 & 4 & -2 \\ 2 & 0 & 4 & 11 \\ 2 & -2 & -4 & 2 \\ 2 & 1 & 2 & 1 \end{bmatrix}$$

and so we get

$$Y = \begin{bmatrix} 0 & 5 & 8 & 0 \\ 6 & 10 & 1 & 5 \\ 4 & 0 & 2 & 11 \\ 0 & 1 & 11 & 3 \end{bmatrix} \quad (115)$$

Maxpooling and average pooling gives us

$$\max(Y) = \begin{bmatrix} 10 & 8 \\ 4 & 11 \end{bmatrix} \text{ and } \text{avg}(Y) = \begin{bmatrix} 21/4 & 7/2 \\ 5/4 & 27/4 \end{bmatrix} \quad (116)$$

## 4 Recurrent Neural Networks

Let's focus on what is lacking in the vanilla feedforward neural net architecture. In a vanilla feedforward neural net architecture, we had a one to one map, where we take an input of fixed size and we map it to an output of fixed size. Perhaps we would want a one-to-many model, which takes in an image for example and outputs a variable-length description of the image. Or a many-to-many (e.g. machine translation from a sequence of words to a sequence of words) or many-to-one. Just as a convolutional neural network is specialized for processing a grid of values such as an image, a recurrent neural network is specialized for processing a sequence of values (e.g. audio, video, text, speech, time series).

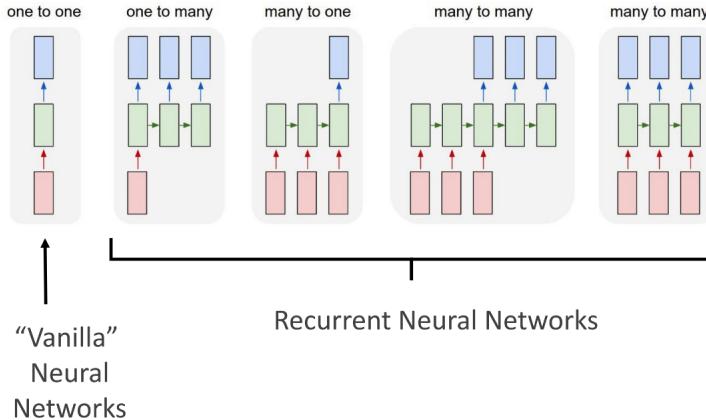


Figure 14: It is not limited to a fixed size of inputs and outputs.

Now to build such a model where the input or output elements are unbounded, we must take advantage of *weight sharing* (as seen in the CNN architecture) to control the size of our neural net. Furthermore, the fact that we should take in a sequence of inputs means that we may want to introduce some recursive structure in our neural net. Consider the classical form of a dynamical system driven by an external signal  $\mathbf{x}$  as

$$\mathbf{s}_t = f(\mathbf{s}_{t-1}, \mathbf{x}_t; \boldsymbol{\theta}) \quad (117)$$

which defines a recurrent relationship. Similarly, we can write  $\mathbf{h}$  to represent hidden neurons and write

$$\mathbf{h}_t = f(\mathbf{h}_{t-1}, \mathbf{x}_t; \boldsymbol{\theta}) \quad (118)$$

which indicates that the state of a hidden neuron is dependent on both the previous neuron and an input at time  $t$ . Through recursion, the hidden state  $\mathbf{h}_t$  contains all information about the inputs  $\mathbf{x}_1, \dots, \mathbf{x}_t$  in the form of a complex function  $\mathbf{g}$ .

$$\mathbf{h}_t = \mathbf{g}_t(\mathbf{x}_t, \mathbf{x}_{t-1}, \dots, \mathbf{x}_1) \quad (119)$$

$$= f(\mathbf{h}_{t-1}, \mathbf{x}_t; \boldsymbol{\theta}) \quad (120)$$

The fact that we can factorize  $\mathbf{g}_t$  into a repeated application of function  $f$  gives us two advantages:

1. Regardless of the sequence length, the learned model always has the same input size because it is specified in terms of transition from one state to another state, rather than specified in terms of a variable-length history of states.
2. It is possible to use the same transition function  $f$  with the same parameters at every time step. Since we do not have a growing number of parameters to optimize as our sequential data grows, training an RNN is still computationally feasible.

These two factors make it possible to learn a single model  $f$  that operates on all time steps and all sequence lengths, rather than needing to learn a separate model  $\mathbf{g}_t$  for all possible time steps.

## 4.1 Unidirectional RNNs

A single layer unidirectional RNN is a direct application of the idea mentioned in the previous section. We can first look at its computational graph

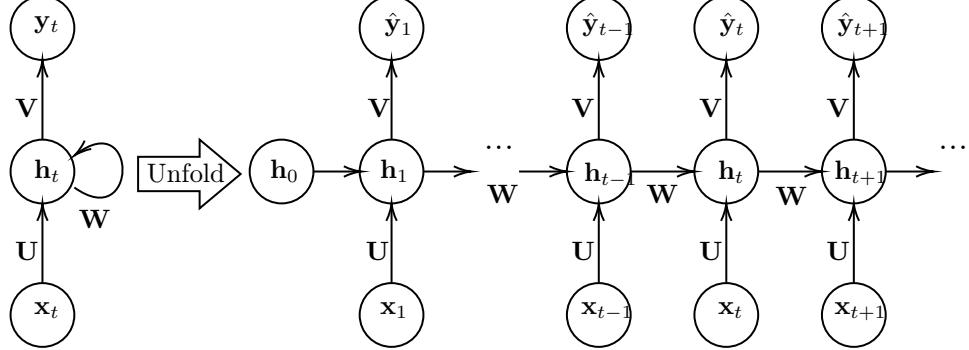


Figure 15: The circular arrow is notation for an RNN that “unfolds” to the graph on the right.

The activation functions that map to the hidden nodes and the outputs will be labeled  $\sigma_h$  and  $\sigma_y$ , respectively. In general the  $W$  will represent the left and right mappings between hidden nodes, the  $U$  will represent the map going up from the input or hidden node to a hidden node, and  $V$  is the final mapping from a hidden node to an output. We only label the arrows with the matrices, though a bias term and the nonlinear activation function are still there. That is, we can summarize our network as

$$\mathbf{h}_t = \mathbf{f}(\mathbf{h}_{t-1}, \mathbf{x}_t; \boldsymbol{\theta}) = \sigma_h(\mathbf{W}\mathbf{h}_{t-1} + \mathbf{U}\mathbf{x}_t + \mathbf{b}_h) \quad (121)$$

$$\mathbf{y}_t = \sigma_y(\mathbf{V}\mathbf{h}_t + \mathbf{b}_y) \quad (122)$$

for  $t = 1, \dots, \tau$ , where  $\mathbf{h}_0$  is initialized to be zeroes or some small vector. The dimensions of the maps and the variables are listed for clarification:

1.  $\mathbf{x}_t \in \mathbb{R}^d$  for all  $t$
2.  $\mathbf{h}_t \in \mathbb{R}^h$  for all  $t$
3.  $\mathbf{b}_h \in \mathbb{R}^h$
4.  $\mathbf{U} \in \mathbb{R}^{h \times d}$
5.  $\mathbf{W} \in \mathbb{R}^{h \times h}$

As we can see, the hidden node from the previous time step provides a form of memory, or context, that encodes earlier processing and informs the decisions to be made at later points in time. Adding this temporal dimension makes RNNs appear to be more complex than non-recurrent architectures, but in reality, they’re not all that different. Consider the rearranged architecture of an RNN below.

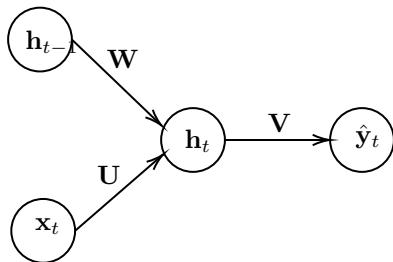


Figure 16: RNNs as an MLP.

### 4.1.1 Loss Functions

The form of the loss for a RNN will have to be slightly modified, since we can have multiple outputs. If we have a given input-output pair  $\mathbf{x}^{(n)}, \mathbf{y}^{(n)}$ , and we are interested producing a single output, then this is similar to what we already do with regular NNs. If we are interested in producing a sequence of outputs, then we can average the loss functions individually so that equal weight is placed on the prediction at each relevant timestep. This is called

$$L = \frac{1}{|T|} \sum_{t \in T} L_t \quad (123)$$

Sometimes, even with single inputs it may be good to include other intermediate terms in the loss so that we can direct the neural net to converge faster to what the correct answer should be.

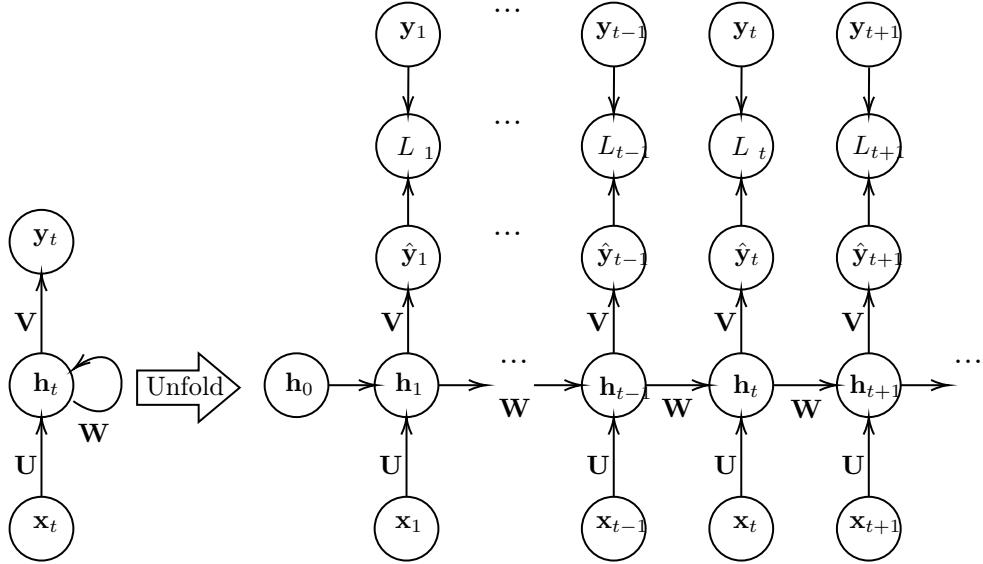


Figure 17

Note that one problem is that the errors can build up as the RNN predicts outcomes. For example, if we predicted  $\mathbf{x}_1 \mapsto \hat{\mathbf{y}}_1$  we can compute the loss as  $L_1(\mathbf{y}_1, \hat{\mathbf{y}}_1)$ . However, there are two ways to compute the second loss: with inputs  $L_2(\mathbf{x}_1, \mathbf{x}_2)$  or with  $L_2(\mathbf{x}_1, \hat{\mathbf{y}}_1)$ . One just uses the ground truth while the other uses the previous prediction for the next prediction, which can accumulate error. Both ways are feasible for loss computation, but it is generally done in the former way, called **teacher forcing**. This is analogous to a human student taking a multi-part exam where the answer to each part depends on the answer to the preceding part. Rather than grading every answer in the end, with the risk that the student fails every single part even though they only made a mistake in the first one, a teacher records the score for each individual part and then tells the student the correct answer, to be used in the next part.

### 4.1.2 Backpropagation Through Time

Now if we wanted to backpropagate through this RNN, we can compute

$$\frac{\partial L_t}{\partial \mathbf{W}} = \frac{\partial L_t}{\partial \hat{\mathbf{y}}_t} \frac{\partial \hat{\mathbf{y}}_t}{\partial \mathbf{h}_t} \frac{\partial \mathbf{h}_t}{\partial \mathbf{W}} \quad (124)$$

where the first term depends on the specific form of the loss and the second is simply the matrix  $\mathbf{V}$ . This all looks the same as backpropagation for a MLP, but since  $\mathbf{W}_{hh}$  is used at multiple layers, we can reduce the third term in the equation to

$$\frac{\partial L_t}{\partial \mathbf{W}} = \frac{\partial L_t}{\partial \hat{\mathbf{y}}_t} \frac{\partial \hat{\mathbf{y}}_t}{\partial \mathbf{h}_t} \left( \sum_{k=1}^t \frac{\partial \mathbf{h}_t}{\partial \mathbf{h}_k} \frac{\partial \mathbf{h}_k}{\partial \mathbf{W}} \right) \quad (125)$$

where

$$\frac{\partial \mathbf{h}_t}{\partial \mathbf{h}_k} = \prod_{i=k+1}^t \frac{\partial \mathbf{h}_i}{\partial \mathbf{h}_{i-1}} \quad (126)$$

is computed as a multiplication of adjacent time steps. Now this can be very problematic, since if we have a lot of multiplications, then depending on the randomness of these matrices the gradient may be highly unstable, causing the vanishing or exploding gradient problem. We can elaborate on this a little further. Note that the hidden linear maps are known to be square matrices. We can expand out the derivative without the constant terms on the left as such:

$$\sum_{k=1}^t \frac{\partial \mathbf{h}_t}{\partial \mathbf{h}_k} \frac{\partial \mathbf{h}_k}{\partial \mathbf{W}} = \sum_{k=1}^t \prod_{k < i \leq t} \frac{\partial \mathbf{h}_i}{\partial \mathbf{h}_{i-1}} \frac{\partial \mathbf{h}_k}{\partial \mathbf{W}} \quad (127)$$

and we can see if at some point one of the  $\frac{\partial \mathbf{h}_j}{\partial \mathbf{h}_{j-1}}$  tend to be small just from randomness, then their product for all coefficients where  $k \leq j$  will be small too. This means that all the information, or memory, from the  $j$ th hidden state and before will vanish. In fact, if the spectrum (the set of eigenvalues and eigenvectors) is less than 1, then the multiplication of these derivatives will converge to a 0 matrix, and so we have an exponential memory loss throughout the network.

Furthermore, we can compute these gradients in batches by splitting up the corpus into several sentences, and sampling the sentences for gradient computation. Therefore, a forward or backward pass has a runtime complexity of  $O(\tau)$  and cannot be reduced by parallelization because the forward propagation graph is inherently sequential. Each time step may only be computed after the previous one. States computed in the forward pass must be stored until they are reused during the backward pass, so the memory cost is also  $O(\tau)$ .

#### 4.1.3 Stacked Unidirectional RNNs

Note that since we really have three matrices to optimize in the regular RNN, this may not be so robust. Therefore, we would like more hidden layers to capture further nonlinearities in an RNN, which is why we introduce a **stacked RNN** as shown below:

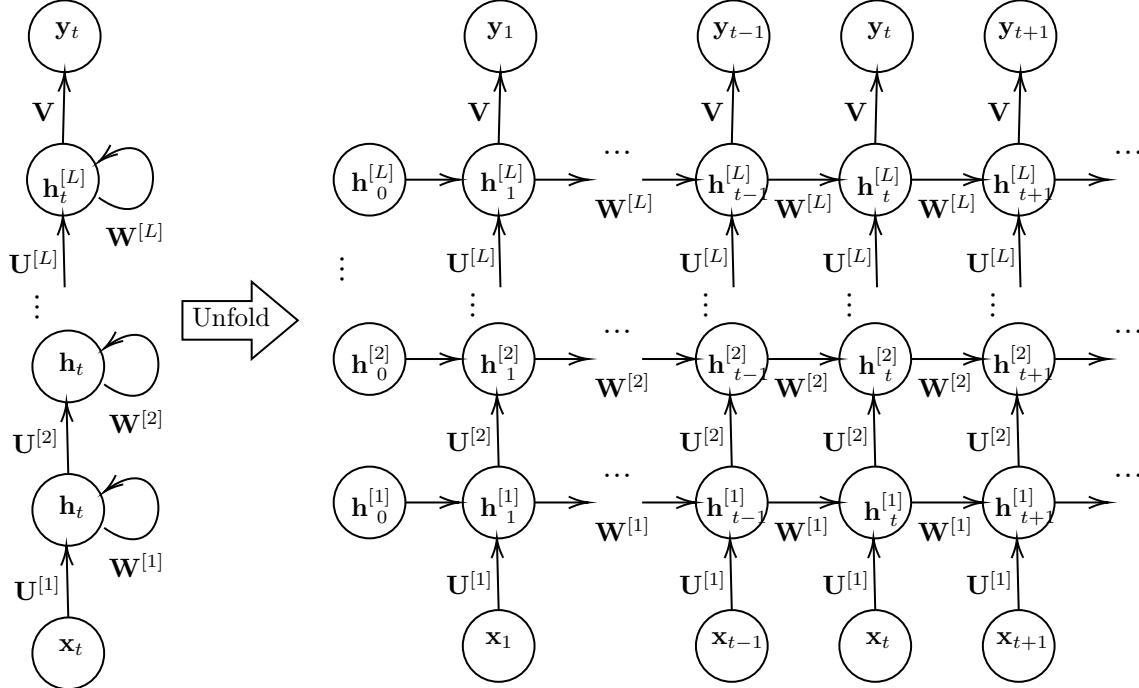


Figure 18: Stacked RNNs.

Now in this case, there are more layers of hidden nodes that an input must go through before it reaches the output node. We can expand out the computations as such, for  $t = 1, \dots, \tau$ ,  $l = 2, \dots, L$ :

$$\mathbf{h}_t^{[1]} = \sigma_h(\mathbf{W}^{[1]}\mathbf{h}_{t-1}^{[1]} + \mathbf{U}^{[1]}\mathbf{x}_t + \mathbf{b}_h^{[1]}) \quad (128)$$

$$\mathbf{h}_t^{[l]} = \sigma_h(\mathbf{W}^{[l]}\mathbf{h}_{t-1}^{[l]} + \mathbf{U}^{[l]}\mathbf{x}_t + \mathbf{b}_h^{[l]}) \quad (129)$$

$$\mathbf{y}_t = \sigma_y(\mathbf{V}\mathbf{h}_t^{[L]} + \mathbf{b}_y^{[L]}) \quad (130)$$

or we could get rid of the first equation all together if we set  $\mathbf{x}_t = \mathbf{h}_t^{[0]}$ . Note that the hidden nodes  $\mathbf{h}_t^{[l]}$  for all  $t$  and all  $l \neq 0$  are all in  $\mathbb{R}^h$ , i.e. all hidden nodes will be  $h$ -dimensional. Therefore, most of the parameter matrices that we work with are square:  $\mathbf{W}^{[l]} \in \mathbb{R}^{h \times h}$  and  $\mathbf{U}^{[l]} \in \mathbb{R}^{h \times h}$  except for  $\mathbf{U}^{[1]} \in \mathbb{R}^{h \times d}$ .

## 4.2 Bidirectional RNNs

### 4.2.1 PyTorch Implementation

The implementation in PyTorch actually uses *two* bias terms  $\mathbf{b}_{hW}^{[l]}$  and  $\mathbf{b}_{hU}^{[l]}$  rather than just  $\mathbf{b}_h^{[l]}$ . This is technically not needed since the bias terms will just cancel out, but this is just how cuDNN (Cuda Deep Neural Network) is implemented.

$$\mathbf{h}_t^{[l]} = \sigma_h(\mathbf{W}^{[l]}\mathbf{h}_{t-1}^{[l]} + \mathbf{b}_{hW}^{[l]} + \mathbf{U}^{[l]}\mathbf{x}_t + \mathbf{b}_{hU}^{[l]}) \quad (131)$$

Let us look at a 2 layer RNN of sequence length 5. The input features will be set to 10, meaning that each  $\mathbf{x} \in \mathbb{R}^{10}$ . The hidden nodes will all be in  $\mathbb{R}^{20}$ .

```

1  input_features = 10
2  hidden_features = 20
3  num_layers = 2
4  sequence_length = 5
5
6  rnn = nn.RNN(input_features, hidden_features, num_layers)
7  input = torch.randn(sequence_length, input_features)
8  h0 = torch.randn(num_layers, hidden_features)
9  print(input.size(), h0.size())
10 # torch.Size([5, 10]) torch.Size([2, 20])
11
12 print([weight.data.size() for weights in rnn.all_weights for weight in weights])
13 # [torch.Size([20, 10]), torch.Size([20, 20]), torch.Size([20]), torch.Size([20]),
14 torch.Size([20, 20]), torch.Size([20, 20]), torch.Size([20]), torch.Size([20])]
15
16 output, hn = rnn(input, h0)
17 print(output.size(), hn.size())
18 # torch.Size([5, 20]) torch.Size([2, 20])

```

The corresponding diagram is shown below.

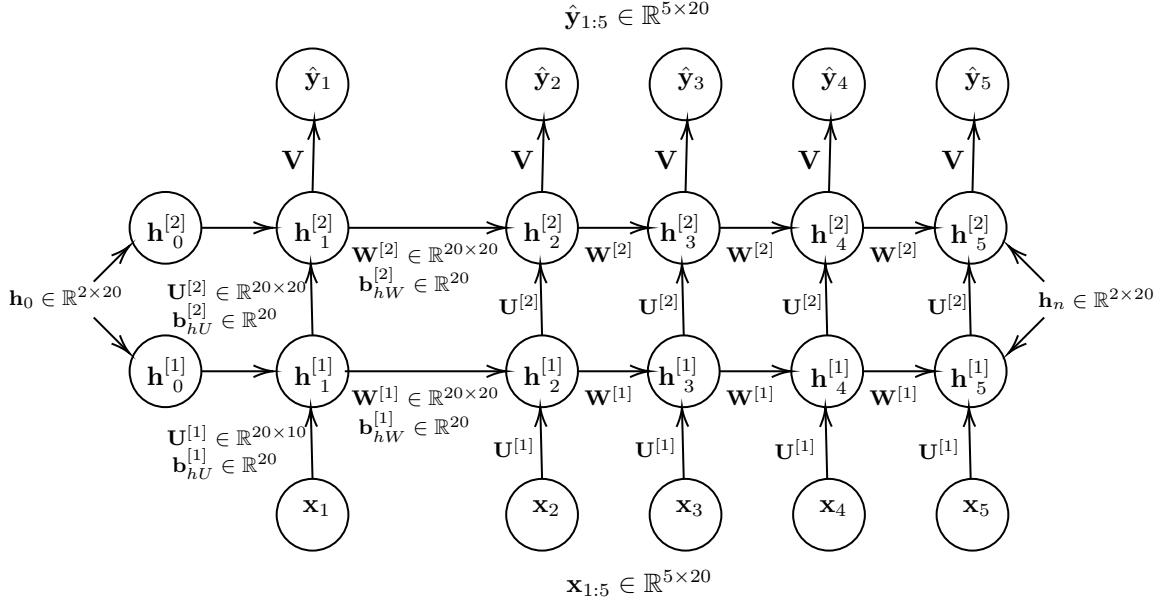


Figure 19

As we expect, there are 8 vectors/matrices we must optimize:  $\mathbf{W}^{[1]}, \mathbf{W}^{[2]}, \mathbf{U}^{[1]}, \mathbf{U}^{[2]}, \mathbf{b}_{hU}^{[1]}, \mathbf{b}_{hW}^{[1]}, \mathbf{b}_{hW}^{[2]}, \mathbf{b}_{hU}^{[2]}$ .

### 4.3 Long Short Term Memory (LSTMs)

In theory, RNNs are very beautiful and can be applied in all cases, but in practice they do not perform very well, mainly due to the vanishing/exploding gradient problem.

1. An exploding gradient is easy to fix, since we can just use the max-norm regularization, i.e. **gradient clipping**, to just set a max value for the gradients if they grow too large.
2. The **truncated backpropagation through time** (TBPTT) simply limits the number of time steps the signal can backpropagate after each forward pass, e.g. even if the sequence has 100 time steps, we may only backpropagate through 20 or so.
3. The **LSTM** model uses a memory cell for modeling long-range dependencies and avoids the vanishing gradient problems.

Historically LSTMs were used in achieving state-of-the-art results in 2013 through 2015, in tasks such as handwriting recognition, speech recognition, machine translation, parsing, and image captioning, as well as language models. They became the dominant approach for most NLP tasks, but in 2021, they have been overshadowed by transformer models, which we will talk about next.

LSTMs have a much more complicated unit to work with, so let's go through it slowly. Note that so far, a one-layer RNN consisted of recursive mappings of the form

$$(\mathbf{x}_t, \mathbf{h}_{t-1}) \mapsto (\mathbf{h}_t, \hat{\mathbf{y}}_t) \quad (132)$$

We can interpret the vector  $\mathbf{h}_{t-1}$  as the **short term memory**, or **hidden state**, that contains information used to predict the next output value. However, this can be corrupted (e.g. forgetting information from many steps ago), so we add an additional **long term memory**, or **cell state**, vector  $\mathbf{c}_t$  that should be preserved. Therefore, we have two arrows coming out of each hidden layer, as shown below in the one-layer LSTM.

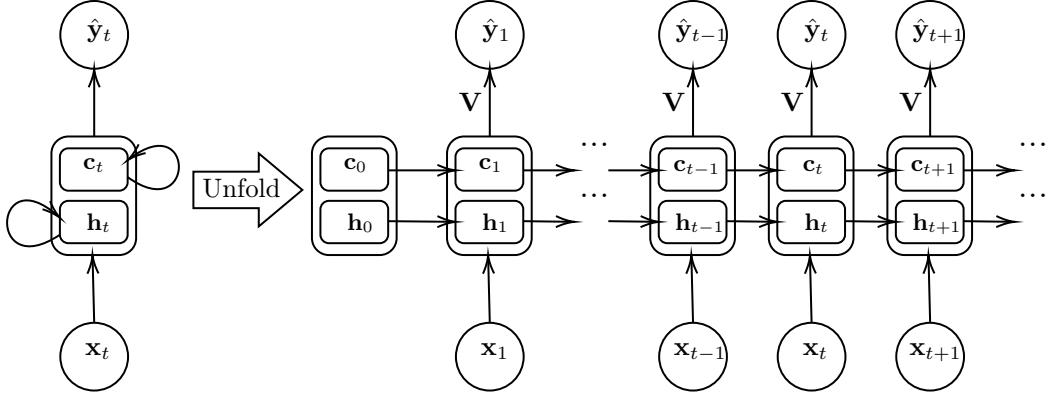


Figure 20

The mechanisms of the cell is quite complex, but the three basic steps are: (1) we forget a portion of the long term memory, (2) we add new long term memory, (3) we add new short term memory. Let us demonstrate this step by step. We are given three inputs: the previous long-term memory  $\mathbf{c}_{t-1}$ , the previous short-term memory  $\mathbf{h}_{t-1}$ , and the input at current time  $\mathbf{x}_t$ . In LSTMs, we only use the sigmoid and tanh activation functions, so we will denote them explicitly as  $\sigma$  and  $\tanh$ . For clarity, we will not write the matrix operations in the diagram anymore.

1. The **forget gate** (denoted by  $\mathbf{f}$ ) takes an affine combination of  $\mathbf{h}_{t-1}$  and  $\mathbf{x}_t$  and puts it through the sigmoid activation function to generate a vector  $\mathbf{f}_t$  that has every element in  $(0, 1)$ . Then it element-wise multiplies it with  $\mathbf{c}_{t-1}$ , which essentially “forgets” a portion of the long-term memory.

$$\mathbf{f}_t = \sigma(\mathbf{W}_f \mathbf{h}_{t-1} + \mathbf{U}_f \mathbf{x}_t + \mathbf{b}_f) \quad (133)$$

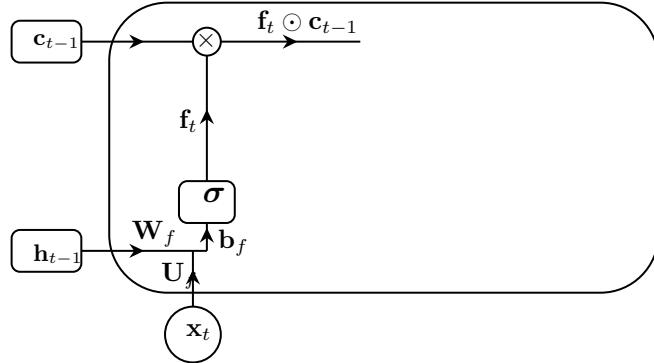


Figure 21

2. The **input gate** (denoted by  $\mathbf{i}$ ) consists of two activations with the following operations.

$$\mathbf{i}_t = \sigma(\mathbf{W}_i \mathbf{h}_{t-1} + \mathbf{U}_i \mathbf{x}_t + \mathbf{b}_i) \quad (134)$$

$$\tilde{\mathbf{c}}_t = \tanh(\mathbf{W}_c \mathbf{h}_{t-1} + \mathbf{U}_c \mathbf{x}_t + \mathbf{b}_c) \quad (135)$$

$$\mathbf{c}_t = \mathbf{f}_t \odot \mathbf{c}_{t-1} + \mathbf{i}_t \odot \tilde{\mathbf{c}}_t \quad (136)$$

The layer  $\mathbf{i}$  can be seen as the filter that selects which information can pass through it and what information to be discarded. To create this layer, we pass the short-term memory and current input into a sigmoid function, which will transform the values to be between 0 and 1, indicating which information is unimportant. The second layer  $\tilde{\mathbf{c}}$  takes the short term memory and current input and

uses the tanh to transform the elements to be in  $(-1, 1)$ , which allows us to add or subtract the necessary information from the long term memory.

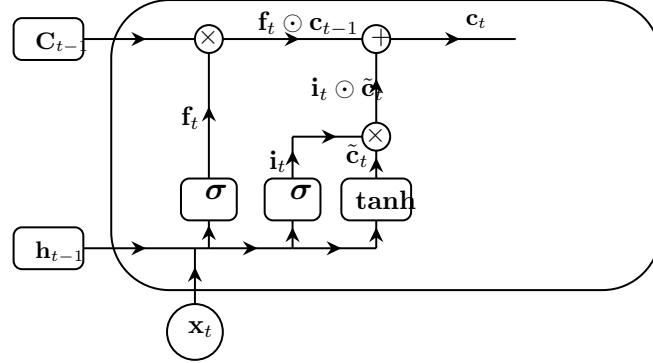


Figure 22

3. The **output gate** (denoted by  $\mathbf{o}$ ) consists of two activations with the following operations. This again creates a separate filter that selects the relevant information needed for the short term memory.

$$\mathbf{o}_t = \sigma(\mathbf{W}_o \mathbf{h}_{t-1} + \mathbf{U}_o \mathbf{x}_t + \mathbf{b}_o) \quad (137)$$

$$\mathbf{h}_t = \mathbf{o}_t \odot \tanh(\mathbf{c}_t) \quad (138)$$

$$\hat{\mathbf{y}}_t = \sigma_y(\mathbf{V} \mathbf{h}_t + \mathbf{b}_y) \quad (139)$$

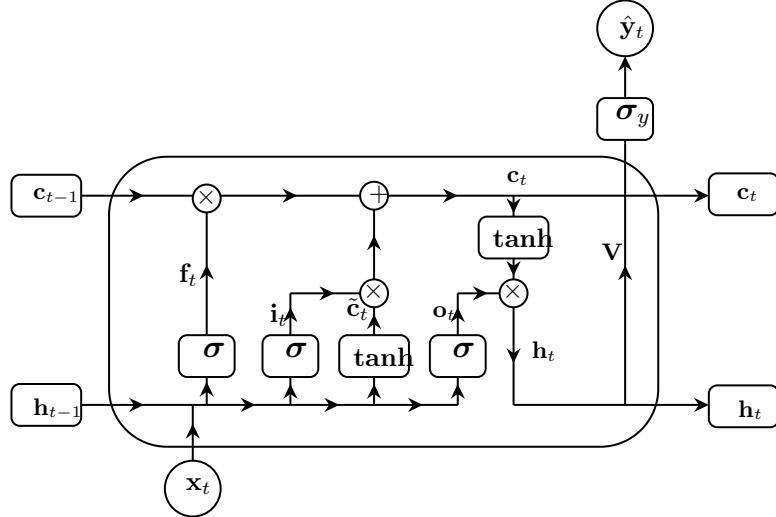


Figure 23

That is it! Now focusing on the cell state in the diagram above. Note that in order to go from cell state  $\mathbf{c}_{t-1}$  to  $\mathbf{c}_t$ , there was not a whole lot done to it. We really just multiply it once, which potentially deletes some content, and add it once, which adds new content, and we are done. The magic is this addition, since unlike multiplication, which can result in an exponential decay of knowledge, you are just constantly adding new numbers to update the storage, allowing the cell state to behave much more like RAM of a computer.

The LSTM architecture also makes it easier for the RNN to preserve information over many timesteps. For example, if the forget gate  $f_t$  is set to  $1$  and the input gate set to  $0$ , then the information of that cell is preserved indefinitely. In contrast, it's harder for a vanilla RNN to learn a recurrent weight matrix  $\mathbf{W}$  that

preserves information in the hidden state. In practice, a vanilla RNN would preserve memory up to maybe 7 timesteps (and increasing this is extremely difficult) while a LSTM would get about 100 timesteps, so in practice you should almost always just use a LSTM.

Unfortunately, LSTM doesn't *guarantee* that there is no vanishing or exploding gradients, but it does provide an easier way for the model to learn long-distance dependencies. Note that the gradient problem is not just a problem for RNNs; any neural architecture (including a feed-forward or convolutional) with very deep layers with multiple compositions of functions may suffer. Due to the chain rule and choice of nonlinearity function, these gradients can become vanishingly small and lower layers are learned very slowly. However, we can still implement residual connections to allow for more gradient flow such as ResNet, DenseNet, and HighwayNet.

### 4.3.1 Multilayer LSTMs

We can extend this architecture in the exactly same way for multilayer LSTMs. Note that we should be careful of the transformations each arrow represents. For the arrows going from  $\mathbf{h}_t^{[l]} \mapsto \mathbf{h}_t^{[l+1]}$ , there is no further transformation since we are just pushing this vector as an input to the next LSTM node. However, the arrow pushing from  $\mathbf{c}_t^{[L]} \mapsto \hat{\mathbf{y}}_t$  does have an extra affine transformation with  $\mathbf{V}$  and  $\mathbf{b}_y$ , followed by some link function  $\sigma_y$  before we have the true prediction.

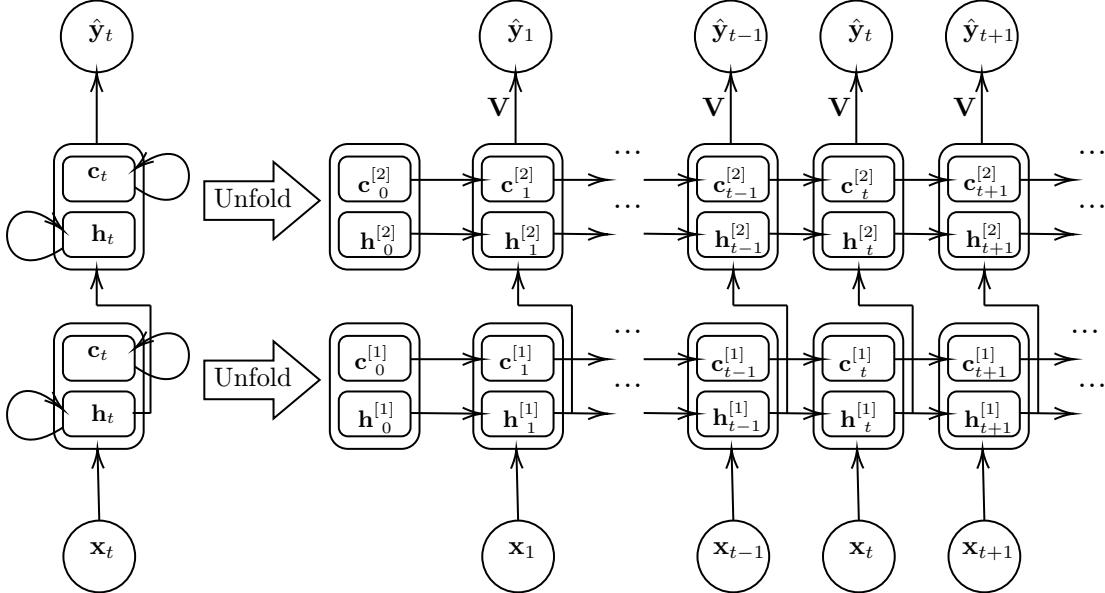


Figure 24

This follows the recursive equations, with  $\mathbf{x}_t = \mathbf{h}_t^{[0]}$ .

$$\text{Forget Gate } \begin{cases} \mathbf{f}_t^{[l]} = \sigma(\mathbf{W}_f^{[l]} \mathbf{h}_{t-1}^{[l]} + \mathbf{U}_f^{[l]} \mathbf{h}_t^{[l-1]} + \mathbf{b}_f^{[l]}) \end{cases} \quad (140)$$

$$\text{Input Gate } \begin{cases} \mathbf{i}_t^{[l]} = \sigma(\mathbf{W}_i^{[l]} \mathbf{h}_{t-1}^{[l]} + \mathbf{U}_i^{[l]} \mathbf{h}_t^{[l-1]} + \mathbf{b}_i^{[l]}) \\ \tilde{\mathbf{c}}_t^{[l]} = \tanh(\mathbf{W}_c^{[l]} \mathbf{h}_{t-1}^{[l]} + \mathbf{U}_c^{[l]} \mathbf{h}_t^{[l-1]} + \mathbf{b}_c^{[l]}) \\ \mathbf{c}_t^{[l]} = \mathbf{f}_t^{[l]} \odot \mathbf{c}_{t-1}^{[l]} + \mathbf{i}_t^{[l]} \odot \tilde{\mathbf{c}}_t^{[l]} \end{cases} \quad (141)$$

$$\text{Output Gate } \begin{cases} \mathbf{o}_t^{[l]} = \sigma(\mathbf{W}_o^{[l]} \mathbf{h}_{t-1}^{[l]} + \mathbf{U}_o^{[l]} \mathbf{h}_t^{[l-1]} + \mathbf{b}_o^{[l]}) \\ \mathbf{h}_t^{[l]} = \mathbf{o}_t^{[l]} \odot \tanh(\mathbf{c}_t^{[l]}) \end{cases} \quad (142)$$

$$\text{Output } \begin{cases} \hat{\mathbf{y}}_t = \sigma_y(\mathbf{V} \mathbf{h}_t^{[L]} + \mathbf{b}_y) \end{cases} \quad (143)$$

where

1.  $\mathbf{x}_t \in \mathbb{R}^d$  for all  $t$
2.  $\mathbf{f}_t^{[l]}, \mathbf{i}_t^{[l]}, \mathbf{o}_t^{[l]} \in (0, 1)^h$
3.  $\mathbf{h}_t^{[l]}, \tilde{\mathbf{c}}_t^{[l]} \in (-1, 1)^h$
4.  $\mathbf{c}_t^{[l]} \in \mathbb{R}^h$

and we must optimize the parameters

$$(\mathbf{W}_f^{[l]}, \mathbf{U}_f^{[l]}, \mathbf{b}_f^{[l]}), (\mathbf{W}_i^{[l]}, \mathbf{U}_i^{[l]}, \mathbf{b}_i^{[l]}), (\mathbf{W}_c^{[l]}, \mathbf{U}_c^{[l]}, \mathbf{b}_c^{[l]}), (\mathbf{W}_o^{[l]}, \mathbf{U}_o^{[l]}, \mathbf{b}_o^{[l]}) \quad (144)$$

for  $l = 1, \dots, L$ . The fact that a LSTM uses the long term memory, in addition to the short term memory and the input, allows each cell to regulate the information to be kept or discarded at each time step before passing on the long-term and short-term information to the next cell. They can be trained to selectively remove any irrelevant information.

#### 4.4 Gated Recurrent Units

## 5 Encoder-Decoder Models

Encoder decoder models refer to a model consisting of two neural nets: the encoder that takes in the input and maps it to some lower-dimensional vector. Then, the decoder takes in this encoded vector and attempts to use it to decode what we're trying to get. The type of neural network can be any: MLP, CNN, or RNN, depending on what problem you're trying to achieve.

Now, why would we want to do something like encode the input into some lower dimensional setting, and then have the decoder neural net extract what we want? It seems like we're making the problem harder. There are two reasons:

1. The input vector may not be in the correct form that we want. This is the motivation for the *seq2seq* model, where we are working with sequences of vectors that suffer from the problem of *locality* in RNNs. Therefore, it is necessary to encode this entire sequence into one vector, at the loss of dimension.
2. The input vector may be noisy or too high-dimensional itself. In CNNs, we saw that convolutional layers or pooling layers allow us to reduce the dimension to extract meaningful features from it. Likewise, we can train the encoder to extract useful features into a lower dimensional space, and then the decoder can efficiently work with this representation. This motivates the use of **autoencoders**, which can be done with MLPs, CNNs, or even RNNs.

Note that while these two algorithms fall in the paradigm of encoder-decoder networks, the seq2seq model is supervised while the autoencoder is unsupervised. In the seq2seq model, which deals with things like machine translation, we have a labeled dataset of sentences in language A corresponding with sentences in language B. However, in autoencoders, what we do is take a sample  $x$  from our dataset and use it both as the input and output to train our network. Since there is no additional labeling required, this is an unsupervised learning technique.

### 5.1 Autoencoders

In the totally linear case, we have PCA. Some input  $\mathbf{x} \in \mathcal{X} = \mathbb{R}^d$  is mapped to a smaller-dimensional  $\mathcal{Z} = \mathbb{R}^k$ .

$$\mathbf{x} \xrightarrow{V} \mathbf{z} \xrightarrow{U} \hat{\mathbf{x}}$$

and so the “network” essentially computes  $\hat{\mathbf{x}} = UV\mathbf{x}$ . Obviously the fact that  $k < d$  is essential, since if  $k \geq d$  then we can choose  $U$  and  $V$  such that  $UV = I$ , which is trivial.

This can be used for the following problem: Given  $m$  points  $\mathbf{x}_1, \dots, \mathbf{x}_m \in \mathbb{R}^d$  and target dimension  $k < d$ , find the best  $k$ -dimensional subspace approximating the data. Formally, we want to find the matrices  $U \in \mathbb{R}^{d \times k}$  and  $V \in \mathbb{R}^{k \times d}$  that minimizes

$$f(U, V) = \sum_{i=1}^m \|\mathbf{x}_i - UV\mathbf{x}_i\|_2^2$$

where  $V$  is the *compressor* and  $U$  is the *decompressor*. Now unfortunately, this loss  $f$  is not convex, though  $f(U, \cdot)$  and  $f(\cdot, V)$  are both convex.

#### Theorem 5.1 ()

We claim that the optimal solution is achieved when  $U = V^T$  and  $U^T U = I$ .

#### Proof.

For any  $U, V$ , the linear map  $\mathbf{x} \mapsto UV\mathbf{x}$  has a range  $R$  that forms a subspace of dimension  $k$ . Let  $w_1, \dots, w_k$  be an orthonormal basis for  $R$ , which we arrange into columns of  $W$ . Hence, for each  $x_i$  there is  $z_i \in \mathbb{R}^k$  such that  $UVx_i = Wz_i$ . Note that by construction,  $W^T W = I$ . Now we want to find out which  $z$  minimizes  $f(x_i, z) = \|x_i - Wz\|_2^2$ . We know that for all  $x \in \mathbb{R}^d, z \in \mathbb{R}^k$ ,

$$f(x, z) = \|x\|_2^2 + z^T W^T W z - 2z^T W^T x = \|x\|_2^2 + \|z\|_2^2 - 2z^T W^T x$$

We want to minimize w.r.t. to  $z$ , so by taking the derivative and setting to 0, we get  $z = W^T x$ . This means that

$$\sum_{i=1}^m \|x_i - UVx_i\|^2 \geq \sum_{i=1}^m \|x_i - UVx_i\|^2 \geq \sum_{i=1}^m \|x_i - WW^T x_i\|^2$$

and since  $U, V$  are optimal, equality is achieved and so instead of  $U, V$ , we can take  $W, W^T$ , with  $WW^T x$  being the orthogonal projection of  $x$  onto  $R$ .

One application of PCA is eigenfaces, which assumes that the set of all faces (projected onto an image) approximately lies in a hyperplane.

Autoencoders are a nonlinear generalization of PCA. We only use the inputs  $\mathbf{x}_t$  for learning. We want to automatically extract meaningful features for the data and leverage the availability of unlabeled data. It can be used for visualization and compression. We can also build generative models with autoencoders. We can have several architectures, with none, one, or both the encoder/decoder having nonlinear activation functions. Here is one architecture.

### Definition 5.1 (Autoencoder)

An autoencoder is a feed-forward neural net whose job is to take an input  $\mathbf{x}$  and output  $\hat{\mathbf{x}}$ . It consists of an encoder  $E_\phi : \mathcal{X} \rightarrow \mathcal{Z}$  and decoder  $D_\theta : \mathcal{Z} \rightarrow \mathcal{X}$ , where  $\mathcal{X}$  is the input/output space and  $\mathcal{Z}$  is the latent feature space.

1. The encoder model transforms  $\mathbf{x}$  to a latent feature representation  $\mathbf{z}$ . It is a feed-forward, bottom-up neural net.
2. The decoder model maps  $\mathbf{z}$  to a reconstruction  $\hat{\mathbf{x}}$ . It is generative, top-down.

where we have

$$\text{Encoder : } \mathbf{h}(\mathbf{x}) = g(\mathbf{a}(x)) = \sigma(\mathbf{b} + \mathbf{W}\mathbf{x})$$

$$\text{Decoder : } \hat{\mathbf{a}}(\mathbf{x}) = \sigma(\mathbf{c} + \mathbf{W}^*\mathbf{h}(\mathbf{x}))$$

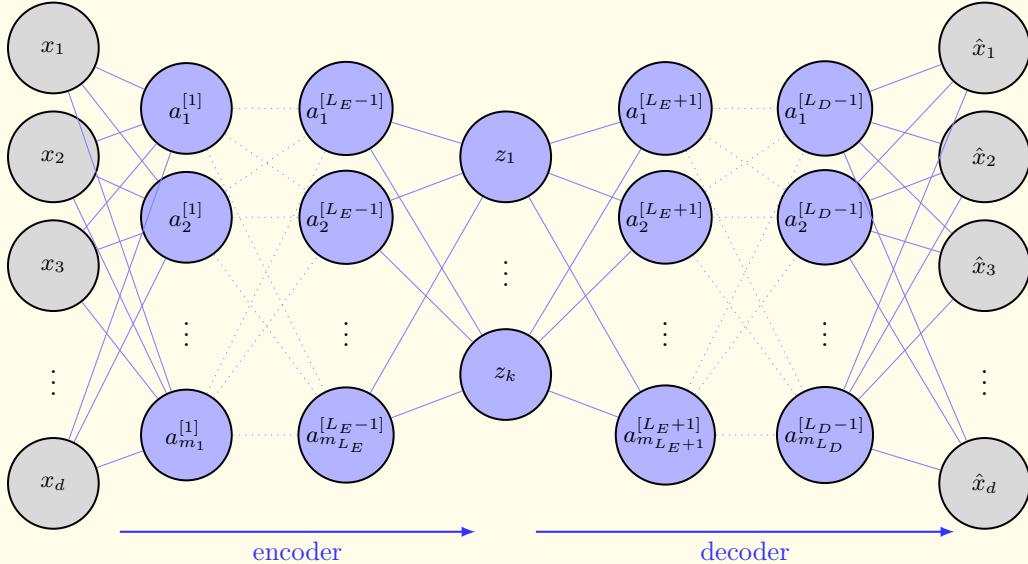


Figure 25: A graphical model of an autoencoder. The  $z$  is called the **bottleneck layer**, which compresses the input into a lower-dimensional representation. The  $x$  is known as the **input layer**, the  $\hat{x}$  as the **output layer**, and everything else are **hidden layers**.

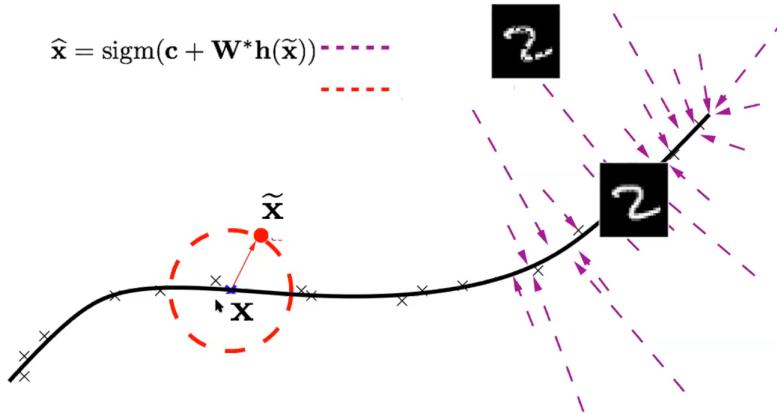
The parameter gradients are obtained by backpropagating the gradient  $\nabla_{\theta}\mathcal{L}$  like a regular network, but if we force tied weights (i.e.  $W^* = W^T$ ), then  $\nabla_{\mathbf{W}}\mathcal{L}$  is the sum of two gradients. This is because  $\mathbf{W}$  is present both in the encoder and decoder.

I want to train the whole neural network such that the error between  $\mathbf{x}$  and  $\hat{\mathbf{x}}$  is minimized. We can consider a squared-error, for example.

$$\mathcal{L}(\mathbf{x}, \hat{\mathbf{x}}) = \frac{1}{2} \|\mathbf{x} - \hat{\mathbf{x}}\|_2^2 \quad (145)$$

There are three things we can do to extract meaningful hidden features:

1. **Undercomplete Representation:** Make the latent dimension small. It compresses the input, but it may only be good for the training distribution and may not be robust to other types of input. If it is overcomplete, there is no guarantee that we will extract meaningful features.
2. **Denoising Autoencoder:** Injecting noise to the input. The idea is that the representation should be robust to the introduction of noise. We take the original input  $\mathbf{x}$  and we randomly assign a subset of the inputs to 0, with probability  $\nu$ , similar to dropout, to get our noisy input  $\tilde{\mathbf{x}}$ . Then we train the autoencoder with the loss comparing the output  $\hat{\mathbf{x}}$  to the original, un-noisy input  $\mathbf{x}$ . We can do this for Gaussian additive noise too. As the visual below suggests, we are essentially “pushing” out inputs away from the manifold and training the autoencoder to denoise it, pulling it back.



3. **Contractive Autoencoder:** If we have the latent dimension greater than the input, then we can just add an explicit term in the loss that penalizes that solution (e.g. promoting sparsity). For example, we can have the loss be

$$\mathcal{L}(f(\mathbf{x}^{(t)}) + \lambda \|\nabla_{\mathbf{x}^{(t)}} \mathbf{h}(\mathbf{x}^{(t)})\|_F^2$$

where

$$\|\nabla_{\mathbf{x}^{(t)}} \mathbf{h}(\mathbf{x}^{(t)})\|_F^2 = \sum_{j,k} \left( \frac{\partial h(\mathbf{x}^{(t)})_j}{\partial x_k^{(t)}} \right)^2$$

which forces the encoder to throw away information. If one of the elements are 0, then we know that the  $k$ th element of the input has no effect on the  $j$ th element of the encoded output. Therefore, it tries to throw away as many elements of  $\mathbf{x}$  as possible since the identity matrix will have a large Frobenius norm, essentially contracting the input representation.

We can also promote sparsity by adding a L1 penalty, forcing the feature space to be sparse.

The **predictive sparse decomposition** shows that the loss should be

$$\min_{W, W^*, \mathbf{z}} \|W^* \mathbf{z} - \mathbf{x}\|_2^2 + \lambda |\mathbf{z}|_1 + \|\sigma(W \mathbf{x}) - \mathbf{z}\|_2^2 \quad (146)$$

where the first term tells the decoder to reconstruct the original input well, the second tells the latent vector to be sparse, and the third tells us that we shouldn't lose too much information when we encode.

We could also have **stacked autoencoders**, with each layer of latent features having some desired sparsity.

## 5.2 Sequence to Sequence

We have mentioned that RNNs and LSTMs have the advantage of mapping from variable length inputs to variable length outputs. This can be done for any length input and any length output. However, the RNN has the problem of *locality*, that the words next to the current word have a greater effect, and we are trying to generate sequences on the fly by reading in each word. Even for bidirectional RNNs, where we go through the whole sentence first, the effects of adjacent words have a greater effect when generating outputs. It would be wiser to read the *whole* sentence and then start to generate a sequence. This is the motivation for the **encoder-decoder model**. It is conventionally divided into a two-stage network.

1. The encoder neural net would convert a sequence into a single latent space representation  $z = f(x)$ . This latent representation  $z$  essentially refers to a feature (vector) representation, which is able to capture the underlying semantic information of the input that is useful for predicting the output.
2. The decoder neural net would decode this feature vector, called the **context vector**, into a sequence of the desired output  $y = g(z)$  by using it as the initial hidden state. It uses the previous output as the next input for decoding.

Note that the encoder and decoder are two completely separate neural networks with their own parameters. This is important, since the fact that these are two completely separate networks allows us to work in different "paradigms" within either the feature or target space. For example, if we want to perform machine translation from English to Spanish, our encoder RNN parameters have been tuned to the English syntax and language, while the decoder RNN parameters are tuned to the Spanish language. Since we are modeling different languages, it makes sense to have different sequence models for each one.

We will talk about a specific type of encoder-decoder model called **seq2seq**, which maps sequences to sequences using RNN encoders and decoders. Conventionally, the hidden nodes of the encoder are denoted with  $\mathbf{h}$ , and those of the decoder are denoted with  $\mathbf{s}$ .

1. For the encoder, we take in the inputs  $\mathbf{x}_t$  and generate the hidden states as

$$\mathbf{h}_t = f(\mathbf{x}_t, \mathbf{h}_{t-1}) = \mathbf{W}_e \mathbf{h}_{t-1} + \mathbf{U}_e \mathbf{x}_t + \mathbf{b}_e \quad (147)$$

In general, the encoder transforms the hidden states at all time steps into a context variable through the composition of functions  $q$

$$\mathbf{C} = q(\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_T)$$

In the figure below, the context variable is just  $\mathbf{C} = \mathbf{h}_T$ .

2. Now, given the target output sequence  $\hat{\mathbf{y}}_1, \dots, \hat{\mathbf{y}}_{t'+1}$  for each timestep  $t'$  (we use  $t'$  to differentiate from the input sequence time steps), the decoder assigns a predicted probability to each possible token occurring at step  $\hat{\mathbf{y}}_{t'+1}$  conditioned on both the previous tokens  $\hat{\mathbf{y}}_1, \dots, \hat{\mathbf{y}}_{t'+1}$  and the context variable  $\mathbf{C}$ , i.e.

$$\mathbb{P}(\hat{\mathbf{y}}_{t'+1} | \hat{\mathbf{y}}_1, \dots, \hat{\mathbf{y}}_{t'+1}, \mathbf{C})$$

Therefore, to decode the subsequent token  $\hat{\mathbf{y}}_{t'+1}$ , we calculate the hidden state  $\mathbf{s}_{t'+1}$  as a gated hidden unit computed by

$$\mathbf{s}_{t'+1} = g(\mathbf{s}_{t'}, \hat{\mathbf{y}}_{t'}, \mathbf{C})$$

with the math mentioned here.

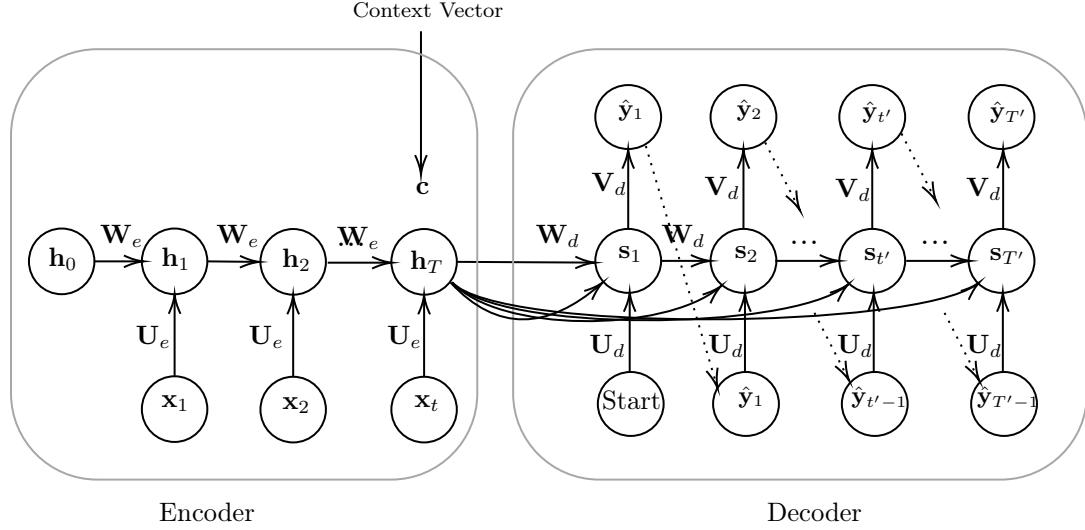


Figure 26

Again, note that this encoder-decoder model is comprised of two completely separate deep models with their own parameters, and so it is *not* simply just one long RNN that starts generating outputs only after it takes in all the inputs. Sometimes, the inputs to the decoder may not be shown in diagrams since it is assumed that they are always the previous node's outputs. Furthermore, we can also see that there is no clear-defined first input for the decoder model, since this is the beginning of the sequence. We usually just put some special "start" element in here to denote the beginning of the output.

Here is a diagram for a encoder-decoder model for a 2-layer LSTM which is the standard for practical use, which encodes the sentence meaning in the vectors  $c_t^{[2]}, h_t^{[2]}, c_t^{[1]}, h_t^{[1]}$ . In practice, high performing RNNs are usually multilayer (almost always greater than 1, but diminishing performance returns as number of layers increases), but are not as deep as convolutional or feed forward networks.

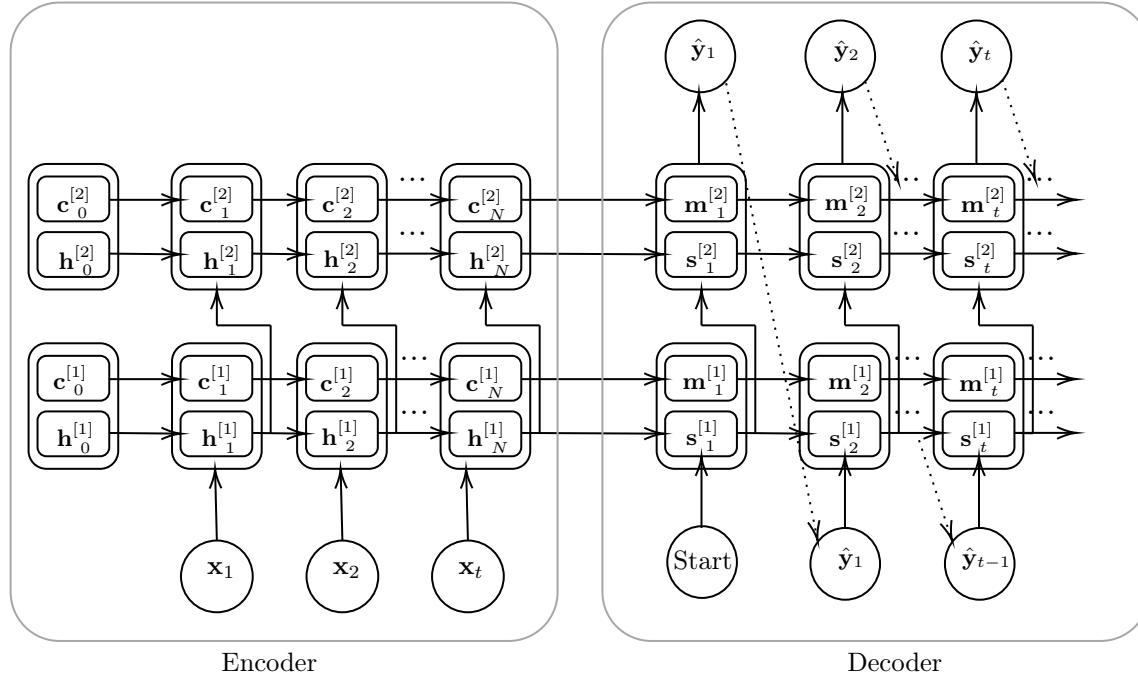


Figure 27

Again, to train this model, we do the same backpropagation algorithm on a normalized loss function with teacher forcing over a parallel dataset. What is nice about the encoder-decoder seq2seq is that it can be completely implemented end-to-end, so we can backpropagate through the entire decoder and encoder to train the both models simultaneously.

### 5.3 More Flexible Models

By combining these neural nets, we can essentially create image captioning (with a CNN encoder and RNN decoder) and image generation (RNN encoder and CNN decoder).

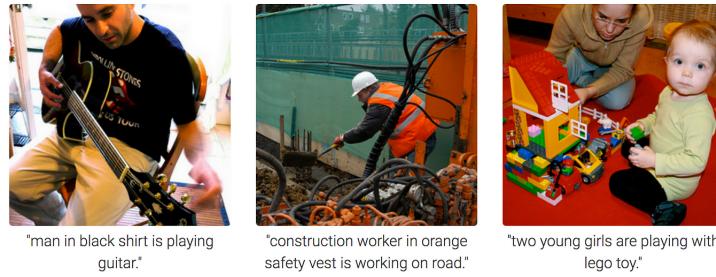


Figure 28: Image captioning on various image prompts.

## 6 Energy Models

Note from our machine learning notes that for unsupervised tasks, we have estimated the density of complex distributions by factoring them in *graphical models*, e.g. Bayesian networks or Markov random fields. We will extend this into deep learning architectures.<sup>10</sup> If you are not familiar, you should probably go over graphical models in my ML notes before reading further.

Note that many of the theories behind energy models are very old (from the 1980s) and established. All of them essentially rely on the fact that we can model a probability density as

$$p(x) = \frac{e^{-f(x)}}{Z} \quad (148)$$

for some function  $f : \mathbb{R}^n \rightarrow \mathbb{R}$ , and  $Z$  is what we call the **partition function**. We have seen from the Hammersley-Clifford theorem in my machine learning notes that we can model a joint probability distribution on an undirected graph with the product of potential functions on the max cliques.<sup>11</sup> Therefore, we will take advantage of this in the specific instance of MRFs that are *bipartite graphs*, i.e. a non-feedforward (since its cyclic) 2-layer neural network. We will talk about RBMs, deep belief networks, and hopfield networks. Diffusion models, which can also be considered an energy model, will be talked separately.

### 6.1 Boltzmann Machines

Consider the graph  $x_1, \dots, x_D$  which represents a random vector  $x$  for which we would like to model the probability distribution of.



What we can do is model the dependencies between these random elements with linear parameters  $W$  and  $b$ , which essentially gives us a Markov Random Field. Let's consider when  $x_i$ 's are all Bernoulli, so  $x \in \{0, 1\}^D$ , which are known as *Ising models* in statistical mechanics. By Hammersley-Clifford, we don't even need to specify the individual functions over the maximal cliques, and rather we can just specify the energy function  $E(x)$  of the Boltzmann distribution that the MRF encodes. We parameterize  $\theta = \{W, b\}$ .

#### Example 6.1 (Bernoulli Pairwise Markov Random Fields)

We define it to capture the interactions between Bernoulli random variables  $x_i$  up to order 2.

$$p_\theta(x) = \frac{1}{Z} \exp(E(x)) = \frac{1}{Z} \exp \left( \sum_{ij \in E} x_i x_j W_{ij} + \sum_{i \in V} x_i b_i \right) = \frac{1}{Z} \exp(x^T W x + b^T x) \quad (149)$$

Now let's check its conditional distribution. Let  $x_{-k}$  denote the joint distribution of all random variables minus  $x_k$ .

$$p(x_k = 1 | x_{-k}) = \frac{p(x_k = 1, x_{-k})}{p(x_{-k})} \quad (150)$$

$$= \frac{p(x_k = 1, x_{-k})}{p(x_k = 0, x_{-k}) + p(x_k = 1, x_{-k})} \quad (151)$$

$$= \frac{\exp \left( \sum_{kj \in E} x_j W_{kj} + x_k b_k \right)}{\exp(0) + \exp \left( \sum_{kj \in E} x_j W_{kj} + x_k b_k \right)} \quad (152)$$

$$= \sigma \left\{ -b_k x_k - \sum_{kj \in E} x_j W_{kj} \right\} \quad (153)$$

<sup>10</sup>This is *not* to be confused with graph neural networks (GNNs), which are designed for tasks whose inputs are graphs.

<sup>11</sup>But finding max cliques is NP-hard?

where the penultimate step comes from evaluating

$$p(x_k = 1, x_{-k}) = \frac{1}{Z(\theta)} \exp \left( \sum_{ij \in E, k \neq i, j} x_i x_j W_{ij} + \sum_{ij \in E, k = i, j} x_i x_j W_{ij} + \sum_{i \in V, i \neq k} x_i b_i + x_k b_k \right) \quad (154)$$

$$= \frac{1}{Z(\theta)} \exp \left( \sum_{ij \in E, k \neq i, j} x_i x_j W_{ij} + \sum_{kj \in E} x_j W_{kj} + \sum_{i \in V, i \neq k} x_i b_i + b_k \right) \quad (155)$$

$$p(x_k = 0, x_{-k}) = \frac{1}{Z(\theta)} \exp \left( \sum_{ij \in E, k \neq i, j} x_i x_j W_{ij} + \sum_{i \in V, i \neq k} x_i b_i \right) \quad (156)$$

and canceling out like terms in the numerator and denominator. This tells us that MRFs are related to logistic function.

### Example 6.2 (Gaussian Markov Random Fields)

If we assume that  $p_\theta(x)$  follows a multivariate Gaussian distribution, we have

$$p(x | \mu, \Sigma) = \frac{1}{Z} \exp \left( -\frac{1}{2}(x - \mu)^T \Sigma^{-1} (x - \mu) \right) \quad (157)$$

Since the Gaussian distribution represents at most second-order relationships, it automatically encodes a pairwise MRF. Therefore, we can rewrite

$$p(x) = \frac{1}{Z} \exp \left( -\frac{1}{2} x^T J x + g^T x \right) \quad (158)$$

where  $J = \Sigma^{-1}$  and  $\mu = J^{-1}g$ .

However, this is still quite a limited model. For one, due to the linearity of the weight matrix, it always turns out that the probability of  $x_k = 1$  is always given by a linear model (logistic regression) from the values of the other units. This family of distributions parameterized by  $\theta = \{W, b\}$  may not be broad enough to capture the true  $p(x)$ . Therefore, we can add latent variables that can act similarly to hidden units in a MLP and model higher-order interactions among the visible units. Just as the addition of hidden units to convert logistic regression into MLP results in the MLP being a universal approximator of functions, a Boltzmann machine with hidden units is not longer limited to modeling linear relationships between variables. Instead, the Boltzmann machine becomes a universal approximator of probability mass functions over discrete random variables.

### Definition 6.1 (Boltzmann Machine)

The original **Boltzmann machine** has the energy function

$$E(v, h) = -v^T R v - v^T W h - h^T S h - b^T v - c^T h \quad (159)$$

It can represent the undirected graph that has connections within the  $x$ , within the  $h$ , and between the  $x$  and  $h$ .

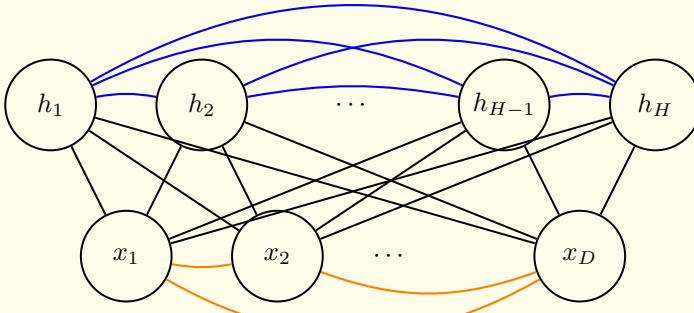


Figure 29: 2-layer undirected graph representing a Boltzmann machine.

Therefore, by adding latent variables and connecting everything together, this gives us a very flexible model that can capture a lot of distributions.

## 6.2 Restricted Boltzmann Machines

Unfortunately, there are problems with training this, and so the restricted Boltzmann machine allowed for efficient training. Therefore, we will limit ourselves to **pairwise MRFs**, which only capture dependencies between cliques of maximum size 2. We usually write  $x$  as the observed and  $z$  as the latent, but in the literature  $v$  and  $h$  are used, respectively. Now, if we put a restriction saying that there cannot be any intra-connections in the  $x$  and  $h$ , then we get the *restricted Boltzmann machine*, which has a slightly more restricted form of the energy function than the general BM.

### Definition 6.2 (Restricted Boltzmann Machine)

The **restricted Boltzmann machine** has the energy function

$$E(v, h) = -v^T Wh - b^T v - c^T h \quad (160)$$

with connections only allowed between  $x_i$ 's and  $h_j$ 's, known as a **bipartite graph**, implying that the maximum clique length is 2. This model allows the elements of  $x$  to be dependent, but this architecture allows for *conditional independence*, and not just for  $x$  given  $h$ , but also  $h$  given  $x$ . Therefore, we already have the extremely nice property that

$$p(x | h) = \prod_{k=1}^D p(x_k | h) \quad (161)$$

$$p(h | x) = \prod_{j=1}^F p(h_j | x) \quad (162)$$

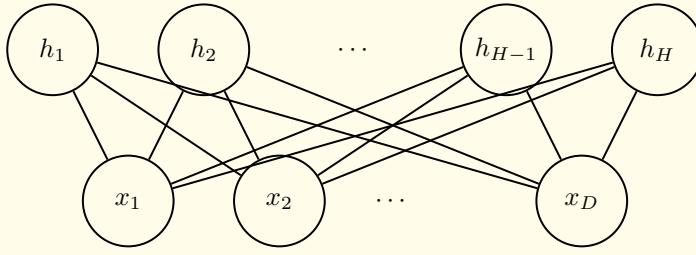


Figure 30: 2-layer undirected graph representing a restricted Boltzmann machine. Note that the intra-connections (blue and orange) are gone.

Note that this form of the probability  $E(x)$  is equivalent to the product of max-cliques, which are of size 2 in this case.

$$p(v, h) = \exp(-E(v, h))/Z \quad (163)$$

$$= \exp(v^T Wh + b^T v + c^T h)/Z \quad (164)$$

$$= \exp(v^T Wh) \exp(b^T v) \exp(c^T h)/Z \quad (165)$$

$$= \frac{1}{Z} \prod_j \prod_k \exp(W_{jk} h_j v_k) \prod_k \exp(c_k v_k) \prod_j \exp(b_j h_j) \quad (166)$$

Therefore, we can think of the  $\exp(h^T W x)$  as encoding the cliques of length 2 and the others as cliques of length 1. The fact that we can calculate  $p(h | x)$  means that inferring the distribution over the hidden variables is easy.

### 6.2.1 Contrastive Divergence

Now that we've done this, we can finally get to training the model. Now, essentially this is density estimation problem given dataset  $\mathcal{D} = \{x^{(t)}\}$  of iid random variables, we want to maximize the likelihood of  $p_\theta$ , which is really just equivalent to optimizing  $E_\theta$ . So, let's take the average negative log-likelihood and take the derivative of it

$$\frac{\partial}{\partial \theta} \frac{1}{T} \sum_t -\log p_\theta(x^{(t)}) \quad (167)$$

There's a lot of computation to do here, so let's focus on one sample  $x^{(t)}$  and claim that the gradient ultimately ends up as the following.

#### Theorem 6.1 (Decomposition of Derivative)

The derivative of the log-likelihood decomposes into the following terms.

$$\frac{\partial}{\partial \theta} -\log p(x^{(t)}) = \sum_h p(h | x^{(t)}) \frac{\partial E(x^{(t)}, h)}{\partial \theta} - \sum_{x,h} p(x, h) \frac{\partial E(x, h)}{\partial \theta} \quad (168)$$

$$= \underbrace{\mathbb{E}_h \left[ \frac{\partial E(x^{(t)}, h)}{\partial \theta} \mid x^{(t)} \right]}_{\text{positive phase}} - \underbrace{\mathbb{E}_{x,h} \left[ \frac{\partial E(x, h)}{\partial \theta} \right]}_{\text{negative phase}} \quad (169)$$

which reduces to

$$-\nabla_\theta \ln p(x) = \begin{cases} -\nabla_W \ln p(x) & = \sum_h p(h | x) h x^T - \sum_{x,h} p(x, h) h x^T \\ -\nabla_b \ln p(x) & = \sum_h p(h | x) h - \sum_{x,h} p(x, h) h \\ -\nabla_c \ln p(x) & = \sum_h p(h | x) x - \sum_{x,h} p(x, h) x \end{cases} \quad (170)$$

**Proof.**

From the energy model form, we can see that  $Z = \sum_{x,h} \exp(-E(x, h))$ . Therefore,

$$\ln(Z) = \ln \left( \sum_{x,h} \exp(-E(x, h)) \right) \quad (171)$$

$$\frac{\partial}{\partial \theta} \ln(Z) = \frac{1}{Z} \sum_{x,h} \exp(-E(x, h)) \cdot -1 \cdot \frac{\partial}{\partial \theta} E(x, h) \quad (172)$$

$$= -\frac{1}{Z} \sum_{x,h} \exp(-E(x, h)) \cdot \frac{\partial}{\partial \theta} E(x, h) \quad (173)$$

$$= -\frac{1}{Z} \sum_{x,h} Z \cdot p(x, h) \cdot \frac{\partial}{\partial \theta} E(x, h) \quad (174)$$

$$= -\sum_{x,h} p(x, h) \frac{\partial E(x, h)}{\partial \theta} \quad (175)$$

We have by definition

$$-\ln p(x) = -\ln \left\{ \sum_h \exp(-E(x, h)) \right\} + \ln(Z) \quad (176)$$

and so when taking the derivative, the second term is solved from above and the first term, we apply the chain rule to get

$$-\frac{\partial}{\partial \theta} \ln p(x) = \frac{\sum_h \exp(-E(x, h)) \frac{\partial E(x, h)}{\partial \theta} / Z}{\sum_h \exp(-E(x, h)) / Z} + \frac{\partial \ln(Z)}{\partial \theta} \quad (177)$$

$$= \frac{\sum_h p(x, h) \frac{\partial E(x, h)}{\partial \theta}}{p(x)} + \frac{\partial \ln(Z)}{\partial \theta} \quad (178)$$

$$= \sum_h p(h | x) \frac{\partial E(x, h)}{\partial \theta} - \sum_{x,h} p(x, h) \frac{\partial E(x, h)}{\partial \theta} \quad (179)$$

We can use the closed form of  $E$  to then compute its partials.

$$\left( \frac{\partial E(x, h)}{\partial W} \right)_{ij} = \frac{\partial E(x, h)}{\partial W_{ij}} = \frac{\partial}{\partial W_{ij}} \left\{ -\sum_{i,j} W_{ij} h_i x_j - \sum_j c_j x_j - \sum_i b_i h_i \right\} = h_i x_j \quad (180)$$

$$\left( \frac{\partial E(x, h)}{\partial b} \right)_i = \frac{\partial E(x, h)}{\partial b_i} = h_i \quad (181)$$

$$\left( \frac{\partial E(x, h)}{\partial c} \right)_j = \frac{\partial E(x, h)}{\partial c_j} = x_j \quad (182)$$

which in matrix form is

$$\nabla_{\theta} E(x, h) = \{\nabla_W E(x, h), \nabla_b E(x, h), \nabla_c E(x, h)\} = \{hx^T, h, x\} \quad (183)$$

The conditional probability can be factorized out given  $x$  and computed easily by conditional independence.

$$p(h | x) = \prod_j p(h_j | x) \quad (184)$$

and so given that we have computed this for all  $h$ , we can write our gradient as

$$-\nabla_{\theta} \ln p(x) = \begin{cases} -\nabla_W \ln p(x) &= \sum_h p(h | x) hx^T - \sum_{x,h} p(x, h) hx^T \\ -\nabla_b \ln p(x) &= \sum_h p(h | x) h - \sum_{x,h} p(x, h) h \\ -\nabla_c \ln p(x) &= \sum_h p(h | x) x - \sum_{x,h} p(x, h) x \end{cases} \quad (185)$$

Therefore, we can easily compute the left summation in the gradient form, but the right summation requires us to compute  $p(x, h)$  as a general joint distribution, which is intractable. So we just approximate this with a Monte Carlo estimator, specifically Gibbs sampling. This method is known as *contrastive divergence*.

### Algorithm 6.1 (Contrastive Divergence)

The general idea is to replace by the expectation by a point estimate at  $\tilde{x}$ , which we can obtain by sampling the conditions over and over through Gibbs. Since we know  $p(x | h)$  and  $p(h | x)$  easily, we can start sampling the chain for some predetermined  $K$  steps (actually  $2K$  since we are sampling the  $x$  and  $h$  back and forth), and whatever  $\tilde{x}, \tilde{h}$  you sample at the end is your estimate. You then use this to approximate the negative phase

$$\mathbb{E}_{x,h} \left[ \frac{\partial E(x, h)}{\partial \theta} \right] \approx \frac{\partial}{\partial \theta} E(\tilde{x}, \tilde{h}) \quad (186)$$

Here are the steps.

1. Initialize  $x^0 = x$  and sample  $h^0$  from  $p(h | x^0)$ .
2. For  $k = 1, \dots, K$ ,
  - (a) Sample  $x^k$  from  $p(x | h^{k-1})$ .
  - (b) Sample  $h^k$  from  $p(h | x^k)$ .
3. Once you get  $\tilde{x} = x^K$ ,<sup>a</sup> use this to approximate

$$-\nabla_W \ln p(x) = \sum_h p(h | x) h x^T - \sum_{x,h} p(x, h) h x^T \approx \sum_h p(h | x) h x^T - \sum_h p(h | \tilde{x}) h \tilde{x}^T \quad (187)$$

$$-\nabla_b \ln p(x) = \sum_h p(h | x) h - \sum_{x,h} p(x, h) h \approx \sum_h p(h | x) h - \sum_h p(h | \tilde{x}) h \quad (188)$$

$$-\nabla_c \ln p(x) = \sum_h p(h | x) x - \sum_{x,h} p(x, h) x \approx \sum_h p(h | x) x - \sum_h p(h | \tilde{x}) \tilde{x} \quad (189)$$

We can tweak this procedure, such as **persistent CD**, where instead of initializing the chain to  $x^{(t)}$ , we can initialize the chain to the negative sample of the last iteration.

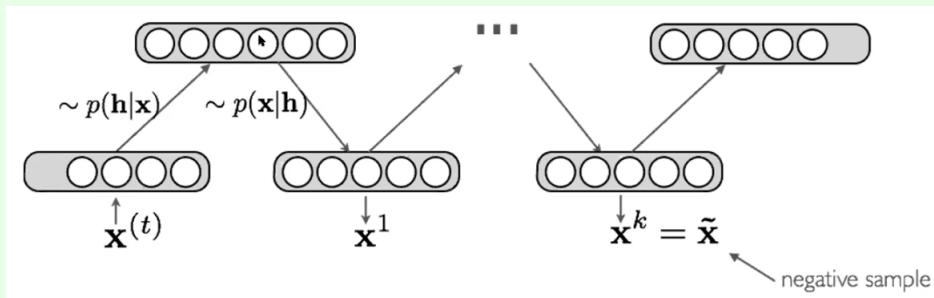


Figure 31: In general, the bigger  $k$  is, the less biased the estimate of the gradient will be, and in practice  $k = 1$  works well for learning good features. The reason this is called contrastive divergence is that in the gradient update step, we have a positive sample and a negative sample that both approximates the expected gradient, which contrasts to each other.

Therefore, contrastive divergence with  $k$  iterations gives us the **CD-k algorithm**.

<sup>a</sup>Note that we do not use  $\tilde{h} = h^K$ .

**Algorithm 6.2 (Fitting)**

Therefore, for updating  $\theta$ , we get the following

$$W = W - \alpha(\nabla_W(-\log p(x^{(t)}))) \quad (190)$$

$$= W - \alpha(\mathbb{E}_h[\nabla_W E(x^{(t)}, h) | x^{(t)}] - \mathbb{E}_{x,h}[\nabla_W E(x, h)]) \quad (191)$$

$$= W - \alpha(\mathbb{E}_h[\nabla_W E(x^{(t)}, h) | x^{(t)}] - \mathbb{E}_h[\nabla_W E(\bar{x}, h) | \bar{x}]) \quad (192)$$

$$= W + \alpha(h(x^{(t)})(x^{(t)})^T - h(\bar{x})\bar{x}^T) \quad (193)$$

and doing this over all three parameters leads to

$$W \leftarrow W + \alpha(h(x^{(t)})(x^{(t)})^T - h(\bar{x})\bar{x}^T) \quad (194)$$

$$b \leftarrow b + \alpha(h(x^{(t)}) - h(\bar{x})) \quad (195)$$

$$c \leftarrow c + \alpha(x^{(t)} - \hat{x}) \quad (196)$$

**Example 6.3 (Collaborative Filtering)**

Netflix dataset.

**6.2.2 Inference with Bernoulli-Bernoulli RBMs**

We have talked about RBMs of a general form, but the standard is that the hidden units are almost always Bernoulli, while the visible ones are either Bernoulli or Gaussian. Let's talk about when  $x, h$  are both Bernoulli, which allows us to simplify the general form of training.

**Definition 6.3 (Bernoulli-Bernoulli RBM)**

For now, let us assume that we are trying to estimate the distribution of a Bernoulli random vector  $x \in \{0, 1\}^D$  with Bernoulli latent variables  $h \in \{0, 1\}^F$ . Then, the energy of the joint configuration is

$$E(v, h; \theta) = -\sum_{ij} W_{ij} v_i h_j - \sum_i b_i v_i - \sum_j a_j h_j = -v^T Wh - b^T v - a^T h \quad (197)$$

where  $\theta = \{W, a, b\}$  are the model parameters.

Let's get some calculations out of the way.

**Lemma 6.1 (Conditional Distributions)**

For the Bernoulli RBM, we have

$$p(h_j = 1 | x) = \sigma(b_j + W_{j,:}x) \quad (198)$$

$$p(x_k = 1 | h) = \sigma(c_k + h^T W_{:,k}) \quad (199)$$

**Proof.**

Just use the definition of conditional probability and substitute the result below in the denominator. The terms will cancel out.

**Lemma 6.2 (Free Energy)**

For the Bernoulli RBM, we want to compute the marginal  $p(x)$  as

$$\begin{aligned} p(x) &= \frac{\exp(-F(x))}{Z} \\ &= \frac{1}{Z} \exp \left( c^T x + \sum_{j=1}^H \log (1 + \exp(b_j + W_{j,:}x)) \right) \\ &= \frac{1}{Z} \exp \left( c^T x + \sum_{j=1}^H \text{softplus}(b_j + W_{j,:}x) \right) \end{aligned}$$

where  $F$  is called the **free energy** and the softplus is defined.

$$\text{softplus}(x) = \ln(1 + e^x) \quad (200)$$

Therefore,  $p(x)$  is calculated by taking the product of these terms, which is why it's known as a **product of experts model**.

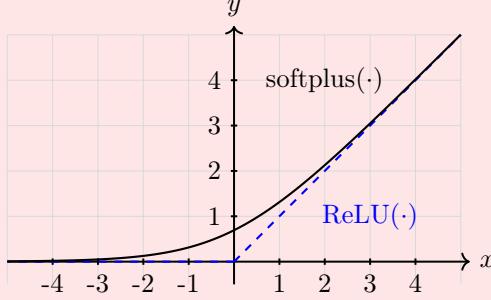


Figure 32: A graph of the softplus activation function, with the dotted ReLU.

**Proof.**

We have

$$p(x) = \sum_{h \in \{0,1\}^H} \exp(hWx + c^T x + b^T h)/Z \quad (201)$$

$$= \exp(c^T x) \sum_{h_1=0,1} \dots \sum_{h_H=0,1} \exp \left( \sum_j h_j W_{j,:} x + b_j h_j \right) / Z \quad (202)$$

$$= \exp(c^T x) \left( \sum_{h_1=0,1} \exp(h_1 W_{1,:} x + b_1 h_1) \right) \dots \left( \sum_{h_H=0,1} \exp(h_H W_{H,:} x + b_H h_H) \right) / Z \quad (203)$$

$$= \exp(c^T x) (1 + \exp(b_1 + W_{1,:}x)) \dots (1 + \exp(b_H + W_{H,:}x)) / Z \quad (204)$$

$$= \exp(c^T x) \exp \{ \log (1 + \exp(b_1 + W_{1,:}x)) \} \dots \exp \{ \log (1 + \exp(b_H + W_{H,:}x)) \} / Z \quad (205)$$

$$= \frac{1}{Z} \exp \left( c^T x + \sum_{j=1}^H \log (1 + \exp(b_j + W_{j,:}x)) \right) \quad (206)$$

When training, we can use the closed form to simplify our calculations.

$$\frac{\partial E(x, h)}{\partial W_{jk}} = \frac{\partial}{\partial W_{jk}} \quad (207)$$

and so

$$\mathbb{E}_h \left[ \frac{\partial E(x, h)}{\partial W_{jk}} \middle| x \right] = \mathbb{E}_h[-h_j x_k \mid x] = \sum_{h_j=0,1} -h_j x_k p(h_j \mid x) = -x_k p(h_j = 1 \mid x) \quad (208)$$

where the final term is a sigmoid. Hence, we have

$$\mathbb{E}_h[\nabla_W E(w, h) \mid x] = -h(x)x^T, \text{ where } h(x) := \begin{pmatrix} p(h_1 = 1 \mid x) \\ \vdots \\ p(h_H = 1 \mid x) \end{pmatrix} = \sigma(b + Wx) \quad (209)$$

Now we can substitute what we solved into the second expectation, but again this is infeasible to calculate

$$\mathbb{E}_{x,h} \left[ \frac{\partial E(x, h)}{\partial \theta} \right] = \sum_{x,h} h(x)x^T p(x, h) \quad (210)$$

### 6.2.3 Inference with Gaussian-Bernoulli RBMs

Now we can talk about Gaussian Bernoulli RBMs.

#### Definition 6.4 (Gaussian-Bernoulli RBM)

If we assume that  $v$  is a real-valued (unbounded) input that follows a Gaussian distribution (with  $h$  still Bernoulli), then we can add a quadratic term to the energy function

$$E(x, h) = -h^T Wx - c^T x - b^T h - \frac{1}{2}x^T x \quad (211)$$

In this case,  $p(x \mid h)$  becomes a Gaussian distribution  $N(c + W^T h, I)$ . The training process is slightly harder for this, so what we usually do is normalize the training set by subtracting the mean off each input and dividing the input by the training set standard deviation to get

$$E(v, h; \theta) = \sum_i \frac{(v_i - b_i)^2}{2\sigma_i^2} - \sum_{ij} W_{ij} h_j \frac{v_i}{\sigma_i} - \sum_j a_j h_j \quad (212)$$

You should also use a smaller learning rate  $\alpha$  compared to Bernoulli RBM.

#### Algorithm 6.3 (Implementation)

For an implementation with PyTorch, see [here](#).

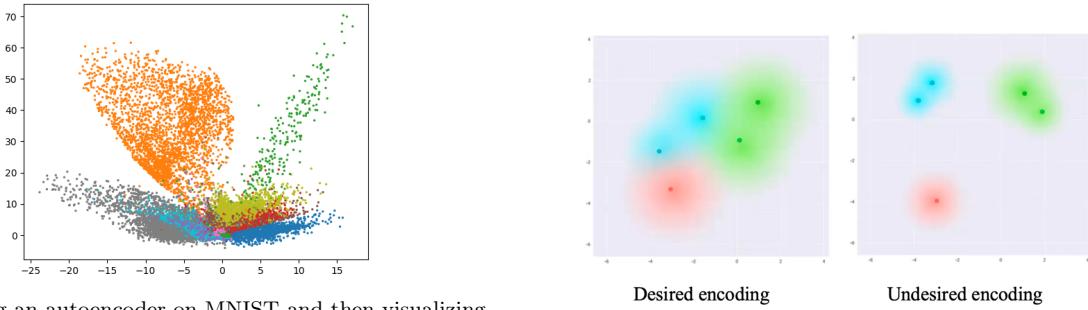
## 6.3 Deep Belief Network

So far, BMs and RBMs aren't really *deep* since they are shallow 2-layer networks, and I could have placed them in my machine learning notes in graphical models. However, RBMs provided the foundations for deep belief networks, a pivotal moment in deep learning, and thus they are considered part of the deep learning curriculum.

## 6.4 Hopfield Networks

## 7 Variational Autoencoders

Note that like linear latent variable models such as PCA, autoencoders “encode” our samples in a latent space, which we will call  $\mathcal{Z}$ . If we wanted to create a generative model from autoencoders, we can use the analogous transition from PCA to PPCA, by changing our points to distributions. Like in PPCA, we might want to define a standard Gaussian over the latent space  $\mathcal{Z}$  and transform this into the original space  $\mathcal{X}$ . However, there is a small problem with autoencoders. The latent space where the encoded vectors lie may not be contiguous, which means that the distribution of the latent space may not be very simple either. Look at the encodings of MNIST below. Trying to sample from this space with a isotropic Gaussian results in a high probability of hitting the “dead” zones which may give garbage generative results. If the space has discontinuities and you sample a variation from there, the decoder will simply generate an unrealistic output.



(a) Training an autoencoder on MNIST and then visualizing the encodings from a 2D latent space shows the formation of distinct clusters, but there are huge empty spaces where the labeling may be ambiguous and not allow us to interpolate effectively.

(b) Therefore, we want the encodings to be contiguous while still being distinct. This allows smooth interpolation which is easy to sample from with a simple pdf, e.g. Gaussian, and enables construction of *new* samples.

Figure 33

In 2013, Kigma introduced this generative model that bridges between latent variable models and deep neural nets. We can think of the relationship between the linear model PCA and its latent counterpart PPCA as the relationship between the nonlinear autoencoders and variational autoencoders. This is a good time to review linear and nonlinear latent variable models in my ML notes. Note that in a LVM, the family of functions  $\{D_\beta\}$  is used to map a latent variable  $z$  to the likelihood  $p(x | z)$ . This can be done by a direct transformation of the random variable  $Z$  (e.g. PPCA or as we will see later, *normalizing flows*), or we can have  $D_\beta(z)$  be an explicit parameterization (e.g. Gaussian mixture models and variational autoencoders). Given neural networks, we can do the latter method quite easily, and we are already familiar with the architectures to do so.

### Example 7.1 (Classification Nets Parameterize Multinomials)

In a classification neural network with parameters  $\beta$ , it takes in an input  $x$  and outputs a softmax vector  $f_\beta(x) = (p_1, \dots, p_K)^T$ . This basically means that  $f_\beta(x) = \theta$  parameterizes the conditional distribution (in this case, multinomial) of  $y$  given  $x$ .

$$Y | X = x \sim \text{Multinomial}(\theta = f_\beta(x)) \quad (213)$$

This is a much more efficient way to store conditional distributions than a  $\dim(X)(K - 1)$  lookup table.

Therefore, by generating a latent variable  $p(z)$  (that is simple and fixed), we can use a deep neural network  $D_\beta$  to generate  $\theta = D_\beta(z)$  which serve as the parameters of the conditional distribution  $p_\theta(x | z)$ , and then sampling from this distribution is easy because we assume that  $p_\theta(x | z)$  is in an explicitly parameterized

family of distributions. This allows us to easily sample from the joint distribution.

$$p_{\theta}(x, z) = p_{\theta}(x | z) p(z) \quad (214)$$

This is all great, but computing

$$p(x) = \int p(x, z) dz = \int p_{\theta}(x | z) p(z) dz \quad (215)$$

is computationally intractable. With strong assumptions, like conditional independence of not just  $p(x | z)$  but also  $p(z | x)$ , in RBMs, we can construct pretty good approximations. Recall that for RBMs, the derivative of the log of  $p(x)$  decomposes into a positive phase that requires you to integrate over  $p(z | x)$ , which is easy, and  $p(x, h)$ , which is hard to do in general. But through contrastive divergence, we can approximate the integral by sampling a  $\tilde{x}$  and constructing another integral over  $p(z | x)$ , which is then easy to compute.

### Example 7.2 (Bernoulli-Bernoulli RBM)

We would like to approximate a  $d$ -dimensional Bernoulli vector  $x$  with a latent variable  $z \in \mathbb{R}^K$ . We will assume a prior  $p(z) \sim N(0, I)$ , and let us have a neural net  $D_{\beta}$  that parameterizes the random vector  $x$ , where  $x_i \sim \text{Bernoulli}(\theta_i)$  for  $\theta_i$ . Then, by conditional independence,

$$p(x | z) = \prod_{i=1}^d p_{\theta}(x_i | z) = \prod_{i=1}^d \theta_i^{x_i} (1 - \theta_i)^{1-x_i} = \prod_{i=1}^d [D_{\beta}(z)]_i^{x_i} (1 - [D_{\beta}(z)]_d)^{1-x_i} \quad (216)$$

and we can see that since  $p$  has the flexibility of whatever vector in  $[0, 1]^D$  it can be captured by the neural net  $D_{\beta}$ . It encompasses a broad family of Bernoulli probability distributions. We can see that we have some method to compute  $p(x | z)$ . We train a neural net (somehow) and do forward prop on it to generate the correct parameters modeling the distribution of  $x$ . Note that in RBMs the conditional independence allowed us to integrate over  $z$  easily. To see why, in the example above, the integral becomes

$$p(x) = \sum_{z \in \{0,1\}^k} \left\{ \prod_{i=1}^d [D_{\beta}(z)]_i^{x_i} (1 - [D_{\beta}(z)]_d)^{1-x_i} \right\} p(z) \quad (217)$$

where  $k$  is the dimension of the latent space. However, integrating over all  $z$ 's for more complex spaces is not feasible.

$D_{\beta}$  is clearly nonlinear and we can't just do some simple closed form optimization, so we must use the tools introduced in nonlinear latent variable models. Namely, we revisit the variational lower bound. Recall that estimating the true  $p(x)$  can be reduced to the problem of finding a good approximate of the true  $p(z | x)$ , the *posterior* or *inference component*, with some family of distributions  $\{q_{\phi}\}$ . Just like the generation model, we can build another neural network  $E_{\alpha}$  such that  $\phi = E_{\alpha}(x)$  parameterizes the conditional distribution of  $z$ , called our *encoder*.

$$p(z | x) \approx q_{\phi}(z | x) = q_{E_{\alpha}(x)}(z) \quad (218)$$

### Example 7.3 (Encoder Neural Net Generates Parameters of Likelihood)

If  $\phi = (\mu, \sigma)$ , where  $\sigma$  is just the vector representing variances of independent Gaussians, then we can use the neural network  $E$  to get  $\phi = E_{\alpha}(x)$ . In the example,  $\phi = (\mu, \log \sigma^2)$  since we want to allow negative values, and

$$q_{\phi}(z | x) \sim \mathcal{N}(E_{\alpha}(x)) = \mathcal{N}(\phi) = \mathcal{N}(\mu, \sigma^2) \quad (219)$$

Therefore, by modeling both the likelihood and posterior with probability distributions that can be parameterized by an output of neural networks, we have a *variational autoencoder*.

### Definition 7.1 (Variational Autoencoders)

In a **variational autoencoder (VAE)**, we assume that the covariates  $x^{(i)} \sim X$  are generated as the marginal of a joint distribution  $p(x, z)$  with latent variable  $z \sim Z$ . We model the sub-distributions as such:

1. We assume that the prior  $p(z)$  is of fixed simple form, e.g. a standard Gaussian.
2. We assume that the likelihood  $p(x | z)$  can be approximated by a parameteric family of distributions  $p_\theta(x | z)$ , where  $\theta = D_\beta(z)$  is generated by a **decoder** neural network parameterized by  $\beta$ .
3. We assume that the posterior  $p(z | x)$  can be approximated by a parameteric family of distributions  $q_\phi(z | x)$ ,<sup>a</sup> where  $\phi = E_\alpha(x)$  is generated by an **encoder** neural network parameterized by  $\alpha$ .

We can optimize  $\theta, \lambda$  by equivalently optimizing the parameters  $\alpha, \beta$  of the nets. Once this is done,

1. To conduct inference, we can input in some data  $x$  and retrieve the distribution of its latent representation as  $q_{E_\alpha(x)} \approx p(z | x)$ .
2. To generate data, we can sample  $z$  from  $p(z)$  and sample from  $p_{D_\beta(z)}(x) \approx p(x | z)$ .

<sup>a</sup>Note that this is an assumption! The posterior may be an arbitrary shape or form.

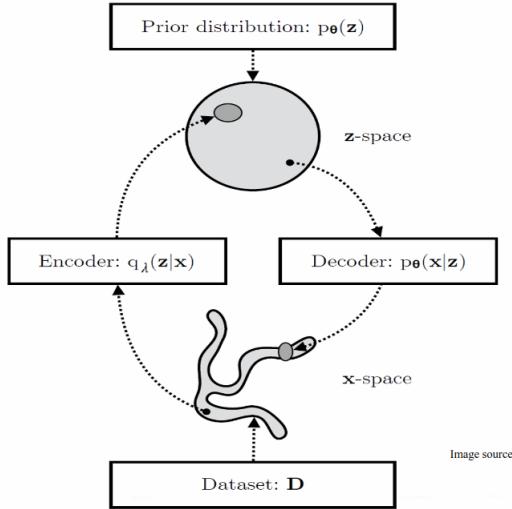


Figure 34: A pictorial diagram of a nonlinear latent variable model to refresh your memory.

So how do we actually train this? Just like with every other nonlinear latent variable models, we can use the evidence lower bound. We do a quick review. Recall that the KL divergence can be decomposed into the sum of conditional entropies, and hence we can use the fact the KL divergence is always nonnegative to create this bound.

$$\log p_\theta(x) = KL(q_\phi(z | x) || p_\theta(z | x)) + \mathbb{E}_{q_\phi(z|x)}[\log p_\theta(x, z)] - \mathbb{E}_{q_\phi(z|x)}[\log q_\phi(z | x)] \quad (220)$$

$$\geq \mathbb{E}_{q_\phi(z|x)}[\log p_\theta(x, z)] - \mathbb{E}_{q_\phi(z|x)}[\log q_\phi(z | x)] = \text{ELBO}(x, \phi, \theta) \quad (221)$$

and therefore by summing over all the data points we can get the evidence lower bound, which holds for any set of distributions  $q_\phi^{(1)}, \dots, q_\phi^{(N)}$ .

$$\sum_{i=1}^N \log p_\theta(x^{(i)}) \geq \sum_{i=1}^N \mathbb{E}_{q_\phi(z|x^{(i)})}[\log p_\theta(x^{(i)}, z)] - \sum_{i=1}^N \mathbb{E}_{q_\phi(z|x^{(i)})}[\log q_\phi(z | x^{(i)})] = \text{ELBO}(\mathcal{D}, \phi, \theta) \quad (222)$$

Therefore, minimizing the KL divergence is equivalent to maximizing the ELBO w.r.t.  $\theta$  and  $\phi$ . As we have seen in my ML notes, the gradient of the ELBO w.r.t.  $\theta$  be solved by computing the gradient directly and using SGD. However, taking the gradient w.r.t.  $\phi$  is more complicated since we cannot put the gradient in the expectation (since we are deriving and integrating w.r.t.  $\phi$ ). We can use the log-derivative trick<sup>12</sup>, but this is known to have high variance and is not sufficient to backpropagate huge neural nets. This is not actually the biggest problem either, as we will see that the extra parameters we've introduce with the neural nets do not allow us to backpropagate across stochastic variables.

Now we talk about more implementation details presented in the paper, which is a simplified form.

1. The first is that [KW22] fixes a prior isotropic multivariate Gaussian  $p_\theta(z) = \mathcal{N}(0, I)$ , which lacks parameters.
2. It also assumes that  $p_\theta(x | z)$  be a multivariate Gaussian (for real-valued data) or Bernoulli (in binary data). This gives us a nice parameteric form that may hopefully approximate the true posterior, which may be extremely complicated.

$$p_\theta(x | z) = \mathcal{N}(\mu^{(i)}, \sigma^{2(i)} I) \quad \theta = \{\mu^{(i)}, \sigma^{2(i)}\} = D_\beta(z^{(i)}) \quad (223)$$

$$p_\theta(x | z) = \text{Bernoulli}(\theta) \quad \theta = D_\beta(z^{(i)}) \quad (224)$$

3. It finally assumes that the true posterior  $p_\theta(z | x)$ , which is intractable, takes on a form  $q_\phi(z | x)$  that can be approximated by a Gaussian with diagonal covariance.

$$q_\phi(z | x^{(i)}) = \mathcal{N}(\mu^{(i)}, \sigma^{2(i)} I) \quad \phi = \{\mu^{(i)}, \sigma^{2(i)}\} = E_\alpha(x^{(i)}) \quad (225)$$

So let's walk through the forward propagation with the likelihood set to Bernoulli. We have a dataset  $\{x^{(i)}\}$ . For each  $x^{(i)}$

1. We put it into our encoder network and get out the parameters  $\phi^{(i)} = E_\alpha(x^{(i)})$  for our latent Gaussian. We output the mean  $\mu_\alpha^{(i)}$  and either the variance  $(\sigma_\alpha^{(i)})^2$ , or the log-variance  $\log(\sigma_\alpha^{(i)})^2$ .<sup>13</sup>
2. We sample a  $z^{(i)}$  from this Gaussian and feed it into the decoder network  $D_\beta(z^{(i)})$ , which returns the parameters  $\theta^{(i)} = D_\beta(z^{(i)})$  for our Bernoulli likelihood.
3. We sample  $\hat{x}^{(i)}$  from this Bernoulli and retrieve another sampled version of our input.

Great, so we can draw a computation graph for this, but before we do, let's revisit the basics and draw a simpler example.

#### Example 7.4 (Softmax)

In the graph below, note that our “prediction”  $\hat{y}^{(i)}$  for the data point  $x^{(i)}$  is not really a prediction at all. If we have three categories (cat, dog, fish) and I give you an image, the model will output a vector of probabilities, e.g.  $\hat{y}^{(i)} = [0.1, 0.2, 0.7]$ . While we can easily infer that the probability of a fish is highest, and therefore should be our prediction, the model didn't actually output one answer. Rather, we should interpret this output vector  $\hat{y}^{(i)}$  as a *parameter*  $\theta$  of a multinomial distribution. From this we can *sample* an actual prediction  $\hat{y}^{(i)} \sim \text{Multinomial}(\theta)$ .

When we compute the loss of a sample, we compute the likelihood by taking the true output  $y^{(i)}$  and one-hot encoding it. One-hot encoding allows us to convert the label  $y^{(i)}$  into a parameter of a

<sup>12</sup>explained in my ML notes

<sup>13</sup>Since variances must always be positive, sometimes a slight tweaking of transformations is needed. For example, if an encoder network has a final linear layer, then the variances may not be always positive, which is a problem, so we may do an exponential or a ReLU at the end. You may notice that the log may often return negative numbers, but as we will see later, we can add a corresponding transformation in our *reparamaterization trick*, which will exponentiate the log-variances (this is how it's implemented in the code) before using them as variances. Calculating the log-variance first and then exponentiating it may also bring better numerical stability.

multinomial itself, and this process is hidden inside  $\ell$ . Therefore we want to maximize

$$\log p(y^{(i)} | x^{(i)}) = p_{\hat{\theta}^{(i)}}(y^{(i)}) = \sum_j y_j^{(i)} \log \hat{\theta}_j^{(i)} \quad (226)$$

which is the cross entropy.

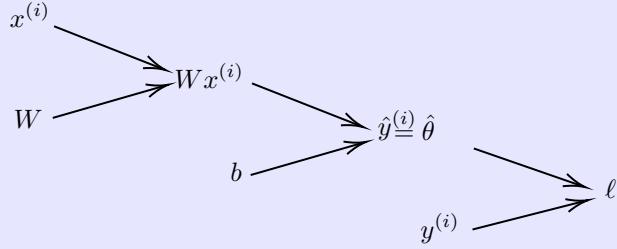


Figure 35: When we draw a computation graph to visualize the backpropagation of a softmax regression function, note that we need to have the gradients start from the log-likelihood  $\ell$  and reach “back” to  $W$  and  $b$ , our model parameters.

Another way to approximate the log likelihood  $\ell$  is to simply take the output parameter  $\hat{\theta}^{(i)}$ , keep on sampling  $y$ 's from it, penalizing when needed, and averaging the penalties.<sup>a</sup>

$$\log p(y^{(i)} | x^{(i)}) = \log \mathbb{E}_{y \sim \hat{\theta}^{(i)}} [\mathbb{1}_{y^i=y}] \quad (227)$$

$$= \log \int \mathbb{1}_{y^{(i)}=y} p_{\hat{\theta}^{(i)}}(y) dy \quad (228)$$

$$\approx \log \left\{ \frac{1}{N} \sum_{l=1}^L \mathbb{1}_{y^{(i)}=y^{(i,l)}} \right\} \quad (229)$$

where  $y^{(i,l)} \sim \text{Multinomial}(\hat{\theta}^{(i)})$ .

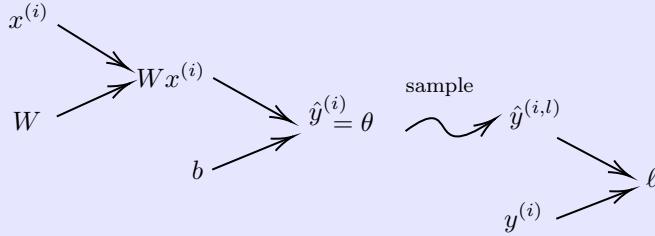


Figure 36: Note that since it's much harder to sample and converge onto a good approximation, it's tougher to go through the curly arrow. That is, it is harder to backpropagate through **stochastic nodes**.

Therefore, we can think of backpropagating as either one of two things. Either backpropagate straight through the parameter like we did first, or sample from the estimated distribution and sum up to approximate the samples.

<sup>a</sup>This is useful if we can easily sample, but do not know the closed form of the likelihood distribution.

Let's keep this in the back of our mind, and focus on the computation for a bit. By the simplifying form that  $q_\phi$  is a Gaussian, we can even get a nearly closed form of the ELBO.

**Theorem 7.1 ()**

Given the assumptions above,

$$\text{ELBO}(x, \phi, \theta) := \mathbb{E}_{q_\phi(z|x)}[\log p_\theta(x | z)] + \mathbb{E}_{q_\phi(z|x)}[\log p(z)] - \mathbb{E}_{q_\phi(z|x)}[\log q_\phi(z | x)] \quad (230)$$

$$= \mathbb{E}_{q_\phi(z|x)}[\log p_\theta(x | z)] + \frac{1}{2} \sum_{d=1}^D \left( 1 + \log((\sigma_d)^2) - (\mu_d)^2 - (\sigma_d)^2 \right) \quad (231)$$

Therefore, the derivative of last two terms are *exact*, i.e. we don't need to estimate them with SGD.

**Proof.**

Let's evaluate the last two expectations.

$$\mathbb{E}_{q_\phi(z|x)}[\log p(z)] = \int \log p(z) \cdot q_\phi(z | x) dx \quad (232)$$

$$= \int \log\{\mathcal{N}(z | 0, I)\} \cdot \mathcal{N}(z | \mu, \sigma^2) dz \quad (233)$$

$$= -\frac{D}{2} \log(2\pi) - \frac{1}{2} \sum_{d=1}^D \mu_d^2 + \sigma_d^2 \quad (234)$$

$$\mathbb{E}_{q_\phi(z|x)}[\log q_\phi(z | x)] = \int \log q_\phi(z | x) q_\phi(z | x) dz \quad (235)$$

$$= \int \log\{\mathcal{N}(z | \mu, \sigma^2)\} \mathcal{N}(z | \mu, \sigma^2) dx \quad (236)$$

$$= -\frac{D}{2} \sum_{d=1}^D 1 + \log(\sigma_d^2) \quad (237)$$

**Corollary 7.1 (Bernoulli Likelihood)**

If  $p_\theta(x | z)$  is Bernoulli, then the ELBO can be estimated by estimating the likelihood

$$\text{ELBO}(x, \phi, \theta) = \frac{1}{L} \sum_{l=1}^L + \frac{1}{2} \sum_{d=1}^D \left( 1 + \log((\sigma_d)^2) - (\mu_d)^2 - (\sigma_d)^2 \right) \quad (238)$$

With these two things, let's take a look at the computation graph of the VAE.

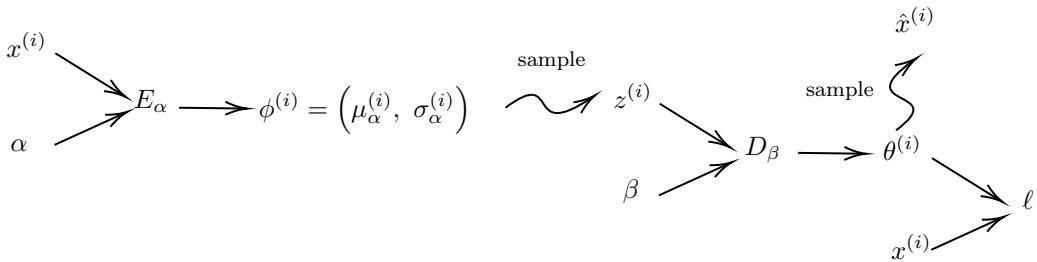


Figure 37: Computational graph of a VAE.

Note that since we have shown that the derivative of the last two expectations (i.e. the derivative of the KL divergence) is dependent on the outputs  $\sigma$  and  $\mu$  of the neural net, we must also backpropagate amongst them as well, which is why you see the giant arrow from  $\phi$  to  $\ell$ .

We can see that since we know the closed form of  $p_\theta(x | z)$ , backpropagating over  $\theta^{(i)}$  is no problem. However, we must reach  $\alpha$  to update the neural network weights, and to do this we must go backprop through the stochastic node  $z^{(i)}$ , which may stump you. In fact, how do you even backpropagate against something that's a random variable? Remember that in our softmax example, we could simply compute the log likelihood of a bunch of samples at this node to get an approximate average log likelihood. This is a start, but in this case we want to compute the *gradient* of the log likelihood. Fortunately, the *log-derivative trick*<sup>14</sup> allows us to swap the gradient and expectation under a certain form, putting the expectation on the outside and therefore allowing us to sample gradients.

$$\nabla_\phi \mathbb{E}_{q_\phi(z)}[f(z)] = \mathbb{E}_{q_\phi(z)}[f(z) \nabla_\phi \log q_\phi(z)] \quad (239)$$

So we apply the same idea by sampling  $z^{(1)}, \dots, z^{(L)}$  from the Gaussian with parameters  $\phi^{(i)}$  and for each sample we fix  $z^{(l)}$ , allowing us to backpropagate to  $\alpha$  to get a noisy estimate. By averaging these noisy gradients we have an approximation of the true gradient w.r.t.  $x^{(i)}$ .<sup>15</sup> Unfortunately, when doing this for gradients the variance tends to be very high up to a point where it is impractical, and even with a lot of sampling this frequently undershoots or overshoots the actual gradient. Therefore, we must come up with an alternative solution to estimate the gradient efficiently.

## 7.1 Reparameterization Trick

In 2013, Durk Kigma, then a PhD student in machine learning at the University of Amsterdam, introduced a solution in [KW22] called the *reparameterization trick*, which is just an application of a change of basis.

### Theorem 7.2 (Reparameterization Trick)

Let  $q_\phi(z|x)$  be a continuous distribution that can be sampled by first sampling  $\epsilon \sim p(\epsilon)$  from a parameter-free distribution and then applying a differentiable transformation  $g_\phi(\epsilon, x)$ . Then:

$$\nabla_\phi \mathbb{E}_{q_\phi(z|x)}[f(z)] = \nabla_\phi \mathbb{E}_{p(\epsilon)}[f(g_\phi(\epsilon, x))] = \mathbb{E}_{p(\epsilon)}[\nabla_\phi f(g_\phi(\epsilon, x))] \quad (240)$$

or in integrals,

$$\nabla_\phi \int f(z) q_\phi(z | x) dz = \nabla_\phi \int f(g_\phi(\epsilon, x)) p(\epsilon) d\epsilon = \int \nabla_\phi f(g_\phi(\epsilon, x)) p(\epsilon) d\epsilon \quad (241)$$

where  $f$  is any differentiable function.

### Proof.

We clearly state our assumptions:

- We have a distribution  $q_\phi(z|x)$  that can be reparameterized using  $g_\phi(\epsilon, x)$
- $\epsilon$  is sampled from a parameter-free distribution  $p(\epsilon)$
- $g_\phi$  is differentiable with respect to  $\phi$
- $f$  is any differentiable function

The first equality to prove is:

$$\nabla_\phi \mathbb{E}_{q_\phi(z|x)}[f(z)] = \nabla_\phi \mathbb{E}_{p(\epsilon)}[f(g_\phi(\epsilon, x))]$$

This follows directly from the reparameterization property. Since  $z = g_\phi(\epsilon, x)$  where  $\epsilon \sim p(\epsilon)$ , we can rewrite any expectation over  $q_\phi(z|x)$  as an expectation over  $p(\epsilon)$ :

$$\mathbb{E}_{q_\phi(z|x)}[f(z)] = \mathbb{E}_{p(\epsilon)}[f(g_\phi(\epsilon, x))]$$

<sup>14</sup>Mentioned in my ML notes

<sup>15</sup>This like a SGD inside a SGD, since we're sampling over minibatches of the samples  $x^{(i)}$  as well.

Taking  $\nabla_\phi$  of both sides gives us the first equality. The second equality to prove is:

$$\nabla_\phi \mathbb{E}_{p(\epsilon)}[f(g_\phi(\epsilon, x))] = \mathbb{E}_{p(\epsilon)}[\nabla_\phi f(g_\phi(\epsilon, x))] \iff \nabla_\phi \int f(g_\phi(\epsilon, x))p(\epsilon)d\epsilon = \int \nabla_\phi f(g_\phi(\epsilon, x))p(\epsilon)d\epsilon \quad (242)$$

To justify exchanging the gradient and integral, we invoke the Leibniz integral rule. This exchange is valid when  $f \circ g_\phi$  is differentiable with respect to  $\phi$  (given in our assumptions), the domain of integration (support of  $p(\epsilon)$ ) is independent of  $\phi$ , and there are suitable integrability conditions (which we assume hold). Then we exchange the gradient and expectation:

$$\nabla_\phi \int f(g_\phi(\epsilon, x))p(\epsilon)d\epsilon = \int \nabla_\phi f(g_\phi(\epsilon, x))p(\epsilon)d\epsilon \quad (243)$$

A crucial observation is that  $p(\epsilon)$  does not depend on  $\phi$  (it is parameter-free), which is essential for this exchange to work.

$$\nabla_\phi \mathbb{E}_{q_\phi(z|x)}[f(z)] = \nabla_\phi \mathbb{E}_{p(\epsilon)}[f(g_\phi(\epsilon, x))] = \mathbb{E}_{p(\epsilon)}[\nabla_\phi f(g_\phi(\epsilon, x))] \quad (244)$$

This result is fundamental to variational inference and deep learning, particularly in training Variational Autoencoders (VAEs). The key insight is that by reparameterizing the random variable  $z$  in terms of a parameter-free random variable  $\epsilon$ , we can separate the stochastic sampling (which is not differentiable) from the deterministic transformation  $g_\phi$  (which is differentiable).

The biggest advantage to this is that we although we do not avoid sampling to approximate the log likelihood, the rate at which it converges is much faster than simple sampling or the log-derivative trick, which is demonstrated in the example below.

### Example 7.5 (Gradient of Expectation of $f(x) = x^2$ w.r.t. Gaussian)

Assume we have a normal distribution  $q$  that is parameterized by  $\phi$ , specifically  $q_\phi(x) = N(\phi, 1)$ . We want to solve the below problem

$$\min_\phi \mathbb{E}_q[x^2] \quad (245)$$

This is of course a rather silly problem and the optimal  $\phi = 0$  is obvious. One way to calculate  $\nabla_\phi \mathbb{E}[x^2]$  is using the log-derivative trick as follows

$$\nabla_\phi \mathbb{E}_q[x^2] = \nabla_\phi \int q_\phi(x)x^2dx \quad (246)$$

$$= \int x^2 \nabla_\phi q_\phi(x) \frac{q_\phi(x)}{q_\phi(x)} dx \quad (247)$$

$$= \int q_\phi(x) \nabla_\phi \log q_\phi(x) x^2 dx \quad (248)$$

$$= \mathbb{E}_q[x^2 \nabla_\phi \log q_\phi(x)] \quad (249)$$

For our example where  $q_\phi(x) = N(\phi, 1)$ , this method gives

$$\nabla_\phi \mathbb{E}[x^2] = \mathbb{E}_q[x^2(x - \phi)] \quad (250)$$

and we can sample from  $q \sim N(\phi, 1)$ . Reparameterization trick is a way to rewrite the expectation so that the distribution with respect to which we take the gradient is independent of parameter  $\phi$ . To achieve this, we need to make the stochastic element in  $q$  independent of  $\phi$ . Hence, we write  $x$  as

$$x = \phi + \epsilon, \quad \epsilon \sim N(0, 1) \quad (251)$$

Then, we can write

$$\mathbb{E}_q[x^2] = \mathbb{E}_\epsilon[(\phi + \epsilon)^2] \quad (252)$$

where  $p(\epsilon)$  is the distribution of  $\epsilon$ , i.e.,  $N(0, 1)$ . Now we can write the derivative of  $\mathbb{E}_q[x^2]$  as follows

$$\nabla_\phi \mathbb{E}[x^2] = \nabla_\phi \mathbb{E}_p[(\phi + \epsilon)^2] = \mathbb{E}_p[2(\phi + \epsilon)] \quad (253)$$

If we actually plot the variances, for sample sizes of  $N = 10, 100, 1000, 10000, 100000$ , we can see that the reparameterization trick produces estimates where the variances of the sampling distribution is an order of magnitude smaller.

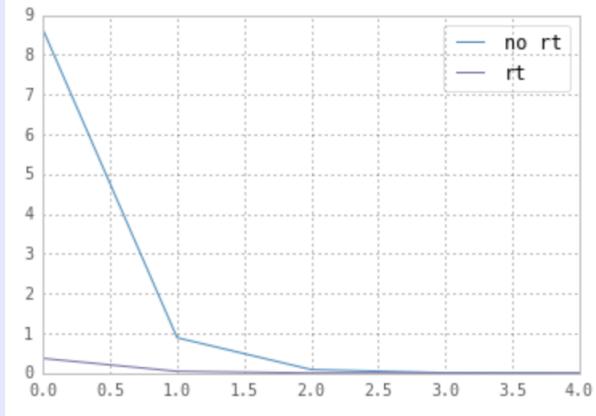


Figure 38: Credits to here.

Therefore, given that  $\phi_\mu = \mu^{(i)}$  and  $\phi_\sigma = (\sigma^{(i)})^2$  are the outputs of our encoder neural net, our transformation is

$$g_\phi(x, \epsilon^{(l)}) = \phi_\mu + \sqrt{\phi_\sigma} \odot \epsilon^{(l)} = \mu^{(i)} + \sigma^{(i)} \odot \epsilon^{(l)} \quad \epsilon^{(l)} \sim \mathcal{N}(0, I) \quad (254)$$

or in the log-variance case, where the encoder outputs  $\phi_\sigma = \log(\sigma^{(i)})^2 = 2 \log \sigma^{(i)}$ , we have

$$g_\phi(x, \epsilon^{(l)}) = \mu^{(i)} + e^{\phi_\sigma/2} \odot \epsilon^{(l)} = \mu^{(i)} + \sigma^{(i)} \odot \epsilon^{(l)} \quad \epsilon^{(l)} \sim \mathcal{N}(0, I) \quad (255)$$

where  $\odot$  is element-wise multiplication, can be used to model  $p(z)$ .<sup>16</sup> The intuition behind this is to “push” the stochastic node  $z^{(i)}$  back so that we don’t have to go through it to reach  $\alpha$ . Therefore, to compute the noisy gradient for  $\alpha$ , we can sample  $\epsilon^{(l)} \sim \mathcal{N}(0, I)$  and treat it as a fixed variable when doing backpropagation, which essentially means that the mapping  $g_\phi$  is a deterministic function (and so  $g_\phi \circ E_\alpha$  is a deterministic neural net). Then we do this  $L$  times to get  $L$  gradients, and average them to get the unbiased estimate of the gradient of the single sample  $x^{(i)}$ . Then we must do this for all  $x^{(i)}$  in a minibatch in SGD. Since this is still too computationally heavy, we usually set  $L = 1$ .

<sup>16</sup>This is called **factorized Gaussian posterior**, but it can be extended to the **full-variance Gaussian posterior** where the variance is parameterized through a lower triangular matrix  $L$ , from the Cholesky decomposition.

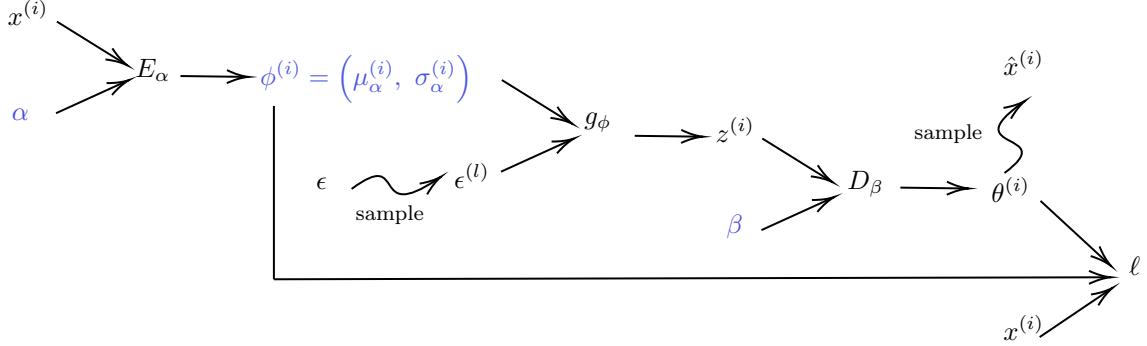


Figure 39: Note that the  $\epsilon$  variable was added into the graph, and the blue variables are the parameters we want to backpropagate and optimize. Therefore the path from  $\ell$  to  $\alpha$  does not directly go through a stochastic node. Note that autograd calculates gradients for  $\phi$  while on its way to  $\alpha$ . But since  $\ell$  is directly dependent on  $\phi^{(i)}$ , we want to make sure to update the  $\phi^{(i)}$  directly with a step in the right direction. The rest of the parameters, while they do have their gradients computed, do not need to be updated with a step. A similar figure on a smaller scale can be found in Kigma's workshop presentation in NIPS.

Another advantage is that this is more general. Although we must meet the conditions that the posterior  $p_\phi(z | x)$  should be an absolutely continuous distribution that can be modeled as the transformation of a simple random variable  $\epsilon$ , since any distribution that is differentiable with respect to its parameters can be reparametrized by inverting the multivariate CDF function and applying the implicit method.

In order to see how the gradients are calculated, recall the following theorem.

### Theorem 7.3 (Change of Basis)

We have

$$\log q_\phi(z | x) = \log p(\epsilon) - \log \left| \det \left( \frac{\partial z}{\partial \epsilon} \right) \right| \quad (256)$$

where  $\partial z / \partial \epsilon$  denotes the Jacobian matrix computed through  $g_\phi(x, \epsilon)$ .

### Corollary 7.2 ()

This applied to the affine function  $g_\phi$  above defined for the log-variance gives

$$\frac{\partial z}{\partial \epsilon} = \text{diag}(\sigma) \implies \log \left| \det \left( \frac{\partial z}{\partial \epsilon} \right) \right| = \sum_i \log \sigma_i \quad (257)$$

### Corollary 7.3 (Auto-Encoding VB (AEVB) Algorithm)

Applying the reparameterization trick to the gradient of the ELBO gives the following corollary.

$$\nabla_\phi \text{ELBO}(x, \phi, \theta) = \mathbb{E}_{p(\epsilon)} [\nabla_\phi \log p_\theta(x | z) - \nabla_\phi \log q_\phi(z | x) + \nabla_\phi \log p(z)] \quad (258)$$

Therefore we can unbiasedly approximate the gradient by sampling  $L$  points  $\epsilon^{(1)}, \dots, \epsilon^{(L)}$  from  $p(\epsilon)$ , transforming them to  $z^{(1)}, \dots, z^{(L)}$  through the function  $g_\phi$ , and finally computing the gradient of the log posterior (which is easy since we know the closed form of the conditional distribution given

$z$ ), and finally averaging them.

$$\begin{aligned}\nabla_{\phi} \text{ELBO}(x, \phi, \theta) &\approx \frac{1}{L} \sum_{l=1}^L [\nabla_{\phi} \log p_{\theta}(x | z^{(l)}) - \nabla_{\phi} \log q_{\phi}(z^{(l)} | x) + \nabla_{\phi} \log p(z^{(l)})] \\ &= \frac{1}{L} \sum_{l=1}^L [\nabla_{\phi} \log p_{\theta}(x | g_{\phi}(\epsilon^{(l)}, x)) - \nabla_{\phi} \log q_{\phi}(g_{\phi}(\epsilon^{(l)}, x) | x) + \nabla_{\phi} \log p(g_{\phi}(\epsilon^{(l)}, x))]\end{aligned}$$

which is guaranteed to converge by the law of large numbers, and furthermore we can do this for any batch size  $L$ .

Really the VAEs were just a straightforward application of CAVI with the reparamaterization trick, plus the extra variables  $\alpha, \beta$  that are used to generate the  $\theta, \phi$ .

#### Algorithm 7.1 (Implementation of VAE)

To see an implementation of a VAE with PyTorch, see [here](#).

## 7.2 Importance Weighted Autoencoders

## 7.3 Conditional VAEs

Note that once our VAE is trained, we have no control on the data generation process. That is, if we want to generate only the digit 2, we can't since we must just sample from the Gaussian  $p(z)$  in the latent space. Therefore, conditioning all the distributions on what we want is the objective of *conditional VAEs*, which uses the *conditional ELBO*.

#### Definition 7.2 (Conditional ELBO)

The **conditional ELBO** of  $x, \theta, \phi$  given some conditioning vector  $c^a$ , is defined

$$\mathbb{E}_{q_{\phi}(z|x)} [\log p_{\theta}(x | z, c) - \text{KL}(q_{\phi}(z | x, c) || p(z | c))] \quad (259)$$

<sup>a</sup>Analogous to the digit we want in MNIST.

## 8 Generative Adversarial Networks

The year after Kigama published his paper on VAEs, Ian Goodfellow in 2014 published [GPAM<sup>+</sup>14] on *generative adversarial networks*. Unlike the current generative models, which relied on “fancy” methods like variational Bayes or contrastive divergence, Goodfellow claimed that we can just do this with vanilla MLPs. The general idea is to approximate the true density  $p^*(x)$ , you are trying to build a function (a neural network)  $G_\alpha$  that is a transformation of a simple latent variable, e.g.  $Z \sim \mathcal{N}(0, 1)$ , such that the pdf of  $G_\alpha(Z)$  is similar to  $p^*(x)$ .

Remember that for the generative models that we have so far, we were able to *explicitly model* the true pdf.

1. *Explicit and Analytical.* The simplest types of densities can be analytically written and can be sampled from directly (e.g. Gaussian with inverse CDF, Box-Muller transform, and even GMMs).
2. *Explicit and Approximate.* More complicated models such as the RBM and VAE cannot be analytically written, but can still be directly sampled from with probabilities. Boltzmann machines approximate the explicit density as  $p_\theta(x) = \frac{1}{Z} e^{-E(x,z)}$  for some quadratic term  $-E(x, z)$ . VAEs construct another family of posterior distributions  $\{q_\lambda\}$  where each  $\lambda$  is the output of an encoder neural network  $E_\alpha$ . Later on, we will see that normalizing flows and autoregressive models also fall in this category.
3. *Implicit.* GANs approximate the true pdf through a transformation of random variables and are implicit in the way that you can't estimate the probabilities but you can still sample from them.<sup>17</sup>

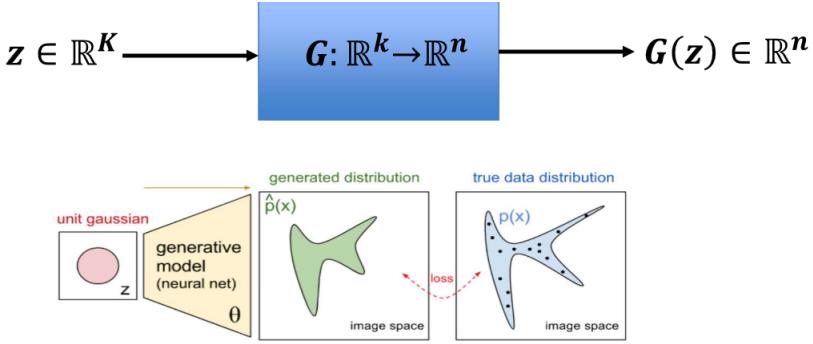


Figure 40: You essentially want to take some simple latent distribution and construct a differentiable a **generator model** that maps it to a more complicated distribution in the observable space.

The problem with VAEs is that they tend to generate blurry images, which is the result of optimizing a variational lower bound rather than the true objective. This makes it easy to identify whether a given image is from the true dataset or has been artificially generated. In contrast, GANs generate high-resolution images because we are directly optimizing the true objective.

### Definition 8.1 (Generative Adversarial Networks)

A **generative adversarial network (GAN)** is a nonlinear latent-variable model consisting of by optimizing a pair of generator and discriminator neural networks, which play a game where one tries to beat the other.

1. A latent random variable  $Z$  with pdf  $p(z)$ .
2. The **generator** tries to generate fake samples to fool the discriminator. We sample from a latent space  $\mathbf{z}$  and run that through the neural network to get  $\mathbf{x} = \mathcal{G}_{\theta_g}(\mathbf{z})$ . It should be differentiable, but does not have to be invertible.
3. The **discriminator** tries to distinguish between real and fake samples, like a critic which can tell

<sup>17</sup>Given  $Z \sim \mathcal{N}(0, 1)$  and the sine function  $f(z) = \sin(z)$ , it's hard to analytically compute the pdf of  $X = f(Z)$ . However, to sample from this, we can just sample  $z$  from  $Z$  and then transform it through  $f$ .

from real from fake. It should also be differentiable, and its output is essentially  $0 \leq \mathcal{D}_{\theta_d}(\mathbf{x}) \leq 1$ , with a value of 1 if real, 0 if fake.

We want to train these two models against each other, and in the end, we throw  $\mathcal{D}$  away, since it's only role is to force  $\mathcal{G}_{\theta_g}$  to work harder, which leaves us with a really good generative  $\mathcal{D}_{\theta_g}$ .

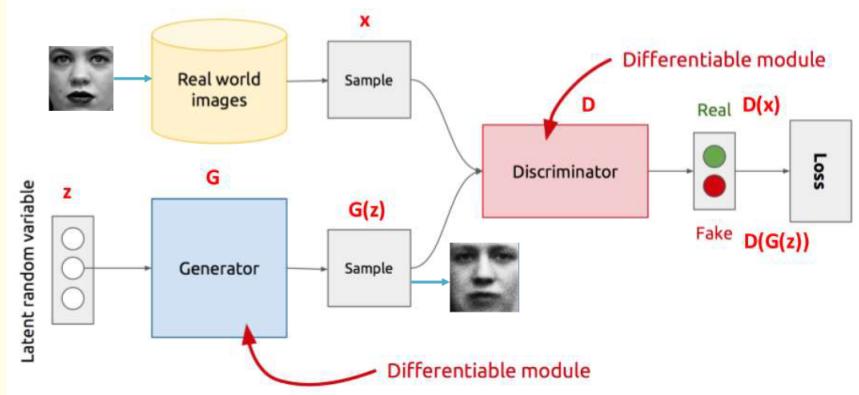


Figure 41

### Definition 8.2 (GAN Loss)

Now each of these networks will have its own set of parameters which we have to optimize. We want to optimize them by maximizing the likelihood such that the model says "real" to the samples from the world and "fake" to the generated samples. This leads to

$$\mathcal{L}(\theta_d, \theta_g) = V(\mathcal{D}, \mathcal{G}) = \underbrace{\mathbb{E}_{x \sim \text{real}} [\log \mathcal{D}_{\theta_d}(\mathbf{x})]}_{\substack{\text{log-prob that } \mathcal{D} \text{ correctly} \\ \text{predicts real data as real}}} + \underbrace{\mathbb{E}_{\mathbf{z}} [\log (1 - \mathcal{D}_{\theta_d}(\mathcal{G}_{\theta_g}(\mathbf{z})))]}_{\substack{\text{log-prob that } \mathcal{D} \text{ correctly} \\ \text{predicts generated data as fake}}} \quad (260)$$

Therefore, the discriminator is trying to maximize its reward (to get max value of 0), and the generator is trying to minimize the discriminator's reward (pulling this log probability down to  $-\infty$ ). This is known as a **minimax** optimization problem, and we have to find

$$\min_{\theta_g} \max_{\theta_d} V(\mathcal{D}_{\theta_d}, \mathcal{G}_{\theta_g}) \quad (261)$$

which is some saddle point.

Before we even talk about evaluating the gradients for this, let's prove a result on the properties of such an optimum.

### Theorem 8.1 (Global Optimality)

Given the minimax loss above, for a fixed  $\mathcal{G}$ , the optimal discriminator  $\mathcal{D}_G^*$  is given by

$$\mathcal{D}_G^*(\mathbf{x}) = \frac{p(\mathbf{x} \mid \text{real})}{p(\mathbf{x} \mid \text{real}) + p(\mathbf{x} \mid \text{synthesized})} \quad (262)$$

Therefore, the global minimum of the training criterion,  $\max_{\mathcal{D}} V(\mathcal{D}, \mathcal{G})$  is achieved if and only if

$$p(\mathbf{x} \mid \text{real}) = p(\mathbf{x} \mid \text{synthesized}) \quad (263)$$

**Proof.**

We first have

$$V(\mathcal{D}, \mathcal{G}) = \mathbb{E}_{\mathbf{x} \sim \text{real}} \log \mathcal{D}_{\theta_d}(\mathbf{x}) + \mathbb{E}_{\mathbf{z}} \log (1 - \mathcal{D}_{\theta_d}(\mathcal{G}_{\theta_g}(\mathbf{z}))) \quad (264)$$

Since  $\mathcal{G}$  is fixed (i.e.  $\theta_g$  is fixed) and acting, we can write the second expectation with respect to the probability measure induced by  $\mathcal{G}$ .

$$\begin{aligned} V(\mathcal{D}, \mathcal{G}) &= \mathbb{E}_{\mathbf{x} \sim \text{real}} \log \mathcal{D}_{\theta_d}(\mathbf{x}) + \mathbb{E}_{\mathbf{w} \sim \text{fake}} \log (1 - \mathcal{D}_{\theta_d}(\mathbf{w})) \\ &= \int p(\mathbf{x} \mid \text{real}) \log \mathcal{D}_{\theta_d}(\mathbf{x}) d\mathbf{x} + \int p(\mathbf{x} \mid \text{fake}) \log (1 - \mathcal{D}_{\theta_d}(\mathbf{x})) d\mathbf{x} \end{aligned}$$

where the  $\mathbf{x}$  in the second integral is a dummy variable. Taking the derivative w.r.t.  $\mathbf{x}$  and setting equal to 0 gives

$$p(\mathbf{x} \mid \text{real}) \frac{1}{\mathcal{D}_{\theta_d}(\mathbf{x})} + p(\mathbf{x} \mid \text{fake}) \cdot \frac{-1}{1 - \mathcal{D}_{\theta_d}(\mathbf{x})} = 0 \quad (265)$$

implies that

$$\mathcal{D}_{\theta_d}(\mathbf{x}) = \frac{p(\mathbf{x} \mid \text{real})}{p(\mathbf{x} \mid \text{real}) + p(\mathbf{x} \mid \text{fake})} \quad (266)$$

If the discriminator  $\mathcal{D}$  is optimal, then the generator is minimizing the **Jensen-Shannon divergence** between the real and generated (model distributions). However,  $\mathcal{D}$  is not optimal in practice since we have limited computational resources, the loss is non-convex, etc.

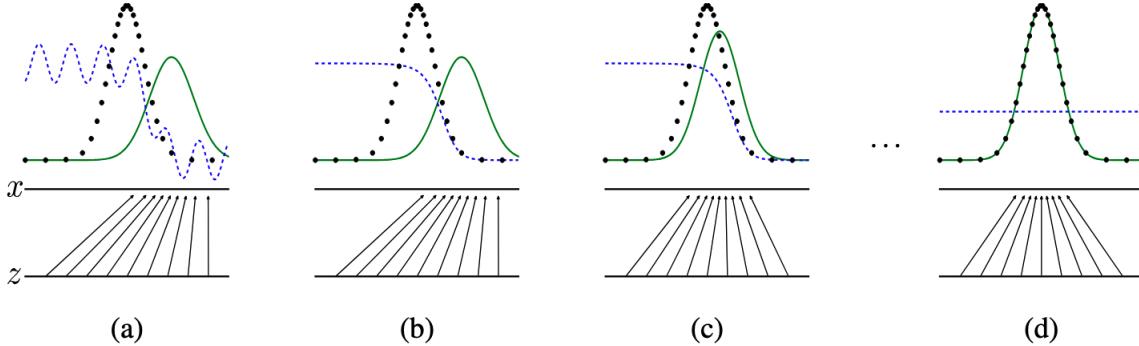


Figure 42

Now we can talk about evaluating the gradients and optimizing it. What is the gradient of such a loss function? This is quite easy since the expectations are over the true data distribution and the known prior  $z$ , and so we can swap gradients and expectations accordingly.

**Lemma 8.1 (Gradients of GAN Loss)****Proof.**

Note that the generator has no effect on the probability of  $\mathcal{D}$  correctly identifying real images, so it only focuses on the latter term.

**Algorithm 8.1 (Alternative Gradient Descent)**

The idea is to train both models simultaneously via SGD using mini-batches consisting of some generated samples and some real-world samples, which is called the **alternative gradient descent algorithm**. It is usually the case that the generator does better than the discriminator, so we sometimes make  $k > 1$  to allow more steps for training.

**Algorithm 2** Minibatch stochastic gradient descent training of generative adversarial nets. The number of steps to apply to the discriminator,  $k$ , is a hyperparameter. We used  $k = 1$ , the least expensive option, in our experiments.

---

```

1: for number of training iterations do
2:   for  $k$  steps do
3:     Sample minibatch of  $m$  noise samples  $\{z^{(1)}, \dots, z^{(m)}\}$  from noise prior  $p_g(z)$ .
4:     Sample minibatch of  $m$  examples  $\{x^{(1)}, \dots, x^{(m)}\}$  from data generating distribution
    $p_{\text{data}}(x)$ .
5:     Update the discriminator by ascending its stochastic gradient:

$$\nabla_{\theta_d} \frac{1}{m} \sum_{i=1}^m \left[ \log D(x^{(i)}) + \log (1 - D(G(z^{(i)}))) \right].$$

6:   end for
7:   Sample minibatch of  $m$  noise samples  $\{z^{(1)}, \dots, z^{(m)}\}$  from noise prior  $p_g(z)$ .
8:   Update the generator by descending its stochastic gradient:

$$\nabla_{\theta_g} \frac{1}{m} \sum_{i=1}^m \log (1 - D(G(z^{(i)}))).$$

9: end for

```

---

The gradient-based updates can use any standard gradient-based learning rule. We used momentum in our experiments.

There is a vanishing gradient problem in GANs. For instance, assume that the model  $\mathcal{G}_{\theta_g}$  has very bad parameters, and it generates very bad samples that the discriminator can detect very well. Then,  $\mathbb{E}_{\mathbf{z}} [\log (1 - \mathcal{D}_{\theta_d}(\mathcal{G}_{\theta_g})))]$  will be very close to 0, and the generator's cost will be very flat. Therefore, the gradient would die out and the generator can't improve! For example, if  $\mathcal{D}$  was just a sigmoid function, then we can approximate the gradient of the expectation with a sample of the gradient, which would die out.

$$\begin{aligned}
\nabla_{\theta_g} V(\mathcal{D}, \mathcal{G}) &= \nabla_{\theta_g} \mathbb{E}_{\mathbf{z} \sim q((\mathbf{z})} [\log (1 - \mathcal{D}(\mathcal{G}(\mathbf{z})))] \\
&\approx \nabla_a \log (1 - \sigma(a)) \\
&= -\frac{\sigma(a) (1 - \sigma(a))}{1 - \sigma(a)} = -\sigma(a) = -\mathcal{D}(\mathcal{G}(\mathbf{z}))
\end{aligned}$$

and so the gradient goes to 0 if  $\mathcal{D}$  is confident, i.e.  $\mathcal{D}(\mathcal{G}(\mathbf{z})) \rightarrow 0$ . Therefore, we can modify the cost for the generator term by changing the cost to

$$\mathbb{E}_{\mathbf{z}} \log (1 - \mathcal{D}_{\theta_d}(\mathcal{G}_{\theta_g}(\mathbf{z}))) \tag{267}$$

and trying to minimize it.

**Theorem 8.2 (Convergence)**

8.1 Conditional GAN

8.2 CycleGAN

8.3 Deep Convolution GAN (DCGAN)

## 9 Normalizing Flows

We have seen many examples of generative models that attempt to produce a probability distribution  $p$  that approximates the true pdf  $p^*$  of the data samples. Some are given by an explicit model (e.g. GMMs, RBMs, VAEs) which approximate with parameterized form  $p^* \sim p_\theta$ , while in others (GANs) the model is implicit since we model the random variable as a transformation  $X = G_{g_\theta}(Z)$  through a neural network with  $Z \sim \mathcal{N}(0, I)$ . If we focus on VAEs—specifically variational inference—for a second, recall that the performance of the model really just depends on the fact that we can approximate the intractable posterior  $p(z | x)$  with some parameterized family  $q_\phi(z)$ <sup>18</sup>

$$\text{ELBO}(x^{(i)}, \phi, \theta) = \underbrace{\mathbb{E}_{q_\phi(z|x^{(i)})}[\log p_\theta(x^{(i)} | z)]}_{\substack{\text{likelihood term} \\ (\text{reconstruction part})}} - \underbrace{KL(q_\phi(z | x^{(i)}) || p(z))}_{\substack{\text{closeness of encoding to } p(z) \\ (\text{typically Gaussian})}} \quad (268)$$

This may not be advantageous and flexible enough to capture the true posterior if  $q_\phi(z)$  is far away from  $p(z | x)$

To address this problem, in 2015, Google Deepmind through [RM16] introduced the idea of *flow-based* models<sup>19</sup> which—like GANs—want to map simple distributions (e.g. a Gaussian) to complex densities representing the data. This would normally result in an implicitly defined pdf, but by making the transformation to be *invertible*, we can use the change of basis formula to get a closed-form of the pdf, making flow models an *explicit* model of the pdf. Recall the lemma below from multivariate calculus.

### Lemma 9.1 (Jacobi)

Let  $X, Z$  be absolutely continuous random variables in  $\mathbb{R}^n$ . Given that  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$  is invertible and differentiable everywhere, with  $X = f(Z), Z = f^{-1}(X)$ , we claim

$$p_X(x) = p_Z(z) \cdot \left| \det \frac{\partial f^{-1}}{\partial x} \right| = p_Z(z) \cdot \left| \det \frac{\partial f}{\partial z} \right|^{-1} \quad (269)$$

where  $\det$  is the determinant of the total derivative (Jacobian).

### Proof.

For  $n = 1$ , we have

$$p_X(x) = \frac{d}{dx} F_X(x) \quad (270)$$

$$= \frac{d}{dx} F_Z(f^{-1}(x)) \quad (271)$$

$$= p_Z(f^{-1}(x)) \cdot \frac{d}{dx} f^{-1}(x) \quad (272)$$

$$= p_Z \quad (273)$$

Therefore, if we parameterize  $f$  with some  $\theta$ , then the marginal likelihood of  $x$  given  $\theta$  can be written as

$$p_X(x; \theta) = p_Z(f_\theta^{-1}(x)) \cdot \left| \det \frac{\partial f_\theta^{-1}}{\partial x} \right| \quad (274)$$

Therefore, if  $X$  is a complex distribution and  $Z$  is a simple one (e.g. uniform), we might have hope to efficiently compute  $p_X(x)$  for any  $x \in \mathbb{R}^n$  if

<sup>18</sup>This can be written  $q_\phi(z) = q_\phi(z | x)$ , but since the encoder network produces the  $\phi = E_\alpha(x)$ , the  $q_\phi(z)$  really represents a conditional distribution given  $x$ .

<sup>19</sup>This has nothing to do with flow graphs and the max-flow-min-cut theorem in graph theory.

1. we can efficiently compute  $f_\theta^{-1}(x)$ , which allows us to compute  $p_Z(f^{-1}(x))$  efficiently since  $Z$  is simple.
2. we can efficiently compute the determinant of the Jacobian  $|\det(\partial f_\theta^{-1}/\partial x)|$ .<sup>20</sup>

## 9.1 Finite Normalizing Flows

It looks like we have split this enormously hard problem of modeling  $X$  with two slightly less difficult problems. However, with some tricks, we may be able to get a simple enough parameterization of  $f$  to be able to compute its inverse plus the determinant of the Jacobian. Note that the construction of a neural network was to take a simple function (one layer) and construct a complex family of functions composed of multiple layers. This is what we can do as well.

### Corollary 9.1 (Finite Normalizing Flow)

Given a sequence of transformations

$$Z = Z_0 \xrightarrow{f_1} Z_1 \xrightarrow{f_2} \dots \xrightarrow{f_{K-1}} Z_{K-1} \xrightarrow{f_K} Z_K = X \quad (275)$$

where each  $f_k$  is invertible and differentiable everywhere, let us denote  $f = f_K \circ \dots \circ f_1 : Z \rightarrow X$ , which is invertible. Then

$$p_X(x) = p_Z(f^{-1}(x)) \cdot \prod_{k=1}^K \left| \det \frac{\partial f_k}{\partial z_{k-1}} \right|^{-1} \quad (276)$$

This sequence of random variables  $Z_k$  is called a **flow**, and the sequence of the corresponding pdfs  $p_{Z_k}$  is called the **normalizing flow**. As for how we parameterize this, our notation will assume that  $\theta = (\theta_1, \dots, \theta_M)$  and each  $\theta_m$  parameterizes  $f_m$ .

### Proof.

This can automatically be proved by induction. For an example, consider the sequence of invertible functions  $Z \xrightarrow{f} Y \xrightarrow{g} X$ , where  $Z$  is a simple distribution that gets transformed to a slightly more complicated distribution  $Y$  that then gets transformed to a complex distribution  $X$ . We can apply the Jacobi theorem above to see  $p_Y(y) = p_Z(f^{-1}(y)) \cdot |(Df^{-1})(y)|$ , and so we have

$$p_X(x) = p_Y(g^{-1}(x)) \cdot |(Dg^{-1})(x)| \quad (277)$$

$$= p_Z(f^{-1}(g^{-1}(x))) \cdot |(Df^{-1})(g^{-1}(x))| \cdot |(Dg^{-1})(x)| \quad (278)$$

$$= p_Z((g \circ f)^{-1}(x)) \cdot |(Df^{-1})(g^{-1}(x))| \cdot |(Dg^{-1})(x)| \quad (279)$$

Therefore, by taking a sequence of these functions  $f_m$ , which may each have a simple parameterization, we may construct a very complex composition  $f_\theta$  that may result in a very expressive  $Z$ . Again, this is very similar to how a composition of linear mappings plus an activation gives us a very expressive neural network, and unsurprisingly, there is an analogue of the universal approximation theorem for transformations of this form.

### Theorem 9.1 (Probability Integral Transform)

Any  $n$ -dimensional random variable in  $\mathbb{R}^n$  that is absolutely continuous w.r.t. the Lebesgue measure can be constructed from the uniform distribution  $U$  on  $[0, 1]^n$ . Since we can map to and back from invertibility, any two such random variables  $X$  and  $Y$  can be mapped from each other,

$$X \mapsto U \mapsto Y \quad (280)$$

<sup>20</sup>Note that computing determinants are approximately  $O(n^{2.4})$ , which may not be practical.

Now given this, our job is to maximize the log-likelihood. Since  $x = z_K$  and  $z = z_0$ , we substitute this in

$$\ln p_{Z_K}(x) = \ln p_{Z_0}(f^{-1}(x)) - \sum_{k=1}^K \ln \left| \det \frac{\partial f_k}{\partial z_{k-1}} \right| \quad (281)$$

and over the dataset we want to find

$$f^* = \underset{f}{\operatorname{argmax}} \sum_{i=1}^N \ln p_{Z_0}(f^{-1}(x^{(i)})) - \sum_{k=1}^K \ln \left| \det \frac{\partial f_k}{\partial z_{k-1}} \right| \quad (282)$$

where we are really optimizing over  $f_1, \dots, f_K$ , i.e. their parameters  $\theta_1, \dots, \theta_K$ . Great, now let's define the parametric form of  $f$ . There are two different types of invertible transformations that we can calculate in linear time.

### Definition 9.1 (Planar Contractions)

Let us have  $\theta = \{w \in \mathbb{R}^D, u \in \mathbb{R}^D, b \in \mathbb{R}\}$  and define the family of **planar contractions**

$$\{f(z) = z + u \cdot h(w^T z + b)\}_\theta \quad (283)$$

for some smooth nonlinearity  $h$ .<sup>a</sup> This is not always invertible, but the paper uses  $h(x) = \tanh(x)$  with the fact that  $w^T u \geq -1$  is sufficient for  $f$  to be invertible.

<sup>a</sup>As the paper states, this flow can be visualized as modifying the initial density by applying a series of contractions and expansions in the direction perpendicular to the hyperplane  $w^T z + b$ .

This already looks like a single layer, so you might wonder why one can't just directly make an invertible neural net? There is already literature on this, but the typical computational complexity of computing the determinant (plus the gradient of the determinant) is of scale  $O(LD^3)$ , where  $L$  is the number of hidden layers and  $D$  is the dimension of each hidden layer. It turns out that this decomposition gives us a very cute formula for computing determinants.

### Lemma 9.2 ()

The determinant of a planar contraction is

$$\left| \det \frac{\partial f}{\partial z} \right| = \left| \det(I + u\psi(z)^T) \right| = |1 + u^T \psi(z)| \quad (284)$$

where  $\psi(z) = h'(w^T z + b) \cdot w$ . This can be computed in  $O(D)$  time.

### Proof.

Use block matrix multiplication and the matrix determinant lemma.

The other type mentioned is a radial contraction.

### Definition 9.2 (Radial Contraction)

Let us have  $\theta = \{c \in \mathbb{R}^D, \alpha \in \mathbb{R}^+, \beta \in \mathbb{R}\}$  and define the family of **radial contractions**

$$\{f(z) = z + \beta h(\alpha, r)(z - c)\}_\theta \quad (285)$$

where  $r = |z - c|$  and  $h(\alpha, r) = \frac{1}{\alpha+r}$ .<sup>a</sup>

<sup>a</sup>It applies radial contractions and expansions around the reference point  $c$  and are referred to as radial flows.

**Lemma 9.3 ()**

The determinant of a radial contraction is

$$\left| \det \frac{\partial f}{\partial z} \right| = [1 + \beta h(\alpha, r)]^{d-1} [1 + \beta h(\alpha, r) + \beta h'(\alpha, r)r] \quad (286)$$

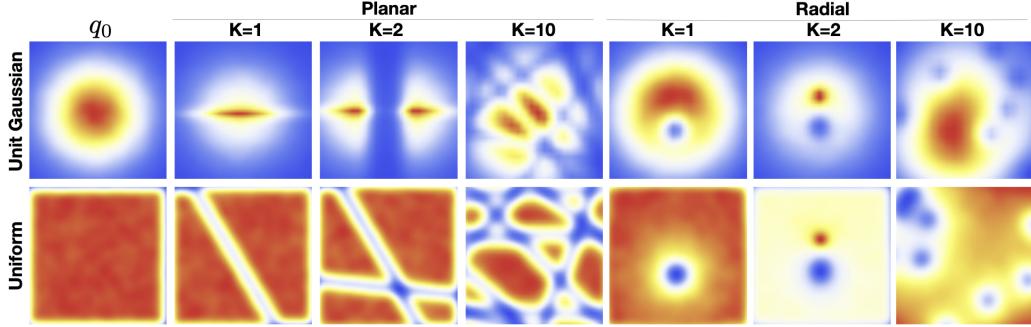


Figure 43: The effects of normalizing flow on two distributions. For example, for  $k = 2$  we can transform a spherical Gaussian into a bimodal distribution by applying 2 successive transformations.

With this form, we can now substitute this into the variational lower bound. Note that we have not just simplified it with the following theorem, but we have also set it up as an expectation over the initial density  $p(z)$ , analogous to the reparamaterization trick that we have used for VAEs.

**Theorem 9.2 ()**

The variational lower bound can be written in the simplified form where the

$$\text{ELBO}(x) = \mathbb{E}_{q_0(z_0)}[\log q_0(z_0)] - \mathbb{E}_{q_0(z_0)}[\log p(x, z_K)] - \mathbb{E}_{q_0(z_0)} \left[ \sum_{k=1}^K \log |1 + u_k^T \psi_k(z_{k-1})| \right] \quad (287)$$

for flow models.

**Proof.**

By definition  $q_\phi(z | x) := q_K(z_K)$ , and substituting this in along with our simplified formula for the log likelihood gives us

$$\text{ELBO}(x) := \mathbb{E}_{q_\phi(z|x)} [\log q_\phi(z | x) - \log p(x, z)] \quad (288)$$

$$= \mathbb{E}_{q_K(z_K)} [\log q_K(z_K)] - \mathbb{E}_{q_K(z_K)} [\log p(x, z_K)] \quad (289)$$

$$= \mathbb{E}_{q_K(z_K)} \left[ \log q_0(z_0) - \sum_{k=1}^K \log |1 + u_k^T \psi_k(z_{k-1})| \right] - \mathbb{E}_{q_K(z_K)} [\log p(x, z_K)] \quad (290)$$

But since  $z_K = f(z_0)$ , using LOTUS we can get

$$\text{ELBO}(x) = \mathbb{E}_{q_0(z_0)}[\log q_0(z_0)] - \mathbb{E}_{q_0(z_0)} \left[ \sum_{k=1}^K \log |1 + u_k^T \psi_k(z_{k-1})| \right] - \mathbb{E}_{q_0(z_0)} [\log p(x, z_K)] \quad (291)$$

At this point we can take the gradients, freely swap them with the expectations, and compute them.

## 9.2 Coupling-Layer Flows

This general method allowing linear-time computation of Jacobian determinants is an example of a **general normalizing flow**. Before, we have just constructed some family of invertible functions  $\{f\}$  to transform the data, such that it was simple enough to calculate the Jacobian determinants in linear time. But note that in general, computing determinants requires you to have an triangular matrix (multiply all the diagonals). Therefore, if we can create a neural network  $f$  such that its Jacobian is triangular, we will be done. In order to have such an architecture to support this, we should introduce a special type of layer.

### Definition 9.3 (Coupling Layer)

Let us have an input  $z \in \mathbb{R}^D$  such that it can be partitioned into its first  $d$  elements and the rest.

$$z = [z_{1:d}, z_{d+1:D}] \quad (292)$$

Now let's have 2 neural networks (not necessarily invertible)  $F : \mathbb{R}^d \rightarrow \mathbb{R}^{D-d}$  and  $H : \mathbb{R}^d \rightarrow \mathbb{R}^{D-d}$  defined

$$F(z') = \beta, \quad G(z') = \gamma \quad (293)$$

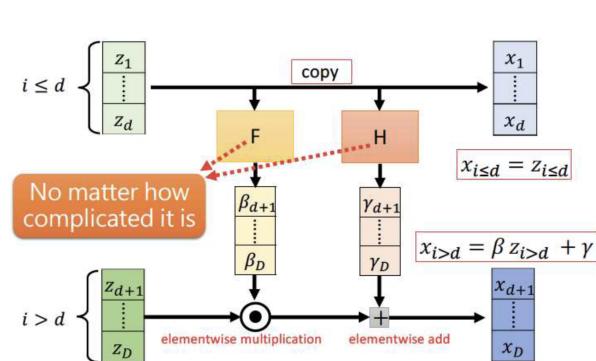
Then the **coupling layer**  $g : \mathbb{R}^D \rightarrow \mathbb{R}^D$  with parameters  $\theta = (\theta_F, \theta_H)$  is defined as the transformation  $x = g(z)$ , where

$$x_{1:d} = z_{1:d} \quad (294)$$

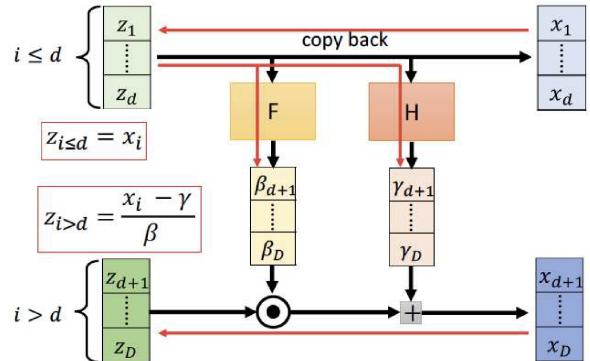
$$x_{d+1:D} = z_{d+1:D} \odot \beta + \gamma = z_{d+1:D} \odot F(x_{1:d}) + H(x_{d+1:D}) \quad (295)$$

So this “layer” really composes of two neural networks, and it has both properties that we want. It is invertible, with inverse  $z = g^{-1}(x)$  defined

$$z' = x', \quad \bar{z} = \frac{\bar{z} - \gamma}{\beta} = \frac{\bar{z} - H(z')}{F(z')} \quad (296)$$



(a) Forward pass of the coupling layer.



(b) Backward pass of the coupling layer

Figure 44: Coupling layers are easily invertible. For both the forward and backward pass, we must do a forward pass through  $F$  and  $H$ .

Second, the determinant of this is easy to calculate since it is simply  $\beta_1 \times \dots \times \beta_{D-d}$ . Therefore, we can stack these layers on top of each other, parameterized by different sequences of neural nets.

### 9.2.1 RealNVP

By setting each function  $f_i$  to be a cascading layer, we can model  $f = f_K \circ \dots \circ f_1$  and do the exact same normalizing flow model as mentioned before. This is pretty much NVP.

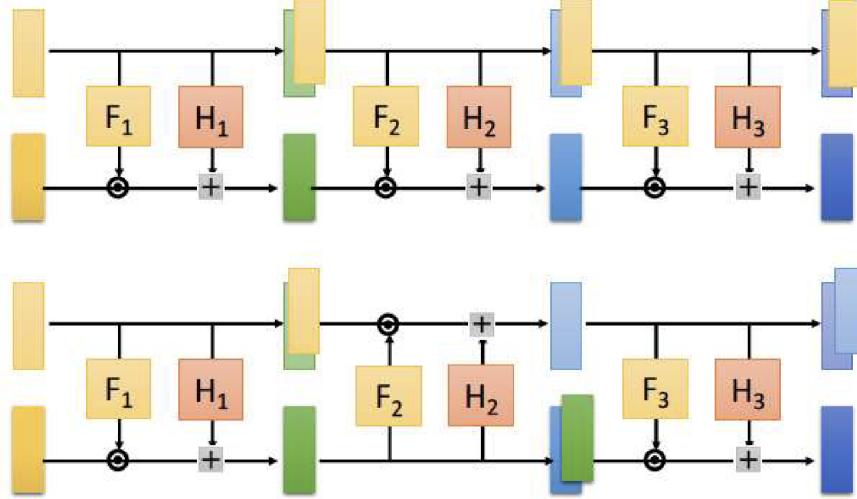


Figure 45: Cascading coupling layers represents  $f$ , where each layer is  $f_i$ .

### 9.2.2 NICE

**Volume preserving flows** design the flow such that the Jacobian determinant is equal to 1 (which is more restrictive but allows  $O(1)$  computation) but still allows for rich posteriors. Therefore, even though computing the transformation  $f_K \circ \dots \circ f_1$  will take longer due to the forward pass of neural nets, the lack of need to calculate the determinant keeps this fast. An example of such a volume-preserving coupling-layer flow model was introduced in [DKB15] by Dinh in 2014.

#### Definition 9.4 (NICE)

The **nonlinear independent components estimation (NICE)** model uses **additive coupling layers** of the form

$$x_{1:d} = z_{1:d} \quad (297)$$

$$x_{d+1:n} = z_{d+1:n} + H(x_{1:d}) \quad (298)$$

which we can see has a Jacobian determinant of one. The final layer of NICE is a multiplication by a diagonal matrix with all diagonal elements nonzeros, i.e.  $x_i = \beta_i z_i$ , which is invertible and has the absolute value of the determinant  $\prod_i |\beta_i|$ .

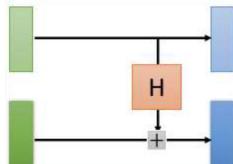


Figure 46: An additive coupling layer.

### 9.3 GLOW

A lot of hacks to improve it (no math). Improved normalizing flow dramatically. You have a flow and squeeze a bunch of times is GLOW.

### 9.4 Augoregressive Flows

### 9.5 Infinitesimal Flows

## 10 Score Based Models

We have built several types of generative models so far that estimated densities. While calculating PDFs is called *density estimation*, we can indirectly estimate it by calculating the gradient of the PDF (with respect to the sample), which is known as **score matching**.

### Definition 10.1 (Score)

Let  $X$  be a continuous random variable defined on  $\mathbb{R}^n$ , and let  $p$  be its pdf, parameterized by  $\theta$ . The score function of  $p$  is the gradient of the log-pdf with respect to the sample.<sup>a</sup>

$$\psi(x; \theta) = \begin{bmatrix} \frac{\partial \log p(x; \theta)}{\partial x_1} \\ \vdots \\ \frac{\partial \log p(x; \theta)}{\partial x_n} \end{bmatrix} = \begin{bmatrix} \psi_1(x; \theta) \\ \vdots \\ \psi_n(x; \theta) \end{bmatrix} = \nabla_x \log p(x; \theta) \quad (299)$$

Note that the score is a function  $\psi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ .

<sup>a</sup>Note that this is w.r.t. the sample, not the parameter, unlike what we do usually in machine learning.

The reason Hyvarinen introduced this score function in 2005 is because we want to have such a score is that it does not depend on the normalizing constant  $Z$  (since the log derivative gets rid of it). [Hyv05] Therefore, rather than maximizing the likelihood, we want to minimize the L2 distance between the score functions.

$$R(\theta) = \mathbb{E}_X [||\psi(x; \theta) - \psi_{\mathcal{D}}(x)||^2] \quad (300)$$

[SSK<sup>+</sup>20].

## 11 Attention Models

We have seen the power of encoder decoder models, which can be used with a combination of RNNs or CNNs. Since we can plug and play different architectures, we can process and output different types of data.<sup>21</sup> CNNs were quite strong and have really no problem with scaling ever since the ResNet architecture, but historically, RNNs had two main problems.

1. They compute sequentially, since the hidden states must be a function of previous hidden states. This results in a linear time complexity, which is not ideal.
2. By encoding the entire sequence in a hidden latent space of dimension  $h$ , we are essentially trying to compress a possibly very long sequence into a single vector of predetermined dimension. This causes a *bottleneck problem* and words that are further away may be “forgotten.”

We will see that attention solves the second bottleneck problem, and self-attention solves the sequential problem.

In general, feed forward networks treat features as independent, convolutional networks focus on relative location and proximity, and RNNs have tend to read in one direction. This may not be the most flexible way to process data, and we have some other problems.

1. When processing images, we may want our CNN to focus on a specific part of the image. For example, when we see a cat in the corner, other parts of the image does not matter, and we can have our CNN focus on the specific portion of the image containing the cat.
2. When reading sentences, different words may be interdependent, even if they are not next to each other, and so we may want to focus on different portions of a sentence (e.g. words 1 3, plus 10 15 which describes an object).

This is where attention comes in to the rescue. Attention is, to some extent, motivated by how we pay visual attention to different regions of an image or correlate words in one sentence. Human attention allows us to focus on certain regions or portions of our data with “high resolution” while perceiving the surrounding data in “low resolution.” In a nutshell, attention in deep learning can be broadly interpreted as a vector of importance weights. First, we will introduce attention in the general setting, then move onto its specific implementation in RNNs through the seq2seq attention model, and finally its application in CNNs through Vision transformers.

### 11.1 Seq2Seq with Attention

The idea of **attention** provides a solution to this bottleneck problem. Basically, we want to establish connections from the decoder to not just the last hidden state of the encoder, but to all of its nodes. Each encoder node represents some information about each word, and by taking some weighted sum of these nodes, we can choose which one to put this attention on.

#### Definition 11.1 (Score Function)

Before we begin, let’s define a metric, called a **score function**, to determine how similar two words (more specifically, their embeddings) are. The two simplest ways to do this are:

1. the standard dot product.

$$\text{score}(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y} \quad (301)$$

2. cosine similarity.

$$\text{score}(\mathbf{x}, \mathbf{y}) = \frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{x}\| \|\mathbf{y}\|} \quad (302)$$

Now that we have the score defined, the heart of attention comes with the query, key, value model. The general idea is this: for every prediction we want to make (whether it is classifying something or generating

<sup>21</sup>CNNs can be used to encode or output images and RNNs can be used to encode or output sequential data.

a new output word/token), we want to get its respective query vector and use it to look through key-value dictionary in order to get the most relevant information from it. With this information, combined with the query and whatever other information we have, we can make a prediction.

Let's go through this step by step. What we want to do is associate every input hidden node  $\mathbf{h}_t$  with a 2-tuple consisting of a key-value pair.

$$\mathbf{h}_t \mapsto (\mathbf{k}_t, \mathbf{v}_t) \quad (303)$$

and associate every hidden output node  $\mathbf{s}_t$  with a query value.

$$\mathbf{s}_T \mapsto \mathbf{q}_t \quad (304)$$

### Definition 11.2 (Seq2Seq with Vanilla Attention)

Eventually, we would like to learn these key, value, queries, but for now let's focus on the forward propagation.

1. The input has been sequentially encoded and we have a special start token  $\mathbf{s}_0$ .
2. For  $t' = 0$  until the  $\mathbf{s}_{T'}$  is the end token, do the following.
  - (a) Take the query  $\mathbf{s}_i$  and compute the attention score  $\text{score}(\mathbf{s}_i, \mathbf{h}_t)$  for all  $t = 1, \dots, T$ . This determines which encoder hidden state we should pay attention to.

$$\mathbf{e}^{t'} = [\text{score}(\mathbf{s}_{t'}, \mathbf{h}_1), \dots, \text{score}(\mathbf{s}_{t'}, \mathbf{h}_T)] \in \mathbb{R}^T \quad (305)$$

- (b) We take its softmax to get the **attention distribution**  $\boldsymbol{\alpha}^{t'}$  for this step (a discrete probability distribution)

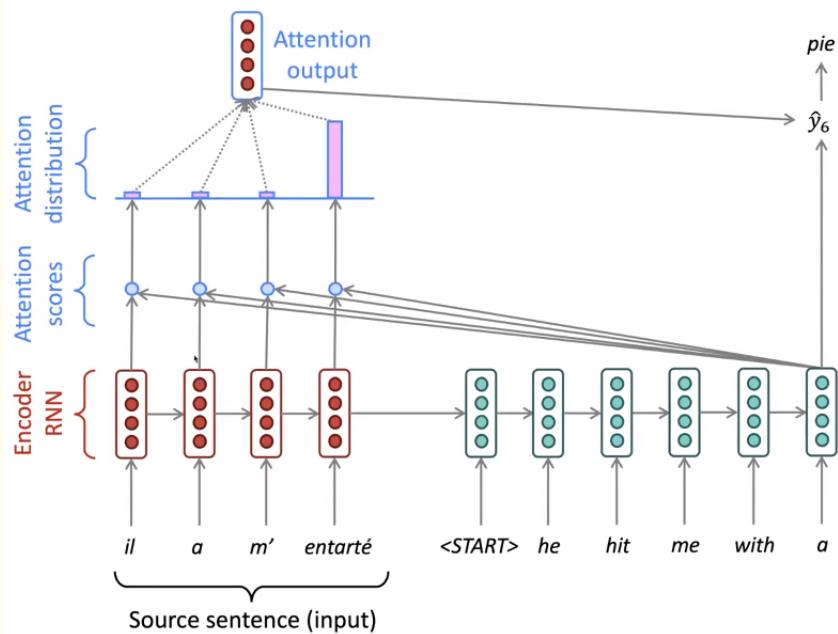
$$\boldsymbol{\alpha}^{t'} = \text{softmax}(\mathbf{e}^{t'}) \in \mathbb{R}^T \quad (306)$$

- (c) We use  $\boldsymbol{\alpha}^{t'}$  to take a weighted sum of the encoder hidden states to get the attention output  $\mathbf{a}_{t'}$

$$\mathbf{a}_{t'} = \sum_{t=1}^T \alpha_t^{t'} \mathbf{h}_t \in \mathbb{R}^h \quad (307)$$

which acts as our context vector  $\mathbf{C}_{t'}$  that we can now use in our vanilla seq2seq model.<sup>a</sup>  
Note that this context vector is different for every  $\mathbf{s}_{t'}$ , so at every step we can choose which encoder states/words to focus on.<sup>b</sup>

Another trick to improve performance is that these attention context vectors can be concatenated with the previous decoder hidden state to get more information in the already decoded part of the sentence.

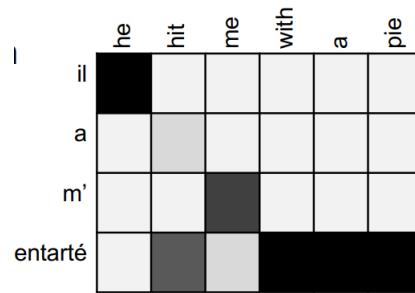


<sup>a</sup>This weighted sum is a selective summary of the information contained in the values, where the query determines which values to focus on. Attention is a way to obtain a fixed size representation of an arbitrary set of representations (the values), dependent on some other representation (the query).

<sup>b</sup>This is similar to a hash map where you have a set of key-value pairs. When you have a query, you want to search through the keys to see if it matches the query, and then it returns the value of the matched key. In our case, we have a query, and rather than looking for exact matches, we want to return a similarity score of the query  $q_i$  across all  $k_i$ 's and provide a weighted sum of the corresponding values.

Overall, attention is extremely useful in improving all performance, and it is intuitive with how humans analyze things, too. It significantly improves neural machine translation by allowing the decoder to focus on certain parts of the source. It also provides more "human-like" model of the machine translation process (you can look back at the source sentence while translating, rather than needing to remember it all). It solves the bottleneck problem and helps with the vanishing gradient problem with these pseudo-residual connections through the context vector.

Finally, it provides some interpretability, as we can inspect the attention distribution to see what the decoder was focusing on (which again, we've never set explicitly but was learned by the model).



### Code 11.1 ()

For an implementation of this in PyTorch, look [here](#).

Now let's talk about how these parameters are already learned. The parameters of the model are.

1. The encoding matrices for the usual seq2seq model:  $\mathbf{W}_e, \mathbf{U}_e$ .
2. Generating key, value, and query vectors for every possible embedding is not practical.<sup>22</sup> A more compact way to represent them are through linear maps, so we are learning matrices  $\mathbf{Q}, \mathbf{K}, \mathbf{V}$  such that

$$\begin{aligned}\mathbf{q}_{t'} &= \mathbf{Q}\mathbf{s}_{t'} \\ \mathbf{k}_t &= \mathbf{K}\mathbf{h}_t \\ \mathbf{v}_t &= \mathbf{V}\mathbf{h}_t\end{aligned}$$

3. We should now have the decoding matrices  $\mathbf{W}_d$  that takes in the attention context vector (plus maybe the previous hidden decoder state) and the original matrix  $\mathbf{U}_d$ .

Therefore, this problem reduces to learning the matrices  $\mathbf{W}_e, \mathbf{U}_e, \mathbf{Q}, \mathbf{K}, \mathbf{V}, \mathbf{W}_d, \mathbf{U}_d$ .

### Example 11.1 (Score Functions)

Having additional flexibility with the score functions can also improve learning. We provide more examples here, which give more parameters to learn as well.

1. The general attention model allows us to train a shared-weight matrix, allowing for  $s \neq h$ .

$$e_t^{t'} = \text{score}(\mathbf{s}_{t'}, \mathbf{h}_t) = \mathbf{s}_{t'}^T \mathbf{W}_a \mathbf{h}_t \in \mathbb{R}$$

However, it may seem like there are too many parameters in  $\mathbf{W}_a$ , having to learn  $sh$  values.

2. The reduced rank multiplicative attention uses low rank matrices, allowing us to learn only  $ks + kh$  parameters for matrices  $\mathbf{U}_a \in \mathbb{R}^{k \times s}, \mathbf{V}_a \in \mathbb{R}^{k \times h}$  where  $k \ll s, h$ .

$$e_t^{t'} = \text{score}(\mathbf{s}_{t'}, \mathbf{h}_t) = \mathbf{s}_{t'}^T (\mathbf{U}_a^T \mathbf{V}_a) \mathbf{h}_t = (\mathbf{U}_a \mathbf{s}_{t'})^T (\mathbf{V}_a \mathbf{h}_t) \in \mathbb{R}$$

3. Additive attention uses a neural net layer defined

$$e_t^{t'} = \mathbf{v}_a^T \tanh(\mathbf{W}_a \mathbf{h}_t + \mathbf{V}_a \mathbf{s}_{t'}) \in \mathbb{R}$$

where  $\mathbf{W}_a \in \mathbb{R}^{r \times h}, \mathbf{V}_a \in \mathbb{R}^{r \times s}$  are weight matrices,  $\mathbf{v}_a \in \mathbb{R}^r$  is a weight vector, and  $r$  (the attention dimensionality) is a hyperparameter.

This can be naturally extended to other architectures, as we will explore later.

### Example 11.2 (Images)

Given an image of size  $224 \times 224$ , we can make patches of size  $16 \times 16$ , and then flatten them to get a  $196 \times 768$  matrix with a 2-dimensional positional encoding scheme. We can then apply a linear transformation to get the query, key, and value vectors.

## 11.2 Self-Attention Layer

While we have solved the bottleneck problem, this entire process is still sequential since every hidden decoder node requires us to know the previous hidden node. There are two sequential processes in the regular seq2seq attention model.

1. The sequential encoding of the input sentence.
2. The sequential decoding of the output sentence. This unfortunately is not possible in transformers to parallelize.

<sup>22</sup>You would need three  $d_{\text{embedding}} \times |\mathcal{V}|$  matrices, where  $\mathcal{V}$  is the set of our vocabulary, which can go easily past 500,000 elements.

We will focus on parallelizing the first part by temporarily forgetting about encoder-decoder models and just thinking about how to incorporate a good encoder with attention that is parallelizable. This extension is quite simple. Let  $\mathbf{w}_{1:n}$  be a sequence of words in vocabulary  $\mathcal{V}$ . The key here is that rather than inputs having key-values and outputs having queries, *all* words are associated with a 3-tuple of key, value, query.

$$\mathbf{x}_i \mapsto (\mathbf{q}_i, \mathbf{k}_i, \mathbf{v}_i) \quad (308)$$

### Definition 11.3 (Standard Scaled Dot-Product Attention)

If we keep the score function to be the dot-product, the derivations become quite simple.

1. For each  $\mathbf{w}_i$ , let  $\mathbf{x}_i = E\mathbf{w}_i$  be the word embedding (with  $E \in \mathbb{R}^{d \times |\mathcal{V}|}$  the embedding matrix).
2. We transform each word embedding with the (learned) weight matrices  $\mathbf{Q}, \mathbf{K}, \mathbf{V}$ .

$$\begin{aligned}\mathbf{q}_i &= \mathbf{Q}\mathbf{x}_i \implies Q = \mathbf{Q}X \\ \mathbf{k}_i &= \mathbf{K}\mathbf{x}_i \implies K = \mathbf{K}X \\ \mathbf{v}_i &= \mathbf{V}\mathbf{x}_i \implies V = \mathbf{V}X\end{aligned}$$

where  $X = [x_1, \dots, x_n] \in \mathbb{R}^{d \times n}$ .

3. We compute pairwise similarities between keys and queries and normalize with the softmax to get the attention distribution for each word.

$$\mathbf{e}_{ij} = \mathbf{q}_i^T \mathbf{k}_j, \quad \alpha_{ij} = \frac{\exp(\mathbf{e}_{ij})}{\sum_{j'} \exp(\mathbf{e}_{ij'})} \quad (309)$$

4. Compute the output for each word as a weighted sum of values.

$$\mathbf{o}_i = \sum_j \alpha_{ij} \mathbf{v}_j \quad (310)$$

Ultimately, this can be parallelized into one matrix operation.<sup>a</sup>

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{E_k}}\right)V \quad (311)$$

where the softmax is done to each row.<sup>b,c</sup>

Therefore, when you do a forward pass on an attention layer with input  $x$ , you first get the query vector  $q$ , extract the attention-weighted values from the key-value dictionary, and then return the weighted sum of the values. To give explicit parameterizations using the query, key, value encoding matrices, we can write this as

$$\text{Attention}(x; Q, K, V) = \text{softmax}\left(\frac{(\mathbf{Q}x)(\mathbf{K}x)^T}{\sqrt{E_k}}\right)(\mathbf{V}x) \quad (312)$$

This will give us a vector  $\mathbf{o}_{1:n}$  consisting of the encoded vectors for each word in the sentence, and best of all, this is parallelizable!

<sup>a</sup>Note that in order to even do such a thing, we must know  $n$  beforehand. This can be solved by simply fixing some maximum length, padding everything to be some null token after the end token, and masking all the null tokens to be 0. More on masking later.

<sup>b</sup>We divide by  $\sqrt{E_k}$  to stabilize the gradients since as dimensionality increases, the dot product between random vectors tend to get large, leading to large softmax inputs. You can simply compute the variance of two  $d$ -dimensional Gaussian vectors and see that their variances scales linearly with  $d$ .

<sup>c</sup>You can see that if we have simple dot-product similarity scores, then  $E_k = E_v$ , but this need not be true in general. We will explore other similarity score in the next subsection.

There are three problems however.

1. This self-attention encoding does not account for the position/order of the words. Therefore, some

positional embedding is needed.

2. Our plan is to stack this layer multiple times on top of each other. However, we are just composing linear maps ultimately, so some nonlinearity is needed.
3. To use self-attention in *decoders*, as we will see later on, we don't want to have any attention on later parts of a sentence, so we need some way to *mask* future words.

We will deal with the first two problems and address the third problem in the transformer architecture.

### 11.2.1 Tokenization and Positional Embeddings

Given an input (or an output)  $\mathbf{x}$ , it must be tokenized into a sequence of tokens. This is a general preprocessing step that is done for any input, whether it be a sequence of words, a sequence of regions in an image, or a sequence of anything. The raw token data will be denoted  $w_i$  for  $i = 1, \dots, n$ . We can then embed these tokens into a vector space  $x_i \in \mathbb{R}^d$ .

As we will see later, attention does not have a way to discern the order of the input sequences. Therefore, we must add this positional information to the encoding. The most obvious way would be to simply concatenate the position of the token to the end with an index.

$$x_i \mapsto [x_i, i] \quad (313)$$

However, this is not ideal since this tends to corrupt the embedding of the token. Instead, we can think of adding certain vectors representing components to the original embedding.

$$x_i \mapsto x_i + p_i \quad (314)$$

Certain ways come to mind, such as simply letting  $p_i$  be the vector of all  $i$ 's. This tends not to work in progress since the values of  $i$  get too large and corrupts the embeddings too much.<sup>23</sup> Normalizing the values of  $i$  to be in  $[0, 1]$  is disadvantageous because now the positional embedding  $p_i$  is dependent on the length of the total input sequence. Therefore, we need two properties:

1. The positional encoding should be independent of the input sequence length.
2. The positional encoding shouldn't be too large that it corrupts the semantic meaning behind the original embedding.

It turns out that the sinusoidal function satisfies these properties.

#### Definition 11.4 (Sinusoidal Position Embedding)

Given the embeddings  $x_i \in \mathbb{R}^d$ , we can add a positional encoding to it by

$$x_i \mapsto x_i + p_i$$

where the positional encoding is given by the vector where each component is defined as

$$(p_i)_j = \begin{cases} \sin\left(\frac{i}{10000^{2j/d}}\right) & \text{if } j \text{ is even} \\ \cos\left(\frac{i}{10000^{2j/d}}\right) & \text{if } j \text{ is odd} \end{cases} \quad (315)$$

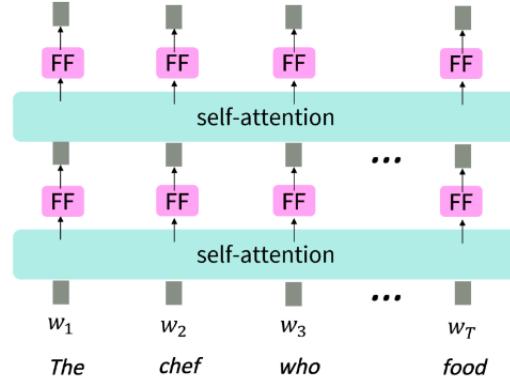
where  $i$  iterates through the tokens and  $j$  iterates through the dimensions of the embedding.

### 11.2.2 Stacked Attention Layers and Multi-Head Attention

The second problem of introducing nonlinearities is quite simple. Once we have the output of the first self-attention layer  $\mathbf{o}_{1:n} = [\mathbf{o}_1, \dots, \mathbf{o}_n]$ , we can just input each  $\mathbf{o}_i$  through a small MLP to introduce nonlinearity before inputting it into the next self-attention layer.

<sup>23</sup>A helpful Medium article here

$$\begin{aligned} m_i &= \text{MLP}(\text{output}_i) \\ &= W_2 * \text{ReLU}(W_1 \times \text{output}_i + b_1) + b_2 \end{aligned}$$



Boom, problem solved.

Going back, if we want to look at the attention for token  $x_i$ , we want to look through all  $q_i^T k_j$  for all  $j$  and find out where it is high. But perhaps we want to focus on different  $j$  for different reasons. The following example may illustrate why.

### Example 11.3 (Semantic and Syntactic Attention)

Given the sentence *I went to the bank and got some money.*, one type of attention may look at the semantic meaning of the words, such as associating *bank* with *money*. However, we may also want to look at the syntactic meaning of the words, such as associating *went* with *bank*. When we read sentences, we have different types of attention for different reasons, and so having multiple heads of attention may be useful.

### Definition 11.5 (Multi-Head Attention)

Therefore, let us construct multiple attention heads by defining multiple triplets of  $(Q, K, V)$  matrices. This may be more computationally inefficient, so we simply scale down the size of these matrices from

$$Q \in \mathbb{R}^{E_q \times d}, K \in \mathbb{R}^{E_k \times d}, V \in \mathbb{R}^{E_v \times d}$$

to

$$Q_\ell \in \mathbb{R}^{E_q \times d/h}, K_\ell \in \mathbb{R}^{E_k \times d/h}, V_\ell \in \mathbb{R}^{E_v \times d/h}$$

where  $h$  is the number of heads. We are essentially decreasing the size of the token embedding dimension in order to get more heads. We can then do attention on each head separately.

$$\text{Attention}_\ell = \text{Attention}(Q_\ell, K_\ell, V_\ell) = \text{softmax}\left(\frac{Q_\ell K_\ell^T}{\sqrt{E_k/h}}\right) V_\ell \quad (316)$$

and we can simply concatenate them together to get the final output.

$$\text{MultiHead}(Q, K, V) = \text{Concat}(\text{Attention}_1, \dots, \text{Attention}_h) W^O$$

where  $W^O \in \mathbb{R}^{d \times E_v}$  is a learnable weight matrix that mixes these heads together with a final linear transformation.<sup>a</sup> This entire process is shown in Figure 47.

<sup>a</sup>There is a valid concern that these heads may all end up learning the same thing and may just converge onto the same thing. However, this is not what happens in practice.

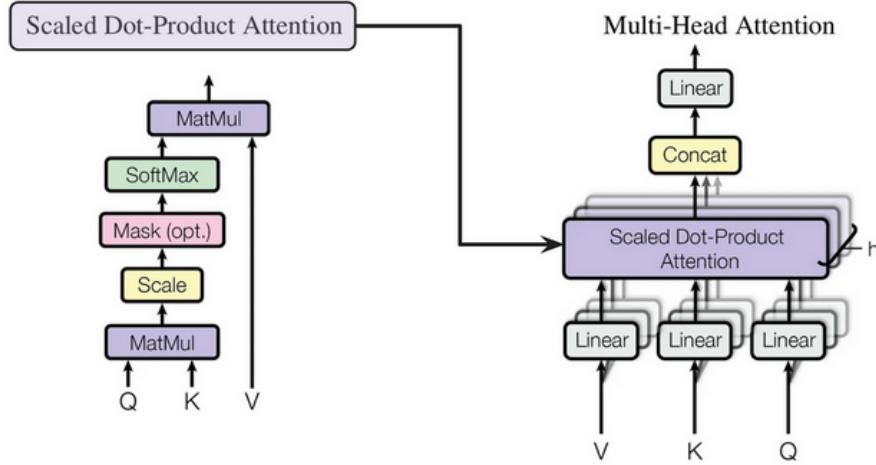


Figure 47: Diagram of multi head attention.

### 11.3 Transformers

With self-attention out of the way, the transformer architecture becomes quite simple. An overview of it is shown in Figure 48.

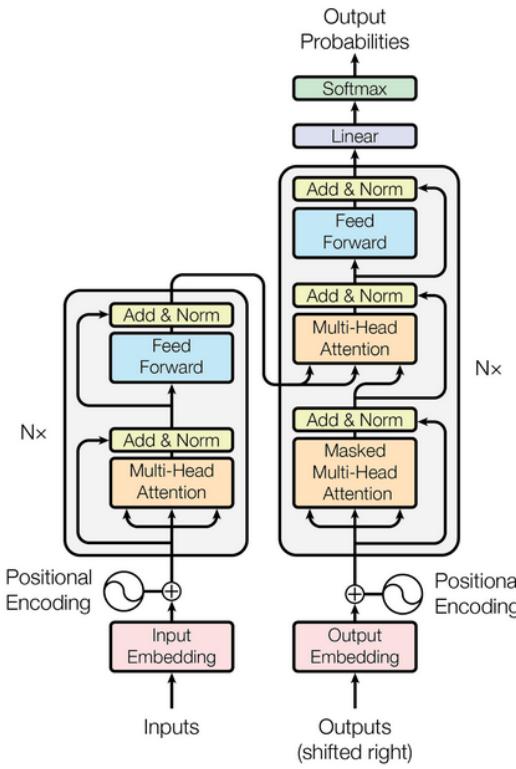


Figure 48: Transformer architecture.

The encoder is quite simple. You take the input embedding and add the positional embeddings to get  $\{x_i \in \mathbb{R}^d\}_{i=1}^n$ . You then pass it through a multi-head self-attention layer, which has outputs of shape  $E_v \times n$ , and then pass it through a feed forward network, adding residual connections and normalization

layers to help with training. You then repeat this process  $N$  times, which gives out the encoded sequence  $\mathbf{h}_{1:n} = [\mathbf{h}_1, \dots, \mathbf{h}_n]$ , now ready to be fed into the decoder.<sup>24</sup>

The decoder has two different self-attention layers. First, we run the generated output sequence through a masked self-attention layer, which generates the hidden nodes  $\mathbf{z}_{1:n} = [\mathbf{z}_1, \dots, \mathbf{z}_n]$  representing the state of the currently decoded sentence. Again, we have some maximum output length to ensure that we are working with a fixed size, and manually mask all tokens after the current one to be 0.

Then, another **cross-attention** layer takes both  $\mathbf{h}_{1:n}$  and  $\mathbf{z}_{1:n}$  and with its trained  $(\mathbf{K}, \mathbf{V}, \mathbf{Q})$ , computes the key, value, and query matrices as

$$K = \mathbf{Kh}_{1:n}, \quad V = \mathbf{Vh}_{1:n}, \quad Q = \mathbf{Qz}_{1:n}, \quad (317)$$

now ready to be plugged into to the self-attention formulas, integrating both the inputs and the current output to generate the result. This again outputs another list of vectors, which are run through an MLP and then have another set of  $(\mathbf{K}, \mathbf{V}, \mathbf{Q})$  matrices waiting for them. This makes sense, since we want to use the output sequence to query the input key-values and attend to the correct set of tokens.

The output of this is then passed through a feed forward network, with some residual connections and normalization, and finally a linear layer transforms the output dimensions to whatever is needed (e.g. size of the vocabulary, or number of classes). Once this is done, a new word is generated,<sup>25</sup> and this word (along with all previous words) is now used as the new input to the decoder in place of the start token. This process is done until the stop token is generated by the decoder. Notice that we encode with a bidirectional model (no masking) and generated the target with a unidirectional model (masking).

Note that again, parallelization of the decoder is not possible in the transformer architecture. Additionally, you can see that more normalization layers and residual connections are needed to train efficiently. This is very important in practice.

Despite all its advantages, self-attention has quadratic runtime complexity with respect to the sequence length since we need to compute attention for all pairs of words. This is worse than the linear runtime complexity in RNNs.

### 11.3.1 Masking

The final aspect we did not address is the masking. When we are training the transformer on a corpus of data, the decoder first computes self-attention on all the previous outputs first to get the query, and then takes in the output of the encoder self-attention layer as the keys and values. Then it does self-attention once more over these triplets, essentially doing a self-attention layer over the entire input and all tokens up to the current decoded output.

When training this model, we have access to the entire decoded output, and we want to make sure that we do not perform self-attention on any future words since it will most likely attend 100% to the next word to generate the next word! This does not learn anything, so we artificially set the attention distribution for all future output words to be 0. This is usually done by setting the attention scores to  $-\infty$  (or more practically, a very negative number) which will result in 0 after softmaxing.<sup>26</sup>

## 11.4 Practical Implementation

In here we go over the nitty gritty details that comes into implementing a transformer in `pytorch==2.3.0`.

### 11.4.1 Key, Value, Query Matrices and In Projections

The first thing is that these key, value, query does not have to necessarily equal to the dimension embedding, which we will denote as  $E$ . One flexibility is that we don't necessarily need to set the dimensions of the keys,

<sup>24</sup>You can see that to support iterating through  $n$  times,  $E_v$  should equal  $d$ .

<sup>25</sup>Note that we have not specified how to get the corresponding word given an embedding vector. This is not within the scope of these notes and are covered in my natural language processing notes.

<sup>26</sup>Here is a nice explanation here.

values, and queries the same. We can see in the constructor of the `torch.nn.MultiheadAttention` module that you can input your own dimensions for the keys and values, but queries must be the same as  $E$ .

```

1 def __init__(self, embed_dim, num_heads, dropout=0., bias=True, add_bias_kv=False,
2                 add_zero_attn=False,
3                 kdim=None, vdim=None, batch_first=False, device=None, dtype=None) -> None:
4     ...
5     self.embed_dim = embed_dim
6     self.kdim = kdim if kdim is not None else embed_dim
7     self.vdim = vdim if vdim is not None else embed_dim
8     self._qkv_same_embed_dim = self.kdim == embed_dim and self.vdim == embed_dim

```

In fact,  $K \in \mathbb{R}^{d_k \times E}$ ,  $V \in \mathbb{R}^{d_v \times E}$ , then  $QK^T \in \mathbb{R}^{E \times d_k}$ . Since this obviously leads to dimension mismatch problem when we multiply it with the matrix  $V$ , what we do is have an **in projection** layer that maps everything to dimension  $E$ . We can check this for the following.

$$K_{proj} \in \mathbb{R}^{E \times d_k}, V_{proj} \in \mathbb{R}^{E \times d_v}, Q_{proj} \in \mathbb{R}^{E \times E} \quad (318)$$

There are two ways to store these projection matrices, as shown in the constructor.

```

1 # in the constructor
2 ...
3 self._qkv_same_embed_dim = self.kdim == embed_dim and self.vdim == embed_dim
4
5 if not self._qkv_same_embed_dim:
6     self.q_proj_weight = Parameter(torch.empty((embed_dim, embed_dim), **factory_kwargs))
7     self.k_proj_weight = Parameter(torch.empty((embed_dim, self.kdim), **factory_kwargs))
8     self.v_proj_weight = Parameter(torch.empty((embed_dim, self.vdim), **factory_kwargs))
9     self.register_parameter('in_proj_weight', None)
10 else:
11     self.in_proj_weight = Parameter(torch.empty((3 * embed_dim, embed_dim), **factory_kwargs))
12     self.register_parameter('q_proj_weight', None)
13     self.register_parameter('k_proj_weight', None)
14     self.register_parameter('v_proj_weight', None)

```

1. If these shapes are different, then we store them in separate matrices as above.

```

1 att = nn.MultiheadAttention(embed_dim=50, num_heads=1, bias=False, kdim=30, vdim=40)
2 att.q_proj_weight.shape # torch.Size([50, 50])
3 att.k_proj_weight.shape # torch.Size([50, 30])
4 att.v_proj_weight.shape # torch.Size([50, 40])

```

2. If these shapes are the same, then we just store them in a  $3E \times E$  matrix by concatenation them.

```

1 att = nn.MultiheadAttention(embed_dim=50, num_heads=1, bias=False)
2 att.in_proj_weight.shape # torch.Size([150, 50])

```

These conditions are asserted throughout the forward pass as well.

#### 11.4.2 Masking

We multiply by a masking matrix.

#### 11.4.3 Computing Attention

First we reshape them so that they are batch first.

If `needs_weights = True`, we also output the attention weights in addition to the output, but it is said that this degrades performance. It is by default true but should be set to false for small tasks.

#### 11.4.4 Forward Pass of MultiheadAttention

First, we should look at the main function that computes self-attention. We omit a large part of the code to focus on the relevant details.

```

1  # torch.nn.functional
2  def multi_head_attention_forward(
3      query: Tensor,
4      key: Tensor,
5      value: Tensor,
6      embed_dim_to_check: int,
7      num_heads: int,
8      in_proj_weight: Optional[Tensor],
9      in_proj_bias: Optional[Tensor],
10     bias_k: Optional[Tensor],
11     bias_v: Optional[Tensor],
12     add_zero_attn: bool,
13     dropout_p: float,
14     out_proj_weight: Tensor,
15     out_proj_bias: Optional[Tensor],
16     training: bool = True,
17     ...
18 ):
19     # first unsqueezes the input if it is not batched.
20
21     # look at the input dimensions and check that multiheads divide it evenly
22     #
23     assert embed_dim == embed_dim_to_check, \
24         f"was expecting embedding dimension of {embed_dim_to_check}, but got {embed_dim}"
25     if isinstance(embed_dim, torch.Tensor):
26         # embed_dim can be a tensor when JIT tracing
27         head_dim = embed_dim.div(num_heads, rounding_mode='trunc')
28     else:
29         head_dim = embed_dim // num_heads
30     assert head_dim * num_heads == embed_dim, f"embed_dim {embed_dim} not divisible by num_heads \
31         {num_heads}"
32     if use_separate_proj_weight:
33         # allow MHA to have different embedding dimensions when separate projection weights are
34         # used
35         assert key.shape[:2] == value.shape[:2], \
36             f"key's sequence and batch dims {key.shape[:2]} do not match value's {value.shape[:2]}"
37     else:
38         assert key.shape == value.shape, f"key shape {key.shape} does not match value shape \
39             {value.shape}"
40
41     # Computes in-projection, which is an affine map before doing attention.
42     # in_proj_weight = [W_q, W_k, W_v], in_proj_bias = [b_q, b_k, b_v]
43     # computes q = q * W_q + b_q, k = k * W_k + b_k, v = v * W_v + b_v
44     if not use_separate_proj_weight:
45         q, k, v = _in_projection_packed(query, key, value, in_proj_weight, in_proj_bias)
46     else:
47         if in_proj_bias is None:
48             b_q = b_k = b_v = None
49         else:
50             b_q, b_k, b_v = in_proj_bias.chunk(3)
51         q, k, v = _in_projection(query, key, value, q_proj_weight, k_proj_weight, v_proj_weight,
```

```

    b_q, b_k, b_v)
49
50 # prepare attention mask
51 # add bias along batch dimension
52 # more preparation with mask
53 ...
54 # Now calculate attention
55 if need_weights:
56     # scale q_scaled for the sqrt(E) division factor
57     B, Nt, E = q.shape
58     q_scaled = q * math.sqrt(1.0 / float(E))
59
60 if attn_mask is not None:
61     # torch.baddbmm is a pybinded C function implementing matrix multiplication
62     # of form attn_mask + q_scaled @ k^T
63     attn_output_weights = torch.baddbmm(attn_mask, q_scaled, k.transpose(-2, -1))
64 else:
65     # torch.bmm is also a pybinded C function q_scaled + k^T
66     attn_output_weights = torch.bmm(q_scaled, k.transpose(-2, -1))
67 ...
68 # softmax it and then multiply it by V.
69 attn_output_weights = softmax(attn_output_weights, dim=-1)
70 attn_output = torch.bmm(attn_output_weights, v)
71
72 # final linear layer for more weightings.
73 attn_output = attn_output.transpose(0, 1).contiguous().view(tgt_len * bsz, embed_dim)
74 attn_output = linear(attn_output, out_proj_weight, out_proj_bias)
75 attn_output = attn_output.view(tgt_len, bsz, attn_output.size(1))
76
77 # optionally average attention weights over heads
78 attn_output_weights = attn_output_weights.view(bsz, num_heads, tgt_len, src_len)
79 if average_attn_weights:
80     attn_output_weights = attn_output_weights.mean(dim=1)
81
82 if not is_batched:
83     # squeeze the output if input was unbatched
84     attn_output = attn_output.squeeze(1)
85     attn_output_weights = attn_output_weights.squeeze(0)
86 return attn_output, attn_output_weights

```

This is precisely the function that is called in the forward method of the MultiheadAttention module.

#### 11.4.5 Transformer

In the transformer, we can see that if we peek at the state dictionary, it composes of an encoder and a decoder, each with a certain number of attention layers. There are 6 attention layers each by default.

```

1 transformer = nn.Transformer()
2 transformer.state_dict
3 # output
4 <bound method Module.state_dict of Transformer(
5     encoder): TransformerEncoder(
6         (layers): ModuleList(
7             (0-5): 6 x TransformerEncoderLayer(
8                 (self_attn): MultiheadAttention(
9                     (out_proj): NonDynamicallyQuantizableLinear(in_feat
10                        ureas=512, out_features=512, bias=True)
11                )

```

```

12     (linear1): Linear(in_features=512, out_features=2048,
13     bias=True)
14     (dropout): Dropout(p=0.1, inplace=False)
15     (linear2): Linear(in_features=2048, out_features=512,
16     bias=True)
17     (norm1): LayerNorm((512,), eps=1e-05, elementwise_aff
18     ine=True)
19     (norm2): LayerNorm((512,), eps=1e-05, elementwise_aff
20     ine=True)
21     (dropout1): Dropout(p=0.1, inplace=False)
22     (dropout2): Dropout(p=0.1, inplace=False)
23   )
24 )
25   (norm): LayerNorm((512,), eps=1e-05, elementwise_affine=T
26 rue)
27 )
28   (decoder): TransformerDecoder(
29     (layers): ModuleList(
30       (0-5): 6 x TransformerDecoderLayer(
31         (self_attn): MultiheadAttention(
32           (out_proj): NonDynamicallyQuantizableLinear(in_feat
33             ures=512, out_features=512, bias=True)
34           )
35         (multihead_attn): MultiheadAttention(
36           (out_proj): NonDynamicallyQuantizableLinear(in_feat
37             ures=512, out_features=512, bias=True)
38           )
39         (linear1): Linear(in_features=512, out_features=2048,
40         bias=True)
41         (dropout): Dropout(p=0.1, inplace=False)
42         (linear2): Linear(in_features=2048, out_features=512,
43         bias=True)
44         (norm1): LayerNorm((512,), eps=1e-05, elementwise_aff
45         ine=True)
46         (norm2): LayerNorm((512,), eps=1e-05, elementwise_aff
47         ine=True)
48         (norm3): LayerNorm((512,), eps=1e-05, elementwise_aff
49         ine=True)
50         (dropout1): Dropout(p=0.1, inplace=False)
51         (dropout2): Dropout(p=0.1, inplace=False)
52         (dropout3): Dropout(p=0.1, inplace=False)
53       )
54     )
55   (norm): LayerNorm((512,), eps=1e-05, elementwise_affine=T
56 rue)
57 )
58 )>

```

## 11.5 Vision Transformers

We have hinted at attention being applicable in other architectures, and the most popular is in computer vision. Historically, CNNs were very useful because they take into account the locality and translational-invariance of objects in images inherently in the convolutions. This is a great strength of convolutional networks.

Can transformers beat this? These assumptions are not built into the architecture, and researchers were quite unsuccessful in passing the benchmarks set by CNNs, but it turned out that in 2020, with enough

training and a large enough architecture, *vision transformers* in fact did surpass CNNs.

## 12 Diffusion Models

## 13 Semi Supervised Learning

There has been good stream of work done at Google Brain that first came up with MixMatch in 2019 [BCG<sup>+</sup>19], which combined the state of the art semi supervised methods. This model was then improved the next year with ReMixMatch [BCC<sup>+</sup>20], and then improved again with a much more simple model called FixMatch [SBL<sup>+</sup>20].

### 13.1 Pseudo Label Learning

Generating psuedo labels on unlabeled datasets and training on them.

### 13.2 Consistency Regularization

Ensuring that the model is consistent with its predictions on certain inputs and neighbors of the inputs. It relies on the assumption that perturbed versions of the same input should have the same output. When wanting to make sure that the outputs are consistent with augmentations of the input, this is called **augmentation anchoring**. There are ways in which we use a combination of **weak augmentation** and **strong augmentation** to achieve this.

### 13.3 Distribution Alignment

### 13.4 Weak Supervision

### 13.5 Student Teacher Models

## References

- [BCC<sup>+</sup>20] David Berthelot, Nicholas Carlini, Ekin D. Cubuk, Alex Kurakin, Kihyuk Sohn, Han Zhang, and Colin Raffel. Remixmatch: Semi-supervised learning with distribution alignment and augmentation anchoring, 2020.
- [BCG<sup>+</sup>19] David Berthelot, Nicholas Carlini, Ian Goodfellow, Nicolas Papernot, Avital Oliver, and Colin Raffel. Mixmatch: A holistic approach to semi-supervised learning, 2019.
- [CLHN93] An Mei Chen, Haw-minn Lu, and Robert Hecht-Nielsen. On the geometry of feedforward neural network error surfaces. *Neural Computation*, 5(6):910–927, 11 1993.
- [DDS<sup>+</sup>09] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. Imagenet: A large-scale hierarchical image database. In *2009 IEEE Conference on Computer Vision and Pattern Recognition*, pages 248–255, 2009.
- [DKB15] Laurent Dinh, David Krueger, and Yoshua Bengio. Nice: Non-linear independent components estimation, 2015.
- [FC19] Jonathan Frankle and Michael Carbin. The lottery ticket hypothesis: Finding sparse, trainable neural networks, 2019.
- [GPAM<sup>+</sup>14] Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial networks, 2014.
- [Hyv05] Aapo Hyvärinen. Estimation of non-normalized statistical models by score matching. *Journal of Machine Learning Research*, 6(24):695–709, 2005.
- [KW22] Diederik P Kingma and Max Welling. Auto-encoding variational bayes, 2022.
- [LBBH98] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324, 1998.
- [Mis20] Diganta Misra. Mish: A self regularized non-monotonic activation function, 2020.
- [RM16] Danilo Jimenez Rezende and Shakir Mohamed. Variational inference with normalizing flows, 2016.
- [SBL<sup>+</sup>20] Kihyuk Sohn, David Berthelot, Chun-Liang Li, Zizhao Zhang, Nicholas Carlini, Ekin D. Cubuk, Alex Kurakin, Han Zhang, and Colin Raffel. Fixmatch: Simplifying semi-supervised learning with consistency and confidence, 2020.
- [SHK<sup>+</sup>14] Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever, and Ruslan Salakhutdinov. Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research*, 15(56):1929–1958, 2014.
- [SSK<sup>+</sup>20] Yang Song, Jascha Sohl-Dickstein, Diederik P. Kingma, Abhishek Kumar, Stefano Ermon, and Ben Poole. Score-based generative modeling through stochastic differential equations. *CoRR*, abs/2011.13456, 2020.
- [TD20] Edric Tam and David Dunson. Fiedler regularization: Learning neural networks with graph sparsity, 2020.