Notebook credit: based on the F. Chollet's original notebook here.

Fundamentals of machine learning

Improving model fit

Many DL projects will go through the following progression (also listed are ideas that help you make progress if you're stuck at a particular stage):

- 1. Training loss goes down over time. (如果失败则 try changing gradient descent parameters)
- 2. Model meaningfully generalizes: you can beat a common-sense baseline you set. (如果失败则 leverage better architecture priors)
- 3. Your model is able to *overfit* (low training loss, high validation loss). (如果失败则 increase model capacity.)

Now—4. refine generalization by fighting overfitting.

Tuning key gradient descent parameters

Training a MNIST model with an incorrectly high learning rate

An inappropriately large learning rate(of value 1) can cause training to fail even on a simple problem like MNIST.

```
import numpy as np
import matplotlib.pyplot as plt
import tensorflow as tf

from tensorflow.keras.datasets import mnist
from tensorflow import keras
from tensorflow.keras import layers
```

```
(train images, train labels), = mnist.load data()
train images = train images.reshape((60000, 28 * 28))
train images = train_images.astype("float32") / 255
model = keras.Sequential([
 layers.Dense(512, activation="relu"),
 layers.Dense(10, activation="softmax")
1)
model.compile(optimizer=keras.optimizers.RMSprop(1.), # use a learning rate of 1.0 \
      loss="sparse categorical crossentropy",
      metrics=["accuracy"])
model.fit(train_images, train_labels,
    epochs=10,
    batch_size=128,
    validation split=0.2)
  Epoch 1/10
  Epoch 2/10
  Epoch 3/10
  Epoch 4/10
  Epoch 5/10
  Epoch 6/10
  Epoch 7/10
  Epoch 8/10
  Epoch 9/10
  Epoch 10/10
  <keras.src.callbacks.History at 0x7bc7292a7bb0>
```

The same model with a more appropriate learning rate

```
model = keras.Sequential([
 layers.Dense(512, activation="relu"),
 layers.Dense(10, activation="softmax")
1)
model.compile(optimizer=keras.optimizers.RMSprop(1e-2), # use a smaller learning ra-
     loss="sparse categorical crossentropy",
     metrics=["accuracy"])
model.fit(train images, train labels,
   epochs=10,
   batch size=128,
   validation split=0.2)
 Epoch 1/10
 Epoch 2/10
 Epoch 3/10
 Epoch 4/10
 Epoch 5/10
 Epoch 6/10
 Epoch 7/10
 Epoch 8/10
 Epoch 9/10
 Epoch 10/10
 <keras.src.callbacks.History at 0x7bc71b34be80>
```

If training appears to get stuck, you can try the following:

- Lowering or increasing the learning rate. A learning rate that is too high may lead to updates that vastly overshoot a proper fit, like in the preceding example, and a learning rate that is too low may make training so slow that it appears to stall.
- Increasing the batch size. A batch with more samples will lead to gradients that are more informative and less noisy (lower variance).

Leveraging better architecture priors

You are able to get training started, but for some reason your validation metrics aren't improving at all. They remain no better than what a random classifier would achieve: your model trains but

doesn't generalize. There might be several reasons why this might be happening. Two common ones are:

Input data simply doesn't contain sufficient information to predict your targets

- what happened when we tried to fit an MNIST model where the labels were shuffled
- the model would train just fine, but validation accuracy would stay stuck at 10%
- it was plainly impossible to generalize with such a dataset

The kind of model you're using is not suited for the problem at hand

- In a timeseries prediction problem, a densely connected architecture may be less appropriate: a *recurrent* architecture might generalize better
- Using a model that makes the right assumptions about the problem is essential to achieve generalization: you should leverage the right architecture priors
- We will learn about the best architectures to use for a variety of data modalities—images, text, timeseries, and so on

Increasing model capacity

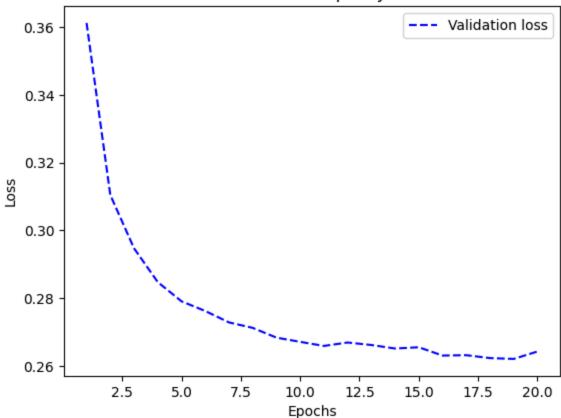
A simple logistic regression on MNIST

```
model = keras.Sequential([layers.Dense(10, activation="softmax")])
model.compile(optimizer="rmsprop",
     loss="sparse categorical crossentropy",
     metrics=["accuracy"])
history small model = model.fit(
 train images, train labels,
 epochs=20,
 batch size=128,
 validation split=0.2)
 Epoch 1/20
 Epoch 2/20
 Epoch 3/20
 Epoch 4/20
 Epoch 5/20
 Epoch 6/20
 Epoch 7/20
 Epoch 8/20
```

```
Epoch 9/20
Epoch 10/20
Epoch 11/20
Epoch 12/20
Epoch 13/20
Epoch 14/20
Epoch 15/20
Epoch 16/20
Epoch 17/20
Epoch 18/20
Epoch 19/20
Epoch 20/20
```

<matplotlib.legend.Legend at 0x7bc73c20da20>

Effect of insufficient model capacity on validation loss



- Validation metrics seem to stall, or to improve very slowly, instead of peaking and reversing course.
- You can fit, but you can't clearly overfit, even after many iterations over the training data.

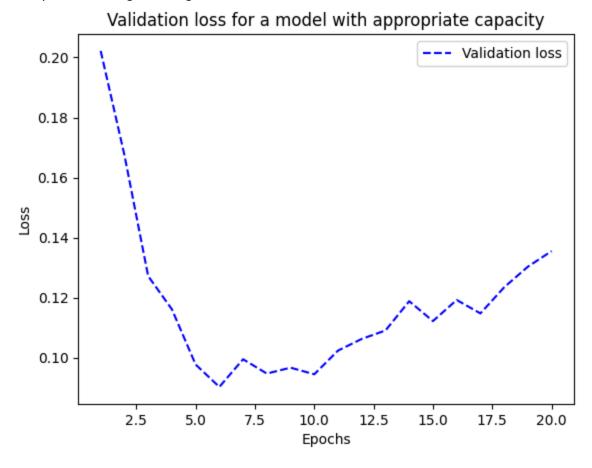
It should always be possible to overfit

- If you can't seem to be able to overfit, it's likely a problem with the representational power of your model
- You're going to need a bigger model, one with more capacity, that is to say, one able to store more information
- · You can increase representational power by
 - o adding more layers
 - $\circ \ \ using \ bigger \ layers \ (layers \ with \ more \ parameters)$
 - using kinds of layers that are more appropriate for the problem at hand (better architecture priors).

Let's try training a bigger model, one with two intermediate layers with 96 units each:

```
model = keras.Sequential([
 layers.Dense(96, activation="relu"),
 layers.Dense(96, activation="relu"),
 layers.Dense(10, activation="softmax"),
1)
model.compile(optimizer="rmsprop",
   loss="sparse_categorical_crossentropy",
   metrics=["accuracy"])
history_large_model = model.fit(
 train images, train labels,
 epochs=20,
 batch_size=128,
 validation split=0.2)
 Epoch 1/20
 Epoch 2/20
 Epoch 3/20
 Epoch 4/20
 Epoch 5/20
 Epoch 6/20
 Epoch 7/20
 Epoch 8/20
 Epoch 9/20
 Epoch 10/20
 Epoch 11/20
 Epoch 12/20
 Epoch 13/20
 Epoch 14/20
 Epoch 15/20
 Epoch 16/20
 Epoch 17/20
 Epoch 18/20
 Epoch 19/20
 Epoch 20/20
```

<matplotlib.legend.Legend at 0x7bc71a79a470>



Improving generalization

Regularizing your model

Regularization: actively impeding the model's ability to fit perfectly to the training data, with the goal of making the model perform better during validation.

 regularizing a model is a process that should always be guided by an accurate evaluation procedure · you will only achieve generalization if you can measure it!

Let's review some of the most common regularization techniques in the context of IMDB movie reviews problem

Reducing the network's size

- · a model that is too small will not overfit
- simplest way to mitigate overfitting is to reduce the size of the model
- number of learnable parameters in the model is determined by the number of layers and the number of units per layer
- however, you should use models that have enough parameters that they don't underfit!
- compromise is to be found between too much capacity and not enough capacity
- no magical formula to determine the right number of layers or the right size for each layer
- evaluate an array of different architectures (on your validation set, not on your test set, of course) in order to find the correct model size for your data
- general workflow for finding an appropriate model size:
 - start with relatively few layers and parameters
 - increase the size of the layers or add new layers until you see diminishing returns with regard to validation loss

Original model

```
from tensorflow.keras.datasets import imdb
(train_data, train_labels), _ = imdb.load_data(num_words=10000)
def vectorize_sequences(sequences, dimension=10000):
    results = np.zeros((len(sequences), dimension))
    for i, sequence in enumerate(sequences):
        results[i, sequence] = 1.
    return results
train_data = vectorize_sequences(train_data)
model = keras.Sequential([
    layers.Dense(16, activation="relu"),
    layers.Dense(16, activation="relu"),
    layers.Dense(1, activation="sigmoid")
1)
model.compile(optimizer="rmsprop",
              loss="binary crossentropy",
              metrics=["accuracy"])
history_original = model.fit(train_data, train_labels,
                             epochs=20, batch size=512, validation split=0.4)
```

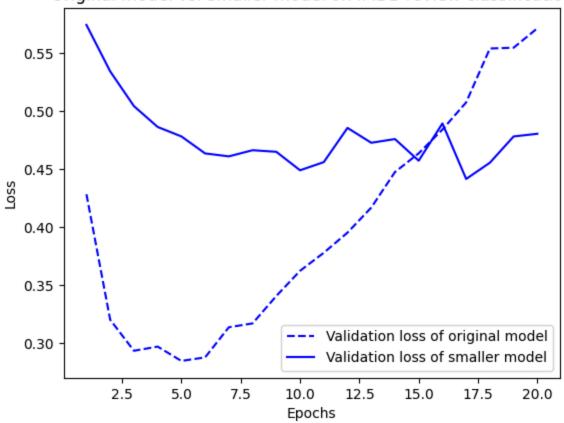
```
Epoch 1/20
Epoch 2/20
Epoch 3/20
Epoch 4/20
Epoch 5/20
30/30 [=========================== ] - 1s 43ms/step - loss: 0.1571 - accuracy:
Epoch 6/20
Epoch 7/20
Epoch 8/20
Epoch 9/20
Epoch 10/20
Epoch 11/20
Epoch 12/20
Epoch 13/20
Epoch 14/20
Epoch 15/20
Epoch 16/20
Epoch 17/20
Epoch 18/20
Epoch 19/20
30/30 [=========================== ] - 1s 44ms/step - loss: 0.0204 - accuracy:
Epoch 20/20
30/30 [=========================== ] - 1s 40ms/step - loss: 0.0170 - accuracy:
```

Version of the model with lower capacity

```
model = keras.Sequential([
 layers.Dense(4, activation="relu"),
 layers.Dense(4, activation="relu"),
 layers.Dense(1, activation="sigmoid")
1)
model.compile(optimizer="rmsprop",
    loss="binary_crossentropy",
    metrics=["accuracy"])
history_smaller_model = model.fit(
 train_data, train_labels,
 epochs=20, batch size=512, validation split=0.4)
 Epoch 1/20
 30/30 [=========================== ] - 3s 94ms/step - loss: 0.6234 - accuracy:
 Epoch 2/20
 Epoch 3/20
 Epoch 4/20
 Epoch 5/20
 Epoch 6/20
 Epoch 7/20
 Epoch 8/20
 Epoch 9/20
 Epoch 10/20
 Epoch 11/20
 Epoch 12/20
 Epoch 13/20
 Epoch 14/20
 Epoch 15/20
 Epoch 16/20
 Epoch 17/20
 Epoch 18/20
 Epoch 19/20
 Epoch 20/20
 30/30 [=========================== ] - 1s 31ms/step - loss: 0.2502 - accuracy:
```

<matplotlib.legend.Legend at 0x7bc720ce2710>

Original model vs. smaller model on IMDB review classification



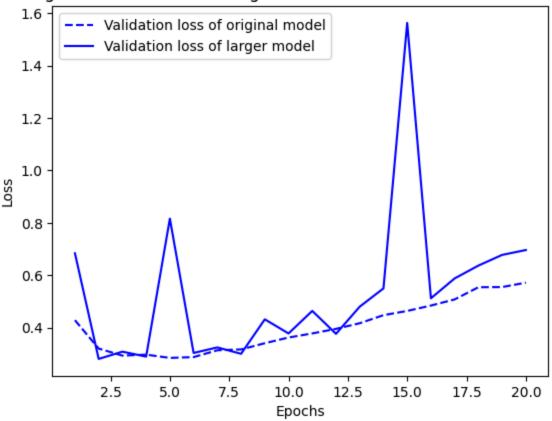
- the smaller model starts overfitting later than the reference model
- its performance degrades more slowly once it starts overfitting

Version of the model with higher capacity

```
model = keras.Sequential([
 layers.Dense(512, activation="relu"),
 layers.Dense(512, activation="relu"),
 layers.Dense(1, activation="sigmoid")
1)
model.compile(optimizer="rmsprop",
    loss="binary_crossentropy",
    metrics=["accuracy"])
history_larger_model = model.fit(
 train_data, train_labels,
 epochs=20, batch size=512, validation split=0.4)
 Epoch 1/20
 30/30 [============== ] - 13s 400ms/step - loss: 0.5620 - accurac
 Epoch 2/20
 Epoch 3/20
 Epoch 4/20
 Epoch 5/20
 Epoch 6/20
 Epoch 7/20
 Epoch 8/20
 Epoch 9/20
 Epoch 10/20
 Epoch 11/20
 Epoch 12/20
 Epoch 13/20
 Epoch 14/20
 Epoch 15/20
 Epoch 16/20
 Epoch 17/20
 Epoch 18/20
 Epoch 19/20
 Epoch 20/20
```

<matplotlib.legend.Legend at 0x7bc7259e9990>

Original model vs. much larger model on IMDB review classification



- bigger model starts overfitting almost immediately
- it overfits much more severely
- its validation loss is also noisier
- it gets training loss near zero very quickly
- a very high capacity model will
 - fit the the training data quickly (resulting in a low training loss)
 - but will be more susceptible it is to overfitting (resulting in a large difference between the training and validation loss)

Adding weight regularization

Adding L2 weight regularization to the model

Regularization can be applied to:

- weights using kernel_regularizer
- biases using bias_regularizer
- output of the layer using activity_regularizer

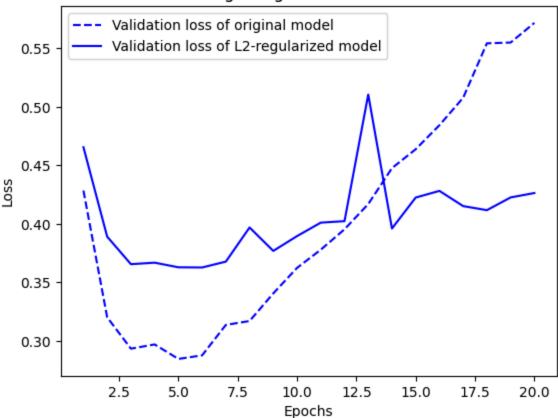
We will use weight regularization below.

```
from tensorflow.keras import regularizers
model = keras.Sequential([
  # every coefficient in the weight matrix of the layer will add
  # 0.002 * weight coefficient value ** 2
  # to the total loss of the model
  layers.Dense(16,
         kernel regularizer=regularizers.12(0.002),
         activation="relu"),
  layers.Dense(16,
         kernel regularizer=regularizers.12(0.002),
         activation="relu"),
  layers.Dense(1, activation="sigmoid")
1)
model.compile(optimizer="rmsprop",
       loss="binary_crossentropy",
       metrics=["accuracy"])
history l2 reg = model.fit(
  train_data, train_labels,
  epochs=20, batch size=512, validation split=0.4)
  Epoch 1/20
  Epoch 2/20
  Epoch 3/20
  Epoch 4/20
  Epoch 5/20
  Epoch 6/20
  Epoch 7/20
  Epoch 8/20
  Epoch 9/20
  30/30 [=========================== ] - 1s 34ms/step - loss: 0.2360 - accuracy:
```

```
Epoch 10/20
30/30 [=========================== ] - 1s 36ms/step - loss: 0.2248 - accuracy:
Epoch 11/20
Epoch 12/20
Epoch 13/20
Epoch 14/20
Epoch 15/20
Epoch 16/20
Epoch 17/20
Epoch 18/20
Epoch 19/20
Epoch 20/20
```

<matplotlib.legend.Legend at 0x7bc72018e1d0>

Effect of L2 weight regularization on validation loss



- model with L2 regularization has become much more resistant to overfitting than the reference model
- both models have the same number of parameters

Total loss when using weight regularization includes prediction losses as well as layer losses

- "loss" as a metric changes meaning when you have weight regularization
- without regularization, loss is simply the average of the prediction loss function over the dataset
- with weight regularization, loss includes both prediction losses as well as regularization losses for regularized layers

Different weight regularizers available in Keras

```
from tensorflow.keras import regularizers
regularizers.l1(0.001)
regularizers.l1_l2(l1=0.001, l2=0.001)
```

<keras.src.regularizers.L1L2 at 0x7bc72b6f3640>

- weight regularization is more typically used for smaller deep learning models
- large deep learning models tend to be so overparameterized that imposing constraints on weight values hasn't much impact on model capacity and generalization
- in these cases, a different regularization technique is preferred: dropout

Adding dropout

Adding dropout to the IMDB model

```
model = keras.Sequential([
 layers.Dense(16, activation="relu"),
 layers.Dropout(0.5),
 layers.Dense(16, activation="relu"),
 layers.Dropout(0.5),
 layers.Dense(1, activation="sigmoid")
1)
model.compile(optimizer="rmsprop",
    loss="binary crossentropy",
    metrics=["accuracy"])
history_dropout = model.fit(
 train data, train labels,
 epochs=20, batch size=512, validation split=0.4)
 Epoch 1/20
 Epoch 2/20
 Epoch 3/20
 Epoch 4/20
 Epoch 5/20
 Epoch 6/20
 Epoch 7/20
 Epoch 8/20
 Epoch 9/20
 Epoch 10/20
 Epoch 11/20
 Epoch 12/20
 Epoch 13/20
```

<matplotlib.legend.Legend at 0x7bc724d25570>

- dropout achieves clear improvement over the reference model
- it also seems to be working much better than L2 regularization (lowest validation loss reached has improved)



How does dropout work?



- dropout, applied to a layer, consists of randomly dropping out (setting to zero) a number of output features of the layer during training
- after applying dropout, the layer output will have a few zero entries distributed at random
- the dropout rate is the fraction of the features that are zeroed out; it's usually set between 0.2 and 0.5.

```
1 \
                                                                        ı
batch_size = 4
feature dim = 5
layer_output = tf.random.uniform((batch_size, feature_dim)) # in reality, layer_outp
layer output.numpy()
    array([[0.02471972, 0.04226112, 0.6676756 , 0.28473115, 0.10217285],
            [0.43423676, 0.8592428 , 0.5135548 , 0.03304565, 0.91238153],
            [0.41194844, 0.9791504 , 0.8356286 , 0.2270031 , 0.373057 ],
            [0.95226467, 0.92783797, 0.4603274, 0.34082532, 0.12339067]],
          dtype=float32)
dropout = 0.2 # dropout probability
mask = tf.random.uniform(shape=layer output.shape) < 1 - dropout # random boolean a</pre>
mask = tf.cast(mask, tf.float32) # convert True/False to 1/0
mask.numpy()
    array([[1., 1., 1., 0., 1.],
            [1., 1., 1., 1., 1.],
            [0., 1., 1., 1., 1.]
            [1., 1., 0., 0., 1.]], dtype=float32)
layer_output_dropout = layer_output * mask
layer output dropout.numpy() # roughly half of the entries will have been zeroed ou
    array([[0.02471972, 0.04226112, 0.6676756, 0.
                                                           , 0.10217285].
            [0.43423676, 0.8592428 , 0.5135548 , 0.03304565, 0.91238153],
                      , 0.9791504 , 0.8356286 , 0.2270031 , 0.373057 ],
            [0.95226467, 0.92783797, 0.
                                                           , 0.12339067]].
                                               . 0.
```