

# OAT40 Day 3: Transfer learning

```
In [1]: #FTO COMPLETE AND RUN
name: "Juan Nicolas"
surname: "Rodrigo RANCARICO"
```

## Setup

```
In [4]: import numpy as np
import tensorflow as tf
from tensorflow import keras
```

## Introduction

**Transfer learning** consists of taking features learned on one problem, and leveraging them on a new, similar problem. For instance, features from a model that has learned to identify racoons may be useful to kick-start a model meant to identify tanukis.

Transfer learning is usually done for tasks where your dataset has too little data to train a full-scale model from scratch.

The most common incarnation of transfer learning in the context of deep learning is the following workflow:

1. take layers from a previously trained model.
2. freeze them so as to avoid destroying any of the information they contain during future training rounds;
3. add some new, trainable layers on top of the frozen layers. They will learn to turn the old features into predictions on a new dataset;
4. train the new layers on your dataset.

A last, optional step is **fine-tuning**, which consists of unfreezing the entire model you obtained above (or part of it), and re-training it on the new data with a very low learning rate. This can potentially achieve meaningful improvements by incrementally adapting the pretrained features to the new data.

First, we'll go over the Keras `Trainable` API in detail, which underlies most transfer learning & fine-tuning workflows.

Then, we'll demonstrate the typical workflow by taking a model pretrained on the ImageNet dataset, and retraining it on the Kaggle "cats vs dogs" classification dataset.

## Freezing layers: understanding the `trainable` attribute

Layers & models have three weight attributes:

- `weights`: is the list of all weights variables of the layer.
- `trainable_weights`: is the list of those that are meant to be updated (via gradient descent) to minimize the loss during training.
- `non_trainable_weights`: is the list of those that aren't meant to be trained.

Typically they are updated by the model during the forward pass.

**Example: the `Dense` layer has 2 trainable weights (kernel & bias)**

```
In [5]: layer = keras.layers.Dense(3)
layer.build((None, 4)) # Create the weights

print("tensors:", len(layer.weights))
print("weights shape:", layer.weights[0].shape)
print("biases shape:", layer.weights[1].shape)
print("trainable tensors:", len(layer.trainable_weights))
print("non-trainable tensors:", len(layer.non_trainable_weights))

tensors: 2
weights shape: (4, 3)
biases shape: (3,)
trainable tensors: 2
non-trainable tensors: 0

In general, all weights are trainable weights. The only built-in layer that has non-trainable weights is the BatchNormalization layer. It uses non-trainable weights to keep track of the mean and variance of its inputs during training. To learn how to use non-trainable weights in your own custom layers, see the guide to writing new layers from scratch.
Example: the BatchNormalization layer has 2 trainable weights and 2 non-trainable weights
```

```
In [6]: layer = keras.layers.BatchNormalization()
layer.build((None, 4)) # Create the weights

print("tensors:", len(layer.weights))
print("trainable tensors:", len(layer.trainable_weights))
print("non-trainable tensors:", len(layer.non_trainable_weights))

tensors: 4
trainable tensors: 2
non-trainable tensors: 2

Layers & models also feature a boolean attribute trainable. Its value can be changed. Setting layer.trainable = False moves all the layer's weights from trainable to non-trainable. This is called "freezing" the layer: the state of a frozen layer won't be updated during training (either when training with fit() or when training with any custom loop that relies on trainable_weights to apply gradient updates).
Example: setting trainable = False
```

```
In [7]: layer = keras.layers.Dense(3)
layer.build((None, 4)) # Create the weights
layer.trainable = False

print("tensors:", len(layer.weights))
print("trainable tensors:", len(layer.trainable_weights))
print("non-trainable tensors:", len(layer.non_trainable_weights))

tensors: 2
trainable tensors: 0
non-trainable tensors: 2

When a trainable weight becomes non-trainable, its value is no longer updated during training.
```

```
In [8]: # Make a model with 2 layers
layer1 = keras.layers.Dense(2, activation="relu")
layer2 = keras.layers.Dense(3, activation="sigmoid")
model = keras.Sequential([keras.layers.Input(shape=(3,)), layer1, layer2])

# Freeze the first layer
layer1.trainable = False

# Keep a copy of the weights of layer1 for later reference
initial_layer_weights_values = layer1.get_weights()

# Train the model
model.compile(optimizer="adam", loss="mse")
model.fit(np.random.random((2, 3)), np.random.random((2, 3)))

# Check that the weights of layer1 have not changed during training
final_layer_weights_values = layer1.get_weights()
np.testing.assert_allclose(
    initial_layer_weights_values[0], final_layer_weights_values[0]
)
np.testing.assert_allclose(
    initial_layer_weights_values[1], final_layer_weights_values[1]
)

print("\n Weights in layer 1 before training . . .")
print(initial_layer_weights_values[0])
print(" . . . and after training")
print(final_layer_weights_values[0])
print("\n Biases in layer 1 before training . . .")
print(initial_layer_weights_values[1])
print(" . . . and after training")
print(final_layer_weights_values[1])

1/5 ----- 1s 1s/step - loss: 0.8576

Weights in layer 1 before training . . .
[[ 0.988589  -0.7976346 -0.8738829]
 [-0.2171748  0.9916198 -0.86871846]
 [-0.6248955  0.2249184 -0.2598319 ]
 . . . and after training
[[ 0.988589  -0.7976346 -0.8738829]
 [-0.2171748  0.9916198 -0.86871846]
 [-0.6248955  0.2249184 -0.2598319 ]

Biases in layer 1 before training . . .
[0. 0.]
 . . . and after training
[0. 0.]

Do not confuse the layer.trainable attribute with the argument training in layer.__call__() (which controls whether the layer should run its forward pass in inference mode or training mode). For more information, see the Keras FAQ.
```

## Recursive setting of the `trainable` attribute

If you set `trainable = False` on a model or on any layer that has sublayers, all children layers become non-trainable as well.

```
Example:

In [9]: backbone_model = keras.Sequential( #define a sequential model with input of shape (3,), followed by two dense layers of size 3, relu-activated
[
    keras.layers.Input(shape=(3,)),
    keras.layers.Dense(3, activation="relu"),
    keras.layers.Dense(3, activation="relu")
]
)

model = keras.Sequential(
    [keras.Input(shape=(3,)), backbone_model, keras.layers.Dense(3, activation="sigmoid"),]
)

model.trainable = False # Freeze the outer model

assert backbone_model.trainable == False # All layers in 'model' are now frozen
assert backbone_model.layers[0].trainable == False # 'trainable' is propagated recursively
```

## The typical transfer-learning workflow

This leads us to how a typical transfer learning workflow can be implemented in Keras:

1. Instantiate a base model and load pre-trained weights into it.
2. Freeze all layers in the base model by setting `trainable = False`.
3. Create a new model on top of the output of one (or several) layers from the base model.
4. Train your new model on your new dataset.

Note that an alternative, more fglhweight workflow could also be:

1. Instantiate a base model and load pre-trained weights into it.
2. Run your new dataset through it and record the output of one (or several) layers from the base model. This is called **feature extraction** 3. Use that output as input data for a new, smaller model.

A key advantage of that second workflow is that you only run the base model once on your data, rather than once per epoch of training. So it's a lot faster & cheaper.

An issue with that second workflow, though, is that it doesn't allow you to dynamically modify the input data of your new model during training, which is required when doing data augmentation. For instance, Transfer learning is typically used for tasks where your new dataset has too little data to train a full-scale model from scratch, and in such scenarios data augmentation is very important. So in what follows, we will focus on the first workflow.

Here's what the first workflow looks like in Keras:

```
First, instantiate a base model with pre-trained weights.

base_model = keras.applications.ResNet50V2(
    weights='imagenet', # Load weights pre-trained on ImageNet.
    input_shape=(150, 150, 3),
    include_top=False) # Do not include the ImageNet classifier at the top.

Then, freeze the base model.

base_model.trainable = False

Create a new model on top.

inputs = keras.Input(shape=(150, 150, 3))
# We make sure that the base_model is running in inference mode here,
# by passing 'training=False'. This is important for fine-tuning, as you will
# lose it in a few paragraphs.
x = base_model(inputs, training=False)
# Convert features of shape 'base_model.output_shape[i:]' to vectors
x = keras.layers.GlobalAveragePooling2D()(x)
# A dense classifier with a single unit (binary classification)
outputs = keras.layers.Dense(1)(x)
model = keras.Model(inputs, outputs)
Train the model on new data.

model.compile(optimizer=keras.optimizers.Adam(),
              loss=keras.losses.BinaryCrossentropy(from_logits=True),
              metrics=[keras.metrics.BinaryAccuracy()])

model.fit(new_dataset, epochs=20, callbacks=..., validation_data=...)
```

## Fine-tuning

Once your model has converged on the new data, you can try to unfreeze all or part of the base model and retrain the whole model end-to-end with a very low learning rate.

This is an optimal last step that can potentially give you incremental improvements. It could also potentially lead to quick overfitting -- keep that in mind.

It's critical to only do this step after the model with frozen layers has been trained to convergence. If you mix randomly-initialized trainable layers with trainable layers that hold pre-trained features, the randomly-initialized layers will cause very large gradient updates during training, which will destroy your pre-trained features.

It's also critical to use a very low learning rate at this stage, because you are training a much larger model than in the first round of training, on a dataset that is typically very small. As a result, you are at risk of overfitting very quickly if you apply large weight updates. Here, you only want to readapt the pretrained weights in an incremental way.

This is how to implement fine-tuning of the whole base model:

```
# Unfreeze the base model
base_model.trainable = True

# It's important to recompile your model after you make any changes
# to the 'trainable' attribute of any layer, so that your changes
# are taken into account
model.compile(optimizer=keras.optimizers.Adam(1e-5), # Very low learning rate
              loss=keras.losses.BinaryCrossentropy(from_logits=True),
              metrics=[keras.metrics.BinaryAccuracy()])

# Train end-to-end. Be careful to stop before you overfit!
model.fit(new_dataset, epochs=10, callbacks=..., validation_data=...)

Important note about compile() and trainable

Calling compile() on a model is meant to "freeze" the behavior of that model. This implies that the trainable attribute values at the time the model is compiled should be preserved throughout the lifetime of that model, until compile is called again. Hence, if you change any trainable value, make sure to call compile() again on your model for your changes to be taken into account.
Important notes about BatchNormalization layer

Many image models contain BatchNormalization layers. That layer is a special case on every imaginable count. Here are a few things to keep in mind.
```

- `BatchNormalization` contains 2 non-trainable weights that get updated during training. These are the variables tracking the mean and variance of the inputs.

- When you set `bn_layer.trainable = False`, the `BatchNormalization` layer will

run in inference mode, and will not update its mean & variance statistics. This is not the case for other layers in general, as weight trainability & inference/training modes are two orthogonal concepts. But the two are tied in the case of the `BatchNormalization` layer.

- When you unfreeze a model that contains `BatchNormalization` layers in order to do

fine-tuning, you should keep the `BatchNormalization` layers in inference mode by passing `training=False` when calling the base model. Otherwise the updates applied to the non-trainable weights will suddenly destroy what the model has learned.

You'll see this pattern in action in the end-to-end example at the end of this guide.

## Transfer learning & fine-tuning with a custom training loop

If instead of `fit()`, you are using your own low-level training loop, the workflow stays essentially the same. You should be careful to only take into account the list `model.trainable_weights` when applying gradient updates:

```
# Create base model
base_model = keras.applications.ResNet50V2(
    weights='imagenet',
    input_shape=(150, 150, 3),
    include_top=False)

# Freeze base model
base_model.trainable = False

# Create new model on top.
inputs = keras.Input(shape=(150, 150, 3))
x = base_model(inputs, training=False)
x = keras.layers.GlobalAveragePooling2D()(x)
outputs = keras.layers.Dense(1)(x)
model = keras.Model(inputs, outputs)

loss_fn = keras.losses.BinaryCrossentropy(from_logits=True)
optimizer = keras.optimizers.Adam()

# Iterate over the batches of a dataset.
for inputs, targets in new_dataset:
    # Open a GradientTape.
    with tf.GradientTape() as tape:
        # Forward pass.
        predictions = model(inputs)
        # Compute the loss value for this batch.
        loss_value = loss_fn(targets, predictions)

        # Get gradients of loss wrt the "trainable" weights.
        gradients = tape.gradient(loss_value, model.trainable_weights)
        # Update the weights of the model.
        optimizer.apply_gradients(zip(gradients, model.trainable_weights))

Likewise for fine-tuning.
```

## An end-to-end example: fine-tuning an image classification model on a cats vs. dogs dataset

To solidify these concepts, let's walk you through a concrete end-to-end transfer learning & fine-tuning example. We will load the Xception model, pre-trained on ImageNet, and use it on the Kaggle "cats vs dogs" classification dataset.

### Getting the data

First, let's fetch the cats vs. dogs dataset using TFDS. If you have your own dataset, you'll probably want to use the utility `tf.keras.preprocessing.image_dataset_from_directory`, to generate similar labeled dataset objects from a set of images on disk filed into class-specific folders.

Transfer learning is most useful when working with very small datasets. To keep our dataset small, we will use 40% of the original training data (25,000 images) for training, 10% for validation, and 10% for testing.

```
In [12]: import tensorflow_datasets as tfds

tfds.disable_progress_bar()

train_ds, validation_ds, test_ds = tfds.load(
    "cats_vs_dogs",
    # Reserve 10% for validation and 10% for test
    splits=["train[:40%]", "train[40%:50%]", "train[50%:60%]"],
    as_supervised=True, # Include labels
    with_data=True
)

print("Number of training samples: %d" % tf.data.experimental.cardinality(train_ds))
print("Number of validation samples: %d" % tf.data.experimental.cardinality(validation_ds))
print("Number of test samples: %d" % tf.data.experimental.cardinality(test_ds))

WARNING:absl:Variant folder: C:\Users\juann\anaconda3\lib\site-packages\tensorflow_datasets\cats_vs_dogs\1.0.3 has no dataset_info.json
Downloading and preparing dataset unknown size (download: unknown size, total: unknown size) to C:\Users\juann\anaconda3\lib\site-packages\tensorflow_datasets\cats_vs_dogs\1.0.3...
-----
Cell In[12], line 5
      1 import tensorflow_datasets as tfds
      2 tfds.disable_progress_bar()
----> 3 train_ds, validation_ds, test_ds = tfds.load(
      4     "cats_vs_dogs",
      5     # Reserve 10% for validation and 10% for test
      6     splits=["train[:40%]", "train[40%:50%]", "train[50%:60%]"],
      7     as_supervised=True, # Include labels
      8     with_data=True
      9 )
     10
     11 print("Number of training samples: %d" % tf.data.experimental.cardinality(train_ds))
     12 print("Number of validation samples: %d" % tf.data.experimental.cardinality(validation_ds))
     13 print("Number of test samples: %d" % tf.data.experimental.cardinality(test_ds))

File C:\Users\juann\anaconda3\lib\site-packages\tensorflow_datasets\core\logging__init__.py:176, in _FunctionDecorator.__call__(self, function, instance, args, kwargs)
    174 metadata = self._start_call()
    175 try:
--> 176     return function(*args, **kwargs)
    177 except Exception:
    178     metadata.mark_error()

File C:\Users\juann\anaconda3\lib\site-packages\tensorflow_datasets\core\load.py:666, in load(name, split, data_dir, batch_size, shuffle_files, download, as_supervised, decoders, read_config, with_info, builder_kwargs)
    654
    655
    656
    657
    658
    659
    660
    661
    662
    663
    664
    665
    666
    667
    668
    669
    670
    671
    672
    673
    674
    675
    676
    677
    678
    679
    680
    681
    682
    683
    684
    685
    686
    687
    688
    689
    690
    691
    692
    693
    694
    695
    696
    697
    698
    699
    700
    701
    702
    703
    704
    705
    706
    707
    708
    709
    710
    711
    712
    713
    714
    715
    716
    717
    718
    719
    720
    721
    722
    723
    724
    725
    726
    727
    728
    729
    730
    731
    732
    733
    734
    735
    736
    737
    738
    739
    740
    741
    742
    743
    744
    745
    746
    747
    748
    749
    750
    751
    752
    753
    754
    755
    756
    757
    758
    759
    760
    761
    762
    763
    764
    765
    766
    767
    768
    769
    770
    771
    772
    773
    774
    775
    776
    777
    778
    779
    780
    781
    782
    783
    784
    785
    786
    787
    788
    789
    790
    791
    792
    793
    794
    795
    796
    797
    798
    799
    800
    801
    802
    803
    804
    805
    806
    807
    808
    809
    810
    811
    812
    813
    814
    815
    816
    817
    818
    819
    820
    821
    822
    823
    824
    825
    826
    827
    828
    829
    830
    831
    832
    833
    834
    835
    836
    837
    838
    839
    840
    841
    842
    843
    844
    845
    846
    847
    848
    849
    850
    851
    852
    853
    854
    855
    856
    857
    858
    859
    860
    861
    862
    863
    864
    865
    866
    867
    868
    869
    870
    871
    872
    873
    874
    875
    876
    877
    878
    879
    880
    881
    882
    883
    884
    885
    886
    887
    888
    889
    890
    891
    892
    893
    894
    895
    896
    897
    898
    899
    900
    901
    902
    903
    904
    905
    906
    907
    908
    909
    910
    911
    912
    913
    914
    915
    916
    917
    918
    919
    920
    921
    922
    923
    924
    925
    926
    927
    928
    929
    930
    931
    932
    933
    934
    935
    936
    937
    938
    939
    940
    941
    942
    943
    944
    945
    946
    947
    948
    949
    950
    951
    952
    953
    954
    955
    956
    957
    958
    959
    960
    961
    962
    963
    964
    965
    966
    967
    968
    969
    970
    971
    972
    973
    974
    975
    976
    977
    978
    979
    980
    981
    982
    983
    984
    985
    986
    987
    988
    989
    990
    991
    992
    993
    994
    995
    996
    997
    998
    999
```

**keyError: "There is no item named 'train\_images/Cat\\\\\\\\0.jpg' in the archive"**

These are the first 5 images in the training dataset -- as you can see, they're all different sizes.

```
In [ ]: import matplotlib.pyplot as plt

plt.figure(figsize=(10, 10))
for i, (image, label) in enumerate(train_ds.take(5)):
    ax = plt.subplot(2, 3, i + 1)
    plt.imshow(image)
    plt.title(int(label))
    plt.axis('off')
```

We can also see that label 1 is "dog" and label 0 is "cat".

## Standardizing the data

Our raw images have a variety of sizes. In addition, each pixel consists of 3 integer values between 0 and 255 (RGB level values). This isn't a great fit for feeding a neural network. We need to do 2 things:

- Standardize to a fixed image size. We pick 150x150.
- Normalize pixel values between -1 and 1. We'll do this using a `Normalization` layer as

part of the model itself.

In general, it's most beneficial to develop models that take raw data as input, as opposed to models that take already-preprocessed data. The reason being that, if your model expects preprocessed data, any time you export your model to use it elsewhere (on a web browser, in a mobile app) you'll need to reimplement the exact same preprocessing pipeline. This gets very tricky very quickly. So we should do as little as possible amount of preprocessing before hitting the model.

Here, we'll do image resizing in the data pipeline (because a deep neural network can only process contiguous batches of data), and we'll do the input value scaling as part of the model, when we create it.

Let's resize images to 150x150:

```
In [ ]: size = (150, 150)

train_ds = train_ds.map(lambda x, y: (tf.image.resize(x, size), y))
validation_ds = validation_ds.map(lambda x, y: (tf.image.resize(x, size), y))
test_ds = test_ds.map(lambda x, y: (tf.image.resize(x, size), y))
```

Besides, let's batch the data and use caching & prefetching to optimize loading speed.

```
In [ ]: batch_size = 32 #you can modify the batchsize according to the computational resources available

train_ds = train_ds.cache().batch(batch_size).prefetch(buffer_size=10)
validation_ds = validation_ds.cache().batch(batch_size).prefetch(buffer_size=10)
test_ds = test_ds.cache().batch(batch_size).prefetch(buffer_size=10)
```

## Using random data augmentation

When you don't have a large image dataset, it's a good practice to artificially introduce sample diversity by applying random yet realistic transformations to the training images, such as random horizontal flipping or small random rotations. This helps expose the model to different aspects of the training data while slowing down overfitting.

```
In [ ]: from tensorflow import keras
from tensorflow.keras import layers

data_augmentation = keras.Sequential(
    [layers.RandomFlip("horizontal"), layers.RandomRotation(0.85)], #you can add more augmentations, like in the example at https://www.tensorflow.org/tutorials/images/data_augmentation
)

Let's visualize what the first image of the first batch looks like after various random transformations:
```

```
In [ ]: import numpy as np

for image, label in train_ds.take(1):
    plt.figure(figsize=(10, 10))
    first_image = images[0]
    for i in range(9):
        ax = plt.subplot(3, 3, i + 1)
        augmented_image = data_augmentation(
            tf.expand_dims(first_image, 0), training=True
        )
        plt.imshow(augmented_image[0].numpy().astype("int32"))
        plt.title(int(label[i]))
        plt.axis('off')
```

## Build a model

Now let's build a model that follows the blueprint we've explained earlier.

Note that:

- We add a `Rescaling` layer to scale input values (initially in the `[0, 255]` range) to the `[-1, 1]` range.
- We add a `Dropout` layer before the classification layer, for regularization.
- We make sure to pass `training=False` when calling the base model so that

it runs in inference mode, so that batchnorm statistics don't get updated even after we unfreeze the base model for fine-tuning.

```
In [ ]: base_model = keras.applications.MobileNetV2(input_shape=(150, 150, 3))
weights='imagenet', # Load weights pre-trained on ImageNet.
input_shape=(150, 150, 3),
include_top=False,
) # Do not include the ImageNet classifier at the top.

# Freeze the base model
base_model.trainable = False

# Create new model on top
inputs = keras.Input(shape=(150, 150, 3))
x = data_augmentation(inputs) # Apply random data augmentation

# Pre-trained weights requires that input be scaled
# from (0, 255) to a range of (-1., +1.), the rescaling layer
# outputs: (inputs * scale) + offset
scale_layer = keras.layers.Rescaling(scale=1 / 127.5, offset=-1)
x = scale_layer(x)

# The base model contains batchnorm layers, we want to keep them in inference mode
# when we unfreeze the base model for fine-tuning, so we make sure that the
# base_model is running in inference mode here.
# base_model.trainable = False
x = keras.layers.GlobalAveragePooling2D()(x)
x = keras.layers.Dropout(0.5)(x) # Regularize with dropout
outputs = keras.layers.Dense(1)(x)
model = keras.Model(inputs, outputs)
model.summary()
```

## Train the top layer

```
In [ ]: model.compile(
    optimizer=keras.optimizers.Adam(),
    loss=keras.losses.BinaryCrossentropy(from_logits=True),
    metrics=[keras.metrics.BinaryAccuracy()],
)

epochs = 18 #make the number of epochs adequate depending on the computational resources available
model.fit(train_ds, epochs=epochs, validation_data=validation_ds)
```

After 10 epochs, fine-tuning gains us a nice improvement here.

## Extra

You can try to train a smaller model on the same task (let us say, the LeNet-5 model developed in lab2) to observe a gap in performance!

```
In [ ]: #Here you can put the code for training a shallow model
```

## Acknowledgement

This notebook has been modified starting from This is adapted from Deep Learning with Python and the 2016 blog post "Building powerful image classification models using very little data" (<https://blog.keras.io/building-powerful-image-classification-models-using-very-little-data.html>), successfully adapted in the notebook prepared by fchollet.