Molly Weaver

February 28, 2021

Foundations of Programming: Python

Assignment 07 – Pickling

<https://github.com/molweave532/IntroToProg-Python-Mod07>

Pickling in Python

# Introduction

For homework 07 we were asked to explain the concept of pickling. I offer up a few web sites for background information, then go through some basic coding as an example.

## Background Information

I am going to briefly introduce the concept of pickling in Python. The first thing I always do when trying to learn something new is to go online and look for videos of someone explaining the concept. I am a very visual learner. Sometimes it’s easier to learn by watching someone else do something than to read about it. You can always go back and read to get a more granular view. Unfortunately, all the videos I found on pickling seemed to cover more complex concepts that a novice programmer like myself could handle. So, here are a few web sites that do a good job of sticking to the basics –

<https://www.pythoncentral.io/how-to-pickle-unpickle-tutorial/> (external link)

<https://codewithharry.com/videos/python-tutorials-for-absolute-beginners-84> (external link)

The second website does include a video. Unfortunately, it is in Hindu, a language I do not have the good fortune to speak.

### Why Pickle?

Pickling is different than simply writing data to a file in that it transfers the information in binary. It can be used to save more complex data than a simple .txt or .csv file. Because it is written in binary, it can offer a level of security. This can also be a disadvantage. If you read data from a pickled file from an unknown source you could unwittingly download a virus on to your computer. So, unpickle with care!

#### How to Pickle Data

In order to use pickling in your code, you must first import the pickle module (**figure 1**).

Text

Description automatically generated

***Figure 1.*** Open the pickle module.

This will allow you to use all the functions associated with pickling. Next, create a simple data set that you want to pickle. Here I’m using a dictionary of my family’s dogs and their fetching scores (**figure 2**).

Text

Description automatically generated with low confidence

***Figure 2.*** Create data to be pickled.

Next, open the file where the data is to be written (**figure 3**).

Graphical user interface, text

Description automatically generated

***Figure 3.*** Opening a file in binary mode.

Note, that we are using “wb” to open the file in write binary mode, instead of “w”. Also, note that the file extension is .pkl for the pickled file. Next, write the dictionary into the binary file using the dump() function (**figure 4**).

A screenshot of a computer

Description automatically generated with low confidence

***Figure 4.*** Writing data to a binary file.

We are writing the contents of “dicScores” into the binary file “pickledScores.pkl” using dump() instead of write(). Always remember to close the file after writing the data to it.

##### How to Unpickle Data

Now, let’s read the data back out of the file (**figure 5**).

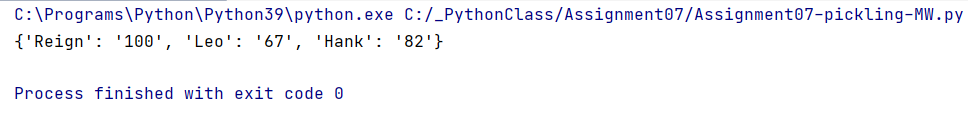
Text

Description automatically generated

***Figure 6.*** Reading data from a binary file.

To read the data out of the binary file, we first open it. We are using “rb” instead of just “r” that is used with text files to open it in read binary mode. Also, instead of using read(), we are using load() to pull the data out of the file and put it in a new dictionary called “dicScoresP”. Again, always remember to close the binary file when finished with it.

Finally, we will print out the new dictionary to see if it matches the original one (**figure 7**).



***Figure 7.*** The final output.

Looks the same to me. We have successfully pickled and unpickled data!

###### Conclusion

Pickling data is very similar to reading and writing data to a text file. The biggest difference is that you pickle in binary mode, instead of simple text. This allows you to write more complex data and gives an added measure of security. The file can’t simply be clicked open and read by the human eye. To use pickling functions you must first import the pickle module. The functions are dump() and load() instead of write() and read(), and you have to use “wb” and “rb” to open the pickled file in the correct mode, but the basic formatting is the same. Here we used a dictionary, but pickled data can be of any type. When the data is loaded back out of the pickled file, it will be of the same data type.