Project 4

Kyle McClintick
ECE 579

April 22, 2020

The following sections document the training of various models on the 32-bit dataset by printing grid-search validation results, as well as the testing of those models by printing test accuracy and displaying a confusion matrix of test predictions. Conclusions of results are presented at the end.

1 SVM

```
( 1 / 12 ) validation CE acc for h ['linear' '0.01'] :
0.1924
new best!
( 2 / 12 ) validation CE acc for h ['linear' '0.1'] :
0.1885
( 3 / 12 ) validation CE acc for h ['linear' '1.0'] :
0.1877
( 4 / 12 ) validation CE acc for h ['poly' '0.01'] : 0.1345
( 5 / 12 ) validation CE acc for h ['poly' '0.1'] : 0.1765
( 6 / 12 ) validation CE acc for h ['poly' '1.0'] : 0.1886
( 7 / 12 ) validation CE acc for h ['rbf' '0.01'] : 0.1953
new best!
( 8 / 12 ) validation CE acc for h ['rbf' '0.1'] : 0.1923
( 9 / 12 ) validation CE acc for h ['rbf' '1.0'] : 0.1918
( 10 / 12 ) validation CE acc for h ['sigmoid' '0.01'] :
0.1909
( 11 / 12 ) validation CE acc for h ['sigmoid' '0.1'] :
0.1901
```

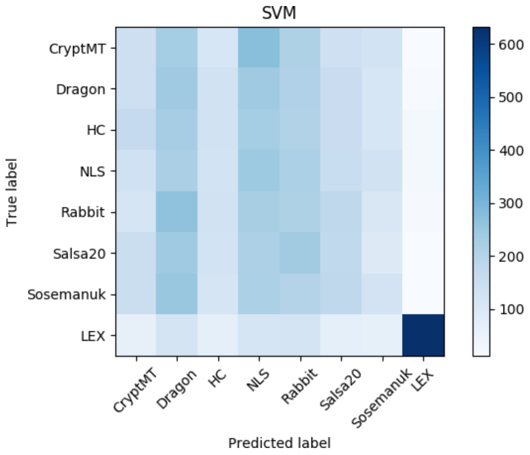

Figure 1: SVM testing confusion matrix

```
( 12 / 12 ) validation CE acc for h ['sigmoid' '1.0'] :
0.1747
Test accuracy: 0.1907
```

2 KNN

```
( 1 / 8 ) validation CE acc for h ['1' 'uniform'] : 0.187
new best!
( 2 / 8 ) validation CE acc for h ['1' 'distance'] : 0.187
( 3 / 8 ) validation CE acc for h ['5' 'uniform'] : 0.1846
( 4 / 8 ) validation CE acc for h ['5' 'distance'] : 0.1863
( 5 / 8 ) validation CE acc for h ['20' 'uniform'] : 0.1805
( 6 / 8 ) validation CE acc for h ['20' 'distance'] :
0.1823
( 7 / 8 ) validation CE acc for h ['100' 'uniform'] :
0.1883
new best!
( 8 / 8 ) validation CE acc for h ['100' 'distance'] :
0.188
Test accuracy: 0.1848
```

3 Decision Tree

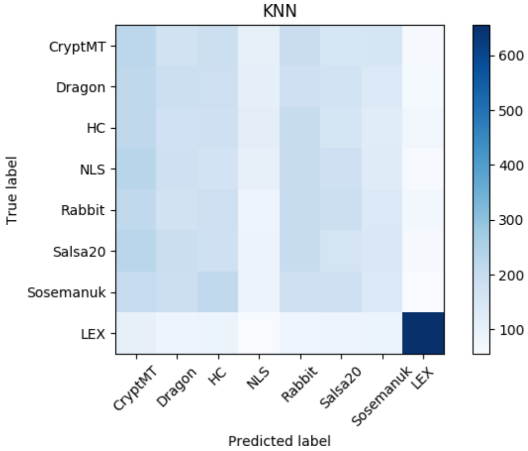

Figure 2: KNN testing confusion matrix

```
( 1 / 4 ) validation CE acc for h ['best' 'entropy'] :
0.1817
new best!
( 2 / 4 ) validation CE acc for h ['best' 'gini'] : 0.1831
new best!
( 3 / 4 ) validation CE acc for h ['random' 'entropy'] :
0.1869
new best!
( 4 / 4 ) validation CE acc for h ['random' 'gini'] :
0.184
Test accuracy: 0.1837
```

4 CNN

```
( 1 / 32 ) validation CE loss for h [ 1.  1.  8. 10.  0.] :
1.9803774406909942
new best!
( 2 / 32 ) validation CE loss for h [ 1.  2.  8. 10.  0.] :
1.9624101159572602
new best!
( 3 / 32 ) validation CE loss for h [ 5.  1.  8. 10.  0.] :
1.9801361447572707
( 4 / 32 ) validation CE loss for h [ 5.  2.  8. 10.  0.] :
```

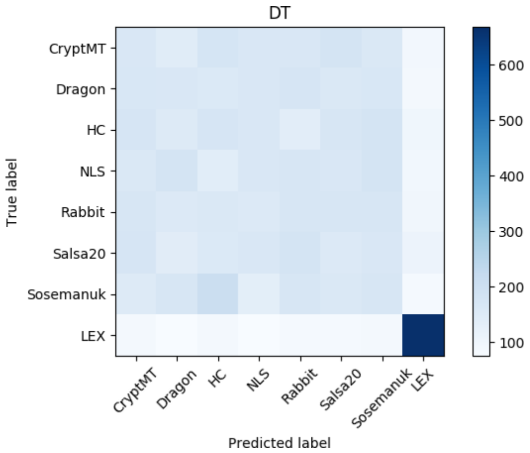

Figure 3: DT testing confusion matrix

```
1.9322150354385377
new best!
( 5 / 32 ) validation CE loss for h [ 1.  1. 64. 10.  0.] :
1.97840079498291
( 6 / 32 ) validation CE loss for h [ 1.  2. 64. 10.  0.] :
1.967854782819748
( 7 / 32 ) validation CE loss for h [ 5.  1. 64. 10.  0.] :
1.9817535619735718
( 8 / 32 ) validation CE loss for h [ 5.  2. 64. 10.  0.] :
1.9330822721719743
( 9 / 32 ) validation CE loss for h [  1.   1.   8. 100.
0.] :  1.9870078706741332
( 10 / 32 ) validation CE loss for h [  1.   2.   8. 100.
0.] :  1.969883623123169
( 11 / 32 ) validation CE loss for h [  5.   1.   8. 100.
0.] :  1.9783750224113463
( 12 / 32 ) validation CE loss for h [  5.   2.   8. 100.
0.] :  1.9340772116184235
( 13 / 32 ) validation CE loss for h [  1.   1.  64. 100.
0.] :  1.9850046968460082
( 14 / 32 ) validation CE loss for h [  1.   2.  64. 100.
0.] :  1.9642873203754425
( 15 / 32 ) validation CE loss for h [  5.   1.  64. 100.
0.] :  1.979574373960495
( 16 / 32 ) validation CE loss for h [  5.   2.  64. 100.
0.] :  1.9334622061252593
( 17 / 32 ) validation CE loss for h [ 1.   1.   8.  10.
0.5] :  1.982558416724205
( 18 / 32 ) validation CE loss for h [ 1.   2.   8.  10.
0.5] :  1.967083939433098
( 19 / 32 ) validation CE loss for h [ 5.   1.   8.  10.
0.5] :  2.123026450753212
( 20 / 32 ) validation CE loss for h [ 5.   2.   8.  10.
0.5] :  1.985194055080414
( 21 / 32 ) validation CE loss for h [ 1.   1.  64.  10.
0.5] :  1.9811646745204925
( 22 / 32 ) validation CE loss for h [ 1.   2.  64.  10.
0.5] :  1.965677388906479
( 23 / 32 ) validation CE loss for h [ 5.   1.  64.  10.
0.5] :  2.1143733478188516
( 24 / 32 ) validation CE loss for h [ 5.   2.  64.  10.
0.5] :  1.9324175395965577
( 25 / 32 ) validation CE loss for h [  1.    1.    8.
100.    0.5] :  1.98762988448143
( 26 / 32 ) validation CE loss for h [  1.    2.    8.
100.    0.5] :  1.9749135899543762
( 27 / 32 ) validation CE loss for h [  5.    1.    8.
100.    0.5] :  2.08123899102211
( 28 / 32 ) validation CE loss for h [  5.    2.    8.
100.    0.5] :  1.9652364706993104
( 29 / 32 ) validation CE loss for h [  1.    1.   64.
100.    0.5] :  1.9852925634384155
( 30 / 32 ) validation CE loss for h [  1.    2.   64.
100.    0.5] :  1.9690076756477355
( 31 / 32 ) validation CE loss for h [  5.    1.   64.
100.    0.5] :  2.295687341094017
( 32 / 32 ) validation CE loss for h [  5.    2.   64.
100.    0.5] :  1.933114459514618
 Test accuracy: 0.1872
```

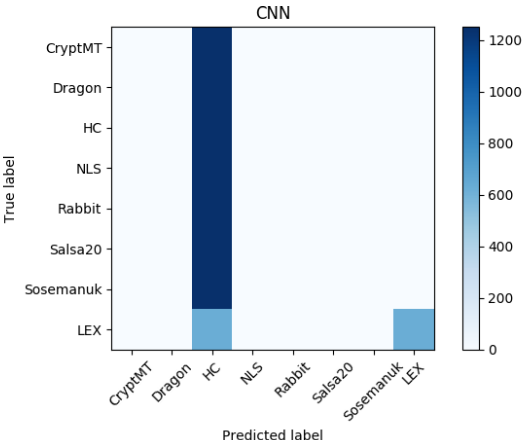

Figure 4: CNN testing confusion matrix

5 Bonus: LSTM RNN

```
( 1 / 8 ) validation CE acc for h [ 0.  2. 10.  0.] :
1.9374558271169662
new best!
( 2 / 8 ) validation CE acc for h [ 0.  8. 10.  0.] :
1.9334418396949768
new best!
( 3 / 8 ) validation CE acc for h [ 1.  2. 10.  0.] :
1.9366709034442902
( 4 / 8 ) validation CE acc for h [ 1.  8. 10.  0.] :
1.933216926932335
new best!
( 5 / 8 ) validation CE acc for h [ 0.   2.  10.   0.5] :
1.940027032852173
( 6 / 8 ) validation CE acc for h [ 0.   8.  10.   0.5] :
1.9344673713445664
( 7 / 8 ) validation CE acc for h [ 1.   2.  10.   0.5] :
1.9383841136693953
( 8 / 8 ) validation CE acc for h [ 1.   8.  10.   0.5] :
1.934400724053383
Test accuracy: 0.1878999998047948
```

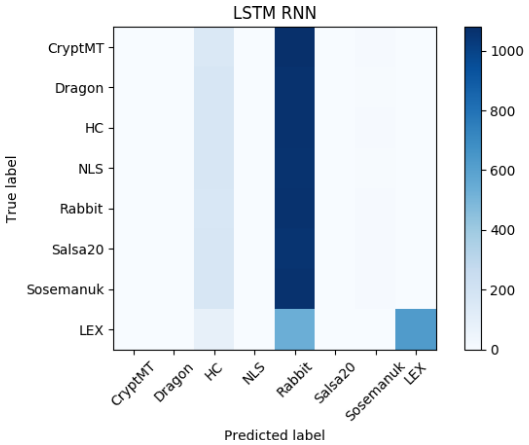

Figure 5: LSTM testing confusion matrix

Table 1: A summary of the test accuracy of the models studied on the 32-bit sequence dataset

Model	SVM	KNN	DT	CNN	LSTM
Test Acc	19.07	18.48	18.37	18.72	18.79

6 Conclusions

While some models performed slightly better than others (Table 1), none seemed to excel at inferring the generator used by observing the sequences of digits produced. Given that the data set has eight classes, random predictions would result in a 12.5 % test accuracy. The difficulty in breaking 20 % test accuracy with any model seems to be due to all predictions being guesses besides the ~ 650 LEX predictions. These correct predictions account for a bonus 6.5% accuracy since the test set has $n = 10000$ samples, resulting in $\sim 19\%$ test accuracy for most models.

Consequentially, it is determined that LEX is an insecure pseudo random generation scheme, as it can be inferred by observations through the use of many common classifier models, while the other generators studied are secure from inference.

Repeating the experiment for the 64-bit dataset, performance seemed to increase, as validation accuracy was typically ~ 25 % (only LEX improved). This is interesting as a larger state space should be more challenging to classify, but the larger state space seems to expose patterns more highly correlated to outcomes.

The experiment was unable to be repeated for the 128-bit dataset as the dataset has some missing columns.