

Section III: Results

Learning on a Single Layer

Models were trained on datasets of size 100k, unless otherwise noted. The results for restricted datasets and fuzzy datasets are also presented in the tables below; no significant difference was made. Bitwise accuracy is the average proportion of correct bits outputted. Accuracies and loss are from the final epoch. The round parameter represents which round of SHA-1 is being reversed.

Feed-Forward Neural Networks

Table 1: Accuracies and loss for multilayer feed-forward neural networks with varying hyperparameters and training datasets

| Layer Amount | Learning Rate | Round | Epochs | Batch Size | Loss | Train Accuracy | Test Accuracy | Dataset | Bit Accuracy |
|--------------|---------------|-------|--------|------------|----------|----------------|---------------|-------------------|--------------|
| 3 | 0.001 | 2 | 11 | 32 | 377.5233 | 0 | 0 | | 0.49 |
| 3 | 0.001 | 2 | 11 | 64 | 377.6703 | 0 | 0 | | 0.49 |
| 7 | 0.01 | 2 | 11 | 64 | 377.4963 | 0 | 0 | | 0.49 |
| 3 | 0.001 | 2 | 11 | 64 | 377.5508 | 0 | 0 | | 0.49 |
| 3 | 0.001 | 16 | 11 | 64 | 405.3415 | 0 | 0 | | 0.49 |
| 3 | 0.01 | 16 | 11 | 64 | 405.2192 | 0 | 0 | | 0.49 |
| 3 | 0.01 | 2 | 11 | 64 | 379.9132 | 0 | 0 | | 0.49 |
| 3 | 0.01 | 3 | 11 | 64 | 428.5194 | 0 | 0 | | 0.49 |
| 3 | 0.01 | 3 | 50 | 64 | 428.6604 | 0 | 0 | | 0.49 |
| 3 | 0.01 | 3 | 11 | 64 | 438.9447 | 0 | 0 | restricted input | 0.46 |
| 3 | 0.01 | 3 | 11 | 64 | 399.1621 | 0 | 0 | 1 million dataset | 0.51 |
| 3 | 0.01 | 3 | 11 | 64 | 468.2508 | 0 | 0 | fuzzy data | 0.48 |

As seen in Table 1, simple feed-forward neural networks with no key-space restrictions generally achieved an accuracy of 0, with very high loss that did not decrease over epochs. Feed-forward neural networks on the same dataset with a key-space restricted to alphanumeric ASCII characters also achieved an accuracy of 0.

Recurrent Neural Networks

Table 2: Accuracies and loss for recurrent neural networks with varying hyperparameters and training datasets

| Layer Amount | Learning Rate | Round | Epochs | Batch Size | Loss | Train Accuracy | Test Accuracy | Dataset | Bit Accuracy |
|--------------|---------------|-------|--------|------------|----------|----------------|---------------|------------------|--------------|
| 3 | 0.01 | 3 | 11 | 64 | 428.6908 | 0 | 0 | | 0.49 |
| 3 | 0.01 | 3 | 11 | 64 | 439.0123 | 0 | 0 | restricted input | 0.46 |
| 3 | 0.01 | 3 | 11 | 64 | 399.1277 | 0 | 0 | 1 million | 0.51 |
| 3 | 0.01 | 3 | 11 | 64 | 468.1121 | 0 | 0 | fuzzy data | 0.48 |

As shown in Table 2, recurrent neural networks, regardless of keyspace restrictions, achieved an accuracy of 0. Results were incredibly similar to feed-forward networks, including the decrease in bitwise accuracy with keyspace restrictions. Loss similarly did not decrease at all over epochs.

Chained Models

Due to the dismal accuracies of the single-layer models, they were unable to be chained.