Stability of Internal States in Recurrent Neural Networks Trained on Regular Languages

Christian Oliva and Luis F. Lago-Fernández

Escuela Politécnica Superior, Universidad Autónoma de Madrid
28049 Madrid, Spain
christian.oliva@estudiante.uam.es
luis.lago@uam.es

June 22, 2020

Abstract

We provide an empirical study of the stability of recurrent neural networks trained to recognize regular languages. When a small amount of noise is introduced into the activation function, the neurons in the recurrent layer tend to saturate in order to compensate the variability. In this saturated regime, analysis of the network activation shows a set of clusters that resemble discrete states in a finite state machine. We show that transitions between these states in response to input symbols are deterministic and stable. The networks display a stable behavior for arbitrarily long strings, and when random perturbations are applied to any of the states, they are able to recover and their evolution converges to the original clusters. This observation reinforces the interpretation of the networks as finite automata, with neurons or groups of neurons coding specific and meaningful input patterns.

1 Introduction

The relationship between Recurrent Neural Networks (RNNs) and formal languages has been extensively studied since the early 90s [7, 19]. It is well known that RNNs are able to learn different kinds of regular and context independent languages [2, 6, 15], and it has been demonstrated that they are equivalent to Turing machines [16]. Aiming at improving interpretability, many works in the literature have explored different methods to extract a Deterministic Finite Automaton (DFA), or a set of rules, from a RNN trained with positive and negative examples of a regular language [2, 4, 11, 18]. However this approach has sometimes been criticized [13], since the process of mapping the network activation to a discrete set of states usually depends on an artificial quantization of a continuous space. Hence, in spite of the computational power of RNNs, it is still not clear whereas a RNN trained to recognize a formal language can be reduced to the corresponding abstract machine.

A more recent work [14] has shown that the introduction of noise in the activation function of a RNN, together with proper regularization, forces the neurons to work in an almost binary regime. In that situation the activation of the recurrent units forms clusters that may be interpreted as states in a finite state machine [14] without the need of an explicit quantization. Although the extracted automata seem to be valid, no in-depth analysis of the stability of the states was performed.

In this article we build on their work adding the following contributions. First, we include a theoretical analysis of the effect of the noise on the discretization of the network activity. Second, we show that the networks are able to generalize to sequences that are several orders of magnitude longer than those used for training without any loss of accuracy. This is in contrast with the results obtained for traditional RNNs or LSTMs, for which a decrease of the accuracy is always observed as the string length increases. Finally, we analyze stability by introducing small perturbations that take the networks out of the activity clusters. We observe that the networks are able to assimilate these perturbations and move back to the original states recovering their initial behavior. Our results on several simple regular languages show that noise introduces stability in the networks, not only improving generalization but also contributing to the formation of stable activity clusters that are robust against small perturbations. These clusters can be mapped to discrete states in a DFA, showing that the networks learn to solve the problems by implementing abstract machines that are equivalent to the languages used for training.

2 Methodology

2.1 Network description

Following the work of [13], here we use a simple Elman RNN [5] with one single recurrent layer, tanh activation function and a noise term introduced into the preactivation:

\[ h_t = \tanh(W_{xh} x_t + W_{hh} h_{t-1} + h_{t-1} \circ X_{\nu} + b_h) \]  (1)
where $W_{xh}$ is the weight matrix connecting the input layer to the recurrent layer, $W_{hh}$ is the weight matrix in the recurrent connection, and $b_h$ is a bias vector. The noise term $h_{t-1} \odot X_\nu$ is an element-wise product between the activation in the previous time step $h_{t-1}$ and the vector $X_\nu$, whose components are randomly drawn from a normal distribution $N(0, \nu)$. The output $h_t$ of the recurrent layer is fed into an output layer with softmax activation function:

$$y_t = \sigma(W_{hy}h_t + b_y)$$

(2)

where $W_{hy}$ is the weight matrix and $b_y$ is the bias vector.

### 2.2 The effect of noise on the network activation

The introduction of noise during neural network training has been frequently used as a regularizer [1, 12]. It has also been reported that it may help the neurons escape from saturation, guaranteeing a better learning even with hard sigmoid or hard tanh activation functions [8]. Here we consider the possibility of using noise also to force the neurons into the saturation regime. As we show in figure 1 (left plot), if a neuron with tanh activation function needs to provide a stable response when noise is introduced into its pre-activation $z$, it needs to move towards the saturation region, where the noise is counterbalanced by the almost null slope of $\tanh(z)$.

The noisiest region is of course that with the highest slope, so the neuron will try by all means to avoid staying close to $z = 0$. If the networks are trained using regularization, however, there is a second element to take into account. In such a situation, the noise and the regularization have opposite effects: while the regularization tends to inactivate the neurons, pushing them towards zero activation, the noise pushes the neurons towards the saturation region. In order to avoid this tug of war, the noise enters equation 1 multiplied by the neuron’s activity in the previous time step. This way a neuron that has been inactivated by the regularization is not affected by the noise.

In the right side of figure 1 we show two typical histograms of a neuron’s activation. The first case (top) corresponds to a neuron in a network trained without noise. The second one (bottom) is from a network trained with noise $\nu = 1.0$. It is clear from these histograms that the noise encourages neuron saturation: while the activation of the noiseless neuron spans the whole range $[-1, 1]$, the noisy neuron sits only at the extreme values. Neural networks trained with pre-activation noise will always display this behavior, with their neurons operating in an almost binary mode.

### 2.3 Network training

In all our experiments we use networks with 20 units in the recurrent layer. The networks are trained to minimize a cross-entropy loss using a standard gradient descent optimizer with the Keras library [3]. L1 regularization with parameter $r = 0.0004$ is applied to all the network weights, but not to the biases. The networks are trained for 500 epochs with a learning rate $l = 2.5$ and clipping the gradients to $c = 0.002$. The gradients are backpropagated through time for $s = 25$ time steps.

The noise parameter is set to $\nu = 1.0$ for most of the experiments. However for some tests we have observed that the use of a gradually increasing noise parameter, that starts being 0 and linearly increases during training, helps to obtain better results.
2.4 Data
We consider two different kinds of problems that can be well modeled with finite automata: the recognition of regular languages and the addition of two integer numbers in numerical bases 2 and 4.

2.4.1 Regular languages.
First, we consider several simple regular languages on the alphabet \( \Gamma = \{a, b\} \) (see description in table 1). They comprise the set of strings with an even number of appearances of the \( a \) symbol, the set of strings starting with a \( b \) symbol and ending with an \( a \) symbol, and the seven Tomita Grammars [17]. The datasets for training and evaluating the networks are generated as described in [14], including the $ symbol used as a separator. The input data are random strings built with the symbols \( a, b \) and $. For each input symbol the networks must predict if the partial substring starting at the last $ symbol belongs or not to the language under consideration. Table 2 shows an example of input-output strings for the Tomita 3 problem. A network’s accuracy is evaluated by measuring the number of correct predictions on a validation set that is not used during the training phase.

2.4.2 Addition in numerical bases 2 and 4.
The second problem consists of predicting the result of a sum of two integer numbers that are presented to the network digit by digit. We consider additions in the numerical bases 2 and 4. At each time step the network is expected to return a single digit in the corresponding base which is the result (without carry) of the addition of the two inputs plus the possible carry generated in the previous time step. One example of input and output for base 4 is shown in table 2, where the strings must be read from left to right, with the most significant digit at the rightmost position. Note that we also include the separator symbol $ in the input strings, which represents the end of a particular sum. Whenever it appears, the $ symbol is present in both input strings at the same time. The expected output for a $ input is simply the last carry. As before, the input strings are randomly generated, and the networks are evaluated by measuring the number of correct predictions on a validation set.

2.5 Analysis
For all the above problems, we train the networks until they obtain a 100% accuracy on both the training and validation datasets, which usually occurs in no more than 500 training epochs. Once they are trained, we analyze the networks in terms of interpretability by inspecting the weight values and the activation space of the recurrent layer neurons. When we observe that the network activation forms well defined clusters, we analyze the stability of these clusters by: (1) measuring the network response to very long input strings that are several orders of magnitude longer than the strings used for training; and (2) introducing small perturbations into the activation clusters and observing if the network is able to recover its normal behavior.

3 Results
In this section we describe mainly qualitative results that illustrate the behavior of RNNs trained with noise in the activation function. The networks are able to reach a 100% accuracy in both the training and validation datasets for all the problems described above. Additionally, the activation in the recurrent layer is highly

| Problem | Regular language |
|---------|------------------|
| parity  | Strings with an even number of \( a \)'s. |
| bxa     | Strings starting with \( b \) and ending with \( a \). |
| tomita1 | Strings with only \( a \)'s. |
| tomita2 | Strings with only sequences of \( ab \)'s. |
| tomita3 | Strings with no odd number of consecutive \( b \)'s after an odd number of consecutive \( a \)'s. |
| tomita4 | Strings with fewer than 3 consecutive \( b \)'s. |
| tomita5 | Strings with even length with an even number of \( a \)'s. |
| tomita6 | Strings where the difference between the number of \( a \)'s and \( b \)'s is a multiple of 3. |
| tomita7 | \( b^*a^*b^*a^* \) |

Table 2: Example of input and output strings for the Tomita 3 and the base 4 addition problems.

| Tomita 3                  | Input | Output |
|---------------------------|-------|--------|
| $baa$abaababbaba$abaabbbb$ab$aba$abb$babbaababbbb | $111111000000000000001111111111111111111011101111111101$ |

| Base 4 addition           | Input 1 | Input 2 | Output |
|---------------------------|---------|---------|--------|
| $23111120100033320001110100033312006236320021600321521223$ | $3123111110062120305031122822113023330810021362322830123$ | $0110303312000111110102320211320011030230122210112300$ |
3.1 Activation in the recurrent layer

Figure 2 shows the activation in the recurrent layer for a network trained on the Tomita 3 problem (top plots) and a network trained on the base 4 addition problem (bottom plots). On the left hand side we show the output of the 20 recurrent neurons in response to the first 60 symbols in the test set. Only a small fraction of these neurons are active, namely neurons \{0, 2, 8, 15\} for the Tomita 3 problem and neurons \{1, 5, 6, 7, 11, 14\} for the base 4 addition, displaying a completely binary output. The remaining neurons are always silent with an almost zero activation. As an additional way to visualize the recurrent layer activity, we have performed Principal Component Analysis of the activation vectors for the complete validation sets, which contain 100000 input symbols for the Tomita 3 problem and 50000 symbols for the addition. A scatter plot of the first two principal components is displayed on the right hand side of figure 2, showing that the recurrent layer output self-organizes into a set of clusters, each corresponding to one of the unique binary activation vectors displayed as columns in the left side plots. There are 8 clusters for the Tomita 3 problem and 14 clusters for the base 4 addition problem.

3.2 Network weights

Weight visualization is also a good way of understanding the behavior of a recurrent neural network. In figure 3 we plot in color scale the weight matrices \(W_{xh}\) (input to recurrent layer, top) and \(W_{hh}\) (recurrent layer to itself, bottom), for the Tomita 3 problem (left) and the base 4 addition problem (right). Only the weights involving the neurons that are active according to our previous analysis are significantly different from 0. A very interesting observation regarding the addition problem is that only one recurrent neuron (neuron 14) projects back onto the recurrent layer. This means that neuron 14 is presumably coding the carry, which is the only information that must be kept from one time step to the next one in order to solve the addition problem.

3.3 Network interpretation as a finite state machine

Analyzing the transitions from each of the activation clusters in response to each of the input symbols, we observe that these transitions are deterministic. That is, if we initialize the recurrent layer to any of the points of one of the clusters shown in figure 2 and we observe the recurrent layer output after the network has processed one input symbol, we see that all the outputs belong again to the same cluster. Hence, in response to a given input sequence the network jumps from cluster to cluster just as a deterministic finite automata. Figure 4 shows an example of the transitions departing from one of the activation clusters in the Tomita 3 problem with the three input symbols \(a, b\) and \(\$\). Note that, as before, a small Gaussian noise has been added to all the points in order to improve the visualization. The real clusters are more compact than shown.
Automata extraction. The activation clusters in the recurrent layer may be interpreted as the states of a deterministic finite automaton. Then it is not difficult to use transition plots like the one shown in figure 4 to obtain the transition table and, from this table, extract the corresponding DFA. The left panel in figure 5 shows the table obtained for the network trained with the Tomita 3 data, displaying the transitions from the 8 clusters/states with each of the 3 input symbols. It is not difficult to see that some of these states are equivalent. If we apply a DFA minimization algorithm [10] we obtain an automaton with just 5 states whose transition table is shown in the middle panel of figure 5. The right panel of this figure also shows the transitions graph of the minimum DFA.

The extracted automaton is in fact the minimum DFA for the Tomita 3 language, and this observation is repeated for all the problems that we considered. To summarize, in all cases we were able to reduce the trained networks to a DFA that recognizes the regular language that was used as input. The DFA states appear automatically when the networks are trained with noise in the activation of the recurrent neurons, and are not a result of artificial quantization of the hidden layer activation space.

4 Stability

Although the results presented in section 3 are very interesting from the point of view of interpretability, the efforts made for reducing a recurrent neural network to a set of rules have been frequently criticized [13]. One major problem here is the stability of the extracted states. If the states are not stable, a small deviation of the network activation with respect to the expected state may cause divergence in the long term, with unexpected behavior for very long input strings or inputs that differ substantially from the training samples. In this section we perform a study of the stability of the trained networks, by analyzing their response to very long inputs and studying their behavior when small perturbations are introduced.

4.1 Response to very long strings

For this experiment we use additional test data sets with very long input strings ($10^6$ characters) where the $\$\$ symbol appears only once, in the first position. Note that the typical training and test strings are in no case longer than 100 characters, this means that we are testing the networks with strings that are 4 orders of magnitude longer than those used for training. For each problem, we train 20 different networks, which in all cases get 100% accuracy on the standard validation sets. Then we test these networks on 100 different long strings, and analyze their average accuracy for each input symbol. Figure 6 shows a plot of the network accuracy versus the position of the symbol in the input string for the Tomita 3 and the BxA problems. The latter problem has been included in this section because it requires that the network remembers the first input symbol for all later time steps, and so it is more challenging than the other problems. To put these results in a proper context, the solution obtained with a standard LSTM network [9] is also included.
Figure 4: Example of deterministic transitions departing from an activation cluster in the network trained with the Tomita 3 data, in response to the input symbols a (left), b (middle) and $ (right). Orange points represent the initial states, and they all belong to the same cluster. Red points are the destination states, which for a given input symbol also belong to the same cluster.

Figure 5: Left. Transition table. States marked with an asterisk are acceptance states. Middle. Transition table after minimization. States marked with an asterisk are final states. The state marked with an arrow is the initial state. Right. Minimum DFA.

The most remarkable observation is that the noisy RNN networks are able to maintain the 100% accuracy regardless of the string length. In contrast, the LSTM starts failing for string lengths around $3 \cdot 10^5$ for the Tomita 3 problem, and much earlier for the BxA problem. This result suggests that the activation clusters observed in the recurrent layer are in fact stable and that the DFA interpretation may be valid.

4.2 State perturbation

After the analysis presented in the previous section, it seems that the activation clusters observed in the recurrent layer are indeed stable. In this section we test this hypothesis analyzing the network behavior when small perturbations are introduced into the clusters. With this purpose, we initialize the networks in one of the observed clusters, introduce some Gaussian noise and measure the activation in the recurrent layer as the input symbols are presented. Figure 7 shows one example for the Tomita 3 problem. Each of the plots in the first 4 rows shows the output of one of the 4 neurons that are active in the recurrent layer in 1000 different tests. The red lines represent the expected activation while the blue dots are the actual values. Each column represents one different time step, with the first one being the initial situation and the others showing the activation after presentation of the input symbols $, a$ and $b$. The figure shows that, in spite of the noise introduced in the initial states, the network is able to converge to the expected solution in just a few time steps. Note that the network can recover from the perturbation even though some neurons are forced to be initially out of the valid range $[-1, 1]$.

In order to quantify this observation, we finally show in figure 8 the average dispersion of the activation vectors with respect to the cluster centers for 5 time steps after initialization and different perturbation levels. All possible initial clusters and all input strings of length 5 have been considered. Although the initial dispersion is quite high, in just a few iterations the dispersion reduces to almost zero, indicating the convergence of the activation vectors to the cluster centers and reinforcing the idea of stability.
Figure 6: Accuracy versus string length for the noisy RNN ($\nu = 1.0$) and a standard LSTM network on the Tomita 3 problem (left) and the BxA problem (right). Note the logarithmic scale in the horizontal axis.

5 Conclusions

In this article we have explored the use of noise in a recurrent neural network to force the neurons into the saturation region of their activation function, where their response is more binary and interpretable. When these noisy RNNs are trained with regular languages, the activation in the recurrent layer becomes a discrete set of clusters or states and, when an input sequence is presented to the network, its time evolution is reduced to a transition between states in response to each input symbol. This behavior resembles the operation of a finite state machine.

The stability of the activation clusters has been tested in two different ways. First, we have shown that the networks are able to generalize to sequences several orders of magnitude longer than those used for training with no apparent accuracy reduction. Second, we have studied the resilience of the networks when disturbing the activation clusters with small random perturbations, and we have shown that they are always able to assimilate these perturbations and recover the initial behavior.

In essence, networks trained with noise in the activation function self-organize into a set of well defined, discrete and stable activity clusters which are robust against small perturbations. They obtain a perfect generalization and admit a direct interpretation as deterministic finite automata.

References

[1] Bishop, C.M.: Training with noise is equivalent to tikhonov regularization. Neural Computation 7(1), 108–116 (1995). https://doi.org/10.1162/neco.1995.7.1.108, https://doi.org/10.1162/neco.1995.7.1.108

[2] Casey, M.: The dynamics of discrete-time computation, with application to recurrent neural networks and finite state machine extraction. Neural Computation 8(6), 1135–1178 (Aug 1996). https://doi.org/10.1162/neco.1996.8.6.1135

[3] Chollet, F., et al.: Keras. https://keras.io (2015)

[4] Cohen, M., Caciuaru, A., Rejwan, I., Berant, J.: Inducing regular grammars using recurrent neural networks. CoRR abs/1710.10453 (2017), http://arxiv.org/abs/1710.10453

[5] Elman, J.L.: Finding structure in time. Cognitive Science 14(2), 179–211 (1990). https://doi.org/10.1207/s15516709cog1402_1

[6] Gers, F.A., Schmidhuber, J.: Lstm recurrent networks learn simple context-free and context-sensitive languages. Trans. Neur. Netw. 12(6), 1333–1340 (Nov 2001). https://doi.org/10.1109/72.963769, https://doi.org/10.1109/72.963769

[7] Giles, C.L., Miller, C.B., Chen, D., Sun, G., Chen, H., Lee, Y.: Extracting and learning an unknown grammar with recurrent neural networks. In: Advances in Neural Information Processing Systems 4, [NIPS Conference, Denver, Colorado, USA, December 2-5, 1991]. pp. 317–324 (1991)

[8] Gülçehre, Ç., Moczulski, M., Denil, M., Bengio, Y.: Noisy activation functions. CoRR abs/1603.00391 (2016), http://arxiv.org/abs/1603.00391

[9] Hochreiter, S., Schmidhuber, J.: Long short-term memory. Neural Comput. 9(8), 17351780 (Nov 1997). https://doi.org/10.1162/neco.1997.9.8.1735, https://doi.org/10.1162/neco.1997.9.8.1735

[10] Hopcroft, J.E., Motwani, R., Ullman, J.D.: Introduction to Automata Theory, Languages, and Computation (3rd Edition). Addison-Wesley Longman Publishing Co., Inc., USA (2006)

[11] Jacobsson, H.: Rule extraction from recurrent neural networks: A taxonomy and review. Neural Comput. 17(6), 12231263 (Jun 2005). https://doi.org/10.1162/0899766053630350, https://doi.org/10.1162/0899766053630350
Figure 7: Activation in the recurrent layer of a network trained with the Tomita 3 data. The first 4 rows display the output of each of the 4 active neurons, in the initial state and after processing the input symbols $\xi$, $\alpha$ and $\beta$, for 1000 random tests. For each test, the recurrent neurons are first placed in a specific state (red lines in the first column) and then perturbed with random noise. Red lines in the plots represent the expected outputs, blue dots are the actual activations. The last row displays the recurrent layer activation (orange) superimposed to the activation clusters (black).

[12] Jim, K.C., Giles, C., Horne, W.: An analysis of noise in recurrent neural networks: Convergence and generalization. Neural Networks, IEEE Transactions on 7, 1424 – 1438 (12 1996). https://doi.org/10.1109/72.548170

[13] Kolen, J.: Fool’s gold: Extracting finite state machines from recurrent network dynamics. pp. 501–508 (01 1993)

[14] Oliva, C., Lago-Fernández, L.F.: On the interpretation of recurrent neural networks as finite state machines. In: Artificial Neural Networks and Machine Learning - ICANN 2019: Theoretical Neural Computation - 28th International Conference on Artificial Neural Networks, Munich, Germany, September 17-19, 2019, Proceedings, Part I. pp. 312–323 (2019). https://doi.org/10.1007/978-3-030-30487-4_25

[15] Omlin, C.W., Giles, C.L.: Extraction of rules from discrete-time recurrent neural networks. Neural Networks 9(1), 41–52 (1996). https://doi.org/10.1016/0893-6080(95)00086-0, https://doi.org/10.1016/0893-6080(95)00086-0

[16] Siegelmann, H.T., Sontag, E.D.: On the computational power of neural nets. Journal of Computer and System Sciences 50(1), 132 – 150 (1995). https://doi.org/https://doi.org/10.1006/jcss.1995.1013, http://www.sciencedirect.com/science/article/pii/S0022000085710136

[17] Tomita, M.: Dynamic construction of finite automata from examples using hill-climbing. In: Proceedings of the Fourth Annual Conference of the Cognitive Science Society. pp. 105–108. Ann Arbor, Michigan (1982)

[18] Wang, Q., Zhang, K., II, A.G.O., Xing, X., Liu, X., Giles, C.L.: An empirical evaluation of recurrent neural network rule extraction. CoRR abs/1709.10380 (2017), http://arxiv.org/abs/1709.10380

[19] Zeng, Z., Goodman, R.M., Smyth, P.: Learning finite state machines with self-clustering recurrent networks. Neural Computation 5(6), 976–990 (1993). https://doi.org/10.1162/neco.1993.5.6.976, https://doi.org/10.1162/neco.1993.5.6.976
Figure 8: Average dispersion of the recurrent layer activation vectors with respect to the expected cluster centers versus time, for networks trained with the Tomita 3 data (left) and the base 4 addition data (right). Three different perturbation levels (0.05, 0.1 and 0.2) are considered.

A State transitions

In this appendix we include additional figures showing the transitions starting from all the clusters/states in the Tomita 3 problem and the base 4 addition problem.

Figure 9: State transitions for the network trained with the Tomita 3 data. The orange dots represent the starting points, the white dots represent the destinations. Each group of three plots represents the transitions from a given cluster/state with each of the input symbols (8, a, b).
Figure 10: State transitions for the network trained with the base 4 addition data. The orange dots represent the starting points, the white dots represent the destinations. Each row represents the transitions from one of the first 7 clusters/states. Each column represents the transitions with an input symbol. Only 5 different symbols are shown.
Figure 11: State transitions for the network trained with the base 4 addition data. The orange dots represent the starting points, the white dots represent the destinations. Each row represents the transitions from one of the first 7 clusters/states. Each column represents the transitions with an input symbol. Only 5 different symbols are shown.