Can SGD Learn Recurrent Neural Networks with Provable Generalization?*

Zeyuan Allen-Zhu
Microsoft Research AI
zeyuan@csail.mit.edu

Yuanzhi Li
Carnegie Mellon University
yuanzhil@andrew.cmu.edu

Abstract

Recurrent Neural Networks (RNNs) are among the most popular models in sequential data analysis. Yet, in the foundational PAC learning language, what concept class can it learn? Moreover, how can the same recurrent unit simultaneously learn functions from different input tokens to different output tokens, without affecting each other? Existing generalization bounds for RNN scale exponentially with the input length, significantly limiting their practical implications.

In this paper, we show using the vanilla stochastic gradient descent (SGD), RNN can actually learn some notable concept class efficiently, meaning that both time and sample complexity scale polynomially in the input length (or almost polynomially, depending on the concept). This concept class at least includes functions where each output token is generated from inputs of earlier tokens using a smooth two-layer neural network.

1 Introduction

Recurrent neural networks (RNNs) is one of the most popular models in sequential data analysis [25]. When processing an input sequence, RNNs repeatedly and sequentially apply the same operation to each input token. The recurrent structure of RNNs allows it to capture the dependencies among different tokens inside each sequence, which is empirically shown to be effective in many applications such as natural language processing [28], speech recognition [12] and so on.

The recurrent structure in RNNs shows great power in practice, however, it also imposes great challenge in theory. Until now, RNNs remains to be one of the least theoretical understood models in deep learning. Many fundamental open questions are still largely unsolved in RNNs, including

1. (Optimization). When can RNNs be trained efficiently?
2. (Generalization). When do the results learned by RNNs generalize to test data?

Question 1 is technically challenging due to the notorious question of vanishing/exploding gradients, and the non-convexity of the training objective induced by non-linear activation functions.

Question 2 requires even deeper understanding of RNNs. For example, in natural language processing, “Juventus beats Bacerlona” and “Bacerlona beats Juventus” have completely different meanings. How can the same operation in RNN encode a different rule for “Juventus” at token 1 vs. “Juventus” at token 3, instead of merely memorizing each training example?

There have been some recent progress towards obtaining more principled understandings of these questions. On the optimization side, Hardt, Ma, and Recht [13] show that over-parameterization can help in the training process of a linear dynamic system, which is a special case of RNNs with linear activation functions. Allen-Zhu, Li, and Song [2] show that over-parameterization also helps in training RNNs with ReLU activations. This latter result gives no generalization guarantee.


On the generalization side, our understanding to RNN is even more limited. The VC-dimension bounds \cite{12} and \cite{13} polynomially depend on the size of the network, and either only apply to linear (or threshold) networks or to networks with one dimension input. However, a bound scaling with the total number of parameters usually cannot be applied to modern neural networks, which are heavily over-parameterized. Others \cite{9, 31} (or the earlier work \cite{14}) establish sample complexity bounds that exponentially grow in the input length. In particular, they depend on the operator norm of the recurrent unit, that we denote by $\beta$. If $\beta > 1$, their bounds scale exponentially with input length. Since most applications do not regularize $\beta$ and allow $\beta > 1$ for a richer expressibility\footnote{For instance, if $W \in \mathbb{R}^{m \times m}$ is the recurrent weight matrix, and is followed with an ReLU activation $\sigma$. Under standard random initialization $\mathcal{N}(0, \frac{2}{m})$, the combined operator $\sigma(Wx) : \mathbb{R}^m \rightarrow \mathbb{R}$^m has operator norm $\sqrt{2}$ with high probability. If instead one uses $\mathcal{N}(0, \frac{\sqrt{2}}{m})$, then $\beta$ becomes 1 but gradients will vanish exponentially fast in $L$.} their bounds are still insufficient.

Indeed, bridging the gap between optimization (question 1) and generalization (question 2) can be quite challenging in neural networks. The case of RNN is particularly so due to the (potentially) exponential blowup in input length.

- **Generalization $\rightarrow$ Optimization.** One could imagine adding a strong regularizer to ensure $\beta \leq 1$ for generalization purpose; however, it is unclear how an optimization algorithm such as stochastic gradient descent (SGD) finds a network that both minimizes training loss and maintains $\beta \leq 1$. One could also use such a very small network so the number of parameters is limited; however, it is not clear how SGD finds a small network with small training loss.

- **Optimization $\rightarrow$ Generalization.** One could try to train RNNs without any regularization; however, it is then quite possible that the number of parameters need to be large and $\beta > 1$ after the training. This is so both in practice (since “memory implies larger spectral radius” \cite{24}) and in theory \cite{2}. All known generalization bounds fail to apply in this regime.

In this paper, we give arguably the first theoretical analysis of RNNs that captures optimization and generalization simultaneously. Given any set of input sequences, as long as the outputs are (approximately) realizable by some smooth function in a certain concept class, then after training a vanilla RNN with ReLU activations, SGD provably finds a solution that has both small training and generalization error. Our result allows $\beta$ to be larger than 1 by a constant, but is still efficient: meaning that the iteration complexity of the SGD, the sample complexity, and the time complexity scale only polynomially (or almost polynomially) with the length of the input.

## 2 Notations

We denote by $||\cdot||_2$ (or sometimes $||\cdot||$) the Euclidean norm of vectors, and by $||\cdot||_2$ the spectral norm of matrices. We denote by $||\cdot||_\infty$, the infinite norm of vectors, $||\cdot||_0$ the sparsity of vectors or diagonal matrices, and $||\cdot||_F$ the Frobenius norm of matrices. Given matrix $W$, we denote by $W_k$ or $w_k$ the $k$-th row vector of $W$. We denote the row $\ell_p$ norm for $W \in \mathbb{R}^{m \times d}$ as $||W||_{2,p} := \left( \sum_{i \in [m]} ||w_i||_2^p \right)^{1/p}$.

By definition, $||W||_{2,2} = ||W||_F$. We use $\mathcal{N}(\mu, \sigma)$ to denote Gaussian distribution with mean $\mu$ and variance $\sigma$; or $\mathcal{N}(\mu, \Sigma)$ to denote Gaussian vector with mean $\mu$ and covariance $\Sigma$. We use $x = y \pm z$ to denote that $x \in [y - z, y + z]$. We use $I_{\text{event}}$ to denote the indicator function of whether event is true. We denote by $e_k$ the $k$-th standard basis vector. We use $\sigma(\cdot)$ to denote the ReLU function $\sigma(x) = \max\{x, 0\} = I_{x \geq 0} \cdot x$. Given univariate function $f : \mathbb{R} \rightarrow \mathbb{R}$, we also use $f$ to denote the same function over vectors: $f(x) = (f(x_1), \ldots, f(x_m))$ if $x \in \mathbb{R}^m$.

Given vectors $v_1, \ldots, v_n \in \mathbb{R}^m$, we define $U = \text{GS}(v_1, \ldots, v_n)$ as their Gram-Schmidt orthonormalization. Namely, $U = [\hat{v}_1, \ldots, \hat{v}_n] \in \mathbb{R}^{m \times n}$ where $\hat{v}_1 = \frac{v_1}{\|v_1\|}$ and for every $i \geq 2$, $\hat{v}_i = \frac{\prod_{j=1}^{i-1}(I - \hat{v}_j \hat{v}_j^\top)v_i}{\|\prod_{j=1}^{i-1}(I - \hat{v}_j \hat{v}_j^\top)v_i\|}$. Note that in the occasion that $\prod_{j=1}^{i-1}(I - \hat{v}_j \hat{v}_j^\top)v_i$ is the zero vector, we let $\hat{v}_i$ be an arbitrary unit vector that is orthogonal to $\hat{v}_1, \ldots, \hat{v}_{i-1}$.

We say a function $f : \mathbb{R}^d \rightarrow \mathbb{R}$ is $L$-Lipschitz continuous if $|f(x) - f(y)| \leq L\|x - y\|_2$; and say it is $L$-smooth if its gradient is $L$-Lipschitz continuous, that is $\|\nabla f(x) - \nabla f(y)\|_2 \leq L\|x - y\|_2$.

**Function complexity.** The following notions from \cite{1} measure the complexity of any infinite-order smooth function $\phi : \mathbb{R} \rightarrow \mathbb{R}$. Suppose $\phi(z) = \sum_{i=0}^{\infty} c_i z^i$ is its Taylor expansion. Given
We have scaled down the input signals by \( \ell \)
\( G \)
growth assumption to simplify our notations: for instance, \( 3.4 \) each input sequence \( x \)
\( D \) the data are generated from an unknown distribution \( 3 \) problem formulation

\( O \)
\( approximations of them so we can truncate their Taylor expansions to degree
\( 1 - \varepsilon \) or low degree polynomials, they only differ by \( o(1/\varepsilon) \).

**Example 2.1.** If \( \phi(\varepsilon) = \varepsilon^d \) for constant \( d \) then \( C_\phi(\phi, R) \leq O(R^d), C_\phi(\phi, R) \leq O(R^d \log(1/\varepsilon)) \).

For functions such as \( \phi(\varepsilon) = e^\varepsilon - 1, \sin \varepsilon, \text{sigmoid}(\varepsilon) \) or \( \text{tanh}(\varepsilon) \), it suffices to consider \( \varepsilon \)-approximations of them so we can truncate their Taylor expansions to degree \( O(\log(1/\varepsilon)) \). This gives \( C_\phi(\phi, R), C_\phi(\phi, R) \leq (1/\varepsilon)^{O(\log R)} \).

### 3 Problem Formulation

The data are generated from an unknown distribution \( D \) over \( (x^*, y^*) \in (\mathbb{R}^d)^{(L-2)} \times \mathcal{Y}^{(L-2)} \).

Each input sequence \( x^* \) consists of \( x^*_1, \ldots, x^*_{L-1} \in \mathbb{R}^d \) with \( \|x^*_i\| = 1 \) and \( \|x^*_1\| = 1/2 \) without loss of generality.

Each label sequence \( y^* \) consists of \( y^*_1, \ldots, y^*_L \in \mathcal{Y} \). The training dataset \( \mathcal{Z} = \{(x^*_i, y^*_i)\}_{i=1}^N \) is given as \( N \) i.i.d. samples from \( D \). When \( (x^*, y^*) \) is generated from \( D \), we call \( x^* \) the true input sequence and \( y^* \) the true label.

**Definition 3.1.** Without loss of generality (see Remark 3.4), for each true input \( x^* \), we transform it into an actual input sequence \( x_1, x_2, \ldots, x_L \in \mathbb{R}^{d_e+1} \) as follows.

\[ x_1 = (0^{d_e}, 1) \quad \text{and} \quad x_\ell = (\varepsilon x x^*_\ell, 0) \quad \text{for} \quad \ell = 2, 3, \ldots, L - 1 \quad \text{and} \quad x_L = (0^{d_e}, \varepsilon x) \]

where \( \varepsilon x \in (0, 1) \) is a parameter to be chosen later. We then feed this actual sequence \( x \) into RNN.

**Definition 3.2.** We say the sequence \( x_1, \ldots, x_L \in \mathbb{R}^{d_e+1} \) is normalized if

\[ \|x_1\| = 1 \quad \text{and} \quad \|x_\ell\| = \varepsilon x \quad \text{for all} \quad \ell = 2, 3, \ldots, L. \]

### 3.1 Our Learner Network: Elman RNN

To present the simplest result, we focus on the classical Elman RNN with ReLU activation. Let \( W \in \mathbb{R}^{m \times m}, A \in \mathbb{R}^{m \times (d_e+1)} \), and \( B \in \mathbb{R}^{d \times m} \) be the weight matrices.

**Definition 3.3.** Our Elman RNN can be described as follows. On input \( x_1, \ldots, x_L \in \mathbb{R}^{d_e+1} \),

\[
\begin{align*}
    h_0 &= 0 \in \mathbb{R}^m \\
    g_\ell &= W \cdot h_{\ell-1} + Ax_\ell \in \mathbb{R}^m \\
    y_\ell &= B \cdot h_\ell \in \mathbb{R}^d \\
    h_\ell &= \sigma(W \cdot h_{\ell-1} + Ax_\ell) \in \mathbb{R}^m
\end{align*}
\]

We say that \( W, A, B \) are at random initialization, if the entries of \( W \) and \( A \) are i.i.d. generated from \( \mathcal{N}(0, \frac{2}{m}) \), and the entries of \( B \) are i.i.d. generated from \( \mathcal{N}(0, \frac{1}{d}) \).

For simplicity, in this paper we only update \( W \) and let \( A \) and \( B \) be at their random initialization. Thus, we write \( F_\ell(x^*; W) = y_\ell = Bh_\ell \) as the output of the \( \ell \)-th layer.

Our goal is to use \( y_3, \ldots, y_L \in \mathbb{R}^d \) to fit the true label \( y^*_3, \ldots, y^*_L \in \mathcal{Y} \) using some loss function \( G: \mathbb{R}^d \times \mathcal{Y} \to \mathbb{R} \). In this paper we assume, for every \( y^* \in \mathcal{Y} \), \( G(0^d, y^*) \in [-1, 1] \) is bounded, and \( G(\cdot, y^*) \) is convex and 1-Lipschitz continuous in its first variable. This includes for instance the cross-entropy loss and \( \ell_2 \)-regression loss (for \( y^* \) being bounded).

**Remark 3.4.** Since we only update \( W \), the label sequence \( y^*_3, \ldots, y^*_L \) is off from the input sequence \( x^*_2, \ldots, x^*_{L-1} \) by one. The last \( x_L \) can be made zero, but we keep it normalized for notational simplicity. The first \( x_L \) gives a random seed fed into the RNN (one can equivalently put it into \( h_0 \)). We have scaled down the input signals by \( \varepsilon x \), which can be equivalently thought as scaling down \( A \).

---

3This is without loss of generality, since \( \frac{1}{2} \) can always be padded to the last coordinate, and \( \|x^*_1\| = 1 \) can always be ensured from \( \|x^*_1\|_2 \leq 1 \) by padding \( \sqrt{1 - \|x^*_1\|_2^2} \) to the second-last coordinate. We make this assumption to simplify our notations: for instance, \( (x^*_1)_{d_e} = \frac{1}{2} \) allows us to focus only on networks in the concept class without bias.

4We use \([-1, 1]\) and 1-Lipschitzness for notation simplicity. In generally, our final time and sample complexity bounds only scale polynomially with the boundedness and Lipschitzness parameters.
3.2 Concept Class

Let \( \{ \Phi_{i \rightarrow j, r, s} : \mathbb{R} \to \mathbb{R} \}_{i, j \in [L], r \in [p], s \in [d]} \) be infinite-order differentiable functions, and \( \{ w_{i \rightarrow j, r, s} \in \mathbb{R}^{d_s} \}_{i, j \in [L], r \in [p], s \in [d]} \) be unit vectors. Then, for every \( j = 3, 4, \ldots, L \), we consider target functions \( F_j^* : \mathbb{R}^{d_s} \to \mathbb{R}^d \) where \( F_j^* = (F_{j,1}^*, \ldots, F_{j,d}^*) \) can be written as

\[
F_j^*(x^*) := \sum_{i=2}^{j-1} \sum_{r \in [p]} \Phi_{i \rightarrow j, r, s}(\langle w_{i \rightarrow j, r, s}, x_i^* \rangle) \in \mathbb{R}.
\]  

(3.1)

For proof simplicity, we assume \( \Phi_{i \rightarrow j, r, s}(0) = 0 \). We also use

\[
\mathcal{C}_e(\Phi, R) = \max_{i,j,r,s} \mathcal{C}_e(\Phi_{i \rightarrow j, r, s}, R)
\]

and suppose we are given training dataset \( D \). We consider the following stochastic training objective

\[
\text{Obj}(W) := \mathbb{E}_{(x^*, y^*) \sim D} \left[ \sum_{j=3}^{L} G \left( F_j^*(x^*), y_j^* \right) \right] \leq \text{OPT}.
\]

(4)

where \( \text{Obj}(x^*, y^*; W') := \sum_{j=3}^{L} G (\lambda F_j(x^*; W + W'), y_j^*) \)

Above, \( W \in \mathbb{R}^{m \times m} \) is random initialization, \( W' \in \mathbb{R}^{m \times m} \) is the additional shift, and \( \lambda \in (0, 1) \) is a constant scaling factor on the network output. We consider the vanilla stochastic gradient descent (SGD) algorithm with step size \( \eta \). In each iteration \( t = 1, 2, \ldots, T \), it updates

\[
W_t = W_{t-1} - \eta \nabla_{W} \text{Obj}(x^*, y^*; W_{t-1})
\]

(5)

for a random sample \((x^*, y^*)\) from the training set \( D \).

Theorem 1. For every \( 0 < \varepsilon < \tilde{O}\left( \frac{1}{\text{poly}(L, d)} \right) \), define complexity \( C = \mathcal{C}_e(\Phi, \sqrt{L}) \) and \( \lambda = \tilde{O}\left( \frac{\varepsilon}{\sqrt{d}} \right) \), if the number of neurons \( m \geq \text{poly}(C, \varepsilon^{-1}) \) and the number of samples is \( N = |D| \geq \text{poly}(C, \varepsilon^{-1}, \log m) \), then SGD with \( \eta = \tilde{O}\left( \frac{1}{\varepsilon \sqrt{md}} \right) \) and

\[
T = \tilde{O}\left( \frac{p^2 C^2 \text{poly}(L, d)}{\varepsilon^2} \right)
\]

Theorem 1. For every \( 0 < \varepsilon < \tilde{O}\left( \frac{1}{\text{poly}(L, d)} \right) \), define complexity \( C = \mathcal{C}_e(\Phi, \sqrt{L}) \) and \( \lambda = \tilde{O}\left( \frac{\varepsilon}{\sqrt{d}} \right) \), if the number of neurons \( m \geq \text{poly}(C, \varepsilon^{-1}) \) and the number of samples is \( N = |D| \geq \text{poly}(C, \varepsilon^{-1}, \log m) \), then SGD with \( \eta = \tilde{O}\left( \frac{1}{\varepsilon \sqrt{md}} \right) \) and

\[
T = \tilde{O}\left( \frac{p^2 C^2 \text{poly}(L, d)}{\varepsilon^2} \right)
\]

(6)

\[\tilde{O}\left( \frac{1}{\text{poly}(L, d)} \right)\]

(7)

\[\frac{1}{\varepsilon \sqrt{md}}\]

\[\tilde{O}\left( \frac{p^2 C^2 \text{poly}(L, d)}{\varepsilon^2} \right)\]

(8)

\[\frac{1}{\text{poly}(L, d)}\]

(9)

\[\frac{1}{\sqrt{d}}\]

(10)

\[\tilde{O}\left( \frac{1}{\varepsilon \sqrt{md}} \right)\]

(11)

\[\tilde{O}\left( \frac{p^2 C^2 \text{poly}(L, d)}{\varepsilon^2} \right)\]

(12)

\[\frac{1}{\text{poly}(L, d)}\]

(13)

\[\frac{1}{\sqrt{d}}\]

(14)

\[\tilde{O}\left( \frac{1}{\varepsilon \sqrt{md}} \right)\]

(15)

\[\tilde{O}\left( \frac{p^2 C^2 \text{poly}(L, d)}{\varepsilon^2} \right)\]

(16)
satisfies that, with probability at least \(1 - e^{-\Omega(\rho^2)}\) over the random initialization

\[
E_{\text{sgd}} \left[ \frac{1}{T} \sum_{t=0}^{T-1} E_{(x^*, y^*) \sim D} \left[ \text{Obj}(x^*, y^*; W_t) \right] \right] \leq \text{OPT} + \varepsilon .
\]

Above, \(E_{\text{sgd}}\) takes expectation with respect to the randomness of SGD. Since SGD takes only one example per iteration, the sample complexity \(N\) is also bounded by \(T\).

### 4.1 Our Contribution, Interpretation, and Discussion

**Sample complexity.** Our sample complexity only scales with \(\log(m)\), making the result applicable to over-parameterized RNNs that have \(m \gg N\). Following Example 2.1, if \(\phi(z)\) is constant degree polynomial we have \(C = \text{poly}(L, \log \varepsilon^{-1})\) so Theorem 1 says that RNN learns such concept class with size \(m = \frac{\text{poly}(L, d, p)}{\text{poly}(\varepsilon)}\) and sample complexity \(\min\{N, T\} = \frac{p^2 \text{poly}(L, d, \log m)}{\varepsilon^2}\).

If \(\phi(z)\) is a function with good Taylor truncation, such as \(e^z - 1, \sin z, \text{sigmoid}(z)\) or \(\text{tanh}(z)\), then \(C = L^{O(\log(1/\varepsilon))}\) is almost polynomial.

**Non-linear measurements.** Our result shows that vanilla RNNs can efficiently learn a weighted average of non-linear measurements of the input. As we argued in Example 3.5, this at least includes functions where the output at each token is generated from inputs of previous tokens using any two-layer neural networks. Average of non-linear measurements can be quite powerful, achieving the state-of-the-art performance in some sequential applications such as sentence embedding [4] and many others [23], and acts as the base of attention mechanism in RNNs [5].

**Adapt to tokens.** In the target function, \(\Phi_{i \rightarrow j, r, s}\) can be different at each token, meaning that they can adapt to the position of the input tokens. We emphasize that the positions of the tokens (namely, the values \(i, j\)) are not directly fed into the network, rather it is discovered through sequentially reading the input. As one can see from our proofs, the ability of adapting to the tokens comes from the inhomogeneity in hidden layers \(h\); even when \(x_t = x_{t'}\) for different tokens \(t' \neq t\), there is still big difference between \(h_t\) and \(h_{t'}\). Albeit the same operator is applied to \(x_t\) and \(x_{t'}\), RNNs can still use this crucial inhomogeneity to learn different functions at different tokens.

In our result, the function \(\Phi_{i \rightarrow j, r, s}\) only adapts with the positions of the input tokens, but in many applications, we would like the function to adapt with the values of the past tokens \(x_1^*, \ldots, x_{t-1}^*\) as well. We believe a study on other models (such as LSTM [15]) can potentially settle these questions.

**Long term memory.** It is commonly believed that vanilla RNNs cannot capture long term dependencies in the input. This does not contradict our result. Our complexity parameter \(C \sqrt{L}\) of the learning process in Theorem 1 indeed suffers from \(L\), the length of the input sequence. This is due to the fact that vanilla RNN, the hidden neurons \(h_t\) will incorporate more and more noise as the time horizon \(t\) increases, making the new signal \(A x_t\) less and less significant.

**Comparison to feed-forward networks.** Recently there are many interesting results on analyzing the learning process of feed-forward neural networks [7, 8, 11, 16, 18, 20, 26, 27, 29, 30, 32]. Most of them either assume that the input is structured (e.g. Gaussian or separable) or only consider linear networks. Allen-Zhu, Li, and Liang [1] show a result in the same flavor as this paper but for two and three-layer feedforward networks. Since RNNs apply the same unit repeatedly to each input token in a sequence, our analysis is significantly different from [1] and creates lots of difficulties in the analysis.

---

6 More specifically, Allen-Zhu, Li, and Liang [1] study two (or three) layer feedforward networks, which use one (or two) hidden weight matrix to learn one target function. Here in RNN, there is only one weight matrix shared across the entire time horizon to learn \(L\) target functions at different input positions. In other words, using “one weight” to learn “one target function” is known from prior work, but using “one weight” to efficiently learn “\(L\) different target functions” is substantially more difficult, especially when the position information is not given as the input to the network. For example, our theorem implies that an RNN can distinguish the sequences “AAAB” from “AABA”, since the order of A and B are different. This requires the RNN to keep track, using one weight matrix, of the position information of the symbols in the sequence.
4.2 Conclusion

We show RNN can actually learn some notable concept class efficiently, using simple SGD method with sample complexity polynomial or almost-polynomial in input length. This concept class at least includes functions where each output token is generated from inputs of earlier tokens using a smooth neural network. To the best of our knowledge, this is the first proof that some non-trivial concept class is efficiently learnable by RNN. Our sample complexity is almost independent of \( m \), making the result applicable to over-parameterized settings. On a separate note, our proof explains why the same recurrent unit is capable of learning various functions from different input tokens to different output tokens.

Section 6 through 9 continue to give sketch proofs. Our final proofs reply on many other technical properties of RNN that may be of independent interests: such as properties of RNN at random initialization (which we include in Section B and C), and properties of RNN stability (which we include in Section D, E, F). Some of these properties are simple modifications from prior work, but some are completely new and require new proof techniques (namely, Section C, D and E).

**Proof Sketch**

Our proof of Theorem 1 divides into four conceptual steps.

1. We obtain first-order approximation of how much the outputs of the RNN change if we move from \( W \) to \( W + W' \). This change (up to small error) is a linear function in \( W' \). (See Section 6).
   
   (This step can be derived from prior work [2] without much difficulty.)

2. We construct some (unknown) matrix \( W* \in \mathbb{R}^{m \times m} \) so that this “linear function”, when evaluated on \( W* \), approximately gives the target \( F* \) in the concept class (see Section 5).
   
   (This step is the most interesting part of this paper.)

3. We argue that the SGD method moves in a direction nearly as good as \( W* \) and thus efficiently decreases the training objective (see Section 7).
   
   (This is a routine analysis of SGD in the non-convex setting given Steps 1&2.)

4. We use the first-order linear approximation to derive a Rademacher complexity bound that does not grow exponentially in \( L \) (see Section 8). By feeding the output of SGD into this Rademacher complexity, we finish the proof of Theorem 1 (see Section 9).

   (This is a one-paged proof given the Steps 1&2&3.)

Although our proofs are technical, to help the readers, we write 7 pages of sketch proofs for Steps 1 through 4. This can be found in Section 5 through 9. Due to space limitation, we only include Section 5 in the main body. We introduce some notations for analysis purpose.

**Definition 4.1.** For each \( \ell \in [L] \), let \( D_\ell \in \mathbb{R}^{m \times m} \) be the diagonal matrix where

\[
(D_\ell)_{k,k} = 1_{(W \cdot h_{\ell-1} + Ax_\ell)_k \geq 0} = 1_{(g_\ell)_k \geq 0}.
\]

As a result, we can write \( h_\ell = D_\ell Wh_{\ell-1} \). For each \( 1 \leq \ell \leq a \leq L \), we define

\[
\text{Back}_{\ell \rightarrow a} = BD_a W \cdots D_{\ell+1} W \in \mathbb{R}^{d \times m}.
\]

with the understanding that \( \text{Back}_{\ell \rightarrow \ell} = B \in \mathbb{R}^{d \times m} \).

Throughout the proofs, to simplify notations when specifying polynomial factors, we introduce

\[
\rho := 100Ld \log m \quad \text{and} \quad \rho := 100Ldp \cdot \mathcal{E}_\varepsilon(\Phi, \sqrt{L}) \cdot \log m
\]

We assume \( m \geq \text{poly}(\rho) \) for some sufficiently large polynomial factor.

5 Existence of Good Network Through Backward

One of our main contributions is to show the existence of some “good linear network” to approximate any target function. Let us explain what this means. Suppose \( W, A, B \) are at random initialization. We consider a linear function over \( W* \in \mathbb{R}^{m \times m} \):

\[
f_{j'} := \sum_{j''=2}^{j'} \text{Back}_{j'' \rightarrow j'} D_{j'} W* h_{j''-1}.
\]
As we shall see later, in first-order approximation, this linear function captures how much the output of the RNN changes at token \( j' \), if one we move \( W \) to \( W + W' \). The goal in this section is to construct some \( W^* \in \mathbb{R}^{m \times m} \) satisfying that, for any true input \( x^* \) in the support of \( D \), if we define the actual input \( x \) according to \( x^* \) (see Definition 3.1), then with high probability,

\[
\forall s' \in [d] \quad f_{j',s'} \approx F_{j',s'}(x^*) = \sum_{i=2}^{j'-1} \sum_{r \in [p]} \Phi_{i \rightarrow j',r,s'}((w_{i \rightarrow j',r,s'})^*)
\]

In our sketched proof below, it shall become clear how this same matrix \( W^* \) can simultaneously represent functions \( \Phi_{i \rightarrow j'} \) that come from different input tokens \( i \). Since SGD can be shown to descend in a direction “comparable” to \( W^* \), it converges to a matrix \( W \) with similar guarantees.

### 5.1 Indicator to Function

In order to show (5.2), we first show a variant of the “indicator to function” lemma from [1].

**Lemma 5.1** (indicator to function). For every smooth function \( \Phi: \mathbb{R} \rightarrow \mathbb{R} \), every unit vector \( w^* \in \mathbb{R}^d \) with \( w^*_{d_0} = 0 \), every constant \( \sigma \geq 0.1 \), every constant \( \gamma > 1 \), every constant \( \varepsilon \in (0, \frac{1}{\varepsilon(\sigma \cdot \Phi(O(\sigma)))}) \), there exists

\[
C' = C_{\varepsilon, \Phi(\sigma)} \quad \text{and a function } H: \mathbb{R} \rightarrow [-C', C'],
\]

such that for every fixed unit vectors \( x^* \in \mathbb{R}^d \) with \( x^*_{d_0} = \frac{1}{2} \),

\[
(a) \quad |E_{a \sim N(0,1), n \sim N(0, a^2)} [1_{(a,x^*)^+ \in [n \geq 0]H(a)}] - \Phi(⟨w^*, x^*⟩)| \leq \varepsilon \quad \text{(on target)}
\]

\[
(b) \quad |E_{a \sim N(0,1), n \sim N(0, a^2)} [1_{(a,x^*)^+ \in [\gamma n \geq 0]H(a)}] - \Phi(0)| \leq \varepsilon + O\left(C' \frac{\log(\gamma^2)}{\gamma^2}\right) \quad \text{(off target)}
\]

Above, Lemma 5.1a says that we can use a bounded function \( 1_{(a,x^*)^+ \in [n \geq 0]H(a)} \) to fit a target function \( \Phi(⟨w^*, x^*⟩) \), and Lemma 5.1b says that if the magnitude of \( n \) is large then this function is close to being constant. For such reason, we can view \( n \) as “noise.” While the proof of 5.1a is from prior work [1], our new property 5.1b is completely new and it requires some technical challenge to simultaneously guarantee 5.1a and 5.1b. The proof is in Appendix G.1.

### 5.2 Fitting a Single Function

We now try to apply Lemma 5.1 to approximate a single function \( \Phi_{i \rightarrow j,r,s}(⟨w_{i \rightarrow j,r,s}, \ell⟩) \). For this purpose, let us consider two (normalized) input sequences. The first (null) sequence \( x(0) \) is given as

\[
x_i(0) = (0^4, 1) \quad \text{and} \quad x_i(0) = (0^d, \varepsilon) \quad \text{for } i = 2, 3, \ldots, L
\]

The second sequence \( x \) is generated from an input \( x^* \) in the support of \( D \) (recall Definition 3.1). Let

- \( h_t, D_t, B_{i \rightarrow j} \) be defined with respect to \( W, A, B \) and input sequence \( x \), and
- \( h_t^{(0)}, D_t^{(0)}, B_{i \rightarrow j}^{(0)} \) be defined with respect to \( W, A, B \) and input sequence \( x(0) \)

We remark that \( h_t^{(0)} \) has the good property that it does not depend \( x^* \) but somehow stays “close enough” to the true \( h_t \) (see Appendix D for a full description).

**Lemma 5.2** (fit single function). For every \( 2 \leq i < j \leq L, r \in [p], s \in [d] \) and every constant \( \varepsilon \in (0, \frac{1}{\varepsilon(\Phi_{i \rightarrow j,r,s}\cdot O(\Phi))}) \), there exists \( C' = C_{\varepsilon, \Phi_{i \rightarrow j,r,s}, \sqrt{L}} \) so that, for every

\[
\varepsilon_x \in (0, \frac{1}{\varepsilon(\Phi_{i \rightarrow j,r,s}, \sqrt{L})}) \quad \text{and} \quad \varepsilon = \frac{\varepsilon_x \varepsilon_{e(\Phi_{i \rightarrow j,r,s}, \sqrt{L})}}{\sqrt{L}}
\]

there exists a function \( H_{i \rightarrow j,r,s}: \mathbb{R} \rightarrow [-\frac{4(C')^2}{\varepsilon_x \varepsilon_e}, \frac{4(C')^2}{\varepsilon_x \varepsilon_e}] \), such that, let

- \( x \) be a fixed input sequence defined by some \( x^* \) in the support of \( D \) (see Definition 3.1),
- \( W, A \) be at random initialization,
- \( h_t \) be generated by \( W, A, x \) and \( h_t^{(0)} \) be generated by \( W, A, x(0) \), and
- \( \tilde{w}_k, \tilde{a}_k \sim N(0, \frac{1}{m}) \) be freshly new random vectors,

with probability at least \( 1 - e^{-\Omega(n^2)} \) over \( W \) and \( A \),

\[
(\text{a) (on target)} \quad \left| \mathbb{E}_{\tilde{w}_k, \tilde{a}_k} \left[ 1_{(\tilde{w}_k, \tilde{a}_k)_{i \rightarrow j,r,s} \leq \varepsilon} - \Phi_{i \rightarrow j,r,s}(⟨w_{i \rightarrow j,r,s}, \ell⟩) \right] \right| \leq \varepsilon
\]

\[
(\text{b) (off target)} \quad \left| \mathbb{E}_{\tilde{w}_k, \tilde{a}_k} \left[ 1_{(\tilde{w}_k, \tilde{a}_k)_{i \rightarrow j,r,s} \leq \varepsilon} - \Phi_{i \rightarrow j,r,s}(⟨w_{i \rightarrow j,r,s}, \ell⟩) \right] \right| \leq \varepsilon
\]
(b) (off target), for every \( i' \neq i \)

\[
\left| \sum_{\alpha_k, \tilde{\alpha}_k} \mathbb{E}_{\tilde{w}_k, \tilde{w}_k} \left[ I_{\{(\tilde{w}_k, h_{i'}^{0})\} \leq \frac{1}{\sqrt{m}} H_{j, r, s}(\tilde{\alpha}_k)} \right] \right| \leq \varepsilon_c
\]

Lemma 5.2 implies there is a quantity \( I_{\{(\tilde{w}_k, h_{i'}^{0})\} \leq \frac{1}{\sqrt{m}} H_{j, r, s}(\tilde{\alpha}_k)} \) that only depends on the target function and the random initialization (namely, \( \tilde{w}_k, \tilde{\alpha}_k \)) such that,

- when multiplying \( I_{\langle \tilde{w}_k, h_{i'} \rangle + \langle \tilde{\alpha}_k, x_i \rangle \geq 0} \) gives the target \( \Phi_{i \rightarrow j, r, s}(\langle w_{i'}^{*} \rangle_{j, r, s}, x_i^{*}) \), but
- when multiplying \( I_{\langle \tilde{w}_k, h_{i'} \rangle + \langle \tilde{\alpha}_k, x_i \rangle \geq 0} \) gives near zero.

The full proof is in Appendix G.2 but we sketch why Lemma 5.2 can be derived from Lemma 5.1.

**Sketch proof of Lemma 5.2.** Let us focus on indicator \( I_{\langle \tilde{w}_k, h_{i'} \rangle + \langle \tilde{\alpha}_k, x_i \rangle \geq 0} \):

- \( \langle \tilde{\alpha}_k, x_i' \rangle \) is distributed like \( N'(0, \frac{2\varepsilon^2}{m}) \) because \( \langle \tilde{\alpha}_k, x_i' \rangle = \langle \tilde{\alpha}_k, (\varepsilon x_i^{*}, 0) \rangle \); but
- \( \langle \tilde{w}_k, h_{i'} \rangle \) is roughly \( N'(0, \frac{2\varepsilon}{m}) \) because \( \| h_{i'} \| \approx 1 \) by random init. (see Lemma B.1a).

Thus, if we treat \( \langle \tilde{w}_k, h_{i'} \rangle \) as the “noise” in Lemma 5.1 it can be \( \frac{1}{\varepsilon} \) times larger than \( \langle \tilde{\alpha}_k, x_i' \rangle \).

To show Lemma 5.2a, we only need to focus on \( \langle \tilde{w}_k, h_{i'} \rangle \leq \frac{1}{\sqrt{m}} \) because \( i = i' \). Since \( h(0) \) can be shown close to \( h \) (see Lemma D.1), this is almost equivalent to \( \langle \tilde{w}_k, h_{i'} \rangle \leq \frac{1}{\sqrt{m}} \). Conditioning on this happens, the “noise” \( n \) must be small so we can apply Lemma 5.1a.

To show Lemma 5.2a, we can show when \( i' \neq i \), the indicator on \( \langle \tilde{w}_k, h_{i-1} \rangle \) \( \leq \frac{1}{\sqrt{m}} \) gives little information about the true noise \( \langle \tilde{w}_k, h_{i-1} \rangle \). This is so because \( h_{i-1} \) and \( h_{i'} \) are somewhat uncorrelated (details in Lemma B.1k). As a result, the “noise” \( n \) is still large and thus Lemma 5.1b applies with \( \Phi_{i \rightarrow j, r, s}(0) = 0 \). \( \square \)

### 5.3 Fitting the Target Function

We are now ready to design \( W^* \in \mathbb{R}^{m \times m} \) using Lemma 5.2.

**Definition 5.3.** Suppose \( \varepsilon_c \in (0, \frac{1}{\varepsilon_c(\Phi, O(\sqrt{\varepsilon_e}))}) \), \( C' = C_{\varepsilon_c} \), \( C \), \( C_{i \rightarrow j, s} := \frac{1}{m} \left\| e_s^T \text{Back}(i, j) \right\|_2 \left\| h_{i-1}^{(0)} \right\|_2 \). We construct \( W^* \in \mathbb{R}^{m \times m} \) by defining its \( k \)-th row vector as follows:

\[
w_k := \sum_{i=2}^{L-1} \sum_{j=i+1}^{L} \sum_{r \in [p], s \in [d]} \frac{1}{mC_{i \rightarrow j, s}} \left[ e_s^T, \text{Back}(i, j) \right]_k \mathbb{E} \left\| e_s^T \text{Back}(i, j) \right\|_2 \left\| h_{i-1}^{(0)} \right\|_2 \left\| h_{j}^{(0)} \right\|_2 \]

above, functions \( H_{i \rightarrow j, r, s} : \mathbb{R} \rightarrow [-C, C] \) come from Lemma 5.2.

The following lemma that says \( f_{j', s'} \) is close to the target function \( F_{j', s'} \).

**Lemma 5.4** (existence through backward). The construction of \( W^* \) in Definition 5.3 satisfies the following. For every normalized input sequence \( x \) generated from \( x^* \) in the support of \( D \), we have with probability at least \( 1 - e^{-O(\varepsilon_c)} \) over \( W, A, B \), it holds for every \( 3 \leq j' \leq L \) and \( s' \in [d] \):

\[
f_{j', s'} = \sum_{i=2}^{j'-1} \sum_{r \in [p]} \Phi_{i \rightarrow j', r, s'} \left\langle \left( w_{i'}^{*} \right), x_i^{*} \right\rangle \left( p^{1/11} \cdot O(\varepsilon_c, \Phi, 1)\varepsilon_c^{1/3} + Cm^{-0.05} \right) .
\]
Proof sketch of Lemma 5.4. Using definition of $f_{j', s'}$ in (5.1) and $W^*$, one can write down

$$f_{j', s'} = \sum_{i', j, r \in [p], e \in [d]} \sum_{k \in [m]} \left( \frac{1}{mc_{i' \rightarrow j'}} [e_{s'}^r \text{Back}_{i' \rightarrow j'}]_k [e_{s}^r \text{Back}_{i \rightarrow j}]_k \right) \cdot \mathbb{I}_{[\langle w_k, h_{i-1}^{(0)} \rangle \leq \varepsilon]} \mathbb{I}_{[g_{i'}^{(0)} \leq 0]}$$

(5.3)

Now,

- The summands in (5.3) with $i \neq i'$ are negligible owing to Lemma 5.2b.
- The summands in (5.3) with $i = i'$ but $j \neq j'$ are negligible, after proving that Back$_{i \rightarrow j}$ and Back$_{i' \rightarrow j'}$ are very uncorrelated (details in Lemma C.1).
- The summands in (5.3) with $s \neq s'$ are negligible using the randomness of $B$.
- One can also prove Back$_{i' \rightarrow j'} \approx$ Back$_{i' \rightarrow j'}$ and $h_{i'-1} \approx h^{(0)}_{i'-1}$ (details in Lemma D.1).

Together,

$$f_{j', s'} \approx \sum_{i'=0}^{j'-1} \sum_{r \in [p]} \left( \frac{1}{mc_{i' \rightarrow j'}} \left( [e_{s'}^r \text{Back}_{i' \rightarrow j'}]_k \right)^2 \right) \cdot \mathbb{I}_{[\langle w_k, h_{i-1}^{(0)} \rangle \leq \varepsilon]} \mathbb{I}_{[g_{i'}^{(0)} \leq 0]}$$

Applying Lemma 5.2a and using our choice of $C_{i' \rightarrow j', s'}$, this gives (in expectation)

$$f_{j', s'} \approx \sum_{i'=0}^{j'-1} \sum_{r \in [p]} \Phi_{i' \rightarrow j', r, s'}(\langle w_{i'}^{(0)} \rightarrow j', r, s', x_{i'-1}^r \rangle) = F_{j', s'}(x^*) .$$

Proving concentration (with respect to $k \in [m]$) is a lot more challenging due to the sophisticated correlations across different indices $k$. To achieve this, we replace some of the pairs $w_k, a_k$ with fresh new samples $\tilde{w}_k, \tilde{a}_k$ for all $k \in \mathcal{N}$ and apply concentration only with respect to $k \in \mathcal{N}$. Here, $\mathcal{N}$ is a random subset of $[m]$ with cardinality $m^{1/2}$. We show that the network stabilizes (details in Section E) against such re-randomization. Full proof is in Section G.3.

Finally, one can show $\|W^*\|_F \leq O\left(\frac{Lp^3C}{\sqrt{m}}\right)$ (see Claim G.1). Crucially, this Frobenius norm scales in $m^{-1/2}$ so standard SGD analysis shall ensure that our sample complexity does not depend on $m$ (up to log factors).

References


9


