Universality and Limitations of Prompt Tuning

Abstract

Despite the demonstrated empirical efficacy of prompt tuning to adapt a pretrained language model for a new task, the theoretical underpinnings of the difference between "tuning parameters before the input" against "the tuning of model weights" are limited. We thus take one of the first steps to understand the role of soft-prompt tuning for transformer-based architectures. By considering a general purpose architecture, we analyze prompt tuning from the lens of both: universal approximation and limitations with finite-depth fixed-weight pretrained transformers for continuous-valued functions. Our universality result guarantees the existence of a strong transformer with a prompt to approximate any sequence-to-sequence function in the set of Lipschitz functions. The limitations of prompt tuning for limited-depth transformers are first proved by constructing a set of datasets, that cannot be memorized by a prompt of any length for a given single encoder layer. We also provide a lower bound on the required number of tunable prompt parameters and compare the result with the number of parameters required for a low-rank update (based on LoRA) for a single-layer setting. We finally extend our analysis to multi-layer settings by providing sufficient conditions under which the transformer can at best learn datasets from invertible functions only. Our theoretical claims are also corroborated by empirical results.

1 Introduction

The surge in the empirical research of large-scale models has led to the emergence of a new paradigm of prompt tuning. Current large models consist of billions of parameters [Brown et al., 2020, Chowdhery et al., 2022], which greatly exacerbate the cost of tuning the entire model weights via gradient-based optimization. On the other hand, the power of scale in both model size and pretraining dataset size has demonstrated strong capabilities by achieving reasonable performance through a learnable prompt appended before the input [Li and Liang, 2021, Lester et al., 2021]. Despite this, several questions emanate around the abilities and limitations of prompt tuning.

In this work, we aim to characterize some natural yet essential questions about prompt tuning with transformer architectures. Firstly, are prompts universal approximators, i.e. with a fixed pretrained transformer network, can we find a prompt to approximate any sequence-to-sequence function in a given space? If yes, can we construct the transformer for this universality result? Second, can we identify failure modes of prompt tuning when applied on potentially non-optimal but non-trivial transformers? Moreover, since prompt tuning is usually compared against LoRA [Hu et al., 2021] in consideration to parameter-efficient tuning, is prompt tuning then more/less parameter-efficient than LoRA? Answering these questions can lead to important insights on when and how to perform prompt tuning to adapt a pretrained transformer network to a given downstream task of interest.
In this work, we seek to answer these questions with appropriate theoretical analysis and further validate our claims with empirical results. We first characterize the universal nature of prompt tuning by constructing a specific transformer network. We show that for a given approximation error and the space of sequence-to-sequence Lipschitz functions, we can construct a transformer network, with a suitable number of layers, that can leverage prompt tuning to approximate any function in this space. Despite this universality of prompt tuning with a carefully constructed pretrained transformer, we then identify some limitations of prompt tuning with weaker but non-trivial transformers. We prove this by constructing sequence-to-sequence datasets with shared input tokens, which are surprisingly simple but cannot be memorized by prompt tuning for a given transformer. We also extend our analysis to more general settings where the shared token is not required. In this setting, we first prove that prompt tuning on a single-layer transformer requires $\Omega(n)$ trainable parameters to memorize $n$ training examples, wherein for LoRA, it suffices with $O(n)$ trainable parameters. We finally extend our analysis to the multi-layer setting and provide sufficient conditions under which prompt tuning exhibits extremely limited capacity to at best memorizing datasets from invertible functions.

Our contributions can be summarized as below:

- We characterize the universal nature of prompt tuning by explicitly constructing a transformer network (Theorem 1).
- We provide a construction-based argument for sequence-to-sequence datasets that cannot be learned by prompt tuning with a given single-layer transformer (Theorem 2).
- We provide the lower bound on the required number of parameters for prompt tuning to memorize any sequence-to-sequence functions (Theorem 3).
- We provide a sufficient condition for multi-layer transformers, under which datasets with shared output tokens cannot be learned with prompt tuning (Theorem 4).
- We conduct empirical studies, including real-world datasets, to verify our theoretical claims.

2 Related Work

Theoretical Analysis of Transformers Various works have characterized the theoretical properties of transformers and its primary self-attention component. [Yun et al., 2020] study the universal approximation ability of transformers for continuous permutation equivariant sequence-to-sequence functions with compact support and further examined the role of using positional encodings to circumvent permutation equivariant condition. [Pérez et al., 2021] show that transformer with a hard-attention is Turing complete based on their capacity to perform computations and access the internal dense representations of the data. [Wei et al., 2021] further show that transformers can approximate Turing machines with bounded computation time with a new notion of approximation. [Dong et al., 2021] provided a negative yet interesting result signifying the limitations of pure self-attention in terms of rank diminishing of the input. Other works including [Kim et al., 2021, Dasoulas et al., 2021] derive upper bounds on the Lipschitz constant of respective modifications of the attention mechanism. The works by [Li et al., 2022, Zhang et al., 2020] documented optimization perspective on transformer training via SGD.

Fine-tuning and Prompt Tuning Fine-tuning is the standard way to adapt a pretrained model to downstream tasks. The most standard and popular paradigm is tuning the model weights via a suitable optimization procedure along with a linear head on the output representations [Radford et al., 2018, Devlin et al., 2019]. Subsequent works studied more parameter-efficient ways of fine-tuning by updating either a subset of model parameters [Ben Zaken et al., 2022] or restricting the parameter-updates to a low-dimensional subspace [Aghajanyan et al., 2021]. [Hu et al., 2021, Mahabadi et al., 2021]. The work by [Hu et al., 2021] (their framework referred to as LoRA) has garnered particular interest in the community and [Malladi et al., 2023] has provided an interpretation of LoRA via the kernel mechanism. In the particular context of LLMs, prompt tuning has emerged as the de facto approach where only the prompt is updated while keeping the rest of the transformer weights and architecture fixed [Shin et al., 2020, Lester et al., 2021, Li and Liang, 2021].

Analysis of Prompt Tuning [Wei et al., 2022] studied the link between prompt tuning and downstream tasks with an underlying latent variable generative model of text, which is confined to a Hidden Markov Model. However, they focused on the discrete vocabulary setting contrary to our
results for continuous sequence-to-sequence functions. Some more recent works \[Akyürek et al., 2023\] [Von Oswald et al., 2023\] characterized an intriguing property of a specific form of prompting, referred to as in-context learning, where they proved by construction that transformers can implement learning algorithms for linear models based on gradient descent and closed-form ridge regression. This work however pursued a different and specific direction from the prompting results we aim to provide for generic settings.

Memorization Capacity of Neural Networks A series of works have sought to provide finite sample universal memorization capacity results of neural networks and the understanding of expressive power of neural networks. \[Huang and Huang, 1990\] [Huang and Babri, 1998\] [Huang, 2003\] [Yamasaki, 1993\] analyzed the memorization capacity of FNNs with sigmoid and other bounded activation functions. \[Hardt and Ma, 2016\] [Zhang et al., 2021\] [Nguyen and Hein, 2018\] provided results for modern ReLU networks including FNNs and CNNs. For transformer architectures, \[Kim et al., 2021\] proved that transformers can memorize a dataset with finite parameters. To the best of our knowledge, similar results for prompt tuning have not been studied in continuous settings for transformer architectures.

3 Transformers and Parameter Efficient Training

3.1 Preliminaries

We use the following notations throughout the paper. A bold lower case character, e.g. \(x\), denotes a vector. A bold upper case character, e.g. \(W\), denotes a matrix while \(W_{i,j}\), \(W_{i,:}\) and \(W_{:,j}\) is the \((i, j)\)-th element, \(i\)-th row, \(j\)-th column, respectively. We use a single superscript or subscript to denote the index of a matrix, e.g. \(X_i, X^j\) denote the \(i\)-th matrix in a matrices sequence. We use \(\sigma\) and \(\bar{\sigma}\) for softmax and hardmax operators, respectively. We use \(\text{ReLU}(\mathbf{v}) = \max(\mathbf{v}, \mathbf{0})\) to denote the ReLU activation function where \(\max(\cdot)\) function is applied entry-wise to a vector. We use \(\text{Cone}(a_1, a_2, ..., a_m)\) to denote a convex cone where \(\text{Cone}(a_1, a_2, ..., a_m) = \{x : x = \sum_{i=1}^m a_i x_i, a_i > 0\}\). We also define the minus operation between a set \(S\) and a vector \(\mathbf{v}\) as \(S - \mathbf{v} = \{x - \mathbf{v} : x \in S\}\). In Section 4 we use \([a : b : c]\) to denote a grid \([a, a + b, a + 2b, ..., c - b]\) from \(a\) to \(c\), with an interval \(b\).

Transformer networks \[Vaswani et al., 2017\] are a stack of multiple transformer layers, composed subsequently. A transformer layer has two key components: an attention layer and a token-wise MLP layer, with residual connections around both blocks. We consider the input and output to be sequences of tokens \(X \in \mathbb{R}^{d \times m}\) and \(Y \in \mathbb{R}^{d \times m}\), where \(m\) is the number of tokens in the sequence and \(d\) is the token dimension.

**Definition 1** (Attention Layer). We define an \(h\)-head attention layer parameterized with \(W_q, W_k, W_o, W_v\) between a single token \(x\) and a token sequence \(X\) as

\[
\text{Att}(x, X) = \sum_{i=1}^h W_o^i W_k^i x \cdot \sigma((W_k^i X)^\top W_q^i x).
\]

The normalizing factor of \(\frac{1}{\sqrt{d_{k_i}}}\) is subsumed in the weight matrices \(W_k^i\) for notational simplicity.

We can then define the cross attention between two sequences \(X_1 \in \mathbb{R}^{d \times m_1}\) and \(X_2 \in \mathbb{R}^{d \times m_2}\) (We use \(x_k = (X_1)_{:,k}\) for simplicity):

\[
\text{Att}(X_1, X_2) = [\text{Att}(x_1, X_2), \text{Att}(x_2, X_2), ..., \text{Att}(x_{m_1}, X_2)].
\]

**Definition 2** (Standard Transformer Layer). With definition 1 we define a standard transformer layer \(\tau\) as

\[
\text{MLP}(X) = [W_2 \text{ReLU}(W_1 X_{:,1} + b_1) + b_2 + X_{:,1}, \ldots, W_2 \text{ReLU}(W_1 X_{:,n} + b_1) + b_2 + X_{:,n}]
\]

\[
\tau(X) = \text{MLP}(\text{Att}(X, X) + X).
\]

The definition here omits the layer normalization block for simplicity (following \[Kim et al., 2021\]).
Without loss of generality, we assume that the support and range set of all considered sequence-to-
sequence functions $f$ is $[0, 1]^{d \times m}$ in this section. We define $F_L$ as the collection of all continuous
sequence-to-sequence $L$-lipschitz functions under norm $p$ and sequence length $m$. For $f \in F_L$ and any two inputs $\mathbf{X}, \mathbf{X}' \in [0, 1]^{d \times m}$, we have $\|f(\mathbf{X}) - f(\mathbf{X}')\|_p \leq L\|\mathbf{X} - \mathbf{X}'\|_p$. Furthermore, given functions $f_1, f_2$, the approximation error under a $p$-norm (which is entry-wise) is measured as:

$$d_p(f_1, f_2) = \left( \int \|f_1(\mathbf{X}) - f_2(\mathbf{X})\|_p^p d\mathbf{X} \right)^{1/p}.$$  

(5)

Primarily, we show that there exists a Transformer network $g \in T^{2,1,4}$ such that for any $f \in F_L$, prompt tuning on $g$ can approximate this function upto some error budget $\epsilon > 0$.

**Theorem 1.** Let $1 \leq p < \infty$ and $\epsilon > 0$, there exist a transformer network $g \in T^{2,1,4}$ and prompt length $m_p$, such that for any $f \in F_L$ we can find a prompt $\mathbf{P} \in \mathbb{R}^{d \times m_p}$ with $d_p(g([\mathbf{P}, \cdot]; m_p, f)) \leq \epsilon$.

Here we use the transformer in an encoder mode which generates the $m$ outputs in one step. In Appendix C.4 a similar result can be obtained for next-token prediction, which is widely used in many recent language models.

The proof is inspired from [Yun et al. 2019a], which follows the typical construction based proof mechanism to show universality. Thereby, we can construct a “meta-transformer” for prompt tuning to approximate any sequence-to-sequence function with prompt tuning. Next we briefly describe the two steps for the construction of this meta-transformer. We start by building a meta-function for $F_L$.

**Building the Meta-Function** We denote the length of all inputs as $m$ and the prompt length as $m_p$. Then we can build a sequence-to-sequence meta-function that accepts inputs with length $m + m_p$.

**Lemma 1.** For the sequence-to-sequence function space $F_L$ with functions $f : [0, 1]^{d \times m} \rightarrow [0, 1]^{d \times m}$, we can build a sequence-to-sequence function $\tilde{g} : [0, 1]^{d \times (m_p + m)} \rightarrow [0, 1]^{d \times (m_p + m)}$ such that for any $f \in F_L$, we can find $\mathbf{P} \in \mathbb{R}^{d \times m_p}$ with $d_p(\tilde{g}([\mathbf{P}, \cdot]; m_p, f)) \leq \epsilon/2$.

The complete proof is given in Appendix C.1. Succinctly, we first quantize the input and output sequence space of $[0, 1]^{d \times m}$ into a grid $G_{\delta, m} = \{0, \delta, 2\delta, ..., 1 - \delta\}^{d \times m}$, thus leading to $C' = \frac{1}{\delta^{d \times m}} m^{1 \times m}$ possible functions mappings from the input to the output, in this discrete space. By
this quantized function space as $F_L = \{ \bar{f}_1, \bar{f}_2, ..., \bar{f}_C \}$, we can select $\delta$ such that the approximation error for any function is less than $\epsilon/2$. Then we construct a set of quantized prompts in $G_{\delta,m} = \{0, \delta, 2\delta, ..., 1 - \delta\}^{d \times m_p}$ to index these $C$ functions and construct a quantized function $\bar{g}$ where $\bar{g}(\{\bar{P}_i, \bar{X}_i\})_{i=1,2,...,C} = \bar{f}_i(\bar{X}_i)$, $i = 1, 2, ..., C$, for all $\bar{X}_i \in G_{\delta,m}$, thereby concluding the lemma.

Next we can utilize some conclusions in [Yun et al., 2019a] to construct a transformer for $\bar{g}$.

**Constructing the Meta-Transformer** We first introduce a useful lemma which enables the construction of a transformer for any quantized sequence-to-sequence function.

**Lemma 2.** For any given quantized function $\bar{f} : [0, 1]^{d \times m} \rightarrow [0, 1]^{d \times m}$ with quantization at interval $\delta$, $\exists \bar{h} \in T^{2,1,1}$ such that $\bar{f} = \bar{h}$ with positional embedding $E = \begin{bmatrix} 0 & 1 & 2 & \ldots & m - 1 \\ 0 & 1 & 2 & \ldots & m - 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & 2 & \ldots & m - 1 \end{bmatrix}$.

The proof mainly follows the discussions in Section C of [Yun et al., 2019a]. To prove this lemma, the network $\bar{h}$ can be constructed in the following three steps. We first use a series of MLP layers to quantize the input to grid $[0 : \delta : 1 - \delta]^{d \times m}$ and then a series of attention layers to obtain a unique contextual mapping for each quantized input. Finally we can use a series of MLP layers to map the unique contextual mapping to the desired outputs. While a transformer network usually stacks self-attention and MLP layers alternately within a single layer, the aforementioned construction can be trivially attained via the use of skip connections. The complete proof of Lemma 2 is deferred to Appendix C.2.

Since $\bar{g}$ is a quantized function in grid $G_{\delta,m+m_p}$, following Lemma 2 we can find a modified version of transformer $\bar{h} \in T^{2,1,1}$ such that $\bar{g}(\{\bar{P}, \bar{X}\}) = \bar{h}(\{\bar{P}, \bar{X}\})$. The modified version of function $\bar{g}$ with hardmax operators can then be approximated with a standard transformer $g$ with softmax operators by Lemma 3.

**Lemma 3 (Lemma 9 in [Yun et al., 2019a]).** For each $\bar{h} \in T^{2,1,1}$, $\epsilon > 0$ and $1 \leq p < \infty$, $\exists g \in T^{2,1,1}$ such that $d_p(h, g) \leq \epsilon/2$.

Since the approximation error can be treated uniformly amongst the $\bar{P}_i$, we have that $d_p(\bar{h}(\{\bar{P}_i, \cdot\})_{i=1,2,...,m_p}, g(\{\bar{P}_i, \cdot\})_{i=1,2,...,m_p}) \leq d_p(\bar{h}(\{\bar{P}_i, \cdot\}), g(\{\bar{P}_i, \cdot\})) \leq \epsilon/2$. Therefore, we can build a transformer $g \in T^{2,1,1}$, such that for any sequence-to-sequence $f \in F_L$, we can find a quantized version $\bar{f}_i \in F_L$ and the corresponding prompt $\bar{P}_i \in G_{\delta,m_p}$ such that

$$d_p(g(\{\bar{P}_i, \cdot\})_{i=1,2,...,m_p}, f) \leq d_p(\bar{g}(\{\bar{P}_i, \cdot\})_{i=1,2,...,m_p}, \bar{h}(\{\bar{P}_i, \cdot\})) + d_p(\bar{h}(\{\bar{P}_i, \cdot\})_{i=1,2,...,m_p}, \bar{f}_i) + d_p(\bar{f}_i, f) \leq \epsilon.$$  

Theorem 1 provides the construction for a large transformer (discussed more in appendix) that is sufficient for prompt tuning to exhibit universal approximation over a Lipschitz function space. However, even this strong transformer also has limitations with prompt tuning when the target function $f \notin F_L$. Is this an essential limitation for prompt tuning on any transformer? In the next section, we will theoretically analyze the limitations of prompt tuning with transformers and target functions under more general conditions.

## 5 Limitations of Prompt-Tuning: Single Layer Transformer

To analyze the failure modes and therefore the limitations under the setting where a transformer has fixed pretrained weights, we follow the lens of exact memorization in the subsequent sections.

**Definition 3 (Memorization of a Sequence-to-Sequence Dataset).** Given a sequence-to-sequence dataset $S = \{(X_1, Y_1), ..., (X_n, Y_n)\}$ where $X_i, Y_i \in \mathbb{R}^{d \times m}$ are the input/output sequences, we consider a function $f$ exactly memorizing dataset $S$ if $f(X_i) = Y_i$. In the following proofs of this section, we explicitly focus on the last output token, i.e., $f(X_{1:-1})_{-1} = (Y_{1:-1})_{-1}$.

We start from the analysis on a single layer transformer and extend to multi-layer settings in Section
5.1 Failure modes of Prompt Tuning

It is straightforward to note that prompt tuning has limited expressive power when the number of trainable parameters is limited. A natural question to then ask is: Does increasing the number of trainable prompt tokens suffice? While it is known that for MLPs, even with a single hidden layer, increasing the number of hidden neurons can memorize any training data [Yun et al., 2019b]. However, as we will prove next, this is not the case for prompt tuning. This result highlights an essential limitation of prompt tuning compared to model fine-tuning.

Before providing the theorem statement, we first outline some straightforward assumptions on the pretrained transformer and datasets, without which prompt tuning trivially loses expressive power.

We consider sequence-to-sequence datasets of the form \( S = \{ (X_1, Y_1), (X_2, Y_2), \ldots, (X_n, Y_n) \} \) with \( n \) distinct examples and a single-layer single-head standard transformer defined in Definition 2. The results can be directly extended to the single-layer multi-head scenario, which we skip here to avoid notational clutter.

**Assumption 1** (Non-trivial conditions). We assume that all output tokens \((Y_i)_{i,k} \) are in the range set of MLP, otherwise the expressivity becomes trivially weak. We assume that \( W_q, W_k, W_v \) are full rank matrices and that \( \text{Att}(X_i, X_i) + X_i \) are distinct for \( i = 1, 2, \ldots, n \).

**Assumption 2** (Assumption for the MLP layer). We assume that \( d \geq 2 + \delta \text{dim}(\text{MLP}^{-1}(y_{10})) \cup \text{MLP}^{-1}(y_{20})) \) for the dataset constructed in Theorem 2 and token dimension \( d \). \( \delta \text{dim}(S) \) measures the dimension of subspace spanned by vectors in a set \( S \) and \( \text{MLP}^{-1}(y) = \{ x : \text{MLP}(x) = y \} \).

We provide an example for this assumption in Example 1 and a sufficient condition in the following Lemma 4.

**Lemma 4.** If \( \| W_1 \|_2 \times \| W_2 \|_2 < 1 \), where \( \| \cdot \|_2 \) is the matrix spectral norm, then the MLP block in Definition 2 is invertible, i.e., \( \text{MLP}^{-1} \) is a singleton set.

Therefore, if Lemma 4 holds and \( d \geq 4 \), Assumption 2 also holds.

Proof of Lemma 4 can be found in Appendix C.5. The experimental evidence in [Dong et al., 2021] shows that for most architectures, the norm of the weight matrices indeed admits small values and thus the requirement that \( \| W_1 \|_2 \times \| W_2 \|_2 < 1 \) is a mild condition.

With these assumptions, here we introduce our first theorem on the unlearnability of prompt tuning.

**Theorem 2.** For a single layer transformer \( \tau \) defined above with Assumptions 1 and 2, we can build a sequence-to-sequence dataset \( S = \{ (X_1 = [x_1, x_0], Y_1 = [y_{11}, y_{10}]), (X_2 = [x_2, x_0], Y_2 = [y_{21}, y_{20}]) \} \), and we cannot find a prompt \( P \in \mathbb{R}^{d \times m_p} \) with any \( m_p > 0 \) such that \( \tau([P, X_1]) = Y_i \) holds for any \( i = 1, 2 \). The vectors \( x_0, x_1, x_2 \) are denoted post positional encodings.

An important feature of this dataset is that the same token \( x_0 \) is shared between the two examples, and the expressive capability of prompt tuning is limited by the correlation of outputs corresponding to this token in different examples. We show a concrete example here to illustrate this theorem (note that Lemma 4 is in fact not required in the following construction) and defer the formal proof to Appendix C.6.

**Example 1.** We consider a single-head transformer layer \( \tau \), where \( b_1 = b_2 = 0 \), \( W_1 = 1^{r \times d} \), \( W_2 = 1^{d \times r} \). Then the token-wise MLP layer is a concatenation of two linear functions:

\[
\text{MLP}(x) = \begin{cases} 
(W_2W_1 + I)x, & (W_1x)_0 > 0 \\
 x, & (W_1x)_0 \leq 0
\end{cases}
\]

Here \((W_1x)_0\) denotes the first element of vector \( W_1x \).

\( W_2W_1 + I \) is a non-singular matrix. Therefore, for any \( y \) in \( \text{MLP}(X) \)’s output set, \( \text{MLP}^{-1}(y) \) contains at most two points \( \{ y, (W_2W_1 + I)^{-1}y \} \). We arbitrarily choose \( x_0, y_{10} \) and \( y_{20} \).

As long as \( d \geq 6 \) (from Assumption 2), we can find \( c_1, c_2 \) such that \( c_1, c_2 \perp y_{10} - x_0, y_{20} - x_0, (W_2W_1 + I)^{-1}y_{10} - x_0, (W_2W_1 + I)^{-1}y_{20} - x_0 \), \( \text{Att}(x_0, X_1) \| c_1 \) and \( \text{Att}(x_0, X_2) \| c_2 \) (Lemma 7 in Appendix). Then \( \text{Cone}(\text{Att}(x_0, X_1), a - x_0) \cap \text{Cone}(\text{Att}(x_0, X_2), b - x_0) = \emptyset \), for any \( a \in \{ y_{10}, (W_2W_1 + I)^{-1}y_{10} \} \) and \( b \in \{ y_{20}, (W_2W_1 + I)^{-1}y_{20} \} \). Here \( \text{Cone} \) stands for a convex cone as defined in Section 3.1.
If a $P$ exists such that $\tau([P,X_1]) = Y_1$ holds for both $i = 1, 2$, then we have

$$\text{Att}(x_0, [P, X_1]) = \lambda(X_1, x_0, [P, X_1])\text{Att}(x_0, X_1) + \lambda(P, x_0, [P, X_1])\text{Att}(x_0, P)$$

(8)

$$\text{Att}(x_0, [P, X_2]) = \lambda(X_2, x_0, [P, X_2])\text{Att}(x_0, X_2) + \lambda(P, x_0, [P, X_2])\text{Att}(x_0, P)$$

where $\lambda(\cdot, \cdot, \cdot)$ is a positive scalar. We also have

$$\text{Att}(x_0, [P, X_1]) + x_0 \in \text{MLP}^{-1}(y_{10})$$

$$\text{Att}(x_0, [P, X_2]) + x_0 \in \text{MLP}^{-1}(y_{20})$$

as $\text{MLP}(\text{Att}(x_0, [P, X_1]) + x_0) = y_{i0}, i = 1, 2$.

Therefore, $\text{Att}(x_0, P)$ must be in both $\text{Cone}(a - x_0, -\text{Att}(x_0, X_1))$ and $\text{Cone}(b - x_0, -\text{Att}(x_0, X_2))$, where $a \in \{y_{10}, (W_2W_1 + I)^{-1}y_{10}\}$ and $b \in \{y_{20}, (W_2W_1 + I)^{-1}y_{20}\}$, which contradicts the existence of $P$ as $\text{Cone}(-\text{Att}(x_0, X_1), a - x_0) \cap \text{Cone}(-\text{Att}(x_0, X_2), b - x_0) = \emptyset$. Therefore, in this example, even though we allow an arbitrary number of trainable parameters in prompt $P$, we cannot find one to exactly memorize the training set with only two training examples.

This theorem reveals an important difference between prompt tuning and adjusting the model weights directly. For any training dataset $S$ with two training examples $\{(X_1, Y_1), (X_2, Y_2)\}$, so long as $\text{Att}(X_1, X_1) + X_1$ and $\text{Att}(X_2, X_2) + X_2$ are distinct, MLP can easily map the post-attention features to expected output tokens with finite number of hidden neurons. As a result, tuning the MLP parameters for this pretrained transformers can memorize any dataset in the form of Assumption 1. However, prompt tuning cannot achieve this even if the number of tunable tokens $\rightarrow \infty$, thereby limiting the expressiveness of prompt tuning when compared to model fine-tuning.

### 5.2 Comparison with a More General Dataset

In Section 5.1, we constructed sequence-to-sequence datasets that cannot be learned by a given transformer layer with prompt tuning, by utilizing the shared token between different training examples. In this section, we compare the expressive power of prompt tuning and fine-tuning under a more general dataset construction where the former requirement can be relaxed.

Since the primary essence of prompt tuning is to perform parameter-efficient tuning, wherein we seek to adapt a pretrained large model to a new task with fewer tunable parameters, we compare prompt tuning with another parameter-efficient version of model-tuning: LoRA [Hu et al., 2021]. Succinctly, we compare the required number of parameters to memorize a given dataset. Again, consider a sequence-to-sequence dataset $S = \{(X_1, Y_1), (X_2, Y_2), \ldots, (X_n, Y_n)\}$, where $X_i = [x_{i1}, x_{i2}, \ldots, x_{imi}]$ and $Y_i = [y_{i1}, y_{i2}, \ldots, y_{imi}]$. We again discuss the memorization of the last output token for simplicity and results can be directly extended.

We first give the required number of parameters of LoRA to memorize dataset $S$.

**Lemma 5** (LoRA). For a standard single-layer transformer $\tau$ defined in Definition 2 with $r \geq n$ MLP hidden neurons, for any sequence-to-sequence dataset $S$ satisfying Assumptions 1, we can apply a low-rank update to MLP weights with $O(nd)$ parameters to memorize $\tau(X_i)_{im} = y_{im}$.

This lemma is derived based on the memorization capabilities of 1-hidden layer MLPs [Yun et al., 2019b]. As the post-attention values for different training inputs are different from Assumption 1, we can construct a low rank update with $O(nd)$ parameters on the MLP layer to memorize $S$. We defer the complete proof to Appendix C.7.

For prompt tuning, we derive a result in the next theorem which shows that it requires $\Omega(nd)$ tunable parameters to memorize some constructed dataset $S$ with $n$ examples.

**Theorem 3** (Lower bound on Tunable Prompt Parameters). For any single layer transformer $\tau$ defined in Definition 2 there exists a sequence-to-sequence dataset $\{(X_1 = [x_{10}, x_1], [y_{10}, y_{11}]), (X_2 = [x_{20}, x_2], [y_{20}, y_{21}]), \ldots, (X_n = [x_{n0}, x_n], [y_{n0}, y_{n1}])\}$ that satisfies Assumption 1 with $n < d$ training examples such that we need at least $n$ prompt tokens in $P$ to memorize the training set, i.e., for $\tau([P, X_1])_{im} = y_{im}$ to hold for all $i = 1, 2, \ldots, n$.

This dataset can be constructed by including $n$ examples that require $n$ linearly independent prompts tokens. The complete proof is deferred to Appendix C.8.
Note that in Theorem 3, we provide a key lower bound on the required number of prompt tokens for exact memorization and this can very well more than $nd$. This partially (but not necessarily) explains the worse empirical performance of prompt tuning against LoRA under a comparable number of trainable parameters.

6 Extension to Multi-Layer Setting

In this section, we extend our analysis to multi-layer setting and provide a sufficient condition under which the expressiveness of prompt tuning is restricted. An immediate consequence of our result is an interesting connection to the spectral norm of soft prompts surfaces. This result provides us a partial understanding of the phenomenon that soft prompt vectors typically exhibit larger norms compared to the actual input $X$, after the tuning.

With some further notation adjustments, we denote an $H$ layer pretrained transformer network as $g \in \mathcal{T} = \tau_1 \circ \tau_2 \circ ... \circ \tau_H$, the input set as $\mathcal{X}^1$, and the set of possible prompts as $\mathcal{P}^1$. We assume that the following compactness condition is satisfied:

$$
\|[[P_l, X_l]]_2 \leq D_l
$$

s.t. $[P_{l+1}, X_{l+1}] = \tau_l([P_l, X_l]), \forall l = 1, ..., H.$

Here $[P_1, X_1]$ is the input to the first layer $\tau_1$ with $P_1 \in \mathcal{P}^1, X_1 \in \mathcal{X}^1$ and $\| \cdot \|_2$ is the spectral norm. Similarly, $[P^{H+1}, X^{H+1}]$ denotes the output set.

We start by providing an upper bound to the Lipschitz constant of attention, pertaining to eq 9. This derivation is different from the works of [Dasoulas et al., 2021, Vuckovic et al., 2020] and thus can be of independent interest.

Lemma 6. Under the compactness condition, the Lipschitz constant of the $i$-th attention head in the $l$-th transformer layer, denoted for simplicity as $\text{Att}_{i,l}$, admits the following bound w.r.t the entire input sequence of length $m$:

$$
\text{Lip}(\text{Att}_{i,l}(\cdot, \cdot)) \leq (1 + 8\sqrt{m}(D_l)^2\| \langle W_{k}^{i,l} \rangle_T \|_{2} \| W_{q}^{i,l} \|_{2})\| W_{v}^{i,l} \|_{2},
$$

and the Lipschitz constant of the entire attention block in layer $l$, denoted as $\text{Att}_l$, admits the bound:

$$
\text{Lip}(\text{Att}_l(\cdot, \cdot)) \leq \sqrt{\sum_{i=1}^{h}(\| W_{o}^{i,l} \|_{2} \times \text{Lip}(\text{Att}_{i,l})^2)}.
$$

It is noteworthy that this upper bound is dependent on $D_l$, the spectral norm of the input prepended with the prompt. In conjunction with the following theorem, we obtain a result on limited expressivity of prompt tuning by showing that the transformer becomes invertible, in consideration to functions from $\mathcal{P}^1 \times \mathcal{X}^1 \to \mathcal{P}^{H+1} \times \mathcal{X}^{H+1}$ (an extension to functions of the from $\mathcal{X}^1 \to \mathcal{X}^{H+1}$ is provided in Appendix Section C.11).

Theorem 4. A transformer $g \in \mathcal{T}$ is invertible, ie, $g^{-1}(Y) = \{X : g(X) = Y\}$ is a singleton set $\forall Y$ in range of $g$, if:

1. The Lipschitz constant of the attention block in each layer $\tau_i$ is strictly less than 1
2. The Lipschitz constant of the 2-layer ReLU block in each layer $\tau_i$, which is bounded by $\| W_2^{i,l} \|_{2} \times \| W_1^{i,l} \|_{2}$, is strictly less than 1.

Proof of Theorem 4 can be found in Appendix C.9. Combining Lemma 6 and Theorem 4, we observe that the invertibility is guaranteed if the upper bound for the Lipschitz constant of the attention, eq 11, and the MLP layer, is strictly less than 1. In this case, we can then construct arbitrarily many datasets where two different inputs share the same output, and prompt tuning cannot learn (more subtly: memorize) these datasets with a restricted prompt norm.
7 Experiments

7.1 Experimental Settings

In Section 7.2, we use a standard single-layer single-head transformer from Definition 2 to justify the infinite prompt-length limitation. In Section 7.3, we justify the increasing prompt norm on the pretrained LLaMA 7B model \cite{touvron2023hight}. For prompt tuning and LoRA, we use the Huggingface Peft library \cite{mangrulkar2022peft}. On the dataset front, we utilize the RTE subtask of SuperGlue dataset \cite{wang2019superglue} and WMT14 En-Fr translation \cite{bojar2014wmt}. More details and hyperparameter settings can be found in Appendix A.

7.2 Limited Expressivity of Infinite Length Prompt

We first construct the dataset following the proof of Theorem 2 and then show that prompt tuning cannot memorize this simple dataset \{(X_1 = [x_1, x_0], Y_1 = [y_{11}, y_{10}]), (X_2 = [x_2, x_0], Y_2 = [y_{21}, y_{20}])\} even with very large prompt lengths.

We set the token dimension \(d = 10\). We follow the default pytorch weight initialization and then normalize \(W_1, W_2\) such that \(\|W_2\|_2 \times \|W_1\|_2 < 1\), following Assumption 2. We randomly sample \(x_0, y_{10}, y_{20}\) in a uniform distribution in \([0, 1]^d\) and construct the corresponding vectors: \(x_1\) and \(x_2\) following Theorem 2. To compute \(\text{MLP}^{-1}(y)\), we follow \cite{kim2021mlp} Section 4.1 with 5000 iterations at convergence. We solve \(\text{Att}(x_0, [x_0, x_1]) \cdot c\) in Lemma 7 with gradient descent terminating at \(\langle\text{Att}(x_0, [x_0, x_1]), c\rangle < 0.0001\). We repeat this setup to obtain 3 different datasets for distinct \(x_0, y_{10}, y_{20}\) and denote these with \(S_i, i = 1, 2, 3\).

We perform prompt tuning, MLP fine-tuning and MLP LoRA training on the constructed datasets for 5 runs and report the mean and standard deviation of per-element Mean Squared Error (MSE) loss \(y_{10}, y_{20}\) at convergence. We show the comparison between prompt-tuning and MLP fine-tuning in Figure 1. As we can observe from the figure, increasing the number of soft prompt tokens post a certain threshold that does not exhibit any reduction in MSE. On the contrary, fine-tuning on the MLP layer tends to easily memorize the training set by reducing the training loss to almost zero (all the three curves for fine-tuning overlap and thus not differentiated). Note that we plot the standard deviation, however it is negligible in the range. Similar to fine-tuning on the MLP layer, LoRA with width 2 on the MLP layer also achieves near-zero training loss which is less than \(10^{-10}\) on the constructed dataset. We don’t plot the comparison on Figure 1 as all the six curves are overlapped. This result validates our Theorem 3 that LoRA can memorize a dataset with \(n\) examples with trainable parameters \(O(n)\) while prompt-tuning may require more.

7.3 Increasing Prompt Spectral Norm during Tuning

As discussed in Section 6, a major constraint on the expressive power of prompt tuning is the spectral norm of soft prompts. In Figure 2, we plot the curve for spectral norm of soft prompt as training progresses and the loss reduces on RTE dataset. The curve for WMT14 En-Fr dataset can be found in Appendix B. This trend clearly highlights that in order to counter the limit on the capacity, the spectral norm consistently increases till the training loss saturates.

8 Conclusions

In this work, we embark on exploring the capabilities of prompt tuning in the continuous regime, contrasting it with fine-tuning, as an initial endeavor towards a theoretical comprehension. We prove by construction that prompt tuning admits universal approximation within the space of Lipschitz functions. Additionally, we identified inherent limitations of prompt tuning on single-layer transformers by constructing theoretically difficult datasets for prompt tuning. These limitations are then extended to multi-layer setting under a specific prompt-norm restriction.

From the analysis in Theorem 2 and 3, we note that the limitation of prompt-tuning primarily arises from the correlation across different inputs. Broadly describing, prompt-tuning implements transformation on different inputs via “additional attention values”, which is more restrictive as compared to the transformations from MLP layers on input tokens. An interesting potential direction to improve prompt-tuning is: “designing a mechanism to leverage prompting in order to generate...
Figure 1: MSE losses at convergence for the 3 constructed datasets (following Theorem 2). We plot the bold curves with increasing prompt length in prompt tuning and dashed fixed lines in fine-tuning (all three datasets overlapping).

Figure 2: Increasing prompt spectral norm during tuning on SuperGlue RTE dataset.

We expect to have some future work focusing on designing novel prompt-tuning strategies along this direction.

Limitations While our results provide valuable insights, extending the construction in Theorem 2 to multiple layers and deriving tighter bounds for Lemma 6 are critical steps for a deeper understanding of the limitations of prompt tuning.

Acknowledgments and Disclosure of Funding

We thank the reviewers for their invaluable feedbacks. The work is supported in part by NSF 2008173, 2048280, 2325121, 2331966, ONR N00014-23-1-2300:P00001.

References


A  Experimental Details

All the experiments are run on a NVIDIA RTX A6000 GPU. For experiments with Llama 7B model, we use batch size 32 and learning rate 0.001. For experiment on WMT14 En-Fr translation, we only compute the loss on the first 100 examples for computational efficiency.

We use Adam optimizer and optimal learning rate from grid search at 0.1 for prompt-tuning and at 0.001 for fine-tuning in Section 7.2.

In Section 7.3, we use the default loss function in Huggingface implementation for causal language models. We use prompt length $m = 10$ and the prompt tokens are initialized as the first $m$ tokens in the model vocabulary.

B  Additional Experiments

As mentioned in Section 7.3, the second real world dataset used in our experiment is WMT14 En-Fr translation in order to illustrate that the spectral norm of soft prompts increases during training. We show the curve in Figure [B].

C  Proof of Lemmas and Theorems

C.1  Proof of Lemma 1

For the sequence-to-sequence function space $\mathcal{F}_L$ with functions $f : [0, 1]^{d \times m} \rightarrow [0, 1]^{d \times m}$, we can build a sequence-to-sequence function $\tilde{g} : [0, 1]^{d \times (m_p + m)} \rightarrow [0, 1]^{d \times (m_p + m)}$ such that for any $f \in \mathcal{F}_L$, we can find $P \in \mathbb{R}^{d \times m_p}$, $d_p(\tilde{g}([P, \cdot])_{i, m_p}, f) \leq \epsilon / 2$.

Proof. we first quantize the input and output sequence space of $[0, 1]^{d \times m}$ into a grid space $G_{\delta, m} = \{0, \delta, 2\delta, \ldots, 1 - \delta\}^{d \times m}$, which leads to $C = \left(\frac{1}{\delta \times m}\right)^{d \times m}$ functions considering all input and output mappings in this grid. We index these $C$ functions as $\tilde{F}_L = \{\tilde{f}_1, \tilde{f}_2, \ldots, \tilde{f}_C\}$. For $X \notin G_{\delta, m}$, we let $\tilde{f}_i(X) = \tilde{f}_i(X^*)$ if $k_{i,j} \leq (k_{i,j} + 1)\delta$ and $X^* \in G_{\delta, m}$.

Then for any $f \in \mathcal{F}_L$, we can find a function $\tilde{f} \in \tilde{F}_L$ such that $d_p(\tilde{f}, f) = (\int ||\tilde{f}(X) - f(X)||_p^p dX)^{1/p} \leq (\int L^{pmd\delta^p} dX)^{1/p} = (L(md)^{1/p} \delta$. We choose $\delta = \delta_1$ such that $L(md)^{1/p} \delta \leq \epsilon / 2$.

For the prompt part, we choose $m_p$ such that $\frac{mc}{m_p} \geq C$. Then we can build a set of quantized prompts in $G_{\delta, m_p} = \{0, \delta, 2\delta, \ldots, 1 - \delta\}^{d \times m_p}$ to index these $C$ functions. We denote this set of prompts as $\{P_1, P_2, \ldots, P_C\}$. Finally we can create the quantized function $\tilde{g}$ and let
For any $\overline{\bar{P}} \in \mathbb{R}^{d \times m_P}$, we set $\overline{\bar{g}}(\overline{\bar{P}}, X) = \overline{\bar{g}}(\overline{\bar{P}}^*, X)$ if $k_{i,j} \delta < \bar{P}_{i,j}, \bar{P}_{i,j} \leq (k_{i,j} + 1) \delta$ and $\overline{\bar{P}}^* \in G_{\delta, m_P}$.

Therefore, with a properly chosen $\delta = \delta_1$, for any $f \in \mathcal{F}_L$, we can find $\overline{\bar{P}} \in \mathbb{R}^{d \times m_P}$ such that $d_p(f, \overline{\bar{g}}(\overline{\bar{P}}, \cdot)) = d_p(f, f) \leq \epsilon/2$. \hfill $\square$

### C.2 Proof of Lemma 2

For any given quantized function $\bar{f} : [0, 1]^{d \times m} \rightarrow [0, 1]^{d \times m}$ with quantization at interval $\delta$, $\exists \bar{h} \in \mathbb{T}^{2,1,1}$ such that $\bar{f} = \bar{h}$ with positional embedding $E = \begin{pmatrix} 0 & 1 & 2 & \cdots & m - 1 \\ 0 & 1 & 2 & \cdots & m - 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & 2 & \cdots & m - 1 \end{pmatrix}$

**Proof.** The proof is given following Section C in [Yun et al., 2019a] appendix. With Section C.1 in [Yun et al., 2019a], there exists a function $g_q$ composed of $\frac{m}{\epsilon^2}$ token-wise feed-forward layers with hidden layer size $r = 1$ and ReLU activation to implement this scalar quantization on each input element:

$$g_q^{ent}(t) = \begin{cases} k\delta & \text{if } k\delta \leq t < (k + 1)\delta, k = 0, 1, ..., \frac{m}{\delta} - 1 \\ -\delta^{-md} & \text{otherwise} \end{cases}$$

Then with Section C.2 in [Yun et al., 2019a], we can stack $m(1/\delta)^d + 1$ attention layers to map all possible input sequences in grid $[0 : \delta : 1 - \delta]^d \times [1 : \delta : 2 - \delta]^d \times \cdots \times [m - 1 : \delta : m - \delta]^d$ to distinct numbers which are at least $\delta$ from each other.

Finally we only require $O(m(1/\delta)^d m)$ layers to map these distinct numbers to expected outputs. \hfill $\square$

### C.3 Proof of Lemma 3

Lemma 3 is almost the same as [Yun et al., 2019a] except that we use $\epsilon/2$ instead of $\epsilon/3$.

### C.4 Extension of Theorem 1 to Next-token Predictors

As an extension of Theorem 1, we consider approximating a set of sequence-to-sequence functions when we use a transformer layer as a next-token predictor. We consider a set of sequence-to-sequence functions $\mathcal{F}_L$ with Lipschitz constant $L$ under norm $p$. $f \in \mathcal{F}_L : [0, 1]^{d \times m_1} \rightarrow [0, 1]^{d \times m_2}$ accepts an input of length $m_1$ and outputs a sequence of length $m_2$. For any $X, X' \in [0, 1]^{d \times m_1}$, we have $\|f(X) - f(X')\|_p \leq L\|X - X'\|_p$.

Next we show that we can construct a transformer $\tau$ which can approximate any $f \in \mathcal{F}_L$ with prompt-tuning when we use it as a next-token predictor.

**Theorem 5.** For any $f \in \mathcal{F}_L$, we can construct a transformer $\tau$ such that for any $f \in \mathcal{F}_L$, $1 \leq p < \infty$ and $\epsilon > 0$, we can find a prompt $P \in [0, 1]^{d \times m_P}$ such that $d_p(f, h(P)) \leq \epsilon$, where

$$h(P) = \tau_1([P, \cdot])_{:-1} \times \tau_2([P, \cdot])_{:-1} \times \cdots \times \tau_{m_2}([P, \cdot])_{:-1}.$$  

$\tau_{i}$ is the sequence-to-sequence function implemented with the transformer $\tau$ when accepting sequences with length $m_p + m_1 + i$.

**Proof.** Similar to Theorem 1, we quantize the inputs to grid of $[0 : \delta : 1 - \delta]$ with interval $\delta$ and set $m_p = (\delta d \times m_2\delta d \times m_1)$. $\delta$ is chosen such that $L(m_1d)^{1/p} \epsilon \leq m_2^{-1/p} \epsilon$. We index the $C = (\delta d \times m_2\delta d \times m_1)$ different $f$s as $f^1, f^2, ..., f^C$ and its sub-function to generate the $i$-th output token as $f_i^1$. The $C$ sequence-to-sequence functions can then be indexed by $C$ distinct prompts. Similar to Lemma 2, we can construct a transformer which can map all possible input sequences in grids $[0 : \delta : 1 - \delta] \times \cdots \times [m - 1 : \delta : m - \delta]^d$, $0 < m \leq m_1 + m_2 + m_p - 1$ to distinct numbers. A final series of MLP layers then map these distinct numbers to desired output vectors where inputs
in the same grid are mapped to the same output token at each step. Then for any input \( x \in [0, 1]^{d \times m_1} \) and any \( f^j \), we can find a prompt \( P_j \) such that

\[
\| \tau([P_j, x]_0, \cdots, \tau([P_j, x]_0, \cdots) \|_p \leq m_2^{-1/p} \epsilon
\]

Then we have \( d_p(h(P_j), f^j) \leq \epsilon \).

\[\square\]

C.5 Proof of Lemma 4

If \( \|W_1\|_2 \times \|W_2\|_2 < 1 \), where \( \| \cdot \|_2 \) is the matrix spectral norm, then the MLP block in Definition 2 is invertible, i.e., MLP\(^{-1}\) is a singleton set.

**Proof.** Based on the sufficient conditions for invertibility of a residual block [Behrmann et al., 2019], we have that if the feedforward part of a residual block \( W_2\text{ReLU}(W_1X_1 + b_1) + b_2 \) is a contraction with respect to some metric, i.e., its Lipschitz constant \( \leq 1 \), and the metric space on which it is defined is complete, then MLP in eq (2) is invertible. Since we are dealing with the euclidean space, any metric induced by the \( \| \cdot \|_p \) norm for \( p \in [1, \infty) \) ensures the space is complete.

The Lipschitz constant of \( W_2\text{ReLU}(W_1x + b_1) + b_2 \) is simply \( \|W_1\|_2 \times \|W_2\|_2 \). Thus the statement of the lemma follows.

\[\square\]

C.6 Proof of Theorem 2

For a single layer transformer \( \tau \) defined above with Assumptions 1 and 2, we can build a seq-to-seq dataset \( \{(X_1 = [x_1, x_0], Y_1 = [y_{11}, y_{10}]), (X_2 = [x_2, x_0], Y_2 = [y_{21}, y_{20}])\} \), and we cannot find a prompt \( P \in \mathbb{R}^{d \times m_f} \) with any \( m_f > 0 \) such that \( \tau([P, X_i]) = Y_i \) holds for any \( i = 1, 2 \). The vectors \( x_0, x_1, x_2 \) are denoted post positional encodings.

**Proof.** Before proving Theorem 2 we first provide a lemma that will be used in proof and also Theorem 3.

**Lemma 7.** Given any \( c \in \mathbb{R}^{d \times m_f} \), there are \( x_0 \) almost anywhere for which we can find another vector \( x_1 \in \mathbb{R}^{d \times m_f} \) such that \( \text{Att}(x_0, [x_0, x_1]) \parallel c \) with full rank attention weights \( W_q, W_k, W_v \).

**Proof.** If \( W_vx_0 \parallel c \), we can just set \( x_1 = x_0 \), which makes \( \text{Att}(x_0, [x_0, x_1]) \parallel c \) hold.

If \( W_vx_0 \parallel c \), let \( v = \alpha c - W_vx_0 \) where \( \alpha \in \mathbb{R} \). As \( W_v \) is full-rank, we can find \( x \) such that \( x = W_v^{-1}v = \alpha W_v^{-1}c - x_0 \). Then we will have

\[
\text{Att}(x_0, [x_0, x_1]) = \frac{\exp((W_qx_0)^\top(W_kx_0))(W_qx_0) + \exp((W_qx_0)^\top(W_k(\alpha W_v^{-1}c - x_0)))(\alpha c - W_vx_0)}{\exp((W_qx_0)^\top(W_kx_0)) + \exp((W_qx_0)^\top(W_k(\alpha W_v^{-1}c - x_0)))}
\]

Therefore, as long as \( W_qx_0 \not\parallel W_k(\alpha W_v^{-1}c) \), we can change \( \alpha \) such that \( \text{Att}(x_0, [x_0, x_1]) = \beta W_vx_0 + (1 - \beta)(\alpha c - W_vx_0) \) where \( \beta = \frac{\exp((W_qx_0)^\top(W_kx_0)) + \exp((W_qx_0)^\top(W_k(\alpha W_v^{-1}c - x_0))))}{\exp((W_qx_0)^\top(W_kx_0)) + \exp((W_qx_0)^\top(W_k(\alpha W_v^{-1}c - x_0))))} \).

When \( \alpha = 0 \), \( \text{Att}(x_0, [x_0, x_1]) = W_vx_0 \) when \( \alpha \to -\infty \) or \( \alpha \to \infty \), \( \text{Att}(x_0, [x_0, x_1]) \to \alpha c - W_vx_0 \). As \( \text{Att}(x_0, [x_0, x_1]) \) is continuous w.r.t changing \( \alpha \), there must exist an \( \alpha \) such that \( \text{Att}(x_0, [x_0, x_1]) \parallel c \).

Pass the two input sequences \( X_1, X_2 \) through the attention layer \( \text{Att} \) with any prompt \( P \), we can get the last output token as:

\[
\text{Att}(x_0, [P, X_1]) = \lambda(X_1, x_0, [P, X_1])\text{Att}(x_0, [X_1]) + \lambda(P, x_0, [P, X_1])\text{Att}(x_0, P)
\]

\[
\text{Att}(x_0, [P, X_2]) = \lambda(X_2, x_0, [P, X_2])\text{Att}(x_0, [X_2]) + \lambda(P, x_0, [P, X_2])\text{Att}(x_0, P)
\]
Here $\lambda(x_1, x_2, X_3) = |X_1, X_2| \in (0, 1)$ is a positive scalar, defined as

$$
\lambda(x_1, x_2, X_3) = \frac{\sum_j \exp((W_k x_1)^T (W_q x_2))}{\sum_j \exp((W_k x_1)^T (W_q x_2))},
$$

$x_{ij}$ is the $j$th token in $X_i$ for notation simplicity.

1. Then from equation\[12\] $\text{Att}(x_0, P)$ must be on $\text{Cone}(-\text{Att}(x_0, X_1), \text{Att}(x_0, [P, X_1]))$ and $\text{Cone}(-\text{Att}(x_0, X_2), \text{Att}(x_0, [P, X_2]))$.

2. On the otherhand, as we want to memorize the two examples, we must have $\text{Att}(x_0, [P, X_1]) + x_0 \in \text{MLP}^{-1}(y_{10})$ and $\text{Att}(x_0, [P, X_2]) + x_0 \in \text{MLP}^{-1}(y_{20})$.

We construct the dataset $S$ with arbitrary $x_0, y_{10}$ and $y_{20}$. Then if $\dim(\text{MLP}^{-1}(y_{10}) - x_0) + \dim(\text{MLP}^{-1}(y_{20}) - x_0) + 2 \leq d$ (Assumption\[2\]), we can find two vectors $c_1, c_2$ such that $c_1, c_2 \perp v + x_0 \in \text{MLP}^{-1}(y_{10})$ or $v + x_0 \in \text{MLP}^{-1}(y_{20})$ and $c_1 \perp c_2$. Then we can choose $x_1, x_2$ such that $\text{Att}(x_0, X_1) \parallel c_1$ and $\text{Att}(x_0, X_2) \parallel c_2$ (Lemma\[7\]). Combine this construction with assumption\[1\] we have that $\text{Cone}(-\text{Att}(x_0, X_1), \text{Att}(x_0, [P, X_1]))$ and $\text{Cone}(-\text{Att}(x_0, X_2), \text{Att}(x_0, [P, X_2]))$ has no intersection, which means that we cannot find a $P$ to memorize this constructed dataset. □

### C.7 Proof of Lemma\[5\]

For a standard single-layer transformer $\tau$ defined in Definition\[2\] with $r \geq n$ MLP hidden neurons, for any sequence-to-sequence dataset $S$ satisfying Assumptions\[1\] we can apply a low-rank update to MLP weights with $O(nd)$ parameters to memorize $\tau(x_{i,:m} = y_{im}$.

**Proof.** We use $\text{MLP}_j(x)$ to denote the $jth$ output of the MLP layer for an input token $x$, which is

$$
\text{MLP}_j(x) = x_j + b_{2,j} + \sum_{k=1}^{m} w_{k,j} \max(\langle a_k, x \rangle + b_{1,k}, 0)
$$

According to our assumption, $\text{Att}(x_{im}, X_i)$ are unique vectors for $i = 1, 2, ..., n$. Then we only need to use the MLP layer to map each $x_i = \text{Att}(x_{im}, X_i) + x_{im}$ to $y_{im}$, where we get a new token-wise dataset $\{(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)\}$

Then we need to find $w_k, a_k$ and $b_k$ such that

$$
\text{MLP}_j(x_i) = x_{i,j} + b_{2,j} + \sum_{k=1}^{m} w_{k,j} \max(\langle a_k, x_i \rangle + b_{1,k}, 0) = y_{i,j}, i = 1, 2, ..., n, j = 1, 2, ..., d
$$

(14)

, which is equivalent to constructing a standard MLP to memorize a dataset:

$$
\sum_{k=1}^{n} w_{k,j} \max(\langle a_k, x_i \rangle + b_{1,k}, 0) = y_{i,j} - x_{i,j} - \sum_{k=n+1}^{m} w_{k,j} \max(\langle a_k, x_i \rangle + b_{1,k}, 0) - b_{2,j}
$$

(15)

Follow Theorem 1 in \[Yun et al., 2019b\], we can construct $a, b_1, ..., b_n$ such that for $x_1, x_2, ..., x_n$, we have $z_i = \langle a, x_i \rangle, b_1 < z_1 < b_2 < ... < b_n < z_n$. Then we can find $w_1, ..., w_n$ which solves equation\[15\]. For $d$-dimension output, we need to find $W \in \mathbb{R}^{n \times d}$ and $a \in \mathbb{R}^d$ and $b \in \mathbb{R}^n$.

With LoRA, we need a low-rank update of size $m \times n + n \times d$ for $W_2$, a low-rank update of size $d \times n + n \times m$ for $W_1$ and an update of size $n$ for $b_1$, which is $O(n \times d)$ in total. Normally we have $m \approx d$, then we need an update with parameter size around $(4n + 1)d$ to memorize the last token of $n$ training examples. □

### C.8 Proof of Theorem\[3\]

For any single layer transformer $\tau$ defined in Definition\[2\] there exists a seq-to-seq dataset $\{(x_1 = [x_{10}, x_{1}], [y_{10}, y_{11}]),(x_2 = [x_{20}, x_{2}], [y_{20}, y_{21}]),..., (x_n = [x_{n0}, x_{n}], [y_{n0}, y_{n1}])\}$ that satisfies Assumption\[1\] with $n < d$ training examples such that we need at least $n$ prompt tokens in $P$ to memorize the training set, i.e., for $\tau([P, X_i])_{-1} = y_{1i}$ to hold for all $i = 1, 2, ..., n$.  

17
Proof. Without loss of generality, we assume $W_2$ has no zero elements, otherwise we can just ignore this hidden neuron in MLP layer.

$\mathbb{R}^d$ has $d$ bases $\{t_j : j = 1, 2, ..., d\}$, then $\text{MLP}^{-1}(y_{i1})$ must be bounded on either positive or negative part of these $d$ directions, which means there exists $B \geq 0$ such that

$$\frac{\langle v^\top t_j \rangle}{\|t_j\|} \leq B, \forall v \in \text{MLP}^{-1}(y_{i1}), j = 1, 2, ..., d$$

Otherwise $\forall B > 0$, $\exists t_j$, we can find a $v \in \text{MLP}^{-1}(y_i)$ that $\frac{\langle v^\top t_j \rangle}{\|t_j\|} \geq B$. Meanwhile we have $\text{MLP}(v) = v + b_2 + W_2 \text{ReLU}(W_1 v + b_1)$. As $\|v\|$ can be arbitrarily large, if $W_1 v = 0$, $\|\text{MLP}(v)\| \to \infty$ if $\|v\| \to \infty$. If $W_1 v \neq 0$, $\|\text{MLP}(v)\|$ can also be arbitrarily large when increasing the norm of $v$ due to the non-linearity of $\text{ReLU}(W_1 v + b_1)$.

Then we can find a set of $n$ linearly independent vectors $\{c_1, c_2, ..., c_n\}$ such that $\{a_i : a_i \perp c_i \in \text{MLP}^{-1}(y_{i1})\} = \emptyset$ by enlarging the norm of $c_i$. With the $n$ $c_i$ vectors, we can begin to construct our dataset:

We set $x_i = c_i, i = 1, 2, ..., n$ and find $x_{i0}$ such that $c_i \perp \text{Att}(x_i, x_i)$ (Lemma 7) and $\text{Att}(x_i, X_i)$ are distinct for $i = 1, 2, ..., n$ (Assumption 1), which makes $\{a_1 - x_i - \lambda(X_i, x_i, P, X_i)\text{Att}(x_i, X_i), ..., a_n - x_i - \lambda(X_n, x_n, P, X_n)\text{Att}(x_n, X_n)\}$ linearly independent for any $a_i \in \text{MLP}^{-1}(y_{i1})$. Here $\lambda(\cdot, \cdot, \cdot)$ is the same as defined in Section C.6.

Moreover, we have

$$\text{Att}(x_i, [P, X_i]) = \lambda(X_i, [P, X_i])\text{Att}(x_i, P) + \lambda(X_i, x_i, [P, X_i])\text{Att}(x_i, X_i)$$

$$\in \text{MLP}^{-1}(y_{i1}) - x_i$$

Then $\text{Att}(x_i, P), i = 1, 2, ..., n$ must be $n$ linearly independent vectors, which requires

$$\text{rank}(W_o \text{PA}) = n,$$

where $A \in \mathbb{R}^{m_p \times n}$ is the attention score matrix between $x_i$ and $P$, $P \in \mathbb{R}^{d \times m_p}$ is the prompt token sequence and $W_o$ is the attention value weight. Therefore, we must have $m_p \geq n$.

\section*{C.9 Proof of Theorem 4}

A transformer $T$ is invertible if:

1. The Lipschitz constant of the attention block in each layer $\tau^l$ is strictly less than 1
2. The Lipschitz constant of the 2-layer ReLU block in each layer $\tau^l$, which is bounded by $\|W_2\|_2 \times \|W_1\|_2$, is strictly less than 1

\begin{proof}
This proof is based on the proof provided for lemma 7 thus we restrict ourselves to the sketch:

Based on the sufficient condition for invertibility in Behrmann et al. [2019], condition (1) implies that the attention block (eq 1) with the residual connection, i.e. $X + \text{Att}(X, X)$, is an invertible function. Similarly, condition (2) implies that the MLP block which constitutes of the 2-layer ReLU block with the residual connection (eq 2) also exhibit invertibility.

Thus each transformer layer $\tau^l$ (eq 3) is invertible by noting that its a composition of two invertible functions. The same property ensures that the entire transformer architecture $T$ is also invertible.
\end{proof}

\section*{C.10 Proof of Lemma 6}

Under the compactness condition, the Lipschitz constant of the $i$-th attention head in the $l$-th transformer layer, denoted for simplicity as $\text{Att}^{i,l}$, admits the following bound w.r.t the entire input sequence of length $m$:

$$\text{Lip}(\text{Att}^{i,l}(\cdot, \cdot)) \leq (1 + 8\sqrt{m}(D^l)^2 \|\text{Att}^{i,l}W_{i,l}^l\|_2)\|W_{i,l}^l\|_2,$$

and the Lipschitz constant of the entire attention block in layer $l$, denoted as $\text{Att}^l$, admits the bound:

$$\text{Lip}(\text{Att}^l(\cdot, \cdot)) \leq \sum_{i=1}^{h} (\|W_{i,l}^l\|_2 \times \text{Lip}(\text{Att}^{i,l}))^2.$$
Proof. We drop the superscripts $i, l$ in the proof to avoid notation clutter. Similarly, we denote the concatenation of the prompt matrix $P$ and the original input matrix $X$, simply with $X$.

Derivation for single head eq $[18]$
Consider two matrices $X_1, X_2 \in \mathcal{X} = \{X \in \mathbb{R}^{d \times m}; \|X\|_2 \leq D\}$. Denote with $A_1, A_2$ the corresponding attention matrices respectively, which can be defined as:

\[
    A_1 = \sigma \left((W_k X_1)^T W_q X_1 \right) \\
    A_2 = \sigma \left((W_k X_2)^T W_q X_2 \right)
\]

(20)

The output of the attention head, denoted with $\text{Att}()$ admits the following:

\[
    \|\text{Att}(X_1) - \text{Att}(X_2)\|_2 = \|W_c X_1 A_1 - W_c X_2 A_2\|_2
\]

(21)

\[
    \leq \|X_1 A_1 - X_2 A_2\|_2 \|W_c\|_2
\]

(22)

\[
    = \|X_1 A_1 - X_2 A_1 + X_2 A_1 - X_2 A_2\|_2 \|W_c\|_2
\]

(23)

\[
    \leq (\|A_1\|_2 \|X_1 - X_2\|_2 + \|X_2\|_2 \|A_1 - A_2\|_2) \|W_c\|_2
\]

(24)

\[
    \leq (\|X_1 - X_2\|_2 + \|A_1 - A_2\|_2 D) \|W_c\|_2
\]

(25)

where (a) holds from the spectral norm properties and in (b) we use the bounded input spectral norm assumptions.

We now focus on the second term $\|A_1 - A_2\|_2$ in eq $[25]$. From the bound in lemma $[9]$ we have:

\[
    \|A_1 - A_2\|_2 \leq 2\sqrt{m} \|G\|_2
\]

(26)

where $G$ is the diagonal matrix with entries described in lemma $[8]$

We can now invoke lemma $[10]$ to obtain the following:

\[
    \|A_1 - A_2\|_2 \leq 2\sqrt{m} \times 2 \times 2 \|W_k^T W_q D\| \times \|X_1 - X_2\|_2
\]

(27)

Combining the previous inequality with eq $[25]$ we have the following bound:

\[
    \|\text{Att}(X_1) - \text{Att}(X_2)\|_2 \leq (1 + 8\sqrt{m} \|W_k^T W_q D^2\| \|W_c\|_2 \|X_1 - X_2\|_2
\]

(28)

Derivation for the entire block eq $[11]$
The proof follows simply by leveraging the following property:

Property: for a matrix $C = [A, B]$, the spectral norm of $C$ admits the bound:

\[
    \|C\|_2 \leq \sqrt{\|A\|_2^2 + \|B\|_2^2}
\]

We then simply combine the definition of the attention block and the lipschitz constant bound in eq $[18]$ with the above property in order to obtain the desired bound.

Lemma 8 (Dong et al. [2021] Lemma A.1). For the column stochastic matrix $A_1$ obtained by performing column-wise softmax of some matrix $Z_1$ (where in our setting $Z_1 = (W_k X_1)^T W_q X_1$), and another row stochastic matrix $A_2$ obtained by performing column-wise softmax of some matrix $Z_2$, where $Z_2 = Z_1 - E$ (for some $E$, which need not belong to $\mathcal{X}$), we have the following bound:

\[
    A_2(I - G) \leq A_1 \leq A_2(I + 2G)
\]

(29)

where the inequality is elementwise and $G$ is a diagonal matrix with entries as $G_{ii} = \max_{j\neq i} |\delta_j^T E(\delta_j^T - \delta_i^T)|$. Here $\delta_i$ is a one-hot vector with the entry 1 in the $i^{th}$ dimension.

Lemma 9. Following the notations of lemma $[8]$ we have the following spectral norm bound:

\[
    \|A_1 - A_2\|_2 \leq 2\sqrt{m} \|G\|_2
\]

(30)

Proof. We begin by noting the following entry-wise inequality from eq $[29]$

\[
    A_2 G \leq A_1 - A_2 \leq 2A_2 G
\]

(31)
which ensures that \( \|A_1 - A_2\|_F \leq 2\|A_2G\|_F \).
We also have the following using matrix norm equivalence:
\[
\|A_1 - A_2\|_F \leq \|A_1 - A_2\|_2 \leq \|A_1 - A_2\|_F
\]  
(32)

Invoking the matrix norm equivalence again, we have that
\[
2\|A_2G\|_F \leq 2\sqrt{\text{rank}(A_2G)}\|A_2G\|_2
\]  
(33)

where \( \text{rank}(\cdot) \) is the matrix rank.
Combining the inequalities, we attain the bound:
\[
\|A_1 - A_2\|_2 \leq 2\sqrt{m}\|A_2\|_2\|G\|_2
\]  
(34)

since \( A_2 \) is column-stochastic, \( \|A_2\|_2 = 1 \)

**Lemma 10.** The term \( G \) in lemma 9 admits the following spectral norm bound:
\[
\|G\|_2 \leq 2D\|W_q W_k^T\|_2\|X_1 - X_2\|_2
\]  
(35)

here \( D \) is the previously stated spectral norm bound of the inputs \( X^l \in \mathcal{X} \).

**Proof.** We begin by noting that since \( G \) is a square diagonal matrix with non-negative real values, the singular values of \( G \) are the corresponding diagonal elements.

We thus have that \( \|G\|_{\max} = \|G\|_2 \), where \( \|\cdot\|_{\max} \) is the \( \max \) norm.

Since \( G \) admits the form described in lemma 8, it is trivial to note that:
\[
\|G\|_{\max} = \max_{i,j,j'} |E_{i,j} - E_{i',j'}| \leq 2\|E\|_{\max} \leq 2\|E\|_2
\]  
(36)\( (37) \)

where the second inequality follows from the matrix norm equivalence.
Now, we can bound the last term \( \|E\|_2 \) by noting that the inputs \( X \) belong to a bounded set. This allows us to provide the following bounds:
\[
\|E\|_2 = \|(W_kX_1)^T W_q X_1 - (W_k X_2)^T W_q X_2\|_2 \leq 2\|W_k\|_2\|W_q\|_2\|X_1 - X_2\|_2
\]  
(38)

\[
\leq \|W_k^T W_q\|_2\|X_1\|_2\|X_2\|_2 + \|X_1\|_2\|W_q\|_2\|X_1 - X_2\|_2
\]  
(39)

\[
\leq 2\|W_q\|_2\|X_1 - X_2\|_2
\]  
(40)\( (41) \)

\[
\]

**C.11 Extension of Lemma 6**

Lemma 6 and theorem 4 operate over functions from \( \mathcal{P}^1 \times \mathcal{X}^1 \to \mathcal{P}^{L+1} \times \mathcal{X}^{L+1} \). We can relax the requirement of the prompt and provide the Lipschitz constant upper bound in consideration to functions of the form \( \mathcal{X}^1 \to \mathcal{X}^{L+1} \) by using the following assumption:

**Assumption 3.** Assume for simplicity that \( \|P_1 - P_2\|_2 \leq \alpha\|X_1 - X_2\|_2 \); \( \forall l \geq 1 \). \( \alpha^l = 0 \) when \( l = 1 \).

**Note:** A recursive expression for \( \alpha^l \) in the above assumption can be provided, but the expression does not admit a simplified form and we thus omit it here.

We will use \( D_X \), akin to eq 9, to denote the compactness corresponding to the input matrix across the layers.

Based on this assumption, we have the following Lipschitz constant upper bound:

**Lemma 11.** The Lipschitz constant of the single head \( \text{Attn}^{l,l} \) admits the following bound w.r.t the input part, \( X^l \) of length \( m_X \), of the input sequence:

\[
\text{Lip}(\text{Attn}^{l,l}(\cdot, \cdot)) \leq \left( \sqrt{1 + (\alpha^l)^2} + 8\sqrt{m_X} (D_X)^2 (1 + (\alpha^l)^2) \|W_q^{l,l} W_{q,l}^T\|_2 \right) \|W_{q,l}^T\|_2
\]  
(42)

For \( l = 1 \), \( \alpha^l = 0 \) in the above bound.

The Lipschitz constant of the entire attention block in layer \( l \) follows similarly.
Proof. For some first layer input $X_1^i$ and prompt $P$, let us denote the direct output of the attention head in the $l$-th layer with $X^i_l$. We have the following update rule for $X^i_l$:
\[
X^i_l = W^{i,l}_v[P^i_l, X^i_1] \cdot \sigma((W^{i,l}_k[P^i_l, X^i_1])^T W^{i,l}_q X^i_1) = W^{i,l}_v[P^i_l, X^i_1] \cdot A^i_l \tag{43}
\]
Here, $P^i_l$ is the updated prompt matrix w.r.t. the input. For two different inputs $X^i_1$ and $X^i_2$ at the first layer, $P^i_1 = P^i_2 = P$, since the prompt is same across all inputs. $A^i_1$ is then simply the corresponding column-stochastic matrix.

With the context clear, we now drop the superscripts $i, l$, as done previously. For $\|\tilde{X}^i_1 - \tilde{X}^i_2\|_2$, we have:
\[
\|\tilde{X}^i_1 - \tilde{X}^i_2\|_2 \leq \|[P_1, X_1]A^i_1 - [P_2, X_2]A^i_2\|_2 \|W^i_v\|_2
\]
\[
\leq \left(\|A^i_1\|_2 \sqrt{\|P_1 - P_2\|^2 + \|X_1 - X_2\|^2} + \sqrt{\|P_2\|^2 + \|X_2\|^2} \|A^i_1 - A^i_2\|_2 \right) \|W^i_v\|_2 \tag{44}
\]
where the second inequality is attained using the property of spectral norm of concatenated matrices.

We now consider the term $\|A^i_1 - A^i_2\|_2$. By invoking lemmas 9 and 10, we have that:
\[
\|A^i_1 - A^i_2\|_2 \leq 2\sqrt{m} \|X\|_2\|E\|_2
\]
where $E = (W^i_k[P_1, X_1])^T W^i_q X_1 - (W^i_k[P_2, X_2])^T W^i_q X_2 \tag{45}$

Invoking assumption 3, $\|E\|_2$ can further be bounded as:
\[
\|E\|_2 \leq 2D \sqrt{1 + \alpha^2} \|(W^i_k)^T W^i_q\|_2 \tag{46}
\]
Finally, by combining the bound for $\|E\|_2$ and assumption 3 with eq 44, we obtain:
\[
\|\tilde{X}^i_1 - \tilde{X}^i_2\|_2 \leq \left(\sqrt{1 + \alpha^2} + D \sqrt{1 + \alpha^2} \times 8\sqrt{m} \sqrt{D} \sqrt{1 + \alpha^2} \|(W^i_k)^T W^i_q\|_2 \right) \|W^i_v\|_2 \|X_1 - X_2\|_2 \tag{47}
\]
which provides us the desired bound. \hfill \Box

By setting $\alpha^i = 0$, the case when there is no prompt, we obtain a similar bound as lemma 6.