Context-PEFT: Efficient Multi-Modal, Multi-Task Fine-Tuning

Avelina Asada Hadji-Kyriacou
University of St Andrews
Department of Computer Science
lhk3@st-andrews.ac.uk

Ognjen Arandjelovic
University of St Andrews
Department of Computer Science
oa73@st-andrews.ac.uk

Abstract

This paper introduces a novel Parameter-Efficient Fine-Tuning (PEFT) framework for multi-modal, multi-task transfer learning with pre-trained language models. PEFT techniques such as LoRA, BitFit and IA^3 have demonstrated comparable performance to full fine-tuning of pre-trained models for specific downstream tasks, all while demanding significantly fewer trainable parameters and reduced GPU memory consumption. However, in the context of multi-modal fine-tuning, the need for architectural modifications or full fine-tuning often becomes apparent. To address this we propose Context-PEFT, which learns different groups of adaptor parameters based on the token's domain. This approach enables LoRA-like weight injection without requiring additional architectural changes. Our method is evaluated on the COCO captioning task, where it outperforms full fine-tuning under similar data constraints while simultaneously offering a substantially more parameter-efficient and computationally economical solution.

1. Introduction

Recent advancements in Parameter-Efficient Fine-Tuning (PEFT), exemplified by techniques such as LoRA, BitFit, and IA^3 [16, 21, 40], have demonstrated their ability to deliver performance on par with full fine-tuning of pre-trained models for specific downstream tasks, all while significantly reducing the number of trainable parameters and GPU memory consumption. However, in the realm of multi-modal transfer-learning, there often arises a need for architectural adjustments – such as Multi-Modal Causal Attention [39] – or full fine-tuning – as demonstrated by LLaVA [23].

In response to these challenges we introduce a novel PEFT framework, Context-PEFT, which learns different groups of adaptor parameters based on the token's domain or purpose. This approach necessitates no further architectural modifications and is adaptable to various PEFT techniques. We conduct an extensive evaluation of our method on the COCO captioning tasks [20], demonstrating its superior performance compared to full fine-tuning under similar data constraints, all while delivering a substantially more parameter-efficient and computationally economical solution.

We experiment with LoRA, BitFit and IA^3 as adaptor methods for Context-PEFT and examine how they perform compared to full fine-tuning, no fine-tuning, as well as vanilla context-agnostic PEFT.

2. Previous Work

2.1. Parameter-Efficient Fine-Tuning

Large Language Models (LLMs) have been increasing in scale over recent years, with popular 'baseline' models increasing in size from 350 million parameters in 2018 (BERT Large [10]) to 7 billion parameters in 2023 (Llama 2 7B [35]). With this increase in scale there has been an increase in popularity of PEFT techniques which have enabled the fine-tuning of large models using less compute and fewer resources. PEFT methods can be categorised by the ways they modify the underlying model architecture, which parameters are trainable and where new weights are introduced.

Adaptor Modules MLP Adaptors [15, 29] come in multiple variations but all share the same core idea of introducing a small residual fully-connected network after sub-layers in the transformer backbone. These adaptor layers are then trained while the original transformer layers remain frozen.

Soft Prompts Soft prompt techniques – such as Prefix-Tuning [18, 19] – introduce learnable embeddings as a prefix to the input sequence. These embeddings can be trained as inputs to only the first layer and then propagated to all layers like normal tokens, or learned for each transformer sub-layer, replacing the results of embeddings of prior layers in the prefix region.

Selective Training Selective training involves only training a subset of parameters. Such techniques include BitFit [40] which trains only the bias terms of projection layers and LN-Tuning [26] which learn only the bias and scale parameters of the layer normalisation layers.

Additive Methods Additive methods involve introducing learnable vectors that are applied point-wise to the activations in transformer sublayers. IA^3 [21] applies an element-wise multiplication of learnable vectors to the queries and keys in attention layers as well as the intermediate activations of the feed-forward layers.

Reparameterization Methods Another method to reduce the number of trainable parameters is by augmenting the original pre-trained weights using low-rank representations. One popular method is LoRA [16] which computes delta weights for the pre-trained projection matrices using low-rank matrix decompositions, $\delta W = AB$. Originally, LoRA was proposed for the key, query, value and output projections of attention layers, but the technique can also be applied to the FFN layers.

2.2. Vision-Language Models

Vision-Language models can often be classified under two categories: dual-encoder models which are more suited to classification and retrieval tasks [13, 17, 28, 33, 41], and vision-encoder text-decoder models which are more suited to generative tasks such as captioning and VQA. Vision-encoder text-decoder models – often refered to as Large Vision Language Models (LVLMs) – can further be split into two categories based on their attention styles: causal-attention only models which incorporate image embeddings into the input context as projected tokens [2, 23, 39], and cross-attention augmented models which add additional attention layers to incorporate visual information [1].

Among LVLMs, the causal-only style models have some advantages over cross-attention style models when augmenting pre-trained text-only models to accept other modalities. Cross-attention style LVLMs introduce a significant number of extra parameters which need to be trained, increasing both training compute requirement and inference latency. Care must also be taken when using cross-attention for multi-turn interleaved text and image input to ensure images are correctly localised to the corresponding text segments.

For causal LVLMs there are a multiple methods for adapting pre-trained text-only LLMs to accept visual inputs. DeepSpeed-VisualChat [39] opts to completely freeze the LLM and vision-encoder, training only the text embeddings and image projection layer. Additionally, the authors augment the attention mechanism such that two separate attention matrices are used for (1) text attending to text to-

kens and (2) text attending to visual tokens. They name this augmentation the 'Multi-Modal Causal Attention Mechanism (MMCA),' with their intuition being that the attention weights of the two different modalities may interfere if jointly normalised. Alternatively, LLaVa [23] takes a two stage approach. Firstly the LLM and vision-encoder are frozen while the image projection weights are trained on a large image caption corpus. Next the LLM is unfrozen and is jointly fine-tuned with the image projections on a smaller language and vision multi-turn conversational dataset.

Both approaches have their own merits and their own drawbacks. The MMCA approach only trains a small subset of weights, but increases the compute requirements compared to vanilla attention using accelerated kernels such as FlashAttention [8]; as of writing, FlashAttention does not support explicit masks, which means the attention matrices for both modalities cannot be jointly computed using this acceleration structure and must instead fall back to either non-accelerated attention (which uses more GPU memory) or multiple rounds of FlashAttention (which increases training and inference latency). Since LLaVa uses vanilla causal attention it can take advantage of FlashAttention, but requires full fine-tuning of the LLM in the second stage of training.

3. Our Approach

We form a similar approach to that of LLaVa [23], opting to fully freeze the vision-encoder and learn a linear projection to adapt image embeddings as inputs to the language model. Our method, however, differs in that we replace the full fine-tuning of the LLM with Context-PEFT and choose not to pre-train the linear projection on an auxiliary image-caption corpus as we want to train and evaluate our models on a standard dataset without any auxiliary training data.

3.1. Model Selection

The focus of this paper is efficiency, and with that in mind we have selected small and efficient models for this research.

For the LLM we wanted to use a Llama 2 style model with a similar size to GPT-2 small [27, 35]. However with Llama models starting at 7 billion parameters we opted to train our own model in house on 5 billion tokens from The Pile text corpus [12]. Details of the LLM are described in supplementary material Section 7.

For the vision-encoder we opted to utilise the Swin Transformer V2 family of models due to their efficiency and size of produced embeddings [25]; for images of size 256×256 the Swin family produce 64 embeddings. Details of the chosen Swin models are detailed in supplementary material Section 6.
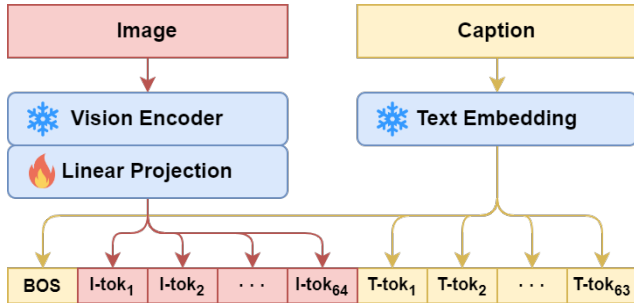
2

Figure 1. Image and text input structure. A pre-trained vision encoder produces image embeddings which are projected through a linear layer and concatenated with text embeddings of the corresponding caption.

3.2. Image Inputs

After passing the images through the vision-encoder the embeddings are projected to the LLM embedding dimension and added to the token sequence. The sequence is constructed such that it begins with a [BOS] token, followed by the 64 projected image embeddings, and up to 63 caption tokens which are post-padded by an [EOS] token and [PAD] tokens to achieve a fixed context length of 128. Almost all COCO captions fit into this 63 token budget with only a tiny faction of captions exceeding this length (and thus are truncated). This is illustrated in Figure 1.

3.3. Context-PEFT

Our motivation behind Context-PEFT is inspired by Microsoft's introduction of MMCA; by decomposing the attention mechanism into two mode-specific sub mechanisms they change the way in which the text and image modalities interact and thus aggregate information. This is further exemplified by the fact that the authors found the addition of LoRA to have minimal effects on the results [39], which further highlights the importance of controlling inter-modality interactions. Our approach is to instead directly modulate the weights applied to tokens of different modalities which we hypothesise would yield similar results to MMCA by modifying the embeddings passed to the attention mechanism rather than altering the mechanism itself. Our approach also has similarities to Mixture-of-Experts methods which have been shown to greatly improve performance of multi-domain tasks such as any-to-any machine translation [14, 32].

Each token in the sequence has a corresponding 'context number' identifier which designates which adaptor weights should be used at each position of the sequence. When performing vanilla context-agnostic PEFT experiments we simply set all tokens to use the same context number. For all PEFT variants, context-specific and context-agnostic, we freeze all original model parameters and train only the
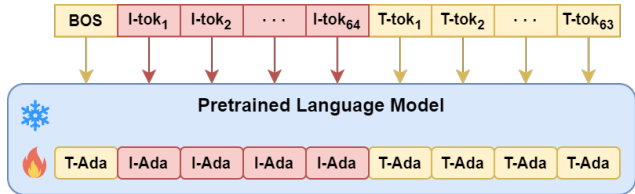

Figure 2. The overall model structure showing trainable adaptors used for different token types in the frozen language model.

injected adaptor parameters. The overall structure of the model is shown in Figure 2.

Our choice of adaptor methods was motivated by their fine-tuning performance as reported in their original papers, ability to augment into context-specific forms, and ability to integrate into existing models with minimal modification. Although we opted to modify the code of our in-house model to facilitate easier debugging of adaptors during development, all adaptor methods can be incorporated into a PyTorch model using forward hooks without modifying any of the original code.

Context-LoRA We formulate a memory efficient way of computing context-specific LoRA such that the delta weight matrix is never fully materialised. To adapt any projection, W, for context LoRA with low rank matrices A and B the following algorithm is used:

Algorithm 1 Memory efficient Context-LoRA algorithm

$x \leftarrow states$
$s \leftarrow OneHot(contextNum)$
$\delta h \leftarrow Einsum(\text{'...ld,cdr,crD,...lc} \rightarrow \text{...lD'}, x, A, B, s)$
$h \leftarrow Wx + \delta h$

The letters in the einsum correspond to different input and output dimensions. l corresponds to the sequence length dimension, d and D are the input and output dimensions of the projection, r is the rank of the A and B decomposition matrices, and c is the context selector dimension.

We apply context-LoRA to the query, key, value, and output projections in the attention layers as well as the up and down projections in the feed-forward layers.

Context-BitFit Traditionally, BitFit fine-tuning is performed by training only the bias terms; however this does not easily facilitate per-token bias terms. To combat this we reparameterize BitFit training by adding a secondary trainable bias term that depends on the token's context number. We apply BitFit to all projections in all layers of the transformer backbone.

Context-IA^3 Our application of Context-IA^3 is almost identical to Context-BitFit, with the main difference being
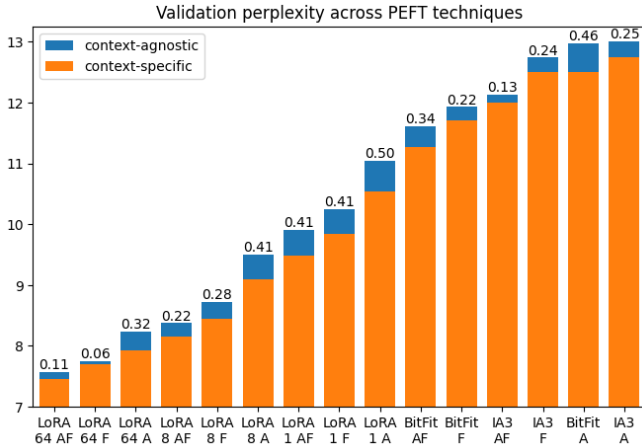
Figure 3. Validation perplexity after 8 epochs using the tiny Swin variant. 'A' and 'F' in the run name represent attention and feed-forward adaptation respectively, with the number representing the LoRA rank. The values above the bars represent the improvement in PPL for the context-specific variant.

Adaptor	A			F			AF		
IA3	13.01	12.75	(-0.25)	12.74	12.51	(-0.24)	12.13	12.0	(-0.13)
BitFit	12.97	12.51	(-0.46)	11.93	11.70	(-0.22)	11.61	11.27	(-0.34)
LoRA 1	11.04	10.54	(-0.50)	10.25	9.83	(-0.41)	9.91	9.49	(-0.41)
LoRA 8	9.50	9.09	(-0.41)	8.72	8.44	(-0.28)	8.38	8.15	(-0.22)
LoRA 64	8.24	7.92	(-0.32)	7.75	7.69	(-0.06)	7.57	**7.46**	(-0.11)

Table 1. Validation perplexity after 8 epochs using the tiny Swin variant. 'A' and 'F' in the column name represent attention and feed-forward adaptation respectively. Context-agnostic PPL, context-specific PPL, and difference in PPL are represented by the left, center and right values in each column respectively.

element-wise multiplication of the projected states rather than addition. We apply IA^3 to the key, value and intermediate FFN activations, as described by the original authors [21].

4. Evaluation

For most experiments we use caption perplexity (PPL) on the validation or test sets as a benchmark of model performance. When reporting results we the use weights from the epoch with best validation loss.

4.1. Training

Across all experiments we train using a batch size of 96 for eight epochs over the COCO dataset unless otherwise stated. We use the Adam optimizer with a fixed learning rate of $1e^{-4}$ and beta values of $(0.9, 0.95)$. We apply a dropout of 0.1 before the image projection layer, and a residual dropout after attention and feed-forward layers in the language model. We also apply flip, crop and colour augmentations to the images during training. For the loss function we use typical language modelling loss applied to the last 64 tokens of the sequence. Each experiment is conducted on a single RTX A4500 GPU and we make use of mixed precision training. We only use the training split of the COCO dataset to fine-tune our models, making no use of additional training data; this is to ensure repeatability and to explore the efficacy of context-PEFT in a data-constrained environment.

4.2. Adapting Attention and Feed-Forward Layers

To gain an understanding of how context-PEFT affects different parts of the transformer backbone we evaluate the performance of various PEFT methods when applying adaptation to both attention and FFN layers, and to either the attention or FFN layers. Our comparisons are conducted using the 'tiny' version of the Swin transformer, where we analyze validation perplexity across both context-specific and context-agnostic versions of the three PEFT methods and while also varying the rank of the LoRA adaptors.

From the results summarised in Figure 3 we consistently find the context-specific adaptors outperforming their context-agnostic variant across all configurations, with the attention and feed-forward adaptor configurations performing best among each technique, and LoRA with a rank of 64 performing best overall.

When applying fine-tuning to a subset of layers (the 'A' and 'F' columns of Table 1) we discover that adapting the feed-forward layers generally yields lower perplexity than adapting only the attention layers. However we observe the largest gains in perplexity for context-PEFT in the attention-only configurations compared to the context-agnostic variants which suggests that attention layers benefit the most from context-specific adaption, further validating our hypothesis of the importance of modality specific attention routing, but unlike DeepSpeed-VisualChat [39], we are able to achieve this through context-PEFT alone.
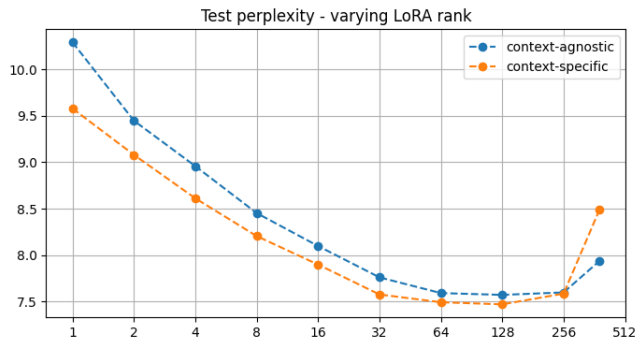

Figure 4. Test perplexity after 8 epochs using the tiny Swin variant, varying LoRA rank from 1 to 384 in the attention and feed-forward adaptor configuration.
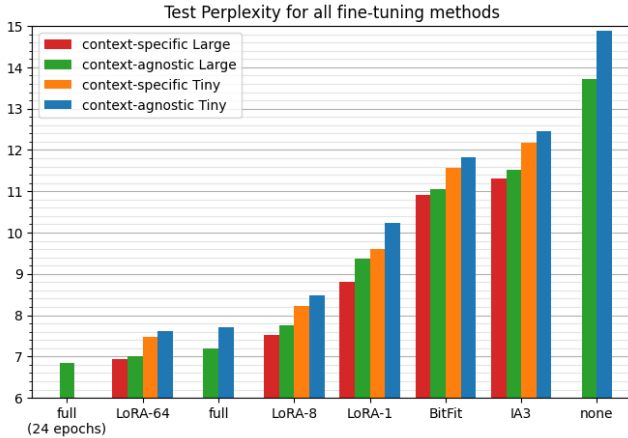
Figure 5. Test perplexity of different fine-tuning methods after 8 epochs for both vision encoder sizes.

Adaptor	Tiny		Large	
IA3	12.46	12.18	11.52	11.32
BitFit	11.83	11.56	11.04	10.90
LoRA 1	10.23	9.61	9.38	8.82
LoRA 8	8.48	8.22	7.76	7.53
LoRA 64	7.61	7.48	7.00	6.93
None	14.88		13.71	
Full FT	7.70		7.18	
Full FT (24 epochs)			6.83	

Table 2. Test perplexity of different fine-tuning methods after 8 epochs for both vision encoder sizes. The left and right values correspond to context-agnostic and context-specific results respectively.

4.3. Varying LoRA Rank

Using the attention and feed-forward configuration with the 'tiny' Swin model we sweep the LoRA rank from 1 to 384 (half of d_{model}) to evaluate how rank affects performance for both context-specific and context-agnostic variants.

From the results shown in Figure 4 it can be seen that test perplexity decreases as rank increases. However as the rank approaches 64 the perplexity plateaus and then sharply increases after a rank of 256, implying an optimal rank value between 64 and 128 for both context-specific and context-agnostic variants in our LLM. This suggests that the low-rank nature of LoRA has a beneficial regularising effect in data-constrained environments, such as our fine-tuning on the COCO dataset. This may also explain why full fine-tuning underperforms both in our experiments and some experiments carried out in the original LoRA paper [16].

4.4. Effect of Vision Transformer Size

We evaluate how vision encoder size affects test perplexity by comparing the 'tiny' and 'large' Swin models for a range of adaptors. We compare their performance for both the context-specific and context-agnostic adaptor variants in the

Adaptor	Context-Agnostic	Context-Specific
IA3	55,296	110,592
BitFit	119,808	239,616
LoRA-1	202,752	405,504
LoRA-8	1,622,016	3,244,032
LoRA-64	12,976,128	25,952,256
Full FT	153,196,032	

Table 3. The number of trainable parameters in the LLM backbone for different adaptor variants in the attention and feed-forward configuration.

'AF' configuration, with our results summarised in Figure 5 and Table 2.

For each adaptor variant it can be seen that the large vision encoder with context-specific adaptation performs best, followed by the large vision encoder with context-agnostic adaption, both of which still perform better than the tiny vision encoder with context-specific adaptation. This is not surprising at all considering the large version of the Swin model has 7 times as more parameters $(195, 202, 932)$ than the tiny version $(27, 578, 154)$, which is a significantly larger increase in parameters than for context-specific vs context-agnostic adaption as shown in Table 3. This implies that higher quality image token embeddings are more important for image understanding in our models than the introduction of context-specific adaptation which only has twice as many trainable parameters than context-agnostic adaptation; despite this we can still see that context-specific adaptation can further lower perplexity which is especially evident in the lower rank LoRA adaptors.

Even though the Large swin transformer outperforms the Tiny swin transformer for each adaptor configuration in isolation, we can see that Context-LoRA-64 with Swin-Tiny outperforms all lower rank LoRA variants with Swin-Large; so even though Context-LoRA-64 has the most *trainable* parameters, a full vision-text pipeline utilising Swin-Tiny + Context-LoRA-64 has fewer *total* parameters and lower perplexity than Context-LoRA-8 + Swin-Large. This has important implications for scenarios where model size may be more important than model performance, for example when performing inference on embedded systems with resource limitations preventing the use of a larger vision encoder.

We can also see that LoRA with a rank of 64 outperforms full fine-tuning for the respective vision transformer sizes when given the same data budget of 8 epochs, both with and without context-specific adaptation. We do an additional run and find it takes 24 epochs of full fine-tuning to outperform context-LoRA with the large Swin model as the vision encoder.

4.5. Attention Map Observations

The vision transformers we used were pre-trained for image classification on ImageNet-1k (with the large version trained on ImageNet-22k before finetuned for ImageNet-1k), meaning it may be reasonable to assume the captioning abilities of our models come purely from the image classification abilities of the vision-encoder, rather than the language model's ability to extract and reason with the information in the image tokens themselves. However, we show this is not the case by analysing the attention weights of our trained models.

To collect these attention heatmaps we take image-caption pairs from the the COCO test set, forward pass them through our trained Context-LoRA-64-AF model and observe the attention weights for spans of caption tokens to
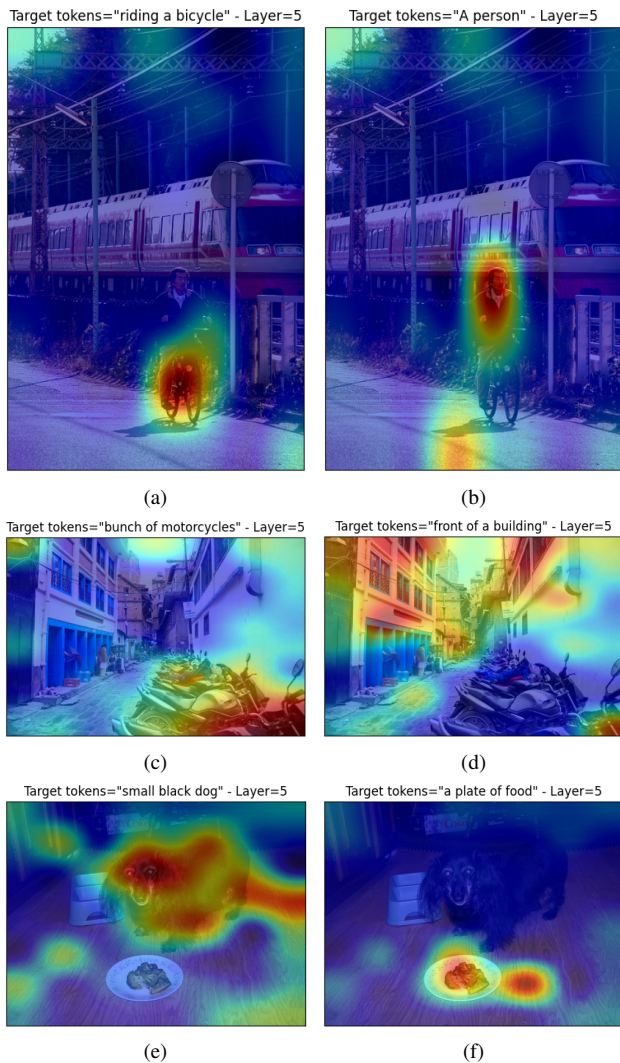

(a)

(b)

(c)

(d)

(e)

(f)

Figure 6. Heatmap visualisations depicting image token attention weights for spans of caption tokens.

gain an understanding of the importance of different parts of the image for different parts of the caption. More specifically, we take the attention weight matrix for layer n and slice the resulting matrix such that we only keep columns corresponding to the image tokens and rows corresponding to the desired span of caption tokens. Finally we sum across the query and head dimension and reshape the resulting vector into an 8×8 matrix which we upscale and overlay on the original image using a colour gradient.

From examples given in Figure 6 and supplementary Section 8 we observe that the text tokens place attention on specific regions of the images which have clear semantic relevance with surprisingly fine granularity; for example, we observe that the model is able to tell the difference between a bicycle and the person riding on it, as shown in Figures 6a and 6b. This shows that – even though we train on image segmentation data – the model could generalise to perform panoptic segmentation by learning linear classifiers on the attention maps.

We also notice that the first and last image tokens (top-left and bottom-right image patches) occasionally have unusually high attention weights. The large top-left weighting may be explained through the attention sinking phenomenon [37], while the bottom-right weighting can be explained by the fact that the last image token is also the location that produces the first text-token in auto-regressive text generation. We hypothesise that both phenomena would disappear if we wrapped the image embeddings between additional 'beginning' and 'end' tokens which may further lead to performance improvements through more salient attention behavior.

5. Discussion

5.1. Applications and Limitations

The primary application for Context-PEFT is in compute and data-constrained environments; for example when there is a low volume of training data, when there are GPU memory restrictions necessitating the use of smaller models and/or fewer trainable parameters, when there is limited training time which may prevent full fine-tuning from converging to a good minima, or when models must be deployed for inference on low-resource hardware such as consumer grade workstations, mobile devices and embedded systems.

However, if the aforementioned constraints are not a concern, it is unlikely Context-PEFT will outperform full fine-tuning. This is likely due to the fact that the embedding spaces of SOTA language models are often wide enough to represent multiple modalities without the need for context-specific weights when trained to convergence on a large volume of training data, as shown by Qwen-VL and LLaVa [2, 23].

5.2. Future Work

There are numerous improvements that can be integrated from concurrent and previous works to further push the performance of Context-PEFT as a fine-tuning method. These methods and some novel suggestions for future work are summarized below:

Exploring More PEFT Techniques   Further exploration of PEFT techniques may also yield greater fine-tuning performance at potentially lower budgets. One such example would be investigating how context-specific scaling and offset parameters affect the performance of LN-tuning. Another avenue worth exploring is combining PEFT techniques, such as combining LoRA and BitFit to not only perform low rank updates of linear layers but also update their corresponding bias terms.

Improved Vision Encoder   From our evaluation in Section 4.4 we have shown that the quality of input embeddings for other modalities can greatly affect the performance of the fine-tuned language model. There are many vision encoder alternatives:
- **CLIP-ViT** [28], which was trained specifically to connect vision and textual content in addition to producing a larger number of image embeddings than the Swin Transformer family.
- **VQ-VAE** [36], which produces a greater number of image embeddings than ViT. Additionally, instead of using an image projector to align the latent space for the language model, we can instead take advantage of the discrete nature of the latent space by learning a set of embeddings that map from the VAE 'vocabulary' directly into the embedding space of the language model.
- **VQ-GAN** [11], which has the same benefits as VQ-VAE with the addition of producing latents which were also trained with conditioning on textual features, especially if the VQ-GAN/VQ-VAE was fine-tuned for use with latent diffusion model [30].
- **DETR** [4] object detection encoder, which may allow the language model to learn better semantic connections between text tokens and image tokens.
- **Encoder Fine-Tuning** as in Qwen-VL [2], where a pre-trained Vision Transformer is used a starting point and then further fine-tuned with a Visual Question Answering (VQA) objective.
- **Encoder PEFT**, similar to Qwen-VL, it is worth exploring the use of PEFT techniques like LoRA to fine-tune the vision encoder without performing full parameter updates.

Improved Pre-Training   As shown in the LLaVa paper [23], pre-training on a mass image-caption corpus im-proves the alignment of the image projector which may have similar effect to using an improved vision encoder. CC3M and LAION-COCO are two such corpora which are well suited to pre-training the image-projector.

Improved Image Projection   Replacing the linear projector with an MLP has also been shown to improve alignment quality, as explored in LLaVa-1.5 [22]. It is also worth investigating the addition of learnt absolute position embeddings after the image projection as the some vision encoder architectures, such as CNNs, do not produce embeddings which contain positional information.

Improved Base Language Model   It is well known that larger language models have improved zero-shot generative capabilities over smaller language models [3], so an obvious choice for future work is to apply our framework to a larger base language model as this should also lead to higher quality caption generation.

Exploring Hyperparameters   Optimal hyperparameter choice can often improve the quality of a model without changing the model architecture or training objective itself. It is therefor worth exploring the impact of optimizer choice (exploring alternative such as AdamW, Sophia, Adabelief, Lookahead, Sharpness-Aware-Minimization), optimizer hyperparemeters, learning rate schedules, and the impact of dropout when applied to different subsets of layers and with different drop-rates.

Pruning and Quantization   Context-PEFT (and PEFT techniques in general) are often lightweight for both training and inference, but these techniques can further be combined with weight quantization and pruning to further reduce model footprint with minimal effect on performance [5, 9].

Training Objectives   In our work we made use of only the causal language modelling loss as our training objective, but there are numerous other choices which may lead to a higher quality model. One example of a training objective that may improve model quality is causal masked language modelling, where a span of tokens in the caption are replaced with a single `[mask]` token and the model is tasked with predicting the string of masked tokens; this objective may also condition the model for down-stream tasks such as visual question answering due to its similarity with the training objective. Another training objective worth exploring would be online reinforcement learning where the reward signal for generated sequences is given by CLIP alignment score [28].

Other Modalities   We believe that Context-PEFT can be extended to many other modalities and potentially allow the fusion of several modalities into a unified model. Examples of a multi-modal tasks suitable for Context-PEFT include processing audio for speech recognition, and processing video for Video Question Answering.

Boundary Tokens   As shown in Section 4.5 there are some unusual attention behaviours at the boundaries between different modalities. We hypothesize that it may be possible to alleviate these phenomena by wrapping each modality segment with special tokens, `[section]` and `[/section]`. The introduction of these section boundary tokens also opens up opportunities for auxiliary training losses by treating the end of section token as a `[CLS]` token [10], which would facilitate the learning of linear classification heads for a wider variety of downstream tasks.

Prompt Injection Mitigation   Prompt injection attacks are typically mitigated through cleansing incoming messages and using special formatting to prevent exploits such as the model interpreting user inputs as system messages. However, bad actors often still find ways to overcome these protections and bypass the safety guardrails of publicly available LLMs-as-a-service. We hypothesize that Context-PEFT could potentially be used to mitigate prompt injection by using different adaptors for system messages, user inputs and generated responses, which – when combined with re-inforcement learning as is typically used for 'chat' models – may condition the model to completely ignore any attempts to inject harmful prompts within user input segments.

Parallel Training   We also believe that Context-PEFT has untapped potential for parallel training on different tasks to then assemble the learnt adaptors into a unified model for further fine-tuning on a combined task. One example use case – illustrated in Figure 7 – is training one set of context-PEFT adaptors for image captioning, training another set of context-PEFT adaptors for textual question answering (where questions and answers represent different contexts), and then fine-tuning the unified ensemble of adaptors for a downstream Visual Question Answering task. Taking this to the extreme, we could train context-PEFT on dozens of tasks and modalities in parallel, effectively treating each set of adaptors as 'plugins' which can be integrated into a single unified model.

5.3. Conclusion

In this paper, we have introduced Context-PEFT as a multi-modal, multi-task fine-tuning framework to efficiently adapt pre-trained language models to other modalities in a data- and parameter-efficient manor by learning multiple groups
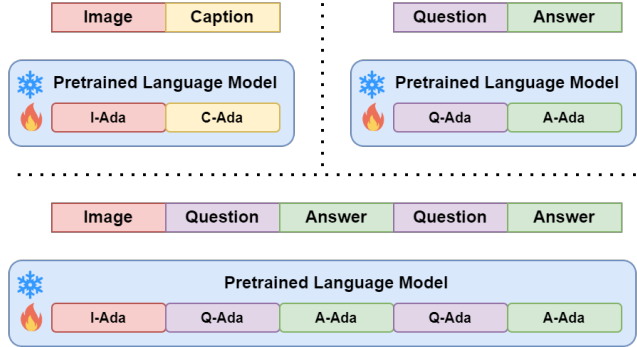

Figure 7. Parallel training for VQA with Context-PEFT.

of adaptor parameters which are specific to each token's domain.

Through extensive experimentation with the COCO dataset and captioning task we validate the potential of Context-PEFT, evaluating our framework for a variety of adaptor methods and fine-tuning configurations, and we show our method is very competitive with full fine-tuning for data-constrained and compute-limited environments.

Finally, we suggest a range of possible applications for context-PEFT and provide a variety of future research directions and potential improvements to further explore its performance and capabilities beyond our use-case of image captioning.

References

[1] Jean-Baptiste Alayrac, Jeff Donahue, Pauline Luc, Antoine Miech, Iain Barr, Yana Hasson, Karel Lenc, Arthur Mensch, Katie Millican, Malcolm Reynolds, Roman Ring, Eliza Rutherford, Serkan Cabi, Tengda Han, Zhitao Gong, Sina Samangooei, Marianne Monteiro, Jacob Menick, Sebastian Borgeaud, Andrew Brock, Aida Nematzadeh, Sahand Sharifzadeh, Mikolaj Binkowski, Ricardo Barreira, Oriol Vinyals, Andrew Zisserman, and Karen Simonyan. Flamingo: a visual language model for few-shot learning, 2022. 2

[2] Jinze Bai, Shuai Bai, Shusheng Yang, Shijie Wang, Sinan Tan, Peng Wang, Junyang Lin, Chang Zhou, and Jingren Zhou. Qwen-vl: A versatile vision-language model for understanding, localization, text reading, and beyond, 2023. 2, 6, 7

[3] Tom B. Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, Sandhini Agarwal, Ariel Herbert-Voss, Gretchen Krueger, Tom Henighan, Rewon Child, Aditya Ramesh, Daniel M. Ziegler, Jeffrey Wu, Clemens Winter, Christopher Hesse, Mark Chen, Eric Sigler, Mateusz Litwin, Scott Gray, Benjamin Chess, Jack Clark, Christopher Berner, Sam McCandlish, Alec Radford, Ilya Sutskever, and Dario Amodei. Language models are few-shot learners, 2020. 7

[4] Nicolas Carion, Francisco Massa, Gabriel Synnaeve, Nicolas

Usunier, Alexander Kirillov, and Sergey Zagoruyko. End-to-end object detection with transformers, 2020. 7

[5] Tianlong Chen, Jonathan Frankle, Shiyu Chang, Sijia Liu, Yang Zhang, Zhangyang Wang, and Michael Carbin. The lottery ticket hypothesis for pre-trained bert networks, 2020. 7

[6] Aakanksha Chowdhery, Sharan Narang, Jacob Devlin, Maarten Bosma, Gaurav Mishra, Adam Roberts, Paul Barham, Hyung Won Chung, Charles Sutton, Sebastian Gehrmann, Parker Schuh, Kensen Shi, Sasha Tsvyashchenko, Joshua Maynez, Abhishek Rao, Parker Barnes, Yi Tay, Noam Shazeer, Vinodkumar Prabhakaran, Emily Reif, Nan Du, Ben Hutchinson, Reiner Pope, James Bradbury, Jacob Austin, Michael Isard, Guy Gur-Ari, Pengcheng Yin, Toju Duke, Anselm Levskaya, Sanjay Ghemawat, Sunipa Dev, Henryk Michalewski, Xavier Garcia, Vedant Misra, Kevin Robinson, Liam Fedus, Denny Zhou, Daphne Ippolito, David Luan, Hyeontaek Lim, Barret Zoph, Alexander Spiridonov, Ryan Sepassi, David Dohan, Shivani Agrawal, Mark Omernick, Andrew M. Dai, Thanumalayan Sankaranarayana Pillai, Marie Pellat, Aitor Lewkowycz, Erica Moreira, Rewon Child, Oleksandr Polozov, Katherine Lee, Zongwei Zhou, Xuezhi Wang, Brennan Saeta, Mark Diaz, Orhan Firat, Michele Catasta, Jason Wei, Kathy Meier-Hellstern, Douglas Eck, Jeff Dean, Slav Petrov, and Noah Fiedel. Palm: Scaling language modeling with pathways, 2022. 1

[7] Zihang Dai, Zhilin Yang, Yiming Yang, Jaime Carbonell, Quoc V. Le, and Ruslan Salakhutdinov. Transformer-xl: Attentive language models beyond a fixed-length context, 2019. 1

[8] Tri Dao, Daniel Y. Fu, Stefano Ermon, Atri Rudra, and Christopher Ré. Flashattention: Fast and memory-efficient exact attention with io-awareness, 2022. 2, 1

[9] Tim Dettmers, Artidoro Pagnoni, Ari Holtzman, and Luke Zettlemoyer. Qlora: Efficient finetuning of quantized llms, 2023. 7

[10] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. Bert: Pre-training of deep bidirectional transformers for language understanding, 2019. 1, 8

[11] Patrick Esser, Robin Rombach, and Björn Ommer. Taming transformers for high-resolution image synthesis, 2021. 7

[12] Leo Gao, Stella Biderman, Sid Black, Laurence Golding, Travis Hoppe, Charles Foster, Jason Phang, Horace He, Anish Thite, Noa Nabeshima, Shawn Presser, and Connor Leahy. The pile: An 800gb dataset of diverse text for language modeling, 2020. 2

[13] Rohit Girdhar, Alaaeldin El-Nouby, Zhuang Liu, Mannat Singh, Kalyan Vasudev Alwala, Armand Joulin, and Ishan Misra. Imagebind: One embedding space to bind them all, 2023. 2

[14] Jiatao Gu, Hany Hassan, Jacob Devlin, and Victor O. K. Li. Universal neural machine translation for extremely low resource languages, 2018. 3

[15] Neil Houlsby, Andrei Giurgiu, Stanislaw Jastrzebski, Bruna Morrone, Quentin de Laroussilhe, Andrea Gesmundo, Mona Attariyan, and Sylvain Gelly. Parameter-efficient transfer learning for nlp, 2019. 1

[16] Edward J. Hu, Yelong Shen, Phillip Wallis, Zeyuan Allen-Zhu, Yuanzhi Li, Shean Wang, Lu Wang, and Weizhu Chen. Lora: Low-rank adaptation of large language models, 2021. 1, 2, 5

[17] Chao Jia, Yinfei Yang, Ye Xia, Yi-Ting Chen, Zarana Parekh, Hieu Pham, Quoc V. Le, Yunhsuan Sung, Zhen Li, and Tom Duerig. Scaling up visual and vision-language representation learning with noisy text supervision, 2021. 2

[18] Brian Lester, Rami Al-Rfou, and Noah Constant. The power of scale for parameter-efficient prompt tuning, 2021. 1

[19] Xiang Lisa Li and Percy Liang. Prefix-tuning: Optimizing continuous prompts for generation, 2021. 1

[20] Tsung-Yi Lin, Michael Maire, Serge Belongie, Lubomir Bourdev, Ross Girshick, James Hays, Pietro Perona, Deva Ramanan, C. Lawrence Zitnick, and Piotr Dollár. Microsoft coco: Common objects in context, 2015. 1

[21] Haokun Liu, Derek Tam, Mohammed Muqeeth, Jay Mohta, Tenghao Huang, Mohit Bansal, and Colin Raffel. Few-shot parameter-efficient fine-tuning is better and cheaper than in-context learning, 2022. 1, 2, 4

[22] Haotian Liu, Chunyuan Li, Yuheng Li, and Yong Jae Lee. Improved baselines with visual instruction tuning, 2023. 7

[23] Haotian Liu, Chunyuan Li, Qingyang Wu, and Yong Jae Lee. Visual instruction tuning, 2023. 1, 2, 6, 7

[24] Hong Liu, Zhiyuan Li, David Hall, Percy Liang, and Tengyu Ma. Sophia: A scalable stochastic second-order optimizer for language model pre-training. *arXiv preprint arXiv:2305.14342*, 2023. 1

[25] Ze Liu, Han Hu, Yutong Lin, Zhuliang Yao, Zhenda Xie, Yixuan Wei, Jia Ning, Yue Cao, Zheng Zhang, Li Dong, Furu Wei, and Baining Guo. Swin transformer v2: Scaling up capacity and resolution, 2022. 2, 1

[26] Wang Qi, Yu-Ping Ruan, Yuan Zuo, and Taihao Li. Parameter-efficient tuning on layer normalization for pre-trained language models, 2022. 2

[27] Alec Radford, Jeff Wu, Rewon Child, David Luan, Dario Amodei, and Ilya Sutskever. Language models are unsupervised multitask learners. 2019. 2

[28] Alec Radford, Jong Wook Kim, Chris Hallacy, Aditya Ramesh, Gabriel Goh, Sandhini Agarwal, Girish Sastry, Amanda Askell, Pamela Mishkin, Jack Clark, Gretchen Krueger, and Ilya Sutskever. Learning transferable visual models from natural language supervision, 2021. 2, 7

[29] Sylvestre-Alvise Rebuffi, Hakan Bilen, and Andrea Vedaldi. Learning multiple visual domains with residual adapters, 2017. 1

[30] Robin Rombach, Andreas Blattmann, Dominik Lorenz, Patrick Esser, and Björn Ommer. High-resolution image synthesis with latent diffusion models, 2022. 7

[31] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, Alexander C. Berg, and Li Fei-Fei. Imagenet large scale visual recognition challenge, 2015. 1

[32] Tianxiao Shen, Myle Ott, Michael Auli, and Marc'Aurelio Ranzato. Mixture models for diverse machine translation: Tricks of the trade, 2019. 3

[33] Amanpreet Singh, Ronghang Hu, Vedanuj Goswami, Guillaume Couairon, Wojciech Galuba, Marcus Rohrbach, and Douwe Kiela. Flava: A foundational language and vision alignment model, 2022. 2

[34] Jianlin Su, Yu Lu, Shengfeng Pan, Ahmed Murtadha, Bo Wen, and Yunfeng Liu. Roformer: Enhanced transformer with rotary position embedding, 2022. 1

[35] Hugo Touvron, Louis Martin, Kevin Stone, Peter Albert, Amjad Almahairi, Yasmine Babaei, Nikolay Bashlykov, Soumya Batra, Prajjwal Bhargava, Shruti Bhosale, Dan Bikel, Lukas Blecher, Cristian Canton Ferrer, Moya Chen, Guillem Cucurull, David Esiobu, Jude Fernandes, Jeremy Fu, Wenyin Fu, Brian Fuller, Cynthia Gao, Vedanuj Goswami, Naman Goyal, Anthony Hartshorn, Saghar Hosseini, Rui Hou, Hakan Inan, Marcin Kardas, Viktor Kerkez, Madian Khabsa, Isabel Kloumann, Artem Korenev, Punit Singh Koura, Marie-Anne Lachaux, Thibaut Lavril, Jenya Lee, Diana Liskovich, Yinghai Lu, Yuning Mao, Xavier Martinet, Todor Mihaylov, Pushkar Mishra, Igor Molybog, Yixin Nie, Andrew Poulton, Jeremy Reizenstein, Rashi Rungta, Kalyan Saladi, Alan Schelten, Ruan Silva, Eric Michael Smith, Ranjan Subramanian, Xiaoqing Ellen Tan, Binh Tang, Ross Taylor, Adina Williams, Jian Xiang Kuan, Puxin Xu, Zheng Yan, Iliyan Zarov, Yuchen Zhang, Angela Fan, Melanie Kambadur, Sharan Narang, Aurelien Rodriguez, Robert Stojnic, Sergey Edunov, and Thomas Scialom. Llama 2: Open foundation and fine-tuned chat models, 2023. 1, 2

[36] Aaron van den Oord, Oriol Vinyals, and Koray Kavukcuoglu. Neural discrete representation learning, 2018. 7

[37] Guangxuan Xiao, Yuandong Tian, Beidi Chen, Song Han, and Mike Lewis. Efficient streaming language models with attention sinks, 2023. 6

[38] Wenhan Xiong, Jingyu Liu, Igor Molybog, Hejia Zhang, Prajjwal Bhargava, Rui Hou, Louis Martin, Rashi Rungta, Karthik Abinav Sankararaman, Barlas Oguz, Madian Khabsa, Han Fang, Yashar Mehdad, Sharan Narang, Kshitiz Malik, Angela Fan, Shruti Bhosale, Sergey Edunov, Mike Lewis, Sinong Wang, and Hao Ma. Effective long-context scaling of foundation models, 2023. 1

[39] Zhewei Yao, Xiaoxia Wu, Conglong Li, Minjia Zhang, Heyang Qin, Olatunji Ruwase, Ammar Ahmad Awan, Samyam Rajbhandari, and Yuxiong He. Deepspeed-visualchat: Multi-round multi-image interleave chat via multi-modal causal attention, 2023. 1, 2, 3, 4

[40] Elad Ben Zaken, Shauli Ravfogel, and Yoav Goldberg. Bitfit: Simple parameter-efficient fine-tuning for transformer-based masked language-models, 2022. 1, 2

[41] Xiaohua Zhai, Xiao Wang, Basil Mustafa, Andreas Steiner, Daniel Keysers, Alexander Kolesnikov, and Lucas Beyer. Lit: Zero-shot transfer with locked-image text tuning, 2022. 2

Context-PEFT: Efficient Multi-Modal, Multi-Task Fine-Tuning

Supplementary Material

6. Vision Encoder Details

We experiment with two versions of the Swin Transformer V2 [25], 'Tiny' and 'Large'.

The tiny variation is used for initial experimentation and fine grained comparisons of different adaptors. This variation was pre-trained for image classification on ImageNet-1k [31] and has a final embedding dimension of 768. The weights and model were provided by HuggingFace[1].

The large variation is used for final evaluation and coarse grained comparisons with the best adaptor variants. This variation was pre-trained for image classification on ImageNet-21k [31], further fine-tuned for ImageNet-1k, and has a final embedding dimension of 1536. The weights and model were provided by HuggingFace[2].

7. LLM Pre-Training Details

The LLM has 150 million parameters with an embedding dimension of 768, 12 layers of transformer blocks, 12 attention heads per attention layer utilising Rotary Position Embeddings [34] with an adjusted base frequency (RoPE ABF [38]), SwiGLU activation [6] in the feed forward layers with an intermediate size of 6144/3072, and using a frozen embedding layer taken from OPT-125m[3] to speed up convergence. We make use of FlashAttention 2 [8] to attain better performance and memory utilisation than vanilla dot-product attention.

We also train the model with a Transformer-XL style cache and shifting window [7], although instead of saving keys and values we cache the hidden states pre-projection and recompute them for each segment. This introduces some additional training and inference latency when the cache is in use, but comes with the advantage of generating partial gradients for the XL-cache and halves the persistent memory cost for the cache when accumulating gradients over several sub-batches.

The Sophia optimiser was used [24] for pre-training, with a warm-up of approximately 2000 batches to a learning rate of 6e-4 and cosine annealed to a learning rate of 6e-5, using a batch size of 480, sequence length of 1024 tokens (with additional XL memory of 1024 states for total context size of 2048) and optimiser hyper-parameters suggested by the original Sophia authors.

We train for 5 billion tokens on the now defunct Pile dataset. The Pile was removed from its hosting platform due to containing some copyrighted materials, but this removal occurred after the start of this work. Alternatives such as the Pile-Uncopyrighted[4] exist and should provide comparable performance in terms of pre-training.

8. Heatmaps

We provide auxiliary heatmap visualisations to further illustrate the image-text semantic understanding capabilities of our model.

Target tokens="little girl" - Layer=5
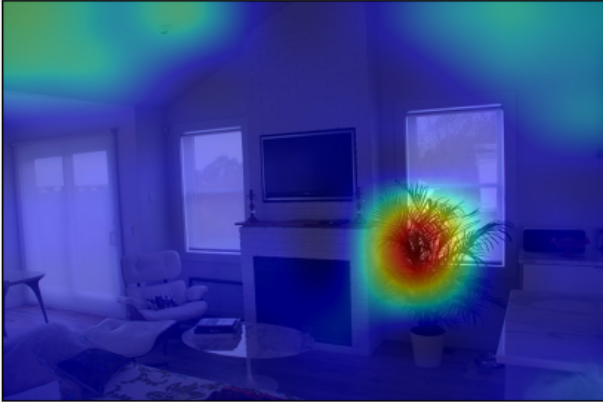

Target tokens="Group of sheep" - Layer=5

---

[1]SwinT V2 Tiny on Hugging Face
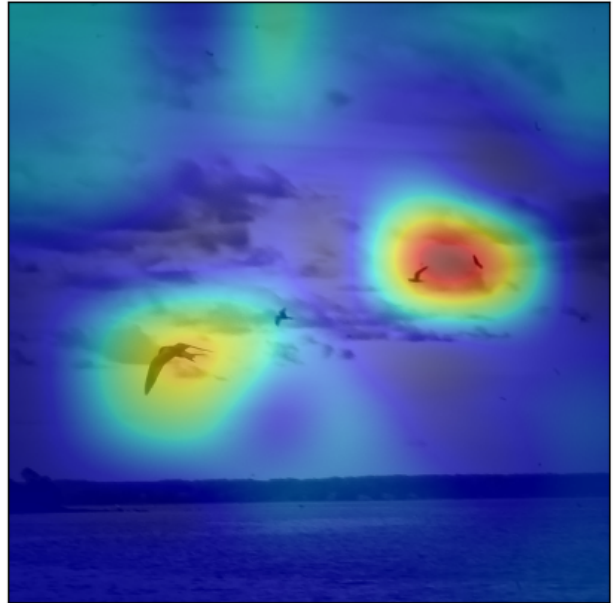[2]SwinT V2 Large on Hugging Face
[3]OPT-125m on Hugging Face
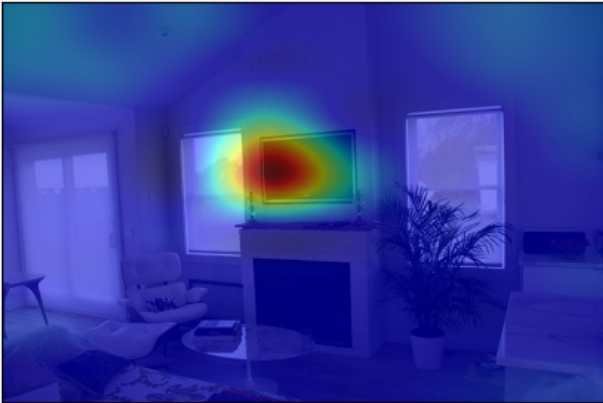[4]Pile-Uncopyrighted on Hugging Face

Target tokens=", plant" - Layer=5

Target tokens="flock of small birds" - Layer=5
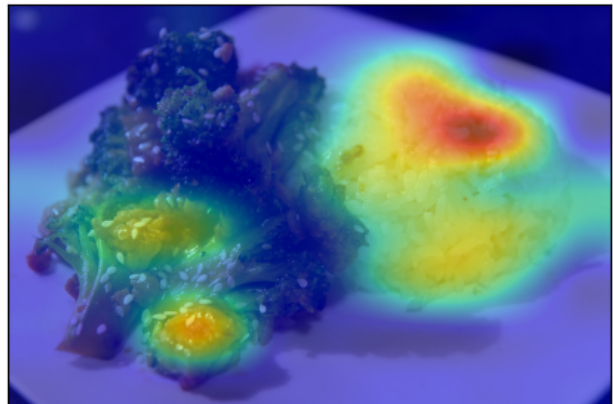

Target tokens="a TV" - Layer=5

Target tokens="blowing out a candle" - Layer=5

Target tokens="red stop sign" - Layer=9

Target tokens="rice" - Layer=5

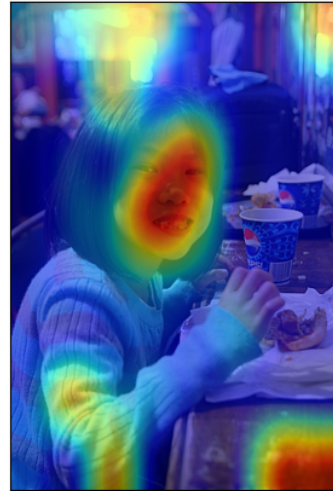Target tokens="herd of livestock" - Layer=5

Target tokens="A woman" - Layer=5

Target tokens="child standing" - Layer=5

Target tokens="A young girl" - Layer=5

Target tokens="plate full" - Layer=5

Target tokens="as she eats her sandwich" - Layer=5