# CENG501 – Deep Learning Week 9

Fall 2024

Sinan Kalkan

Dept. of Computer Engineering, METU

# In-context Learning (Prompt Engineering)

### Three ways of in-context learning:

#### Zero-shot

The model predicts the answer given only a natural language description of the task. No gradient updates are performed.



#### One-shot

In addition to the task description, the model sees a single example of the task. No gradient updates are performed.



### In a single sequence input, the prompted example can learn from previous demonstrations.

### Few-shot

In addition to the task description, the model sees a few examples of the task. No gradient updates are performed.



# In-context Learning: How/Why Does it Work?

A Bayesian interpretation:

 $p(\text{output}|\text{prompt}) = \int_{\text{component}} p(\text{output}|\text{concept}, \text{prompt}) p(\text{concept}|\text{prompt}) d(\text{concept})$ 

- During pretraining, the network learns a latent concept space.
- With the prompt, we provide sufficient examples to estimate the most relevant concept –  $p$ (concept | prompt).



Hendel et al., "In-Context Learning Creates Task Vectors", 2023.



Figure 5: A t-SNE plot of task vectors. A 2D t-SNE plot visualizing 50 task vectors for each task, each generated from a different choice of  $S$  and  $x'$  using LLaMA 7B. Points are color-coded according to the task. Each task can be seen to form its own distinct cluster.



Figure 1: ICL as learning in a Hypothesis Class. In ICL, one provides an LLM with a prompt including demonstrations  $S$  of some task, and a query  $x$ . The model generates the output for  $x$  (here "Yellow"). We show that the underlying process can be broken down into two parts:  $A$ , a "learning algorithm" (marked in blue), computes a query-agnostic vector  $\theta(S)$ , which we view as a parameter of a function in a hypothesis class. The second part, denoted by  $f$  and marked in yellow, is the application of the rule defined by  $\theta$  on the query  $x$ , without direct dependence on  $S$ .

# In-context Learning: Important Factors

**Min et al., "Rethinking the Role of Demonstrations:** What Makes In-Context Learning Work?", 2022.



Figure 7: Four different aspects in the demonstrations: the input-label mapping, the distribution of the input text, the label space, and the use of input-label pairing as the format of the demonstrations.

### **Abstract**

Large language models (LMs) are able to incontext learn—perform a new task via inference alone by conditioning on a few inputlabel pairs (demonstrations) and making predictions for new inputs. However, there has been little understanding of how the model learns and which aspects of the demonstrations contribute to end task performance. In this paper, we show that ground truth demonstrations are in fact not required—randomly replacing labels in the demonstrations barely hurts performance on a range of classification and multi-choce tasks, consistently over 12 different models including GPT-3. Instead, we find that other aspects of the demonstrations are the key drivers of end task performance, including the fact that they provide a few examples of  $(1)$  the label space,  $(2)$  the distribution of the input text, and (3) the overall format of the sequence. Together, our analysis provides a new way of understanding how and why in-context learning works, while opening up new questions about how much can be learned from large language models through inference alone.

# Ingéontext Learning: Limitations

- **Model Parameters and Scale:** Scale helps!
- **Training Data Dependency:** Dataset size matters!
- **Domain Specificity:**
	- "While LLMs can generalize across various tasks, there might be limitations when dealing with highly specialized domains. Domain-specific data might be required to achieve optimal results."

### • **Model Fine-Tuning:**

- "Even with ICL, there might be scenarios where model fine-tuning becomes necessary to cater to specific tasks or correct undesirable emergent abilities."
- **Ethics and Fairness**
- **Privacy and Security**

Wei et al., "Chain-of-Thought Prompting Elicits Reasoning in Large Language Models", NeurlPS 2022.

# Clarin of Thought

### **Model Input**

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: The answer is 11.

Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?

A: The answer is 27.  $\blacktriangleright$ 

**Model Output** 

### **Chain-of-Thought Prompting**

### **Model Input**

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: Roger started with 5 balls. 2 cans of 3 tennis balls each is 6 tennis balls.  $5 + 6 = 11$ . The answer is 11.

Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?

### **Model Output**

A: The cafeteria had 23 apples originally. They used 20 to make lunch. So they had  $23 - 20 = 3$ . They bought 6 more apples, so they have  $3 + 6 = 9$ . The answer is  $9.$ 

Kojima et al., "Large Language Models are Zero-Shot Reasoners", NeurlPS 2022.

# Zero-shot Chain of Thought

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: The answer is 11.

А:

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

(Output) The answer is 8. X

### (c) Zero-shot

 $Q: A$  juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A: The answer (arabic numerals) is

(Output)  $8 X$ 

### (b) Few-shot-CoT

 $Q:$  Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: Roger started with 5 balls. 2 cans of 3 tennis balls each is 6 tennis balls,  $5 + 6 = 11$ . The answer is 11.

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

А:

(Output) The juggler can juggle 16 balls. Half of the balls are golf balls. So there are  $16 / 2 = 8$  golf balls. Half of the golf balls are blue. So there are  $8/2 = 4$  blue golf balls. The answer is 4.  $\checkmark$ 

### (d) Zero-shot-CoT (Ours)

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A: Let's think step by step.

(Output) There are 16 balls in total. Half of the balls are golf balls. That means that there are 8 golf balls. Half of the golf balls are blue. That means that there are 4 blue golf balls. V

Standard Prompting

> Meta Prompting

Thang et al., "Meta Prompting for AI Systems", 2024.<br>
Solution: The domain of the expression  $\frac{\sqrt{x-2}}{5-x}$ .<br>
Solution: The expressions inside each square root must be non-negative. Therefore,  $x-2\geq 0$ , so<br>  $x\geq 2$ , an Problem: Find the domain of the expression  $\frac{\sqrt{x-2}}{\sqrt{5-x}}$ . Solution: The expressions inside each square root must be non-negative. Therefore,  $x - 2 \ge 0$ , so  $x \ge 2$ , and  $5 - x \ge 0$ , so  $x \le 5$ . Also, the denominator cannot be equal to zero, so  $5 - x > 0$ , which gives  $x < 5$ . Therefore, the domain of the expression is  $(2, 5)$ . Final Answer: The final answer is  $[2, 5)$ . I hope it is correct.

> Problem: If det  $A = 2$  and det  $B = 12$ , then find det( $AB$ ). Solution: We have that  $\det(AB) = (\det A)(\det B) = (2)(12) = 24$ . Final Answer: The final answer is 24. I hope it is correct.

**Problem Statement:** 

 $\cdots$ 

• Problem: [question to be answered]

### **Solution Structure:**

- 1. Begin the response with "Let's think step by step."
- 2. Follow with the reasoning steps, ensuring the solution process is broken down clearly and logically.
- 3. End the solution with the final answer encapsulated in a LaTeX-formatted box,  $\Box$ , for clarity and emphasis.
- 4. Finally, state "The answer is [final answer to the problem].", with the final answer presented in LaTeX notation.

Figure 1: A structure meta prompt presented in markdown format for solving MATH [17] problems.



Figure 1: An example for comparison between Chain-of-Thought (CoT) and Chain-of-Symbol (COS) that elicits large language models in tackling complex planning tasks with higher performance and fewer input tokens. We let the model generate CoT/COS during inference in a few-shot manner. Results were taken in May 2023 with ChatGPT and can be subject to change.

Liu et al., "Generated Knowledge Prompting for Commonsense Reasoning", 2022.

# Gereen were die termated knowledge prompting

sense reasoning while maintaining the flexibility of pretrained sequence models. To investigate this question, we develop generated knowledge prompting, which consists of generating knowledge from a language model, then providing the knowledge as additional input when answering a question. Our method does not require task-specific supervision for knowledge integration, or access to a structured knowledge base, yet it improves performance of large-scale, state-of-the-art models on four commonsense reasoning tasks, achieving state-of-the-art results on numerical commonsense (NumerSense), general commonsense (CommonsenseQA 2.0), and scientific commonsense (QASC) benchmarks. Generated knowledge prompting highlights largescale language models as flexible sources of external knowledge for improving common-



Figure 1: Generated knowledge prompting involves (i) using few-shot demonstrations to generate questionrelated knowledge statements from a language model; (ii) using a second language model to make predictions with each knowledge statement, then selecting the highest-confidence prediction.



Wang et al., "Self-Consistency Improves Chain of Thought Reasoning in Language Models", 2023.



Figure 1: The self-consistency method contains three steps: (1) prompt a language model using chain-of-thought (CoT) prompting; (2) replace the "greedy decode" in CoT prompting by sampling from the language model's decoder to generate a diverse set of reasoning paths; and (3) marginalize out the reasoning paths and aggregate by choosing the most consistent answer in the final answer set.

# Automatic Prompt Engineer Zhou et al., "LARGE LANGUAGE MODELS ARE

HUMAN-LEVEL PROMPT ENGINEERS", 2023.



(a) Automatic Prompt Engineer (APE) workflow

### (b) Interquartile mean across 24 tasks



Figure 1: Schematic illustrating various approaches to problem solving with LLMs. Each rectangle box represents a *thought*, which is a coherent language sequence that serves as an intermediate step toward problem solving. See concrete examples of how thoughts are generated, evaluated, and searched in Figures 2,4,6.

# Progression-Aided LMs

### Gao et al., "PAL: Program-aided Language Models", 2023.

tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: Roger started with 5 tennis balls. 2 cans of 3 tennis balls each is 6 tennis balls.  $5 + 6 = 11$ . The answer is 11.

Q: The bakers at the Beverly Hills Bakery baked 200 loaves of bread on Monday morning. They sold 93 loaves in the morning and 39 loaves in the afternoon. A grocery store returned 6 unsold loaves. How many loaves of bread did they have left?

#### Model Output

A: The bakers started with 200 loaves. They sold 93 in the morning and 39 in the afternoon. So they sold 93 + 39 = 132 loaves. The grocery store returned 6 loaves. So they had  $200 - 132 - 6 = 62$  loaves left.

The answer is 62.

Program-aided Language models (this work)

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

```
A: Roger started with 5 tennis balls.
tennis balls = 52 cans of 3 tennis balls each is
bought balls = 2 * 3tennis balls. The answer is
answer = tennis balls + bought balls
```
Q: The bakers at the Beverly Hills Bakery baked 200 loaves of bread on Monday morning. They sold 93 loaves in the morning and 39 loaves in the afternoon. A grocery store returned 6 unsold loaves. How many loaves of bread did they have left?

Model Output

>>> print(answe

Input

A: The bakers started with 200 loaves loaves baked =  $200$ They sold 93 in the morning and 39 in the afternoon  $loaves sold morning = 93$ loaves sold afternoon =  $39$ The grocery store returned 6 loaves. loaves returned =  $6$ The answer is answer = loaves baked - loaves sold morning - loaves sold afternoon + loaves returned LLMS as Agents Wang et al., "A Survey on Large Language Model based Autonomous Agents", 2024. **Profile Memory Planning Action Profile Contents Memory Structure Action Target Planning w/o Feedback**  $\triangleright$  Unified Memory  $\triangleright$  Task Completion  $\triangleright$  Exploration > Demographic Information  $\triangleright$  Communication  $\triangleright$  Single-path Reasoning  $\triangleright$  Hybrid Memory  $\triangleright$  Personality Information **Action Production**  $\triangleright$  Multi-path Reasoning **Memory Formats**  $\triangleright$  Social Information > Memory Recollection  $\triangleright$  External Planner  $\triangleright$  Languages  $\triangleright$  Databases  $\triangleright$  Plan Following **Generation Strategy**  $\triangleright$  Embeddings  $\triangleright$  Lists **Planning w/ Feedback Action Space Memory Operation**  $\triangleright$  Handcrafting Method > Tools > Self-Knowledge  $\triangleright$  Environment Feedback  $\triangleright$  Memory Reading > LLM-Generation Method **Action Impact**  $\triangleright$  Human Feedback  $\triangleright$  Memory Writing  $\triangleright$  Environments  $\triangleright$  New Actions > Dataset Alignment Method  $\triangleright$  Model Feedback > Memory Reflection  $\triangleright$  Internal States

Fig. 2 A unified framework for the architecture design of LLM-based autonomous agent.

LLMS as Agents

### Prompting/Planning with feedback

(1d) ReAct (Reason + Act)

Thought 1: I need to search Apple Remote and find the program it was originally designed to interact with. Act 1: Search [Apple Remote] Obs 1: The Apple Remote is a remote control introduced in October 2005 by Apple ... originally designed to control the Front Row media center program ...

Thought 2: Apple Remote was originally designed to control the Front Row media center program. I need to search Front Row next and find what other device can control it. Act 2: Search [Front Row] Obs 2: Could not find [Front Row]. Similar: ['Front Row Seat to Earth', 'Front Row Motorsports',' Front Row  $(software)$ ', ...]

Thought 3: Front Row is not found. I need to search Front Row (software).

Act 3: Search [Front Row (software)

Obs 3: Front Row is a discontinued media center software ...

Thought 4: Front Row (software) is controlled by an Apple Remote or the keyboard function keys. So the answer is keyboard function keys. Act 4: Finish [keyboard function keys]

Yao et al., "ReAct: Synergizing Reasoning and Acting in Language Models", 2023.

# Prejiously of Autogen, LangChain, AutoGPT, Langroid, OpenAgents, ....



Autogen:

**Agent Customization** 

**WS as Agents** 

**Flexible Conversation Patterns** 

# LLWS as Agents: Challenges Example 1103. UIIdIIeng

- **Role-playing capability**: LLM-based agents typically need to adapt a role to effectively complete tasks in a domain. For roles that the LLM doesn't characterize well, it's possible to fine-tune the LLM on data that represent uncommon roles or psychology characters.
- **Long-term planning and finite context length**: planning over a lengthy history remains a challenge that could lead to errors that the agent may not recover from. LLMs are also limited in context length they can support which could lead to constraints that limit the capabilities of the agent such as leveraging short-term memory.
- **Generalized human alignment**: it's also challenging to align agents with diverse human values which is also common with standard LLMs. A potential solution involves the potential to realign the LLM by designing advanced prompting strategies.
- **Prompt robustness and reliability**: an LLM agent can involve several prompts designed to power the different modules like memory and planning. It's common to encounter reliability issues in LLMs with even the slightest changes to prompts. LLM agents involve an entire prompt framework which makes it more prone to robustness issues. The potential solutions include crafting prompt elements through trial and error, automatically optimizing/tuning prompts, or automatically generating prompts using GPT. Another common issue with LLMs is hallucination which is also prevalent with LLM agents. These agents rely on natural language to interface with external components that could be introducing conflicting information leading to hallucination and factuality issues.
- **Knowledge boundary**: similar to knowledge mismatch issues that could lead to hallucination or factuality issues, it's challenging to control the knowledge scope of LLMs which can significantly impact the effectiveness of simulations. Concretely, an LLM's internal knowledge could introduce biases or utilize user-unknown knowledge that could affect the agent's behavior when operating in specific environments.
- **Efficiency**: LLM agents involve a significant amount of requests that are handled by the LLM which could affect the efficiency of agent actions because it would depend heavily on the LLM inference speed. Cost is also a concern when deploying multiple agents.



Gao et al., "Retrieval -Augmented Generation for Large Language Models: A Survey", 2024. <sup>20</sup> • Parameter-efficient Finetuning (vs. Full Finetuning)

• Update a subset of parameters

Finetuning an LLM

- LoRA, LoRA+
- LASER (not finetuning actually)

Hu et al., "LORA: LOW-RANK ADAPTATION OF LARGE LANGUAGE MODELS", 2021.



Target: Attention blocks

Fig: https://magazine.sebastianraschka.com/p/practical-tips-for-finetuning-llms

**Abstract** 

LONEY ONT In this paper, we show that Low Rank Adaptation (LoRA) as originally introduced in (Hu et al., 2021) leads to suboptimal finetuning of models with large width (embedding dimension). This is due to the fact that adapter matrices  $A$  and  $B$  in LoRA are updated with the same learning rate. Using scaling arguments for large width networks, we demonstrate that using the same learning rate for  $A$  and  $B$  does not allow efficient feature learning. We then show that this suboptimality of LoRA can be corrected simply by setting different learning rates for the LoRA adapter matrices  $A$  and  $B$  with a well-chosen fixed ratio. We call this proposed algorithm LoRA+. In our extensive experiments,  $LoRA+$ improves performance  $(1\% - 2\%$  improvements) and finetuning speed (up to  $\sim 2X$  SpeedUp), at the same computational cost as LoRA.

Hayou et al., "LoRA+: Efficient Low Rank Adaptation of Large Models", 2024.



Figure 1. The key difference between standard LoRA and LoRA+ is in how learning rates are set (the matrices  $G_A$  and  $G_B$  are 'effective' gradients from AdamW) With standard LoRA, the learning rate is the same for  $A$  and  $B$ , which provably leads to suboptimal learning when embedding dimension is large. In LoRA+, we set the learning rate of B to be  $\lambda \times$  that of A, where  $\lambda \gg 1$  is fixed. We later provide guidelines on how to set  $\lambda_3$ 

# Fineturing an LLM: Challenges

1. Overfitting: Fine-tuning can be prone to overfitting, a condition where the model becomes overly specialized on the training data and pertowns poorly on unseen data. This risk is particularly pronounced when the task-specific dataset is small or not representative of the **broader** context.

**2. Catastrophic Forgetting:** During fine-tuning for a specific task, the model may forget previously acquired general knowledge. This phenomenon, known as catastrophic forgetting, can impair the model's adaptability to diverse tasks.

- **3. Bias Amplification:** Pre-trained models inherit biases from their training data, which fine-tuning can inadvertently amplify when applied to task-specific data. This amplification may lead to biased predictions and outputs, potentially causing ethical concerns.
- **4. Generalization Challenges:** Ensuring that a fine tuned model generalizes effectively across various inputs and scenarios is challenging. A model that excels in fine-tuning datasets may struggle when presented with out-of-distribution data.
- **5. Data Requirements:** Fine-tuning necessitates task-specific labelled data, which may not always be available or clean. Inadequate or noisy data can negatively impact the model's performance and reliability.
- **6. Hyperparameter Tuning Complexity:** Selecting appropriate hyperparameters for fine-tuning can be intricate and time-consuming. Poor choices may result in slow convergence, overfitting, or suboptimal performance.
- **7. Domain Shift Sensitivity:** Fine-tuning data significantly different from the pre-training data can lead to domain shift issues. Addressing this problem often requires domain adaptation techniques to bridge the gap effectively.
- **8. Ethical Considerations:** Fine tuned large language models may inadvertently generate harmful or inappropriate content, even when designed for benign tasks. Ensuring ethical behaviour and safety is an ongoing challenge, necessitating responsible AI practices.
- **9. Resource Intensiveness:** Fine-tuning large models demands substantial computational resources and time, posing challenges for smaller teams or organizations with limited infrastructure and expertise.
- **10.Unintended Outputs:** Fine-tuning cannot guarantee that the model consistently produces correct or sensible outputs. It may generate plausible but factually incorrect responses, requiring vigilant post-processing and validation.
- **11.Model Drift:** Over time, a fine tuned model's performance can deteriorate due to changes in data distribution or the evolving environment. Regular monitoring and re-fine-tuning may become necessary to maintain optimal performance and adapt to evolving conditions.

### The Batch



https://www.deeplearning.ai/the-batch/issue-276/

# Today

- Vision Models
	- Vision Transformers
	- Swin Transformers
	- Fast/Faster ViTs
	- Pretraining

## Administrative Notes

- New quiz this week
	- Deadline: Tomorrow midnight

### • Time plan for the projects

- 1. Milestone (November 24, midnight):
	- Github repo will be ready
	- Read & understand the paper
	- Download the datasets
	- Prepare the Readme file excluding the results & conclusion
- 2. Milestone (December 8, midnight)
	- The results of the first experiment
- 3. Milestone (January 5, midnight)
	- Final report (Readme file)
	- Repo with all code & trained models

### AN IMAGE IS WORTH 16X16 WORDS: **TRANSFORMERS FOR IMAGE RECOGNITION AT SCALE**

Alexey Dosovitskiy\*,<sup>†</sup>, Lucas Beyer\*, Alexander Kolesnikov\*, Dirk Weissenborn\*, Xiaohua Zhai\*, Thomas Unterthiner, Mostafa Dehghani, Matthias Minderer, Georg Heigold, Sylvain Gelly, Jakob Uszkoreit, Neil Houlsby\*,† \*equal technical contribution, <sup>†</sup>equal advising Google Research, Brain Team {adosovitskiy, neilhoulsby}@google.com

Vision Transformers (ViT)

## ViT: Motivation

- NLP:
	- Successful results of Transformers
	- De facto architecture
- Vision:
	- CNNs are dominantly used
- Prior work
	- Self-attention among pixels. Limit attention to local regions to reduce complexity (Parmar et al., 2018)
	- Self-attention among blocks of different sizes (Weissenborn et al., 2019)
	- Self attention between 2x2 patches (Cordonnier et al., 2020)

## ViT: Motivation

- Prior work
	- Self attention between 2x2 patches (Cordonnier et al., 2020)



Figure 1: Illustration of a Multi-Head Self-Attention layer applied to a tensor image  $X$ . Each head h attends pixel values around shift  $\Delta^{(h)}$  and learn a filter matrix  $W_{val}^{(h)}$ . We show attention maps computed for a query pixel at position  $q$ .

## ViT: Motivation

- Contributions
	- Use plain transformers without modifications
	- Compared to Cordonnier et al. (2020):
		- ViT shows strong results with large datasets & pretraining
		- ViT works with larger patches (generalizes better)
- Challenges in using Transformers with images:
	- How to convert an image into tokens?
	- How to encode position?
	- Transformers lack translation invariance and locality
	- Spoiler: They underperform on "small" datasets

Applied to classification tasks only!

### VIT: Architecture





# ViT: Pretraining

- Supervised pretraining on large datasets and finetuning on smaller downstream tasks
- Higher resolutions:
	- The whole network can easily be applied to longer sequences (= higher resolutions)
	- Learned position embeddings are interpolated

### **ViT: Results**







This ICCV paper is the Open Access version, provided by the Computer Vision Foundation. Except for this watermark, it is identical to the accepted version; 2021 the final published version of the proceedings is available on IEEE Xplore.



This CVPR paper is the Open Access version, provided by the Computer Vision Foundation. Except for this watermark, it is identical to the accepted version; the final published version of the proceedings is available on IEEE Xplore.



### Swin Transformer: Hierarchical Vision Transformer using Shifted Windows

Ze Liu<sup>1,2†\*</sup> Yutong Lin<sup>1,3†\*</sup> Yue Cao<sup>1\*</sup> Han Hu<sup>1\*‡</sup> Yixuan Wei<sup>1,4†</sup> Zheng Zhang<sup>1</sup> Stephen  $Lin<sup>1</sup>$  Baining Guo<sup>1</sup> <sup>1</sup>Microsoft Research Asia  $\frac{2 \text{University of Science and Technology of China}}{2 \text{University of Science}}$  $3X$ ian Jiaotong University  $4T\sin\phi$ hua University

{v-zeliu1, v-yutlin, yuecao, hanhu, v-yixwe, zhez, stevelin, bainguo}@microsoft.com

### Swin Transformer V2: Scaling Up Capacity and Resolution

Ze Liu<sup>2\*</sup> Han Hu<sup>1\*†</sup> Yutong Lin<sup>3</sup> Zhuliang Yao<sup>4</sup> Zhenda Xie<sup>4</sup> Yixuan Wei<sup>4</sup> Jia Ning<sup>5</sup> Yue Cao<sup>1</sup> Zheng Zhang<sup>1</sup> Li Dong<sup>1</sup> Furu Wei<sup>1</sup> Baining Guo<sup>1</sup> <sup>1</sup>Microsoft Research Asia  $\frac{2 \text{University of Science and Technology of China}}{2 \text{University of Science}}$  ${}^{3}$ Xian Jiaotong University  ${}^{4}$ Tsinghua University  ${}^{5}$ Huazhong University of Science and Technology {t-liuze, hanhu, t-yutonglin, t-zhuyao, t-zhxie, t-yixuanwei, v-jianing}@microsoft.com {yuecao, zhez, lidong1, fuwei, bainguo}@microsoft.com

# Swin Transformers

# Swin Transformer v1

- Motivation:
	- ViT is promising but limited to classification
	- Challenges in using Tranformers:
		- large variations in scales of visual entities,
		- more pixels compared to words in text
	- Existing Transformers use fixed token size across layers
- Contributions:
	- Limit self-attention to non -overlapping windows while allowing cross -window attention
	- Change token size across layers






Figure 3. (a) The architecture of a Swin Transformer (Swin-T); (b) two successive Swin Transformer Blocks (notation presented with Eq.  $(3)$ ). W-MSA and SW-MSA are multi-head self attention modules with regular and shifted windowing configurations, respectively.



 $\frac{37}{37}$  Image: http://dx.doi.org/10.48550/arXiv.2206.03336







Figure: https://amaarora.github.io/posts/2022-07-04-swintransformerv1.html

**Relative position bias** In computing self-attention, we follow  $[49, 1, 32, 33]$  by including a relative position bias  $B \in \mathbb{R}^{M^2 \times M^2}$  to each head in computing similarity:

Attention(Q, K, V) = SoftMax( $QK^T/\sqrt{d} + B)V$ , (4)

where Q, K,  $V \in \mathbb{R}^{M^2 \times d}$  are the *query*, key and *value* matrices; d is the *querylkey* dimension, and  $M^2$  is the number of patches in a window. Since the relative position along each axis lies in the range  $[-M+1, M-1]$ , we parameterize a smaller-sized bias matrix  $\hat{B} \in \mathbb{R}^{(2M-1)\times(2M-1)}$ , and values in B are taken from  $\hat{B}$ .

#### Plot from https://arxiv.org/pdf/2107.14222:



#### $(a)$  top-left

(b) center

Figure 6: Visualization of Euclidean method. The red star  $\star$  presents the reference position. Different color means different bucket. The relative positions with the same color share the same encoding.

**Relative position bias** In computing self-attention, we follow  $[49, 1, 32, 33]$  by including a relative position bias  $B \in \mathbb{R}^{M^2 \times M^2}$  to each head in computing similarity:

Attention(Q, K, V) = SoftMax( $QK^T/\sqrt{d} + B)V$ , (4)

where Q, K,  $V \in \mathbb{R}^{M^2 \times d}$  are the *query*, key and *value* matrices; d is the *querylkey* dimension, and  $M^2$  is the number of patches in a window. Since the relative position along each axis lies in the range  $[-M+1, M-1]$ , we parameterize a smaller-sized bias matrix  $\hat{B} \in \mathbb{R}^{(2M-1)\times(2M-1)}$ , and values in B are taken from  $\hat{B}$ .



Table 4. Ablation study on the *shifted windows* approach and different position embedding methods on three benchmarks, using the Swin-T architecture. w/o shifting: all self-attention modules adopt regular window partitioning, without *shifting*; abs. pos.: absolute position embedding term of ViT; rel. pos.: the default settings with an additional relative position bias term (see Eq.  $(4)$ ); app.: the first scaled dot-product term in Eq.  $(4)$ .

# Swin Transformer v1: Results



Table 1. Comparison of different backbones on ImageNet-1K classification. Throughput is measured using the GitHub repository of  $[62]$  and a V100 GPU, following  $[57]$ .



Table 2. Results on COCO object detection and instance segmentation.  $\dagger$  denotes that additional decovolution layers are used to produce hierarchical feature maps. \* indicates multi-scale testing.

Motivation:

- "Large-scale NLP models have been shown to significantly improve the performance on language tasks with no signs of saturation".
- "They also demonstrate amazing few-shot capabilities like that of human beings" Contribution:
- "Explore large-scale models in computer vision"
- Three major issues & solutions:
	- Training stability: "1) a residual-post-norm method combined with cosine attention to improve training stability"
	- resolution gaps between pre-training and fine-tuning: "2) A log-spaced continuous position bias method to effectively transfer models pre-trained using low-resolution images to downstream tasks with high-resolution inputs"
	- hunger on labelled data: "3) A self-supervised pretraining method, SimMIM, to reduce the needs of vast labeled images"

- Issues with v1
	- "An instability issue when scaling up model capacity."
	- "Degraded performance when transferring models across window resolutions."



Figure 3. SwinV1-H versus SwinV2-H in training [72].



Scaling up model capacity

- Residual post normalization: Prevents output to diverge
- Scaled cosine attention:
	- learnt attention maps of some blocks and heads are frequently dominated by a few pixel pairs, especially in the res -post -norm configuration => cosine yields values in a smaller range



#### Scaling Up Window Resolution

#### • Continuous relative position bias

 $B(\Delta x, \Delta y) = \mathcal{G}(\Delta x, \Delta y),$  $(3)$ 

where  $G$  is a small network, e.g., a 2-layer MLP with a ReLU activation in between by default.

The meta network  $G$  generates bias values for arbitrary relative coordinates, and thus can be naturally transferred to fine-tuning tasks with arbitrarily varying window sizes.

#### **Log-spaced coordinates**

Log-spaced coordinates When transferring across largely varying window sizes, a large portion of the relative coordinate range needs to be extrapolated. To ease this issue, we propose using log-spaced coordinates instead of the original linear-spaced ones:

$$
\widehat{\Delta x} = \text{sign}(x) \cdot \log(1 + |\Delta x|),
$$
  
\n
$$
\widehat{\Delta y} = \text{sign}(y) \cdot \log(1 + |\Delta y|),
$$
\n(4)

where  $\Delta x$ ,  $\Delta y$  and  $\widehat{\Delta x}$ ,  $\widehat{\Delta y}$  are the linear-scaled and logspaced coordinates, respectively.



#### Self-Supervised Pre-training

- Prior work used JFT-3B
- Use SimMIM to train 3B-size Swin Transformer



Figure 1. An illustration of our simple framework for masked language modeling, named SimMIM. It predicts raw pixel values of the randomly masked patches by a lightweight one-layer head, and performs learning using a simple  $\ell_1$  loss.

#### From SimMIM paper.



Table 2. Comparison with previous largest vision models on ImageNet-1K V1 and V2 classification. \* indicates the sparse model; the "pre-train time" column is measured by the TPUv3 core days with numbers copied from the original papers. † That of SwinV2-G is estimated according to training iterations and FLOPs.



Table 5. Comparison with previous best results on Kinetics-400 video action classification.



This CVPR paper is the Open Access version, provided by the Computer Vision Foundation. Except for this watermark, it is identical to the accepted version; 2022 the final published version of the proceedings is available on IEEE Xplore.

#### A ConvNet for the 2020s

Zhuang Liu<sup>1,2\*</sup> Hanzi Mao<sup>1</sup> Chao-Yuan Wu<sup>1</sup> Christoph Feichtenhofer<sup>1</sup> Trevor Darrell<sup>2</sup> Saining Xie<sup>1†</sup> <sup>1</sup>Facebook AI Research (FAIR) <sup>2</sup>UC Berkeley Code: https://github.com/facebookresearch/ConvNeXt

# ConvNeXt



This CVPR paper is the Open Access version, provided by the Computer Vision Foundation. Except for this watermark, it is identical to the accepted version; the final published version of the proceedings is available on IEEE Xplore.

2023

#### ConvNeXt V2: Co-designing and Scaling ConvNets with Masked Autoencoders

Sanghyun  $Woo^{1*}$ Shoubhik Debnath<sup>2</sup> Ronghang  $Hu^2$ Xinlei Chen<sup>2</sup> Zhuang Liu<sup>2</sup> In So Kweon<sup>1</sup> Saining  $Xie^{3\dagger}$ <sup>2</sup> Meta AI, FAIR  ${}^{1}$ KAIST <sup>3</sup>New York University

Code: https://github.com/facebookresearch/ConvNeXt-V2

• "Modernized" ResNet

ImageNet-1K Acc.



Figure 1. ImageNet-1K classification results for • ConvNets and o vision Transformers. Each bubble's area is proportional to FLOPs of a variant in a model family. ImageNet-1K/22K models here take  $224^2/384^2$  images respectively. ResNet and ViT results were obtained with improved training procedures over the original papers. We demonstrate that a standard ConvNet model can achieve the same level of scalability as hierarchical vision Transformers while being much simpler in design.







- Training ConvNeXt v1 with Masked AE performs poorly
- Introduce
	- fully convolutional masked autoencoder framework and
	- a new Global Response Normalization to enhance inter -channel competition



Figure 1. ConvNeXt V2 model scaling. The ConvNeXt V2 model, which has been pre-trained using our fully convolutional masked autoencoder framework, performs significantly better than the previous version across a wide range of model sizes.

- Training ConvNext v1 with Masked AE performs poorly
- Introduce
	- fully convolutional masked autoencoder framework and
	- a new Global Response Normalization to enhance inter -channel competition



Figure 1. ConvNeXt V2 model scaling. The ConvNeXt V2 model, which has been pre-trained using our fully convolutional masked autoencoder framework, performs significantly better than the previous version across a wide range of model sizes.  $_{56}$ 

#### Fully Convolutional Masked Autoencoder

- Encoder:
	- Sparse conv to prevent simple copy-paste of input (not a problem in MAE with transformers)
	- Consider image as a 2D array of pixels
- Decoder: ConvNeXt block





Figure 2. Our FCMAE framework. We introduce a fully convolutional masked autoencoder (FCMAE). It consists of a sparse convolution-based ConvNeXt encoder and a lightweight ConvNeXt block decoder. Overall, the architecture of our autoencoder is asymmetric. The encoder processes only the visible pixels, and the decoder reconstructs the image using the encoded pixels and mask tokens. The loss is calculated only on the masked region.

Global Response Normalization

• Feature collapse: many dead/saturated feature maps





Global Response Normalization

- Inspiration from lateral inhibition in brain
- Three steps:
	- 1. global feature aggregation,
	- 2. feature normalization, and
	- 3. feature calibration.

Algorithm 1 Pseudocode of GRN in a PyTorch-like style.

# gamma, beta: learnable affine transform parameters # X: input of shape (N, H, W, C)

 $qx = torch.norm(X, p=2, dim=(1,2), keepdim=True)$  $nx = qx / (qx.mean(dim=-1, keepdim=True) + le-6)$ return gamma \*  $(X * nx)$  + beta + X

First, we aggregate a spatial feature map  $X_i$  into a vector *gx* with a global function  $G(\cdot)$ :

$$
\mathcal{G}(X) := X \in \mathcal{R}^{H \times W \times C} \to gx \in \mathcal{R}^C. \tag{1}
$$

Next, we apply a response normalization function  $\mathcal{N}(\cdot)$ to the aggregated values. Concretely, we use a standard divisive normalization as follows,

$$
\mathcal{N}(||X_i||) := ||X_i|| \in \mathcal{R} \to \frac{||X_i||}{\sum_{j=1,\dots,C} ||X_j||} \in \mathcal{R}, \tag{2}
$$

where  $||X_i||$  is the L2-norm of the *i*-th channel. <sup>1</sup> Intu-

Finally, we calibrate the original input responses using the computed feature normalization scores:

$$
X_i = X_i * \mathcal{N}(\mathcal{G}(X)_i) \in \mathcal{R}^{H \times W} \tag{3}
$$

#### Global Response Normalization



(a) Global aggregation  $G(\cdot)$ . L2 Norm-based aggregation function produces the best result.



(b) **Normalization operator,**  $N(\cdot)$ . Divisive normalization is an effective channel importance calibrator.







(d) Feature normalization. GRN outperforms (e) **Feature re-weighting**. GRN does effective and effi-(f) GRN in pre-training/fine-tuning. To be other normalizations through global contrasting. cient feature re-weighting without parameter overhead. effective, GRN should be used in both stages.

Table 2. GRN ablations with ConvNeXt-Base. We report fine-tuning accuracy on ImageNet-1K. Our final proposal is marked in gray.



Table 3. Co-design matters. When the architecture and the learning framework are co-designed and used together, masked image pre-training becomes effective for ConvNeXt. We report the finetuning performance from 800 epoch FCMAE pre-trained models. The relative improvement is bigger with a larger model.



Table 4. Comparisons with previous masked image modeling **approaches.** The pre-training data is the IN-1K training set. All self-supervised methods are benchmarked by the end-to-end finetuning performance with an image size of 224. We underline the highest accuracy for each model size and bold our best results.



This ICCV paper is the Open Access version, provided by the Computer Vision Foundation. Except for this watermark, it is identical to the accepted version; the final published version of the proceedings is available on IEEE Xplore.

2023

#### **FastViT: A Fast Hybrid Vision Transformer** using Structural Reparameterization

Pavan Kumar Anasosalu Vasu<sup>†</sup> James Gabriel Jeff Zhu Oncel Tuzel Anurag Ranjan<sup>†</sup>

Apple

Published as a conference paper at ICLR 2024

#### FASTERVIT: FAST VISION TRANSFORMERS WITH HIERARCHICAL ATTENTION

Ali Hatamizadeh, Greg Heinrich, Hongxu Yin, Andrew Tao, Jose M. Alvarez, Jan Kautz, Pavlo Molchanov **NVIDIA** {ahatamizadeh, pmolchanov}@nvidia.com

# Fast/Faster ViTs

# **Fast ViT**



Figure 2: (a) Overview of FastViT architecture which decouples train-time and inference-time architecture. Stages 1, 2, and 3 have the same architecture and uses RepMixer for token mixing. In stage 4, self attention layers are used for token mixing. (b) Architecture of the convolutional stem. (c) Architecture of convolutional-FFN (d) Overview of RepMixer block, which reparameterizes a skip connection at inference.

#### Faster ViT

Figure 2: Visualization of the proposed Hierarchical Attention in the feature space. By performing local window attention and hierarchical attention we can achieve global information propagation at reduced costs.





Figure 1: Comparison of image throughput and ImageNet-1K Top-1 accuracy. Throughput is measured on A100 GPU with batch size of 128.

# Pretraining Vision Transformers



# Kaiming He\*,† Xinlei Chen\* Saining Xie Yanghao Li Piotr Dollár Ross Girshick<br>
Tacebook Al Research (FAIR)<br>
CVPR 2022



Figure 1. Our MAE architecture. During pre-training, a large random subset of image patches  $(e.g., 75\%)$  is masked out. The encoder is applied to the small subset of *visible patches*. Mask tokens are introduced *after* the encoder, and the full set of encoded patches and mask tokens is processed by a small decoder that reconstructs the original image in pixels. After pre-training, the decoder is discarded and the encoder is applied to uncorrupted images (full sets of patches) for recognition tasks.



Figure 4. Reconstructions of ImageNet validation images using an MAE pre-trained with a masking ratio of 75% but applied on inputs with higher masking ratios. The predictions differ plausibly from the original images, showing that the method can generalize.

#### MSE loss between pixels for masked tokens only! **Example 20 and Security 10 an**

# Kaiming He\*,† Xinlei Chen\* Saining Xie Yanghao Li Piotr Dollár Ross Girshick<br>Facebook AI Research (FAIR)<br>CVPR 2022



(a) Decoder depth. A deep decoder can improve linear probing accuracy.



(d) Reconstruction target. Pixels as reconstruction targets are effective.



(b) **Decoder width**. The decoder can be narrower than the encoder (1024-d).



(e) Data augmentation. Our MAE works with minimal or no augmentation.



(c) Mask token. An encoder without mask tokens is more accurate and faster (Table 2).



(f) Mask sampling. Random sampling works the best. See Figure 6 for visualizations.

Table 1. MAE ablation experiments with ViT-L/16 on ImageNet-1K. We report fine-tuning (ft) and linear probing (lin) accuracy  $(\%)$ . If not specified, the default is: the decoder has depth 8 and width 512, the reconstruction target is unnormalized pixels, the data augmentation is random resized cropping, the masking ratio is 75%, and the pre-training length is 800 epochs. Default settings are marked in gray.

# Kaiming He\*,† Xinlei Chen\* Saining Xie Yanghao Li Piotr Dollár Ross Girshick<br>Facebook AI Research (FAIR)<br>CVPR 2022



Figure 8. MAE pre-training vs. supervised pre-training, evaluated by fine-tuning in ImageNet-1K (224 size). We compare with the original ViT results  $[16]$  trained in IN1K or JFT300M.



Table 3. Comparisons with previous results on ImageNet-**1K.** The pre-training data is the ImageNet-1K training set (except the tokenizer in BEiT was pre-trained on 250M DALLE data [50]). All self-supervised methods are evaluated by end-to-end fine-tuning. The ViT models are B/16, L/16, H/14 [16]. The best for each column is underlined. All results are on an image size of 224, except for ViT-H with an extra result on 448. Here our MAE reconstructs normalized pixels and is pre-trained for 1600 epochs.

#### **SimMIM: a Simple Framework for Masked Image Modeling**

**CVPR 2022** 

Zhenda Xie<sup>1\*</sup> Zheng Zhang<sup>2\*</sup> Yue  $Cao^{2*}$ Qi Dai<sup>2</sup> Yutong  $Lin<sup>3</sup>$ Jianmin Bao<sup>2</sup> Zhuliang Yao<sup>1</sup> Han  $Hu^{2*}$ <sup>1</sup>Tsinghua University <sup>2</sup>Microsoft Research Asia <sup>3</sup>Xi'an Jiaotong University

{t-zhxie, zhez, yuecao, t-yutonglin, jianmin.bao, t-zhuyao, qid, hanhu}@microsoft.com

![](_page_66_Picture_4.jpeg)

Figure 1. An illustration of our simple framework for masked language modeling, named SimMIM. It predicts raw pixel values of the randomly masked patches by a lightweight one-layer head, and performs learning using a simple  $\ell_1$  loss.

![](_page_66_Picture_59.jpeg)

Table 6. System-level comparison using ViT-B as the encoder. Training costs are counted in relative to our approach. <sup>†</sup> BEiT requires an additional stage to pre-train dVAE, which is not counted.

### SimMIM

### DINO v1 & v2 (ICCV'21 & TMLR'24)

![](_page_67_Picture_1.jpeg)

Figure 1: Self-attention from a Vision Transformer with  $8 \times 8$  patches trained with no supervision. We look at the self-attention of the [CLS] token on the heads of the last layer. This token is not attached to any label nor supervision. These maps show that the model automatically learns class-specific features leading to unsupervised object segmentations.

#### DINO v1 & v2 (ICCV'21 & TMLR'24)

![](_page_68_Figure_1.jpeg)

Figure 2: Self-distillation with no labels. We illustrate DINO in the case of one single pair of views  $(x_1, x_2)$  for simplicity. The model passes two different random transformations of an input image to the student and teacher networks. Both networks have the same architecture but different parameters. The output of the teacher network is centered with a mean computed over the batch. Each networks outputs a  $K$  dimensional feature that is normalized with a temperature softmax over the feature dimension. Their similarity is then measured with a cross-entropy loss. We apply a stop-gradient (sg) operator on the teacher to propagate gradients only through the student. The teacher parameters are updated with an exponential moving average (ema) of the student parameters.

#### Algorithm 1 DINO PyTorch pseudocode w/o multi-crop.

```
gs, gt: student and teacher networks
  C: center(K)tps, tpt: student and teacher temperatures
 1, m: network and center momentum rates
gt. <i>params</i> = <i>gs. <i>params</i></i>for x in loader: # load a minibatch x with n samples
    x1, x2 = augment (x), augment (x) # random views
    s1, s2 = gs(x1), gs(x2) # student output n-by-K
    t1, t2 = gt(x1), gt(x2) # teacher output n-by-K
    loss = H(t1, s2)/2 + H(t2, s1)/2loss.backward() # back-propagate
    # student, teacher and center updates
    update(gs) # SGD
    gt. params = l * qt. params + (l-1) * qs. params
    C = m*C + (1-m) * cat([t1, t2]). mean (dim=0)
def H(t, s):
    t = t.detach() # stop gradient
    s = softmax(s / tps, dim=1)t = softmax((t - C) / tpt, dim=1) # center + sharpenreturn - (t * log(s)) . sum(dim=1) . mean()
```
![](_page_69_Figure_0.jpeg)

![](_page_69_Figure_1.jpeg)

Figure 2: Uniform frame sampling: We simply sample  $n_t$  frames, and embed each 2D frame independently following ViT [18].

![](_page_69_Figure_3.jpeg)

Anurag Arnab\* Mostafa Dehghani\* Georg Heigold Chen Sun Mario Lučić<sup>†</sup> Cordelia Schmid<sup>†</sup> Google Research {aarnab, dehghani, heigold, chensun, lucic, cordelias}@google.com  $|CCV 2021$ 

![](_page_69_Figure_6.jpeg)

Figure 3: Tubelet embedding. We extract and linearly embed nonoverlapping tubelets that span the spatio-temporal input volume.  $\frac{1}{2}$ 

![](_page_70_Figure_0.jpeg)

![](_page_70_Figure_1.jpeg)

Table 1: Comparison of input encoding methods using ViViT-B and spatio-temporal attention on Kinetics. Further details in text.

![](_page_70_Picture_75.jpeg)

Table 2: Comparison of model architectures using ViViT-B as the backbone, and tubelet size of  $16 \times 2$ . We report Top-1 accuracy on Kinetics 400 (K400) and action accuracy on Epic Kitchens (EK). Runtime is during inference on a TPU-v3.

![](_page_70_Picture_76.jpeg)

#### **VideoMAE: Masked Autoencoders are Data-Efficient Learners for Self-Supervised Video Pre-Training**

NeurlPS 2022

Zhan Tong<sup>1,2\*</sup> Yibing Song<sup>2</sup> Jue Wang<sup>2</sup> Limin Wang<sup>1,3†</sup> <sup>1</sup>State Key Laboratory for Novel Software Technology, Nanjing University <sup>2</sup>Tencent AI Lab <sup>3</sup>Shanghai AI Lab tongzhan@smail.nju.edu.cn {vibingsong.cv, arphid}@gmail.com lmwang@nju.edu.cn

![](_page_71_Figure_3.jpeg)

VideoMAE

Figure 1: VideoMAE performs the task of masking random cubes and reconstructing the missing ones with an asymmetric encoder-decoder architecture. Due to high redundancy and temporal correlation in videos, we present the customized design of tube masking with an extremely high ratio (90% to 95%). This simple design enables us to create a more challenging and meaningful self-supervised task to make the learned representations capture more useful spatiotemporal structures.