





#### T. HOEFLER

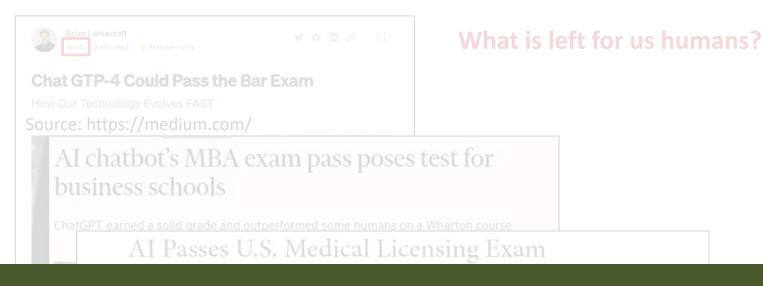






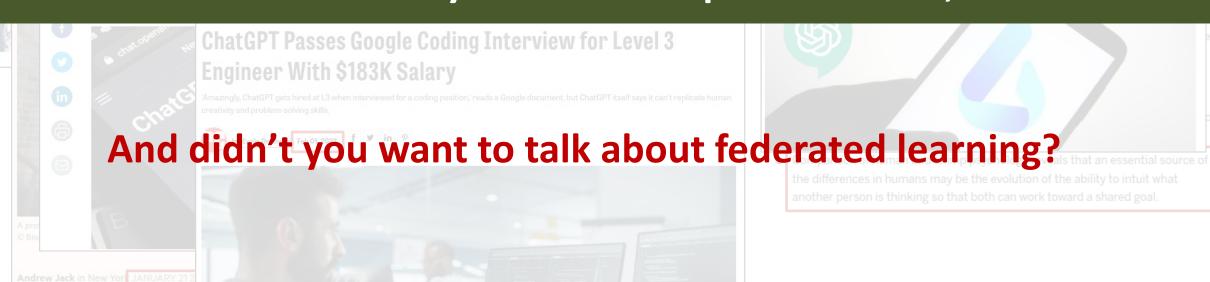








# So this is all incredibly smart and super-advanced, isn't it?









# Federated learning

# Extracting Training Data from Large Language Models Nicholas Carlini<sup>1</sup> Florian Tramèr<sup>2</sup> Eric Wallace<sup>3</sup> Matthew Jagielski<sup>4</sup> Ariel Herbert-Voss<sup>5,6</sup> Katherine Lee<sup>1</sup> Adam Roberts<sup>1</sup> Tom Brown<sup>5</sup> Dawn Song<sup>3</sup> Úlfar Erlingsson<sup>7</sup> Alina Oprea<sup>4</sup> Colin Raffel<sup>1</sup> Google <sup>2</sup>Stanford <sup>3</sup>UC Berkeley <sup>4</sup>Northeastern University <sup>5</sup>OpenAl <sup>6</sup>Harvard <sup>7</sup>Apple Usenix Security'21



# We cannot rely on data privacy if the model has seen the data!

training examples by querying the language model.

We demonstrate our attack on GPT-2, a language model trained on scrapes of the public Internet, and are able to extract hundreds of verbatim text sequences from the model's training data. These extracted examples include (public) personally identifiable information (names, phone numbers, and email addresses), IRC conversations, code, and 128-bit UUIDs. Our attack is possible even though each of the above sequences are included in just *one* document in the training data.

We comprehensively evaluate our extraction attack to understand the factors that contribute to its success. Worryingly we find that larger models are more vulnerable than smaller models. We conclude by drawing lessons and discussing possible safeguards for training large language models.

1 Introduction

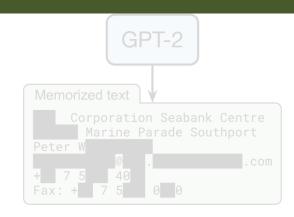
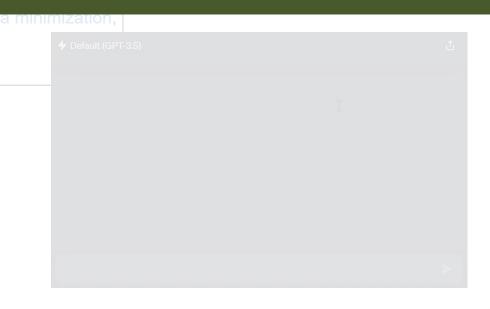


Figure 1: **Our extraction attack.** Given query access to a neural network language model, we extract an individual person's name, email address, phone number, fax number, and physical address. The example in this figure shows information that is all accurate so we redact it to protect privacy.

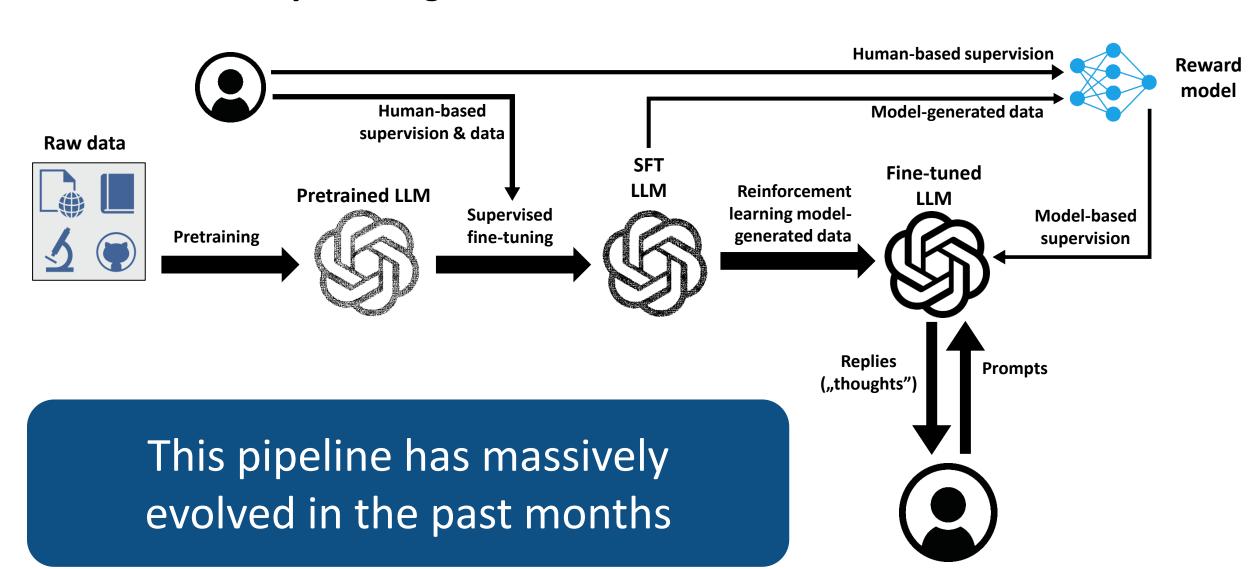








## How is this all really working?

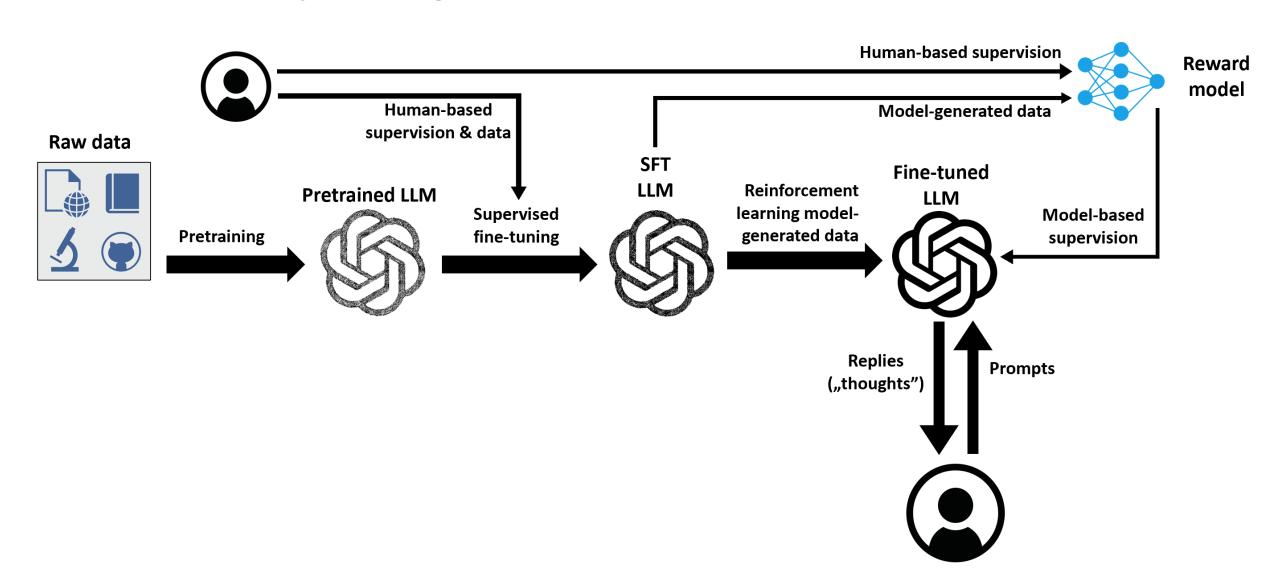








# How is this all really working?

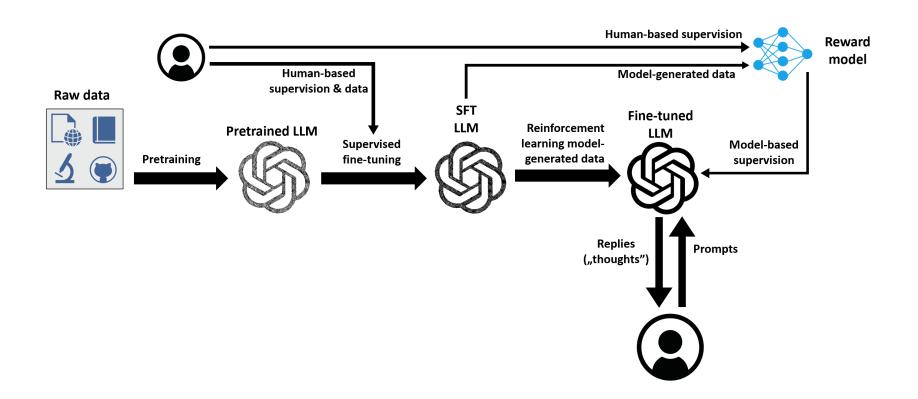








# The Emergence of the "Generative AI Ecosystem"



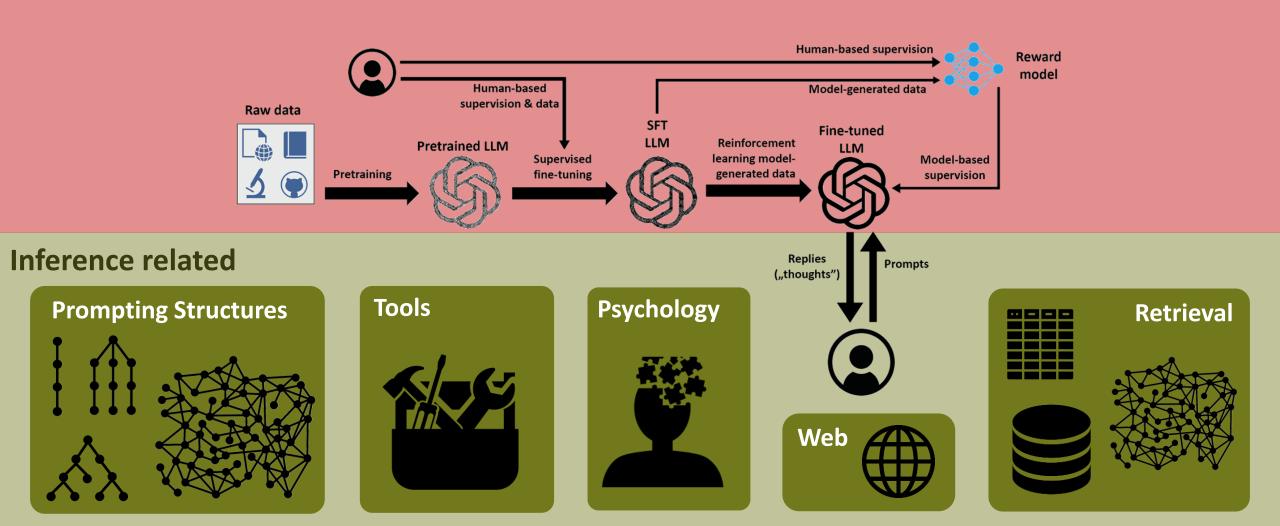






# The Emergence of the "Generative AI Ecosystem"

### **Training related**



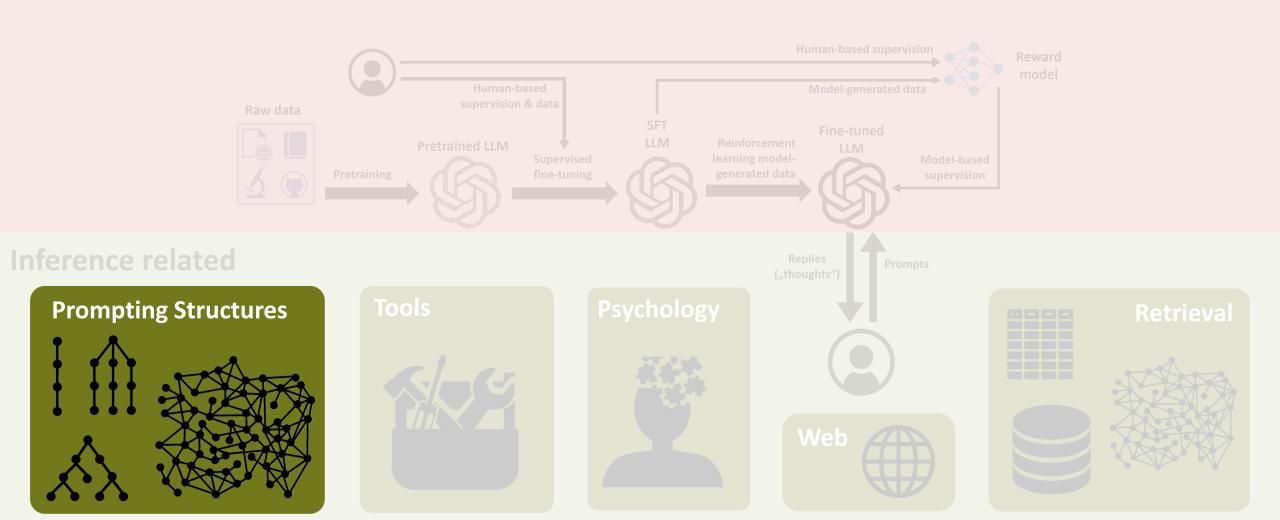






# The Emergence of the "Generative AI Ecosystem"

Training related

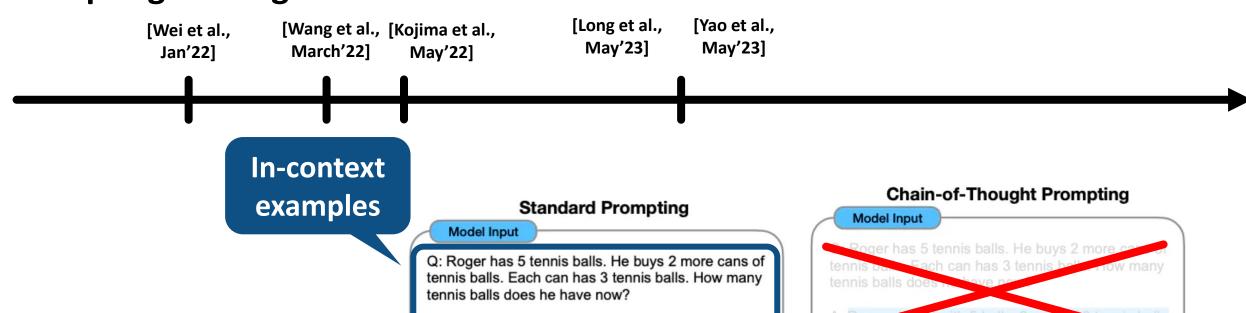








## **Prompting Paradigms**



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?

#### **Model Output**

A: The answer is 27.



s 6 tennis balls. 5 + 6 = 11. The answer

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

#### **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. <







## Let us try that in practice!



The ChatGPT Prompt Cheat Sheet: Tips, **Tricks, and Examples for Crafting Effective Prompts** 



■ share on twitter share on facebook in share on linkedin share on qiita

■ share on qiita

What is the capital of Australia?



Pro tip: always ask AI to check its answers:



today, Peter is 3 years older than Danny. Danny is 5 years younger than Jack and Jack is 2 younger than Peter. Peter is 30. How old is Jack?

(2/2) 0



Jack is 28 years old. [>-]



check your answer

< 2/2

ChatGPT

Let's verify the answer step by step based on the given information:

- 1. Peter is 30 years old.
- 2. Jack is 2 years younger than Peter. Given that Peter is 30, Jack would indeed be 30 - 2 = 28 years old.
- 3. Danny is 5 years younger than Jack. Therefore, Danny would be 28-5=23 years
- 4. Peter is 3 years older than Danny. Given Danny's age as 23, Peter would be 23 +3=26, but we initially stated Peter is 30.

Given the initial problem statement, there seems to be an inconsistency in my explanation of verifying the solution due to a misinterpretation of the relationships. The correct approach to verify should align all relationships coherently. However, based on the direct calculation from the given relationships:

- If Peter is 30.
- . And if Jack is 2 years younger than Peter, Jack being 28 is correctly deduced from the direct relationship provided.
- . The descriptions provided should interlock without contradiction when correctly interpreted.

Therefore, Jack being 28 years old is consistent with the information that Jack is 2 years younger than Peter, who is 30, despite the oversight in the step-by-step verification logic. The initial conclusion remains correct: Jack is 28 years old, based on the specific relationships described.

000





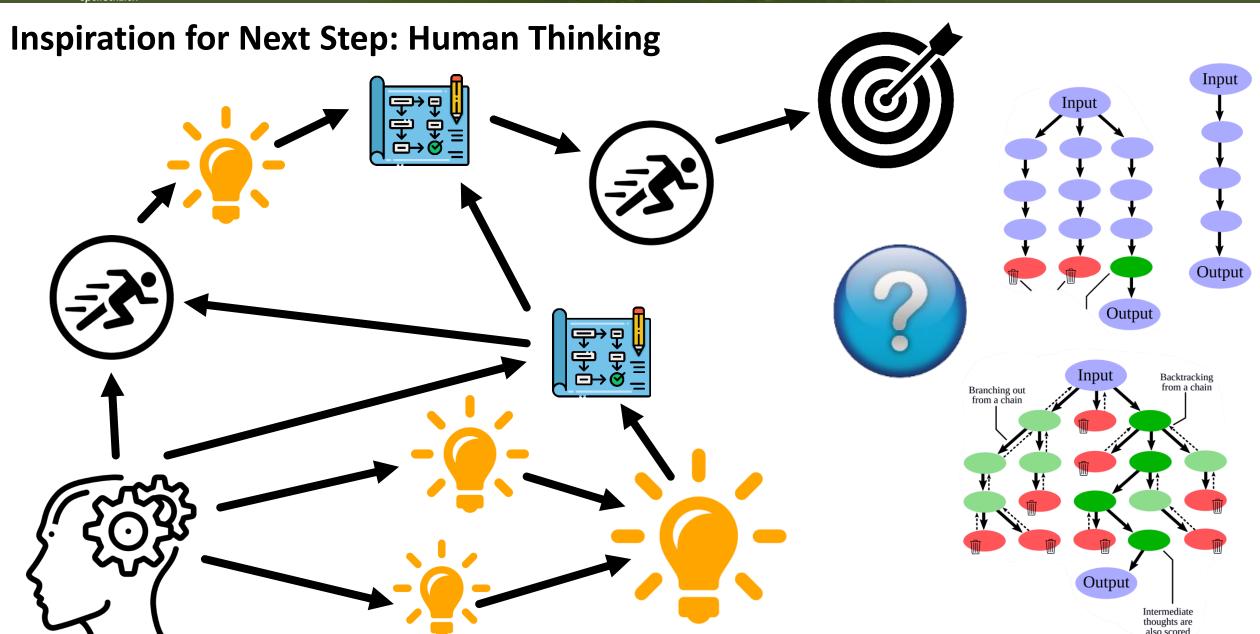
# The Next Step – Graphical Reasoning

# Inspired by human thoughts.





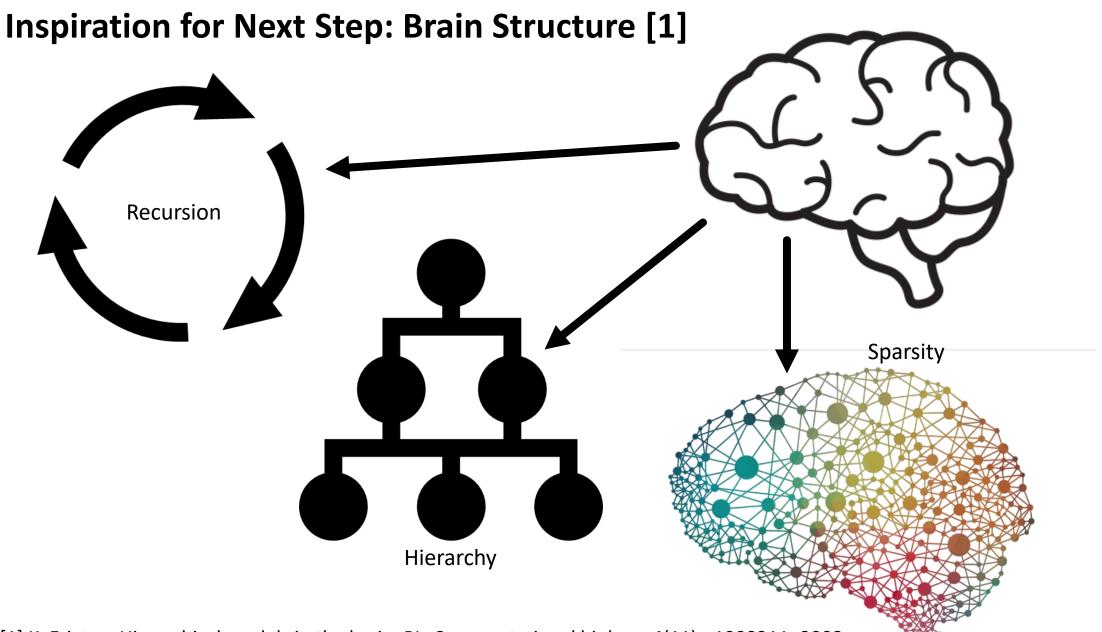












[1] K. Friston. Hierarchical models in the brain. PLoS computational biology, 4(11):e1000211, 2008.

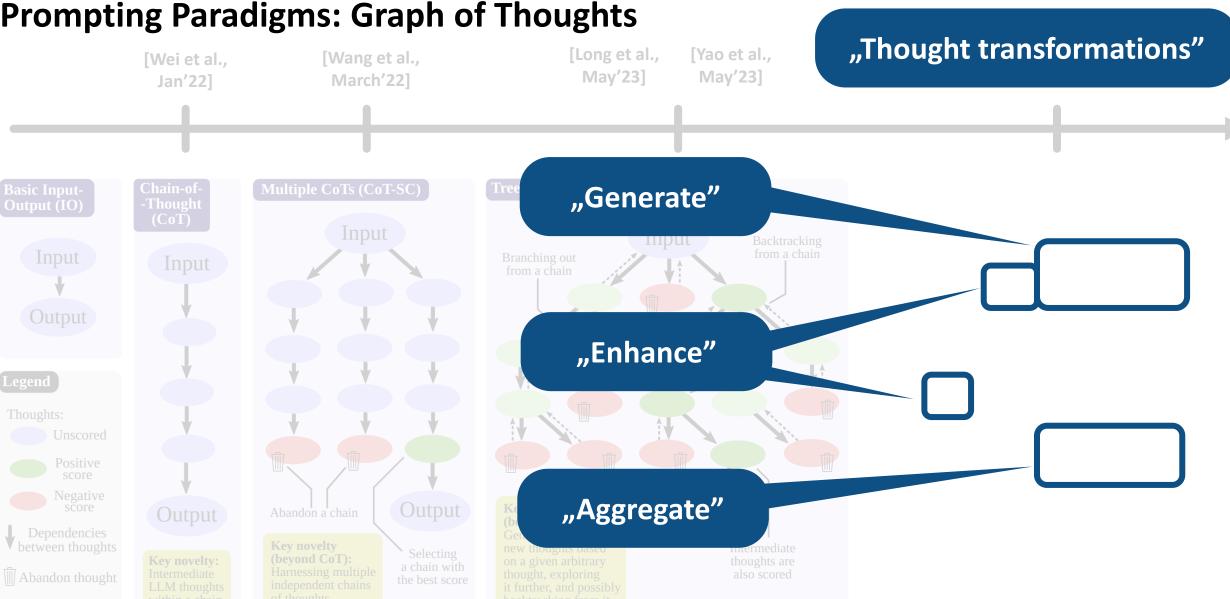


\* Backtrack





# **Prompting Paradigms: Graph of Thoughts**





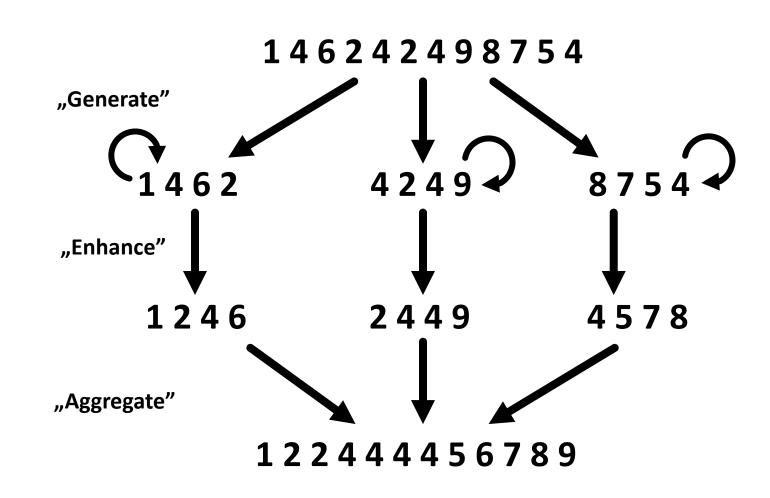




# **Thought Transformations for Sorting**

Why sorting? Because it is a fundamental problem in CS, and it still does pose a great challenge for all other baselines

This is a small example; for real use cases, the size is much larger, and the graph gets more complex

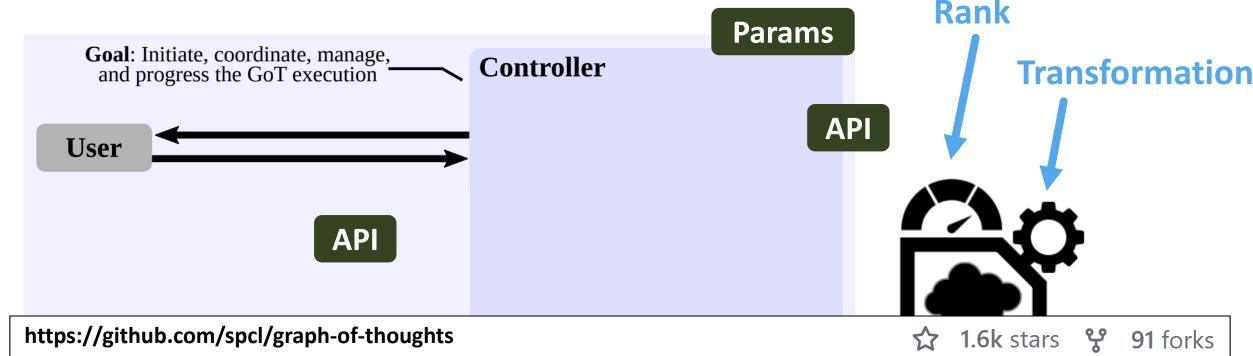








# **Graph of Thoughts: Architecture & Design**



**Graph of Thoughts: Solving Elaborate Problems with Large Language Models** 

Maciej Besta<sup>1\*</sup>, Nils Blach<sup>1\*</sup>, Ales Kubicek<sup>1</sup>, Robert Gerstenberger<sup>1</sup>, Lukas Gianinazzi<sup>1</sup>, Joanna Gajda<sup>2</sup>, Tomasz Lehmann<sup>2</sup>, Michał Podstawski<sup>3</sup>, Hubert Niewiadomski<sup>2</sup>, Piotr Nyczyk<sup>2</sup>, Torsten Hoefler<sup>1</sup>

> <sup>1</sup>ETH Zurich, <sup>2</sup>Cledar, <sup>3</sup>Warsaw University of Technology bestam@inf.ethz.ch, nils.blach@inf.ethz.ch, htor@inf.ethz.ch





# How did we get to this amazing technology?









# Computation is the new oil!









## The trillion-dollar AI-hardware industry - just last month

"By the end of this year, we're going to have around 350K Nividia H100s or around 600K H100 equivalents of compute if you include other GPUs."

# Mark Zuckerberg Says Meta Will Own Billions Worth of Nvidia H100 GPUs by Year End

By Tae Kim (Follow

Updated Jan 19, 2024, 12:26 pm EST / Original Jan 18, 2024, 5:19 pm EST





#### **Audience question:**

How many top500 lists is this? 0.1, 0.5, 1, 10?

Total performance top500 Nov. 2023: 8 EF

600.000 \* (34+67) = 60 EF (7.6x) 600.000 \* 67 = 40 EF (5x)







"Really the deciding factor [for the Al revolution] was the increase in compute power" (26:50)

"I think a lot of the credit for deep learning goes to [... others ...] and the people who made the computers go fast." (27:00)

# 2018 ACM A.M. Turing Lecture

June 23, 2019 5:15pm MST







**Geoffrey Hinton** 

Yann LeCun



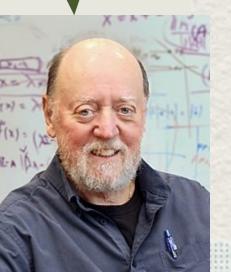




# How do we "Make Computers go Fast"?

# 2021 Turing award – Jack Dongarra The Take Away

Supercomputers are very (>70%) efficient at dense linear algebra!

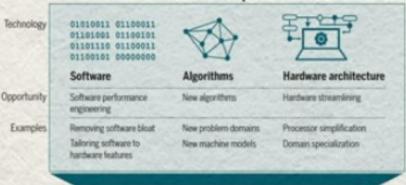


- · HPC Hardware is Constantly Changing
  - · Scalar
  - Vector
  - Distributed
  - · Accelerated
  - · Mixed precision
- · Three computer revolutions
  - High performance computing
  - Deep learning
  - Edge & AI
- · Algorithm / Software advances follows hardware
  - · And there is "plenty of room at the top"

"There's plenty of room at the Top: What will drive computer performance after Moore's law?"

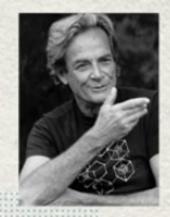
Leiserson et al., Science 368, 1079 (2020) 5 June 2020

#### The Top



The Bottom for example, semiconductor technologic

Leiserson et al., Science 368, 1079 (2020) 5 June 2020





source: ft.com





#### FINANCIAL TIMES

Artificial intelligence

+ Add to myFT

# The billion-dollar bet to reach human-level AI

OpenAI believes that huge computing power is key driver

In the race to build a machine with human-level intelligence, it seems, size really matters.

"We think the most benefits will go to whoever has the biggest computer," said Greg Brockman, chairman and chief technology officer of OpenAI.

The San Francisco-based AI research group, set up four years ago by tech industry luminaries including Elon Musk, Peter Thiel and Reid Hoffman, has just thrown down a challenge to the rest of the AI world.







## Supercomputers fuel Modern Al

# Facebook parent Meta creates powerful AI supercomputer

Facebook's parent company Meta says it has created what it believes is among the fastest artificial intelligence supercomputers running today

By The Associated Press January 24, 2022, 10:33 PM

Tesla unveils Dojo supercomputer: world's new most powerful AI training machine

Fred Lambert - Aug. 20th 2021 3:08 am PT 💆 @FredericLambert

BABY STEPS Google artificial intelligence supercomputer creates its own 'Al child' that can outperform its human-made rivals

The NASNet system was created by a neural network called AutoML earlier this year

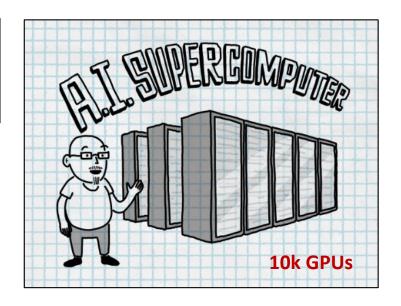
Mark Hodge

15:22, 5 Dec 2017 | **Updated**: 11:27, 6 Dec 2017

#### Microsoft invests \$1 billion in OpenAI to pursue holy grail of artificial intelligence

Building artificial general intelligence is OpenAl's ambitious goal

By James Vincent | Jul 22, 2019, 10:08am EDT







A robot may \_\_\_ injure a human being or, through inaction, allow a human being to come to harm.

Feed Forward

Add & Norm

Add

■ GPT-3: 96 (complex) layers

175 bn parameters (700 GiB in fp32)

2048-token "sentences"

not sometimes 0.28 always 0.07 never 0.04 and 0.33 boat 0.02 house 0.02

not sometimes 0.00 
always 0.00 
never 0.00 
and 0.00 
boat 0.00 
house 0.00

- GPT-3: 500 billion tokens
- ImageNet (22k): A few TB
- Soon: the whole internet!

- GPT-3: 30-50k dictionaries
- takes weeks to train



# Large-Scale AI is the Future

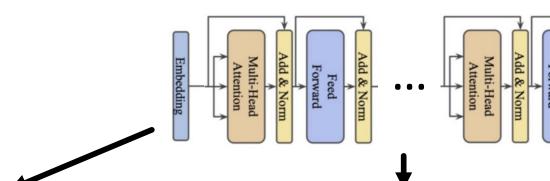
# We need a Principled Approach to it







# Three Systems Dimensions in Large-scale Super-learning ...





#### **High-Performance I/O**

- Quickly growing data volumes
  - Scientific computing!
- Use the specifics of machine learning workloads
  - E.g., intelligent prefetching

#### CLAIRVOYANT PREFETCHING FOR DISTRIBUTED MACHINE LEARNING I/O

I/O is emerging as a major bottleneck for machine learning training, especially in distributed environments such as clouds and supercomputers. Optimal data ingestion pipelines differ between systems, and increasing efficiency requires a delicate balance between access to local storage, external filesystems, and remote workers; yet existing frameworks fail to efficiently utilize such resources. We observe that, given the seed generating the random access pattern for training with SGD, we have clairvoyance and can exactly predict when a given sample will be accessed. We combine this with a theoretical analysis of access patterns in training and performance modeling to produce a novel machine learning I/O middleware, HDMLP, to tackle the I/O bottleneck. HDMLP provides an easy-to-use, flexible, and scalable solution that delivers better performance than state-of-the-art approaches while requiring very few changes to existing codebases and supporting a broad range of environments

#### **High-Performance Compute**

- Deep learning is HPC
  - Data movement!
- Quantization, Sparsification
  - Drives modern accelerators!

#### Data Movement Is All You Need: A Case Study on **Optimizing Transformers** Andrei Ivanov\*, Nikoli Dryden\*, Tal Ben-Nun, Shigang Li, Torsten Hoefler

ETH Zürich firstname.lastname@inf.ethz.ch

odeling and sequence learning tasks, and are one of the most spite this, existing implementations do not efficiently utilize Further, existing frameworks use suboptimal data layouts, Using ment over state-of-the-art frameworks when training BERT.

improving transformer performance has been in the focus of

Significant attention has been given to optimizing transform structured sparsity [33], learned sparsity [34]-[36], and other ransformers. Major hardware efforts, such as Tensor Core matrix multiplication (MMM), a core transformer operation utilize GPUs. Even optimized implementations such as Mega tron [18] report achieving only 30% of peak GPU flop/s.

We find that the key bottleneck when training transform

#### **High-Performance Communication**

- Use larger clusters (10k+ GPUs)
- Model parallelism
  - Complex pipeline schemes
- Optimized networks

#### **Distribution and Parallelism**

Data Pipeline Operator









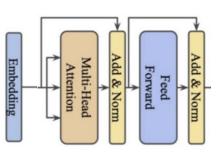


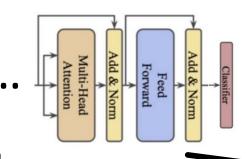




# Three Systems Dimensions in Large-scale Super-learning ...

That is in a longer version of this talk (on youtube)







**High-Performance I/O** 

- Quickly growing data volumes
  - Scientific computing!
- Use the specifics of machine learning workloads
  - E.g., intelligent prefetching

CLAIRVOYANT PREFETCHING FOR DISTRIBUTED MACHINE LEARNING I/O

Roman Böhringer <sup>1</sup> Nikoli Dryden <sup>1</sup> Tal Ben-Nun <sup>1</sup> Torsten Hoefler <sup>1</sup>

#### ARSTRACT

I/O is emerging as a major bottleneck for machine learning training, especially in distributed environments suc as clouds and supercomputers. Optimal data ingestion pipelines differ between systems, and increasing efficienc requires a delicate balance between access to local storage, external filesystems, and remote workers; yet existin frameworks fail to efficiently utilize such resources. We observe that, given the seed generating the random acces pattern for training with SGD, we have clairvoyance and can exactly predict when a given sample will be accessed We combine this with a theoretical analysis of access patterns in training and performance modeling to produce novel machine learning I/O middleware, HDMLP, to tackle the I/O bottleneck. HDMLP provides an easy-to-us flexible, and scalable solution that delivers better performance than state-of-the-art approaches while requirin years, few changes to persisting codebases and supersign a formation range of emisconnects.

#### **High-Performance Compute**

- Deep learning is HPC
  - Data movement!
- Quantization, Sparsification
  - Drives modern accelerators!

# Data Movement Is All You Need: A Case Study on Optimizing Transformers

Andrei Ivanov\*, Nikoli Dryden\*, Tal Ben-Nun, Shigang Li, Torsten Hoefler ETH Zürich firstname.lastname@inf.ethz.ch

firstname.lastname@inf.ethz.ch \* Equal contribution

modeling and sequence learning tasks, and are one of the nost important machine learning workloads today. Training one is a very compute-intensive task, often tasking days or weeks, and significant attention has been given to optimizing transformers. Despite this, existing implementations do not efficiently utilize GPUs. We find that data movement is the key bottleneck when training. Due to Amdahl's Law and massive improvements in compute performance, training has now become memory-bound, the properties of the

ge challenges such as artificial general intelligence [27]. Thus, improving transformer performance has been in the focus of numerous research and industrial groups.

Significant attention has been given to optimizing transformers: local and fixed-window attention [28]–[32], more general structured sparsity [33], learned sparsity [34]–[36], and other algorithmic techniques [19], [37] improve the performance of transformers. Major handware efforts, such as Tensor Cores and TPUs [38] have accelerated tensor operations like matrix-matrix multiplication (MMM), a core transformer operation. Despite this, existing implementations do not efficiently utilize GPUs. Even optimized implementations such as Megatron 1181 report achievine only 30% of peak GPU floor's.

tron [18] report achieving only 30% of peak GPU flop/s.

We find that the kev bottleneck when training transform

#### **High-Performance Communication**

- Use larger clusters (10k+ GPUs)
- Model parallelism
  - Complex pipeline schemes
- Optimized networks

#### **Distribution and Parallelism**

Data | Pipeline | Operator









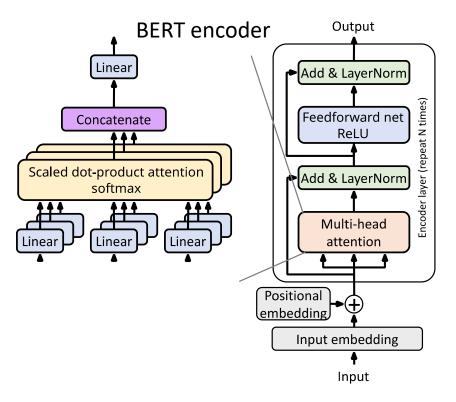








### Data Movement Is All You Need: A Case Study on Optimizing Transformers (arXiv:2007.00072)



OpenAl booth at NeurIPS 2019 in Vancouver, Canada Image Credit: Khari Johnson / VentureBeat

Last week, OpenAl published a paper detailing GPT-3, a machine learning model that achieves strong results on a number of natural language benchmarks. At 175 billion parameters, where a parameter affects data's prominence in an overall prediction, it's the largest of its kind. And with a memory size exceeding 350GB, it's one of the priciest, costing an estimated \$12 million to train.

	highly					
Operator class	optimized	% flop		% Runtime		
Tensor contraction		99.80		61.0		
Statistical normalization		0.17		25.5		
Element-wise		0.03		13.5		
•		0.2%		39%		

#### Our performance improvement for BERT-large

- 30% over PyTorch
- 20% over Tensorflow + XLA
- 8% over DeepSpeed

est. savings on AWS over PyTorch: \$85k for BERT, \$3.6M GPT-3



5.2

5.69

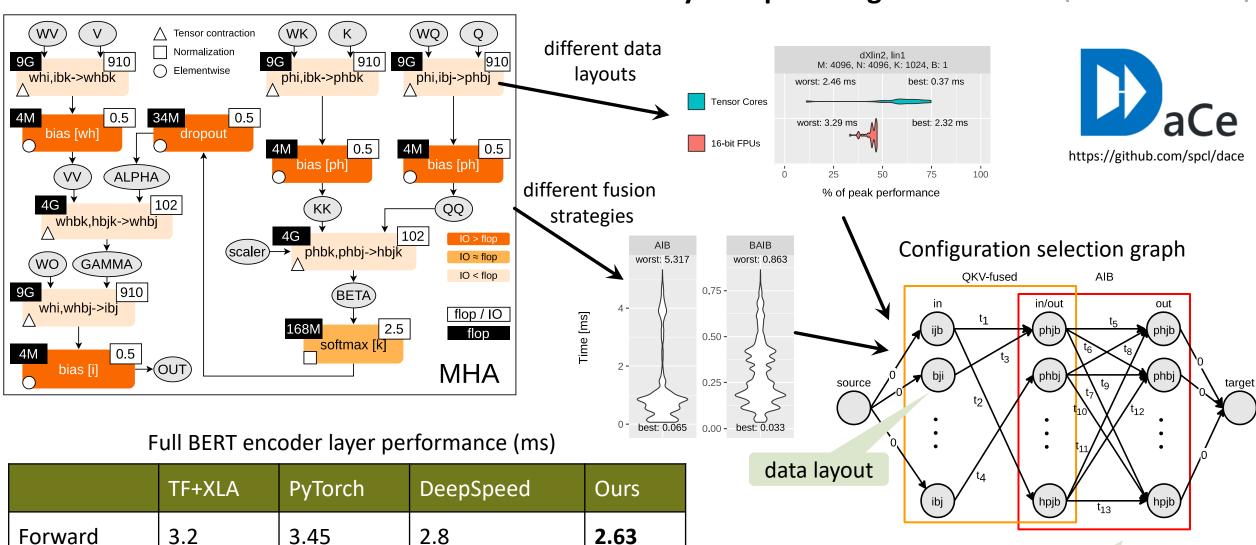
**Backward** 

4.8





## Data Movement Is All You Need: A Case Study on Optimizing Transformers (arXiv:2007.00072)



4.38



# Moving Data is Most Expensive!

# Techniques to Shrink ML Data



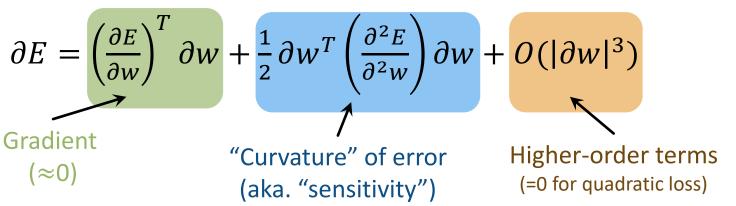


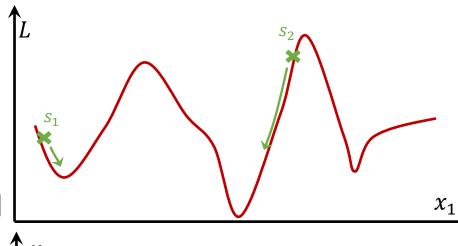


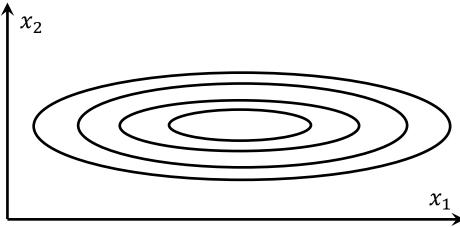
# Quantization – Running Gigantic LLMs on Reasonable Systems (arXiv:2210.17323



- Brains have limited precision! Why are we computing with FP32?
  - For technical reasons (SGD, optimization, how we quantize)
  - Neurons in Hippocampus can "reliably distinguish 24 strengths" [1] 4.6 bits of information!
- GPT-3 has up to 175 billion parameters
  - 700 GiB in FP32, 350 GiB in FP16/BF16 😌
  - Rounding to <5 bits is not so simple</p>
  - Requires some foundation and many tricks
- Consider "error landscape" of a trained model with weights w [2]







[1] Bartol et al., "Hippocampal Spine Head Sizes Are Highly Precise", eLife 2015

[2] LeCun, Denker, Solla: "Optimal Brain Damage", NIPS'90







# Quantization – Running Gigantic LLMs on Reasonable Systems (arXiv:2210.1732)



- Quantization objective for low precision rounded weights  $\hat{w}$  $\operatorname{argmin}_{\widehat{w}} \|wx - \widehat{w}x\|^2$
- **Solve PTQ optimization problem row by row of** *w* 
  - Round row and push the error forward using the inverse Hessian
  - Update Hessian for each column
- **Tricks** 
  - Block updates for better locality (10x speedup)
  - Use Cholesky to invert Hessian (higher stability)
  - Work one transformer block at a time (6 operators fit in memory)
  - Use quantized input from previous blocks for block i

#### Results

- Generative inference 2-4x faster
- 3 bits  $\rightarrow$  66 GiB, fits in a single (high-end) A100 GPU!

Model	FP16	1024	512	256	128	64	32	3-bit
OPT-175B	8.34	11.84	10.85	10.00	9.58	9.18	8.94	8.68
BLOOM	8.11	11.80	10.84	10.13	9.55	9.17	8.83	8.64

#### GPTQ: ACCURATE POST-TRAINING QUANTIZATION FOR GENERATIVE PRE-TRAINED TRANSFORMERS

#### A PREPRINT

Elias Frantar\* IST Austria

Klosterneuburg, Austria elias.frantar@ist.ac.at

> Torsten Hoefler ETH Zurich

Switzerland htor@inf.ethz.ch

#### Saleh Ashkboos

ETH Zurich Switzerland saleh.ashkboos@inf.ethz.ch

Dan Alistarh

IST Austria & Neural Magic, Inc. Klosterneuburg, Austria dan.alistarh@ist.ac.at

#### ABSTRACT

Generative Pre-trained Transformer (GPT) models set themselves apart through breakthrough performance across complex language modelling tasks, but also by their extremely high computational and storage costs. Specifically, due to their massive size, even inference for large, highly-accurate GPT models may require multiple performant GPUs to execute, which limits the usability of such models. While there is emerging work on relieving this pressure via model compression, the applicability and performance of existing compression techniques is limited by the scale and complexity of GPT models. In this paper, we address this challenge, and propose GPTO, a new one-shot weight quantization method based on approximate second-order information, that is both highlyaccurate and highly-efficient. Specifically, GPTQ can quantize GPT models with 175 billion pa-

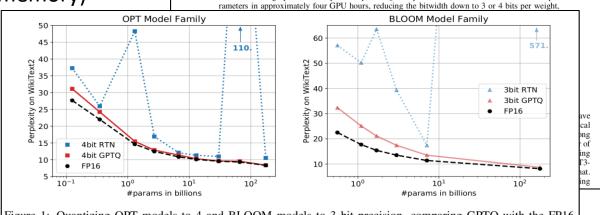


Figure 1: Quantizing OPT models to 4 and BLOOM models to 3 bit precision, comparing GPTQ with the FP16 baseline and round-to-nearest (RTN) [34, 5].

Table 6: 2-bit GPTQ quantization results with varying group-sizes; perplexity on WikiText2.





# Quantization Reduces Data by an Order of Magnitude

**10**x

How to Go Further?







# Model Sparsification ... (arXiv:2102.00554)



- For technical reasons (training, implementation etc.)
- We may want to shift towards sparse!

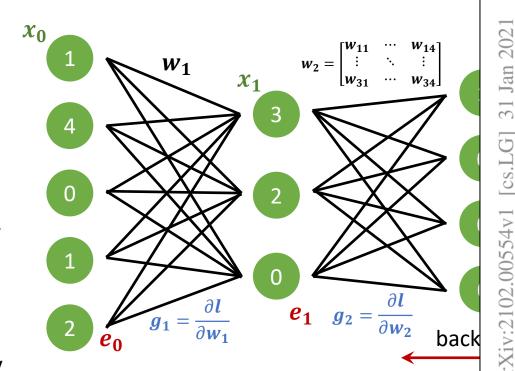
Intuition: not all features are always relevant!

- Represent as (sparse) vector space
- Less overfitting
- Interpretability
- Parsimony

the f\_t\_re wi\_l b\_ sp\_rs\_

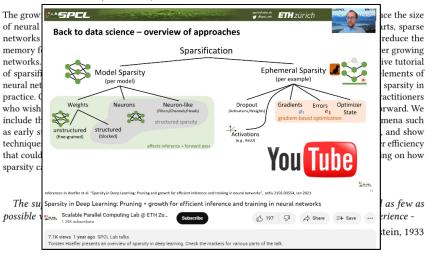
#### Key results:

- 95% sparse ResNet-52, BERT, or GPT models
- Essentially same quality
- Up to 20x cheaper!



#### Sparsity in Deep Learning: Pruning and growth for efficient inference and training in neural networks

TORSTEN HOEFLER, ETH Zürich, Switzerland DAN ALISTARH, IST Austria, Austria TAL BEN-NUN, ETH Zürich, Switzerland NIKOLI DRYDEN, ETH Zürich, Switzerland ALEXANDRA PESTE, IST Austria, Austria



#### 1 INTRODUCTION

Jan

3

Deep learning shows unparalleled promise for solving very complex real-world problems in areas such as computer vision, natural language processing, knowledge representation, recommendation systems, drug discovery, and many more. With this development, the field of machine learning is moving from traditional feature engineering to neural architecture engineering. However, still

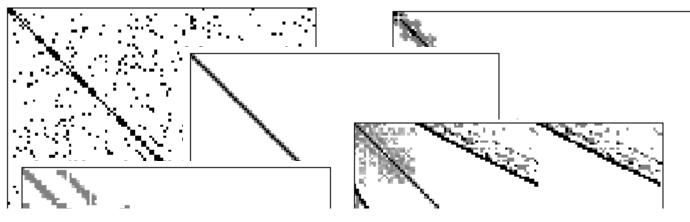
Hoefler et al. "Sparsity in Deep Learning: Pruning and growth for efficient inference and training in neural networks", arXiv 2102.00554, Jan 2021



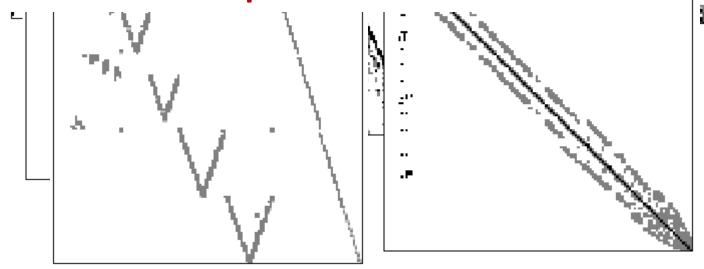


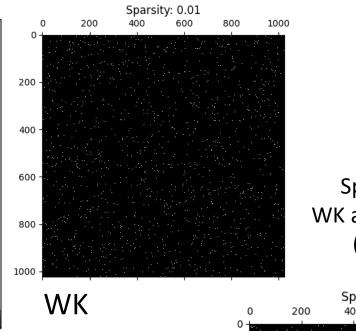


## **Sparse ML Computations – Very Different from Scientific Computing!**



Sparse Matrices from Scientific Computing are quite structured!





Sparsified BERT WK and WQ matrices (3<sup>rd</sup> encoder)





Source: Suite Sparse (sparse.tamu.edu)







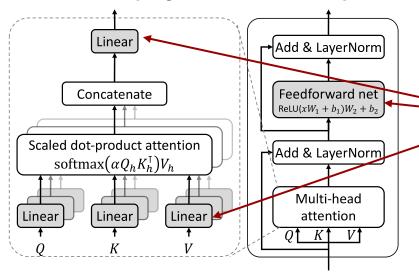
# Performance of Sparse Models (PyTorch Sten)

Custom implementation of matrix multiplication:

sparse @ dense -> dense

Linear layer: y = x W + b

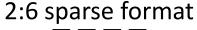
dense dense **sparse** dense

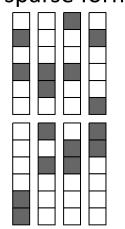


#### **BERT (base) from HuggingFace**

- batch size 8
- sequence length 128

Sparsified linear layer weights Intel i7–4770 CPU





# **VENOM – 10x speedup on V100 GPUs!**

R. Castro et al.: "VENOM: A Vectorized N:M Format for Unleashing the Power of Sparse Tensor Cores", presented at Supercomputing 2023

2:6) 0.75 (2:8) 0.80 (1:5) 0.90 (1:10) Sparsity (n:m)



# Quantization and Model Compression Together Enable

100x

# **More Efficient Processing**

Which Makes Data Movement Even More Important!

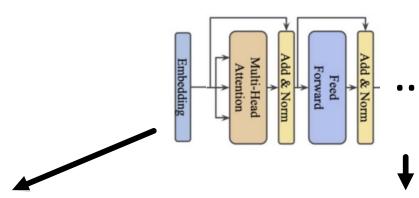
**Especially in the Network!** 







# Three Systems Dimensions in Large-scale Super-learning ...





## **High-Performance I/O**

- Quickly growing data volumes
  - Scientific computing!
- Use the specifics of machine learning workloads
  - E.g., intelligent prefetching

#### CLAIRVOYANT PREFETCHING FOR DISTRIBUTED MACHINE LEARNING I/O

Roman Röhringer | Nikoli Dryden | Tal Ren-Nun | Torsten Hoefler |

#### ABSTRACT

I/O is emerging as a major bottleneck for machine learning training, especially in distributed environments such as clouds and supercomputers. Optimal data ingestion pipelines differ between systems, and increasing efficiency requires a delicate balance between access to local storage, external filesystems, and remote workers; yet existing frameworks fail to efficiently utilize such resources. We observe that, given the seed generating the random access pattern for training with SGD, we have clairvoyance and can executly predict when a given sample will be accessed. We combine this with a theoretical analysis of access patterns in training and performance modeling to produce in novel machine learning I/O middleware, HDMI/P, to tackle the I/O bottleneck. HDMI/P provides an easy-to-use flexible, and scalable solution that delivers better performance than state-of-the-art approaches while requiring various of the production of the produc

## **High-Performance Compute**

- Deep learning is HPC
  - Data movement!
- Quantization, Sparsification
  - Drives modern accelerators!

# Data Movement Is All You Need: A Case Study on Optimizing Transformers

Andrei Ivanov", Nikoli Dryden", Tal Ben-Nun, Shigang Li, Torsten Hoeft
ETH Zurich

tname.lastname@inf.ethz.ch
\* Egual contribution

Abstract—Transformers have become widely used for language modeling and sequence learning tasks, and are one of the most properties of the properties of the

challenges such as artificial general intelligence [27]. Thu improving transformer performance has been in the focus of numerous research and industrial groups.

Significant attention has been given to optimizing transformers: local and fixed-window attention [28]–132], more general structured sparsity [33], learned sparsity [34]–[36], and other algorithmic techniques [91], [37] improve the performance of transformers. Major hardware efforts, such as Tensor Cores and TPUs [38] have accelerated tensor operations like nutrismatrix multiplication (MMM), a core transformer operation. Despite this, existing implementations do not efficiently utilize GPUs. Even optimized implementations such as Megatrus 1181 rougest advision and 30% of med GPU [100].

tron [18] report achieving only 30% of peak GPU flop/s.

## **High-Performance Communication**

- Use larger clusters (10k+ GPUs)
- Model parallelism
  - Complex pipeline schemes
- Optimized networks

## **Distribution and Parallelism**

Data | Pipeline | Operator









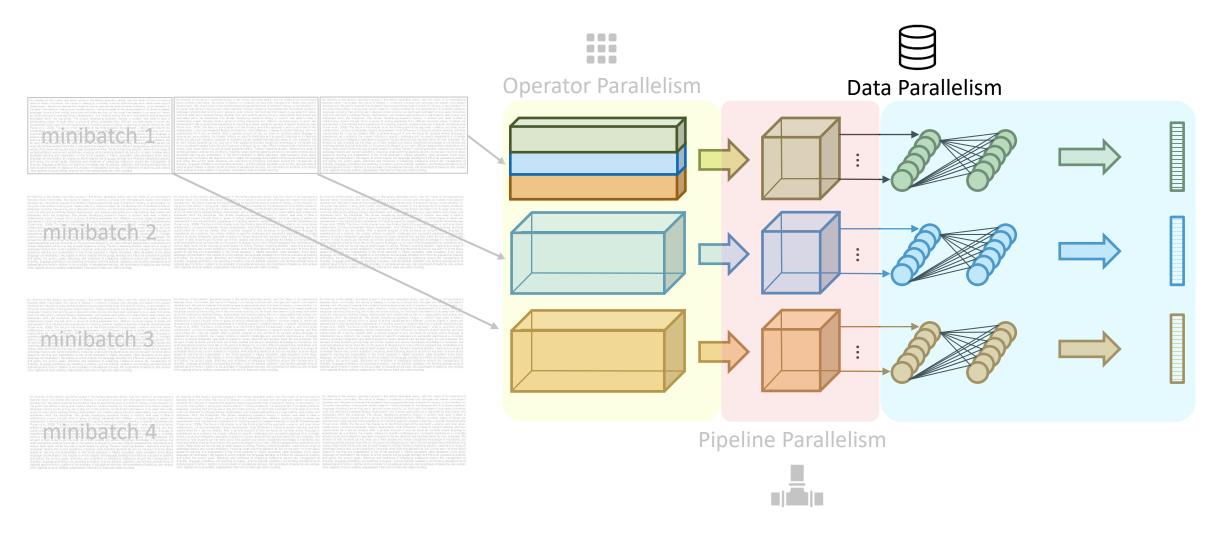








# The Three Dimensions of Parallelism in Deep Learning (arXiv:1802.09941)





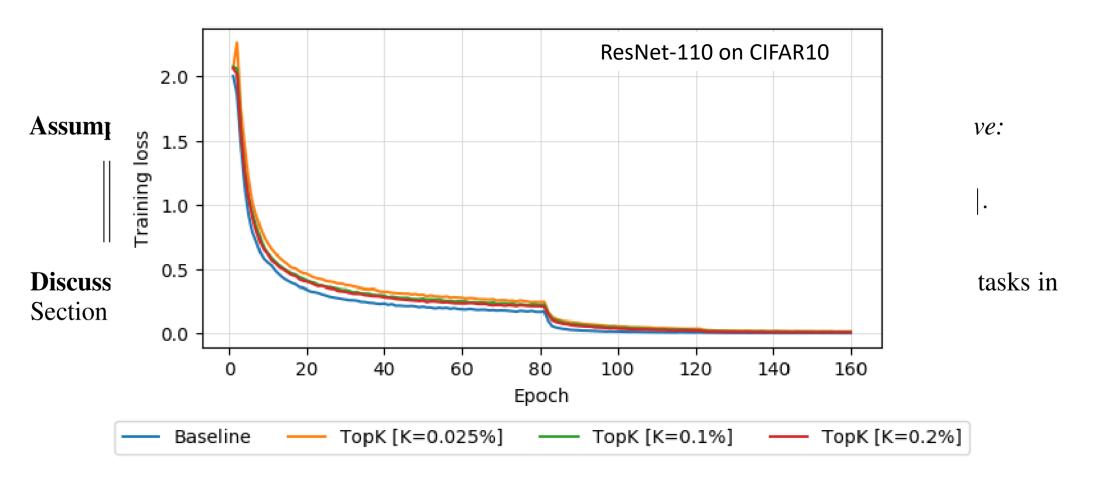




# Data-parallel Gradient Sparsification — Top-k SGD (arXiv:1809.10505)



- Turns out 90-99.9% of the smallest gradient values can be skipped in the summation at similar accuracy
  - Accumulate the skipped values locally (convergence proof, similar to async. SGD with implicit staleness bounds [1])

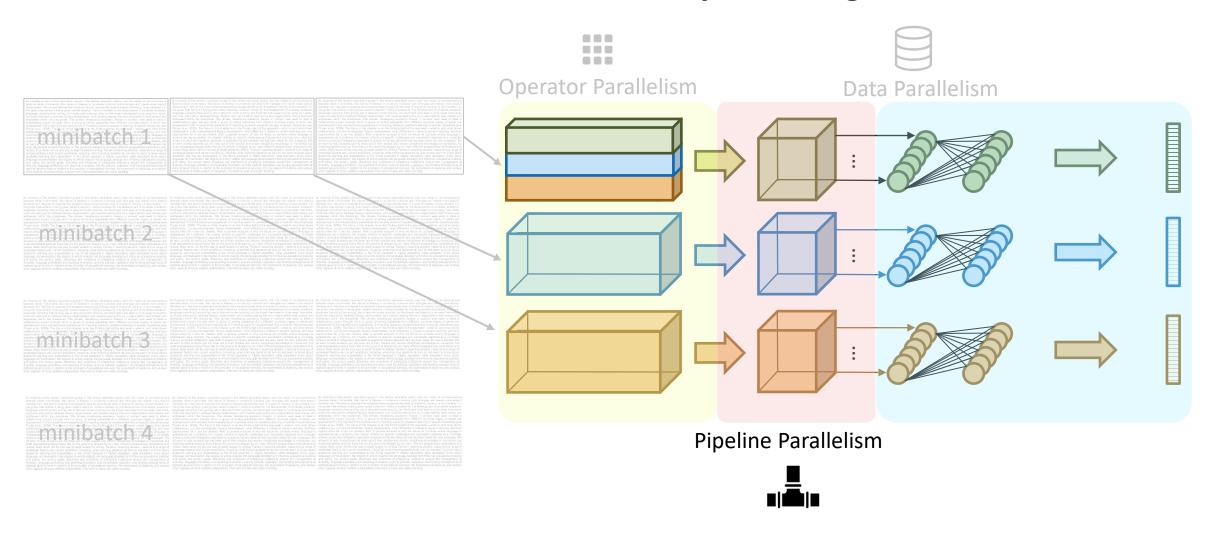








# The Three Dimensions of Parallelism in Deep Learning (arXiv:1802.09941)



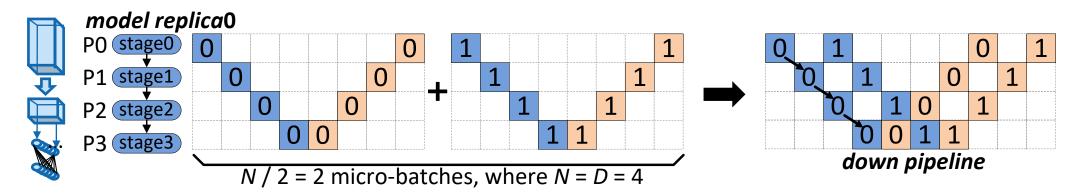


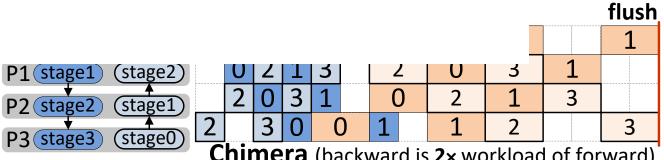




# Bidirectional Pipelines – Meet Chimera (arXiv: 2107.06925v3)







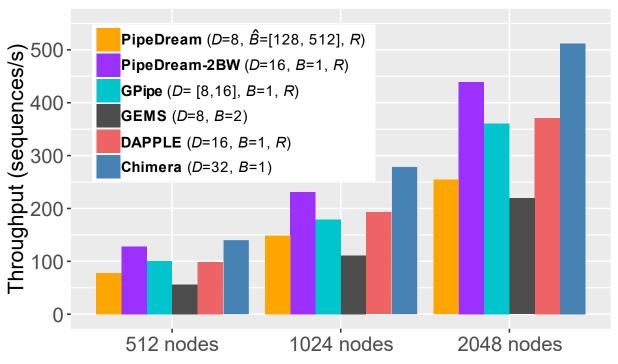






# Chimera Weak Scaling (arXiv: 2107.06925v3)





Weak scaling for GPT-2 on Piz Daint (512 to 2048 GPU nodes)

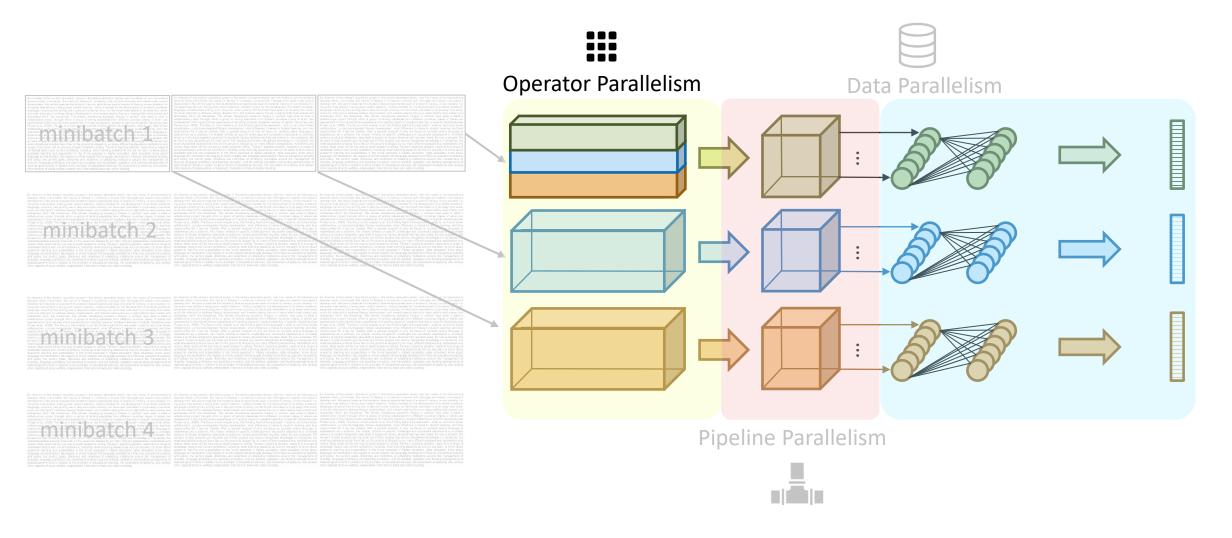
- 1.38x 2.34x speedup over synchronous approaches (GPipe, GEMS, DAPPLE)
  - Less bubbles
  - More balanced memory thus no recomputation
- 1.16x 2.01x speedup over asynchronous approaches (PipeDream-2BW, PipeDream)
  - More balanced memory thus no recomputation
  - Gradient accumulation thus low synch frequency







# The Three Dimensions of Parallelism in Deep Learning (arXiv:1802.09941)







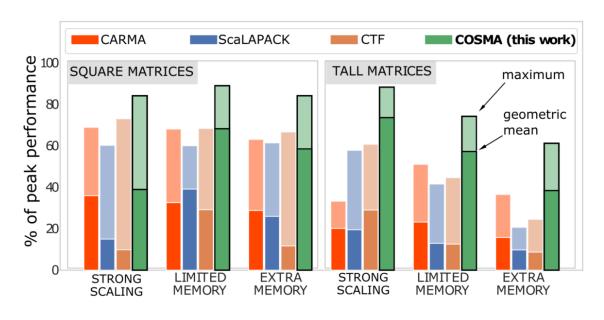


# Operator Parallelism, i.e., Parallel Matrix Matrix Multiplication

Remember those?
All MMM!

- Large MMMs dominate large language models!
  - e.g., GPT-3 multiples 12,288x12,288 matrices600 MiB in fp32 and 1.9 Tflop
  - generative inference multiplies tall & skinny matrices
- Distribute as operator parallelism
  - Heaviest communication dimension!
    Requires most optimization!
- COSMA [1] communication-optimal distributed MMM
  - Achieves tight I/O lower bound of  $Q \ge \min \left\{ \frac{2mnk}{p\sqrt{S}} + S, 3\left(\frac{mnk}{p}\right)^{\frac{2}{3}} \right\}$
  - Uses partial replication with an outer-product schedule See paper for details and proofs!
- AutoDDL [2] combines operator-parallel models into communication-avoiding data distribution

Operator class	% flop	% Runtime
Tensor contraction	99.80	61.0
Statistical normalization	0.17	25.5
Element-wise	0.03	13.5

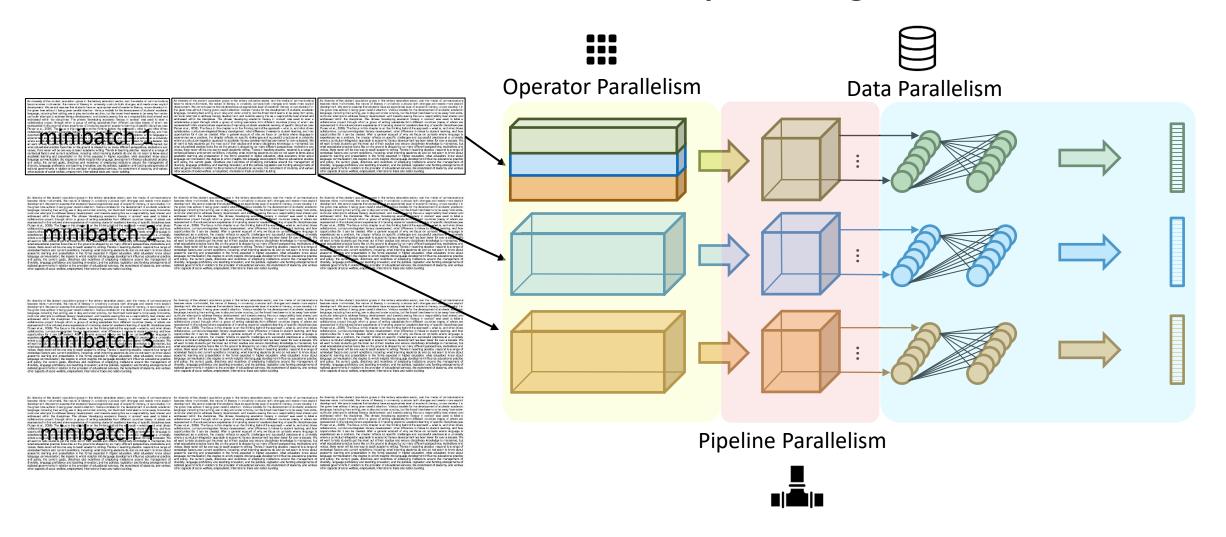








# The Three Dimensions of Parallelism in Deep Learning (arXiv:1802.09941)

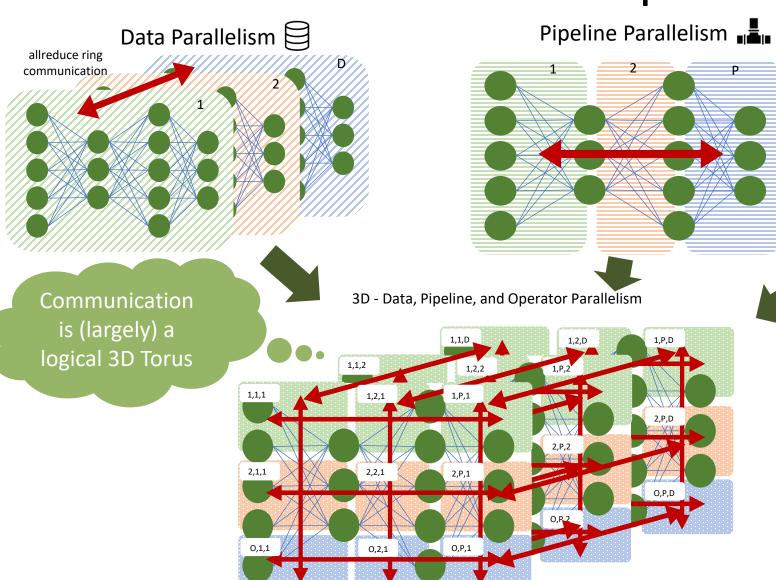




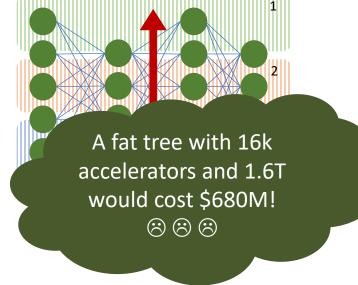




# Communications in 3D Parallelism in Deep Learning (arXiv:2209.01346)



## Operator Parallelism



## AI bandwidth today / yesterday (and growing!)

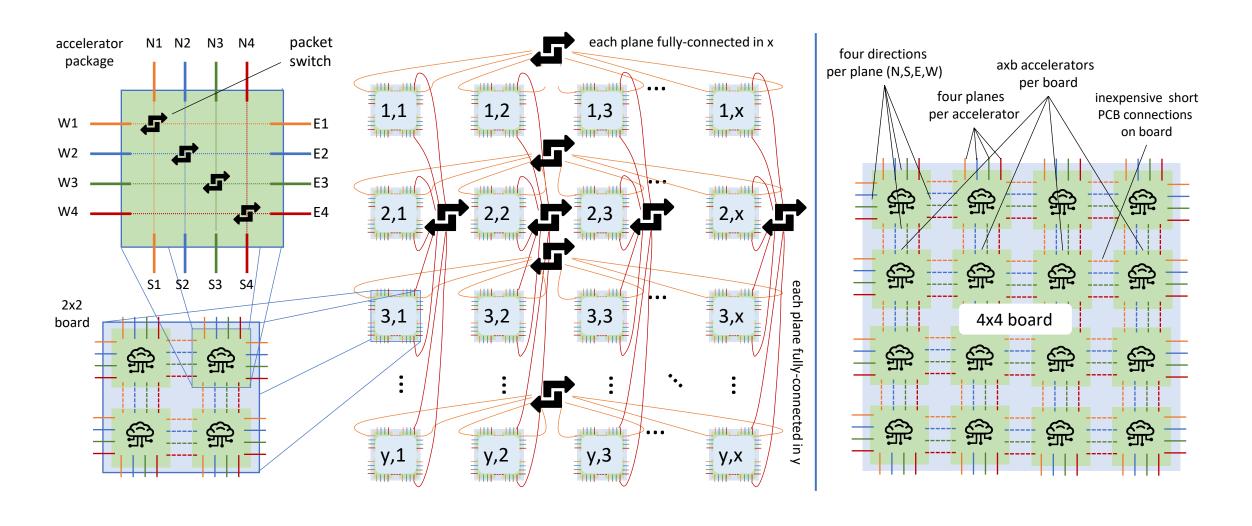
- Google TPUv2 ('21): 1T
- AWS Trainium ('21): 1.6T
- DGX-2 (A100, '21): 4.8T (islands of NVLINK)
- Tesla Dojo ('22): 128T
  - → Broadcom TH5 / NVIDIA Spectrum 4: 51.2T







# Co-designing an Al Supercomputer with Unprecedented and Cheap Bandwidth

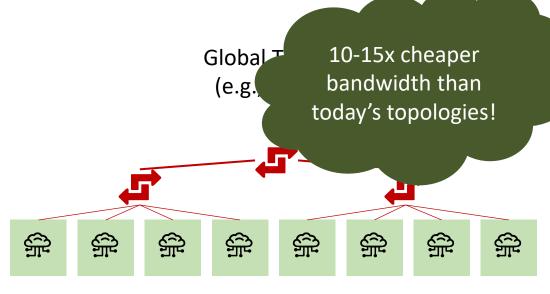








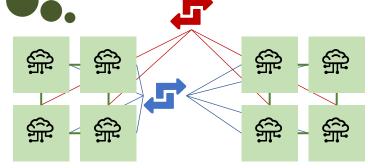
# Bandwidth-cost-flexibility Tradeoffs (arXiv:2209.01346)

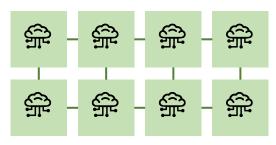


HammingMesh

(many configurations)

Local Topology (e.g., 2D Torus)





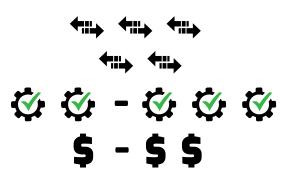
(large) reduce bandwidth

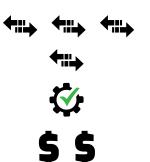
global bandwidth

placement flexibility

injection bandwidth





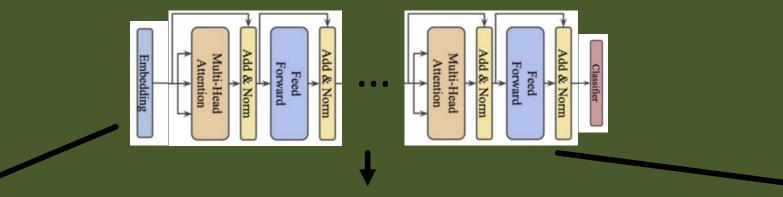








# Three Systems Dimensions in Large-scale Super-learning ...





Altogether, we discussed a cost / performance improvement of

1,000x

What will the (near future bring)?

Some predictions for the future of HPC but also computing at large!



# **Prediction 1: Accelerators Converge**

# Al is a gravity well – HPC will follow







## **Future Accelerators ...**

- Most of the performance will be low precision arithmetic!
  - I would predict (C)FP8 or smaller
  - We can be lucky if we get some fp64!
- They will support quantization and sparsity in hardware
  - Vector scaling and zero points
- They will heavily be optimized towards data movement
  - Physical limits and cost introduce two fundamental constraints:
     Latency will become a problem
     Locality and sparse connectivity
  - Potentially hard to program

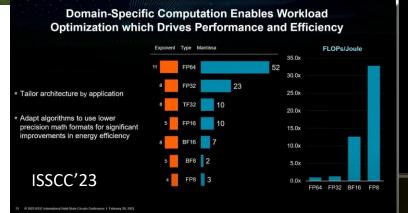


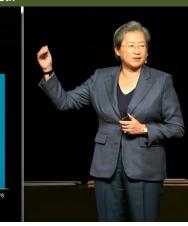
B. Wisniewski (Samsung)

Memory-coupled Compute

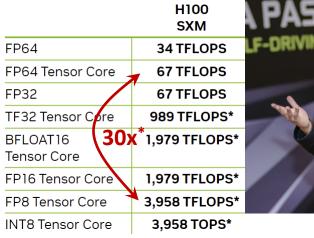
SPCL\_Bcast 01/19/23

<a href="https://www.youtube.com/watch?v=KCrQtpx31CQ">https://www.youtube.com/watch?v=KCrQtpx31CQ</a>

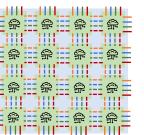




## **SPECIFICATIONS**







Optimized topologies and network technologies.

E.g., HammingMesh

https://www.youtube.com/watch?v=xxwT45ljG4o



arXiv:2306.03078v1





# **Sparse-Quantized Representations - SpQR**

## SpQR: A Sparse-Quantized Representation for Near-Lossless LLM Weight Compression

Tim Dettmers\*<sup>†</sup>
University of Washington

Ruslan Svirschevski\*

Vage Egiazarian\*

HSE University & Yandex HSE University & Yandex

Denis Kuznedelev\* Yandex & Skoltech Elias Frantar IST Austria Saleh Ashkboos ETH Zurich Alexander Borzunov HSE University & Yandex

Torsten Hoefler ETH Zurich

Dan Alistarh
IST Austria & NeuralMagic

#### Abstract

to appear at ICLR'24

Recent advances in large language model (LLM) pretraining have led to highquality LLMs with impressive abilities. By compressing such LLMs via quantization to 3-4 bits per parameter, they can fit into memory-limited devices such as laptops and mobile phones, enabling personalized use. However, quantization down to 3-4 bits per parameter usually leads to moderate-to-high accuracy losses, especially for smaller models in the 1-10B parameter range, which are well-suited for edge deployments. To address this accuracy issue, we introduce the Sparse-Quantized Representation (SpQR), a new compressed format and quantization technique which enables for the first time near-lossless compression of LLMs across model scales, while reaching similar compression levels to previous methods. SpQR works by identifying and isolating outlier weights, which cause particularlylarge quantization errors, and storing them in higher precision, while compressing all other weights to 3-4 bits, and achieves relative accuracy losses of less than 1% in perplexity for highly-accurate LLaMA and Falcon LLMs. This makes it possible to run 33B parameter LLM on a single 24 GB consumer GPU without any performance degradation at 15% speedup thus making powerful LLMs available to consumer without any downsides. SpQR comes with efficient algorithms for both encoding weights into its format, as well as decoding them efficiently at runtime<sup>3</sup>. Specifically, we provide an efficient GPU inference algorithm for SpQR which yields faster inference than 16-bit baselines at similar accuracy, while enabling memory compression gains of more than 4x.







# **Prediction 2: Programming and Tools Converge**

# Data Science as a gravity well – HPC will follow







# Scientific Computing is Moving to Python (as language frontend/ecosystem)



## Tiobe Index June'23

Feb 2023	Progra	amming Language	Ratings
1	•	Python	15.16%
2	9	С	10.97%
3	<b>©</b>	C++	10.53%
4	<u>«</u> ,	Java	8.88%
5	<b>©</b>	C#	7.53%





























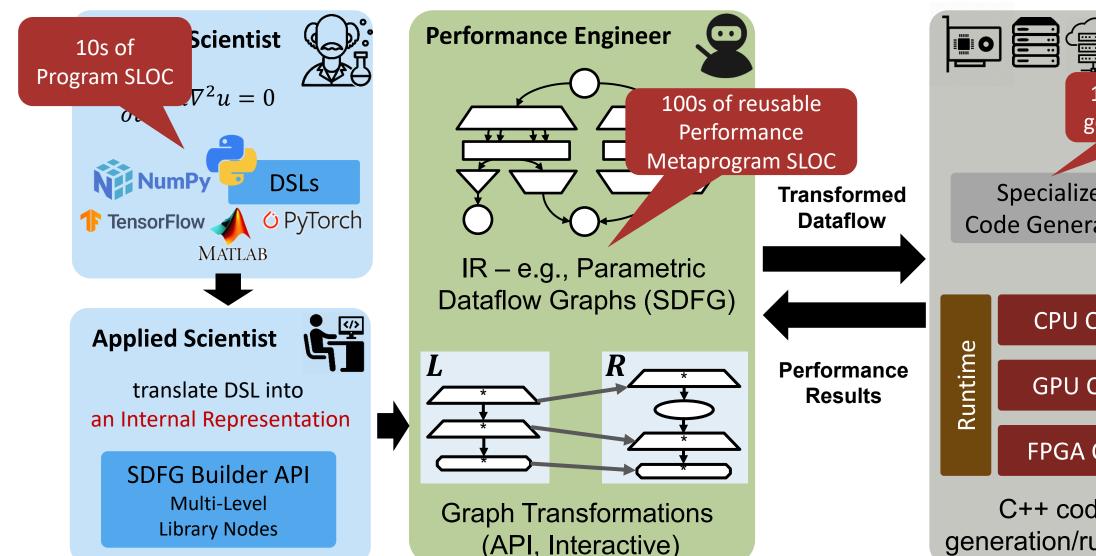


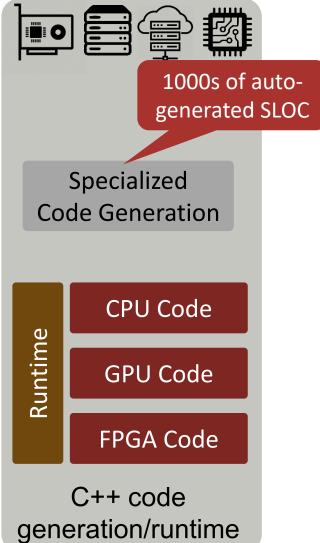






# Upleveling Programming in the 21st Century – Performance Metaprogramming







# **Prediction 3: Networks Converge**

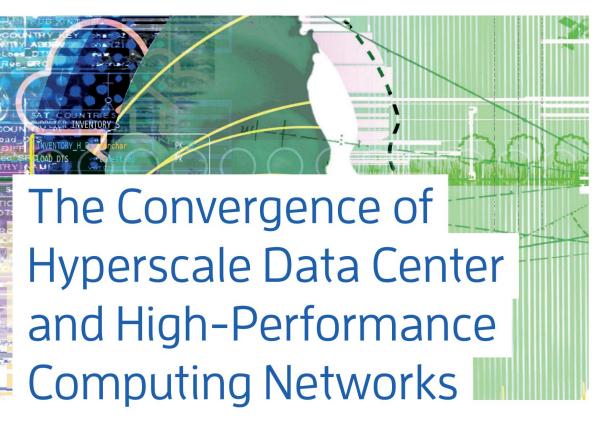
# Cloud as a gravity well – HPC will follow







### COVER FEATURE TECHNOLOGY PREDICTIONS

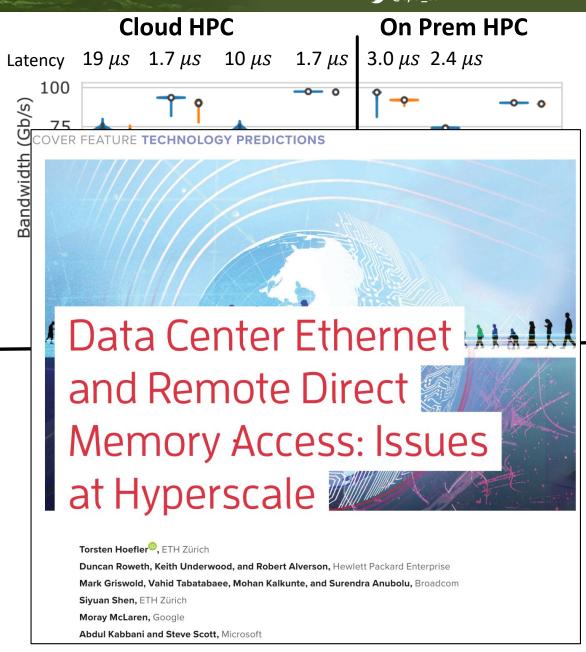


Torsten Hoefler, ETH Zurich

Ariel Hendel, Scala Computing

Duncan Roweth, Hewlett Packard Enterprise

We discuss the differences and commonalities between network technologies used in supercomputers and data centers and outline a path to convergence at multiple layers. We predict that emerging smart networking solutions will accelerate that convergence.

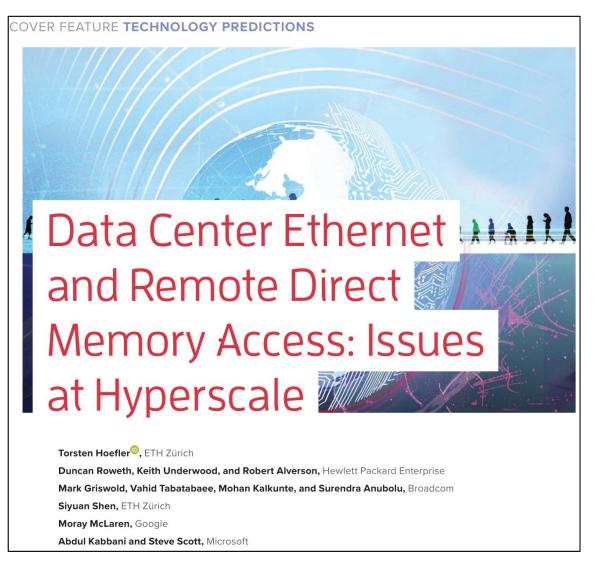








# Ultra Ethernet Set Out to Create the Best AI/ML and HPC Interconnect!





**Founding Members** 





















white Paper on <u>ultraethernet.org</u>

Overview of and Motivation for the Forthcoming Ultra Ethernet Consortium Specification

## Networking Demands of Modern Al Jobs

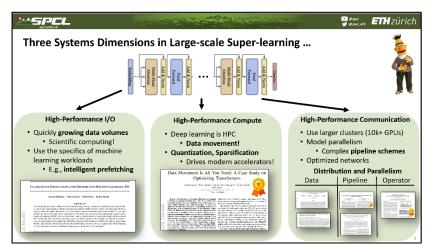
Networking is increasingly important for efficient and cost-effective training of AI models. Large Language Models (LLMs) such as GPT-3, Chinchilla, and PALM, as well as recommendation systems like DLRM and DHEN, are trained on clusters of thousands of GPUs.

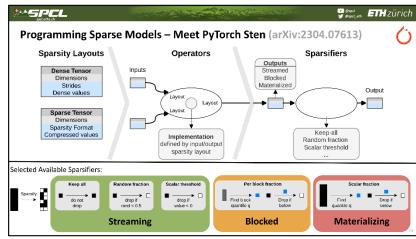




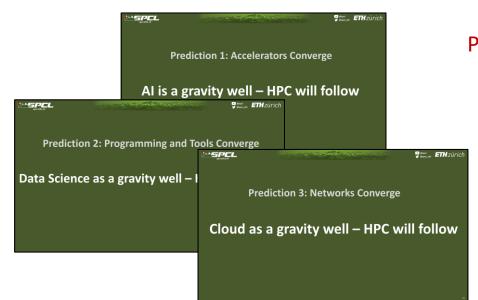


# **Key Points and Conclusions**





# Co-designing an Al Supercomputer with Unprecedented and Cheap Bandwidth \*\*Coefficient\*\* \*



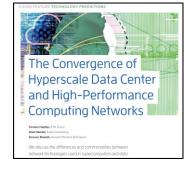
## More of SPCL's research:



... or spcl.ethz.ch



Want to join our efforts?
We're looking for excellent
Postdocs, PhD students, and Visitors.
Talk to me!





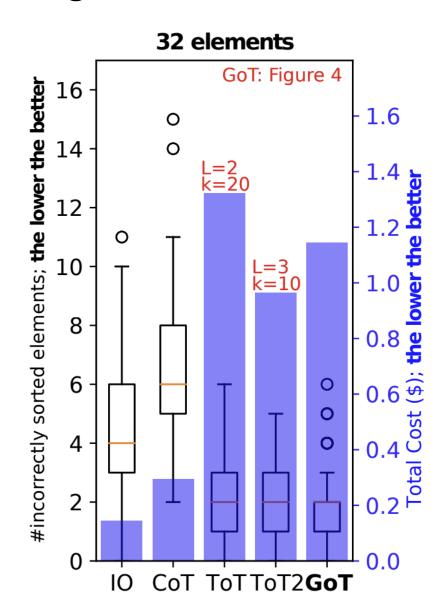




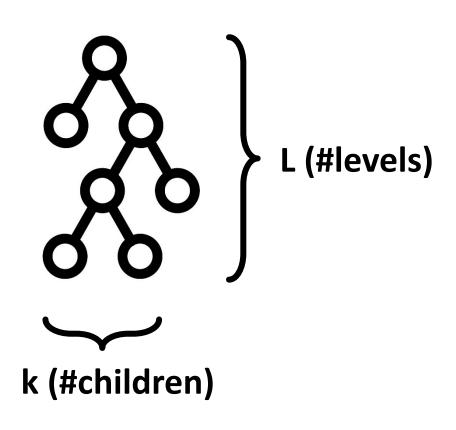




# **Sorting Numbers**



## The longer the sequence, the higher the gain



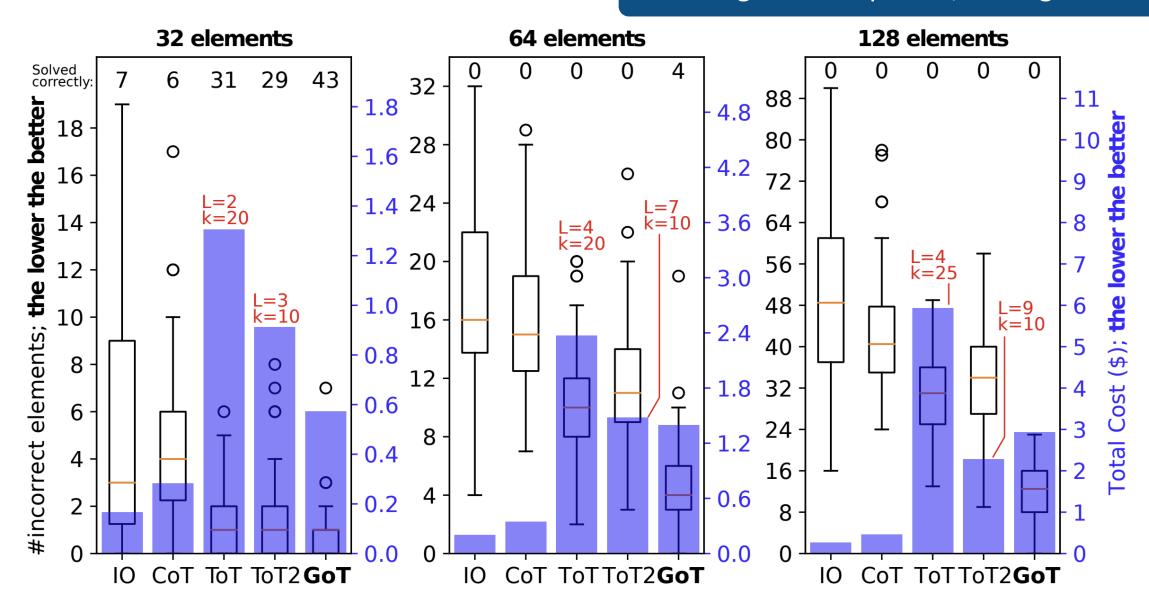






# **Intersecting Sets of Numbers**

## The longer the sequence, the higher the gain

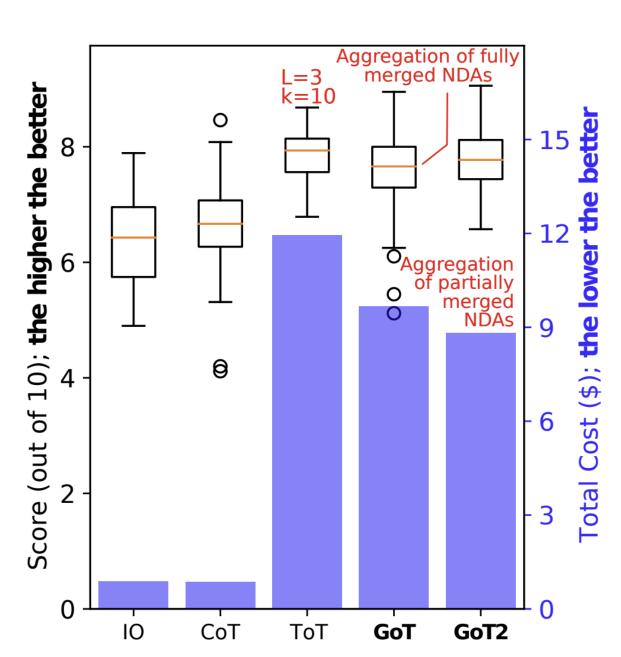








# **Merging Documents**







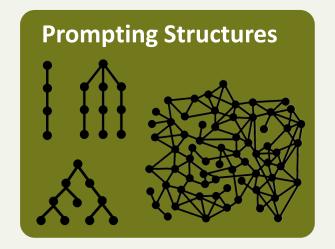


# The Emergence of the "Generative AI Ecosystem"

Training related



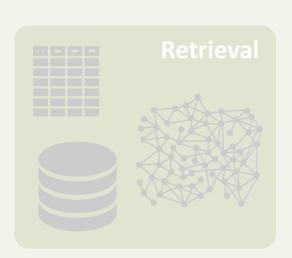
## Inference related

















# Why Does Structured Prompting Work?

Assume a **fixed thought size** (#tokens) and a **fixed context size** (#thoughts in the LLM context, denoted with N)

**Volume** – for a given thought t – is the number of preceding LLM thoughts that could have impacted t

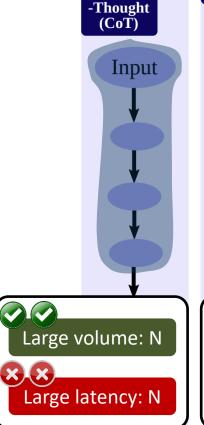




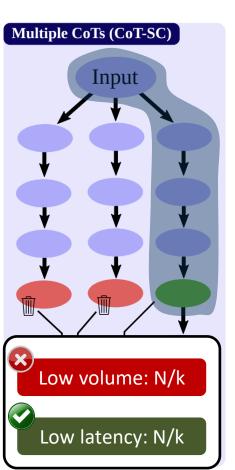


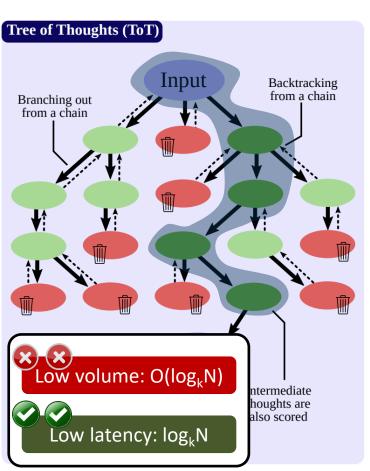
# Why Does Structured Prompting Work?

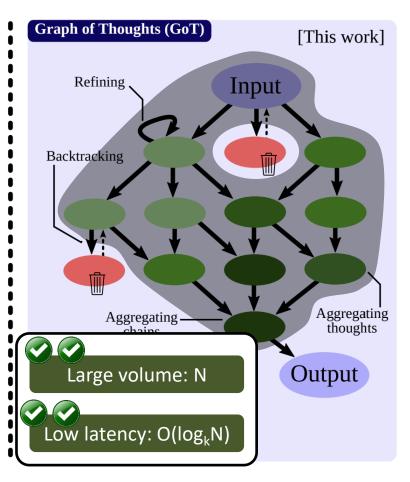
Assume a **fixed thought size** (#tokens) and a **fixed context size** (#thoughts in the LLM context, denoted with N)



Chain-of-





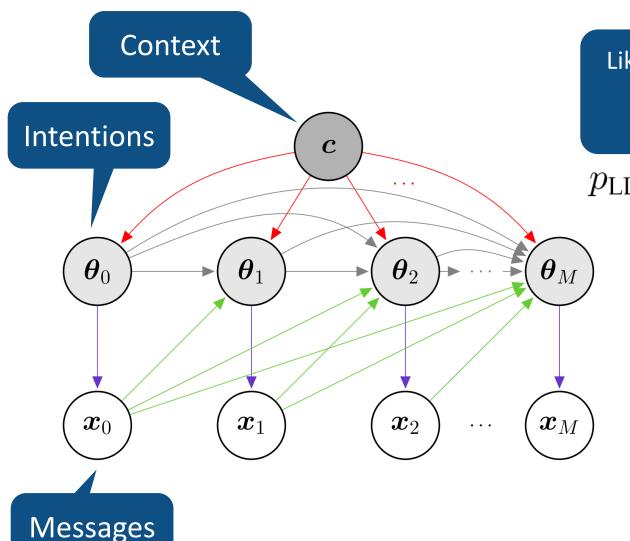








# Why Does Structured Prompting Work? Probabilistic Graphical Models [1]



Likelihood of generating a chain of thoughts, basing on a pre-prompt with input I and with N CoT in-context examples, but without access to the true context.

 $p_{\text{LLM}} \equiv p_{LLM} \left( \text{CoT} | I, \text{CoT-Examples}(N) \right)$ 

Likelihood of generating the same chain of thoughts as above, but using the true language (and context) conditioned on the same input *I* 

 $p_{\text{True}} \equiv p_{\text{True}} \left( CoT | I, \text{True-Context} \right)$ 

$$|p_{\rm LLM} - p_{\rm True}| \le \rho^N$$

"A function of the language ambiguities", < 1

[1] R. Tatunov et al. Why Can Large Language Models Generate Correct Chain-of-Thoughts? Arxiv, 30 October 2023.

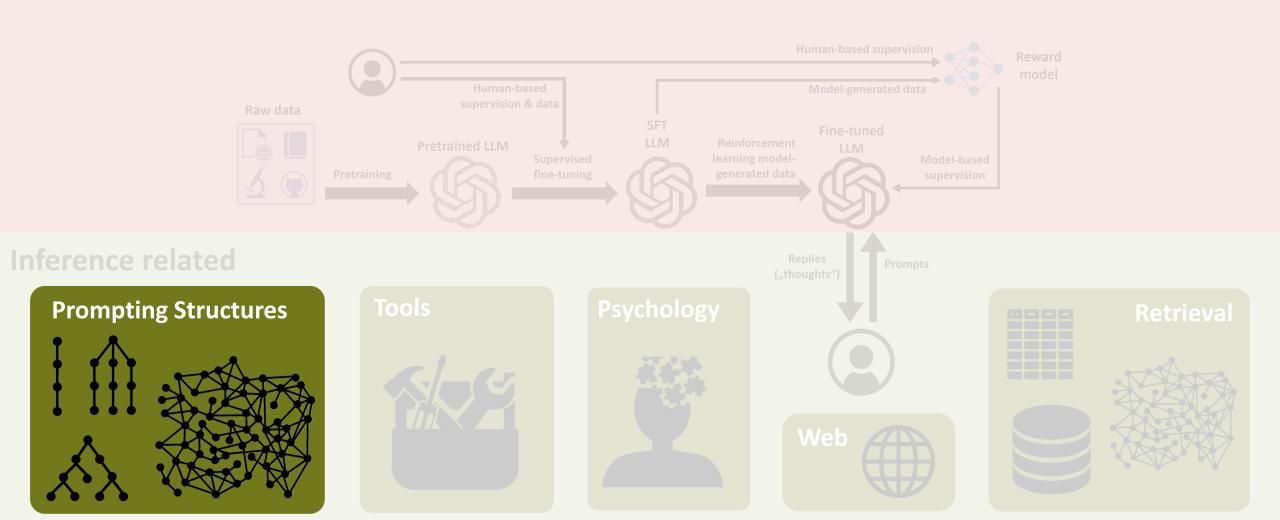






# The Emergence of the "Generative AI Ecosystem"

Training related



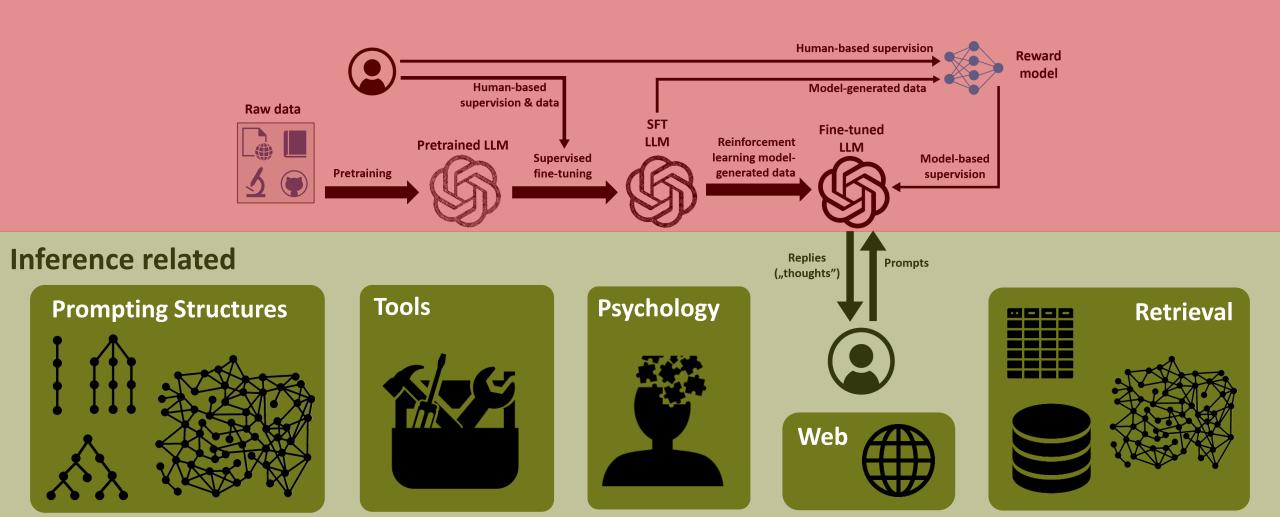






# The Emergence of the "Generative AI Ecosystem": Training

## **Training related**

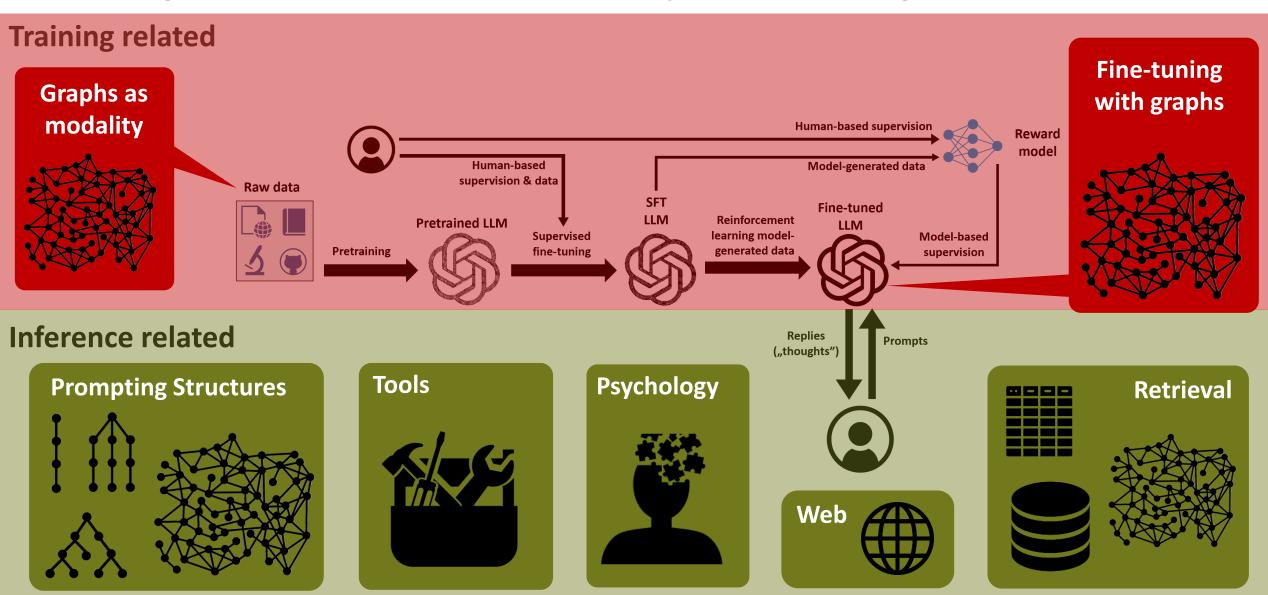








# The Emergence of the "Generative AI Ecosystem": Training



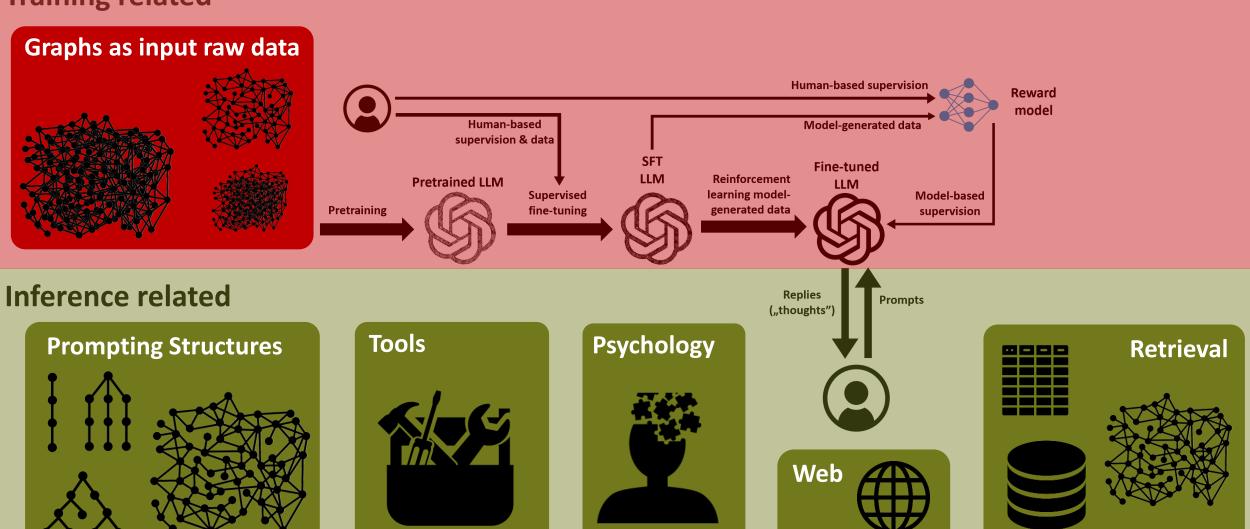






# **Graph Foundation Models & Graph Prompting**

## **Training related**









M. Besta, T. Hoefler

WITH N. BLACH, A. KUBICEK, R. GERSTENBERGER, AND MANY OTHERS

# **Graph of Thoughts: Solving Elaborate Problems with Large Language Models**













Hello. I want to sort the following input sequence of numbers: {input}



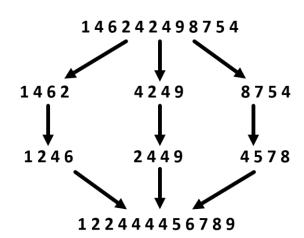


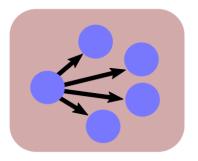


**>\_** 

<Instruction> Split the following list of 64 numbers into 4 lists of 16 numbers each, the first list should contain the first 16 numbers, the second list the second 16 numbers, the third list the third 16 numbers and the fourth list the fourth 16 numbers. Only output the final 4 lists in the following format without any additional text or thoughts!

```
{{
    "List 1": [3, 4, 3, 5, 7, 8, 1, ...],
    "List 2": [2, 9, 2, 4, 7, 1, 5, ...],
    "List 3": [6, 9, 8, 1, 9, 2, 4, ...],
    "List 4": [9, 0, 7, 6, 5, 6, 6, ...]
}} </Instruction>
```





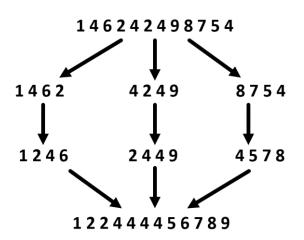


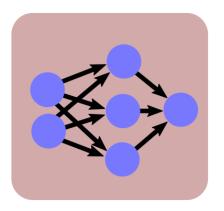




**>**\_

<Instruction> Merge the following 2 sorted lists of length {length1} each, into one sorted list of length {length2} using a merge sort style approach. Only output the final merged list without any additional text or thoughts!
</Instruction>

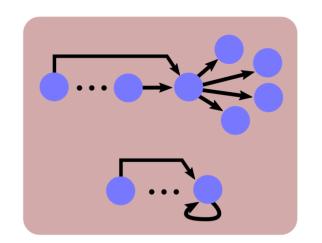


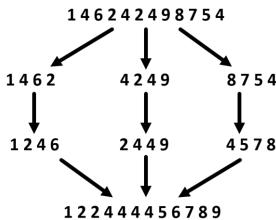












<Instruction> Sort the following list of numbers in ascending order. Output only the sorted list of numbers, no additional text.

## <*Example*>

Input: [3, 7, 0, 2, 8, 1, 2, 2, 2, 4, 7, 8, 5, 5, 3, 9, 4, 3, 5, 6, 6, 4, 4, 5, 2, 0, 9, 3, 3, 9, 2, 1]

Output: [0, 0, 1, 1, 2, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 6, 6, 7, 7, 8, 8, 9, 9, 9]

</Example>

*Input:* {input}

The input thought t

